Cisco DNA Assurance User Guide, Release 2.3.4

First Published: 2022-09-21

Last Modified: 2023-07-14

CONTENTS

New and Changed Information

• New and Changed Features in Cisco DNA Assurance, on page 1

New and Changed Features in Cisco DNA Assurance

The following table summarizes the new and changed features in the *Cisco DNA Assurance User Guide, Release 2.3.4*.

Feature	Description
Site Analytics	You can view KPI statistics for sites that do not meet the configured performance thresholds. See Monitor and Troubleshoot the Overall Health of Your Enterprise, on page 97 and Monitor and Troubleshoot Your Network Using Site Analytics, on page 183.
MS Teams Application	You can monitor and troubleshoot the health of an **MS Teams** application. See Monitor and Troubleshoot the Health of a Microsoft Teams Application, on page 147, Monitor the Health of All Applications, on page 134, and Monitor and Troubleshoot the Health of a Client Device, on page 113.
New AP-Disconnect Issue	A new global AP disconnect issue is being introduced. AP disconnect issues that happen on the same switch are aggregated and raised as a single issue with a list of affected APs. The new aggregated AP disconnect issue will be logged both on the **Device 360** window and the Global dashboard. The previous AP disconnect issue will still be logged. However, it will only appear on the **Device 360** window, not on the global **Issue** dashboard. See Issue Instance Details for AP-Disconnect Issues, on page 196.
New Charts for Embedded Cisco Wireless Controllers	You can choose to display a number of new charts for embedded wireless controllers in the **Device 360** window. New charts include KPIs, such as Air Quality, Channel Utilization, Total Frame Errors, and so on. See Monitor and Troubleshoot the Health of a Device, on page 74.
RF Charts for APs	You can choose to display RF charts for APs in the **Device 360** window. New charts include KPIs, such as Throughput, Client Count, Channel Utilization, Top SSIDs by Client/Packet Count, and so on. See Monitor and Troubleshoot the Health of a Device, on page 74.

Feature	Description
New Global Client Counts for Embedded Cisco Wireless Controllers	The **Device 360** window for an embedded wireless controller displays the following new counts in the Client Count chart: **Anchor entries**: Counts for clients who have recently roamed to another wireless controller. The client is no longer connected to the wireless controller that is reporting this data. **Foreign entries**: Counts for clients who recently roamed to the wireless controller. The client connected to thewireless controller that is reporting this data, but may not be currently connected. **Local entries**: Counts for clients that are currently connected to the wireless controller. **Idle State entries**: Counts for clients who are in a temporary idle state.
New BGP Down Issue	A new BGP Down issue is added to Router, Core, Distribution, and Access issues. The BGP Down issue is triggered when the BGP connectivity is down with its neighbor. You can modify the issue trigger condition to a maximum time duration of 10 minutes. See Core, Distribution, and Access Issues, on page 214 and Router Issues, on page 212.

Automatic Issue Resolution	With this release, the system automatically resolves issues for the following issue types:
	
	   • Switch Power Failure
	
	   • Switch Fan Failure
	
	See Automatic Issue Resolution, on page 208.

Endpoint Events	The **Events** dashboard in Assurance provides a more contextual view of endpoint events. Instead of having to search for events triggered by endpoints that are connected to the devices involved in an event, Assurance provides these details for you. See View and Manage Events, on page 227.
Client Dashboard Enhancements	In the Assurance **Client** dashboard, you can exclude clients for specific Cisco Wireless Controllers using the **Excluded Clients** option in the **Client Devices** dashlet. In the **Client 360** window, you can exclude the device for specific wireless controllers using the hyperlink for the **Excluded** status in the **Device Info** tab under **Client Details**. See Monitor and Troubleshoot the Health of All Client Devices, on page 101, Configure Excluded Clients, on page 112 and Monitor and Troubleshoot the Health of a Client Device, on page 113.
PoE Power Usage Dashlet Enhancements	In the Assurance **PoE** dashboard, the power usage dashlet is enhanced with **Allocation** and **Consumption** views. The latest and trend tabs display the device power consumption and allocation data based on the selected view. See Monitor PoE-Capable Devices in Your Network, on page 270.
Client 360 Enhancements for Fabric	With this release, client device details include fabric attributes such as **Security Group (Tag Value)** and **Bridge-Mode Virtual Machine**. See Monitor and Troubleshoot the Health of All Client Devices, on page 101 and Monitor and Troubleshoot the Health of a Client Device, on page 113.

Feature	Description
Cisco AI Network Analytics: Network Heatmap Enhancements	With this release, you can generate **Network Heatmaps** for **Switches**. You can filter the heatmap data based on the KPIs and on a specific **Switch Family** for direct comparisons.
	The following temperature KPIs are supported for switches:
	• **Temperature: All Sensors**
	• **Temperature: Core**
	• **Temperature: Hotspot**
	• **Temperature: Inlet**
	• **Temperature: Outlet**
	See Compare Access Points and Switches in Network Heatmaps, on page 292.
6-GHz Radio Band Support	The 6-GHz radio band support is added to the **Enhanced RRM** dashboard.
	See View the RF Network Using the Enhanced RRM Dashboard, on page 303.
RF Simulator	Using the AI RF Simulator, you can simulate changes to the current RF profile configurations and visualize the projected outcome against the enhanced RRM dashlets on the **Enhanced RRM** dashboard.
	See View the RF Network Using the Enhanced RRM Dashboard, on page 303.

CHAPTER **2**

Cisco DNA Assurance Overview

Cisco DNA Assurance Overview

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

Assurance provides 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 describe the Assurance architecture:

Figure 1: Assurance Architecture
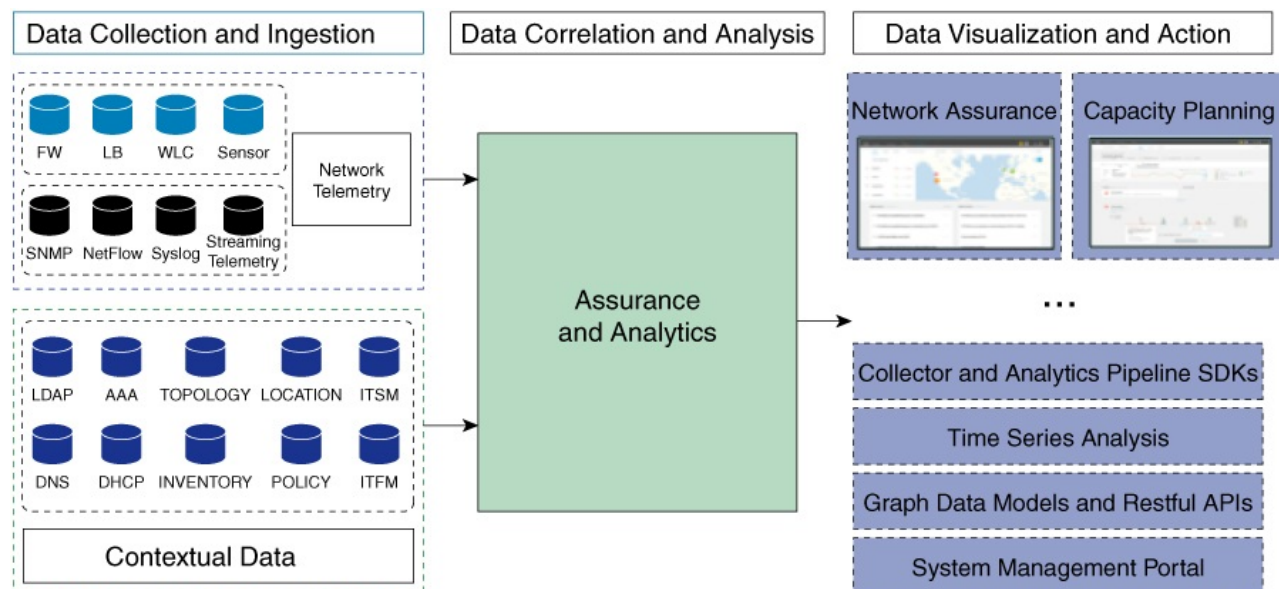
- **Data Collection and Ingestion**: Assurance leverages streaming technologies to collect a variety of network telemetry and contextual data in real time.

- **Data Correlation and Analysis**: As and when data is ingested, Assurance correlates and analyzes the data.

- **Data Visualization and Action**: Data is stored in databases and exposed through APIs to Assurance as well as other applications for capacity planning. Assurance is an open system that provides the following:

  - Collector and analytics pipeline SDKs

  - Time-series analysis

  - Graph data models and restful APIs

  - System management portal

IPv6 Address Support

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

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

User Profile Roles and Permissions

Cisco DNA Center supports role-based access control (RBAC). The roles assigned to a user profile define the capabilities that a user has permission to perform. Cisco DNA Center has three main default user roles:

- SUPER-ADMIN-ROLE

- NETWORK-ADMIN-ROLE

- OBSERVER-ROLE

The SUPER-ADMIN-ROLE gives users broad capabilities and permits them to perform all actions in the Cisco DNA Center GUI, including creating custom roles and assigning them to user profiles. The NETWORK-ADMIN-ROLE and the OBSERVER-ROLE have more limited and restricted capabilities in the Cisco DNA Center GUI.

If you're unable to perform an action in Cisco DNA Center, the reason might be that your user profile is assigned a role that doesn't permit it. For more information, check with your system administrator or see the *Cisco DNA Center Administrator Guide*.

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 (existing deployment), start by running Discovery. After you run Discovery, all your devices are displayed on the **Inventory** window. For more information, see Basic Setup Workflow, on page 13.

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

Cisco AI Network Analytics Overview

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
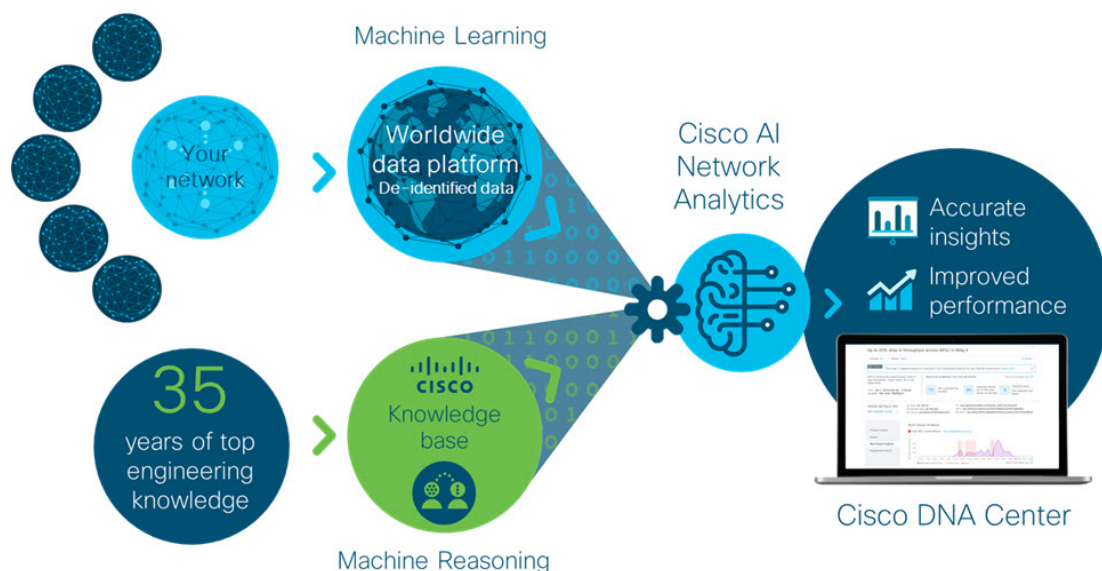
Cisco AI Network Analytics consists of the following:

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

Figure 3: Cisco AI Network Analytics Features
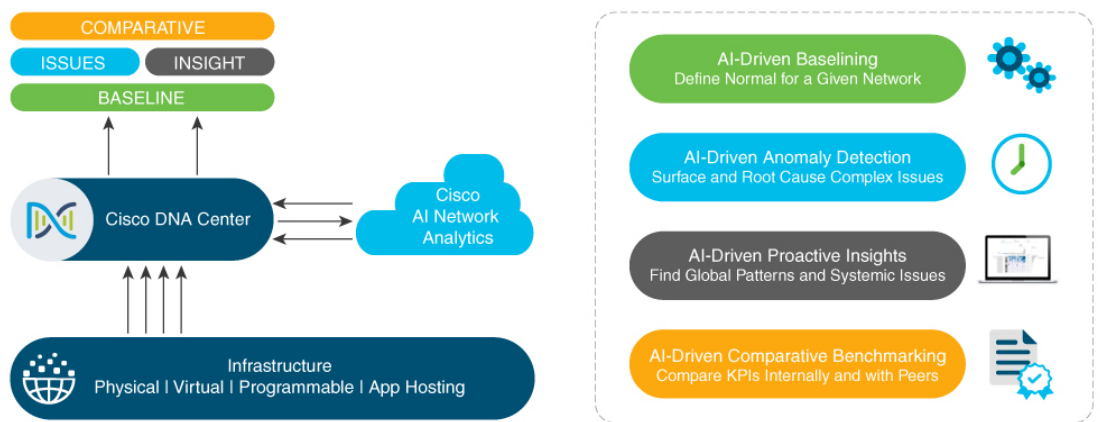
Cisco AI Network Analytics provides the following:

- **Cloud-Based Infrastructure**: Network events information is deidentified 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 deidentified network event data and brings the issues and overall insights back to Cisco DNA Center.

- **Intelligent Issue Detection and Analysis**, which includes:

  - **AI-Driven Baselining**: Baselining is a method used to analyze network dynamics to extract behavioral patterns that help define what is the *normal* (baseline) behavior for that specific network. The actual network performance is then compared with that baseline.

    Cisco AI Network Analytics uses the most advanced machine learning techniques to define the baseline that is relevant to your specific network and sites with the current conditions. With this information, Cisco AI Network Analytics is able to define what is normal for each network and site at a specific moment, and identify the most important issues.

  - **AI-Driven Anomaly Detection**: Detect anomalies to determine their root causes and ease troubleshooting.

    Cisco AI Network Analytics can detect the following types of AI-driven issues:

    - **Connection Issues** (onboarding issues): Excessive Time, Excessive Failures, Excessive DHCP Time, Excessive DHCP Failures, Excessive AAA Time, Excessive AAA Failures, Excessive Association Time, and Excessive Association Failures.

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

- **Trends and Insights**, which includes:

  - **Trend Deviations**: Determine global patterns (trends) and deviations to provide system-generated insights.

  - **AP Performance Advisories**: Detect APs that have a consistently poor client experience, and provide a root cause and suggested actions.

- **Comparative Benchmarking**, which includes:

  - **AI-Driven AP Comparisons in Network Heatmaps**: Compare all of the APs in your network for a given month in a heatmap to spot trends and gain insights.

  - **AI-Driven Peer Comparisons**: Determine how your network is performing in comparison to your peer networks for a selected Key Performance Indicator (KPI).

  - **AI-Driven Network Comparisons**: Determine how a network (such as sites, buildings, AP models, client types) is performing compared to another network for a selected KPI.

Cisco AI Network Analytics Benefits

Cisco AI Network Analytics provides the following benefits:

- **More Visibility**: Each network is unique, with the network environment always changing. Cisco AI Network Analytics continuously collects the relevant data from the local networks, correlates the data against the aggregate de-identifed data set, and then leverages sophisticated machine learning models to create baselines that are relevant to specific networks and sites. These baselines learn and adapt as the network environments change and as the number of devices, users, and applications evolve.

- **Greater Insight**: Cisco AI Network Analytics uses machine learning to correlate the immense amount of data that is coming from the network against the individualized network baselines, to uncover the issues that can have the greatest impact on the network. This improves issue relevancy. Cisco AI Network Analytics discovers trends and patterns in the network behavior, so that IT can identify issues before they become a problem.

- **Guided Action**: Cisco AI Network Analytics uses machine learning algorithms and automated workflows to perform logical troubleshooting steps, which enable an engineer to execute and resolve an issue. This helps IT detect issues and vulnerabilities, analyze the root causes, and quickly execute corrective actions.

Cisco AI Network Analytics Licensing and Deployment

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

Deploying Cisco AI Network Analytics requires a working instance of 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 deidentified before it is sent to the cloud. Results and insights are returned by the Cisco AI Network Analytics cloud services, and are displayed after decryption, directly into the Assurance user interface. For more information, see "Addendum 1 Cisco AI Network Analytics" in the Cisco DNA Center Privacy Data Sheet.

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

Set Up Cisco DNA Center to Use Assurance

Limitations and Restrictions of Assurance

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

Basic Setup Workflow

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

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

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
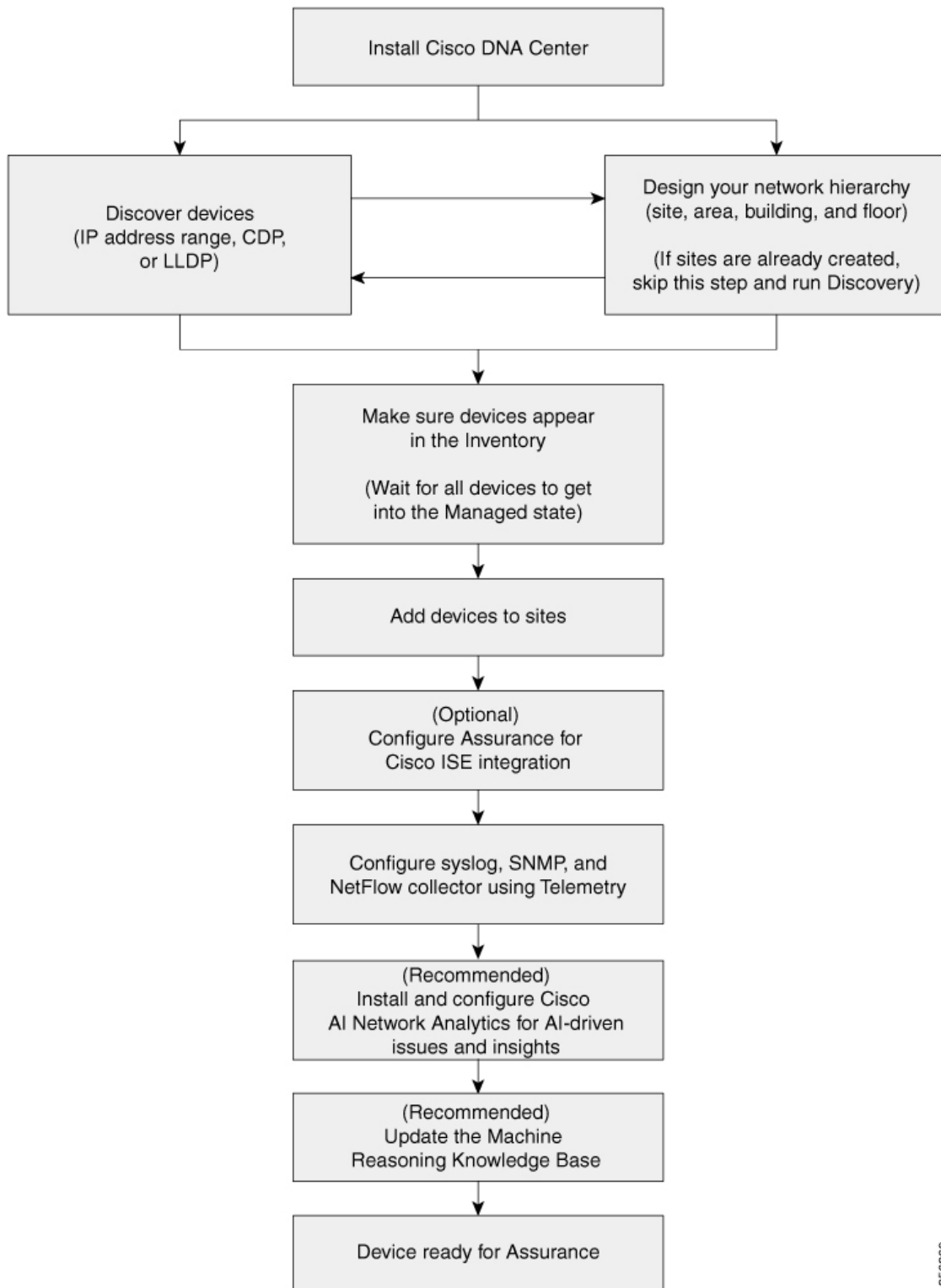
Before you begin

See Limitations and Restrictions of Assurance, on page 13.

Step 1 Install Cisco DNA Center.

See the *Cisco DNA Center Installation Guide*.

Step 2 Do the following in any order:

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

  See Discover Your Network Using an IP Address Range, on page 25, Discover Your Network Using CDP, on page 23 and Discover Your Network Using LLDP, on page 26.

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

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

  See Create a New Network Hierarchy, on page 30 or Use an Existing Cisco Network Hierarchy, on page 33.

  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 50.

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

Step 4 Add devices to sites.

See Add a Device to a Site, on page 55.

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

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

See About Cisco ISE Configuration for Cisco DNA Center, on page 56.

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

See Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 60.

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

See Configure Cisco AI Network Analytics, on page 61.

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 64.

Step 10   Start using the Assurance application.

Discover Devices

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

Discovery Overview

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

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

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 loopback address.

> **Note**   For Cisco SD-Access Fabric and Cisco DNA Assurance, we recommend that you specify the device 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, such as Hot Standby Router Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP), the device might be discovered and added to the inventory along with its floating IP address. Later, if HSRP or VRRP fails, the IP address might be reassigned to a different device. This situation can cause issues with the data that 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 *Cisco DNA Center Compatibility Matrix*.

- Understand that the preferred network latency between Cisco DNA Center and devices is 100 ms round-trip time (RTT). (The maximum latency is 200 ms RTT.)

- Ensure that at least one SNMP credential is configured on your devices for use by Cisco DNA Center. At a minimum, this can be an SNMPv2C read credential.

- Configure SSH credentials on the devices you want Cisco DNA Center to discover and manage. Cisco DNA Center discovers and adds a device to its inventory if at least one of the following criteria is met:

  - The account that is being used by Cisco DNA Center to SSH into your devices has privileged EXEC mode (level 15).

  - You configure the device's enable password as part of the CLI credentials configured in the Discovery job. For more information, see Discovery Configuration Guidelines and Limitations, on page 18.

Preferred Management IP Address

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

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

- If the device has one loopback interface, Cisco DNA Center uses that loopback interface IP address.

- If the device has multiple loopback interfaces, Cisco DNA Center uses the loopback interface with the highest IP address.

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

- If there are no Ethernet interfaces, Cisco DNA Center uses the serial interface with the highest IP address.

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

Discovery Configuration Guidelines and Limitations

The following are the guidelines and limitations for Cisco DNA Center to discover your Cisco Catalyst 3000 Series Switches and Catalyst 6000 Series Switches:

- Configure the CLI username and password with privileged EXEC mode (level 15). These credentials are 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 windows will not display any data.

Discovery Credentials

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

- Network devices: CLI and SNMP credentials.

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

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

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

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

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

- Discover Your Network Using CDP, on page 23
- Discover Your Network Using an IP Address Range, on page 25
- Discover Your Network Using LLDP, on page 26

Table 1: CLI Credentials

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

Table 2: SNMPv2c Credentials

Field	Description
Read	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Read Community**: Read-only community string password used only to view SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.
Write	• **Name/Description**: Name or description of the SNMPv2c settings that you are adding. • **Write Community**: Write community string used to make changes to the SNMP information on the device. **Note** Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 3: SNMPv3 Credentials

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

Field	Description
Mode	Security level that an SNMP message requires. Choose one of the following modes: • **Authentication and Privacy**: Provides both authentication and encryption. • **Authentication, No Privacy**: Provides authentication, but does not provide encryption. • **No Authentication, No Privacy**: Does not provide authentication or encryption.
Auth. Type	Authentication type to be used. (Enabled if you select **Authentication and Privacy** or **Authentication, No Privacy** as **Mode**.) Choose one of the following authentication types: • **SHA**: Authentication based on HMAC-SHA. • **MD5 (not recommended)**: Authentication based on HMAC-MD5.
Auth. Password	SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least eight characters in length. **Note** • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center. • Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy Type	Privacy type. (Enabled if you select **Authentication and Privacy** as **Mode**.) Choose one of the following privacy types: • **AES128**: 128-bit CBC mode AES for encryption. • **CISCOAES192**: 192-bit CBC mode AES for encryption on Cisco devices. • **CISCOAES256**: 256-bit CBC mode AES for encryption on Cisco devices. **Note** • Discovery and Inventory features support only CISCOAES192 and CISCOAES256 privacy types. • Cisco DNA Assurance does not support any of these privacy types.

Field	Description

Privacy Password	SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support encryption standards. Passwords (or passphrases) must be at least eight characters long.
	
	Note
	    • Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.
	
	    • Passwords are encrypted for security reasons and are not displayed in the configuration.

Table 4: SNMP Properties

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

Table 5: HTTP(S) Credentials

Field	Description
Type	Specifies the kind of HTTPS credentials you are configuring. Valid types are **Read** or **Write**.

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

Table 6: NETCONF Setting

Field	Description
Port	Port on the device. You can use one of the following ports: • Port 830 (default). • Any other port that is available on the device. • A custom port that Cisco DNA Center configures. (You can use a custom port only if Device Controllability is enabled. For more information, see the Device Controllability section in the *Cisco DNA Center Administrator Guide*.)

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 25 and Discover Your Network Using LLDP, on page 26.

Note
- The Discovery function requires the correct SNMP Read Only (RO) community string. If an SNMP RO community string is not provided, as a *best effort*, the Discovery function uses the default SNMP RO community string, public.

- CLI credentials are not required to discover hosts; hosts are discovered through the network devices to which they are connected.

Before you begin

- Enable CDP on your network devices.

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

- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Step 1   Click the menu icon (≡) and choose **Tools** > **Discovery**.

Step 2   In the **Discovery** window, click ⊕ Add Discovery .
The window appears.

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

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

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

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

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

You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 0 to 32.

d) Click ⊕.

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

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

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

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

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

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

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

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

Step 5   Expand the **Credentials** area and choose any of the global credentials that have already been created or configure your own.

If you want to use existing credentials, make sure that to select them. If you don't want to use a credential, deselect it.

Step 6   To configure your own credentials, click **Add Credentials**.

You must configure CLI and SNMP v2c credentials. All other credentials are optional. For field information, see Discovery Credentials, on page 18.

To save credentials for *only* the current job, click **Save**. To save them for the current job and future jobs, check the **Save as global settings** check box and then click **Save**.

Step 7   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 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 8   Click **Start**.

Note	• You can configure up to five devices to be scheduled with recurrence.
	• The recurring discovery discovers only new devices. If a device is already present in Cisco DNA Center, it is not updated as part of discovery.

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

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

Discover Your Network Using an IP Address Range

You can discover devices using an IP address range, CDP, or LLDP. This procedure shows you how to discover devices and hosts using an IP address range. For more information about the other Discovery methods, see Discover Your Network Using CDP, on page 23 and Discover Your Network Using LLDP, on page 26.

Before you begin

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

Step 1 Click the menu icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

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

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

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

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

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

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

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

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

d) (Optional) In the **Subnet Filter** field, enter an IP address/range or subnet to exclude from the Discovery scan. You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless interdomain routing (CIDR) address (*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 0 to 32.

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

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

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

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

Step 5 Expand the **Credentials** area and choose any of the global credentials that have already been created or configure your own.

If you want to use existing credentials, make sure that to select them. If you don't want to use a credential, deselect it.

Step 6 To configure your own credentials, click **Add Credentials**.

You must configure CLI and SNMP v2c credentials. All other credentials are optional. For field information, see Discovery Credentials, on page 18.

To save credentials for *only* the current job, click **Save**. To save them for the current job and future jobs, check the **Save as global settings** check box and then click **Save**.

Step 7 (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 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 8 Click **Start**.

Note	• You can configure up to five devices to be scheduled with recurrence.
	• The recurring discovery discovers only new devices. If a device is already present in Cisco DNA Center, it is not updated as part of discovery.

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 23 and Discover Your Network Using an IP Address Range, on page 25.

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

Before you begin

• Enable LLDP on your network devices.

• Configure your network devices, as described in Discovery Prerequisites, on page 17.

> • Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Step 1 Click the menu icon (≡) and choose **Tools** > **Discovery**.
The **Discovery** window appears with dashlets.

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

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

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

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

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

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

   You can enter addresses either as an individual IP address (*x.x.x.x*) or as a classless inter-domain routing (CIDR) address (*x.x.x.x/y*), where *x.x.x.x* refers to the IP address and *y* refers to the subnet mask. The subnet mask can be a value from 0 to 32.

d) Click ⊕.

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

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

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

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

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

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

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

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

Step 5 Expand the **Credentials** area and choose any of the global credentials that have already been created or configure your own.

   If you want to use existing credentials, make sure that to select them. If you don't want to use a credential, deselect it.

Step 6 To configure your own credentials, click **Add Credentials**.

   You must configure CLI and SNMP v2c credentials. All other credentials are optional. For field information, see Discovery Credentials, on page 18.

   To save credentials for *only* the current job, click **Save**. To save them for the current job and future jobs, check the **Save as global settings** check box and then click **Save**.

Step 7   (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 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 8   Click **Start**.

Note	• You can configure up to five devices to be scheduled with recurrence.
	• The recurring discovery discovers only new devices. If a device is already present in Cisco DNA Center, it is not updated as part of discovery.

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

The following sections provide information about how to manage the Discovery jobs.

Stop and Start a Discovery Job

Step 1   Click the menu icon (≡) and choose **Tools** > **Discovery**.

Step 2   In the **Discovery** window, click **View All Discoveries**.

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

   a)   In the left pane, click a Discovery job.

   b)   In the bottom pane, click **Stop**.

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

   a)   In the left pane, click a Discovery job.

   b)   In the bottom pane, click **Re-discover**.

Clone a Discovery Job

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

Before you begin

You should have run at least one Discovery job.

Step 1   Click the menu icon (≡) and choose **Tools** > **Discovery**.

Step 2   In the **Discovery** window, click **View All Discoveries**.

Step 3 In the left pane, click a Discovery job.

Step 4 In the bottom pane, click **Copy & Edit**.

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

Step 5 (Optional) To change the name of the Discovery job, replace the default name in the **Discovery Name** field with a new name.

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

Delete a Discovery Job

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

Step 1 Click the menu icon (≡) and choose **Tools** > **Discovery**.

Step 2 In the **Discovery** window, click **View All Discoveries**.

Step 3 In the left pane, click the Discovery job that you want to delete.

Step 4 In the bottom pane, click **Delete**.

Step 5 Click **OK** to confirm.

View Discovery Job Information

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

Before you begin

Run at least one Discovery job.

Step 1 Click the menu icon (≡) and choose **Tools** > **Discovery**.

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

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

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

- **Discovery Details**: Displays the parameters that were used to run the Discovery job. Parameters include attributes such as the CDP or LLDP level, IP address range, and protocol order.

- **Credentials**: Provides the names of the credentials that were used.

- **History**: Lists each Discovery job that was run, including the time the job started, and whether any devices were discovered.

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

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

Design Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations. The hierarchical organization enables you to easily apply design settings or configurations to a specific hierarchical element. For example, you can apply design settings to an entire area or to only a floor.

You can name hierarchical elements to help you identify where to apply design settings later.

The hierarchical elements that you can create have rules that dictate under which elements they can reside and which elements can reside under them.

- **Global**: Default element under which all other hierarchical elements reside. are the only elements that can reside directly under **Global**.

- **Areas** and **Sites**: Areas and sites reside under **Global** or under other areas or sites. They do not have a physical address. As the largest element, they identify a geographic region. They provide a way to group areas and sites.

- **Buildings**: Buildings reside under areas or sites. When you create a building, you need to specify a physical address or latitude and longitude coordinates. Buildings can't contain areas. However, they can contain floors.

- **Floors**: Floors reside under buildings. You can add floors to buildings with or without maps that contain various building components, like walls and windows. If you decide to use floor maps, you can manually create them or import them from files, such as DXF, DWG, JPG, GIF, PNG, or PDF file types. Then you can position your wireless devices on the floor maps to visualize your wireless network coverage.

  You can change the site hierarchy for unprovisioned devices while preserving AP locations on floor maps. Note, however, that you can't move an existing floor to a different building.

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

- Create a new network hierarchy. For more information, see .

- Import an existing network hierarchy from Cisco Prime Infrastructure or Ekahau Pro. For more information, see the *Cisco DNA Center User Guide*..

Create a New Network Hierarchy

Create a new network hierarchy by creating new sites (or areas), building, and floors.

Create, Edit and Delete a Site

Cisco DNA Center allows you to easily define physical sites and then specify common resources for those sites. The **Design** area uses a hierarchical format for intuitive use, while eliminating the need to redefine the

same resource in multiple places when provisioning devices. By default, there is one site called **Global**. You can add more sites, buildings, and areas to your network hierarchy. You must create at least one site before you can use the provision features.

Step 1   Click the menu icon (☰) and choose **Design** > **Network Hierarchy**.

A world map appears in the right pane.

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

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

Add, Edit, and Delete a Building

Step 1   Click the menu icon (☰) and choose **Design** > **Network Hierarchy**.

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

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

Add, Edit, and Delete a Floor

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

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

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

Step 1 Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

Action	Steps
Add a basic floor.	**a.** In the left pane, hover your cursor over the ellipsis ⬤⬤⬤ next to the desired building and choose **Add Floor**. **b.** In the **Floor Name** field, enter a name for the floor. The **Floor Name** field has the following restrictions: • The floor name cannot exceed 40 characters. • Special characters & > < ? ' " / [ ] aren't allowed. **c.** If you have wireless devices, for the **Type (RF Model)** drop-down list, choose the RF model to apply to the floor. The RF model determines how the RF is calculated when computing 2D and 3D heatmaps that show the relative intensity of the RF signals in the coverage area. **d.** Configure the **Floor Number**, **Floor Type** and **Floor Thickness** fields. The floor type and thickness are used when calculating a heatmap for wireless devices. **e.** Skip uploading a floor map image in **Floor Image** area. **f.** Configure map dimensions in the **Width**, **Length**, and **Height** fields. **g.** Click **Add**.
Edit a floor.	**a.** In the left pane, hover your cursor over the ellipsis ⬤⬤⬤ next to the floor and choose **Edit Floor**. **b.** In the **Edit Floor**dialog box, make the necessary changes. **c.** Click **Update** to save the changes.
Delete a floor.	**a.** In the left pane, hover your cursor over the ellipsis ⬤⬤⬤ next to the floor and choose **Delete Floor**. **b.** Click **Ok**.

Use an Existing Cisco Network Hierarchy

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

The following information is available for you to re-create your network hierarchy:

• **Site Hierarchy**: Your existing site hierarchy is downloaded in a CSV file format. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.

• **Map Archive**: Map information is downloaded as a map archive in a TAR file format. The map archive file contains data such as the date and time, number of floors, and APs. Depending on what you choose to download, the map archive can also include map information, such as floor dimensions (length, width, and height) and details about the APs and overlay objects that have been placed on the floor maps. You can also choose to download calibration information, such as the RF attenuation model that has been applied to each floor.

You can choose to base the map archive on the global hierarchy or the hierarchy of a single site, building, or floor, as follows:

- **Site**: The chosen site and all of its subsites, buildings, and floors are exported.

- **Building**: The chosen building and all of its floors are exported.

- **Floor**: The chosen floor is exported.

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

FIPS mode has the following impact on the export and import of map archives.

If FIPS mode is *enabled*:

- Exported map archives are unencrypted.

- Only unencrypted map archives can be imported.

If FIPS mode is *disabled*:

- Exported map archives are encrypted.

- Both encrypted and unencrypted map archives can be imported.

For details, see the *Cisco DNA Center User Guide*.

Export Your Site Hierarchy from Cisco Prime Infrastructure

You can export your site hierarchy from Cisco Prime Infrastructure in a CSV file format. The CSV file contains details such as site names, parent hierarchy, number of floors, location, and site address.

Before you begin

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

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

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

Step 3 In the **Export Groups** dialog box, click the **APIC-EM** radio button.

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

The CSV file is downloaded.

Export Your Map Archive from Cisco Prime Infrastructure

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

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

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

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

Step 3 Check the check box adjacent to a specific site, campus, building, or floor that you want to export. Alternatively, check the **Select All** check box to export all the maps.

Step 4 Select at least one of the following options:

- **Map Information**: Click the **On** button to export floor dimensions (length, width, and height) and details about the APs and overlay objects that have been placed on the floor maps.

- **Calibration Information**: Click the **On** button to export the RF attenuation model that has been applied to each floor. It is a good practice to export the existing calibration data from Cisco Prime Infrastructure. Otherwise, you must re-enter the calibration details manually.

  If you choose to include calibration information, you also need to specify whether to include information for the selected maps or all the information, as follows:

  - **Calibration Information for selected maps**: Calibration information for the selected site maps is exported.

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

Step 5 Click **Generate Map Archive**.

The following message shows the progress of the operation:

```
Exporting data is in progress
```

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

Step 6 Click **Done**.

Import Your Site Hierarchy to Cisco DNA Center

You can import a site hierarchy that you exported from Cisco Prime Infrastructure as a CSV file. For information about exporting the site hierarchy, see the *Cisco DNA Center User Guide*.

Before you begin

- Make sure that you have Cisco Wireless Controllers and APs in your Cisco DNA Center inventory. If not, discover them using the **Discovery** feature.

- Add and position APs on a floor map.

- If you manually created sites in Cisco DNA Center that are present in Cisco Prime Infrastructure, you must remove them from Cisco DNA Center before you can import them.

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

Step 2   From the map tool bar, click **Import** and choose **Import Sites**.

Step 3   In the dialog box, click one of the following radio buttons:

- **Merge with Existing Sites**: The downloaded site information is combined with the existing site information.

- **Overwrite Existing Sites**: If the same site already exists in Cisco DNA Center, the existing site information is overwritten with the downloaded site information.

Step 4   In the dialog box, drag and drop your CSV file into the download area. Alternatively, you can click **Choose a file** and navigate to where your CSV file is located, then click **Upload**.

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

Import Your Map Archive to Cisco DNA Center

You can import a map archive TAR file into Cisco DNA Center. For example, you can upload the TAR file that you exported from Cisco Prime Infrastructure.

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

For information about exporting site hierarchy, see Export Your Map Archive from Cisco Prime Infrastructure, on page 35.

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

Step 4   Click **Import**.

The map archive file is imported.

Use an Existing Ekahau Network Hierarchy

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

Export an Ekahau Project from Cisco DNA Center

You can export your network hierarchy from Ekahau Pro and import it into Cisco DNA Center for further planning.

Before you begin

Cisco DNA Center supports Ekahau Pro tool version 10.2.

Step 1 In the Ekahau Pro tool, plan the floor layout:

- Create buildings and floors.

  It is not mandatory to create buildings in the Ekahau Pro tool.

- Import the floor plan.

- Add the planned APs or hypothetical APs.

- Add building coordinates.

- Define the site name.

  The AP name that you provide here will be used to update the AP name on the Cisco Wireless Controller during the wireless controller configuration.

- Add obstacles.

- Export the project.

Step 2 Deploy the planned APs at locations designed on the floor layout.

- The physical AP is mounted at the designed location that is specified on the floor layout. The MAC address of the planned AP is updated with the MAC address of the physical AP.

- The physical AP is connected to the VLAN of the intended wireless controller.

Step 3 In Cisco DNA Center, configure the Cisco Wireless Controller .

   a. Discover the Cisco Wireless Controller and APs in your network by running the **Discovery** job, so that the discovered wireless controllers and APs are listed on the **Inventory** window.

   b. Update the AP name on the wireless controller with the AP name given in the Ekahau Pro project during the floor planning.

Step 4 Import the Ekahau project into Cisco DNA Center.

Step 5   Map the planned APs to real APs in Cisco DNA Center.

Import an Ekahau Project to Cisco DNA Center

Step 1   Click the menu icon (☰) and choose **Design** > **Network Hierarchy**.

Step 2   Design your network hierarchy by adding sites, buildings, and floors.

         Note   For more information, see Create, Edit and Delete a Site, on page 30, Add, Edit, and Delete a Building, on page 31, and Add, Edit, and Delete a Floor, on page 32.

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

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

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

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

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

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

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

        The following attempts are made to map the planned APs to real APs:

           • If the newly discovered APs match the planned AP, the planned AP is replaced with the discovered real AP.

           • If a planned AP remains unmapped, you can manually replace the planned AP with the real AP, providing reasons for the failure.

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

        The **Assign Planned APs** panel appears.

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

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

Step 9   Click **Save**.

Import an Ekahau Site Survey to Cisco DNA Center

You can upload an Ekahau site survey to create the buildings and floors in your network hierarchy. The site survey includes information about wireless devices, including the site, building, and floor to which it is assigned and its position on the floor map. However, it doesn't include the AP antenna information. So, you need to upload this information separately using a CSV file.

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

Figure 5: The CSV template file contains the following fields and defaults:

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

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

The naming convention is AP, followed by the last four digits of the AP's MAC address, for example, AP-c4:e0. Using this information, Cisco DNA Center attempts to match the provided digits with the last four digits of an AP's Ethernet MAC or radio MAC address. If this information isn't available or a match is unsuccessful, Cisco DNA Center attempts to match AP names.

Step 1 Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

Alternatively, you can hover your cursor over the ellipsis ••• next to the parent site or **Global** in the left pane, and choose **Add Area**. For more information, see Create, Edit and Delete a Site, on page 30.

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

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

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

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

Step 6 Click **Import**.

After the files are successfully downloaded, a success message is displayed.

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

Hover the cursor over a device to view its details.

Configure 2D Floor Map Devices and Overlay Objects

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

Devices

- **APs**: An access point (AP) serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In 2D maps, an AP represents an actual, installed device. For a list of APs that Cisco DNA Center supports, see the *Cisco DNA Center Compatibility Matrix*.

- **Planned APs**: Planned APs are representations of APs that have not been installed yet. By placing planned APs on a map, you can envision your wireless network RF coverage and make changes before you actually install the APs.

- **Sensors**: A sensor is a dedicated Cisco Aironet 1800S Active Sensor that gets bootstrapped using Cisco PnP. After it obtains the Assurance server reachability details, it communicates directly with the Assurance server. For more details, including information about sensor tests, see the Manage Sensors and Sensor-Driven Tests, on page 235.

Overlay Objects

- **Coverage Areas**: By default, any area defined as part of a floor map is considered as a wireless coverage area. However, if you have a building that is nonrectangular or you want to mark a nonrectangular or polygon-shaped area on a floor, you can use the **Coverage Areas** drawing tool to create a coverage area.

- **Openings**: An opening, also called an atrium, is an open-air or skylight-covered area within a building. An opening can extend through multiple floors and can affect wireless signal coverage areas.

- **Location Regions**: Location regions define areas that are included in or excluded from the computation of heatmaps. Inclusion areas are included in the calculations. and exclusion areas are not included. For example, you might want to exclude areas such as openings, atriums, or stairwells within a building, but include a work area, such as cubicles, labs, or manufacturing floors.

- **Walls**: Walls are exterior or interior vertical structures in a building and can be made of different materials and thicknesses. As such, they affect how heatmaps are calculated.

- **Shelving Units**: Shelving units are obstacles that affects signal attenuation. An example of a location with shelving units would be a high-ceiling warehouse.

- **Markers**: A marker identifies a location on a map. When you create a marker, you can name it and position it to help you identify it later.

- **GPS Markers**: When integrated with Cisco DNA Center, location services, such as Cisco DNA Spaces or Cisco Connected Mobile Experiences (CMX), use GPS markers to calculate the approximate geographical location of clients.

- **Align Points**: Align points are markers that are used to position multiple floors that have different physical shapes. In 3D maps, floors are aligned at the top-left corner of the map (point 0,0). If you manage each floor independently, the misalignment is not a problem. However, to use some of the features of 3D maps, the floors need to be aligned as they are in reality. To compensate this misalignment, you can

insert one or more align points on two or more floors, so that the floors align properly one on top of the other in a 3D map.

Add, Position, Edit, and Remove APs

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

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

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

Action	Steps

Edit an AP.	**a.** In the map, right click the AP and choose **Edit**.
	
	b. Change any of the editable AP settings. Note the information about the following fields:
	
	    • **Antenna**: For external APs, you must select an antenna, or the AP will not be present in the map.
	
	    • **Azimuth**: The azimuth is the angle of the antenna, measured relative to the x axis, clockwise. The azimuth range is 0 to 360. In Cisco DNA Center, pointing right is 0 or 360 degrees; pointing down is 90 degrees.
	
	        You can manually enter the value or use the blue arrow under the field to change the value.
	
	        For omnidirectional antennas, the azimuth is not relevant if the elevation is 0.
	
	    • **Elevation**: You can manually enter the elevation in degrees or use the blue arrow under the field to change the value.
	
	        For APs and antenna models that are designed to be placed on a ceiling, 0 elevation means pointing down. For APs and antenna models that are designed to be placed on a wall, 0 elevation means pointing horizontally and negative values means pointing down.
	
	c. Click **Update**.

Remove an AP.	**a.** Click the AP, or to select multiple APs, click the first AP and while pressing the **Shift** key, click the rest of the APs. **b.** In the **Edit** pane, click **Remove Selected**. **c.** From the map toolbar, click **Save**.

Add, Position, and Remove Sensors

Before you begin

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

Step 1   Click the menu icon (≡) and choose .

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

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

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

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

Add, Edit, and Remove Coverage Areas

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

For more information about coverage areas, see Configure 2D Floor Map Devices and Overlay Objects, on page 40.

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

Step 4   To add a coverage area, do the following:

a)   In the **Coverage Area** dialog box, enter a name for the coverage area in the field.

b)   Click **Add Coverage**.

c)   Click on the map to create a point and initiate the drawing tool.

d)   Continue creating points to define the coverage area shape.

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

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

Step 5   To edit a coverage area, do the following:

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

b)   To redefine the shape of a coverage area, click and drag a point.

c)   To edit a coverage area name, right-click the coverage area and choose **Edit**.

Step 6   To delete a coverage area, do the following:

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

b) Right-click the coverage area and choose **Remove**.

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

Add, Edit, Copy, and Remove Openings

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

For more information about openings, see Configure 2D Floor Map Devices and Overlay Objects, on page 40.

Step 1 Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

Step 4 To add an opening, do the following:

a) From the left pane of the map, click **Opening**.

b) Click on the map to create a point and initiate the drawing tool.

c) Continue creating points to define the opening shape.

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

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

Step 5 To edit an opening, do the following:

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

b) To redefine the shape of an opening, click and drag a point.

c) To move an opening, click inside the shaded area. Then, drag and drop the opening where you want to place it.

Step 6 To copy an opening from one floor to another, do the following:

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

b) Right-click the opening and choose **Copy to other floors**.

c) In the dialog box, check the check boxes next to the relevant floors.

d) Click **Copy**.

e) Click **Close**.

Step 7 To remove an opening, do the following:

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

b) Right-click the opening and choose **Remove**.

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

Add, Edit, and Remove Location Regions

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

Add, Edit, and Remove an Inclusion Region

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

- Inclusion regions can be any polygon-shaped area and must have at least three points.

- You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor area when it is created. The inclusion region is indicated by a solid aqua line, and generally outlines the entire floor area.

For more information about inclusion regions, see Configure 2D Floor Map Devices and Overlay Objects, on page 40.

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

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

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

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

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

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

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

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

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

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

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

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

Add, Edit, and Remove an Exclusion Region

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

- Exclusion regions can be any polygon-shaped area and must have at least three points.

- Exclusion regions are defined within the borders of an inclusion region.

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

For more information about exclusion regions, see Configure 2D Floor Map Devices and Overlay Objects, on page 40.

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

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

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

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

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

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

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

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

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

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

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

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

Add, Edit, and Remove Walls

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

For more information about walls, see Configure 2D Floor Map Devices and Overlay Objects, on page 40.

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

Step 4   To add walls, do the following:

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

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

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

     c)   Move the cursor to the next point, where you want to end the wall or where you want to create a corner and click again.

     d)   Continue creating points to define the wall shape.

     e)   To end a wall, double-click the map.

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

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

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

     a)   Click the wall that you want to change.

         The **Wall Type** dialog box opens.

     b)   From the **Wall Type** drop-down list, choose the type of wall.

     c)   Configure any other parameters that are appropriate for the new wall type.

     d)   Click **Update**.

Step 6   To move a wall, do the following:

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

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

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

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

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

Add, Copy, Edit, and Remove Shelving Units

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

For information about shelving units, see Configure 2D Floor Map Devices and Overlay Objects, on page 40.

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

Step 4   To add shelving units, do the following:

a) In the left pane of the map, click the shelving type you want to add.

b) In the shelving dialog box, configure the name, dimensions, orientation, and whether the unit is double-sided, or leave the default values. Orientation means the angle of the shelving unit. A shelving unit with an orientation of 0 means that the shelving unit is vertical and parallel to the y-axis.

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

c) Click **Add Shelving**.

   The shelving unit is displayed on the map.

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

Step 5   To create a copy or an array of a shelving unit, do one of the following:

   • To create a copy, right-click the shelving unit and choose **Clone**.

   • To create an array, right-click the shelving unit and choose **Array**. Then specify the number of units and the distance between them.

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

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

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

Add, Edit, and Remove Markers

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

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

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

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

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

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

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

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

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

Add, Edit, and Remove GPS Markers

This procedure shows you how to add, edit, and remove GPS markers. For more information about GPS markers, see Configure 2D Floor Map Devices and Overlay Objects, on page 40.

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

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

Step 4   To add a GPS marker, do the following:

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

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

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

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

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

    d)   Click **Add GPS Marker**.

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

Step 6   To remove a GPS marker, right-click the GPS marker and choose **Remove**.

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

Add, Edit, and Remove Align Points

This procedure shows you how to add, edit, and remove align points. For more information about align points, see Configure 2D Floor Map Devices and Overlay Objects, on page 40.

Step 1   Click the menu icon (≡) and choose **Design** > **Network Hierarchy**.

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

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

Step 4   To add an alignment point, do the following:

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

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

Step 5   To edit the name of an alignment point, do the following:

    a)   Right-click the alignment point and choose **Edit**.

    b)   Change the name and click **Edit Marker**.

Step 6   To change the location of an alignment point, do the following:

    a)   Right-click the alignment point and choose **Edit**.

    b)   Click **Edit Marker**.

    c)   Drag and drop the alignment point to the new location.

Step 7   To remove an alignment point, right-click the alignment point and choose **Remove**.

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

Manage Inventory

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

About Inventory

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

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

Inventory uses 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 Endpoint Discovery. (This protocol is used to discover IP phones and some servers.)

- Network Configuration Protocol (NETCONF). For a list of devices, see Discovery Prerequisites, on page 17.

After the initial discovery, Cisco DNA Center maintains the inventory by polling the devices at regular intervals. The default interval is every 24 hours. However, you can change this interval as required for your network environment. For more information, see Update the Device Polling Interval, on page 50. Also, a configuration change in the device triggers an SNMP trap, which in turn triggers device resynchronization. Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than one day are displayed. This prevents stale device data, if any, from being displayed. On average, polling 500 devices takes approximately 20 minutes.

Update the Device Polling Interval

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

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

Before you begin

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

Step 1   Click the menu icon (≡) and choose **Provision** > **Network Devices** > **Inventory**.

Step 2   Select the devices that you want to update.

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

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

Step 5   Select the resync type.

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

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

Step 7   Click **Update**.

Display Information About Your Inventory

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

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

When you select devices and choose a different view from the **Focus** drop-down list, your selection persists in each new view.

If you choose the **Default** view from the **Focus** drop-down list, the **Inventory** table displays only the **Device Name**, **IP Address**, **Device Family**, and **MAC Address** of the listed devices.

By default, 25 entries are shown in the **Inventory** table. Click **Show More** to view more entries. You can view up to 500 entries in the **Inventory** table.

If there are more than 25 entries in the **Inventory** table and you choose a different view from the **Focus** drop-down list, the same number of entries is displayed in each new view.

Before you begin

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

Click the menu icon (☰) and choose **Provision** > **Network Devices** > **Inventory**.

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

Table 7: Inventory

Column	Description
Device Name	Name of the device. Click the device name for more information about that device. **Note** A device name that is displayed in red means that inventory has not polled the device and updated its information for more than 30 minutes.
IP Address	IP address of the device.

Support Type	Shows the device support level:
	• **Supported**: The device pack is tested for all applications on Cisco DNA Center. You can open a service request if any of the Cisco DNA Center functionalities for these devices do not work.
	• **Limited**: The device pack for legacy devices is tested only for the following features on Cisco DNA Center.
	  • Discovery
	  • Topology
	  • Device Reachability
	  • Config Change Audit
	  • Inventory
	  • Software Image Management (Software images may not be available for EOL devices on cisco.com. Not recommended for EOL devices.)
	  • Template Provisioning (Applicable only for switches.)
	For more information, see the Cisco DNA Center Compatibility Matrix.
	• **Unsupported**: All remaining Cisco and third-party devices that are not tested and certified on Cisco DNA Center. You can try out various functionalities on Cisco DNA Center for these devices, as a best effort. However, you cannot raise a service request or a bug if Cisco DNA Center features do not work as expected.
	• **Third Party**: Device pack is built by customers or business partners and goes through the certification process. Third-party devices support base automation capabilities such as Discovery, Inventory, Topology, and so on. Cisco TAC provides an initial level of support for these devices. However, if there is a problem with the device pack, you need to contact the business partner.

Column	Description
Reachability	The following is a list of the various statuses: • **Reachable**: The device is reachable by Cisco DNA Center using SNMP, HTTP(S), and NETCONF polling. • **Ping Reachable**: The device is reachable by Cisco DNA Center using ICMP polling and not reachable using SNMP, HTTP(S), and NETCONF polling. • **Unreachable**: The device is not reachable using SNMP, HTTP(S), NETCONF, or ICMP polling.
EoX Status	Shows the EoX scan status: • **Success**: The device is scanned for EoX alerts successfully. • **Not Scanned**: The device is not scanned for EoX alerts. • **Scan Failed**: Cisco DNA Center is not able to scan the device for EoX alerts. • **Scanning**: Cisco DNA Center is scanning the device for EoX alerts. Hover your cursor over the **i** icon next to **EoX Status**, and click **Click here to accept** to initiate an EoX scan. For the devices that are scanned successfully, the **EoX Status** column shows the number of alerts, if any. Click the number of alerts to view the alerts in detail. In the slide-in pane, click the **Hardware**, **Software**, and **Module** tabs to view the hardware, software, and module EoX alerts.
Manageability	Shows the device status: • **Managed with green tick icon**: Device is reachable and is fully managed. • **Managed with orange error icon**: Device is managed with some error, such as unreachable, authentication failure, missing NETCONF ports, internal error, and so on. You can hover the cursor over the error message to view more details about the error and the impacted applications. • **Unmanaged**: Device cannot be reached and no inventory information was collected because of device connectivity issues.
MAC Address	MAC address of the device.
Image Version	Cisco IOS software that is currently running on the device.
Platform	Cisco product part number.
Serial Number	Cisco device serial number.
Uptime	Period of time for which the device has been up and running.

Column	Description
Device Role	Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Cisco DNA Center is unable to determine a device role, it sets the device role to Unknown. **Note** If you manually change the device role, the assignment remains static. Cisco DNA Center does not update the device role even if it detects a change during a subsequent device resynchronization. If required, you can use the drop-down list in this column to change the assigned device role.
Site	The site to which the device is assigned. Click **Assign** if the device is not assigned to any site. Click **Choose a Site**, select a site from the hierarchy, and click **Save**. For more information, see Design Network Hierarchy, on page 30.
Last Updated	Most recent date and time on which Cisco DNA Center scanned the device and updated the database with new information about the device.
Device Family	Group of related devices, such as routers, switches, hubs, or wireless controllers.
Device Series	Series number of the device, such as Cisco Catalyst 4500 Series Switches.
Resync Interval	The polling interval for the device. Set the resync interval from the **Inventory** window by choosing **Actions** > **Edit Device** > **Resync Interval**. To set the resync type as **Global**, from the main menu, choose **System** > **Settings**. For more information, see the *Cisco DNA Center Administrator Guide*.
Last Sync Status	Status of the last Discovery scan for the device: • **Managed**: Device is in a fully managed state. • **Partial Collection Failure**: Device is in a partial collected state and not all the inventory information has been collected. Hover the cursor over the **Information (i)** icon to display additional information about the failure. • **Unreachable**: Device cannot be reached, and no inventory information was collected because of device connectivity issues. This condition occurs when periodic collection takes place. • **Wrong Credentials**: If device credentials are changed after adding the device to the inventory, this condition is displayed. • **In Progress**: Inventory collection is occurring.

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

Delete a Network Device

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

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

Before you begin

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

Step 1 Click the menu icon (≡) and choose **Provision** > **Network Devices** > **Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.

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

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

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

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

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

Add a Device to a Site

Adding devices to a site configures Cisco DNA Center as the syslog and SNMP trap server, which enables Syslog Level 2 and configures global telemetry settings.

Step 1 Click the menu icon (≡) and choose **Provision** > **Network Devices** > **Inventory**.
The **Inventory** window displays the device information gathered during the discovery process.

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

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

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

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

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

Step 7 Check **Application and Endpoint Visibility is enabled on all applicable devices. Check this to skip enabling it on all devices** check box.

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

Step 8   Review summery settings and click **Next**.

Step 9   In the **Task Name** name field, enter a task name of your choice.

Step 10   Choose whether you want to assign the device to a site **Now** or schedule it for later.

Step 11   Click **Assign**.

Step 12   To preview the CLI configuration, click the **Generate Configuration Preview** radio button and do the following:

    a.   In the **Task Name** name field, enter a task name of your choice and click **Preview**.

        Later, you can use the created configuration preview to deploy to the selected devices.

    b.   In the **Task Submitted** dialog box, click the **Work Items** link.

Note	This dialog box displays for a few seconds and then disappears. To navigate to the **Work Items** window, click the menu icon (☰) and choose **Activities** > **Work Items**.

    c.   In the **Work Items** window, click the CLI preview task for which you submitted the configuration preview request.

    d.   View the CLI configuration details and click **Deploy**.

    e.   To immediately deploy the device, click the **Now** radio button, and click **Apply**.

    f.   To schedule the device deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment.

    g.   In the confirmation window, click **Yes**.

Note	The CLI task is marked as completed in the **Work Items** window. You can view the CLI configuration for this task, but you cannot deploy it again.

Step 13   When assigning devices to a site, if Device Controllability is enabled, a workflow is automatically triggered to push the device configuration from the site to the devices.
From the **Focus** drop-down list, choose **Provision** and click **See Details** in the **Provision Status** column. The configuration that is pushed to the device is shown in a separate window if you enabled Device Controllability.

About Cisco ISE Configuration for Cisco DNA Center

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

Cisco ISE configuration is centralized within NCP (Network Control Platform), which enables you to configure Cisco ISE at one GUI location. The workflow for configuring Cisco ISE is as follows:

1.   Click the menu icon (☰) and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**, and enter the Cisco ISE server details.

2.   After the Cisco ISE server is successfully added, NCP establishes a connection with NDP (Network Data Platform) and sends the details of the pxGrid nodes, keystore, and truststore files.

3.   NDP uses the configuration received from NCP to establish a pxGrid session.

4.   NCP automatically detects pxGrid node failovers, persona moves, and communicates it to NDP.

5. If there are ISE deployment changes, NDP starts a new pxGrid session with a new pxGrid ACTIVE node.

Configure Authentication and Policy Servers

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

Before you begin

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

- If you are using another product (not Cisco ISE) to perform AAA functions, make sure to do the following:

  - Register Cisco DNA Center with the AAA server, including defining the shared secret on both the AAA server and Cisco DNA Center.

  - Define an attribute name for Cisco DNA Center on the AAA server.

  - For a Cisco DNA Center multihost cluster configuration, define all individual host IP addresses and the virtual IP address for the multihost cluster on the AAA server.

- Before you configure Cisco ISE, confirm that:

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

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

Note   Although pxGrid 2.0 allows up to four pxGrid nodes in the Cisco ISE deployment, Cisco DNA Center releases earlier than 2.2.1.x do not support more than two pxGrid nodes.

  - If you have a distributed Cisco ISE deployment:

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

Note   We recommend that you use ERS through the PAN. However, for backup, you can enable ERS on the PSNs.

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

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

- You must enable communication between Cisco DNA Center and Cisco ISE on the following ports: 443, 5222, 8910, and 9060.

- The Cisco ISE host on which pxGrid is enabled must be reachable from Cisco DNA Center on the IP address of the Cisco ISE eth0 interface.

- The Cisco ISE node can reach the fabric underlay network via the appliance's NIC.

- The Cisco ISE admin node certificate must contain the Cisco ISE IP address or FQDN in either the certificate subject name or the Subject Alternative Name (SAN).

- The Cisco DNA Center system certificate must list both the Cisco DNA Center appliance IP address and FQDN in the SAN field.

Note   For Cisco ISE 2.4 Patch 13, 2.6 Patch 7, and 2.7 Patch 3, if you are using the Cisco ISE default self-signed certificate as the pxGrid certificate, Cisco ISE might reject that certificate after applying those patches. This is because the older versions of that certificate have the Netscape Cert Type extension specified as the SSL server, which now fails (because a client certificate is required).

This issue does not occur in Cisco ISE 3.0 and later. For more information, see the Cisco ISE Release Notes.

Step 1   Click the menu icon (≡) and choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers**.

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

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

- **Server IP Address**: IP address of the AAA server.

- **Shared Secret**: Key for device authentications. The shared secret can contain up to 100 characters.

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

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

- **Shared Secret**: Key for device authentications.

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

Note   This user must be a Super Admin.

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

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

Note
- We recommend that you copy the FQDN that is defined in Cisco ISE (**Administration** >
Deployment > **Deployment Nodes** > **List**) and paste it directly into this field.

- The FQDN that you enter must match the FQDN, Common Name (CN), or Subject Alternative
Name (SAN) defined in the Cisco ISE certificate.

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

hostname.domainname.com

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

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

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

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

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

When you enable this option, ensure that:

- The Cisco DNA Center certificate is generated by the same Certificate Authority (CA) as is in use by Cisco
ISE (otherwise, the pxGrid authentication fails).

- The Certificate Extended Key Use (EKU) field includes "Client Authentication."

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

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

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

- **Accounting Port**: Port used to relay important events to the AAA server. The default UDP port is 1813.

- **Port**: The default TACACS 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.

- **Timeout**: The time period for which the device waits for the AAA server to respond before abandoning the attempt
to connect. The default timeout is 4 seconds.

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

Cisco ISE server registration phase:

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

pxGrid subscriptions registration phase:

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

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

Step 6   Click **Add**.

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

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

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

Before you begin

Create a site and assign a device to the site. See Create, Edit and Delete a Site, on page 30.

Step 1   Click the menu icon (≡) and choose **Design** > **Network Settings** > **Telemetry**.

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

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

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

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

Step 4   In the **NetFlow** area, do one of the following:

- Click the **Use Cisco DNA Center as NetFlow collector server** radio button. The NetFlow configuration on the device interfaces is completed only when you enable application telemetry on the device. Select the NetFlow collector at the site level to configure the NetFlow destination server to the device.

- Click the **Add Cisco Telemetry Broker (CTB)** radio button and add the IP address and port number of the Cisco Telemetry Broker. The Cisco Telemetry Broker collects NetFlow records from the device and sends the information to the destination.

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

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

If you don't want to enable IPDT for the site, click the **Disable** radio button (the default).

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

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

Step 7   Click **Save**.

Configure Cisco AI Network Analytics

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

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 the latest version of the AI Network Analytics application is installed. 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   Click the menu icon (☰) and choose **System** > **Settings**.

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

AI Network Analytics

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

[Configure]

Recover from a config file ⓘ

Step 3 Do one of the following:

- If you have an earlier version of Cisco AI Network Analytics installed in your appliance, do the following:

  a. Click **Recover from a config file**.

  The Restore AI Network Analytics window appears.

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

  c. Click **Restore**.

  Cisco AI Network Analytics might take a few minutes to restore, and then the **Success** dialog box appears.
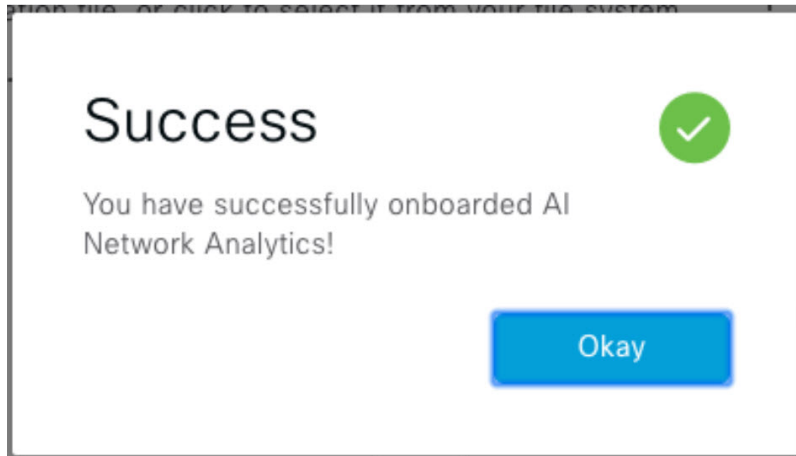
- If this is the first time you are configuring Cisco AI Network Analytics, do the following:

  a. Click **Configure**.

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

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

  c. Click **Next**.

  The terms and conditions window appears.

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

   Cisco AI Network Analytics might take a few minutes to enable, and then the **Success** dialog box appears.
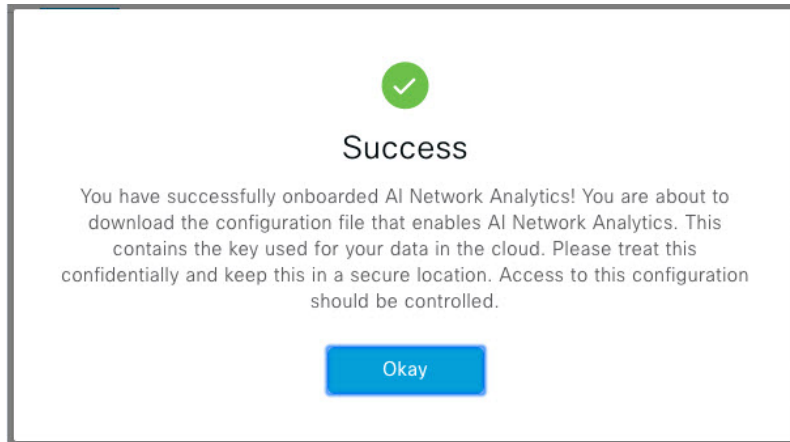
Step 4   In the **Success** dialog box, click **Okay**.
The **AI Network Analytics** window appears, and the **Enable AI Network Analytics** toggle button displays ✓☐.

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

Disable Cisco AI Network Analytics

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

Step 1   Click the menu icon (☰) and choose **System** > **Settings**.

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

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

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

Step 4   Click **Update**.

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

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

Update the Machine Reasoning Knowledge Base

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

Step 1 Click the menu icon (≡) and choose **System** > **Settings**.

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

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

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

- **AUTO UPDATE**: Automatically updates the Machine Reasoning Knowledge Base in Cisco DNA Center on a daily basis.

- **CISCO CX CLOUD SERVICE FOR NETWORK BUG IDENTIFIER AND SECURITY ADVISORY**: Integrates Cisco DNA Center with CX Cloud that allows you to perform an automated config. This integration provides enhanced vulnerability detection on devices directly from security advisories tool on Cisco DNA Center.

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

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

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

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

  a. Click **Download**.

     The **Opening mre_workflow_signed** dialog box appears.

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

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

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

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

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

Enable Localization

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

To change the default language, perform the following task:

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

- From Google Chrome, do the following:

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

   b. Click **Languages**.

   c. Click **Add languages**.

   d. In the **Add languages** dialog box, choose **Chinese**, **Japanese**, or **Korean**, and then click **Add**.

- From Mozilla Firefox, do the following:

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

   b. From the **Language and Appearance** > **Language** area, click **Choose**.

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

   d. Click **OK**.

Step 2   Log in to Cisco DNA Center.

The GUI is shown in the selected language.

Monitor and Troubleshoot Network Health

About Network

A network consists of one or more devices, including routers, switches, wireless controllers, and access points.

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

Before you begin

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

Step 1   Click the menu icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **Network** tab.

The **Network** health dashboard appears.

Figure 6: Network Health Dashboard
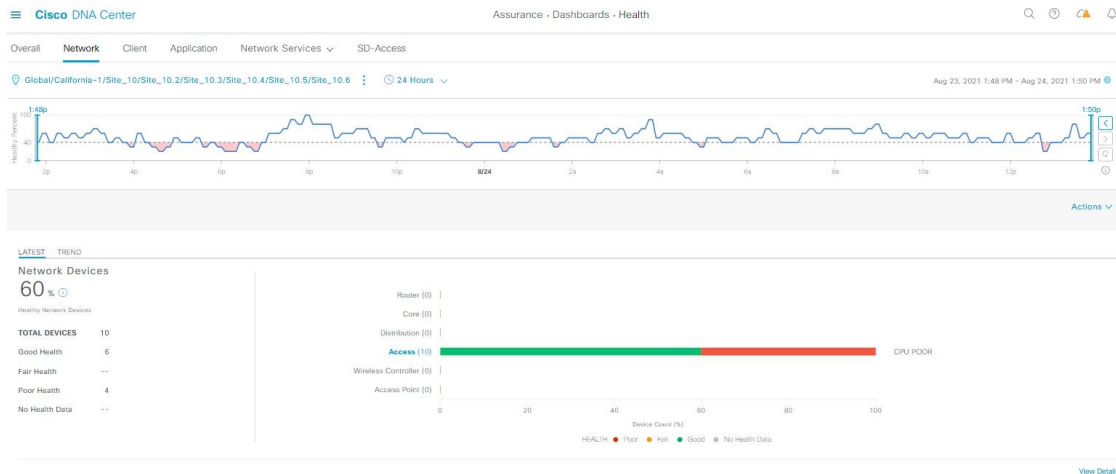
Step 3 Click the location option ( ) in the top menu bar to select the site, building, or floor from the Site hierarchy.

Step 4 Click next to the location icon and choose **Site Details** to view the Sites table.

The location pane has the following functionality:

Location Option	
Item	**Description**
toggle button **List View**	Click this toggle button to display the sites and buildings from your network in a list format. Click the drop-down list for the following options: • **Hierarchical Site View**: Sorts the list at a site level. From the **Go to sites** column, click for a site or building to display data only for that location on the **Network** dashboard. • **Building View**: Sorts the list at a building level. From the **Go to sites** column, click for a site or building to display data only for that location on the **Network** dashboard.
toggle button **Map View**	Click this toggle button to display the health of all the network sites on a geographic location-oriented network health map. By default, the network sites are color coded according to the severity of the problem.
Hide Sites	Click the **Hide Sites** icon to hide the sites table.

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

Step 5   Click the time range setting (🕐) in the top menu bar to specify the time range of data that appears on the dashboard.

     a) From the drop-down menu, choose the time range: **3 Hours**, **24 Hours**, or **7 Days**.
     b) Specify the **Start Date** and time, and the **End Date** and time.
     c) Click **Apply**.

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

     • **Export Dashboard**: Enables you to export the network dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**.

     • **Edit Dashboard**: Enables you to customize the dashboard display. See and .

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

     You can specify a more granular time range. You can click and drag the timeline boundary lines to specify the time range. This sets the context for the custom charts on the dashboard.

     You can use the arrow buttons on the right of the timeline to view data for up to 30 days.

     Hover your cursor within the timeline chart to view the network device health score percentage at a specific time.

     The dotted horizontal line represents the threshold for a healthy network, which by default is set to 40%.

     To change the threshold value:

     a. Hover your cursor over the information (ⓘ) icon.

     b. In the tooltip, click the edit (✏️) icon.

     c. In the **Network Health Threshold** slide-in pane, click and drag the blue line to set the threshold percentage value.

     d. Click **Save**.

     Note   Changing the custom threshold affects when the Network Device Summary Health Score is displayed as red. The custom threshold does not change the number of healthy or unhealthy devices.

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

Network Devices Health Summary Dashlet	
Item	**Description**

Network Devices Health Summary area	Includes the following tabs:
	
	• **Latest**: Displayed by default. The left pane provides the network health summary score and the total number of devices. The right pane displays charts.
	
	    • **Network Health Summary Score**: The Network Health Summary score is the percentage of healthy (good) devices in your overall network or selected site. See Network Health Score, on page 90.
	
	    • **Total Devices**: Provides the total number of network devices and the count of devices that have Good Health, Fair Health, Poor Health, and No Health Data.
	
	    • **Charts**: This color-coded snapshot-view chart shows the performance of each device category (Access, Core, Distribution, Router, Wireless Controller, and Access Points) over the last 5 minutes.
	
	    Hover your cursor over a color to display the health score and the number of devices associated with that color.
	
	    If the chart shows a low health score (red or orange), the KPIs that contributed to the low health score are shown next to the bar. Examples include link errors, high CPU, high memory, high noise, and low air quality.
	
	    You can also click a hyperlinked device category (**Access**, **Core**, **Distribution**, **Router**, **Wireless Controller**, and **Access Point**) to open a slide-in pane with additional details.
	
	• **Trend**: Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the performance of devices over a time range. Hover your cursor over the chart to display the total number of devices and their health over time.
	
	The color in the charts represent the health of the network devices:
	
	●: Poor network devices. Health score range is 1 to 3.
	●: Fair network devices. Health score range is 4 to 7.
	●: Good network devices. Health score range is 8 to 10.
	●: No Health data. Health score is 0.

View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

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

Total APs Up/Down Dashlet
Color-coded chart that provides the following AP status information: number of APs that are connected to the network and the number of APs that are not connected to the network.
The **Latest** tab provides a 5-minute snapshot view.
The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Top N APs by Client Count Dashlet
Chart that provides information about the APs that have the highest number of clients.
The **Latest** tab provides a 5-minute snapshot view.
The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Top N APs by High Interference Dashlet
Information about the APs that have high interference. You can choose 2.4 GHz or 5 GHz.
The **Latest** tab provides a 5-minute snapshot view.
The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Step 10   Use the **Network Devices** dashlet for the following functionality:

Network Devices Dashlet	
Item	**Description**
Type	Filter the table based on the device type with the following options: **All**, **Access**, **Core**, **Distribution**, **Router**, **WLC**, and **AP**.
	Note When you filter the devices based on device type "Router", it displays the device(s) with device role "Border Routers".
	For SDA Fabric Domain, filter the table based on the fabric type with the following options: **All**, **Fabric Control Plane**, **Fabric Border**, **Fabric Edge**, **Fabric WLC**, **Fabric AP**, and **Extended Node**.

Network Devices Dashlet	
Item	**Description**

Overall Health	Filter the table based on the overall health score of the device with the following options:
	
	   • **All**
	
	   • **Poor**: Devices with a health score range from 1 to 3.
	
	   • **Fair**: Devices with a health score range from 4 to 7.
	
	   • **Good**: Devices with a health score range from 8 to 10.
	
	   • **No Health**: Devices with no health data.

Network Devices table	View device information for all the devices in the network or for a selected site in a table format. **Note** The Overall Health Score is the minimum subscore of the following KPI metric health scores: System Health, Data Plane Connectivity, and Control Plane Connectivity. In the **Overall Health Score** column, hover your cursor over a health score. The **Device Health** score is displayed along with the health and percentage value of all of the KPI metrics. The **Device Health** score is the minimum subscore of the KPI metrics, depending on the type of device. For routers and switches, the following are the KPI metrics: System Resources (memory utilization and CPU utilization), Data Plane (uplink availability and link errors), and Fabric (Control Plane Reachability). The **Fabric Domain Name**, **Fabric Name** and **Fabric Role** columns display the fabric domain name, fabric name, and fabric role (Edge, Border, Map Server, and so on). The **Reachability** column displays the status of the device (Reachable, Up, Unreachable, Rebooting, and so on).
Device 360	Display a 360° view of a device by clicking the device name in the **Device** column. **Device 360** provides detailed information for troubleshooting device issues.
⬆ Export	Click **Export** to export the device information to a CSV file.
⋮	Customize the data you want displayed in the table: **a.** Click ⋮ . A list of options is displayed. **b.** Check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.

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

Network Devices Reachability Dashlet
Color-coded chart shows the reachability status of routers, switches, and wireless controllers.
• **Reachable**
• **Unreachable**
The **Latest** tab provides a 5-minute snapshot view.
The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can hover your cursor over the timeline slider to view the reachability status of over a time period. The Reachability status count of top devices based on role and location is displayed below the timeline slider as horizontal bar graphs.
You can select the data displayed as horizontal bars to filter the table based on the reachability status, device types, and location with the following options: All, Access, Core, Distribution, Router, and WLC.

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

WAN Link Utilization Dashlet
The bar chart shows the status of the WAN link utilization percentage only for the available WAN links.
Note   For a link to be considered a WAN link, you must manually assign the system-generated WAN tag to the required port. See "Assign Tags to Ports" in the Manage Your Inventory chapter of the Cisco DNA Center User Guide.
The **Latest** tab provides a 10-minute snapshot view of **Available** and **Not Available** WAN links.
The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can select an element on the chart to view more detailed data.
You can select the data displayed as horizontal bars below the timeline slider to filter the table based on top locations, device types, and location.

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

WAN Link Availability Dashlet
Color-coded chart displays the information on the available WAN links in your network.
The **Latest** tab provides the percentage of WAN links utilized.
The **Trend** tab provides a trend view for the time range that you selected in the time range settings. For example, if the time range is set to the last three hours, the trend tab displays three hours of data.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can select an element on the chart to view more detailed data.
You can select the data displayed as horizontal bars below the timeline slider to filter the table based on top locations (link count) and device types (link count).

Monitor and Troubleshoot the Health of a Device

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

Step 1   Click the menu icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **Network** tab.

Step 3   In the **Network** health dashboard, do one of the following:

- In the **Network Devices** dashlet, click a device name in the **Device Name** column.
- In the **Search** field, enter the device name, IP address, or MAC address.

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

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

Figure 7: Device 360 Window
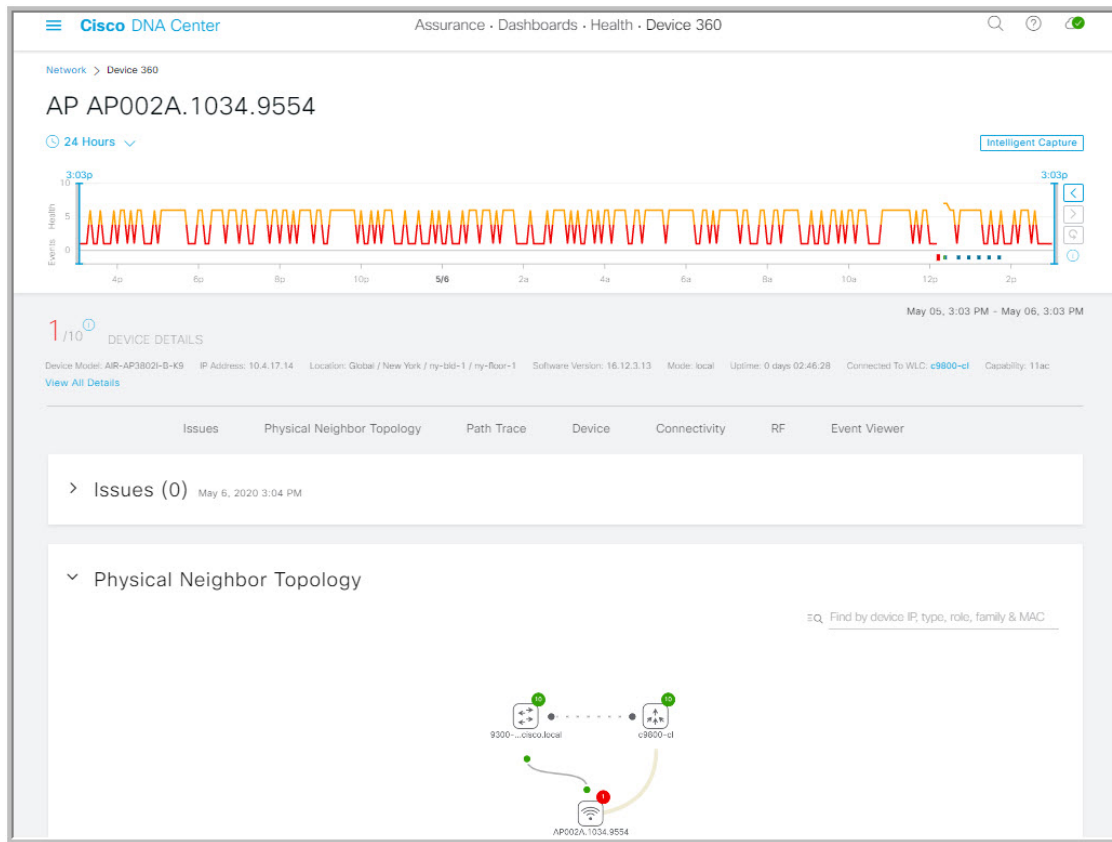
Step 4   Click the time range setting (⏱ 24 Hours ⌄) to specify the time range of data that is displayed on the window:

a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.

b) Specify the Start date and time; and the End date and time.

c) Click **Apply**.

Step 5   Click **Intelligent Capture** to view, monitor, and troubleshoot captured onboarding and data packets for a specific network device and to determine if there are potential issues that must be addressed. See View RF Statistics and Manage Spectrum Analysis Data for an Access Point, on page 331.

> **Note**   Intelligent Capture is not supported for all AP models. If **Intelligent Capture** is not displayed, verify that the AP is a supported model, and that the AP is assigned to a location on the **Network Health** dashboard.

Step 6   Use the timeline slider to view the health and events information about the network device over a period of time.

> **Note**   Gaps in the timeline indicate that no health data was retrieved from the device. This situation can occur when a device is in maintenance mode.

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 displays the timeline slider in 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 displays the timeline slider in a 1-hour time period. The entire window is refreshed, providing updates for that hour. Note that the timestamps next to each category (**Issues**, **Connectivity**, and so on) are also refreshed.

- **Events**: Event data is displayed as color-coded vertical bars on the graph. Green vertical bars indicate successful events and red vertical bars indicate events that failed.

  Each vertical bar represents 5 minutes of time. Multiple significant events can be generated during each 5-minute window. Hover your cursor over the vertical bar to get more information about the events.

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

Note   Devices in maintenance mode are not included in the calculation of a device's health score.

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

- **Switch**: The health score for switches is the minimum subscore of the following parameters: memory utilization, CPU utilization, link errors, link discards, uplink availability, and reachability to the control plane. In addition, for fabric devices, it includes fabric health. For more information, see Switch Health Score, on page 91.

  Note   **Switches**: Uplink availability is based on infrastructure links.

  Cisco StackWise Virtual: Uplink availability is based on infrastructure links, Cisco StackWise Virtual links (SVL), and Dual Active Detection (DAD) links. See About Cisco StackWise Virtual and Its Limitations, on page 86.

  Cisco StackWise: Uplink availability is based on infrastructure links and Cisco StackWise links. See About Cisco StackWise and Its Limitations, on page 87.

- **Router**: The health score for routers is the minimum subscore of the following parameters: memory utilization, CPU utilization, link errors, link discards, uplink availability, and reachability to the control plane. For more information, see Router Health Score, on page 92.

  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 93.

- **Wireless Controller**: The health score for wireless controllers is the minimum subscore of the following parameters: memory utilization, free timers, free memory buffers (MBufs), work queue element (WQE) pools, packet pools, and link errors. For fabric wireless controllers, it includes fabric health. For more information, see Wireless Controller Health Score, on page 94.

The color of the health score represents its severity. The health is measured on a scale of 1 to 10, where 10 is the best score. A score of 0 indicates that data could not be obtained or the device is in maintenance mode.

- ●: Critical issues. Health score range is 1 to 3.
- ●: Warnings. Health score range is 4 to 7.
- ●: No errors or warning. Health score range is 8 to 10.
- ●: No data available (includes devices in maintenance mode). Health score is 0.

Step 8 Use the **Device Details** area, below the timeline, to view the most current information about the device, such as the building and floor where the device is located, the device model, IP address, software version installed on the device, device role, HA status, the IP address or MAC address, and the uptime.

> **Note** For **Fabric**, the following elements are displayed in the device details area: **Fabric Role**, **Fabric Domain**, **Fabric Site**, **System Resources**, **Data Plane**, **Virtual Network**, and **Events**.
>
> For **Cisco StackWise Virtual**, two additional elements are displayed: **Stack Status: StackWise Virtual** and **StackWise Virtual Domain**.
>
> For **Cisco StackWise**, an additional **StackWise** element is displayed, along with the number of switches in the stack, such as **StackWise (2)**. A stack can contain a maximum of eight switches.
>
> For **Mesh APs**, the following details are displayed in the device details area: **Mode**, **Mesh Role** and **RAP**.
>
> For PoE-capable devices, the following elements are also displayed in the device details area: **IEEE Class**, **Negotiated Power Level**, and **PoE Status**.

Step 9 Click **View All Details** in the **Device Details** area to open a slide-in pane that displays additional attributes of a device, such as general information, network information, and rack location. Depending on the device type, additional device-specific details may be included.

Step 10 Use the **Issues** category to view issues that must be addressed.

> **Note** When a device is in maintenance mode, it does not trigger any issues.

Issues are listed based on the timestamp. The most recent issue is listed first.

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

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

- To resolve an issue:

  a. From the drop-down list, choose **Resolve**.

  b. Click **Resolved Issues** to view the issues that are resolved.

- To ignore an issue:

  a. From the drop-down list, choose **Ignore**.

  b. On the slider, set the number of hours to ignore the issue.

  c. Click **Confirm**.

  d. Click **Ignored Issues** to view the issues that have been ignored.

Step 11 Use the **Physical Neighbor Topology** category to view the topology of the device and how that device is connected to neighboring devices.

You can do the following:

- Click a node to display a slide-in pane that displays information about the node.

- Click a link between two devices to see the details about that specific link, such as the port/interface corresponding to the link, admin status, port mode, and so on.

- Hover your cursor over the link ends (dots) to see the status of the link.

- Hover your cursor over a group of devices and click **View Devices List** to view the list of devices and their details.

- In the Search field in the **Onboarding** area, you can search for a specific device. The specific node is selected, and the corresponding information about the device is displayed.

Note For AP 360, the 2-GHz and 5-GHz clients are displayed, and the dotted link lines going from these two clients are not clickable. Also, the link line between AP to wireless controller and wireless controller to AP is not clickable.

Note For an SD-Access Fabric, the fabric groups are displayed with a fabric badge icon.

Note The Cisco StackWise Virtual and Cisco StackWise are displayed with a stack icon (▤).

Path Trace displays a switch icon if a Cisco StackWise Virtual or a Cisco StackWise is involved in that path.

Step 12 Use the **Event View** category to view an audit trail of events for the device. The Event Viewer table provides information about the issue such as the reason code and the time stamp when the event occurred. Click an event to view details about that event in the right pane.

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

- For **For Switches and Routers**: Displays all syslogs that have a severity of Critical and above (Emergency and Alert), events for any links that are up or down, and events for devices that are reachable or unreachable. Syslogs that are less severe than Critical level (Error, Warning, Notice, and Info) are also displayed. For more information, see Selected Syslogs Below Critical Level for Switches and Routers, on page 84.

- **Wireless Controllers**: Lists wireless controller events. For Cisco AireOS devices, selected traps and syslogs are displayed. For Cisco IOS controllers, selected syslogs and events are displayed.

Step 13 Use the **Path Trace** category to run a path trace.

Click **Run New Path Trace** to display a network topology between a specified source device and a destination device. The topology includes the path's direction and the devices along the path, including their IP addresses. The display also shows the protocol of the devices along the path (**Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**) or other source type.

See Perform a Path Trace, on page 341.

Step 14 Click the **Application Experience** category to view the running applications in your network.

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

See About Application Experience and Application Visibility, on page 125 and View Application Experience of a Host, on page 131.

Note This category is displayed only for routers.

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

Click the following tabs to view the respective details:

Device Info Tab

Displays information about the device CPU, memory, uptime, temperature, and so on.

Note   If there are multiple sensors for a wireless controller, the data reflects the latest maximum temperature of all sensors.

Note   For network devices that are configured out of band, the uptime chart does not correlate correctly with the heath score and other data. For example, the uptime chart for a 24-hour window shows that the device was down at 11:39 am and at 2:40 pm. Then, if you choose a 3-hour window, 11:00 am – 2:00 pm (in the timeline slider), the downtime is not displayed. This issue occurs because Cisco DNA Center is not able to receive the sys uptime information from the device. To work around this issue, synchronize the configuration between the device and Cisco DNA Center.

Connectivity Tab

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

The Connectivity tab contains radio-specific KPIs, such as Radio 0, Radio 1, and Radio 2. Click the appropriate radio to view information such as Current Channel, Extended Channel(s), RF Profile, Band, Mode, and Current Channel Width. You can also view charts for Traffic, Client Count, and so on.

- **Traffic**: The traffic (in Mbps) for radios is displayed. The Rx (receiver) data packets and Tx (transmitter) data packets (in bytes) are shown as color-coded lines on the chart.

  Hover your cursor over a time instance on the graph to view the amount of traffic (Rx or Tx) sent or received for a particular day and time.

- **Client Count**: The number of clients for radios is displayed. The client count is shown as color-coded lines on the chart.

  Hover your cursor over a time instance on the graph to view the number of clients connected to an AP for a particular day and time.

- **Link Error**: To display information about interfaces, check the check boxes next to the interfaces on the right of the chart. Based on the interfaces you choose, the error percentage for each interface is displayed as color-coded lines on the chart.

  Hover your cursor over a time instance on the graph to view the error percentage for a particular day and time. You can choose a maximum of five interfaces.

- **Ethernet Interface KPI**: The Ethernet interface KPIs contain interfaces such as GigabitEthernet0 and GigabitEthernet1. Click the appropriate interface to display the charts for Utilization, Error, and Rate. You can also view the total and average values for the KPIs aggregated for a time range selected on the top of AP 360.

  Note   A Connected Switch banner is displayed for interfaces connected with switches.

- **Retries**: The connection retries for radios are displayed in the retries chart.

  Note   Only infrastructure links are considered for link errors. Infrastructure links are topological links connecting network devices, such as switches, routers, wireless controllers, and APs.

Fabric Site Tab

This tab is available for SD-Access fabric.

Fabric KPIs are grouped under different categories: **Fabric Site Connectivity**, **Fabric Infrastructure**, and **Fabric Control Plane**. You can filter based on these categories to view the respective KPIs: **CP Reachability**, **LISP Session Status**, and **Pub-Sub Session Status for INFRA VN**. Based on the selection, view the table with reachability information, such as the destination, IP address, and type. Check the check box next to destination to view the control plane reachability status, lisp, and pubsub session status charts.

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

Interfaces Tab

Contains information about the selected interface, such as the name, description, operational status, and link speed.

Use the PORT TYPE tabs to display information about a specific port type. The tabs that are displayed depend on the type of device selected:

- **Switches and Routers**: Displays **All**, **Access**, **Auto**, **Routed**, and **Trunk** port types.

- **Cisco StackWise Virtual**: Displays **All**, **Access**, **Auto**, **Routed**, **TrunkSVL**, and **DAD** port types.

- **Cisco StackWise**: Displays **All**, **Access**, **Auto**, **Routed**, **Trunk**, and **StackWisePort** port types.

- **Wireless Controller**: Displays **All**, **Ethernet**, and **Virtual** port types.

The table contains sortable columns. However, if you try to sort a column with a new parameter, the expanded interface list collapses.

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

To display the operational status of the interfaces for a particular day and time in a chart format, check the check boxes next to the interfaces. You can choose a maximum of five interfaces. The first interface in the table is selected by default.

The **Interface Availability**, **Utilization**, **Error**, and **Link Discard** charts are displayed below the table.

Note   For wireless controllers, link discard information is not provided in a separate chart. It is provided, along with other data, in a **Traffic Summary** table. Data in the **Traffic Summary** table is shown only for the physical and Ethernet interfaces of a wireless controller.

The **Tx Utilization** and **Rx Utilization** chart values are populated in **Percentage** and **Rate (bps)**. You can toggle between the Percentage and Rate to view the utilization values.

PoE Tab

This tab is available for PoE-capable switches and APs.

Displays the device's Power over Ethernet (PoE) telemetry.

Switches

The **POWER SUMMARY** section displays the switch's overall PoE telemetry:

- **Power Budget**: The overall power that the switch allocates for use with PoE-capable devices.

- **Used Power**: The power being supplied by the switch to PoE-capable devices.

- **Remaining Power:** The unused power available for use by PoE-capable devices.

- **Power Usage**: The percentage of power being supplied by the switch to PoE-capable devices. This value is equal to the value of the **Used Power** divided by the value of the **Power Budget**.

The **Power Stack** section lists the power stack devices connected to PoE, such as Power Stack Name, Stack Mode, Stack Topology, Allocated Power, Consumed Power, Remaining Power, and so on.

The **Module Power Details** section lists the components in the switch that supply power for PoE.

The **PoE Interfaces** section lists the PoE-capable devices connected to the switch's interfaces. At the top of the section is a count of interfaces that are currently off.

You can customize the table by doing the following:

- Use the **POE CONFIG**, **ADMIN STATUS**, and **POE OPER STATUS (SIGNAL PAIR)** filters above the table to filter the interfaces.

- Use the search bar to perform searches for specific interfaces, PoE-capable devices, or any other values.

- Click ⋮ to open a menu where you can add and remove columns for specific data types.

APs

The **Detail Information** section displays the AP's PoE telemetry: IEEE PD Class, Power Level, PoE Admin Status, PoE Oper Status, PoE Policing Status, Switch Name, Interface Name, Allocated Power, Consumed Power, Max Power Drawn, PoE Priority, PoE Configuration, and Perpetual PoE.

The **Power Distribution** section displays a trend chart of the power distribution (allocated and consumed power) for the selected time range.

StackWise Tab

This tab is available for Cisco StackWise.

Displays information about the Cisco StackWise, such as the serial number, product ID, MAC address, role, state, priority, and the neighboring switch number.

StackWise Virtual Tab

This tab is available for Cisco StackWise Virtual.

Displays information about the Cisco StackWise Virtual, such as the serial number, product ID, MAC address, role, state, priority, uptime, and port numbers.

RF Tab

This tab is available for APs and wireless clients.

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

  Note   **RF Tab Limitation**

  When an AP with three radios (for example, a Cisco Catalyst 9130 AP) connects to a wireless controller running 17.2 or later, the device supports all three radios, and three radios (Radio 0, Radio 1, and Radio 2) are displayed under the RF tab.

  When that same AP connects to a wireless controller running version 17.1 older, the device supports two radios, and two radios (Radio 0 and Radio 1) are displayed under the RF tab.

  However, if an AP moves from a wireless controller running a newer version to one running an older version (17.2+ > 17.1), the RF tab continues to display the three radios (Radio 0, Radio 1, and Radio 2) that were initially detected.

- For AP 5-GHz radios, a DFS tab provides information about Dynamic Frequency Selection (DFS) radar events.

- For AP 360, the RF tab contains the **Neighbors and Rogues** tab. It contains **Band** (2-GHz and 5-GHz radio frequencies), **Type** (All, Neighbor, Rogue), and **RSSI Range** (0 to -100 dBm) filters. Depending on the filter selection, the AP table is refreshed.

  AP table data contains information, such as the Identifier, Radio, RSSI (dBm), Channel, Type, and SSID of the AP. Use the search bar to find AP devices, radios, or any other values.

  Click ⚙ to open a menu where you can use **Edit Table Column** to enable or disable specific columns.

  Click **Export** to export the table data to a CSV file.

- Click the **KPI** drop-down list and check the check boxes next to the charts that you want to display. The charts provide various information, such as Throughput, Client Count, Channel Utilization, Top SSIDs by Client/Packet Count, and so on. Selected charts are displayed in the **RF** tab.

- Depending on the filter selection, the Wi-Fi analyzer graph is displayed below the table. The Wi-Fi graph summarizes the total and average values for the KPIs aggregated for a time range selected on the top of the AP 360 timeline slider.

  Check the check boxes next to the APs to view the Wi-Fi analyzer graph for the specific AP. Hover your cursor over the chart to view details.

  Click the **Chart Setting** icon to enable or disable the **Access Point Label**, which is shown in the graph for each AP.

Virtual Network Tab

This tab is available for SD-Access fabric.

The KPIs are grouped under the **VN Services** and **Fabric Control plane** categories. You can select the category to view the **Multicast (external RP) an d Default Route Registration** and **Pub-Sub Session Status** KPIs. You can filter the categories to display the table with reachability information, such as the destination, IP address, and type. Check the check box next to destination to view the control plane reachability status, lisp and pubsub session status charts.

Transits and Peers Network Tab
This tab is available for SD-Access fabric.
The **Transits and Peers Network** tab contains these **Transit Site Control Plane** KPIs: **LISP Session from Border to Transit Site Control Plane** and **Pub-Sub Session from Border to Transit Site Control Plane**. Check the appropriate KPI check box to display the charts and table with reachability information, such as the destination, IP address, and type.

Mesh Tab
This tab is available for Mesh APs.
The **Mesh** tab shows a device's mesh role, mesh profile, downstream MAPs, mesh backhaul channel, hops to RAP, bridge group name, and backhaul interface.
It also provides the following radio-specific KPIs: **Current Channel**, **Extended Channel(s)**, **Mode**, **RF Profile**, **Band**, **Tx Power**, **Clean Air Status**, **Admin State**, and **Current Channel Width**.

Step 16 To compare the health of AP radios across the floor in a building, click the toggle button in the top-right corner to switch between **Detail View** and **Map and Comparison View**.

Map and Comparison View displays a floor map with the AP radios placed on it.

Step 17 From the **View Floor** drop-down list, choose the floor on which you want to compare the AP radios.

Hover your cursor over the AP icon on the floor map to view the device details of an AP radio, such as **MAC Address**, **Model**, **Mode**, and **Issue Count**.

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

The **Map View** appears by default, showing the last 5 minutes of AP radio data.

Step 19 Click the AP icon on the floor map.

A dialog box appears to select or deselect the radios for comparison.

Step 20 Check the check boxes next to the list of radios that you want to compare on a floor.

Note
- By default, Cisco DNA Center selects the current AP for comparison only if the first radio of the respective AP is in monitor mode.
- **Local**, **Remote**, and **Hybrid** modes are the only AP radio modes enabled for comparison.
- You can select up to five AP radios at a time for comparison.

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

You can compare **Radio**, **IP Address**, **Model**, **Uptime**, **Connected to WLC**, and **Floor**.

Step 22 Use **Comparative Metrics** to view the comparative metrics for the selected KPIs.

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

You can select from the following KPIs:

- Channel Information
- Throughput (Rx Rate)

- Radio Retries

- Interference

- Air Quality

- Management Frames

- Tx Errors

- Tx Power

- Traffic Utilization

- Tx Traffic Utilization

- Throughput (Tx Rate)

- Connected Client Count

- Channel Utilization

- Noise

- Wireless Latency

- Data Frames

- Rx Errors

- Multicast Counter

- Rx Traffic Utilization

Step 24   Click the toggle button to switch between **Map View** and **Table View**.

The **Access Point Radios** table view lists the AP radios.

Step 25   Check the check box next to the AP radios that you want to compare on a floor map.

Step 26   To remove all radios from the comparison in the **AP Radio Comparison** area, click **Clear Selection**.

Step 27   Click **Exit Comparison** to exit.

Selected Syslogs Below Critical Level for Switches and Routers

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

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

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

About Cisco StackWise Virtual and Its Limitations

Cisco StackWise Virtual is a network system visualization technology that allows two physical switches to operate as a single logical virtual switch using a 40-G or 10-G Ethernet connection.

Supported Devices for StackWise Virtual

The following table lists the Cisco Catalyst Switches that support StackWise Virtual:

Device	Minimum Supported IOS-XE Software Version
Cisco Catalyst 9300 Series Switches	16.11+
Cisco Catalyst 9400 Series Switches	16.11+
Cisco Catalyst 9500 Series Switches	16.11+

StackWise Virtual Limitations

Cisco StackWise Virtual has the following known limitations:

- After you have configured Cisco StackWise Virtual, the second switch still appears in the inventory, and stops responding because it does not have its own IP address. As a workaround, do the following:

  1. Delete both the switches from the inventory. See Delete a Network Device, on page 55.

  2. Configure StackWise Virtual. (Configure the two switches into one virtual switch.)

  3. Discover the devices. See Discover Your Network Using an IP Address Range, on page 25, Discover Your Network Using CDP, on page 23, or Discover Your Network Using LLDP, on page 26.

> **Note**
>
> After StackWise Virtual is discovered, one switch plays the active role, while the other a standby role. Both switches in the stack get associated with one primary management IP address.

- After you remove Cisco StackWise Virtual, the two switches are independent. They both have the same IP address and operate in Dual Active Detection (DAD) state. As a workaround, do the following:

  1. Configure a different IP address on the second switch.

  2. Rediscover the devices. See Discover Your Network Using an IP Address Range, on page 25, Discover Your Network Using CDP, on page 23, or Discover Your Network Using LLDP, on page 26.

About Cisco StackWise and Its Limitations

The Cisco StackWise technology provides an innovative new method for collectively utilizing the capabilities of a stack of switches. Individual switches intelligently join to create a single switching unit with a 32-Gbps switching backplane. Configuration and routing information is shared by every switch in the stack, creating a single switching unit.

Supported Devices for Cisco StackWise

The following devices support Cisco StackWise:

- Cisco Catalyst 3650 Series Switches

- Cisco Catalyst 3850 Series Switches

- Cisco Catalyst 9300 Series Switches

Cisco StackWise Limitations

Cisco StackWise has the following known limitations:

- Ring status is not displayed in the **Device 360** header.

- Link Speed information is not provided in the. **Detail Information** > **Interfaces** tab.

Configure Health Score Settings for Network Devices

Use this procedure to configure the health score settings for network devices. You can customize the health score calculation for network devices by changing the KPI thresholds and specifying the KPIs that are included for the calculation.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Manage** > **Health Score Settings**.

The **Health Score** window appears.

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

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

Step 3   From the **KPI Name** column, click the KPI name link.

The slide-in pane for the KPI appears.

Step 4   Configure the KPI health score settings:

a) If the KPI threshold is quantitative, you can customize the threshold value for what is considered a good health score.

b) To Sync or Unsync the common KPI threshold between the health and issues settings, use the Synced toggle button. The sync works vice-versa when it is synced from health or issue settings page.

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

Note	A network device's health score is the lowest score from all its included KPI scores.
Restriction	At least one KPI must be included for the health score calculation.
Attention	When viewing the KPI health scores for a network device, excluded KPIs display a `NA` instead of a health score.

d) To restore the default settings, hover your cursor over **View Default Setting** and click ✔ **Use Default**.

Step 5   Click **Apply**.

A confirmation dialog box is displayed.

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   Click the menu icon (≡) and choose **System** > **Data Platform**.

Step 2   Click **Collectors**.

A list of collectors is displayed.

Step 3   Click **COLLECTOR-SNMP**.

The **COLLECTOR-SNMP** window opens.

Step 4 Click + **Add**.

The **SNMP Configuration** dialog box opens.

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

Figure 8: SNMP Configuration

Step 6 In the **Configuration Name** field, enter a unique name for the SNMP configuration.

Step 7 Click **Save Configuration**.

Understand Network Health Score and KPI Metrics

This section provides information about how the network health scores and KPI metrics are computed.

Network Health Score

The Network Health score is a percentage of the number of healthy network devices (a health score from 8 to 10) divided by the total number of network devices. The score is calculated every 5 minutes.

For example:

90% (health score) = 90 (network devices with health score from 8 to 10) ÷ 100 (total number of network devices)

Device Category Health Score

The Device Category Health score (Access, Core, Distribution, Router, Wireless) is the percentage of the number of healthy network devices (a health score from 8 to 10) in a target category, divided by the total number of network devices in that category. The score is calculated every 5 minutes.

For example:

90% (health score) = 90 (network devices in a target category with health score from 8 to 10) ÷ 100 (network devices in that category)

Individual Device Health Score

The Individual Device Health score is the minimum score of following KPI metric health scores: System Health, Data Plane Connectivity, and Control Plane Connectivity. The KPI metric score is based on the threshold that is defined per KPI.

Device Health Score = MIN (System Health, Data Plane Connectivity, Control Plane Connectivity)

Depending on the type of device, the metrics vary.

System Health	
Device Type	**Description**
Switch (Access and Distribution)	Includes system-monitoring metrics, such as CPU utilization and memory utilization.
Wireless	Includes the following system-monitoring metrics: • For wireless controllers, it includes memory utilization, free timers, and free Mbufs. • For AP, it includes CPU utilization and memory utilization.
Router	Includes system-monitoring metrics, such as CPU utilization and memory utilization.

System Health	
Device Type	**Description**
Fabric	Includes system-monitoring metrics, such as CPU utilization and memory utilization.

Data Plane Connectivity	
Device Type	**Description**
Switch (Access and Distribution)	Includes metrics, such as link errors and link status. For switches, the Inter-device Link Availability metric counts physical stack ports, network device-connected links, and fabric edge-facing port channels.
Wireless	Includes the following metrics: • For wireless controllers, it includes metrics, such as WQE pool, packet pools, and link errors. • For AP, it includes RF metrics, such as interface, noise, air quality, and radio utilization.
Router	Includes metrics, such as link errors.

Control Plane Connectivity	
Device Type	**Description**
Wireless	Includes the following KPIs: • For wireless controllers, it includes connectivity to the Control Plane node servers. • For fabric devices, it includes metrics, such as connectivity to the Control Plane node.

Switch Health Score

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

Parameter	Score Calculation
CPU Utilization	• If CPU utilization is 95 percent or less, the score is 10. • If CPU utilization is more than 95 percent, the score is 1.
Memory Utilization	• If memory utilization is 95 percent or less, the score is 10. • If memory utilization is more than 95 percent, the score is 1.

Parameter	Score Calculation
Link Errors (Rx and Tx)	Only infrastructure links are considered for link errors. Infrastructure links are topological links between network devices, such as switches, routers, wireless controllers, and APs. If a physical infrastructure interface has errors, the score is 8, if all links are down, it is 1, otherwise it is 10.
Link Discards	Only infrastructure links are considered for link discards. Infrastructure links are topological links between network devices, such as switches, routers, wireless controllers, and APs. If a physical infra link has packet drops (discards), the score is 8, if all links encounter discards, it is 1, otherwise it is 10.
Link Status	Only infrastructure links are considered for link status UP/DOWN. Infrastructure links are topological links between network devices, such as switches, routers, wireless controllers, and APs. If a physical infrastructure interface is down, the score is 8, if all interfaces are down, it is 1, otherwise it is 10.
Connection to Control Plane Node—Fabric Devices Only (Edge and Border)	• If the Control Plane node is reachable, the score is 10. • If the Control Plane node is unreachable, the score is 1. **Note** If there is more than 1 Control Plane node in a fabric network, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1. **Note** For the health score to populate correctly for fabric devices, enable SNMP Collector metrics. See Enable SNMP Collector Metrics for Fabric Devices, on page 88.

Router Health Score

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

Parameter	Score Calculation
CPU Utilization	• If CPU utilization is 95 percent or less, the score is 10. • If CPU utilization is more than 95 percent, the score is 1.
Memory Utilization	• If memory utilization is 95 percent or less, the score is 10. • If memory utilization is more than 95 percent, the score is 1.
WAN Connectivity	• If the WAN connectivity is down, the score is 1. • If the WAN connectivity is up, the score is 10.

Parameter	Score Calculation
Link Errors	Only infrastructure links are considered for link errors. Infrastructure links are topological links between network devices, such as switches, routers, wireless controllers, and APs. If a physical infrastructure interface has errors, the score is 8, if all links are down, it is 1, otherwise it is 10.
Link Discards	Only infrastructure links are considered for link discards. Infrastructure links are topological links between network devices, such as switches, routers, wireless controllers, and APs. If a physical infra link has packet drops (discards), the score is 8, if all links encounter discards, it is 1, otherwise it is 10.

AP Health Score

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

Parameter	Score Calculation
CPU Utilization	• If CPU utilization is 90 percent or less, the score is 10. • If CPU utilization is more than 90 percent, the score is 1.
Memory Utilization	• If memory utilization is less than 90 percent, the score is 10. • If available memory is 90 percent or more, the score is 1.
Radio Utilization Score	The score is calculated individually for each radio, and then the average radio score is determined. • If radio utilization is less than 70 percent, the score is 10. • If radio utilization is 70 percent or more, the score is 1.
Interference Score	The score is calculated individually for each radio, and then the average radio score is determined. For 2.4-GHz radio: • If interference is less than or equal to 50 percent, the score is 10. • If interference is more than 50 percent, the score is 1. 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 1.

Parameter	Score Calculation
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 1. 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 1.
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 1. 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 1.

Wireless Controller Health Score

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

Parameter	Score Calculation
Memory Utilization	• If memory utilization is less than 90 percent, the score is 10. • If the available memory is 90 percent or more, the score is 1.
Free Timer Score	• If the number of free timers is 20 percent or more, the score is 10. • If the number of free timers is 20 percent or less, the score is 1.
Free Memory Buffers (MBufs)	• If the number of free memory buffer is 20 percent or more, the score is 10. • If the number of free memory buffer is less than 20 percent, the score is 1.

Parameter	Score Calculation
Work Queue Element (WQE) Pool Score	• If the wqe pool is greater than wqe pool threshold, the score is 10. • If the wqe pool is at the same level as or lower than the wqe pool threshold, the score is 1.
Packet Pools	• If the packet pool is greater than the packet pool threshold, the score is 10. • If the packet pool is at the same level as or lower than the packet pool threshold, the score is 1.
Link Errors	• If link errors are less than 1 percent, the score is 10. • If link errors are 1 percent or more, the score is 1.
Connection to Control Plane Node—Fabric Wireless Controllers Only	• If the Control Plane node is reachable, the score is good. • If the Control Plane node is unreachable, the score is poor. **Note** If there is more than 1 Control Plane node in a fabric network, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1.

Effects of Maintenance Mode on Network Health Scores and KPI Metrics

When a network device (router, switch, wireless controller, or access point) is placed in maintenance mode, its clients are also placed in maintenance mode. For example, when you place a Cisco Wireless Controller in maintenance mode, any APs associated with the wireless controller are also placed in maintenance mode. Cisco DNA Center treats all devices in maintenance mode the same, regardless of whether a device was placed in maintenance mode as an administrative action or as a result of its association with a device.

Network health scores and KPI metrics do not include network devices that are in maintenance mode, because while a network device is in maintenance mode, Cisco DNA Center does not perform the following tasks for the device:

- Gather health data.

- Collect interface statistics.

- Trigger issues.

- Include the device in calculating health scores, such as site health scores.

When you access network health scores and KPI metrics while a device is in maintenance mode, Cisco DNA Center displays a banner indicating that a device is in maintenance mode. In addition, start and end times of the maintenance window are indicated in the device 360 pages and logged as events in the system status log. The dashboards allow you to filter by devices that are in maintenance mode.

Figure 9: Device 360 Page With Maintenance Banner
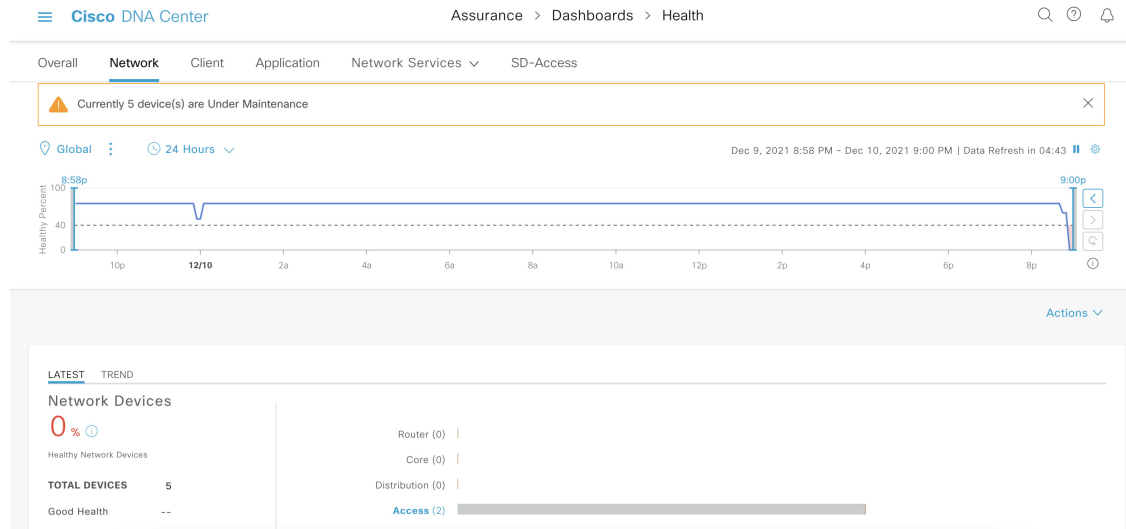
Cisco DNA Center continues to perform the following tasks for a device that is in maintenance mode:

- Relevant events are still generated and can be displayed in the event viewer during maintenance mode.

- Maintenance-related operations, such as image upgraded, bulk provisioning, and so on still trigger events.

- The availability report in Assurance is not impacted.

- Topology is not impacted.

Monitor and Troubleshoot Overall Enterprise Health

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.

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

Monitor and Troubleshoot the Overall Health of Your Enterprise

Use this procedure to get a global view of the health of your enterprise, which includes network devices and clients, and to determine if there are potential issues that must be addressed.

Before you begin

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

Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Figure 10: Overall Health Dashboard
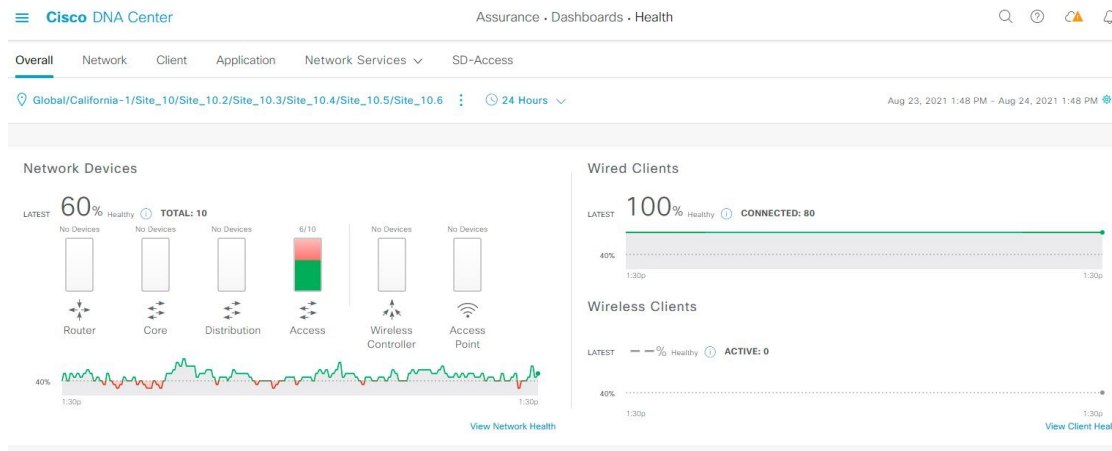
Step 2 Use the **Overall** health dashboard top menu bar for the following functionality:

Overall Health Dashboard Top Menu Bar	
Item	**Description**

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

Time range	Enables you to display data for the last 3 hours, 24 hours, or 7 days.

Overall Health Dashboard Top Menu Bar	
Item	**Description**
Actions drop-down list	Enables you to export the overall dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**. Enables you to customize the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 281 and Create a Custom Dashboard, on page 277.

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

Overall Health Summary Dashlet	
Item	**Description**
Network Devices	**Network Score**: Percentage of healthy (good) devices (routers, switches, wireless controllers, and access points) in your overall enterprise. See Network Health Score, on page 90. **Device Category Health Score**: Percentage of healthy (good) network devices for the following device categories: **Router**, **Core**, **Distribution**, **Access**, **Controller** and **Access Point**. **Note** When an SD-Access fabric is selected, this area provides the percentage of healthy network devices for the following categories: **Fabric Edge**, **Fabric Border**, and **Fabric Control Plane**. Click **View Network Health** to open the **Network Health** dashboard. See Monitor and Troubleshoot the Health of Your Network, on page 67.
Wired Clients and **Wireless Clients**	Provides the score distribution between wired and wireless clients. The **Wired Client** score or the **Wireless Client** score is the percentage of healthy (good) wired or wireless client devices in your overall enterprise. See Client Health Score, on page 121. Click **View Client Health** to open the **Client Health** dashboard. See Monitor and Troubleshoot the Health of All Client Devices, on page 101.

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

Network Services Dashlet	
Item	**Description**
AAA	Provides the total percentage of successful and failure transactions for all the AAA servers in your overall enterprise. Click **View AAA Dashboard** to open the **Network Services AAA** dashboard. See Monitor the AAA Network Service, on page 153.
DHCP	Provides the total percentage of successful and failure transactions for all the DHCP servers in your overall enterprise. Click **View DHCP Dashboard** to open the **Network Services DHCP** dashboard. See Monitor the DHCP Network Service, on page 156.

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

Note	AI Network Analytics must be enabled for site analytics data to be collected. Click the **Enable AI Network Analytics** link to go directly to the **Cisco AI Analytics** window where you can configure this system setting. For more information, see Configure Cisco AI Network Analytics, on page 61.
	If AI Network Analytics isn't enabled, Assurance displays an example dashlet with sample data.

Site Analytics Dashlet

Displays the aggregated coverage, onboarding, roaming, and connection speed KPI statistics for sites that fall below the performance thresholds.

Under each KPI category, click a site name to display more information about the site and its performance.

Step 6 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 188.

Monitor and Troubleshoot Client Health

About Clients

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

Monitor and Troubleshoot the Health of All Client Devices

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

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

Assurance uses machine learning algorithms to extract behavioral patterns in the network and predict trends. These trends are displayed as baselines in the **Client Onboarding Time** and **Client Count Per SSID** dashlets.

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

Before you begin

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

Step 1 Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2 Click the **Client** tab.

The **Client** health dashboard appears.

Figure 11: Client Health Dashboard
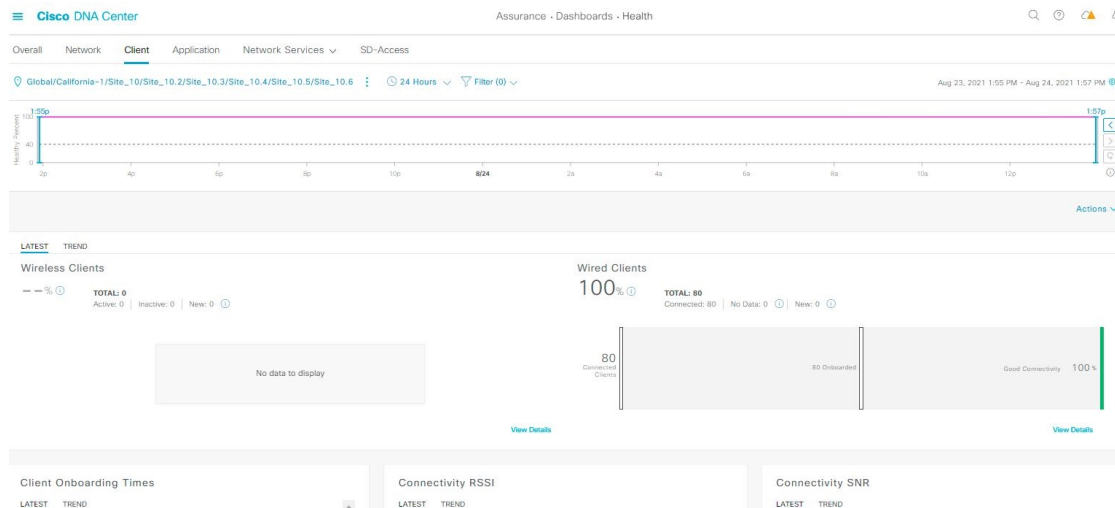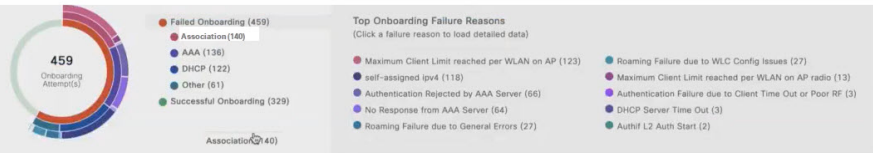
Step 3 Use the **Client** health dashboard top menu bar for the following functionality:

Client Health Dashboard Top Menu Bar	
Item	**Description**

ⓥ Global
 	
Location pane
	Click to display the following icons:
	
	• Click ⓥ Global ⋮ to choose an area/site or building from the left hierarchy tree pane. You can also click down arrow from global to navigate to its associated area, site, and building.
	
	  You cannot choose a floor from the network hierarchy.
	
	• Click ⋮ next to the location icon and choose **Site Details** to view the Sites table.
	
	• Click ⊘ **Hide Sites** to hide the Sites table.
	
	• ☰ ◨ : Click this toggle button and use the drop-down list to view the percentage of healthy clients in a table format for a site or building. Click **Apply** for a location to only display the location's client information in the **Client Health** dashboard.
	
	• ☰ ◨ : Click this toggle button to display the health of all the client sites on a geographic location-oriented client health map. By default, the client sites 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 the client is inactive.
	
	  From the **Go to sites** column, click ⇥ for a site or building to display data only for that location on the **Client Health** dashboard.

Client Health Dashboard Top Menu Bar	
Item	**Description**
🕐 **Time Range** setting	Enables you to display data within a specified time range on the dashboard. Do the following: a. From the drop-down menu, choose the length of the range: **3 Hours**, **24 Hours**, or **7 Days**. b. Specify the **Start Date** and time; and the **End Date** and time. c. Click **Apply**.
Filter icon	Contains the **SSID** and **Band** options. Choose the SSIDs and band frequency from the drop-down list by selecting the check boxes next to them, and then click **Apply**. Depending on your selection, the information in the dashboard is refreshed. **Note** You can choose multiple SSIDs. For example, if you choose Class 1 and Class 2 SSIDs, the dashboard displays information for the clients that are connected to Class 1 SSID and Class 2 SSID.
Actions drop-down list	Enables you to export the client dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**. Enables you to customize the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 281 and Create a Custom Dashboard, on page 277.

Step 4   Use the **Timeline Slider** to view the healthy client percentage for a more granular time range.

Hover your cursor within the timeline to view the wireless and wired client health score percentage at a specific time.

You can click and drag the timeline boundary lines to specify the time range. This sets the context for client data that is displayed in the dashboard dashlets.

You can use the arrow buttons on the right of the timeline to view data for up to 30 days.

The dotted horizontal line represents the threshold value for healthy clients, which by default is set to 40%.

To change the threshold value:

a. Hover your cursor over the information (🛈) icon.

b. In the tooltip, click the edit (✏) icon.

c. In the **Client Health Threshold** slide-in pane, click and drag the blue line to set the threshold percentage value.

d. Click **Save**.

Note   Changing the custom threshold affects when the Client Summary Health Score is displayed as red. The custom threshold does not change the number of healthy or unhealthy devices.

Step 5   Use the **Client Health Summary** dashlet for the following functionality:

Client Health Summary Dashlet	
Item	**Description**

Client Health Summary area	Includes the following tabs:
	
	• **Latest**: Displayed by default. Includes the following:
	
	    • **Wireless Clients** and **Wired Clients Health Summary Score**: The Wireless and Wired Client Summary Health score is the percentage of clients that onboarded successfully and have good connectivity. See Client Health Score, on page 121.
	
	    • **Total Devices**: Provides the total number of clients and the count of active, inactive, and new clients. Cisco DNA Center defines active, inactive, and new clients based on their activity within a 5-minute health score calculation window, as follows:
	
	        • **Active**: Clients who have successfully onboarded and are sending sufficient data to meet the data threshold, clients who have successfully onboarded and then disconnected, clients attempting to onboard and fail, and clients attempting to onboard but were excluded.
	
	        • **Inactive**: Clients who don't send sufficient data to meet the data threshold. After a user-idle timeout period expires, the wireless controller deauthenticates inactive clients.
	
	        • **New**: Clients who are in the process of onboarding. The health score for these clients is included in the next 5-minute calculation window.
	
	    • **Charts**: This snapshot-view chart provides the distribution of clients that passed or failed to onboard within the last 5 minutes. Then, from the number of clients that onboarded successfully (passed), the chart provides the percentage of clients that have good or fair connectivity.
	
	• **Trend**: Displays a trend chart that shows the health of clients over a time period.
	
	For the clients that failed to onboard, the reason for the onboarding failure is provided. Examples include AAA, DHCP, and Other.
	
	The color in the charts represents the health of the client devices:
	
	🔴: Poor client devices. Health score range is 1 to 3.
	🟠: Fair client devices. Health score range is 4 to 7.
	🟢: Good client devices. Health score range is 8 to 10.
	⚪: Inactive client devices. Health score is 0.

View Details	Click **View Details** to open a slide-in pane with additional details. The radial bar chart provides the distribution of clients that failed to onboard, and the reason for the onboarding failure. You can click each segment to view the failure reasons. • 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 in your network. The following tables describe the KPI dashlets.

> **Note**   The chart data is updated every 5 minutes.

Client Onboarding Times Dashlet	
Item	**Description**
Client Onboarding Times chart	Distribution of all clients' attempts to onboard, in all the sites or a selected site, over time. This dashlet provides the percentage of clients that took less than 10 seconds to successfully onboard. Client onboarding covers Association, Authentication, Addressing, WebAuth, and DNS phases. There are two types of charts: **Latest**: Displayed by default. This snapshot-view chart provides the distribution of clients that passed or failed to onboard within the last 5 minutes. Then, from the number of clients that onboarded successfully (passed), the chart provides the percentage of clients that have good or fair connectivity. **Trend**: Contains the **Client Count** and **Baseline** tabs. Click the **Baseline** tab to display the onboarding time baseline chart, which is generated through machine learning. **Note** The **Baseline** tab will be deprecated in the near future. For AI Network Analytics features, you must enable AI Network Analytics. See Configure Cisco AI Network Analytics, on page 61 and Cisco AI Network Analytics Overview, on page 9. **Important** To view the baseline chart, you must choose a site and SSID from the **Filter** options. The chart details for the baseline charts are represented by different colors. **Green band**: Predicted baseline value. **Solid blue line**: Actual value. For the clients that failed to onboard, the reason for the onboarding failure is provided. Examples include AAA, DHCP, and Other.

Client Onboarding Times Dashlet	
Item	**Description**
View Details	Click **View Details** to open a slide-in pane with additional details: - The left pane contains the **Overall**, **Association**, **Authentication** and **DHCP** tabs. Click the tabs to populate the charts in the right pane. - The right pane contains **Charts** that have the following tabs: **Latest**: Contains the overall average onboarding time. For Authentication and DHCP, the Latest tab contains a drop-down list to filter the data based on the Avg Latency Time, Avg Authentication Time for Authentication, and Avg DHCP Time for DHCP. **Trend**: Contains the **Baseline** tab, which allows you to view machine learning baseline charts. Depending on the tab you choose in the left pane, additional tabs display under **Trend** > **Baseline**. For example, the **Client Count**, **Time Baseline**, or **Failure Baseline** tabs appear for Association, Authentication, or DHCP data. Note: **Failure Baseline** data is available only for the Global site. Note: The **Baseline**, **Time Baseline**, and **Failure Baseline** tabs will be deprecated in the near future. For AI Network Analytics features, you must enable AI Network Analytics. See Configure Cisco AI Network Analytics, on page 61 and Cisco AI Network Analytics Overview, on page 9. - Hover and move your cursor over the charts to view synchronized tooltips that display information at a selected point in time. - Click a color segment in the chart to view the following: - Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs**, **Top Bands**, and **Top Host Operating Systems**. - A table with detailed data of the clients in that segment.

Connectivity RSSI Dashlet	
Item	**Description**
Connectivity RSSI chart	Received Signal Strength Indication (RSSI) distribution for all clients, in all sites or a selected site. This dashlet provides the percentage of RSSI measurements for all clients whose RSSI measurement is higher than the threshold value of -72 dBm.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: - Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs**, **Top Bands**, and **Top Host Operating Systems**. - A table with detailed data of the clients in that segment.

Connectivity SNR Dashlet	
Item	**Description**
Connectivity SNR chart	Signal-to-Noise ratio (SNR) distribution of all clients, in all sites or a selected site. This dashlet provides the percentage of SNR measurements for all clients whose SNR measurement is higher than the threshold value of 10 dB.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs**, **Top Bands**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Client Roaming Times Dashlet	
Item	**Description**
Client Roaming Times chart	Distribution of the clients by roaming times and failures. This dashlet provides the percentage of clients with roaming times less than 3000 ms.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Access Points**, **Top SSIDs**, **Top Host Device Types**, **Top Bands**, **Top Locations**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Client Count per SSID Dashlet	
Item	**Description**

Client Count per SSID chart	Distribution of the number of clients per SSID, in all sites or a selected site, over time.
	
	There are two types of charts:
	
	   • **Latest**: Displayed by default. This snapshot-view chart provides the distribution of clients per SSID or selected site.
	
	   • **Trend**: Contains **Client Count** and **Baseline** tabs. Click the **Baseline** tab to display the SSID baseline chart, which is generated through machine learning.
	
	      Note The **Baseline** tab will be deprecated in the near future. For AI Network Analytics features, you must enable AI Network Analytics. See Configure Cisco AI Network Analytics, on page 61 and Cisco AI Network Analytics Overview, on page 9.
	
	      Important To view the SSID machine learning baseline chart, you must choose a site and SSID from the **Filter** options.
	
	   • The chart details for the baseline charts are represented by different colors.
	
	      • **Green band**: Predicted baseline value.
	
	      • **Solid blue line**: Actual value.

View Details	Click **View Details** to open a slide-in pane with additional details.
	
	Contains two types of charts:
	
	   • **Latest**
	
	   • **Trend**: Contains the **Baseline** tab, which allows you to view machine learning baseline charts.
	
	      Note The **Baseline** tab will be deprecated in the near future. For AI Network Analytics features, you must enable AI Network Analytics. See Configure Cisco AI Network Analytics, on page 61 and Cisco AI Network Analytics Overview, on page 9.
	
	Hover and move your cursor over the charts to view synchronized tooltips that display information at a selected point in time.
	
	Click a color segment in the chart to view the following:
	
	   • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top Bands**, and **Top Host Operating Systems**.
	
	   • A table with detailed data of the wireless clients in that segment.

Connectivity Physical Link Dashlet	
Item	**Description**
Connectivity Physical Link chart	Distribution of wired client device link state—the number of client devices that had their physical links up, down, and had errors.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Locations**, **Top Switches**, **Top Host Device Types**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Client Count per Band Dashlet	
Item	**Description**
Client Count per Band chart	Distribution of wireless clients connected to the 2.4-GHz band or 5-GHz band. Hover your cursor over a segment to view the percentage and number of clients connected to a specific band.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs** and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Client Data Rate Dashlet	
Item	**Description**
Client Data Rate chart	Distribution of a client's data rates. Use the **Client Protocol** drop-down list to filter clients based on the client protocol they are using. Options are **802.11n/ac/ax** and **802.11a/b/g**.
View Details	Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to view: • Data type categories by client count: **Top Locations**, **Top Access Points**, **Top Host Device Types**, **Top SSIDs**, **Top Bands**, and **Top Host Operating Systems**. • A table with detailed data of the clients in that segment.

Step 7   Use the **Client Devices** dashlet to view detailed information about the clients in your network. This dashlet provides the following functionality:

Client Devices Dashlet	
Item	**Description**
Type	Filter the table based on client type. Options are **Wired** and **Wireless** clients.
Health	Filter the table based on the client health with the following options: • **All** • **Inactive**: Client devices with a health score of 0. • **Poor**: Client devices with a health score range from 1 to 3. • **Fair**: Client devices with a health score range from 4 to 7. • **Good**: Client devices with a health score range from 8 to 10. • **No Data**: Client devices with no data.
Data	Filter the table based on data type with the following options: • **Onboarding Time >= 10 s**: Onboarding time is greater than or equal to the 10-second threshold value. • **Association >= 5 s**: Association time is greater than or equal to the 5-second threshold value. • **DHCP >= 5 s**: DHCP time is greater than or equal to the 5-second threshold value. • **Authentication >= 5 s**: Authentication time is greater or equal to 5 seconds. • **RSSI <= -72 dBm**: RSSI is less than or equal to the -72-dBm threshold value. • **SNR <= 9 dB**: SNR is less than or equal to the 9-dB threshold value.

Client Devices Dashlet	
Item	**Description**

Client Device table	View detailed client device information in a table format. The client device table displays the following information by default:
	
	• **Identifier**: Displays the client's user ID, hostname, or MAC address based on availability, in that order. For example, if the user ID is not available, the hostname is displayed. If the user ID and hostname are not available, the MAC address is displayed.
	
	  The **Identifier** column also has specific icons that allow you to determine if the client device is wired or wireless.
	
	• **MAC Address**: Displays the MAC address, which includes Device MAC and Randomized and Changing MAC Address (RCM). The Private MAC ⧉ icon appears in front of the RCM. You can filter the table based on the type of MAC address, such as All, Device MAC, and RCM.
	
	• **IPv4 Address**: Displays the client's IPv4 address based on availability.
	
	  Note You can display the client's IPv6 address by checking the **IPv6 Address** check box in the ⋮ menu.
	
	• **Device Type**: Displays the device type.
	
	• **Health**: Displays the average of the onboarding and connected scores. The Client Health score is calculated every 5 minutes.
	
	  Note A score of -- indicates that the client has recently onboarded (new). New clients are clients that attempted to onboard after the 5-minute health score calculation window started. The health score for these new clients is included in the next 5-minute calculation window.
	
	• **Tracked**: Displays client tracking status.
	
	• **Last Seen**
	
	• **AP Name** (for wireless clients only): Displays the name of the access point.
	
	• **Switch** (for wired clients only)
	
	• **Port** (for wired clients only)
	
	• **Location**: Displays the assigned location of the client.
	
	• **Security Group (Tag Value)**: Displays the security group tag value for wired clients only.
	
	• **Bridge-Mode Virtual Machine**: Displays bridge mode virtual machine for wireless clients only.
	
	• **Link Speed** (for wired clients only): Indicates the speed capacity of the interface or physical port. If the port has negotiated to a certain speed, the negotiated speed is displayed.
	
	  Note You can display the link speed by checking the **Link Speed** check box in the ⋮ menu.

Client Devices Dashlet	
Item	**Description**
Tracked Clients	Click **Tracked Clients** to view the slide-in pane that displays a table containing the **MAC Address**, **Last Detected**, **Tracking Duration**, **Description**, and **Randomized MACs**.
Excluded Clients	Click **Excluded Clients** to view the slide-in pane that displays the client exclusion list containing the **Excluded MAC address**, **Excluded Since**, **Impacted Wireless Controllers**, and **Description**. For more information about excluding clients, see Configure Excluded Clients, on page 112.
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.
⋮	Customize the data you want displayed in the table: a. Click ⋮ . b. Check the check boxes for the data you want displayed in the table. c. Click **Apply**.
Export	Click **Export** to export the table data to a CSV file. **Note** The data from all available columns is included even if the column was not selected for the table. Filters applied to the client table are applied to the exported data.

Configure Excluded Clients

Use this procedure to configure excluded clients for Cisco Wireless Controllers. Using the **Excluded Clients** option, you can configure the following:

- Add clients to the exclusion list.
- Edit the clients in the exclusion list.
- Add the wireless controllers for which you want to exclude clients.
- Delete clients from the exclusion list.

Step 1 Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2 Click the **Client** tab.

Step 3 From the **Client Devices** dashlet, click **Excluded Clients**.

Step 4 In the **Excluded Clients** slide-in pane, to add clients to the exclusion list, use one of the following methods:

- To select clients from the drop-down list, click **Add** and configure the following.

    a. From the **MAC Address** drop-down list, choose a MAC address. Alternatively, you can enter a valid MAC address in the search field and click the plus icon (┼) to add the MAC address.

    b. In the **Description for Exclusion** field, enter a description.

    c. (Optional) To add another MAC address, click the plus icon (⊕).

    d. Click **Next**.

    e. Check the check box next to the wireless controller for which you want to exclude clients.

    f. Click **Save**.

    • To import the list of clients in CSV format, click **Import Client List (CSV)**.

    a. Click **CSV Sample** to download the sample CSV file.

    b. Edit the sample CSV file to include the client information.

    c. Drag and drop the CSV file into the file upload area. Alternatively, you can click **Choose a file** and navigate to where your CSV file is located, and then click **Upload**.

    d. Click **Next**.

    e. Check the check box next to the wireless controller for which you want to exclude clients.

    f. Click **Save**.

Step 5   To edit the clients in the exclusion list, do the following:

    a) Check the check box next to the excluded MAC addresses that you want to edit.
    b) Hover your cursor over **Actions** and choose **Edit**.
    c) Edit the description and click **Save**.

Step 6   To add the wireless controllers for which you want to exclude clients, do the following:

    a) Check the check box next to the excluded MAC addresses for which you want to add wireless controllers.
    b) Hover your cursor over **Actions** and choose **Add WLC**.
    c) Check the check box next to the wireless controller for which you want to exclude clients.
    d) Click **Save**.

Step 7   To delete clients from the exclusion list, do the following:

    a) Check the check box next to the excluded MAC addresses that you want to delete.
    b) Hover your cursor over **Actions** and choose **Delete**.
    c) Click **Yes**.

Monitor and Troubleshoot the Health of a Client Device

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

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

Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **Client** tab.

The **Client** health dashboard appears.

Step 3   Do one of the following:

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

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

Figure 12: Client 360 Window
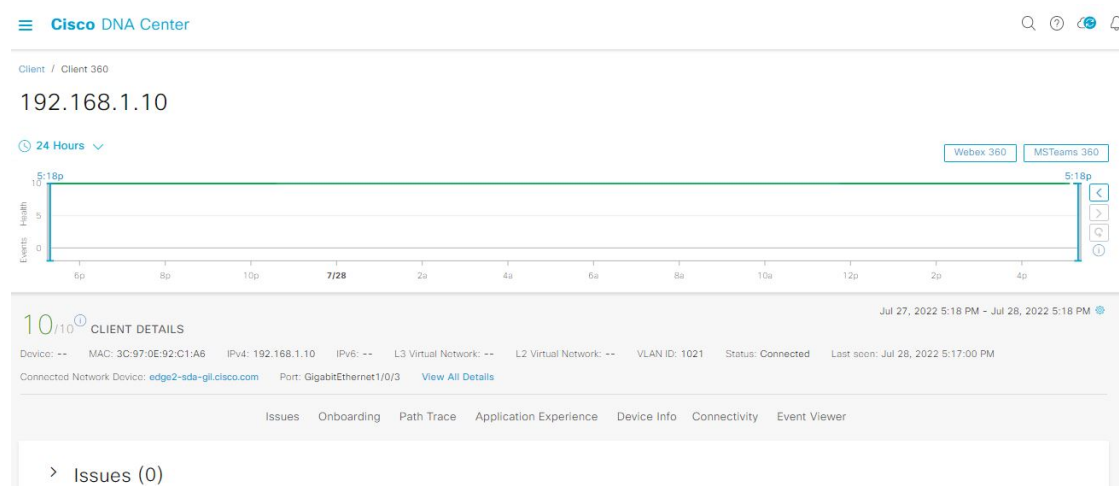
Step 4   Click the time range setting (🕘) at the top-left corner to specify the time range of the data that you want displayed on the window:

a)   From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.

b)   Specify the **Start Date** and time; and the **End Date** and time.

c)   Click **Apply**.

Step 5   Click **Intelligent Capture** at the top-right corner of the window to view, monitor, and troubleshoot captured onboarding and data packets for a specific client device to determine if there are potential issues that must be addressed. See Enable a Live Capture Session for a Client Device, on page 318.

Note	Intelligent Capture is not supported for all AP models. If **Intelligent Capture** is not displayed, verify that the client is connected to a supported AP model, and that the AP is assigned to a location on the **Network Health** dashboard.

Step 6 Click **MS Teams 360** at the top-right corner above the timeline slider to view, monitor the client MS Teams meetings.

The **Application Experience for MS Teams** slide-in pane is displayed.

To configure a Microsoft Teams integration, see *Configure MS Teams Integration* in the Cisco DNA Center Administrator Guide.

Use the **Application Experience** slide-in pane for the following functionality:

- **Search bar**: You can search for meetings in the table displayed.

- **Time Range filter**: Click time filter to specify time range for the data you want to be displayed in the table.

- Client Meetings table is displayed, which contains **Meeting Name**, **MS Teams Score**, **Network APM Score**, **Duration**, **Start Time**, **End Time**, **Status**, **Meeting Type**, and **Participants**.

Note Network APM score is a health score, which is calculated based on NetFlow exported from the managed network devices. For more information regarding APM, see Supported Platforms, on page 126.

You can select the meeting to view the meeting quality KPI data displayed below the table as following:

- Click **Audio Quality** tab to display an **MS Teams Score** and **Network APM Score**. You can see the Metrics such as **Packet loss**, **Jitter**, and **Media Bitrate** in a graph view.

- Click **Video Quality** tab to display an **MS Teams Score** and **Network APM Score**. You can see the Metrics such as **Packet loss**, **Jitter**, and **Media Bitrate** in a graph view.

- Click **Share Quality** tab to display an **MS Teams Score** and **Network APM Score**. You can see the Metrics such as **Packet loss**, **Jitter**, and **Media Bitrate** in a graph view.

Step 7 Click **Webex 360** at the top-right corner above the timeline slider to view, monitor the client Webex meetings. The search meeting pop-up window is displayed.

To configure Webex integration, see *Configure Webex Integration* in the Cisco DNA Center Administrator Guide.

a) Enter the email associated with the client's Webex meeting.
b) Click **Search Meetings**. The Application Experience for Webex slide-in pane is displayed.
c) Use the Application Experience slide-in pane for the following functionality:

- **Search bar**: You can search for meetings in the table displayed.

- **Time Range filter**: Click time filter to specify time range for the data you want to display in the table.

- Client Meetings table is displayed, which contains meeting number, meeting name, application, network duration, start time, end time, and status.

  You can select the meeting to view the meeting quality KPI data displayed below the table as horizontal bars showing Audio quality, Video Quality and Share Quality based on application (data retrieved using Webex API) and network (data retrieved using NetFlow) latencies. You can use the drop-down list to filter the data based on Transmitting and Receiving options to display the application and network latency graphs related metrics such as packet loss, jitter, and so on.

Step 8 Use the timeline slider to view the health and events information about the client device over a period of time. 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. |

- **Onboarding**: You can hover your cursor over the timeline slider to view the client's onboarding times, including Association, Authentication, and DHCP.

- **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   View the individual client health score in the **Client Details** area, below the timeline.

The individual client health score is an aggregate of the client's onboarding status, RSSI, and SNR.

If you search by the user ID, the Individual Client Health score that is displayed is the minimum score of all the monitored client devices associated with that user. For more information, see Individual Client Health Score, on page 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 10   Use the **Client Details** area, below the timeline, to view the following information:

- For wireless clients, this area provides information about the client device such as its OS version, MAC address includes Device MAC and RCM, IPv4 and IPv6 address, Bridge-Mode Virtual Machine, connected VLAN ID, connection status, last seen timestamp, connected network device, SSID, and last known location.

- For wired clients, this area provides information about the client device such as its MAC address, IPv4 and IPv6 address, Security Group (Tag Value), connected VLAN ID, connection status, last seen timestamp, connected network device, port, and last known location.

- For PoE-capable devices, the following elements are also displayed in the client details area: **IEEE Class**, **Negotiated Power Level**, and **PoE Status**.

Step 11   In the **Client Details** area, click **View All Details** to open a slide-in pane with additional details about the client device.

Step 12   Use the collapsible categories to view information about issues, onboarding, event viewer, path trace, application experience, and details:

Issues Category

Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first.

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

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

- To resolve an issue:

    a. From the drop-down list, choose **Resolve**.

    b. To view the list of issues that have been resolved, click **Resolved Issues**.

- To ignore an issue:

    a. From the drop-down list, choose **Ignore**.

    b. Set the number of hours to ignore the issue on the slider.

    c. Click **Confirm**.

    d. To view the list of issues that have been ignored, click **Ignored Issues**.

For information about the types of issues, see .

Onboarding Category

Topology of how a client got on the network, including information about the following services: AAA and DHCP.

Example of wired client topology: Client > Switch > Router

Example of wireless client topology: Client > SSID > Access Point > Wireless Controller

In the topology, you can do the following:

- Click a node to display a slide-in window that displays information about the node.

- Hover your cursor over the link ends (dots) to see the status and port details of the link.

- Hover your cursor over a group of devices and click **View Devices List** from the pop-up to view the list of devices and their details.

- In the Search field in the top-right corner of the **Onboarding** area, you can search for a specific device. The specific node is selected, and the corresponding information about the device is displayed.

Event View Category

For Wireless Clients: Lists scenarios and the sequence of subevents that led to each scenario. This allows you to pinpoint during which subevent an issue occurred. The following scenarios are provided for wireless clients:

- **Re-Authentication**

- **Broadcast Rekey**: Process of changing the session key—the encryption key of an ongoing communication—to limit the amount of data encrypted with the same key.

- **Onboarding**

- **DHCP**

- **Delete**

- **INTRA-Roaming**

- **INTER-Roaming**

- **ASSOC**

- **AUTH**

- **EAP**

- **DISASSOC**

- **DEAUTH**

- **11r Failure**

- **OKC Failure**

- **EAP Failure**

When an issue occurs, that event is marked red; otherwise, it's green. The Event Viewer table provides information about the failure, such as the error message, the AP and wireless controller to which the client device is connected, and the timestamp when the event occurred. Click an event to view details about that event in the right pane.

For Wired Clients: Lists ISE server events, switch system level syslogs, switch port or interface-specific events, and client-specific events. For the list of messages under each event category, see Messages Displayed in the Event Viewer for Wired Clients, on page 120.

Successful events are displayed as green; failure events that impact the health score are displayed as red. The Event Viewer table provides information about the failure, such as the type of message, the device information to which the wired client device is connected, and the timestamp when the event occurred. Click an event to view details about that event in the right pane.

Path Trace Category

Click **Run New Path Trace** to display a network topology between a specified source device and a destination device. The topology includes the path's direction and the devices along the path, including their IP addresses. The display also shows the protocol of the devices along the path (**Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**) or other source type.

See Perform a Path Trace, on page 341.

Application Experience Category

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

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

See About Application Experience and Application Visibility, on page 125 and View Application Experience of a Host, on page 131.

Detail Information Category

Click one of the following tabs to display the corresponding information:
 	
• **Device Info**: Displays basic information about the device.
 	
  For Samsung devices, this tab displays additional information, such as build number, origin, country code, device type (mobile, tablet, and so on), and host operating system.
 	
  This tab also displays the **Tracked** and **Exclusion** status of the device. If required, click the corresponding hyperlink to update the tracked and exclusion status of the device.
 	
  In the **Track Client** slide-in pane, do the following:
 	
  a. Use the toggle button to configure the tracked status of the device.
 	
  b. If you enable the toggle button, choose the required option for **Tracking Expires After** and **Notification Frequency**.
 	
  c. Click **Save**.
 	
  In the **Exclude clients** slide-in pane, do the following:
 	
  a. Use the toggle button to configure the exclusion status of the device.
 	
  b. If you enable the toggle button, enter a description in the **Description for Exclusion** field, and check the check box next to the wireless controller for which you want to exclude the device.
 	
  c. Click **Save**.
 	
  Station Information: Only available for Intel devices. Displays details such as HW model, SW version, AC/DC voltage, and so on.
 	
• **RF**: Only available for wireless devices.
 	
• **User Defined Network**: Only available for UDN-enabled network devices. This tab displays the Registered UDN, Connected UDN details, device MAC address, device owner, device name, device type, and current status.
 	
• **Connectivity**: Displays the new connection KPI named Retries. The connection retries for radios are displayed in the retries chart.
 	
• **PoE**: Only available for PoE-capable clients.
 	
• **iOS Analytics**: Only available for Apple devices.
 	
• **Intel Connectivity Analytics**: Only available for devices supported by Intel wireless adapters. Displays the Roam Events, Reported Errors, Temporary Disconnection Reports, and Low RSSI Reports reported by the supported client.

Messages Displayed in the Event Viewer for Wired Clients

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

ISE Server Event
Client AUTH FAILURE
Client AUTH SUCCESS

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

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

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

Understand Client Health Score and KPI Metrics

This section provides information about how the client health scores and KPI metrics are computed.

Client Health Score

The Client Health score (Wireless or Wired) is the percentage of the number of healthy client devices (a health score from 8 to 10) in a target category, divided by the total number of client devices in that category. The score is calculated every 5 minutes.

For example: 90% (health score) = 90 (client devices in a target category with health score from 8 to 10) ÷ 100 (total number of client devices in that category)

The Individual Client Health score is the sum of the Client Onboarding score and the Client Connectivity score. The client health score ranges from 1 to 10, with a score of 0 for inactive clients. It is calculated as follows:

Wired Client: Link to first switch is up, authentication and authorization is successful and IP address is received. Client score is 10.

Wireless Client: Client joined the network and has good connection in terms of the RSSI and SNR KPIs.

Client Onboarding Score

The Client Onboarding score indicates the experience of a client device *while* connecting to the network.

- If a client connects to the network successfully, the score is 4.

- If a client failed to connect to the network, the score is 1.

- If a client is idle, the score is 0.

The Client Onboarding score is calculated as follows:

Wired Client: Link to the first switch is up, authentication and authorization is successful, and IP address is received.

Wireless Client: Client Onboarding score range is from 1 to 4. When the client connects to the network successfully, the score is 4. If the client failed to connect to the network, the score is 1.

Client Connectivity Score

The Client Connectivity score indicates the experience of the client device *after* the device is connected to the network. The score is calculated as follows:

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

- If a client onboards successfully but has link errors, the Connectivity score is 2 and the Overall Health score is 6.

- If the client onboards successfully and there are no link errors between the client and the first-hop switch, the Connectivity score is 6 and the Overall Health score is 10.

Wireless Client: Connectivity score can be 0, 4, or 10. The RSSI and SNR range determines the Connectivity score and the resulting Overall Health score is calculated as the weighted average of the RSSI-driven Connectivity score and the SNR-driven Connectivity score.

RSSI-Driven Connectivity Score	
Client's RSSI	**RSSI-Driven Connectivity Score**
If RSSI is less than or equal -72 dBm.	The client receives a RSSI-driven connectivity score of 4 and is considered to be in fair health.
If RSSI is greater to -72 dBm.	The client receives a RSSI-driven connectivity score of 10 and is considered to be in good health.

SNR-Driven Connectivity Score	
Client's SNR	SNR-Driven Connectivity Score
If SNR is less than or equal to 9.	The client receives a SNR-driven connectivity score of 4 and is considered to be in fair health.
If SNR is greater than 9.	The client receives a SNR-driven connectivity score of 10 and is considered to be in good health.

Individual Client Health Score

The Individual Client Health score is the sum of the Client Onboarding score and the Client Connectivity score. The client health score ranges from 1 to 10, with a score of 0 for inactive clients. It is calculated as follows:

Wired Client: Link to first switch is up, authentication and authorization is successful, and IP address is received. Client score is 10.

Wireless Client: Client joined the network and has good connection in terms of RSSI and SNR KPIs.

Client's Onboarding and Connectivity	Resulting Client Health Score
If the client failed onboarding.	The client receives a health score of 1 and is considered to be in poor health.
If the client's RSSI and SNR are below threshold.	The client receives a health score of 4 and is considered to be in fair health.
If either the client's RSSI or SNR is below threshold.	The client receives a health score of 7 and is considered to be in fair health.
If the client's RSSI and SNR is above threshold.	The client receives a health score of 10 and is considered to be in good health.

Monitor Application Health

About Application Experience and Application Visibility

Assurance processes complex application data and presents the findings in Assurance health dashboards to provide insight into the performance of applications.

You can view the health data from a device perspective (**Device 360** window), from the user perspective (**Client 360** window), or from the application perspective (**Application 360** window).

Depending from where the data is collected, you can see some or all of the following:

- Application Name
- Throughput
- DSCP Markings
- Performance Metrics (Latency, Jitter, and Packet Loss)

Application Name and Throughput are collectively referred to as **Quantitative** metrics. Data for the Quantitative metrics comes from enabling **Application Visibility**.

DSCP Markings and Performance Metrics (Latency, Jitter, and Packet Loss) are collectively referred to as **Qualitative** metrics. Data for the Qualitative metrics comes from enabling **Application Experience**.

Application Visibility

Application Visibility data is collected from switches running IOS-XE, and from wireless controllers running AireOS.

For switches running IOS-XE, Application Visibility data is collected using a predefined NBAR template that is applied bidirectionally (ingress and egress) to the physical layer access switch ports.

For wireless controllers running AireOS, Application Visibility data is collected at the wireless controller, and then streaming telemetry is used to transport this data to Cisco DNA Center.

Application Experience

Application Experience data is collected from Cisco IOS-XE router platforms, specifically using the Cisco Performance Monitor (PerfMon) feature and the Cisco Application Response Time (ART) metrics.

Examples of router platforms include ASR 1000, ISR 4000, and CSR 1000v. For device compatibility with Cisco DNA Center, see the Cisco DNA Center Compatibility Matrix.

To view the Cisco Performance Monitor feature availability, use the Cisco Feature Navigator tool. Click **Research Features**, and then add **Easy Performance Monitor Phase II** in the filter field.

Optimized Application Performance Monitoring

Optimized Application Performance Monitoring (APM) is a feature on the device that reduces the overhead in collecting NetFlow data. APM is supported on Cisco IOS-XE routers, Cisco 9800 series wireless controllers, and the Cisco DNA Traffic Telemetry Appliance. For minimum software versions, see .

Supported Platforms

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

> **Note** For device compatibility with Cisco DNA Center, see Cisco DNA Center Compatibility Matrix.

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

Cisco Platform Support for Application Experience and Application Visibility in Cisco DNA Center		
Platform	**Data Collection**	**Notes**
Catalyst 9000 Series Switches	Application Visibility data collection for 9200, 9300, 9400.	• Requires a Cisco DNA Advantage license. • IOS XE 16.10.1 minimum software version. • IP routing must be enabled.
Cisco AireOS Wireless Controllers	Application Visibility data collection.	• Requires a Cisco DNA Advantage license. • Requires 8.8 MR2 software version—8.8.114.130 or later.
Cisco 9800 Series Wireless Controller	Application Visibility data collection for Flex/Fabric SSIDs. Application Experience data collection for central switching/local SSIDs.	• For Optimized APM—IOS XE 16.12.1 minimum software version.
Cisco DNA Traffic Telemetry Appliance	Application Experience data collection.	• Requires a Cisco DNA Advantage license. • For Optimized APM—IOS XE 17.3 minimum software version.

Criteria for Enabling Application Telemetry on Devices

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

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

Note
- The conventional tagging-based algorithm is supported and has precedence over the newer automatic interfaces or WLAN selection algorithm.

- If you want to switch over from the automatic selection algorithm to the tagging-based algorithm, you must disable telemetry before provisioning the tagged SSIDs to the devices.

The following table provides the criteria for selecting interfaces and WLANs based on the conventional tagging-based algorithm (with **lan** keyword) and the new automatic selection algorithm for all the supported platforms:

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm

Router	• Interface description has the **lan** keyword.[12]
	
	• Interface is a physical interface.
	
	• Interface has an IP address other than the management IP address.
		• Interface has an IP address other than the management IP address.
		
		• Interface is not any of the following:
		
		  • WAN
		
		  Note An interface is treated as a WAN-facing interface if it has a public IP address, and if there is a route rule with a public IP address that routes through the interface.
		
		    In this context, a public IP address is not in a private range (for example, not in 192.168.x.x, 172.16.y.y, 10.z.z.z), or is an IP address that is not in the system's IP pools.
		
		    Route rules can be dynamically learned. In this context, the **show ip route** command does not show a route to a public IP address that goes through this interface.
		
		  • Loopback.
		
		  • Management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, or FASTETHERNET1.

Switch	• Interface description has the **lan** keyword.[1, 2]
	
	• Switch port is configured as an access port.
	
	• Switch port is configured with the **switch-mode access** command.
		• Interface is a physical interface.
		
		• Access port does not have neighbors.
		
		• Interface is not any of the following:
		
		  • Management interface: FASTETHERNET0, FASTETHERNET1, GIGABITETHERNET0/0, or MGMT0
		
		  • LOOPBACK0, Bluetooth, App Gigabit, WPAN, Cellular, or Async
		
		  • VSL interface.

Platform	Conventional Tagging-Based Algorithm	Automatic Selection Algorithm
Cisco AireOS Controller	• WLAN profile name is tagged with the **lan** keyword.[1, 2]	If the SSIDs are mixed, that is Local mode, Flex mode, and Fabric mode, Wireless Service Assurance (WSA) processing is enabled. If all the SSIDs are in Local mode, NetFlow is enabled.
Cisco Catalyst 9800 Series Wireless Controller with Optimized Application Performance Monitoring (APM) profile and IOS release 16.12.1 and later.	WLAN profile name is tagged with the **lan** keyword.[1, 2]	If the SSIDs are mixed—that is, Local mode, Flex mode, and Fabric mode—the Cisco Application Visibility and Control (AVC) basic record is configured. If all the SSIDs are in Local mode, the Optimized APM record is configured.
	Note If you want to update the telemetry configuration, you must disable telemetry and then enable it after making the configuration changes.	
Cisco DNA Traffic Telemetry Appliance with Optimized APM profile and IOS release 17.3 and later.	• Interface description has the **lan** keyword.[1, 2] • Interface is a physical interface.	• Interface is a physical interface. • Interface is not a management interface: GIGABITETHERNET0, GIGABITETHERNET0/0, MGMT0, FASTETHERNET0, and FASTETHERNET1.

[1] The **lan** keyword is case insensitive and can be separated by a space, hyphen, or underscore.
[2] Resynchronize the network device to read the **lan** interface description.

Application Health Prerequisites

This topic provides the prerequisites relating to application health for routers, AireOS wireless controllers, and switches.

Application Experience Prerequisites on Routers

- Requires Cisco IOS XE software with an active NBAR2 license.

- Application flows within the Layer 3 network are not visible.

- Traffic associated with the management interface is not part of Application Experience.

- Ports cannot be enabled for ETA.

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

- The conventional tagging-based algorithm (with keyword `lan`) is supported, but the newer automatic interface or WLAN selection algorithm allows you to enable Application Telemetry on interfaces or WLANs without tagging them with the keyword `lan`. For information about the criteria that is used, see .

Application Visibility Prerequisites on Switches

- Requires Cisco IOS XE software.

- Requires a Cisco DNA Advantage license.

- Implemented only on access ports that contain the command `switchport mode access`.

- Support for L2 logical interfaces is not available.

- Limited visibility if the switch port is connected to an AP and configured with `switchport mode access`.

- Ports cannot be enabled for ETA.

- Only IPv4 flows are monitored.

- Management interface Gig0/0 cannot be used as the source interface of a NetFlow export.

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

- The conventional tagging-based algorithm (with keyword `lan`) is supported, but the newer automatic interface or WLAN selection algorithm allows you to enable Application Telemetry on interfaces or WLANs without tagging them with the keyword `lan`. For information about the criteria that is used, see Criteria for Enabling Application Telemetry on Devices, on page 127.

Application Visibility Prerequisites on AireOS Wireless Controllers

- Requires a Cisco DNA Advantage license.

- Supported only on wireless controllers that have AireOS software and not on wireless controllers that have IOS XE software.

- NetFlow must be enabled on the Cisco AireOS wireless controllers.

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

- Flexible NetFlow (FNF) flow monitors are not implemented. Instead, Application Visibility data is collected using streaming telemetry by subscribing to the Client-app-stat-events channel.

- The conventional tagging-based algorithm (with keyword `lan`) is supported, but the newer automatic interface or WLAN selection algorithm allows you to enable Application Telemetry on interfaces or WLANs without tagging them with the keyword `lan`. For information about the criteria that is used, see Criteria for Enabling Application Telemetry on Devices, on page 127.

Application Visibility Prerequisites on Cisco 9800 Series Wireless Controller

- Requires IOS XE software for Optimized APM. See Criteria for Enabling Application Telemetry on Devices, on page 127.

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

Application Experience Prerequisites on Cisco DNA Traffic Telemetry Appliance

- Requires a Cisco DNA Advantage license.

- Requires IOS XE software for Optimized APM. See Criteria for Enabling Application Telemetry on Devices, on page 127.

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

- To enable visibility of CAPWAP-encapsulated wireless traffic, manually enter the **ip nbar classification tunneled-traffic CAPWAP** command on the Cisco DNA Traffic Telemetry Appliance.

Provision Application Telemetry Settings

Configure global telemetry settings as described in Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 60.

Step 1 Click the menu icon (☰) and choose **Provision** > **Network Devices** > **Inventory**.

The Inventory window displays the device information gathered during the discovery process. To view devices available in a particular site, expand the Global site in the left pane and select the site, building, or floor.

Step 2 Choose the devices that you want to provision.

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

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

a) **Enable Application Telemetry**: To configure application telemetry for the selected devices.
b) **Disable Application Telemetry**: To remove the application telemetry configuration from the chosen devices.

Step 4 Click **Apply**.

The **Application Telemetry** column shows the telemetry configuration status. If you don't see the **Application Telemetry** column in the default column setting, click the ellipsis icon (⋮) at the right end of the column headings and check the **Application Telemetry** check box.

View Application Experience of a Host

Use this procedure to view the qualitative and quantitative metrics of the applications running on a host.

Before you begin

- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover Your Network Using an IP Address Range, on page 25, Discover Your Network Using CDP, on page 23, or Discover Your Network Using LLDP, on page 26.

- Enable and configure Application Telemetry profile on network devices. See Provision Application Telemetry Settings, on page 131.

- See Application Health Prerequisites, 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, latency, and jitter. You can also include application delay for health score calculation. For more information, see Individual Application Health Score, on page 152.

         • **Usage Bytes**: The number of bytes transferred by the client for this application.

         • **Average Throughput**: The rate of the application traffic (in Mbps) flowing between the client and the server.

         • **DSCP**: The application's current (**Observed**) and default (**Expected**) DSCP value.

           Note   This metric is not available for Optimized APM.

         • **Packet Loss**: The percentage (maximum and average) of packet loss.

         • **Network Latency**: The network latency time (maximum and average) in milliseconds.

         • **Jitter**: The variance in time delay in milliseconds (maximum and average) between data packets over your network.

    c) To view the Application Experience metrics in chart format, click the radio button next to an application. The metrics are: **Throughput**, **Packet Loss**, **Jitter**, **Network Latency**, **Client Network Latency**, **Server Network Latency**, and **Application Server Latency**.

        Note   Application Visibility data that is exported by a Cisco Catalyst 9200 switch, Cisco Catalyst 9300 switch, or a Cisco AireOS wireless controller only provides data for Application Name, Usage, and Throughput.

View Application Experience of a Network Device

Use this procedure to view the qualitative and quantitative metrics of the applications running on a network device.

Before you begin

    • Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover Your Network Using an IP Address Range, on page 25, Discover Your Network Using CDP, on page 23, or Discover Your Network Using LLDP, on page 26.

- Enable and configure Application Telemetry profile on network devices. See Provision Application Telemetry Settings, on page 131.

- See Application Health Prerequisites, 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: **Business Relevant**, **Business Irrelevant**, or **Default**.

Note   The displayed data is based on the time you selected from the drop-down menu in the **Device 360** window. Options are **3 Hours**, **24 Hours** (the default), and **7 Days**.

b) Filter the Application Experience data for a specific VRF or a specific router interface by using the appropriate filters: **All VRFs** and **All Interfaces**.

Note   The **All VRFs** and **All Interfaces** filters are only available for routers.

c) View Application Experience data in the table:

- **Name**: The application name.

- **Health**: The health score is calculated on the basis of a combination of metrics of packet loss, latency, and jitter. You can also include application delay for health score calculation.

  Note   The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.

- **Usage Bytes**: The number of bytes transferred by the client for this application.

- **Average Throughput**: The rate of the application traffic (in Mbps) flowing between the client and the server.

- **DSCP**: The application's current (**Observed**) and default (**Expected**) DSCP value.

  Note   This metric is not available for Optimized APM.

- **Packet Loss**: The percentage (maximum and average) of packet loss.

- **Network Latency**: The network latency time (maximum and average) in milliseconds.

- **Jitter**: The variance in time delay in milliseconds (maximum and average) between data packets over your network.

d) To view the Application Experience metrics in chart format, click the radio button next to an application. The metrics are **Throughput**, **Packet Loss**, **Jitter**, **Network Latency**, **Client Network Latency**, **Server Network Latency**, **Application Server Latency**, and **Application Response Time**.

Note   Application Visibility data that is exported by a Cisco Catalyst 9200 switch, Cisco Catalyst 9300 switch, or a Cisco AireOS wireless controller only provides data for Application Name, Usage, and Throughput.

Monitor the Health of All Applications

Use this procedure to get a global view of applications at a site.

Before you begin

- Make sure that the devices (routers, switches, wireless controllers, and access points) are discovered. See Discover Your Network Using an IP Address Range, on page 25, Discover Your Network Using CDP, on page 23, or Discover Your Network Using LLDP, on page 26.

- Enable and configure the Application Telemetry profile on network devices. See Provision Application Telemetry Settings, on page 131.

- See Application Health Prerequisites, on page 129.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **Application** tab.

The **Application** health dashboard appears.

Figure 13: Application Health Dashboard

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

Application Health Dashboard Top-Menu Bar	
Item	**Description**
⦿ Global ⌄ **Location** drop-down list	Click to display the location icon. Click the location icon to display the **Site List View**. To view the application information from a specific site or building, click **Apply** in the appropriate row. The information is refreshed in the dashboard based on your selection.
🕐 **Time Range** setting	Enables you to display data within a specified time range on the dashboard. Do the following: a. From the drop-down menu, choose the length of the range: **3 Hours**, **24 Hours**, or **7 Days**. b. Specify the **Start Date** and time; and the **End Date** and time. c. Click **Apply**.
Filter	Choose the SSID from the drop-down list and then click **Apply**. Depending on your selection, the information in the dashboard is refreshed.
Actions drop-down list	Enables you to customize the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 281 and Create a Custom Dashboard, on page 277.
Application Health Timeline Slider	Enables you to view the healthy business-relevant application percentage, throughput, and agent test result for a more granular time range. Hover your cursor within the timeline to view the health score percentage at a specific time. You can click and drag the timeline boundary lines to specify the time range. This sets the context for application data that is displayed in the dashboard dashlets. You can use the arrow buttons on the right of the timeline to view data for up to 30 days.

Step 4 Use the **Summary** dashlet for the following functionality:

Summary Dashlet	
Item	**Description**
Summary	Displays the total number of business-relevant applications, data usage, and average throughput in your overall network or selected site.
Netflow	Displays the total number of NetFlow packets. Displays the total number of exporters. Click an exporter to view a slide-in pane that displays a table that contains device name, packet count, record count, and rate limit drops.

Summary Dashlet	
Item	**Description**
Enterprise Agent Tests	Displays the total number of ThousandEyes enterprise agents, tests, percentage of passed tests, alerts, and active alerts running on your supported Cisco Catalyst 9300 or 9400 Series switch. The following types of ThousandEyes agent tests are supported: • Network agent-to-server test: Collects network data, including jitter, packet loss, and latency • Web HTTP server test: Collects HTTP server data, including response time. To configure ThousandEyes Integration, see *Configure ThousandEyes Integration* in the Cisco DNA Center Administrator Guide.

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

Application Health Dashlet	
Item	**Description**
Business Relevant Application Health	Contains a health score for business-relevant applications. The health score is the percentage of healthy (good) business-relevant applications in your overall network, or selected site. See Understand Application Health Score and KPI Metrics, on page 152. The following charts are displayed: • Application count distribution trend chart that shows the count of all business-relevant applications over time, which is shown as a stacked area chart based on their health scores. • Circle chart that shows the count of business-relevant applications categorized by the application's health score. You can click a category to show the list of applications with the lowest health score within the category.

Application Health Dashlet	
Item	**Description**
Application Usage	• Circle chart: Shows the total application usage categorized by the application's business-relevance group. You can click a category to show the list of the top 10 applications by usage within the category.
	Note The application usage is the taken from the application's bidirectional traffic.
	• **View Details**: Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can:
	• Click the **All Applications**, **Business Relevant**, **Business Irrelevant**, and **Default** tabs to display a chart with its application usage and the top 10 applications by usage.
	• Filter the chart by application group or traffic class with the drop-down list at the top right of the slide-in pane.
	• Click a category in the chart to display the applications and its detailed information in the **Application** table.

Step 6   Use the **Application** dashlet for the following functionality:

Application Dashlet	
Item	**Description**
Type	Filter the table based on the business-relevance groups. Options are **Business Relevant**, **Business Irrelevant**, and **Default**.
Health	Filter the table based on the application's health scores. Options are:
	• **Poor**: Applications with a health score range from 1 to 3.
	• **Fair**: Applications with a health score range from 4 to 7.
	• **Good**: Applications with a health score range from 8 to 10.
	• **All**: All applications.
	• **Unknown**: Applications are missing qualitative metrics for determining a health score.

Application Dashlet	
Item	**Description**

Application table	View detailed application information in a table format. The application table displays 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).
	
	    Changing an application's name with the Application Policy package does not show the changed name in Application Experience. There is no integration between the Application Policy package and Application Experience.
	
	• If an application is not a standard application from the NBAR, its HTTP hostname or SSL common name is displayed, if available. These applications are assigned to the **Default** business-relevance group.
	
	    You can click the name to display a 360° view of an application. See Monitor the Health of an Application, on page 140.
	
	• Application table lists new applications as following:
	
	    ms-teams-video, **ms-teams-app-sharing**, **ms-teams-audio**, **ms-teams-media** and **ms-teams** applications. These are grouped under **microsoft-teams**.
	
	    Click **microsoft-teams** to display an MS Teams 360 view of Microsoft Teams applications. See Monitor and Troubleshoot the Health of a Microsoft Teams Application, on page 147.
	
	    webex-video, webex-audio, and webex-app-sharing. These are grouped under **webex**, where the data is collected from the NetFlow data.
	
	    Click **webex** to display a Webex 360 view of Webex applications. See Monitor and Troubleshoot Health of a Webex Application, on page 144.
	
	• **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. Jitter is for Real-time Transport Protocol (RTP)-based applications.

Application Dashlet	
Item	**Description**
⋮	Customize the data you want displayed in the table: a. Click ⋮ . b. Check the check boxes for the data you want displayed in the table. c. Click **Apply**.
Export	Click **Export** to export the table data to a CSV file. **Note** The data from all available columns is included even if the column is not selected for the table. Filters applied to the application table are applied to the exported data.

Step 7   Use the **Enterprise Agent Tests** dashlet for the following functionality:

Enterprise Agent Tests	
Item	**Description**
Enterprise Agent Tests table	View detailed **Enterprise Agent Tests** information in a table format. The agent table displays the following information by default: • **Test Name**: Displays the enterprise agent test name. Click the name to go to the ThousandEyes Agent page. • **Test Type**: Displays the name of the test type. • **Target**: Displays the target server used for the agent test. • **Device Name**: Displays the device name. • **Average Packet Loss (%)**: The average percentage of packet loss during data collection between agents and servers. • **Average Jitter**: The variance in time delay in milliseconds between data packets over your network. Jitter is for RTP-based applications. • **Average Latency**: The network latency time, in milliseconds, for TCP-based applications. • **# of Active Alerts**: Displays the number of active alerts during the agent test. • **# of Alerts**: Displays the total number of alerts during the agent test. • **# of Failed Tests**: Displays the number of failed agent tests. • **# of Alerts**: Displays the total number of agent tests.

Enterprise Agent Tests	
Item	**Description**
⚙	Customize the data that you want displayed in the table: a. From the **Table Appearance** tab, set the table density and striping. b. From the **Edit Table Columns** tab, check the check boxes for the data you want displayed in the table. c. Click **Apply**.
⬆ Export	Click **Export** to export the table data to a CSV file.

Monitor the Health of an Application

Use this procedure to view details about a specific application.

Step 1   Click the menu icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **Application** tab.

The **Application** health dashboard appears.

Step 3   In the **Application** table, click the name of an application.

The **Application 360** window appears, which provides a 360° view of the application.

Step 4   Click the time range setting (🕒) at the top-left corner to specify the time range for the data that you want displayed on the window:

a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.

b) Specify the **Start Date** and time; and the **End Date** and time.

c) Click **Apply**.

Step 5   To display application information for a particular location, choose the location from the *Location* drop-down list.

Step 6   From the **Filter** drop-down list, choose the SSID and click **Apply** to display the information for a particular SSID.

Step 7   Use the application health timeline slider to view the application's health score for a more granular time range and to view the application quality information.

Hover your cursor within the timeline to view the following information:

Health Score: The health score at a specific time is displayed. Metrics that are color-code in the Quality area contribute to the health score.

Quality: The Quality information area displays information about latency, jitter, and packet loss. For latency, the following aspects of delay between the client and the application are displayed:

     • LAN delay—The delay in milliseconds between the client and router.

• WAN delay—The delay in milliseconds between the router and server.

• Application delay—The delay in milliseconds between the server and the application.

Under Maintenance: When a device is under maintenance mode during the specific time period, the specific device name is displayed below the Under Maintenance banner.

You can click and drag the timeline boundary lines to specify the time range. This sets the context for the application data that is displayed in the Application 360 window.

Step 8   Use the **Application Details** area, below the timeline, to view the following information:

Application Details	
Item	**Description**
Health Score	The health score of an application is calculated based on the weighted average of the application's qualitative metrics, which include packet loss, network latency, and jitter. **Note** The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Time and Date range	Displays the time and date range for the data that is displayed in the **Application 360** window.
Business Relevance **Traffic Class** **Category**	Displays the application's Next Generation Network-Based Application Recognition (NBAR) classifying information.
Issues tab	Click to view the list of issues. See Step 8.
Exporters tab	Click to view the list of devices that send NetFlow traffic to Cisco DNA Center and other details. See Step 9.

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

Issues
Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first.
Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions.

From the slide-in pane, you can do the following:
 	
   • To resolve an issue:
 	
      a. From the drop-down list, choose **Resolve**.
 	
      b. To view the list of issues that have been resolved, click **Resolved Issues**.
 	
   • To ignore an issue:
 	
      a. From the drop-down list, choose **Ignore**.
 	
      b. Set the number of hours to ignore the issue on the slider.
 	
      c. Click **Confirm**.
 	
      d. To view the list of issues that have been ignored, click **Ignored Issues**.
 	
For information about the types of issues, see View and Manage Issues, on page 187.

Step 10 Click **Exporters** to view the following information:

Exporters	
Item	**Description**
Device	Displays the list of devices that is sending NetFlow traffic to Cisco DNA Center such as router, switch, wireless controller, and appliance. **Note** The following warning message is displayed for the device under maintenance mode during specific time range: The exporters with warning icon were in maintenance mode during the selected period of time.
Health Score	The last 5-minute health score. The health score is calculated on the basis of the application's qualitative metrics, which include packet loss, network latency, and jitter. **Note** The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Traffic Class	Displays the application's NBAR classifying information if available.
Go to Device 360	Click to open the **Device 360** window for a specific device.

Step 11 To view metric charts, do the following:

- For routers and appliances, click the exporter row to display charts (below the row) for the following metrics: usage, average throughput, packet loss, jitter, and latency.

- For switches and wireless controllers, click the device name to open a slide-in pane to view charts for the following metrics: usage and average throughput.

    You can also click **Device 360** in the slide-in pane to open the **Device 360** window for a specific device.

Metric Charts	
Charts	**Description**
Usage	The number of bytes transferred by the client for the particular application.
Throughput	The rate of the application traffic (in Mbps) flowing between the client and the server.
Packet Loss	The percentage (maximum and average) of packet loss. **Note** This metric is not available for switches and wireless controllers.
Latency	The network latency time (maximum and average) in milliseconds. The following latency charts are available: • Network Latency • Client Network Latency • Server Network Latency • Application Network Latency **Note** This metric is not available for switches and wireless controllers.
Jitter	The variance in time delay in milliseconds (maximum and average) between data packets over your network. **Note** This metric is not available for switches and wireless controllers.
DSCP	• **Observed**: The application's current DSCP value. • **Expected**: The default DSCP value assigned by NBAR. **Note** This metric is not available for Optimized APM.

Step 12 View the list of clients that are accessing the application in the **Application Endpoint** table (displayed after the metric charts).

Click the **Managed Clients** tab, if you want to view only the clients that are managed by Cisco DNA Center.

Details about each client is provided in the table, such as identifier (user ID, hostname, IP address, or MAC address, whichever is available in that order), client, client health, app health, usage, device type, MAC address, and VLAN ID.

For active clients, you can click the **Identifier** column to open the **Client 360** window.

You can view up to 100 clients in this table. To view additional clients, click **Show More**.

Step 13 (Optional) Customize the data you want displayed in the table:

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

Step 14 (Optional) To export the table data to a CSV file, click **Export**.

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

Monitor and Troubleshoot Health of a Webex Application

Use this procedure to view details about a Webex application.

Step 1 Click the menu icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2 Click the **Application** tab.

The **Application** health dashboard appears.

Step 3 In the **Application** table, click the **Webex** application.

The **Webex 360** window appears, which provides a 360° view of the application.

Figure 14: Webex 360

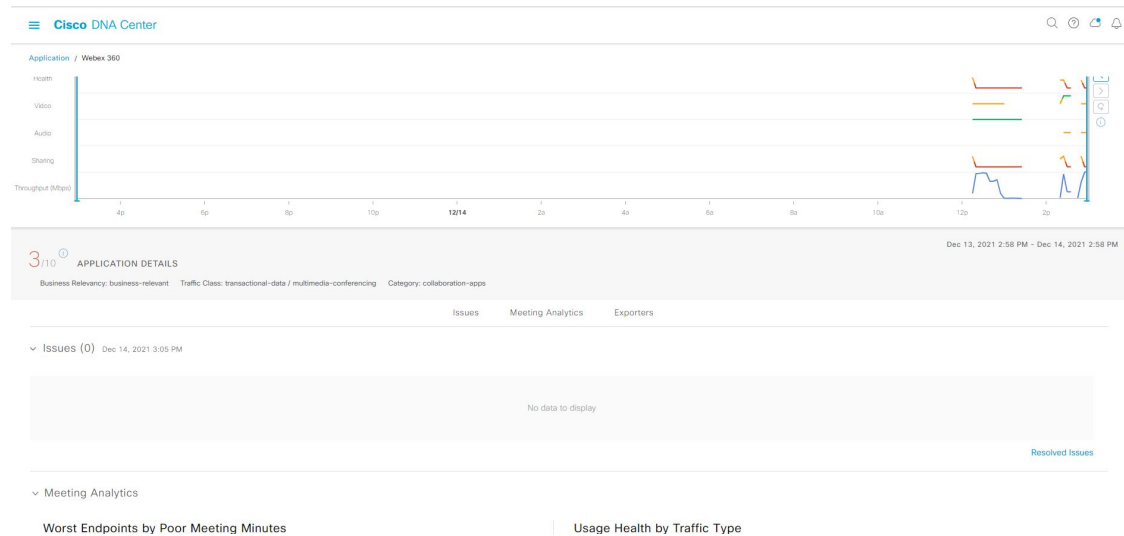**Step 4**   Use the **Summary dashlet** to view the total number of data usage, average throughput, and active clients in your overall network, or selected site.

Step 5   Click the time range setting ( ) at the top-left corner to specify the time range for the application data that you want displayed on the window:

a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.

b) Specify the **Start Date** and time; and the **End Date** and time.

c) Click **Apply**.

Step 6   To display application information for a particular location, choose the location from the *Location* drop-down list.

Step 7   Use the application health timeline slider to view the application's health score for a more granular time range, sub applications, the network quality and application quality information.

Hover your cursor within the timeline to view the health score at a specific time.

Step 8   Use the **Application Details** area, below the timeline, to view the following information:

Application Details

Item	Description
Health Score	The health score of an application is calculated based on the weighted average of the application's qualitative metrics, which include packet loss, network latency, and jitter.
Time and Date range	Displays the time and date range for the data that is displayed in the **Webex 360** window.
Business Relevance **Traffic Class** **Category**	Displays the application's Next Generation Network-Based Application Recognition (NBAR) classifying information.
Issues category	Click to view the list of issues. See Step 9.
Meeting Analytics	Click to view the Meeting Analytics data. See Step 10.
Exporters tab	Click to view the list of devices that send NetFlow traffic to Cisco DNA Center and other details. See Step 11.

Step 9   You can view information about issues from the **Issues** category:

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

b) From the slide-in pane, you can do 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 187.

Step 10   Use the **Meeting Analytics** dashlets for the following functionality:

Worst Endpoints by Poor Meeting Minutes
Click **Latest** and **Trend** chart to view the status of worst endpoints by poor meeting minutes. You can filter the data based on **By Percentage** or **By Total Poor Minutes**.

Usage Health by Traffic Type
Click **Latest** to view the chart to view usage health based on the traffic type for Audio, Sharing, and Video.
Click **Trend** to view the chart displays usage health based on the traffic type for Audio, Sharing, and Video.
You can hover on a color segment in the chart to view the percentage of health.

Step 11   Click **Exporters** to view the following information:

Exporters	
Item	**Description**
Device	Displays the list of devices that is sending NetFlow traffic to Cisco DNA Center such as router, switch, wireless controller, and appliance.
	Note The following warning message is displayed for the device under maintenance mode during specific time range:
	The exporters with warning icon were in maintenance mode during the selected period of time.
Health Score	The last 5-minute health score. The health score is calculated on the basis of the application's qualitative metrics, which include packet loss, network latency, and jitter.
	Note The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Traffic Class	Displays the application's NBAR classifying information if available.
Go to Device 360	Click to open the **Device 360** window for a specific device.

Step 12   To view metric charts for audio, video and sharing, do the following:

Metric Charts	
Charts	**Description**
Usage	The number of bytes transferred by the client for the particular application.

Metric Charts	
Charts	**Description**
Throughput	The rate of the application traffic (in Mbps) flowing between the client and the server. You can hover your cursor over chart to view the throughput value for audio, video, and sharing.
Packet Loss	The percentage (maximum and average) of packet loss. **Note** This metric is not available for switches and wireless controllers.
Latency	The network latency time (maximum and average) in milliseconds. The following latency charts are available: • Network Latency • Client Network Latency • Server Network Latency • Application Network Latency **Note** This metric is not available for switches and wireless controllers.
Jitter	The variance in time delay in milliseconds (maximum and average) between data packets over your network. **Note** This metric is not available for switches and wireless controllers.

Step 13   View the list of clients that are accessing the application in the **Application Endpoint** table (displayed after the metric charts).

Details about each client is provided in the table, such as identifier (user ID, hostname, IP address, or MAC address, whichever is available in that order), client, client health, app health, usage, device type, MAC address, and VLAN ID.

For active clients, you can click the **Identifier** column to open the **Client 360** window.

You can view up to 100 clients in this table. To view additional clients, click **Show More**.

Monitor and Troubleshoot the Health of a Microsoft Teams Application

Use this procedure to view details about a **Microsoft Teams** application.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.

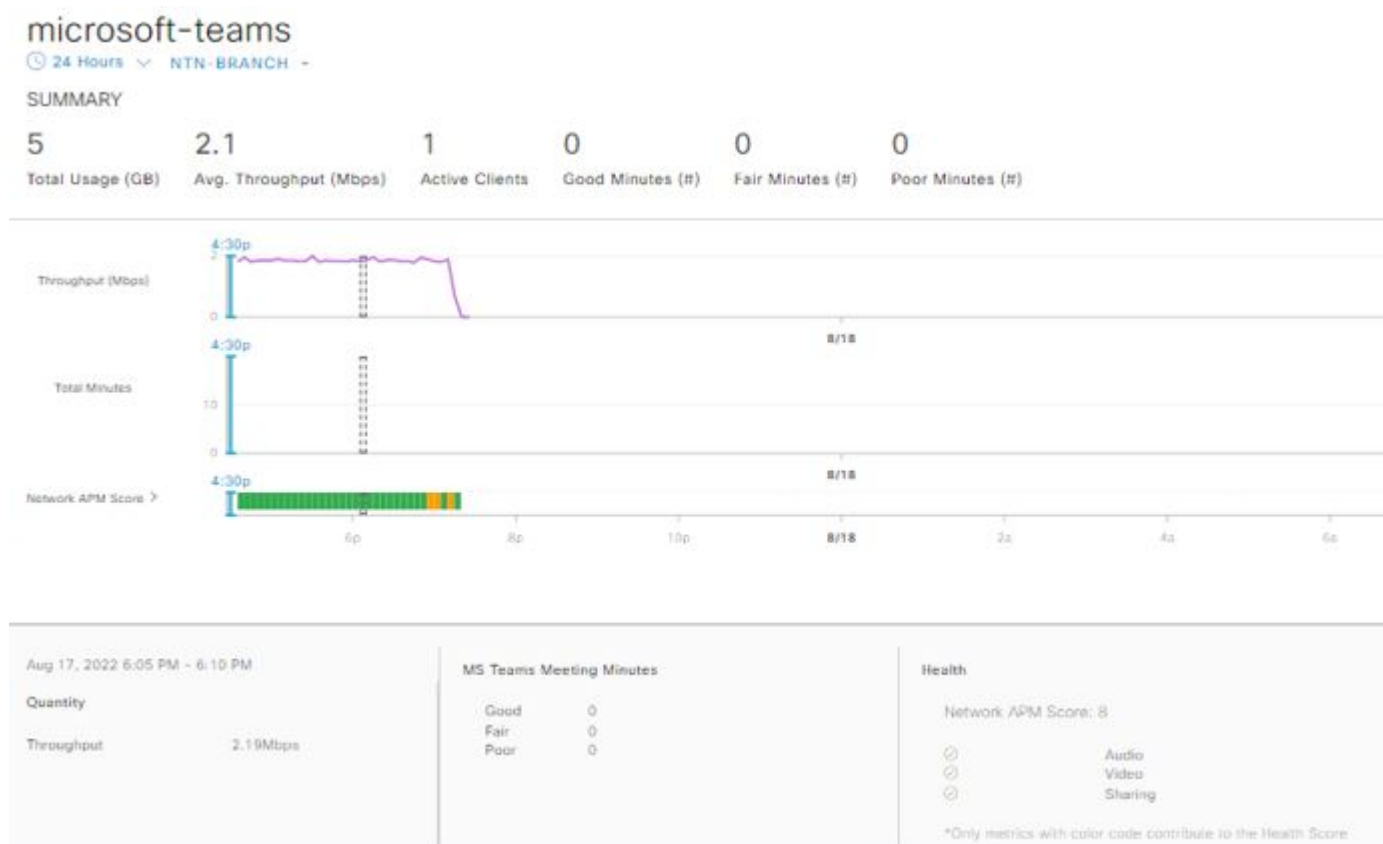The **Overall** health dashboard is displayed.

Step 2   Click the **Application** tab.

The **Application** health dashboard is displayed.

Step 3   In the **Application** table, click a **microsoft-teams** application.

An **MS Teams 360** window is displayed, which provides a 360° view of an application.

Figure 15: MS Teams 360

Step 4   Use the **Summary** dashlet to view the total number of data usage, average throughput, active clients, good minutes, fair minutes, and poor minutes in your overall network or selected site.

Step 5   In the top-left corner, click the time range setting (🕐) to specify the time range for the application data that you want to be displayed on the window.

   a)   From the drop-down menu, 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**.

   Note   By default, selected site and time range in the Application dashboard is displayed in an MS Teams 360.

Step 6   To display application information for a particular location, choose the location from the **Location** drop-down list.

Step 7   Use the application health timeline slider to view the **Throughput**, **Total Minutes**, and **Network APM Score**.

   Hover your cursor in the timeline to view the health score at a specific time.

   Note   Network APM score is a health score, which is calculated based on NetFlow exported from the managed network devices. For more information regarding APM, see Supported Platforms, on page 126.

Step 8   Use the **Application Details** area, below the timeline, to view the following information:

Application Details	
Item	**Description**
Time and Date range	Displays the time and date range for the data that is displayed in the **MS Teams 360** window.
Health	Displays the health score of **Audio**, **Video**, and **Sharing**.
Quantity	Displays **Throughput** data.
MS Teams Meeting Minutes	Displays information about **Good**, **Fair**, and **Poor** minutes.
Business Relevance **Traffic Class** **Category**	Displays the application's next generation Network-Based Application Recognition (NBAR) classifying information.
Issues category	Click to view the list of issues. See Step 9.
Meeting Analytics	Click to view the Meeting Analytics data. See Step 10.
Exporters tab	Click to view the list of devices that send NetFlow traffic to Cisco DNA Center and other details. See Step 11.

Step 9 You can view information about issues from the **Issues** category:

a) Click an issue to open a slide-in pane to view the corresponding details, such as a 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 187.

Step 10 Use the **Meeting Analytics** dashlets for the following functionality:

Meeting Analytics	
Item	**Description**
Top Access Devices	Click the **Latest** and **Trend** charts to view the status of top access devices by good and poor minutes.
	You can filter the data based on **By Poor Meeting Minutes**, **By Total Meeting Minutes**, **By Total Usage**, and **By Poor Network APM Score**.

Meeting Analytics	
Item	Description
Top Endpoints	Click the **Latest** and **Trend** charts to view the status of top access devices by good and poor minutes. You can filter the data based on **By Poor Meeting Minutes**, **By Total Meeting Minutes**, **By Total Usage**, and **By Poor Network APM Score**.

Step 11   Click **Exporters** to view the following information:

Exporters	
Item	Description
Device	Displays the devices that are sending NetFlow traffic to Cisco DNA Center. **Note** The following warning message is displayed for the device under maintenance mode during a specific time range: The exporters with warning icon were in maintenance mode during the selected period of time.
Health Score	The last 5-minute health score. The health score is calculated based on the application's qualitative metrics, which include packet loss, network latency, and jitter. **Note** The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.
Traffic Class	Displays the application's NBAR classifying information, if available.

Step 12   To view metric charts for audio, video, and sharing, do the following:

Metric Charts	
Charts	Description
Usage	The number of bytes transferred by the client for the particular application.
Throughput	The rate of the application traffic (in Mbps) flowing between the client and the server. You can hover your cursor over the chart to view the throughput value for audio, video, and sharing.
Packet Loss	The percentage (maximum and average) of packet loss. **Note** This metric is not available for switches and wireless controllers.

Metric Charts	
Charts	**Description**
Jitter	The variance in time delay in milliseconds (maximum and average) between data packets over your network. **Note** This metric is not available for switches and wireless controllers.

Step 13   View the list of clients that are accessing the application in the **Application Endpoint** table (displayed after the metric charts).

The table shows details about each client, such as identifier (user ID, hostname, IP address, or MAC address), client health, Network APM score, Microsoft Teams Score, usage, device type, MAC address, and VLAN ID.

For active clients, click the **Identifier** column to open the **Client 360** window.

You can view up to 100 clients in this table. To view additional clients, click **Show More**.

Configure Health Score Settings for Applications

Use this procedure to configure the health score settings for applications. You can customize the health score calculation for applications by changing the KPI thresholds on a per-traffic class basis and specifying the KPIs that are included for the calculation.

Step 1   Click the menu icon (☰) and choose **Assurance** > **Manage** > **Health Score Settings**.

Step 2   Click the **Application Health** tab.

Step 3   Click the tab of the application category to customize its health score calculation settings.

The tab displays the KPIs that affect the health score calculation of the application.

Step 4   From the **KPI Name** column, click the KPI name link.

The slide-in pane for the KPI appears.

Step 5   Configure the KPI health score settings:
a)   Customize the KPI threshold value for **Poor**, **Fair**, and **Good** health score.
b)   **Weight**: Valid weights are between 1–10. The higher the weight is, the KPI has more impact on the application health.
c)   Check **Include for health score** check box if you want this KPI to be included in the health score calculation.
d)   Click **Reset to Default** to restore the default KPI settings.

Step 6   Click **Apply**.

Understand Application Health Score and KPI Metrics

This section provides information about how the overall and individual application health scores and KPI metrics are computed.

Overall Application Health Score

The Application Health score is the percentage of the number of healthy business-relevant applications (a health score from 8 to 10), divided by the total number of business relevant applications. The score is calculated over the latest 5-minute interval.

Example: 90% (health score) = 90 (business-relevant applications with a health score from 8 to 10) ÷ 100 (total number of business-relevant applications)

Individual Application Health Score

The Individual Application Health score is calculated based on the weighted average of the application's qualitative metrics, which include packet loss, network latency, and jitter.

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

Individual Application Health Score = (Latency_Weight * Latency_VoS_Score + Jitter_Weight * Jitter_VoS_Score + PacketLoss_Weight * PacketLoss_VoS_Score) ÷ (Latency_Weight + Jitter_Weight + PacketLoss_Weight)

Note The health score is not available for Cisco Catalyst 9000 Series Switches and Cisco AireOS wireless controller. These devices do *not* poll the KPIs that are required to calculate a health score.

The workflow for calculating the Individual Application Health score is as follows:

1. Obtain the KPIs: Jitter, Latency, and Packet Loss.

2. Determine the application's Traffic Class based on the DSCP value from the flow record.

3. Convert the KPI numbers into Validation of Service score (VoS score) using the Cisco Validated Design (CVD) thresholds for each Traffic Class and KPI metric.

4. Get the weightage of the KPIs based on the application's Traffic Class and Tolerance level. The weightage is based on RFC4594.

5. Calculate the Application Health score. This is the weighted average of packet loss, network latency, and jitter.

Monitor Network Services

Monitor the AAA Network Service

Use this procedure to view and monitor all the AAA server transactions reported by wireless controllers in your network.

Note   **AAA Limitations**

- AAA Network Service supports wireless clients and Local mode.

- AAA Network Service does not support the following:

 - AireOS Wireless Controller

  - Flex mode or fabric mode

Before you begin

Ensure that you have installed a Cisco Catalyst 9800 Series Wireless Controller with version 17.6.1 or later and deployed with local mode AP.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.
The **Overall** health dashboard appears.

Step 2   Choose **Network Services** > **AAA**.

The **AAA** dashboard appears.

Figure 16: AAA Dashboard
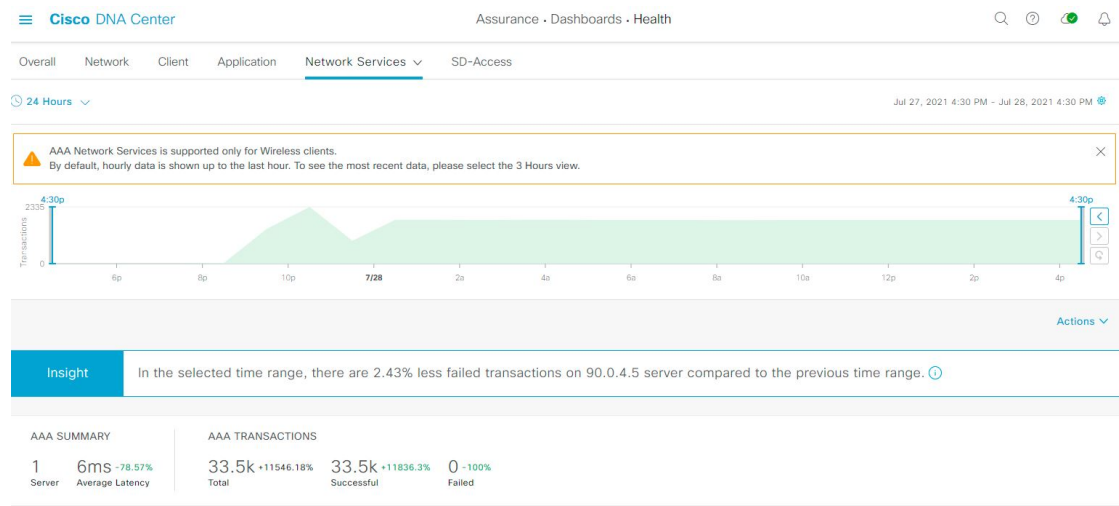
Step 3 Click the time range setting (🕐) at the top-left corner to specify the time range of the data that you want displayed:

a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.

b) Specify the **Start Date** and time and the **End Date** and time.

c) Click **Apply**.

Step 4 Click the autorefresh setting ⚙ at the top-right corner to enable or disable the **Data Auto Refresh** on the supported Assurance pages in a 5-minute refresh interval.

Step 5 Use the timeline slider to view the information about the total successful and failed transactions of the AAA server over a period of time. The timeline slider has the following functionality:

- You can hover your cursor over the timeline slider to view the AAA server transactions for a 5-minute window.

- When you double-click the timeline, it brings the timeline slider to a 1-hour time period. The entire window is refreshed, providing updates for that hour.

Step 6 Click the **Actions** drop-down list below the timeline slider for the following functionality:

- **Edit Dashboard**: Enables you to customize the dashboard display. See Change the Position of a Dashlet, on page 281 and Create a Custom Dashboard, on page 277.

Step 7 Use the **Insight** area, below the timeline, to view the percentage of successful AAA server transactions compared with the current and previous time range.

Step 8 Use the AAA summary dashlet to view the following information:

AAA Summary	
Item	**Description**
AAA Summary	Displays the number of AAA server and average latency (in ms) of your network.
AAA Transactions	Displays the percentage of total number of AAA transactions, successful transactions, and failed transactions in your network.

Step 9 Use the AAA server dashlets for the following functionality:

Top Sites by Highest Latency
The chart displays the top sites with the highest AAA server latency, in milliseconds.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can hover on a color segment in the chart to view the site with the highest AAA server latency.
You can select the data displayed as horizontal bars to filter the client table based on the top AAA servers, sites, SSIDs, and APs.

Top Sites by Transaction Failures
The chart displays the top sites with the highest AAA server transaction failures.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can hover on a color segment in the chart or its corresponding legend to view the site with the most AAA server transaction failures.
You can select the data displayed as horizontal bars to filter the client table based on the top AAA servers, sites, SSIDs, and APs.

AAA Server Latency
The chart displays the average AAA latency for each AAA server. You can filter the latencies based on **All**, **MAB**, or **EAP**.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can display the chart based on the filter selection to view the AAA server latencies.
You can select the data displayed as horizontal bars to filter the client table based on the top AAA servers, sites, SSIDs, APs, and so on.

AAA Server Transactions
The chart displays the average AAA server transaction status for each AAA server reported by wireless controllers. You can filter the status based on **All**, **Failures**, or **Successes**.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can display the chart based on the filter selection to view the AAA server transactions.
You can select the data displayed as horizontal bars to filter the client table based on the top AAA servers, sites, SSIDs, APs, and so on.

Step 10 Use the AAA Servers by WLC dashlets for the following functionality:

AAA Server by WLC Dashlet	
Item	**Description**
AAA Server table	View the AAA server information in a table format that contains AAA Server IP, WLC Name, WLC Location, Transactions, Failures, Avg Latency, and so on. Click **AAA Server IP** to open a slide-in pane that display the AAA server Avg Latency and Transaction charts.
	You can select the data displayed as horizontal bars to filter the client table based on the top AAA servers, sites, SSIDs, APs, and so on.

AAA Server by WLC Dashlet	
Item	**Description**
⬆ Export	Click **Export** to export the device information to a CSV file.
⚙	Customize the data that you want displayed in the table: a. From the **Table Appearance** tab, set the table density and striping. b. From the **Edit Table Columns** tab, check the check boxes for the data that you want displayed in the table. c. Click **Apply**.

Monitor the DHCP Network Service

Use this procedure to view and monitor all the DHCP server transactions reported by wireless controllers in your network.

✎

Note **DHCP Limitations**

      • DHCP Network Service supports wireless clients and Local mode.

      • DHCP Network Service does not support the following:

            • SD-Access fabric clients

            • AireOS Wireless Controller
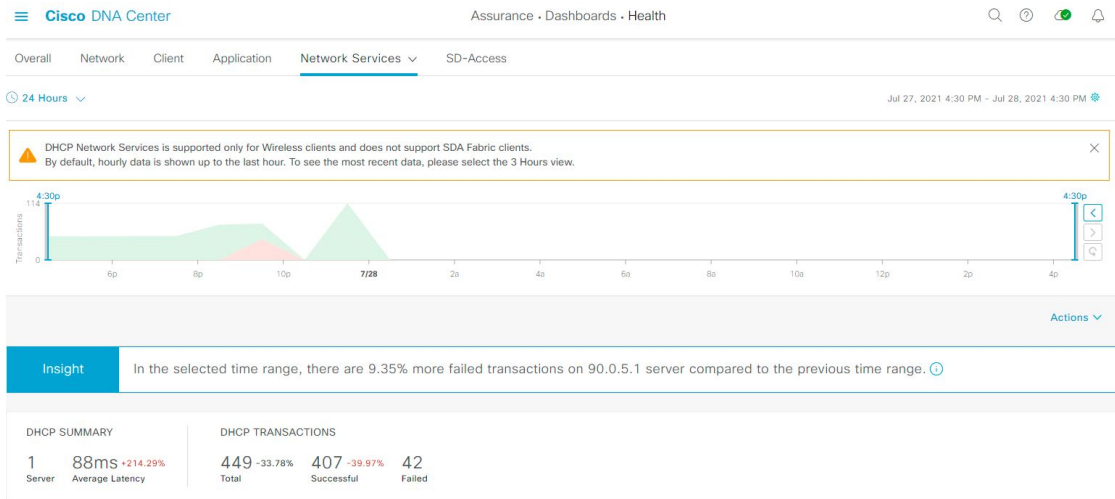
            • Flex mode or fabric mode

Before you begin

Ensure that you have installed a Cisco Catalyst 9800 Series Wireless Controller with version 17.6.1 or later.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.
The **Overall** health dashboard appears.

Step 2   Choose **Network Services** > **DHCP**.

The **DHCP** dashboard appears.

Figure 17: DHCP Dashboard

Step 3   Click the time range setting ( ) at the top-left corner to specify the time range of the data that you want displayed in the window:

a)   From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.

b)   Specify the **Start Date** and time and the **End Date** and time.

c)   Click **Apply**.

Step 4   Click the autorefresh setting at the top-right corner to enable or disable the **Data Auto Refresh** on the supported Assurance pages in a 5-minute refresh interval.

Step 5   Use the timeline slider to view the information about the total successful and failed transactions of the DHCP server over a period of time. The timeline slider has the following functionality:

   • You can hover your cursor over the timeline slider to view the DHCP server transactions for a 5-minute window.

   • When you double-click the timeline, it brings the timeline slider to a 1-hour time period. The entire window is refreshed, providing updates for that hour.

Step 6   Click the **Actions** drop-down list below the timeline slider for the following functionality:

   • **Edit Dashboard**: Enables you to customize the dashboard display. See Change the Position of a Dashlet, on page 281 and Create a Custom Dashboard, on page 277.

Step 7   Use the **Insight** area below the timeline to view the percentage of successful DHCP server transactions compared with the current and previous time range.

Step 8   Use the DHCP summary dashlet to view the following information:

DHCP Summary	
Item	**Description**
DHCP Summary	Displays the count of DHCP servers and average latency (in ms) of your network.
DHCP Transactions	Displays the percentage of total number of DHCP transactions, successful transactions, and failed transactions in your network.

Step 9 Use the DHCP server dashlets for the following functionality:

Top Sites by Highest Latency
The chart displays the top sites with the highest DHCP server latency, in milliseconds.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can hover on a color segment in the chart to view the site with highest DHCP server latency.
You can select the data displayed as horizontal bars to filter the client table based on the top DHCP servers, sites, SSIDs, and APs.

Top Sites by Transaction Failures
The chart displays the top sites with the most DHCP server transaction failures.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can hover on a color segment in the chart or its corresponding legend to view the site with the most DHCP server transaction failures.
You can select the data displayed as horizontal bars to filter the client table based on the top DHCP servers, sites, SSIDs, and APs.

DHCP Server Latency
The chart displays the average DHCP latency for each DHCP server. You can filter the latencies based on **All**, **Discover-offer**, or **Request-Ack**.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can display the chart based on the filter selection to view the DHCP server latencies.
You can select the data displayed as horizontal bars to filter the client table based on the top DHCP servers, sites, SSIDs, APs, and so on.

DHCP Server Transactions
The chart displays the average DHCP server transactions status for each DHCP server reported by wireless controllers. You can filter the status based on **All**, **Failures**, or **Successes**.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can display the chart based on the filter selection to view the DHCP server transactions.
You can select the data displayed as horizontal bars to filter the client table based on the top DHCP servers, sites, SSIDs, APs, and so on.

Step 10 Use the DHCP Servers by WLC dashlets for the following functionality:

DHCP Server by WLC Dashlet	
Item	**Description**
DHCP Server table	View the DHCP server information in a table format that contains AAA Server IP, WLC Name, WLC Location, Transactions, Failures, Avg Latency, and so on. Click **DHCP Server IP** to open the slide-in pane that display the Server Avg Latency and Transaction charts.
	You can select the data displayed as horizontal bars to filter the client table based on the top DHCP servers, sites, SSIDs, APs, and so on.

DHCP Server by WLC Dashlet	
Item	**Description**
⬆ Export	Click **Export** to export the device information to a CSV file.
⚙	Customize the data that you want displayed in the table: **a.** From the **Table Appearance** tab, set the table density and striping. **b.** From the **Edit Table Columns** tab, check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.

Monitor and Troubleshoot SD-Access Health

SD-Access Fabric

Fabric technology is an integral part of SD-Access. A fabric network is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric network in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.

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.

Add a Fabric Site

Before you begin

You can create a fabric site only if IP Device Tracking (IPDT) is already configured for the site.

Step 1	Click the menu icon (☰) and choose **Provision** > **Fabric Sites**.
Step 2	Under **SUMMARY**, click the number that indicates the count of fabric sites.
Step 3	Click **Create Fabric Sites and Fabric Zones**.
	Alternatively, instead of the first three steps, click the menu icon (☰) and choose **Workflow** > **Create Fabric Sites and Fabric Zones**.
Step 4	In the **Create Fabric Sites and Fabric Zones** window, click **Let's Do it** to go directly to the workflow.
Step 5	In the **Fabric Site Location** window, choose an area, building, or floor to add as a fabric site.

Step 6   In the **Wired Endpoint Data Collection** window, ensure that the **Wired Endpoint Data Collection** check box is checked.

Step 7   In the **Authentication Template** window, do the following:

a)   Choose an authentication template for the fabric site:

- **Closed Authentication**: Any traffic before authentication is dropped, including DHCP, DNS, and ARP.

- **Open Authentication**: A host is allowed network access without having to go through 802.1X authentication.

- **Low Impact**: Security is added by applying an ACL to the switch port, to allow very limited network access before authentication. After a host has been successfully authenticated, additional network access is granted.

- **None**

b)   (Optional) If you choose **Closed Authentication**, **Open Authentication**, or **Low Impact**, click **Edit** to edit the authentication settings:

- **First Authentication Method**: Choose **802.1x** or **MAC Authentication Bypass (MAB)**

- **802.1x Timeout (in seconds)**: Use the slider to specify the 802.1x timeout, in seconds.

- **Wake on LAN**: Choose **Yes** or **No**.

- **Number of Hosts**: Choose **Unlimited** or **Single**.

- **BPDU Guard**: Use this check box to enable or disable the Bridge Protocol Data Unit (BPDU) guard on all the **Closed Authentication** ports.

- **Pre-Authentication Access Control List**: Enable the toggle button to configure preauthentication control for **Low Impact** authentication. From the **Implicit Action** drop-down list, choose an implicit action. Enter a description for the rule. To add an access contract, click **Add Contract Action**, choose the rules, and click **Apply Table**.

Step 8   In the **Fabric Zones** window, choose one of the following options:

- To designate fabric zones later, click **Setup Fabric Zones Later**.

- To designate fabric zones and create scoped subnets, click **Setup Fabric Zones Now** and choose a fabric site from the network hierarchy displayed.

Step 9   In the **Summary** window, review the fabric site settings.

You can edit any of the fabric site or zone settings here.

Step 10   Click **Deploy**.

It takes a few seconds for the site and zones to be provisioned. Upon successful creation of the site, a **Success! Your fabric site is created** message is displayed.

Add a Device to a Fabric

After you have created a fabric site, you can add devices to the fabric site. You can also specify whether the device should act as a control plane node, an edge node, or a border node.

You can add a new device to the fabric site only if IP Device Tracking (IPDT) is configured for the fabric site.

A device which is assigned the Access role and has been provisioned before enabling IPDT on the site can't be added to the fabric. Reprovision such devices before adding them to the fabric site. Check the Provision workflow to confirm the status of **Deployment of IPDT** on the device.

Note

- It's optional to designate the devices in a fabric site as control plane nodes or border nodes. You might have devices that don't occupy these roles. However, every fabric site must have at least one control plane node device and one border node device. In the current release for wired fabric, you can add up to six control plane nodes for redundancy.

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

Before you begin

Provision the device if you haven't already provisioned it:

- The **Provision** > **Network Devices** > **Inventory** window displays the discovered devices.

- The topology view shows a device in gray 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.

Note

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

Step 1 Click the menu icon (☰) and choose **Provision** > **Fabric Sites**.

Step 2 Under **SUMMARY**, click the number that indicates the count of fabric sites.

Step 3 Select the fabric site to add a device.

The resulting topology view displays all devices in the network that have been inventoried. In the topology view, any device that is added to the fabric is shown in blue.

Step 4 From the **List** view under the **Fabric Infrastructure** tab, click a device. A slide-in pane displays the following **Fabric** options:

Option	Description
Edge Node	Toggle the button next to this option to enable the selected device as an edge node.
Border Node	Toggle the button next to this option to enable the selected device as a border node.
Control Plane Node	Toggle the button next to this option to enable the selected device as a control plane node.

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

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

Step 5   Click **Add**.

What to do next

After a device is added to the fabric, fabric compliance checks are automatically performed to ensure that the device is fabric-compliant. The topology displays a device that has failed the fabric compliance check in blue color with a cross-mark beside it. Click **See more details** on the error notification to identify the problem area and correct it.

Monitor and Troubleshoot the Health of Your SD-Access Fabric

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

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

Before you begin

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

To monitor and troubleshoot fabric sites, you must first configure the fabric site. See Add a Fabric Site, on page 161 and Add a Device to a Fabric, on page 162.

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

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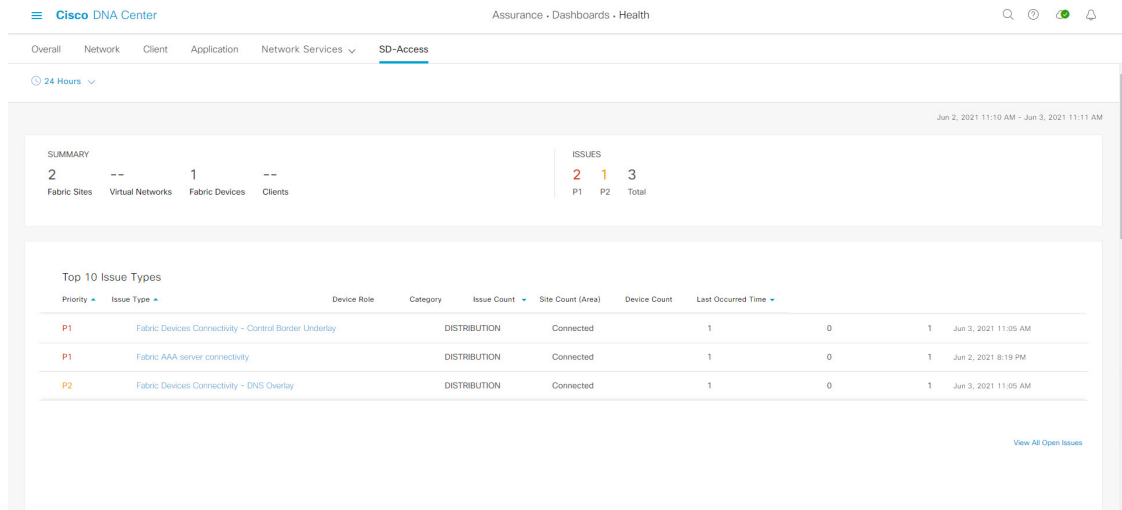

Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **SD-Access** tab.

The **SD-Access** health dashboard appears.

Figure 18: Network Health Dashboard

Step 3   Click the time range setting ( ) in the top-menu bar to specify the time range of data that appears on the dashboard.

a) From the drop-down menu, choose the time range: **3 Hours**, **24 Hours**, or **7 Days**.

b) Specify the **Start Date** and time; and the **End Date** and time.

c) Click **Apply**.

Step 4   Use the SD-Access Health Summary dashlet for the following functionality:

Item	Description
Summary	• **Fabric Sites**: Number of fabric sites. • **Virtual Networks**: Number of virtual networks. • **Fabric Endpoints**: Number of fabric endpoints. • **Endpoints**: Number of endpoints. • **Transits and Peer Networks**: Number of transits and peer networks.
Issues	• **P1**: Number of priority 1 issues. • **P2**: Number of priority 2 issues. • **Total**: Total number of P1, P2, and P3 issues.

Step 5   Use the SD-Access **Top 10 Issue Types** dashlet for 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:<ol type="a"> - From the **Status** drop-down list, choose **Ignore**.   - Set the number of hours to ignore the issue on the slider.   - Click **Confirm**.   Click **View All Open Issues** to open the **Open Issues** window.

Step 6   Use the **Fabric Sites** dashlet to view detailed information about the fabric sites in your network. This dashlet provides the following functionality:

Fabric Sites Dashlet	
Item	**Description**
Health	Filter the table based on the client health with the following options: **All** **Inactive**: Fabric sites with a health score of 0. **Poor**: Fabric sites with a health score range from 1 to 3. **Fair**: Fabric sites with a health score range from 4 to 7. **Good**: Fabric sites with a health score range from 8 to 10. **No Data**: Fabric sites with no data.
Fabric Site table	View detailed fabric site information in a table format. The fabric site table displays the following information by default: **Fabric Site**: Name of the fabric site. You can click the name to display a 360° view of a fabric site. See Monitor the Health of a Fabric Site, on page 169. **# of Fabric Devices**: Number of fabric devices in the fabric site. **Fabric Site Health**: **Overall**: Overall health of the fabric site. **Fabric Site Connectivity**: Health of the connectivity with the fabric site. **Fabric Control Plane**: Health of the control plane in the fabric site. **Fabric Infrastructure**: Health of the devices that make up the fabric site.

Fabric Sites Dashlet	
Item	**Description**
Export	Click **Export** to export the table data to a CSV file. **Note** The data from all available columns is included even if the column was not selected for the table. Filters applied to the client table are applied to the exported data.
⚙	Customize the table display: a. From the **Table Appearance** tab, set the table density and striping. b. From the **Edit Table Columns** tab, select the data you want displayed in the table. c. Click **Apply**.

Step 7   Use the **Virtual Networks** dashlet to view detailed information about the virtual networks in your fabric site. This dashlet provides the following functionality:

Virtual Networks Dashlet	
Item	**Description**
Health	Filter the table based on the virtual network health with the following options: • **All** • **Inactive**: Virtual networks with a health score of 0. • **Poor**: Virtual networks with a health score range from 1 to 3. • **Fair**: Virtual networks with a health score range from 4 to 7. • **Good**: Virtual networks with a health score range from 8 to 10. • **No Data**: Virtual networks with no data.

Virtual Networks table	View detailed virtual network information in a table format. The virtual network table displays the following information by default:
	
	• **VN Name**: Name of the virtual network.
	
	  You can click the name to display a 360° view of a virtual network. See Monitor the Health of a Virtual Network, on page 178.
	
	• **# of Active Sites**: Number of active sites in the virtual network.
	
	• **# of Clients**: Number of endpoints in the virtual network.
	
	• **Virtual Network Health**:
	
	    • **Overall**: Overall health of the virtual network.
	
	    • **Fabric Control Plane**: Health of the control plane in the virtual network.
	
	    • **VN Services**: Health of the virtual network services.

Virtual Networks Dashlet	
Item	**Description**
Export	Click **Export** to export the table data to a CSV file. **Note** The data from all available columns is included even if the column was not selected for the table. Filters applied to the client table are applied to the exported data.
⚙	Customize the table display: a. From the **Table Appearance** tab, set the table density and striping. b. From the **Edit Table Columns** tab, select the data you want displayed in the table. c. Click **Apply**.

Step 8   Use the **Transits and Peer Networks** dashlet to view the detailed information about the transits and peer networks in your fabric site. This dashlet provides the following functionality:

Table 8: Transits and Peer Networks

Item	Description
Health	Filter the table based on the transit and peer network health with the following options: • **All** • **Inactive**: Transits and peer networks with a health score of 0. • **Poor**: Transits and peer networks with a health score range from 1 to 3. • **Fair**: Transits and peer networks with a health score range from 4 to 7. • **Good**: Transits and peer networks with a health score range from 8 to 10. • **No Data**: Transits and peer networks with no data.

Item	Description

Transits and Peer Networks table	View detailed transits and peer network information in a table format. The transits and peer network table displays the following information by default:
	
	• **Transit/ Peer Network Name**: Name of the virtual network.
	
	  You can click the name to display a 360° view of a virtual network. See Monitor the Health of a Virtual Network, on page 178.
	
	• **Type**: Number of active sites in the virtual network.
	
	• **# of Clients**: Number of endpoints in the virtual network.
	
	• **Associated Fabric Sites**
	
	• **Transit and Peer Networks Health**:
	
	  • **Overall**: Overall health of the transit and peer network.
	
	  • **Transit Control Plane**: Health of the transit control plane.

Export	Click **Export** to export the table data to a CSV file. Note The data from all available columns is included even if the column was not selected for the table. Filters applied to the client table are applied to the exported data.
⚙	Customize the table display: a. From the **Table Appearance** tab, set the table density and striping. b. From the **Edit Table Columns** tab, select the data you want displayed in the table. c. Click **Apply**.

Monitor the Health of a Fabric Site

Use this procedure to view details about a specific fabric site.

Step 1   Click the menu icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

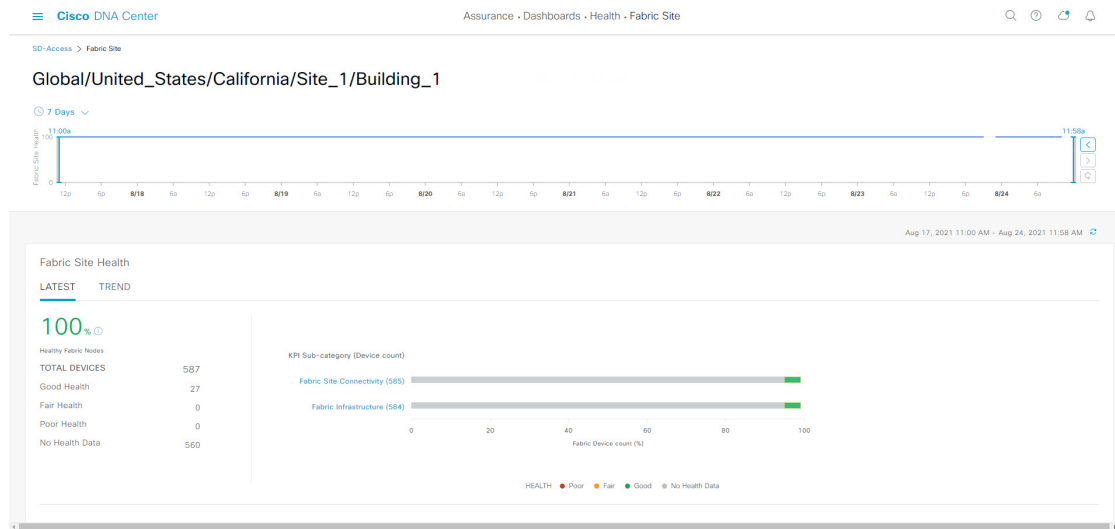**Step 2**   Click the **SD-Access** tab.

The **SD-Access** health dashboard appears.

Step 3   In the **Fabric Site** table, click the name of a fabric site.

The **Fabric Site 360** window appears, which provides a 360° view of the fabric site.

Figure 19: Fabric Site 360

Step 4   Click the time range setting (🕐) at the top-left corner to specify the time range for the data that you want displayed in the window:

a)   From the drop-down list, choose a time range: **3hours 24 hours**, or **7 days**.

b)   Specify the **Start Date** and time; and the **End Date** and time.

c)   Click **Apply**.

Step 5   Use the health timeline slider to view the health score for a more granular time range and to view quality information.

Hover your cursor within the timeline to view the following information:

Fabric Site Health: Health is the percentage of healthy fabric nodes in this site; it does not include device health of control planes. Fabric Sub Category Health is the minimum of underlying KPI Scores.

Note   The KPI is not included for Health Score.

Fabric Site Connectivity: The control plane is unreachable.

Fabric Infrastructure:

You can click and drag the timeline boundary lines to specify the time range. This boundary sets the context for the fabric site data that is displayed in the Fabric Site 360 window.

• Click the Latest and Trend tabs to change the scope of data displayed in the category:

• Latest: Displays the data from the selected time window in the timeline on the top of the window.

• Trend: Displays data from the last 24 hours.

Step 6 Use the **Fabric Site Health** area, below the timeline, to view the following information:

Fabric Site Health	
Item	**Description**
Latest	Displayed by default. Includes two panes. The left pane provides the network health summary score and the total number of devices. The right pane displays charts. • **Health Fabric Nodes**: The percentage of healthy (good) nodes in your selected site. • **Total Devices**: Total number of network devices and the count of devices which has Good Health, Fair Health, Poor Health, and No Health Data. • **Charts**: This color-coded snapshot-view chart shows the fabric site connectivity and infrastructure over the last 5 minutes. Hover your cursor over a color to display the health score and the number of devices that are associated with that color. If the chart shows a low health score (red or orange), the KPIs that contributed to the low health score are provided next to the bar. For example, Fabric CP reachability, Multicast RP, AAA Server Status, and so on. You can also click a hyperlinked fabric category in the charts to open a side pane to view the respective KPI Sub-categories: • **Fabric Site Connectivity** - Control Plan Reachability. • **Fabric Control Plane** - LISP Session Status. • **Fabric Infrastructure** - AAA Server Status and Pub-Sub Session Status for INFRA VN.
Trend	Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the performance of devices over a time range. Hover your cursor over the chart to display the total number of devices and their health over time. The color in the chart represents the health of the network devices: ●: Poor network devices. Health score range is 1 to 3. ●: Fair network devices. Health score range is 4 to 7. ●: Good network devices. Health score range is 8 to 10. ●: No Health data. Health score is 0.

Step 7 Use the **Top 10 Issue Types** area to view the following information:

Issues
Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first.
Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions.
From the slide-in pane, you can do the following:
• To resolve an issue:
a. From the drop-down list, choose **Resolve**.
b. To view the list of issues that have been resolved, click **Resolved Issues**.
• To ignore an issue:
a. From the drop-down list, choose **Ignore**.
b. Set the number of hours to ignore the issue on the slider.
c. Click **Confirm**.
d. To view the list of issues that have been ignored, click **Ignored Issues**.
For information about the types of issues, see View and Manage Issues, on page 187.

Step 8 Use the **Fabric Nodes** dashlet for the following functionality:

Network Devices Dashlet	
Item	**Description**
Type	Filter the table based on the fabric node type with the following options: **All**, **Fabric Control Plane**, **Fabric Border**, **Fabric Edge**, **Fabric WLC**, **Fabric AP**, and **Extended Node**.
Fabric Site Health	Filter the table based on the overall health score of the fabric site with the following options: • **All** • **Poor**: Devices with a health score range from 1 to 3. • **Fair**: Devices with a health score range from 4 to 7. • **Good**: Devices with a health score range from 8 to 10. • **No Health**: Devices with no health data.

Network Devices Dashlet	
Item	**Description**
Fabric Node table	View device information for all the fabric nodes for the selected site in a table format.
	Note The overall health score is the minimum subscore of the following KPI metric health scores: fabric site connectivity and fabric infrastructure.
	The **Name**, **Issue Type Count** and **Fabric Role** columns display the fabric name, Issue count and fabric role (Edge, Border, Map Server and so on).
	Under **Device Fabric Site Health**, in the **Overall** column, hover your cursor over a health score. The overall **Device Fabric Site Health** score is displayed along with the health and percentage value of all the KPI metrics.
	Hover your cursor over the **Fabric Site Connectivity**, **Fabric Control Plane**, and **Fabric Infrastructure** icons to display the health scores.
Device 360	Display a 360° view of a device by clicking the device name in the **Name** column.
	Device 360 provides detailed information for troubleshooting device issues.
⬆ Export	Click **Export** to export the device information to a CSV file.
⚙	Customize the data that you want displayed in the table:
	a. Click ⚙.
	A list of options is displayed.
	b. Check the check boxes for the data you want displayed in the table.
	c. Click **Apply**.

Monitor the Health of a Transit and Peer Network

Use this procedure to view the details about a specific transit network.
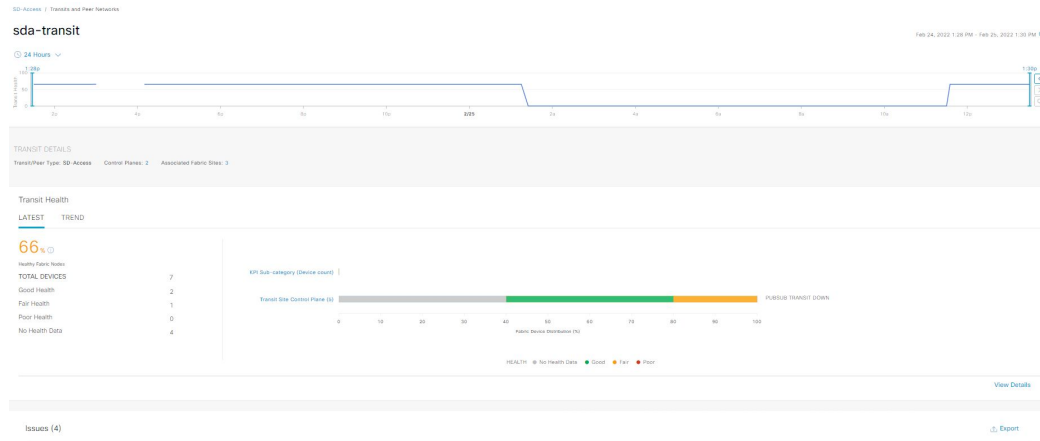
Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **SD-Access** tab.

The **SD-Access** health dashboard appears.

Step 3   In the **Transit and Peer Network** table, click the name of a transit.

The **Transit Site 360** window appears, which provides a 360° view of the fabric site.

Figure 20: Transit 360

Step 4   Click the time range setting ( ) at the top-left corner to specify the time range for the data that you want displayed in the window:

a)   From the drop-down list, choose a time range: **3hours 24 hours**, or **7 days**.

b)   Specify the **Start Date** and time; and the **End Date** and time.

c)   Click **Apply**.

Step 5   Use the health timeline slider to view the health score for a more granular time range and to view quality information.

Hover your cursor within the timeline to view the following information:

Transit Network Health: Health is the percentage of healthy fabric nodes in this site; it does not include device health of control planes. Fabric Sub Category Health is the minimum of underlying KPI Scores.

Transit Site Control Plane: Lists the KPI subcategory such as LISP and PubSub session of the transits. If the Transit health score is low, click **View Device List** to display a list of devices that contribute to the low score and their associated down sessions. Click of the hyperlinked name of the device to display device information.

• Click the Latest and Trend tabs to change the scope of data displayed in the category:

• Latest: Displays the data from the selected time window in the timeline on the top of the window.

• Trend: Displays data from the last 24 hours.

Step 6   Use the **Transit Health** area, below the timeline, to view the following information:

Transit Health	
Item	**Description**
Latest	Displayed by default. Includes two panes. The left pane provides the network health summary score and the total number of devices. The right pane displays charts. **Health Fabric Nodes**: The percentage of healthy (good) nodes in your selected site. **Total Devices**: Total number of network devices and the count of devices which has Good Health, Fair Health, Poor Health, and No Health Data. **Charts**: This color-coded snapshot-view chart shows the transit control plane over the last 5 minutes. Hover your cursor over a color to display the health score and the number of devices that are associated with that color. You can also click a hyperlinked **Transit Control Plane** in the charts to open a side pane to view the following KPI Subcategories in the Transit Control plane: **LISP session from Border to Transit Control Plane** **PubSub session from Border to Transit Control Plane** You can hover on a color segment in the chart to view the fabric node details in the table format such as name of the fabric node, issue count, fabric role, fabric site and device transit health.
Trend	Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the performance of devices over a time range. Hover your cursor over the chart to display the total number of devices and their health over time. The color in the chart represents the health of the network devices: 🔴: Poor network devices. Health score range is 1 to 3. 🟠: Fair network devices. Health score range is 4 to 7. 🟢: Good network devices. Health score range is 8 to 10. ⚪: No Health data. Health score is 0.

Step 7   Use the **Top 10 Issue Types** area to view the following information:

Issues

Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first. Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions. From the slide-in pane, you can do the following: - To resolve an issue:
   a. From the drop-down list, choose **Resolve**.
   b. To view the list of issues that have been resolved, click **Resolved Issues**.   - To ignore an issue:
   a. From the drop-down list, choose **Ignore**.
   b. Set the number of hours to ignore the issue on the slider.
   c. Click **Confirm**.
   d. To view the list of issues that have been ignored, click **Ignored Issues**.   For information about the types of issues, see View and Manage Issues, on page 187.

Step 8 Use the **Associated Fabric Sites** dashlet for the following functionality:

Associated Fabric Sites Dashlet	
Item	**Description**
Health	Filter the table based on the overall health score of the fabric site with the following options: **All** **Poor**: Devices with a health score range from 1 to 3. **Fair**: Devices with a health score range from 4 to 7. **Good**: Devices with a health score range from 8 to 10. **No Health**: Devices with no health data.
Associated Fabric Sites table	Displays the following details in the fabric table: **Fabric Site**, **Health**, number of available **Connected Transit/ Peer Networks**, **Layer 3 Virtual Networks**, and **Fabric Devices**.
Device 360	Display a 360° view of a device by clicking the device name in the **Name** column. **Device 360** provides detailed information for troubleshooting device issues.
⮙ Export	Click **Export** to export the device information to a CSV file.

Associated Fabric Sites Dashlet	
Item	**Description**
⚙	Customize the data that you want displayed in the table: **a.** Click ⚙. A list of options is displayed. **b.** Check the check boxes for the data you want displayed in the table. **c.** Click **Apply**.

Step 9 Use the **Fabric Nodes** dashlet for the following functionality:

Fabric Nodes Dashlet	
Item	**Description**
Type	Filter the table based on the fabric node type with the following options: **All**, **Transit Control Plane**, and **Border**.
Transit and Peer Network Health	Filter the table based on the overall health score of the transit with the following options: • **All** • **Poor**: Devices with a health score range from 1 to 3. • **Fair**: Devices with a health score range from 4 to 7. • **Good**: Devices with a health score range from 8 to 10. • **No Health**: Devices with no health data.
Fabric Node table	View device information for all the fabric nodes for the selected transit in a table format. **Note** The overall health score is the minimum subscore of the following KPI metric health scores: Transit Site Control Plane. The **Name**, **Issue Type Count**, **Fabric Role**, and **Fabric Site** columns display the fabric name, issue count, fabric role, and fabric site. Under **Device Transit Health**, in the **Overall** column, hover your cursor over a health score. The overall **Device Transit Health** score is displayed along with the health and percentage value of all the KPI metrics. Hover your cursor over the **Transit Site Control Plane** icons to display the health scores.
Device 360	Display a 360° view of a device by clicking the device name in the **Name** column. **Device 360** provides detailed information for troubleshooting device issues.
⬆ Export	Click **Export** to export the device information to a CSV file.

Fabric Nodes Dashlet	
Item	**Description**
⚙	Customize the data that you want displayed in the table: a. Click ⚙. A list of options is displayed. b. Check the check boxes for the data you want displayed in the table. c. Click **Apply**.

Monitor the Health of a Virtual Network

Use this procedure to view details about a specific virtual network.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **SD-Access** tab.

The **SD-Access** health dashboard appears.

Step 3   Scroll down and click **Virtual Network**.

Step 4   In the **Virtual Network** table, click the name of a virtual network.

The **Virtual Network 360** window appears, which provides a 360° view of the virtual network.

Figure 21: Virtual Network 360
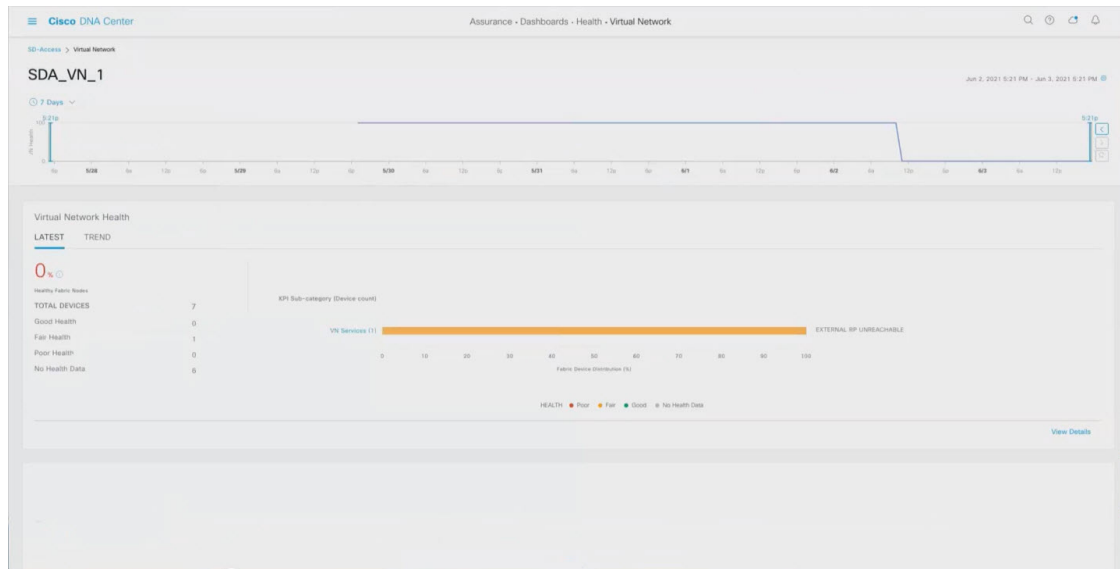
Step 5 Click the time range setting ( ) at the top-left corner to specify the time range for the data that you want displayed in the window:

    a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.

    b) Specify the **Start Date** and time; and the **End Date** and time.

    c) Click **Apply**.

Step 6 Use the virtual network health timeline slider to view the virtual network's health score for a more granular time range and to view the virtual network's quality information.

Hover your cursor within the timeline to view the following information:

Virtual Network Health: Health score is the percentage of healthy devices in the VN. VN Category Health is the minimum of corresponding sub-category KPI scores. **VN Services** Category includes **Multicast (external RP)** and **Default Route Registration** and VN Control Plane.

If the VN health score is low, click **View Device List** to display a list of devices that contribute to the low score and their associated down sessions. Click of the hyperlinked name of the device to display device information.

You can click and drag the timeline boundary lines to specify the time range. This sets the context for the data that is displayed in the 360 window.

• Click the Latest and Trend tabs to change the scope of data displayed in the category:

• Latest: Displays the data from the selected time window in the timeline on the top of the window.

• Trend: Displays data from the last 24 hours.

Step 7 Use the **Virtual Network Health** area, below the timeline, to view the following information:

Virtual Network Health	
Item	**Description**
Latest	Displayed by default. Includes two panes. The left pane provides the virtual network health summary score and the total number of devices. The right pane displays charts. • **Healthy Fabric Nodes**: The percentage of healthy (good) nodes in your selected site. • **Total Devices**: Total number of fabric devices and the count of devices which have Good Health, Fair Health, Poor Health, and No Health data. • **Charts**: This color-coded snapshot-view chart shows the KPIs with sub-categories such as **VN Control Plane** (Pub-Sub Sessions Status) and **VN Services** (Multicast-external RP and Default Route Registration). Hover your cursor over a color to display the health score and the number of devices that associated with that color. If the chart shows a low health score (red or orange), the KPIs that contributed to the low health score are provided next to the bar. You can also click a hyperlinked category to open a side pane with more details.
Trend	Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the performance of devices over a time range. Hover your cursor over the chart to display the total number of devices and their health over time. The color in the chart represents the health of the network devices: ●: Poor network devices. Health score range is 1 to 3. ●: Fair network devices. Health score range is 4 to 7. ●: Good network devices. Health score range is 8 to 10. ●: No Health data. Health score is 0.

Step 8   Use the **Top 10 Issue Types** area to view the following information:

Issues
Displays any issues that must be addressed. Issues are listed based on the timestamp. The most recent issue is listed first.
Click an issue to open a slide-in pane to view the corresponding details, such as the description of the issue, impact, and suggested actions.
From the slide-in pane, you can do the following:
• To resolve an issue:
a. From the drop-down list, choose **Resolve**.
b. To view the list of issues that have been resolved, click **Resolved Issues**.
• To ignore an issue:
a. From the drop-down list, choose **Ignore**.
b. Set the number of hours to ignore the issue on the slider.
c. Click **Confirm**.
d. To view the list of issues that have been ignored, click **Ignored Issues**.
For information about the types of issues, see .

Step 9   Use the **Virtual Network Devices** dashlet for the following functionality:

Virtual Network Devices Dashlet	
Item	**Description**
Type	Filter the table based on the type.
Virtual Network Health	Filter the table based on the overall health score of the virtual network with the following options:
	• **All**
	• **Poor**: Devices with a health score range from 1 to 3.
	• **Fair**: Devices with a health score range from 4 to 7.
	• **Good**: Devices with a health score range from 8 to 10.
	• **No Health**: Devices with no health data.
Virtual Network Devices table	View device information for the selected item in a table format.
	Note The overall health score is the minimum subscore of the following KPI metric health scores: virtual network connectivity and infrastructure.
	Hover your cursor over the various health scores and icons to display additional information.

Virtual Network Devices Dashlet	
Item	**Description**
Device 360	Display a 360° view of a device by clicking the device name in the **Name** column. **Device 360** provides detailed information for troubleshooting device issues.
⬆ Export	Click **Export** to export the device information to a CSV file.
⚙	Customize the data that you want displayed in the table: a. Click ⚙. A list of options is displayed. b. Check the check boxes for the data you want displayed in the table. c. Click **Apply**.

Virtual Network Health Score

Currently, the Multicast VN service is the only KPI that contributes to the VN health score.

C H A P T E R 11

Monitor and Troubleshoot Your Network Using Site Analytics

About Site Analytics

Site Analytics provide you with key performance metrics (KPIs) about sites, buildings, and floors throughout your network. These metrics help you to identify opportunities where you can improve network performance or find problem areas.

You can define KPI thresholds that can be used to alert you of network-wide issues. Based on a KPI value, you can determine the worst offending site and drill down to the specific building and floor to find the problem. You can analyze issues pertaining to onboarding and roaming.

The Site Analytics dashboard is available from the Assurance health dashboard **AI Analytics** menu option.

The **AI Analytics** menu option also provides access to AI Network Analytics tools. For information about these tools, see Observe Network Trends and Gain Insights, on page 283.

View Site Analytics

Use this procedure to display KPI statistics for sites that do not meet the configured performance thresholds.

Before you begin

- AI Network Analytics must be enabled for site analytics data to be collected. Click the **Enable AI Network Analytics** link to go directly to the **Cisco AI Analytics** window where you can configure this system setting. For more information, see Configure Cisco AI Network Analytics, on page 61.

  If AI Network Analytics isn't enabled, Assurance displays an example dashlet with sample data.

- Configure site analytic settings. For details, see Configure Site Analytics Settings, on page 185.

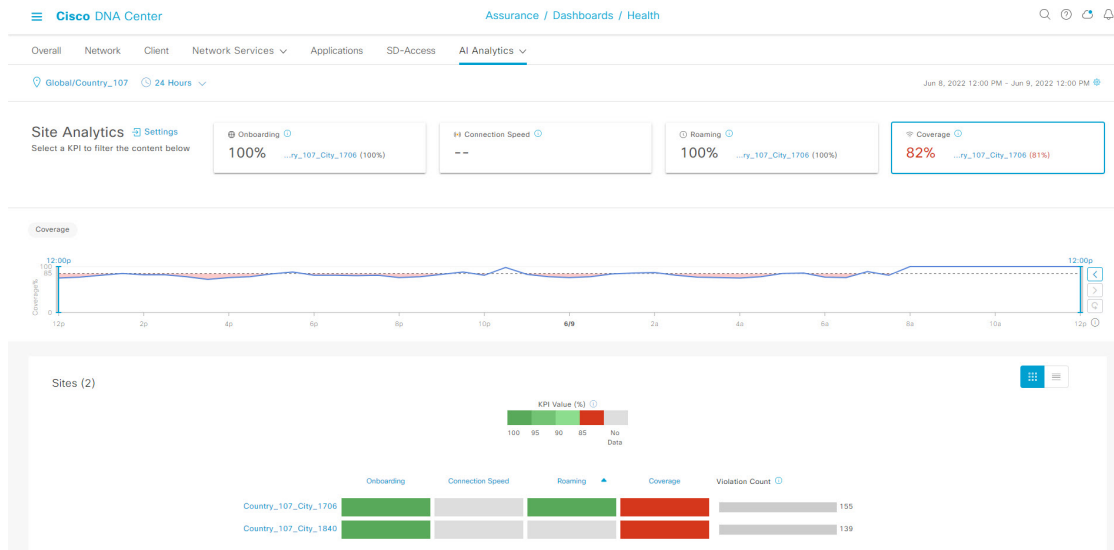**Step 1**   Click the menu icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard appears.

Step 2   Choose **AI Analytics** > **Site Analytics**.

The **Site Analytics** health dashboard appears.

Figure 22: Site Analytics Health Dashboard

**Step 3**   Use the top menu bar for the following functionality:

Item	Description
◎ Global **Location** pane	• Click ◎ Global to choose the site, building, or floor from the Site hierarchy.
Time range	Enables you to display data for the last 3 hours, 24 hours, or 7 days.

Step 4   View the aggregated KPI statistics for sites that fall below the configured performance thresholds.

For each KPI category, click the site name to display more information about the site and its performance.

Step 5   Click a KPI category to view a timeline for the particular KPI category. The dotted horizontal line in the timeline represents the configured threshold value.

- Use the timeline slider to view a more granular time range.

- Hover your cursor within the timeline to view the KPI percentage for a specific time range.

- Click and drag the timeline boundary lines to specify the time range. This sets the context for KPI data that is displayed below the timeline.

- Use the arrow buttons on the right of the timeline to view data for up to 30 days.

Step 6   Use the Sites KPI chart to view the KPI values for each site.

- Hover your cursor over a color segment in the chart to display details for a particular site. Data type categories by site include the KPI percentage, AP count, client count, and violation count.

- Click the ⊞ ≡ toggle button to switch between Map View and Table View.

Configure Site Analytics Settings

This procedure shows you how to configure the thresholds for key client performance metrics.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Site Analytics Settings**.

The **Site Analytics Settings** window appears.

Step 2   To change the threshold **KPI Value %**, do the following:

a) Click **Edit**.
b) In the slide-in pane, enter the target percentage for the site performance metrics. This threshold defines a healthy percentage of KPI data points for any site. The target for green (GOOD) is 100% and cannot be changed. The target for red (POOR) must be a number between 0 and 95. These target values affect all the client performance metrics.

Step 3   From the **KPI Name** column, click the KPI name link.

The slide-in pane for the KPI appears.

Step 4   Configure the KPI threshold settings:

- If the KPI threshold is quantitative, you can customize the threshold value for what is considered a good health score.

- To return to the default setting, click **View Default Setting**.

Step 5   Click **Apply**.

A confirmation dialog box is displayed.

View and Manage Issues

About Issues

Assurance provides both system-guided as well as self-guided troubleshooting. For a large number of issues, Assurance provides a system-guided approach, where multiple Key Performance Indicators (KPIs) are correlated, and the results from tests and sensors are used to determine the root cause of the problem, and then possible actions are provided to resolve the problem. The focus is on highlighting an issue rather than monitoring data. Quite frequently, Assurance performs the work of a Level 3 support engineer.

With Cisco DNA Center, you can view and troubleshoot AI-driven issues using Cisco AI Network Analytics. Cisco AI Network Analytics leverages a cloud-based learning platform with advanced artificial intelligence (AI) and machine learning (ML) technologies to provide intelligent issue detection and analysis. It detects anomalies to determine their root causes and ease troubleshooting.

Cisco AI Network Analytics can detect the following types of cloud-based AI-driven issues:

- **Connection Issues** (Onboarding Issues): Excessive Time, Excessive Failures, Excessive Association Time, Excessive Association Failures, Excessive Authentication Time, Excessive Authentication Failures, Excessive DHCP Time, and Excessive DHCP Failures

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

Note   Currently, Cisco AI Network Analytics use cases are supported only for wireless environments that are running AireOS controllers.

About the Machine Reasoning Engine

The Machine Reasoning Engine (MRE) is a network automation engine that uses artificial intelligence (AI) to automate complex network operation workflows. It encapsulates human knowledge and expertise into a fully automated inference engine to help you perform complex root cause analysis, detect issues and vulnerabilities, and either manually or automatically perform corrective actions. MRE is powered by a cloud-hosted knowledge base, built by Cisco networking experts.

You can use the MRE to troubleshoot wired client, Layer 2 loop, and PoE issues. For the list of issues, see MRE Issues, on page 226.

For procedures, see Troubleshoot Wired Client Issues Using MRE, on page 201, Issue Instance Details for Layer 2 Loop Issue, on page 197, and Issue Instance Details for a PoE Issue, on page 199.

About the Layer 2 Loop Issue Involving VLANs

A Layer 2 Loop issue occurs when a forwarding loop forms in the path of one or more VLANs. In this case, packets are forwarded and multiplied indefinitely along the affected path, until the links and devices reach maximum capacity. A broadcast storm occurs and the entire Layer 2 network shuts down very quickly. The MRE enables you to troubleshoot the Layer 2 Loop issue by:

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

Note   The scale constraints for the Layer 2 loop are the following:

- The number of VLANs is 10.
- The number of devices per VLAN is 30.

Important   Currently, the MRE does not perform root cause analysis on Layer 2 loops that occur as a result of unmanaged network devices, virtual machines, or other entities that are not part of the topology known to Cisco DNA Center.

View Open Issues

Use this procedure to view all open issues, which fall under the following categories:

- **Threshold-based issues**: Issues detected by Assurance.

- **AI-Driven Issues**: Issues detected by Cisco AI Network Analytics. These issues are triggered based on deviations from the predicted baseline for your specific network environment.

  If you have installed and configured the Cisco AI Network Analytics application with Cisco DNA Center, you can view the following types of cloud-based, AI-driven issues:

  - **Connection Issues** (Onboarding Issues): Excessive Time, Excessive Failures, Excessive Association Time, Excessive Association Failures, Excessive Authentication Time, Excessive Authentication Failures, Excessive DHCP Time, and Excessive DHCP Failures.

  Note For Connection issues to display, make sure that the APs are properly assigned to sites.

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

  Note For Application Experience issues to display, make sure that Application Visibility and Control (AVC) is enabled on the wireless controllers. The throughput issues rely on the AVC data for baselining and anomaly detection.

- **Layer 2 Loop Issue** and **PoE Issue**: Issues detected by Assurance that you can troubleshoot using the MRE workflow. See About the Machine Reasoning Engine, on page 188.

Before you begin

- To view AI-driven, cloud-based issues that use artificial intelligence (AI) and machine learning (ML) technologies to provide intelligent issue detection and analysis, make sure that you have configured Cisco AI Network Analytics data collection. See Configure Cisco AI Network Analytics, on page 61.

- To view syslog messages, make sure that you have configured syslog. See Configure Syslog, SNMP Traps, NetFlow Collector Servers, and Wired Client Data Collection Using Telemetry, on page 60 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**.
- Click the menu icon (≡) and choose **Assurance** > **Dashboards** > **Issues**.

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

Figure 23: Open Issues Dashboard

Open Issues Dashboard	
Item	**Description**
⊘ Global	• Click ⊘ Global ⋮ in the top menu bar to choose the site, building, or floor from the Site hierarchy. • Click ⋮ next to the location icon and choose **Site Details** to view the Sites table. • Choose **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table is refreshed. • From the **Go to sites** column, click ⊡ for a site or building to display data only for that location on the **Open Issues** dashboard.
⊘ **Time Range** setting	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do the following: a. From the **24 Hours** drop-down list, choose a time range: **3 hours**, **24 hours**, or **7 days**. b. Specify the **Start Date** and time, and the **End Date** and time. c. Click **Apply**. This sets the range of the timeline.
Most Impacted Areas	Provides information about the areas that are most impacted based on issue priority. Click the hyperlinked location to drill down to the exact building and floor where the issue occurred.

Open Issues Dashboard	
Item	**Description**

Timeline Slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.
	
	The colors represent the issue priority:
	
	    🟥 : P1
	    🟧 : P2
	    ⬛ : P3 and P4
	
	Note The intensity of the color indicates its significance, whether more or fewer issues have occurred for that priority level. For example, a lighter shade of yellow indicates fewer P2 issues (still open) than a deeper shade of yellow.

Total Open	Provides the total count of open issues that require action. The **Total Open** value changes depending on the tab you choose. Options are **All** (the default), **P1**, **P2**, **P3**, **P4**, and **AI-Driven**.

Step 2   Click the **All**, **P1**, **P2**, **P3**, **P4**, or **AI-Driven** tab to display a list of issues in that category in the **Issue Type** table.

Issue Type Table in the Open Issues Window	
Item	**Description**
Priority	Preassigned priority level of the issue type.
Issue Type	Type of issue. **Note** For AI-driven issues, the 🆎 icon appears in front of the issue type.
Device Role	Role assigned to the device on which the issue was detected. The role is Access, Core, Distribution, Border Router, or Unknown.
Category	Category under which the issue type falls, such as Connectivity, Availability, Onboarding, and Utilization.
Issue Count	Number of times this type of issue occurred.
Site Count (Area)	Number of sites where this type of issue occurred.
Device Count	Number of devices that were impacted by this type of issue.
Last Occurred Time	Most recent date and time this issue occurred.

Step 3   From the **Issue Type** table, click an issue type.

The first slide-in pane, **Issue Instances**, lists all the issues for that issue type with the following information:

Issue Instances (First Slide-In Pane)	
Item	**Description**
Open Issues	Number of open issues for that issue type.
Area	Number of buildings and floors that are impacted by the issue.
Device	Number of devices that are impacted by the issue.
Actions drop-down list	Allows you to resolve or ignore a single issue or a bulk of issues at a time. See Resolve or Ignore Issues, on page 206.
Issue	Description of the issue.
Site	Site, building, or floor that was impacted by the issue.
Device	Device that was impacted by the issue. Click the device name to open the **Device 360** window.
Device Type	Type of device that was impacted by the issue.
Issue Count	Number of times this type of issue occurred.
Last Occurred Time	Date and time this issue occurred.
Last Updated Time	Date and time this issue was last updated.
Updated By	Name of the entity who updated this issue.

Step 4 From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, provides specific details about the issue. Depending on the issue, the description and suggested actions are displayed. See the following sections for more details about these issues:
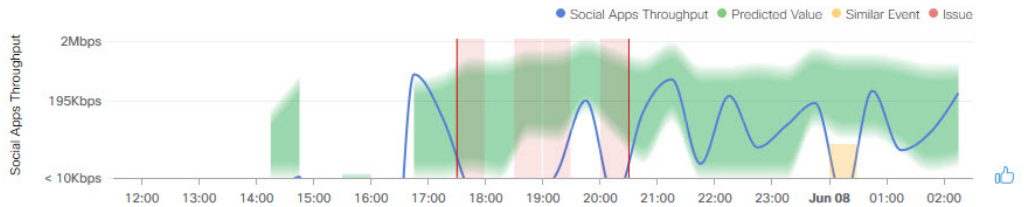
Issue Instance Details for AI-Driven Issues

Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View Open Issues, on page 188.

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

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**
Description	Description of the issue.

Status drop-down list	Allows you to change the status of the issue. Do the following:
	
	• To resolve an issue, from the **Status** drop-down list, choose **Resolve**.
	
	• To stop an issue from being reported, do the following:
	
	  1. From the **Status** drop-down list, choose **Ignore**.
	
	  2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.

Summary area	Brief summary of the issue, which can include information such as the radios that are impacted, the location of the radios, the time and date the issue occurred, and the location of the issue.
Impacted Summary for this Network	Displays information about the location that was impacted and the number of clients that were impacted by the issue.
Feedback icon	Click the 👍 👎 icon to provide your comments on whether the information on this page was helpful, and then click **Submit**.
Problem	Provides brief text that describes the problem along with a chart that provides a visual of how the actual KPI value deviated from the predicted normal behavior. By default, the chart is zoomed-in, 6 hours before and 6 hours after the issue, as shown in the following figure: **Figure 24: Problem Chart** The chart details for the AI-driven issues are represented by different colors. • **Green band**: Predicted normal behavior for your network based on machine learning. • **Solid blue line**: Actual KPI value. • **Vertical red line or bars**: Indicates an issue. When the blue line (actual KPI value) falls outside the green band (predicted normal behavior), an issue is raised. • **Vertical yellow bars**: Indicates that a similar event has occurred. Hover and move your cursor over the charts to view synchronized information, such as the KPI value, the predicted lower value, and the predicted upper value at a selected point in time.

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**
Impact	Provides information about the connected clients, APs, devices, and applications that are impacted by the issue.
	For Excessive Onboarding Time and Failures; and Excessive DHCP, Association, or Authentication Time and Failures, the following tabs are provided: **Impacted Clients** and **Top 10 Impacted APs**.
	For Total Radio Throughput and Applications Throughput (Cloud, Collab, Media, and Social), the following tabs are provided: **Impacted Clients**, **Device Breakout**, and **Applications by TX/RX**.
	Click the tab to update the chart and the table below the chart.

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**
Root Cause Analysis	Provides the issue along with the probable network causes for that issue, displayed in charts, as shown in the following figure:
	Figure 25: Root Cause Analysis Charts
	For Excessive Onboarding Time and Failures, the following tabs are provided: **Network Causes**, **Failed Distribution**, **Failed Percentage**, and **Failed Count**.
	For Excessive DHCP, Association, or Authentication Time, the following tabs are provided: **Network Causes**, **Top Impacted APs**, and **Top Impacted Times**.
	For Excessive DHCP, Association, or Authentication Failures, the following tabs are provided: **Network Causes**, **Top Impacted APs**, and **Top Impacted Failures**.
	For Total Radio Throughput and Applications Throughput (Cloud, Collab, Media, and Social), the following tabs are provided: **Network Causes**.
	Click the tab to update the charts below.
	To view the charts for additional KPIs, click the ➕ **KPI** icon, choose the KPI, and then click **Apply**.
Suggested Actions	Provides the actions you can take to resolve the issue.

Issue Instance Details for AP-Disconnect Issues

Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View Open Issues, on page 188.

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

AP-Disconnect Issue Instance Details (Second Slide-In Pane)	
Item	**Description**

Status drop-down list	• To resolve an issue, from the **Status** drop-down list, choose **Resolve**.
	
	• To stop an issue from being reported, do the following:
	
	   1. From the **Status** drop-down list, choose **Ignore**.
	
	   2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.

Insights	Provides a brief summary of the issue, which can include information such as the switch that is impacted, the date and time of the issue, and the location of the switch.
Impact Summary	Displays the counts of impacted sites, clients, and APs.
Problem Details	Provides the following details: • Description of the devices involved with the issue, if known. • Related issue, if any, with a link directly to the issue details. • Details about the problem, such as the impacted APs, their location and power information, and the reason for the disconnect. • Physical neighbor topology, which includes the switch and the neighboring devices that are connected to it.
Impact Details	Lists the wireless clients that were connected to the impacted APs and their locations.
Suggested Actions	Provides the actions you can take to resolve the issue.

Issue Instance Details for Layer 2 Loop Issue

Note
The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View Open Issues, on page 188.

To understand the Layer 2 Loop issue and the Machine Reasoning Engine, see About the Machine Reasoning Engine, on page 188.
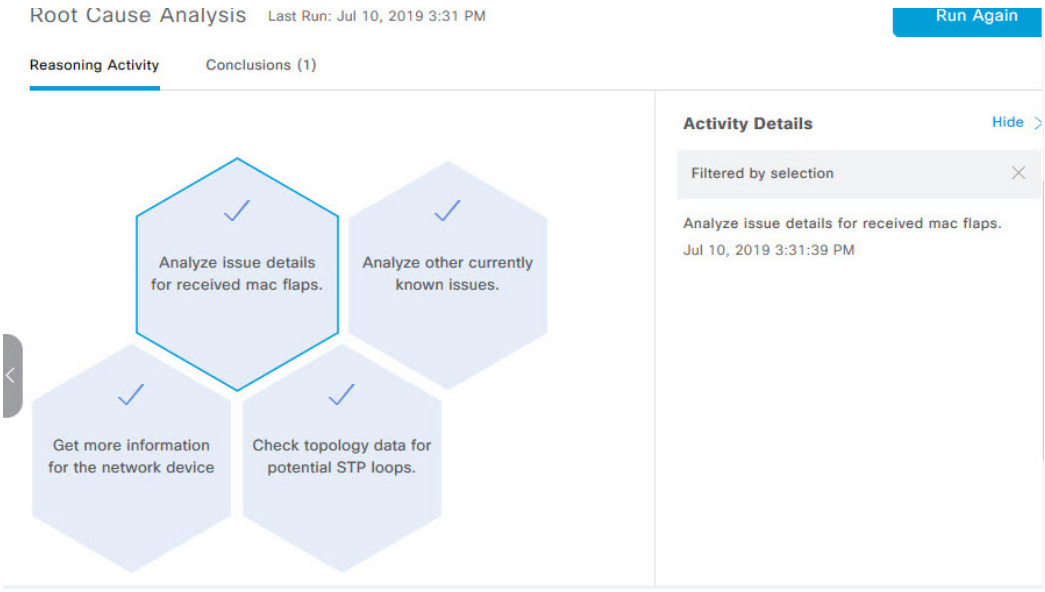
Note
The scale constraints for the Layer 2 Loop are the following:

- Number of VLANS is 10.

- Number of devices per VLAN is 30.

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

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**

Status drop-down list	Allows you to change the status of the issue. Do the following:
	
	 • To resolve an issue, from the **Status** drop-down list, choose **Resolve**.
	
	 • To stop an issue from being reported, do the following:
	
	     1. From the **Status** drop-down list, choose **Ignore**.
	
	     2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.

Summary	Brief summary of the issue, which can include information, such as device, role, time, location. and potential root cause. This also provides the initial assessment, such as the VLANs and ports in the potential loop.
Problem Details	Provides a brief text that describes the problem along with the following: • **Relevant Events** drop-down list: Lists the events that occurred during the loop. Click an event to view details in the side pane. • **Potential Loop Details** drop-down list: Provides loop information, such as the device, role, port in the loop, duplex mode, and VLAN that was involved in the loop.

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**
Root Cause Analysis	The Machine Reasoning Engine (MRE) allows you to perform complex root cause analysis and suggests corrective actions. 1. Click **Run Machine Reasoning** to allow the MRE to start troubleshooting. After the troubleshooting is completed, the **Machine Reasoning Completed** pop-up dialog box appears. 2. In the pop-up dialog box, click **View Details**. The **Root Cause Analysis** area appears with the **Conclusions** tab opened by default providing the details of the root cause analysis. 3. From the **Conclusions** area, click **View Relevant Activities** to view activity details. The activity shows commands that were used at each step of the root cause analysis. 4. Click the 👍 👎 icon to provide your feedback, whether the information on this page was helpful or not, 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 cancel the reasoning activity while it is running, click **Stop**. **Note** The check mark indicates that the step is complete. **Figure 26: Reasoning Activity** 6. Click **Run Again** if you want to rerun the MRE.
Topology icon	Click the ✛ icon to view the topology of the network segment in which the loop occurred.

Issue Instance Details for a PoE Issue
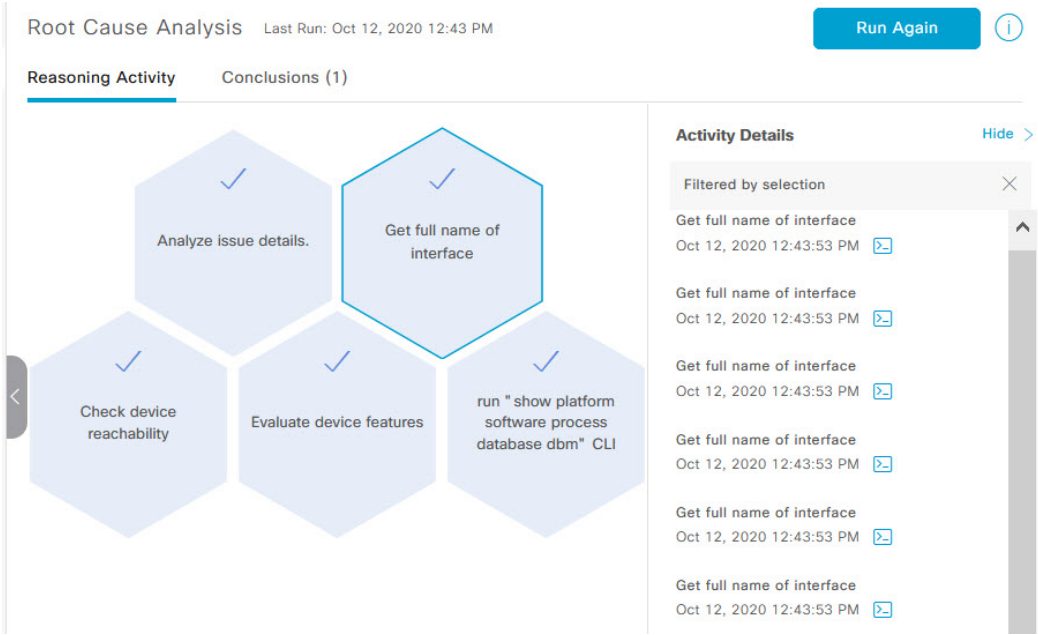
✎

Note The **Issue Instance Details** slide-in pane is part of the **Open Issues** workflow. See Step 4 in View Open Issues, on page 188.

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

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**

Status drop-down list	Allows you to change the status of the issue. Do the following:
	
	 • To resolve an issue, from the **Status** drop-down list, choose **Resolve**.
	
	 • To stop an issue from being reported, do the following:
	
	    1. From the **Status** drop-down list, choose **Ignore**.
	
	    2. Using the slider, set the number of hours to ignore the issue and click **Confirm**.

Summary	Summary of the issue, which can include information, such as device, role, time, location, and potential root cause.
Problem Details	Provides a brief description of the problem along with the following: • **Event Types** tabs: Contains tabs for the types of events that occurred. Click an event tab to view the list of errors for the event type. • **Errors**: Errors that occurred for each event type. The errors are refreshed based on the **Event Types** tab you click. • **Detailed Information** Click an error to view additional information about it.

Issue Instance Details (Second Slide-In Pane)	
Item	**Description**
Root Cause Analysis	The Machine Reasoning Engine (MRE) allows you to perform complex root cause analysis and suggests corrective actions. 1. Click **Run Machine Reasoning** to allow the MRE to start troubleshooting. After the troubleshooting is completed, the **Machine Reasoning Completed** dialog box appears. 2. In the pop-up dialog box, click **View Details**. The **Root Cause Analysis** area appears with the **Conclusions** tab opened by default providing the details of the root cause analysis. 3. From the **Conclusions** area, click **View Relevant Activities** to view activity details. The activity shows commands that were used at each step of the root cause analysis. 4. Click the 👍 👎 icon to provide your feedback, whether the information on this page was helpful or not. 5. Click the **Reasoning Activity** tab to understand how the MRE reached that conclusion. Each reasoning activity is provided in hexagon shaped blocks as shown in the following figure. Click each hexagon shaped block to view **Activity Details** in the right pane. To cancel the reasoning activity while it is running, click **Stop**. **Note** The check mark indicates that the step is complete. *Figure 27: Reasoning Activity* 6. Click **Run Again** if you want to rerun the MRE.

Troubleshoot Wired Client Issues Using MRE

Use this procedure to view wired client issues detected by Assurance and troubleshoot them using the MRE workflow. For a list of wired client issues that support MRE, see MRE Issues, on page 226.

Before you begin

Make sure that the MRE knowledge base is updated with the latest knowledge packs. See Update the Machine Reasoning Knowledge Base, on page 64.

Step 1   Click the menu icon (☰) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **Client** tab.

The **Client** health dashboard appears.

Step 3   In the **Wired Clients** summary area, click **View Details** to open a slide-in pane.

Step 4   In the slide-in pane, in the **Wired Clients** chart, click **Authentication** or **DHCP**.

If you click **Authentication**, the following information is displayed below the chart: Top Authentication Failure Reason, Top Location, Top Switch, Top Host Device Type. A table is also displayed, which provides a list of clients that failed authentication.

If you click **DHCP**, the following information is displayed below the chart: Top DHCP Failure Reason, Top Location, Top Switch, Top Host Device Type. A table is also displayed.

Step 5   Do one of the following:
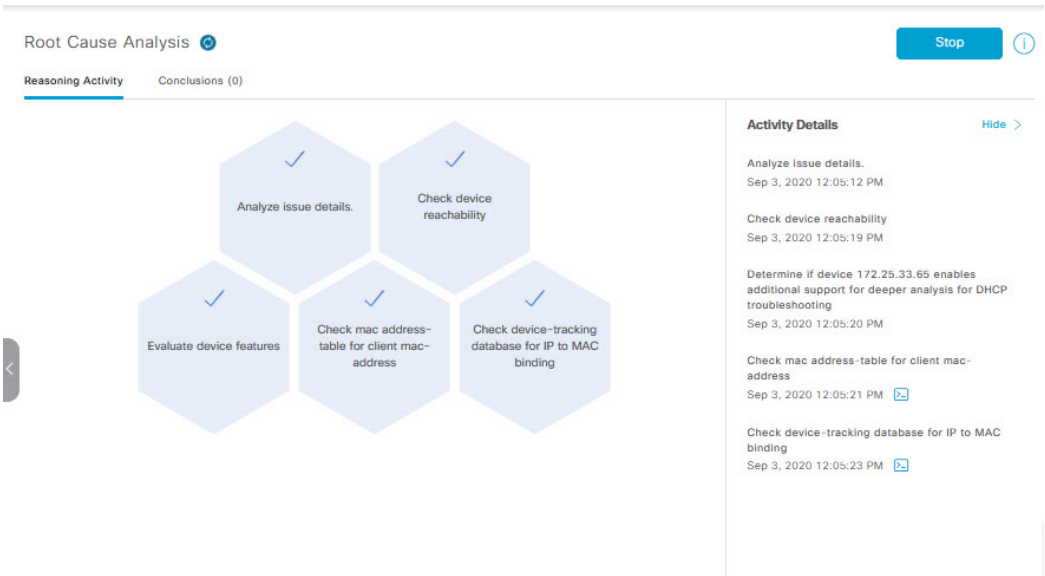
- If you are a user with SUPER-ADMIN-ROLE privileges, enter the client's MAC address in the search tool.
- In the table, from the **Identifier** column, click the hyperlinked identifier.

The **Client 360** window for the client is displayed.

Step 6   In the **Client 360** window, from the **Issues** dashlet, click an authentication or DHCP issue.

The **Issue Details** window is displayed with the following information:

Issue Details	
Item	**Description**

Status drop-down list	Provides the current status of the issue, which you can change. Do the following:
	
	• To resolve an issue, from the **Status** drop-down list, choose **Resolve**.
	
	• To stop an issue from being reported, do the following:
	
	  a. From the **Status** drop-down list, choose **Ignore**.
	
	  b. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.

Summary	Brief summary of the issue, which can include information, such as device, role, time, location. and potential root cause.

Issue Details

Item	Description
Root Cause Analysis	The Machine Reasoning Engine (MRE) allows you to perform complex root cause analysis and suggests corrective actions.
	a. Click **Run Machine Reasoning** to allow the MRE to start troubleshooting. After the troubleshooting is completed, the **Machine Reasoning Completed** dialog box appears.
	b. In the dialog box, click **View Details**. The **Root Cause Analysis** area appears with the **Conclusions** tab opened by default providing the details of the root cause analysis.
	c. From the **Conclusions** area, click **View Relevant Activities** to view activity details.
	d. Click the 👍 👎 icon to provide your feedback, whether the information on this page was helpful or not, and then click **Submit**.
	e. Click the **Reasoning Activity** tab to understand how the MRE reached that conclusion. Each reasoning activity is provided in hexagon shaped blocks, as shown in the following figure. Click each hexagon shaped block to view activity details in the right pane.
	To stop the reasoning activity while it is running, click **Stop**.
	Note The check mark indicates that the step is complete.
	Figure 28: Reasoning Activity
	f. Click **Run Again** if you want to rerun the MRE.

View Resolved Issues

Use this procedure to view all resolved issues, which fall under the following categories:

- Threshold-based issues: Issues detected by Assurance.

- AI-driven issues: Issues detected by Cisco AI Network Analytics. These issues are triggered based on deviations from the predicted baseline for your specific network environment.

Before you begin

To view AI-driven resolved issues, make sure that you have configured Cisco AI Network Analytics data collection. See Configure Cisco AI Network Analytics, on page 61.

Step 1   Click the menu icon (☰) and choose **Assurance** > **Dashboards** > **Issues**.

The **Open Issues** dashboard appears.

Step 2   Click the **Resolved** tab.

The **Resolved Issues** window appears.

Step 3   Use the **Resolved Issues** window to view the following information:

Resolved Issues Window	
Item	**Description**
⦿ Global	• Click ⦿ Global ⋮ in the top menu bar to choose the site, building, or floor from the Site hierarchy. • Click ⋮ next to the location icon and choose **Site Details** to view the Sites table. • Choose **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table is refreshed. • From the **Go to sites** column, click ⤢ for a site or building to display data only for that location on the **Resolved Issues** dashboard.
24 Hours drop-down list	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do the following: a. From the **24 Hours** drop-down list, choose a time range: **3 hours**, **24 hours**, or **7 days**. b. Specify the **Start Date** and time and the **End Date** and time. c. Click **Apply**. This sets the range of the timeline.

Resolved Issues Window	
Item	**Description**
Timeline slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.
Total Resolved	Provides the total count of resolved issues. The **Total Resolved** value changes depending on the tab you choose. Options are **All** (the default), **P1**, **P2**, **P3**, **P4**, and **AI-Driven**.

Step 4 Click the **All**, **P1**, **P2**, **P3**, **P4**, or **AI-Driven** tab to display a list of issues in that category in the **Issue Type** table.

Issue Type Table in the Resolved Issues Window	
Item	**Description**
Priority	Preassigned priority level of the issue type.
Issue Type	Type of issue. **Note** For AI-driven issues, the ⊡ icon appears in front of the issue type.
Device Role	Role assigned to the device on which the issue was detected. Roles are Access, Core, Distribution, Border Router, or Unknown.
Category	Category under which the issue type falls, such as Connectivity, Availability, Onboarding, and Utilization.
Issue Count	Number of times this type of issue occurred.
Site Count (Area)	Number of sites where this type of issue occurred.
Device Count	Number of devices that were impacted by this type of issue.
Last Occurred Time	Most recent date and time this issue occurred.

Step 5 From the **Issue Type** table, click an issue type.

The first slide-in pane, **Issue Instances**, lists all the resolved issues for that issue type and information such as site, device, device type, occurrence, last occurrence timestamp, last updated timestamp, and the name of the entity that updated the issue.

If the issue condition no longer exists, the system automatically resolves the issue and displays **System** in the **Updated By** column. See

Step 6 From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, provides details about the issue, the name of the entity that resolved the issue, and the timestamp. Depending on the issue, the description and suggested actions are displayed.

View Ignored Issues

Use this procedure to view all issues that are marked as ignored. Ignored issues fall under the following categories:

- Threshold-based issues: Issues detected by Assurance.

- AI-driven Issues: Issues detected by Cisco AI Network Analytics. These issues are triggered based on deviations from the predicted baseline for your specific network environment.

Before you begin

To view the AI-driven ignored issues, make sure that you have configured Cisco AI Network Analytics data collection. See Configure Cisco AI Network Analytics, on page 61.

Step 1 Click the menu icon (☰) and choose **Assurance** > **Dashboards** > **Issues**.

The **Open Issues** dashboard appears.

Step 2 Click the **Ignored** tab.

The **Ignored Issues** window appears.

Step 3 Use the **Ignored Issues** window to view the following information:

Ignored Issues Window

Item	Description
ⓥ Global	• Click ⓥ Global ⋮ in the top menu bar to choose the site, building, or floor from the Site hierarchy. • Click ⋮ next to the location icon and choose **Site Details** to view the Sites table. • Choose **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table is refreshed. • From the **Go to sites** column, click ⤳ for a site or building to display data only for that location on the **Ignored Issues** dashboard.
24 Hours drop-down list	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do the following: a. From the **24 Hours** drop-down list, choose a time range: **3 hours**, **24 hours**, or **7 days**. b. Specify the **Start Date** and time and the **End Date** and time. c. Click **Apply**. This sets the range of the timeline.

Ignored Issues Window	
Item	**Description**
Timeline slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.
Total Ignored	Provides the total count of ignored issues. The **Total Ignored** value changes depending on the tab you choose. Options are **All** (the default), **P1**, **P2**, **P3**, **P4**, and **AI-Driven**.

Step 4   Click the **All**, **P1**, **P2**, **P3**, **P4**, or **AI-Driven** tab to display a list of issues in that category in the **Issue Type** table.

Issue Type Table in the Ignored Issues Window	
Item	**Description**
Priority	Preassigned priority level of the issue type.
Issue Type	Type of issue. **Note** For AI-driven issues, the ⊞ icon appears in front of the issue type.
Device Role	Role assigned to the device on which the issue was detected. Roles are Access, Core, Distribution, Border Router, or Unknown.
Category	Category under which the issue type falls, such as Connectivity, Availability, Onboarding, and Utilization.
Issue Count	Number of times this type of issue occurred.
Site Count (Area)	Number of sites where this type of issue occurred.
Device Count	Number of devices that were impacted by this type of issue.
Last Occurred Time	Most recent date and time this issue occurred.

Step 5   From the **Issue Type** table, click an issue type.

The first slide-in pane, **Issue Instances** lists all the ignored issues for that issue type and information such as site, device, device type, occurrence, and the time stamp of the last occurrence.

Step 6   From the **Issue** column in the **Issue Instances** slide-in pane, click an issue.

A second slide-in pane, **Issue Instance Details**, provides details about the issue. Depending on the issue, the description and suggested actions are displayed.

Resolve or Ignore Issues

Use this procedure to resolve or ignore a bulk of issues or to resolve or ignore a single issue.

Step 1 Click the menu icon (☰) and choose **Assurance** > **Dashboards** > **Issues**.

The **Open Issues** dashboard appears.

Step 2 To resolve or ignore a bulk of issues, do the following:

a) From the **Issue Type** table in the **Open Issues** dashboard, click an issue type.

The first slide-in pane, **Issue Instances**, opens, which lists all the open issues for that issue type. This slide-in-pane allows you to resolve or ignore a bulk of issues.

b) Do one of the following:

- To resolve or ignore specific issues, check the check boxes adjacent to those issues.

- To resolve or ignore all open issues that are displayed in the browser window for an issue type, check the check box adjacent to the **Issue** column. All the issues that are displayed in the browser window are selected.

- If the open issue count is more than 25 (for example, 100), the first 25 issues are displayed in the browser window. To select all the open issues, do the following:

  1. Check the check box adjacent to the **Issue** column.

      The first 25 issues are selected and the **Select all** *number* **open issues** tab appears next to the **Actions** drop-down list.

  2. Click the **Select all** *number* **open issues** to select all open issues for that issue type (for example, all 100 issues).

  3. (Optional) To view the next 25 issues in the browser window, click **Show More** located on the bottom of the page. The next 25 issues are appended to the browser window increasing the displayed issue count to 50. Click **Show More** to view the next 25 issues on the browser window, and so on.

c) To resolve the issues, from the **Actions** drop-down list, choose **Resolve**.

A Warning dialog box appears. Click **Yes** in the Warning dialog box to proceed with the action.

After the issues are resolved, the **View resolved issues** tab is displayed. Click the **View resolved issues** to open the **Resolved Issues** window.

d) To ignore the issues, from the **Actions** drop-down list, choose **Ignore**.

Set the number of hours to ignore the issues on the slider, and then click **Confirm**.

After the issues are ignored, the **View ignored issues** tab is displayed. Click the **View ignored issues** tab to open the **Ignored Issues** window.

Note   If you try to resolve or ignore more than 750 issues, a warning message appears letting you know that it might take up to a minute to complete the action.

Step 3 To resolve or ignore a single issue, do the following:

a) From the **Issue** column in the **Issue Instances** slide-in pane (first slide-in pane), click an issue.
A second slide-in pane, **Issue Instance Details**, opens, which provides details about the issue. This second slide-in-pane allows you to resolve or ignore the issue that you are viewing.

b) To resolve an issue, from the **Status** drop-down list, choose **Resolve**.

c) To stop an issue from being reported, do the following:

1. From the **Status** drop-down list, choose **Ignore**.

2. Set the number of hours to ignore the issue on the slider, and then click **Confirm**.

No Activity on Radio Issue Triggers

A "No Activity on Radio" issue is triggered when all of the following conditions are met for 60 minutes, which is the default trigger time.

Note To change the default trigger time, choose **Assurance** > **Manage** > **Issue Settings**. See Manage Global Issue Settings, on page 209.

- The AP radio operation state is **up**.

- The AP mode is Local or FlexConnect.

- The client count on this radio is equal to 0.

- The RX data or management frame count is *not* increasing.

- The AP radio channel utilization is equal to 0.

- The AP is not an `isolated` AP.

Automatic Issue Resolution

For the following types of issues, if the issue condition no longer exists, the system automatically resolves the issue:

- Switch fan failure.

- Switch power failure.

- Interface is down.

- Wireless Controller/Switch/Router unreachable.

- AP Disconnect from wireless controller.

- No activity on radio.

Note The system automatically resolves this issue when one of the following conditions no longer exists:

   • Client count on this radio is equal to 0.

   • The RX data or management frame count is *not* increasing.

   • The AP radio channel utilization is equal to 0.

After the issue is resolved, the **Updated By** column in the **Resolved Issues** > **Issue Instance** slide-in pane displays **System**. See View Resolved Issues, on page 203.

Manage Global 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 Click the menu icon (≡) and choose **Assurance** > **Manage** > **Issue Settings**.

The **Issue Settings** window appears, with the **Global Profile** tab selected.

Step 2 Set the **DEVICE TYPE** and **CATEGORY** filters to view the type of issues you want to configure.

To view the AI-driven issues, click the **AI-Driven** tab in the **CATEGORY** filter.

Step 3 Click an issue in the **Issue Name** column to open an slide-in pane with the settings:

Note For some issues, changes made to the settings are shared across multiple device types. In the slide-in pane, hover your cursor over the information icon (ⓘ) to display the affected device types.

a) To enable or disable if the issue can be triggered, click the **Enabled** toggle.
b) To set the issue priority, click the **Priority** drop-down list and select the priority. The options are:

   • **P1**: A critical issue that needs immediate attention which can result in wider impact on network operations.

   • **P2**: A major issue that can potentially impact multiple devices or clients.

   • **P3**: A minor issue that has a localized or minimal impact.

   • **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

c) (For certain issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Note For "No Activity on Radio" trigger conditions, see No Activity on Radio Issue Triggers, on page 208.

Examples of a trigger condition:

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
```

```
Memory Utilization of Access Points greater than 90%
```

d) (Optional) If there are any changes to the settings, you can hover your cursor over **View Default Settings** to display the default issues. Click **Use Default** to restore all the issue settings to the default values.

e) Click **Apply**.

Step 4 (For certain issues) Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered. See Enable Issue Notifications, on page 211.

Manage Custom Issue Settings

You can create custom issue settings for a specific site or group of sites. These settings are called network profiles for Assurance and can be managed from both Assurance and Cisco DNA Center.

By creating a network profile for Assurance, you can control which issue settings are monitored, and you can change the issue priority.

Notes:

- Synchronization to the network device health score is available only for global issue settings, not custom issue settings. For information, see Monitor and Troubleshoot the Health of a Device, on page 74.

- Some global issues are not customizable. These issues are not displayed in the list of custom issues for you to modify.

- To display modified issues at the top of the list, sort by **Last Modified**.

- To delete custom settings, you need to unassign all the sites first.

Step 1 Click the menu icon (≡) and choose **Assurance** > **Manage** > **Issue Settings**.

The **Issue Settings** window appears, with the **Global Profile** tab selected.

Step 2 Click the **Custom Profile** tab.

Step 3 Click **+Add Profile**.

Step 4 In the **Profile Name** field, enter a valid profile name and click **Next**.

Cisco DNA Center adds the profile and the **Edit Profile** window appears.

Step 5 Set the **DEVICE TYPE** and **CATEGORY** filters to view the type of issues you want to configure.

Step 6 Click an issue in the **Issue Name** column to open a slide-in pane with the settings.

Note For some issues, changes made to the settings are shared across multiple device types. In the slide-in pane, Cisco DNA Center displays a caution that indicates the affected device types.

Step 7 To enable or disable whether Cisco DNA Center monitors the issue, click the **Enabled** toggle button.

Step 8 To set the issue priority, click the **Priority** drop-down list and select the priority. The options are:

- **P1**: A critical issue that needs immediate attention which can result in wider impact on network operations.

- **P2**: A major issue that can potentially impact multiple devices or clients.

- **P3**: A minor issue that has a localized or minimal impact.

- **P4**: A warning issue that may not be an immediate problem but addressing it can optimize the network performance.

Step 9   (For certain issues) In the **Trigger Condition** area, you can change the threshold value for when the issue is reported.

Examples of a trigger condition:

```
No Activity on Radio(2.4 GHz) >= 60 minutes.
Memory Utilization of Access Points greater than 90%
```

Step 10   (Optional) If there are any changes to the settings, you can hover your cursor over **View Default Settings** to display the default settings. Click **Use Default** to restore all the issue settings to the default values.

Step 11   Click **Apply**.

Step 12   (For certain issues) Click **Manage Subscription** to subscribe to external notifications for supported issues when they are triggered.

Step 13   To assign the profile to sites, click **Assign Sites**. Check the check box next to the sites that you want to associate with this profile and click **Save**.

The **Edit Profile** window appears.

> **Note**   You can select a parent node or the individual sites. If you select a parent node, all the children under the parent node are also selected. You can uncheck the check box to deselect a site.

Step 14   Click **Done**.

The newly added profile appears on the **Issue Settings** window, in the **Custom Profile** tab.

Enable Issue Notifications

Use this procedure to receive external notifications for when specific issues are triggered in Assurance. When an issue is triggered and there is status change, Assurance can generate a REST or email notification.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Manage** > **Issue Settings**.

The **Issue Settings** window appears.

Step 2   Click **Manage Subscriptions**.

The **Events** window appears.

Step 3   Check the check boxes of the events that you want to subscribe to.

> **Note**   The **Event** name in Cisco DNA Center platform is the same as the **Issue Name** in Assurance.

Step 4   Click **Subscribe**.
The **Subscribe** dialog box appears.

Step 5 In the **Subscribe** dialog box, enter the details for the subscription:

a) Enter a name for the subscription in the **Name** field.

b) Click the **Subscription Type** drop-down list to select the notification type. You can receive REST or email notifications:

Notification Type	Details
REST	Receive a REST notification when the issue/event is triggered. Configure the following settings: • Select the option **Select an existing endpoint** or **Create a new endpoint** to specify the endpoint and configure the subsequent fields for the endpoint. • **Trust Certificate** • **HTTP Method**: Options are **POST** or **PUT**. • **Headers**: Enter the header details in the **Header Key** and **Header Value** fields.
EMAIL	Receive an email notification when an issue/event is triggered. **Important** To receive email notifications, make sure you have the email server configured under **System** > **Settings** > **External Services** > **Destinations**, in the **Email** tab.

c) Click **Subscribe**.

A subscription for the issue/event is created. A notification is sent when the issue/event is triggered and there is a status change.

What to do next

You can view and manage existing event subscriptions in Cisco DNA Center platform. For details, see "*Working with Events*" in the *Cisco DNA Center Platform User Guide*.

Assurance, Cisco AI Network Analytics, and MRE Issues

Router Issues

The following table lists the router issues detected by Assurance:

Router Issues		
Category	**Issue Name**	**Summary**
Connectivity	BGP tunnel connectivity	Border Gateway Protocol (BGP) connectivity failure with peer due to wrong autonomous system (AS) number.
Connectivity	Interface connecting network devices is down	An interface connecting to network devices is down.
Connectivity	Layer 2 loop symptoms	Host MAC address flapping seen on network device.

Router Issues

Category	Issue Name	Summary
Connectivity	Network device Interface connectivity - BGP Flap	Border Gateway Protocol (BGP) connectivity is flapping with neighbor.
Connectivity	Network Device Interface Connectivity - BGP Down	BGP connectivity is down with neighbor.
Connectivity	Network device interface connectivity - EIGRP adjacency failure	Enhanced Interior Gateway Routing Protocol (EIGRP) adjacency failed with neighbor.
Connectivity	Network device interface connectivity - Interface down	Interface on device is down.
Connectivity	Network device interface connectivity - ISIS adjacency failure	Intermediate System Intermediate System (ISIS) adjacency failed on device.
Connectivity	Network device interface connectivity - OSPF adjacency failure	Open Shortest Path First (OSPF) adjacency failed with neighbor.
Connectivity	WAN Interface Down	A WAN interface is down.
Connected	Failure to install an access policy for SGT	Failure to install a Security Group Access Control List (SGACL) access policy for a Security Group Tag (SGT).
Connected	High input/output error on router interfaces	A high input or output error is detected on the router interfaces. The threshold values can be customized.
Connected	High input/output discards on router interfaces	A high input or output discard is detected on the router interfaces. The threshold values can be customized.
Connected	High input/output utilization on router interfaces	High input or output utilization is detected on the router interfaces. The threshold values can be customized.
Connected	High input/output discards on router WAN interfaces	A high input or output discard is detected on the router's WAN interface. The threshold values can be customized.
Connected	High input/output utilization on router WAN interfaces	High input/output utilization on WAN interfaces. High input or output utilization is detected on the router's WAN interfaces. The threshold values can be customized.
Connected	SGT access policy download failed on the device	Failed to download the Security Group Access Control List (SGACL) access control entries ACEs for a Security Group Tag (SGT).
Connected	SGT access policy installation failed on the device	Failure to install an access policy for a Security Group Tag (SGT). Policy rule error found in Role Based Access Control List (RBACL).
Connected	Unable to download SGT access policy from the policy server	Failure to download the source list for access policy for Security Group Tag (SGT).
Connected	Uninstall of SGT access policy failed on the device	Failure to uninstall an Security Group Access Control List (SGACL) access policy for Security Group Tag (SGT).

Router Issues

Category	Issue Name	Summary
Device	DNA Center and network device time has drifted	Excessive time lag between Cisco DNA Center and device.
Device	Issues based on syslog events - High temperature	Issues created by single occurrence of syslog event related to high temperature.
Device	Router experiencing high CPU utilization	The router is experiencing high CPU utilization. The threshold values can be customized.
Device	Router experiencing high memory utilization	The router is experiencing high memory utilization. The threshold values can be customized.
Availability	Network device HA switchover	The network device went through an High Availability (HA) switchover.
Availability	Router unreachable	The router is unreachable from Cisco DNA Center through ICMP or SNMP.

Core, Distribution, and Access Issues

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

Core, Distribution, and Access Issues

Category	Issue Name	Summary
Connectivity	BGP tunnel connectivity	BGP connectivity failure with peer due to wrong autonomous system (AS) number.
Connectivity	Interface connecting network devices is down	An interface connecting to network devices is down.
Connectivity	Layer 2 loop symptoms	Host MAC address flapping seen on a network device.
Connectivity	Network Device Interface Connectivity- BGP Down	BGP connectivity is down with neighbor.
Connectivity	Network device Interface connectivity - BGP Flap	BGP connectivity is flapping with neighbor.
Connectivity	Network device interface connectivity - EIGRP adjacency failure	EIGRP (Enhanced Interior Gateway Routing Protocol) adjacency failed with neighbor.
Connectivity	Network device interface connectivity - Interface down	Interface on device is down.
Connectivity	Network device interface connectivity - ISIS adjacency failure	Intermediate System Intermediate System (IS-IS) adjacency failed on the device.
Connectivity	Network device interface connectivity - OSPF adjacency failure	Open Shortest Path First (OSPF) adjacency failed with neighbor.

Core, Distribution, and Access Issues

Category	Issue Name	Summary
Connectivity	WAN Interface Down	A WAN interface is down.
Connectivity	Dual Active Detection link failed on network device	The Dual Active Detection link has failed on the network device *Switch Name*.
Connectivity	StackWise Virtual link failed on network device	The StackWise Virtual link has failed on the network device *Switch Name*.
Connectivity	StackWise link failed on network device	The StackWise link has failed on the network device *Switch Name*.
Connected	Fabric devices connectivity - Border overlay	The fabric edge lost connectivity to the fabric border in the virtual network.
Connected	Fabric devices connectivity - Border underlay	The fabric edge lost connectivity to the fabric border in the physical network.
Connected	Fabric devices connectivity - Control border underlay	The fabric node lost connectivity to the co-located fabric border and control plane in the physical network.
Connected	Fabric devices connectivity - Control underlay	The fabric node lost connectivity to the fabric control plane device in the physical network.
Connected	Fabric devices connectivity - DHCP overlay	The fabric node lost connectivity to the DHCP server in the virtual network.
Connected	Fabric devices connectivity - DHCP underlay	The fabric node lost connectivity to the DHCP server in the physical network.
Connected	Fabric devices connectivity - DNS overlay	The fabric node lost connectivity to the DNS server in the virtual network.
Connected	Fabric devices connectivity - DNS underlay	The fabric node lost connectivity to the DNS server in the physical network.
Connected	Fabric devices connectivity - External URL	The fabric border cannot reach the user-provisioned external URL.
Connected	Fabric devices connectivity - ISE server	The fabric edge lost connectivity to the ISE server in the physical network.
Connected	Fabric devices connectivity - Multicast RP	The fabric border node lost connectivity to multicast rendezvous point (RP).
Connected	Fabric devices connectivity - AAA server	The fabric edge node lost connectivity to the AAA server in the physical network.
Connected	Fabric devices connectivity - Border anchored	The fabric border node lost connectivity to the fabric anchored border node in the physical network.

Core, Distribution, and Access Issues		
Category	**Issue Name**	**Summary**
Connected	Fabric WLC to MapServer connectivity	The fabric wireless controller lost connectivity to the fabric control plane node.
Connected	Failure to install an access policy for SGT	Failure to install an SGACL access policy for SGT.
Connected	High input/output error on switch interfaces	A high input or output error is detected on the switch interfaces. The threshold values can be customized.
Connected	High input/output discard on switch interfaces	A high input or output discard is detected on the switch interfaces. The threshold values can be customized.
Connected	High input/output utilization on switch interfaces	High input or output utilization is detected on the switch interfaces. The threshold values can be customized.
Connected	SGT access policy download failed on the device	Failed to download SGACL ACEs for SGT.
Connected	SGT access policy installation failed on the device	Failure to install an access policy for SGT. Policy rule error found in RBACL.
Connected	Unable to download SGT access policy from the policy server	Failure to download the source list for access policy for SGT.
Connected	Uninstall of SGT access policy failed on the device	Failure to uninstall an SGACL access policy for SGT.
Device	Device reboot crash	Device has rebooted due to a hardware or software crash.
Device	Device time has drifted from Cisco DNA Center	Excessive time lag between Cisco DNA Center and the device network.
Device	Interface is flapping on network device	A port interface is flapping on a switch.
Device	Issues based on syslog events - High temperature	Issues created by single occurrence of syslog event related to high temperature.
Device	Issues based on syslog events - POE	Issues created by single occurrence of syslog event related to power.
Device	PoE port in error state	PoE port is error disabled as reported by a syslog event.
Device	PoE powered device flagged faulty	PoE-capable device connected to a PoE port has been flagged faulty as reported by a syslog event.
Device	Power denied for PoE powered device	PoE-capable device connected to a PoE port has been power denied as reported by a syslog event.
Device	Stack member removal	Stack member was removed.
Device	Stack member running incompatible image	Stack member is running an incompatible image.

Core, Distribution, and Access Issues		
Category	**Issue Name**	**Summary**
Device	Switch experiencing high CPU utilization	The switch is experiencing high CPU utilization. The threshold values can be customized.
Device	Switch experiencing high memory utilization	The switch is experiencing high memory utilization. The threshold values can be customized.
Device	Switch fan failure	Fan failure on the switch.
Device	Switch power failure	Power supply failure on the switch.
Device	TCAM utilization high issues	Issues for TCAM exhaustion in Layer 2, Layer 3, QoS, and SGACL.
Availability	Network device HA switchover	The network device went through an HA switchover.
Availability	Switch unreachable	The switch is unreachable from Cisco DNA Center through ICMP or SNMP.
Utilization	Map cache limit reached	Map cache entries have exceeded the limit on the map server.

Controller Issues

The following table lists the controller issues detected by Assurance:

Controller Issues		
Category	**Issue Name**	**Summary**
Connectivity	Interface connecting network devices is down	An interface connecting to network devices is down.
Connected	Fabric WLC to MapServer connectivity	The fabric wireless controller lost connectivity to the fabric control plane node.
Device	Device time has drifted from Cisco DNA Center	Excessive time lag between Cisco DNA Center and the network device.
Availability	Network device HA switchover	The network device went through an HA switchover.
Availability	WLC monitor	The network controller is not receiving data from the wireless controller.
Availability	WLC power supply failure	The power supply failed on this wireless controller.
Availability	WLC reboot crash	A wireless controller reboot crash occurred.
Availability	WLC unreachable	The wireless controller is unreachable from Cisco DNA Center through ICMP or SNMP.
Utilization	AP license exhausted on WLC	The wireless controller currently has no free AP licenses.
Utilization	WLC memory high utilization	The wireless controller is experiencing high memory utilization.

Access Point Issues

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

Access Point Issues		
Category	**Issue Name**	**Summary**
Availability	AP coverage hole	The wireless LAN controller detected a coverage hole around the AP.
Availability	AP Disconnect from Cisco WLC	The AP is disconnected from the wireless LAN controller. The AP's CAPWAP link to the wireless LAN controller is down.
Availability	AP flap	The AP has flapped. The AP disconnected from the wireless LAN controller and then connected back to the wireless LAN controller. This issue is triggered when the AP flaps more than two time within a 15-minute period.
Availability	AP reboot crash	AP has rebooted due to a hardware or software crash.
Utilization	AP CPU high utilization	AP is experiencing high CPU utilization.
Utilization	AP memory high utilization	AP is experiencing high memory utilization.
Utilization	Radio high utilization (2.4GHz)	2.4-GHz radios on APs are experiencing high utilization.
Utilization	Radio high utilization (5GHz)	5-GHz radios on APs are experiencing high utilization.
Utilization	Radio high utilization (6GHz)	6-GHz radios on APs are experiencing high utilization.
Utilization	No activity on radio (2.4GHz)	No activity on 2.4-GHz radio on AP.
Utilization	No activity on radio (5GHz)	No activity on 5-GHz radio on AP.
Utilization	No activity on radio (6GHz)	No activity on 6-GHz radio on AP.
AP Anomaly	AP anomaly	AP encountered anomaly issue.
Availability	Poor RF (2.4 GHz) on a floor	This issue is triggered when APs have a poor wireless experience. The poor RF issue occurs when at least one AP has interference or noise above the threshold within a 30-minute timeframe.
Availability	Poor RF (5 GHz) on a floor	This issue is triggered when APs have a poor wireless experience. The poor RF issue occurs when at least one AP has interference or noise above the threshold within a 30-minute timeframe.
Availability	Poor RF (6 GHz) on a floor	This issue is triggered when APs have a poor wireless experience. The poor RF issue occurs when at least one AP has interference or noise above the threshold within a 30-minute timeframe.
Availability	Radio Down (2.4GHz)	2.4-GHz radio is down on AP.
Availability	Radio Down (5GHz)	5-GHz radio is down on AP.
Availability	Radio Down (6GHz)	6-GHz radio is down on AP.

Wired Client Issues

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

Wired Client Issues		
Category	**Issue Name**	**Summary**
Onboarding	Client DHCP reachability issue	The client has failed to obtain an IP address from DHCP server.
Onboarding	Wired client authentication failures - Dot1.x failure	The wired client failed authentication due to Dot1.x problems. **Note** This issue is applicable only for single wired clients.
Onboarding	Wired client authentication failures - MAB failure	The wired client failed authentication due to MAC authentication bypass problems. **Note** This issue is applicable only for single wired clients.

Wireless Client Issues

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

✎

Note These issues are applicable for both single clients and multiple clients.

Wireless Client Issues		
Category	**Issue Name**	**Summary**
Onboarding	802.11r client roaming slowly	While roaming, a wireless client capable of fast roaming is doing full authentication instead of fast authentication.
Onboarding	Client DHCP reachability issue	The client has failed to obtain an IP address from DHCP server.
Onboarding	Wireless client excluded - Client was excluded before roaming	Wireless client excluded - Client was excluded before roaming.
Onboarding	Wireless client failed to connect - Client timeout	Wireless client failed to connect - Failed to authenticate due to client timeout.
Onboarding	Wireless client failed to connect - DHCP timeout	Wireless clients took longer than 10 seconds to connect. The delay was in the IP Learning phase due to DHCP server or client timeout.
Onboarding	Wireless client failed to connect - Incorrect PSK	Multiple wireless clients failed to connect and were excluded by the wireless controller. They were excluded because the client's PSK did not match the configured WLAN PSK.
Onboarding	Wireless client failed to connect - WLC internal error	Wireless client failed to connect - wireless controller internal error.

Wireless Client Issues

Category	Issue Name	Summary
Onboarding	Wireless client failed to roam - AAA server rejected client	Wireless client failed to roam - AAA server rejected client.
Onboarding	Wireless client failed to roam - AAA server timeout	Wireless client failed to roam - AAA server timeout.
Onboarding	Wireless client failed to roam - Client PMK not found	Wireless client failed to roam - Client PMK not found.
Onboarding	Wireless client failed to roam - Client timeout	Wireless client failed to roam - Failed to authenticate due to client timeout.
Onboarding	Wireless client failed to roam - Security parameter mismatch	Wireless client failed to roam - Security parameter mismatch.
Onboarding	Wireless client failed to roam - WLC configuration error	Wireless client failed to roam - wireless controller configuration error.
Onboarding	Wireless client failed to roam - WLC internal error	Wireless client failed to roam - wireless controller internal error.
Onboarding	Wireless client failed to roam between APs - External error	Wireless client failed to roam between APs - External error.
Onboarding	Wireless client failed to roam between APs - WLC configuration mismatch	Multiple wireless clients failed to roam between APs due to a wireless LAN controller configuration mismatch.
Onboarding	Wireless clients took a long time to connect - Excessive time due to authentication timeouts	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to authentication timeouts. The clients that run into this problem are grouped by AAA server or wireless controller.
Onboarding	Wireless clients took a long time to connect - Excessive time due to DHCP server failures	Multiple wireless clients took a long time to connect. The excessive onboarding time is due to DHCP server failures. The clients that run into this problem are grouped by the DHCP server or wireless controller.
Onboarding	Wireless clients took a long time to connect - Excessive time due to failed credentials	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to authentication delays caused by failed credentials. The clients that run into this problem are grouped by AAA server or wireless controller.
Onboarding	Wireless clients took a long time to connect - Excessive time due to WLC failures	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to wireless LAN controller failures during authentication. The clients that run into this problem are grouped by wireless controller.
Onboarding	Wireless clients took a long time to connect - Excessive time for authentication due to AAA server or network delays	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to authentication delays. The authentication delays were caused by AAA server or network delays.

Wireless Client Issues

Category	Issue Name	Summary
Onboarding	Wireless clients excluded - IP theft issue	Multiple wireless clients have been excluded from connecting to the wireless network. IP theft issues were detected on the clients. The clients that run into this problem are grouped by wireless controller.
Onboarding	Wireless clients failed to connect - AAA server rejected clients	Multiple wireless clients failed during authentication with a AAA Server Reject failure reason. The AAA server rejected the client's authentication requests. The clients that run into this problem are grouped by AAA server or wireless controller.
Onboarding	Wireless clients failed to connect - AAA server timeout	Multiple wireless clients failed during authentication with a AAA Server Timeout failure. This failure occurs when the wireless controller doesn't receive a response from the AAA to the client's authentication messages and times out after retries. The clients that run into this problem are grouped by AAA server or wireless controller.
Onboarding	Wireless clients failed to connect - Client PMK not found	Multiple wireless clients failed to connect due to authentication problems. The client's PMK was not found.
Onboarding	Wireless clients failed to connect - DHCP server timeout	Multiple wireless clients failed to connect. The failure was in the IP Learning phase due to DHCP server timeout. The DHCP server timed out and did not respond to DHCP messages. The clients that run into this problem are grouped by DHCP server or wireless controller.
Onboarding	Wireless clients failed to connect - Failed to authenticate due to client timeouts	Multiple wireless clients failed to connect. They failed to authenticate due to client timeouts. The clients failed to respond in time to authentication messages. The clients that run into this problem are grouped by site or AP group.
Onboarding	Wireless clients failed to connect - Failed to get an IP address due to client timeouts	Multiple wireless clients failed to connect. They failed to get an IP address due to client timeouts. The clients failed to respond in time to DHCP messages. The clients that run into this problem are grouped by site or AP group.
Onboarding	Wireless clients failed to connect - Failed to get an IP address due to DHCP server or client timeouts	Multiple wireless clients failed to connect. They failed to get an IP address due to DHCP server timeouts or client timeouts. Either the DHCP server or the clients failed to respond in time to DHCP messages. The clients that run into this problem are grouped by site or AP group.
Onboarding	Wireless clients failed to connect - Security parameter mismatch	Multiple wireless clients failed to connect due to authentication problems caused by a security parameter mismatch.
Onboarding	Wireless clients failed to connect - WLC configuration error	Multiple wireless clients failed to connect due to authentication problems. There are wireless LAN controller configuration errors. The clients that run into this problem are grouped by wireless controller.
Onboarding	Wireless clients failed to roam - Client exclusion policies on the WLC	Multiple wireless clients failed to roam. Clients were excluded due to client exclusion policies on the wireless LAN controller. The clients that run into this problem are grouped by wireless controller.

Wireless Client Issues		
Category	**Issue Name**	**Summary**
Onboarding	Wireless clients failed to roam - Clients were excluded before roaming	Multiple wireless clients failed to roam. The clients were excluded on the wireless LAN controller before roaming. The clients that run into this problem are grouped by wireless controller.
Onboarding	Wireless clients failed to roam - WLC configuration mismatch	Multiple wireless clients failed to roam between APs due to a wireless LAN controller configuration mismatch.
Onboarding	Wireless clients took a long time to connect - WLC failures	Multiple wireless clients took a long time to connect. The excessive onboarding time was due to wireless LAN controller failures during authentication. The clients that run into this problem are grouped by wireless controller.
Connected	Dual band capable client prefers 2.4 GHz over 5 GHz	Dual-band capable client is consistently connecting to a 2.4-GHz radio, even though a 5-GHz radio that provides a better experience is available.
Connected	Wireless client has poor RF	Wireless client is experience poor RF condition because the client has no better neighboring APs to roam to.
Connected	Wireless client shows sticky behavior	Wireless client is maintaining an association with an AP that has a weaker signal. It should roam to an available AP that has the stronger signal.

Enable AAA Failure Root Cause Analysis Issues

Cisco DNA Center integrates with Cisco ISE syslogs to troubleshoot the following issues:

- Wireless clients failed to connect: AAA server rejected clients

- Wireless clients failed to connect: AAA server timeout

The troubleshooting workflow is an MRE workflow that you access from a single client issue in the **Client 360** window, or from wireless client issues in the **Issues** dashboard.

Cisco DNA Center shows the syslogs generated by Cisco ISE for client authentication failures, enabling you to determine the root cause of the client authentication failure without having to log in to Cisco ISE and search for clients there.

To enable AAA Failure Root Cause Analysis issues in Assurance, do the following:

Step 1   In Cisco DNA Center, choose **System** > **Settings** > **External Services** > **Authentication and Policy Servers** and add and configure Cisco ISE to the Cisco DNA Center cluster. This step adds the Cisco ISE policy service node (PSN) to the syslog allowed list.

Step 2   In Cisco ISE, choose **Administration** > **System** > **Logging** > **Remote Logging Targets** and add Cisco DNA Center as a syslog destination.

Step 3   In Cisco ISE, choose **Administration** > **System** > **Logging** > **Logging Categories** and add the target that you added in the previous step to the following logging categories: **Failed Attempts**, **Authentication Flow Diagnostics**, and **RADIUS Diagnostics**.

Cisco ISE syslogs can now be sent to Cisco DNA Center. Cisco DNA Center processes and saves the Cisco ISE syslogs for client onboarding problems.

Application Issues

The following table lists the application issues detected by Assurance:

Application Issues		
Category	**Issue Name**	**Summary**
Application	Application experience issues	All issues pertaining to Application Experience.

Sensor Issues

The following table lists the sensor issues detected by Assurance.

When two or more sensors on the same floor fail a test in a 30-minute period, the sensor can raise an issue based on the failed root cause. These sensor issues are all global issues, meaning that the sensor issue from any floor is escalated and shown in the **Issues** dashboard.

Sensor Issues		
Category	**Issue Name**	**Summary**
Sensor Test	Sensors - Speed test HTTP error	Multiple sensors are reporting speed test HTTP error while accessing query server.
Sensor Test	Sensors - DHCP failures	Multiple sensors failed to get an IPv4 address.
Sensor Test	Sensors - DNS resolution failed	Multiple sensors failed to resolve domain name with DNS server.
Sensor Test	Sensors - Failed association during onboarding	Multiple sensors failed to associate during onboarding.
Sensor Test	Sensors -Failed authentication during onboarding	Multiple sensors failed to authenticate during onboarding.
Sensor Test	Sensors - FTP test fail	Multiple sensors are reporting unable to connect to FTP server.
Sensor Test	Sensors - FTP transfer fail	Multiple sensors are reporting failed to transfer file with FTP server.
Sensor Test	Sensors - FTP unreachable	Multiple sensors are reporting unreachable FTP server.
Sensor Test	Sensors - IPerf invalid config error	Multiple sensors have failed to conduct the iPerf test due to receiving invalid iPerf configurations.
Sensor Test	Sensors - IPerf server busy	Multiple sensors have failed to conduct the iPerf test due to an iPerf busy error.
Sensor Test	Sensors - IPerf test network error	Multiple sensors have failed to conduct the iPerf test due to an iPerf network error.

Sensor Issues

Category	Issue Name	Summary
Sensor Test	Sensors - IPerf undefined error	Multiple sensors have failed to conduct the iPerf test due to an undefined error.
Sensor Test	Sensors - IPSLA no IP address	Multiple sensors are reporting IPSLA test IP address not received from Cisco DNA Center.
Sensor Test	Sensors - IPSLA no response	Multiple sensors are reporting IPSLA test - no response from IPSLA responder.
Sensor Test	Sensors - IPSLA socket error	Multiple sensors are reporting IPSLA test socket error.
Sensor Test	Sensors - IPSLA test fail	Multiple sensors are reporting IPSLA test failed.
Sensor Test	Sensors - IPSLA unsupported probe type	Multiple sensors are reporting IPSLA test unsupported probe type.
Sensor Test	Sensors - Mail server test fail	Multiple sensors are reporting failed to connect to mail server.
Sensor Test	Sensors - Mail server unreachable	Multiple sensors are reporting unreachable mail server.
Sensor Test	Sensors - No NDT server	Multiple sensors are reporting speed test NDT server does not exist.
Sensor Test	Sensors - Onboarding failures	Sensors failed to connect to the wireless network.
Sensor Test	Sensors - Outlook server test fail	Multiple sensors are reporting failed to connect to Outlook Web Access.
Sensor Test	Sensors - Outlook server unreachable	Multiple sensors are reporting unreachable Outlook Web Access host.
Sensor Test	Sensors - Query server timeout	Multiple sensors are reporting speed test query server timeout.
Sensor Test	Sensors - RADIUS authentication fail	Multiple sensors are reporting failed to authenticate with RADIUS server.
Sensor Test	Sensors - Speed test fail	Multiple sensors are reporting speed test failed.
Sensor Test	Sensors - Speed test generic error	Multiple sensors are reporting speed test generic failure.
Sensor Test	Sensors - Speed test uplink timeout	Multiple sensors are reporting speed test uplink test timeout.
Sensor Test	Sensors - Speed test URL error	Multiple sensors are reporting speed test URL error while accessing query server.
Sensor Test	Sensors - Unreachable host	Multiple sensors are reporting ping failure to the host. Unreachable host.
Sensor Test	Sensors - Unreachable RADIUS	Multiple sensors are reporting unreachable RADIUS server.
Sensor Test	Sensors - Web authentication fail	Multiple sensors are reporting clients are failing web authentication test.
Sensor Test	Sensors - Web server test failed	Multiple sensors are reporting failed to load page from web server.
Sensor Test	Sensors - Web server unreachable	Multiple sensors are reporting unreachable web server.
Sensor Test	Sensors - Web socket error	Multiple sensors are reporting speed test websocket error during the test.

Sensor Issues		
Category	**Issue Name**	**Summary**
Sensor Test	Sensors - Speed test uplink proxy error	Multiple sensors are reporting speed test uplink test proxy error.

AI-Driven Issues

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

AI-Driven Issues		
Category	**Issue Name**	**Summary**
Connection Issues		
Onboarding	AI Excessive time to connect - High deviation from baseline	The network is experiencing excessive onboarding time compared to usual. Clients are taking longer than the usual time to connect to *SSID*.
Onboarding	AI Excessive failures to connect - High deviation from baseline	The network is experiencing excessive onboarding time compared to usual. Clients are taking longer than the usual time to connect to *SSID*.
Onboarding	AI Wireless clients took a long time to connect - Total time above baseline	Wireless clients took longer to connect to *SSID* at *location*.
AAA	AI Excessive time to get Associated - High deviation from baseline	Excessive time to get associated - At least *value*% increase in time on *SSID*.
AAA	AI Excessive failures to Associate - High deviation from baseline	Excessive failures to get associated - At least *value*% increase in failures on *SSID*.
AAA	AI Excessive time to get Authenticated - High deviation from baseline	Excessive time to get authenticated - At least *value*% increase in time on *SSID*.
AAA	AI Excessive failures to get Authenticated - High deviation from baseline	Excessive failures to get authenticated - At least *value*% increase in failures on *SSID*.
DHCP	AI Excessive time to get an IP Address - High deviation from baseline	Excessive time to get an IP address - At least *value*% increase in time from *server_IP*.
DHCP	AI Excessive failures to get an IP address - High deviation from baseline	Excessive failures to get an IP address - At least *value*% increase in failures from *server_IP*.
Network Connectivity Issue		
Connectivity	AI Host MAC address flapping seen on network device	Network is experiencing Layer 2 loop symptoms.
Application Experience Issues		

AI-Driven Issues

Category	Issue Name	Summary
Throughput	[AI] Drop in total radio throughput for All Applications	APs in network are experiencing a drop in total radio throughput for all applications. These radios are in the *frequency* band. These radios are located at *location*.
Throughput	[AI] Drop in radio throughput for Cloud Applications	APs in network are experiencing a drop in Cloud Applications throughput. These radios are in the *frequency* band. These radios are located at *location*.
Throughput	[AI] Drop in radio throughput for Social Applications	APs in network are experiencing a drop in Social Applications throughput. These radios are in the *frequency* band. These radios are located at *location*.
Throughput	[AI] Drop in radio throughput for Media Applications	APs in network are experiencing a drop in Media Applications throughput. These radios are in the *frequency* band. These radios are located at *location*.
Throughput	[AI] Drop in radio throughput for Collab Applications	APs in network are experiencing a drop in Collab Applications throughput. These radios are in the *frequency* band. These radios are located at *location*.

MRE Issues

The following table lists the issues detected by Assurance that you can troubleshoot using the MRE workflow:

MRE Issues

Category	Issue Name	Summary
Wired Client Issues		
Onboarding	Client DHCP reachability issue	The client has failed to obtain an IPv4 address from the DHCP server.
Onboarding	Wired client authentication failures - Dot1.x failure	The wired client failed authentication due to Dot1.x problems. **Note** This issue is applicable only for single wired clients.
Onboarding	Wired client authentication failures - MAB failure	The wired client failed authentication due to MAC authentication bypass problems. **Note** This issue is applicable only for single wired clients.
PoE Issue		
Device	PoE powered device flagged faulty	Syslog event flagged a PoE-capable device connected to a PoE port as faulty.

C H A P T E R **13**

View and Manage Events

Events Dashboard Overview

The **Events** dashboard provides a contextual view of events for devices (routers, switches, wireless controllers, APs) and endpoints (wired and wireless). Instead of having to search for events triggered by devices that are connected to other devices involved in an event, Assurance provides these details for you.

By default, the **Events** dashboard displays a timeline chart and a list view.

The timeline chart provides a color representation of the number of events by device type that occurred over a period of time.

The list view displays a table of events. Up to 10,000 events can be displayed, even if more events have been logged. You can export up to 5000 events to a CSV file. However, if there are more than 5000 events, the export capability is disabled.

From the list view, you can click an event to view its details, including events triggered by connected devices. You can configure the event time period in 15-minute increments, up to one hour (+/- 15 minutes, +/- 30 minutes, +/- 45 minutes, +/- 1 hour).

When you select more than one event, you can view multiple cards with event details. When you have multiple event cards displayed, you can minimize, maximize, and close cards. For example, to view the connected device events table for an event, maximize the event card. To return to the multiple card view, minimize the card.

View Device Events

Use this procedure to view events generated by routers, switches, wireless controllers, and APs.

Step 1   Click the menu icon (☰) and choose **Assurance** > **Dashboards** > **Issues and Events**.

The **Events** dashboard opens with **Device** selected as the **Category Type** by default.

Figure 29: Device Events Dashboard

Device Events Dashboard	
Item	**Description**
⊘ Global	• Click ⊘ Global ⋮ in the top menu bar to choose the site, building, or floor from the Site hierarchy. • Click ⋮ next to the location icon and choose **Site Details** to view the event counts for each site. • Choose **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table is refreshed. • From the **Go to sites** column, click ⊡ for a site or building to display events for only that location.

Device Events Dashboard	
Item	**Description**
🕐 **Time Range** setting	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do the following: a. From the **24 Hours** drop-down list, choose a time range: **3 hours**, **24 hours**, or **7 days**. b. Specify the **Start Date** and time, and the **End Date** and time. c. Click **Apply**. This sets the range of the timeline.

Timeline Slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range.
	
	The colors represent the device type:
	
	   : Router
	   : Switch
	   : Wireless controller
	   : AP
	
	The intensity of the color indicates its significance, whether more or fewer events have occurred for that device. For example, a lighter shade of blue indicates fewer router events than a deeper shade of blue.

Total Events	The total number of events for all device types for a specific time range.

Step 2 Under **Events**, for the **Category Type**, click the **Router**, **Switch**, **Wireless Controller**, or **AP** tab to display a list of events for that device type in the table.

Events Table	
Item	**Description**
Event Name	Name of the event. Click the event name to open a slide-in pane with details about the event.
Status	Status of the device. The color represents the severity of the event. ● : Error. ● : Warning. ● : Info. ● : No data available.
Severity	Severity of the event: Critical and above (Emergency and Alert) and less severe than Critical level (Error, Warning, Notice, and Info).
Timestamp	Date and time when the event occurred.

Events Table	
Item	**Description**
Device Name	Name of the device that was impacted by the event. Click the device name to open the **Device 360** window.
Event Type	Category of the event: **Syslog**, **Trap**, **Event**, or **AP Event**.
Device IP	IP address of the device.

Step 3 To view multiple events, check the check box next to each event you want to view and click **Show Selected Events**.

The **Multiple Events** slide-in pane opens with each event displayed in a separate card.

From inside a card, you can do the following:

- Minimize, maximize, and close a card.

- Display more details by clicking the down arrow.

- Click hyperlinks to launch the respective device 360 window.

When a card is maximized, any connected device events are displayed.

Step 4 From the **Multiple Events** slide-in pane, click the list view icon ≡ to display a compilation of all the subevents sequentially in a list.

To return to the card view, click the card view icon .

View Endpoint Events

Use this procedure to view events generated by wired and wireless endpoints.

Step 1 Click the menu icon (≡) and choose **Assurance** > **Dashboards** > **Issues and Events**.

Step 2 Click the **Events** tab.

The **Events** dashboard opens.

Step 3 For the **Category Type**, click the **Endpoints** tab.

Figure 30: Endpoint Events Dashboard

Device Events Dashboard	
Item	**Description**
📍 Global	• Click 📍 Global ⋮ in the top menu bar to choose the site, building, or floor from the Site hierarchy. • Click ⋮ next to the location icon and choose **Site Details** to view the event counts for each site. • Choose **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table is refreshed. • From the **Go to sites** column, click 🔳 for a site or building to display events for only that location.

Device Events Dashboard	
Item	**Description**
🕐 **Time Range** setting	Allows you to display information on the window based on the time range you select. The default is **24 Hours**. Do the following: a. From the **24 Hours** drop-down list, choose a time range: **3 hours**, **24 hours**, or **7 days**. b. Specify the **Start Date** and time, and the **End Date** and time. c. Click **Apply**. This sets the range of the timeline.
Timeline Slider	Allows you to specify a more granular time range. Click and drag the timeline boundary lines to specify the time range. The colors represent the endpoint type: ████: Wired ████: Wireless The intensity of the color indicates its significance, whether more or fewer events have occurred for that device. For example, a lighter shade of purple indicates fewer endpoint events than a deeper shade of purple.
Total Events	The total number of events for all endpoint types for a specific time range.

Step 4 Click the **Wired** or **Wireless** tab to display a list of events for that endpoint type in the table.

Events Table	
Item	**Description**
Event Name	Name of the event. Click the event name to open a slide-in pane with more details.
Status (Wired Endpoints Only)	The color represents the severity of the event. 🔴: Error. 🟢: Warning. 🔵: Info. ⚫: No data available.
Severity (Wired Endpoints Only)	Severity of the event. Severity can be critical and above (Emergency and Alert) and less severe (Error, Warning, Notice, and Info).
Timestamp	Date and time when the event occurred.
Identifier	Identifier of the endpoint. It can be either user ID, hostname, IP Address, or MAC address, depending on the availability in that order. Click the identifier to open a slide-in pane with more details.

Events Table	
Item	**Description**
Event Type	Category of the event: **Syslog**, **Trap**, **Event**, or **AP Event**.
IPv4 Address	IPv4 address of the device that is connected to the endpoint.
AP Name (Wireless Endpoints Only)	Name of the AP that is connected to the wireless endpoint. Click the AP name to open the AP **Device 360** window.
Switch (Wired Endpoints Only)	Name of the switch that is connected to the wired endpoint. Click the switch name to open the **Device 360** window.
MAC Address	MAC address of the device that is connected to the endpoint.
Port (Wired Endpoints Only)	Switch port that is connected to the wired endpoint.
VLAN ID (Wired Endpoints Only)	VLAN ID of the switch port that is connected to the wired endpoint.
Switch IP Address (Wired Endpoints Only)	IP address of the switch connected to the wired endpoint.
AP MAC (Wireless Endpoints Only)	MAC address of the AP that is connected to the wireless endpoint.
SSID (Wireless Endpoints Only)	SSID that the wireless endpoint is using.
UserID (Wireless Endpoints Only)	User ID of the wireless endpoint.
Wireless Controller Name (Wireless Endpoints Only)	Name of the wireless controller that is connected to the wireless endpoint.
Band (Wireless Endpoints Only)	Radio band that the wireless endpoint is using.
DHCP Server (Wireless Endpoints Only)	DHCP server that the wireless endpoint is using.

Step 5   To view multiple events, check the check box next to each event you want to view and click **Show Selected Events**.

The **Multiple Events** slide-in pane opens with each event displayed in a separate card.

From inside a card, you can do the following:

- Minimize, maximize, and close a card.

- Display more details by clicking the down arrow.

- Click any hyperlinked data.

When a card is maximized, any connected device events are displayed.

Step 6 From the **Multiple Events** slide-in pane, click the list view icon ☰ to display a compilation of all the subevents sequentially in a list.

To return to the card view, click the card view icon ⊞.

Manage Sensors and Sensor-Driven Tests

About Sensors and Sensor-Driven Tests

Sensors use sensor-driven tests to determine the health of wireless networks. A wireless network includes AP radios, WLAN configurations, and wireless network services.

Assurance supports a dedicated sensor, which is dedicated hardware for performing sensor functions.

The dedicated Cisco Aironet 1800s Active Sensor gets bootstrapped using PnP. After this sensor obtains Assurance server-reachability details, it directly communicates with the Assurance server.

Provision Sensors

Provision the Wireless Cisco Aironet 1800s Active Sensor

Step 1 If you are using the Cisco Aironet AP 1800S Sensor without an Ethernet module, you must enable `CiscoProvisioningSSID` on the wireless controller.

> **Note** For the Cisco Aironet 1800s Active Sensor earlier than Software Release 1.3.1.2, make sure that you do not choose the sensor device profile `CiscoProvisioningSSID`. Instead, choose your own SSID for backhaul purposes. See Manage Backhaul Settings, on page 248.

For Cisco Wireless Controllers, see Enable Provisioning SSID on the Wireless Controller, on page 236.

For Cisco Catalyst Wireless Controllers, see Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller, on page 236.

Step 2 Create a backhaul configuration for the sensor.

See Manage Backhaul Settings, on page 248.

Step 3   Provision the Cisco Aironet 1800s Active Sensor.

See Provision a Wireless or Sensor Device, on page 237.

Step 4   (Optional) After the sensor device is available in the device inventory, you can choose to upgrade the software image. See the "Provision Software Images" topic in the *Cisco DNA Center User Guide*.

Enable Provisioning SSID on the Wireless Controller

Step 1   Log in to the Cisco Wireless Controller.

The **Network Summary** page appears.

Step 2   Click the **Advanced** tab.

The **Summary** page appears.

Step 3   In the top menu bar, click the **Management** tab.

Step 4   From the left-navigation pane, choose **Cloud Services** > **Sensor**.

The **Backhaul Configuration** page appears.

Step 5   In the **SSID** field, enter `TFTP`.

Step 6   From the **Auth-type** drop-down list, choose **Open**.

Step 7   From the **Provisioning** drop-down list, choose **Enable**.

Step 8   Make sure that the **DHCP Interface** drop-down list is set to **management**.

Step 9   Click **Apply**.

After provisioning is enabled, a hidden WLAN called `CiscoSensorProvisioning` is created, and the sensor joins using an EAP-TLS client certificate. This enables the sensor to find the Cisco DNA Center IP address, which is done using DHCP Option 43 or through DNS.

Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller

Step 1   Log in to the Cisco Catalyst Wireless Controller GUI.

Step 2   From the left-navigation pane, choose **Configuration** > **Cloud Services**.

The **Cloud Services** page appears.

Step 3   In the **Network Assurance** tab, do the following:

    a)   From the **Network Assurance Configuration** area, set the **Service Status** toggle to **Enabled**.

    b)   From the **Provisioning** area, set the **Provisioning** toggle to **Enabled**.

Step 4   (Optional) In the **VLAN Interface** field, enter the name of the VLAN interface.

Step 5   Click **Apply**.

After Provisioning is enabled, a hidden WLAN called **CiscoSensorProvisioning** is created.

The following error message appears in the bottom-right corner of the window.

Error in Configuring
```
CLI Line 2 Please associate the wlan and policy profile CiscoSensorProvisioning to the desired AP.
```

Note   This message is not an error. The message provides information about the action that must be performed.

Step 6   Verify that the **CiscoSensorProvisioning** policy profile is created.

a)   From the left-navigation pane, choose **Configuration** > **Policy**.

The **Policy Profile** page appears.

b)   Verify that the **CiscoSensorProvisioning** policy appears under the **Policy Tag Name** column.

Step 7   Associate the WLAN and policy profile **CiscoSensorProvisioning** to the appropriate AP. Do the following:

a)   From the left-navigation pane, choose **Configuration** > **Tags**.

The **Manage Tags** page appears.

b)   In the **Policy** tab, click **Add**.

c)   In the **Name** field, enter a unique name for the Policy Tag.

d)   Click **Add**.

e)   From the **WLAN Profile** drop-down list, choose **CiscoSensorProvisioning**.

f)   From the **Policy Profile** drop-down list, choose **CiscoSensorProvisioning**.

g)   Click ✓.

h)   Click **Save & Apply to Device** to save the Policy Tag.

Note   Changing the Policy Tag on an AP may cause clients associated with the AP to disconnect and reconnect.

Provision a Wireless or Sensor Device

This procedure explains how to claim a device from the Plug and Play Devices list. Alternatively, you can claim a device from the device details window by clicking **Claim**.

Before you begin

- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the Network Plug and Play Troubleshooting Guide for Cisco DNA Center.

- Define the site within the network hierarchy. See Design Network Hierarchy, on page 30.

- Define the CLI and SNMP credentials for the devices.

Note   You can claim wireless devices using CLI, SNMPv2c, or SNMPv3 credentials.
If you use SNMPv2c, provide both Read Only and Read Write credentials.

- Optionally, ensure that the software images for any Cisco Catalyst 9800-CL devices to be provisioned are uploaded and marked as golden in the Image Repository, if you want to deploy images.

Note The image deployment process used by Plug and Play during Day-0 provisioning is not the same as that used when updating a device image later. During Plug and Play provisioning, there are no device prechecks, auto flash cleanup, or postchecks done, as it is expected that devices are in the factory default state.

- For provisioning a sensor device, ensure that the sensor is reachable through the Cisco DNA Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Cisco DNA Center; however, to claim the device, it must be reachable from the interface enp9s0 IP address. In the DHCP server, configure the NTP server (DHCP option 42) and the vendor-specific DHCP option 43 with ACSII value "5A1D;B2;K4;I172.16.x.x;J80;", where 172.16.x.x is the virtual IP address of Cisco DNA Center associated with the enp9s0 interface.

Step 1 Click the menu icon (☰) and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can use the **Filter** or **Find** option to find specific devices.

Step 3 Check the check box next to one or more wireless devices that you want to claim.

Step 4 From the menu bar above the device table, choose **Actions** > **Claim**.

The **Claim Devices** window opens, showing the first step, **Assign Site**. If, instead, you see a window that shows mandatory tasks such as defining a site and defining device credentials, you must click **Add Site** to define a site, and **Add device credentials** to define device credentials. These are prerequisites for the claim process and, after these tasks are completed, you can return to claiming a device by clicking **Refresh** in this window.

Step 5 (Optional) Change the device name, if needed, in the first column.

Step 6 (Optional) Change the device type, if needed, in the second column. You can choose AP 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 Cisco Wireless Controller or sensor devices.

Step 7 From the **Select a Site** drop-down list, choose a site and floor to assign to each device. AP devices must be assigned to a floor with a wireless controller.

To apply the same site as the first device to all other devices, check the **Apply Site to All** check box. To assign the site from any device to some other devices, click **Assign this Site to Other Devices**, choose the devices, and click **Assign**. Wireless devices can be assigned only to floors within a building, not to the building itself.

Step 8 Click **Next**.
The **Assign Configuration** window appears.

Step 9 (Optional) You can change which columns are displayed in the table by clicking the three dots at the right end of the table headings and choosing the desired columns. Click **Apply** to save the changes.

Step 10 In the **Configuration** column, click **Assign** for the device that you want to configure and follow these steps:

a) View the device configuration summary and click **Cancel** if no changes are needed.

b) (Optional) In the **Device Name** field, change the device name, if needed.

   c) For an AP device, in the **Radio Frequency Profile** drop-down list, choose a radio frequency profile to apply to the device. This may be set if you designated one profile as a default.

   d) For a wireless controller, enter values in the following fields: **Wireless management IP**, **Subnet mask**, **Gateway**, **IP interface name**, and optionally, **VLAN ID**.

   e) For a Mobility Express device, enter values in the following fields: **Wireless management IP**, **Subnet mask**, and **Gateway**.

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

| **Note** | For Cisco Aironet 1800s Active Sensor earlier than Release 1.3.1.2, make sure that you do not choose the sensor device profile `CiscoProvisioningSSID`. Instead, choose your own SSID for backhaul purposes. |

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

   h) You can apply a configuration that you assigned to one device to other devices of the same type by clicking **Apply … to Other Devices** in the **Actions** column.

Step 11 (Optional) For a wireless sensor device, to assign a software image, do the following:

   a. In the **Image** column, click **Assign**.

   b. From the **Image** drop-down list, choose a golden software image.

   c. Click **Save**.

Step 12 If any devices are a Cisco Catalyst 9800-CL Wireless Controller, click **Assign** next to **Image** in the **Configuration** column and follow these steps:

   a) (Optional) In the **Image** drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.

   b) Click **Save**.

Step 13 If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration, until you have done this for all devices.

Step 14 Click **Next**.
The **Summary** window appears, where you can view details about the devices and configuration.

Step 15 Check the **Day-0 Config** column for each device to see if the configuration preview was successful.

If the preview shows an error, you can click the **Actions** link in the error message above the table to see what actions you need to take. You can click an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Assign Configuration** step and change the configuration, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. After you have resolved the problem, you can go back to this tab, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless controller that is managing a device has been added to the inventory and assigned to the site where the wireless device is assigned.

Step 16 Click **Claim**.

Step 17 In the confirmation dialog box, click **Yes** to claim the devices and start the provisioning process.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, see the "Complete the Provisioning Process" in the *Cisco DNA Center User Guide*

Monitor and Troubleshoot Network Health with Sensors

Monitor and Troubleshoot Network Health with All Wireless Sensors

Use this procedure to get a global view of the network health from the data received from all wireless sensors.

Before you begin

Make sure you have added and scheduled sensor-driven tests. See Create and Run Sensor-Driven Tests Using Templates, on page 251.

Step 1 Click the menu icon (☰) and choose **Assurance** > **Dashboards** > **Wireless Sensors**.

Figure 31: Wireless Sensors Dashboard
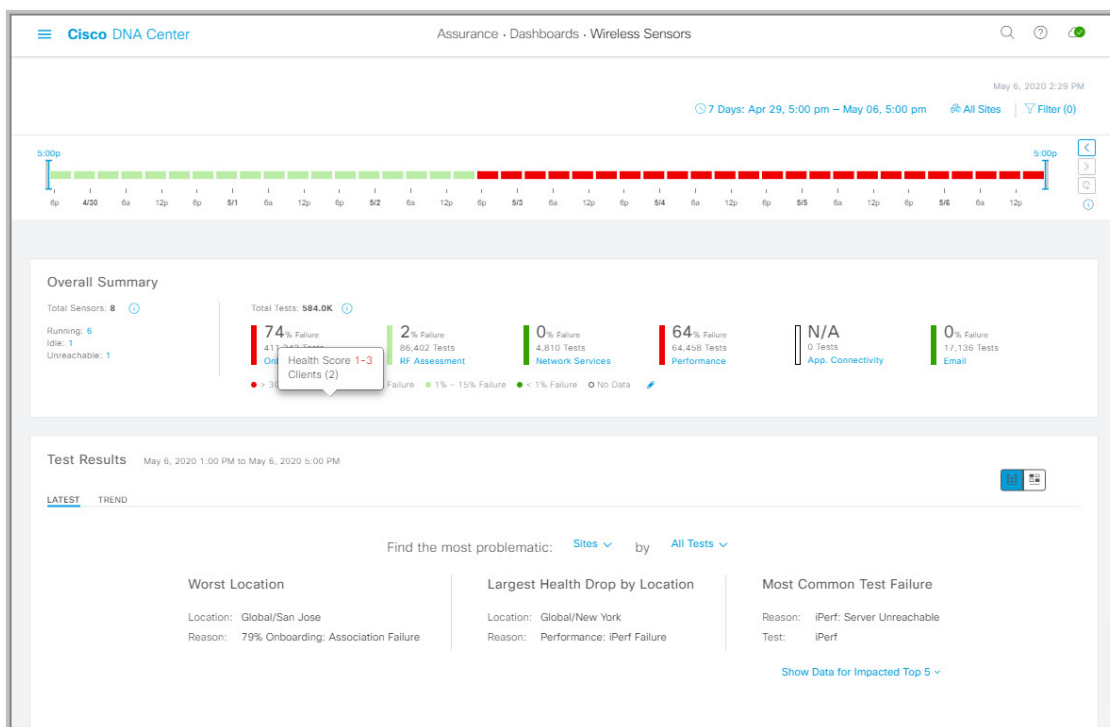
Step 2 Use the **Wireless Sensors** dashboard top-menu bar for the following functionality:

Timeline Area	
Item	**Description**
🕐 **Time Range** setting	Enables you to display data within a specified time range on the dashboard. Do the following: **a.** From the drop-down menu, choose the length of the range: **3 Hours**, **24 Hours**, or **7 Days**. **b.** Specify the **Start Date** and time; and the **End Date** and time. **c.** Click **Apply**.
🏛 **Hierarchy Location** setting	Enables you to choose the data displayed on the dashboard from the selected locations in your network. Check the check boxes for the sites, buildings, or floors in your network to display its sensor data on the dashboard. **Note** You can't exclude all locations from displaying data on the dashboard. Unchecking all locations results in data from all locations to be displayed on the dashboard.
Filter icon	Enables you to choose the data displayed on the dashboard based on SSIDs and radio frequency bands. To add filters: **a.** Click **Filter**. **b.** From the drop-down menu, click the **SSID** tab and check the check boxes for the desired SSIDs. **c.** From the drop-down menu, click the **Band** tab and select the radio button for **2.4 GHz** or **5 GHz**. **d.** Click **Apply**. To remove all selected filters: **a.** Click the **Filter** icon. **b.** Click **Clear Filters**.

Step 3   Use the **Timeline** to view the percentage of overall test failures for a specific time within a time range.

The time range is determined by what is configured in the 🕐 setting above the timeline.

The blocks in the timeline represents a specific time window within the time range. The period of time for each block is determined by time range set for the timeline:

- For a **3 Hours** time range, each block represents 15 minutes.

- For a **24 Hours** time range, each block represents 30 minutes.

- For a **7 Days** time range, each block represents 4 hours.

The blocks are color-coded to indicate the severity of percentage of test failures.

Hover your cursor over a block to view a breakdown of percentage of test result failures for each test category.

Step 4   Use the **Overall Summary** dashlet for the following functionality:

Overall Summary Dashlet	
Item	**Description**
Total Sensors area	Provides an overall view of all the sensors in your network and their status. The following are the status types of the sensor: • **Idle**: The sensor is onboarded and does not have any scheduled tests. • **Running**: The sensor is onboarded and is included in a test suite or test template. • **Unreachable**: No heartbeat received from the sensor. Click the hyperlinked number next to the status type to open a slide-in pane that displays the sensors with that status. In the slide-in pane, you can click the sensor name under the **Name** column to get a 360° view of that sensor. See Monitor and Troubleshoot Network Health with a Wireless Sensor, on page 244.
Total Tests	Displays the total number of tests performed by all sensors and a breakdown of the test results based on the following test categories: **Onboarding** **RF Assessment** **Network Services** **Performance** **App. Connectivity** **Email** You can click a test category to open a slide-in pane with additional details about its test results. In the slide-in pane, click the test type tabs on the left to populate the slide-in pane with data from the test type. The slide-in pane displays the following: • A chart that displays the test results, future trends, and list of APs used in the tests. **Note** For the **RF Assessment** test category, the chart displays the KPIs data rate and SNR, instead of test results. • Data type categories: **Top Failure Reasons** (if applicable), **Top APs**, **Top Locations**, **Top Bands**, and **Top SSIDs** (if applicable). • A table with detailed data of the sensors that ran the tests. You can click the data segments from the data type categories to filter the data that appears in the table.

Overall Summary Dashlet

Item	Description
✏️ **Edit Threshold**	Enables you to customize the thresholds of the color-coded ranges that indicate the severity of percentage of test result failures. ● > 30% Failure ● 15% – 30% Failure ● 1% – 15% Failure ● < 1% Failure To customize the thresholds: a. Click the edit (✏️) icon. b. In the **Edit Threshold** menu, enter the percentage values in the fields for each color-coded range. c. Click **Apply**.

Step 5 Use the **Test Results** dashlet to view the locations in your network with the most sensor test result failures:

Test Results Dashlet

Item	Description
Latest tab and **Trend** tab	These tabs determine the scope of the data that is displayed in the dashlet: • **Latest**: Displays the data from the selected time window in the timeline on the top of the window. • **Trend**: Displays data from the last 24 hours.
▦ ▥ **Heatmap View** and **Card View** toggle	This toggle button allows you to change the view of the dashlet to the **Heatmap View** and the **Card View**. The **Heatmap View** is displayed by default.

Test Results Dashlet	
Item	**Description**
⊞ **Heatmap View**	Displays the top 5 rankings of the following statistical categories at the top of the dashlet: • **Worst Location, Buildings, Floors,** or **Sensors**: Sites, buildings, floors, or sensors with the highest test result failure percentage. • **Largest Health Drop by Location, Buildings, Floors,** or **Sensors**: Sites, buildings, floors, or sensors with the largest sudden drop. • **Most Common Test Failure**: Test types that had the highest test result failures. Only the top spot for each statistical category is displayed. Click **Show Data for Impact Top 5** to see the complete rankings. Below the rankings is a heatmap representation of the sensor test result failures. In the heatmap, the blocks are color-coded to indicate the severity of percentage of test result failures. • Use the drop-down lists in the **Find the most problematic** area to sort the data that is displayed in the rankings and heatmap. In the first drop-down list you can sort the data by locations or sensors. In the second drop-list you can sort the data by test types. • Use the search field to filter the heatmap for specific locations or sensors. • Hover your cursor over a block to view the exact percentage value for test result failures. • Click a color-coded block to open a slide-in pane with further details about the test results at that intersect.
⊞ **Card View**	Displays the data in a card format for high-level monitoring and comparison. Use the drop-down lists in the **Find the most problematic** area to sort the data.

Monitor and Troubleshoot Network Health with a Wireless Sensor

Use this procedure to get a 360° view of a specific wireless sensor. You can view a sensor's test results, performance trends, and neighboring APs. You can also view and download a sensor's event logs.

Step 1 Click the menu icon (≡) and choose **Assurance** > **Dashboards** > **Wireless Sensors**.

The **Sensor Dashboard** appears.

Step 2 From the **Sensors Dashboard**, do one of the following:

• In the **Overall Summary** dashlet, click the hyperlinked number from the **Running**, **Idle**, or **Unreachable** areas.

Then in the **Sensor Status** slide-in pane, click the hyperlinked name of the sensor.

- In the **Overall Summary** dashlet, click a hyperlinked test category.

  In the slide-in pane, click the hyperlinked name of the sensor from the table.

- In the **Test Results** dashlet, click a color-coded box from the heatmap.

  In the slide-in pane, click the hyperlinked name of the sensor from the table.

A 360° view of the sensor appears.

Step 3 Click the 🕐 **Time Range** setting at the top-right corner to specify the time range of data that is displayed on the window:

a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.

b) Specify the Start date and time; and the End date and time.

c) Click **Apply**.

Step 4 Use the header above the timeline to view the basic information of the sensor such as the sensor's serial number, current state, uptime, backhaul type, IP address, and so on. You can also view and download the sensor's event logs.

To view and download the event logs:

a) Click **View Logs** at the end of the header.
The **Event Logs** slide-in pane appears which displays the event logs.

b) In the **Event Logs** slide-in pane, click **Request Support Bundle** to generate the support bundle file which contains the event logs.

> **Attention**   It takes about three to five minutes for a support bundle request to be ready for download.

c) Click **Download Support Bundle** to open the download prompt for the support bundle.

Step 5 Use the timeline to view the percentage of overall test failures for a specific time within a specified time range. The timeline has the following functionality:

- Set the time range with the 🕐 **Time Range** setting above the time line.

- View the percentage of overall test failures for a specific time window indicated by the blocks in the timeline. You can hover your cursor over a block to view a breakdown of percentage of test result failures for each test category.

Step 6 Use the collapsible categories to view information about test results, performance trends, and neighboring APs:

Test Results Category

Displays a heatmap representation of the sensor test result failures for each tested AP. In the heatmap, the blocks are color-coded to indicate the severity of percentage of test result failures.
 	
 • Use the **Test Type** drop-down list to sort the data by test type.
 	
 • Use the search field to filter the heatmap for specific APs.
 	
 • Hover your cursor over a block to view the exact percentage value for test result failures.
 	
 • Click the **Latest** and **Trend** tabs to change the scope of data displayed in the category:
 	
   • **Latest**: Displays the data from the selected time window in the timeline on the top of the window.
 	
   • **Trend**: Displays data from the last 24 hours.

Sensor Performance Trend Category
Displays a line graph or chart of the sensor performance data based on test types. For time-based test types, a comparative view is used to display the performance of the current sensor, top performing sensor, and worst performing sensor. • Use the **Test Type** drop-down list to display data for a specific test type. • For time-based test types, click + **Add Custom Location** to add the sensor performance data for a specific location using the menu. You can select the sensor performance for sites, buildings, or floors.

Neighboring APs Category
Displays the sensor's neighboring APs along with its RSSI in a list view and a map view. To filter the APs based on frequency bands, use the radio buttons in the **Band** area. Note   The sensor scans for neighboring APs every 30 minutes.

Manage Sensors and Backhaul Settings

Manage Sensors in Your Network

Use this procedure to view the onboarded sensors in your network. You can enable SSH, enable the status LED, and change the name for these sensors.

Before you begin

Make sure the sensors are assigned to a site.

Step 1   Click the menu icon (☰) and choose **Assurance** > **Manage** > **Sensors**.

The **Sensor List** window appears.

Figure 32: Sensor List Window

Step 2   Use the left pane to specify the network hierarchy you want to view.

Step 3   Click the categories above the table to view the sensors that fit its criteria. The categories are:

- **Total**: All the sensors in the selected network hierarchy.

- **Running**: Displays the sensors that are currently running tests.

- **Idle**: Displays the sensors that have no assigned tests.

- **Unreachable**: Displays the sensors that are onboarded but are not responding to Cisco DNA Center.

Step 4   You can customize the data that is displayed in the table:

a) Click .
b) From the menu, check the check boxes of the data you want displayed in the table.
c) Click **Apply**.

Step 5   To configure the SSH settings for a sensor, do the following:

a) Check the check box of the sensor.
b) Hover your cursor over the **Actions** drop-down list and choose **Edit SSH**.

The **Edit SSH** slide-in pane appears.

c) In the **Edit SSH** slide-in pane, click the **SSH** toggle to enable SSH.
d) In the **Username** and **Password** fields, enter the desired SSH credentials.
e) Click **Save**.

Step 6   To change the status LED of a sensor, do the following:

a) Check the check box of the sensor.
b) Hover your cursor over the **Actions** drop-down list and choose **Edit LED**.

The **Edit LED** slide-in pane appears.

    c)   In the **Edit LED** slide-in pane, click the **LED** toggle to enable or disable the status LED.

Step 7   Click **Save**.

Step 8   To change the name of a sensor, do the following:

    a)   Check the check box of the sensor.

    b)   From the **Actions** drop-down list, choose **Edit Sensor Name(s)**.

        The **Edit Sensor Name(s)** slide-in pane appears.

    c)   In the **Edit Sensor Name(s)** slide-in pane, enter the name in the **Name** field.

    d)   Click **Save**.

Step 9   To enroll the sensors using SCEP Profiles, do the following:

    a)   Check the check box of the sensor.

    b)   From the **Actions** drop-down list, choose **Enroll using SCEP**.

        The **Enroll using SCEP** slide-in pane appears.

    c)   Choose the SCEP profile from the **Select SCEP Profile** drop-down list.

        See Manage SCEP Profiles for more information.

    d)   Select the **Username** and **Password** and provide the required details. If you choose the **Custom** username option, then select **No Password**.

    e)   Click **Save**.

    f)   To check status, see the **SCEP Profile** column in the **Sensor List** window. A green check mark (✔) indicates success and a red **X** icon indicates failure. Hover your cursor over the ✔ or **X** icon to get more information.

Manage Backhaul Settings

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

For information about a persistent wireless backhaul connection, see Persistent Wireless Backhaul Connections on Sensor Devices, on page 250.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Manage** > **Sensors**.

The **Sensor List** window appears.

Step 2   Hover your cursor over the **Settings** tab and choose **Backhaul Settings**.

Step 3   You can add and manage backhaul SSIDs by doing the following:

    a)   Click + **Add Backhaul**.

        The **Create Sensor Backhaul SSID Assignment** window appears with two areas: **Wired Backhaul** and **Wireless Backhaul**.

    b)   In the **Settings Name** field, enter a name for the backhaul SSID.

    c)   In the **Wired Backhaul** area, configure the following:

        • **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:

- **802.1x EAP**: Standard used for passing Extensible Authentication Protocol (EAP) over wired LAN.

- **Open**: No security or authentication is used.

- **EAP Method**: If you choose **802.1x EAP**, you must choose one of the following EAP methods for user authentication from the drop-down list:

  - **EAP-FAST**: Enter the username and password in the fields provided.

  - **PEAP-MSCHAPv2**: Enter the username and password in the fields provided.

  - **EAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click + **Add New Certificate Bundle**, and enter the username and certificate bundle password.

  - **PEAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

    If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click + **Add New Certificate Bundle**, and enter the username and certificate bundle password.

d) In the **Wireless Network Name (SSID)** area, select the wireless network (SSID) and configure the following.

  - **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:

    - **WPA2 Enterprise**: Provides a higher level of security using Extensible Authentication Protocol (EAP) (802.1x) to authenticate and authorize network users with a remote RADIUS server.

    - **WPA2-Personal**: Provides a good security using a passphrase or a preshared key (PSK). This allows anyone with the passkey to access the wireless network.

      If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.

    - **PSK Format**: The available preshared key formats are:

      - **ASCII**: Supports ASCII PSK passphrase.

      - **HEX**: Supports 64-character HEX key PSK password.

    - **Open**: No security or authentication is used.

e) Click **Save**.

Step 4 You can edit the existing backhaul configurations by doing the following:
  a) Check the check box of the backhaul configuration.
  b) Hover your cursor over the **Actions** drop-down list and choose **Edit**.

Step 5 You can delete a backhaul configuration by doing the following:
  a) Check the check box of the backhaul configuration.
  b) Hover your cursor over the **Actions** drop-down list and choose **Delete**.

Persistent Wireless Backhaul Connections on Sensor Devices

Cisco DNA Center supports a persistent wireless backhaul connection on sensor devices, which means that the wireless connection is "always on" regardless of wireless testing activities.

- With a dedicated backhaul connection, the wireless sensor uses the following two MAC addresses for backhaul and wireless purposes:

    - Base Radio + 0x10 (Backhaul SSID)

    - Base Radio + 0x11 (Test SSID)

    The wired sensor uses the Base Radio + 0x10 (Test SSID) MAC address for testing purposes.

- The sensor uses *dual* concurrent radio operations, one for the backhaul connection and the other for wireless tests.

- Backhaul connection interruptions occur during scanning and switching interfaces to test different bands.

- The frequency of backhaul connection disruptions is dependent on the test configuration.

- The backhaul connection is not persistent if both backhaul and test SSIDs are in one band.

Manage SCEP Profiles

Use this procedure to view, create, and manage Simple Certificate Enrollment Protocol (SCEP) profiles, which are used to enroll wireless sensors.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Manage** > **Sensors**.

Step 2   Click **Setting** > **SCEP Profiles**.

Step 3   To add and manage a SCEP Profile, do the following:

a)   Click **Add SCEP Profiles**.

The **Create SCEP Profile** window appears.

b)   In the **Create SCEP Profile** window, provide the following details:

- **SCEP Profile Name**: Enter a name for the SCEP profile.

- **URL Base**: Enter a valid server.

    Note   For **ISE**, enter the following:

    http://*ISE_IP_or_FQDN_Name***:9090/auth/caservice/pkiclient.exe**

    For **Microsoft CA**, enter the following:

    http://*Microsoft_SCEP_IP_or_FQDN_Name***/CertSrv/mscep/mscep.dll**

- **Common Name**: Enter a valid name.

- **State**

- **Country Code**

           • **Locality**

           • **Organization**

           • **Organization Unit**

           • **Email**

           • **Server certificate fingerprint**

    c)   Click **Save**.

Step 4   To edit an existing SCEP Profile, do the following:
    a)   Check the check box next to the SCEP Profile.
    b)   From the **Actions** drop-down list, choose **Edit**.

Step 5   To delete a SCEP Profile, do the following:
    a)   Check the check box next to the SCEP Profile.
    b)   From the **Actions** drop-down list, choose **Delete**.

Sensor-Driven Tests

Create and Run Sensor-Driven Tests Using Templates

Use this procedure to create and run sensor-driven tests using templates. The workflow for sensor-driven tests using templates consists of two parts:

1. **Create the test template**: Configure the test configurations such as the SSIDs to test, test types to use, and the AP coverage.

2. **Deploy the test template**: After a test template is created, select the locations for testing and set the test schedule. After a test template is deployed, it is ready to be run.

Using templates is beneficial if you have a use case that requires a sensor-driven test to be run at different locations and with different schedules. With templates, you can create duplicates that can be deployed for each instance of the test location and schedule. This saves you time from having to recreate the same test for each instance.

Before you begin

• If you are using the Cisco Aironet 1800s Active Sensor to run sensor-driven tests, make sure that the sensor is provisioned using PnP, so that it displays under **Inventory**. See Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 235.

• Note that if a sensor test template restarts, all sensors on that template begin running their tests at the same time, which causes the result graphs to show a cyclical pattern.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Manage** > **Sensors**.

Step 2   Click the **Test Templates** tab.

The **Test Templates** window appears.

Figure 33: Test Templates Window
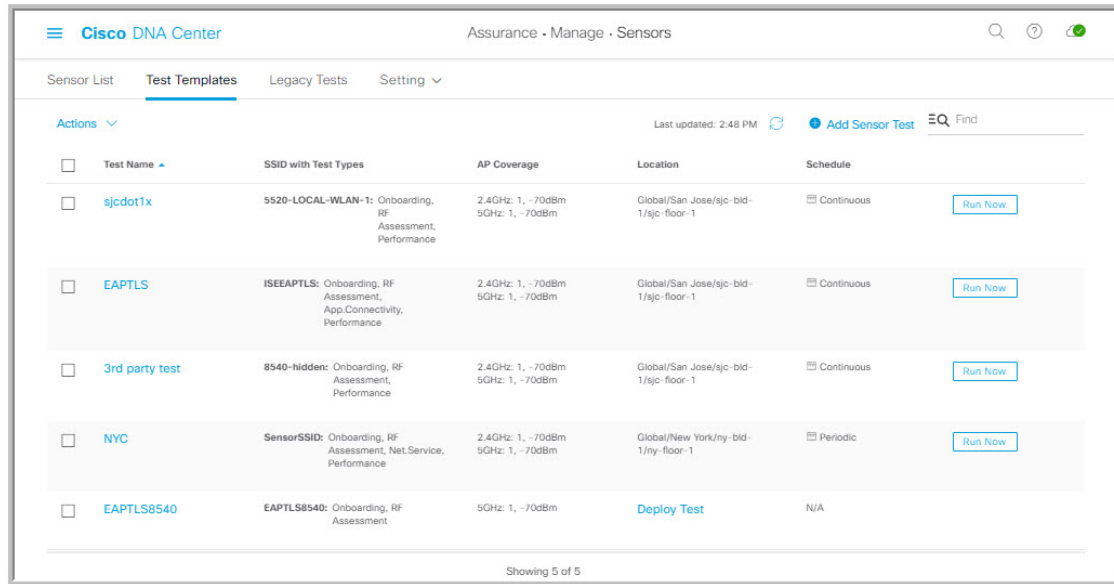
Step 3   To create a new sensor test template, click + **Add Sensor Test**.
The wizard for creating a sensor test template appears.

Step 4   For the **Set up Sensor Test** step, configure the following settings:

- **Test Template Name**: Enter the name for the test.

     Note   Use only letters, numbers, underscores, hyphens, and periods.

- **SSID Selection**: Check the check boxes for the SSIDs you want to include for the sensor test.

Step 5   Click **Next**.

Step 6   For the **Enter SSID Credentials** step, enter the credentials for the selected SSIDs:

- For SSIDs with **Open** security, select the following:

     - **Open**: For SSIDs with WebAuth passthrough, enter the email address.

     - **ISE Guest Portal**: Choose the labels for the ISE guest portal.

     - **Clearpass Guest Portal**: Choose the labels for the Clearpass guest portal and then click **Apply**.

- For SSIDs with **WPA2 Personal** security, enter the password.

- For SSIDs with **WPA2 Enterprise** security, enter the EAP method, username, and password.

Step 7   Check the **Add Proxy Settings** check box, to enable proxy settings.

Step 8   Configure the following proxy settings:

- **Proxy Server**

- **Proxy Port**

- **Proxy UserName**

- **Proxy Password**

Step 9   Click **Next**.

Step 10   For the **Define Sensor Test Category Details** step, check the check boxes for the test types to include:

    a) For the **Onboarding** test category, the test types are **Association**, **Authentication**, and **DHCP**.

       Note   All of these test types are selected by default and cannot be excluded from the test template.

    b) For the **RF Assessment** test category, the test types are **Data Rate** and **SNR**.

       Note   All of these test types are selected by default and cannot be excluded from the test template.

    c) For the **Network Services Tests** test category, select from the following test types:

- **DNS**: Resolves IP address for the domain name.

- **RADIUS**: The sensor acts as a Dot1x supplicant and authenticates through wireless.

    d) For the **Performance Tests** test category, select from the following test types:

- **Internet (NDT)**: Performs a speed test using Network Diagnostic Tool (NDT).

  If you have a Network Diagnostics Test (NDT) server, enter the IP address of the NTD server in the field provided. If the NDT server is reachable through a proxy server, enter the IP address of the proxy server in the field provided.

- **iPerf3**: iPerf3 test is a tool used to measure network performance. This feature allows you to perform a speed test in the network with a certain amount of traffic to determine whether the test is able to pass through the traffic.

  To run the iPerf3 test, check the iPerf3 check box, and then enter the IP address of the iPerf3 server, UDP bandwidth, and port details in the fields provided.

  iPerf3 Limitations

  - You can add up to five iPerf3 servers.

  - You can configure each iPerf3 server to use a maximum of five ports per template. Sensors randomly select the port in which it wants to run the iPerf3 test.

  - Two sensors cannot connect to the same port concurrently on a given iPerf3 server.

  - The "iPerf: Server Busy" error message indicates that there are not enough iPerf3 instances to support the number of the sensors that are running the iPerf3 test.

    To resolve this issue, do *one* of the following:

    - Add iPerf3 server instances. To do so, expand the ports that support iPerf3 testing on the existing servers.

    - Reduce the number of sensors that are configured to run the iPerf3 test. To do so, create a separate template for iPerf3 testing.

- **IP SLA**: Runs UDP jitter, UDP echo, packet loss, and latency measurements from sensor to APs.

To run the IPSLA test, choose a **Service Level** option for each SSID from the drop-down list. Options are **Platinum** (voice), **Gold** (video), **Silver** (best effort), and **Bronze** (background).

e) For the **Application Tests** test category, select from the following test types:

- **Host Reachability**: Tests for reachability using (ICMP) echo request.

- **Web**: Tests for access to the provided URL and verification of the response data.

- **FTP**: Tests for file upload and download operations

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

f) For the **Email** test category, select from the following test types:

- **POP3**: Post Office Protocol3, connects to POP3 server TCP port (110).

- **IMAP**: Internet Message Access Protocol, connects to IMAP server TCP port (143).

- **Outlook Web Access**: Logs into the Outlook Web Server (OWS) and verifies access.

Step 11 Click **Next**.

Step 12 For the **Select AP Coverage** step, do the following:

a) Select the frequency bands to test with the **2.4GHz** and **5GHz** check boxes.

b) In the **Number of Target APs** drop-list for the selected bands, choose the number of APs you want the sensor to test against.

  Note You can choose a maximum of five APs.

c) In the **RSSI Range** slider for the selected bands, drag the slider to the desired RSSI.

Step 13 Click **Next**.

Step 14 For the **Summary** step, review the template settings.

Click **Edit** for the **SSIDs** or **AP Coverage** steps to reconfigure its settings.

Step 15 Click **Create Test** to create the template.
The test template is created and a dialog box appears for confirmation.

Step 16 For the **Done! Sensor Test Created** confirmation window, click **Deploy Test to Locations** to configure the locations and schedule for the test template.

  Important If you return to the **Test Templates** window without deploying the test, click **Deploy Test** from the **Location** column to continue to the next step of deploying the test.

Step 17 For the **Select Location** step, use the hierarchy menu on the left to check the check boxes for the sites, buildings, or locations that you want to deploy the test template.

Step 18 Click **Next**.

Step 19 For the **Set Schedule** step, select from one of the options for the test frequency:

- **Periodic**: Runs the test at specified intervals. Use the **Interval** drop-down list to select the time between intervals.

- **Scheduled**: Runs the tests on designated days of the weeks for a specified duration:

  a. Click the **S**, **M**, **T**, **W**, **T**, **F**, and **S** buttons to select the days of the week to run the test.

      b.   For selected days, specify the start and end time for the test period from the **From** time pickers.

      c.   In the **Select Value** drop-down menu, select the desired test duration for the test period.

      d.   To add another test period for the selected day, click + **Add** to add a new row for configuring the test period.

      e.   To remove a test period, click the trash can icon.

     • **Continuous**: The test runs indefinitely and repeats after completion.

Step 20   Click **Next**.

Step 21   For the **Summary** step, review the deployment details.

             Click **Edit** for the **Location** or **Schedule** steps to reconfigure its settings.

Step 22   Click **Deploy Test**.
             The test template appears in the **Test Template** window.

Step 23   Click **Run Now** for the test template to run the test.

Manage Sensor-Driven Test Templates

Use this procedure to manage sensor-driven test templates. You can duplicate and delete sensor-driven test templates, as well as undeploy running sensor-driven test templates.

Before you begin

Create sensor-driven test templates. See .

Step 1   Click the menu icon (≡) and choose **Assurance** > **Manage** > **Sensors**.

Step 2   Click the **Test Templates** tab.

             The **Test Templates** window appears.

Figure 34: Test Templates Window

Step 3   To duplicate a test template, do the following:

a)   Check the check box for the test template you want to duplicate.

b)   Choose **Actions** > **Duplicate**.

c)   In the **Input the new Test Name** dialog box, enter the name for the duplicate of test template.

d)   Click **Save**.
The duplicate of the test template appears in the **Test Templates** window. To deploy the test, click **Deploy Test** from the **Location** step.

Step 4   To delete a test template, do the following:

a)   Check the check box for the test template you want to duplicate.

b)   Choose **Actions** > **Delete**.

c)   In the **Warning** dialog box, click **Yes**.
The test template is deleted.

Step 5   To undeploy a test template, do the following:

a)   Check the check box for the running test template you want to undeploy.

b)   Choose **Actions** > **Undeploy**.

c)   In the **Warning** dialog box, click **Yes**.
The test template stops running.

Warning   If you undeploy a test template, its location and schedule settings are removed.

Monitor Wi-Fi 6E and 6 Readiness

- About Wi-Fi 6E and 6 Readiness and Its Benefits, on page 257
- Assure the Readiness of Your Wi-Fi 6E and 6 Network, on page 258

About Wi-Fi 6E and 6 Readiness and Its Benefits

You use the Wi-Fi 6E and 6 Readiness feature to determine the following:

- The percentage of clients that are Wi-Fi 6E and 6 capable.

- The percentage of AP infrastructure that is Wi-Fi 6E and 6 ready.

- Based on the preceding information, recommendations are provided about the actions that you can take to experience the full benefits of the Wi-Fi 6E and 6 network.

To provide these recommendations, Cisco DNA Center does the following:

- Assesses the Wi-Fi capabilities of wireless clients.

- Collects AP inventory to determine which of the APs are managed by Cisco DNA Center, and then assesses the Wi-Fi capabilities of those APs.

- Determines the types of wireless controllers that are in the network and whether the software that is installed on the wireless controllers is Wi-Fi 6E and 6 ready.

- Determines the wireless LAN configuration and whether are not Wi-Fi 6E and 6 features are enabled.

Note Under certain conditions, Wi-Fi 6E wireless client latency or airtime efficiency data might be less optimal than Wi-Fi 6 or legacy Wi-Fi, regardless of the capability of the AP platforms. For example, Wi-Fi 6E might be less optimal when:

- Significantly more clients are connected to Wi-Fi 6E APs than to non-Wi-Fi 6E APs.

- There is more interference from poor RF design in the Wi-Fi 6E environment than in the non-Wi-Fi 6E environment.

- Clients connected to Wi-Fi 6E are positioned to have poor signal strength (RSSI).

The preceding scenarios also apply to Wi-Fi 6 versus legacy Wi-Fi.

Assure the Readiness of Your Wi-Fi 6E and 6 Network

Use this procedure to assure the readiness of your Wi-Fi 6E and Wi-Fi 6 network.

Before you begin
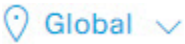
Configure Assurance. See .

Step 1   Click the menu icon (☰) and choose **Assurance** > **Wi-Fi 6**.

The **Wi-Fi 6** dashboard appears.

Step 2   Use the top-menu bar for the following functionality:

Item	Description
◉ Global ⌄ **Location** pane	Click to display the following icons: • ☰ ⊞ : Click this toggle button to display the **Hierarchical Site View** table. It provides the percentage of wireless clients and wireless network devices in a site. To view information for a particular building, choose **Building View** from the drop-down list. • ☰ ⊞ : Click this toggle button to display the health of all the network sites on a geographic location-oriented network health map. By default, the network sites that are represented are color coded according to the severity of the problem.
🕐 **Time Range** setting	Enables you to display data within a specified time range on the dashboard. Do the following: a. From the drop-down menu, choose the length of the range: **3 Hours**, **24 Hours**, or **7 Days**. b. Specify the **Start Date** and time; and the **End Date** and time. c. Click **Apply**.

Item	Description
Filter icon	Contains the **SSID** and **Band** options. Choose the SSIDs and band frequency from the drop-down list by selecting the check boxes adjacent to them, and then click **Apply**. Depending on your selection, the information in the dashboard is refreshed.
Actions drop-down list	Enables you to export the dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**. Enables you to customize the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 281 and Create a Custom Dashboard, on page 277.

Step 3   Use the **Insights** area to get an insight about your network. It provides the following information:

- The percentage of clients that are Wi-Fi 6E and Wi-Fi 6 capable.

- The percentage of AP infrastructure that is Wi-Fi 6E and Wi-Fi 6 ready.

- Based on the above information, recommendations on what actions you can take to enjoy the full benefits of the Wi-Fi 6E and Wi-Fi 6 network are provided.

Step 4   Use the **Client Distribution By Capability** dashlet to compare the distribution capability of clients between Wi-Fi 6E and Wi-Fi 6 and to determine if the Wi-Fi 6E or Wi-Fi 6 capable clients joined to the network.

Based on the AP to which the clients are associated, the clients might function at their Wi-Fi 6 capability or at a lesser capability. For example, a Wi-Fi 6 client associated to a 11ac AP will function as an 11ac client.

Client Distribution By Capability Dashlet

You can view all the clients that are associated with the wireless network based on the following status: **Wi-Fi 6E** and **Wi-Fi 6E**.

This dashlet includes the following tabs:

- **Latest**: Displayed by default.

    - The **outer** segment of the circle shows the number of Wi-Fi 6E capable clients joined (are associated with) the Wi-Fi 6E, Wi-Fi 6 and non Wi-Fi 6 network.

    - The **outer** segment of the circle shows the number of Wi-Fi 6 capable clients joined (are associated with) the Wi-Fi 6 and non Wi-Fi 6 network.

    - The **inner** circle shows the actual wireless capability of the clients joined to the network. The wireless clients are capable of functioning in one of the following protocols:

        - **Wi-Fi 6E**: 802.11ax 6 GHz capable client(s).

        - **Wi-Fi 6**: 802.11ax capable client(s).

        - **11ac**: 802.11ac Wave1 and Wave2 capable client(s).

        - **11n**: 802.11n capable client(s).

        - **11abg**: 802.11a, b, or g capable client(s).

        - **Unclassified**: The client is listed under **Unclassified** due to the following reasons:

            - The capabilities of the client device is not reported due to network delay.

            - The AP or wireless controller to which the client device is connected, does not have the correct software version installed.

    Hover your cursor over a color in the chart to display the number of clients associated with that color.

- **Trend**: Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the number of the clients that are associated to Wi-Fi 6E, Wi-Fi 6, or non-Wi-Fi 6 protocols over a time range based on the chosen status (Wi-Fi 6E or Wi-Fi 6).

    Hover your cursor over the chart to display the total number of clients and their protocol for that specific day and time.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Step 5   Use the **Network Readiness** dashlet to determine how many APs are Wi-Fi 6E and Wi-Fi 6 capable and are configured (enabled) to operate in Wi-Fi 6E or Wi-Fi 6 mode.

Network Readiness Dashlet

You can view all the clients that are associated with the wireless network based on a status of **Wi-Fi 6E** or **Wi-Fi 6E**.

- The **outer** segment of the circle shows the number of Wi-Fi 6E APs with the 6-GHz band enabled or Wi-Fi 6 APs with 11ax disabled.

    Note   Wi-Fi 6E APs can operate in Wi-Fi 6E mode only if the wireless controllers and APs are running a software version that supports 6 GHz band.

- The **inner** circle shows the number of APs that are Wi-Fi 6E, Wi-Fi 6, and non-Wi-Fi 6 (11ac/n/a/b/g) capable.

    Note   Wi-Fi 6 APs can operate in Wi-Fi 6 mode under the following conditions:

    - The 11ax configuration on the Wi-Fi 6 APs is enabled.

    - The wireless controllers and APs are running a software version that supports Wi-Fi 6 (11ax).

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, click a color segment in the chart; **AP** and **WLC** tabs display. Click the **AP** and **WLC** tabs to display Wi-Fi 6 readiness at radio and band levels, respectively.

Step 6   Use the **AP Distribution by Protocol** dashlet to determine the number of APs that have the hardware capability to support the Wi-Fi standards: Wi-Fi 6E, Wi-Fi 6, and 11 ac/n/a/b/g.

AP Distribution by Protocol Dashlet

This dashlet includes the following tabs:

- **Latest**: Displayed by default. It shows the number of APs that support Wi-Fi 6E, Wi-Fi 6 (11ax) protocol and the number of APs that support non-Wi-Fi 6 (11ac/n/a/b/g) protocols:

    - **Wi-Fi 6E**: 802.11ax 6 GHz band capable AP(s).

    - **Wi-Fi 6**: 802.11ax capable AP(s).

    - **11ac**: 802.11ac capable AP(s).

    - **11n**: 802.11n capable AP(s).

    - **11abg**: 802.11a/b/g capable AP(s).

    Hover your cursor over a color in the chart to display the number of APs associated with that color.

- **Trend**: Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the number of the APs that are associated to the different protocols (Wi-Fi 6E, Wi-Fi 6 or non-Wi-Fi 6) over a time range.

    Hover your cursor over the chart to display the total number of APs and their protocol for that specific day and time.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Step 7   Use the **Wireless Airtime Efficiency** dashlet to compare the Average Airtime Efficiency between Wi-Fi 6E, Wi-Fi 6 traffic and non-Wi-Fi 6 traffic for each of the access categories (voice, video, best effort, and background).

Wireless Airtime Efficiency Dashlet

You can view the wireless airtime efficiency for the following access categories: **Voice**, **Video**, **Best Effort**, **Background**, and **All**. Default is **Voice**.

This dashlet includes the following tabs:

- **Latest**: Displayed by default. The bar graph allows you to compare the average airtime efficiency (in units of Bytes per mill-seconds) between Wi-Fi 6E, Wi-Fi 6 traffic and non-Wi-Fi 6 traffic for the chosen access category.

  The spectrum is efficiently used if the APs radios can send more traffic (successful Bytes transmitted to the client) in less airtime (microseconds) than other networks under similar RF conditions. An efficient network might allow more video or voice calls.

  Traffic is classified as the following:

  - Wi-Fi 6E traffic is the traffic sent from Wi-Fi 6E APs to clients that are associated as Wi-Fi 6E.

  - Wi-Fi 6 traffic is the traffic sent from Wi-Fi 6 APs to clients that are associated as Wi-Fi 6.

  - Non-Wi-Fi 6 Traffic is the aggregate of the following:

    - Wi-Fi 6 APs to non-Wi-Fi 6 capable clients.

    - Non-Wi-Fi 6 APs to non-Wi-Fi 6 capable clients.

    - Non-Wi-Fi 6 APs to Wi-Fi 6 capable clients.

  Note   A Wi-Fi 6 capable client operates in non-Wi-Fi 6 mode when it connects to a non-Wi-Fi 6 AP.

- **Trend**: Click the **Trend** tab to display a trend chart. This color-coded trend chart shows the number of clients that are associated to the different wireless network modes (Wi-Fi 6E, Wi-Fi 6 or non-Wi-Fi 6) over a time range.

  Hover your cursor over the chart to display the total number of clients and their protocol for that specific day and time.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Step 8   Use the **Wireless Latency by Client Count** dashlet to compare the Average Wireless Latency between Wi-Fi 6E, Wi-Fi 6 traffic and non-Wi-Fi 6 traffic for each of the access categories (voice, video, best effort, and background).

Typically, AP radios with a higher client count have more latency compared to radios with a lower client count under similar RF conditions.

Wireless Latency by Client Count Dashlet

You can view the wireless latency for the following traffic: **Voice**, **Video**, **Best Effort**, and **Background**. Default is **Voice**.

This dashlet includes the following tabs:

- **Latest**: Displayed by default. It provides the Average Wireless Latency comparison between the Wi-Fi 6E, Wi-Fi 6 and non-Wi-Fi 6 AP radios serving similar number of "active" clients. Wireless latency is measured by the time (microseconds) it takes for a packet to be successfully transmitted from an AP to the client.

  Note   Active clients count include those clients that are actively sending traffic for a given Access category and not just Associated clients.

- **Trend**: Click the **Trend** tab to display a trend chart. The trend chart displays the average wireless latency across all access categories.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart to refresh the data in the table that is displayed below the chart.

Monitor Power over Ethernet

About PoE

The Cisco DNA Center Power over Ethernet (PoE) enables you to monitor the PoE-capable devices in your network. It also monitors the power summary of switches supplying PoE, which provides information such as a switch's power budget, used power, remaining power, and power usage and allows viewing the allocated power and power load of switches.

Setup Workflow for PoE Telemetry

To enable PoE telemetry and analytics in Assurance, you need to perform the required setup tasks. A basic workflow for setup involves the following tasks:

1. Configure NETCONF on the network devices used for PoE telemetry.

   For details, see Configure NETCONF on Your Devices for PoE Telemetry, on page 267.

2. Update the telemetry settings in Cisco DNA Center.

   For details, see Update Telemetry Settings for PoE Telemetry, on page 269.

Setup Workflows

The setup workflow for PoE telemetry varies depending on the software version and configuration of Cisco DNA Center and network devices that support PoE telemetry.

If you are doing a fresh installation of Cisco DNA Center, refer to the following table:

Fresh Installation of Cisco DNA Center	
Network Device Configuration	**Required Setup Tasks**
• IOS XE version is 16.12.3s. • NETCONF is disabled.	1. Enable NETCONF on the device. 2. Update the telemetry settings in Cisco DNA Center.
• IOS XE version is upgraded from 16.12.2 to 16.12.3s with SWIM. • NETCONF is disabled.	1. Enable NETCONF on the device. 2. Update the telemetry settings in Cisco DNA Center.
• IOS XE version is upgraded from 16.12.2 to 16.12.3s with SWIM. • NETCONF is enabled.	1. Update the telemetry settings in Cisco DNA Center.

If you are upgrading to Cisco DNA Center from an earlier release, refer to the following table:

Upgrade from an Earlier Release	
Network Device Configuration	**Required Setup Tasks**
• IOS XE version is upgraded from 16.12.2 to 16.12.3s with SWIM. • NETCONF disabled.	1. Enable NETCONF on the device. 2. Update the telemetry settings in Cisco DNA Center.
• IOS XE version is upgraded from 16.12.2 to 16.12.3s with SWIM. • NETCONF is enabled.	1. Update the telemetry settings in Cisco DNA Center.
• IOS XE version is 16.12.3s. • NETCONF is disabled.	1. Enable NETCONF on the device. 2. Update the telemetry settings in Cisco DNA Center.
• IOS XE version is 16.12.3s. • NETCONF is enabled.	1. Update the telemetry settings in Cisco DNA Center.

If there are changes to the network device that supports PoE telemetry in **Inventory**, refer to the following table:

Network Device Changes in Inventory	
Change to Network Device	**Required Setup Tasks**
Remove a device from Cisco DNA Center **Inventory**, and then add it back.	1. Enable NETCONF on the device. 2. Update the telemetry settings in Cisco DNA Center.

Network Device Changes in Inventory	
Change to Network Device	**Required Setup Tasks**
Add a new device to Cisco DNA Center **Inventory**.	1. Enable NETCONF on the device. 2. Update the telemetry settings in Cisco DNA Center.
Use a replacement device in Cisco DNA Center **Inventory**.	1. Enable NETCONF on the device. 2. Update the telemetry settings in Cisco DNA Center.

Configure NETCONF on Your Devices for PoE Telemetry

Use this procedure to configure NETCONF on your network devices for PoE telemetry. To use PoE telemetry, the supporting network devices must have NETCONF enabled.

Before you begin

Depending on the configuration of your Cisco DNA Center and network devices, you might not need to do this procedure to set up PoE telemetry. For details, see Setup Workflow for PoE Telemetry, on page 265.

Step 1 Configure the NETCONF port for an existing network device:

a) Click the menu icon (☰) and choose **Provision** > **Inventory**.

The **Inventory** window appears.

b) Check the check box of the network device to be configured to enable NETCONF.

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

d) From the **Type** drop-down list, choose **Network Device**.

e) Expand the **NETCONF** area.

f) In the **Port** field, enter `830`.

Note   NETCONF provides a mechanism to install, manipulate, and delete configurations of network devices.

g) Click **Update**.

The device's NETCONF port is configured.

Step 2 Create a **Template Editor** project for NETCONF configuration:

a) Click the menu icon (☰) and choose **Tools** > **Template Editor**.

The **Template Editor** window appears.

b) From the left pane, click the ⊕ icon and choose **Create Project**.

c) In the **Name** field, enter a name for the project.

d) Click **Add**.

The project is added to the left pane of **Template Editor**.

Step 3   Create a template in the project for NETCONF configuration:

a)   From the left pane, hover your cursor over the ✱ icon to the right of the project and choose **Add Template**.
b)   In the **Name** field, enter a name for the template.
c)   In the **Device Type(s)** field, click **Edit**.
d)   Check the check box of **Switches and Hubs** to apply the template to add switches and hubs.

> **Note**   If you want to specify the exact models of the switches, expand **Switches and Hubs** and check the check box of the specific switch model.

e)   Click **Back to Add New Template**.
f)   Click the **Software Type** drop-down list and choose **IOS-XE**.
g)   Click **Add**.

The template is created and appears.

Step 4   Add content in the template:

a)   In the template, enter the following:

```
netconf-yang
```

b)   From the **Actions** drop-down list, choose **Save**.

The content is saved to the template.

c)   From the **Actions** drop-down list, choose **Commit**.
d)   In the **Commit Note** text box, enter a note.
e)   Click **Commit**.

Step 5   Create a network profile and associate the template:

a)   Click the menu icon (≡) and choose **Design** > **Network Profile**.

The **Network Profiles** window appears.

b)   Click +**Add Profile** and choose **Switching**.
c)   In the **Profile Name** field, enter a name for the network profile.
d)   Click the **Day-N Templates** tab.
e)   Click +**Add**.
f)   From the **Device Type** drop-down list, choose **Switches and Hubs**.
g)   From the **Template** drop-down list, choose the template that was created in Step 3.
h)   Click **Save**.

The network profile is created and appears in the **Network Profiles** window.

Step 6   Assign the site(s) for the network profile:

a)   From the **Sites** column, click **Assign Site**.
b)   Check the check box of the site that the network device is assigned to.
c)   Click **Save**.

Step 7   Provision the NETCONF configuration to the network device:

a)   Click the menu icon (≡) and choose **Provision** > **Inventory**.

The **Inventory** window appears.

b) Check the check box of the network device for PoE telemetry.

c) From the **Actions** drop-down list, choose **Provision** > **Provision Device**.

d) In the **Assign Site** step, click **Next**.

e) In the **Advanced Configuration** step, check the **Provision these templates even if they have been deploy before** check box.

f) Click **Next**.

g) In the **Summary** step, click **Deploy**.

h) Click **Apply**.

Provisioning starts and the NETCONF configuration is pushed to the network device.

Update Telemetry Settings for PoE Telemetry

Use this procedure to update the telemetry settings in Cisco DNA Center. This is a required step after setting the NETCONF port and pushing the NETCONF configuration to the network devices for PoE telemetry.

Before you begin

Ensure that the network devices being set up for PoE telemetry have an established NETCONF port and the correct NETCONF configuration. For details, see Configure NETCONF on Your Devices for PoE Telemetry, on page 267.

Step 1   Click the menu icon (☰) and choose **Provision** > **Inventory**.

The **Inventory** window appears.

Step 2   Check the check boxes of the network devices that have been set up for PoE telemetry.

Step 3   From the **Actions** drop-down list, choose **Telemetry** > **Update Telemetry Settings**.

Step 4   Check the **Force Configuration Push** check box.

> **Note**   This option pushes the configuration changes to the device.

Step 5   Click **Next**.

Step 6   Set the schedule for when the telemetry settings are updated by clicking a radio button:

- **Now**: Choose this option to update the telemetry settings immediately.

- **Later**: Choose this option to schedule the task for another time. Specific the time and date.

Step 7   Click **Apply**.

Monitor PoE-Capable Devices in Your Network

Use this procedure to get a global view of PoE-capable devices in your network.

Step 1   Click the menu icon (☰) and choose **Assurance** > **PoE**.

The **PoE** dashboard appears.

Figure 35: PoE Dashboard
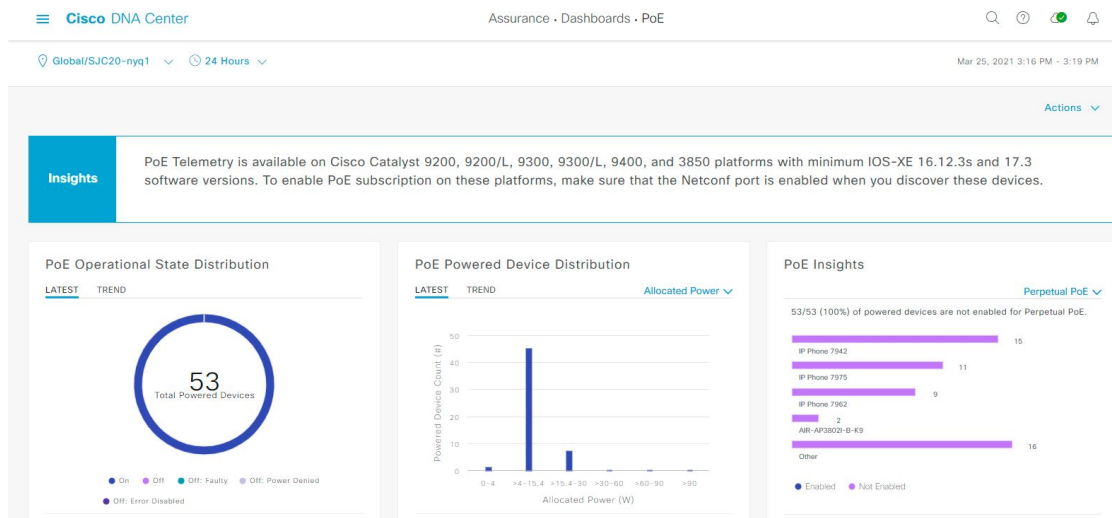
Step 2   Click the location option (⦿ Global ⌄) in the top-menu bar to display the location pane.

The location pane has the following functionality:

Location Option	
Item	**Description**
☰ 🗺 toggle button **List View**	Click this toggle button to display the sites and buildings from your network in a list format. Click the drop-down list for the following options: • **Hierarchical Site View**: Sorts the list at a site level. From the **Apply to Page Location** column, click **Apply** for a site or building to display data only for that location on to the **Network** dashboard. • **Building View**: Sorts the list at a building level. From the **Apply to Page Location** column, click **Apply** for a building to display data only for that building on to the **Network** dashboard.
☰ 🗺 toggle button **Map View**	Click this toggle button to display the health of all the network sites on a geographic location-oriented network health map. By default, the network sites that are represented are color-coded according to the severity of the problem.

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

Step 3   Click the time range setting (🕐) in the top-menu bar to specify the time range of data that appears on the dashboard.

     a)   From the drop-down menu, choose the time range: **3 Hours**, **24 Hours**, or **7 Days**.

     b)   Specify the **Start Date** and time; and the **End Date** and time.

     c)   Click **Apply**.

Step 4   Click the **Actions** drop-down list in the top-menu bar for the following functionality:

     • **Export Dashboard**: Enables you to export the PoE dashboard to PDF format. Click **Export Dashboard** to view the preview page and click **Save**.

     • **Edit Dashboard**: Enables you to customize the dashboard display. See and .

Step 5   Use the PoE dashlets for the following functionality:

PoE AP Power Mode Distribution Dashlet
Displays the distribution of fully powered and partially powered APs.
The **Latest** tab provides a 10-minute snapshot view.
The **Trend** tab provides the following:
• If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range.
• If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range.
Note   The data point displayed is the start time of the corresponding 10 minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available after the end of the corresponding window.
Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data in the table that is displayed below the chart.

PoE Operation State Distribution Dashlet

Displays the number of PoE-capable devices in your network. The color-coded chart provides the count of devices based on whether they are being supplied with PoE or not. For devices that are not being supplied with PoE, this is further characterized by the reason why.

The **Latest** tab provides a 10-minute snapshot view.

The **Trend** tab provides the following:

- If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range.

- If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range.

Note	The data point displayed is the start time of the corresponding 10 minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available after the end of the corresponding window.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data in the table that is displayed below the chart.

PoE Powered Device Distribution

View the distribution of the devices currently using PoE for a certain criteria. Use the drop-drop list to specify the following criteria:

- **Allocated Power**

- **Powered Device Class**

The **Latest** tab provides a 10-minute snapshot view.

The **Trend** tab provides the following:

- If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range.

- If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range.

Note	The data point displayed is the start time of the corresponding 10 minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available after the end of the corresponding window.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data in the table that is displayed below the chart.

Power Load Distribution

View the distribution of switches based on its power load for PoE.

The **Latest** tab provides a 10-minute snapshot view.

The **Trend** tab provides the following:

- If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range.

- If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range.

Note	The data point displayed is the start time of the corresponding 10 minute or 1-hour window. For example, all the data that is received between 10:00 to 10:10 is displayed with the time value of 10:00. Similarly, for hourly window, the data that is received between 10:00 to 11:00 is displayed with a time stamp of 10:00. This data point is available after the end of the corresponding window.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data in the table that is displayed below the chart.

PoE Insights

View the percentage of the devices currently using PoE which are configured to support the following PoE technologies or meet IEEE Compliance:

- **Perpetual PoE**

- **Fast PoE**

- **IEEE Compliant**

- **UPOE+**

Use the drop-down list to choose the characteristic.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a color segment in the chart or its corresponding legend to refresh the data that is displayed in the table below the chart.

Power Usage

View the total power consumption and allocated power by devices currently using PoE. Use the drop-down list to select **Consumption** or **Allocation** view to display the respective data in the Latest and Trend tab.

The **Latest** tab provides the 10 minutes snapshot view. The pie-chart displays the Power Allocation details such as PoE Power Allocation, System Power Allocation, and Available Power, and Power Consumption details such as PoE Power Consumption and System Power Consumption measured in Watt.

The **Trend** tab provides the following:

- If you chose 24 hours in the time range settings, the trend chart provides 10-minute data points for the entire 24-hour range of power usage.

- If you chose greater than 24 hours in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click on a color segment in the chart or its corresponding legend to view the System Power information (System Power Consumption and System Power Allocation) and PoE Power information (PoE Power Consumption and PoE Power Allocation) of the devices over a time period in the table that is displayed below the chart.

You can select the data displayed as horizontal bars to filter the preceeding table that is displayed based on the power usage, device role and location.

PoE Port Availability

View the availability of ports based on their power load for PoE.

The **Latest** tab provides a 10-minute snapshot view.

The **Trend** tab provides the following:

- If you chose 24 hours or less in the time range settings, the trend chart provides 1-hour data points (aggregated from the 10-minute data) for the entire time range.

- If you chose 7 days in the time range settings, the trend chart provides 12-hour data points (aggregated from the 1-hour data) for the entire time range.

Click **View Details** to open a slide-in pane with additional details. From the slide-in pane, you can click a 1-hour data point in the chart to refresh the data in the table that is displayed below the chart.

Monitor the Rogue Management Dashboard

• Manage Security Threats on Networks, on page 275

Manage Security Threats on Networks

With the Cisco DNA Center Rogue Management application, you can monitor the threats on your network from unauthorized access points. You can quickly identify the highest priority threats and monitor those threats from the Assurance dashboard.

For details about the Cisco DNA Center Rogue Management application, see the Cisco DNA Center Rogue Management Application Quick Start Guide.

Manage Dashboards

About Dashboards

You can create custom dashboards for monitoring your network. Dashboards contain one or more dashlets, which include charts, tables, geographic maps, and other types of information.

Any custom dashboard that you create is visible only to your user account. Other users cannot see your custom dashboards.

Create a Custom Dashboard

Step 1 Click the menu icon (≡) and choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all the defined dashboards.

Step 2 Click + **Create a Dashboard**.

Step 3 In the **Create a Dashboard** dialog box, enter a title for the dashboard.

Step 4 Click **Save**.
A blank dashboard appears.

Step 5 You can do the following in your dashboard:

a) Click + **Add Dashlet** to add content to the dashboard.

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

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

c) Click **Add** to include the dashlet in your dashboard.

Step 6 (Optional) Drag and drop any dashlet to customize its location on your dashboard.

Step 7 You can remove a dashlet from your dashboard by doing the following:

a) Click the trash can icon located in the top-right corner of the dashlet.

b) In the dialog box, click **Delete**.

Step 8 Click **Save** to save the dashboard.

Create a Dashboard from a Template

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

Step 1 Click the menu icon (☰) and choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all defined dashboards and the templates (at the bottom).

Step 2 In the **Templates** area, click a dashboard template.

Step 3 In the **Create a Dashboard** dialog box, enter a title for the dashboard.

Step 4 Click **Save**.

Step 5 If you want to use an existing scope, select an existing scope and click **Select Scope**.

Skip to Step Step 15 if you selected an existing scope, or continue with the next step if you want to create a new scope.

Step 6 To create a new scope, click **Create New Scope**.
The first step, **Create New Scope**, is displayed.

Step 7 Enter a scope name and click **Next**. If you enter a space in the scope name, the space is converted to an underscore.
The second step, **Select Location(s)**, is displayed.

Step 8 Choose one or more locations to include in the scope by checking or unchecking the check boxes next to them.

Note You can use the search field to filter locations.

Step 9 Click **Next**.
The third step, **Select Filters**, is displayed.

Step 10 If you are using the **Client Health** template, you can use the following filters:

- **Client Type**: Choose wired or wireless to include these types of devices in the scope by checking or unchecking the boxes next to them.
- **SSIDs**: Choose SSIDs to include in the scope by checking or unchecking the boxes next to them. Type in the search field to filter SSIDs. This filter applies only to wireless devices.
- **Host Name**: Enter the hostnames to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **Device Type**: Enter the device OS types (for example, IOS or Android) to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **MAC Address**: Enter the MAC addresses to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **IP Address**: Enter the IP addresses to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.

Step 11   If you are using the **Network Health** template, you can use the following filters:

- **Network Device Type**: Choose one or more device types to include in the scope by checking or unchecking the check boxes next to them. Type in the search field to filter devices.
- **Network OS**: Choose network OS versions to include in the scope by checking or unchecking the check boxes next to them. Type in the search field to filter versions.
- **IP Address**: Enter the IP addresses to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.
- **Host Name**: Enter the hostnames to include in the scope. Use the percent sign (%) as a wildcard and press **Enter** after each entry.

Step 12   Click **Next**.
The fourth step, **Preview**, is displayed.

Step 13   Click the **Dynamic list** toggle to enable or disable a dynamic list of clients that is updated based on the selected filters.

Step 14   Click **Save** to save the scope.
A confirmation dialog is displayed.

Step 15   (Optional) Drag and drop any dashlet to customize its location on your dashboard.

Step 16   You can remove a dashlet from your dashboard from doing the following:

a)   Click the trash can icon located in the top-right corner of the dashlet.

b)   In the dialog box, click **Delete**.

Step 17   Click **Save** to save your dashboard.

> **Note**   If this is a new scope, it can take up to 15 minutes to display data in the dashboard.

View a Dashboard

Step 1   Click the menu icon (≡) and choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by entering its name in the **Find** field.

> **Note**   When you sort the dashboards by **Date Modified**, even if no modifications were made on the dashboards, the dashboards get sorted by the last time the dashboards were open.

Step 2   To see dashboards marked as favorites, click the **Favorite Dashboards** tab.

Step 3   Click the dashboard that you want to view.

Step 4   In the dashboard controls, click **Show** or **Hide** to show or hide the map, if applicable.

Step 5   (Optional) Filter dashboard data by time period, sites, or domains by choosing the appropriate values from the filters.

Edit or Delete a Dashboard

Step 1   Click the menu icon (☰) and choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by entering its name in the **Find** field.

Step 2   Click the dashboard that you want to edit or delete.

Step 3   Do one of the following:

- To make changes, choose **Edit Dashboard** from the **Actions** menu. You can add or delete dashlets and drag dashlets to different positions in the dashboard. Click **Save** when you are done.

- To delete the dashboard, choose **Delete Dashboard** from the **Actions** menu. Click **Delete** in the confirmation dialog.

Duplicate a Dashboard

Step 1   Click the menu icon (☰) and choose **Assurance** > **Dashboard Library**.
The **Dashboard Library** window appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by entering its name in the **Find** field.

Step 2   Click the duplicate icon for a dashboard (next to the star icon).

Step 3   In the **Duplicate Dashboard** dialog box, enter a title for the dashboard copy.

Step 4   Click **Save**.

Step 5   You can change this copied dashboard by adding, deleting, or rearranging dashlets.

Step 6   Click **Save** to save the dashboard.
A confirmation dialog is displayed.

Step 7   Click **OK**.

Mark a Dashboard as a Favorite

Step 1   Click the menu icon (☰) and choose **Assurance** > **Dashboard Library**.

The **Dashboard Library** window is displayed, 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:

- Click the menu icon (≡) and choose **Assurance** > **Health**.

  The **Overall Health** dashboard appears.

- Click the menu icon (≡) and choose **Assurance** > **Health** > **Network Health**.

  The **Network Health** dashboard appears.

- Click the menu icon (≡) and choose **Assurance** > **Health** > **Client Health**.

  The **Client Health** dashboard appears.

- Click the menu icon (≡) and choose **Assurance** > **Health** > **Application Health**.

  The **Application Health** dashboard appears.

Step 2   Click the **Actions** drop-down list 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**.

Observe Network Trends and Gain Insights

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.

- **AP Performance Advisories**: Detect APs that have a consistently poor client experience, and provide a root cause and suggested actions.

- **Comparative Analytics**, which includes:

  - **AI-Driven AP Comparisons in Network Heatmaps**: Compare all of the APs in your network for a given month in a heatmap to spot trends and gain insights.

  - **AI-Driven Peer Comparisons**: Determine how your network is performing in comparison to your peer networks for a selected Key Performance Indicator (KPI).

  - **AI-Driven Network Comparisons**: View, compare, and identify performance improvement opportunities for objects in your network (buildings, AP model families, wireless endpoints) across selected KPIs.

View Wireless Access Point Performance Advisories

Cisco AI Network Analytics uses machine learning algorithms to identify wireless APs with a potentially poor client experience. APs are continually analyzed over long periods and those suspected of providing a

suboptimal client experience are grouped by underlying root cause and suggested improvements. Insights are generated, which consist of a set of radio and network features that can be used to diagnose any underlying issue that can be rectified. Insights have the following main components:

- Discover underperforming APs via various client experience KPIs.

- Find appropriate features that can discriminate between APs with a poor or good client experience that is both significant and actionable by the customer as a basis of root-cause analysis (RCA).

APs are analyzed on separate frequency bands of 2.4 GHz, 5 GHz and 6GHz. Poor client experience is detected using statistical analysis of different KPIs, such as SNR, RSSI, link speed, packet retries, and packet failures.

Use this procedure to view AP performance advisories that highlight the most active APs with poor client experience based on analysis of four weeks of data.

Step 1 Click the menu icon (☰) and choose **Assurance** > **Trends and Insights** > **AP Performance Advisories**.

Step 2 Click the **AP Performance Advisories** tab, which provides a summary of the number of different types of insights with common root-cause analysis category and affected radios.

Figure 36: Access Points Performance Advisories
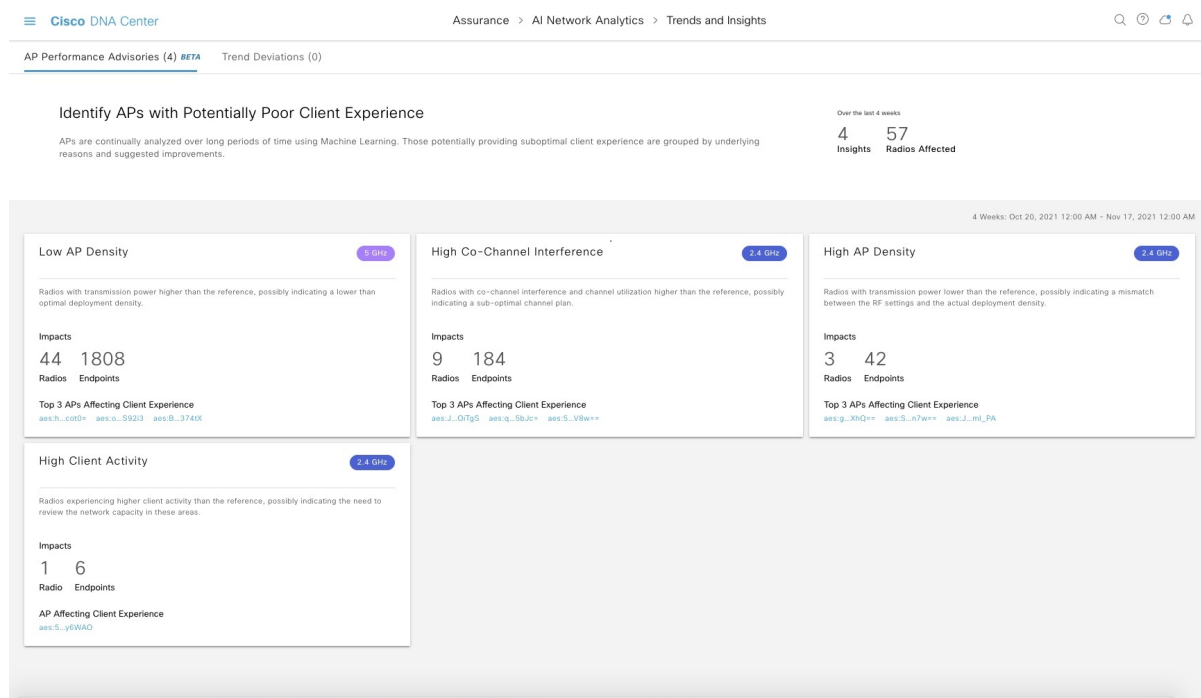
The following are the possible occurrences of insights with common root-cause analysis:

- External RF load

- External RF load with high client activity

- Frequent channel change

- High RF load

- High channel utilization

- High client activity

- High client load

- High AP deployment density

- Low AP deployment density

- Low AP deployment density and external interference

- Low AP deployment density and high load

Step 3 Use the **AP Performance Advisories** dashboard for the following insights summary:

Network Overview Window	
Item	**Description**
Insights Summary	Displays the name of the insight (Low AP Density, High Client Activity, and so on) and problem definition for a particular frequency band.
Impacts	Displays the number of impacted **Radios** and **Endpoints** for each insight.
Top 3 APs Affecting Client Experience	Displays the top three impacted APs for a particular frequency band. These are hyperlinks to the detailed page, shown in Step 5.

Step 4 Click each insight dashlet for the following information, where a common root-cause analysis is provided with the suggested actions for all radios in this category.

Figure 37: Insights Summary Dashboard for Impacted Radios

Insight Dashboard	
Item	**Description**
Summary	Displays the total number of radios analyzed over four weeks, the number of buildings, and the top three impacted APs.
KPI charts	Displays multiple KPI charts depending on the RCA category, which indicates the distribution of the KPI across all the radios. The charts can be used to compare and contrast the performance of radios with this common RCA, against reference radios that have no detected client experience problem.
Radios Impacting Client Experience table	Contains Insights Details, Impact (low, medium, or severe), AP Model, Location, # of Clients Affected, and KPIs Impacting Client Experience.
Export	Click **Export** to export the table data to a CSV file.

Step 5 In the **Radios Impacting Client Experience** table, click the hyperlinked AP to view the following detailed insights summary for a specific AP.

Figure 38: Insight Summary for Access Point

Insight Dashboard	
Item	**Description**
Top bar	Provides information such as AP model, location, impacted clients, and additional AP details hyperlinked to the Assurance Device window. Also provides suggested actions that are specific to the identified root cause and anomalous KPIs to improve the client experience.

Insight Dashboard	
Item	**Description**
Client Experience KPIs	• The histogram shows the distribution of the different KPIs that impact client experience, facilitating a comparison between the individual AP and the reference AP across the customer's network (APs without observed client experience problems). • By default, only KPIs with detected anomalies are shown. You can add more numbers of KPIs that display the distribution of KPIs, including the SNR, RSSI, link speed, packet retries, and packet failures. • You can hover your cursor over the histogram bin value to view additional details of the observed occurrence rate in the selected AP, versus the reference set of APs.
Radio Specific Root-Cause Context	• The histogram shows the distribution of the different root-cause analysis KPIs that impact radios. By default, only KPIs with detected anomalies are shown. • You can add more numbers of KPIs that display the distribution of RCA KPIs, including the SNR, RSSI, link speed, packet retries, and packet failures. • You can hover your cursor over the histogram bin value to view additional details of the observed occurrence rate in the selected radio, versus the reference set of radios.

View Network Trends and Obtain Insights

Trends are long-term evolutions of behavior in your network observed over a time period. These trends provide insights about the performance of your network (represented in beeswarm charts). 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   Click the menu icon (≡) and choose **Assurance** > **Trends and Insights** > **Trend Deviations**.

The **Network Insights** window appears with filters: **Capacity**, **Coverage**, and **Throughput**. Click the appropriate filter to refresh the data in the table. The Capacity filter is selected by default.

Note   The filters are dynamic. If there are no insights available for a filter, that filter is not displayed.

Insights Table	
Item	**Description**
Occurrence	Time duration when this trend was observed, such as May 27 - June 03 2019.
Insight Type	List the insight types that are named as **Daily** and **Weekly**
Insight	List of all the AI-driven insights that were observed during a specific time period.
Category	Category under which the insight was observed. Insight KPIs are grouped under the following categories: • **Capacity**: Radio Client Count, Channel Change Count • **Coverage**: Interference, Avg Client SNR, Avg Client RSSI, Traffic, Utilization • **Throughput**: Total Radio Throughput
Frequency band	Band frequency used on the AP on which the insight was observed. Values are **2.4 GHz**, **5 GHz**, and **6GHz** or all the band frequencies.
KPI	Key Performance Indicator (KPI) for that specific insight.
⋮ icon	Allows you to customize the columns that you want displayed in the Insights table. Click the ⋮ icon, uncheck the check box for the column that you do not want displayed, and then click **Apply**.

Step 2   From the **Insight** column, click an insight to open a slide-in pane, which provides the following information:

Insight Details Slide-In Pane	
Item	**Description**
Cisco AI	Provides information about how the insights are computed. Click Learn More to get an overview of Artificial Intelligence.
Insight Summary	A brief summary about the trend that is observed in the beeswarm chart. The summary provides information such as the name of the site or AP, client count, radio band frequency, and time period during which the deviation was observed.
Weekly Client Load	Client load per week.

Insight Details Slide-In Pane	
Item	**Description**

Troubleshoot	Provides links that allow you to troubleshoot and fix the trend before it becomes a critical issue:
	
	• **Network Heatmap** opens the heatmap and provides information about the AP or building that is highlighted in the beeswarm chart. The heatmap that displays is for the specific month in which the trend was observed.
	
	    • **Intra-Site**: The heatmap launches with the specific AP highlighted and prioritized in the list.
	
	    • **Inter-Site**: The heatmap launches with the filtered view of the APs in the building (site).
	
	• *AP_Name* opens the **Device 360** page for that AP.

Issue Count	Issue count gradient.

Insight Details Slide-In Pane	
Item	**Description**
Chart	

Insight Details Slide-In Pane	
Item	**Description**
	The beeswarm chart displays the performance of the client devices in your network in a 4-day (daily insights) and week (weekly insights) time interval as shown in the following figure. If there is a systematic deviation of network behavior over a time period, that trend is displayed by arrows in the chart.
	Figure 39: Beeswarm Chart
	Daily Insights
	Weekly Insights

Insight Details Slide-In Pane	
Item	**Description**

Note	• Each circle in the beeswarm chart represents the following:
	
	     • **Intra-Site**: The circle represents a radio.
	
	     • **Inter-Site**: The polygon represents a building.
	
	 • The size of the circle represents the number of clients in the AP. A small circle has a lower client count; a large circle has a higher client count.

Step 3   Hover your cursor over a circle in the chart for information, such as the name and MAC address of the AP, the band frequency, the AP group, the location of the AP, issue count, client count, and the KPI value.

         Note   For Global sites, when you hover your cursor over a circle in the chart, you see information about the building in which the trend was observed and the client count.

Compare Access Points and Switches in Network Heatmaps

Use the Network Heatmap to visually compare all of the APs in your network for a given month to spot trends and gain insights. You can 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 Click the menu icon (≡) and choose **Assurance** > **Network Heatmap**.

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

Figure 40: Network Heatmap Window

Network Heatmap Window	
Item	**Description**
Show	Display the heatmap information based on the device type that you choose from the drop-down list. You can choose **Access Points** or **Swithces**. Default is Acces Points.
KPI drop-down list	Displays information in the heatmap for the KPI you choose from the drop-down list. For Access Points, the default KPI is **Client Count**. For Switches, the default KPI is **Temperature: All Sensors**.
Swtich Family drop-down list	Displays information in the heatmap based on the switch family you choose from the drop-down list. This drop-down list is displayed only when you choose the device type Switches from the **Show** drop-down.
Time Range	Click the **Time Range** drop-down to choose **Month** or **Day** radio button to display information in the heatmap for a specific month or a day.

Network Heatmap Window	
Item	**Description**
Location	Displays information in the heatmap for your entire global network or for a specific site and building that you choose from the drop-down list. Default is **Global**.
Band	Displays information in the heatmap for the band frequency you choose. Options are: **2.4 GHz**, **5 GHz**, and **6 GHz**. By default all the three band frequencies are selected.
View By	Allows you to view the information in the heatmap based on the option you choose. Based on the KPI you choose, the options displayed in the **View By** list vary. Some KPIs allow you to sort by **Avg**, **Min**, or **Max**, some by **Avg** or **Max**, while other KPIs do not provide any options.
Summary area	Displays a summary of the insight gained from the heatmap analysis. Provides the following type of information: • The day of the month that was the busiest. • Number of APs or Swithes that had no clients per radio. • Number of APs or Swicthes that had more than 50 clients per radio.
Feedback icon	Click the 👍 👎 icon to provide your comments on whether the information on this page was helpful, and then click **Submit**.
KPI gradient	Depending on the KPI you choose from the KPI drop-down list, this area provides information about the performance of the KPI in a color gradient. The darker color block indicates a significant KPI score. For example, a lower RSSI score is more significant than a higher RSSI score. A higher client count score is more significant than a lower client count score.
Search AP drop-down list	Allows you to search for and select an AP. Do the following: a. Click the **Search AP** drop-down list and enter the AP name in the search filter. The AP that you searched for is highlighted in the drop-down list. b. Click the highlighted AP to select it. The individual radios of the AP are displayed separately on the heatmap.
Network Daily Avg, **Min**, or **Max** graph	Depending on the **View By** option you chose, the appropriate graph is displayed • If you chose **Avg**, the graph shows the daily average value and highlights the highest daily average. • If you chose **Min** or **Max**, the graph shows minimum or maximum daily value, and highlights accordingly. Hover your cursor over the bar on the graph to view the KPI value for each day.

Network Heatmap Window	
Item	**Description**
Showing Radios heatmap	Provides a compressed view of the heatmap.
	By default, this area displays the heatmap for the first 100 radios. To view the heatmap data for additional radios, scroll down to the bottom of the compressed heatmap, and then choose the appropriate option from the drop-down list.
AP Heatmap area	Contains the following:
	• **Radios in Your Network**: Displays the name of the AP and the band frequency that was used by the client. Click on the icon next to the AP to open the **Device 360** page for that AP.
	Depending on the band frequency you choose from the **Band** options, this area lists the APs in the corresponding chosen band.
	• **AP Heatmap**: Allows you to determine how the APs are behaving historically: per hour, per day, per week, and during the entire month. The intensity of the color in the blocks indicates its significance. The darker color block is more significant than the lighter color block. Each row in the heatmap represents one AP.
	Hover your cursor over a color block in the **Heatmap** to get information about the AP, such as its name and MAC address, band frequency, location, and daily average KPI score.
	• **AP Daily Average** or **AP Daily Max**: Depending on what you choose in the **Sort By** option, this area displays the average KPI score or the max KPI score for each AP during the month. The AP with the highest score is listed on top.
	Hover your cursor over the **AP Daily Average** or the **AP Daily Max** area to determine the average or max KPI value for an AP during the month.
⬆ Export	Click **Export** to export the heatmap data to a CSV file.
	AP's and Filters applied to the heatmaps are applied to the exported data. Export is enabled only on the daily view and not on the hourly view.

Step 2 To view the heatmap data for additional radios, scroll down to the bottom of the window and choose the appropriate option from the drop-down list.

Compare KPI Values with Peers in Your Network
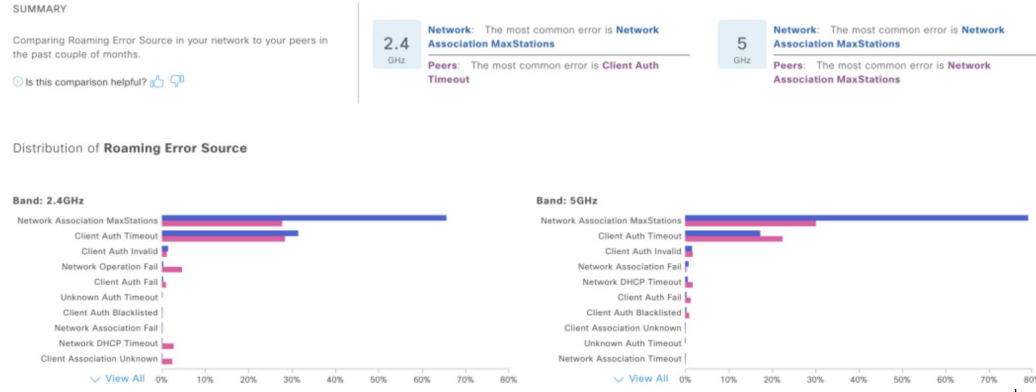
Use this procedure to determine how your network is performing compared to your peer networks for a selected Key Performance Indicators (KPI).

Note   The peer networks that are used for comparison are of similar network size.

For computations, peer comparison uses a couple of months data from the date of onboarding.

Step 1 Click the menu icon (≡) and choose **Assurance** > **Peer Comparison**.

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

Peer Comparison Window	
Item	**Description**
KPI drop-down list	Choose a KPI from the drop-down list. Options are: **Radio Throughput**, **Cloud Apps Throughput**, **Radio Resets**, **Packet Failure Rate**, **Interference**, **Onboarding Error Source**, **Roaming Error Source** and **RSSI**. Default is **Radio Throughput**.
Show	Choose the day for which you want to compare the KPI values between your network and your peer networks. Default is **All**.
Summary	AI Network Analytics analyzes the bar graphs and provides a brief summary about the findings: • **2.4 GHz**: Summary of the Network and Peer values for the 2.4-GHz band frequency. • **5 GHz**: Summary of the Network and Peer values for the 5-GHz band frequency.
Highlight Peers toggle button	Allows you to toggle between your network and the peer network graphs.
Peer Comparison Bar Graph	By default, highlights the KPI values for your network in the **Band 2.4 GHz** and **Band 5 GHz** graphs, as shown in the following figure. To highlight the KPI values for the peer networks, click the **Highlight Peers** button. **Figure 41: Peer Comparison Bar Graph** The colors in the graph represent the following: • **Blue**: Your network. • **Pink**: Peer networks.

Step 2 To display the KPI values for your network and your peer networks for a specific day, choose the appropriate day from the **Show** area.

Compare Buildings, AP Model Families, and Wireless Endpoint Types

Use this procedure to view, compare, and identify performance improvement opportunities for objects in your network (buildings, AP model families, wireless endpoints) across selected Key Performance Indicators (KPIs).

Step 1   Click the menu icon (☰) and choose **Assurance** > **Network Comparison**.

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

Figure 42: Network Comparison Window

Network Comparison Window	
Item	**Description**
Compare drop-down list	Choose the object in your network that you want to compare. Options are: **Buildings** (sites), **AP Model Families**, or **Wireless Endpoints** (Android device, Android phone, IOS tablet, IOS phone, Linux workstation, and so on).

Network Comparison Window	
Item	**Description**
By KPI drop-down list	Choose a KPI that you want to use to compare the objects in your network.
	For **Buildings**, the options are:
	• **Radio Throughput**
	• **Channel Utilization**
	• **Average Client RSSI**
	• **Average Client SNR**
	• **Average Onboarding Time**
	• **Average Authorization Time**
	• **Average DHCP Time**
	• **Cloud Throughput**
	• **Media Throughput**
	• **Social Throughput**
	• **Interference**
	For **AP Model Families**, the options are:
	• **Radio Throughput**
	• **Interference**
	• **Media Apps Throughput**
	• **Average Client RSSI**
	• **Channel Utilization**
	• **Average Client SNR**
	• **Cloud Throughput**
	• **Social Throughput**
	For **Wireless Endpoints**, the options are:
	• **Average AAA Time**
	• **Average Onboarding Time**
	• **Average DHCP Time**

Network Comparison Window	
Item	**Description**
Buildings **AP Model Families** or **Wireless Endpoints** drop-down list	Choose the first network object (building, AP model family, or wireless endpoint), for which you want to compare the KPI values. The first network object is represented in blue color. Choose the second network object whose KPI values you want to compare with the first network object. The second network object is represented in pink/purple color.
Band	Choose the band frequency. Options are: **Band 2.4 GHz** and **Band 5 GHz**.
Summary/Timeline	Displays the average KPI performance for each day of the week, for each network object.
Client Count gradient or **Device Count** gradient	For certain KPIs, such as **Radio Throughput** and **Average Client RSSI**, this area provides the client count per radio for each of the sites. For certain KPIs, such as **Onboarding Time**, this area provides the number of devices for each of the sites. The intensity of the color in the blocks indicates the client count or device count. The darker color block has more clients or devices than the lighter color block.
AP Clusters or **Device Type Clusters**	This area displays two sets of clusters, one for each network object. From this area you can visually compare the performance of the two network objects. It provides the following information: • KPI performance, as a percentage. • How the objects in your network are clustered in each site. • Objects in your network that are experiencing low, medium, and high KPI values. For certain KPIs, such as **Onboarding Time** and **Authorization Time**, this area displays the following: • The types of devices that the client's onboarded in each site. For example, Windows workstation, OS X workstation, Linux workstation, Android phone, IOS device, and so on. • The number of each device type. • The number of devices that are experiencing slow, medium, and fast KPI time.

Step 2   Hover your cursor over a color block in the cluster to get information about the AP, such as the date, the building in which the AP resides, the model number of the AP, radio protocol, and the radio client count. A darker color block has more clients than a lighter color block.

View and Monitor Network Performance Using Baselines

Cisco AI Network Analytics uses the most advanced machine learning techniques to define the baseline that is relevant to your specific network and sites. With this information Cisco AI Network Analytics is able to define what is normal for each network and site at a specific moment, and identify the most important issues.

Use this procedure to explore and monitor the network performance using machine learning algorithm derived baselines.

Step 1   Click the menu icon (☰) and choose **Assurance** > **Baselines**.

The **Baselines** dashboard appears.
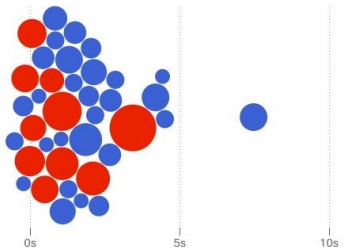
Figure 43: Baselines Dashboard
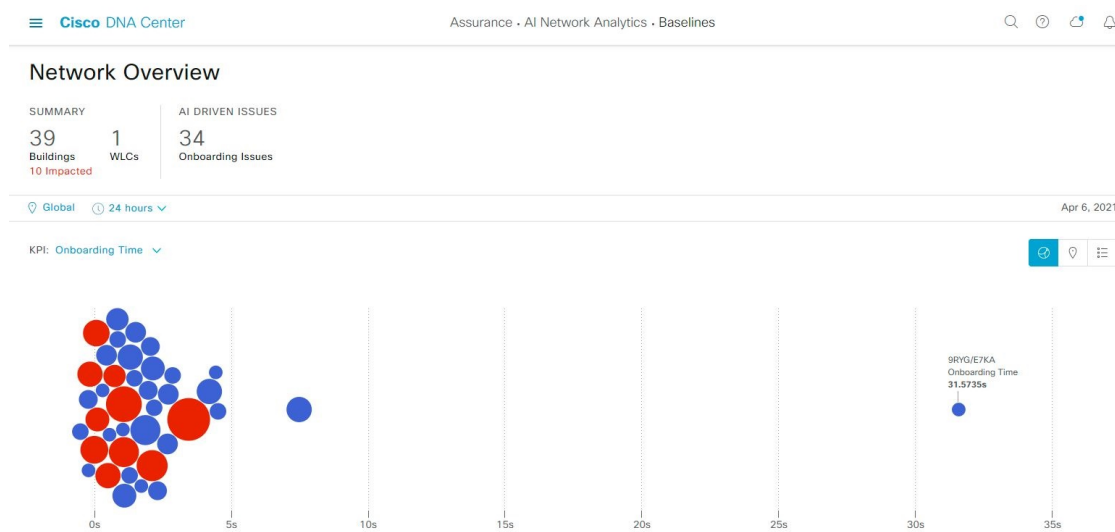
Step 2   Use the Network Overview window to view the following information:

Network Overview Window	
Item	**Description**
Summary	Displays the total number of buildings, buildings impacted with issues and wireless controllers in your network.
AI Driven Issues	Displays the issues detected by Cisco AI Network Analytics, triggered based on deviations from the predicted baseline for your specific network environment.
⊙ Global ⌄ Location drop-down list	Click the location icon to open the slide in pane to select a site or building. The information is refreshed in the dashboard based on your selection.

Network Overview Window	
Item	**Description**
🕐 Time Range setting	Enables you to display data within a specified time range on the dashboard. Do the following: • From the drop-down menu, choose the length of the range: 24 Hours, or the custom range • Specify the Start Date and the End Date. • Click Apply
KPI drop-down list	Choose a KPI from the drop-down list. Options are: **Onboarding Time**, **Onboarding Failures**, **DHCP Time**, **Authentication Time**, and **Association Failures**. Default is **Onboarding Time.**
  Map View	Click this toggle button to display the health of all the network sites on a geographic location-oriented map view of your network.
  List View	Click this toggle button to display the sites and buildings from your network in a list format.

Network Overview Window	
Item	**Description**
  Beeswarm Chart	Click this toggle button to view the beeswarm chart which provides the insights about the performance of the client devices of your network with respect to the selected KPI. In this case, the entity in the beeswarm chart is a building and it is represented in a circles. Each circle in the beeswarm chart represents the following: • Blue color: The circle represents a building. Hover your cursor over a circle in the chart to get information, such as location, KPI, SSID, wireless controllers and client count. • Red color: The circle represents a building impacted with issues. Hover your cursor over a circle in the chart to get information, such as location, KPI value, SSID, wireless controllers, client count, and AI-driven issues. • The size of the circle represents the number of clients connected. A small circle has a lower client count and the large circle has a higher client count.

Step 3 From the beeswarm chart, click a circle to display the building view for the following information:

Building View
Displays the specific information of a site or building. You can select the KPIs, SSID, and wireless controller from the respective drop down list to view the data.
Use the timeline slider to specify a more granular time range. You can click and drag the timeline boundary lines to specify the time range.
Use the color-coded charts below the timeline slider to determine how your network is performing. View issues based on the deviations from the predicted baseline for a selected KPI within the specified time period. Hover and move your cursor over the charts to view synchronized tooltips that display duration, predicted upper, and predicted lower range at a selected point in time.
The color codes represent the following:
• Red represents AI-driven issues
• Blue represents the average KPI duration
• Green represents the predicted KPI
Click **View Details** to open a slide-in pane with additional details, depending on the KPI you choose from the KPI charts. In the slide-in pane, the color-coded charts are displayed for Average KPI Duration(s) (such as Onboarding Time, DHCP Time, Onboarding Failures, and Authentication Time) and Unique Clients.
Sankey charts are displayed to emphasize the major flow between floors and device type (client devices). Below the charts, you can see the AP name, onboardings, failed onboardings, percentage of failed onboardings, client count, and so on.
Note   The client count shown in the table is an average of chosen time interval over the individual client count readings observed in the 30-minute window.

View the RF Network Using the Enhanced RRM Dashboard

Cisco AI Network Analytics uses machine learning algorithms to define the behavior of a radio frequency (RF) network within a building enabled with enhanced Radio Resource Management (RRM).

Before you begin

 • You must assign a location to an AI RF profile to view the enhanced RRM dashboard. For more information, see **Assign Location to an Existing AI RF Profile** in the *Cisco DNA Center User Guide*.

 • You must provision the devices across the AI RF profile assigned locations to access AI-enhanced RRM insights. For more information, see **Provision Wireless Devices** in the *Cisco DNA Center User Guide*.

 • Cisco AI-enhanced RRM is supported only on Cisco Catalyst 9800 Series Wireless Controllers and Cisco IOS XE Release 17.7.1 or later.

 • To perform the following task, you must be a **Super Admin** or **Network Admin**.

Step 1 Click the menu icon (☰) and choose **Assurance** > **Enhanced RRM**.

Step 2 In the left pane, you can either search for a site by entering its name in the **Find Hierarchy** field or expand **Global** to choose the sites.

The **Enhanced RRM** dashboard is displayed.

Figure 44: Enhanced RRM Dashboard
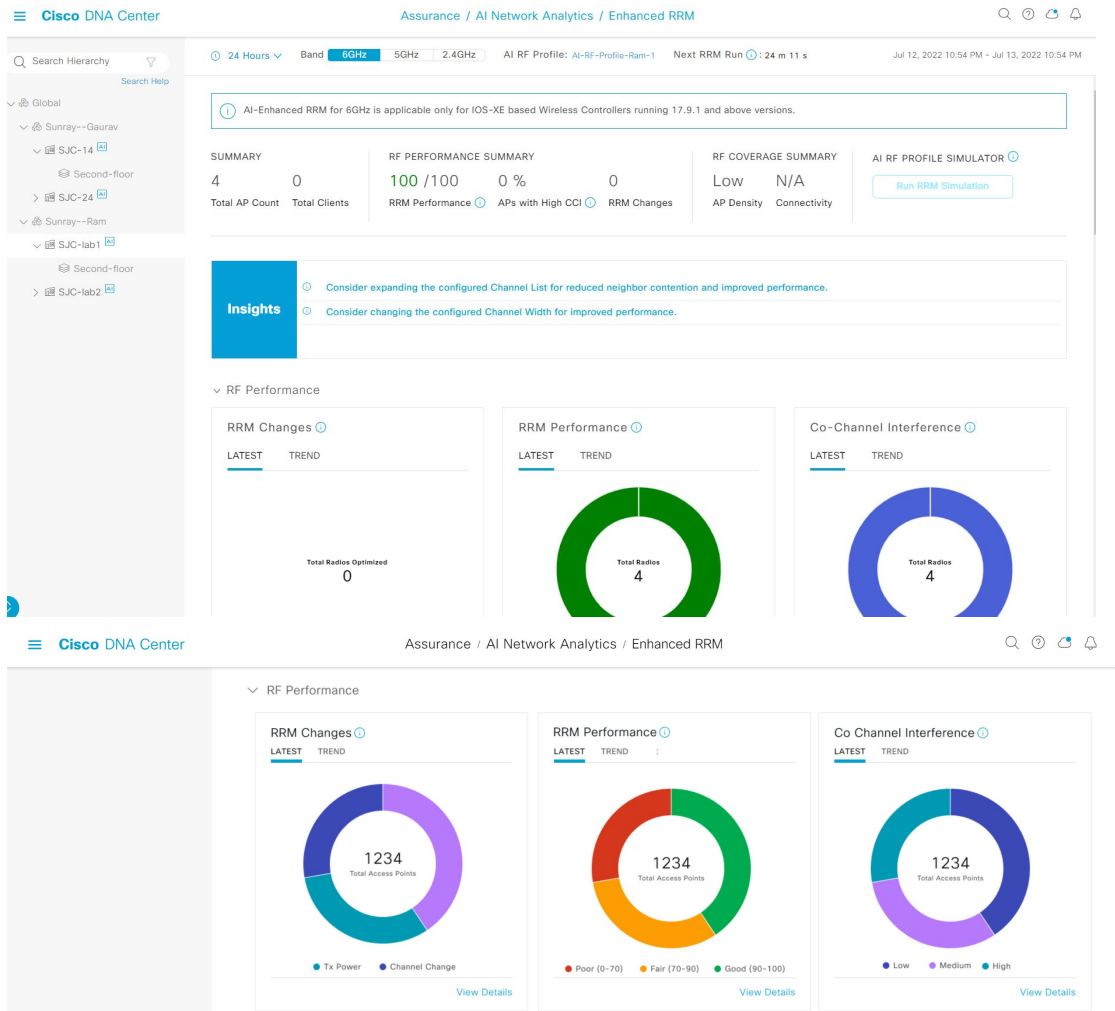
Step 3 Use the **Enhanced RRM** dashboard top-menu bar for the following functionality:

Item	Description
Time Range	Enables you to display data within a specified time range on the dashboard. The available time ranges are **24 Hours**, **7 Days**, or **14 Days**.
Band	Enables you to toggle between the **2.4GHz**, **5GHz**, and **6GHz** band to display the data for a particular band.
AI RF Profile	Displays the current AI RF profile assigned to the building.

Item	Description
Next RRM Run	AI-enhanced RRM computation occurs every 30 minutes. RRM decisions are updated and pushed to the device after the computation.

Step 4   Click the **Insights** icon to view the Cisco recommended insights.

    a) Check the **Channel List** check box to choose the channel list which is currently on the AI RF profile list.

    b) Check the **Channel Width** check box and click **Apply** to set the recommended Dynamic Bandwidth Selection.

    c) Click **Now** or **Later** to indicate when you want to apply the recommendations.

    d) Click **Run Simulation** to view the simulation result.

Step 5   Use the Summary dashlet to view the following information:

Item	Description
Summary	Displays the total number of AP counts and Clients in your network.
RF PERFORMANCE SUMMARY	• **RRM Performance**: Shows a composite metric based on several KPIs, such as co-channel interference, noise, SNR, and radio utilization. • **APs with High CCI**: Shows the lower performance of the wireless network provided by the AP and neighbor. • **RRM Changes**: Shows the total number of RRM channel changes, channel bandwidth changes, and Tx power change events by time of the day.
RF COVERAGE SUMMARY	• **AP Density**: Shows the density of APs as low, medium, or high in RF coverage. • **Connectivity**: Shows the connectivity of APs in RF coverage

Step 6   Use the **Insights** dashlet to review the insights generated by the AI-enhanced RRM. The insights are configuration recommendations that can be applied to the AI RF profile.

The **Insights** dashlet displays the following possible insights:

    • Busy Hours

    • TPC Threshold

    • Channel Width

    • Enable FRA

Step 7   Under **AI RF Profile Simulator**, click **Run RRM Simulation** to simulate RF configurations, visualize the impact, and create a new profile.

The AI RF Profile Simulator allows you to simulate changes to the current RF profile and visualize the projected outcomes against the enhanced RRM dashlets. The RRM simulation runs based on the radio band that you selected on the AI RF profile and cannot be modified in the simulator.

Note   **Run RRM Simulation** is not supported for the 6-GHz radio band.

    a) In the **Welcome to RRM Simulator** window, click **Create Simulation**.

    The current AI RF Profile information appears.

b) You can modify the attributes under **5 GHz**, as needed to see the metrics.

Note Attributes such as busy hour, data rates, client limit, and RX SOP are not considered for simulation.

c) Click **Reset** to change the AI RF profile attribute value to the corresponding base AI RF profile value.

d) Click **Run Simulation**.

A message stating that the **Simulation in Progress** appears.

e) In the **Simulation Result** window, review the simulation configured on the AI profile for the 5-GHz radio band. To edit any details, click the **Edit** option that is displayed in the corresponding area of the window.

- **Simulation Name**

- **Profile Details**

- **RF Performance**

- **RF Coverage**

f) Click **Upgrade AI RF Profile**.

The **Upgrading AI RF Profile** dialog box appears.

g) In the **Upgrading AI RF Profile** dialog box, you can edit the profile name.

Click **Now** or **Later** to indicate when you want to apply the recommendations and click **Apply**.

h) In the **Review Cisco AI Recommendations for RRM** window, review and check the check box of the configurations for the AI RF Profile from the available recommendations for the selected site and click **Apply**.

i) Click **Ok** in the **AI RF Profile Successfully Updated** dialog box.

j) In the **Simulation Result** window, review the simulation result for the configured AI supported RF profile.

Step 8 Expand **RF Performance** for the following functionality:

Item	Description
RRM Changes dashlet	Includes the following tabs: • **LATEST**: Shows the total number of RRM channel changes, channel bandwidth changes, Tx power change and band or role change events in the last 30 minutes. • **TREND**: Shows the channel changes, channel bandwidth change, and Tx power change of APs for the events and selected time in the time range. Click either color segment in the graph or click the **View Details** link to open the **RRM Changes** slide-in pane. a. Hover your cursor over the color segment in the graph to view the **Change Category** and **Total Affected APs**. b. Click the color segment in the graph to view the device data in the **Access Points** table that is displayed below the chart: • Access Point • Change Category c. Click the radio button next to the AP to view the **Event Reasoning** of change categories managed by RRM. **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details. d. Click **Export** to download the AP table data to your local machine.

Item	Description
RRM Health dashlet	Includes the following tabs: • **LATEST**: Shows the total number of APs contributing to **Poor**, **Fair**, and **Good** AP health scores in the last 30 minutes. • **TREND**: Shows the **Poor**, **Fair**, and **Good** RRM health score of APs for the percentage of AP count and selected time in the time range. Click either a color segment in the graph or the **View Details** link to open the **RRM Health** slide-in pane. a. Hover your cursor over the color segment in the graph to view the **Fair**, **Poor**, and **Good** RF performance score of the AP and its radio. b. Click the color segment in the graph to view the following device data in the **Access Points** table that is displayed below the chart: • Access Point • Health Score • Co-Channel Overlapping • Co-Channel Neighbor Utilization • Low RSSI Client Score • Noise Same Channel • Interference Same Channel **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details. c. Click **Export** to download the AP table data to your local machine.

Item	Description
Co-Channel Interference dashlet	Includes the following tabs: • **LATEST**: Shows the total number of APs experiencing **Low**, **Medium**, and **High** co-channel interference in the last 30 minutes. • **TREND**: Shows the percentage of **Low**, **Medium**, and **High** co-channel interference of APs for the percentage of AP count and selected time in the time range. Click either a color segment in the graph or the **View Details** link to open the **Co-Channel Interference** slide-in pane. a. Hover your cursor over the color segment in the graph to view the **Low**, **Medium**, and **High** co-channel interference of APs. b. Click the color segment in the graph to view the following device data in the **Access Points** table that is displayed below the chart: • Access Point • Channel • Impact Score • CCI (dBm) • Duty Cycle **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details. c. Click **Export** to download the AP table data to your local machine.
Utilization Per Channel dashlet	Displays the utilization chart. For the 6-GHz band, the utilization chart is based on the UNII level that you choose in the **View by** drop-down list. The UNII levels are **PSC**, **UNII 5**, **UNII 6 & 7**, and **UNII 8**. The default view is **PSC**. The **LATEST** tab shows the total number of APs experiencing **Low**, **Medium**, and **High** co-channel interference in the last 30 minutes. Hover your cursor over the chart to view the following details: • Number of channels • Tx/Rx utilization • Interference The **TREND** tab displays the utilization per channel details for the percentage of utilization and selected time in the time range. **Note** The **Select Channel** drop-down list allows you to search a channel by entering its name or choose a channel from the list to display the details.

Item	Description
AP and Radar per Channel dashlet	The **LATEST** tab displays the AP and radar per channel details in the chart for APs and channels in the last 30 minutes.
	Hover your cursor over the chart to view the following details:
	• Number of channels
	• Tx/Rx utilization
	• Interference
	The **TREND** tab displays the AP, rogue, and radar per channel details in the chart for the AP or radar and selected time in the time range.

Step 9   Expand **RF Coverage** for the following functionality:

Item	Description
AP Spatial Density dashlet	The AP spatial density value represents the number of APs that are the neighbors of a selected AP in your infrastructure at or above -70 dBm. The density of APs affects the optimal effective values of channels, channel width, and Tx power. • **LATEST**: Shows the number of APs that are the neighbors of a selected AP in your infrastructure for the percentage of radio count, AP neighbor density, and percentage of client count in the last 30 minutes. Hover your cursor over the chart to view the following: • AP Neighbor Density • AP Count • End Point Count • **TREND**: Shows the average neighbor density number and AP count for the AP count and selected time in the time range. Average neighbor density ranges are **<5**, **5-10**, **10-15**, **15-20**, **20-25**, and **>=25**. Under the **LATEST** tab, click either a color segment in the graph or the **View Details** link to open the **AP Spatial Density Details** slide-in pane. a. Hover your cursor over the chart to view the **AP Neighbor Density**, **AP Count**, and **Clients Count** in the selected building. b. Click a color segment in the graph to view the **Top APs** graph by lower/higher neighbor density and the following device data in the **Access Points** table: • Access Point • Neighbor Density Metric • Total Rx Neighbors • Highest on Channel Neighbor RSSI • Total on Channel Neighbors **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details. c. In the **Top APs** area, click the drop-down list to choose top APs by lowest neighbor density or highest neighbor density. d. Hover your cursor over the **Top APs** chart to view the **Min**, **Max**, and **Latest** APs in the chart for AP and neighbor count. e. Click **Export** to download the AP table data to your local machine.

Item	Description
Power Distribution dashlet	The power distribution chart helps you visualize the physical Wi-Fi coverage areas in your environment. It also allows you to identify the APs that are operating at maximum and minimum power levels.
	For the 6-GHz band, you can display the data based on **Power Level** or **Power dBm** that you choose in the **Filter** drop-down list.
	LATEST: Shows the number of APs that are operating at different power level along with radio count percentage and neighbor count percentage in the last 30 minutes. - Hover your cursor over the chart to view the following: - Operating Power Level (for power level view for the 6-GHz band) - Operating Power dBm for the 6-GHz band (for power dBm view) - Radio Count - Neighbor Count **TREND**: Shows the number of APs that are operating at different power levels along with radio count percentage and selected time in the time range. Hover your cursor over the trend chart to view the radio count percentage operating at different power levels. The power levels calculations are from **Level 1** (maximum power level) to **Level 8** (minimum power level).
	Under the **LATEST** tab, click either a color segment in the graph or the **View Details** link to open the **Power Distribution Details** slide-in pane.
	a. Hover your cursor over the graph to view the **Operating Power Level**, **Radio Count**, and **Neighbor Count** in the selected building.
	b. Click a color segment in the graph to view the **Top APs** graph by lower/higher neighbor density and the following device data in the **Access Points** table: - Access Point - Coverage Hole Count - Tx Power (dBm) - Tx Power Level (%) - Neighbor Density Metric - Delta Average Neighbor Tx power (dB) **Note** In the **Access Points** table, hover your cursor over the **i** icon to view more details.
	c. Click **Export** to download the AP table data to your local machine.

Step 10   Expand **Additional Site Level Information** to download a service bundle.

Step 11   In the **Service Bundle** area, click the **Request a Latest Service Bundle** link to download a service bundle for the selected building.

Step 12   To download service bundle data for the last hour, in the **SELECT A PERIOD TO DOWNLOAD** area, specify the **Start Date** and **Start Time**; and **End Date** and **End Time**.

Step 13   Click **Download Service Bundle**.

A service bundle is saved to your local machine that contains configuration parameters and RRM telemetry used for RRM algorithms at the selected time period. This service bundle can be used to troubleshoot and analyze the RF environments of the building for better RRM service.

CHAPTER **20**

Manage Intelligent Capture

About Intelligent Capture

For Cisco DNA Center, all information about device and client health is typically available from Cisco wireless controllers. Intelligent Capture provides support for a direct communication link between Cisco DNA Center and access points (APs), so each of the APs can communicate with Cisco DNA Center directly. Using this channel, Cisco DNA Center can receive packet capture data, AP and client statistics, and spectrum data. With the direct communication link between Cisco DNA Center and APs, Intelligent Capture allows you to access data from APs that is not available from wireless controllers.

Note
- Intelligent Capture is only supported for APs in either local or FlexConnect mode.
- Intelligent Capture is not supported in SDA deployments.

Supported Devices for Intelligent Capture

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

Supported Cisco Wireless Controllers	
Device	**Minimum Supported Software Version**
Cisco 3504 Wireless Controller	AireOS 8.8.125.0
Cisco 5520 Wireless Controller	AireOS 8.8.125.0

Supported Cisco Wireless Controllers	
Device	**Minimum Supported Software Version**
Cisco 8540 Wireless Controller	AireOS 8.8.125.0

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

Supported Cisco Catalyst Wireless Controllers	
Device	**Minimum Supported Software Version**
Cisco Catalyst 9800 Series Wireless Controllers	IOS-XE Gibraltar 16.12.1.s

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

Supported Cisco APs		
Device	**Minimum Supported AireOS Software Version**	**Minimum Supported IOS-XE Software Version**
Aironet 1540 APs[3]	8.10.105.0	16.12.1.s
Aironet 1560 APs	8.10.105.0	16.12.1s
Aironet 1815 APs[1]	8.10.105.0	16.12.1s
Aironet 1830 APs[1]	8.10.105.0	16.12.1s
Aironet 1840 APs[1]	8.10.105.0	16.12.1s
Aironet 1850 APs[1]	8.10.105.0	16.12.1s
Aironet 2800 Series AP	8.8.125.0 or 8.10	16.12.1s
Aironet 3800 Series APs	8.8.125.0 or 8.10	16.12.1s
Aironet 4800 Series APs[4]	8.8.125.0 or 8.10	16.12.1s
Catalyst 9105 AP[1]	8.10 MR3	17.3.1
Catalyst 9115 AP[1]	8.10.105.0	16.12.1s
Catalyst 9120 AP	8.10.105.0 8.10.112.0 (for Spectrum Analysis)	16.12.1s 17.2.1 (for Spectrum Analysis)
Catalyst 9130 AP[2]	8.10 MR3	17.3.1
Catalyst IW6300 Heavy Duty Series APs	8.10.105.0	17.1.1s
Catalyst ESW6300 Embedded Services APs	8.10.105.0	17.1.1s

[3] Spectrum Analysis is *not supported* on the following APs: Aironet 1540 AP, Aironet 1800 Series APs, Catalyst 9105 AP, and Catalyst 9115 AP.

[4] Data Packet Capture is only supported on Aironet 4800 APs and Catalyst 9130 AP.

Intelligent Capture Best Practices

The following are best practices to ensure Intelligent Capture functions optimally in Cisco DNA Center:

- After a new wireless controller device is added to Cisco DNA Center, disable any Intelligent Capture global settings, and then re-enable those settings so that they will be configured on the new wireless controller.

- Before deleting a wireless controller device from Cisco DNA Center, disable all Intelligent Capture settings.

- Before upgrading any of managed wireless controllers or reimaging Cisco DNA Center, disable all Intelligent Capture settings, and then re-enable them after completing the upgrade.

Live and Scheduled Capture Sessions for a Client Device

About Capture Session for a Client Device

You can run the following types of capture sessions for a client device:

Onboarding Packet Capture session captures packets that the client device uses to join a wireless network, such as 802.11 management frames, DHCP, and EAP packets, and collects the client's RF statistics (5-second samples). The data is displayed in Client 360 > Intelligent Capture page. The session can be started immediately (Run Now) or scheduled to run later. The default duration of the session is 30 minutes and set up to eight hours. By default, capture is enabled on the last client connected wireless controller. You can select up to three wireless controllers to cover client roaming scenario.

Onboarding Capture Session Limitations

Onboarding capture sessions have the following limitations:

- There are a total of 16 time slots allocated for capture sessions (live and scheduled), where each client in a session uses one time slot.

  The maximum number of live capture sessions is 16, so if 16 live capture sessions are running at the same time, no slots are available for scheduled capture sessions.

  The maximum number of concurrent scheduled capture sessions is 12, which always leaves four (16 minus 12) available slots for live capture sessions.

  If these maximum values are exceeded, for example, you try to start a seventeenth live capture session, the following error message is displayed. Click **Yes** in the error message dialog box, and then select a capture session for which you want to end the live capture.

> ✎
>
> **Note** The 16-time-slot limit is enforced by the wireless controller.
>
> When capture sessions are configured on Cisco DNA Center, any live or scheduled capture sessions that Cisco DNA Center is not aware of (such as partial packet capture sessions that were directly configured on the wireless controller) are removed.

- A maximum of 100 packets involved in onboarding events can be captured during the time period surrounding the event.

- There is a 3.5-GB limit on the total size of all scheduled onboarding packet files that reside on Cisco DNA Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 3.5-GB limit.

About Client Statistics

Onboarding Packet Capture sessions are global settings that enable supported APs to collect client statistics over 5-second intervals.

Client statistics are also collected over 30-second intervals when AP stats are enabled for the AP to which the client is connected.

When client statistics are collected, they are displayed on the four RF statistic charts on the **Client 360** > **Intelligent Capture** window.

Enable a Live Capture Session for a Client Device

Use this procedure to enable a live capture session for a specific client device and view data packets for the onboarding events and RF statistics.

Step 1 Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2 Click the **Client Health** tab.

The **Client Health** window appears.

Step 3 Open the **Client 360** window of a specific client by doing one of the following:

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

A 360° view of the client device appears.

Step 4 In the **Client 360** window, click **Intelligent Capture**.

The **Intelligent Capture:** *Client Device* window appears with the following information:

Attention   If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or Access Point Unable to Send Intelligent Capture Data to Cisco DNA Center, on page 336 for more details.

Figure 45: Intelligent Capture Window of a Client

Step 5   Use the timeline slider for the following functionality:

Timeline Slider	
Item	**Description**
1 hour drop-down list	Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour**, **3 hours**, and **5 hours**. Default is **1 hour**.
Timeline Slider	The timeline slider determines the time window of all data displayed. A line chart of onboarding events is displayed for the results of a live capture. Green indicates onboarding events and red indicates anomaly events.
	To adjust the timeline to a different time window, click the < and > buttons to the desired time window.
	Note The timeline can display data from up to two weeks in the past.
	For more customization of the timeline range, click and drag the boundary lines.

Step 6   To perform a live capture session, do the following:
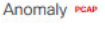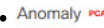
a) Click **Start Live Capture** at the top-right corner to start a live capture session.

During a live capture session, data packets for the **Onboarding Events** and **RF Statistics** dashlets are collected.

b) Click **Stop Capturing** to stop the live capture session.

Note	Live capture sessions run for three hours. After three hours, a dialog box for extending the session appears.

c) View the running live capture sessions in the **Intelligent Capture Settings** window for clients.

Step 7 Use the **Onboarding Events** dashlet to view events that are associated with establishing a network connection:

Onboarding Events Dashlet	
Item	**Description**
All and Anomaly PCAP filter	Allows you to filter the onboarding events. Options are: • **All**: Displays all events. This is the default. • Anomaly PCAP : Filter for only anomaly events. **Note** If the client has issues joining the network, the word "PCAP" is displayed in red beside the specific event. If the client has no issues joining the network, the word "PCAP" is displayed in gray beside the specific event.
Export PCAP	You can download the packets for a range of specified events: a. Click **Export PCAP**. b. Specify the first and last events that you want to include in the PCAP. c. Click **Download PCAP** to start the download. **Note** Since heuristics are used to determine which packets belong to an event, packets from one minute before the first event and one minute after the last event will be included in the download. This ensures that all relevant packets are in the downloaded PCAP. Each export is limited to the first 2000 packets, starting from the oldest timestamp.
List of Onboarding, Incomplete, and Anomaly Events	View the list onboarding, incomplete, and anomaly events in chronological order. Events are color-coded to indicate the following: 🟢: Successful onboarding event. 🔵: Incomplete event. 🔴: Anomaly event. **Note** Events with a 🔲 icon indicates that data packets for this event have been captured for download or analysis. You can click the parent event group to expand it and view the individual events for that group.

Onboarding Events Dashlet	
Item	**Description**
Event Details	You can click an event group or individual event to view the following sections with further details:
	Client Location: Displays the map of the client location and the client's movement during the event.
	Auto Packet Analyzer: This section appears if a live capture, scheduled capture, or anomaly capture session has captured packets for the event. The ⬚ icon that appears next to the event indicates that the event has captured packets.
	The **Auto Packet Analyzer** section displays a graph with the following information:
	• The packets (up to 100) surrounding the event are divided into two groups. Gray sections indicate packets that precede the start of an onboarding session. White sections indicate packets in the onboarding session.
	Deauthentication packets and unexpected patterns of packets are represented by red triangles. These are potentially significant packets that can degrade the client's onboarding experiences.
	You can download the packets by clicking **Download Packets** for further analysis.
	• Packet (from client or from AP)
	• Onboard packet stage identifier
	• Interpacket gap (ms)
	• RSSI (dBm) per packet
	• Associated AP
	RF Statistics: Displays charts with the RF statistic data for the 10 minute interval surrounding the event.
	The RF statistic data is composed of RSSI and SNR measurements in decibels, Rx average data rate and Rx last data rate, Tx packets and Rx packets, and Tx packet retry.
	Note If **Anomaly Capture** is enabled, the packets for anomaly events are captured even if a live or scheduled capture is not running.

Step 8   Use the **Client Location** dashlet to view the a floor map with 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.

Note   The Client Location feature requires that CMX is integrated with Cisco DNA Center. For details, see the Integrate Cisco CMX for Wireless Maps, on page 345 chapter.

Step 9   Use the **RF Statistics** dashlet to view detailed RF information.

There are four charts that displays the AP client statistics for the client. See About Client Statistics, on page 318. The color-coded data contains the following information:

- RSSI and SNR measurements in decibels.

- Rx average data rate (from the past 5 seconds) and Rx last data rate.

- Tx packets and Rx packets.

- Tx packet retry.

You can do the following in the charts:

- Hover your cursor over the chart to see the statistics for a particular time.

- Click and drag within the chart to zoom in on a period. To change the view to the default, click the ⊖ icon.

Step 10   To run a Data Packet Capture for a client device, see Run Data Packet Capture for a Client Device, on page 325.

Schedule and Manage Capture Sessions for a Client Device

Use this procedure to schedule a capture session and to stop, edit, or delete a scheduled capture session.

Client capture sessions collect the following data:

- Data packets for onboarding events and **RF Statistics** chart data (5 second samples) displayed in the **Client 360** > **Intelligent Capture** window. See Enable a Live Capture Session for a Client Device, on page 318.

- Data for the charts and tables displayed in the **Device 360** > **Intelligent Capture** window. See View RF Statistics and Manage Spectrum Analysis Data for an Access Point, on page 331.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Intelligent Capture Settings**.

The **Client Schedule Capture** window appears.

Step 2   To schedule a client capture session, click + **Schedule Client Capture**.

In the **Schedule Client Capture** slide-in pane, do the following:

a)   In the **Start Time** area, specify when you want the capture session to start. Options are **Run Now** and **Run Later**.
b)   Click the **Duration** drop-down list to specify the duration.

c) Click the **Select Client Devices** drop-down list and enter a search string that returns matches for the categories: client user ID, host name, or MAC address.

Note   Search returns a maximum of 10 matches for each category, so refine your search string if you do not find your entry.

Note   For more details about capture sessions, see About Capture Session for a Client Device, on page 317.

d) Click **Save**.

Step 3   To stop a running capture session, do the following:

a) Click the **In-progress Captures** tab.

b) Select a client from the table.

c) Click **Stop Capture**.

Step 4   To edit a capture session that has been scheduled for a future time, do the following:

a) Click the **Scheduled Captures** tab.

b) Select a client from the table.

c) Click **Edit Schedule**.

Step 5   To delete a completed capture session, do the following:

a) Click the **Completed Captures** tab.

b) Select a client from the table.

c) Click **Delete Schedule**.

Data Packet Capture for a Client Device

About Data Packet Capture for a Client Device

Data Packet Capture allows you to capture network data into PCAP files, which can be downloaded and viewed in Wireshark. In addition, if you choose to integrate with the Network Analysis Module (NAM), you can capture the following information for a client device: accessed applications and ports, QoS data, packet loss, wireless delay, and jitter. For more information, see About NAM Integration, on page 324 and Run Data Packet Capture for a Client Device, on page 325.

Data Packet Capture Limitations

Data Packet Capture has the following limitations:

- Data Packet Capture is only supported on Cisco Aironet 4800 APs and Cisco Catalyst 9130, 9136, and 9166 APs. If Data Packet Capture is enabled and the client roams to an AP that does not support it, packet capture stops until the client reconnects to an AP that supports packet capture.

- Only one Data Packet Capture session can run at a time.

- As for all Intelligent Capture features, clocks must be synchronized between Cisco DNA Center and the Cisco Wireless Controller for Data Packet Capture to work. Ensure that the wireless controller is connected to a Network Time Protocol (NTP) server.

• Each Data Packet Capture session can capture up to 1 GB of rolling data. The 1 GB of data is broken into ten 100-MB files for faster downloads.

About NAM Integration

If you have a Network Analysis Module (NAM) or vNAM server running software version 6.4(2) or later, you can integrate your NAM server with Cisco DNA Center. For information about installation and configuration, see the *Cisco Prime Virtual Network Analysis Module (vNAM) Installation and Configuration Guide*.

With NAM integration and Full Packet Capture enabled for a client, data is provided to the **Wireless Packet Application Analysis** charts in the **Client 360** > **Intelligent Capture** window. The table and charts provide information on the applications used by the client, their QoS settings, packet loss, wireless delay, and jitter.

To integrate your NAM server with Cisco DNA Center, do the following:

1. Configure an IP address on the NAM data port.

2. Configure the gRPC collector.

Note   NAM integration is not supported on Cisco DNA Center clusters that use IPv6 addresses.

Configure an IP Address on the NAM Data Port

Use this procedure to configure a valid IP address on the data port of the NAM or vNAM. This is required to integrate with NAM.

Note   The data port is meant for receiving packets only; it does not respond to requests. Consequently, pinging the data port will time out even if you have the IP address configured correctly. Make sure that the IP address is valid and reachable from Cisco DNA Center.

Step 1   Log in to the CLI of the NAM server.

Step 2   Enter the command **show data-port ip-addresses**.
The command displays the port number and IP address:

```
Device# show data-port ip-addresses
Port number: 1
IPv4 address: 172.20.125.125
```

Step 3   If nothing is displayed for the **show data-port ip-addresses** command, enter the command **data-port 1 ip-address** *ip-address* to assign an IP address to port 1.

Step 4   Run the **show data-port ip-addresses** command again to verify that data-port 1 has been assigned an IP address.

Step 5   Record the IP address of data-port 1 or one of the other displayed ports.

Step 6   Verify that **cdb-export** is enabled in Cisco DNA Center. To do this, enter the command **show cdb-export all**. If nothing is displayed, enter the command **cdb-export collector 1 ip-address** *IP-address-of-Cisco-DNA-Center*.

Step 7 Make sure that data packets from Cisco DNA Center are processed by entering the command **autocreate-data-source erspan**.

Step 8 Make sure that the time on the NAM or vNAM server and Cisco DNA Center is synchronized. You can synchronize the time from the NAM user interface by choosing **Administration** > **System** > **System Time**.

Configure the gRPC Collector

Use this procedure to configure a gRPC collector for NAM integration. gRPC is an open source high performance RPC (Remote Procedure Call) framework.

Before you begin

Configure an IP address on the NAM data port. See Configure an IP Address on the NAM Data Port, on page 324.

Step 1 Click the menu icon (≡) and choose **System** > **Data Platform**.

The **Data Platform** window appears.

Step 2 Click the **Collectors** tab.

The **Collectors** window appears.

Step 3 Click **GRPC-COLLECTOR**.

The **GRPC-COLLECTOR** window appears.

Step 4 Click + **Add**.

The **gRPC Collector Configuration** window appears.

Step 5 Add only one **GRPC-COLLECTOR** configuration. Do the following:
   a) In the **ConfigData** area, check the **Agent Export** check box to export the network packet data to NAM.
   b) In the **Agent IP Address** field, enter the IP address of the data port recorded (refer to Step 5, on page 324 from Configure an IP Address on the NAM Data Port, on page 324).
   c) In the **Configuration Name** field, enter a unique name for the GRPC collector configuration.
   d) Click **Save Configuration**.

Run Data Packet Capture for a Client Device

Use this procedure to run a Data Packet Capture for a client device.

Before you begin

To retrieve information about accessed applications and ports, QoS data, packet loss, wireless delay, and jitter, you must enable NAM integration. For details, see About NAM Integration, on page 324.

Step 1 Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2 Click the **Client Health** tab.

The **Client Health** window appears.

Step 3 Open the **Client 360** window of a specific client by doing one of the following:

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

A 360° view of the client device appears.

Step 4 In the **Client 360** window, click **Intelligent Capture**.

The **Intelligent Capture:** *Client Device* window appears with the following information:

Attention If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or Access Point Unable to Send Intelligent Capture Data to Cisco DNA Center, on page 336.

Figure 46: Intelligent Capture Window of a Client

Step 5 Use the timeline slider for the following functionality:

Timeline Slider	
Item	**Description**
1 hour drop-down list	Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour**, **3 hours**, and **5 hours**. Default is **1 hour**.
Timeline Slider	The timeline slider determines the time window of all data displayed.
	To adjust the timeline to a different time window, click the < and > buttons to the desired time window.
	Note The timeline can display data from up to two weeks in the past.
	For more customization of the timeline range, click and drag the boundary lines.

Step 6 To run a Data Packet Capture, use the **Data Packet Capture Area** (located on the top-right corner) for the following functionality:

Data Packet Capture Area	
Item	**Description**
Run Packet Capture button	Click **Run Packet Capture**, to open the **Client Packet Capture** slide-in pane and do the following: a. Choose the **Packet Capture Type**, by clicking Onboarding Packet Capture or Full Packet Capture radio button. b. Choose the **Start Time**. Options are Run Now or Run Later c. From the **Duration** drop-down list, choose the time duration of the packet capture. Default is 30 minutes. d. Select the **Wireless Controllers** for which you need to enable the packet capture. You can select maximum three wireless controllers. e. Click **Save**. **Note** All Onboarding Packet Capture sessions are displayed under **Assurance** > **Intelligent Capture Settings** > **Client Schedule Capture**. When a Data Packet Capture session is configured on Cisco DNA Center, any Data Packet Capture sessions that Cisco DNA Center is not aware of are removed (such as full packet capture sessions that were directly configured on the wireless controller). **Note** As for all Intelligent Capture features, time zones must be synchronized between Cisco DNA Center and the Cisco Wireless Controller for Data Packet Capture to work. Ensure that the wireless controller is connected to a Network Time Protocol (NTP) server. **Note** New sets of PCAP files are started each time a new capture session is started.
Download button	After full packet PCAP files have been captured from a session, click this button to download PCAP files. Click the icon in the **Download** column to download the data packet files. You can download files for either: • Wireless data: 802.11 files for packets between the AP and the client. • Wired data: Ethernet files for packets between the AP and the switch or wireless controller. **Note** A Data Packet Capture file has a limit of 100 MB. The total of all Data Packet Capture files cannot exceed 3.5 GB. **Note** Only PCAP files from the past seven days can be downloaded.

Step 7 Use the **Wireless Packet Application Analysis** dashlet to view details about the data packet capture.

When a data packet capture is running, this dashlet displays details about the analyzed packets, such as the accessed applications and ports, QoS data, packet loss, wireless delay, and jitter.

Note To view data in this dashlet, you must set up the integration for NAM. See About NAM Integration, on page 324.

View Client Data Packet Capture History

Use this procedure to view the history of the client data packet capture sessions, such as the time the first packet and the last data packet was captured, the total size of the captured data packets, and the type of packet.

Step 1 Click the menu icon (≡) and choose **Assurance** > **Intelligent Capture Settings**.

The **Client Schedule Capture** window appears.

Step 2 Click the **Client Data Packet Capture** tab.

The **Client Data Packet Control** window appears.

Step 3 Use the **Intelligent Capture Settings - Client Data Packet Capture** window to view the following information:

Option	Description
Identifier	Displays the client's user ID or hostname. Click the user ID or hostname to open the **Intelligent Capture:** *Client Device* window.
MAC Address	Displays the MAC address of the client device.
First Packet Time	Displays the time the first data packet was captured.
Last Packet Time	Displays the time the last data packet was captured.
Total Size	Displays the total size of the captured data.
Currently Running	Displays whether the data packet capture is currently running.
Type of Packet	Displays the type of packet, for example, **Wired** or **Wireless**.

Intelligent Capture for Access Points

About Intelligent Capture for Access Points

The AP Intelligent Capture feature allows you to enable one or more APs to capture the following data:

- **AP Stats Capture**, which includes:

- AP radio and WLAN statistics that are displayed in the **RF Statistics** tab of the **Device 360** > **Intelligent Capture** window.

- AP Client statistics (30-second samples) that are displayed in the **RF Statistics** area of the **Client 360** > **Intelligent Capture** window for all clients associated with the selected APs.

- **Anomaly Capture** for anomaly onboarding events for all clients that are associated with one or more selected APs. Enabling Anomaly Capture ensures that all anomaly onboarding events (global or for all clients associated with the selected APs) are captured for download and display.

AP Capture Limitation

There is a 1.05-GB limit on the total size of all anomaly triggered packet files that reside on Cisco DNA Center. If the limit is exceeded, then packet files are removed, starting with the oldest, until the total size falls below the 1.05-GB limit.

Enable and Manage Intelligent Capture for an Access Point

Use this procedure to enable one or more access points (APs) to capture the following data:

- **AP Statistics**: Includes AP radio statistics, WLAN statistics, and AP Client statistics. Cisco DNA Center can support up to 1000 APs for AP Stats Capture.

- **Anomaly Capture**: For anomaly onboarding events of all clients that are associated with one or more selected APs. Enabling Anomaly Capture ensures that all anomaly onboarding events (global or for all clients associated with the selected APs) are captured for download and display.

Step 1 Click the menu icon (≡) and choose **Assurance** > **Intelligent Capture Settings**.

The **Client Schedule Capture** window appears.

Step 2 Click the **Access Point** tab.

The **Access Point** window appears.

Step 3 To enable or disable AP Stats Capture, do one of the following:

- If there are no enabled APs, the **Configure AP Enablement** area is displayed. Choose either the **Specific** or **Global** option, and then click **Get Started**.
- If there is least one AP is enabled, the **AP Stats Capture** window appears. From the **AP Stats Capture** window, choose one of the following options:

Option	Description
None - disable all APs	The **None - disable all APs** appears when at least one AP is enabled.
	Allows you to disable AP Stats Capture on all of the APs in which it is currently enabled.

Option	Description

Specific - select specific APs and enable	Allows you to enable AP Stats Capture for selected APs. Do the following:
	
	a. Click the **Specific - select specific APs and enable** radio button.
	
	b. In the left pane, expand **Global**, and drill down to the site > building > floor. The right pane displays the list of APs on that floor and contains three tabs: **Enabled APs**, **Disabled APs**, and **Not-Ready APs**.
	
	c. To enable AP Stats Capture for selected APs, do the following:
	
	   • Click the **Disabled APs** tab. A list of APs that have AP Stats Capture currently disabled, is displayed.
	
	   • Check the check boxes adjacent to the APs for which you want to enable AP Stats Capture, and then click **Enable**.
	
	d. To view incompatible APs, click the **Not-Ready APs** tab.
	
	Note Incompatible APs have the following conditions:
	
	   • The operation mode is not set to `local` or `FlexConnect`.
	
	   • The OS release that is installed on the AP is not compatible. The OS release must be MR1 or later.

Global - enable all capable APs	Allows you to enable the AP Stats Capture for all capable APs.

Step 4   To enable or disable Anomaly Capture, click the **Anomaly Capture** tab, and then do one of the following:

- If no APs are enabled, the **Configure AP Enablement** area displays, choose one of the following options, and then click **Get Started**.
- If at least one AP is enabled, the **Anomaly Capture** window appears. From the **Anomaly Capture** window, choose one of the following options:

Option	Description
None - disable all APs	The **None - disable all APs** appears when at least one AP is enabled. Allows you to disable Anomaly Capture on all of the APs in which it is currently enabled.

Option	Description

Specific - select specific APs and enable or disable	Allows you to enable or disable Anomaly Capture for selected APs. Do the following:
	
	a. Click the **Specific - select specific APs and enable or disable** radio button.
	
	b. In the left pane, expand **Global**, and drill down to the site > building > floor. The right pane displays the list of APs on that floor and contains three tabs: **Enabled APs**, **Disabled APs**, and **Not-Ready APs**.
	
	c. To enable Anomaly Capture for selected APs, do the following:
	   • Click the **Disabled APs** tab. A list of APs that have Anomaly Capture currently disabled, is displayed.
	
	     Note If a previous attempt to enable the AP failed, an error message is displayed in the **Config Status** column.
	
	   • Check the check boxes adjacent to the APs for which you want to enable Anomaly Capture, and then click **Enable**.
	
	d. To disable Anomaly Capture for selected APs, do the following:
	   • Click the **Enabled APs** tab. A list of APs that have Anomaly Capture currently enabled, is displayed.
	
	   • Check the check boxes adjacent to the APs for which you want to disable Anomaly Capture, and then click **Disable**.
	
	e. To view incompatible APs, click the **Not-Ready APs** tab.
	
	     Note Incompatible APs have the following conditions:
	       • The operation mode is not set to `local` or `FlexConnect`.
	       • The OS release that is installed on the AP is not compatible. The OS release must be MR1 or later.
	
	f. To display the list of APs that support Intelligent Capture, click the information (I) icon next to the **Not-Ready APs** tab.

Global - enable all capable APs	Allows you to enable the Anomaly Capture for all capable APs.

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

Use this procedure to view RF statistics and start and manage Spectrum Analysis data for a specific access point.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Health**.

The **Overall** health dashboard is displayed.

Step 2   Click the **Network Health** tab.

The **Network Health** window appears.

Step 3   Do one of the following:

- From the **Network Devices** dashlet, click the device name (hyperlinked identifier) for the AP to view the details for the AP.
- In the **Search** field (located at the top-right corner), enter the device name, IP address, or MAC address.

A 360° view of the AP appears.

Step 4   In the **Device 360** window, click **Intelligent Capture** at the top-right corner.

The **Intelligent Capture:** *AP Name* window appears.

Attention   If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the AP name, see Client or Access Point Unable to Send Intelligent Capture Data to Cisco DNA Center, on page 336 for more details.

Step 5   Click the **RF Statistics** tab to view details about RF statistics.

Note   If **AP Stats Capture** has not been enabled, enable it. See Enable and Manage Intelligent Capture for an Access Point, on page 329.

Step 6   In the **RF Statistics** tab you can do the following:

a)   Use the timeline to view the RF statistics for a given time and specify the scope of the data:

Timeline Slider	
Item	**Description**
1 hour drop-down list	Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour**, **3 hours**, and **5 hours**. Default is **1 hour**.
Timeline Slider	The timeline slider determines the time window of all data displayed. The timeline slider is color-coded to display the health of the AP. You can hover your cursor at a specific time to see details such as the device health score, system resources, and data plane.
	To adjust the timeline to a different time window, click the < and > buttons to the desired time window.
	For more customization of the timeline range, click and drag the boundary lines.

b)   Use the radio frequency selector under the timeline to filter the data that appears in the dashlets based on the frequency bands. Click the drop-down list and select **Radio 0 (2.4 GHz or 5 GHz)**, **Radio 1 (5 GHz)**, or **Radio 2 (6 GHz)** (depending on the number of radios supported).

c)   Use the dashlets to view the RF statistics details:

Note   You can do the following in the charts that are displayed in the dashlets:

- Hover your cursor over the charts to view details.

- Click and drag within the chart to zoom in on a period. To change the view to the default, click 🔍.

- Click the color-coded data types below the chart to disable or enable the data type that is displayed in the chart.

Dashlets	Description
Clients dashlet	Displays the number of clients using the AP. The data source is from the AP WLAN statistics.
Top Clients with Tx Failed Packets by SSID dashlet	Displays the list of SSIDs in the table. The data source for the table is from the AP WLAN statistics. The data source for the bar chart is from AP client statistics. Select an SSID to see the top clients with transmit failed packets for that SSID.
Channel Utilization dashlet	Displays the channel utilization percentage used by the AP and other wireless and non-wireless devices. The data source for the bar chart is from AP Radio Statistics.
Channel Utilization by this Radio dashlet	Displays the current channel utilization percentage used by the AP and a list of SSIDs, the number of clients connected to it, and the number of packets sent or received over the last 15 minutes for its clients. The data source for the table is from the AP WLAN statistics. The data source for the circle chart is from AP radio statistics.
Frame Count dashlet	Displays the number of management and data frames. The data source is from the AP radio statistics.
Frame Errors dashlet	Displays the number of transmit and receive errors. The data source is from the AP radio statistics.
Tx Power and Noise Floor dashlet	Displays the transmit power and noise floor. The data source is from the AP radio statistics.
Multicast/Broadcast Counter dashlet	Displays the multicast and broadcast counts for each SSID. The data source is from the AP WLAN statistics.

Step 7   Click the **Spectrum Analysis** tab.

Step 8   Click **Start Spectrum Analysis** to start a spectrum analysis session.

Note   - The spectrum analysis duration is 10 minutes.

- The maximum number of concurrent spectrum analysis sessions is 20.

Step 9   In the **Spectrum Analysis** tab you can do the following:

a) Use the timeline to view the spectrum analysis data for a given time and specify the scope of the data to display:

Timeline Slider	
Item	**Description**
1 hour drop-down list	Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour**, **3 hours**, and **5 hours**. Default is **1 hour**.
Timeline Slider	The timeline slider determines the time window of data that is displayed. The timeline slider is color-coded to display the health of the AP. You can hover your cursor at a specific time to see the details, such as the device health score, system resources, and data plane.
	For Spectrum Analysis, the time range is set to a 5-minute window.
	To adjust the timeline to a different time window, click the < and > buttons to the desired time window.
	Note The timeline can display data from up to two weeks in the past.
	Click and drag the boundary lines to view data for a specific time.

b) Use the radio frequency selector under the timeline to filter the data that appears in the charts based on the frequency bands. Click **2.4 GHz**, **5 GHz**, or **6 GHz**.

> **Note**   If **Radio Mode** and **Channel** (above the **Spectrum Analysis** charts) do not display any data, this indicates that the AP has no radios operating on the selected band. This occurs when an AP has both the client serving radios operating on **5 GHz**, while the radio frequency selector is set to **2.4 GHz**.
>
> For more details, see .

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

Spectrum Analysis Charts	
Item	**Description**
Top chart (Persistence)	This chart provides in real time the amplitude (power) and the channel frequency for each heard signal in the RF environment. The X axis represents the amplitude and the Y axis represents the channel frequency.
	The colors in the chart represent how many signals are heard at the same amplitude and channel frequency within the selected 5-minute time period:
	• Blue indicates a low number of overlapping signals (or signals heard at the same amplitude and frequency).
	• Red indicates a high number of overlapping signals.
	The intensity of the color increases (from blue > green > yellow > orange > red) as more signals are heard. As the lines in the chart overlap and intersect, they change color.
	The transparency of the colors represents the age of the signal data, with older data being more transparent.
	To view the RF environment in real time, click **Realtime FFT** (Fast Fourier Transform) to enable it. Enabling Realtime FFT limits the persistence chart to display "one" most recent data stream, rather than a collection of data streams from a 5-minute time period.
	To zoom in and view data for a specific range of channels, click and drag your mouse to select the range. The chart refreshes and displays data for the specific channels that you selected.
	To zoom out and view the entire chart, click the magnifying glass on the top-right corner.
Bottom chart (Waterfall)	This chart provides a time-wise interpretation of data. The chart provides the same information as the Persistence chart but in a different format. The X axis shows the time and the Y axis shows the channel frequency. The lines in the chart represent the exact order in which the events have occurred, which can enable you to troubleshoot the root cause if a problem occurs.
	The colors in the chart represent the amplitude. Blue indicates a low value (-100 dBm) and red indicates a high value (-20 dBm).

d) Use the **Interference and Duty Cycle** chart to view the following:

   • Detected interference and its severity:

      • Interference is plotted as a circle where the radius represents the bandwidth of the interference. The X axis represents the frequency in which the interference was heard on and the Y axis represent the severity.

      • Severity measures the impact of the interference and the range. Range is from 0, which indicates no impact, to 100, which indicates a huge impact.

      • The interference type is determined by its RF signature, which is identified by Cisco CleanAir Technology.

   • The duty cycle of each channel.

About Cisco AP Functionality During Spectrum Analysis

The Cisco Aironet 2800 Series, 3800 Series, and 4800 Series Access Points (APs) have dual band radios with flexible radio assignment (FRA) in slot 0. This FRA radio operates on 2.4 GHz, but can be assigned to operate on 5 GHz. Its mode can be changed to differ from the AP's operational mode. When you configure the AP's FRA radio to operate in 5 GHz, no client radios can operate in 2.4 GHz band.

Note Spectrum Analysis is *not supported* on the Aironet 1540 AP, Aironet 1800 Series APs, and Catalyst 9115 AP.

Note Verify that the APs have the correct software version installed. See the **Supported Cisco APs** table in the Supported Devices for Intelligent Capture, on page 315 topic.

Radio slot assignments for spectrum analysis are as follows:

Device Model	Spectrum Analysis Radio Slot Assignment
Aironet 2800 Series APs Aironet 3800 Series APs Aironet 1560 APs Catalyst IW6300 Heavy Duty Series APs Catalyst IW6300 Heavy Duty Series APs	Radio slots 0 and 1 are enabled.
Aironet 4800 Series APs Catalyst 9120 AP Catalyst 9130 APs	These APs have three radio slots. If data packet capture is running, radio slots 0 and 1 are enabled. If data packet capture is not running, radio slot 2 is enabled. **Note** AP spectrum analysis data is not displayed for the 2.4 GHz channel band. Also, if there is no AP radio serving the 2.4 GHz band, the **Radio Mode** and **Channel** fields are empty. This occurs if the FRA radio is set to operate in 5 GHz and packet capture is enabled.

Troubleshoot Intelligent Capture

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

Problem: Client or access point is unable to send Intelligent Capture data to Cisco DNA Center. The warning (⚠️) icon appears with the message **GRPC link is not ready (CONNECTING)**:

Background: In order for APs to send Intelligent Capture data to Cisco DNA Center, the Intelligent Capture port number on the Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller must be set to 32626. Typically, when the Catalyst 9800 Series Wireless Controller or wireless controller is discovered by Cisco DNA Center, the port number is automatically set to 32626.

However, there are some upgrade paths for Cisco DNA Center that can cause the port number from being properly set.

Solution: To resolve this issue, do the following:

1. Check that the Catalyst 9800 Series Wireless Controller or wireless controller has the Intelligent Capture server port number is set to 32626.

2. If the port number is not set to 32626, manually set it.

Trace the Path of a Device

About Path Trace

You can perform a path trace between two nodes in your network—a specified source device and a specified destination device. The two nodes can be a combination of wired or wireless hosts or Layer 3 interfaces or both. In addition, you can specify the protocol that the Cisco DNA Center controller should use to establish the path trace connection, either TCP or UDP.

When you initiate a path trace, the Cisco DNA Center controller reviews and collects network topology and routing data from the discovered devices. It then uses this data to calculate a path between the two hosts or Layer 3 interfaces, and displays the path in a path trace topology. The topology includes the path direction and the devices along the path, including their IP addresses. The display also shows the protocol of the devices along the path (**Switched**, **STP**, **ECMP**, **Routed**, **Trace Route**) or other source type.

Path Trace Known Limitations

Path trace has the following limitations and restrictions.

- Path trace between a fabric client and a nonfabric client is not supported.

- Path trace between two fabric clients over multi virtual routing and forwarding (VRF) virtual networks (VNs) is not supported.

- Path trace between two fabric clients over multi sites (domains) is not supported.

- Clients connected in the same fabric and same site where either edge switch is not part of the fabric is not supported.

- Path trace from a router's loopback interface is not supported.

- Overlapping IP addresses are not supported with or without fabric.

- For path trace to work on a Locator ID/Separation Protocol (LISP) fabric, make sure that the traffic is running and cache is available on the edge switches.

- Path trace in Cisco Adaptive Security Appliances (ASA) is not supported because Cisco ASA does not support CDP. It is not possible to identify the path through the Cisco ASA appliance.

- Path trace is not supported for the management interface in wireless controllers in untagged mode.

- Path trace for centralized Wireless Mobility Modes Asymmetric Mobility Tunneling is not supported.

- Path trace for Virtual Switching System (VSS), Multi-Link Aggregation Control Protocol (MLACP), or Virtual PortChannel (vPC) is not supported.

- Path trace for Equal-Cost Multi-Path Routing (ECMP) over Switched Virtual Interface (SVI) is not supported.

- Path trace is not supported on devices with NAT or firewall.

- Cisco Performance Routing (PfR) is not supported with DMVPN tunnels.

- Path trace that has VLAN ACLs (VACLs) enabled is not supported.

- For a Non Periodic Refresh (NPR) path scenario, after an upgrade, the controller does not refresh the path. Additionally, statistics collection stops. To continue statistics collection, you must initiate a new path request.

- Path trace from a host in a Hot Standby Router Protocol (HSRP) VLAN to a host in a non-HSRP VLAN that is connected to any of the HSRP routers is not supported.

- Object groups are not supported in an ACL trace.

- Port-channel Port Aggregation Protocol (PAgP) mode is not supported. Only LACP mode is supported.

- Applying a performance monitor configuration using Cisco DNA Center fails if there is a different performance monitor policy configuration on the interface. Remove the performance monitor configuration on the interface and resubmit the path trace request.

- Path trace for Performance Monitor statistics is not supported for Cisco ASR 1000 Series routers (Cisco IOS XE 16.3.1).

- Path trace for Performance Monitor statistics is not supported for the Cisco Catalyst 3850 Switch (Cisco IOS XE 16.2.x and 16.3.1).

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

- Path trace for wireless clients that use OTT in Cisco SD-Access fabric is not supported.

- Path trace from a Layer 2 switch is not supported.

- Cisco's Industrial Ethernet (IE) Switches are extended nodes as part of the SD-Access solution. Currently, path trace does not recognize extended nodes, so if a topology contains extended nodes, you will get an error message.

- Dual stack that has both IPv4 and IPv6 addresses for devices is not supported. If this occurs, an error message displays stating that the given address is unknown.

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

  - For a path trace request, Cisco DNA Center does not have the right egress virtual interface highlighted on any foreign wireless controller.

  - The path trace request does not highlight any ACLs applied on the foreign wireless controller.

> **Note** The workaround is to wait for the inventory cycle to complete.

Perform a Path Trace

The path trace feature works in a similar manner in all the devices. You can perform a path trace from the **Client 360** or **Device 360** window.

Before you begin

- Review the path trace known limitations. See Path Trace Known Limitations, on page 339.

- 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 25, Discover Your Network Using CDP, on page 23, or Discover Your Network Using LLDP, on page 26.

- Make sure that CDP is enabled in the devices.

Step 1 From the **Client 360** or **Device 360** window, in the **Path Trace** category, click **Run New Path Trace**.
The **Set up Path Trace** slide-in pane appears.

Step 2 Enter the source IP address, interface, and port number; and the destination IP address, interface, and port number.

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

Field	Action
Port (**optional**) field	Enter the port number of the host from which you want the trace to end.

Step 3   From the **Options** area do the following as appropriate:

Field	Action
Protocol drop-down list	(Optional) Choose either **tcp** or **udp**.
Live Traffic	Enable this toggle to **On** to capture the network packets traveling through select devices in real time as a .pcap file. **Max number of packets to capture** drop down list - Select the maximum number packets to be captured. **Note** **Refresh Every 30sec** toggle button gets disabled automatically when you enable **Live Traffic** toggle button and vice versa.
Refresh Every 30sec	(Optional) Set this toggle to **On** to configure the path trace topology to refresh every 30 seconds.
ACL Trace	(Optional) Set this toggle to **On** to display matched ACLs and the ACL result (Permit or Deny) for a specific traffic flow.

Include Stats options	(Optional) To configure the path trace to collect additional statistics, check the following check boxes as needed:
	
	  • **Device**: Collects and displays information, such as the device CPU and memory usage.
	
	  • **Interface**: Collects and displays information about the device interface.
	
	  • **QoS**: Collects and displays QoS information, such as collector-voice-egress, collector-broadcast-video-egress, collector-real-time-interactive-egress, and so on.

Step 4   Click **Start**.

The path trace topology appears. The IP addresses, protocol, and the time stamp indicating when the path trace was last updated display above the topology.

Step 5   In the path trace topology, you can do the following:

a)   Hover your cursor over a device to display the following information:

    • CPU utilization

    • Memory utilization

    • Average processing delay of ACLs, tunneling, and queues

    • Packet forward decision, which includes the number of packets forwarded and dropped and the drop reason

If **ACL Trace** is set to **On**, the ACL name and ACL result, such as permit or deny display.

If the 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.

Integrate Cisco CMX for Wireless Maps

About Cisco Connected Mobile Experiences Integration

Cisco DNA Center supports the integration of on-premises Connected Mobile Experiences (CMX) for wireless maps. With the CMX integration, you can get the exact location of your wireless clients, rogue access points and interferers on the floor map within the Cisco DNA Center user interface.

Depending on your requirements, you can create CMX settings either at the global level or at the site, building, or floor level. For a small enterprise, you can assign CMX at the global level, which is the parent node. All children inherit their settings from the parent node. For a medium enterprise, you can assign CMX at the building level, and for a large enterprise, you can assign CMX at the floor level.

Note CMX should be anonymized for security purposes.

Add a User for the Cisco CMX API Server

Before adding a Cisco CMX instance to Cisco DNA Center Network Settings, you must add a user for the Cisco CMX API server.

Step 1 SSH to Cisco CMX using a cmxadmin account. Enter the following command:

```
ssh -l cmxadmin (cmx-ip-address)
```

Step 2 Start the Cisco CMX API server. Enter the following command:

```
# cmxos apiserver start
```

Example
The following example shows how to start the Cisco CMX API server:

```
[root@server]# cmxos apiserver start
Starting CMX API Server...
```

Step 3   Add a user for the Cisco CMX API server. Enter the following command:

```
cmxos apiserver user add
```

At the password prompt, use the same password as the Cisco CMX web admin user password.

Example
```
The following example shows how to add a user for the Cisco CMX API server:
[root@server]# cmxos apiserver user add
Please enter the userid for the CMX API Server: user1
Please enter the password for the CMX API Server: password
Please re-enter the password for the CMX API Server: password
Restarting CMX API Server...
Stopping CMX API Server...
Starting CMX API Server...
Successfully updated userid/password and restarted the CMX API Server
```

What to do next

Create Cisco CMX settings in Cisco DNA Center. See Create Cisco CMX Settings, on page 346.

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 345.

Step 1   Click the menu icon (≡) and choose **System** > **Settings**.

Step 2   From the **External Services** section, click **DNA Spaces/CMX Servers**.

The **DNA Spaces/CMX Servers** window opens.

Step 3   From the **CMX Servers** table, click **Add**.

Step 4   Complete the fields in the **Add CMX Server** slide-in pane:

- **IP Address**: Enter the valid IP address of the CMX web GUI.

- **User Name**: Enter the CMX web GUI username.

- **Password**: Enter the password credentials.

- **SSH User Name**: Enter the CMX admin username.

- **SSH Password**: Enter the CMX admin password credentials.

Note   Make sure that CMX is reachable.

Step 5   Click **Add**.

The CMX server is added successfully.

Step 6   To assign a CMX server to a site, building, or a floor, click the menu icon and choose **Design** > **Network Settings**.

Step 7   Click the **Wireless** tab.

Step 8   From the left hierarchy tree, choose either **Global** or the required area, building, or floor.

Step 9   In the **DNA Spaces/CMX Servers** section, use the drop-down list, choose the CMX server.

Step 10   Click **Save**.

The **Create CMX Settings** window opens.

After the CMX is added, if you make any changes to the floor on the **Network Hierarchy** page, the changes are synchronized automatically with the CMX.

When the CMX is synced, Cisco DNA Center starts querying the CMX for the client location and displays the location on the floor map.

Step 11   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, hover your cursor over the ellipsis ••• next to the building or floor on which you made the changes in the left hierarchy tree, and then choose **Sync: DNA Spaces/CMX** to push the changes manually.

Step 13   To edit the CMX server details or delete a CMX server, do the following:

a)   Click the menu icon (≡) and choose **System** > **Settings**.

b)   From the **External Services** section, click **DNA Spaces/CMX Servers**.

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

d)   Select the CMX server that you want to delete and click **Delete**.

e)   Click **OK** to confirm the deletion.

Troubleshoot Cisco CMX

CMX Authentication Failure

- Check if you are able to log in to the CMX web UI with the credentials that you provided at the time of CMX settings creation on Cisco DNA Center.

- Check if you are able to log in to the CMX console using SSH.

- Check if you are able to exercise CMX REST APIs using the API Documentation link on the CMX UI.

Clients Do not Appear on the Floor Map

- Check if the Cisco Wireless Controller on the particular floor is configured with CMX and is active.

- Check if the CMX UI shows clients on the floor map.

- Use the Cisco DNA Center Maps API to list the clients on the floor: `curl -k -u <user>:<password> -X GET /api/v1/dna-maps-service/domains/<floor group id>/clients?associated=true`

C H A P T E R **23**

Reports

About Reports

You can utilize data from the Reports feature to derive insights into your network and its operation. By reporting this data in several formats and providing flexible scheduling and configuration options, both data and reports are easily customized to meet your operational needs.

For details about the Cisco DNA Center Reports, see the Cisco DNA Center Platform User Guide.

View Assurance Audit Logs

View Audit Logs for Assurance

Audit logs are created to capture critical activities, such as when configuration changes were requested, when the configuration changes were executed, and if errors occurred during the configuration. For Assurance, audit logs are provided when configuration changes are made to Intelligent Capture, Issue Thresholds, Sensors, and AI Network Analytics.

To access the audit logs, choose **Activities** > **Audit Logs**. For a detailed procedure, see the "View Audit Logs" topic in the *Cisco DNA Center Administrator Guide*.

For Assurance, the following data is captured in the audit logs:

Table 9: Audit Logs

Item	Description
Date and Time	Date and time the log was received or executed.
Description	A brief description explaining the audit log.
User	The user that requested or executed the change.

Intelligent Capture Audit Logs

For Intelligent Capture, audit logs are provided to capture the following configuration changes:

- Enable or disable AP Statistics, globally.

- Enable or disable AP Statistics for a set of individual APs.

- Enable or disable Anomaly Capture, globally.

- Enable and disable Anomaly Capture for a set of individual APs.

- Enable or disable Spectrum Analysis.

- Enable or disable Scheduled Capture.

- Enable or disable Live Capture.

• Enable or disable Data Packet Capture.

If any errors occurred during the configuration, that information is also provided in the audit logs.

Issue Threshold Audit Logs

For issue threshold, audit logs are provided to capture the following updates:

• Updates on site health.

• Updates on the health score.

• Updates on the issue settings.

Sensor Audit Logs

For sensors, audit logs are provided to capture the following configuration requests:

• Received request to add test suite.

• Received request to update test suite.

• Received request to delete test suite.

• Received request to update tests for certificate bundle.

• Received request to add test status.

AI Analytics Audit Logs

For AI Analytics, audit logs are provided to capture the following AI agent configuration changes:

• Agent onboarded.

• Agent restored.

• Agent reconfigured.

Related Documentation

Related Documentation

We recommend that you read the following documents relating to Cisco DNA Center.

For This Type of Information...	See This Document...
Release information, including new features, limitations, and open and resolved bugs.	*Cisco DNA Center Release Notes*
Installation and configuration of Cisco DNA Center, including postinstallation tasks.	*Cisco DNA Center Installation Guide*
Upgrade information for your current release of Cisco DNA Center.	*Cisco DNA Center Upgrade Guide*
Use of the Cisco DNA Center GUI and its applications.	*Cisco DNA Center User Guide*
Configuration of user accounts, security certificates, authentication and password policies, and backup and restore.	*Cisco DNA Center Administrator Guide*
Security features, hardening, and best practices to ensure a secure deployment.	*Cisco DNA Center Security Best Practices Guide*
Supported devices, such as routers, switches, wireless APs, and software releases.	*Cisco DNA Center Compatibility Matrix*
Hardware and software support for Cisco SD-Access.	*Cisco SD-Access Compatibility Matrix*
Use of the Cisco DNA Assurance GUI.	*Cisco DNA Assurance User Guide*
Use of the Cisco DNA Center platform GUI and its applications.	*Cisco DNA Center Platform User Guide*
Cisco DNA Center platform release information, including new features, deployment, and bugs.	*Cisco DNA Center Platform Release Notes*
Use of the Cisco Wide Area Bonjour Application GUI.	*Cisco Wide Area Bonjour Application User Guide*

For This Type of Information...	See This Document...
Use of the Stealthwatch Security Analytics Service on Cisco DNA Center.	*Cisco Stealthwatch Analytics Service User Guide*
Use of Rogue and aWIPS functionality to monitor threats in Cisco DNA Center.	*Cisco DNA Center Rogue Management and aWIPS Application Quick Start Guide*