



# Assurance Features and Navigation

---

Cisco DNA Center 1.1.2 Training

## Copyright Page

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://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. (1005R)

THIS DOCUMENT IS CONSIDERED CISCO PROPERTY AND COPYRIGHTED AS SUCH. NO PORTION OF COURSE CONTENT OR MATERIALS MAY BE RECORDED, REPRODUCED, DUPLICATED, DISTRIBUTED OR BROADCAST IN ANY MANNER WITHOUT CISCO'S WRITTEN PERMISSION.

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.

### *Assurance Features and Navigation*

© Copyright 2018 Cisco Systems, Inc. All rights reserved.

## Contents

### What Should I Know Before I Start?

- That Assurance Correlates Data to Deliver Network Insights

- Assurance Concepts

  - The Automated Assurance Data Processing Workflow

  - Health Scoring

  - Reviewing Critical Issues

- Skills

- Terms

### Recognizing Assurance Features

- Assurance Features Overview

  - Interface Layout and Features

  - Device and Client 360 Pages

- Assurance Layout and Data Management Tasks

  - Changing Data Time Periods

  - The Geographical Map and Table Network Views

  - Configuring a Custom Dashboard Page

  - Reviewing Detailed Information by Category

  - Reviewing Issues

  - Searching for Devices, Users, or Client Endpoints

### Links

- To Product Information

- To Training

- To Contact Us

# What Should I Know Before I Start?

## That Assurance Correlates Data to Deliver Network Insights

Cisco DNA Center Assurance provides comprehensive functionality that helps you to ensure higher and more consistent service levels to meet growing business demands.

By correlating information from the network, clients, applications, and contextual sources, Cisco DNA Center delivers immediate network monitoring results and proactive insights into:

- Network infrastructure health, including routers, switches, wireless LAN controllers (WLCs), and access points (APs).
- Endpoint client device health, including wired and wireless clients.
- Potential or active infrastructure or client issues or failures that can affect network or business operations.
- The application experience and performance analytics for each client.

Assurance functions include:

- Monitoring and presenting current performance metrics and issues.
- Proactively assessing performance through live traffic analysis and automated sensor-based testing.

You can use Assurance to monitor and evaluate:

- Traditional (non-fabric) WLAN, LAN, and WAN networks.
- In systems with software-defined access (SD-Access), fabric topologies.



**Note:** For more on SD-Access and fabric topologies, [refer to the Software-Defined Access Resources list of links to guides, data sheets, videos, white papers, and other collateral.](#)

- Wired and wireless client services.
- Wireless and wired sensor data.
- Client endpoint analytics, including for some Apple iOS products.
- WAN connectivity and routing protocol failures or errors.
- In systems with router-enabled Application Visibility and Control (AVC), the application experiences that authenticated clients are having.

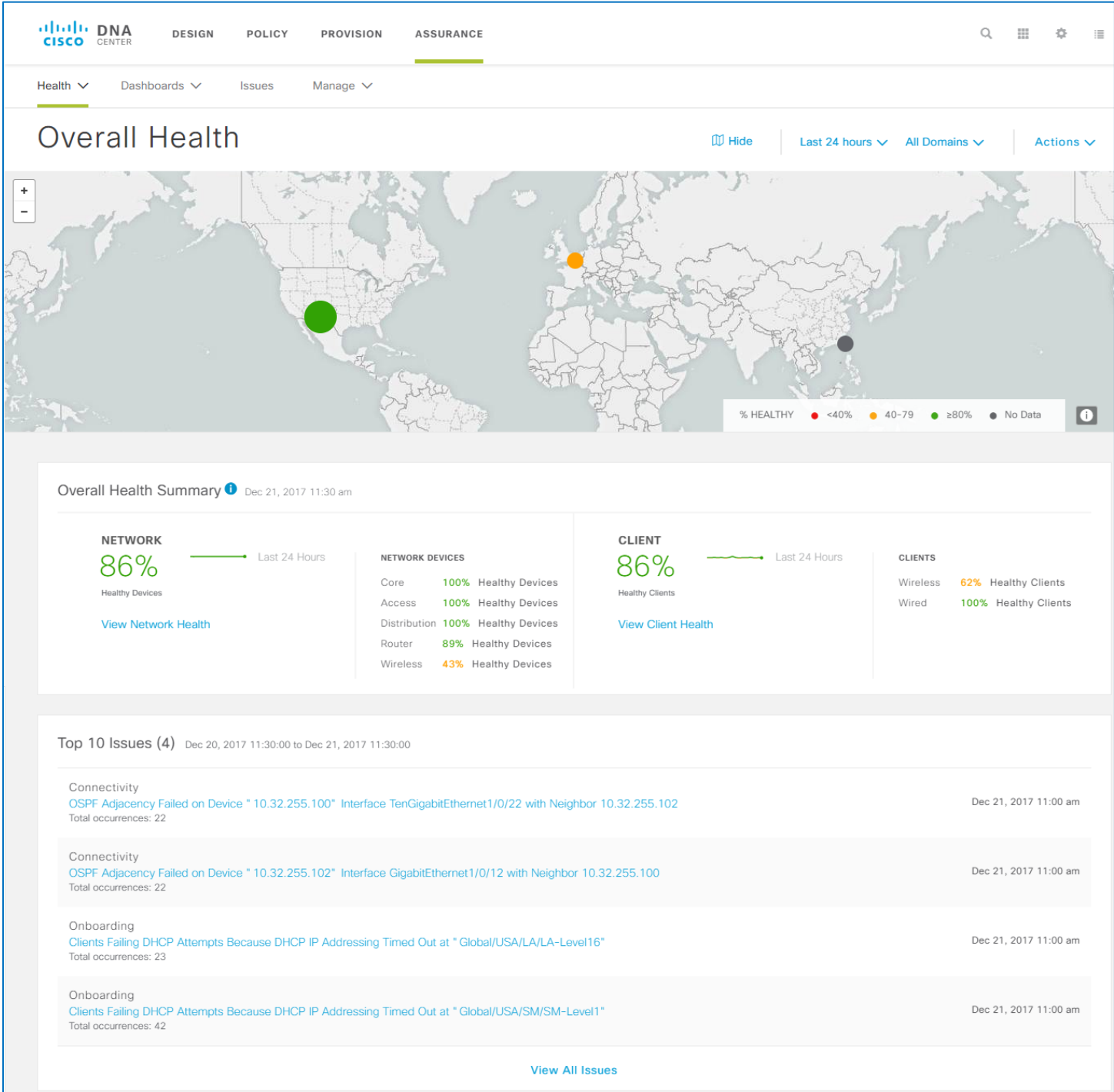


**Note:** For more information on Cisco Application Visibility and Control, [refer to the AVC list of links guides, white papers, case studies, and other collateral.](#)



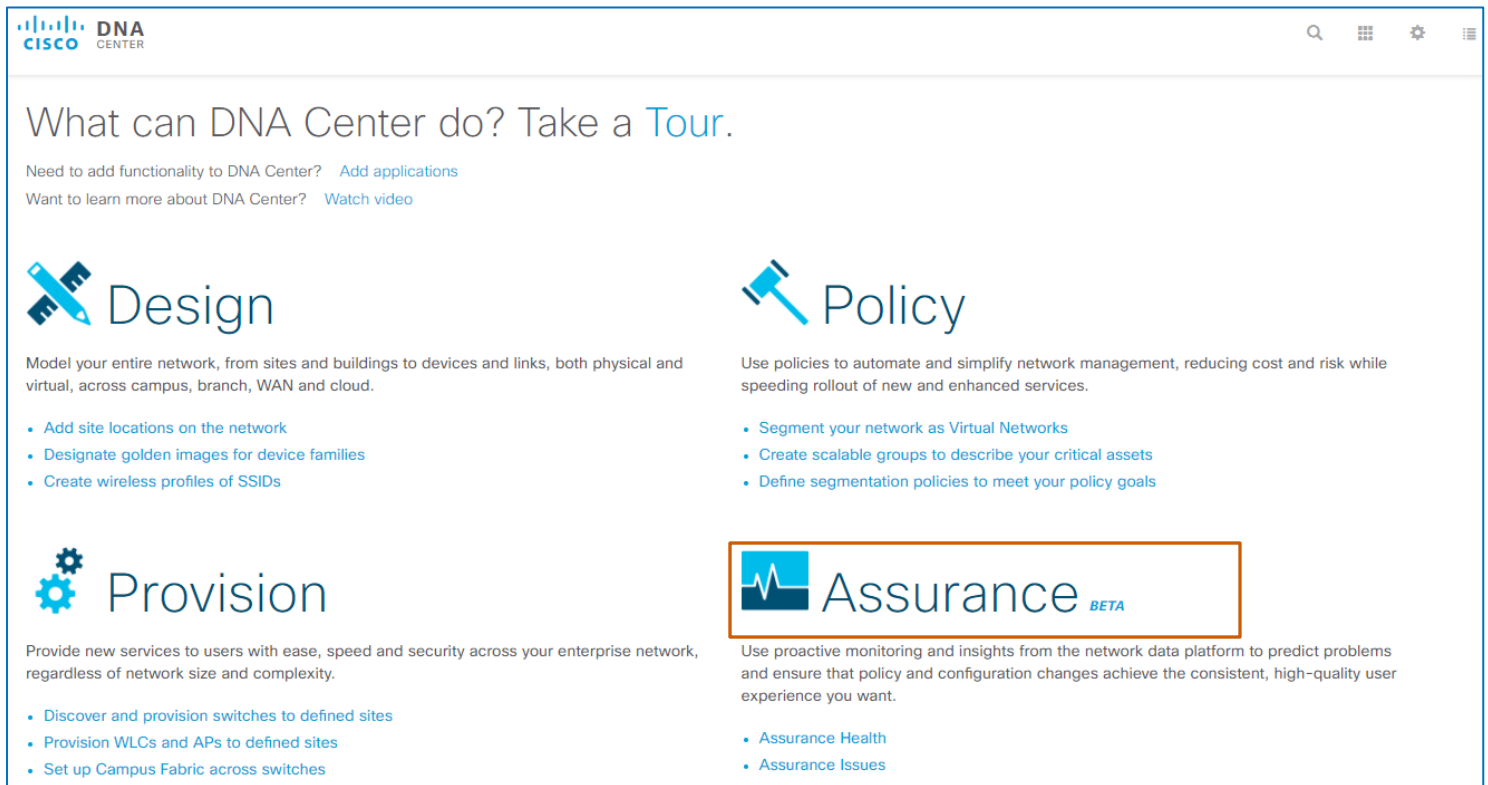
Cisco DNA Center collects data by using traditional SNMP, NetFlow, and SNMP protocols, streaming telemetry, and contextual collectors.

It then correlates and analyzes that data to present robust information, organizing it based on the network's design and topology.



**To open Assurance:**

- On the Cisco DNA Center home page, click **Assurance**.



**Design**

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

**Policy**

Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.

- Segment your network as Virtual Networks
- Create scalable groups to describe your critical assets
- Define segmentation policies to meet your policy goals

**Provision**

Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

- Discover and provision switches to defined sites
- Provision WLCs and APs to defined sites
- Set up Campus Fabric across switches

**Assurance BETA**

Use proactive monitoring and insights from the network data platform to predict problems and ensure that policy and configuration changes achieve the consistent, high-quality user experience you want.

- Assurance Health
- Assurance Issues

This training introduces you to:

- Key Assurance operational concepts.
- The types and levels of information that Assurance provides.
- The organization and layout of Assurance features.
- General navigation and functions that you can use to access the information that you need.



**Note:** While this training does not address Assurance functions for systems with SD-Access specifically, the Assurance information and navigation available to you for monitoring and managing [fabric domains](#) is similar.

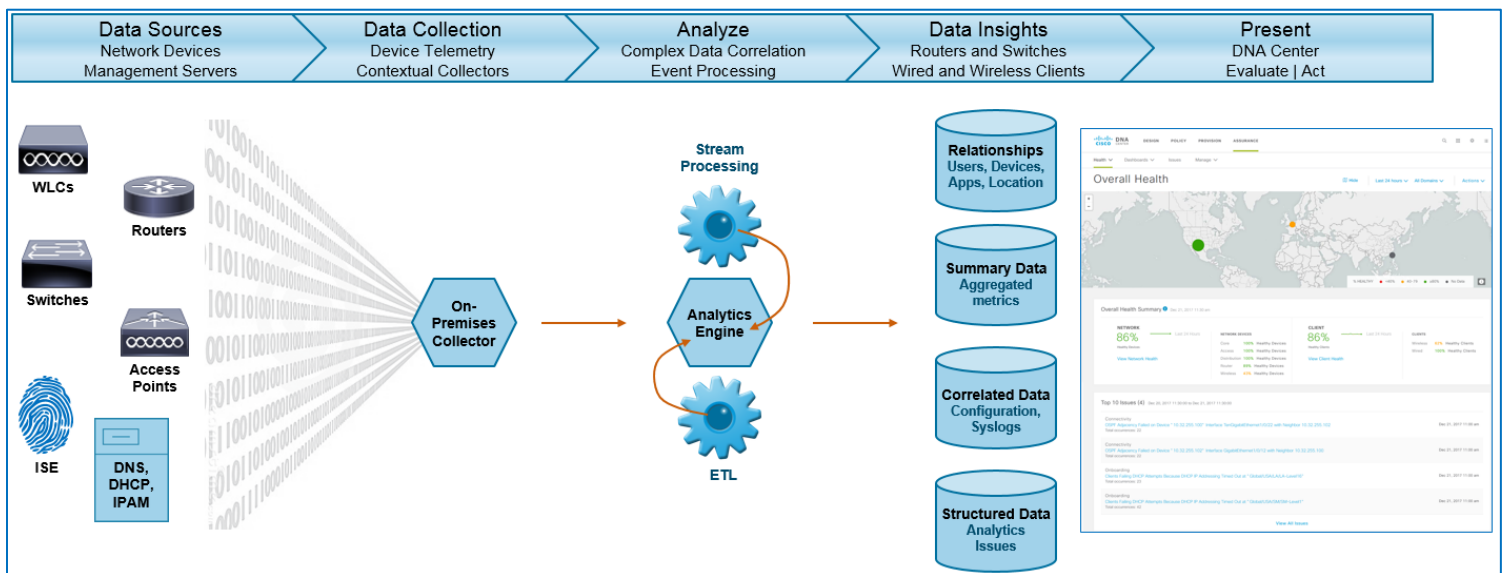
## Assurance Concepts

### The Automated Assurance Data Processing Workflow

Cisco DNA Center performs automated tasks to:

1. Collect raw data from network and contextual sources.
2. Correlate, process, and analyze the raw data.
3. Organize the processed data into meaningful network and client health, performance, and issue metrics and information, referred to as insights.
4. Present insights in the user interface in near real-time.

The following diagram illustrates the flow of data processing and presentation in Cisco DNA Center.



To prepare the system for accurate data collection, system users also:

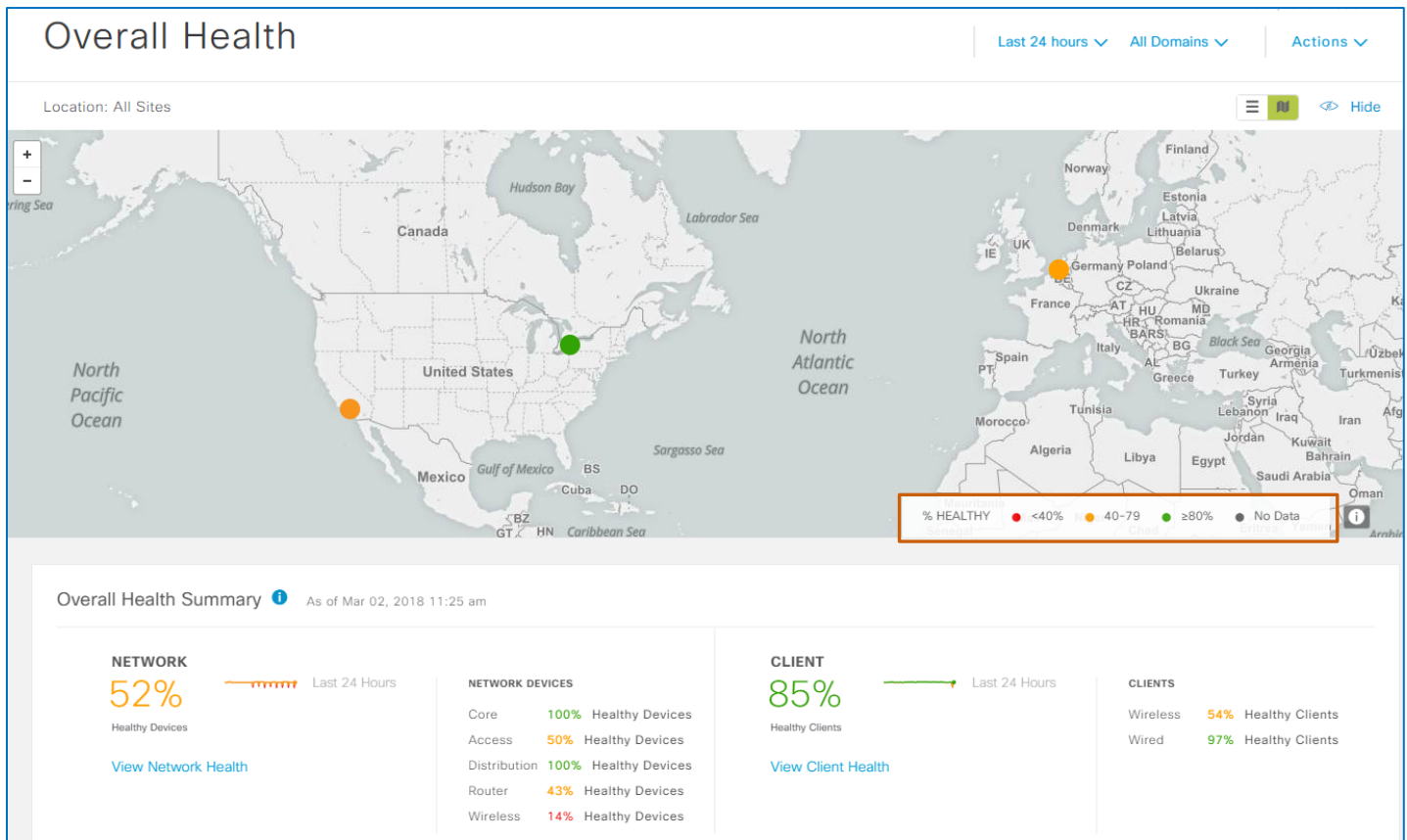
- Initiate device discovery.
- Design network sites and assign devices to them.
- Configure telemetry and external network services.

## Health Scoring

### Scoring Concepts

On the **Overall Health** page, Assurance presents health scores for the entire network, referred to as global health scores.

By providing health score percentages and applying color-coding to them, Assurance emphasizes areas of the network that might require attention or immediate action. Assurance applies the color-coding to location and table view indicators to alert you, also.



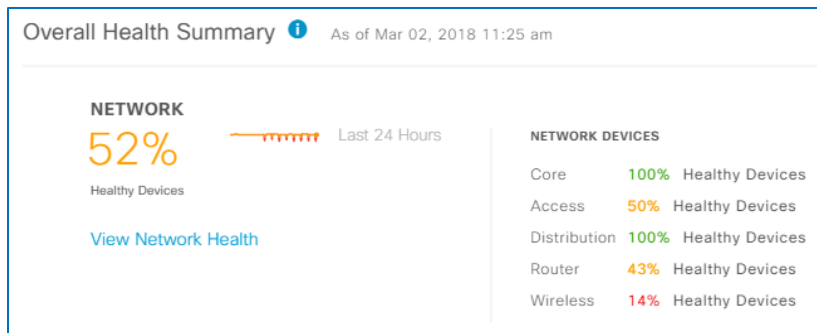
Assurance health scores combine network device performance indicator (KPI) metrics and, for wireless client devices, specific received signal strength indicator (RSSI) measurements, to indicate the number of devices or clients that are experiencing acceptable conditions, which is a healthy state.



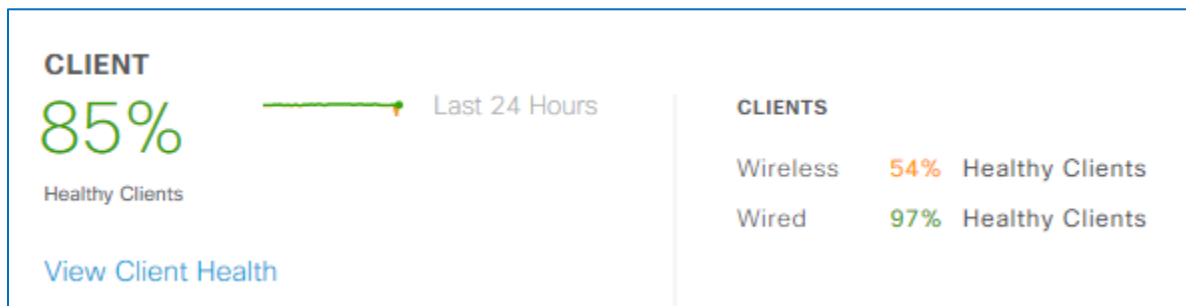
In the example screenshot, under **Network**, 52% of the devices out of the total number of network devices are in a healthy state.

The **Network Devices** section breaks out the percentage of healthy devices based on device roles and types.

All of the core devices, for example, are in a healthy state, while only 14% out of the total number of wireless devices are in a healthy state.



Client health scores are calculated and presented the same way for clients that are attached to and authenticated on the network.



Health scores appear in color-coding, which reinforces the urgency of potential or ongoing issues, as follows:

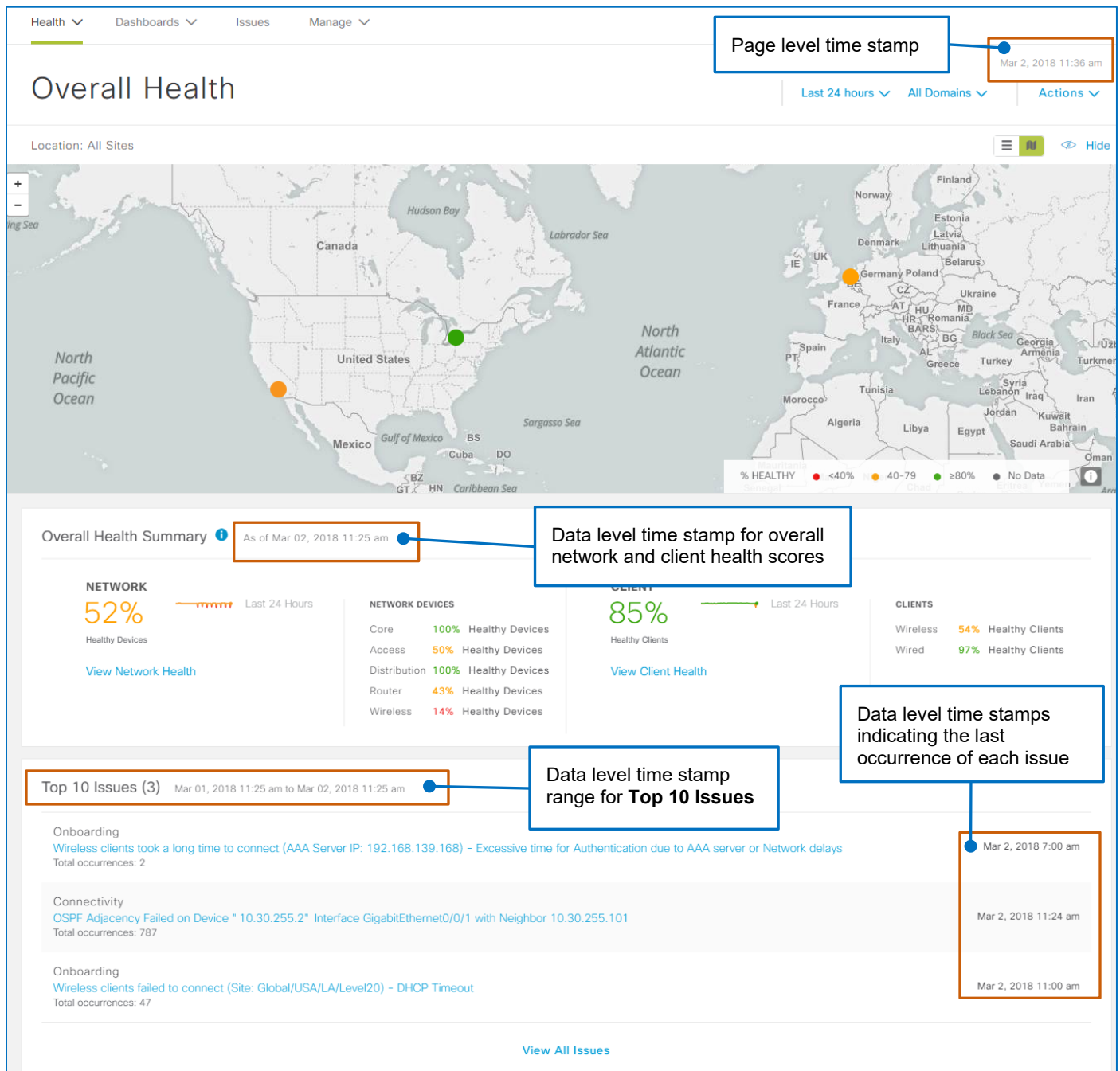
- 80% or more of the total number of network devices are in a healthy state
- Between 40% and 79% of network devices are in a healthy state, indicating that some devices, sites, or areas of the network might require attention
- Less than 40% of the total number of network devices are in a healthy state, indicating that immediate attention to issues is recommended

## Time Stamp and Data Aging Concepts

Assurance provides two types of time stamps:

- The page level time stamp  
Indicates the last time the page was loaded, either by navigating to it or reloading it manually.
- Data level time stamps  
Indicate when the system collected the data that you are seeing.

The time stamps are browser-based, so they indicate the data collection time based on the date and time of your client.



The **Top 10 Issues** time stamp indicates the complete time period for which the system is presenting the issues. Each issue in the **Top 10 Issues** list provides a time stamp that indicates the last occurrence of the issue.



**Note:** The time period also affects health scores and issues that the system is presenting. You can change the default time period of twenty-four hours manually.

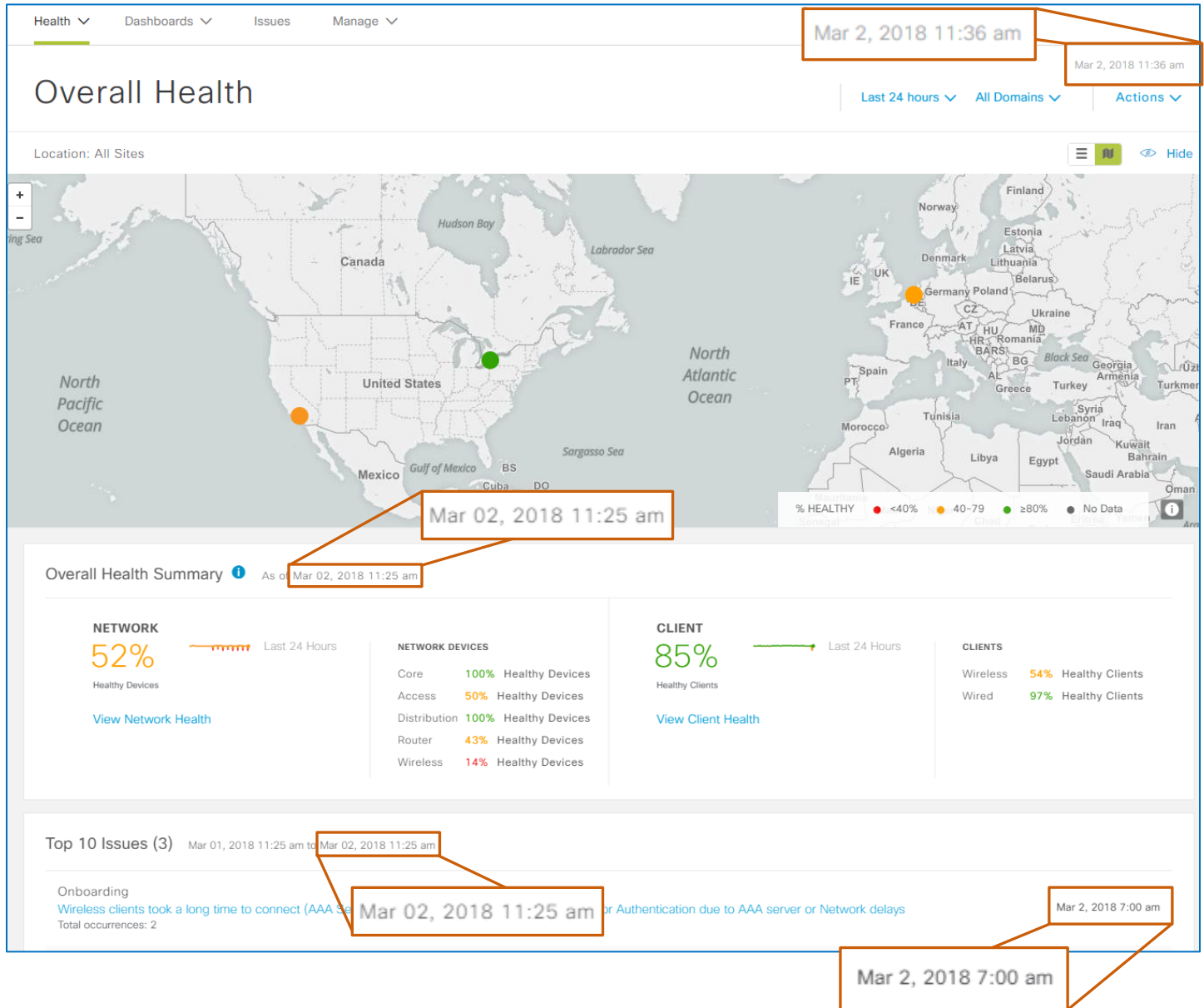
For more information, [refer to the Changing Data Time Periods topic](#).

Cisco DNA Center computes Assurance data at specific time intervals, and those intervals vary slightly based on whether the system is collecting and analyzing network data or client data due to the types of computations that each data type requires.

The slight variation in the collection and analysis intervals means that the time stamp for the **Overall Health Summary** data might vary from the time stamp for the **Top 10 Issues** and the individual issue time stamps.

Because the page level time stamp indicates the last page reload, and the data level time stamps indicate data collection intervals or issue occurrences, these time stamps can vary, also.

In the screenshot below, the page was loaded on March 2, 2018 at 11:36 a.m., the health summary and issue data were collected on the same day at 11:25 a.m., and the **Onboarding** issue was last captured on the same day at 7 a.m.



To ensure that you are seeing current information:

- Reload the page manually by using the browser reload button.



## Reviewing Critical Issues

Cisco DNA Center presents current issues that are occurring on the network, up to 10, on the **Overall Health** page. When issues occur repeatedly, the system provides the number of times the issue has happened for [the time period applied to the page](#).

To identify issues, Cisco DNA Center computes, analyzes, and correlates incoming data and pre-defined key performance indicators (KPIs).

Providing this information with links for immediate access to details helps ensure that potential or ongoing problems receive more immediate attention or action, as needed. The heading indicates the total number of occurring issues.

Total number of active issues for the time period

Click to open details.

**Top 10 Issues (4)** Dec 20, 2017 2:50:00 to Dec 21, 2017 2:50:00

<p>Connectivity</p> <p>OSPF Adjacency Failed on Device " 10.32.255.100" Interface TenGigabitEthernet1/0/22 with Neighbor 10.32.255.102</p> <p>Total occurrences: 22</p>	Dec 21, 2017 2:00 pm
<p>Connectivity</p> <p>OSPF Adjacency Failed on Device " 10.32.255.102" Interface GigabitEthernet1/0/12 with Neighbor 10.32.255.100</p> <p>Total occurrences: 22</p>	Dec 21, 2017 2:00 pm
<p>Onboarding</p> <p>Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at " Global/USA/LA/LA-Level16"</p> <p>Total occurrences: 22</p>	Dec 21, 2017 2:00 pm
<p>Onboarding</p> <p>Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at " Global/USA/SM/SM-Level1"</p> <p>Total occurrences: 42</p>	Dec 21, 2017 2:00 pm

Open the complete issues list.

View All Issues

When more than 10 issues are occurring, you can navigate to the complete list of issues.

### To open a complete list of issues:

- Below the list, click **View All Issues**.

The system navigates to the Issues page and provides lists of open and resolved issues for the time period applied to the page.

DNA CENTER

DESIGN

POLICY

PROVISION

ASSURANCE

Health

Dashboards

Issues

Manage

Issues

Last 24 hours

All Domains

Open

Resolved

View Issue Catalog

Last Occurred Time	Title	Total Occurrences	Category	Device
Mar 9, 2018 6:00 am	Wireless clients took a long time to connect (AAA Server IP: 192.168.139.168) - Excessive time for Authentication due to AAA server or Network delays	1	Onboarding	Client

## Skills

To recognize, evaluate, and manage Assurance information, you need the following experience.

### Basic

- Practical network and LAN or WAN management experience
- Cisco Internetwork Operating System (IOS) concepts

### Proficient

- Cisco DNA Center user interface and navigation
- OSI model
- Network hardware design and concepts
- Networking concepts

## Terms

### Domain

In deployments that include Software-Defined Access (SD-Access), system users can configure fabric domains. A domain is a logical, virtualized network topology that abstracts networking functions from the underlying hardware. The virtualized topology performs routing, switching, and communication functions.



**Note:** For information on seeing Assurance data for a fabric domain, [refer to the Assurance Layout and Data Management Tasks topic](#).

### Sensor-Driven Tests

These tests assess connectivity or application issues by analyzing data from access point (AP) radios, and WLAN configurations for wired and wireless network services.

### Site

An enterprise location, often organized based on the network design or geographical location

# Recognizing Assurance Features

## Assurance Features Overview

### Interface Layout and Features

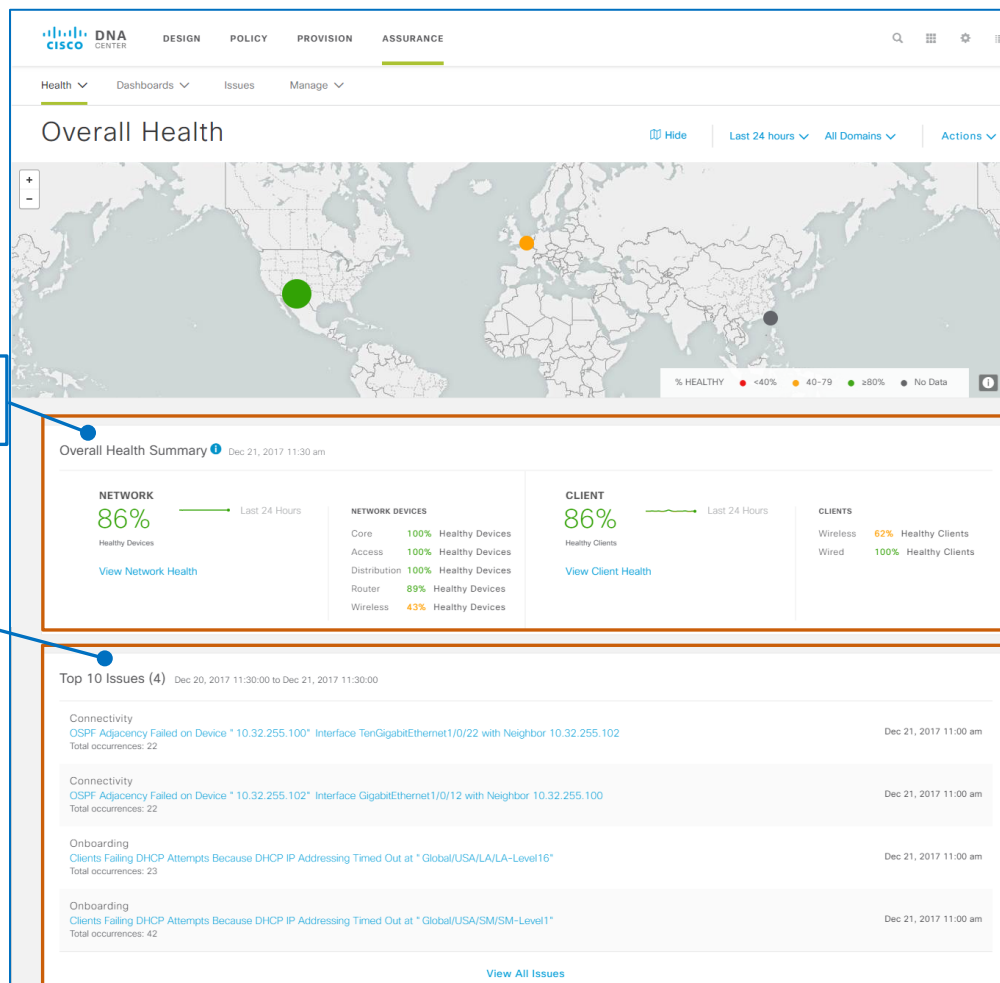
#### The Overall Health Page

When you open Assurance, the system illustrates aggregated network infrastructure and client health metrics, organizes health metrics by category, and escalates the most critical issues on the **Overall Health** page.

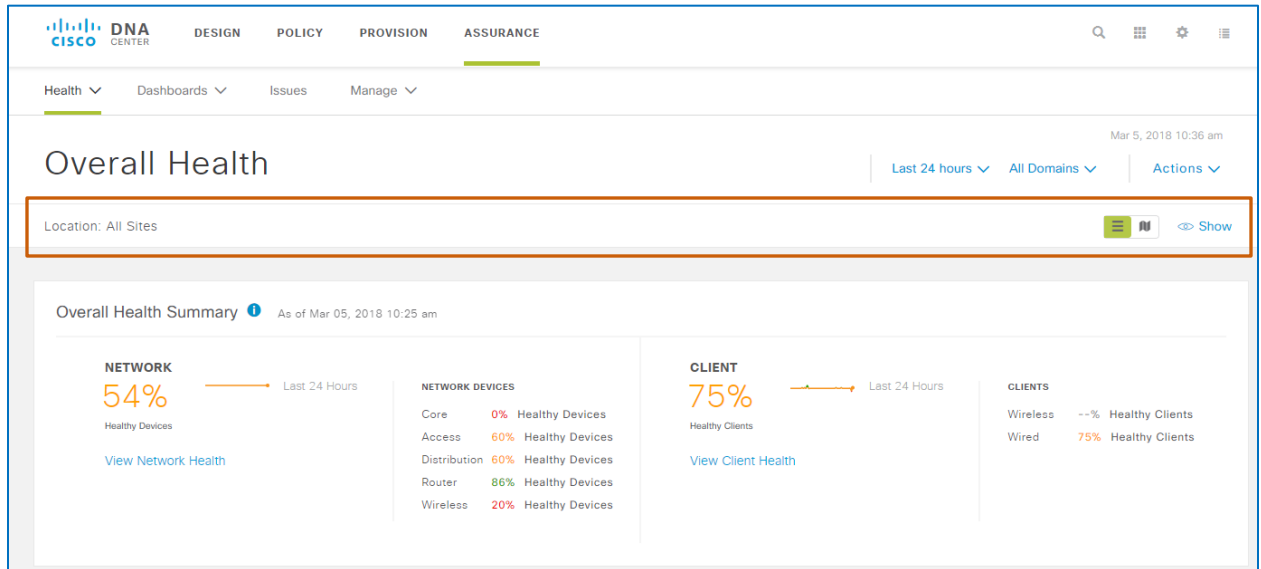
The page comprises dashlets, which are separate data elements that organize or categorize information, such as health performance metrics and critical issues, and present the information in charts, tables, or other graphical representations.

**Overall Health Summary dashlet**

**Top 10 Issues dashlet**



When you open the **Overall Health** page, the top dashlet is collapsed by default.

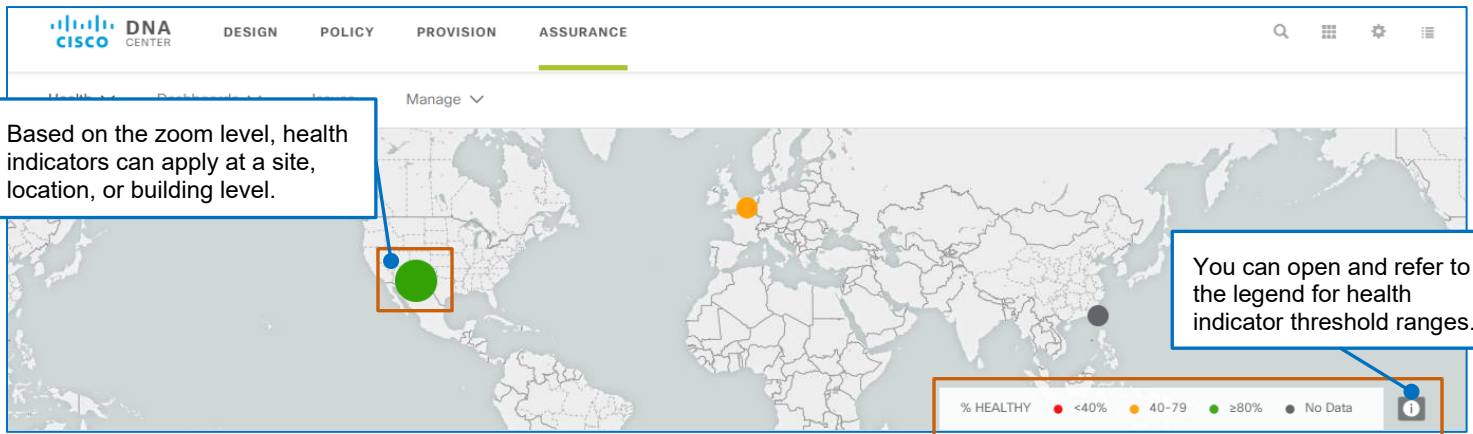


You can expand the dashlet to see a geographical map view or table view of the network and associated health metrics.

The geographical map of the network topology displays network and client health indicators with [health score color-coding](#) based on devices' site assignments and the map zoom level.



**Note:** The system presents the geographical map by using MapBox.  
To see the map, the system requires Internet connectivity.





The table view lists network locations based on the network design hierarchy.

Location: All Sites

Filter Hierarchical Site View As of Mar 5, 2018 10:25 am Export EQ Find

Site/Building/Floor	Client Health (% Healthy Clients)				Network Health (% Healthy Devices)							Client Count	Network Device Count	
	All				All	A	C	D						
> Mexico	50%	--			100%		--					2	8	
All Sites	75%	--			54%		--					4	24	
> Egypt	--	--			--	--	--	--	--	--		0	0	
> New York	--	--			75%	--	--					0	4	
> North Carolina	--	--			50%	--	--					0	2	

The **Overall Health Summary** dashlet displays the [health scores](#) for network infrastructure and endpoint client device health separately and the percentages are color-coded to emphasize any health issues.

Each category also breaks out the health metrics by device type.

Overall Health Summary Dec 21, 2017 2:50 pm

**NETWORK**  
86%  
Healthy Devices  
[View Network Health](#)

**NETWORK DEVICES**

Core	100%	Healthy Devices
Access	100%	Healthy Devices
Distribution	100%	Healthy Devices
Router	89%	Healthy Devices
Wireless	43%	Healthy Devices

**CLIENT**  
79%  
Healthy Clients  
[View Client Health](#)

**CLIENTS**

Wireless	53%	Healthy Clients
Wired	96%	Healthy Clients

Navigate to network infrastructure-specific summary and detailed information.

Navigate to endpoint device-specific summary and detailed information.

The **Top 10 Issues** dashlet lists those issues that can affect the network most significantly to help ensure that they receive more immediate attention.

Top 10 Issues (4) Dec 20, 2017 2:50:00 to Dec 21, 2017 2:50:00

<p>Connectivity</p> <p>OSPF Adjacency Failed on Device " 10.32.255.100" Interface TenGigabitEthernet1/0/22 with Neighbor 10.32.255.102</p> <p>Total occurrences: 22</p>	Dec 21, 2017 2:00 pm
<p>Connectivity</p> <p>OSPF Adjacency Failed on Device " 10.32.255.102" Interface GigabitEthernet1/0/22 with Neighbor 10.32.255.102</p> <p>Total occurrences: 22</p>	Dec 21, 2017 2:00 pm
<p>Onboarding</p> <p>Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at " Global/USA/LA/LA-Level16"</p> <p>Total occurrences: 22</p>	Dec 21, 2017 2:00 pm
<p>Onboarding</p> <p>Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at " Global/USA/SM/SM-Level1"</p> <p>Total occurrences: 42</p>	Dec 21, 2017 2:00 pm

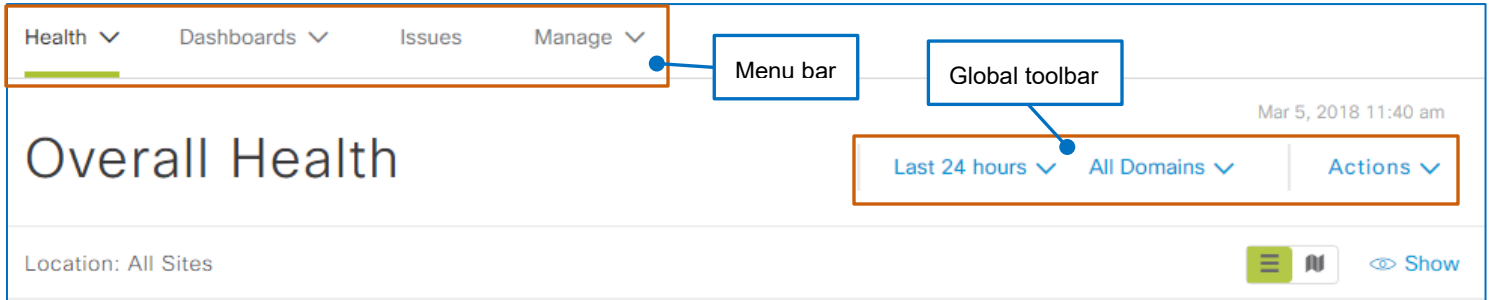
The link opens a panel with issue details and suggestions to correct it.

Navigate to a complete list of all network and client open and resolved issues.

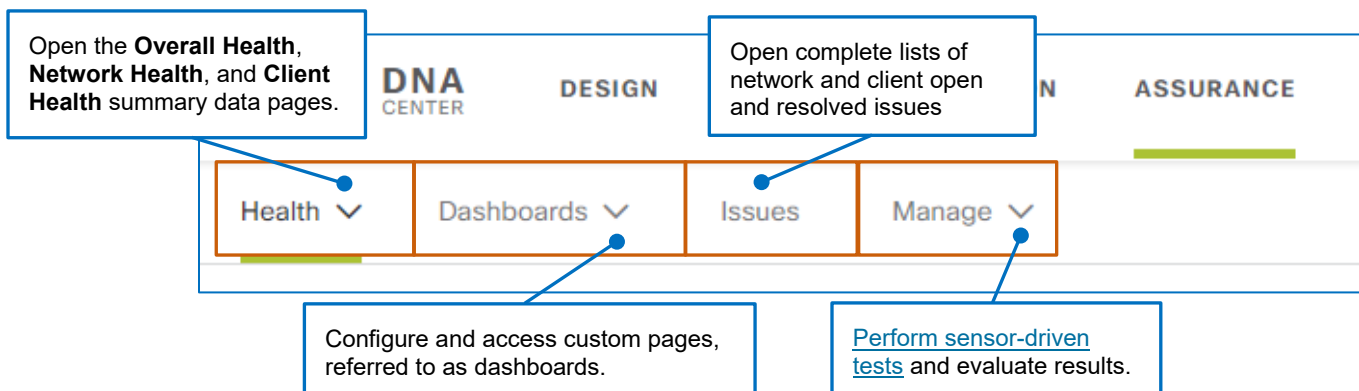
[View All Issues](#)

## The Menu Bar and the Global Toolbar

The menu bar and global toolbar are available on the **Overall Health**, **Network Health**, and **Client Health** pages.



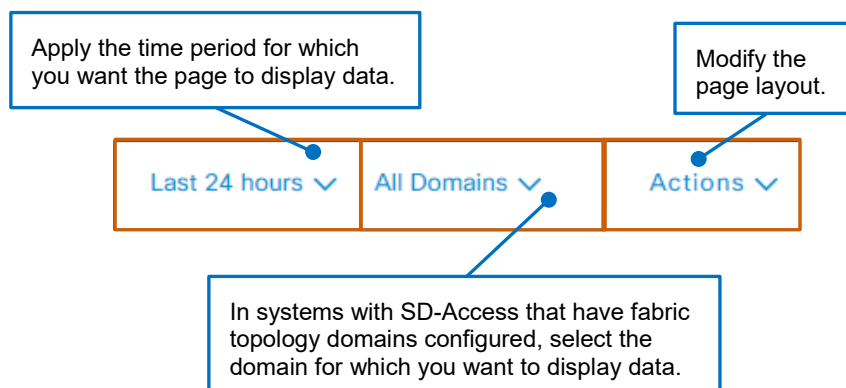
The menu bar provides navigation to detailed assurance information or tasks that you can perform.



You use the global toolbar to manage the display of information and page layout.



**Note:** You also can filter the data [at a site level](#) on the **Network Infrastructure** and **Client Health** pages.

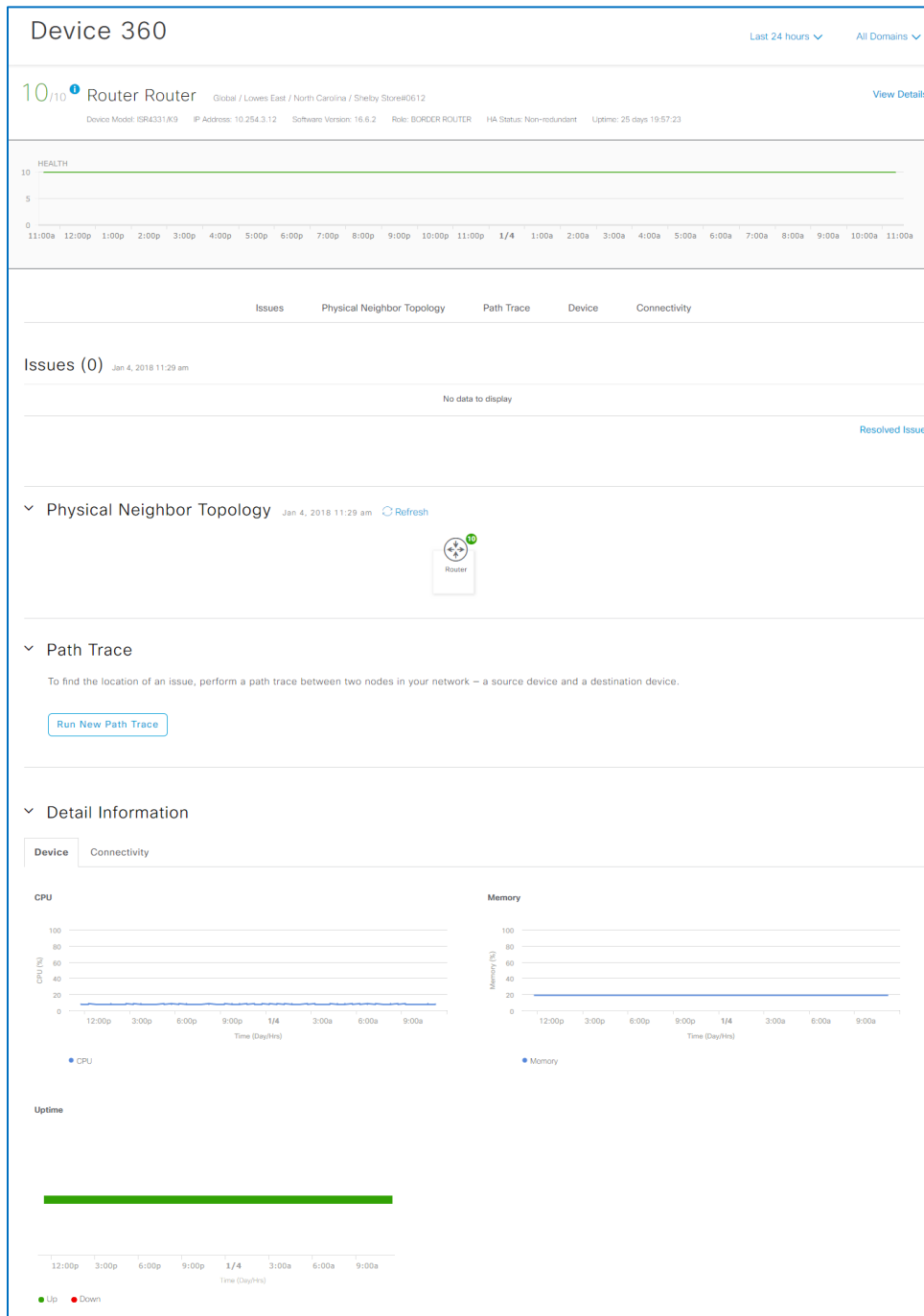


## Device and Client 360 Pages

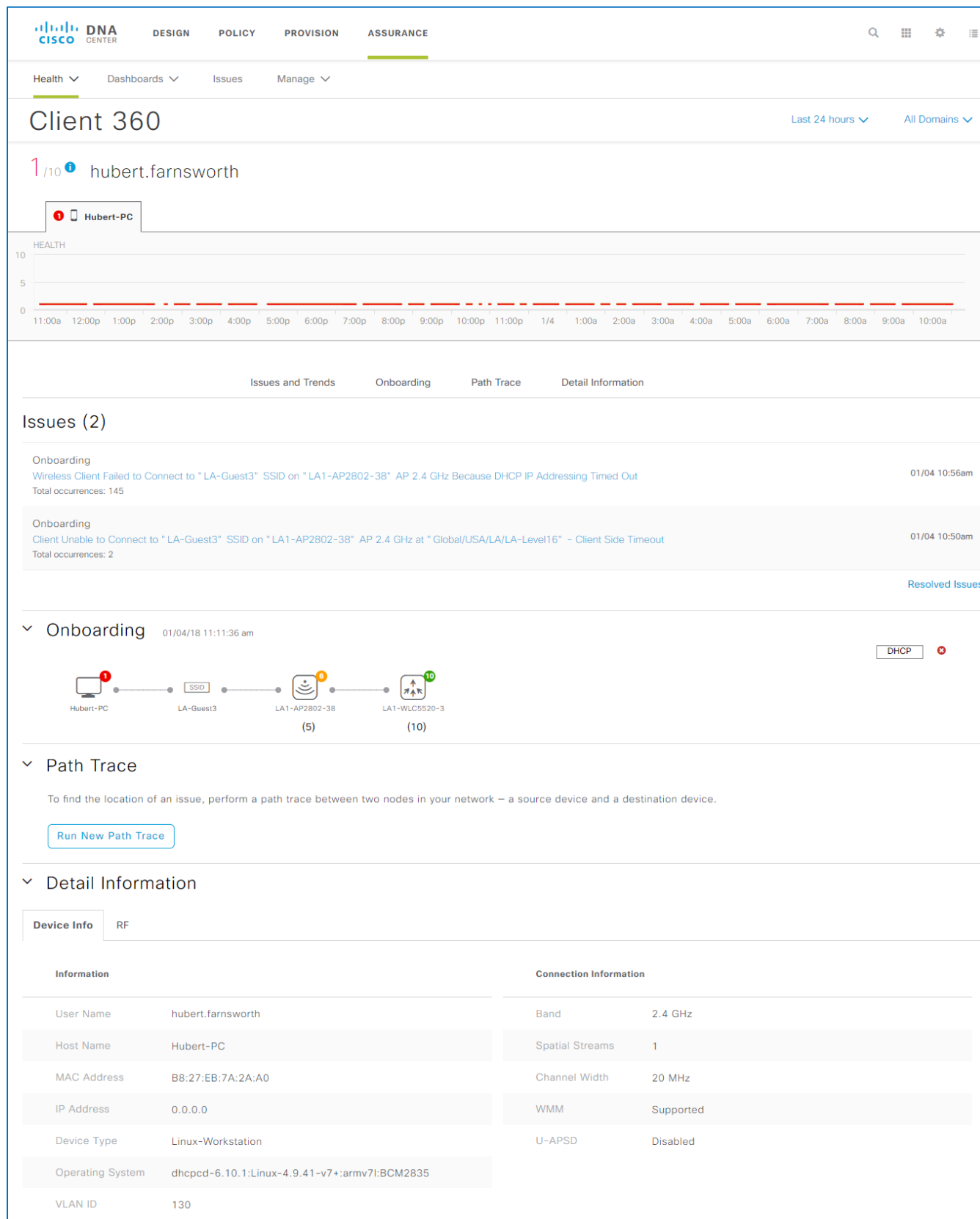
### Holistic Views of Device and Client Health and Performance

To support evaluating metrics or resolving issues occurring on a specific device or for a specific client endpoint, Assurance includes the **Device 360** and the **Client 360** pages, which provide item details, health metrics, associated issues, testing functions, and links to other information.

The following screenshot illustrates information and navigation available on a **Device 360** page.



The following screenshot illustrates information and navigation available on a **Client 360** page.



The screenshot displays the Cisco DNA Center interface for the **Client 360** page. The top navigation bar includes tabs for DESIGN, POLICY, PROVISION, and ASSURANCE. The ASSURANCE tab is active, showing a sub-navigation bar with Health, Dashboards, Issues, and Manage. The main content area is titled **Client 360** and shows the client name **hubert.farnsworth** with a status of **1/10**. Below this, a **Hubert-PC** device is highlighted. A **HEALTH** graph shows a red line at the bottom of the scale (0 to 10) across a 24-hour period. The **Issues and Trends** section shows two onboarding issues: "Wireless Client Failed to Connect to 'LA-Guest3' SSID on 'LA1-AP2802-38' AP 2.4 GHz Because DHCP IP Addressing Timed Out" (Total occurrences: 145) and "Client Unable to Connect to 'LA-Guest3' SSID on 'LA1-AP2802-38' AP 2.4 GHz at 'Global/USA/LA/LA-Level16' - Client Side Timeout" (Total occurrences: 2). The **Onboarding** section shows a timeline of the client's connection process, including a **Path Trace** diagram showing the client's path from Hubert-PC to LA-Guest3, then to LA1-AP2802-38, and finally to LA1-WLC5520-3. The **Detail Information** section provides a table of device and connection information.

Device Info		RF	
<b>Information</b>			
User Name	hubert.farnsworth		
Host Name	Hubert-PC		
MAC Address	B8:27:EB:7A:2A:A0		
IP Address	0.0.0.0		
Device Type	Linux-Workstation		
Operating System	dhcpcd-6.10.1:Linux-4.9.41-v7+:armv7l:BCM2835		
VLAN ID	130		
<b>Connection Information</b>			
Band	2.4 GHz		
Spatial Streams	1		
Channel Width	20 MHz		
WMM	Supported		
U-APSD	Disabled		

To open a **Device 360** or **Client 360** page:

- Follow the steps to search for a device, user, or client endpoint, and then, in the search dialog box, click the associated 360 link.

- On the **Network Health** page, in the **Network Devices** list, click the **Device** name link.

Device	Device Type	IP Address	OS Version	Overall Health Score	System Health	Data Plane Connectivity	Issue Count	Location
Router	ISR4331/K9	10.254.3.12	16.6.2	10	●	●	0	Lowes East/North Carolina/Shelby Store#0612
TEST-SW3650	WS-C3650-24PD-E	10.8.19.1	03.06.05E	10	●	●	0	San Francisco/SF-BLDG-1

- On the **Client Health** page, in the **Client Devices** list, click the **MAC Address** link for the user or endpoint of interest.

UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Onboarding Health	Connected Health	Connected To	Location	VLAN ID	SSID
hubert...	Hubert-PC	B8:27:EB:0C:44:40	0.0.0.0	--	Linux-Wor...	1	●	●	LA2-AP380...	SM/SM-Lev...	130	LA-Guest2
amy.wong	Amy-PC	B8:27:EB:0C:53:E0	0.0.0.0	--	Linux-Wor...	1	●	●	LA2-AP380...	SM/SM-Lev...	130	LA-Guest2

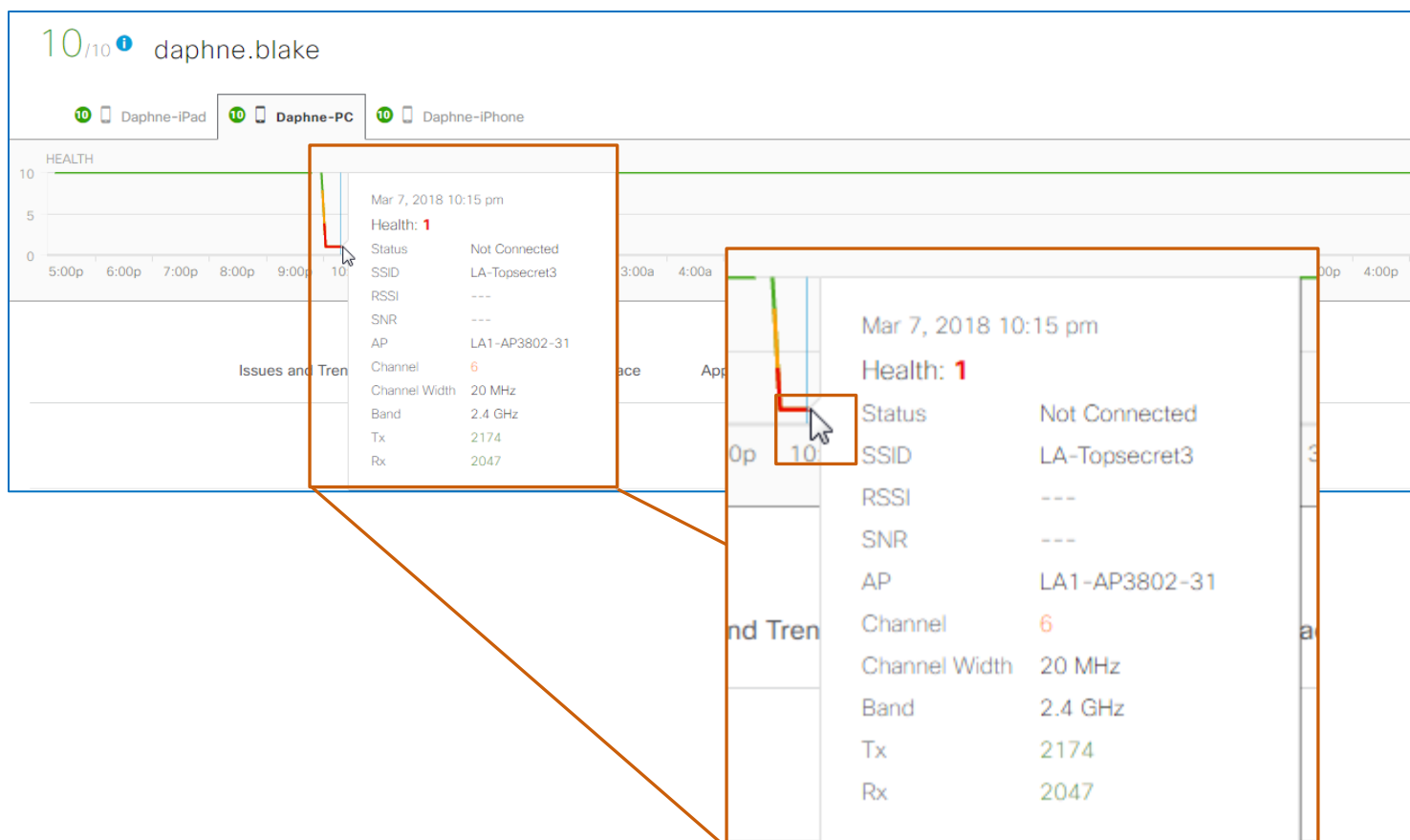
## Obtaining Historical Health and Performance Details

A key feature available on the **Device 360** and **Client 360** pages is your ability to see historical information by using the timeline. Historical data provides context for issue troubleshooting, which supports resolving problem areas, and network planning, which supports proactive responses to changing conditions and helps avoid future problems.

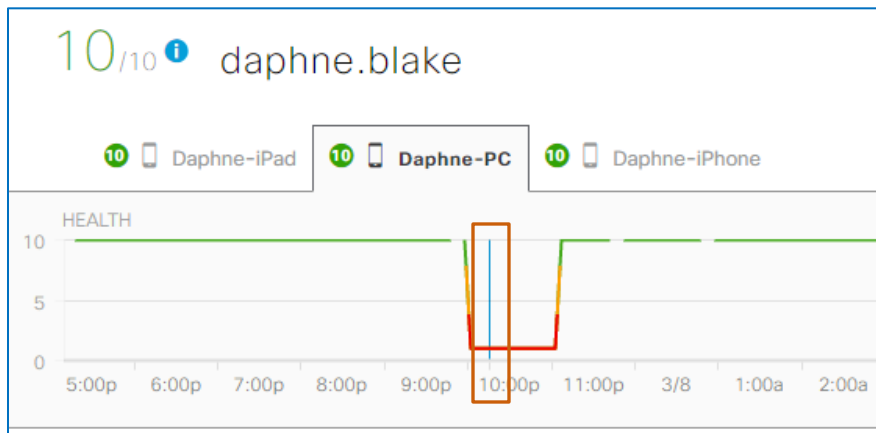
This example uses a **Client 360** page illustrates the feature. The timeline appears below the page heading.



When you point to a time on the timeline, you can see key information about the state of the client, or device in the **Device 360** view, at the indicated time.



When you click a point on the timeline, an indicator emphasizes the time for which the page is displaying information...

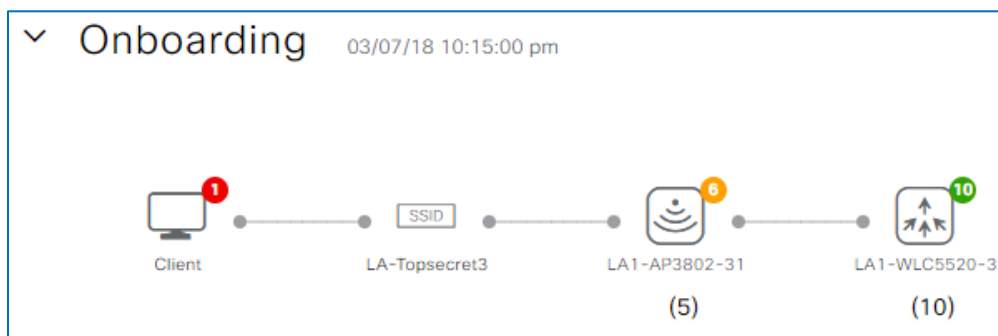


...and the page refreshes to display the details about the client (or device) experience at that time, including:

- Issues

Issues (7)		
Onboarding	Wireless client failed to connect (SSID: LA-Topsecret3, AP: LA1-AP3802-31, Band: 2.4 GHz, Site: Global/USA/LA/Level16) - Failed to authenticate due to Client Timeout	03/07 10:08pm
	Total occurrences: 3	
Onboarding	Wireless client took a long time to connect (SSID: LA-Corporate3, AP: LA1-AP3802-31, Band: 2.4 GHz, Site: Global/USA/LA/Level16) - Excessive time due to RF issues	03/07 9:57pm
	Total occurrences: 4	
Application	Network Latency for Application 'netflix' is Above the Threshold Value of 387ms.	03/07 9:55pm
	Total occurrences: 11	
Application	Network Latency for Application 'cifs' is Above the Threshold Value of 412ms.	03/07 9:55pm
	Total occurrences: 11	
Application	Network Latency for Application 'ssh' is Above the Threshold Value of 362ms.	03/07 9:55pm
	Total occurrences: 6	
Application	Network Latency for Application 'espn-browsing' is Above the Threshold Value of 262ms.	03/07 9:55pm

- The path the client used to onboard onto the network



- The applications the client was using and their behaviors

Application Experience BETA Mar 7, 2018 10:15 pm [Refresh](#)

Business Relevant Business Irrelevant Default

Application (2) [Export](#)

[Filter](#) EQ Find

Name	Domain Name	Health		Destination	Average Throughput (Mbps)	Average Bandwidth Utilization (%)	Traffic Class	Packet Loss (%)		Latency (ms)		Application Delay (ms)	
		Most Recent	Last 24 Hours					Max	Average	Max	Average	Max	Average
All Applications				Multiple	0	0							
<input checked="" type="radio"/> ntp	--	--		unknown	0	0	ops-admin-mgmt	0	0	0	0	0	0
<input type="radio"/> dns	--	--		unknown	0	0	ops-admin-mgmt	0	0	0	0	0	0

- Device or radio frequency (RF) details

Detail Information

**Device Info** RF

Information		Connection Information	
User Name	Unknown --- User	Band	2.4 GHz
Host Name	---	Spatial Streams	0
MAC Address	B8:27:EB:D8:BB:5E	Channel Width	20 MHz
IP Address	---	WMM	Supported
Device Type	---	U-APSD	Disabled
Operating System	---		
VLAN ID	---		

Note that you also can run a trace to determine the complete path through the network from a source (the IP address to which the device or client is connected) to its destination (a host, such as a printer, or a network device interface).

This information can be helpful when you are working to resolve issues or evaluate previous ones.

Path Trace

To find the location of an issue, perform a path trace between two nodes in your network – a source device and a destination device.

[Run New Path Trace](#)



## Assurance Layout and Data Management Tasks

Assurance provides features that you can use to help ensure that the information that you need is immediately visible and to navigate to detailed health or issue information efficiently.

This topic addresses the tasks that you can perform to manage Assurance data, organize page layouts, and find the information that you need.

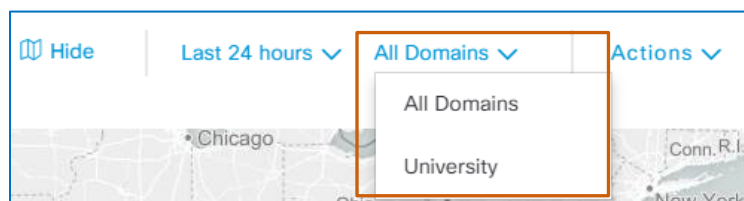


**Note:** In systems with SD-Access and with fabric topologies configured, you can filter the **Overall Health** page and its features to display health metrics and issues for a [specific fabric domain](#).

The features and navigation that you have access to are the same.

### To see overall metrics for a specific fabric topology domain:

- On the global toolbar, in the **All Domains** drop-down list, select the domain of interest.



When you make changes to items such as default time periods, or showing or hiding the map, for example, the page does not retain these changes when you navigate away from it.

## Changing Data Time Periods

When you open Assurance, by default, the system applies the 24-hour time period to all of the page dashlets, including the geographical map, the health summaries, and the top 10 issues list.

You can change the time period so that the page includes data for 3 hours, 24 hours, or 7 days. When you change the time period, the system applies it to all of the dashlets.

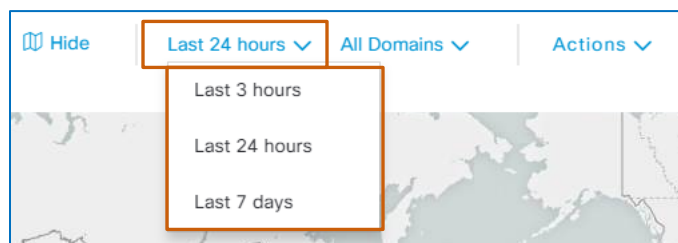


**Important Note:** When you change the default time period, the page does not retain the changes when you navigate away from it.

When you return to the page, it applies the 24-hour default time period.

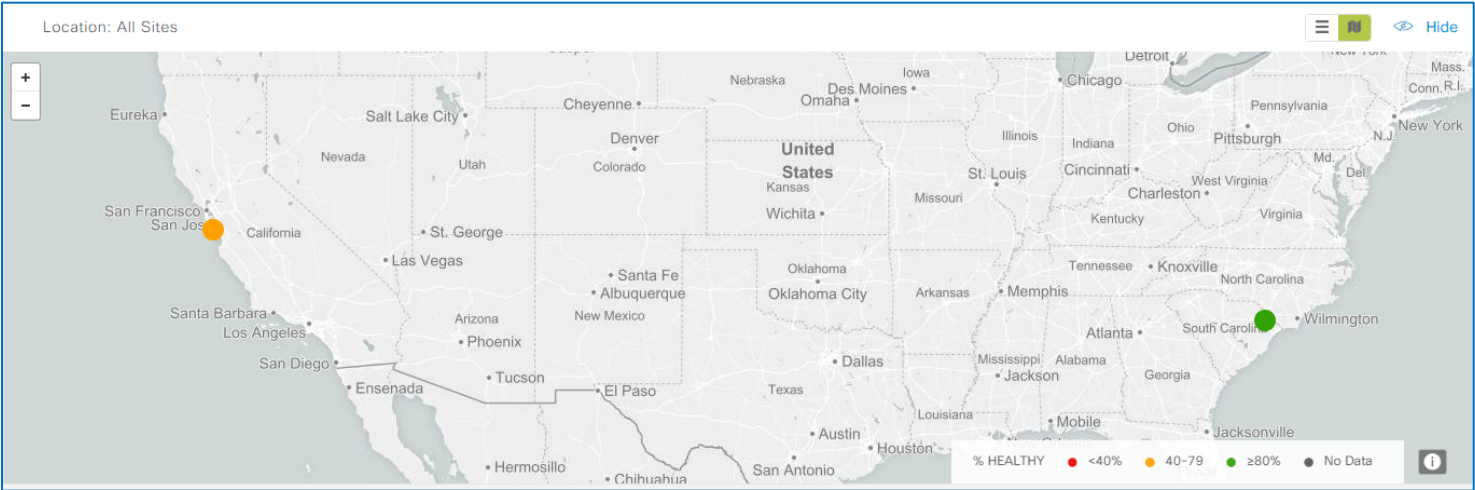
### To change the data time period:

- On the global toolbar, in the time interval drop-down list, select the time period that you want to apply.



## The Geographical Map and Table Network Views

Assurance provides a dashlet that toggles between a geographical map view...



....and a table view of the network.

Location: All Sites														
Filter Hierarchical Site View As of Mar 6, 2018 2:45 pm														
Site/Building/Floor	Client Health (% Healthy Clients)				Network Health (% Healthy Devices)								Client Count	Network Device Count
	All				All	A	C	D						
> USA	84%				85%								43	26
All Sites	86%				84%								49	31
> Australia	100%	--			100%		--	--		--	--		4	2
> Netherlands	100%				67%		--	--					2	3

For the time period that is applied to the page, each view displays color-coded indicators that reflect the health score of devices based on location.

When you navigate to Assurance, the dashlet closes by default.



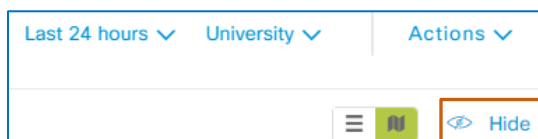
To open the view that you want, below the global toolbar:

- To open the geographical map view, click the map button.
- To open the location list view, click the list button.



To collapse the dashlet, below the global toolbar:

- Click **Hide**.

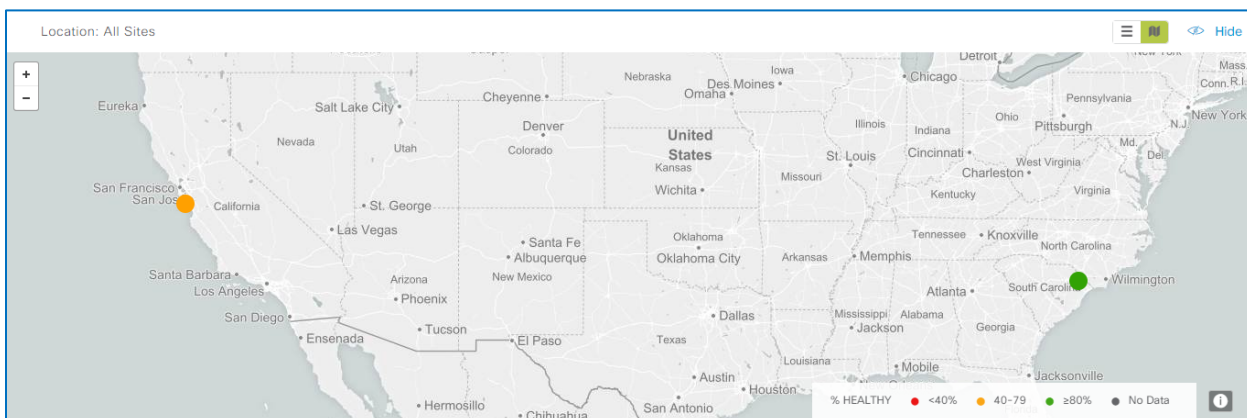


The system removes the dashlet from view, and the **Hide** button toggles to **Show**.



## Navigating the Geographical Map View

Assurance provides a geographical map, which provides a visual view of the enterprise network and current health metrics.



The map opens at a zoom level to include all of the geographical locations that have been identified during network design. The legend below the map defines the health range percentages associated with the color-coding.

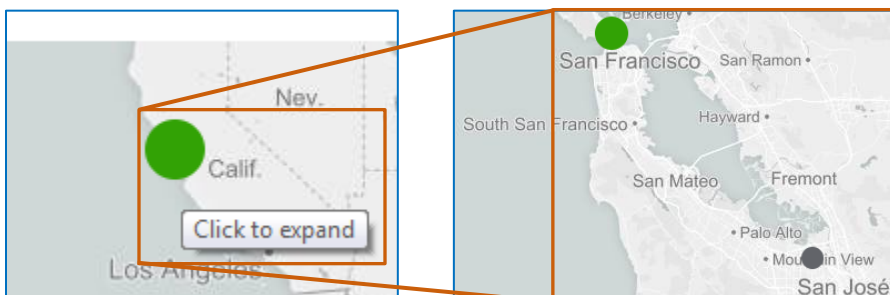


**Important Note:** The system displays locations based on the map coordinates that a system user added during network design.

If you do not see a location that you expect, a system user might need to add the location's coordinates in the network hierarchy.

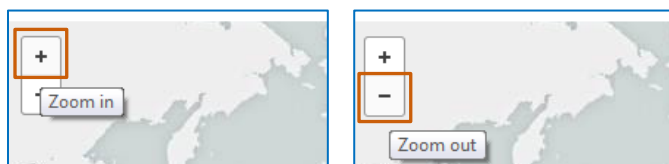
Map zoom levels affect how the map represents locations. When locations are in close proximity and the map is a minimum zoom level, the system collapses location indicators so that they represent multiple locations with a single, larger indicator.

You can adjust map zoom levels to see the information that you need.



### To adjust the map zoom level using the zoom tool:

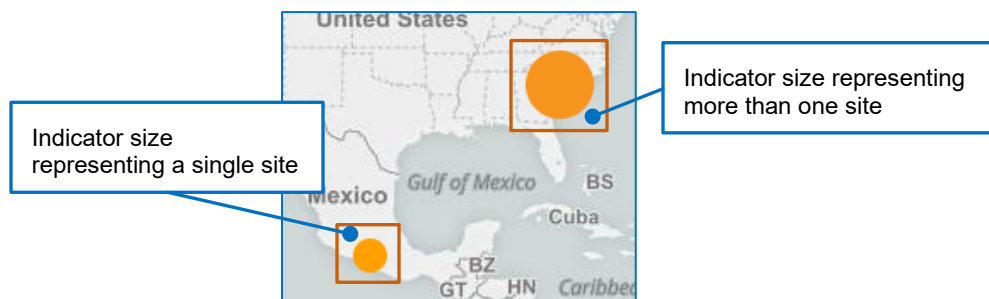
- On the right of the map, click **Zoom in** or **Zoom out**.



### To see whether an indicator represents multiple sites:

- Refer to the size of the indicator.

Larger circle indicators represent more than one site.

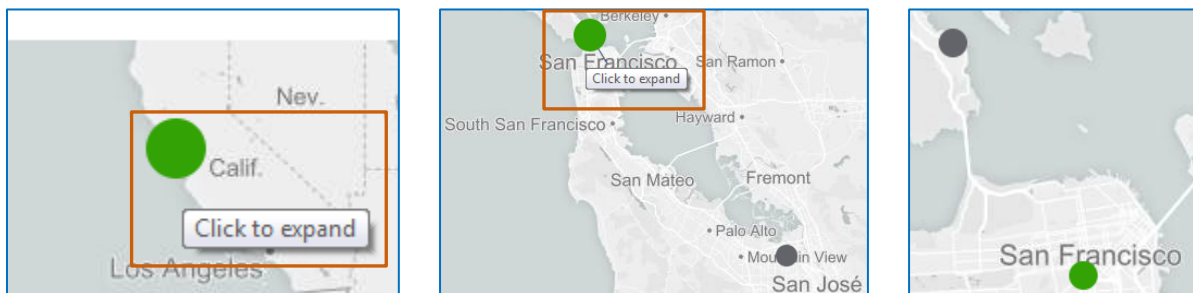


**Important Note:** When an indicator includes multiple sites, the health score color-coding represents the lowest health score at a device level for a single location or building.

### To expand a location group indicator:

- On the map, click the multiple site indicator.

The map zoom level decreases to show the indicators for the locations that the group indicator represented. These locations can include additional locations based on the geographical proximity and network design.



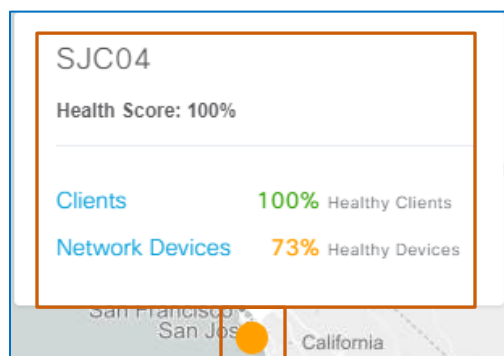
On the map, you can open location level summary health metrics. The summary also provides immediate navigation to detailed health metrics and related information.

This feature is helpful when you see a location indicating health issues. By providing overview metrics and efficient navigation, you can address potential issues or take actions, as needed.

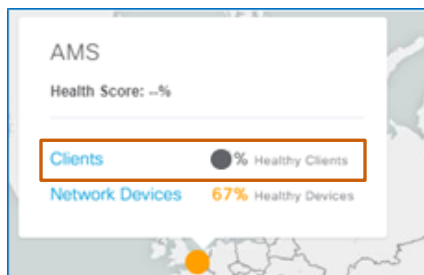
### To see a location's health score:

- At a single location level, click the indicator.

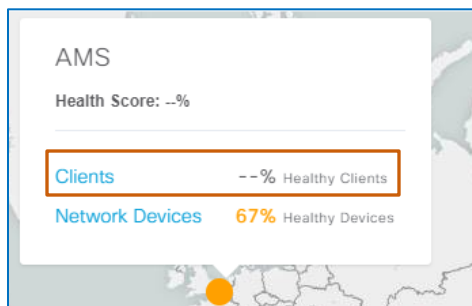
A pop-window opens and displays the percentages of healthy clients and network devices at the location. It also provides links so that you can navigate to pages that provide detailed information on the clients or network devices for that location.



When no data is available for an item, the system displays a gray circle rather than a percentage.



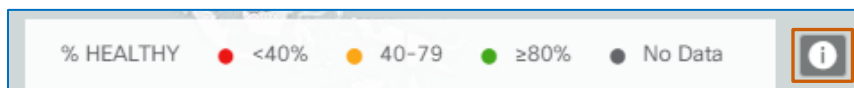
In the case of client data, when the system is collecting data but there are no clients connected, the pop-up window displays a gray dashed line beside the percentage.



For better map visibility, you can collapse the map legend.

**To collapse the legend:**

- To the right of the legend, click the information icon.



The information icon remains available so that you can open the legend, as needed.

## Navigating the Table View

The list view uses a table layout categorized by parent location. It also organizes the health score indicators by client type or device type, so that you can see potential problem areas for clients or network devices more easily.

When you open the table view, the page applies the **Hierarchical Site View** layout by default. The layout lists the location hierarchy that is organized in the network design.

Filter

Hierarchical Site View

As of Mar 6, 2018 2:45 pm

Export

Find

Site/Building/Floor	Client Health (% Healthy Clients)				Network Health (% Healthy Devices)								Client Count	Network Device Count
	All				All	A	C	D						
> USA	84%				85%						--		43	26
All Sites	86%				84%						--		49	31
> Australia	100%	--			100%		--	--		--	--		4	2
> Netherlands	100%				67%		--	--			--		2	3

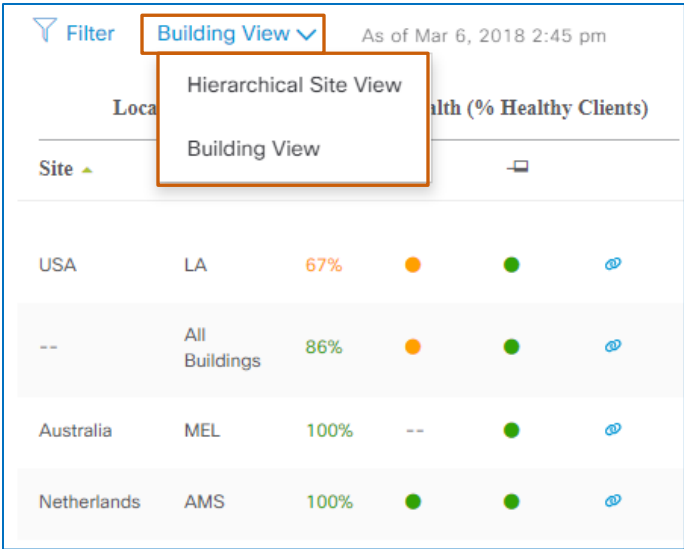
When a location has dependent, or child sites, the parent location displays an arrow to the left of the location name.

### To see the health scores and indicators for child sites:

- Beside the parent location, expand the location group.

Site/Building/Floor	Client Health (% Healthy Clients)				Network Health (% Healthy Devices)								Client Count	Network Device Count
	All				All	A	C	D						
USA	84%				85%								43	26
LA	67%				79%								21	19
DC	100%				100%								22	7

You can toggle the view to the **Building View** layout, which organizes metrics by building. When location groups have child sites or multiple buildings, each building is a separate line item in the list.



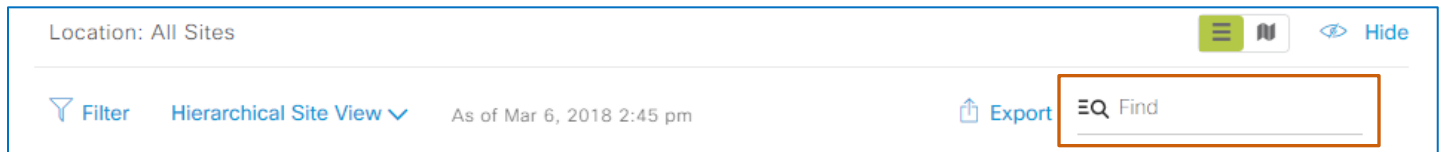
Location	Site	Health (% Healthy Clients)
USA	LA	67%
--	All Buildings	86%
Australia	MEL	100%
Netherlands	AMS	100%

The health score below each **All** column is the percentage of the total number of clients or devices that are in a healthy state and display color-coding that indicates the status of the percentage.

Client Health (% Healthy Clients)				Network Health (% Healthy Devices)					
All				All	A	C	D		
84%				85%					
86%				84%					
100%	--			100%		--	--		--
100%				67%		--	--		



When you have a long list of locations, or are looking for specific data, you can use the search function to filter the list.



### To filter the list:

- In the **Find** field, begin typing a character string that the data includes.

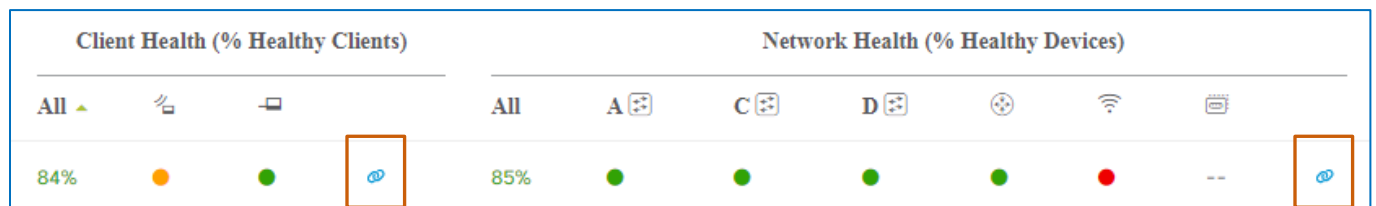
As you type, the list updates to display all of the items that match the criteria.



When you see an item for which you want to see detailed information, the page provides navigation to [the Client Health and Network Health pages](#) in Assurance.

### To navigate to a detailed information page:

- Beside the applicable health score indicators, click the link.




The system opens the **Client Health** or **Network Health** page based on your navigation. When you navigate using a link at a child site or building level, the detailed health page filters to present that location's information only.

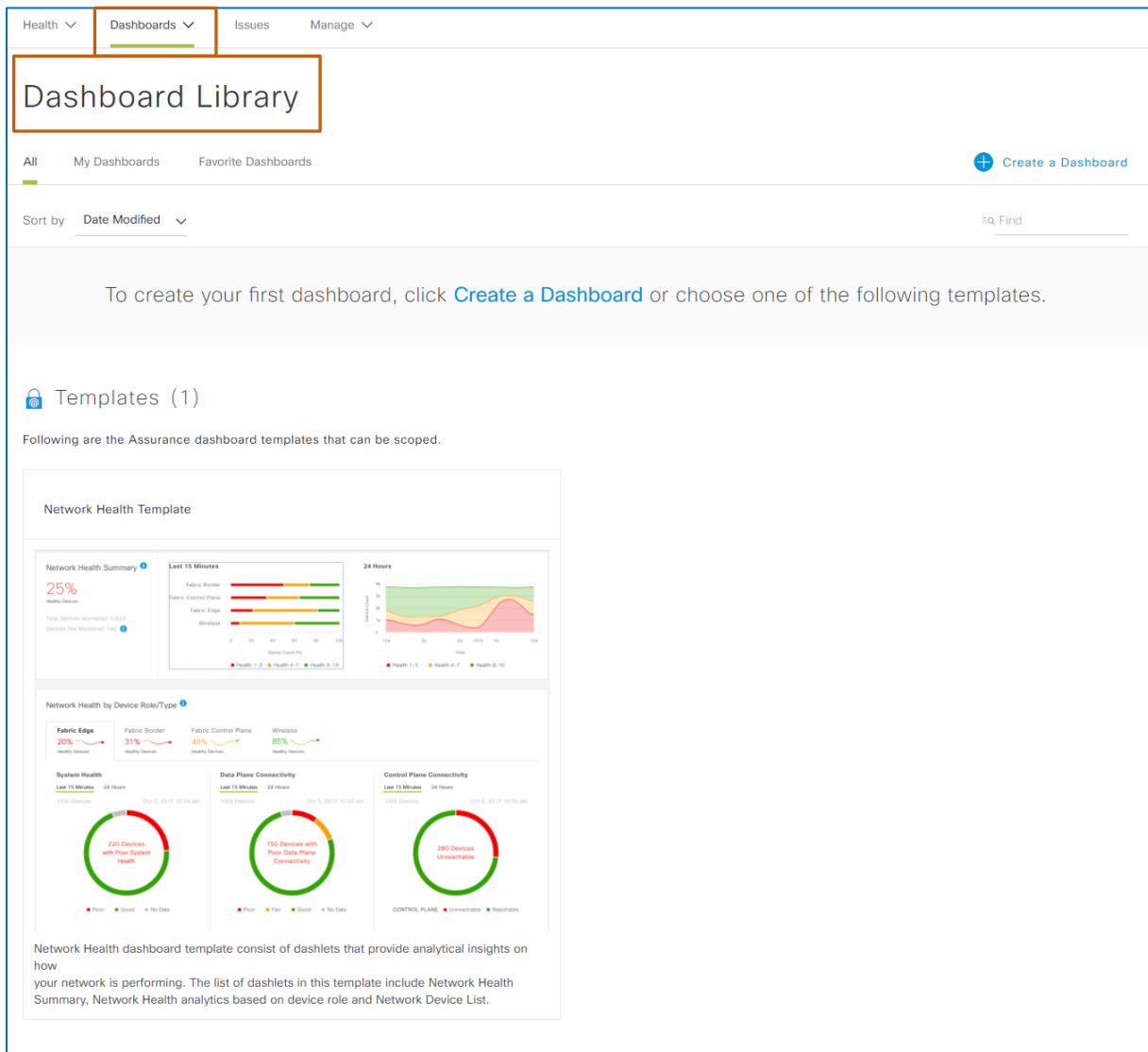
## Configuring a Custom Dashboard Page

You can configure custom pages, referred to as dashboards, which can help you to organize and access the information that is relevant to your work more efficiently. The dashboards that you configure are available to you only, and not visible to other system users.

You access, configure, and manage dashboards on the **Dashboard Library** page, which organizes the dashboards that you add on tabs.

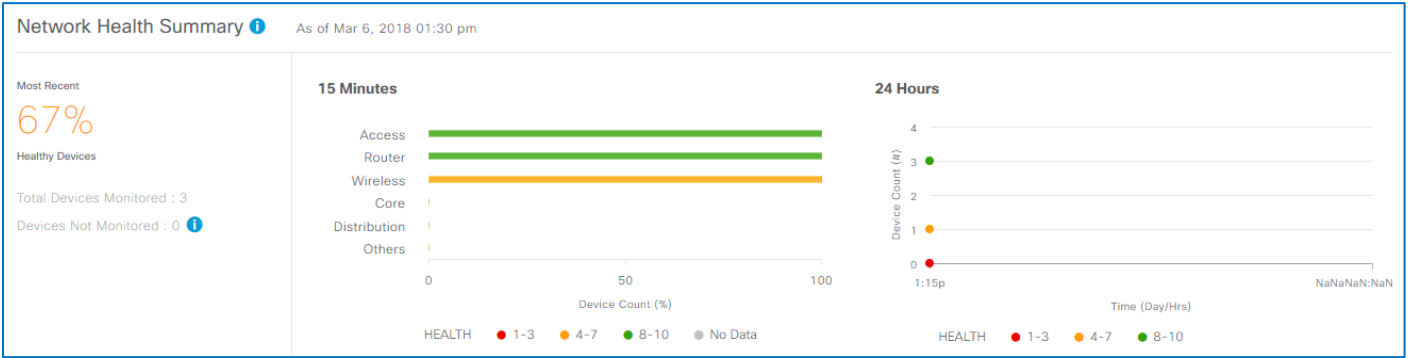
To manage custom dashboards, you can:

- Configure, edit, and delete custom dashboards.
- Copy a custom dashboard that you added and make changes to it.
-  **Tip:** This feature allows you to make minor layout adjustments efficiently without altering the original dashboard.
- Reposition [dashlets](#) on the **Overall Health**, **Network Health**, and **Client Health** pages that are available by default.

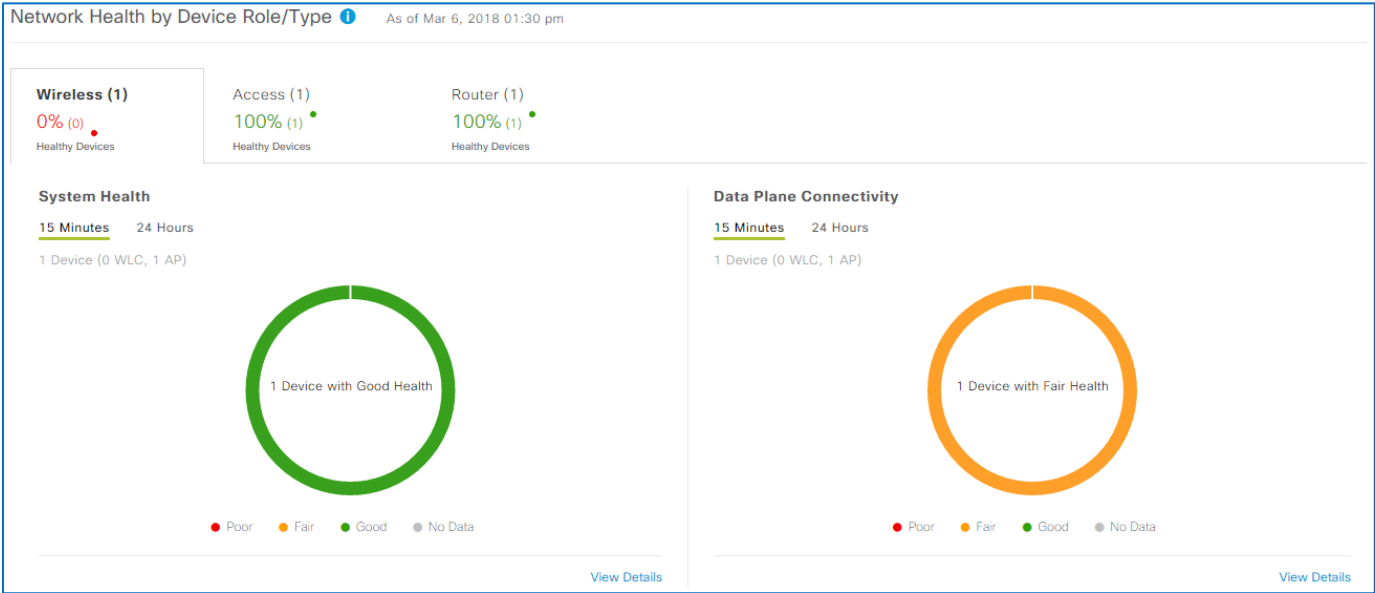


When you use the template, the dashboard includes the following dashlets with links to detailed information:

● **Network Health Summary**



● **Network Health by Device Role/Type**



● **Network Devices**

**Network Devices (3)** ⓘ As of Mar 6, 2018 1:35 pm

DEVICE **Monitored** Unmonitored TYPE **All** Access Core Distribution Router Wireless Others OVERALL HEALTH **All** Poor Fair Good

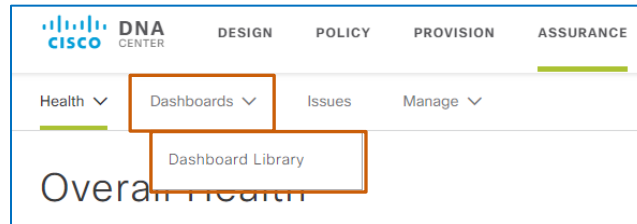
Filter Export Find

Device	Device Type	IP Address	OS Version	Overall Health Score	System Health	Data Plane Connectivity	Issue Count	
AMS-AP3802-34	AIR-AP3802I-B-K9	10.11.19.1	8.5.120.0	6	Good	Fair	0	
AMS-SW3650.test.com	WS-C3650-24PD-E	10.11.255.100	03.06.05E	10	No Data	Good	0	
AMS-ASR1K-INET	ASR1002-X	10.11.255.2	15.5(3)S2	10	Good	Good	1	

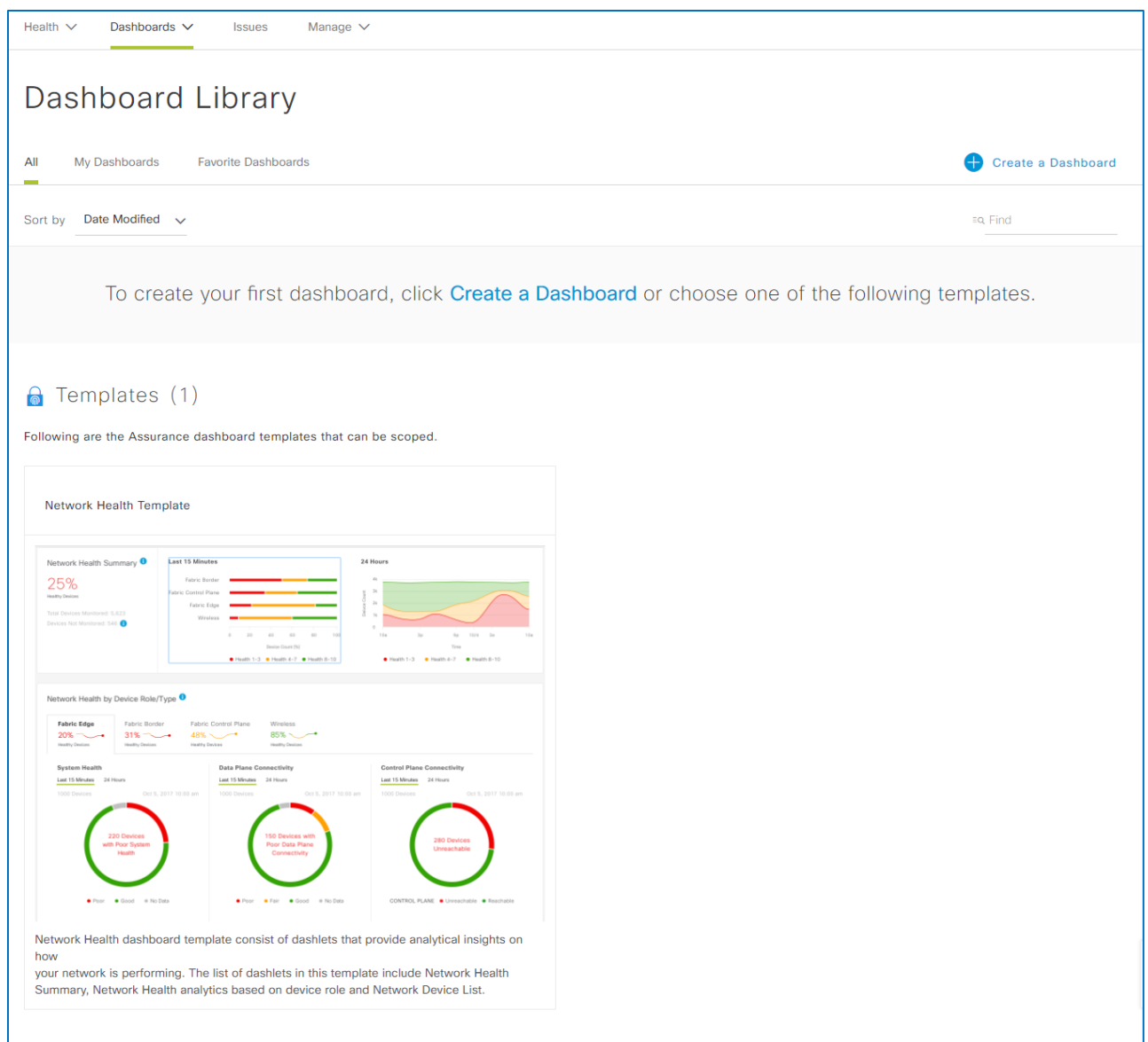
You configure custom dashboards by adding a unique page to the system, and then adding and positioning dashlets on the page.

### To configure a custom dashboard:

1. On the menu bar, on the **Dashboards** menu, click **Dashboard Library**.



The **Dashboard Library** page opens. You can add a new dashboard or copy the template and edit it, as needed.



**Dashboard Library**

All My Dashboards Favorite Dashboards [+ Create a Dashboard](#)

Sort by Date Modified [Find](#)

To create your first dashboard, click [Create a Dashboard](#) or choose one of the following templates.

**Templates (1)**

Following are the Assurance dashboard templates that can be scoped.

**Network Health Template**

**Network Health Summary**

25% Healthy Devices

Total Devices Monitored: 5,625  
Devices Not Monitored: 240

**Last 15 Minutes**

Fabric Border: 100% Healthy  
Fabric Control Plane: 100% Healthy  
Fabric Edge: 100% Healthy  
Wireless: 100% Healthy

**24 Hours**

Health 1-3: 100% Healthy  
Health 4-7: 100% Healthy  
Health 8-10: 100% Healthy

**Network Health by Device Role/Type**

**Fabric Edge**: 20% Healthy Devices

**Fabric Border**: 31% Healthy Devices

**Fabric Control Plane**: 40% Healthy Devices

**Wireless**: 85% Healthy Devices

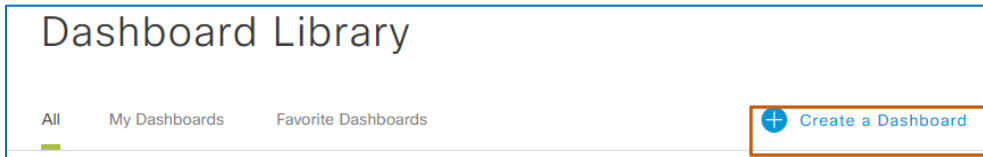
**System Health**: 230 Devices with Poor System Health

**Data Plane Connectivity**: 180 Devices with Poor Data Plane Connectivity

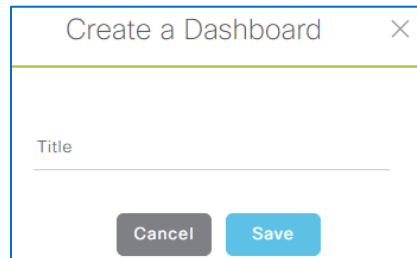
**Control Plane Connectivity**: 280 Devices Unreachable

Network Health dashboard template consist of dashlets that provide analytical insights on how your network is performing. The list of dashlets in this template include Network Health Summary, Network Health analytics based on device role and Network Device List.

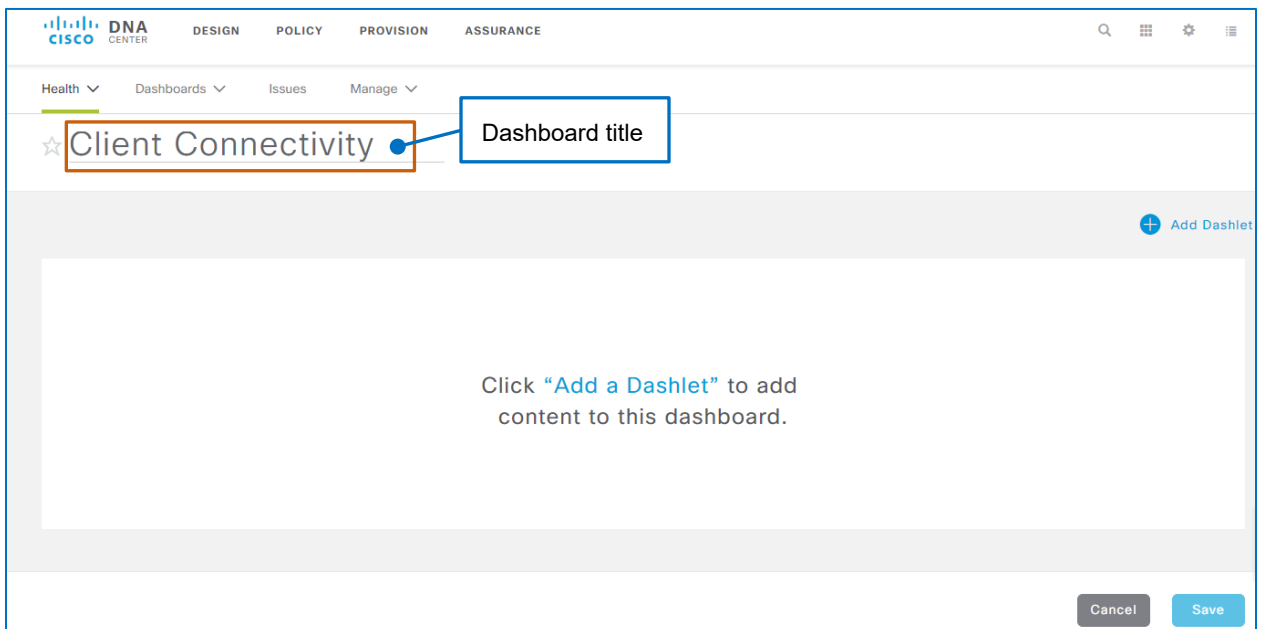
- To add a dashboard, click **Create a Dashboard**.



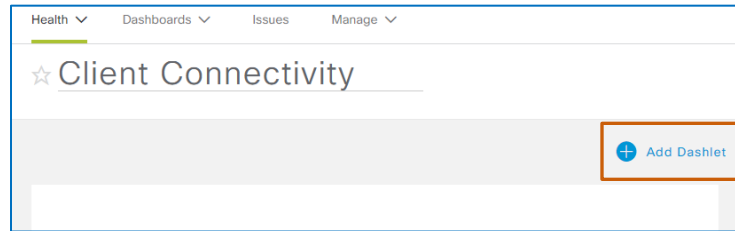
The **Create a Dashboard** dialog box opens.



- In the **Create a Dashboard** dialog box, type a meaningful dashboard name that describes its use, and then click **Save**.
  - When adding a custom dashboard, a blank dashboard page opens with the dashboard title



- To continue configuring the custom dashboard, click **Add Dashlet**.



The **Add Dashlet** panel opens and lists all of the available dashlets by default.



**Tip:** To see a dashlet layout to the right of the list:

- In the list, select the dashlet row.

### Add Dashlet

All
x

Find dashlet by name or tag(s)

#### Client Health Dashlets

☐ **Client Health Summary**  
Overall wired and wireless client device health determined by onboarding response times and failures plus connect...

☐ **Client Onboarding Times**  
Distribution of total response times from start to finish for wired and wireless client onboarding covering Associati...

☒ **Connectivity RSSI**  
Overall wireless client connectivity distribution based on RSSI values.

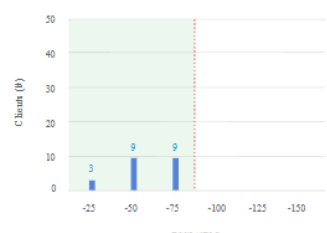
☐ **Connectivity Physical Link**  
Overall wired client physical link connectivity distribution based on link errors.

☐ **Client Count per SSID**  
Overall wireless SSID

#### Connectivity RSSI

Last 30 Minutes
24 Hours

Aug 11, 2017 10:00 am



Tags
connectivity, RSSI

Cancel
Add



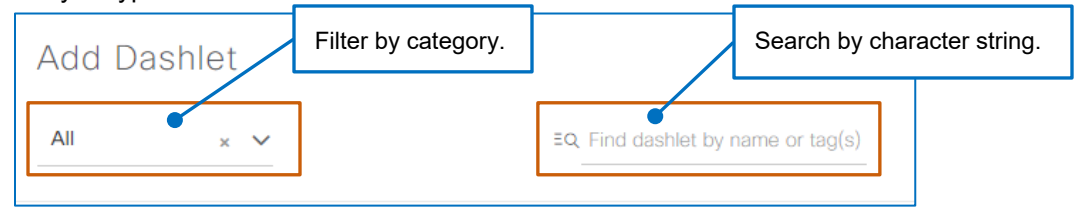
### Search Tips:

To filter the list of dashlets by a category:

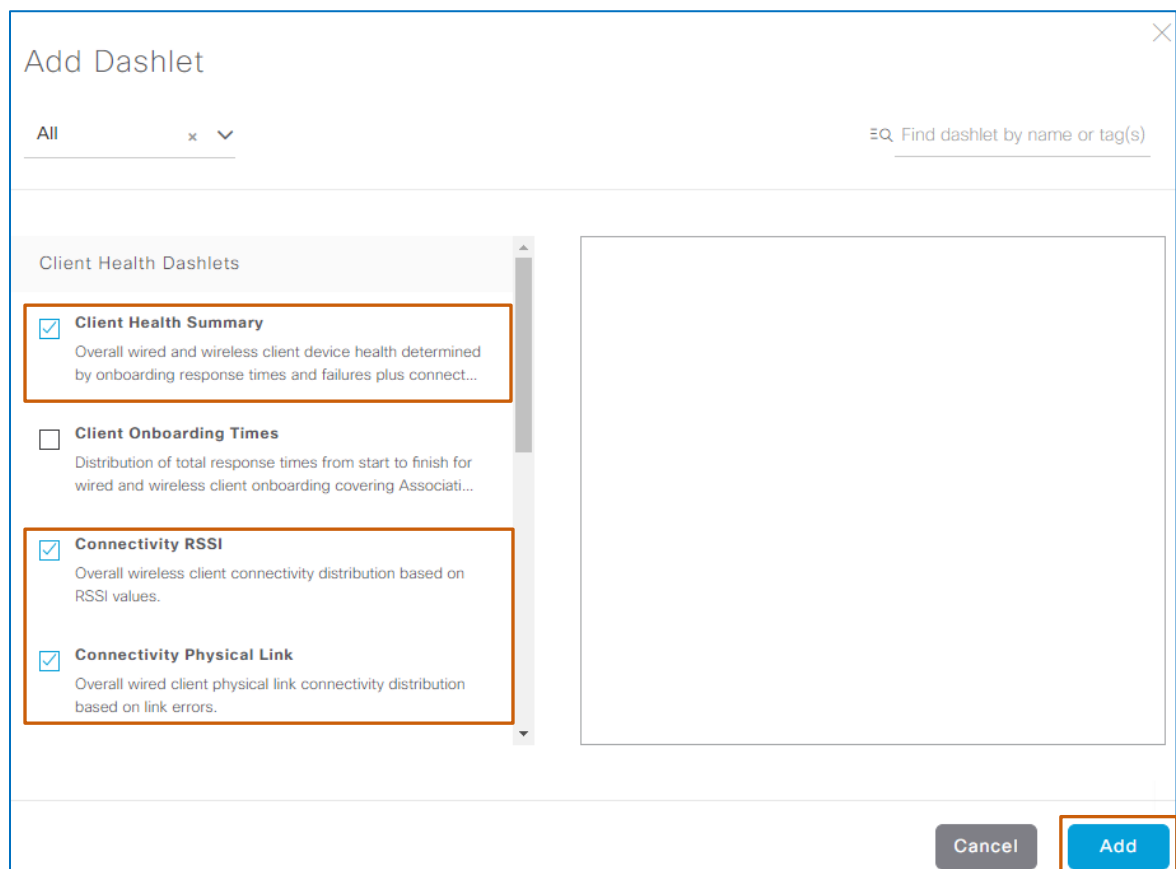
- Below **Add Dashlet**, in the drop-down list, select the category.

To find a dashlet using a character string:

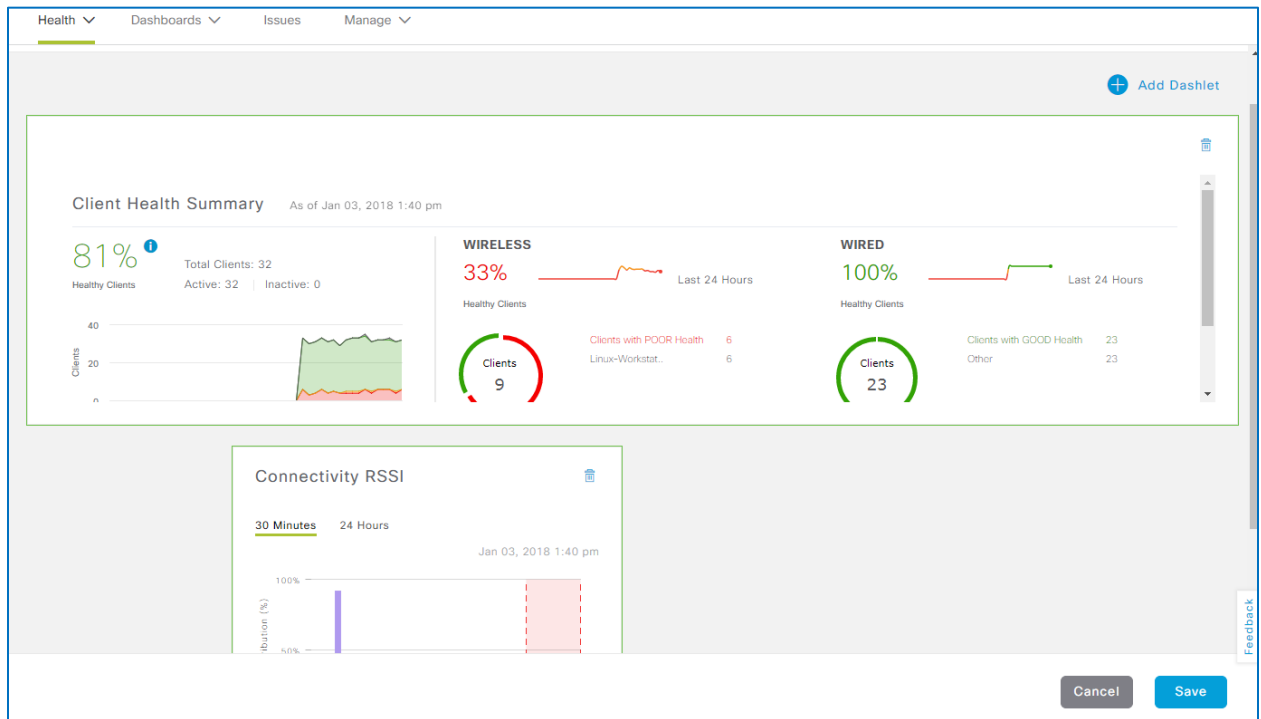
- In the search field, begin typing a character string. The list updates automatically to display all of the dashlets containing the string that you typed.



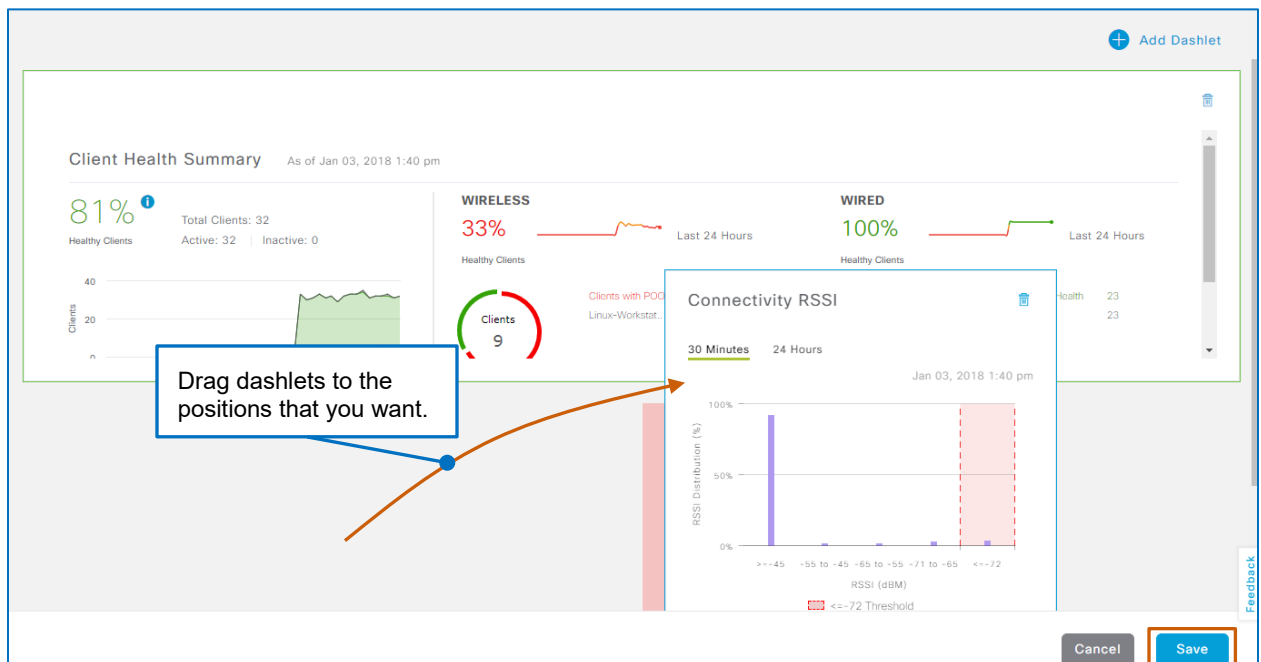
- Beside the name of each dashlet that you want to add, select the check box, and then click **Add**.



The system adds the dashlets to the page.

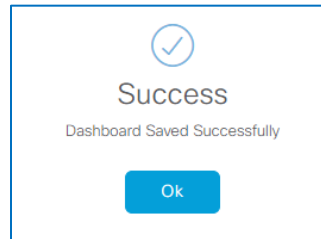


6. To organize the layout, drag each dashlet to the position that you want on the page.
7. To add the dashboard to Cisco DNA Center, click **Save**.



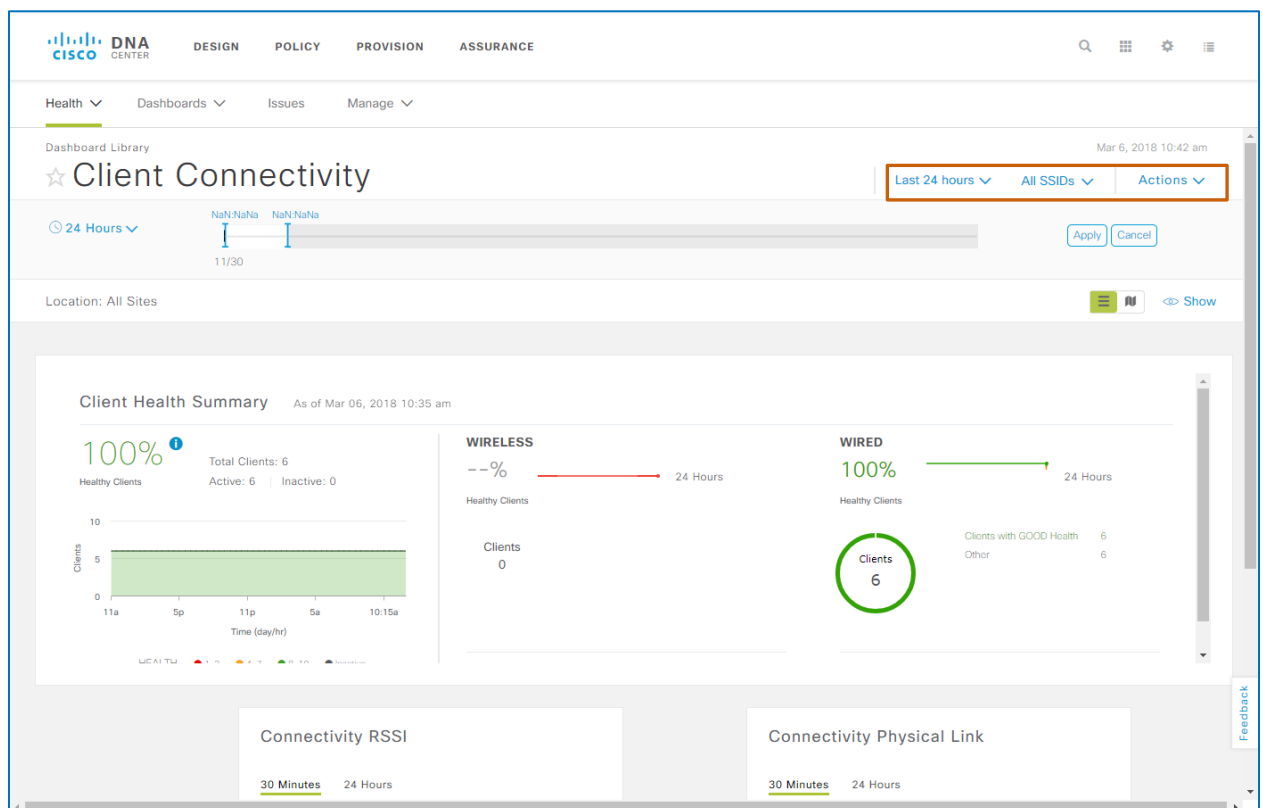


A system message opens confirming the save action.



8. In the message, click **Ok**.

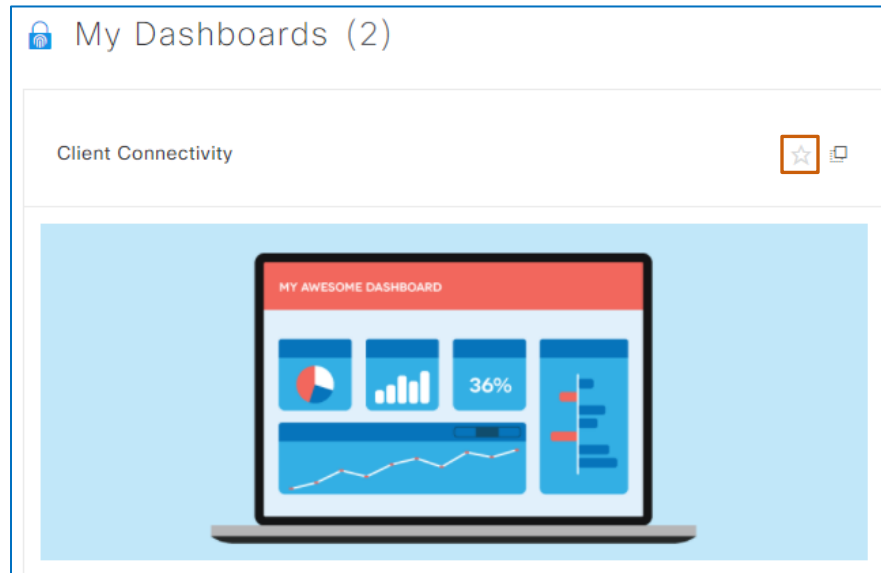
The dashboard that you configured is the active dashboard on the page and a global toolbar is available for use with the dashboard. The dashboard is also available on the **All** and **My Dashboards** tabs on the **Dashboard Library** page.



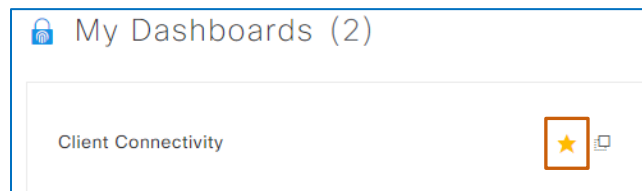
You can identify custom dashboards as favorites, which makes them available on the **Favorite Dashboards** tab.

To make the dashboard available on the **Favorite Dashboards** tab:

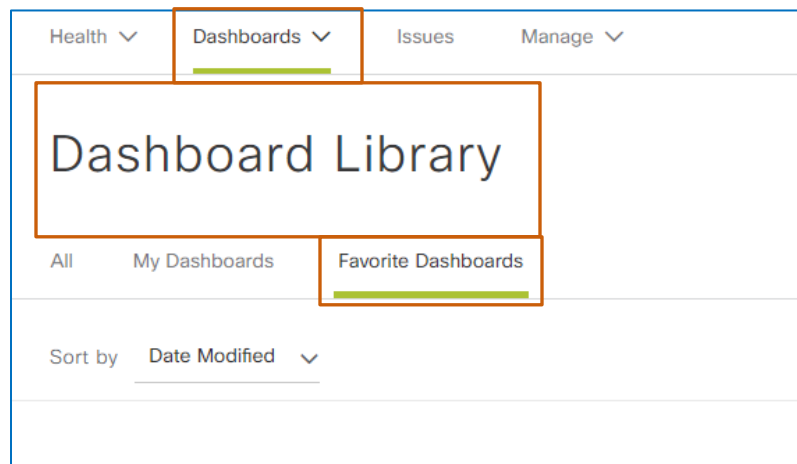
- On any dashboard tab displaying the dashboard, to the right of the dashboard name, click **Add to Favorites**.



The icon turns yellow to indicate that the dashboard is included as a favorite...

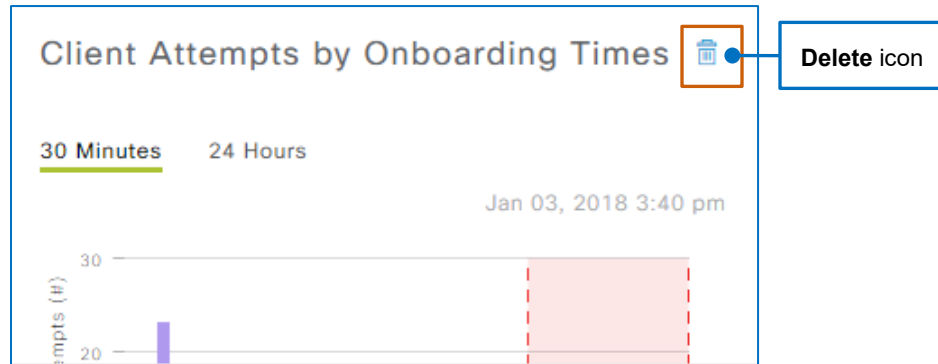


...and the dashboard is available on the **Favorite Dashboards** tab on the **Dashboard Library** page.

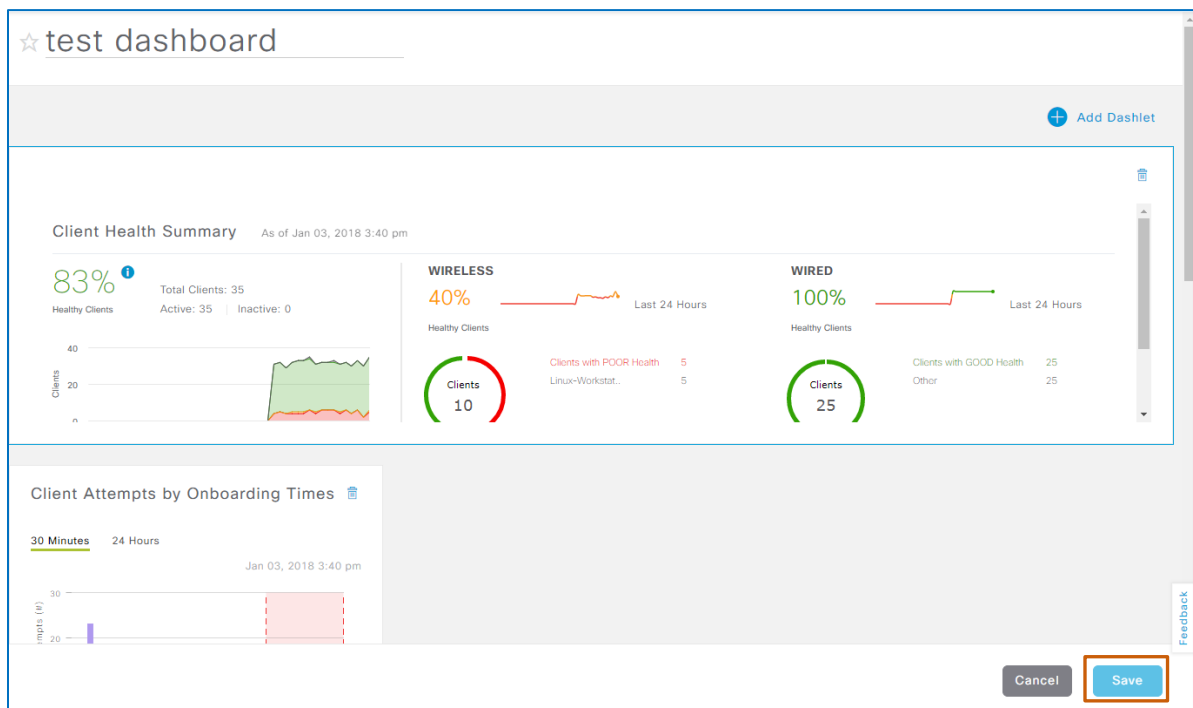


**To edit custom dashboards that you have added:**

1. Open the dashboard page, and then, on the **Actions** menu, select **Edit Dashboard**
2. To add or reposition dashlets, [follow steps 4a - 4d in configuring a custom page.](#)
3. To remove a dashlet, beside the dashlet heading, click **Delete**.

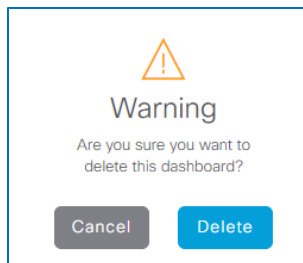


4. When you complete your changes, click **Save**.



**To delete custom dashboards that you have added:**

1. Open the dashboard page, and then, on the **Actions** menu, select **Delete Dashboard**.  
A system message opens so that you can confirm the action.



2. To continue, click **Delete**.  
The system removes the dashboard.

## Reviewing Detailed Information by Category

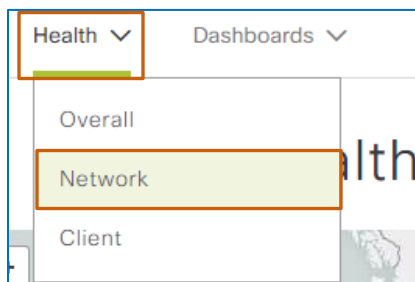
The system provides various ways for you to navigate to see only network infrastructure or client health information.



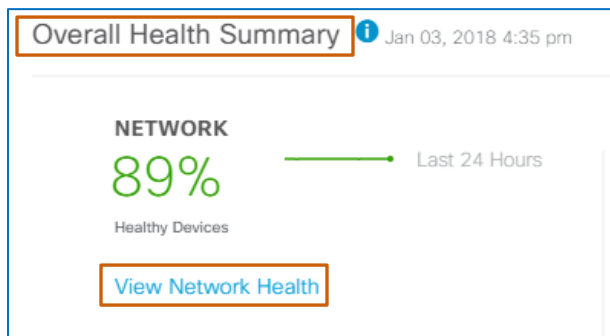
**Important Note:** When you apply a site filter on the **Overall Health** page, and then navigate to network infrastructure or client health information, the system applies the same site filter to that page automatically.

**To open the Network Health page:**

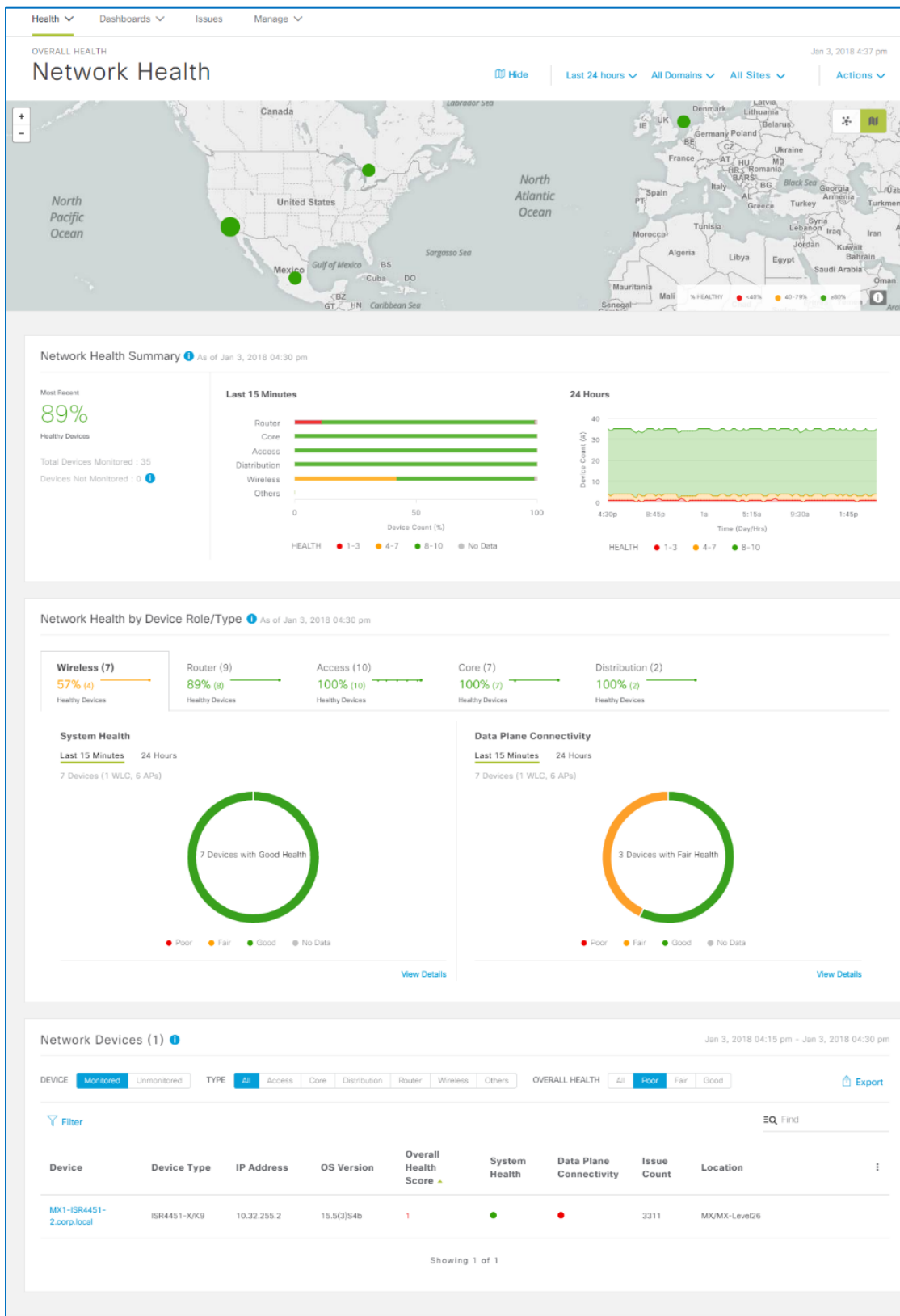
- On the **Health** menu, select **Network**.



- In the **Overall Health Summary** dashlet, under **Network**, click **View Network Health**.

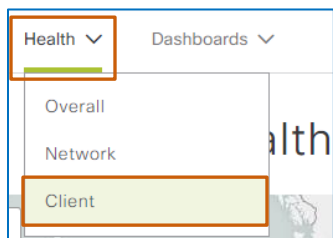


Either action navigates you to detailed network health metrics for all of the network sites.

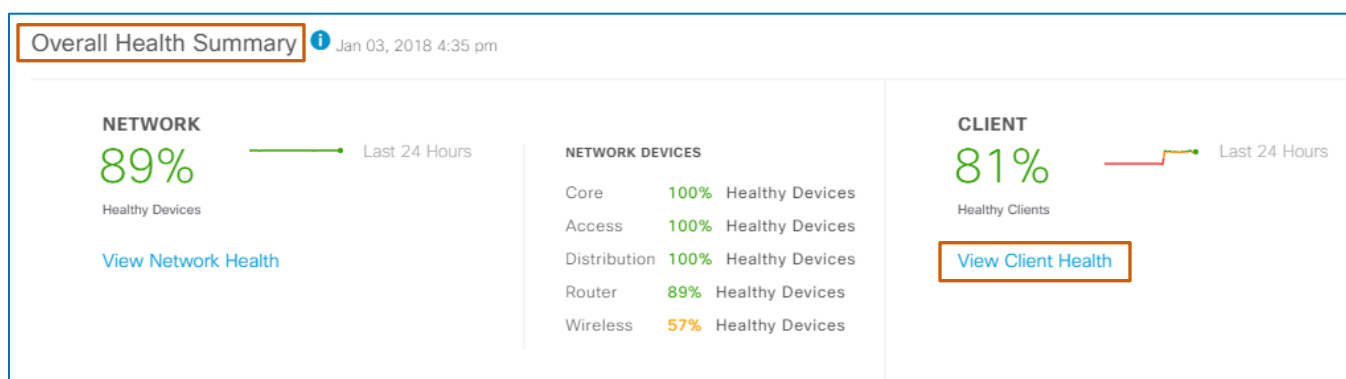


To open the Client Health page:

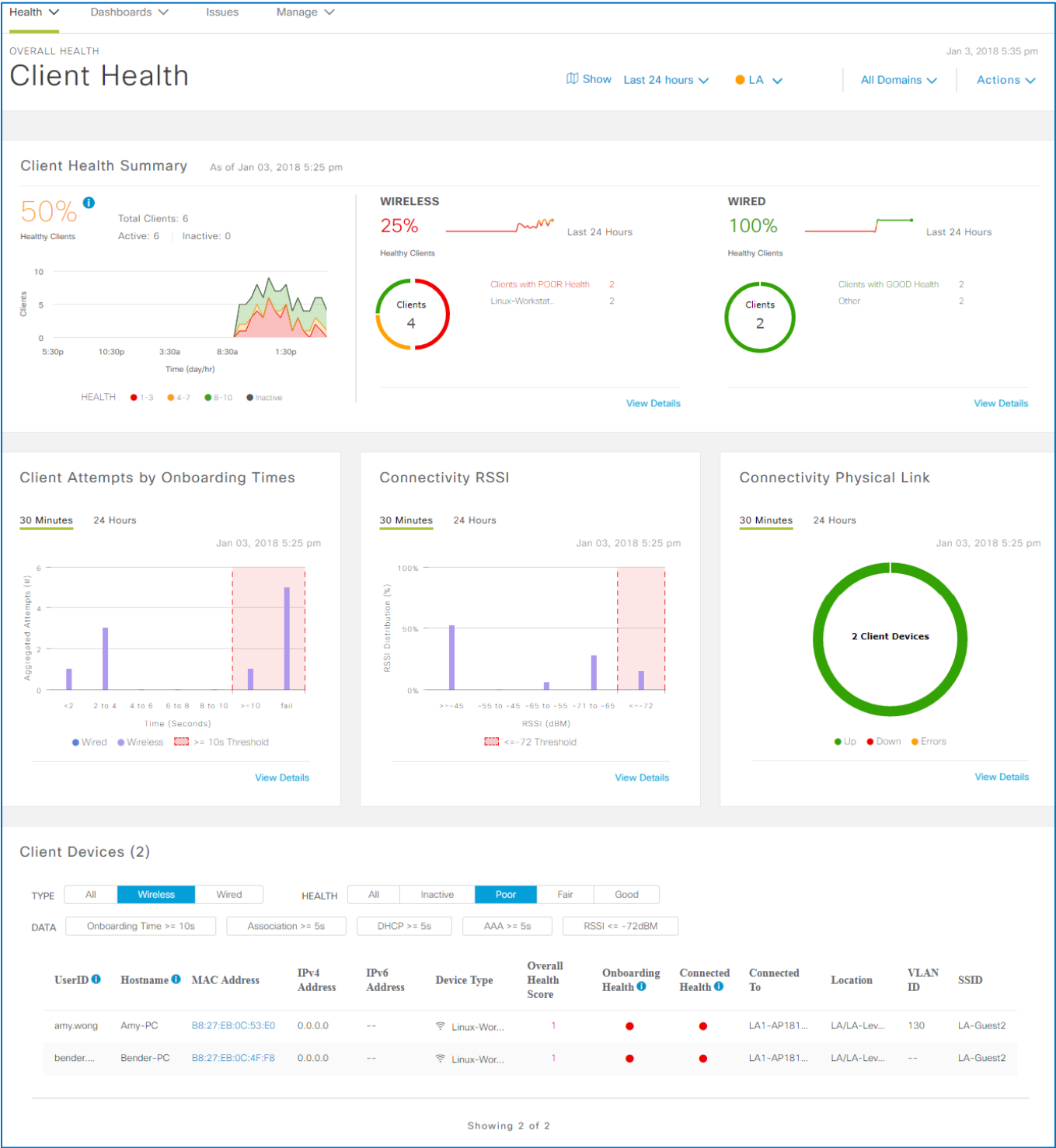
- On the **Health** menu, select **Client**.



- In the **Overall Health Summary** dashlet, under **Client**, click **View Client Health**.



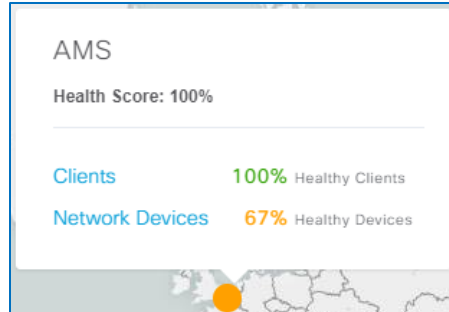
Either action navigates you to detailed client health metrics for all of the network sites.



**To open detailed network infrastructure or client health pages for a specific location:**

1. On the geographical map, click an icon that represents an individual location.

A pop-up window opens with summary health metrics.



2. To open detailed health information for the location:

- To open client health details, click **Clients**.
- To open network infrastructure health details, click **Network Devices**.

The system navigates to the applicable health details page, filtered to display the information for the location that you selected.



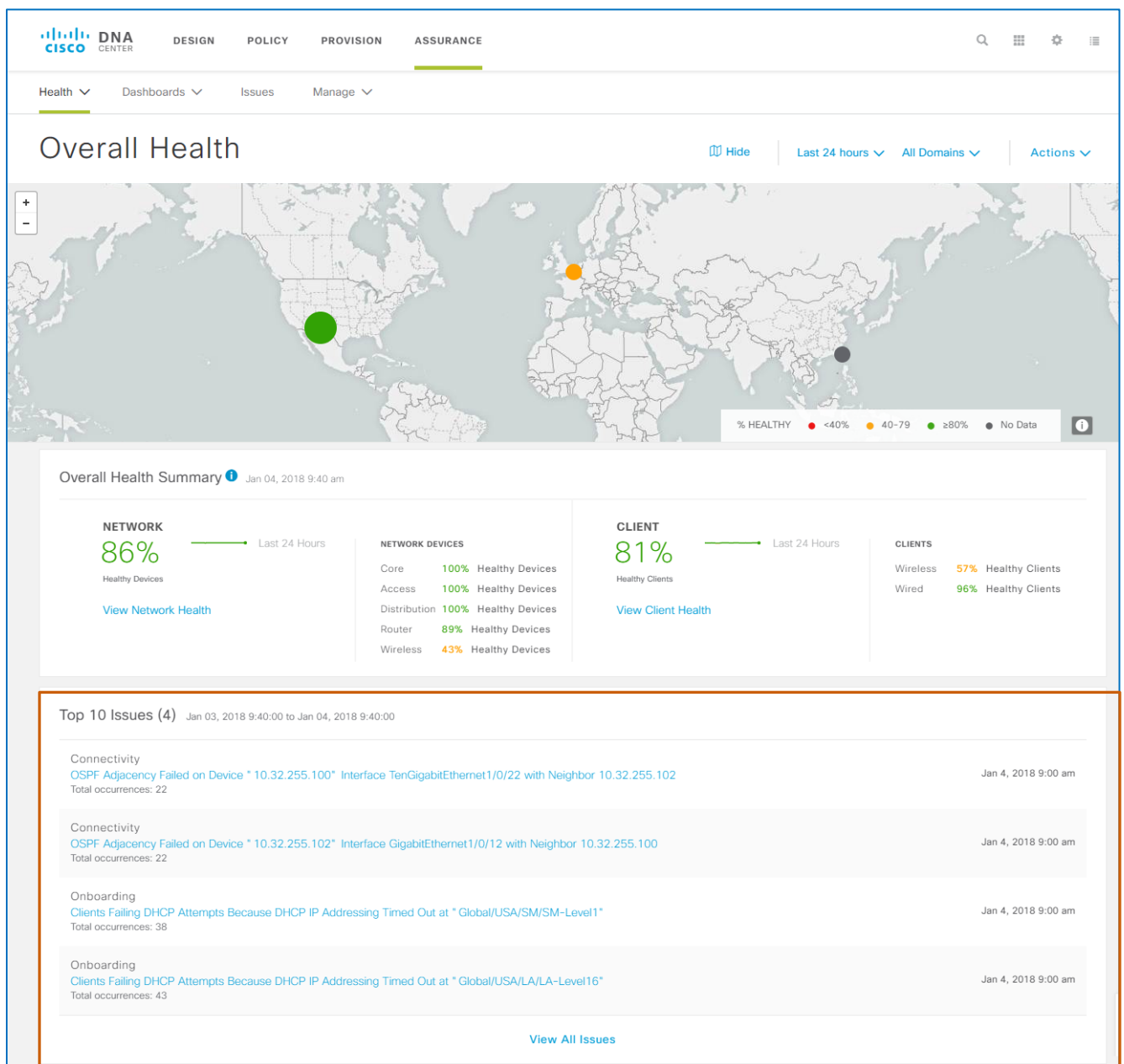
## Reviewing Issues

The **Overall Health** page summarizes [up to 10 of the most critical issues](#) so that users can determine whether an item might need more immediate attention due to the number of affected users.

Each issue item includes the type of issue, a summarized description of the issue, the number of times the issue has occurred [for the time period that is applied to the page](#), and the most recent date and time that it occurred.



**Note:** To review a list of the issues that Cisco DNA Center logs, [refer to the Issue Catalog topic in the Cisco Digital Network Architecture Center User Guide](#).



To open details for an issue listed in the Top 10 Issues list:

- In the list, click the issue description link.


Onboarding

Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at "Global/USA/SM/SM-Level1"

Total occurrences: 38

Jan 4, 2018 9:00 am

A panel opens with detailed information about the issue, metrics, affected locations or clients, and suggestions for resolving the issue.


DNA CENTER

DESIGN
POLICY
PROVISION
ASSURANCE

Health
Dashboard

86%
Healthy Devices
View Network

Top 10 Issues (4)

Connectivity
OSPF Adjacency Fail
Total occurrences: 22

Connectivity
OSPF Adjacency Fail
Total occurrences: 22

Onboarding
Clients Failing DHCP
Total occurrences: 38

Onboarding
Clients Failing DHCP
Total occurrences: 43

Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at "Global/USA/SM/SM-Level1"

Status: Open
Last Occurred: Jan 4, 2018 9:00 AM

**Description**

Clients located in "Global/USA/SM/SM-Level1" timed out and have not been assigned an IP address from the DHCP server.

**Impact**

Location: 1 Building

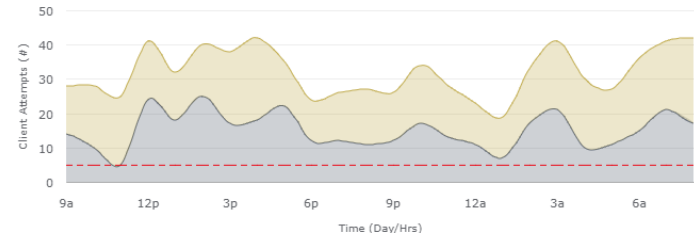
Clients: 4 Wireless Clients

**Suggested Actions (6)**

- 1 Verify that the DHCP scope is configured correctly. Best Practice - Design an IP address pool that is two to three times larger than the expected number of users.
- 2 Reduce the DHCP lease time. Best practice - DHCP lease time for high-density, high mobile environment is 15-30 min.
- 3 Verify whether the IP helper address on Router is configured correctly.
- 4 Verify whether the DHCP server has a route to the subnet of the VLAN.
- 5 Verify that the clients are configured for IPv4 DHCP.
- 6 Verify that the clients are in the range of access points.

**Client DHCP Attempts**

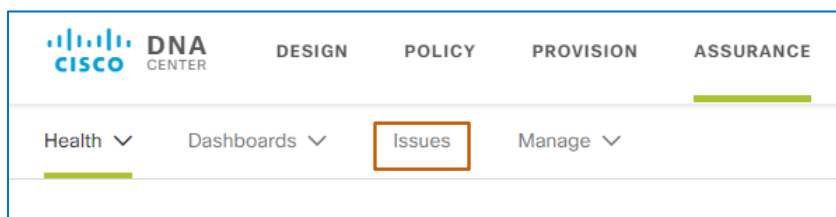
Jan 3, 2018 9:00 am to Jan 4, 2018 9:00 am



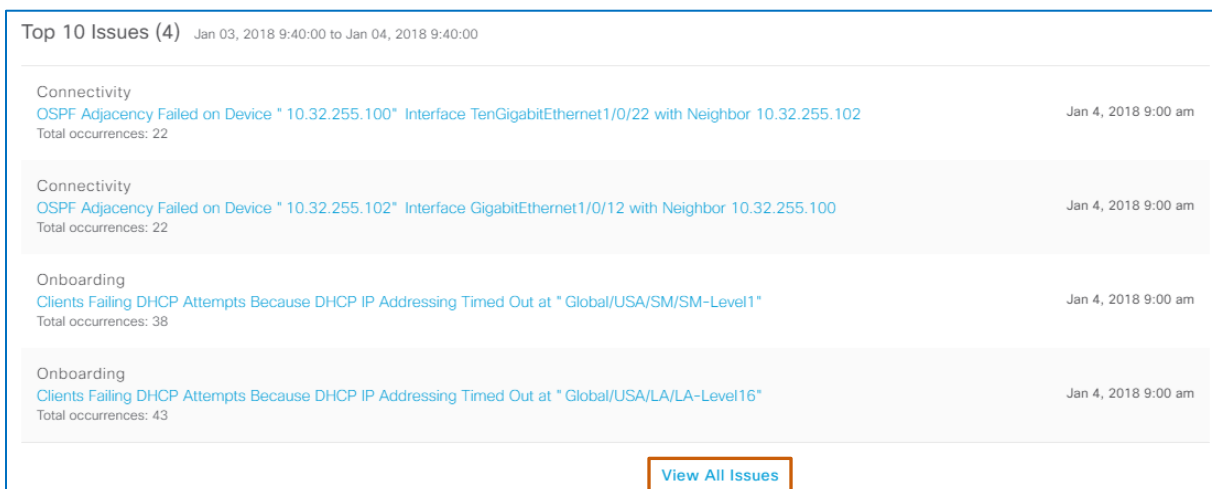
Impacted Client... < ● ● > Impacted Client...

To open lists of all of the open and resolved issues:

- On the menu bar, click **Issues**.



- Below the **Top 10 Issues** list, click **View All Issues**.



The **Issues** page opens and provides complete lists of open and resolved issues, which the system retains for a rolling 7 day period.

The system does not close issues automatically. System users can change an open issue to a resolved status manually. Or, based on the time period applied to the page, the issue will not appear on the list if it has not occurred within that time period, up to the 7 day retention limit.

Health	Dashboards	Issues	Manage
Issues			
Open		Resolved	
Last Occurred Time	Title	Total Occurrences	Category
Jan 4, 2018 10:00 am	OSPF Adjacency Failed on Device "10.32.255.102" Interface GigabitEthernet1/0/12 with Neighbor 10.32.255.100	22	Connectivity
Jan 4, 2018 10:00 am	OSPF Adjacency Failed on Device "10.32.255.100" Interface TenGigabitEthernet1/0/22 with Neighbor 10.32.255.102	22	Connectivity
Jan 4, 2018 9:30 am	Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at "Global/USA/SM/SM-Level1"	38	Onboarding
Jan 4, 2018 9:30 am	Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at "Global/USA/LA/LA-Level16"	43	Onboarding

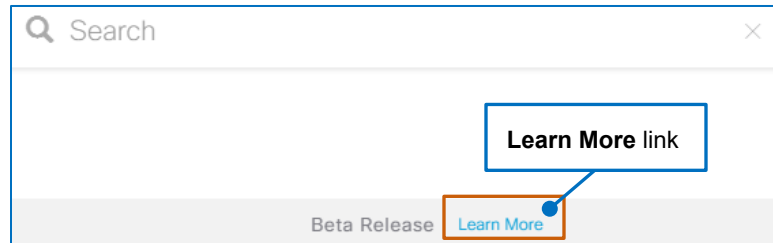
## Searching for Devices, Users, or Client Endpoints

Cisco DNA Center provides a global search function that returns results on various network infrastructure, user names, and client endpoint parameters.

When you receive notifications of issues that affect specific network users or network devices, you can use this feature for more efficient navigation to the metrics that you need to evaluate.

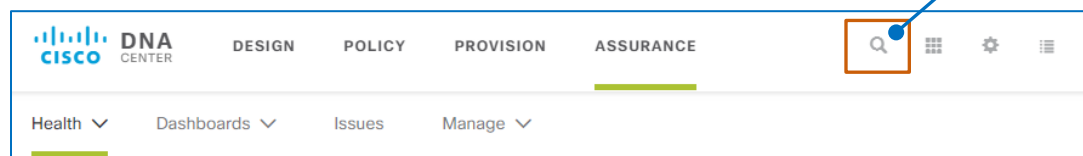


**Tip:** For a complete list of search parameters, in the **Search** dialog box, click **Learn More**.

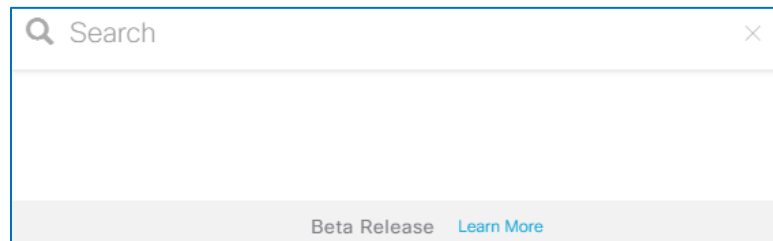


**To perform a search:**

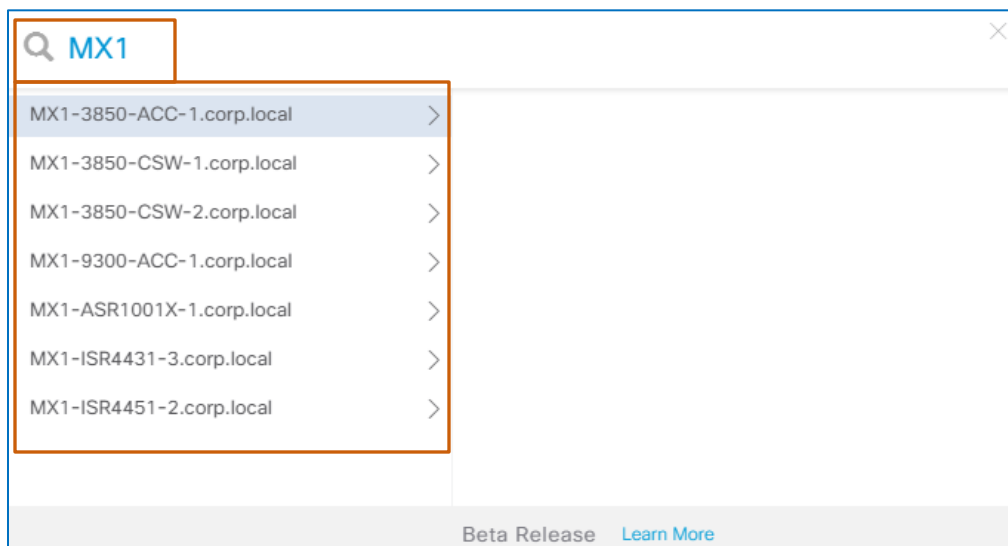
1. On the application toolbar, click the search icon.



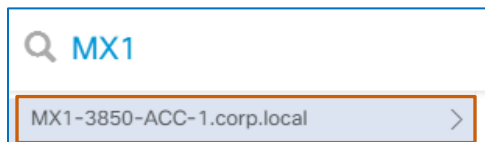
The **Search** dialog box opens.



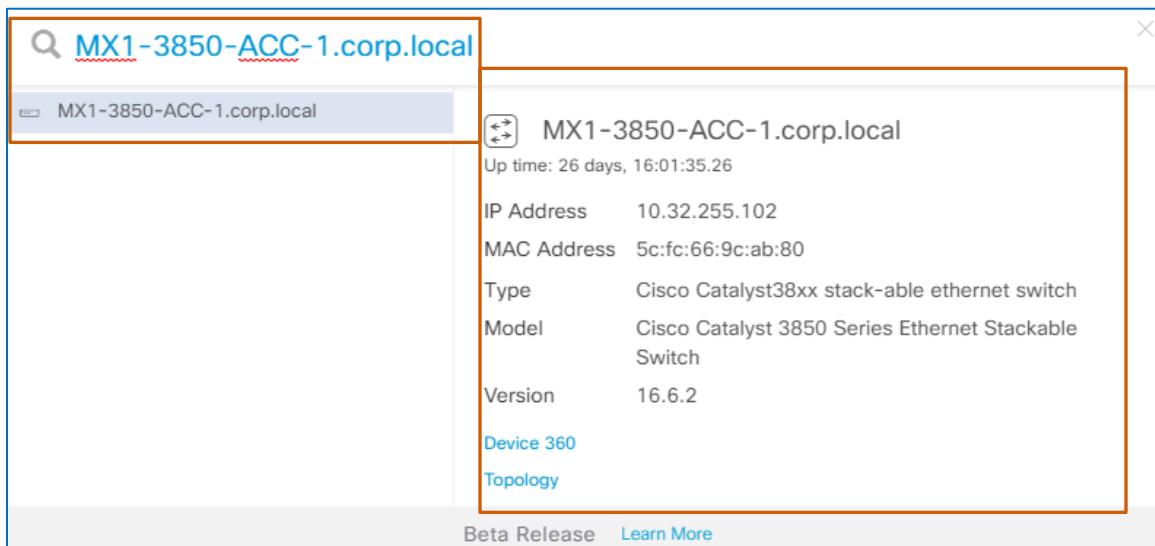
- In the **Search** field, begin typing the applicable character string.  
A list of results matching the characters that you type begins populating automatically.



- To open details about an item in the list, click the item.



Details about the item open in the dialog box and, based on the item type, links to more information are available.



# Links

## To Product Information

[Visit the Cisco Web site to learn more about Cisco DNA Center.](#)

[Visit the Cisco Web site to review or download technical documentation.](#)

## To Training

[Visit the Cisco Web site to access learning opportunities for other Cisco products.](#)

## To Contact Us

[Send us a message with questions or comments about this training.](#)



**Note:** Please send messages that address training content only.  
Follow your regular business process to request technical support or address technical or application-related questions.