NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

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

© 2018–2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

CHAPTER 1
New and Updated Features 1
What's New in Cisco DNA Assurance, Release 1.2.5 1

CHAPTER 2
Cisco DNA Assurance Overview 5
About Cisco DNA Assurance 5
About Assurance and Analytics 5
Log In 6
Log In for the First Time as a Network Administrator 7
Default Home Page 8
Start with Assurance 11

CHAPTER 3
Set Up Cisco DNA Center to Use Assurance 13
Basic Setup Workflow 13
Discover Devices 15
About Discovery 15
Discovery Prerequisites 16
Preferred Management IP Address 17
Discovery Configuration Guidelines and Limitations 17
Discover Your Network Using CDP 18
Discover Your Network Using an IP Address Range 23
Discover Your Network Using LLDP 27
Manage Discovery Jobs 33
Stop and Start a Discovery Job 33
Clone a Discovery Job 33
Delete a Discovery Job 33
View Discovery Job Information 34
View Data for Intelligent Capture 134
Set up Global Auto-Capture 135
Schedule Onboarding Packet Capture and Client RF Statistics 135
Monitor Intelligent Capture Details for a Client 136
Set Up NAM Integration 137
Monitor Intelligent Capture Details for a Device 139

CHAPTER 12
Manage Dashboards 141
About Dashboards 141
Create a Custom Dashboard 141
Create a Dashboard From a Template 143
View a Dashboard 144
Edit or Delete a Dashboard 144
Duplicate a Dashboard 145
Mark a Dashboard as a Favorite 145
Change the Position of a Dashlet 145

CHAPTER 13
Issues Detected by Assurance 147
About Issues 147
View Global Issues 147
View All Issues 148
Client Issues 150
Switch and Fabric Issues 161
Router Issues 163
Access Point and Wireless Controller Issues 164
Sensor Issues 165

CHAPTER 14
Schedule Reports 171
Overview 171
Sample and Schedule Reports 171

CHAPTER 15
Troubleshoot Cisco DNA Center Using Data Platform 175
About Data Platform 175
Troubleshoot Cisco DNA Center Using the Analytics Ops Center 176
New and Updated Features

- What's New in Cisco DNA Assurance, Release 1.2.5, on page 1

What's New in Cisco DNA Assurance, Release 1.2.5

Cisco DNA Assurance is an application that is available from Cisco DNA Center. Starting in Release 1.2.5, we are providing you with this user guide, which deals exclusively with Assurance.

- If you have an existing infrastructure (brownfield deployment), this user guide provides the basic tasks that you must do to set up and use the Assurance application.

- If you do not have an existing infrastructure and are starting from scratch (greenfield deployment), use this guide in conjunction with the Cisco Digital Network Architecture Center User Guide.

The table below summarizes the new and changed Assurance features that are included in Release 1.2.5.

Table 1: GUI Enhancements and Features in Assurance 1.2.5

<table>
<thead>
<tr>
<th>GUI Enhancements</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Health Enhancements</td>
<td>Total APs up and down</td>
</tr>
<tr>
<td></td>
<td>Top N APs by client count</td>
</tr>
<tr>
<td></td>
<td>Top N APs with high interference</td>
</tr>
<tr>
<td>GUI Enhancements</td>
<td>Features</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Device 360 Enhancements       | **AP 360**  
Client count chart per radio or AP over a selected time period  
Link errors chart per interface  
Ignore radios in monitor mode for health scores  
**Router 360**  
Application Experience category in Router 360 window  
**Switches**  
Near real-time update based on link down traps  
Insights—Fabric wireless controller node failed to reach Control Plane server |
| Client Health Enhancements    | Client health summary with new analytics charts  
Timeline slider with healthy client percentage chart |
| Client 360 Enhancements       | Near real-time update (onboarding events and new clients)  
Low health score indicated when you hover your cursor over the charts |
| Application Health Enhancements | Application usage and view details in side bar  
Timeline slider with health score trend line chart  
Site filter support |
| Application Experience 360 Enhancements | Exporter level breakdown |
| Path Trace Enhancements       | Matched ACLs in a specific traffic flow are displayed in the path trace  
Path trace on Layer 3 port channel is supported  
Path trace on Switch Virtual Interface (SVI) associated with a port channel is supported |
| Sensor Enhancements           | IPSLA test  
Speed test  
Floor reassignment for Cisco Aironet 1800s Active Sensors  
Workflow serviceability improvements |
| Intelligent Capture           | Real-time analytics  
Real-time and automated wireless client troubleshooting  
RF and spectrum analysis for AP(s) |
| Issues Enhancements           | Issue Catalog—Time selection slider and table with list of device or site information.  
Priority tags on every issue |
<table>
<thead>
<tr>
<th>GUI Enhancements</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue Insights</td>
<td>Time mismatch between Cisco Wireless Controller and Cisco DNA Center</td>
</tr>
<tr>
<td></td>
<td>AP noise and interference analytics for client timeout issues</td>
</tr>
<tr>
<td></td>
<td>Global client Issues display top OS, device type, and location</td>
</tr>
<tr>
<td>Client Data Sets and Reports</td>
<td>The following client data sets and reports are available after you deploy the Cisco DNA Center platform application:</td>
</tr>
<tr>
<td></td>
<td>Client summary</td>
</tr>
<tr>
<td></td>
<td>Top 10 locations by client count</td>
</tr>
<tr>
<td></td>
<td>Client detail</td>
</tr>
</tbody>
</table>
Cisco DNA Assurance Overview

• About Cisco DNA Assurance, on page 5
• About Assurance and Analytics, on page 5
• Log In, on page 6
• Log In for the First Time as a Network Administrator, on page 7
• Default Home Page, on page 8
• Start with Assurance, on page 11

About Cisco DNA Assurance

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

Assurance provides the following benefits:

• Provides actionable insights into network, client, and application related issues. These issues consist of basic and advanced correlation of multiple pieces of information, thus eliminating white noise and false positives.

• Provides both system-guided as well as self-guided troubleshooting. For a large number of issues, Assurance provides a system-guided approach, where multiple Key Performance Indicators (KPIs) are correlated, and the results from tests and sensors are used to determine the root cause of a problem, after which possible actions are provided to resolve the problem. The focus is on highlighting the issue rather than monitoring data. Quite frequently, Assurance performs the work of a Level 3 support engineer.

• Provides in-depth health scores for a network and its devices, clients, applications, and services. Client experience is assured both for access (onboarding) and connectivity.

About Assurance and Analytics

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

Assurance is a multipurpose, real-time, network data collection and analytics engine that can significantly increase the business potential of network data.
Assurance simplifies and abstracts the collection and analysis layers and offers a rich set of APIs along with a web interface. By using a single set of network data, Assurance powers a broad set of use cases. These advantages streamline the operational and network management overhead of collecting and analyzing network data, thereby allowing companies to effectively focus on their business goals.

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

The following figure and the information that follows describes the Assurance and Analytics architecture:

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

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

- **Data Visualization and Action**—Data is stored in databases and exposed through APIs to Assurance as well as other applications, such as Capacity Planning. Assurance is an open system that provides the following:
  - Collector and analytics pipeline SDKs
  - Time-series analysis
  - Graph data models and restful APIs
  - System management portal

Access Cisco DNA Center by entering its network IP address in your browser. For compatible browsers, see the [Cisco DNA Center Release Notes](https://www.cisco.com/dna-center/releases) for the version of Cisco DNA Center that you are using currently. This IP address connects to the external network and is configured during the Cisco DNA Center installation. For more information about installing and configuring Cisco DNA Center, see the [Cisco Digital Network Architecture Center Installation Guide](https://www.cisco.com/dna-center/installation-guide).
You should continuously use Cisco DNA Center to remain logged in. If you are inactive for too long, Cisco DNA Center logs you out of your session automatically.

---

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

https://server-ip

Example: https://192.0.2.1

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

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

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

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

---

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

If your user ID has the NETWORK-ADMIN-ROLE assigned, and no other user with the same role has logged in before, you will see a "Getting Started" wizard instead of the home page dashboard the first time you log in to Cisco DNA Center.

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

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

**Before you begin**

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

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

---

Cisco DNA Assurance User Guide, Release 1.2.5
• SNMP v2c credentials, including the read community string

---

**Step 1**
If you have not already done so, log in to Cisco DNA Center normally, as explained in Log In, on page 6.

**Step 2**
With the wizard displayed, click **Get Started**.

**Step 3**
In the fields on the following screens, enter the information listed in "Before You Begin" above.

Click **Save & Next** to continue, **Back** to return to the previous screen and revise your entries, or **Skip** to cancel the wizard and display the Cisco DNA Center home page.

**Step 4**
When you are finished, click **Begin Discovery**. Cisco DNA Center displays the home page, which slowly fills with network health information as discovery completes.

---

**Default Home Page**

After you log in, Cisco DNA Center displays its home page. The home page has three main areas: **Network Snapshot**, **Network Configuration**, and **Tools**.

The **Network Snapshot** area includes:

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

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

- **Profiles**: Provides the number of profiles discovered on your network. Clicking **Add New Profiles** takes you to the **Network Profiles** page.

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

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

The **Network Configuration** area includes:

- **Design**: Create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network.

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

- **Provision**: Prepare and configure devices, including adding devices to sites, assigning devices to the Cisco DNA Center inventory, deploying the required settings and policies, creating fabric domains, and adding devices to the fabric.
**Assurance**: Provide proactive and predictive actionable insights about the performance and health of the network infrastructure, applications, and end-user clients.

**Tools**: Use the **Tools** area to configure and manage your network.

*Figure 1: Home Page*

---

**Different Views of Home Page:**

**Getting Started**

When you log in to Cisco DNA Center for the first time, or when there are no devices in the system, you see the following message. Click **Discover** to discover new devices in your network.

In order to gather Assurance data and calculate your network health, we'll need to Discover or import your network devices.

![Import and Discover buttons](image)

**Day 0 Home Page**

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

When there are devices in the system, you see a network snapshot of discovered devices. Click any icons in the main areas to launch the corresponding application or tool.

In addition to the **Network Snapshot**, **Network Configuration**, and **Tool** icons, you can click any icons at the top-right corner of the home page to perform important common tasks:

- **Software Updates**: See a list of available software updates. Click the **Go to Software Updates** link to view Platform and App updates.

- **Applications icon**: Return to the Cisco DNA Center home page from any other page and access the applications and tools. You can do the same thing by clicking the Cisco DNA Center logo in the top-left corner of the home page.

- **Settings icon**: View audit logs, configure Cisco DNA Center system settings, see the Cisco DNA Center version you are using, and log out.

- **Notifications icon**: See recently scheduled tasks and other notifications.

Finally, you can click the following icons, which appear at the right side of every page in Cisco DNA Center:

- **Feedback** icon: Submit your comments and suggestions to Cisco's Cisco DNA Center product team.

- **Help icon**: Launch Cisco DNA Center's context-sensitive online help in a separate tab in your browser.

If you are new to Cisco DNA Center, see **Start with Assurance, on page 11** for tips and suggestions on how to begin.
By default, the login name you provided is displayed in the Welcome text. To change the name, click the name link; for example, admin. You are taken to Users > User Management, where you can edit the display name.

### Start with Assurance

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

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

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

- **New or nonexisting infrastructure**: If you do not have an existing infrastructure and are starting from scratch (greenfield deployment), design a network hierarchy. For information about designing a network hierarchy, see the Cisco Digital Network Architecture Center User Guide.
Set Up Cisco DNA Center to Use Assurance

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

- Basic Setup Workflow, on page 13
- Discover Devices, on page 15
- Design Network Hierarchy, on page 34
- Manage Inventory, on page 44
- Add a Device to a Site, on page 48
- Assurance and Cisco ISE Integration, on page 49
- Configure Syslog, SNMP Traps, and NetFlow Collector Servers Using Telemetry, on page 53
- Assurance Application, on page 59

Basic Setup Workflow

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

Note

Assurance is not supported over NATed connections to managed devices.

See the following illustration and the procedure that follows to understand the basic workflow.
Figure 2: Basic Workflow for Setting Up Cisco DNA Center to Use Assurance

Step 1
Install Cisco DNA Center.
See the Cisco Digital Network Architecture Center Installation Guide.
Step 2  
Do the following in any order:

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

  See Discover Your Network Using an IP Address Range, on page 23, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 27.

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

  See Create a Site in a Network Hierarchy, on page 35, Add Buildings, on page 36, and Add a Floor to a Building, on page 36.

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

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

See Display Information About Your Inventory, on page 45.

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

Step 4  
Add devices to sites.

See Add a Device to a Site, on page 48.

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

See Add, Position, and Delete APs, on page 37.

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

See Assurance and Cisco ISE Integration, on page 49.

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

See Configure Syslog, SNMP Traps, and NetFlow Collector Servers Using Telemetry, on page 53.

Step 8  
Start using the Assurance application.

See Assurance Application, on page 59.

---

### Discover Devices

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

### About Discovery

The Discovery feature scans the devices in your network and sends the list of discovered devices to Inventory.
The Discovery feature can also work with the Device Controllability feature to configure the required network settings on devices, if these settings are not already present on the device. For more information about Device Controllability, see the Cisco Digital Network Architecture Center Administrator Guide.

There are three ways for you to discover devices:

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

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

- **CDP Level** and **LLDP Level**—If you use CDP or LLDP as the Discovery method, you can set the CDP or LLDP level to indicate the number of hops from the seed device that you want to scan. The default, level 16, might take a long time on a large network. So, if fewer devices have to be discovered, you can set the level to a lower value.
- **Subnet Filters**—If you use an IP address range, you can specify devices in specific IP subnets for Discovery to ignore.
- **Preferred Management IP**—Whether you use CDP, LLDP, or an IP address range, you can specify whether you want Cisco DNA Center to add any of the device's IP addresses or only the device's loopback address.

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

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

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

**Discovery Prerequisites**

Before you run Discovery, complete the following minimum prerequisites:

- Understand what devices will be discovered by Cisco DNA Center by viewing the [Cisco DNA Center Supported Devices List](#).
- Ensure at least one SNMP credential is configured on your devices for use by Cisco DNA Center. At a minimum, this can be an SNMP v2C read credential.
• Configure SSH credentials on the devices you want Cisco DNA Center to discover and manage. Cisco DNA Center discovers and adds a device to its inventory if at least one of the following two criteria are met:
  • The account that is being used by Cisco DNA Center to SSH into your devices has privileged EXEC mode (level 15).
  • You configure the device’s enable password as part of the CLI credentials configured in the Discovery job. For more information, see Discovery Configuration Guidelines and Limitations, on page 17.

Preferred Management IP Address

When Cisco DNA Center discovers a device, it logs one of the device's IP addresses as the preferred management IP address for the device. You can configure Cisco DNA Center to log the device's loopback IP address as the preferred management IP address, provided the IP address is reachable from Cisco DNA Center.

If you choose to use a device's loopback IP address as the preferred management IP address, Cisco DNA Center determines the preferred management IP address as follows:

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

After a device is discovered, you can update the management IP address from the Inventory window. For more information, see Update Device Resync Interval, on page 44.

Discovery Configuration Guidelines and Limitations

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

• Configure the CLI username and password with privileged EXEC mode (level 15). This is the same CLI username and password that you configure in Cisco DNA Center for the Discovery function. Cisco DNA Center requires the highest access level to the device.

• Explicitly specify the transport protocols allowed on individual interfaces for both incoming and outgoing connections. Use the transport input and transport output commands for this configuration. For information about these commands, see the command reference document for the specific device type.

• Do not change the default login method for a device's console port and the VTY lines. Cisco DNA Center cannot discover devices that enforce the AAA login method.

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

You can discover devices using Cisco Discovery Protocol (CDP), an IP address range, or LLDP. This procedure shows you how to discover devices and hosts using CDP. For more information about the other discovery methods, see Discover Your Network Using an IP Address Range, on page 23 and Discover Your Network Using LLDP, on page 27.

Note

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

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

Before you begin

- Enable CDP on your network devices.

- Configure your network devices, as described in Discovery Prerequisites, on page 16.

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

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

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

Step 3  Expand the IP Address/Ranges 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)  From the Preferred Management IP drop-down list, choose either None or Use Loopback.
      
      Choose None to allow the device use any of its IP addresses or choose Use Loopback IP to specify the device's loopback interface IP address. 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 4

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

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

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name/Description</strong></td>
<td>Name or phrase that describes the CLI credentials.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Name that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Password that is used to log in to the CLI of the devices in your network.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the password again as confirmation.</td>
</tr>
<tr>
<td><strong>Enable Password</strong></td>
<td>Password used to move to a higher privilege level in the CLI.</td>
</tr>
<tr>
<td></td>
<td>For security reasons, enter the enable password again.</td>
</tr>
</tbody>
</table>

**Note**: Passwords are encrypted for security reasons and are not displayed in the configuration.

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

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

**Note**
Passwords are encrypted for security reasons and are not displayed in the configuration.

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

**Table 4: SNMPv3 Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name/Description</td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td>Username</td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td>Mode</td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td>Auth Type</td>
<td>Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types:</td>
</tr>
<tr>
<td>Auth Password</td>
<td>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</td>
</tr>
</tbody>
</table>

**Note**
- Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.
- Passwords are encrypted for security reasons and are not displayed in the configuration.
Privacy type. (Enabled if you select **AuthPriv** as a the authentication mode.) Choose one of the following privacy types:

- **DES**—DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **AES128**—CBC mode AES for encryption.
- **None**—No privacy.

**Privacy Password**

SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long.

**Note**

- Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.
- Passwords are encrypted for security reasons and are not displayed in the configuration.

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

**Table 5: SNMP Properties**

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

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

**Table 6: HTTP(S) Credentials**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are <strong>Read</strong> or <strong>Write</strong>.</td>
</tr>
</tbody>
</table>
You can configure up to 5 HTTPS read credentials:

- **Name/Description**—Name or description of the HTTPS credentials that you are adding.
- **Username**—Name used to authenticate the HTTPS connection.
- **Password**—Password used to authenticate the HTTPS connection.
- **Port**—Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**  
The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain < > @ ’ : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

You can configure up to 5 HTTPS write credentials:

- **Name/Description**—Name or description of the HTTPS credentials that you are adding.
- **Username**—Name used to authenticate the HTTPS connection.
- **Password**—Password used to authenticate the HTTPS connection.
- **Port**—Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**  
The password must contain at least one lower case, one upper case, one digit, and a special character and must not contain < > @ ’ : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

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

**Note**  
For an Evolved Converged Access (eCA) switch, enter the port number 830. If NETCONF is not already enabled on the devices, you can set up Device Controllability to configure NETCONF for you. For more information about Device Controllability, see the Cisco Digital Network Architecture Center Administrator Guide.

---

**Step 5**  
(Optional) To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

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

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

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

**Step 6**  
Click **Start**.

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

Discover Your Network Using an IP Address Range

You can discover devices using an IP address range, CDP, or LLDP. This procedure shows you how to discover devices and hosts using an IP address range. For more information about the other Discovery methods, see Discover Your Network Using CDP, on page 18 and Discover Your Network Using LLDP, on page 27.

Before you begin

Your devices must have the required device configurations, as described in Discovery Prerequisites, on page 16.

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

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

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

a) For Discovery Type, click Range.

b) In the IP Ranges field, 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) From the Preferred Management IP drop-down list, choose either None or Use Loopback.

Choose None to allow the device to use any of its IP addresses, or Use Loopback IP to specify the device's loopback interface IP address. 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 4  Expand the Credentials area and configure the credentials that you want to use for the Discovery job.

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

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

b) To add additional credentials, click Add Credentials.

c) To configure CLI credentials, configure the following fields:
Table 7: CLI Credentials

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

d) Click SNMP v2c and configure the following fields:

Table 8: SNMPv2c Credentials

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

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

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

**Table 10: SNMP Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Password</td>
<td>SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long.</td>
</tr>
<tr>
<td>Note</td>
<td>• Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.</td>
</tr>
<tr>
<td></td>
<td>• Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>

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


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

**Table 11: HTTP(S) Credentials**

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

- **Name/Description** — Name or description of the HTTPS credentials that you are adding.
- **Username** — Name used to authenticate the HTTPS connection.
- **Password** — Password used to authenticate the HTTPS connection.
- **Port** — Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**

The password must contain at least one lowercase, one uppercase, one digit, and one special character and must not contain `<`, `@`, `;`, `!` or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

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

**Note**

If NETCONF is not already enabled on the devices, you can set up Device Controllability to configure NETCONF for you. For more information about Device Controllability, see the Cisco Digital Network Architecture Center Administrator Guide.

**Step 5** (Optional) To configure the protocols that are to be used to connect with devices, expand the **Advanced** area and do the following tasks:

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

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

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

**Step 6**

Click **Start**.

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 for the selected discovery.

---

**Discover Your Network Using LLDP**

You can discover devices using Link Layer Discovery Protocol (LLDP), CDP, or an IP address range. This procedure shows you how to discover devices and hosts using LLDP. For more information about the other discovery methods, see **Discover Your Network Using CDP**, on page 18 and **Discover Your Network Using an IP Address Range**, on page 23.
Note

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

Before you begin

- Enable LLDP on your network devices.
- Configure your network devices, as described in Discovery Prerequisites, on page 16.
- Configure your network device's host IP address as the client IP address. (A host is an end-user device, such as a laptop computer or mobile device.)

Step 1

From the Cisco DNA Center home page, click Discovery.

Step 2

In the Discovery Name field, enter a name.

Step 3

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

a) For Discovery Type, click 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 $\rightarrow$.

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) From the Preferred Management IP drop-down list, choose either None or Use Loopback.

Choose None to allow the device use any of its IP addresses, or choose Use Loopback IP to specify the device's loopback interface IP address. 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 LLDP neighbor's IP address is reachable from Cisco DNA Center.

Step 4

Expand the Credentials area and configure the credentials that you want to use for the Discovery job.
Choose any of the global credentials that have already been created, or configure your own Discovery credentials. If you configure the credentials, you can choose to save them for future jobs by checking the **Save as global settings** checkbox.

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

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

c) For CLI credentials, configure the following fields:

*Table 12: CLI Credentials*

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

d) Click **SNMPv2c** and configure the following fields:

*Table 13: SNMPv2c Credentials*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>• <strong>Name/Description</strong>—Name or description of the SNMPv2c settings that you are adding.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Read Community</strong>—Read-only community string password used only to view SNMP information on the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>
e) (Optional) Click **SNMP v3** and configure the following fields:

### Table 14: SNMPv3 Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name/Description</strong></td>
<td>Name or description of the SNMPv3 settings that you are adding.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>Name associated with the SNMPv3 settings.</td>
</tr>
<tr>
<td><strong>Mode</strong></td>
<td>Security level that an SNMP message requires. Choose one of the following modes:</td>
</tr>
<tr>
<td></td>
<td>• <strong>noAuthNoPriv</strong>—Does not provide authentication or encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AuthNoPriv</strong>—Provides authentication, but does not provide encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AuthPriv</strong>—Provides both authentication and encryption.</td>
</tr>
<tr>
<td><strong>Auth Type</strong></td>
<td>Authentication type to be used. (Enabled if you select AuthPriv or AuthNoPriv as the authentication mode.) Choose one of the following authentication types:</td>
</tr>
<tr>
<td></td>
<td>• <strong>SHA</strong>—Authentication based on HMAC-SHA.</td>
</tr>
<tr>
<td></td>
<td>• <strong>MD5</strong>—Authentication based on HMAC-MD5.</td>
</tr>
<tr>
<td><strong>Auth Password</strong></td>
<td>SNMPv3 password used for gaining access to information from devices that use SNMPv3. These passwords (or passphrases) must be at least 8 characters in length.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>• Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.</td>
</tr>
<tr>
<td></td>
<td>• Passwords are encrypted for security reasons and are not displayed in the configuration.</td>
</tr>
</tbody>
</table>
Privacy Type  Privacy type. (Enabled if you select AuthPriv as a the authentication mode.) Choose one of the following privacy types:

- **DES**—DES 56-bit (DES-56) encryption in addition to authentication based on the CBC DES-56 standard.
- **AES128**—CBC mode AES for encryption.
- **None**—No privacy.

Privacy Password  SNMPv3 privacy password that is used to generate the secret key for encrypting messages that are exchanged with devices that support DES or AES128 encryption. Passwords (or passphrases) must be at least 8 characters long.

**Note**
- Some wireless controllers require that passwords (or passphrases) be at least 12 characters long. Be sure to check the minimum password requirements for your wireless controllers. Failure to ensure these required minimum character lengths for passwords results in devices not being discovered, monitored, or managed by Cisco DNA Center.
- Passwords are encrypted for security reasons and are not displayed in the configuration.

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

**Table 15: SNMP Properties**

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

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Specifies the kind of HTTPS credentials you are configuring. Valid types are Read or Write.</td>
</tr>
</tbody>
</table>
You can configure up to 5 HTTPS read credentials:

- **Name/Description**—Name or description of the HTTPS credentials that you are adding.
- **Username**—Name used to authenticate the HTTPS connection.
- **Password**—Password used to authenticate the HTTPS connection.
- **Port**—Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**
The password must contain at least one lowercase, one uppercase, one digit, and a special character and must not contain < > @ ; : ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

You can configure up to 5 HTTPS write credentials:

- **Name/Description**—Name or description of the HTTPS credentials that you are adding.
- **Username**—Name used to authenticate the HTTPS connection.
- **Password**—Password used to authenticate the HTTPS connection.
- **Port**—Number of the TCP/UDP port used for HTTPS traffic. The default is port number 443 (the well-known port for HTTPS).

**Note**
The password must contain at least one lowercase, one uppercase, one digit, and a special character and must not contain < > @ ; ; ! or spaces. For security reasons, enter the password again as confirmation. Passwords are encrypted for security reasons and are not displayed in the configuration.

---

**Step 5**  
(Optional) To configure the protocols to be used to connect with devices, expand the **Advanced** area and do the following tasks:

a) Click the names of the protocols that you want to use. A green check mark indicates that the protocol is selected. Valid protocols are **SSH** (default) and **Telnet**.

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

**Step 6**  
Click **Start**.

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

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

Stop and Start a Discovery Job

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

**Step 2**
To stop an active Discovery job, perform these steps:
- a) From the **Discoveries** pane, select the corresponding Discovery job.
- b) Click **Stop**.

**Step 3**
To restart an inactive Discovery job, perform these steps:
- a) From the **Discoveries** pane, select the corresponding Discovery job.
- b) Click **Start**.

Clone a Discovery Job

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

**Before you begin**
You should have run at least one Discovery job.

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

**Step 2**
From the **Discoveries** pane, select the Discovery job.

**Step 3**
Click **Clone**.

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

**Step 4**
(Optional) Change the name of the Discovery job.

**Step 5**
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.

**Before you begin**
You should have run at least one Discovery job.

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

**Step 2**
From the **Discoveries** pane, select the Discovery job that you want to delete.

**Step 3**
Click **Delete**.

**Step 4**
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 can also view the historical information about each Discovery job that was run, including information about the specific devices that were discovered or that failed to be discovered.

Before you begin

You should run at least one Discovery job.

Step 1

From the Cisco DNA Center home page, click Discovery.

Step 2

From the Discoveries pane, select the Discovery job. Alternatively, use the Search function to find a Discovery job by device IP address or name.

Step 3

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 status (completed or in progress), the time it was run, its duration, and whether any devices were discovered. You can click View to display discovery information per device, such as the status of the device and which device credentials were successful.

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

Design Network Hierarchy

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

Design a New Network Infrastructure

The Design area is where you create the structure and framework of your network, including the physical topology, network settings, and device type profiles that you can apply to devices throughout your network. Use the Design workflow if you do not already have an existing infrastructure. If you have an existing infrastructure, use the Discovery feature. For more information, see About Discovery, on page 15.

You can perform these tasks in the Design area:

Step 1

Create your network hierarchy.

Step 2

Define global network settings.

Step 3

Define network profiles.
About Network Hierarchy

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

- Areas or Sites do not have a physical address (for example, United States). You can think of areas as the largest element. Areas can contain buildings and subareas. For example, an area called United States can contain a subarea called California. And the subarea California can contain a subarea called San Jose.

- Buildings have physical address and contain floors and floor plans. When you create a building, you must specify a physical address and latitude and longitude coordinates. Buildings cannot contain areas. By creating buildings, you can apply settings to a specific area.

- Floors are within the building which comprises of cubicles, walled offices, wired closet, and so on. You can add floors only to buildings.

You can:

- Create a new network hierarchy. See Create a Site in a Network Hierarchy, on page 35.
- Upload an existing network hierarchy from Cisco Prime Infrastructure. See Upload an Existing Site Hierarchy, on page 39.

Guidelines for Preparing Image Files to Use Within Maps

- Use a graphical application that can save the map image files to any of these formats: jpg, .gif, .png, .dxf, and .dwg.

- Ensure that the dimension of an image is larger than the combined dimension of all the buildings and outside areas that you plan to add to the campus map.

- Map image files can be of any size. Cisco DNA Center imports the original image to its database at a full definition, but during display, it automatically resizes them to fit the workspace.

- Gather the horizontal and vertical dimensions of the site in feet or meters before importing. This helps you to specify these dimensions during map import.

Create a Site in a Network Hierarchy

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

Step 1 From the Cisco DNA Center home page, choose Design > Network Hierarchy.
A world map is displayed.
Set Up Cisco DNA Center to Use Assurance

Add Buildings

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

A world map is displayed.

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

Step 3 You can also upload an existing hierarchy. See Upload an Existing Site Hierarchy, on page 39.

Step 4 Enter a name for the building.

Step 5 In the Address text field, enter an address. If you are connected to the Internet, as you enter the address, the Design Application narrows down the known addresses to the one you enter. When you see that the correct address appears in the window, select it. When you select a known address, the Longitude and Latitude coordinates fields are automatically populated.

Step 6 Click Add.

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

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

Add a Floor to a Building

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

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

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

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

Step 4 Enter a name for the floor. The floor name has a 21-character limit. The floor name must start with a letter or a hyphen (-) and the string following the first character can include one or more of the following:

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

Step 6 You can drag a floor plan on to the map or upload a file. Cisco DNA Center supports the following file types: .jpg, .gif, .png, .dxf, and .dwg. After you import a map, make sure that you mark the Overlay Visibility as On (Floor > View Option > Overlays). By default, overlays are not displayed after you import a map.

Figure 3: Example of a Floor Plan

Step 7 Click Add.

---

Add, Position, and Delete APs

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

Make sure that you have Cisco APs in your inventory. If not, discover APs using the Discovery feature. See About Discovery, on page 15.

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

Step 2 In the left pane, select the floor.

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

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

Access points that are not assigned to any floors appear in the list.
### Step 5
On the **Add APs** window, check the check boxes of the access points to select APs in bulk, and click **Add Selected**. Alternatively click **Add** adjacent an access point.

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

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

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

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

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

    The AP is placed automatically as per the defined distance between the walls.

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

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

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

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

If a Cisco Connected Mobile Experiences (CMX) is synchronized with Cisco DNA Center, then you can view the location of clients on the heatmap. See **Create Cisco CMX Settings**, on page 130.

**Step 10** In the **Floor Elements** panel, next to **Access Points**, click **Delete**.

The **Delete APs** window appears which lists all the assigned and places access points, appears.

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

• To delete all the access points, click **Select All**, and click **Delete Selected**.

• To delete an access point from the floor, click the **Delete** icon.

• Use **Quick Filter** and search using the AP name, MAC address, Model, or Controller. The search is case-insensitive. The search result appears in the table. Click the **Delete** icon to delete the APs from the floor area.

---

**Manage Network Hierarchy**

**Upload an Existing Site Hierarchy**

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

**Step 1** From the Cisco DNA Center home page, choose **Design > Network Hierarchy**, and then click **Import > Import Sites**.

**Step 2** Drag and drop your CSV file, or navigate to where your CSV file is located, then click **Import** to import the Cisco Prime Infrastructure Groups CSV file.

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

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

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

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

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

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

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

The **Export Map Archive** wizard opens.

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

- **Map Information**—Click the **On or Off** button to include map information in the archive.

- **Calibration Information**—To export calibration information, click the **On or Off** button. Click the **Calibration Information for selected maps** or the **All Calibration Information** radio button. If you select **Calibration Information for selected maps**, the calibration information for the selected site maps is exported. If you select **All Calibration Information**, the calibration information for the selected map, along with additional calibration information that is available in the system, is also exported.

- In the **Sites** left pane, check one or more check boxes of the site, campus, building floor, or outdoor area that you want to export. Check the **Select All** check box to export all the maps.

**Step 4**  Click the **Generate Map Archive**. A message **Exporting data is in progress** is displayed.

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

**Step 5**  Click **Done**.

---

**Search the Network Hierarchy**

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

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

---

**Edit Sites**

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

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

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

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

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

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

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

**Step 4** Confirm the deletion.

---

# Edit a Building

**Step 1** Choose **Design > Network Hierarchy**.

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

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

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

---

# Delete Buildings

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

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

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

**Step 4** Confirm the deletion.

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

---

# Edit a Floor

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

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

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

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

---

# Monitor a Floor Map

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

- Use the **Find** feature located at the top-right corner of the floor map window to find specific floor elements such as APs, sensors, clients, and so on. The elements that match the search criteria are displayed on the
floor map along with a table in the right pane. When you hover your mouse over the table, it points to
the search element on the floor map with a connecting line.

- Click the icon at the top-right corner of the floor map window to:
  - Export a floor plan as a PDF.
  - Measure the distance on the floor map.
  - Set the scale to modify the floor dimensions.

- Click the icon at the bottom-right of the floor map window to zoom in on a location. The zooming
  levels depend upon the resolution of an image. A high-resolution image might provide more zoom levels.
  Each zoom level comprises of a different style map shown at different scales, each one showing the
  corresponding details. Some maps are of the same style, but at a smaller or larger scale.

- Click the icon to see a map with fewer details.

- Click the icon to view the map icon legend.

**Table 17: Map Icons**

<table>
<thead>
<tr>
<th>Floor Map Icons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AP Mode</strong></td>
<td></td>
</tr>
<tr>
<td>L</td>
<td>Local</td>
</tr>
<tr>
<td>F</td>
<td>FlexConnect</td>
</tr>
<tr>
<td>B</td>
<td>Bridge</td>
</tr>
<tr>
<td><strong>Health Score</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Good Health</td>
</tr>
<tr>
<td></td>
<td>Fair Health</td>
</tr>
<tr>
<td></td>
<td>Poor Health</td>
</tr>
<tr>
<td><strong>AP Status</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not covered by sensor</td>
</tr>
<tr>
<td></td>
<td>Covered by sensor</td>
</tr>
<tr>
<td>Floor Map Icons</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td><strong>Radio Band or Mode</strong></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>802.11 a/n/ac (5 GHZ)</td>
</tr>
<tr>
<td>2.4</td>
<td>802.11 b/g/n (2.4 GHZ)</td>
</tr>
<tr>
<td>n</td>
<td>802.11 a/b/g/n (2.4 GHZ)</td>
</tr>
<tr>
<td>Se</td>
<td>Sensor</td>
</tr>
<tr>
<td>M</td>
<td>Monitor 5 GHz</td>
</tr>
<tr>
<td>m</td>
<td>Monitor 2.4 GHz</td>
</tr>
<tr>
<td>Mx</td>
<td>Monitor XOR Mode</td>
</tr>
<tr>
<td>R</td>
<td>Rogue Detector</td>
</tr>
<tr>
<td>...</td>
<td>Other</td>
</tr>
<tr>
<td><strong>Radio Status</strong></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Ok</td>
</tr>
<tr>
<td>5</td>
<td>Minor Fault</td>
</tr>
<tr>
<td>5</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Admin Disable</td>
</tr>
<tr>
<td><strong>Icons</strong></td>
<td></td>
</tr>
<tr>
<td>🌟</td>
<td>Access Points</td>
</tr>
<tr>
<td>🌟</td>
<td>Sensor</td>
</tr>
<tr>
<td>🔹</td>
<td>Markers</td>
</tr>
</tbody>
</table>

**Rx Neighbors Line**

| – –             | 2.4 GHz                                      |
| – –             | 5 GHz                                        |
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. For more information about Device Controllability, see the Cisco Digital Network Architecture Center Administrator Guide.

Inventory uses the following protocols, as required:

• Link Layer Discovery Protocol (LLDP).
• IP Device Tracking (IPDT) or Switch Integrated Security Features (SISF). (IPDT or SISF must be enabled on the device.)
• LLDP Media End-point Discovery. (This protocol is used to discover IP phones and some servers.)
• Network Configuration Protocol (NETCONF). For a list of devices, see Discovery Prerequisites, on page 16.

After the initial discovery, Cisco DNA Center maintains the inventory by polling the devices at regular intervals. The default and minimum interval is every 25 minutes. However, you can change this interval up to 24 hours, as required for your network environment. For more information, see Update Device Resync Interval, on page 44. Polling occurs for each device, link, host, and interface. Only the devices that have been active for less than a day are displayed. This prevents stale device data, if any, from being displayed. On an average, polling 500 devices takes approximately 20 minutes.

Update Device Resync Interval

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

• You can enable and configure a custom resynchronization interval for a specific device.

• You can enable the preconfigured global resynchronization interval that is set for all the devices. (This setting is configured in the Settings > System Settings > Settings > Network Resync Interval window.

• You can disable resynchronization.

Before you begin

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

---

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

**Step 2**  
Select the devices that you want to update.

**Step 3**  
From the Actions drop-down list, choose Update Resync Interval.
The Update Resync Interval dialog box is displayed.

**Step 4** In Select Resync Option, click the radio button that corresponds to the type of resynchronization option you want to configure for the device. Valid choices are Custom, Global, and Disable.

**Step 5** If you chose Custom, in the Resync Interval (in Mins) field, enter the time interval (in minutes) between successive polling cycles. Valid values are from 25 to 1440 minutes (24 hours).

**Step 6** Click Update.

---

### Display Information About Your Inventory

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

**Before you begin**

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

### SUMMARY STEPS

1. From the Cisco DNA Center home page, click **Inventory**.

2. (Optional) To change the layout, click and choose one of the following layouts, or customize your own layout:

### DETAILED STEPS

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

*Table 18: Inventory, on page 46* describes the information that is available.
### Table 18: Inventory

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Name</strong></td>
<td>Name of the device. Click the name to display the Device Overview dialog box with the following information:</td>
</tr>
<tr>
<td></td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• IP Address</td>
</tr>
<tr>
<td></td>
<td>• MAC Address</td>
</tr>
<tr>
<td></td>
<td>• IOS Version</td>
</tr>
<tr>
<td></td>
<td>• Uptime</td>
</tr>
<tr>
<td></td>
<td>• Product Id</td>
</tr>
<tr>
<td></td>
<td>• Associated WLC</td>
</tr>
<tr>
<td></td>
<td>• Interface Name, MAC Address, and Status of the interfaces on the device.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>A device name that is displayed in red means that inventory has not polled the device and updated its information for more than 30 minutes.</td>
</tr>
<tr>
<td><strong>IP Address</strong></td>
<td>IP address of the device.</td>
</tr>
<tr>
<td><strong>Reachability Status</strong></td>
<td>The following is a list of the various statuses:</td>
</tr>
<tr>
<td></td>
<td>• Connecting—Cisco DNA Center is connecting to the device.</td>
</tr>
<tr>
<td></td>
<td>• Reachable—Cisco DNA Center has connected to the device and is able to execute Cisco commands using the CLI.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>A failure indicates that Cisco DNA Center is connected to the device, but is unable to execute Cisco commands using the CLI. This status usually indicates that the device is not a Cisco device.</td>
</tr>
<tr>
<td></td>
<td>• Authentication Failed—Cisco DNA Center has connected to the device, but is unable to determine what type of device it is.</td>
</tr>
<tr>
<td></td>
<td>• Unreachable—Cisco DNA Center is unable to connect to the device.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Sometimes a device is unreachable because the Discovery job does not have its credentials or the Discovery job has the wrong credentials. If you suspect this might be the case, run a new Discovery job and make sure to specify the device's correct credentials.</td>
</tr>
<tr>
<td><strong>MAC Address</strong></td>
<td>MAC address of the device.</td>
</tr>
<tr>
<td><strong>OS Version</strong></td>
<td>Cisco IOS software that is currently running on the device.</td>
</tr>
<tr>
<td><strong>Platform</strong></td>
<td>Cisco product part number.</td>
</tr>
<tr>
<td>Column</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Cisco device serial number.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Period of time that the device has been up and running.</td>
</tr>
</tbody>
</table>
| Config        | Configuration information. Click View to display detailed configuration information similar to what is displayed in the output of the show running-config command.  

**Note** This feature is not supported for access points (APs) and wireless controllers. Therefore, configuration data is not returned for these device types. |
| Device Role   | Role assigned to each discovered device during the scan process. The device role is used to identify and group devices according to their responsibilities and placement within the network. If Cisco DNA Center is unable to determine a device role, it sets the device role to Unknown.  

**Note** If you manually change the device role, the assignment remains static. Cisco DNA Center does not update the device role even if it detects a change during a subsequent device resynchronization.  
If required, you can use the drop-down list in this column to change the assigned device role. The following device roles are available:  
- Unknown  
- Access  
- Core  
- Distribution  
- Border Router |
| Site         | The site to which the device is assigned. For more information, see About Network Hierarchy, on page 35.                                      |
| Last Updated | Most recent date and time that Cisco DNA Center scanned the device and updated the database with new information about the device.            |
| Device Family | Group of related devices, such as routers, switches and hubs, or wireless controllers.                                                      |
| Device Series | Series number of the device, for example, Cisco Catalyst 4500 Series Switches.                                                              |
| Resync Interval | The polling interval for the device. This interval can be set globally in Settings or for a specific device in Inventory. For more information, see the Cisco Digital Network Architecture Center Administrator Guide. |
### Last Sync Status

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status of the last Discovery scan for the device:</td>
</tr>
<tr>
<td>• Managed — Device is in a fully managed state.</td>
</tr>
<tr>
<td>• Partial Collection Failure — Device is in a partial collected state and not all the inventory information has been collected. Move the cursor over the Information (i) icon to display additional information about the failure.</td>
</tr>
<tr>
<td>• Unreachable — Device cannot be reached and no inventory information was collected due to device connectivity issues. This condition occurs when periodic collection takes place.</td>
</tr>
<tr>
<td>• Wrong Credentials — If device credentials are changed after adding the device to the inventory, this condition is noted.</td>
</tr>
<tr>
<td>• In Progress — Inventory collection is occurring.</td>
</tr>
</tbody>
</table>

---

### Step 2

(Optional) To change the layout, click and choose one of the following layouts, or customize your own layout:

- **Status** — Layout shows the Device Name, IP Address, Reachability Status, Uptime, Last Updated Time, Poller Time, and Last Inventory Collection Status.
- **Hardware** — Layout shows the Device Name, IP Address, MAC Address, IOS/Firmware, Platform, Serial Number, Last Inventory Collection Status, Config, and Device Family.
- **Tagging** — Layout shows the Device Name, IP Address, MAC Address, Config, Device Role, Location, and Device Tag.

---

### Add a Device to a Site

**Step 1**
From the Cisco DNA Center home page, click **Provision**.
The Inventory page displays the device information gathered during the Discovery process.

**Step 2**
Check the check box next to the device or devices that you want to associate to a site.

**Step 3**
From the **Action** menu, choose **Add to Site**.

**Step 4**
In the **Find Site** field, enter the name of the site to which you want to associate the device. If you selected multiple devices to add to the same site, click **All Same Site**.

**Step 5**
Click **Assign**.

It takes approximately 15 minutes for devices to start plotting data on Assurance pages.
Assurance and Cisco ISE Integration

If your network uses Cisco ISE for user authentication, you can configure Assurance for Cisco ISE integration. This will allow you to see more information about wired clients, such as the username and operating system, in Assurance. Do the following:

1. Generate keystore file. See Generate the Keystore File, on page 49.
2. Generate truststore file. See Generate the Truststore File, on page 50.

Generate the Keystore File

Use this procedure to generate the keystore file. The keystore.jks file that is generated contains certificates, which Cisco DNA Center uses to communicate with Cisco ISE.

Before you begin

You must have Java Keytool installed to complete this procedure.

Step 1
Log in to Cisco ISE.

Step 2
From the Cisco ISE home page, choose Administration > pxGrid Services > Certificates.

The Generate pxGrid Certificates window opens.

Step 3
Do the following:

a) From the I want to drop-down list, choose Generate cert (without certificate signing request).

b) In the Common Name (CN) field, enter the name of the Cisco DNA Center server, including domain name.

c) From the Subject Alternative Name (SAN) drop-down list, choose IP address, and then enter the Cisco DNA Center IP address in the field provided.

d) From the Certificate Download Format drop-down list, choose PKCS format (including certificate chain; one file for both the certificate name and key).

e) In the Certificate Password field, enter a unique password.

f) In the Confirm Password field, enter the password again.

Save this password. You will need to use this password when you configure Assurance for Cisco ISE integration.

g) Click Create.

A zip file is generated.

h) Extract the files from the zip file.

Step 4
From a terminal prompt, do the following:

a) Go to the directory where you extracted the files; for example:

$ cd /home/user/certificate

b) Enter the following command:

keytool -v -list -storetype pkcs12 -keystore filename -storepass certificate-password | grep –i alias
Example

```
$ keytool -v -list -storetype pkcs12 -keystore cisco-dna-center.cisco.com_192.168.0.1.p12 -storepass Cisco123 | grep -i alias
Alias name: cisco-dna-center.cisco.com_192.168.0.1
```

An alias name is generated.

c) Copy the alias name.
d) Enter the following command:

```
keytool -importkeystore -srckeystore filename -srcstoretype pkcs12 -srcalias alias name -destkeystore keystore.jks -deststoretype jks -deststorepass certificate-password -destalias Keystore
```

Example

```
```

e) At the **Enter the source keystore password:** prompt, enter the Certificate Password that you entered in **Step 3 e.**

The keystore.jks file is created in the same folder where you extracted the files. The keystore.jks file that is generated contains certificates, which Cisco DNA Center uses to communicate with Cisco ISE.

---

**What to do next**

Do the following:

- Generate the truststore file. See *Generate the Truststore File*, on page 50.
- Configure Assurance for Cisco ISE integration. See *Configure Assurance for Cisco ISE Integration*, on page 52.

**Generate the Truststore File**

Use this procedure to generate the truststore file. The truststore.jks keystore file that is generated contains Cisco ISE certificates, which allow Cisco DNA Center to validate the Cisco ISE server in all communications.

**Before you begin**

Make sure you have generated the keystore file. See *Generate the Keystore File*, on page 49.

You must have Java Keytool installed to complete this procedure.

---

**Step 1**

Log in to Cisco ISE.

**Step 2**

From the Cisco ISE home page, choose **Administration > pxGrid Services > Certificates**.

The *Generate pxGrid Certificates* window opens.

**Step 3**

Do the following:
a) From the I want to drop-down list, choose Download Root Certificate Chain.
b) In the Host Name field, enter a hostname.
c) From the Certificate Download Format drop-down list, choose Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKSCB format (including certificate chain).
d) Click Create.
   A zip file is generated.
e) Extract the four files from the zip file.

**Step 4**

From a terminal prompt, do the following:
a) Go to the directory where you extracted the files; for example:

```
$ cd /home/user/certificate
```
b) Enter the following command:

```
keytool -importcert -file filename -keystore truststore.jks -alias filename-without-extension
```
c) At the Enter the keystore password: prompt, enter the certificate password that you created when you generated the keystore file. See Generate the Keystore File, on page 49.
d) At the Re-enter the new password: prompt, enter the password to confirm it.
e) At the Trust this certificate? [no]: prompt, enter yes.

The certificate is added to the keystore. The truststore.jks keystore file that is generated contains Cisco ISE certificates, which allow Cisco DNA Center to validate the Cisco ISE server in all communications.

f) Repeat Step 4 for each of the extracted files.

The truststore.jks file is created in the same folder where you extracted the files. The Cisco ISE server certificate chain is added to the truststore.jks file.

**Example**

```
$ keytool -importcert -file CertificateServicesEndpointSubCA-ise-01_.cer -keystore truststore.jks -alias CertificateServicesEndpointSubCA-ise-01_
Enter keystore password: 
Re-enter new password: 
Owner: CN=Certificate Services Endpoint Sub CA - ise-01 
Issuer: CN=Certificate Services Node CA - ise-01 
Serial number: 9a91699bf1546c19e8cc43fb466b62 
Valid from: Sat Sep 16 11:59:43 PDT 2017 until: Fri Sep 17 11:59:40 PDT 2027 
Certificate fingerprints: 
   SHA256: 
Signature algorithm name: SHA256withRSA 
Subject Public Key Algorithm: 4096-bit RSA k 
Version: 3 

Extensions: 
   #1: ObjectID: 2.5.29.35 Criticality=false 
   AuthorityKeyIdentifier [ 
      KeyIdentifier [ 
         0000: 5A 8A 8D 1B 32 3B 41 31 93 BF 12 E6 53 44 9E 52 Z...2;A1....SD.R 
         0010: 07 0E F1 E2 .... 
      ] 
      [CN=Certificate Services Root CA - ise-01] 
      SerialNumber: [ 332cc5aa 64le4b8a a6b0cf67 a0ac24bd ] 
   ] 
   #2: ObjectID: 2.5.29.19 Criticality=true 
   BasicConstraints:
```

---

Cisco DNA Assurance User Guide, Release 1.2.5
CA:true
PathLen:2147483647
}

#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [ ]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [ ]

Trust this certificate? [no]: yes
Certificate was added to keystore

What to do next
Configure Assurance for Cisco ISE integration. See Configure Assurance for Cisco ISE Integration, on page 52.

Configure Assurance for Cisco ISE Integration

Use this procedure for wired clients.

Before you begin
• Make sure you have generated the keystore file. See Generate the Keystore File, on page 49.
• Make sure you have generated the truststore file. See Generate the Truststore File, on page 50.

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

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

Step 3 Click + Add.
The ISE Collector Configuration window appears.

Step 4 Do the following:
a) In the ISE Service IP Address field, enter the IP address of the Cisco ISE primary pxgrid node.
b) In the Username field, enter the Cisco ISE primary pxgrid node username.
c) In the Password field, enter the Cisco ISE primary pxgrid node password.
d) From the Truststore File area, click Browse, and then upload the truststore file.
e) In the Truststore Passphrase field, enter the certificate password.
f) From the Keystore File area, click Browse, and then upload the keystore file.
g) In the Keystore Passphrase field, enter the certificate password.
You created the certificate password when you generated the keystore file.

h) (Optional) Check the Anonymize check box if you want to hide the username. In the Salt field, enter the Salt string for the username.

When you check the Anonymize check box, the user ID in the Client Health window appears scrambled.

i) In the Subscriber Name field, enter the name of the pxGrid subscriber.

j) In the Configuration Name field, enter a unique name for the Cisco ISE configuration.

k) Click Save Configuration.

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

Step 1 Configure the IP address for the syslog, SNMP, and NetFlow Collector servers. Do the following:

a) From the Cisco DNA Center home page, choose Design > Network Settings > Network.

b) In the Syslog Server field, enter the IP address of a syslog server.

c) In the SNMP Server field, enter the IP address of an SNMP server.

d) Apply Telemetry on the router for maximum visibility. Do the following:

   • Click Network Telemetry.
   
   • Click the Site View tab. A list of devices is displayed.
   
   • Check the check box adjacent to the router.
   
   • From the Actions drop-down list, choose Maximal Visibility.

 e) (Optional) To add a NetFlow Collector server, click Add Servers.

   The Add Servers window opens.

   1. Check the check box adjacent to NetFlow Collector Server. The NetFlow Collector server is added to the Network page.

   2. In the NetFlow Collector Server area, enter the IP address and port number of the NetFlow Collector server.

 f) Click Save.

Step 2 Add the device to a site so that the configuration is pushed from Cisco DNA Center to the devices. See Add a Device to a Site, on page 48.

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

crypto pki trustpoint Cisco-DNA-Center-CA
enrollment mode ra
enrollment terminal
usage ssl-client
revocation-check crl none
!
!
crypto pki certificate chain Cisco-DNA-Center-CA
Set Up Cisco DNA Center to Use Assurance

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

certificate ca 009156FDDCC160F24A 0201009F 9156FDDC C160F24A 300D0609 2A864886
F7000011 0B050030 12311030 0B060355 04030C07 6B756265 2D636130 1B1700D31
3B033530 33303035 392325A 170D3231 30313237 30303539 32335A30 12311030 020E0335 04030C07 6B756265 2D636130 82012230 D06092A 864886F7 D010101
05000382 010F0030 82010A02 8201100 D04771B0 47DF3C65 26AF54CB 32D606B0
CB9C6023 8C66FDDD 5E263A40 715F506D A3F2BF13 3799A1C C79777A9 1800424F
5FE5C49C 5694E6E2 A53FEE15 8ACA186 161A8D88 D442F66 BD9D3142 743D20BA
31DF43A5 E46E5E0B EEAC91B9 6298E01A 80622500 9D31B15 9F0D4E18 121C2726
69B7D768 EDAC319 7CBBF68C 137A5676 8EE7D5C5 71B34592 CAD54B89 590DC27A
A8172A76 104COBE5 1E0D100C 26E49C5B 734E5C9F 045E2E28 36937FSE 48619IC3
656678C9 9393B8B6 C0674594 9194EF4E C2B4845E IACCEB3F 82FEDC08 1548136C
53015248 0F8BD8EA 3F42281B 79A3183A 22E76AAB 20D91016 94CC9339 BF2F94CA
3D343E2F 8CC63BAA 453D35FEB 670C9F6B 02030100 01A55030 4B301D06 03551DOE
04150414 63528371 86225027 1A79B16E D2645368 929946CO 301F0603 551D2034
18016018 14635283 71862250 271A79B1 6E266453 68929A96 C0300C06 03551DD3
04053503 010FP0 0D06092A 864886F7 D01010B 05000382 0101009F 5755D9B9
6C460E8B 892A32F2 450AEEFB 57CD41AA 8EC7CD3D ECE78771 F3AD1CA2 76444620
90CB088B BE07A2ED A2D13325 019568BB F1FE9EAC 123A6A7F C81277D5 74556B3B
4BBDBDE9 785EB7CD 581A95F0 8306101D 54AE51D0 02DB7F32 C210A1E4 449A1F57
02815C71 E8A5C3C3 1828B08D 4C3CE370 1F4EB867 58A9E12A 9E2E106A 87F43E69
37234473 F0081787 733CA176 E5807A00 158F6501 E1B45537 17E3F2BE BBC5200D
C54EB66C B18A30F1 AC4D12AE 809DFF80 B28223E18 18C95395 23A13FA8 45D8C79D
013A80F7 C926F2F8 6DF258AD 86E70BE6 1426B072 3F31BAG8 14F4CAF5 FC039912
E286A1CF 5F2EC9C6 E00B820B 3AF84E3F 32C501F3 5E71A656 BEABE3
quit
interface GigabitEthernet1/0/2
ip device tracking maximum 10

interface GigabitEthernet1/0/3
ip device tracking maximum 10

flow exporter 10.4.48.218
destination 10.4.48.218

snmp-server community cisco RO
snmp-server community cisco123 RW
logging host 7.7.7.7

snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps flowmon
snmp-server enable traps transceiver all
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps rf
snmp-server enable traps memory
snmp-server enable traps wireless bsnMobileStation bsnAccessPoint bsnRogue bsn80211Security bsnAutoRF bsnGeneral SI mobility mfp RRM AP rogue client
snmp-server enable traps cpu threshold
snmp-server enable traps tty
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps cisco-specific state-change nssa-trans-change
snmp-server enable traps cisco-specific state-change shamlink interface
snmp-server enable traps cisco-specific state-change shamlink neighbor
snmp-server enable traps cisco-specific errors
snmp-server enable traps cisco-specific retransmit
snmp-server enable traps cisco-specific lsa
snmp-server enable traps auth-framework sec-violation
Example of Router Syslog, SNMP Traps, and Netflow Collector and Other Configurations

crypto pki trustpoint Cisco-DNA-Center-CA
enrollment mode ra
Configure Syslog, SNMP Traps, and NetFlow Collector Servers Using Telemetry

Set Up Cisco DNA Center to Use Assurance

enrollment terminal
usage ssl-client
revocation-check crl none
!
crypto pki certificate chain Cisco-DNA-Center-CA
certificate ca 00D97DCBDFA3EB517E
308202F7 308201DF 7B1B251F 353CB489 A049FB68 00865F21 C15E14B5 D5EFF90C
8878BCB1 97F49E19 466EB524 0B1700F2 4B31CDA3 1800ED5D FFF4D29F FE953514
DADD2B46 977BACD8 44FCD1AD 9042BE47 11ED9E29 97D9B4C9 E51C37C7 98AE61B0
382540AB F4417FPB A2B8095E 5236D3C6 47052F02 E2E23A46 564D7104 4F8F9098
C15B5FB3 C6ED2108 DA04C6B0 7E9A8EE5 036F9113 575C1567 97EEC40A AA53E91A
7E4E2419 D909E031 4E40F561 F766A4E2 7B6B4281 E95A87BA 01F6A42C 1EF040BD
97358BEB 9A9BC46F C17D3DE3 FA181F4F 41B84392 4E546A9E 3986D125 4B2DD897
6D5CD7AF 6E3425A8 2CF1BA48 DAA5C121 02030100 01A35030 4E301D00 0351510E
04160414 A811B663 0573E872 B4913BEF 69A2A405 9A92D2F5 301F0603 551D2304
1B301680 1A4811B6 630573E8 72B4913B EF698A24 059A92D2 F5300C06 0351510E
04053003 0101FF30 006D092A 864886F7 0D01010B 059A92D2 F5300C06 0351510E
B47E806D 57E55F78 185F566A 1373E05E FB381F07 0F506852 A3DF1048 AB3DF02C
2CE40F77 8251F171 18826E71 08B4D025 469A4A48 D13B4FCF 1482B0A1 6EC6D07F
EB03C989 A6BB99C3 64981957 DD48E0E5 60DFEF22 E4689B7 7BB9B1A4 4C4B319
1A21C571 804AEC36 BEC14CF8 78D1C133 E65B5D18 F4E310B6 3353EF73 511189CF
CF47C243 8D40A0B3 738BB94E 6E434F74 D203DE99 009E6858 B25DC9C7 08CAF030
AE7A68C6 F9BC311C 9FCFED0E 75625B07 602E1369 738BAC07 7AFB3DA4 8E2F4861
FAC5B688 0FB24D79 3B16EB38 3A39BB2 8AD8566B 16883040 A51455C5 826E61BF
AEP6EBE91 12F420B8 8BC9FC28 3A12B3EE 7EDFBA7B 588C355C D94B29
quit
!
flow exporter 10.4.48.218
destination 10.4.48.218
!
snmp-server community cisco RO
snmp-server community cisco123 RW
!
logging host 7.7.7.7
snmp-server enable traps smtp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps pfr
snmp-server enable traps flowmon
snmp-server enable traps ds1
snmp-server enable traps entity-perf throughput-notif	snmp-server enable traps ds3
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps elgrp
snmp-server enable traps caso
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nsaa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps license
snmp-server enable traps smart-license
snmp-server enable traps resource-failure peer-state-change peer-fib-state-change inconsistency
snmp-server enable traps memory bufferpeak
Set Up Cisco DNA Center to Use Assurance

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

```plaintext
cisco-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps dsp video-usage
snmp-server enable traps dsp video-out-of-resource
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ip local pool
snmp-server enable traps ppoe
snmp-server enable traps cpu threshold
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps atm subif
snmp-server enable traps pk1
snmp-server enable traps ethernet evc status create delete
snmp-server enable traps ether-oam
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps entity-state
snmp-server enable traps entity-qfp mem-res-thresh throughput-notif
snmp-server enable traps addalline
snmp-server enable traps flash insertion removal lowspace
snmp-server enable traps srp
snmp-server enable traps entity-diag boot-up-fail hm-test-recover hm-thresh-reached scheduled-test-fail
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps cnpd
snmp-server enable traps bfd
snmp-server enable traps otn
snmp-server enable traps ipsla
snmp-server enable traps sonet
snmp-server enable traps dslaw
snmp-server enable traps resource-policy
snmp-server enable traps stpx inconsistency root-inconsistency loop-inconsistency
snmp-server enable traps c3g
snmp-server enable traps LTE
snmp-server enable traps vtp
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps firewall serverstatus
snmp-server enable traps trustsec-xsp conn-srcaddr-err msg-parse-err conn-config-err binding-err
snmp-server enable traps conn-up conn-down binding-expn-fail oper-nodeid-change binding-conflict
snmp-server enable traps lisp
snmp-server enable traps aaa_server
snmp-server enable traps dhcp
snmp-server enable traps auth-framework sec-violation
snmp-server enable traps pw vc
snmp-server enable traps mpls rfc 1dp
snmp-server enable traps mpls ldp
snmp-server enable traps mpls rfc traffic-eng
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps rsvp
```
Configure Syslog, SNMP Traps, and NetFlow Collector Servers Using Telemetry

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

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

config network assurance server idtoken 1 6b5af7c9808a0b1b7824fc9a801b5478
de751722396b0fe0b221b3be71f3a94ef2fe0716 16 88664b59c40e1f1f2ffbf14097897ed620000000
```
config network assurance server url https://10.4.48.132
config network assurance on-change enable

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

config trapflags client enhanced-802.11-deauthenticate enable
config trapflags client enhanced-802.11-associate enable
config trapflags client max-warning-threshold enable
config trapflags client 802.11-authfail disable
config trapflags client 802.11-associate disable
config trapflags client 802.11-disassociate disable
config trapflags client authentication disable
config trapflags client webauthuserlogout enable
config trapflags client 802.11-deauthenticate disable
config trapflags client neighborclientsignal disable
config trapflags client webauthuserlogin enable
config trapflags client 802.11-assocfail disable
config trapflags client excluded enable
config trapflags client enhanced-802.11-sts enable
config trapflags client enhanced-authentication enable
config trapflags client nac-alert enable
config trapflags client enhanced-802.11-disassociate-stats disable

---

**Assurance Application**

To access the Assurance application, log in to Cisco DNA Center, and then from the home page, click **Assurance**.

**Note**

Before you begin using the Assurance application, you must configure it. See *Basic Setup Workflow, on page 13.*

Use the Assurance application to do the following:

<table>
<thead>
<tr>
<th>Task</th>
<th>Navigation</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get a global view of your entire enterprise, which includes network and clients.</td>
<td>Assurance landing page</td>
<td>See <em>Monitor and Troubleshoot the Overall Health of Your Enterprise, on page 61.</em></td>
</tr>
<tr>
<td>Get a global view of your entire network, which includes routers, switches, access points, and wireless controllers.</td>
<td>Assurance &gt; Health &gt; Network</td>
<td>See <em>Monitor and Troubleshoot the Health of Your Network, on page 65.</em></td>
</tr>
<tr>
<td>Task</td>
<td>Navigation</td>
<td>Reference</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Get an individual 360° view of a specific network element (router, switch, access point, or wireless controller).</td>
<td><strong>Assurance &gt; Health &gt; Network.</strong> In the Network Devices table &gt; <strong>Device</strong> column, click the device name to display the <strong>Device 360</strong> window.</td>
<td>See Monitor and Troubleshoot the Health of a Device, on page 71.</td>
</tr>
<tr>
<td>Get a global view of all wired and wireless clients.</td>
<td><strong>Assurance &gt; Health &gt; Client</strong></td>
<td>See Monitor and Troubleshoot the Health of All Client Devices, on page 85.</td>
</tr>
<tr>
<td>Get a 360° view of a specific client.</td>
<td><strong>Assurance &gt; Health &gt; Client</strong>. In the Client Devices table, click the MAC address to display the <strong>Client 360</strong> window.</td>
<td>See Monitor and Troubleshoot the Health of a Client Device, on page 92.</td>
</tr>
<tr>
<td>Get a 360° view of a specific application.</td>
<td><strong>Assurance &gt; Health &gt; Application</strong>. In the Applications table, click the name of an application to display the <strong>Application 360</strong> window.</td>
<td>See Monitor the Health of All Applications, on page 109.</td>
</tr>
<tr>
<td>Get a 360° view of a specific application.</td>
<td><strong>Assurance &gt; Health &gt; Application</strong>. In the Applications table, click the name of an application to display the <strong>Application 360</strong> window.</td>
<td>See Monitor the Health of an Application, on page 112.</td>
</tr>
<tr>
<td>Manage sensor-driven tests.</td>
<td><strong>Assurance &gt; Sensor Management</strong></td>
<td>See Manage Sensors and Sensor-Driven Tests, on page 117.</td>
</tr>
<tr>
<td>Manage and create custom dashboards.</td>
<td><strong>Assurance &gt; Dashboards &gt; Dashboard Library</strong></td>
<td>See Manage Dashboards, on page 141.</td>
</tr>
<tr>
<td>Display and troubleshoot issues.</td>
<td>Global Issues—<strong>Assurance &gt; Issues</strong>. Overall Health Issues—<strong>Assurance</strong> landing page. Client Issues—<strong>Assurance &gt; Health &gt; Client</strong>. In the Client Devices table, click the MAC address to display the <strong>Client 360</strong> window. Device Issues—<strong>Assurance &gt; Health &gt; Network</strong>. In the Network Devices table &gt; <strong>Device</strong> column, click the device name to display the <strong>Device 360</strong> window. Issue Catalog—<strong>Assurance &gt; Issues &gt; View Issue Catalog</strong></td>
<td>See Issues Detected by Assurance, on page 147.</td>
</tr>
</tbody>
</table>
Monitor and Troubleshoot Overall Enterprise Health

• About Enterprise, on page 61
• Monitor and Troubleshoot the Overall Health of Your Enterprise, on page 61

About Enterprise

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

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

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

Monitor and Troubleshoot the Overall Health of Your Enterprise

Use this procedure to get a global view of the health of your enterprise, which includes network devices and clients, and to determine if there are potential issues that must be addressed.

Before you begin

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

Step 1

From the Cisco DNA Center home page, click Assurance.

The Overall Health window appears with three dashlets, as described in the following table.
Figure 4: Overall Health Window

The colors represent the health of the devices:

- **Red**—Critical issues. Health score range is 1 to 3.
- **Orange**—Warnings. Health score range is 4 to 7.
- **Green**—No errors or warning. Health score range is 8 to 10.
- **Gray**—No data available. Health score is 0.

Table 20: Overall Health Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Last 24 Hours** and **Actions** drop-down lists | • **Last 24 Hours**—Displays information on the window based on the time you choose from the drop-down list. Options are: **Last 3 hours**, **Last 24 hours**, and **Last 7 days**. Default is **Last 24 hours**.  
  • **Actions**—Allows you to make changes to the dashboard display when you choose **Edit Dashboards** from the drop-down list. See **Change the Position of a Dashlet**, on page 145 and **Create a Custom Dashboard**, on page 141. |
## Overall Health Map or Hierarchical Site View or Building View dashlet

The **Show** button allows you to hide or display this dashlet. This dashlet contains two buttons that allow you to display the health of all the components in the enterprise in a map view or site/building view.

- **Overall Health Map**—Click the **book** 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, with 10 being the best score, and a score of 0 indicates that data could not be obtained.

- **Hierarchical Site View or Building View**—Click the **folder** button, and then choose the **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table displays information.

## Overall Health Summary dashlet

Contains the following:

- **Network Devices** area—Provides the following information:

  - **Network Score**—Percentage of healthy (good) devices (routers, switches, wireless controllers, and access points) in your overall enterprise. See, [Network Health Score](#), on page 79.

  - **Device Category Health Score**—Provides score distribution between device categories: **Router**, **Core**, **Access**, **Distribution**, **Controller**, and **Access Point**. The device category score is the percentage of healthy (good) devices in a particular device category.

  **Note** When a fabric domain is selected, this area provides score distribution between the following categories: **Fabric Edge**, **Fabric Border**, and **Fabric Control Plane**.

  Click **View Network Health** to open the **Network Health** window.

- **Wired Clients and Wireless Clients** area—Provides score distribution between wired and wireless clients. The Wired Client score or the Wireless Client score is the percentage of healthy (good) wired or wireless client devices in your overall enterprise. See, [Client Health Score](#), on page 97.

  Click **View Client Health** to open the **Client Health** window.

## Top 10 Issues dashlet

Displays top 10 issues, if any, that must be addressed. By default, the issues are color coded and sorted by their preassigned priority level, starting with P1.

Click an issue to display the corresponding details, such as the description of the issue, impact, and suggested actions. To resolve an issue, from the **Status** drop-down list, choose **Resolve**.

Click **View All Issues** to open the **Issues** window.

For information about issues, see [View Global Issues](#), on page 147.
Step 2  Do the following, as required:

• To view details about an issue, from the Issues dashlet, select an issue.
• If the network health score is red or orange, from the Overall Health Summary dashlet, click View Network Health.
• If the client health score is red or orange, from the Overall Health Summary dashlet, click View Client Health.
• To display a 360° view of a device, in the Search field (located on the top-right corner), enter the following to view the corresponding information:
  • For client devices—User ID (authenticated through Cisco ISE), IP address, or MAC address.
  • For switches, routers, access points, and wireless controllers—Device name, IP address, or MAC address.
Monitor and Troubleshoot Network Health

- About Network, on page 65
- Monitor and Troubleshoot the Health of Your Network, on page 65
- Monitor and Troubleshoot the Health of a Device, on page 71
- Fabric Domains, on page 75
- Enable SNMP Collector Metrics for Fabric Devices, on page 77
- Understand Network Health Score and KPI Metrics, on page 79

About Network

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

Monitor and Troubleshoot the Health of Your Network

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

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

Note

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

Before you begin

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

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

Step 2
Choose Health > Network.
The **Network Health** window appears with four dashlets, as described in the table below.

*Figure 5: Network Health Window*

<table>
<thead>
<tr>
<th>Color</th>
<th>Description</th>
<th>Score Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>Critical issues. Health score range is 1 to 3.</td>
<td>1 to 3</td>
</tr>
<tr>
<td>Orange</td>
<td>Warnings. Health score range is 4 to 7.</td>
<td>4 to 7</td>
</tr>
<tr>
<td>Green</td>
<td>No errors or warning. Health score range is 8 to 10.</td>
<td>8 to 10</td>
</tr>
<tr>
<td>Gray</td>
<td>No data available. Health score is 0.</td>
<td>0</td>
</tr>
</tbody>
</table>

The colors in the charts represent the health of the network devices:

- **Red**—Critical issues. Health score range is 1 to 3.
- **Orange**—Warnings. Health score range is 4 to 7.
- **Green**—No errors or warning. Health score range is 8 to 10.
- **Gray**—No data available. Health score is 0.
### Table 21: Network Health Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **24 Hours, All Domains and Actions drop-down lists** | • **24 Hours**—Displays information on the window based on the time range you select. Do the following:  
1. From the 24 Hours drop-down list, choose a time range: **3 hours**, **24 hours**, or **7 days**.  
2. Specify the Start date and time; and the End date and time.  
3. Click **Apply**. This sets the time boundaries on the timeline slider.  
• **All Domains**—Displays information for all domains or fabric domain. Default is **All Domains**.  
Fabric Domains—To view information about a fabric domain, from the All Domains drop-down list, choose the appropriate option. For multisite fabrics, the sites connected to the fabric domain and the transit area are provided in the drop-down list.  
To monitor and troubleshoot fabric domains, you must first configure the fabric domain. See Create a Fabric Domain, on page 76 and Add Devices to a Fabric, on page 76. For additional details and to understand multisite fabric domains, see the "Provision Your Network" chapter in the Cisco Digital Network Architecture Center User Guide.  
• **Actions**—Allows you to make changes to the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 145 and Create a Custom Dashboard, on page 141. |
| **Timeline Slider with Healthy Network Device Percentage Chart** | Allows you to specify a more granular time range.  
Hover your cursor within the timeline chart to view the network device health score percentage at a specific time.  
View the threshold value, which is 40%, provided in the legend below the chart. The threshold is also provided in the chart as a dotted horizontal line.  
You can click the right timeline slider bar, and move it to the desired time. This sets the context for the 5-minute charts on the window.  
You can also move both the right and left timeline slider bars to the desired time range. This sets the context for the custom charts on the window. |
Monitor and Troubleshoot the Health of Your Network

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Network Health Map, Network Topology, or Hierarchical Site View or Building View dashlet | The Show button allows you to hide or display this dashlet. This dashlet contains three buttons that allow you to display the health of the network in a map view, topology view, or site/building view.  

- **Network Health Map**—Click the 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. 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 indicates that data could not be obtained.  

- **Network Topology**—Click the button to display a topology view of how the components in the network are connected. Hover your cursor over a device to display device information such as device role, IP address, and software version. To obtain a 360° view of the device, click View Details 360.  

- **Hierarchical Site View or Building View**—Click the button, and then choose the Hierarchical Site View or Building View from the drop-down list. Based on what you choose, the table displays information. To view information about a specific site, building, or floor, click Apply in the appropriate row; information is refreshed based on your selection. |
### Device Health Summary dashlet

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 79.

This dashlet includes the following charts:

- **Latest** — Displayed by default. This color coded snapshot-view chart shows the performance of each device category (Access, Core, Distribution, Router, Wireless Controller, and Access Points) over the last 5 minutes.

  Hover your cursor over a color to display the health score and the number of devices associated with that color.

  If the chart shows a low health score (red or orange), the KPIs that contributed to the low health score are provided adjacent to the bar. For example, link errors, high CPU, high memory, high noise, low air quality, and so on.

  You can also click a hyperlinked device category (Access, Core, Distribution, Router, Wireless Controller, and Access Point) to open a side bar with additional details.

  **Note** For Fabric Domains, the color coded percentage chart shows the performance of the following fabric categories: Fabric Edge, Fabric Border, Fabric Control Plane, and Fabric Wireless.

- **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.

  Click [View Details](#) to open a side bar with additional details. From the side pane, click a color in the chart to refresh the data in the table that is displayed below the chart.

### Total APs Up and Down, Top N APs by Client Count, and Top N APs with High Interference dashlets

Contains three dashlets that provide a 15-minute snapshot view and a 24-hour trend view:

- **Total APs Up and Down** — Color coded chart that provides the AP status information: number of APs that are connected to the network and the number of APs that are not connected to the network.

- **Top N APs by Client Count** — Chart that provides information about the APs that have the highest number of clients.

- **Top N APs with High Interference** — Information about the APs that have high interference. You can choose 2.4 GHz or 5 GHz.

  Click [View Details](#) to open a side bar with additional details. From the side pane, click a color in the chart to refresh the data in the table that is displayed below the chart.
### Item | Description
--- | ---
**Network Devices** table dashlet | Allows you to filter, view, export, and customize the network device information:
- Filter the table based on device, type, or overall health, or add custom filters:
  - **Device**—Monitored and Unmonitored. Unmonitored devices are devices for which Assurance did not receive any telemetry data during the specified time range. Unmonitored devices are included in the Network Health Score computation. They are used as part of the total number of devices against which the health device percentage is calculated.
  - **Type**—All, Access, Core, Distribution, Router, WLC, and AP.
  - **Overall Health**—Poor, Fair, and Good.
    - **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.
- View device information for all the devices in the network or for a selected site.
  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 following KPI metrics: System Resources, Data Plane, and Control Plane.
  - Display a 360° view of a device by clicking the device name in the **Device** column.
  - Export the device information to a CSV file by clicking **Export**.
  - Customize the data you want displayed in the table. Do the following:
    1. Click the ![icon](icon.png) icon.
       A list of options are displayed.
    2. Check the check boxes next to the columns you want displayed in the table, and then click **Apply**.

### Step 3
To display a 360° view of the device, do one of the following:
- In the **Network Devices** dashlet, click the device name in the **Device** column.
- In the **Search field** (located at the top-right corner), enter one of the following: device name, IP address, or MAC address.
Monitor and Troubleshoot the Health of a Device

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

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

The **Overall Health** window appears.

**Step 2**
Click **Health > Network**.

The **Network Health** window appears.

**Step 3**
Do one of the following:

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

A 360° view of the device appears, as described in the table below.

*Figure 6: Device 360 Window*
### Table 22: Device 360 Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| 24 Hours and All Domains drop-down lists | **24 Hours**—Displays information on the window based on the time range you select. Do the following:  
1. From the 24 Hours drop-down list, choose a time range: **3 hours, 24 hours**, or **7 days**.  
2. Specify the Start date and time; and the End date and time.  
3. Click **Apply**.  
This sets the time boundaries on the timeline slider.  
*All Domains*—Displays information for all domains or fabric domain. Default is **All Domains**.  
**Fabric Domains**—To view information about a fabric domain, from the All Domains drop-down list, choose the appropriate option. For multisite fabrics, the sites connected to the fabric domain and the transit area are provided in the drop-down list. |
| Intelligent Capture tab | To view and monitor captured onboarding and data packets for a specific device and to determine if there are potential issues that must be addressed, click **Intelligent Capture** located at the top-right corner. For more information, see **Monitor Intelligent Capture Details for a Device**, on page 139.  
**Note**: Intelligent Capture is not supported for all AP models. If the Intelligent Capture tab is not displayed, verify that the AP is a supported model, and that the AP is assigned to a location on the Network Health window. |
### Device Health Score

Health score of a device:

- **Switch** — The Switch Health score is the minimum subscore of the following parameters: memory utilization, CPU utilization, link errors, and link status. In addition, for fabric devices, it includes connectivity to the Control Plane node. For more information, see Switch Health Score, on page 80.

- **Router** — The Router Health score is the minimum subscore of the following parameters: memory utilization, CPU utilization and link errors. For more information, see Router Health Score, on page 81.

- **AP** — The AP Health score 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 81.

- **Wireless Controller** — The Wireless Controller Health score is the minimum subscore of the following parameters: memory utilization, free timers, free memory buffers (MBufs), work queue element (WQE) pools, packet pools, link errors. For fabric wireless controllers, it includes connection to the Control Plane node. For more information, see Wireless Controller Health Score, on page 82.

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 indicates that data could not be obtained.

- Red — Critical issues. Health score range is 1 to 3.
- Orange — Warnings. Health score range is 4 to 7.
- Green — No errors or warning. Health score range is 8 to 10.
- Gray — No data available. Health score is 0.

### Device Information menu bar

Information about a 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.

### View Details tab

To view additional attributes of a device, such as general information, network information, and rack location, click the View Details tab located at the top-right corner.

### Historical Health Graph area

Health information about the selected network device over a period of time.

When you hover your cursor over a time instance on the graph, the device health score is displayed along with the health and percentage value of all the KPI metrics. The Device Health score is the minimum subscore of the System Resources, Data Plane, and Control Plane KPI metrics.

When you click a time, for example, 7:05, the entire window is refreshed, providing updates for that point of time. Note that the timestamp next to each category (Issues, Connectivity, and so on) is also refreshed.
Step 4  View information about issues, physical neighbor topology, path trace, application experience, and detail information under the appropriate category.

Table 23: Categories in the Device 360 Window

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issues</td>
<td>Issues, if any, that must be addressed. Issues are listed based on the time stamp. The most recent issue is listed first.</td>
</tr>
<tr>
<td></td>
<td>Click an issue to view the corresponding details, such as the description of the issue, impact, and suggested actions. To resolve an issue, from the Status field, choose Resolve.</td>
</tr>
<tr>
<td></td>
<td>Click Resolved Issues to view the list of issues that are resolved. For information about the types of issues, see Issues Detected by Assurance, on page 147.</td>
</tr>
<tr>
<td>Physical Neighbor Topology</td>
<td>Displays a topology view of a specific device and shows how that device is connected to neighboring devices.</td>
</tr>
<tr>
<td>Path Trace</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>See Perform a Path Trace, on page 102.</td>
</tr>
<tr>
<td>Application Experience</td>
<td>Applications running on a router with their qualitative and quantitative metrics. To view the metrics in a chart format, click the radio button next to an application, in the table. A side bar opens with the relevant information.</td>
</tr>
<tr>
<td></td>
<td>See About Cisco Application Experience, on page 105 and View the Application Experience of a Client Device or Router, on page 108.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  This category is displayed only for routers.</td>
</tr>
</tbody>
</table>
Depending on the type of device, historical KPIs performing over a period of time are displayed in appropriate charts under tabs, such as Device, Connectivity, and RF.

**Note** For fabric domains, an additional Fabric tab is displayed. This tab displays fabric KPIs, such as reachability and uplink status charts.

- **Device**—Device details, such as CPU, memory, uptime, and so on are displayed.
- **Connectivity**—Health of a device's connection with the network. For example, for APs, the following charts are displayed:
  - **Traffic**—The traffic (in Mbps) for radios is displayed. The Rx (receiver) data packets and Tx (transmitter) data packets (in bytes) are shown as color coded lines on the chart. Hover your cursor over a time instance on the graph to view the amount of traffic (Rx or Tx) sent or received for a particular day and time.
  - **Client Count**—The number of clients for radios is displayed. The client count is shown as color coded lines on the chart. Hover your cursor over a time instance on the graph to view the number of clients connected to an AP for a particular day and time.
  - **Link Error**—To display information about interfaces, check the check boxes adjacent to the interfaces on the right of the chart. Based on the interfaces you choose, the error percentage for each of the interface is displayed as color coded lines on the chart. Hover your cursor over a time instance on the graph to view the error percentage for a particular day and time. You can choose a maximum of five interfaces.
  - **RF**—Radio channel width, utilization, interference, noise, air quality, and so on are displayed.

---

**Fabric Domains**

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

**Fabric Overview**

A fabric domain is a logical group of devices that is managed as a single entity in one or multiple locations. Having a fabric in place enables several capabilities, such as the creation of virtual networks and user and device groups, and advanced reporting. Other capabilities include intelligent services for application recognition, traffic analytics, traffic prioritization, and steering for optimum performance and operational effectiveness.
Cisco DNA Center lets you add devices to a fabric network. These devices can be configured to act as control plane or border devices within the fabric network.

**Before You Begin**

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

### Create a Fabric Domain

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

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

### Add Devices to a Fabric

After you have created a fabric domain, you can add fabric sites, and then add devices to the fabric site. You can also specify whether the devices should act as a control plane node, a border node, or both.

**Note**

It is optional to designate the devices in a fabric domain as control plane nodes or border nodes. You may have devices that do not play these roles. However, every fabric domain must have at least one control plane node device and one border node device. In the current release for wired fabric, you can add up to six control plane nodes for redundancy.

There are three steps to add and configure devices to a fabric domain:

1. Select the devices.
2. Specify devices to act as control plane nodes.
3. Specify devices to act as border nodes.

To add a device to the fabric:

**Before you begin**

You must provision the device. To provision a device, click the **Provision** tab and choose **Devices**. Before you add a device to the fabric, you must perform the pre-verification check by clicking the **Pre-Verification** tab. The pre-verification check can be done only for devices that have been assigned roles. The pre-verification...
procedure performs a check on the **Hardware Version** and **Software Version** of the device. The result shows whether the device passed the test, failed the test, or is not supported.

**Step 1**
From the Cisco DNA Center home page, click **Provision**. The screen displays all provisioned fabric domains.

**Step 2**
From the list of fabric domains, choose a fabric. The screen displays all devices in the network that have been inventoried. You can view devices in the topology view or list view. In the topology view, any device that is added to the fabric is shown in blue.

**Step 3**
Click a device and choose one of the options displayed.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add as CP+Border+Edge</td>
<td>Add the selected device as a control plane and a border node and an edge node.</td>
</tr>
<tr>
<td>Add to Fabric</td>
<td>Add a distribution or access device to the fabric domain.</td>
</tr>
<tr>
<td>Add as CP</td>
<td>Add a core or distribution device as a control plane node. This allows the fabric access device to communicate with the control plane device.</td>
</tr>
<tr>
<td>Add as Border</td>
<td>Add a core device as a border node. This allows the fabric access device to communicate with the fabric border device.</td>
</tr>
<tr>
<td>Add as CP+Border</td>
<td>Add the selected device as a control plane and a border node.</td>
</tr>
<tr>
<td>Run Pre-Provisioning Check</td>
<td>Run a pre-provisioning check.</td>
</tr>
</tbody>
</table>

**Enable Guests**
In the pop-up window, enter the following options:

- Set as control plane: Check this check box if you want the device to act as a control plane.
- Set as a border node: Check this check box if you want the device to act as a border node.
- Select a guest virtual network: All guest virtual networks created are listed. Check the check box of the guest virtual network and click **Enable**.

**Note**
Ensure that you have created a guest virtual network in the **Policy** application.

| View Device Info               | Displays the details of the selected device.                                |

**Step 4**
Click **Save**.

---

**Enable SNMP Collector Metrics for Fabric Devices**

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

**Step 1**
From the Cisco DNA Center home page, click the gear icon 🏢, and then choose **System Settings > Data Platform**.
Step 2  Click **Collectors**.
A list of collectors are displayed.

Step 3  Click **Collector-SNMP**.
The **Collector-SNMP** window appears.

Step 4  Click **+ Add**.
The **SNMP Configuration** side bar opens.

Step 5  Select the checkboxes adjacent to all the metrics except QOS.

**Figure 7: SNMP Configuration**

Step 6  In the **Configuration Name** field, enter a unique name for the SNMP 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

Switch (Access and Distribution)—Includes system-monitoring metrics, such as CPU utilization and memory utilization.

Wireless—Includes the following system-monitoring metrics:
  • For wireless controllers, it includes memory utilization, free timers, and free Mbufs.
  • For AP, it includes CPU utilization and memory utilization.

Router—Includes system-monitoring metrics, such as CPU utilization and memory utilization.

Fabric—Includes system-monitoring metrics, such as CPU utilization and memory utilization.

Data Plane Connectivity

Switch (Access and Distribution)—Includes metrics, such as link errors and link status.
Wireless—including 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—Available for Fabric Devices Only

Wireless—including 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:

- **CPU Utilization:**
  - If CPU utilization is 95 percent or less, the score is 10.
  - If CPU utilization is more than 95 percent, the score is 1.

- **Memory Utilization:**
  - If memory utilization is 95 percent or less, the score is 10.
  - If memory utilization is more than 95 percent, the score is 1.

- **Link Errors (Rx and Tx):**
  - If link errors are 1 percent or less, the score is 10.
  - If link errors are more than 1 percent, the score is 1.

- **Link Status:**
  - If link status is LINK UP, the score is 10.
  - If link status is LINK DOWN, the score is 1.

- **Connection to Control Plane Node—Fabric Devices Only (Edge and Border):**
  - If the Control Plane node is reachable, the score is 10.
  - If the Control Plane node is unreachable, the score is 1.

---

**Note**

If there is more than 1 Control Plane node in a fabric domain, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1.
Router Health Score

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

- **CPU Utilization**:
  - If CPU utilization is 95 percent or less, the score is 10.
  - If CPU utilization is more than 95 percent, the score is 1.

- **Memory Utilization**:
  - If memory utilization is 95 percent or less, the score is 10.
  - If memory utilization is more than 95 percent, the score is 1.

- **Link Errors**:
  - If interface errors are 1 percent or less, the score is 10.
  - If interface errors are more than 1 percent, the score is 1.

AP Health Score

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

- **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** (calculated individually for each radio, and then the average radio score is determined):
  - If radio utilization is less than 60 percent, the score is 10.
  - If radio utilization is 60 percent or more, the score is 0.

- **Interference Score** (calculated individually for each radio, and then the average radio score is determined):
• If interference is less than or equal to 30 percent for 5-GHz radio and less than or equal to 50 percent for 2.4-GHz radio, the score is 10.
• If interference is more than 30 percent for 5-GHz radio and more than 50 percent for 2.4-GHz radio, the score is 0.

• **RF Noise Score** (calculated individually for each radio, and then the average radio score is determined):
  • If RF noise is less than -70dBm, the score is 10.
  • If RF noise is -70dBm or more, the score is 0.

• **Air Quality Score** (calculated individually for each radio, and then the average radio the score is determined):
  • If air quality is 40 percent or more, the score is 10.
  • If air quality is less than 40 percent, the score is 0.

**Wireless Controller Health Score**

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

• **Memory Utilization:**
  • If memory utilization is less than 90 percent, the score is 10.
  • If the available memory is 90 percent or more, the score is 1.

• **Free Timer Score:**
  • If the number of free timers is 20 percent or more, the score is 10.
  • If the number of free timers is 20 percent or less, the score is 1.

• **Free Memory Buffers (MBufs):**
  • If the number of free memory buffer is 20 percent or more, the score is 10.
  • If the number of free memory buffer is less than 20 percent, the score is 1.

• **Work Queue Element (WQE) Pool Score:**
  • If the wqe pool is greater than wqe pool threshold, the score is 10.
  • If the wqe pool is at the same level as or lower than the wqe pool threshold, the score is 1.

• **Packet Pools:**
  • If the packet pool is greater than the packet pool threshold, the score is 10.
  • If the packet pool is at the same level as or lower than the packet pool threshold, the score is 1.

• **Link Errors:**
  • If link errors are less than 1 percent, the score is 10.
• If link errors are 1 percent or more, the score is 1.

• Connection to Control Plane Node—Fabric Wireless Controllers Only:
  • If the Control Plane node is reachable, the score is good.
  • If the Control Plane node is unreachable, the score is poor.

Note
If there is more than 1 Control Plane node in a fabric domain, and all the Control Plane nodes are reachable, the score is 10; otherwise, the score is 1.
Monitor and Troubleshoot Network Health

Wireless Controller Health Score
Monitor and Troubleshoot Client Health

• About Clients, on page 85
• Monitor and Troubleshoot the Health of All Client Devices, on page 85
• Monitor and Troubleshoot the Health of a Client Device, on page 92
• Understand Client Health Score and KPI Metrics, on page 97

About Clients

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

Monitor and Troubleshoot the Health of All Client Devices

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

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

Before you begin

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

Step 1

From the Cisco DNA Center home page, click Assurance.

The Overall Health window appears.

Step 2

Click Health > Clients.

The Client Health window appears with dashlets, as described in the table below.
The colors in the charts represent the health of the client devices.

- Red—Poor client devices. Health score range is 1 to 3.
- Orange—Fair client devices. Health score range is 4 to 7.
- Green—Good client devices. Health score range is 8 to 10.
- Gray—Inactive client devices. Health score is 0.
### Table 24: Client Health Page

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **24 Hours, All SSIDs, All Bands, and Actions** drop-down list | • **24 Hours**—Displays information on the window based on the time range you select. Do the following:  
1. From the **24 Hours** drop-down list, choose a time range: **3 hours, 24 hours,** or **7 days.**  
2. Specify the Start date and time; and the End date and time.  
3. Click **Apply.**  
   This sets the time boundaries on the timeline slider.  
• **All SSIDs**—Displays information for the SSID you choose from the drop-down list. Default is **All SSIDs.**  
• **All Bands**—Displays information for the band frequency you choose from the drop-down list. Options are: **2.4 GHz, 5 GHz,** or **All Bands.**  
• **Actions**—Allows you to make changes to the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Change the Position of a Dashlet, on page 145 and Create a Custom Dashboard, on page 141. |
| **Timeline Slider with Healthy Client Percentage Chart** | Allows you to specify a more granular time range. Click the timeline slider bar, and then move it to the desired time range.  
Hover your cursor within the timeline chart to view the wireless and wired client health score percentage at a specific time.  
View the threshold value, which is 40%, provided in the legend below the chart.  
The threshold is also provided in the chart as a dotted horizontal line. |
| **Client Health Map** or **Hierarchical Site View or Building View** dashlet | The **Show** button allows you to hide or display this dashlet. This dashlet contains two buttons that allow you to display the health of the client devices in a map view or site/building view.  
• **Client Health Map**—Click the **button to display the health of all the client sites on a geographic location-oriented client health map. By default, the client sites that are represented are color coded according to the severity of the problem.  
The color of the health score represents its severity. The health is measured on a scale of 1 to 10, with 10 being the best score, and a score of 0 indicating that the client is inactive.  
• **Hierarchical Site View** or **Building View**—Click the **button, and then choose the **Hierarchical Site View** or **Building View** from the drop-down list. Based on what you choose, the table displays information.  
To view information about a specific site, building, or floor, click **Apply** in the appropriate row; information is refreshed based on your selection. |
This dashlet includes the following information:

- **Wired or Wireless Client Health Summary Score**—The Wired or Wireless Client Summary Health Score is the percentage of clients that onboarded successfully and have good connectivity. See [Client Health Score](#), on page 97.

- **Client Count**—Count of **Active**, **Inactive**, and **New** client devices.

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

- **Client Health Summary Charts**—Provides 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**—Click the **Trend** tab to display a trend chart. This trend chart shows the health of clients over a time period.

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

Click **View Details** to open a side bar with additional details. The latest snapshot-view chart displays by default. To display the trend chart, click **Trend**.

Click a color or bar in the chart to populate and refresh the data in the table that is displayed below the chart.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Health Summary</strong></td>
<td>This dashlet includes the following information:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Wired or Wireless Client Health Summary Score</strong>—The Wired or Wireless Client Summary Health Score is the percentage of clients that onboarded successfully and have good connectivity. See <a href="#">Client Health Score</a>, on page 97.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Client Count</strong>—Count of <strong>Active</strong>, <strong>Inactive</strong>, and <strong>New</strong> client devices.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> New clients are clients that attempted to onboard after the 5-minute health score calculation window started. The health score for these clients will be included in the next 5-minute calculation window.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Client Health Summary Charts</strong>—Provides two types of charts:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Latest</strong>—Displayed by default. This snapshot-view chart provides the distribution of clients that passed or failed to onboard within the last 5 minutes. Then, from the number of clients that onboarded successfully (passed), the chart provides the percentage of clients that have good or fair connectivity.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Trend</strong>—Click the <strong>Trend</strong> tab to display a trend chart. This trend chart shows the health of clients over a time period.</td>
</tr>
<tr>
<td></td>
<td>For the clients that failed to onboard, the breakdown of the reason for the onboarding failure is provided. For example, AAA, DHCP, Other, and so on.</td>
</tr>
<tr>
<td></td>
<td>Click <strong>View Details</strong> to open a side bar with additional details. The latest snapshot-view chart displays by default. To display the trend chart, click <strong>Trend</strong>.</td>
</tr>
<tr>
<td></td>
<td>Click a color or bar in the chart to populate and refresh the data in the table that is displayed below the chart.</td>
</tr>
</tbody>
</table>
Monitor and Troubleshoot Client Health

Monitor and Troubleshoot the Health of All Client Devices

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Client Onboarding Times, Connectivity RSSI, Connectivity SNR, Client Count Per SSID, Client Count Per Band, DNS, and Connectivity Physical Link dashlets | Analyzes the health of the client devices every 5 minutes and updates the charts in the dashlets listed below. Click a dashlet to open a side bar with additional drill-down capabilities.  
  - **Client Onboarding Times**—Distribution of all the clients' attempts to onboard, in all the sites or a selected site, over time. This dashlet provides the percentage of clients who took less than 10 seconds to successfully onboard.  
  - **Connectivity RSSI**—Received Signal Strength Indication (RSSI) distribution for all clients, in all sites or a selected site. This dashlet provides the percentage of RSSI measurements for all clients whose RSSI measurement is higher than the threshold value of -72 dBm.  
  - **Connectivity SNR**—Signal-to-Noise ratio (SNR) distribution for 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.  
  - **Client Count Per SSID**—Distribution of the number of clients per SSID, in all sites or a selected site, over time.  
  - **Client Count Per Band**—Distribution of the number of clients per band frequency (2.4 GHz and 5 GHz), in all sites or a selected site, over time.  
  - **DNS**—Distribution of DNS requests and response counters, in all sites or a selected site, over time.  
  - **Connectivity Physical Link**—Distribution of wired client device link state: the number of devices that had their physical links up, down, and had errors.  

Click **View Details** to open a side bar with additional details. From the side pane, click a color in the chart to populate or refresh the data in the table that is displayed below the chart.
Monitor and Troubleshoot Client Health

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Devices table dashlet</td>
<td></td>
</tr>
</tbody>
</table>
Monitor and Troubleshoot the Health of All Client Devices

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allows you filter, view, export, and customize client device information:</td>
</tr>
<tr>
<td></td>
<td>• Filter the table based on client type, client health, and data.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Client Type</strong>—Options are <strong>Wired</strong> and <strong>Wireless</strong> clients.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Client Health</strong>—Options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>All</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Inactive</strong>—Client devices with a health score of 0.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Poor</strong>—Client devices with a health score range from 1 to 3.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Fair</strong>—Client devices with a health score range from 4 to 7.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Good</strong>—Client devices with a health score range from 8 to 10.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Data</strong>—Options are:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Onboarding Time &gt;= 10s</strong>—Onboarding time is greater than or equal to the 10-second threshold value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Association &gt;= 5s</strong>—Association time is greater than or equal to the 5-second threshold value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AAA &gt;= 5s</strong>—AAA time is greater than or equal to the 5-second threshold value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>DHCP &gt;= 5s</strong>—DHCP time is greater than or equal to the 5-second threshold value.</td>
</tr>
<tr>
<td></td>
<td>• <strong>RSSI &lt;= -72 dBm</strong>—RSSI is less than or equal to the -72 dBm threshold value.</td>
</tr>
<tr>
<td></td>
<td>• View client device information in a table format. The client device table lists information about client devices, such as userID, hostname, MAC address, IP address, device type, last heard, location, VLAN ID, SSID, and the following information:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Identifier</strong>—Displays the client's userID, hostname, or MAC address based on availability, in that order. For example, if the userID is not available, the hostname is displayed. If the user ID and hostname are not available, the MAC address is displayed.</td>
</tr>
<tr>
<td></td>
<td>The Identifier column also has specific icons that allow you to determine if the client device is wired or wireless.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address</strong>—Displays the client's IPv4 or IPv6 IP address based on availability.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Overall Health Score</strong>—This score is the sum of the onboarding and connected scores. The Client Health score is calculated every 5 minutes.</td>
</tr>
<tr>
<td>Note</td>
<td>A score of -- indicates that the client has recently onboarded (new). New clients are clients that attempted to onboard</td>
</tr>
</tbody>
</table>
Monitor and Troubleshoot the Health of a Client Device

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

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

---

Monitor and Troubleshoot Client Health

---

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>after the 5-minute health score calculation window started. The health score for these new clients will be included in the next 5-minute calculation window.</td>
</tr>
<tr>
<td>• Onboarding Score</td>
<td>Indicates the experience of a client device while connecting to the network; whether the client connected (onboarded) to the network successfully or not. For more information, see Client Onboarding Score, on page 97.</td>
</tr>
<tr>
<td>• Connected Score</td>
<td>Indicates the experience of a client device after the device is connected to the network. For more information, see Client Connectivity Score, on page 98.</td>
</tr>
<tr>
<td>• Connected To</td>
<td>Provides the following information:</td>
</tr>
<tr>
<td>• Wireless Clients</td>
<td>Provides the name of the AP or wireless controller to which the client device is connected.</td>
</tr>
<tr>
<td>• Wired Client</td>
<td>Provides the name of the switch to which the client device is connected.</td>
</tr>
<tr>
<td>• Display a 360° view of a client by clicking the MAC Address or Identifier of a client device.</td>
<td></td>
</tr>
<tr>
<td>• Customize the data you want displayed in the table. Do the following:</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Click the icon. A list of options are displayed.</td>
</tr>
<tr>
<td>2.</td>
<td>Check the check boxes next to the columns you want displayed in the table, and then click Apply.</td>
</tr>
</tbody>
</table>

---

Step 3 To display a 360° view of the client, do one of the following: |
| • In the Client Devices table, click the MAC address of the device. |
| • In the Search field (located at the top-right corner), enter one of the following: user ID (authenticated through Cisco ISE), IP address, or MAC address. |
The **Overall Health** window appears.

**Step 2**

Click **Health > Clients**.

The **Client Health** window 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.

A 360° view of the client device appears, as described in the table below.

*Figure 9: Client 360 Window*
Table 25: Client 360 Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>24 Hours and All Domains</strong> drop-down lists</td>
<td>• <strong>24 Hours</strong>—Displays information on the window based on the time range you select. Do the following: 1. From the <strong>24 Hours</strong> drop-down list, choose a time range: 3 hours, 24 hours, or 7 days. 2. Specify the Start date and time; and the End date and time. 3. Click <strong>Apply</strong>. This sets the time boundaries on the timeline slider. • <strong>All Domains</strong>—Displays information for all domains or fabric domains. Default is <strong>All Domains</strong>.</td>
</tr>
<tr>
<td><strong>Intelligent Capture</strong> tab</td>
<td>To view, monitor, and troubleshoot captured onboarding and data packets for a specific client device and to determine if there are potential issues that must be addressed., click <strong>Intelligent Capture</strong> located at the top-right corner. For more information, see <strong>Monitor Intelligent Capture Details for a Client</strong>, on page 136. <strong>Note</strong> Intelligent Capture is not supported for all AP models. If the Intelligent Capture tab 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 page.</td>
</tr>
</tbody>
</table>
| **Individual Client Health Score** | 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 99. 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. • **Red**—Poor client devices. Health score range is 1 to 3. • **Orange**—Fair client devices. Health score range is 4 to 7. • **Green**—Good client devices. Health score range is 8 to 10. • **Gray**—Inactive client devices. Health score is 0. **Note** For clients that are disconnected from the network, the score is represented as a - -.
Item | Description
---|---
**Client Device tabs** | Details about each of the client's devices is represented in a separate tab, for example, `username-macbook` or `username-iphone`. The Client 360 header provides the most current information about the client device, such as device type, OS version, MAC address, IP address, connected status, last seen, connected network device, last known location, and SSID.

**Historical Health and Events Graph** | Health and events information about the selected client device over a period of time are displayed in a graph.

  - **Health**—To obtain the health score at a particular time, hover your cursor over the time instance on the graph, for example, you can hover your cursor at 7:00, 7:05, 7:20, and so on. When you hover your cursor over a time instance, a table providing information about the different KPIs appears below the graph. The KPIs that are color coded in the table contribute to the Client Health score. For example, Onboarding, RSSI, and SNR.

  - To view the list of events that occurred during that time frame, click **See full list** in the Major Events column.

  - When you double-click on the graph, it brings the timeline slider to a 1-hour time period. The entire window is refreshed, providing updates for that 1-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 more than 1-hour, manually move the timeline slider to the desired time range.

  - **Events**—Event data is displayed by color coded vertical bars on the graph. Green vertical bars indicate successful event(s) and the red vertical bars indicate event(s) 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 event(s).

---

**Step 4** View information about issues, onboarding, event viewer, path trace, application experience, and detail information under the appropriate category.

**Table 26: Categories in the Client 360 Window**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issues</strong></td>
<td>Issues, if any, that must be addressed. Issues are listed based on the time stamp. The most recent issue is listed first. Click an issue to view the corresponding details, such as the description of the issue, impact, and suggested actions. To resolve an issue, from the <strong>Status</strong> field, choose <strong>Resolve</strong>. Click <strong>Resolved Issues</strong> to view the list of issues that are resolved. For information about the types of issues, see <strong>Issues Detected by Assurance</strong>, on page 147.</td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Onboarding</td>
<td>Topology of how a client got on the network, including information about the following services: AAA and DHCP. Example of wired client topology: Client &gt; Switch &gt; Router Example of wireless client topology: Client &gt; SSID &gt; Access Point &gt; Wireless Controller</td>
</tr>
</tbody>
</table>
| Event Viewer     | Lists scenarios and the sequence of sub-events that led to each scenario. This allows you to pin-point during which sub-event an issue occurred. The following scenarios are provided:  
  - Re-Authentication  
  - Broadcast Rekey—Process of changing the session key—the encryption key of an ongoing communication—in order to limit the amount of data encrypted with the same key.  
  - Onboarding  
  - DHCP  
  - Delete  
  - INTRA-Roaming  
  When an issue occurs, that event is marked red, otherwise it is green. The second column provides additional information about the issue, such as the error message, and the AP and wireless controller to which the client device is connected. The third column provides the time stamp when the event occurred. Click an event, to view details about that event in the right pane. |
| Path Trace       | 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 102. |
| Application Experience | Applications running on a client device with their qualitative and quantitative metrics.  
  To view the metrics in a chart format, select the radio button next to an application in the table. A side bar opens with the relevant information.  
  See About Cisco Application Experience, on page 105 and View the Application Experience of a Client Device or Router, on page 108. |
Understand Client Health Score and KPI Metrics

This section provides information about how the client health scores and KPI metrics are computed.

Client Health Score

The Client Health score (Wireless or Wired) is the percentage of the number of healthy client devices (a health score from 8 to 10) in a target category, divided by the total number of client devices in that category. The score is calculated every 5 minutes.

For example: 90% (health score) = 90 (client devices in a target category with health score from 8 to 10) ÷ 100 (total number of client devices in that category)

The Individual Client Health score is the sum of the Client Onboarding score and the Client Connectivity score. The client health score ranges from 1 to 10, with a score of 0 for inactive clients. It is calculated as follows:

- **Wired Client**—Link to first switch is up, authentication and authorization is successful and IP address is received. Client score is 10.

- **Wireless Client**—Client joined the network and has good connection in terms of the RSSI and SNR KPIs.

Client Onboarding Score

The Client Onboarding score indicates the experience of a client device while connecting to the network.

- If a client connects to the network successfully, the score is 4.

- If a client is unable to connect to the network, the score is 1.

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 is unable 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 Client Connectivity score is calculated as follows:

- **Wired Client**—Connectivity score can be 0, 2, or 6. Connectivity to the DNS server or link errors determines the Connectivity score and the resulting Overall Health score, as shown below:
  
  - If a client onboards successfully, but is unable to connect to the DNS server, the Connectivity score is 0.
  
  - If a client onboards successfully and is able to connect to a DNS server, 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 range is 0 - 6. 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**

- If RSSI is less than -72 dBm, the RSSI-Driven Connectivity score is 0.

- If RSSI is equal to -71 dBm, the RSSI-Driven Connectivity score is 1.

- If RSSI is equal to -70 dBm, the RSSI-Driven Connectivity score is 2.

- If RSSI is equal to -69 dBm, the RSSI-Driven Connectivity score is 3.

- If RSSI is equal to or greater than -68 dBm and less than -55 dBm, the RSSI-Driven Connectivity score is 4.

- If RSSI is equal to or greater than -55 dBm and less than -45 dBm, the RSSI-Driven Connectivity score is 5.

- If RSSI is equal to or greater than -45 dBm, the RSSI-Driven Connectivity score is 6.

**SNR-Driven Connectivity Score**

- If SNR is from 0 to 9, the SNR-Driven Connectivity score is 0.

- If SNR is equal to 10, the SNR-Driven Connectivity score is 1.

- If SNR is 11 or 12, the SNR-Driven Connectivity score is 2.

- If SNR is 13 or 14, the SNR-Driven Connectivity score is 3.

- If SNR is 15, 16, 17, 18, or 19, the SNR-Driven Connectivity score is 4.

- If SNR is from 20 to 39, the SNR-Driven Connectivity score is 5.

- If SNR is equal to or greater than 40, the SNR-Driven Connectivity score is 6.
**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.

See the following topics:

- Client Onboarding Score, on page 97
- Client Connectivity Score, on page 98
CHAPTER 7

Trace the Path of a Device

- About Path Trace, on page 101
- Path Trace Known Limitations, on page 101
- Perform a Path Trace, on page 102

About Path Trace

You can perform a path trace between two nodes in your network—a specified source device and a specified destination device. The two nodes can be a combination of wired or wireless hosts or Layer 3 interfaces or both. In addition, you can specify the protocol that the Cisco DNA Center controller should use to establish the path trace connection, either TCP or UDP.

When you initiate a path trace, the Cisco DNA Center controller reviews and collects network topology and routing data from the discovered devices. It then uses this data to calculate a path between the two hosts or Layer 3 interfaces, and displays the path in a path trace topology. The topology includes the path direction and the devices along the path, including their IP addresses. The display also shows the protocol of the devices along the path (Switched, STP, ECMP, Routed, Trace Route) or other source type.

Path Trace Known Limitations

Path Trace has the following limitations and restrictions.

- Path trace between a fabric client and a non-fabric client is not supported.
- Path trace between two fabric clients over multi virtual routing and forwarding (VRFs) virtual networks (VNIs) is not supported.
- Path trace between two fabric clients over multi sites (domains) is not supported.
- Path trace with wireless controller or AP as source or destination device 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 ASA (Adaptive Security Appliances) is not supported. This is because Cisco ASA does not support CDP, it is not possible to identify the path through the Cisco ASA appliance.

- Path trace for dynamic interface and untagged management interface in centralized wireless deployment mode is not supported.

- 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 have 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, the statistics collection stops. To continue the statistics collections, 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.

---

**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 101.

- 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 23, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 27.

- 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 dialog box appears.

**Step 2**

Enter the source IP address, interface, and port number; and the destination IP address, interface, and port number.
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.

Choose an interface from the drop-down list.

**Note** This field is displayed if the source IP address is a network device.

Enter the port number of the host from which you want the trace to start.

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.

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.

Enter the port number of the host from which you want the trace to end.

**Step 3** From the **Options** area do the following as appropriate:

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protocol</strong></td>
<td>(Optional) Choose either <strong>tcp</strong> or <strong>udp</strong>.</td>
</tr>
<tr>
<td><strong>Refresh Every 30secs</strong></td>
<td>(Optional) To configure the path trace topology to refresh every 30 seconds, click <strong>Refresh Every 30secs</strong> such that its status is <strong>On</strong>.</td>
</tr>
<tr>
<td><strong>ACL Trace</strong></td>
<td>(Optional) To display matched ACLs and the ACL result (Permit or Deny) for a specific traffic flow, click <strong>ACL Trace</strong> such that its status is <strong>On</strong>.</td>
</tr>
</tbody>
</table>
Field | Action
--- | ---
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.

Hover your cursor over a device to display CPU and memory utilization.

If **ACL Trace** is set to **On**, the ACL name and ACL result, such as permit or deny display.

If the following 5-tuple values (source IP address and port number, destination IP address and port number, and the protocol in use) are provided, then the ACL trace that is displayed is 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.

Click a device to open a side bar with additional device details.

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 side bar with additional information.

Hover your cursor over the path to display the protocol of the devices along the path (**Switched, STP, ECMP, Routed, Trace Route**) or other source type.
Monitor Application Health

About Cisco Application Experience

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

Only application client-server statistics and ART (TCP) metrics can be monitored. Application Experience is based on the Cisco NetFlow records exported by the routers.

Based on the relevancy of an application, it is classified as Business Relevant, Business Irrelevant, or Default. This classification is done based on the NBAR standard.

To enable AX, you must enable Cisco NetFlow collection on the device. See Enable Cisco NetFlow Collection, on page 106.

Note

Cisco DNA Center supports configuring Cisco NetFlow only on routers. You can view this identification in the Cisco DNA Center Inventory window under Device Role.
Enable Cisco NetFlow Collection

To view the applications running on a network device with their qualitative and quantitative metrics, you must enable Cisco NetFlow collection on the device. Do the following:

1. Add a description on device interface(s) containing the keyword "lan." This can be either configured on the device interface manually or by using the Template Editor tool in Cisco DNA Center.

2. Resynchronize the network device to read this interface description. The Telemetry Provisioning module looks for interfaces with "lan" in the description and applies the NetFlow configuration to only those interfaces.

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

4. Configure and apply the NetFlow Telemetry profile to network devices. See Configure a Telemetry Profile, on page 106 and Apply a Telemetry Profile to a Device, on page 107.

---

**Note**

NetFlow telemetry is applied only to interfaces that have the description "lan", have an IP address, and are non-management interfaces.

NetFlow telemetry is supported only on routers running Cisco IOS XE Denali Release 16.3 and later.

---

Configure Telemetry

**About Telemetry**

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

**Configure a Telemetry Profile**

You can create telemetry assessment profiles for your network devices using the Telemetry tool.

---

**Note**

By default, the Disable-Telemetry profile is configured by Network Data Platform (NDP) on all the interfaces on all the capable devices.

---

Before you begin

Discover the devices in your network using Cisco DNA Center.

---

Step 1

From the Cisco DNA Center home page, choose Telemetry from the Tools area.

The Telemetry window appears.
Step 2 Click the **Site View** tab and check to see if network devices are listed in this window.

**Note** After configuring telemetry profiles, you will have to return to this window and apply the telemetry profiles to your devices.

Step 3 Click the **Profile View** tab.

The **Profile View** table displays the following information:

- **Profile Name**—Name of Cisco DNA Center preconfigured profiles and any other profiles that you have configured.
- **Customized**—Information about whether the profile is one of the Cisco DNA Center preconfigured profiles or a user-configured profile.
- **Profile Usage**—Number of devices that the telemetry profile is applied to.
- **Icon**—For Cisco DNA Center preconfigured profiles, by hovering your cursor over an icon, a definition appears. For example, when you hover your cursor over the following icons the following appears:
  - **Maximal Visibility**—Telemetry profile generated by NDP to enable all possible telemetry on all the interfaces on all the capable devices.
  - **Optimal Visibility**—Telemetry profile generated by NDP after analyzing the network topology, device capability, PIN, and enabled Cisco DNA Assurance features.
  - **Disable Telemetry**—Disables the telemetry profiles configured by NDP on all the interfaces on all the capable devices.

Step 4 Click **Add Profile**.

Step 5 In the **Name** field, enter a profile name.

Step 6 (Optional) Click **Syslog** and choose a **Severity Level** from the drop-down list.

Step 7 (Optional) Click **SNMP Traps** and choose an SNMP version from the drop-down list.

Step 8 (Optional) Click **NetFlow** and choose a version and profile from the drop-down list.

Step 9 Click **Save** to save the profile configuration or click **Cancel** to cancel the profile configuration.

---

**What to do next**

Proceed to apply the telemetry profile or profiles to your network devices. Use the **Telemetry Site View** options and fields to accomplish this task.

---

**Apply a Telemetry Profile to a Device**

You can apply a telemetry assessment profile to a network device using the Telemetry tool.

The telemetry profile configured in this procedure is used by Cisco DNA Center to determine what data types to capture. These data types are then used in monitoring the health of the network devices.

**Before you begin**

Perform the following preliminary tasks:

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

**Step 1**
From the Cisco DNA Center home page, choose Telemetry from the Tools area.
The Telemetry window appears.

**Step 2**
Click the Site View tab.

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

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

**Step 5**
From the Actions drop-down list, choose a telemetry profile.

**Step 6**
From the Show drop-down list, choose the telemetry profile that you applied in Step 5.
The device should appear in the filtered list, along with any other devices that have also been configured with the same telemetry profile.

What to do next
Access the Cisco DNA Assurance application and review both Assurance Health and Assurance Issues to check the health of your network devices.

View the Application Experience of a Client Device or Router

Use this procedure to view the applications running on a client device or a router with their qualitative and quantitative metrics.

**Note**
Application Experience is displayed only if the Netflow configuration is enabled on routers.

**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 23, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 27.
Monitor Application Health

Step 1
From the Client 360 or Device 360 window, scroll down to the Application Experience category. The Application Experience table displays three tabs: Business Relevant, Business Irrelevant, or Default.

Note: The information displayed in the table is based on the time you selected from the drop-down list in the Client 360 page or the Device 360 window. Options are: Last 3 Hours and Last 24 Hours. Default is Last 24 Hours.

The following application attributes are provided in the table:

- **Name**—The application name.
- **Domain Name**—HTTP hostname used by the client to access the application.
- **Health**—The health score is calculated on the basis of a combination of metrics of packet loss and latency. For each application, you can hover your cursor over View to view the variations in application health score.
- **Usage**—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.
- **Traffic Class**—The categorization of the application based on the NBAR standard.
- **Packet Loss**—The percentage (maximum and average) of packet loss.
- **Latency**—The network latency time (maximum and average) in milliseconds.
- **Application Delay**—The application delay time (maximum and average) in milliseconds.

Step 2
To view the application experience metrics in chart format in a side bar, click the radio button next to an application in the table.

Monitor the Health of All Applications

Use this procedure to get a global view of the health of all the applications.

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 23, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 27.
- Enable Cisco NetFlow collection on the device. See Enable Cisco NetFlow Collection, on page 106.

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

Step 2
Click Health > Application.
The Application Health window appears with the following information.

The colors in the chart represent the health of the business relevant applications:

- Red—Critical issues. Health score range is 1 to 3.
- Orange—Warnings. Health score range is 4 to 7.
- Green—No errors or warnings. Health score range is 8 to 10.
- Grey—Unknown. Health score is unknown.

### Table 27: Application Health Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| Last 24 Hours drop-down list and Actions drop-down list | • **Last 24 Hours**—Displays information on the window based on the time you select from the drop-down list. Options are: **Last 3 hours** or **Last 24 Hours**.  
  • **Actions**—Allows you to make changes to the dashboard display when you choose **Edit Dashboards** from the drop-down list. See Create a Custom Dashboard, on page 141. |
| Timeline Slider with Health Score Trend Line Chart | Allows you to specify a more granular time range (15-minute interval).  
  Hover your cursor within the time line chart to view the health score percentage of business relevant applications at a specific time. Allows you to zoom in on dips in the spark line.  
  You can click the right timeline slider bar, and move it to the desired time. This sets the context of 15-minute chart on the page. You can also move both the right and left timeline slider bars to the desired time range. This sets the context of the custom chart on the page. |
### Application Health Summary dashlet

This dashlet shows a snapshot view (last 15 minutes’ data) of the application health, and includes the following information.

- **Application Health Summary score** and **Trend Chart**—The Application Health Summary score is the percentage of healthy (good) business-relevant applications in your overall network or selected site. The application count distribution trend chart (located next to the health score) shows the count of all the business-relevant applications over time in the form of a stacked area chart based on their health scores. See **Understand Application Health Score and KPI Metrics**, on page 115.

- **Applications with Good Health**—Provides the list of applications with good/healthy health score. You can click the name of an application to display a 360° view of the application.

- **Application Usage** area—Displays the application usage break-up (Business Relevant, Business Irrelevant, and Default), and the top 10 applications by usage. You can click the name of an application to display a 360° view of the application.

Click **View Details** in the **Application Usage** area to open a side bar with additional details about the application. You can use the **Breakdown By** drop-down list to view the breakdown of the application usage based on Application Group (voice, data, video, control plane) or Traffic Class. The percentages displayed in the application usage is the percentage that is relative to other applications.

### Application dashlet

Allows you to filter, view, and export application health information:

- Filter the table based on application type and health.
  
  - **Application Type**—Options are **All**, **Business-relevant**, **Business-irrelevant**, and **Default** applications.

  - **Application Health**—Options are:
    
    - **Poor**—Applications with a health score range from 1-3.
    - **Fair**—Applications with a health score range from 4-7.
    - **Good**—Applications with a health score range from 8-10.
    - **All**—All applications.

- View application information in a table format. The application table lists information about the application, such as name, health, business class, traffic class, usage, average throughput, packet loss, latency, and application delay.

- Display a 360° view of an application by clicking the name of the application.
Monitor the Health of an Application

Use this procedure to view details about a specific application.

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

Step 2
Choose Health > Application.
The Application Health window appears.

Step 3
In the Application table, click the name of an application.
A 360° view of the application appears with the following information.

Table 28: Application 360 Window

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Historical Health Graph area</td>
<td>Health information about the selected application over a period of time.</td>
</tr>
<tr>
<td></td>
<td>To get the application health score at a particular time, hover your cursor over the time instance on the graph, for example, you can hover your cursor at 7:00, 7:05, 7:20, and so on.</td>
</tr>
<tr>
<td></td>
<td>Click View Details to open a side bar with additional details about the application.</td>
</tr>
</tbody>
</table>
Monitor Application Health

About Skype for Business Application Experience

Skype for Business (SfB) Application Experience (AX) augments the standard AX feature with charts and tables derived from metrics reported by SfB client endpoints.

Standard AX relies on Cisco NetFlow records exported by intermediate routers, which provide transport layer metrics from each router’s respective observation point, but not the end-to-end perspective that can be provided by an application itself.

SfB AX relies on the Skype for Business SDN Interface, which is Microsoft-provided software that consists of Dialog Listener and SDN Manager components. One or more Dialog Listeners receive events and metrics from SfB endpoints, and then send them to the SDN Manager, which in turn constructs and pushes XML messages to one or more configured subscribers, such as the SfB Collector.

At a high level, the flow of data is:

MS SfB Client > MS Dialog Listener(s) > MS SDN Manager > Cisco DNA Center SfB Collector

Note

SfB AX currently supports Skype for Business Server 2015 only.
Enable Skype for Business Application Experience

Use this procedure to enable SfB AX. To do so, you must configure the SDN Manager so that it can push call start and end events as well as quality updates to the Cisco DNA Center SfB collector.

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 23, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 27.

• Enable Cisco NetFlow collection on the device. See Enable Cisco NetFlow Collection, on page 106.

• Install and configure the Microsoft Skype for Business SDN Interface.

Step 1
On the server where the SDN Manager is installed, click the Start menu, and then choose SDNManager Powershell.

Step 2
From the Powershell prompt, enter the following command:

SDNManager p s subscriber-id submituri=subscriber-url

• subscriber-id is any case-insensitive identifier you want to use for the Cisco DNA Center SfB Collector.

• submituri is http://cisco-dna-center-hostname-or-IP-address:30732/api/services/skype/event.

Example:

SDNManager p s CiscoDNACenter submituri=http://cisco-dna-center.example.com:30732/api/services/skype/event

Note In some cases, running the SDNManager command in the SDNManager Powershell might not work because the SDN Interface installation process did not add the folder containing SDNManager.exe to the user or system path. In this case, you can either specify the full path to SDNManager.exe ("C:\Program Files\Microsoft Skype for Business Server\Microsoft Skype for Business SDN Manager\SDNManager.exe" by default), or add the containing folder to the user or system path.

Step 3
To review the default call server configuration, enter the following command: Get-CsMediaConfiguration.

The InCallQoSIntervalSeconds configuration parameter controls both the initial wait period before the SDN Manager sends its first call quality update, as well as the minimum interval between subsequent updates. For example, with the default value of 35 seconds, the first quality update is always sent 35 seconds after the start of a call. After that, if SfB determines that the quality of that call has changed significantly to warrant sending out additional quality updates, those updates will be sent no more than once every 35 seconds.

Before changing the default value, take into consideration that while lowering this value reduces the time before the first quality update is sent and reflected in Cisco DNA Center, it also reduces the minimum interval between quality updates. Because these updates are typically generated due to degraded network conditions, this can have the effect of exacerbating network issues with additional quality update traffic.

To change the default wait period, enter the following command: Set-CsMediaConfiguration -InCallQoSIntervalSeconds new-secs.

After you have completed the preceding steps, SDN Manager starts pushing call start and end events as well as quality updates to the Cisco DNA Center SfB collector.
What to do next

View the SfB AX for a Skype client from the Client 360 window.

View the Skype for Business Application Experience of a Skype Client

Use this procedure to view the SfB AX for a Skype client.

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 23, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 27.
- Enable Cisco NetFlow collection on the device. See Enable Cisco NetFlow Collection, on page 106.
- Enable Skype for Business Application Experience (SfB AX). See Enable Skype for Business Application Experience, on page 114.

Step 1

From the Client 360 page, scroll down to the Application Experience category.

If the client has SfB traffic, the application experience table displays one of the following radio buttons: ms-lync, ms-lync-audio, or skype. The radio button that displays depends on the application signatures that are used by the NBAR classification engines running on intermediate routers.

Step 2

To view the application experience metrics in chart format in a pop-up window, select the ms-lync, ms-lync-audio, or skype radio button.

Note SfB AX currently supports audio-related metrics only.

The following SfB data is provided:

- The line charts for Packet Loss and Network Latency include additional data series labeled Skype for Business, which corresponds to the metrics reported by the SfB client. Each data point represents the average packet loss or latency value reported by the client, aggregated over a 5 minute interval.

  Note The line charts for Throughput and Application Server Latency do not include additional data.

- The MOS bar chart displays Mean Opinion Score (MOS) metrics reported by the SfB client. Each bar represents the average MOS value reported by the client, aggregated over a 5 minute interval.

- The Call Summary table displays a row for each completed call, where the SDN Manager provides summarized metrics for the entire call.

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 15-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 and Network Latency.

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:

\[
\text{Individual Application Health Score} = \frac{\text{Latency\_Weight} \times \text{Latency\_VoS\_Score} + \text{Packet\_Loss\_Weight} \times \text{Packet Loss\_VoS\_Score}}{\text{Latency\_Weight} + \text{Packet\_Loss\_Weight}}
\]

The workflow for calculating the Individual Application Health score is as follows:

1. Obtain the Latency and Packet Loss KPIs from NetFlow record.
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 using the following formula from a scale of 1 to 10:

\[
\text{Individual Application Health Score} = \frac{\text{Latency\_Weight} \times \text{Latency\_VoS\_Score} + \text{Packet\_Loss\_Weight} \times \text{Packet Loss\_VoS\_Score}}{\text{Latency\_Weight} + \text{Packet\_Loss\_Weight}}
\]
CHAPTER 9

Manage Sensors and Sensor-Driven Tests

- About Sensors and Sensor-Driven Tests, on page 117
- View Sensor-Driven Tests, on page 118
- Add a Sensor-Driven Test, on page 119
- Monitor and Troubleshoot the Health of Wireless Sensors, on page 122
- Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 124
- Enable Provisioning SSID on the Wireless Controller, on page 125
- Create a Wireless Sensor Device Profile, on page 125
- Provision a Sensor Device, on page 126
- Edit, Delete, or Run a Sensor-Driven Test, on page 127

About Sensors and Sensor-Driven Tests

Sensors use sensor-driven tests to test the health of wireless networks. A wireless network includes AP radios, WLAN configurations, and wireless network services.

Assurance supports a dedicated sensor, which is dedicated hardware for performing sensor functions.

The dedicated Cisco Aironet 1800s Active Sensor gets bootstrapped using PnP. After this sensor obtains Assurance server-reachability details, it directly communicates with the Assurance server.

Supported Sensor and Cisco Wireless Controller Software Releases

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

- Cisco Wireless Controller (35xx, 55xx, 85xx)—Software Release 8.5.115.0
- Cisco Aironet 1800s Active Sensor—Software Release 8.7.258.0

Note

You can upgrade the Cisco Aironet 1800s Active Sensor with the SWIM App.
View Sensor-Driven Tests

Use this procedure to view all the sensor-driven tests that are configured in the system, and to determine the tests that have passed or failed.

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 124.

Step 1

From the Cisco DNA Center home page, choose Assurance > Manage > Sensor-Driven Tests.

The Sensor-Driven Tests window is displayed, listing all the sensor-driven tests configured in the system. It provides information such as the test name, location, schedule, SSIDs, types of tests that were run, latest results, results in the last 24 hours, and the time the last test was run.

![Figure 10: Sensor-Driven Tests Window](image)

<table>
<thead>
<tr>
<th>Test Name</th>
<th>Location</th>
<th>Schedule</th>
<th>SSIDs</th>
<th>Test Types</th>
<th>Last 24 hours</th>
<th>Latest</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired Test1</td>
<td>Multi-Site/SVC2/ SVC2, Row_1</td>
<td>Daily, every 30 mins</td>
<td>SVC2, 40000</td>
<td>Onboarding Test, IP Addressing Test, Host Reachability Test</td>
<td>Green Pass</td>
<td>Pass</td>
<td>Latest</td>
</tr>
<tr>
<td>Wireless Test2</td>
<td>Multi-Site/SVC2/ SVC2, Row_1</td>
<td>Daily, every 30 mins</td>
<td>SVC2, 40000</td>
<td>Onboarding Test, IP Addressing Test, Host Reachability Test</td>
<td>Green Pass</td>
<td>Pass</td>
<td>Latest</td>
</tr>
</tbody>
</table>

Note

In the test results, the colors indicate the following:

- **Green**—Pass
- **Red**—Fail
- **Yellow**—Slow. Test passed, but the test completion time was above the threshold.

Note

For Onboarding and IP addressing, the threshold is 5 seconds.

For all other sensor-driven tests, the threshold is 2 seconds.
Step 2  From the Details column, click Latest.
A side bar opens providing details, such as the sensor and AP combination used for the sensor-driven tests.

Step 3  If a test fails, the Latest column displays a red box. Click Fail to display information about the failed test.

Step 4  If a test is slow, the Latest column displays a yellow box. Click Slow to display information about the slow test.

---

Add a Sensor-Driven Test

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

Before you begin

- If you are using the Cisco Aironet 1800s Active Sensor to run sensor-driven tests, make sure that the sensor is provisioned using PnP, so that it displays under Inventory. See Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 124.

---

Step 1  From the Cisco DNA Center home page, choose Assurance > Manage > Sensor-Driven Tests.
The Sensor-Driven Tests window is displayed, listing all the sensor-driven tests configured in the system.

Step 2  To add a new sensor, click + Add Test at the top-right corner.
The Add Test window opens and the first step, Schedule Tests, is displayed.
Do the following:

a) In the **Test Name** field, enter the name of the sensor-driven test. Use letters, numbers, underscores, hyphens, and periods.

b) From the **Location** drop-down list, choose the location of the sensor. A table containing information about all the SSIDs, radios to test, security, and credentials, is displayed.

c) In the **Radios to Test** column, check the check box adjacent to the radios that you want to add to the test.

d) In the **Credentials** column, enter the username and password, if required.

e) From the **EAP** drop-down list, choose the Extensible Authentication Protocol (EAP) method. The three methods supported are **EAP-FAST**, **PEAP-MSCHAPv2**, and **EAP-TLS**. If you select the **EAP-TLS** method, you can select and upload a certificate (PKCS bundle) that is needed for the EAP-TLS. Then, enter the password associated with the certificate. Using this certificate and password, the test that is used to connect to the SSID is created.

f) Applicable for WebAuth Enabled SSIDs—For Layer 3 security, if WebAuth is enabled on the SSID, provide the following:

   - For WebAuth with user authentication, provide the necessary credentials.
   - For WebAuth with Passthrough, you can choose to provide an email address.
Manage Sensors and Sensor-Driven Tests

Add a Sensor-Driven Test

- Only **Internal Authentication** is supported for sensor testing.
- WebAuth is supported on Cisco Wireless Controllers and Cisco Aironet 1800s Active Sensors with Software Release 8.7.

Note

- From the **Interval Hours** drop-down list, choose the day and time to run the test. Default is every hour.

Step 3
Click **Next**. The second step, **Select Tests**, is displayed.

Step 4
From the **Select Tests** window, select the tests to run. Do the following:

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

- **IP Addressing Tests (DHCPv4)**—Connects to the SSID with credentials and gets the IP address through DHCP. It then verifies the gateway and DNS server received through DHCP.
- **DNS Tests**—Resolves IP address for the domain name.
- **Host Reachability Tests**—Verifies reachability using the Internet Control Message Protocol (ICMP) echo request.
- **RADIUS Tests**—The sensor acts as a Dot1x supplicant and authenticates through wireless. Dot1x supplicant supports protocols such as Protected Extensible Authentication Protocol (PEAP) with Password Authentication Protocol (PAP) or the Microsoft version of the Challenge-Handshake Authentication Protocol (MS-CHAP).

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

- **Speed Test**—If you have an Network Diagnostics Test (NDT) server, enter the IP address of the NTD server in the field provided. If the NDT server is reachable through a Proxy server, enter the IP address of the Proxy server in the field provided.
- **IPSLA Test**—Runs UDP Jitter, UDP Echo, Packet Loss, and Latency measurements from sensor to APs.
  
  To run the IPSLA test, choose a **Service Level** option for each SSID from the drop-down list. Options are: Platinum (voice), Gold (video), Silver (best effort), and Bronze (background).

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

- **Email Tests**—Includes the following:
  
  - **Internet Message Access Protocol (IMAP)**—Connects to IMAP server TCP port (143).
  - **Post Office Protocol3 (POP3)**—Connects to POP3 server TCP port (110).
  - **Outlook Web Server (OWS)**—Logs into the OWS and verifies access.

- **File Transfer Tests**—Tests for upload and download file operations.

Note

- The maximum file size for sensor test is 5MB.

- **Web Tests**—Tests for access to the provided URL and verification of the response data.

Step 5
Click **Next**. The third step, **Select Sensors**, is displayed.

- To set the RSSI threshold value, do the following:
Monitor and Troubleshoot the Health of Wireless Sensors

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

**Before you begin**

- Make sure you have added and scheduled sensor-driven tests. See [Add a Sensor-Driven Test, on page 119](#).

---

**Step 1**

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

**Step 2**

Choose **Dashboards > Sensor**.

The **Wireless Sensor** window appears with the following information:

**Table 29: Wireless Sensor Window**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
</table>
| **All SSIDs, All Bands, and Actions drop-down lists** | **All SSIDs**—Displays information for the SSID you choose from the drop-down list. Default is **All SSIDs**.  
**All Bands**—Displays information for the band frequency you choose from the drop-down list. Options are: **2.4 GHz, 5 GHz, or All Bands**.  
**Actions**—Allows you to make changes to the dashboard display when you choose **Edit Dashboards** from the drop-down list. See [Change the Position of a Dashlet, on page 145](#) and [Create a Custom Dashboard, on page 141](#). |
### Item Description

| **24 Hours** drop-down list and **Timeline Slider** | - **24 Hours**—Displays information on the window based on the time range you select. Do the following:
  1. From the **24 Hours** drop-down list, choose a time range: **3 hours, 24 hours**, or **7 days**.
  2. Specify the Start date and time; and the End date and time.
  3. Click **Apply**. This sets the time boundaries on the timeline slider.
- **Timeline Slider**—Allows you to specify a more granular time range.
  Move the timeline slider bars to the desired time range, and then click **Apply**. |

| **Hierarchical Site View or Building View** dashlet | - The [Show] button allows you to hide or display this dashlet.
- Click the [ ] button, and then choose the [Hierarchical Site View or Building View] from the drop-down list. Based on what you choose, the table provides the relevant information. To view information about a specific site, building, or floor, click **Apply** in the appropriate row. The information on the window is refreshed based on your selection. |

| **Sensor Health** dashlets | - Includes the following dashlets:
  - **Test Summary**—Donut chart that provides a count of failed, slow, and passed sensor-driven tests. The test results are color-coded and broken down according to the severity of the scores. Hover your cursor over a specific color on the donut chart to display the number of sensor-driven tests associated with that color.
  - **Failed by Test Type**—Donut chart that provides a breakdown of the types of sensor-driven tests that failed. It also provides information about the number of issues that were triggered by the sensor-driven tests.
    - Click **Global Issues** to view sensor-driven test issues.
  - **Top Locations by Failure**—Lists the top sites where the sensor-driven tests failed, and provides the number of tests that failed per site. |
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 Cisco Provisioning SSID on the wireless controller. See [Enable Provisioning SSID on the Wireless Controller, on page 125.](#)

**Step 2**
Create a sensor profile for the Cisco Aironet 1800s Active Sensor. See [Create a Wireless Sensor Device Profile, on page 125.](#)

**Step 3**
Provision the Cisco Aironet 1800s Active Sensor. See [Provision a Sensor Device, on page 126.](#)
Step 4 (Optional) After the sensor device is available in the device inventory, you can choose to upgrade the software image. See the "Provision Software Images" topic in the Cisco Digital Network Architecture Center User Guide.

### Enable Provisioning SSID on the Wireless Controller

**Step 1** Log in to the Cisco Wireless Controller.
The Network Summary page appears.

**Step 2** Click the Advanced tab.
The Summary page appears.

**Step 3** In the top menu bar, click the Management tab.

**Step 4** From the left-navigation pane, choose Cloud Services > Sensor.
The Backhaul Configuration page appears.

**Step 5** In the SSID field, enter TFTP.

**Step 6** From the Auth-type drop-down list, choose Open.

**Step 7** From the Provisioning drop-down list, choose Enable.

**Step 8** Make sure that the DHCP Interface drop-down list is set to Management.

**Step 9** Click Apply.

After Provisioning is enabled, a hidden WLAN is created, called CiscoSensorProvisioning, 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.

### Create a Wireless Sensor Device Profile

Creating the wireless sensor device profile is applicable for the Cisco Aironet 1800s Active Sensor.

**Step 1** Choose Design > Network Settings > Wireless.

**Step 2** Under Sensor Settings, click +Add.

The Create Sensor SSID Assignment window appears. Configure the following parameters:
- In the Settings Name field, enter a name for the sensor device profile.
- In the Wireless Network Name (SSID) field, enter a name for the SSID.
- In the Level of Security area, choose a security level, and then enter the appropriate credentials.

**Note** To provision the Cisco Aironet 1800s Active Sensor with wired connection, enter any proxy name and SSID (for example wired_xyz), and in the Level of Security area, choose Open.
Provision a Sensor Device

Provisioning a sensor device applies to Cisco Aironet 1800s Active Sensors.

Before you begin

Provisioning a sensor device is applicable only for Cisco Aironet 1800s Active Sensors.

- Make sure that the sensor device in your inventory is in an UNCLAIMED state.
- Make sure that you have created a profile for the sensor device. See Create a Wireless Sensor Device Profile, on page 125.
- Make sure that Cisco Aironet 1800s Active Sensor is reachable through the Cisco DNA Center's enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Cisco DNA Center. To claim the device, the device must have reachability to interface enp9s0's IP address.
- In the DHCP server, make sure that you configure the NTP server (DHCP option 42) and the vendor-specific DHCP option 43 with the ASCII value "5A1D;B2;K4;I172.16.x.x;J80", where 172.16.x.x is the virtual IP address of Cisco DNA Center associated with the enp9s0 interface.

Step 1
From the Cisco DNA Center home page, choose Provision > Devices.

The Device Inventory window appears.

Step 2
Click the Unclaimed Devices tab.

All unclaimed devices are displayed.

Step 3
Check the check box next to the sensor device that you want to provision.

Three tabs appear above the list of unclaimed devices.

Step 4
Click the Claim Device tab.

The Claim Device window appears, providing the serial number and device information.

Step 5
From the Choose a floor drop-down list, choose the floor where the sensor device is located.

Step 6
From the Sensor Select SSID Profile drop-down list, choose the profile name to associate to the sensor device.

Step 7
Click Assign.

Provisioning starts, and the sensor device appears in the device inventory.

If the provisioning succeeds, the Provision Status column in the Device Inventory window shows Success.
Edit, Delete, or Run a Sensor-Driven Test

**Step 1**  
From the Cisco DNA Center home page, choose **Assurance > Manage > Sensor-Driven Tests**.  
The Sensor-Driven Tests window is displayed, listing all the sensor-driven tests configured in the system.

**Step 2**  
To edit sensor-driven test information, from the **Actions** column, click the icon, and choose **Edit**.  
The wizard similar to the **Add Test** wizard opens, where you can update the information.

**Step 3**  
To delete a test, from the **Actions** column, click the icon, and choose **Delete**. Click **OK** in the confirmation dialog box.
Edit, Delete, or Run a Sensor-Driven Test
CHAPTER 10

Integrate Cisco CMX for Wireless Maps

- About Cisco Connected Mobile Experiences Integration, on page 129
- Add a User for the Cisco CMX API Server, on page 129
- Create Cisco CMX Settings, on page 130
- Troubleshoot Cisco CMX, on page 131

About Cisco Connected Mobile Experiences Integration

Cisco DNA Center supports the integration of on-premise Connected Mobile Experiences (CMX) for wireless maps. With the CMX integration, you can get the exact location of your clients on the floor map within the Cisco DNA Center user interface.

You can create CMX settings either at the global level or at the site, building, or floor level depending upon your requirement. For a small enterprise, you can assign CMX at the global level, which is the parent node and all the children inherit their settings from the parent node. For a medium enterprise, you can assign CMX at the building level and for a small enterprise, you can assign CMX at the floor level.

Supported Cisco CMX Software Releases

Cisco DNA Center supports the following Cisco CMX Software Releases:

- Cisco CMX 10.4.1
- Cisco CMX 10.5.0

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...
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 130.

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 129.

Step 1
Choose Design > Network Settings > Wireless.

Step 2
In the left tree view menu, select either Global or the area, building, or floor that you are interested in.

Step 3
Under CMX Settings, click Add.

The Create CMX Settings page appears.

Step 4
In the IP Address field, enter the valid IP address of the CMX web GUI.

Step 5
In the User Name and Password fields, enter the CMX web GUI username and password credentials.

Step 6
In the Admin User and Admin Password fields, enter the CMX admin username and password credentials.

Note
Make sure that CMX is reachable.

Step 7
Click Add.

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 synched, Cisco DNA Center starts querying the CMX for the client location and displays the location on the floor map.

From the floor map, you can do the following:
• View the location of the client, which is shown as a blue dot.

• Hover your cursor over an AP. A dialog box is displayed with Info, Rx Neighbor, and Clients tabs. Click each tab for more information. Click Device 360 to open the Device 360 window and view issues. Click an issue to see the location of the issue and the location of the client device.

• Click an AP to open a side bar with details about the AP.

• Perform real-time client tracking when Intelligent Capture and CMX are integrated.

**Step 8** If the CMX was down when you made changes, you must synchronize manually. To do so, on the Network Hierarchy page, click the gear icon next to the building or floor on which you made the changes in the left tree pane, and then choose Sync with CMX to push the changes manually.

---

**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
Manage Intelligent Capture

Note

Intelligent Capture is beta functionality for this release.

- About Intelligent Capture, on page 133
- View Data for Intelligent Capture, on page 134
- Monitor Intelligent Capture Details for a Client, on page 136
- Monitor Intelligent Capture Details for a Device, on page 139

About Intelligent Capture

Traditionally, in Cisco DNA Center, all the information such as device health, network health, and so on, is available from Cisco Wireless Controllers. The Intelligent Capture feature provides support to have a direct communication link between Cisco DNA Center and access points (APs), so each of the APs can communicate with Cisco DNA Center directly. Using this channel, the Cisco DNA Center can receive packet capture data, AP and client statistics, and spectrum data. With the direct communication between the Cisco DNA Center and APs, information is available with higher granularity. Hence, the Intelligent Capture feature in Cisco DNA Center allows you access to data from APs that is not available from the wireless controllers.

Supported Cisco Wireless Controller Software Release

Intelligent Capture is supported on the following wireless controller:

- Cisco Wireless Controller Software Release 8.8 MR1 and above

Supported APs

Intelligent Capture is supported on the following APs:

- AP4800I-X-K9
- AP2802I-X-K9
- AP2802E-X-K9
- AP3802I-X-K9
- AP3802E-X-K9
View Data for Intelligent Capture

Use this procedure to view the captured data coming from the access points and to perform basic setup for capturing data.

Before you begin

- Configure Assurance. See Basic Setup Workflow, on page 13.
- 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 23, Discover Your Network Using CDP, on page 18, or Discover Your Network Using LLDP, on page 27.
- Time zones need to be synchronized between the Cisco DNA Center and the Cisco Wireless Controller for full packet capture to work. Use the `config time` and `show time` commands on the wireless controller to set and display the time.

Step 1

From the Cisco DNA Center home page, click the Assurance tab, and then choose Manage > Scheduled Captures. The Intelligent Capture window appears with the packet capture details, such as Location, Start Time, Duration, Clients, Status, and Actions.

Figure 12: Intelligent Capture Window

Step 2

To configure global AP settings for intelligent capture, click Global Auto-Capture Settings. See Set up Global Auto-Capture, on page 135.
**Step 3** To schedule the capture of onboarding packets and collection of client RF statistics, click **Schedule Onboarding Packet Capture**. See **Schedule Onboarding Packet Capture and Client RF Statistics, on page 135**.

---

**Set up Global Auto-Capture**

Use this procedure to set up access points globally for anomaly feedback and for RF statistics. You can set four Global Auto-Capture settings for each site that a wireless controller has been assigned to.

**Step 1** In the **Intelligent Capture** window, click **Global Auto-Capture Settings** located at the top-right corner of the window.

The **Auto-Capture Settings** window appears.

**Step 2** Select a row (Site), and click the **Anomaly Triggered Packet Capture** or **Anomaly Triggered Event** toggle buttons to turn on/off the capture of anomaly-triggered packets and events generated from the APs.

To enable **Anomaly Triggered Packet Capture**, you must first enable **Anomaly Triggered Event**.

**Step 3** Select a row (Site), and click the **AP Radio Statistics** toggle button to turn on/off the capture of radio statistics generated from the APs.

**Step 4** Select a row (Site), and click the **AP WLAN Statistics** toggle button to turn on/off the capture of WLAN statistics generated from the APs.

---

**Schedule Onboarding Packet Capture and Client RF Statistics**

Use this procedure to schedule the capture of onboarding packets and client RF statistics from the APs in a location or floor. The analysis starts at the scheduled start time when the selected clients associate with the APs at the target location.

**Step 1** In the **Intelligent Capture** window, click **Schedule Onboarding Packet Capture** located in the top-right corner of the window.

The **Schedule Onboarding Packet Capture and Client RF Statistics** window appears.

**Step 2** Use the **Target Location** drop-down list to choose the location or floor from which you want to capture the onboarding packets. You can also use the **Search Dropdown** field to search and select the target location.

**Step 3** Use the **Start Time** radio buttons and the **Duration** drop-down list to specify if you want to capture packets now or at a later time and the duration of the packet capture, respectively. If you choose the **Run Later** radio button, you can specify the date and time for the packet capture to begin.

**Step 4** In the **Client** area, enter the client user ID or MAC address.

You can select a maximum of 16 clients per floor or location.

**Step 5** Click **Save** to save your changes.
Monitor Intelligent Capture Details for a Client

Use this procedure to view, monitor, and troubleshoot captured onboarding and data packets for a specific client device and to determine if there are potential issues that must be addressed.

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

**Step 2**
Click **Health > Clients**.
The **Client Health** window appears.

**Step 3**
Do one of the following:
- In the **Client Devices** table, click the hyper linked 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** located at the top-right corner of the window.
The **Intelligent Capture** window for the specific client that you selected appears with the following information.

**Table 30: Client 360 Intelligent Capture Window**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Timeline Slider with Onboarding Events Line Chart** | Onboarding events—Successful events in green and failed events in red.  
1 Hour drop-down list—Displays information on the onboarding events line chart based on the time range you select. You can select 1 Hour, 3 Hours, or 8 Hours.  
You can click the right and/or left timeline slider bar, and move it to the desired time or time range. |
| **Real-Time Client Tracking area** | The floor map associated with the client that shows the APs and the client locations is displayed. As this is live tracking, if the client moves to another location, that is also displayed. |
| **RF Stats charts** | RF Statistics for the client. Different charts for RSSI and SNR, Tx and Rx Data Rate, and so on, are displayed. You can hover and move your cursor over the charts to see the statistics for a particular time.  
Click the **Play** button at the top-right corner of the window to view the graph of the RF statistics in real-time. The data on the graph moves (at a fixed time interval) for every update. You can use this button to pause the movement on the graph as well. |
### Set Up NAM Integration

If you have a NAM or vNAM server running software version 6.4(1) or later, follow this procedure to integrate Cisco DNA Center with your NAM server. 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 at the bottom of the Summary display on the Intelligent Capture Client 360.
The table and charts provide information on the applications used by the client, their QoS settings, packet loss, and wireless delay and jitter.

**Before you begin**

To integrate the GRPC collector with Network Analysis Module (NAM), you must configure a valid IP address on the data port of the NAM/vNAM if you have not done so already. Note that 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. Do the following:

1. Log in to the CLI of the NAM server.
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
   ```
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.
4. Run the **show data-port ip-addresses** command again to verify that data-port 1 has been assigned an IP address.
5. Record the IP address of data-port 1 or one of the other displayed ports.
6. Verify that **cdb-export** is enabled to 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**.
7. Make sure that the time is synchronized on the NAM/vNAM with Cisco DNA Center. This can be done using the NAM user interface: **Administration > System > System Time**.

---

**Step 1**

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

**Step 2**

Click **GRPC-Collector**. The **GRPC-Collector** window opens.

**Step 3**

Click + Add. The **gRPC Collector Configuration** window opens.

**Step 4**

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

a) In the **ConfigData** area, check the **Agent Export** check box to enable the export of network packet data to NAM.

b) In **Agent IP Address** field, enter the IP address of the data port recorded (refer to Step 5 of the prerequisites).

c) In the **Configuration Name** field, enter a unique name for the GRPC-Collector configuration.

d) Click **Save Configuration**.
Monitor Intelligent Capture Details for a Device

Use this procedure to view and monitor captured onboarding and data packets for a specific device and to determine if there are potential issues that must be addressed.

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

Step 2
Click **Health > Network**.
The **Network Health** window appears.

Step 3
Do one of the following:
- From the **Network Devices** dashlet, click the device name from the **Device** column.
- In the **Search** field (located at the top-right corner), enter the device name, IP address, or MAC address.

A 360° view of the device appears.

Step 4
In the Device 360 window, click the **Intelligent Capture** hyperlink at the top-right corner of the window to open the **Intelligent Capture** page for that specific device.

**Table 31: Device 360 Intelligent Capture Window**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF Stats tab</td>
<td>Contains the different RF statistics charts for the AP.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Clients</strong>—Displays the number of clients using the AP. Hover and move your cursor over the timeline chart to view the number of clients using the AP for a particular time, so more granularity of information is displayed.</td>
</tr>
<tr>
<td></td>
<td>Next to the <strong>Clients</strong> chart, the chart for the <strong>Top Clients with Tx Failed Packets by SSID</strong> is displayed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Channel Utilization</strong>—Displays the channel utilization (%) for the AP. Hover and move your cursor over the bar graph to view the channel utilization details for different devices (AP, Wi-fi devices, and so on) for a particular time.</td>
</tr>
<tr>
<td></td>
<td>Next to the <strong>Channel Utilization</strong> chart, the chart for the <strong>Channel Utilization by This Radio</strong> is displayed with details, such as SSID, Client, and Packet.</td>
</tr>
</tbody>
</table>

More charts such as Frame Count, Tx Power and SNR, and so on are also displayed. All these charts provide more granular readings in the charts.

**Note**
To filter the data shown on this page, you can use the **2.4 GHz** drop-down list to choose either 2.4 GHz or 5 GHz radios. The color-coded statistics in a chart are described by the text below the chart, and can be filtered by selecting the colored radio button.
<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| Spectrum Analysis tab| Contains the Spectrum Analysis and Interference charts for the AP. The Spectrum analysis window is made up of three charts (from top to bottom): Persistence, Waterfall, and Interference charts. All the charts refresh every 30 seconds and show data for the last three minutes.  

  - **Persistence and Waterfall Charts**—The Persistence and Waterfall charts display information relating to the RF environment of the AP. The AP’s radios (in whichever operational mode, band, and channel they are configured for) measure the amplitude of any heard signals. Both charts use the X-axis to represent the signal’s frequency. The Persistence chart plots the amplitude of the heard signals on the Y-axis; the color represents how many signals are heard on the same frequency (refer to the color bar below both charts) and the opacity represents the age of the data on the chart (older data is less opaque). The Waterfall chart plots the time of the measured signal on the Y-axis and uses color to represent the amplitude.  

  - **Interference Chart**—The Interference chart plots any sources of RF interference as circles. The frequency is represented on the X-axis. The Y-axis on the chart is the interference’s calculated severity index (higher severity means more impactful interference). The circle’s diameter represents the interference’s bandwidth. The color of the circle correlates with the type of interference (Bluetooth beacon, radar, video camera, and so on).  

|
Manage Dashboards

- About Dashboards, on page 141
- Create a Custom Dashboard, on page 141
- Create a Dashboard From a Template, on page 143
- View a Dashboard, on page 144
- Edit or Delete a Dashboard, on page 144
- Duplicate a Dashboard, on page 145
- Mark a Dashboard as a Favorite, on page 145
- Change the Position of a Dashlet, on page 145

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.

See the following topics for more information:

- Create a Custom Dashboard, on page 141
- Create a Dashboard From a Template, on page 143
- View a Dashboard, on page 144
- Edit or Delete a Dashboard, on page 144
- Duplicate a Dashboard, on page 145
- Mark a Dashboard as a Favorite, on page 145
- Change the Position of a Dashlet, on page 145

Create a Custom Dashboard

Step 1

From the Cisco DNA Center home page, choose Assurance > Dashboards > Dashboard Library.

The Dashboard Library window appears, listing all the defined dashboards.
Step 2  Click Create a Dashboard located in the top-right corner.

Step 3  In the Create a Dashboard dialog box, enter a title for the dashboard.

Step 4  Click Save.

Step 5  Click Add a Dashlet to add content to this dashboard.

Step 6  Choose a category from the drop-down list or use the search box at the right to find a dashlet by name or tag.

Step 7  Click on a dashlet description to see it in the preview pane.

Step 8  Check the check box next to each dashlet that you want to add to the dashboard.

Step 9  Click Add to display the dashboard.

Step 10  Drag and drop the dashlets to change their arrangement on the dashboard.

Step 11  Click the trash can icon to delete a dashlet.

Step 12  Click Add Dashlet to add another dashlet.

Step 13  Click Save to save the dashboard.

A confirmation dialog is displayed.

Step 14  Click OK.
Create a Dashboard From a Template

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

Step 1 From the Cisco DNA Center home page, choose Assurance > Dashboards > Dashboard Library.

The Dashboard Library window appears, listing all defined dashboards and the templates (at the bottom).

Step 2 Click on 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 14 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.

Step 7 Enter a scope name and click Next.

Step 8 Choose one or more locations to include in the scope by checking or unchecking the check boxes next to them. Use the search field to filter locations.

Step 9 Click Next.

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. Use the search field to filter SSIDs. This filter applies only to wireless devices.
- **Host Name**—Enter the host names to include in the scope. Use the percent sign (%) as a wildcard and press Enter after each entry.
- **Device Type**—Enter the device OS types (for example, iOS or Android) to include in the scope. Use the percent sign (%) as a wildcard and press Enter after each entry.
- **MAC Address**—Enter the MAC addresses to include in the scope. Use the percent sign (%) as a wildcard and press Enter after each entry.
- **IPAddress**—Enter the IP addresses to include in the scope. Use the percent sign (%) as a wildcard and press Enter after each entry.

Step 11 If you are using the Network Health template, you can use the following filters:

- **Network Device Type**—Choose one or more device types to include in the scope by checking or unchecking the check boxes next to them. Use 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. Use 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 host names to include in the scope. Use the percent sign (%) as a wildcard and press Enter after each entry.

Step 12 Click Next to see a preview of the selected clients or network devices.
Step 13  Click **Save** to save the scope with a dynamic list of clients or network devices that updates over time based on the selected filters.

Alternately, click the **Dynamic list** toggle to use a static list of clients that does not update. You can use the **Filter** control, or type any table value in the search field, to filter devices further. Select each device that you want to include in the static list by checking the check box next to it in the table, then click **Save** to save the scope.

A confirmation dialog is displayed.

Step 14  Click **OK**.

Step 15  Drag and drop the dashlets to change their arrangement on the dashboard, which is open in editing mode.

Step 16  Click **Save** to save the dashboard.

A confirmation dialog is displayed.

Step 17  Click **OK**.

If this is a new scope, it can take up to 15 minutes to display data in the dashboard.

---

### View a Dashboard

**Step 1**  From the Cisco DNA Center home page, choose **Assurance > Dashboards > Dashboard Library**.

The **Dashboard Library** window appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by entering its name in the **Find** field.

**Step 2**  To see dashboards marked as favorites, click **Favorite Dashboards**.

**Step 3**  Click on the dashboard that you want to view.

**Step 4**  In the dashboard controls, click **Show** or **Hide** to show or hide the map, if applicable.

**Step 5**  (Optional) Filter dashboard data by time period, sites, or domains by choosing the appropriate values from the filters.

---

### Edit or Delete a Dashboard

**Step 1**  From the Cisco DNA Center home page, choose **Assurance > Dashboards > Dashboard Library**.

The **Dashboard Library** window appears, listing all the defined dashboards. You can use the **Sort By** control to sort dashboards by date or name. You can search for a dashboard by entering its name in the **Find** field.

**Step 2**  Click the dashboard that you want to edit or delete.

**Step 3**  Do one of the following:

- To make changes, choose **Edit Dashboard** from the **Actions** menu. You can add or delete dashlets and drag dashlets to different positions in the dashboard. Click **Save** when you are done.
• To delete the dashboard, choose Delete Dashboard from the Actions menu. Click Delete in the confirmation dialog.

---

**Duplicate a Dashboard**

**Step 1**
From the Cisco DNA Center home page, choose Assurance > Dashboards > Dashboard Library.

The Dashboard Library window appears, listing all the defined dashboards. You can use the Sort By control to sort dashboards by date or name. You can search for a dashboard by entering its name in the Find field.

**Step 2**
Click on the duplicate icon for a dashboard (next to the star icon).

**Step 3**
In the Duplicate Dashboard dialog box, enter a title for the dashboard copy.

**Step 4**
Click Save.

**Step 5**
You can change this copied dashboard by adding, deleting, or rearranging dashlets.

**Step 6**
Click Save to save the dashboard.

A confirmation dialog is displayed.

**Step 7**
Click OK.

---

**Mark a Dashboard as a Favorite**

**Step 1**
From the Cisco DNA Center home page, choose Assurance > Dashboards > Dashboard Library.

The Dashboard Library window appears, listing all the defined dashboards. You can use the Sort By control to sort dashboards by date or name. You can search for a dashboard by entering its name in the Find field.

**Step 2**
Click the star icon.

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 Overall Health window, Network Health window, and the Client Health window.

**Step 1**
Do one of the following as appropriate:

• From the Cisco DNA Center home page, choose Assurance > Health > Overall Health.

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

**Step 2**  From the **Actions** menu (located at the top-right corner), choose **Edit Dashboard**.
The window is refreshed and becomes editable.

**Step 3**  Click the dashlet that you want to move and drag it to a different position in the dashboard.

**Step 4**  Click **Save**.
CHAPTER 13

Issues Detected by Assurance

- About Issues, on page 147
- View Global Issues, on page 147
- View All Issues, on page 148
- Client Issues, on page 150
- Switch and Fabric Issues, on page 161
- Router Issues, on page 163
- Access Point and Wireless Controller Issues, on page 164
- Sensor Issues, on page 165

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.

You can view issues from the following pages:

- **Overall Health** — Assurance landing page.
- **Global Issues** — Assurance > Issues tab.
- **Client 360** — Assurance > Health > Client. From the Client Devices table, click the MAC address to display the Client 360 window.
- **Device 360** — Assurance > Health > Network. From the Network Devices table, in the Device column, click the device name to display the Device 360 window.

Click an issue to display details, such as the summary of the issue, impact, and suggested actions. Some client and AP issues also show an additional floor map to aid troubleshooting. To resolve an issue, from the Status field, choose Resolve.

View Global Issues

Use this procedure to view all the high-impact issues detected by Assurance.
Step 1  From the Cisco DNA Center home page, click Assurance > Issues > Global Issues.
The Global Issues window is displayed with two tabs: Open and Resolved. The open issues are displayed by default.

Step 2  The issues that are displayed are based on the time range you select from the 24 Hours drop-down list.
Options are: 3 Hours, 24 Hours, or 7 Days. Default is 24 Hours.

Step 3  View the priority of the issue in the Priority column.
By default, the issues are color coded and sorted by their preassigned priority level, starting with P1. Click the arrow next to the Priority column to sort the issues.

Step 4  To view issue details, click the hyperlinked issue title.
Details such as the summary of the issue, impact, and suggested actions display. Some client and AP issues also show an additional floor map to help with troubleshooting.
To resolve an issue, from the Status drop-down list, choose Resolve.

Step 5  To view all the issues that are resolved, click the Resolved tab.

---

View All Issues

Use this procedure to view all the issues that Assurance is capable of monitoring in a customer environment, the types of issues that are reported, and the root cause of the issues.

Step 1  From the Cisco DNA Center home page, click Assurance > Issues > View All Issues.
The All Issues window appears with the following information:
24 Hours drop-down list

**24 Hours**—Displays information on the page based on the time range you select. Do the following:

1. From the **24 Hours** drop-down list, choose a time range: 3 hours, 24 hours, or 7 days.
2. Specify the Start date and time; and the End date and time.
3. Click **Apply**. This sets the time boundaries on the timeline slider.

**Timeline Slider**

Allows you to specify a more granular time range. Click the timeline slider bar, and then move it to the desired time range.
**Client Issues**

**Connectivity Issues**

The following table provides a list of connectivity issues detected by Assurance:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Unable to Connect—Invalid Credentials</td>
<td>This client failed to authenticate due to an invalid username or password.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Client Unable to Connect—4-Way Handshake Issue Misconfigured PSK</td>
<td>This client failed to authenticate and complete the 4-way handshake due to a misconfigured WPA or WPA2 preshared key.</td>
</tr>
</tbody>
</table>
| Client Unable to Connect to SSID on AP—Client Side Timeout | This client failed to connect to SSID on AP Name (2.4 GHz | 5 GHz) due to client timeout during the authentication process.  
*Note* These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in Global Issues. |
| Value Clients Unable to Connect to SSID—Credentials Rejected | Value clients failed to connect to SSID because the client credentials are getting rejected during the authentication process. |
| Client Unable to Connect to SSID—AAA Failure | This client failed to connect to SSID because of an AAA failure during the authentication phase.  
*Note* These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in Global Issues. |
| Value Clients Unable to Connect to SSID—Authentication Parameters Rejected | Value clients failed to connect to SSID because the client authentication parameters are getting rejected during the authentication process. |
| Client Unable to Connect to SSID on AP and Wireless Controller—AAA Server Side Timeout | This client failed to authenticate and complete the 4-way handshake SSID on AP Name (2.4 GHz | 5 GHz) and Wireless Controller Name because the wireless controller did not receive a response from the AAA server IP Address.  
*Note* These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in Global Issues. |
| Client Unable to Connect to SSID on Wireless Controller—Security Parameter Mismatch | This client failed to authenticate and complete the authentication because the security parameters have a mismatch issue.  
*Note* These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in Global Issues. |
| Value Clients Unable to Connect to SSID on Wireless Controller—Wireless Controller Operational Errors | Value clients failed to connect because of operational errors on Wireless Controller Name during the authentication process. |
| Client Unable to Connect to SSID on Wireless Controller—Wireless Controller Configuration Issue | This client failed to authenticate and complete the authentication because of issues in the Wireless Controller Name configuration. |
### Client Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Clients Unable to Connect to SSID on Wireless Controller—Wireless Controller Operational Errors</td>
<td>Clients experienced wireless controller operational errors. Value clients failed to connect because of configuration issues in the Wireless Controller Name during the authentication process.</td>
</tr>
<tr>
<td>Client Unable to Connect to SSID through AP and Wireless Controller—Client PMK Not Found</td>
<td>This client failed to connect to SSID through the AP Name (2.4 GHz</td>
</tr>
<tr>
<td>Network Latency for Application is Above the Threshold Value.</td>
<td>The client Client Name is experiencing high network latency for application AP Name located at site Site Name.</td>
</tr>
<tr>
<td>Dual Band-Capable Client Prefers 2.4 GHz over 5 GHz Radio</td>
<td>This dual band-capable client is consistently connecting to 2.4 GHz radio although 5 GHz radio that provides a better experience, is available. This client is on SSID and AP Name, which is connected to Wireless Controller Name.</td>
</tr>
<tr>
<td>Wireless Client Exhibiting Sticky Behavior</td>
<td>This client is maintaining an association with AP Name at RSSI Threshold dBm RSSI, which is a weaker signal. The client should roam to an available AP that has a stronger signal. This client was connected to SSID on frequency GHZ radio on AP Name in location Site Hierarchy. The AP is connected to Wireless Controller Name.</td>
</tr>
<tr>
<td>802.11r FT Client Roaming Slowly</td>
<td>This client supports Fast Transition and is roaming slowly. This client has performed one or more full 802.1X authentications while roaming between APs when it could roam faster with 802.11r/FT.</td>
</tr>
</tbody>
</table>

#### RF Condition Issues

The following table provides a list of RF condition issues detected by Assurance.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Associated with AP Experiencing Poor RF Condition on SSID</td>
<td>This client's RSSI has been below Value dBm for more than Value minutes. This client is experiencing poor RF condition because the client is unable to roam to the available neighboring APs that have better coverage.</td>
</tr>
</tbody>
</table>
### Issue

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This AP has Value clients that have RSSI Values below Value dBm for more than Value minutes. These clients are considered to be in poor RF condition as their signal is weak and they are not roaming to other APs.</td>
</tr>
<tr>
<td>This client is roaming excessively between AP Name and AP Name. This client is probably located in a coverage area where the signal from SSIDs is unstable, or where the signal of several SSIDs and the roaming threshold are similar.</td>
</tr>
<tr>
<td>This client is alternating excessively between SSID and SSID. This client is probably located in a coverage area where the signal from SSIDs is unstable, or where the signal of several SSIDs and the roaming threshold are similar.</td>
</tr>
<tr>
<td>This client is roaming excessively between the 2.4 GHz and 5 GHz radios on AP Name.</td>
</tr>
</tbody>
</table>

### DHCP Issues

The following table provides a list of DHCP issues detected by Assurance.

**Table 35: DHCP Issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Clients Experiencing DHCP Failure on DHCP Server</td>
<td>Value clients have not been assigned an IP Address from the DHCP server Server IP.</td>
</tr>
<tr>
<td>Value Clients in AP Group Experiencing DHCP Failure</td>
<td>Value clients assigned to AP Group Name have not been assigned an IP address from the DHCP server Server IP.</td>
</tr>
<tr>
<td>Wireless Client Failed to Connect to SSID on AP (2.4 GHz</td>
<td>5 GHz) Because DHCP IP Addressing Timed Out</td>
</tr>
<tr>
<td>Note</td>
<td>These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in Global Issues.</td>
</tr>
</tbody>
</table>
| Value Clients Failing DHCP Attempts in AP Group Because DHCP IP Addressing Timed Out | • DHCP Server—Value clients timed out and have not been assigned an IP Address from the DHCP server Server IP.  
• AP Group—Value clients assigned to AP Group Name timed out and have not been assigned an IP address from the DHCP server Server IP. |
### Client Issues

**Description**

This client has not been assigned an IPv4 address by DHCP server Server IP on SSID over VLAN VLAN-ID. This DHCP server has not responded to DHCP discover requests. This client is currently associated with AP Name (2.4 GHz | 5 GHz).

**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**.

| Value Wireless Clients Failed to Connect to SSID—No Response form DHCP Server |
| Description |
| Value clients assigned to VLAN VLAN-ID in Location have not been assigned an IP address. The DHCP server Server IP is not responding to DHCP requests. |

| Client on SSID and Associated with AP (2.4 GHz | 5 GHz) Failed to Obtain IPv4 Address—Client Side Root Cause |
| Description |
| Client failed to complete the DHCP transaction with DHCP server Server IP. Client is associated to SSID on AP Name (2.4 GHz | 5 GHz) radio. |

**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**.

| Value Wireless Clients Failed to Connect to SSID—Client Side Root Cause |
| Description |
| Value assigned to VLAN VLAN-ID in Location failed to complete the DHCP transaction with DHCP server Server IP. |

| Client Failed to Obtain IPv4 Address from DHCP Server |
| Description |
| This client with MAC Address was has not been assigned an IPv4 address from the DHCP server Server IP. This DHCP server is not responding to DHCP discover requests. |

**Apple iOS Client Issues**

The following table provides a list of Apple iOS client issues detected by Assurance.

**Table 36: Apple iOS Client Issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple iOS Client Disconnected from SSID on AP—Client Internal Event</td>
<td>This Apple iOS client, running Apple iOS iOS Version, got disconnected from the network because of reasons that are internal to the client, such as software or operating system actions. This client was connected to SSID on AP Name in Location.</td>
</tr>
</tbody>
</table>

**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**.
This Apple iOS client failed to decrypt multiple frames from the AP, and consequently disconnected from the SSID on AP Name radio Radio Index.

Note These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in Global Issues.

Apple iOS Client Disconnected from SSID on AP—Captive Portal Verification Failure

This Apple iOS client disconnected from SSID on AP Name because the captive-portal internet verification process failed.

Note These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in Global Issues.

### Client Excessive Onboarding Issues

The following table provides a list of client excessive onboarding issues detected by Assurance.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| Apple iOS Client Disconnected from SSID on AP—Decryption Failure | This client is taking longer than expected time to connect to SSID on AP Name (2.4 GHz | 5 GHz):  
  - Onboarding took *Value* seconds (expected time should be less than *Value* seconds).  
  - Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). |
| Apple iOS Client Disconnected from SSID on AP—Captive Portal Verification Failure | These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in Global Issues. |

Some issues provide a floor map with AP positioning.

If Cisco Connected Mobile Experiences (CMX) is being managed, the location of the client is also provided.

### Table 37: Client Excessive Onboarding Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on Authentication and Key Exchange from the Network/Server Side | This client is taking longer than expected time to connect to SSID on AP Name (2.4 GHz | 5 GHz):  
  - Onboarding took *Value* seconds (expected time should be less than *Value* seconds).  
  - Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). |
<p>| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on Authentication and Key Exchange from the Network/Server Side | These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in Global Issues. |</p>
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on Authentication and Key Exchange Because of RF Issue on the Client Side | This client is taking longer than expected to connect to SSID on AP Name (2.4 GHz | 5 GHz):
- Onboarding took \( \text{Value} \) seconds (expected time should be less than \( \text{Value} \) seconds).
- Authentication and Key Exchange took \( \text{Value} \) seconds (expected time should be less than \( \text{Value} \) seconds).

**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**. |
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on IP Addressing | This client is taking longer than expected to connect to SSID on AP Name (2.4 GHz | 5 GHz):
- Onboarding took \( \text{Value} \) seconds (expected time should be less than \( \text{Value} \) seconds).
- Authentication and Key Exchange took \( \text{Value} \) seconds (expected time should be less than \( \text{Value} \) seconds).

| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on Onboarding | This client is taking longer than expected to connect to SSID on AP Name (2.4 GHz | 5 GHz):
- Onboarding took \( \text{Value} \) seconds (expected time should be less than \( \text{Value} \) seconds).
- Association took \( \text{Value} \) seconds (expected time should be less than \( \text{Value} \) seconds).
- Authentication and Key Exchange took \( \text{Value} \) seconds (expected time should be less than \( \text{Value} \) seconds).
- IP Addressing took \( \text{Value} \) seconds (expected time should be less than \( \text{Value} \) seconds).

**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**. |
| Wireless Clients Taking a Long Time to Connect to SSID—Excessive Time on Authentication and Key Exchange Time from the Network/Server Side | Value clients taking longer than expected to connect to SSID in Location. The server is taking longer than usual to respond:
- These clients took \( \text{Value}\% \) longer than association time baseline of \( \text{Value} \) Time-Unit.
- These clients took \( \text{Value}\% \) longer than authentication and 4-way handshake time baseline of \( \text{Value} \) Time-Unit. |
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| Clients Experiencing Excessive Onboarding Time—Excessive IP Addressing on DHCP Server | This client is taking longer than expected to connect to SSID on AP Name (2.4 GHz | 5 GHz):  
• Onboarding took *Value* seconds (expected time should be less than *Value* seconds).  
• Authentication and Key Exchange took *Value* seconds (expected time should be less than *Value* seconds). The wireless controller was identified as the slow component in the process.  
**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in *Global Issues*.  
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on Authentication and Key Exchange Because of Wireless Controller Issues |  
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on Authentication and Key Exchange Because of Issues from the Client Side |  
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | 5 GHz)—Excessive Time on Authentication and Key Exchange Because of Slow Network |  
| | }
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Note</th>
</tr>
</thead>
</table>
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | This client is taking longer than expected to connect to SSID on AP Name (2.4 GHz | 5 GHz):  
  • Onboarding took $Value$ seconds (expected time should be less than $Value$ seconds).  
  • Authentication and Key Exchange took $Value$ seconds (expected time should be less than $Value$ seconds). The network was slow to carry the authentication messages.                                                                 | These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**.                                                                                                                                 |
| (2.4 GHz | 5 GHz)—Excessive Time on Authentication and Key Exchange Because of Server Issues | |                                                                                                                                                                                                                                                                                                                                                                                                     |
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | This client is taking longer than expected to connect to SSID on AP Name (2.4 GHz | 5 GHz):  
  • Onboarding took $Value$ seconds (expected time should be less than $Value$ seconds).  
  • IP addressing took $Value$ seconds (expected time should be less than $Value$ seconds).                                                                                                                                                                                                                                               | These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**.                                                                                                                                 |
| (2.4 GHz | 5 GHz)—Excessive IP Addressing Time Because of DHCP Failures | |                                                                                                                                                                                                                                                                                                                                                                                                     |
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | This client is taking longer than expected time to connect to SSID on AP Name (2.4 GHz | 5 GHz):  
  • Onboarding took $Value$ seconds (expected time should be less than $Value$ seconds).  
  • Association took $Value$ seconds (expected time should be less than $Value$ seconds).                                                                                                                                                                                                                                               | These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**.                                                                                                                                 |
| (2.4 GHz | 5 GHz) - Excessive Association Time | |                                                                                                                                                                                                                                                                                                                                                                                                     |
| Wireless Client Taking a Long Time to Connect to SSID on AP (2.4 GHz | This client is taking longer than expected to connect to SSID on AP Name (2.4 GHz | 5 GHz)—Association Failures  
  • Onboarding took $Value$ seconds (expected time should be less than $Value$ seconds).  
  • Association took $Value$ seconds (expected time should be less than $Value$ seconds).                                                                                                                                                                                                                                               | These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**.                                                                                                                                 |
| (2.4 GHz | 5 GHz)—Association Failures | |                                                                                                                                                                                                                                                                                                                                                                                                     |
### Issue

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Device Authentication Failed—Dot1.x Failure</td>
<td>The client device <em>Device Name</em> could not be authenticated because <em>Failure Reason</em>.</td>
</tr>
<tr>
<td>Client Device Authentication Failed—MAB Failure</td>
<td>The client device <em>Device Name</em> could not be authenticated because <em>Failure Reason</em>.</td>
</tr>
<tr>
<td>Client Failed to Obtain a Response from DNS Server</td>
<td>The client <em>MAC Address</em> failed to obtain a response from the DNS Server <em>DNS Server IP</em> because the server is unreachable or is no longer responding to queries.</td>
</tr>
</tbody>
</table>

### Client Exclusion Issues

The following table provides a list of client exclusion issues that are detected by Assurance:

#### Table 38: Client Exclusion Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Excluded by Wireless Controller—Too Many Web Authentication Failures</td>
<td>This client has been excluded by <em>Wireless Controller Name</em> due to <em>Value</em> or more failed AAA authentication attempts within <em>Value</em> seconds. This client is probably failing authentication because of invalid username or password.</td>
</tr>
<tr>
<td>Wireless Client Unable to Roam to AP—Too Many Web Authentication Failures</td>
<td>This client is unable to roam <em>AP Name</em> (*2.4 GHz</td>
</tr>
<tr>
<td><em>Value</em> Wireless Clients Failed to Roam on <em>SSID</em> as Clients were Excluded Before Roaming—Too Many Web Authentication Failures</td>
<td><em>Value</em> clients connected to <em>SSID</em> in <em>Location</em> have been excluded due to <em>Value</em> or more failed web authentication attempts on web authentication server (LWA, redirect value, or CWA Value) within <em>Value</em> seconds. Because these clients were excluded, they could not roam.</td>
</tr>
<tr>
<td><em>Value</em> Wireless Clients Failed to Roam on <em>SSID</em> as Clients were Excluded Before Roaming—Too Many Failed Authentication</td>
<td><em>Value</em> clients connected to <em>SSID</em> in <em>Location</em> have been excluded due to <em>Value</em> or more failed AAA authentication attempts within <em>Value</em> seconds. Because these clients were excluded, they could not roam.</td>
</tr>
<tr>
<td>Client Excluded on <em>SSID</em> on AP (2.4 GHz</td>
<td>5GHz)—Too Many Authentication Failures</td>
</tr>
<tr>
<td><em>Value</em> Clients Excluded by Wireless Controller—Authentication Failures</td>
<td><em>Value</em> clients have been excluded by <em>Wireless Controller Name</em> due to <em>Value</em> or more failed AAA authentication attempts within <em>Value</em> seconds. These clients are probably failing authentication on AAA server <em>Server IP</em> because of invalid usernames or passwords.</td>
</tr>
</tbody>
</table>
### Client Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
</table>
| Client Excluded on SSID on AP (2.4 GHz | 5 GHz)—Too Many Web Authentication Failures | This client has been excluded by Wireless Controller Name on web authentication server (LWA, redirect value, or CWA Value) due to Value or more failed Web authentication attempts within Value seconds. This client is probably failing authentication because of an invalid username or password.  
**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**. |
| Client Excluded on SSID and Wireless Controller—IP Theft Issue       | This client was excluded on SSID and Wireless Controller Name. The client was rejected for reusing the IP address of another active client.  
**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**. |
| Client Excluded on SSID and Wireless Controller—IDS Shunned List    | This client was excluded on SSID on AP Name (2.4 GHz | 5 GHz) and Wireless Controller Name. This client was identified by the IDS as a threat and was shunned.  
**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**. |
| Client Excluded on SSID and Wireless Controller—Too Many Association Failures | This client was excluded on SSID on AP Name (2.4 GHz | 5 GHz) and Wireless Controller Name because this client failed 802.11 association too many times.  
**Note** These issues are applicable for both single clients and multiple clients. Issues for multiple clients are displayed in **Global Issues**. |

### Mobility Failure Issues

The following table provides a list of mobility failure issues detected by Assurance.

**Table 39: Mobility Failure Issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Unable to Roam on SSID—AAA Server Rejected Client</td>
<td>This client failed to authenticate and complete the 4-way handshake while roaming from AP Name to AP Name because the AAA server IP Address rejected the client.</td>
</tr>
<tr>
<td>Client Unable to Roam on SSID on Wireless Controller—Security Parameter Mismatch.</td>
<td>This client failed to authenticate and complete the authentication while roaming from AP Name and Wireless Controller Name to AP Name and Wireless Controller Name because the security parameters had a mismatch issue.</td>
</tr>
</tbody>
</table>
Switch and Fabric Issues

The following table provides a list of switch and fabric issues detected by Assurance.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Experiencing High CPU Utilization</td>
<td>CPU utilization on Device Name has exceeded threshold% in the last 30 minutes.</td>
</tr>
<tr>
<td>Device Experiencing High Memory Utilization</td>
<td>Memory utilization on Device Name has exceeded threshold% in the last 30 minutes.</td>
</tr>
<tr>
<td>Device Experiencing High Temperature</td>
<td>The temperature on Device Name has exceeded threshold% degree Celsius in the last 30 minutes.</td>
</tr>
<tr>
<td>Fan Failure on Device</td>
<td>The fans in Device Name have failed critically.</td>
</tr>
<tr>
<td>Power Supply Failure on Device</td>
<td>The power supplies in Device Name have failed critically.</td>
</tr>
<tr>
<td>Switch Rebooting</td>
<td>The Switch Name is rebooting because of a power outage or system crash.</td>
</tr>
<tr>
<td>Interface Name Flapping in the Network</td>
<td>The switch port Interface Name has flapped Value times within the past Value minutes.</td>
</tr>
</tbody>
</table>
## Switch and Fabric Issues

**Issue** | **Description**
--- | ---
Controller Unable to Reach Network Device | This network device *Device Name* with *Device Role* is unreachable from the controller.

High Input/Output Utilization on Interface | Interface *Interface Name* is experiencing high input/output utilization:

- **Rx Rx Input Utilization %**
- **Tx Tx Output Utilization %**

High Input/Output Errors on Interface | Interface *Interface Name* is experiencing high input/output errors:

- **Rx Rx Error Percent %**
- **Tx Tx Error Percent %**

Stackmember Running an Incompatible Image | Stack member is running an incompatible image.

Stackmember Removed from Stack | Stack member has been removed from the stack.

PoE Power Controller: *Error Message* | PoE power controller error *Error Message* detected on the switch.

Interface Power Overdrawn | The power on the *Interface Name* is overdrawn.

Switch Experiencing TCAM Exhaustion | The switch *Switch Name* has a TCAM area that exceeds a threshold of 95%.

<table>
<thead>
<tr>
<th><strong>Fabric Issues</strong></th>
</tr>
</thead>
</table>

The following table provides a list of fabric issues detected by Assurance:

**Table 41: Fabric Issues**

<table>
<thead>
<tr>
<th><strong>Issue</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Down on <em>Role</em> Node Fabric-Facing Interface</td>
<td>The status of the <em>Role</em> node fabric-facing <em>Interface Name</em> is down, which is impacting many fabric services from functioning properly.</td>
</tr>
</tbody>
</table>

| Reachability Issue Between Fabric Edge Device and Fabric Border Device in Physical Network | There is a connectivity failure between the Fabric Edge device *Source Device IP* and the Fabric Border device *Destination Device IP* in the physical network, which is impacting many fabric services from functioning properly. |

| Reachability Issue Between Fabric Edge Device and Fabric Control Plane in Physical Network | There is a connectivity failure between the Fabric Edge device *Source Device IP* and the Fabric Control Plane device *Destination Device IP* in the physical network, which is impacting many fabric services from functioning properly. |

| Reachability Issue Between Fabric Border Device and Fabric Control Plane in Physical Network | There is a connectivity failure between the Fabric Border device *Source Device IP* and the Fabric Control Plane device *Destination Device IP* in the physical network, which is impacting many fabric services from functioning properly. |
### Issues Detected by Assurance

#### Router Issues

The following table provides a list of router issues detected by Assurance.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
<th>Data Source</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP Connectivity from Router Interface to Service Provider Gateway Failed</strong></td>
<td>Router &quot;&lt;Router Name&gt;&quot; at &lt;Router location&gt;—IP connectivity from router interface &lt;Interface Name&gt; to service provider gateway &lt;Gateway IP address&gt; failed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Router Received Error Message From Neighbor Interface &quot;Passive 2/2 (Peer in Wrong AS)&quot;</strong></td>
<td>Router &quot;&lt;Router IP Address&gt;&quot; at &lt;Router location&gt;—Border Gateway Protocol (BGP) peering with neighbor interface &lt;Interface IP address&gt; failed due to Autonomous System (AS) Number mismatch. The configured AS number does not match with peer.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>BGP is Flapping on Router Interface Because of Missing BGP Hello Keepalives or Peer Terminating Session</strong></td>
<td>Router &quot;&lt;Router IP Address&gt;&quot; at &lt;Router location&gt;—BGP is flapping on interface &lt;Interface IP Address&gt; because of missing BGP hello keepalives or because of a peer terminating the session.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Access Point and Wireless Controller Issues

The following table provides a list of access point and wireless controller issues detected by Assurance.

**Table 42: AP and Wireless Controller Issues**

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP is Currently Down</td>
<td>This <em>AP Name</em> is no longer connected to a wireless controller. This AP was previously connected to the switch <em>Switch Name</em> and Port ID.</td>
</tr>
<tr>
<td>AP Flapping Between Wireless Controller(s)</td>
<td>The <em>AP Name</em> has disconnected from <em>Old Wireless Controller Name</em> and reconnected to <em>Current Wireless Controller Name</em>.</td>
</tr>
<tr>
<td>AP Experiencing High CPU Utilization</td>
<td>CPU utilization for the <em>AP Name</em> has exceeded the <em>Threshold</em>% threshold. This issue is potentially impacting <em>Value</em> clients.</td>
</tr>
<tr>
<td>AP Experiencing High Memory Utilization</td>
<td>Memory utilization for the <em>AP Name</em> has exceeded the <em>Threshold</em>% threshold. This issue is potentially impacting <em>Value</em> clients.</td>
</tr>
<tr>
<td>AP Rebooted Due to a Hardware or Software Crash</td>
<td>The <em>AP Name</em> has rebooted due to a hardware or software crash.</td>
</tr>
<tr>
<td>The 2.4 GHz Radio on AP Experiencing High Utilization</td>
<td>The 2.4-GHz radio on the <em>AP Name</em> has exceeded the <em>Threshold</em>% threshold and is currently experiencing <em>Utilization</em>% utilization. This issue is impacting <em>Value</em> clients.</td>
</tr>
<tr>
<td>The 5 GHz Radio on AP Experiencing High Utilization</td>
<td>The 5-GHz radio on the <em>AP Name</em> has exceeded the <em>Threshold</em>% threshold and is currently experiencing <em>Utilization</em>% utilization. This issue is impacting <em>Value</em> clients.</td>
</tr>
</tbody>
</table>
## Sensor Issues

The following table provides a list of sensor issues detected by Assurance.

### Table 43: Sensor Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Experiencing a Coverage Hole</td>
<td>The AP Name is currently experiencing a coverage hole. Value client(s) have had their RSSI threshold lower than -60 dBm over the last 3 minutes. These clients are considered to be in a coverage hole because they are unable to roam to neighboring APs with improved coverage because the APs are not available.</td>
</tr>
<tr>
<td>High Memory Utilization on Wireless Controller</td>
<td>Memory utilization in the Wireless Controller Name has exceeded the Threshold % threshold in the past 15 minutes. This issue is potentially impacting Value clients.</td>
</tr>
<tr>
<td>Wireless Controller Rebooted</td>
<td>The Wireless Controller Name has rebooted due to a hardware or software crash.</td>
</tr>
<tr>
<td>High AP License Utilization on Wireless Controller</td>
<td>The Wireless Controller Name is licensed to support Max-Count APs and it currently has In Use Count APs. If this trend continues, this wireless controller will exhaust all of its AP licenses.</td>
</tr>
<tr>
<td>Power Supply on Wireless Controller Failed</td>
<td>The Power Index power supply has failed on the Wireless Controller Name. This wireless controller is now operating with a single power supply.</td>
</tr>
<tr>
<td>Wireless Controller Not Exporting Data</td>
<td>The Wireless Controller Name is not exporting WSA data. It was previously connected to the switch NW Device Name and port Target Interface Name. The switch port is currently Link Status.</td>
</tr>
<tr>
<td>Wireless Controller Not Exporting AP Data</td>
<td>The Wireless Controller Name is not exporting WSA AP data since the last 15 minutes.</td>
</tr>
<tr>
<td>Wireless Controller Not Exporting Client Data</td>
<td>The Wireless Controller Name is not exporting Client data since the last 15 minutes.</td>
</tr>
<tr>
<td>Wireless Controller AP License Exhaustion</td>
<td>The Wireless Controller Name is currently licensed to support Max-Count APs and is now operating at its full licensed capacity. No additional AP can join this wireless controller.</td>
</tr>
<tr>
<td>Excessive Time Lag Between Cisco DNA Center and Wireless Controller</td>
<td>The time on Cisco DNA Center and wireless controller Wireless Controller Name has drifted too far apart. The drift between the two devices is Time. Cisco DNA Center cannot process the wireless client data accurately if the time difference is more than 10 minutes.</td>
</tr>
</tbody>
</table>

### Table 43: Sensor Issues

<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value Sensors Failed to Connect to the Wireless Network</td>
<td>Value sensors from Location failed to connect to SSID. They either failed to associate, or authenticate, or get an IP address.</td>
</tr>
</tbody>
</table>

The time on Cisco DNA Center and wireless controller Wireless Controller Name has drifted too far apart. The drift between the two devices is Time. Cisco DNA Center cannot process the wireless client data accurately if the time difference is more than 10 minutes.
<table>
<thead>
<tr>
<th>Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value Sensors Failed to Get an IPv4 Address from the DHCP Server</strong></td>
<td><em>Value</em> sensors from <em>Location</em> have failed to get an IPv4 address from DHCP server <em>IP Address</em> in <em>VLAN ID</em>. The DHCP server is reachable.</td>
</tr>
<tr>
<td><strong>Value Sensors Slow to Get an IPv4 Address from the DHCP Server</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are slow to get an IPv4 address from DHCP server <em>IP Address</em>. The sensors are getting an IPv4 address on an average in <em>Value</em> seconds. Clients should be able to get an IPv4 address in 5 seconds. If this problem is not resolved, users will have a poor onboarding experience.</td>
</tr>
<tr>
<td><strong>Value Sensors Unable to Reach the DNS Server</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are unable to reach the DNS server <em>IP Address</em>. Pings are failing, which will impact user connectivity.</td>
</tr>
<tr>
<td><strong>Value Sensors Unable to Resolve Domain Name with the DNS Server</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are unable to resolve the given <em>Test Domain Name</em> with the DNS server <em>IP Address</em>. This will impact connectivity. The DNS server is reachable.</td>
</tr>
<tr>
<td><strong>Value Sensors Experiencing Slow Response from the DNS Server Host</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow response from the DNS server host <em>IP Address</em>. The ping response time to the host is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.</td>
</tr>
<tr>
<td><strong>Value Sensors Experiencing Slow Name Resolution from the DNS Server</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow name resolution time from the DNS Server <em>IP Address</em>. The name resolution time is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network or server issue that could lead to slow performance.</td>
</tr>
<tr>
<td><strong>Value Sensors Not Able to Reach the Test Host</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are not able to reach test host <em>IP Address</em>. Pings to the hosts are failing.</td>
</tr>
<tr>
<td><strong>Value Sensors Experiencing Slow Response from the Host</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow response from the host <em>IP Address</em>. The ping response time to the host is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.</td>
</tr>
<tr>
<td><strong>Value Sensors Experiencing Slow Response from the Local Gateway</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow response from their local gateway in VLAN <em>x, y</em>. The ping response time to the gateway is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.</td>
</tr>
<tr>
<td><strong>Value Sensors Not Receiving a Response from their Local Gateway</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are reporting no ping responses from their local gateway in VLAN <em>x, y</em>. This might indicate a network issue that could lead to network access problems.</td>
</tr>
<tr>
<td><strong>Value Sensors Not Able to Reach the RADIUS Server</strong></td>
<td><em>Value</em> sensors from <em>Location</em> are not able to reach the RADIUS server host <em>IP Address</em>. Pings are failing.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Experiencing Slow Response from the RADIUS Server</td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow response from the RADIUS server host <em>IP Address</em>. The ping response time to the host is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow onboarding.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Experiencing Slow Authentication Time with the RADIUS Server</td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow authentication time with RADIUS server <em>IP Address</em>. The sensors are authenticating on an average in <em>Value</em> seconds. Clients should be able to authenticate in 3 seconds. This slow authentication could lead to poor onboarding experience.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Failed to Authenticate with the RADIUS Server</td>
<td><em>Value</em> sensors from <em>Location</em> are unable to authenticate with the RADIUS server <em>IP Address</em>.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Unable to Reach the Outlook Web Access Host</td>
<td><em>Value</em> sensors from <em>Location</em> are not able to reach the Outlook Web Access host <em>IP Address</em>. Pings to the Outlook Web Access hosts are failing.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Experiencing Slow Response from the Outlook Web Access Host</td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow response from the Outlook Web Access host <em>IP Address</em>. The ping response time to the host is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow Outlook Web Access performance.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Experiencing Slow Response from the Outlook Web Access' First Hop Gateway</td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow response from their Outlook Web Access' first hop gateway in VLAN <em>x, y</em>. The ping response time to the gateway is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Experiencing Slow Mail Connection Time to Outlook Web Access</td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow connection time to the Outlook Web Access <em>IP Address</em>. The sensors are connecting to the Outlook Web Access on an average in <em>Value</em> seconds. Clients should be able to connect to the Outlook Web Access in <em>Value</em> seconds. This might lead to poor mail experience.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Failed to Connect to the Outlook Web Access</td>
<td><em>Value</em> sensors from <em>Location</em> are unable to connect to the Outlook Web Access. Users might not be able to send mail.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Unable to Reach the Web Server</td>
<td><em>Value</em> sensors from <em>Location</em> are not able to reach the Web server host <em>IP Address</em>. Pings to the web server hosts are failing.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Experiencing Slow Response from the Web Server</td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow response from the Web server host <em>IP Address</em>. The ping response time to the host is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow web performance.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><em>Value Sensors Experiencing Slow Response from the Web Server First Hop Gateway</em></td>
<td><em>Value sensors from Location</em> are reporting slow response from their Web server's first hop gateway in VLAN <em>x,y</em>. The ping response time to the gateway is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow performance.</td>
</tr>
<tr>
<td><em>Value Sensors Experiencing Slow Web Response Time from the Web Server</em></td>
<td><em>Value sensors from Location</em> are reporting slow web page load time from the Web server <em>IP Address</em>. The sensors are connecting and loading the web page on an average in <em>Value</em> seconds. Clients should be able to load the page in <em>Value</em> seconds. This could lead to poor web experience.</td>
</tr>
<tr>
<td><em>Value Sensors Failed to Load Page from the Web Server</em></td>
<td><em>Value sensors from Location</em> are unable to load a page with the Web server <em>IP Address</em>.</td>
</tr>
<tr>
<td><em>Value Sensors Unable to Reach the SSH Server</em></td>
<td><em>Value sensors from Location</em> are not able to reach the SSH server host <em>IP Address</em>. Pings are failing.</td>
</tr>
<tr>
<td><em>Value Sensors Experiencing Slow Response from the SSH Server</em></td>
<td><em>Value sensors from Location</em> are reporting slow response from the SSH server host <em>IP Address</em>. The ping response time to the host is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow SSH performance.</td>
</tr>
<tr>
<td><em>Value Sensors Experiencing Slow SSH Login Time</em></td>
<td><em>Value sensors from Location</em> are reporting slow SSH login time to SSH server <em>IP Address</em>. The sensors are connecting on an average in <em>Value</em> seconds. Clients should be able to connect in <em>Value</em> seconds. This could lead to poor SSH experience.</td>
</tr>
<tr>
<td><em>Value Sensors Unable to Connect with the SSH Server</em></td>
<td><em>Value sensors from Location</em> are unable to connect with the SSH server <em>IP Address</em>.</td>
</tr>
<tr>
<td><em>Value Sensors Unable to Reach the Mail Server</em></td>
<td><em>Value sensors from Location</em> are not able to reach the Mail server host <em>IP Address</em>. Pings are failing.</td>
</tr>
<tr>
<td><em>Value Sensors Experiencing Slow Response from the Mail Server</em></td>
<td><em>Value sensors from Location</em> are reporting slow response from the Mail server host <em>IP Address</em>. The ping response time to the host is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow mail performance.</td>
</tr>
<tr>
<td><em>Value Sensors Experiencing Slow Connection Time to the Mail Server</em></td>
<td><em>Value sensors from Location</em> are reporting slow connection time to the Mail server <em>IP Address</em>. The sensors are connecting to the Mail server on an average in <em>Value</em> seconds. Clients should be able to connect in <em>Value</em> seconds. This can lead to poor mail experience.</td>
</tr>
<tr>
<td><em>Value Sensors Unable to Connect to the Mail Server</em></td>
<td><em>Value sensors from Location</em> are unable to connect to the Mail server <em>IP Address</em>. Users might not be able to use mail services.</td>
</tr>
<tr>
<td><em>Value Sensors Unable to Reach the FTP Server</em></td>
<td><em>Value sensors from Location</em> are not able to reach the FTP server host <em>IP Address</em>. Pings are failing.</td>
</tr>
<tr>
<td>Issue</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Experiencing Slow Response from the FTP Server</td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow responses from the FTP server host <em>IP Address</em>. The ping response time to the host is on an average <em>Value</em> seconds and it should take less than 2 seconds. This slow response might indicate a network issue that could lead to slow FTP performance.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Experiencing Slow FTP Transfer Time with the FTP Server</td>
<td><em>Value</em> sensors from <em>Location</em> are reporting slow FTP transfer time with the FTP server <em>IP Address</em>. The sensors are transferring a file size <em>Value</em> on an average in <em>Value</em> seconds. Clients should be able to do this in <em>Value</em> seconds. This could lead to poor FTP application experience.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors Failed to Transfer File with the FTP Server</td>
<td><em>Value</em> sensors from <em>Location</em> are unable to transfer file with the FTP server <em>IP Address</em>. Users might not be able to use FTP services on this server.</td>
</tr>
<tr>
<td><strong>Value</strong> Sensors are Unable to Connect to the FTP Server</td>
<td><em>Value</em> sensors from <em>Location</em> are unable to connect to FTP server <em>IP Address</em>. Users might not be able to use FTP services on this server.</td>
</tr>
</tbody>
</table>
Schedule Reports

Use Cisco DNA Center platform to sample and schedule reports. For details, see the Cisco DNA Center Platform User Guide.

- Overview, on page 171
- Sample and Schedule Reports, on page 171

Overview

To deploy Cisco DNA Center platform for your network, perform the following steps:

1. Install or upgrade to the Cisco DNA Center software version that supports Cisco DNA Center platform.

   For information about installing Cisco DNA Center, see the Cisco Digital Network Architecture Center Installation Guide. For information about upgrading to Cisco DNA Center, Release 1.2.5, refer to the specific release notes for Release 1.2.5.

2. Ensure that the Cisco DNA Center platform application is downloaded and installed on Cisco DNA Center.

3. Configure the integration settings.

   For details, see the Cisco DNA Center Platform User Guide at Cisco Digital Network Architecture Center User Guide.

Sample and Schedule Reports

Perform this procedure to configure specialized data reports about your network. You can configure data reports using the Data and Reports window in the Cisco DNA Center GUI.
Before you begin

- Ensure that you have installed or upgraded to Cisco DNA Center Release GA 1.2.5, and have downloaded and installed the Cisco DNA Center platform application. To review the status of the Cisco DNA Center platform application in the GUI, click the gear icon (⚙️) and choose System Settings > Software Updates > Installed Apps. For information about managing applications, see the Cisco Digital Network Architecture Center Administrator Guide.

- Run a successful Discovery job in Cisco DNA Center to configure and schedule reports about device and network data. You can check whether a Discovery job is successful in Device Inventory. From the Home page, click Provision > Device Inventory > Inventory to view discovery results.

Step 1

From the Cisco DNA Center Home page, either click Schedule and Download Data and Reports under the Platform header or click Platform > Developer Toolkit > Data and Reports at the top of the page.

The Catalog view is the default window for Data and Reports and should appear. If it does not appear, then click Catalog underneath the Data and Reports header.

Step 2

Review the Catalog window.

The Catalog window displays supported catalog items that the reports are created about. Each catalog item is represented by a tile and contains links to both a sample report and to configure (schedule) a report.

Step 3

Determine which catalog item you wish to create a report about in the Catalog window.

Step 4

In the catalog item tile, click Sample to view a sample report.

A Preview window appears for the sample report. Use the side bar in the window to scroll down and review the entire sample report. The following data is presented:

- Applied filters (data filters that were used to build the report).
• Graphical representation of the data (including line, bar, and pie graphs).
• Tables that assist you in analyzing the data.

**Note** You can use the sample report in the **Preview** window to determine how you want your report to look.

**Step 5** Click X to close the preview.

**Step 6** In the catalog item tile, click **Schedule** to configure parameters to build a report.

The **Schedule** window opens where you can apply filters for data for your reports, as well as set up schedules for the actual report generation.

**Step 7** In the **Schedule** window, configure the parameters to build your report.

The **Schedule** window is divided into the following fields:

• **Format**—Accept the default report name or create a new one, select the data type (if there is more than one option for data type), and select the file type (if there is more than one option for file type).

• **Filters**—Select the filters for your the data in your report.

• **Schedule**—Select the date and time for the report generation.

**Step 8** Click the **Schedule** button.

The **My Downloads** window opens with instance details of the report that was scheduled.

---

**What to do next**

Proceed to review your report instance in **My Downloads** window.

**Note**

You can duplicate, download, edit, or delete the report in the **My Downloads** window.
Troubleshoot Cisco DNA Center Using Data Platform

• About Data Platform, on page 175
• Troubleshoot Cisco DNA Center Using the Analytics Ops Center, on page 176
• View or Update Collector Configuration Information, on page 177
• Configure Data Retention Settings, on page 178
• View Pipeline Status, on page 178

About Data Platform

Data Platform provides tools that can help you monitor and troubleshoot Cisco DNA Center applications. **Data Platform** displays synthesized data from various inputs to help you identify patterns, trends, and problem areas in your network. For example, if something goes wrong in your network, you can quickly get answers to questions such as whether a pipeline is in an error state and what is the real-time traffic flow in a particular area. The main areas of Data Platform are:

• **Analytics Ops Center**—The Analytics Ops Center provides a graphical representation of how data is streamed through collectors and pipelines and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network. See Troubleshoot Cisco DNA Center Using the Analytics Ops Center, on page 176.

• **Collectors**—Collectors collect a variety of network telemetry and contextual data in real time. As data is ingested, Cisco DNA Center correlates and analyzes the data. You can view the status of collectors and quickly identify any problem areas. See View or Update Collector Configuration Information, on page 177.

• **Store Settings**—Allows you to specify how long data is stored for an application. See Configure Data Retention Settings, on page 178.

• **Pipelines**—Pipelines allow Cisco DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas. See View Pipeline Status, on page 178.
Troubleshoot Cisco DNA Center Using the Analytics Ops Center

The Analytics Ops Center provides a graphical representation of how data is streamed through collectors and pipelines, and provides Grafana dashboards, which can help you identify patterns, trends, and problem areas in your network, such as:

- Missing data in Assurance.
- Inaccurate health score.
- Devices appear as monitored under Inventory but unmonitored under Assurance.

---

**Step 1**
From the Cisco DNA Center home page, click the gear icon and then choose System Settings > Data Platform.

**Step 2**
Click Analytics Ops Center.

A list of applications are displayed. For example, Assurance and Pegasus.

**Step 3**
Click the application name for which you want to view metrics, for example, Assurance.

A graphical representation of all the existing collectors and pipelines in the application appear. CPU or throughput values corresponding to each pipeline are also provided.

The current health status of each component is indicated by its color:

- Red—indicates an error.
- Yellow—indicates a warning.
- Grey—indicates normal operation.

**Step 4**
To view historical data of pipelines, click Timeline & Events.

A timeline bar providing data for the time interval appears. You can also:

- Move the timeline slider to view data for a specific time.
- Hover your cursor over an event in the timeline bar to display additional details or a group of events that occurred at the same time.
- Click on an event to display the Analytics Ops Center visualization at that particular time.

**Step 5**
To view additional details to help you troubleshoot an issue and determine the cause of an error or warning, click a Collector Name.

A side bar appears with the following tabs:

- **Metrics**—Provides a selection of available metrics gathered during the last 30 minutes. It displays summary information indicating the component status, start and stop time, and exceptions if errors have occurred. You can also select a different time interval.
- **Grafana**—Displays a dashboard associated with the respective component for deeper debugging.

**Step 6**
To view whether data is flowing through a specific pipeline, click on a pipeline stream.
A sidebar appears with graphs. The graphs display whether the application is receiving data from the underlying pipelines. The graph information is based on the time interval you select from the drop-down list in the sidebar. Options are Last 30 Min, Last Hour, Last 2 Hours, and Last 6 Hours. Default is Last 30 Min.

Step 7
If a pipeline is not flowing at normal levels, hover your cursor over the stream to display the lag metrics.

Step 8
To view detail information for a specific pipeline, click a Pipeline Name.

The appropriate Pipeline page displays with the following tabs:

- **Note** Make sure to click the Exceptions tab to determine if any exceptions have occurred in the pipeline. Under normal working conditions, this tab displays null.

  - Metrics—Displays metrics, updated every 30 minutes in a graph.
  - Summary—Displays summary information such as stats, run-time, and manifest.
  - Exceptions—Displays any exceptions that have occurred on the pipeline.
  - Stages—Displays the pipeline stages.

Step 9
To change the metrics you want displayed in the Analytics Ops Center page, click Key Metrics, select up to two metrics, and then click Apply.

By default, Cisco DNA Center displays CPU and Throughput metrics.

Step 10
To view metrics for a particular flow, do the following:

a) Click View Flow Details.
b) Select three connected components (collector, pipeline, and store) by clicking the tilde (,) located on the component's top left corner.
c) Click View Flow.

Cisco DNA Center displays the metrics associated with that specific flow.

---

**View or Update Collector Configuration Information**

Collectors collect a variety of network telemetry and contextual data in real time. As data is ingested, Cisco DNA Center correlates and analyzes the data. You can view the status of collectors and quickly identify any problem areas.

**Step 1**
From the Cisco DNA Center home page, click the gear icon and choose System Settings > Data Platform.

**Step 2**
Click Collectors. The colored dot next to each collector indicates its overall status.

**Step 3**
To view additional details, click a collector name.

The appropriate Collector page displays. By default, Cisco DNA Center displays the Current Configurations list.

**Step 4**
To view, update, or delete a configuration, click a specific configuration name.

**Note** In Cisco DNA Center 1.2.x, configuration information for some of the collectors cannot be updated. If you try to update the configuration for those collectors, the following error message is displayed: **Not able to retrieve collector data. Retry?** Ignore this error message.
Step 5 To add a new configuration, click + Add.
In the side bar that opens, enter the required information, and then click Save Configuration.

**Note**
- **Collector-ISE**: To hide a *wired* client's username, check the Anonymize check box in the ISE Collector Configuration window.
- **Wireless-Collector**: To hide a *wireless* client's username, check the Anonymize check box in the Wireless Collector Configuration window.

When you check the Anonymize check box, the user ID in the Client Health window appears scrambled.

Step 6 To view configured instances, click the Instances tab.
Step 7 To view summary information and metrics, choose an instance from the list.

### Configure Data Retention Settings

You can specify how long data is stored for an application.

**Step 1** From the Cisco DNA Center home page, click the gear icon and then choose System Settings > Data Platform.
**Step 2** Click Store Settings.
**Step 3** To view a list of historical purge jobs that have completed, click Data Purge Schedule.
The History table lists the name of the purge job, the result, time, and other data. You can sort, filter, and export data in the table.
**Step 4** To view or modify the current data retention and purge settings, click Data Retention & Purge Configuration.
Click the data for which you want to view or modify data retention and purge configuration settings:
- **Time Series Document Store**—Settings for all time-based data.
- **Trigger Store**—Storage space dedicated to issues detected by various data analysis algorithms.
- **Time Series Graph Store**—Settings for all time-based graphical data.

### View Pipeline Status

Data pipelines allow Cisco DNA Center applications to process streaming data. A data pipeline encapsulates an entire series of computations that accepts input data from external sources, transforms that data to provide useful intelligence, and produces output data. You can view the status of pipelines and quickly identify any problem areas.

**Step 1** From the Cisco DNA Center home page, click the gear icon and choose System Settings > Data Platform.
**Step 2** Click Pipelines.
Step 3  
To view whether the application is receiving data from the underlying pipelines, click a pipeline name.

The appropriate Pipeline page displays with the following tabs:

Note  
Make sure to click the Exceptions tab to determine if any exceptions have occurred in the pipeline. Under normal working conditions, this tab displays null.

- **Metrics**: Displays metrics, updated every 30 minutes in a graph.
- **Summary**: Displays summary information such as stats, run-time, and manifest.
- **Exceptions**: Displays any exceptions that have occurred on the pipeline.
- **Stages**: Displays the pipeline stages.
Related Documentation

The following publications are available for Cisco DNA Center.

<table>
<thead>
<tr>
<th>For this type of information...</th>
<th>See this document...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release information, including new features, system requirements, and open and resolved bugs.</td>
<td>Cisco DNA Center Release Notes</td>
</tr>
<tr>
<td>Installation and configuration of Cisco DNA Center, including post-installation tasks.</td>
<td>Cisco DNA Center Installation Guide</td>
</tr>
<tr>
<td>Use of the Cisco DNA Center GUI and its applications.</td>
<td>Cisco DNA Center User Guide</td>
</tr>
<tr>
<td>Configuration of user accounts, RBAC scope, security certificates, authentication and password policies, and global discovery settings. Monitoring and managing Cisco DNA Center services. Backup and restore.</td>
<td>Cisco DNA Center Administrator Guide</td>
</tr>
<tr>
<td>Supported devices, such as routers, switches, wireless access points, and software releases.</td>
<td>Supported Devices</td>
</tr>
<tr>
<td>Use of the Cisco DNA Assurance GUI.</td>
<td>Cisco DNA Assurance User Guide</td>
</tr>
<tr>
<td>Licenses and notices for open source software used in Cisco DNA Assurance.</td>
<td>Open Source Used in Cisco DNA Assurance</td>
</tr>
<tr>
<td>Use of the Cisco DNA Center platform GUI and its applications.</td>
<td>Cisco DNA Center Platform User Guide</td>
</tr>
<tr>
<td>Cisco DNA Center platform release information, including new features, deployment, and open bugs.</td>
<td>Cisco DNA Center Platform Release Notes</td>
</tr>
<tr>
<td>For this type of information...</td>
<td>See this document...</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>Licenses and notices for open source software used in Cisco DNA Center platform.</td>
<td>Open Source Used in Cisco DNA Center Platform</td>
</tr>
<tr>
<td>Key features and scale numbers.</td>
<td>Cisco DNA Center Data Sheet</td>
</tr>
</tbody>
</table>