



Navigating Assurance Client Health

Cisco DNA Center 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. 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.

Navigating Assurance Client Health

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

Contents

Basics

Why Is It Important?

Where Does It Happen?

What Skills Do I Need?

Basic

Proficient

What Terms Should I Know?

Fabric Domain

Network Hierarchy

WLANs or SSIDs

Evaluating the Big Picture...

...on the Client Health Page.

What Will I See?

And What Will I See...

On the Geographical Map?

In the List View?

Where Do I Find Client Health Organized...

...By SSIDs (WLANs)?

...By Radio Frequencies?

What Are the Common Page Features?

Dashlet Chart Elements on the Client Health Page

Detailed Information Panels

Endpoint Lists

How Can I Add or Position Dashlets?

What Affects the Information That I Am Seeing?

Time Periods and Time Stamps

Changing the Time Period

Persistent Filters on Page Navigation

How are Client Health Metrics Looking?

Get a Summary View of Client Health

What Will I See?

Where Do I Find...

...Client Onboarding Attempts and Lengths of Time until Onboarded?

The Client Onboarding Times Dashlet

The Client Onboarding Times Panel

...The Signal Strengths That Endpoints are Receiving (RSSIs)?

The Connectivity RSSI Dashlet

The Connectivity RSSI Panel

...Signal-to-Noise Ratios for Client Endpoints?

- The Connectivity SNR Dashlet*
- The Connectivity SNR Panel*
- ...The Number of Clients That Are Associated To Each SSID?
 - The Client Count per SSID Dashlet*
 - The Client Count per SSID Panel*
- ...The Number of Clients That Are Using Each Radio Band Frequency?
 - The Client Count per Band Dashlet*
 - The Client Count per Band Panel*
- ...The Physical Link Health of Wired Clients?
 - The Connectivity Physical Link Dashlet*
 - The Connectivity Physical Link Panel*
- ...The Numbers of DNS Requests and Responses per Minute?
 - The DNS Dashlet*
- ...Health Metrics and Attributes for Client Devices?
 - The Client Devices List*

How is a Specific Client Endpoint Doing?

Get a Holistic View on the Client 360

What Will I See?

How Do I Open the Client 360 Page for a Specific Endpoint?

Where Do I Find...

- ...Issues That Are Affecting the Endpoint?
- ...A List of Resolved Issues and Their Details?
- ...The Endpoint's Network Path and the Health of Devices on the Path?
- ...Endpoint-Related Events and Their Statuses?
- ...The Tool for Evaluating the Path That Traffic Is Using?
 - Path Traces for Flow Mapping and Path Health*
 - How Do I Prepare To Run a Path Trace?*
 - How Do I Run a Path Trace?*
- ...Application Use and Health?
- ...More Metrics and Detailed Information?

The Detail Information Section

Reviewing Device Type and Connectivity Attributes

Reviewing Transmit / Receive Metrics and DNS Request / Response Times

Reviewing Signal Strength and Signal to Noise Metrics

Reviewing Apple® iOS Client Metrics and Connectivity to APs

What Was an Endpoint Experiencing at a Certain Time?

How Are All of a Single User's Clients Doing?

Get a Holistic View on the User-Based Client 360

What Will I See?

How Do I Open a User-Based Client 360 Page?



Core Software Group

Watch It Happen in Cisco DNA Center

Video

Evaluating a System User's Printer Connection (8:00)

Want More?

Find Product Information

Find Training

Contact Us About This Training

Basics

Why Is It Important?

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 network monitoring results and proactive insights into:

- Wired or wireless client endpoint device health, such as computers, mobile devices, or equipment.
- Potential or active client issues or failures that can affect business operations.

Cisco DNA Center **Assurance** presents detailed metrics, data, and history on clients, including:

- Wired and wireless client health.
- Client onboarding times.
- Received signal strength indicator (RSSI) measurements.
- Wired client connectivity health.

When you combine current network complexities with bring-your-own-device policies and other integrated equipment, managing clients effectively is critical to:

- Ensuring network service levels, network security, and end users' network experiences.
- Managing enterprise operations.
- Proactively planning for network growth.

Assurance also presents wireless client disconnection information for some Apple iOS devices.

This training introduces you to:

- The types and levels of information that the **Client Health** page provides.
- The organization and layout of page features.
- General navigation and functions that you can use to access the information that you need.



Important Notes: The functionality that you see and the tasks that you can perform depend on the system's licensing and configuration, and on your system user role.

To recognize the overarching features and navigation that are available in **Assurance**, [review the Assurance Features and Navigation training](#).

Where Does It Happen?

You can view client insights, health states, and performance metrics on the **Client Health** page for all of the client endpoints connected to the network [based on the settings that can affect what you see.](#)



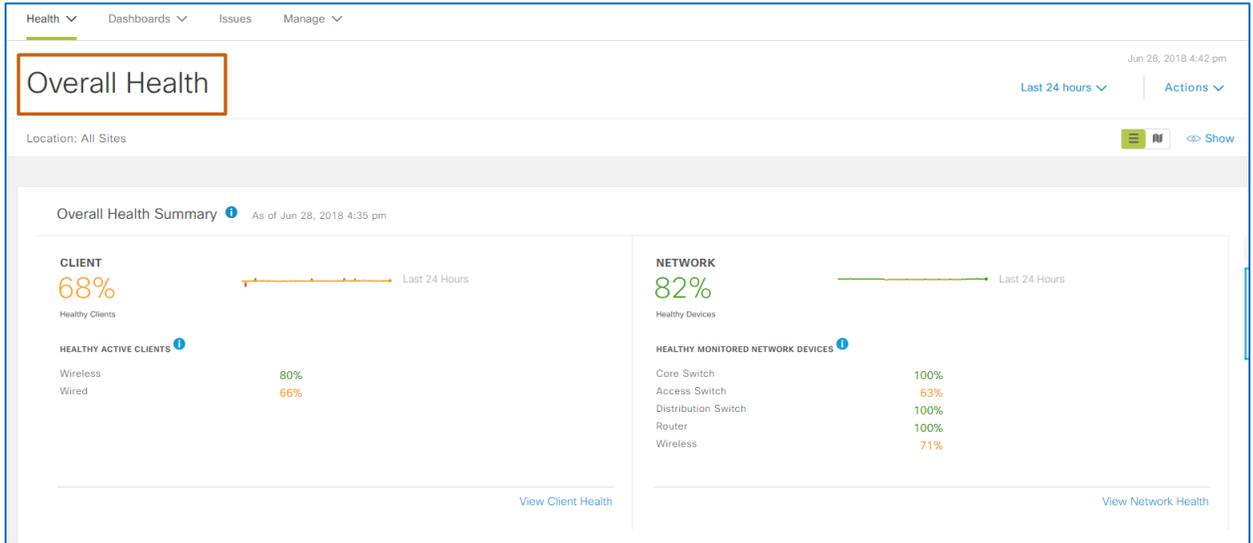
Note: Assurance also provides [the Client 360](#) page for detailed health and metrics data related to a specific client endpoint.

The screenshot displays the 'Client Health' dashboard with the following sections:

- Client Health Summary:** Shows overall health metrics. All Clients: 69% (Healthy Clients: 35, Active: 35, Inactive: 0). Wireless health is 100% (3 Clients: 3 Apple-iPad, 1 Sensor-Client, 1 iPhone 7). Wired health is 66% (32 Clients: 1 Clients with POOR Health, 1 Device Type, 1 Other).
- Client Onboarding Times:** Bar chart showing aggregated attempt (s) over time (seconds).
- Connectivity RSSI:** Bar chart showing RSSI Distribution (%) over time (dBm).
- Connectivity SNR:** Bar chart showing SNR Distribution (%) over time (dB).
- Client Count per SSID:** Donut chart showing 3 Devices (LA-Corporate2, UNKNOWN).
- Client Count per Band:** Donut chart showing 3 Devices (5 GHz).
- Connectivity Physical Link:** Donut chart showing 32 Client Devices (Up, Down, Errors).
- Client Devices (3):** Table listing device details.

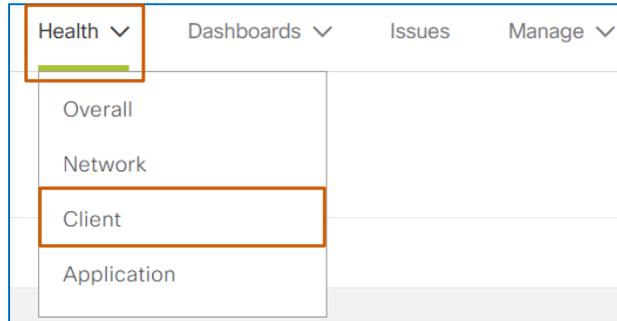
UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Onboarding Health	Connected Health	Connected Network Device	Location	VLAN ID	SSID	AP Group
daphne...	Daphne-iP...	6C:19:CD:8D:87:C9	10.30.100.27	--	Apple-iPad	10	●	●	LA2-AP380...	USA/SM/Le...	100	--	LA1
daphne...	Daphne-iP...	A8:BE:27:36:70:11	10.30.100.29	--	iPhone 7	9	●	●	LA2-AP380...	USA/SM/Le...	100	LA-Corpor...	LA1
sensor...		00:A7:42:CB:AC:E0	10.30.100.25	--	Sensor-CL...	10	●	●	LA2-AP380...	USA/SM/Le...	100	LA-Corpor...	LA1

The **Assurance | Overall Health** page provides several methods by which you can open **Client Health**.



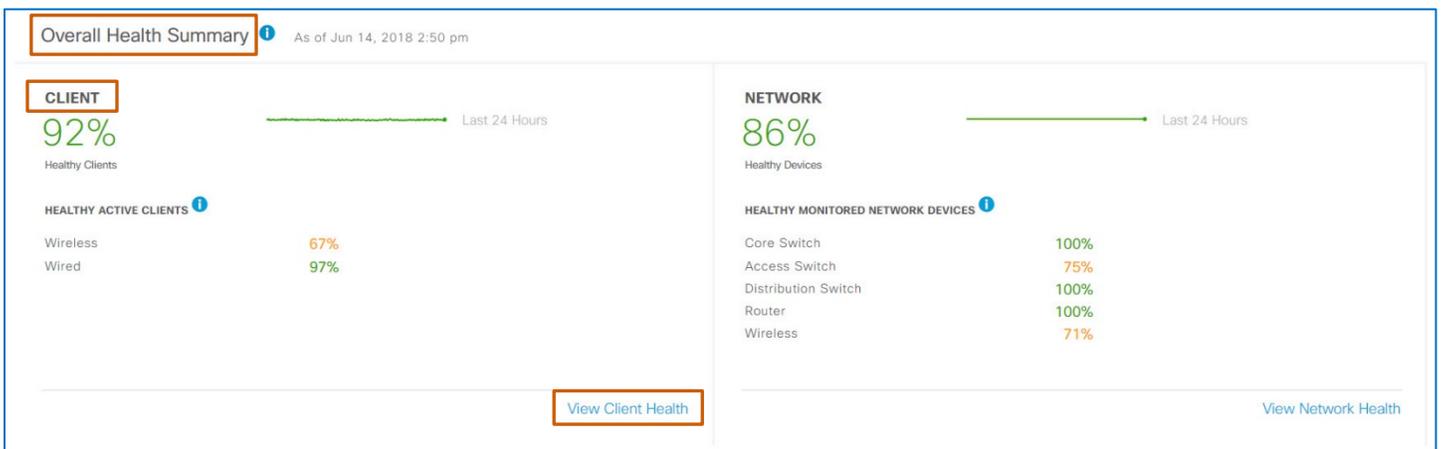
On the menu bar:

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



On the Overall Health Summary dashlet:

- Below **Client**, click **View Client Health**.

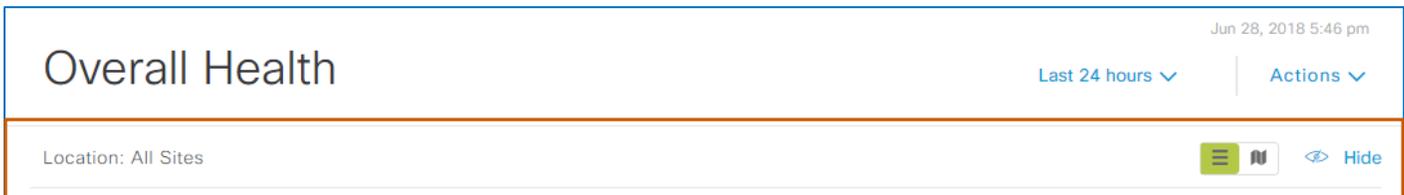


When you use the menu or dashlet methods of navigation, the system opens the **Client Health** page and, by default, presents the health states and metrics for the previous 24-hour period for clients:

- In all of the locations [in the network hierarchy](#).
- That are using all of the radio band frequencies.
- That are on all of [the service set identifiers \(SSIDs\)](#).

You also can open **Client Health** so that it presents the data for a specific location in the network hierarchy automatically.

These methods are available on the geographical map and in the list view in the collapsed dashlet on the **Overall Health** page.



To open Client Health by using the dashlet toolbar:

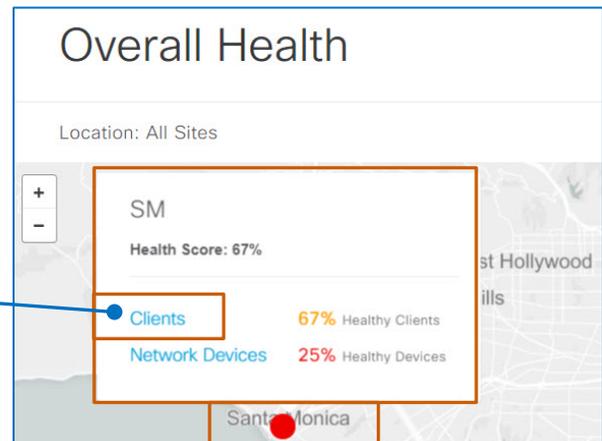
- On the collapsed dashlet, click the list view or geographical map button.



To open Client Health by using a geographical map location:

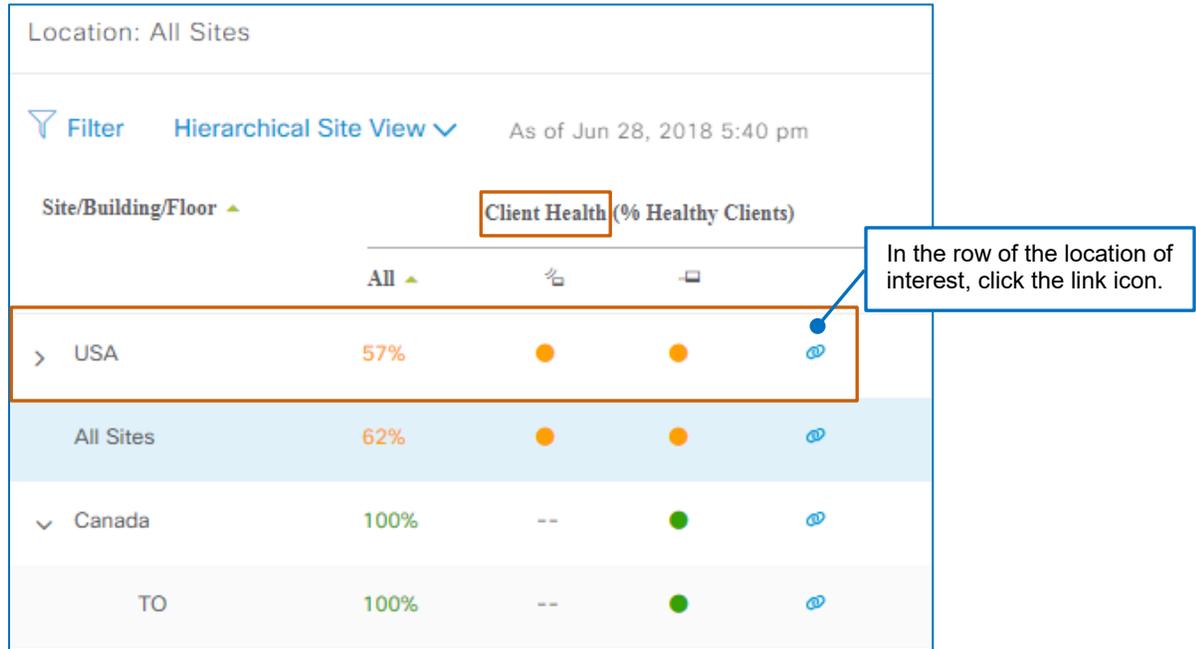
1. Zoom the map view to a single location level.
2. Point to the location health indicator.
A pop-up window opens.
3. In the pop-up window, click **Clients**.

To open **Client Health**, in the pop-up window, click **Clients**.



To open Client Health by using the list view:

- Under **Client Health**, locate the row of the location of interest, and then click the link icon.



Location: All Sites

Filter Hierarchical Site View As of Jun 28, 2018 5:40 pm

Site/Building/Floor	Client Health (% Healthy Clients)			
> USA	57%	●	●	🔗
All Sites	62%	●	●	🔗
∨ Canada	100%	--	●	🔗
TO	100%	--	●	🔗

In the row of the location of interest, click the link icon.

What Skills Do I Need?

To recognize, evaluate, and manage **Assurance Client Health**, 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
- Wired and wireless networking concepts

What Terms Should I Know?

Fabric Domain

A virtual network in a fabric topology, running over the physical infrastructure

Network Hierarchy

As an initial system configuration task, system users organize the network hierarchy, which arranges enterprise locations based on their geographical or organizational relationships. These relationships can include many sites, buildings at each site, and floors in each building in parent/child arrangements.

In the configuration and provisioning processes, system users assign devices to locations in the hierarchy.

Then **Assurance** organizes information based on the network hierarchy in various areas of **Client Health** to support the ability to identify locations or problem areas more easily.

WLANs or SSIDs

During network design, system users configure enterprise WLANs [based on the network hierarchy](#).

Cisco DNA Center refers to WLANs as service set identifiers (SSIDs).

Evaluating the Big Picture...

...on the Client Health Page.

What Will I See?

The screenshot displays the 'Client Health' dashboard with the following sections:

- Client Health Summary:** Shows overall health (62%), total clients (39), and breakdowns for Wireless (57%) and Wired (63%) clients. Includes donut charts for clients with poor health and device types.
- Client Onboarding Times:** Bar chart showing onboarding times for wired and wireless clients.
- Connectivity RSSI:** Bar chart showing RSSI distribution and percentage over threshold.
- Connectivity SNR:** Bar chart showing SNR distribution and percentage over threshold.
- Client Count per SSID:** Donut chart showing device counts per SSID.
- Client Count per Band:** Donut chart showing device counts per frequency band.
- Connectivity Physical Link:** Donut chart showing link status (Up, Down, Errors).
- Client Devices (39):** Table listing active clients with filters for type, health, and data.

Filters and a timeline to control the information that **Client Health** displays

A collapsed dashlet containing [the geographical map and list view](#)

A [summary of client health states](#) for all clients and by client type

[Health states and metrics for various measurements](#) with links to details and possible issues

A list of clients active [during the time period](#) with links to [Client 360 pages](#)

And What Will I See...

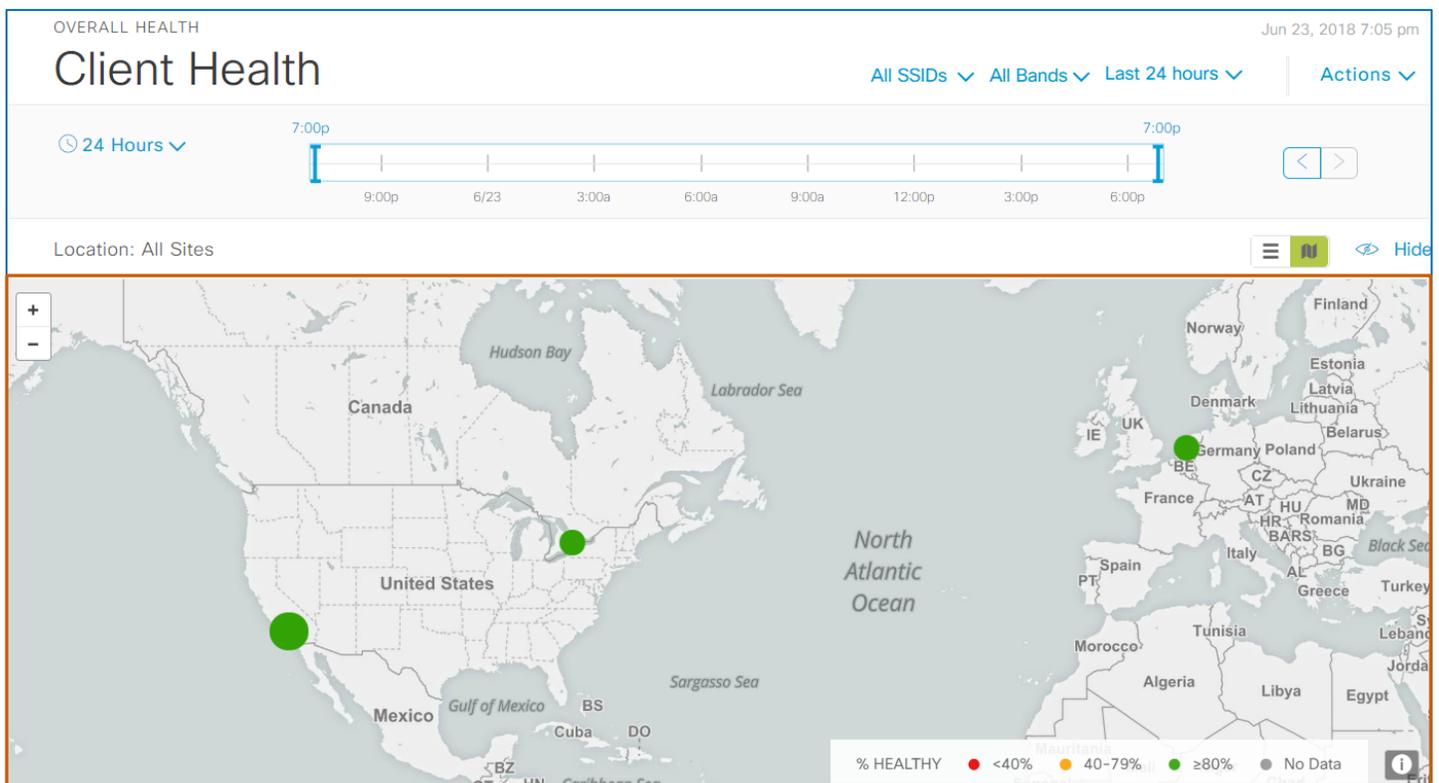
On the Geographical Map?

The geographical map displays a visual representation of the client health states of the enterprise network, indicating each enterprise location [based on the network hierarchy](#), the zoom level of the map [and the other settings that can affect what you see](#).

The location indicators apply color-coding that indicates the most critical client health state occurring at each location.



Important Note: The location level health indicators are non-interactive.



The geographical map is available on the collapsed dashlet below the timeline.

To open the geographical map:

- On the collapsed dashlet, click the geographical map button.



In the List View?

The list view applies a table layout to present client health states for the enterprise network, and selects the **Hierarchical Site View** by default, which organizes the list by the enterprise locations [in the network hierarchy](#).

For each location, it organizes the health score indicators by client type and includes data [based on the other settings that can affect what you see](#).

When you navigate to the **Client Health** page [by using the menu or dashlet method](#), it indicates the health states combined for all sites.

Location: All Sites

Filter Hierarchical Site View As of Jun 29, 2018 8:55 am Export Find

Site/Building/Floor	Client Health (% Healthy Clients)			Client Count	Apply to Page Location
	All	Wireless	Wired		
> USA	53%	38%	57%	36	Apply
All Sites	56%	38%	61%	39	Applied
> Canada	100%	--	100%	3	Apply

Data for all sites organized based on the network hierarchy

When you navigate to the **Client Health** page [by using the geographical map or list method](#), the list selects and applies that location's data.

Location: USA/SM

Filter Hierarchical Site View As of Jun 29, 2018 9:10 am Export Find

Site/Building/Floor	Client Health (% Healthy Clients)			Client Count	Apply to Page Location
	All	Wireless	Wired		
> USA	--	75%	--	36	Apply
DC	--	--	--	23	Apply
LA	--	--	--	3	Apply
SM	50%	38%	100%	10	Applied

Data for a single site organized based on the network hierarchy

The list view is available on the collapsed dashlet below the timeline.

To open the list view:

- On the collapsed dashlet, click the list view button.



The list view indicates the total numbers of clients that are in a healthy state at each location in the **All** column. Parent locations' percentages indicate the average of the health states for all of their child locations.

It also breaks out the percentage of wired and wireless clients in healthy states at each location.

Site/Building	Client Health (% Healthy Clients)			Client Count
	All	Wireless	Wired	
USA	54%	43%	57%	35
DC	57%	--	57%	23
LA	67%	--	67%	3
SM	44%	43%	50%	9
All Sites	60%	50%	63%	40

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

It also includes an entry for all of the buildings in the network hierarchy.

Site		Client Health (% Healthy Clients)		
		All	Wireless	Wired
USA	DC	57%	--	57%
--	All Buildings	64%	67%	63%
USA	LA	67%	--	67%
USA	SM	67%	60%	100%
Canada	TO	100%	--	100%

To review location level data for a parent location:

- Under **Apply to Page Location**, in the row of the parent location, click **Apply**.

Location: All Sites

Filter Hierarchical Site View As of Jun 14, 2018 4:50 pm Export Find

Site/Building/Floor	Client Health (% Healthy Clients)			Client Count	Apply to Page Location
	All	Wireless	Wired		
> USA	85%	43%	96%	34	Apply
All Sites	87%	50%	97%	39	Applied
> Canada	100%	--	100%	4	Apply
> Netherlands	100%	100%	--	1	Apply

To review location level data for a child location:

- Expand the parent location, and then, in the applicable row, click **Apply**.

The **Apply** link toggles to **Applied** and disables the link.

Location: USA/SM

Filter Hierarchical Site View As of Jun 29, 2018 9:10 am Export Find

Site/Building/Floor	Client Health (% Healthy Clients)			Client Count	Apply to Page Location
	All	Wireless	Wired		
USA	--	75%	--	36	Apply
SM	50%	38%	100%	10	Applied

The page updates all of the dashlets and the **Client Devices** list to display the associated data only.



Important Note: When you change the location in the list view, the system applies the change to all of the dashlets.

The **Client Health** page retains the change when you navigate away from it.

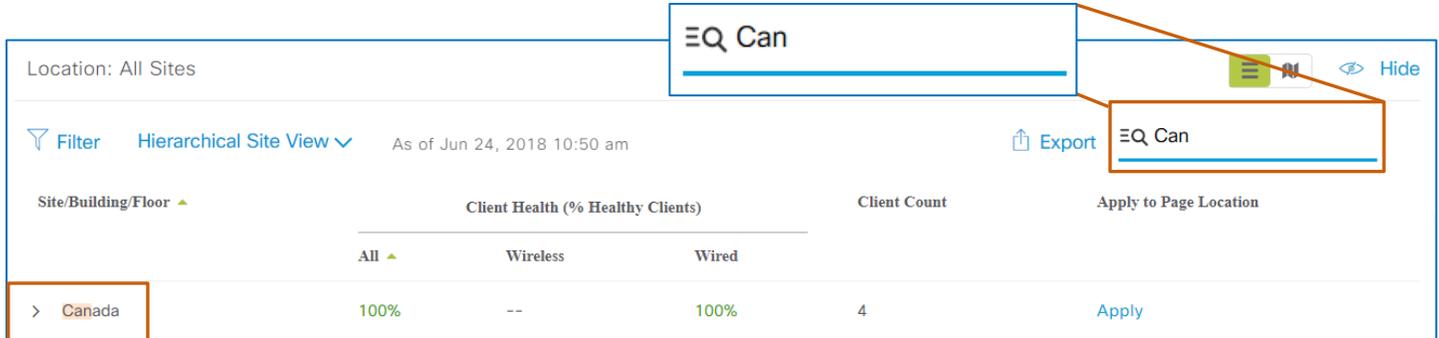
When you have a long list of locations, or are looking for specific data, you can use the search function to filter the list.

Location: All Sites

Filter Hierarchical Site View As of Jun 24, 2018 10:50 am Export Find

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.



Where Do I Find Client Health Organized...

...By SSIDs (WLANs)?

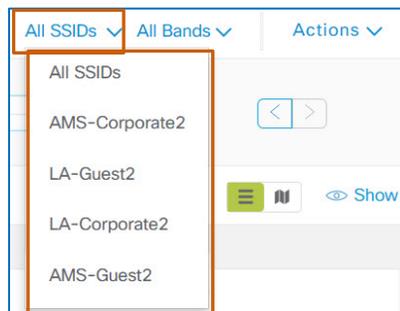
You can display client health states, metrics, and the device list for all of the enterprise SSIDs or a specific SSID.

The **Client Health** page displays information for all of the configured SSIDs by default.



To review the health, metrics, and devices associated with a specific SSID:

- In the SSID drop-down list, select the SSID name.



The page updates to display the specific metrics for the SSID that you selected.



Important Note: The SSID drop-down list is the only indicator on the page that you have applied this filter to the data on the page. [Refer to all of the settings](#) to identify the data that you are seeing.

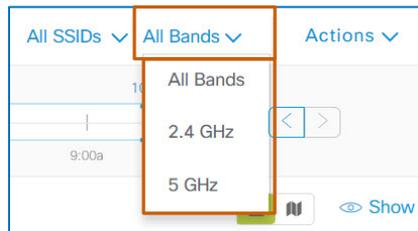
...By Radio Frequencies?

The **Client Health** page displays information for client endpoints on the 2.4 GHz and 5 GHz radio band frequencies combined, by default.



To review metrics and endpoints associated with a specific radio band frequency:

- In the radio bands drop-down list, select the frequency.

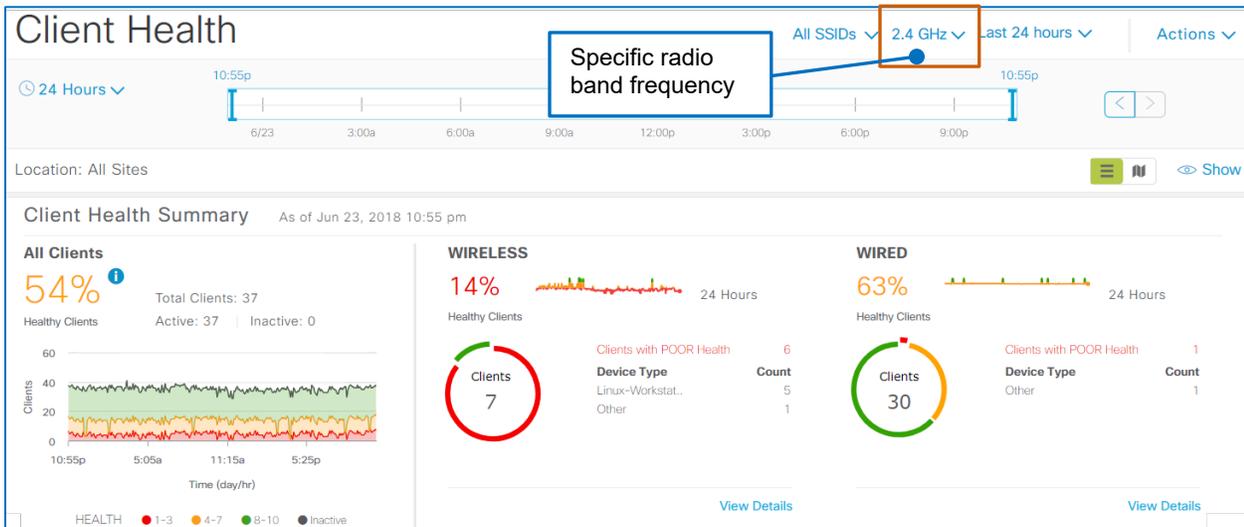


The page updates to display the specific metrics for the radio band frequency that you selected.



Important Note: The radio bands drop-down list is the only indicator on the page that you have applied this filter to the data on the page.

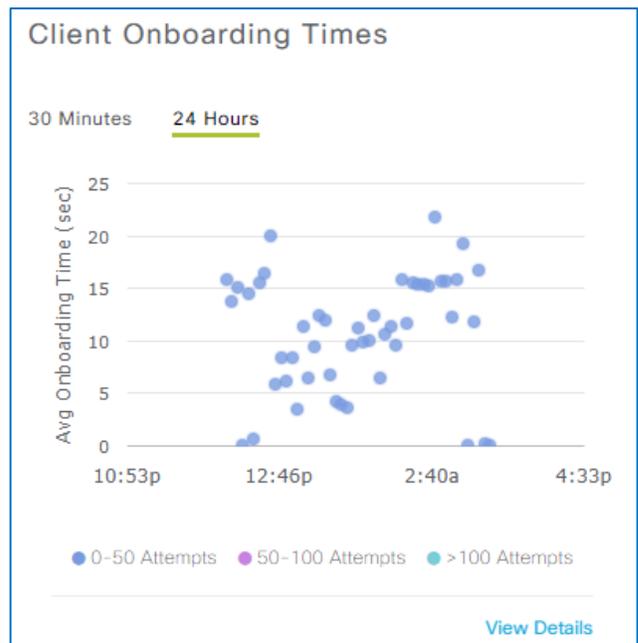
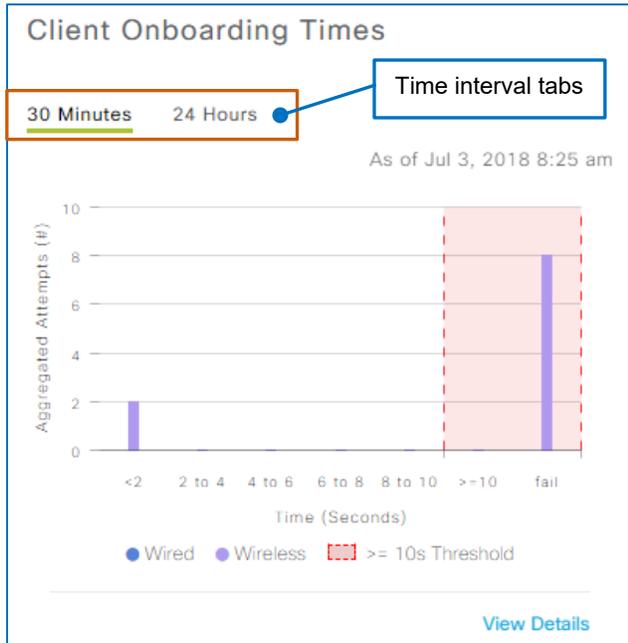
[Refer to the all of the settings](#) to identify the data that you are seeing.



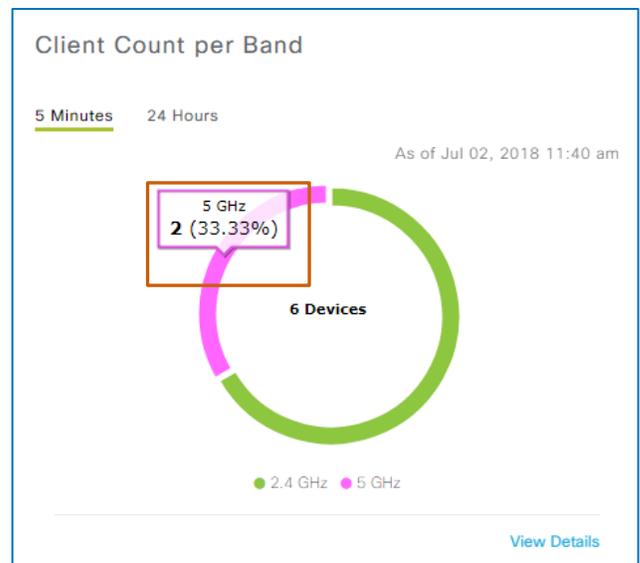
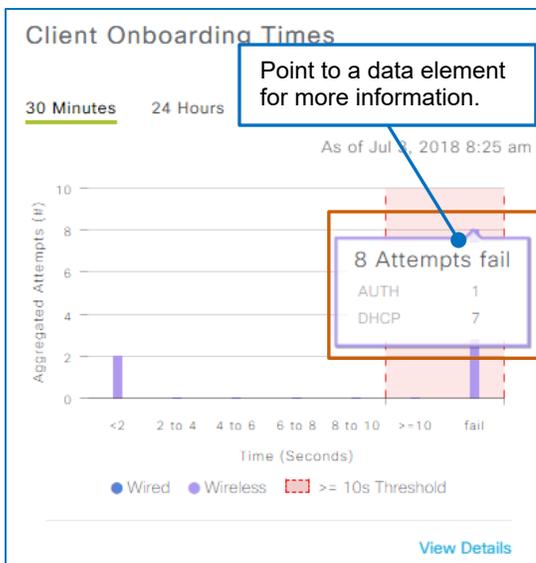
What Are the Common Page Features?

Dashlet Chart Elements on the Client Health Page

Chart elements include time interval tabs. Based on the time interval, the dashlet displays different chart types, such as bar or scatter charts.



For more information about a specific data element on the chart, you can point to it. This action opens a pop-up window with such details as affected numbers or percentages of clients, or of the metrics that the element represents.



Detailed Information Panels

Most **Client Health** dashlets provide access to detailed information on panels by using their **View Details** links.

Client Health Summary As of Jul 02, 2018 10:45 am

All Clients
 67%
 Total Clients: 39
 Healthy Clients: Active: 39 | Inactive: 0

WIRELESS
 43%
 Healthy Clients
 Clients with POOR Health: 4
 Device Type: Linux-Workstat... Count: 4

WIRED
 72%
 Healthy Clients
 Clients with POOR Health: 1
 Device Type: Other Count: 1

View Details links (Callout pointing to 'View Details' buttons)

Client Onboarding Times
 30 Minutes | 24 Hours
 As of Jul 2, 2018 10:45 am
 Aggregated Attempts (#) vs Time (Seconds)

Connectivity RSSI
 30 Minutes | 24 Hours
 As of Jul 2, 2018 10:45 am
 RSSI Distribution (%) vs RSSI (dBm)

Connectivity SNR
 30 Minutes | 24 Hours
 As of Jul 2, 2018 10:45 am
 SNR Distribution (%) vs SNR (dB)

View Details links (Callout pointing to 'View Details' buttons)

The information opens in a panel on the right of the application and overlays the page.

Client Health Summary
 68%
 Total Clients: 39
 Healthy Clients: Active: 39 | Inactive: 0

Client Health Summary
 68%
 Total Clients: 39
 Healthy Clients: Active: 39 | Inactive: 0

Client Onboarding
 30 Minutes | 24 Hours

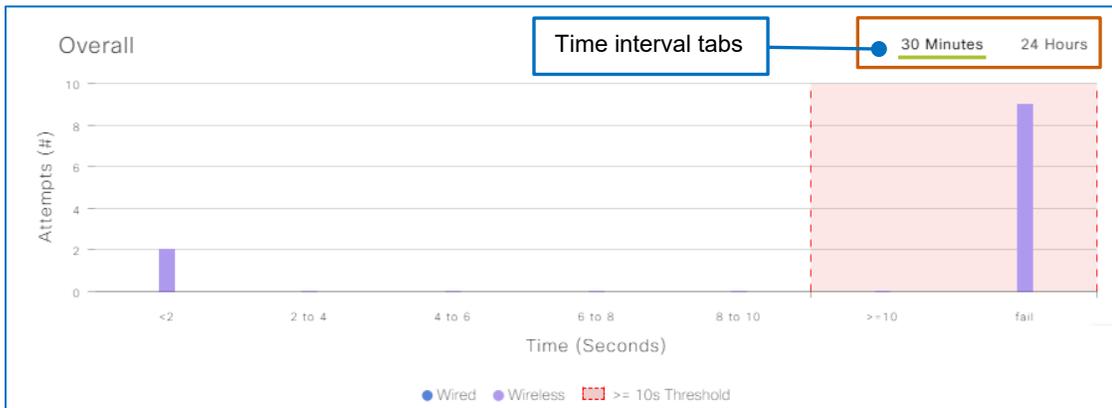
Clients (Open panel)
 Wireless
 Wired
 Clients with POOR Health (1)
 Device Type: Others Count: 1

HEALTH: All Inactive **Poor** Fair Good
 DATA: Onboarding Time >= 10s Association >= 5s DHCP >= 5s AAA >= 5s RSSI <= -72dBm

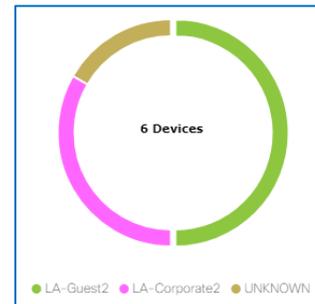
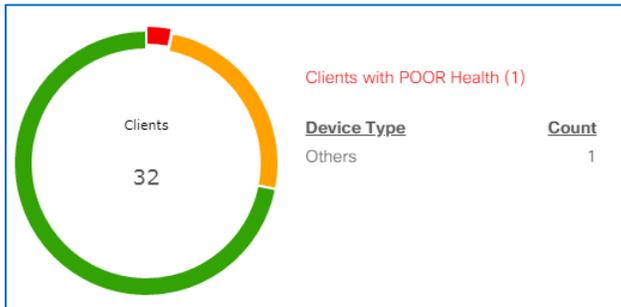
UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Onboarding Health	Connected Health	Connected Network Device	Location	VLAN ID
--	DESKTOP-9...	00:50:56-9A:3B:BE	169.254.74.121	--	UNKNOWN	1	●	●	LA1-9300-...	USA/LA/Le...	3999

Showing 1 of 1 Show More >

Panels include charts displaying related information. Some charts provide tabs that display the chart data information based on time intervals.

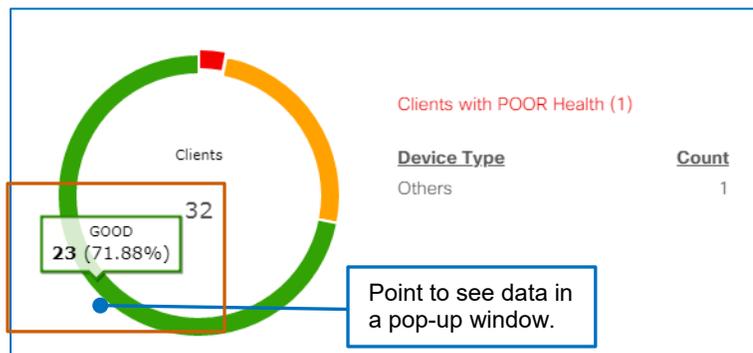


Some charts display color-coding to help distinguish what the segments represent, for example, health states or locations.



Some charts are interactive based on point or click actions.

For example, you can point to chart segments for information on numbers or percentages of endpoints associated with the segment. In the screenshot below, 23 client endpoints are in an acceptable health state out of a total number of 32 endpoints.



When you click a segment, the information beside the chart updates to display the data associated with the chart [and the endpoint list](#) updates to display the applicable endpoints.

In the screenshot below, when you click the red chart segment representing a poor health state, the endpoint list **Health** filter changes to indicate the health state and lists the applicable endpoints.

The screenshot displays the Cisco Assurance Client Health interface. On the left, there are tabs for 'Wireless' and 'Wired'. In the center, a donut chart shows the health status of 32 clients, with a small red segment representing 'Poor' health. To the right, a table titled 'Clients with POOR Health (1)' shows one device of type 'Others'. Below the chart, a filter bar allows selecting 'HEALTH' (All, Inactive, Poor, Fair, Good) and 'DATA' (Onboarding Time >= 10s, Association >= 5s, DHCP >= 5s, AAA >= 5s, RSSI <= -72dBm). A table below the filters lists endpoint details for the selected 'Poor' health state.

UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Onboarding Health	Connected Health	Connected Network Device	Location	VLAN ID
--	DESKTOP-9...	00:50:56:9A:3B:BE	169.254.74.121	--	UNKNOWN	1	●	●	LA1-9300-...	USA/LA/Le...	3999

Panels also can contain tabs below the panel name so that you can see details based on specific device types, metrics, or other information on charts [and in endpoint lists](#).

This close-up shows the 'Clients' panel with a tabbed interface. The 'Wireless' tab is selected, and the donut chart shows the health distribution for wireless clients. A callout box labeled 'Tab navigation' points to the tab controls.

Endpoint Lists

The **Client Health** page and all of [the detailed information panels](#) include a client endpoint list.

It lists the endpoints based on its **Health** and **Data** filter settings and [any other active settings that are affecting what you see](#) on the page and in the list.

HEALTH
All
Inactive
Poor
Fair
Good

DATA
Onboarding Time >= 10s
Association >= 5s
DHCP >= 5s
AAA >= 5s
RSSI <= -72dBm

Filter

UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Location	Onboarding Health
daphne....	Daphne-IP..	6C:19:C0:BD:87:C9	10.30.100.27	--	📶 Apple-iPad	10	USA/SM/Le...	●
shaggy....	Shaggy-PC	B8:27:EB:72:11:FF	10.0.100.16	--	📶 Linux-Wor...	10	USA/SM/Le...	●
daphne....	Daphne-IP..	A8:BE:27:36:70:11	10.30.100.29	--	📶 iPhone 7	9	USA/SM/Le...	●
velma.d...	Galaxy-Ta...	C0:D3:C0:4D:B3:17	10.11.100.50	--	📶 Samsung-D...	9	Netherlan...	●

To see the devices in a specific health state, in the device list:

- Beside **Health**, click the health state.

HEALTH
All
Inactive
Poor
Fair
Good

DATA
Onboarding Time >= 10s
Association >= 5s
DHCP >= 5s
AAA >= 5s
RSSI <= -72dBm

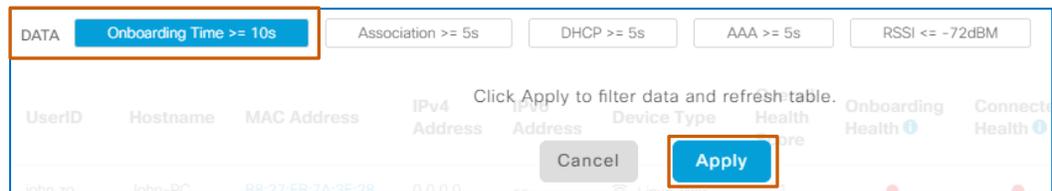
You can use **Data** filters to evaluate devices that are falling outside of metric thresholds, which can indicate potential issues.



To see the devices that are outside of a metric's thresholds:

- Beside **Data**, click the metric type, and then click **Apply**.

The metric indicator turns blue to indicate it is active, and the system filters the list to display those devices that meet the criteria.



Tip: You also can apply filters in combinations to find the information that you need.

To apply additional metrics:

- Click each metric type, and then click **Apply**.

Combining onboarding time and association metrics allows you to determine which clients are above the threshold for being both onboarded and associated to the network.

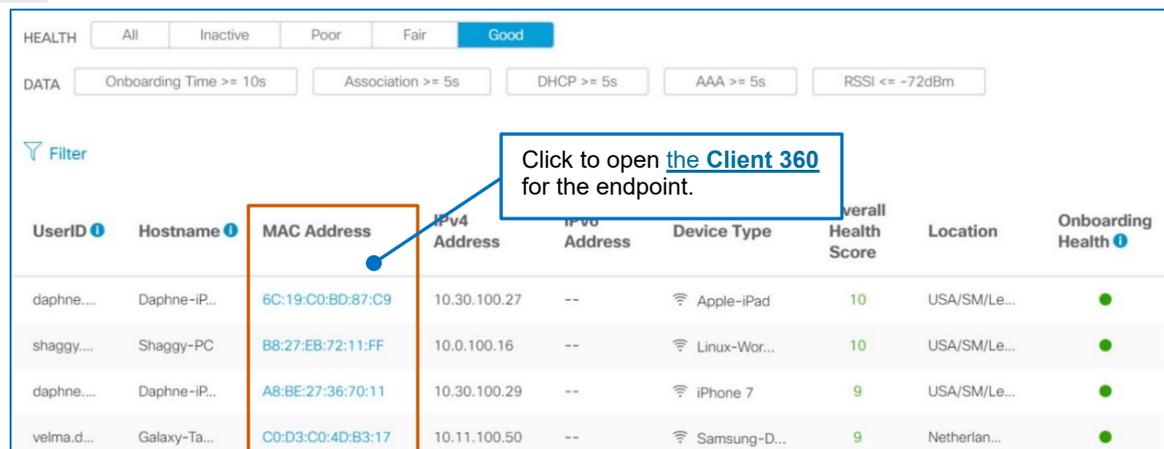
To clear a metric filter:

- Beside **Data**, click the active filter, and then click **Apply**.

To support detailed monitoring or troubleshooting, you can click a client endpoint's MAC address link to navigate to [its associated Client 360 view page](#). The page provides a holistic view of the client endpoint, issues it is experiencing, the performance of applications that it is using, and other details.



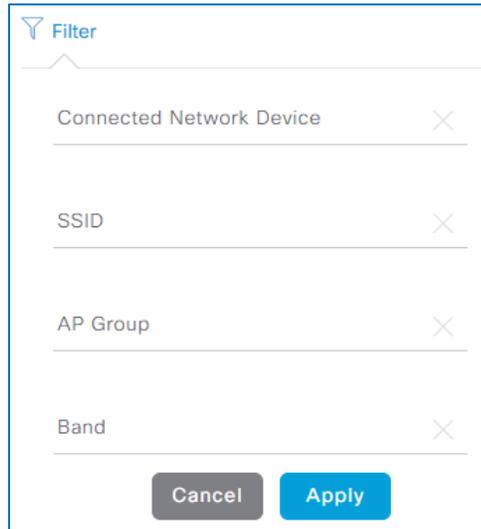
Note: For detailed information on the layout and contents of the **Client Devices** endpoint list on the **Client Health** page, [refer to The Client Devices List topic](#).



You can define a series of attributes for a more specific list.

To apply attribute filters:

- Click **Filter**, in each drop-down list, type or select each attribute parameter, and then click **Apply**.



When you apply attribute filters, they appear below the **Filter** link.



To clear a filter:

- Under **Filter**, click the **X** next to the filter that you want to remove. The list updates automatically.



How Can I Add or Position Dashlets?

Some dashlets in **Client Health** are not visible in the default layout. You can add these dashlets to the page. You also can position dashlets on the page for optimal visibility.

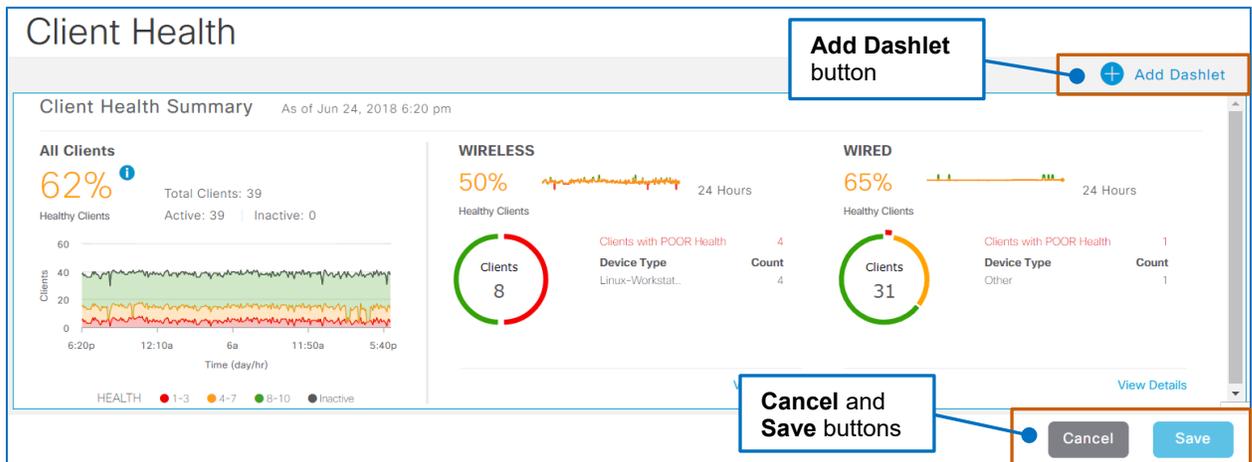
When you add or position dashlets, the system retains the changes when you navigate away from the page or log out of the system. Changes that you make do not affect other users' layouts.

To add or position dashlets:

- On the **Client Health** page, in the **Actions** drop-down list, select **Edit Dashboard**.

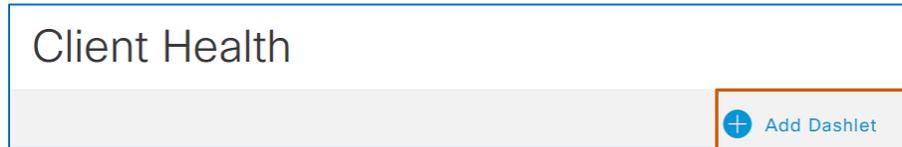


The system makes the page available for editing and opens the **Add Dashlet**, **Cancel**, and **Save** buttons.



To view the available dashlets:

- Click **Add Dashlet**.

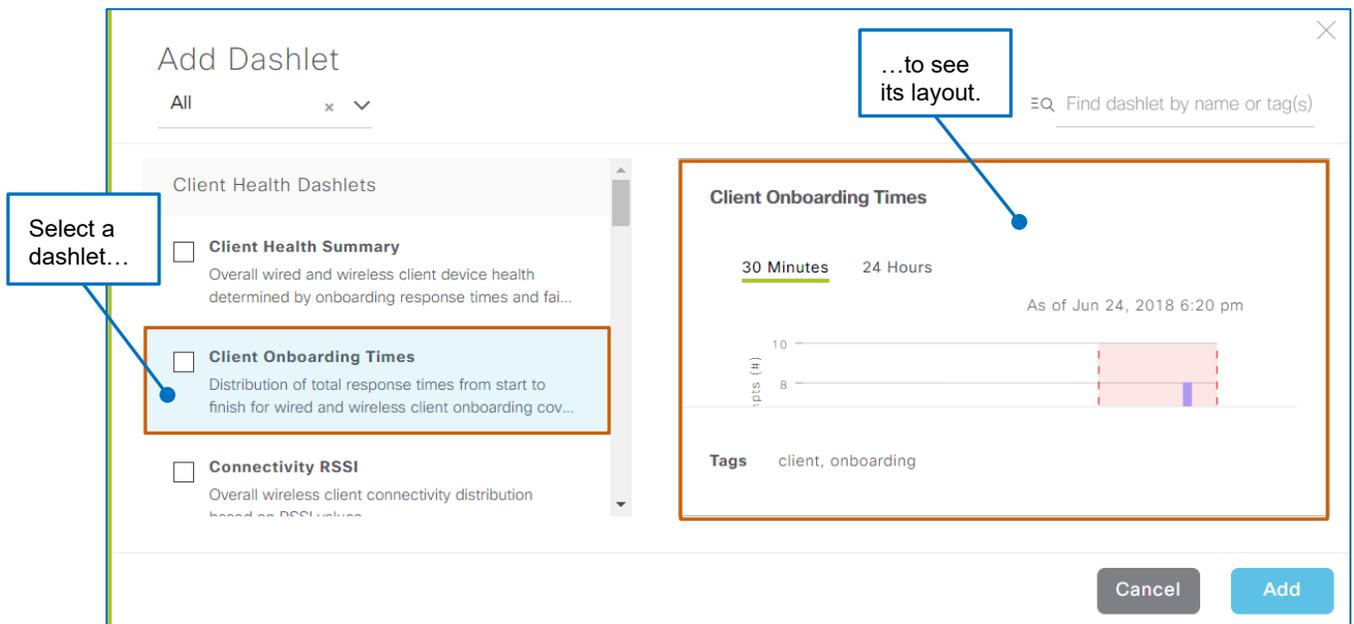


The **Add Dashlet** panel opens and lists all of the dashlets, including those that are visible on the page.



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

- In the list, select the dashlet row.



Search Tips:

To filter the list of dashlets by a category:

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

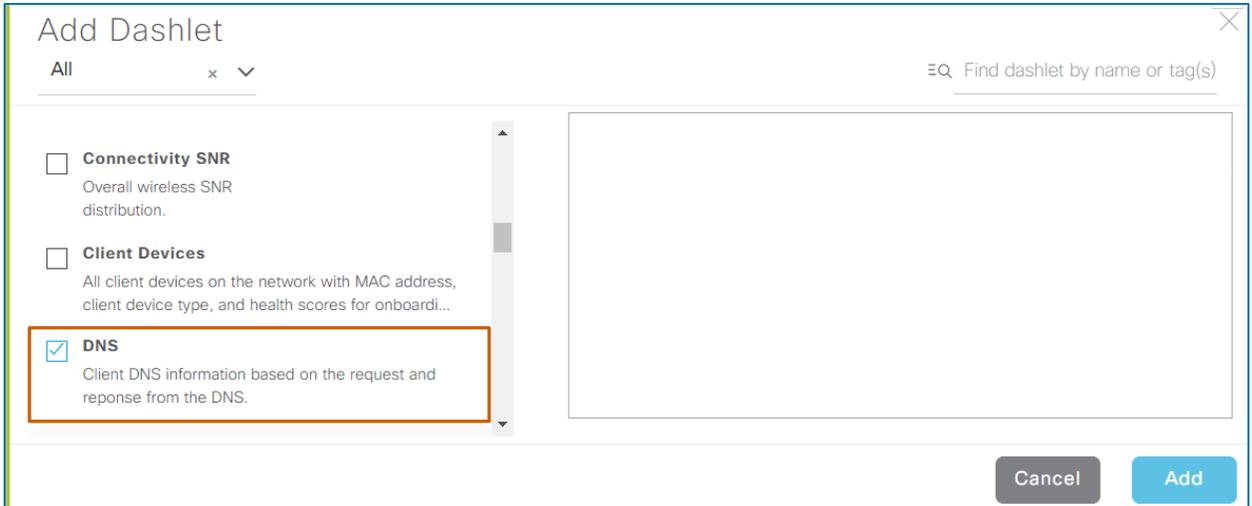
To find a dashlet by using a character string:

- 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.



To add a dashlet or dashlets to the page:

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



Add Dashlet

All x v

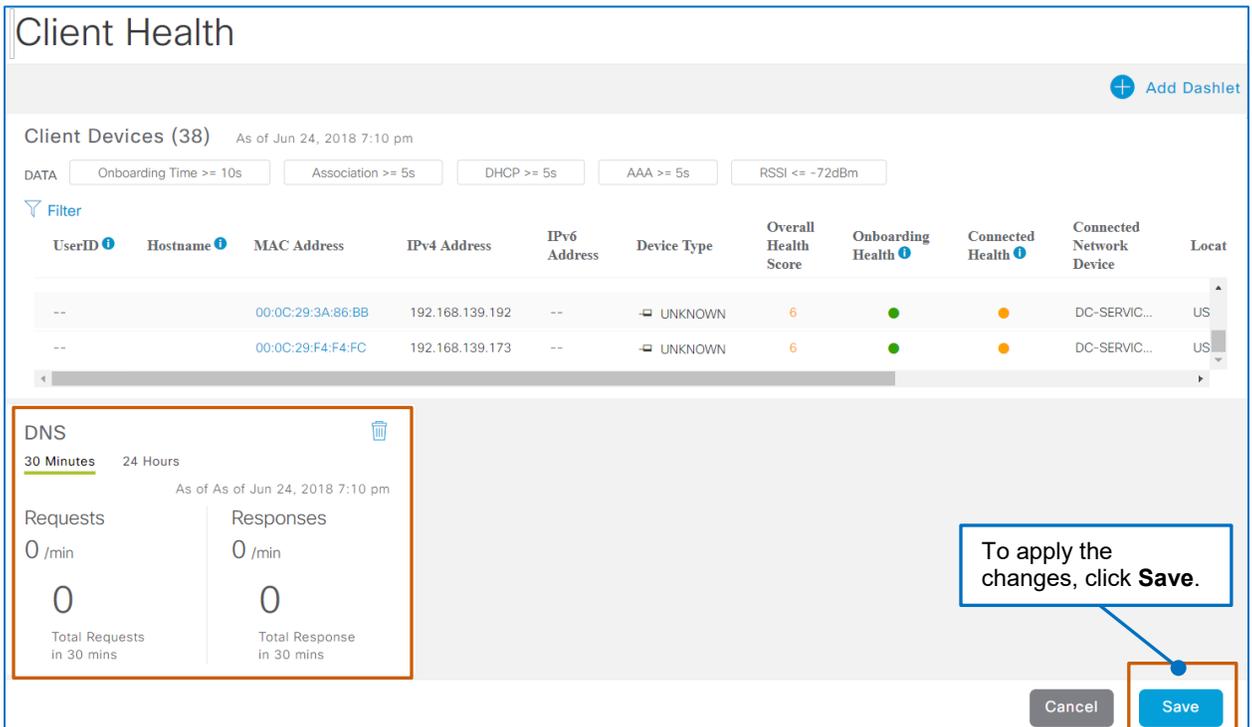
EQ Find dashlet by name or tag(s)

- Connectivity SNR**
Overall wireless SNR distribution.
- Client Devices**
All client devices on the network with MAC address, client device type, and health scores for onboardi...
- DNS**
Client DNS information based on the request and reponse from the DNS.

Cancel Add

The system adds each dashlet to the page.

2. To apply the changes to the page, click **Save**.



Client Health + Add Dashlet

Client Devices (38) As of Jun 24, 2018 7:10 pm

DATA Onboarding Time >= 10s Association >= 5s DHCP >= 5s AAA >= 5s RSSI <= -72dBm

Filter

UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Onboarding Health	Connected Health	Connected Network Device	Locat
--		00:0C:29:3A:86:BB	192.168.139.192	--	UNKNOWN	6	●	●	DC-SERVIC...	US
--		00:0C:29:F4:F4:FC	192.168.139.173	--	UNKNOWN	6	●	●	DC-SERVIC...	US

DNS 30 Minutes 24 Hours As of Jun 24, 2018 7:10 pm

Requests 0 /min Total Requests in 30 mins

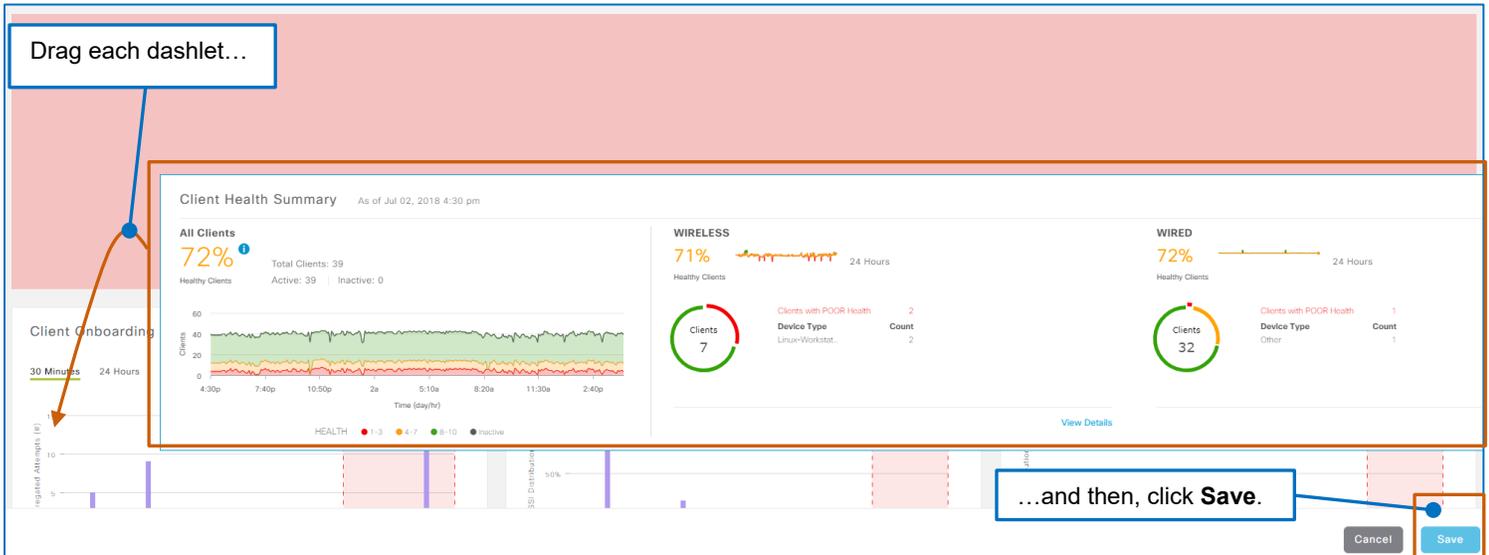
Responses 0 /min Total Response in 30 mins

Cancel Save

To apply the changes, click **Save**.

To position dashlets on the page:

- Drag each dashlet to the position that you want, and then click **Save**.



The screenshot shows a dashboard titled "Client Health Summary" as of Jul 02, 2018 4:30 pm. It features several dashlets: "All Clients" (72% healthy, 39 total), "WIRELESS" (71% healthy), and "WIRED" (72% healthy). A "Client Onboarding" section shows a 30-minute and 24-hour progress bar. A "HEALTH" chart shows client status over time. A "Device Type" table lists counts for Linux-Workstat, Linux-Workstat, and Other. A "View Details" link is present. Annotations include a box "Drag each dashlet..." with an arrow pointing to a blue dot on the dashboard, and another box "...and then, click Save." with an arrow pointing to the "Save" button in the bottom right corner.



Note: In addition to adding a dashlet to a page, you can configure a custom page, referred to as a dashboard, and then add and position dashlets on the page.

For information on configuring and managing custom pages, [refer to the Configuring a Custom Dashboard Page in the Assurance Features and Navigation training.](#)

What Affects the Information That I Am Seeing?

Time Periods and Time Stamps

Client Health displays provides a page level time stamp above the drop-down lists to indicate the last time that the page data was refreshed, which occurs when you first open the page or when you refresh the page manually.

This way, you can determine the age of the information and whether you need to update it manually.



Note: For detailed information on time stamps and data aging, [refer to the Time Stamp and Data Aging Concepts topic in the Assurance Features and Navigation training.](#)

When you open the **Client Health** page, the system displays the time period of the previous 24 hours up to the current system time of the device that you are using by default.

The ending time of the time period applied to the page appears at the top of each dashlet and each dashlet includes metrics up to that ending time.

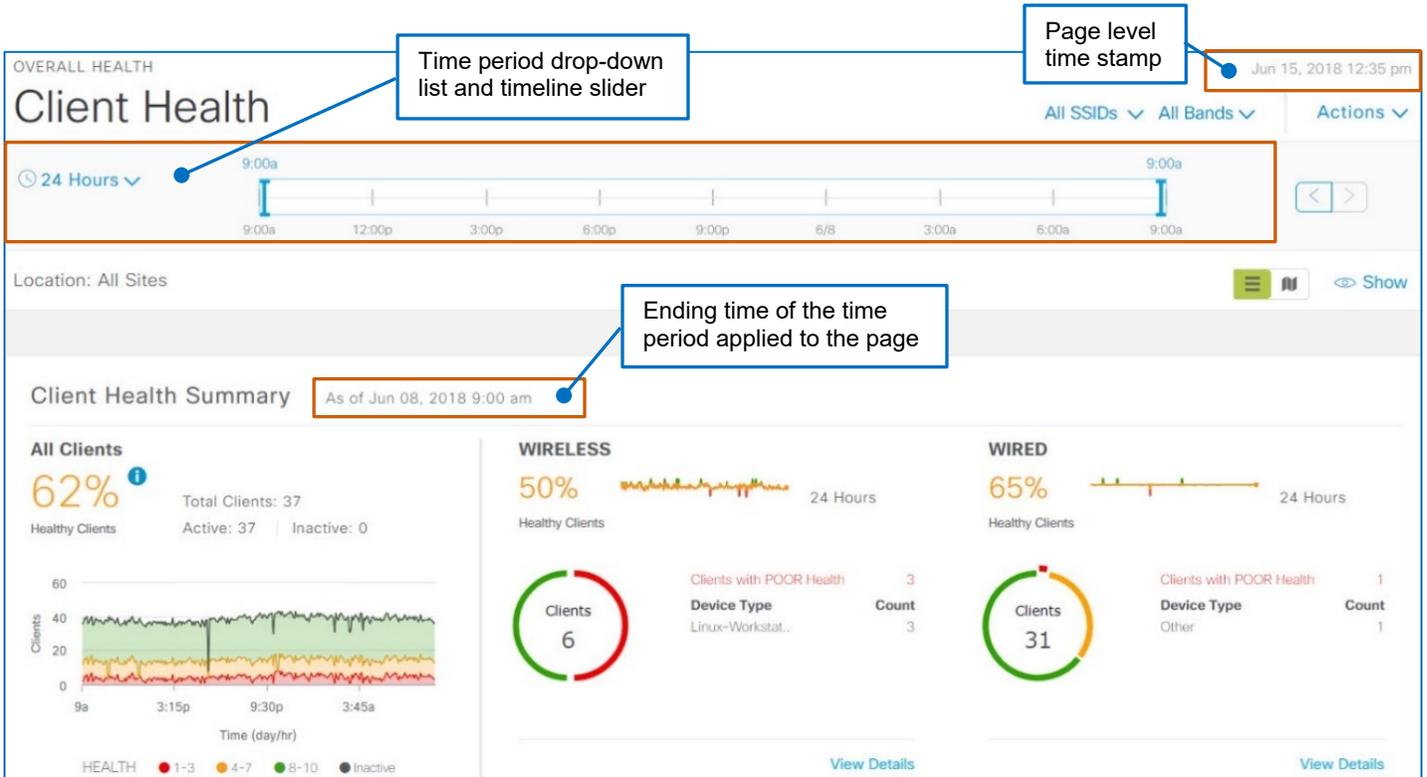


Important Note: The time period drop-down list and the timeline slider work together to affect the time period for which you are seeing data.

For example, you can select an earlier date or date range in the drop-down list, and then refine the time period further by using the slider.

Refer to the time stamps on the page, in dashlets, and in lists to ensure that you are seeing the data that you expect.

For additional information on time period settings, [review the Changing the Time Period topic.](#)



Changing the Time Period

The time interval drop-down list provides time period selections of 3 hours, 24 hours, or 7 days based on your local client time, which constrains the start and end dates and times that you can select.

For example, if the date is 15 June and you select 7 days, the **Start Date** fields change to indicate the date of 8 June and local client time; the **End Date** fields indicate the current date and local client time.



Important Note: If you open the time interval drop-down list and select a start date that is different from today's date and then make other time period changes, those changes remain when you open the drop-down list subsequently and change the time interval or date selections.

For example, today's date is 15 June and you change the start date to 12 June and apply it. The page updates to display the related data.

Then, when you return to the calendar and change the date or time interval, the page refers to the 12 June date as its basis, not the current date.

To reset the automated calendar updates when you change a time interval:

- Refresh the page.

To select a specific time period by using the time interval drop-down list:

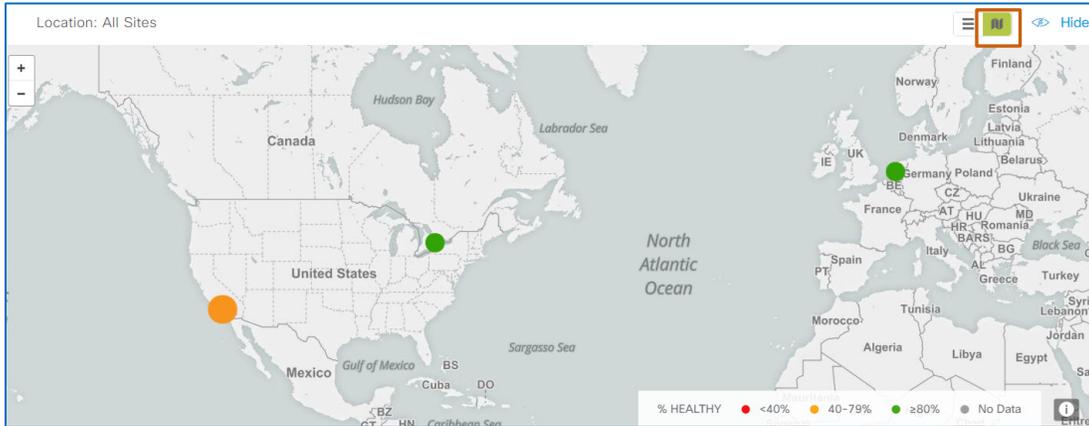
1. To indicate the time interval by which you want to constrain the data, under **Time Range**, click the applicable option button.
2. To indicate a custom time period based on the time constraint, in the **Start Date** and **End Date** fields, select the date and time periods.
3. Click **Apply**.

You also can customize the time interval by using the timeline sliders.

To customize the view by selecting a specific time period on the timeline:

- Drag each timeline slider to the interval that you want to view, and then, click **Apply**.

When you change the time interval, the geographical map displays the health states for the time period...



...as does the list view.

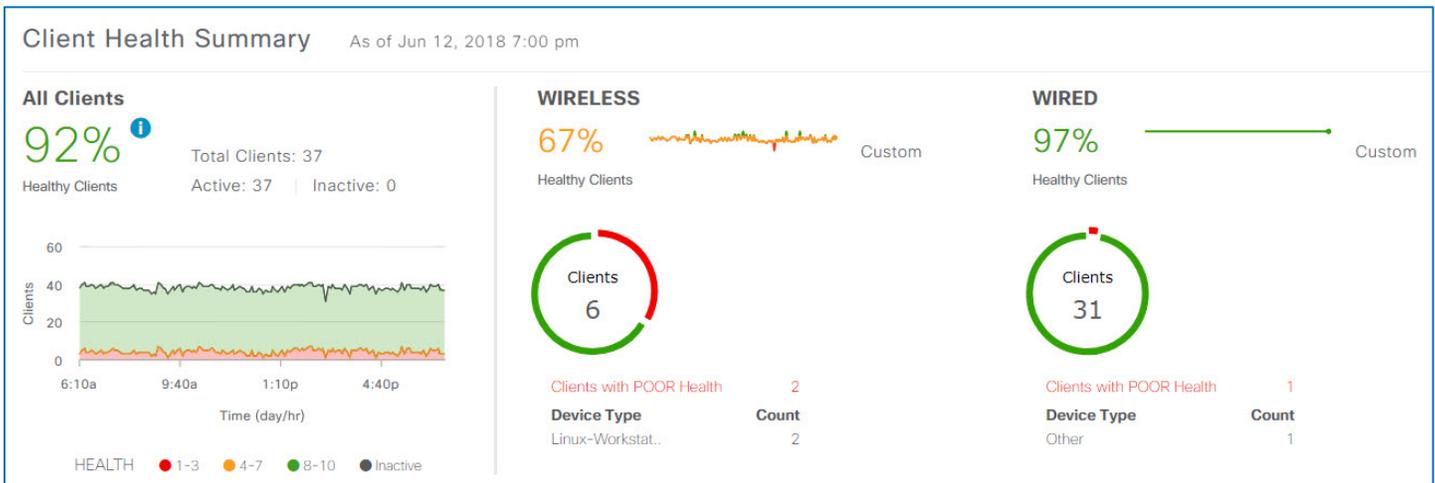
Location: All Sites

Filter Hierarchical Site View As of Jun 12, 2018 7:00 pm Export Find

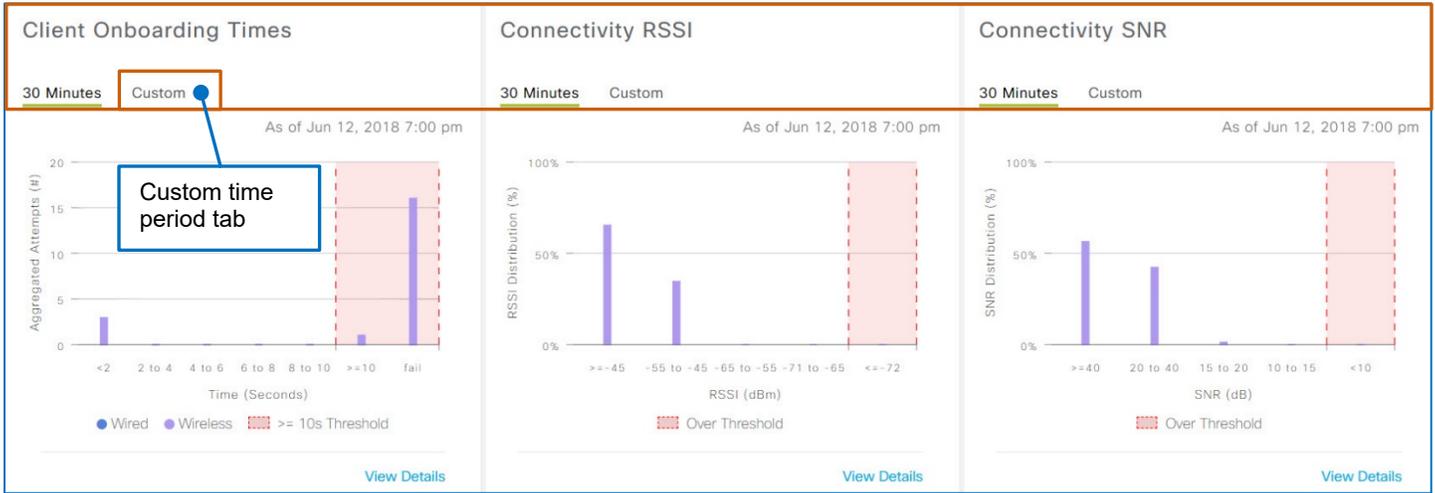
Site/Building/Floor	Client Health (% Healthy Clients)			Client Count	Apply to Page Location
	All	Wireless	Wired		
> USA	91%	60%	96%	32	Apply
All Sites	92%	67%	97%	37	Applied
> Canada	100%	--	100%	4	Apply
> Netherlands	100%	100%	--	1	Apply

The dashlets and device list also display data based on the time period that you apply.

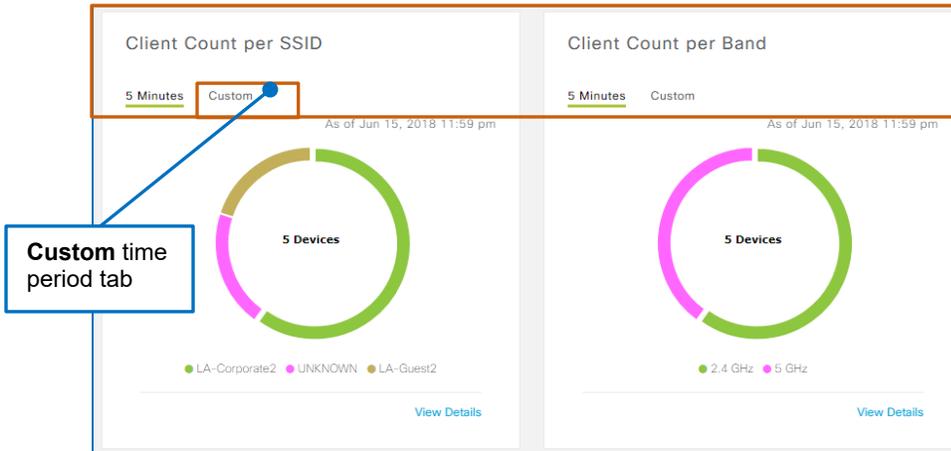
The **Client Health Summary** dashlet displays metrics for the time period...



...most of the metrics dashlets include the **30 Minutes** tabs and update the date range tabs to **Custom** tabs, which display the metrics for the time period that you applied...



...and the client count dashlets and the **Client Devices** list display the **5 Minutes** tabs and update the date range tabs to **Custom** tabs, which display the metrics for the time period that you applied...



Client Devices (2) As of Jul 8, 2018 10:40 pm
 5 Minutes Custom

TYPE: All Wireless Wired HEALTH: All Inactive Poor Fair Good
 DATA: Association >= 5s DHCP >= 5s AAA >= 5s RSSI <= -72dBm

Filter

UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Onboarding Health
daphne...	Daphne-iP...	6C:19:C0:BD:87:C9	10.30.100.27	--	📶 Apple-iPad	10	●
velma.d...	Galaxy-Ta...	C0:D3:C0:4D:B3:17	10.11.100.50	--	📶 Samsung-D...	9	●

Persistent Filters on Page Navigation

When you apply specific settings to **Client Health**, those settings persist when you navigate away from the page. Persistent settings include changes to:

- The network location.
- The SSID.
- The radio frequency.
- [The time period applied on the timeline.](#)

OVERALL HEALTH Aug 29, 2018 12:57 pm

Client Health

All SSIDs ▾ All Bands ▾ Actions ▾

24 Hours ▾

Timeline: 12:50p to 12:50p (8/29)

Location: All Sites Show

When you return to the **Client Health** page, any changes that you made previously still apply.

To determine the location for the data that you are seeing, you can refer to the **Location** field, which is always visible, or the list view.

Location: USA/SM Location field

Filter Hierarchical Site View ▾ As of Jun 29, 2018 9:10 am Export EQ Find

Site/Building/Floor ▾	Client Health (% Healthy Clients)			Client Count	Apply to Page Location
	All ▾	Wireless	Wired		
USA	--	75%	--	36	Apply
SM	50%	38%	100%	10	Applied

Location applied in list

When you change settings by using the drop-down lists, the drop-down list is the only indicator on the page that the information is filtered.

Tip: Refer to the combination of the **Location** field and drop-down list settings to determine the data that you are seeing.

OVERALL HEALTH Aug 29, 2018 12:57 pm

Client Health

All SSIDs ▾ All Bands ▾ Actions ▾

24 Hours ▾

Timeline: 12:50p to 12:50p (8/29)

Location: All Sites Show

How are Client Health Metrics Looking?

Get a Summary View of Client Health

What Will I See?

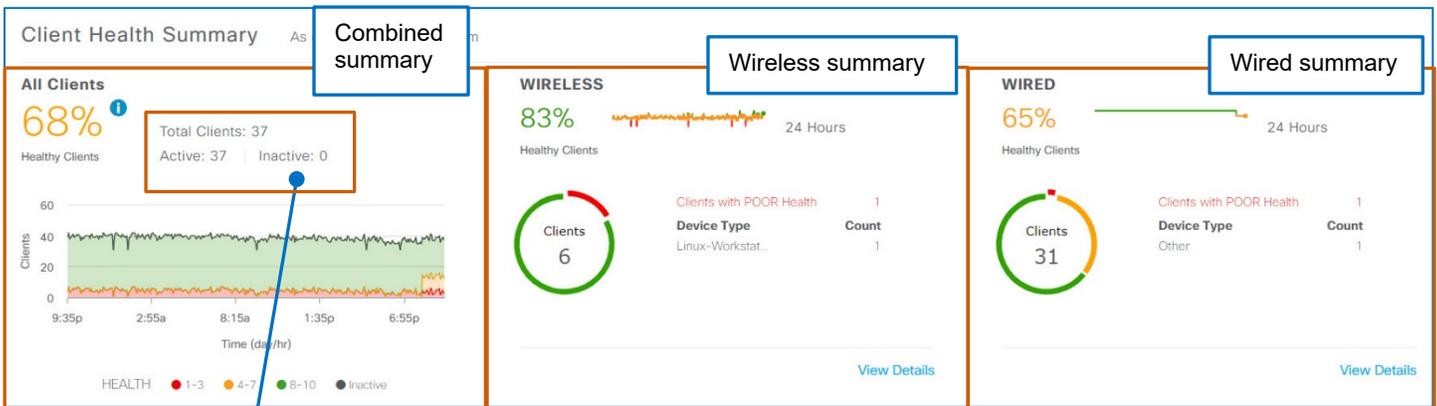
The **Client Health Summary** provides an overview of the numbers of clients in each health state.

Under **All Clients**, the system combines wired and wireless client health percentages into a single metric and provides a timeline of the combined metric [based on the settings that affect what you see](#).

Under **Wireless** and **Wired**, the system displays health metrics by client type, which helps you to determine which portions of the network might need more attention, and provides links to detailed information.



Note: The system does not display health metrics for inactive clients because they are not connected to the network.



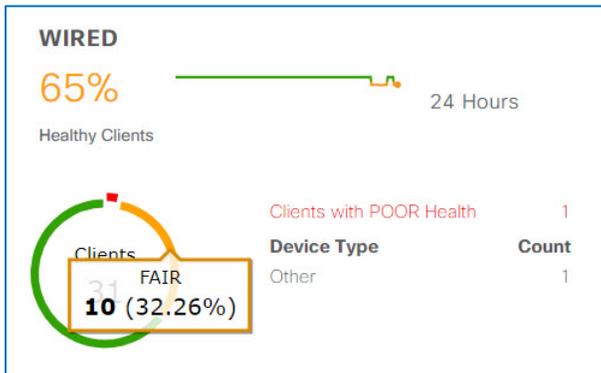
The system does not include inactive clients in the combined percentage.

Under **Wireless** and **Wired**, the dashlet indicates the percentage of client endpoints in a healthy state.

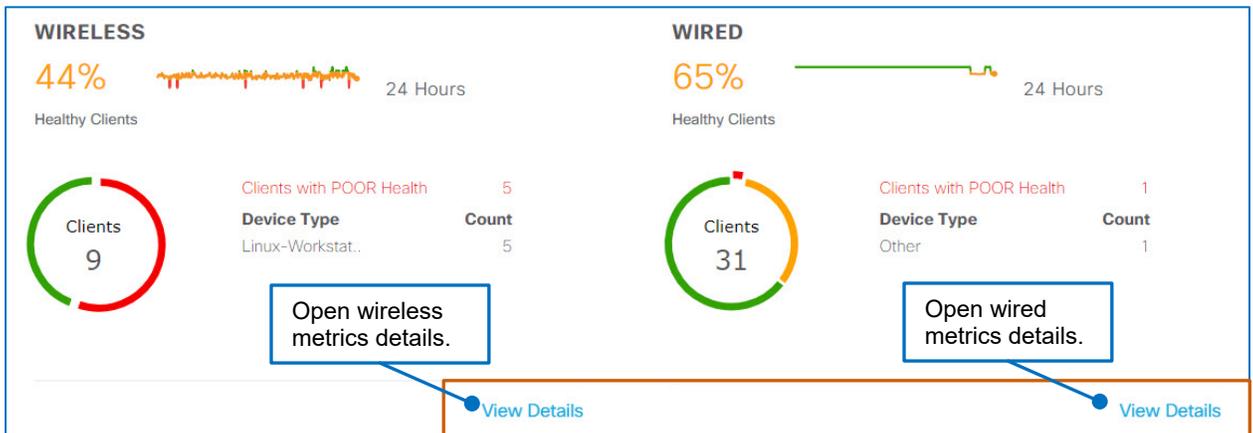
Each chart indicates the total number of active endpoints, which means that they are attached to and authenticated on the network, the segments represent the number of endpoints in all applicable health states, and a list indicates the endpoints in the most critical health state.



To see the number and percentage of clients that are experiencing the health state that the color-coding indicates, you can point to that segment of the chart.



Below **Wireless** and **Wired**, you can access and review detailed wired or wireless client metrics.



When you open details, the **Clients** panel opens, overlaying the page. In the panel, the associated tab is active based on the dashlet in which you clicked **View Details**.

The panel filters to indicate the number of clients in the most critical health state automatically.

DESIGN
POLICY
PROVISION
ASSURANCE
PLATFORM

🔍
🗪
⚙️
☰

Clients
✕

Wireless
Wireless Information

Wired
Wired Information

Clients
9

Clients with POOR Health (5)

Device Type	Count
Linux-Workstat..	5

HEALTH All Inactive Poor Fair Good

DATA Onboarding Time >= 10s Association >= 5s DHCP >= 5s AAA >= 5s RSSI <= -72dBm

🔼 Filter

UserID ⓘ	Hostname ⓘ	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Location	Onboarding Health ⓘ
bender....	Bender-PC	B8:27:EB:0C:4F:F8	0.0.0.0	--	📶 Linux-Wor...	1	USA/SM/Le...	●
amy.wong	Amy-PC	B8:27:EB:0C:53:E0	0.0.0.0	--	📶 Linux-Wor...	1	USA/SM/Le...	●
--	Daphne-PC	B8:27:EB:CA:AA:88	--	--	📶 Linux-Wor...	1	USA/SM/Le...	●
john.zo...	John-PC	B8:27:EB:0C:57:C8	0.0.0.0	--	📶 Linux-Wor...	1	USA/SM/Le...	●
philip....	Philip-PC	B8:27:EB:0C:48:28	0.0.0.0	--	📶 Linux-Wor...	1	USA/SM/Le...	●

Where Do I Find...

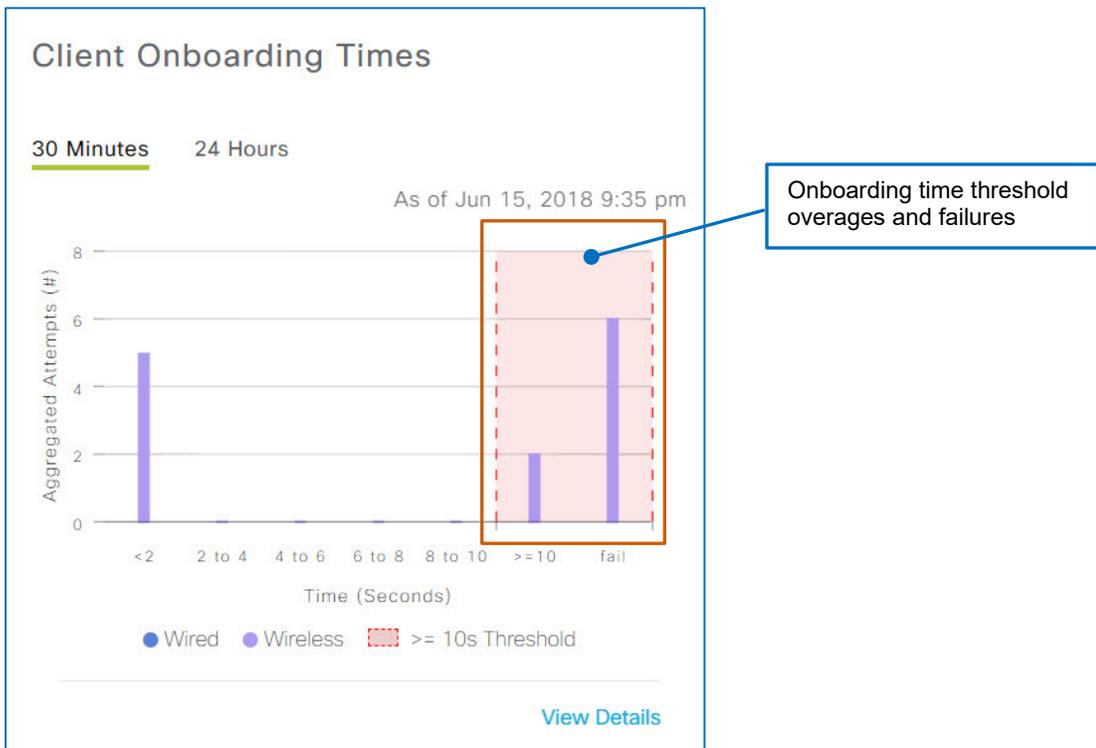
...Client Onboarding Attempts and Lengths of Time until Onboarded?

The Client Onboarding Times Dashlet

The **Client Onboarding Times** dashlet, which is visible by default, displays aggregated wired and wireless client endpoint onboarding attempts and the lengths of time until onboarding process is completed in ranges of seconds.

Onboarding time includes the time that it takes to complete each stage of the onboarding process, including the time that it takes for the endpoint to associate to and be authenticated by the network, and to obtain an IP address by using DHCP.

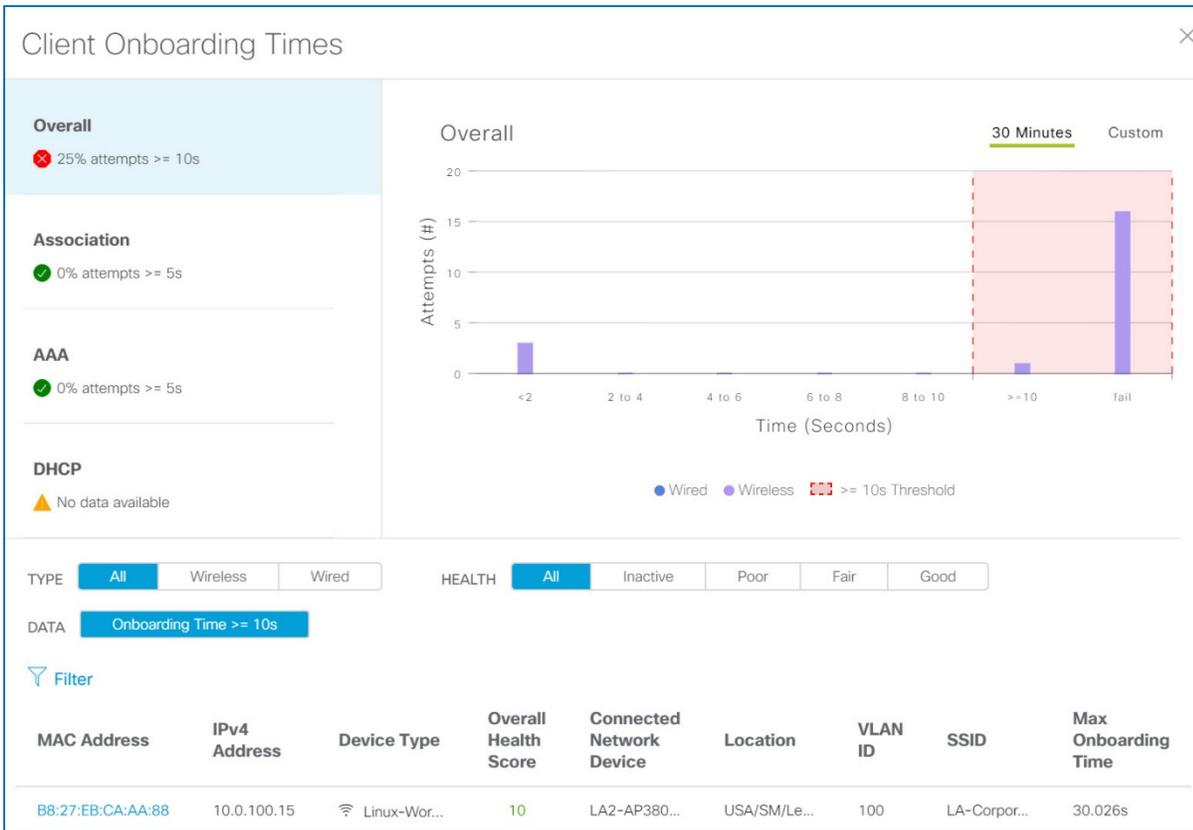
In the 30 minute chart view, the chart emphasizes onboarding times that exceed the system-defined threshold for an acceptable onboarding and failures to onboard in the red highlighted area.



The Client Onboarding Times Panel

In the panel, the **Overall** tab is active and displays times for the entire process, and the device list is filtered to display the endpoints that are experiencing onboarding times that are above the acceptable threshold.

The other tabs provide insight into the health of the client during each stage of onboarding, including association, authentication (AAA), and obtaining an IP address (DHCP).

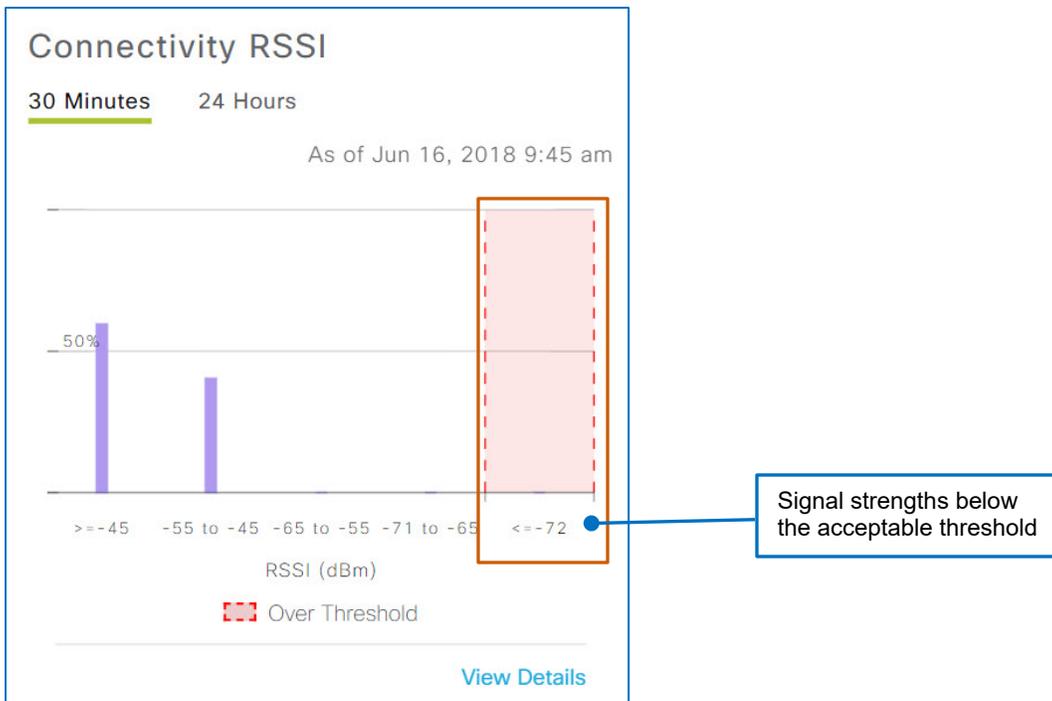


...The Signal Strengths That Endpoints are Receiving (RSSIs)?

The Connectivity RSSI Dashlet

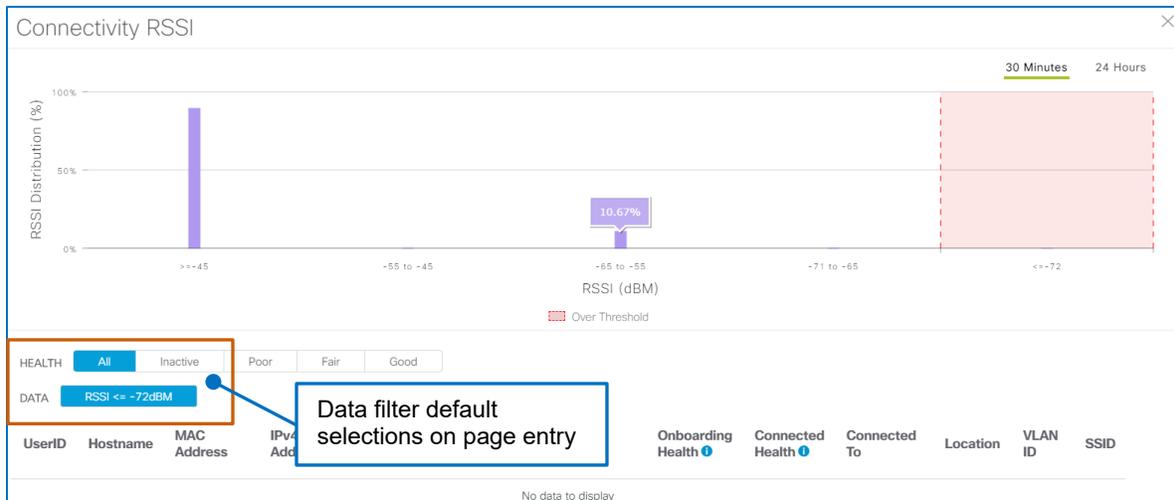
The **Connectivity Received Signal Strength Indicator (RSSI)** dashlet, which is visible by default, indicates the RSSI distribution for all client endpoints.

The dashlet displays the percentage of endpoints receiving signal strengths in each dBm range. In the screenshot below, there are no client endpoints experiencing signal strengths that are below the pre-defined system threshold.



The Connectivity RSSI Panel

When you open the panel, the device list displays any client endpoints with metrics that are below the acceptable RSSI threshold.

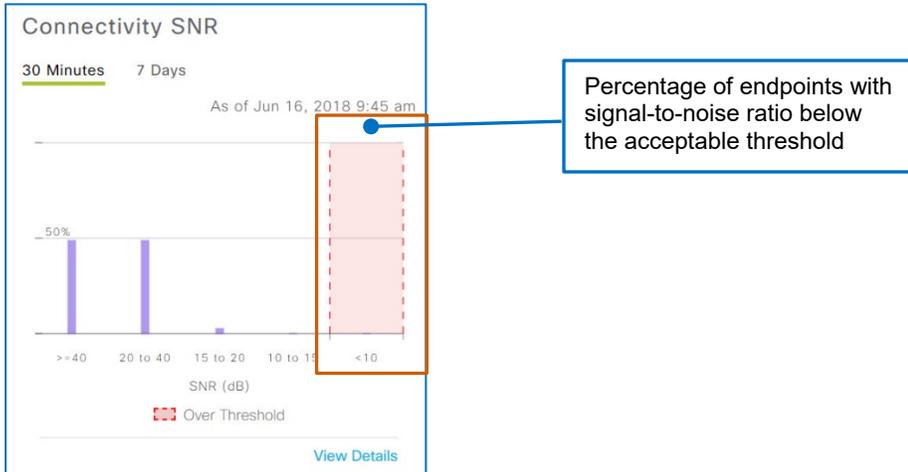


...Signal-to-Noise Ratios for Client Endpoints?

The Connectivity SNR Dashlet

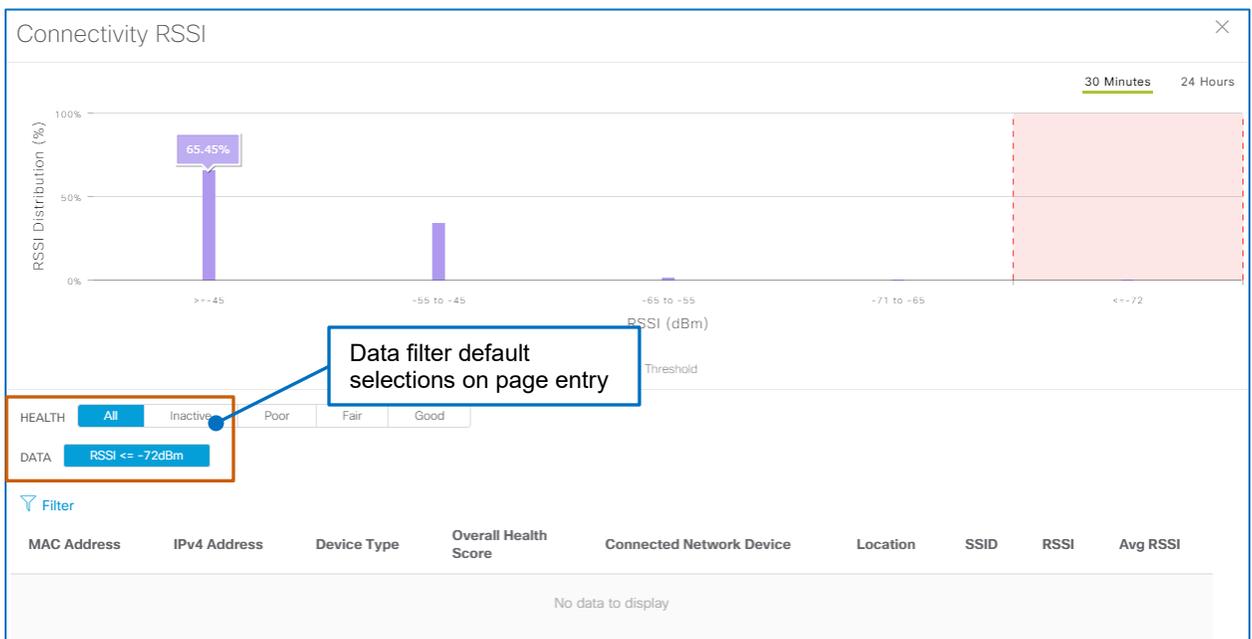
The **Connectivity Signal-to-Noise Ratio (SNR)** dashlet, which is visible by default, indicates the SNR values for all client endpoints.

The dashlet displays the percentages of endpoints experiencing signal-to-noise ratios in each dB range. In the screenshot below, there are no endpoints with SNRs below the pre-defined system threshold.



The Connectivity SNR Panel

When you open the panel, the device list displays all of the endpoints that are below the acceptable SNR threshold by default.



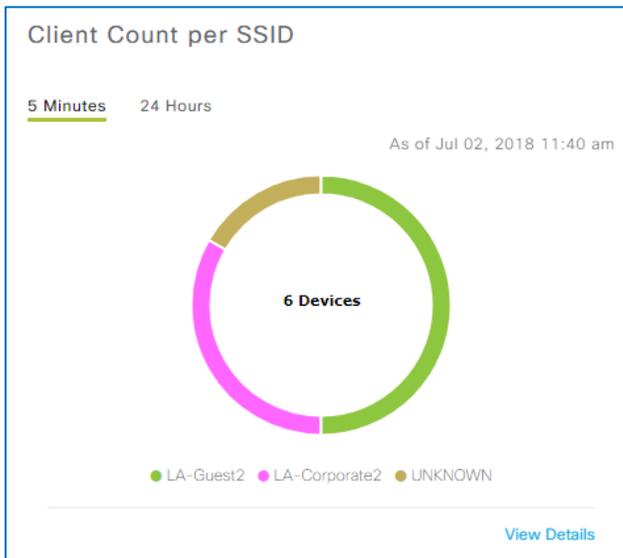
...The Number of Clients That Are Associated To Each SSID?

The Client Count per SSID Dashlet

The **Client Count per SSID** dashlet, which is visible by default, displays the total number of clients that are associated to all of the SSIDs on the network.

Each segment represents an SSID. The chart represents each SSID in color-coding to distinguish them in the chart with a legend below it.

When the system fails to capture the client count for an SSID, it identifies those SSIDs as **UNKNOWN**.



The Client Count per SSID Panel

When you open the panel, it displays dashlet chart and the list displays all of the endpoints associated to all of the SSIDs for all health states.

The list provides health filters for each health state, and data filters so that you can see the number of endpoints that are exceeding acceptable onboarding thresholds, including total onboarding time and the time for each stage of the onboarding process.

Client Count per SSID

5 Minutes 24 Hours

6 Devices

● LA-Guest2 ● LA-Corporate2 ● UNKNOWN

HEALTH All Inactive Poor Fair Good

DATA
Onboarding Time > Threshold
Association > Threshold
DHCP > Threshold
AAA > Threshold
RSSI > Threshold

[Filter](#)

UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Location	Onboarding Health	Connected Health	Connected Network Device	Location
daphne....	Daphne-PC	B8:27:EB:CA:AA:88	10.30.100.20	--	Linux-Wor...	10	USA/SM/Le...	●	●	LA2-AP380...	USA/SM/Le...
john.zo...	John-PC	B8:27:EB:0C:57:C8	0.0.0.0	--	Linux-Wor...	1	USA/SM/Le...	●	●	LA2-AP380...	USA/SM/Le...

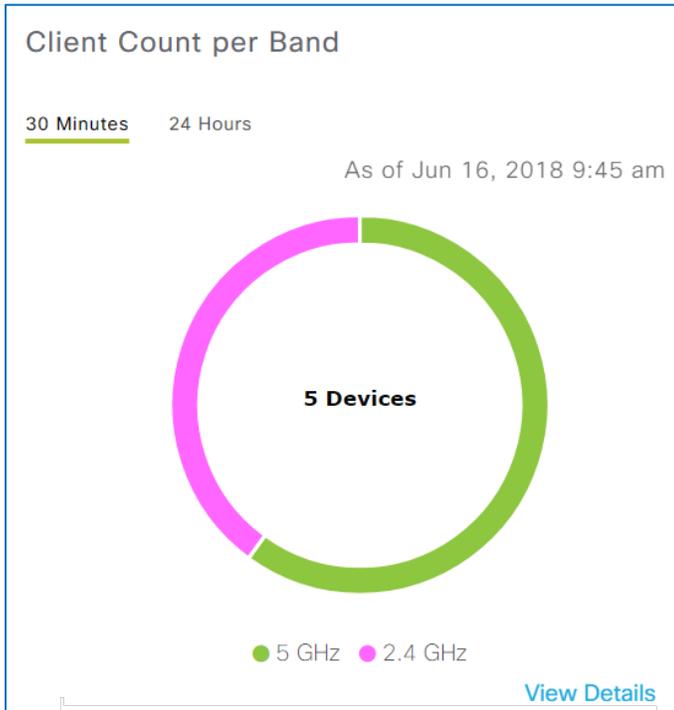
Data filters for total onboarding time and each stage of the onboarding process

...The Number of Clients That Are Using Each Radio Band Frequency?

The Client Count per Band Dashlet

The **Client Count per Band** dashlet, which is visible by default, displays the total number of client endpoints that are using the 2.4 GHz or 5GHz radio band frequencies.

Each segment represents the number and percentage of endpoints on each band.



The Client Count per Band Panel

When you open the panel, it displays the dashlet chart and the list displays all of the endpoints associated to all of the SSIDs for all health states.

The list provides health filters for each health state.

The data filters include seeing the number of endpoints:

- That are exceeding acceptable onboarding thresholds, including total onboarding time and the time for each stage of the onboarding process.
- That are exceeding the acceptable RSSI threshold.

Client Count per Band
✕

5 Minutes 7 Days

5 Devices

● 5 GHz ● 2.4 GHz

Data filter for total onboarding time and each stage of the onboarding process

HEALTH All Inactive Poor Fair Good

DATA Onboarding Time > Threshold Association > Threshold DHCP > Threshold AAA > Threshold RSSI > Threshold

Filter

UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Location	Onboarding Health
velma.d...	Galaxy-Ta...	C0:D3:C0:4D:B3:17	10.11.100.50	--	📶 Samsung-D...	9	Netherlan...	●
daphne....	Daphne-PC	B8:27:EB:CA:AA:88	10.30.100.20	--	📶 Linux-Wor...	10	USA/SM/Le...	●
turanga...	Leela-PC	B8:27:EB:0C:4C:10	0.0.0.0	--	📶 Linux-Wor...	1	USA/SM/Le...	●
daphne....	Daphne-iP...	6C:19:C0:BD:87:C9	10.30.100.27	--	📶 Apple-iPad	10	USA/SM/Le...	●
daphne....	Daphne-iP...	A8:BE:27:36:70:11	10.30.100.29	--	📶 iPhone 7	9	USA/SM/Le...	●

...The Physical Link Health of Wired Clients?

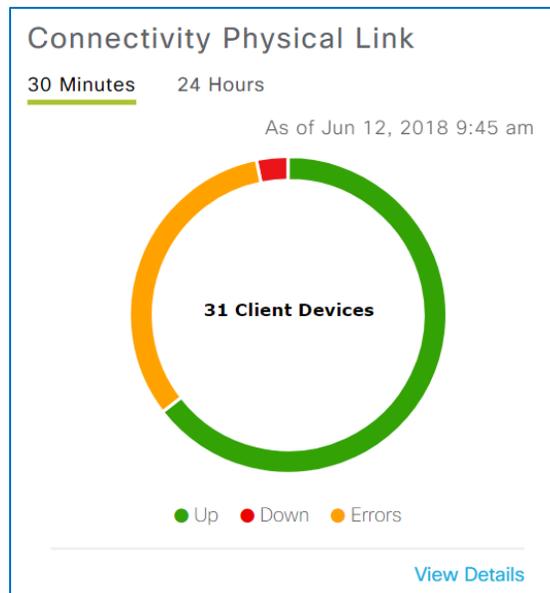
The Connectivity Physical Link Dashlet

The **Connectivity Physical Link** dashlet, which is visible by default, displays the number of devices with physical links that are up or down, or that contain errors

Physical links are wired connections between endpoints and the network, such as network cables.

In the chart, the color-coding represents:

- **Green (Up)**
Endpoint links that are connected physically
- **Yellow (Errors)**
Endpoint connections that are experiencing issues or errors, such as dropped or corrupt packets or mismatches in the packet and frame size configuration
- **Red (Down)**
Endpoint links that are not connected physically



The Connectivity Physical Link Panel

When you open the panel, it displays the dashlet chart and the list displays all of the endpoints in all health states.

The list provides health filters for each health state.

Connectivity Physical Link
✕

30 Minutes
24 Hours

31 Client Devices

● Up ● Down ● Errors

HEALTH All Inactive Poor Fair Good

Filter

UserID ⓘ	Hostname ⓘ	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Onboarding Health ⓘ	Connected Health ⓘ
--		70:DF:2F:4E:5A:D2	192.168.139.155	--	🚫 UNKNOWN	10	●	●
--		00:BE:75:49:F6:C4	192.168.139.73	--	🚫 UNKNOWN	10	●	●
--		38:0E:4D:9C:4A:52	192.168.139.195	--	🚫 UNKNOWN	10	●	●
--		18:80:90:7E:32:C8	192.168.139.172	--	🚫 UNKNOWN	6	●	●
--		00:0C:29:D7:AB:F6	192.168.139.167	--	🚫 UNKNOWN	6	●	●

Showing 5 of 31 [Show More >](#)

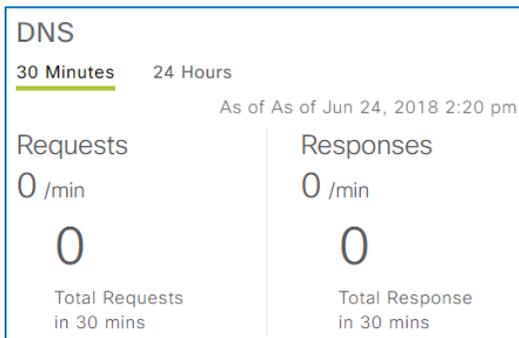
...The Numbers of DNS Requests and Responses per Minute?

The DNS Dashlet

The **DNS** dashlet, which is [a dashlet that you can add to the page](#), displays:

- The average number of DNS requests and responses that client endpoints have made or received at one minute time intervals within a 30 minute time period based on the time stamp.
- The total number of DNS requests and responses that client endpoints have made or received in a 30 minute time period based on the time stamp.

Extensive DNS response times can indicate endpoints' failures to obtain DNS server responses when, for example, the server is unreachable or is not responding to queries.



...Health Metrics and Attributes for Client Devices?

The Client Devices List

Client Devices lists each client endpoint that is active during the time interval indicated on the tab and based on [other settings that can affect the information that you see](#).

On page entry, the list displays all of the endpoint types, wired and wireless, in all health states.



Important Note: When you navigate to a different area of **Assurance**, or make a change to the time interval, the **Client Devices** list refreshes to display endpoints in all health states.

Client Devices (37) As of Jun 12, 2018 7:00 pm

5 Minutes 24 Hours

TYPE: **All** Wireless Wired HEALTH: **All** Inactive Poor Fair Good

DATA: Onboarding Time >= 10s Association >= 5s DHCP >= 5s AAA >= 5s RSSI <= -72dBm

Filter

UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Onboarding Health	Connected Health	Connected Network Device	Location	VLAN ID	SSID	AP Group	Band
hubert...	Hubert-PC	B8:27:EB:0C:44:40	0.0.0.0	--	Linux-Wor...	1	●	●	LA2-AP380...	USA/SM/Le...	130	LA-Guest2	LA1	2.4
velma.d...	Galaxy-Ta...	C0:D3:C0:4D:B3:17	10.11.100.50	--	Samsung-D...	9	●	●	AMS-AP380...	Netherlan...	100	AMS-Corpo...	AMS	5.0
--		00:0C:29:75:BB:FE	192.168.139.160	--	UNKNOWN	10	●	●	DC-SERVIC...	USA/DC	139	--		
--		54:AB:3A:B5:4B:CD	10.31.100.13	--	UNKNOWN	10	●	●	TO-3850-A...	Canada/TO...	100	--		
daphne...	Daphne-iP...	A8:BE:27:36:70:11	10.30.100.29	--	iPhone 7	9	●	●	LA2-AP380...	USA/SM/Le...	100	LA-Corpor...	LA1	5.0

When the Cisco DNA Center deployment includes an Identity Services Engine (ISE) that is integrated for Assurance, the **UserID** field indicates the network user for wired and wireless clients.

For wireless clients, the **Hostname** field indicates the device's name by obtaining the data from the WLC.

The **MAC Address** link indicates the NIC card in the device that is connected to the network and provides a link to [the endpoint's Client 360 page](#).

UserID	Hostname	MAC Address
daphne...	Daphne-iP...	6C:19:C0:BD:87:C9
velma.d...	Galaxy-Ta...	C0:D3:C0:4D:B3:17

Either the **IPv4 Address** or the **IPv6 Address** field indicates the applicable IP address to which the endpoint is connected.

The **Device Type** indicates the specific type of device that is connected to the endpoint.

The device type indicates **Unknown** when the system cannot obtain the information from ISE.

IPv4 Address	IPv6 Address	Device Type
10.30.100.27	--	📶 Apple-iPad
10.11.100.50	--	📶 Samsung-D...

The **Overall Health Score** of each client indicates the sum of the onboarding and connected health scores, up to a maximum of 10.

The **Onboarding Health** indicator indicates a score color-code based on whether the endpoint onboarding process occurred within an acceptable range.

The **Connected Health** indicator indicates a score color-code based on whether the endpoint remains in an acceptable range after the system has authenticated and associated it successfully.

Overall Health Score	Onboarding Health 	Connected Health 
10		
9		
10		



Note: The **Client Device** list only shows clients with completed health score calculations. Because client health score calculations occur every 5 minutes, newly onboarded clients or clients with pending health score calculations might not appear in the device list.

Device Type	Overall Health Score	Onboarding Health 	Connected Health 
☐ UNKNOWN	10		
📶 iPhone 7	9		

For detailed information on health scoring concepts related to time stamps, [refer to the Time Stamp and Data Aging Concepts Page in the Assurance Features and Navigation training.](#)

Client Devices also lists the following for each endpoint:

- The network device to which it is connected
- The endpoint's location [in the network hierarchy](#)
- VLAN identifier
- For wireless devices:
 - ▶ The SSID to which it is connected
 - ▶ The AP group to which it belongs
 - ▶ The radio band frequency it is using.



Note: For client endpoints that Assurance does not recognize, the **SSID**, **AP Group**, and **Band** attributes in the list are blank.

Connected Network Device	Location	VLAN ID	SSID	AP Group	Band
LA1-AP380...	USA/LA/Le...	100	LA-Corpor...	LA1	5.0
AMS-AP380...	Netherlan...	100	AMS-Corpo...	AMS	5.0
LA2-AP380...	USA/SM/Le...	100	LA-Corpor...	LA1	5.0
LA2-AP380...	USA/SM/Le...	100	LA-Corpor...	LA1	5.0

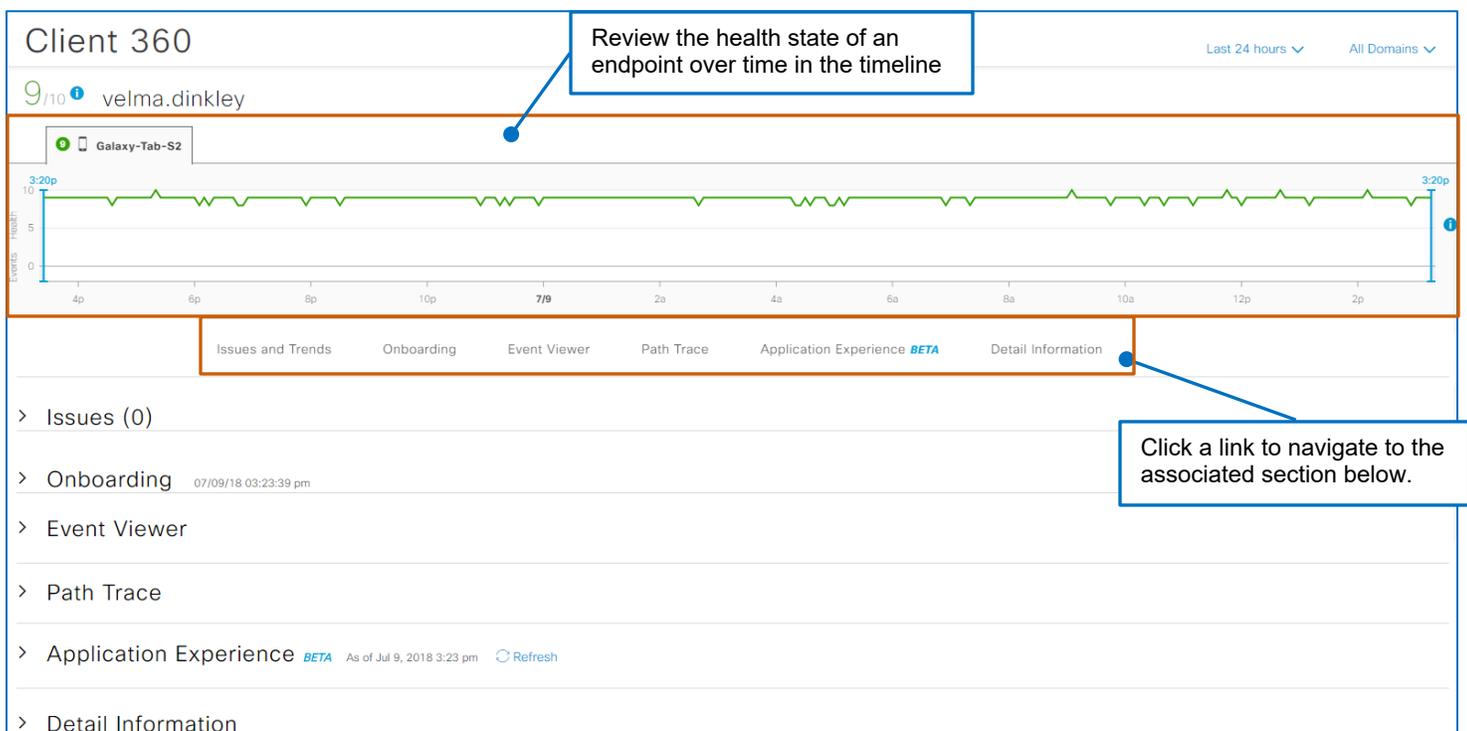
How is a Specific Client Endpoint Doing?

Get a Holistic View on the Client 360

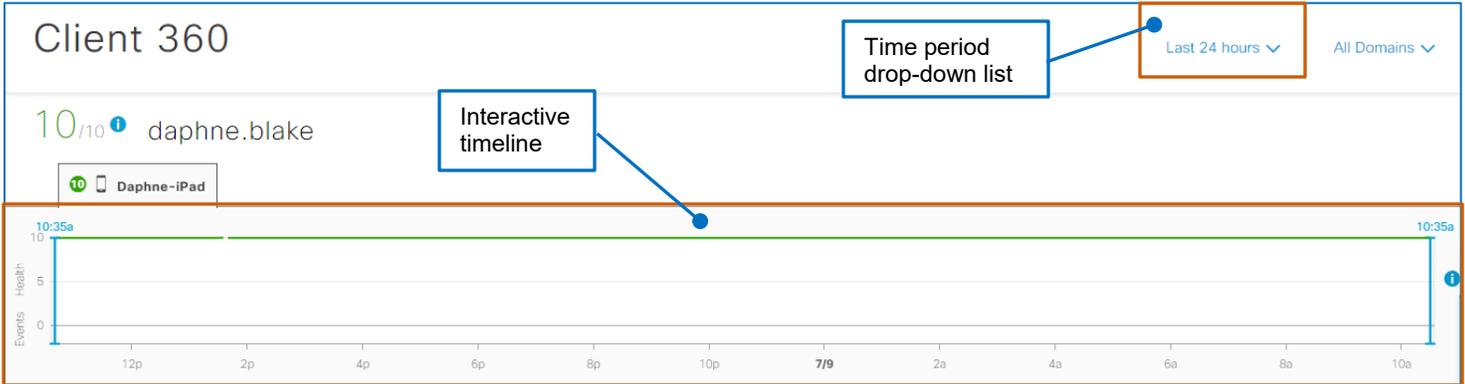
What Will I See?

The **Client 360** page provides information and insights for a specific client endpoint, including:

- A timeline that displays the client endpoint experience at a certain time.
- Issues that affect the endpoint. (**Issues**)
- The onboarding topology, the health and other details of devices on the topology and the states of each stage of onboarding (association, authentication, IP address assignment). (**Onboarding**)
- A list of specific events that Cisco DNA Center is capturing. (**Event Viewer**)
- A tool that evaluates the path that traffic is using between the endpoint and a specific destination point. (**Path Trace**)
- The applications that the endpoint is accessing and their health. (**Application Experience**)
- Additional device attributes and metrics. (**Detail Information**)



When you open a **Client 360** page, the page displays data for the past 24 hours by default.



You can change the time period by using the drop-down list or the timeline to evaluate data related to that interval for more detailed analysis.



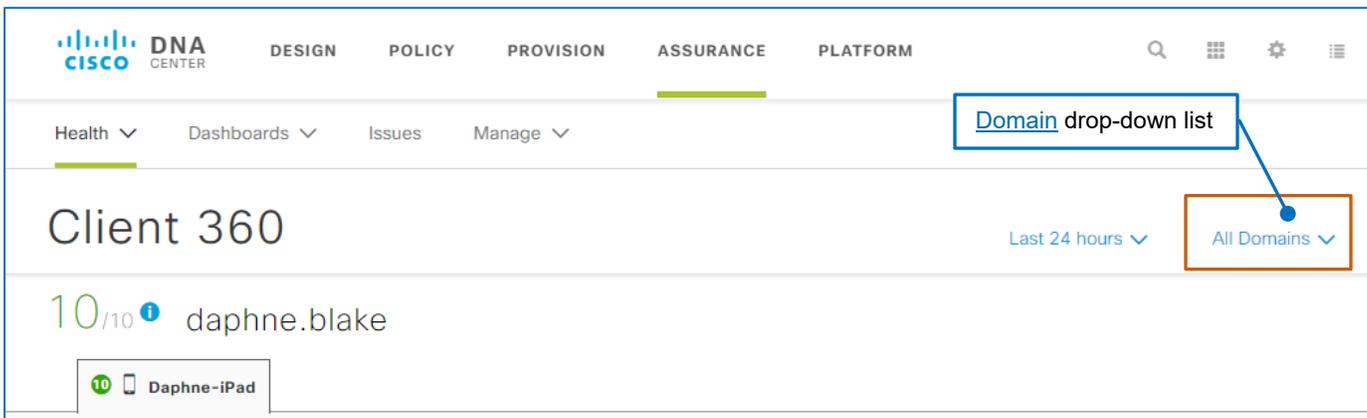
Note: When you apply a different time period and navigate away from the page, the setting does not persist. When you return to the page, the 24-hour default setting applies.

You also can evaluate a specific point in time by using the timeline, which can be helpful when resolving issues.



Note: For more information, [refer to the What Was a Client Endpoint Experiencing at a Certain Time? topic.](#)

In SD-Access deployments, you can apply client-related data for [a specific fabric domain](#) by using the domain drop-down list.



How Do I Open the Client 360 Page for a Specific Endpoint?

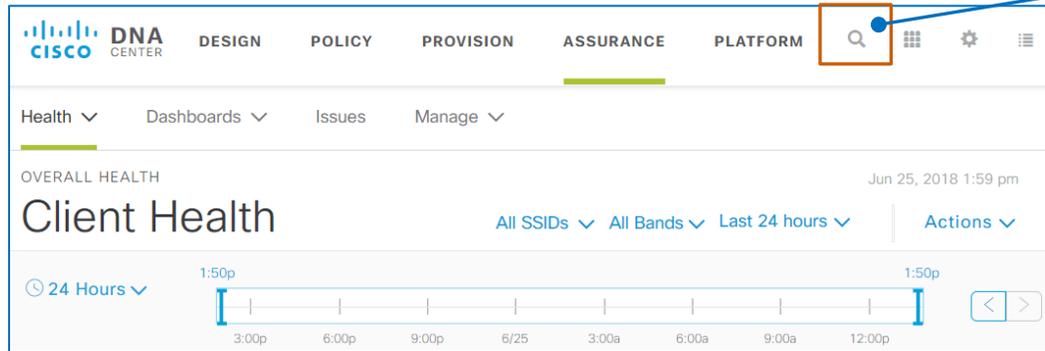
For a single endpoint, you can open **Client 360** pages by using:

- The Cisco DNA Center global search feature on the **Client Health** page.
- The MAC address links available [in endpoint lists on the Client Health page and on dashlet detailed information panels](#).

To open a **Client 360** page for a single endpoint by using the global search feature:

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

Global search icon



The **Search** dialog box opens.

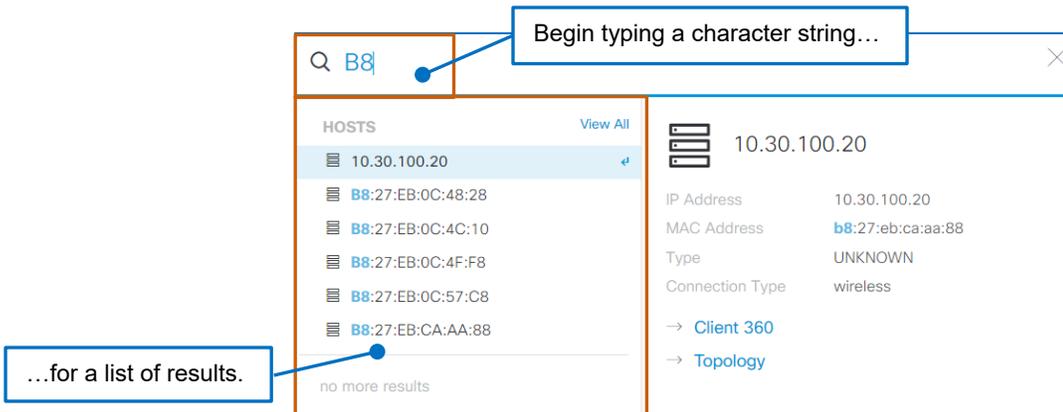


2. In the **Search** field, begin typing the character string for the search.



Note: Your search can include characters in the endpoint's MAC address, host name, the user ID, which is authenticated by the ISE server, or the endpoint IP address.

A list of results matching the characters that you type begins populating automatically.



- To indicate the endpoint that you want to see, in the results list, select the item.

The dialog box provides information about the endpoint and links to more information to the right of the search results.

- To open the **Client 360** page for the endpoint, click the **Client 360** link.

To open a Client 360 by using a MAC address link:

- In the **Client Devices** list, click the MAC address link for the endpoint of interest.



Note: Endpoint lists in panels also provide navigation links to the **Client 360** page.

UserID	Hostname	MAC Address	IPv4 Address	IPv6 Address	Device Type	Overall Health Score	Onboarding Health	Connected Health	Connected Network Device	Location	VLAN ID	SSID	AP Group	Band
hubert...	Hubert-PC	B8:27:EB:0C:44:40	0.0.0.0	--	Linux-Wor...	1	●	●	LA2-AP380...	USA/SM/Le...	130	LA-Guest2	LA1	2.4
velma.d...	Galaxy-Ta...	C0:D3:C0:4D:B3:17	10.11.100.50	--	Samsung-D...	9	●	●	AMS-AP380...	Netherlan...	100	AMS-Corpo...	AMS	5.0

The following screenshot illustrates the information available on a **Client 360** page for an endpoint.

Client 360 Last 24 hours ▼ All Domains ▼

9 / 110 ▼ velma.dinkley

● Galaxy-Tab-S2

Issues and Trends Onboarding Event Viewer Path Trace Application Experience BETA Detail Information

Issues (0)

Onboarding 07/09/18 03:23:39 pm

● AAA ● DHCP

Event Viewer

Filter EQ Find

Jul 9, 2018

>	● Re-Authentication	WLC-LA1-WLC5520-2	3:14:36.044 PM - 3:14:36.329 PM
>	● Re-Authentication	WLC-LA1-WLC5520-2	2:44:17.368 PM - 2:44:17.641 PM
>	● Re-Authentication	WLC-LA1-WLC5520-2	2:13:29.414 PM - 2:13:29.889 PM
>	● Re-Authentication	WLC-LA1-WLC5520-2	1:43:19.834 PM - 1:43:20.395 PM
>	● Re-Authentication	WLC-LA1-WLC5520-2	1:12:41.962 PM - 1:12:42.301 PM
>	● Re-Authentication	WLC-LA1-WLC5520-2	12:42:08.218 PM - 12:42:08.585 PM
>	● Re-Authentication	WLC-LA1-WLC5520-2	12:10:59.334 PM - 12:10:59.784 PM
>	● Re-Authentication	WLC-LA1-WLC5520-2	11:40:22.484 AM - 11:40:22.950 AM
>	● Re-Authentication	WLC-LA1-WLC5520-2	11:09:30.708 AM - 11:09:31.049 AM

Select an event to view details

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

Application Experience BETA As of Jul 9, 2018 3:23 pm Refresh

Business Relevant Business Irrelevant Default

Application (0) Export

Filter EQ Find

Name	Host Name	Health		Usage		Average Throughput	Traffic Class	DSCP		Packet Loss (%)		Network Latency		Application Server Delay	
		Most Recent	Last 24 Hours	Bytes	Percentage (%)			Marking	Preservation	Max	Average	Max	Average	Max	Average
No data to display															

Detail Information

Device Info Connectivity RF

Information		Connection Information	
User Name	velma.dinkley	Band	5 GHz
Host Name	Galaxy-Tab-S2	Spatial Streams	2
MAC Address	C0:D3:C0:4D:B3:17	Channel Width	20 MHz
IP Address	10.11.100.50	WMM	Supported
Device Type	Samsung-Device	U-APSD	Disabled
Operating System	Unknown		
VLAN ID	100		

Where Do I Find...

...Issues That Are Affecting the Endpoint?

Issues lists the problems that are affecting the endpoint. The system identifies issues by computing, analyzing, and correlating incoming data and correlating the data with system-defined metrics.

Issues (4)	
Onboarding Wireless client failed to connect (SSID: LA-Guest2, AP: LA2-AP3802-23, Band: 2.4 GHz) - DHCP Timeout Total occurrences: 189	07/05 9:17am
Onboarding Wireless client failed to connect (SSID: LA-Guest2, AP: LA2-AP3802-23, Band: 2.4 GHz) - DHCP Timeout Total occurrences: 8	07/05 6:43am
Onboarding Wireless client failed to connect (SSID: LA-Guest2, AP: LA2-AP3802-23, Band: 2.4 GHz, Site: Global/USA/SM/Level1) - Failed to authenticate due to Client Timeout Total occurrences: 5	07/05 5:53am
Onboarding Wireless client failed to connect (SSID: LA-Guest2, AP: LA2-AP3802-23, Band: 2.4 GHz, Site: Unknown) - Failed to authenticate due to Client Timeout Total occurrences: 2	07/04 11:42am

[Resolved Issues](#)

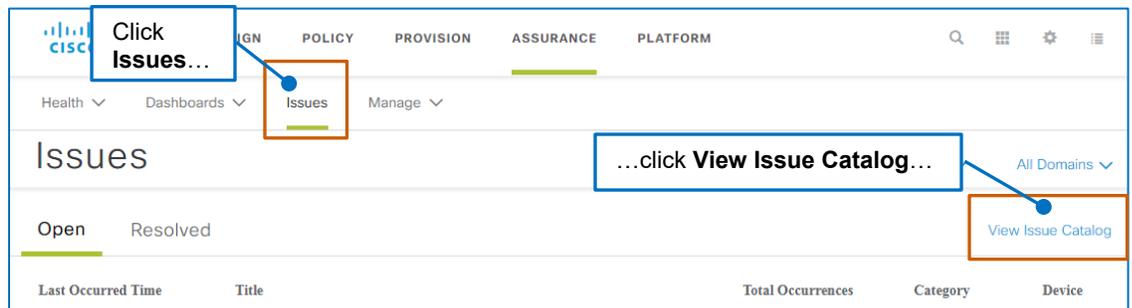
Providing this information with links for immediate access to details helps to ensure that potential or ongoing problems receive more immediate attention or action, as needed.



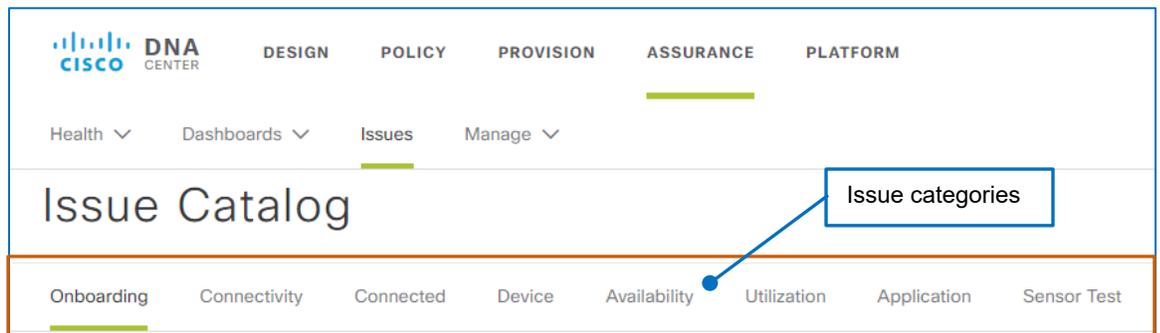
Tip: For your reference, **Assurance** provides an issue catalog that categorizes and lists the issues that Cisco DNA Center presents.

To open the list:

- Click **Issues**, and then, below the toolbar, click **View Issue Catalog**.



The catalog provides tabs for each issue category.



For each category, the issues in the list include descriptions and possible root causes for them.

You can select an issue to see its related information.

Issue Name	Instances	Status	License Type
Wireless client onboarding issues	3923	RUNNING	Advantage Subscription
Onboarding issues due to DHCP Timeout	1226	RUNNING	Advantage Subscription
Client DHCP reachability issue	382	RUNNING	Advantage Subscription
Excessive time for onboarding due to AAA server	0	RUNNING	Advantage Subscription

Wireless client onboarding issues

Issue Description
Wireless client failed to connect or took a long time to connect

Root Causes

- Wireless client failed to connect - Security Parameter Mismatch
- Wireless client failed to connect - AAA Server Rejected Client
- Wireless client failed to connect - AAA Server Rejected Client

Entries in the list are open and are occurring or have occurred during the time period that the page indicates in the time interval drop-down list or on the timeline.

The time stamp beside the issue indicates its most recent occurrence. The number of occurrences of the problem appear below the description link.

To review issue details, under the issue heading:

- Click the issue description link.

A panel opens, overlaying the page.

Issues (3)

Onboarding

[Wireless client failed to connect \(SSID: LA-Guest2, AP: LA2-AP3802-23, Band: 2.4 GHz\) - DHCP Timeout](#)

Total occurrences: 170

07/05 10:29am

The panel provides:

- The option to change the issue status from **Open** to **Resolve**.
- A description of the issue.
- Based on the type of issue and its complexity, related charts and metrics.
- Areas and numbers of clients that the issue affects.
- Suggestions to correct the issue, and depending on issue, the ability to run commands that retrieve additional information or provide corrective suggestions.

When issues are complex, the panel can provide various charts and information on the issue.

Wireless client failed to connect (SSID: LA-Guest2, AP: LA2-AP3802-23, Band: 2.4 GHz) - DHCP Timeout

Status: Open Last Occurred: Jul 3, 2018 3:53 PM

Description

This client failed to get an IPv4 address during onboarding. This happened because the DHCP messages timed out during the DHCP message exchange. In this instance, either the DHCP server or the client failed to respond to the DHCP messages. This client was connecting to 'LA-Guest2' SSID on '130' VLAN on 2.4 GHz radio on 'LA2-AP3802-23' AP in location 'Global/USA/SM/Level1'. The AP was connected to 'LA1-WLC5520-2' WLC.

Impact of Last Occurrence

Jul 03, 2018 03:23 PM to 03:53 PM

- Location: 1 Building
- Clients: 6 Wireless Clients

Client DHCP Attempts (Site: USA/SM/Level1)

Jul 2, 2018 3:53 pm to Jul 3, 2018 3:53 pm

Time (Day/Hrs)

● Failed Attempts - DHCP Server or Client Timeout ● Success Attempts

Event writer Ta... < ● ● ● ● > Authentication ...

Information pages with scroll navigation

Suggested Actions (4)

- 1 Verify that the DHCP server is reachable.
- 2 Verify that the DHCP scope is configured correctly and has adequate free IP addresses.
- 3 If all new clients are not getting assigned IP Address, verify that the IP helper address is configured correctly on the first hop router servicing the VLAN.
- 4 Initiate the Path Trace tool to verify that the DHCP server can reach the first hop router servicing VLAN.

When you determine that an open issue is no longer a problem, you can resolve the issue.

To indicate that the issue is resolved:

- In the **Status** drop-down list, select **Resolve**.
This action moves the issue to the **Resolved Issues** list.



Important Note: You cannot move or change the status of a resolved issue.

Wireless client failed to DHCP Timeout

Status: Open Resolve

Finally, you can review a list of actions you can take to help more clearly identify or resolve the issue.

When suggestions are collapsed, you can expand them to see a list of associated steps that you can take.

Some suggested actions can contain commands that you can run to obtain additional information or additional corrective suggestions.

Suggested Actions (4)

- 1 Verify that the DHCP server is reachable.
- 2 Verify that the DHCP scope is configured correctly and has adequate free IP addresses.
- 3 If all new clients are not getting assigned IP Address, verify that the IP helper address is configured correctly on the first hop router servicing the VLAN.
- 4 Initiate the Path Trace tool to verify that the DHCP server can reach the first hop router servicing VLAN.

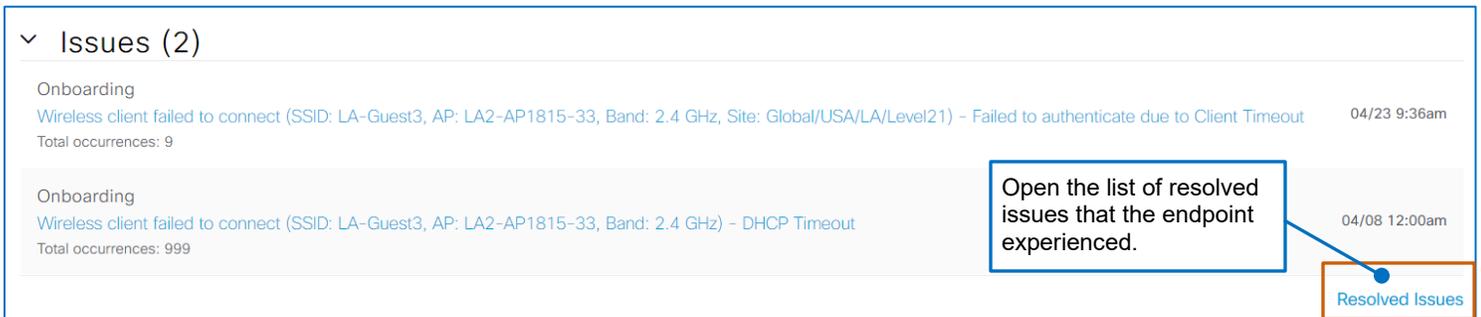
...A List of Resolved Issues and Their Details?

Under **Issues**, you can access a list of previous issues that affected the endpoint that either the system resolved automatically or a system user resolved manually.

This information can provide deeper insight when you are working to evaluate or resolve current issues.

To open the list of resolved issues:

- Below the **Issues** list, click **Resolved Issues**.



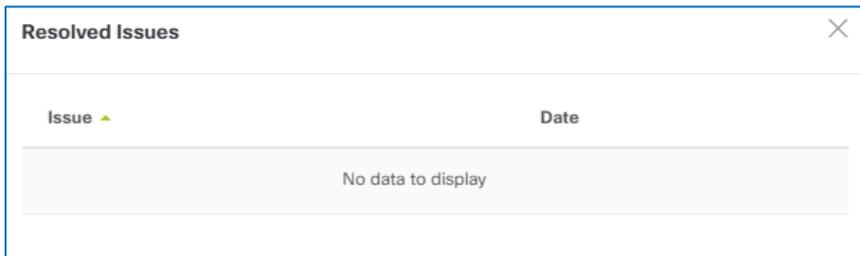
Issues (2)

Onboarding
Wireless client failed to connect (SSID: LA-Guest3, AP: LA2-AP1815-33, Band: 2.4 GHz, Site: Global/USA/LA/Level21) - Failed to authenticate due to Client Timeout 04/23 9:36am
Total occurrences: 9

Onboarding
Wireless client failed to connect (SSID: LA-Guest3, AP: LA2-AP1815-33, Band: 2.4 GHz) - DHCP Timeout 04/08 12:00am

Resolved Issues

A panel opens with a list of resolved issues and includes the date that the issue was resolved.



Resolved Issues

Issue	Date
No data to display	

When the system automatically or system users manually resolve issues, the **Resolved Issues** list retains the issue for 14 days, and then removes it from the list.

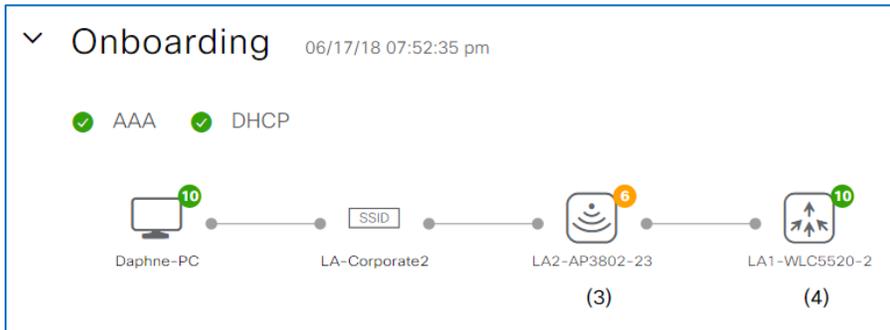


Important Note: You cannot move or change the status of a resolved issue.

...The Endpoint's Network Path and the Health of Devices on the Path?

Onboarding displays the device topology that is connecting the endpoint to the network, the health of those devices, and the status of the AAA and DHCP services.

The following screenshot illustrates the onboarding process for a wireless client. In this example, the client endpoint **Daphne-PC** connects to the hierarchical group **LA-Corporate2's** SSID on a specific AP in that group, which is joined to a WLC in the **LA1** group [in the network hierarchy](#).

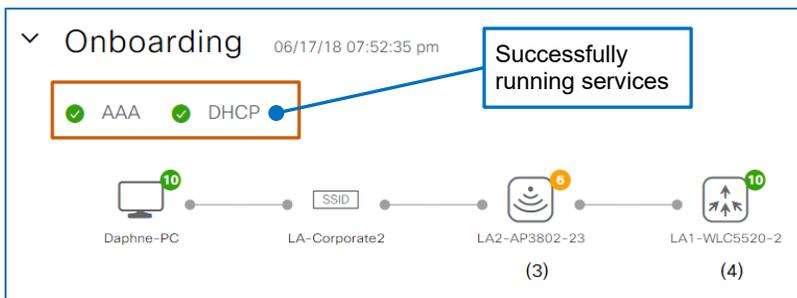


A green checkmark beside **AAA** indicates that the client successfully associated and authenticated to the network.



Note: When a client is onboarding by using open authentication, the AAA status indicator does not appear.

A green checkmark beside **DHCP** indicates that the client obtained an IP address.



A red cross beside either service indicates that the service has failed.



Note: When a service fails during onboarding, the system also captures the corresponding issue in the **Issues** list on the **Client 360** page.

When no services are listed, an issue has occurred during the onboarding process, but the system has not captured any events related to the AAA or DHCP service.

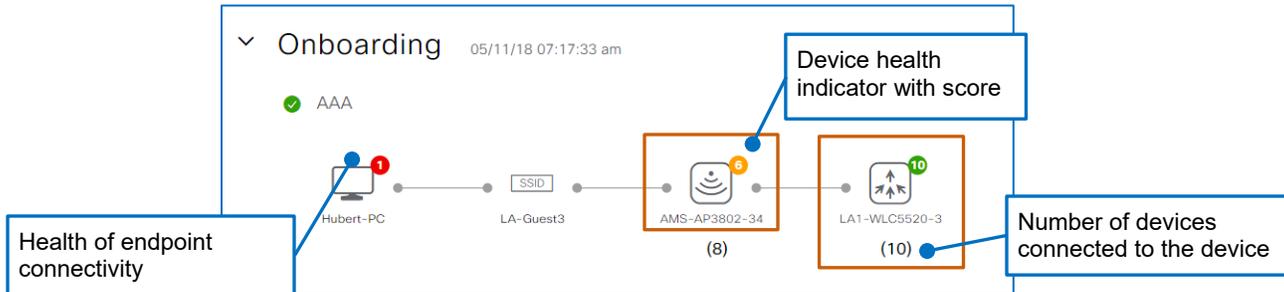


Tip: In this case, you can refer to the **Issues** list to review the events that the system captured.

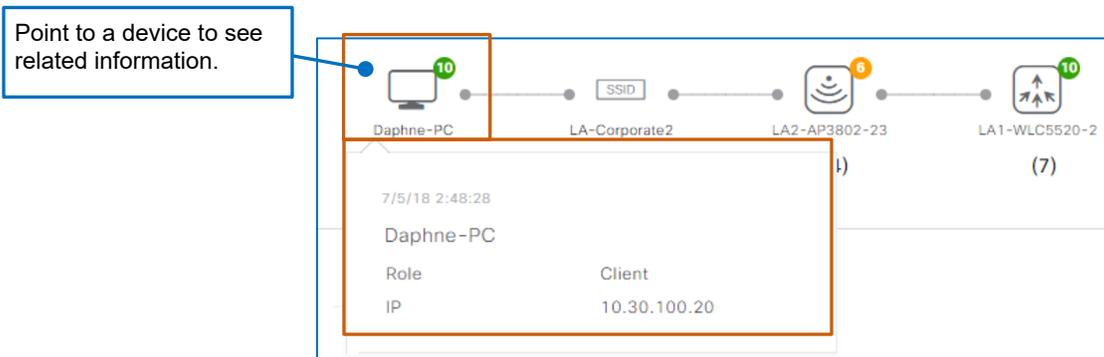
The color-coded number beside the endpoint icon indicates the health of its connectivity.

Color-coded numbers beside device icons indicate their overall health based on applicable metrics. The numbers in parentheses below device icons indicate the number of devices connected to it.

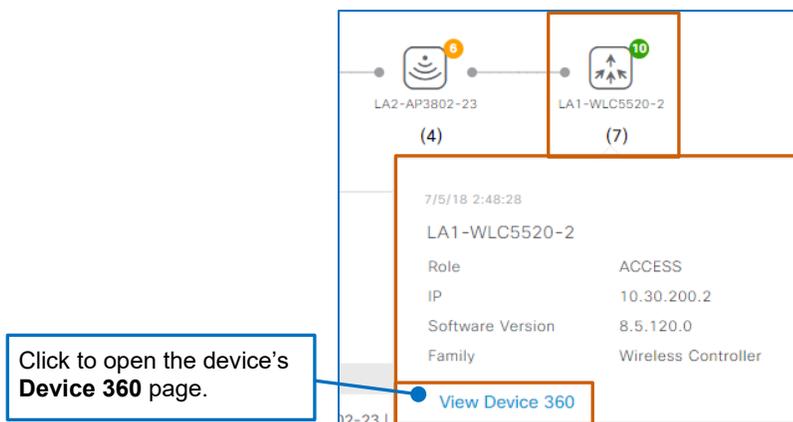
The numbers in parentheses below devices indicate the number of devices connected to it.



You can point to an endpoint icon to see more information.



You can point to a device icon to see device attributes and access a link to its **Device 360**.



...Endpoint-Related Events and Their Statuses?

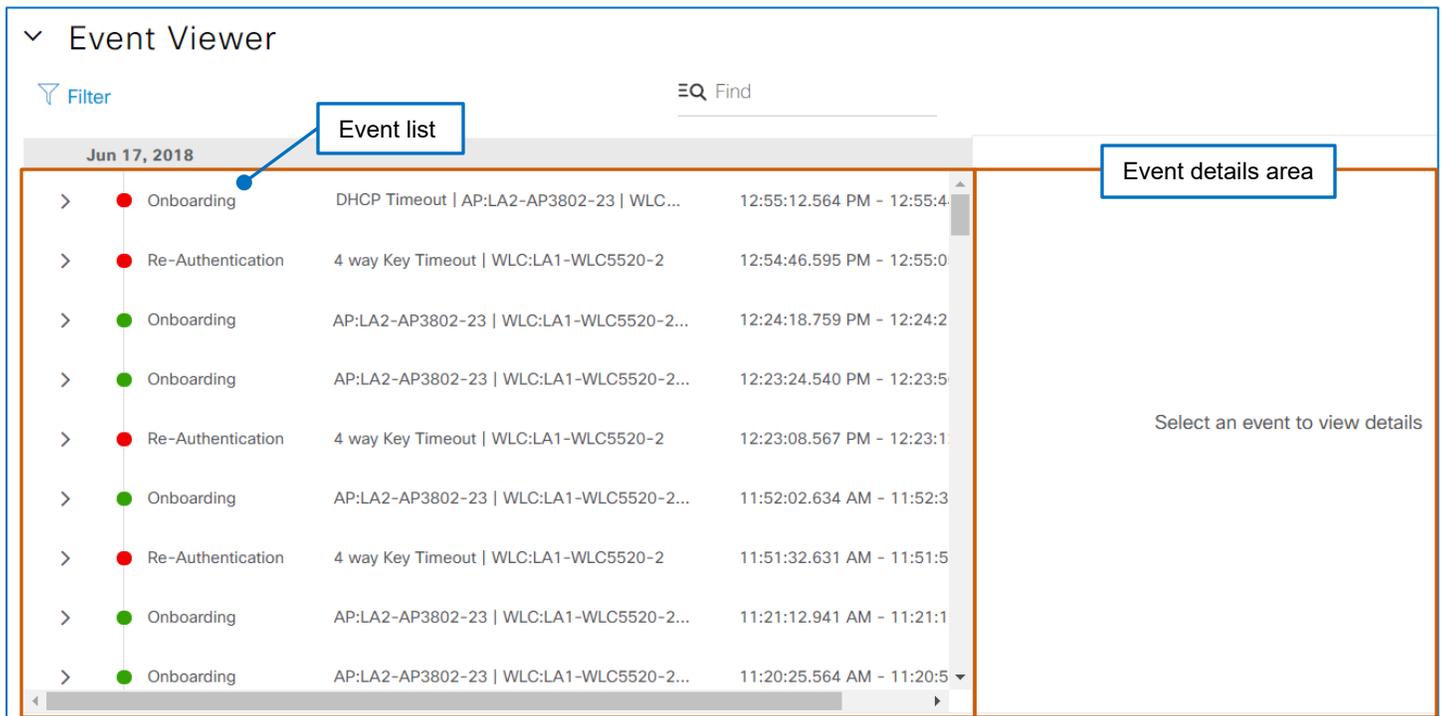
The **Event Viewer** lists the following endpoint-related events that the system collects for the 24-hour time period.

The **Event Viewer** includes information about the following events:

- Re-authentication
- Broadcast encryption rekey
- Onboarding processes
- Intra-roaming of the endpoint among access points
- Application response times that the endpoint is experiencing

Beside each event, color-coding indicates the event's success or failure.

It also has an area to display event details when you select one for review.



The screenshot shows the 'Event Viewer' interface. At the top left, there is a 'Filter' icon and a search bar labeled 'Find'. Below this is a date header 'Jun 17, 2018'. The main area contains a table of events, each with a status indicator (red for failure, green for success), an event name, a description, and a time range. A blue box labeled 'Event list' points to the table. To the right, an orange box labeled 'Event details area' contains the text 'Select an event to view details'.

Status	Event Name	Description	Time Range
Failure	Onboarding	DHCP Timeout AP:LA2-AP3802-23 WLC...	12:55:12.564 PM - 12:55:4...
Failure	Re-Authentication	4 way Key Timeout WLC:LA1-WLC5520-2	12:54:46.595 PM - 12:55:0
Success	Onboarding	AP:LA2-AP3802-23 WLC:LA1-WLC5520-2...	12:24:18.759 PM - 12:24:2
Success	Onboarding	AP:LA2-AP3802-23 WLC:LA1-WLC5520-2...	12:23:24.540 PM - 12:23:5
Failure	Re-Authentication	4 way Key Timeout WLC:LA1-WLC5520-2	12:23:08.567 PM - 12:23:1
Success	Onboarding	AP:LA2-AP3802-23 WLC:LA1-WLC5520-2...	11:52:02.634 AM - 11:52:3
Failure	Re-Authentication	4 way Key Timeout WLC:LA1-WLC5520-2	11:51:32.631 AM - 11:51:5
Success	Onboarding	AP:LA2-AP3802-23 WLC:LA1-WLC5520-2...	11:21:12.941 AM - 11:21:1
Success	Onboarding	AP:LA2-AP3802-23 WLC:LA1-WLC5520-2...	11:20:25.564 AM - 11:20:5

To see a list of contributing events:

- In the list of events, expand an item.
The item opens a list of the additional actions related to that event and their statuses.

Event Viewer

Filter Find

Jun 26, 2018

✓	● Onboarding	DHCP Timeout AP:LA2-AP3...	6:39:31.098 AM - 6:41:33
	● DHCP	DHCP Timeout	6:41:33.671 AM
	● Mobility	MM Handoff Timeout	6:39:33.724 AM
	● KeyExchange		6:39:33.724 AM
	● Authentication Done	Dot1x Full Auth	6:39:33.652 AM
	● Authentication Start		6:39:33.330 AM
	● EAP Start		6:39:33.330 AM
	● Authentication Start		6:39:31.101 AM
	● Association Done		6:39:31.098 AM
	● Association Start	Client Association with AP	6:39:31.098 AM

Select an event to view details

Select an event in the list to see its details.

Jun 26, 2018

✓	● Onboarding	DHCP Timeout AP:LA2-AP3...	6:39:31.098 AM - 6:41:33
	● DHCP	DHCP Timeout	6:41:33.671 AM
	● Mobility	MM Handoff Timeout	6:39:33.724 AM
	● Authentication Done	Dot1x Full Auth	6:39:33.652 AM
	● Authentication Start		6:39:33.330 AM
	● EAP Start		6:39:33.330 AM
	● Authentication Start		6:39:31.101 AM
	● Association Done		6:39:31.098 AM
	● Association Start	Client Association with AP	6:39:31.098 AM

DHCP Jun 26, 2018 6:41:33 AM

Detailed Information

Status: ● Failure

Details:

VLAN	130
Frequency(GHz)	2.4
ROLE	LOCAL
AP_Mac	38:90:A5:DF:3B:60
AP_Name	LA2-AP3802-23
WLC_Name	LA1-WLC5520-2
IPv4	0.0.0.0
WLAN	LA-Guest2
AUTH-Server	192.168.139.168
DHCP-Server	0.0.0.0
USERNAME	bender.rodriguez

...The Tool for Evaluating the Path That Traffic Is Using?

Path Traces for Flow Mapping and Path Health

Path Trace provides the tool that you can use to map the complete path that client traffic is taking from the IP address to which a client is connected to its destination, such as a server or printer.

Running a path trace supports monitoring and troubleshooting end-to-end connectivity, such as when you are evaluating issues.

▼ 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](#)

When you initiate a path trace, Cisco DNA Center reviews and collects network topology and routing data from the devices supporting the traffic. It calculates and displays the path between a client endpoint and its destination in a path trace topology. Following is an example of a complete path trace.

▼ 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.

10.30.100.27 (port: not specified) → 10.30.120.10 (port: not specified) [protocol: tcp] Jul 6, 2018 9:35 am

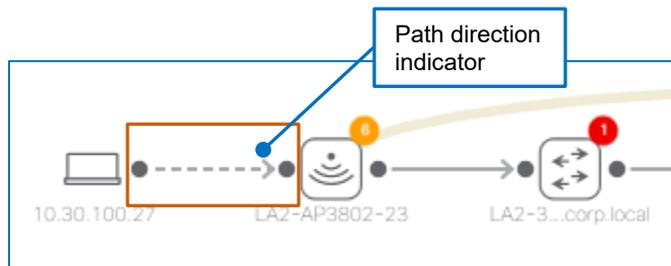
[Run New Path Trace](#)

A completed path trace displays:

- The path direction.

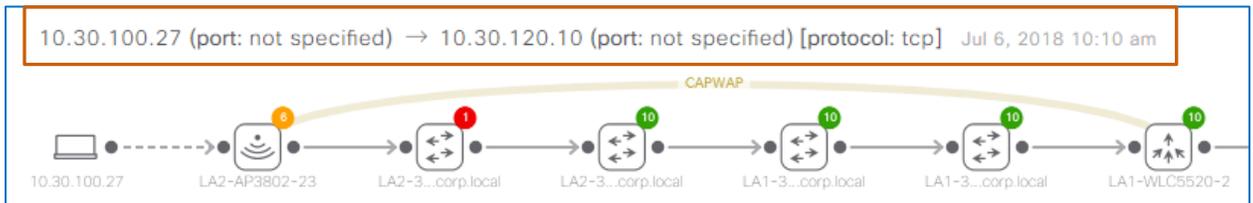


Note: The Path Trace tool provides the flexibility to run a path trace from any source to any destination to support troubleshooting. For example, you can run a separate path trace to evaluate the reverse direction of the flow, when that is helpful.

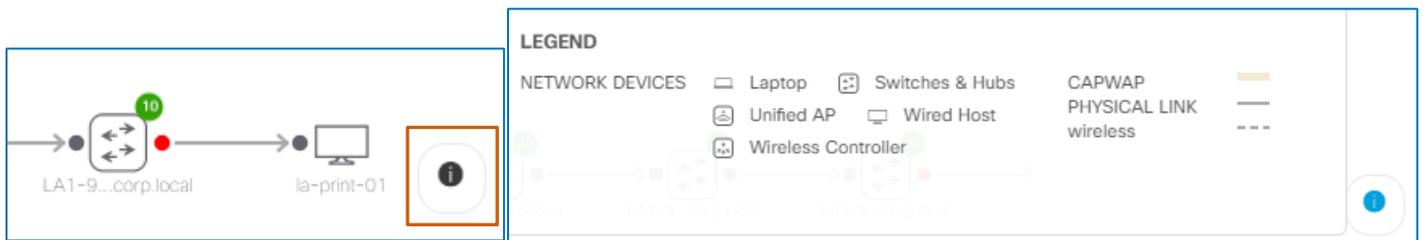


- Each intermediate network device that traffic is using to traverse to its destination and their protocols, its health state, and the number of endpoints connected to it.

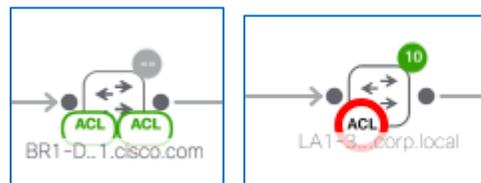
- Above the topology, a description of the path with a time stamp indicating the most recent time that you ran the path trace or the system refreshed it.



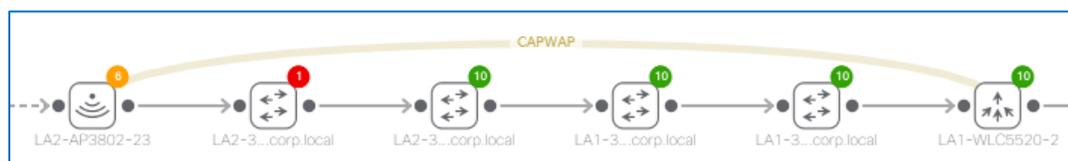
- To the right of the trace topology, a legend defining the device icons and link types.



- Based on items that you can select for the path trace to identify:
 - ▶ At each ingress and egress interface, each access control list (ACL) on that interface that match the criteria that you indicate when you configure the path trace.
 - Permit ACLs appear in green color-coding.
 - Deny ACLs appear in red color-coding.
 - When there is lack of data, such as a missing source or destination interface or protocol, in the trace configuration, the trace returns an ACL result in black color-coding.



- ▶ Device level CPU and memory utilization statistics.
 - ▶ Interface level ingress or egress drops.
- For wireless clients, the CAPWAP tunnel that is connecting the access point to the WLC to which it is joined.



You can point to a device to see device details and access a link to the **Device 360** page, which can provide insight when troubleshooting a problem.

...to see its name and statistics, if included in the trace...

...or open the **Device 360** page.

View Device 360

Point to a device icon...

Jul 6, 2018 9:47 am	
LA2-3850-ACC-1.corp.local	
CPU utilization	3%
Memory utilization	37.02%

You can point to a link to see the protocol running between two devices.

Point to a link...

...to see the protocol.

InterVlan Routing

You can point to ingress and egress interface icons for a device to see the interface that the path is using, the VLAN that the interface is using and packet drop metrics.

When you include interface statistics in the trace, you can click **More Details** to open a panel with the detailed interface statistics.

Point to an ingress or egress interface...

...to see summary interface information....

...or open a panel with detailed interface statistics.

More Details

Panel

Aug 7, 2018 9:55 am	
TenGigabitEthernet1/0/1	
Egress details	
TenGigabitEthernet1/0/1	
Used VLAN	120
Admin status	up
Output Drop	1834475296
Output Queue Count	0
Output Rate	0 bps
Operational status	up
ACL Name	N/A
ACL Result	NONE

Tip: If a link in a pop-up window does not respond, rerun the path trace or refresh the page to enable it.

When you run a path trace with ACL results, you can point to an ACL icon to see the ACL name and its rule.

Aug 2, 2018 2:12 pm
 FD1_Switch
 CPU utilization 3%
 Memory utilization 43.81%

Ingress ACL (GigabitEthernet1/0/6)
 ACL Name int_acl
 ACL Result PERMIT

FD1_Switch → FD1_EDGE_2 → 17.0.57.236

How Do I Prepare To Run a Path Trace?

Before you begin a path trace, ensure that the system inventory contains all of the devices, such as routers, switches, Cisco WLCs, and access points, between the source device and destination device, and that they are in a managed state.

To do so, you can review **Inventory** page, which you can access on the Cisco DNA Center home page.

Inventory

Validate the managed state of devices under **Last Sync Status**.

Device Name	IP Address	Reachability Status	Uptime	Last Updated	Resync Interval	Last Sync Status
DC-SERVICES	10.0.100.8	Reachable	324 days 8 hrs 43 mins	12 minutes ago	00:25:00	Managed
CORE-1	10.0.255.31	Reachable	94 days 19 hrs 12 mins	9 minutes ago	00:25:00	Managed
CORE-2	10.0.255.32	Reachable	328 days 4 hrs 20 mins	10 minutes ago	00:25:00	Managed
CORE-1-VPC-AGG-1	10.0.255.33	Reachable	94 days 19 hrs 17 mins	a minute ago	00:25:00	Managed

When you need to run a path trace for a specific interface or port on either the source or destination device, obtain each interface and port number that you need.

Source

IPv4
 10.30.255.103

Interface (optional)
 -

-
- 10.30.255.103
- 10.30.253.3
- 192.168.0.1

Destination

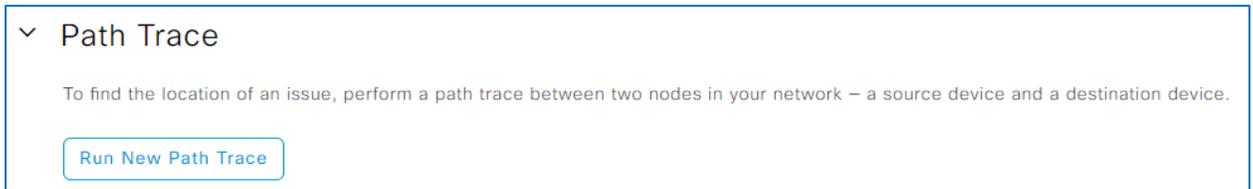
IPv4

Port (optional)

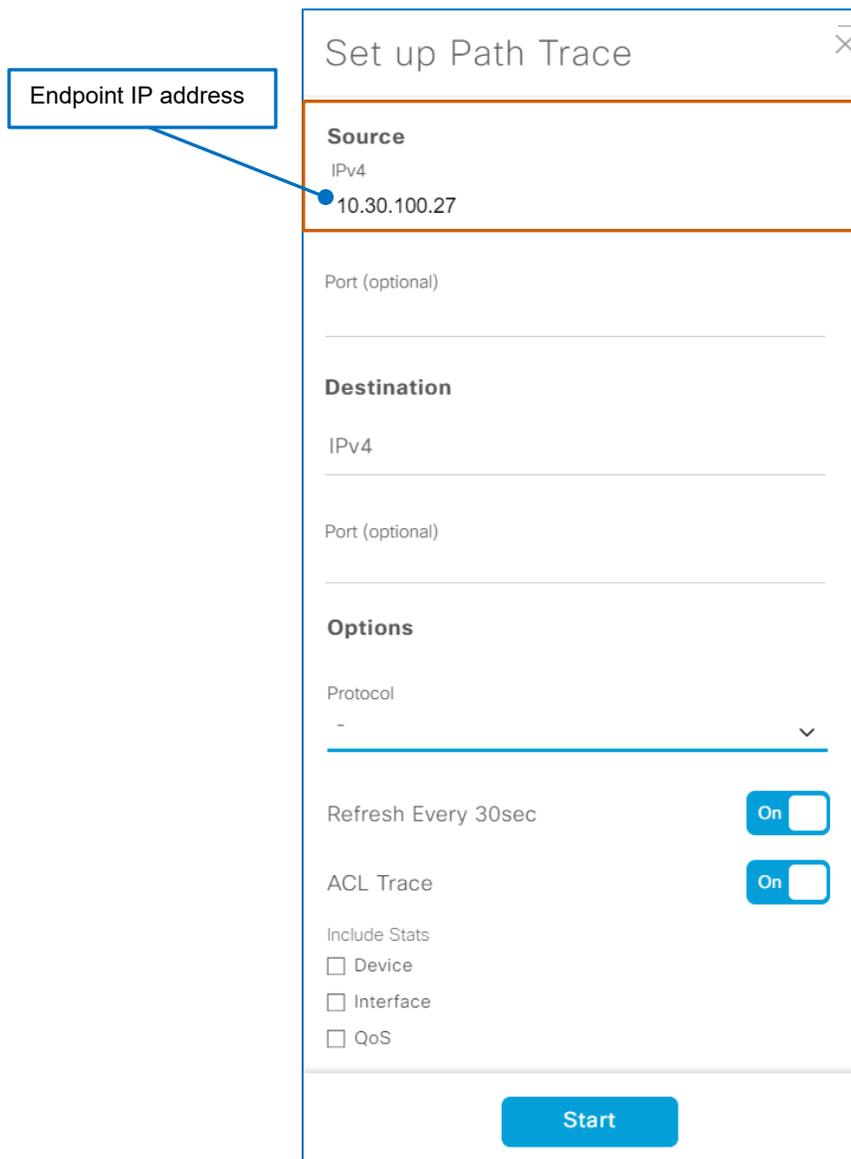
How Do I Run a Path Trace?

To run a path trace:

1. Under **Path Trace**, click **Run New Path Trace**.



The **Set up Path Trace** panel opens, and, under **Source**, the panel populates the **IPv4** field with the endpoint's IP address.



- 2. To identify the client endpoint at which you want the trace to start, under **Source**:
 - a. In the **IPv4** field:

- To use the endpoint IP address, validate and accept the default address that the panel populated.



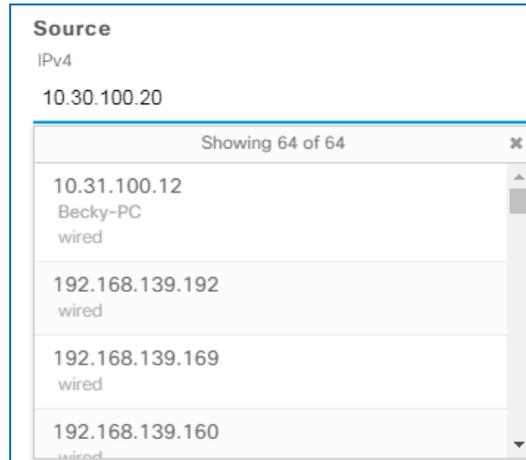
Source
IPv4
10.30.100.20

- To select another endpoint or identifier, click the field, and then, in the drop-down list select the endpoint.



Note: For added flexibility during troubleshooting, you can select any source or destination endpoint to run the trace.

This way, you do not need to navigate to another 360 page to run the trace of interest.



Source
IPv4
10.30.100.20

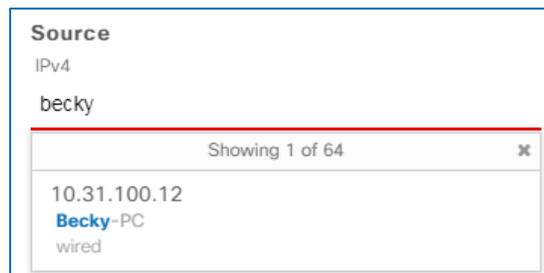
Showing 64 of 64

10.31.100.12 Becky-PC wired
192.168.139.192 wired
192.168.139.169 wired
192.168.139.160 wired



Tip: You can filter the list to find the endpoint that you need by typing an IP address, a host name, a user name, or an application name.

The list filters automatically as you type to display the results that match the string.



Source
IPv4
becky

Showing 1 of 64

10.31.100.12 Becky-PC wired
--

- b. Optionally, to identify the interface on which you need to start the trace, in the **Port** field, type the interface number.

Source

IPv4

10.30.100.20

Port (optional)

- 3. Under **Destination**, to indicate the point at which you want to end the trace.
 - a. In the **IPv4** field, click the field, and then, in the drop-down list, type or select the destination IP address.

Destination

IPv4

Port (optional)



Tip: The **Destination | IPv4** field accepts IP addresses only, but you can filter the drop-down list by using any criteria that is included in the description.

Begin typing to filter the list, which populates automatically as you type with the results that match the string.

Source

IPv4

becky

Showing 1 of 64 x

10.31.100.12

Becky-PC

wired

Based on the type of device you select for the destination, the panel also opens the **Interface** field above the **Port** field.

Destination

IPv4

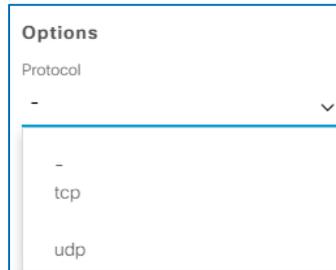
10.0.255.31

Interface (optional)

- v

Port (optional)

- b. Optionally, to indicate the interface on which you need to start the trace, in the **Interface** field, type the interface number.
 - c. Optionally, to indicate a specific port on the interface, in the **Port** field, type the port number.
4. Optionally, to indicate a specific protocol for Cisco DNA Center to use to establish the path trace connection, in the **Protocol** drop-down list, select **tcp** or **udp**.



5. To indicate whether the system runs the trace at 30 second intervals:
- To run the trace every 30 seconds, accept the default selection of **On**.
 - To run the trace once and evaluate the results, toggle the button to **Off**.



Note: The trace will continue to refresh as long as it is available on the page.

Rerunning a path trace at 30 second intervals can be helpful for ongoing troubleshooting, for example, when a network user is experiencing issues connecting to a specific device.

6. To indicate whether devices on the trace contain access control lists (ACLs) that match trace criteria:
- To see the ACL indicators, accept the default selection of **On**.
 - To not see ACL indicators, toggle the button to **Off**.



Important Note: When you include source or destination interfaces or ports, or protocol options in the path trace, the ACL trace results will include only those ACLs that apply based on the combination of items that you defined or selected.

That means that there can be one or more ACLs on the interface that do not appear in the path trace results.

7. To configure the path trace to collect additional metrics, under **Include Stats**:
 - To see device level CPU and memory statistics, select the **Device** check box.
 - To see ingress or egress interface drop statistics, select the **Interface** check box.



Tip: The quality of service statistics are available for routers only and return a subset of complete QoS data.

To ensure that you see the data that you want on any device, run the QoS command directly of that device.

Include Stats

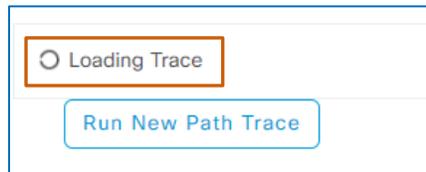
Device

Interface

QoS

8. To run the trace, click **Start**.

The panel closes automatically, and the system indicates that the trace is in progress.



When the path trace is complete, the system displays the topology results based on the settings in the trace configuration.

✓ 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.

10.30.100.27 (port: not specified) → 10.30.120.10 (port: not specified) [protocol: not specified] Jul 6, 2018 11:45 am

[Run New Path Trace](#)

To clear a path trace or run a subsequent one:

- Manually refresh the page by using the browser button.

...Application Use and Health?

You can review the health and metrics of applications that an endpoint is running under **Application Experience** in the **Client 360**.



Important Note: To collect application quantitative and qualitative metrics, a user must enable Cisco NetFlow data collection and apply the applicable telemetry profile by using Cisco DNA Center on the routers that are managing the traffic.

You also can use **Application Experience** to troubleshoot clients that onboard successfully but experience throughput or other issues based on an application’s qualitative metrics.

Application Experience *BETA* As of Jun 27, 2018 12:43 pm [Refresh](#)

Business Relevant Business Irrelevant Default

Application (3) [Export](#)

Filter EQ Find

Name	Host Name	Health		Usage		Average Throughput	Traffic Class	DSCP		Packet Loss (%)		Network Latency		Application Server Delay	
		Most Recent	Last 24 Hours	Bytes	Percentage (%)			Marking	Preservation	Max	Average	Max	Average	Max	Average
<input type="radio"/> http-local-net	us.archive.ubuntu.com	8	View	7.57 MB	100	105.8 Kbps	transactional-data	AF21	Yes	0.13	0.09	2 ms	2 ms	230 ms	180 ms
<input type="radio"/> dns	--	--	--	15.55 KB	0.2	10 bps	ops-admin-mgmt	DF	No	--	--	--	--	--	--
<input type="radio"/> ntp	--	--	--	11.58 KB	0.15	2 bps	ops-admin-mgmt	DF	No	--	--	--	--	--	--

Application Experience categorizes applications by using the network-based application recognition (NBAR) engine’s standard classifications:

- **Business Relevant**
Applications that are critical to business.
Examples: Microsoft Outlook and Cisco WebEx.
- **Business Irrelevant**
Applications that are not critical to business.
Examples: YouTube and Netflix.
- **Default**
Applications that the NBAR engine cannot identify in its classifications.

Application Experience *BETA* As of Jul 6, 2018 12:47 pm [Refresh](#)

Business Relevant Business Irrelevant Default NBAR category tabs

Application (3)

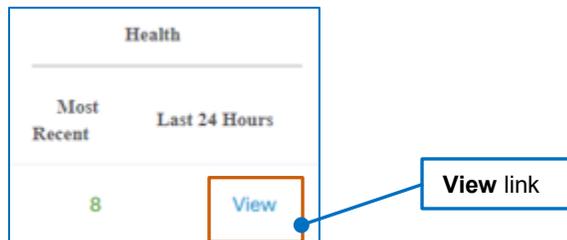
Filter

Application Experience determines the health score of an application by calculating packet loss and network latency. Under **Most Recent**, it presents the health score in color code for the most recent calculation.

Name	Host Name	Health	
		Most Recent	Last 24 Hours
○ outlook-web-service	outlook.live.com	3	View

To see application health details over the last 24 hours:

- Under **Health**, in the **Last 24 Hours** column, for the application of interest, point to **View**.



A pop-up window opens and displays the trend of the application’s health score for the previous 24 hours and is not interactive. The red dot indicates the current time.



Under **Usage**, **Bytes** indicates the number of bytes exchanged between each application and the endpoint.

Percentage indicates the amount of traffic each application is generating out of the total application traffic being exchanged with the endpoint.

Usage	
Bytes	Percentage (%)
341.04 KB	31
500.16 KB	46
328 B	0.03

Under **DSCP**, to indicate each application’s quality of service attributes, **Marking** indicates each application’s DSCP classification.

Preservation indicates whether the application setting that retains the application’s DSCP class as its traffic traverses the network is enabled.

DSCP	
Marking	Preservation
DF	No
DF	No
CS6	No

You also can see each application’s average throughput of traffic between the client and servers and its QoS traffic class.

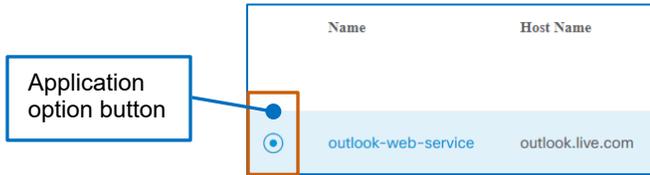
NetFlow data from routers provides the average and maximum percentages for:

- The packet loss that the client is experiencing.
- The latency occurring for the client on the network.
- The amount of time application server delay, which is, for Real-time Transport Protocol (RTP)-based applications, such as voice over IP or video streaming applications, the time that it takes the server to respond to a request from the application.

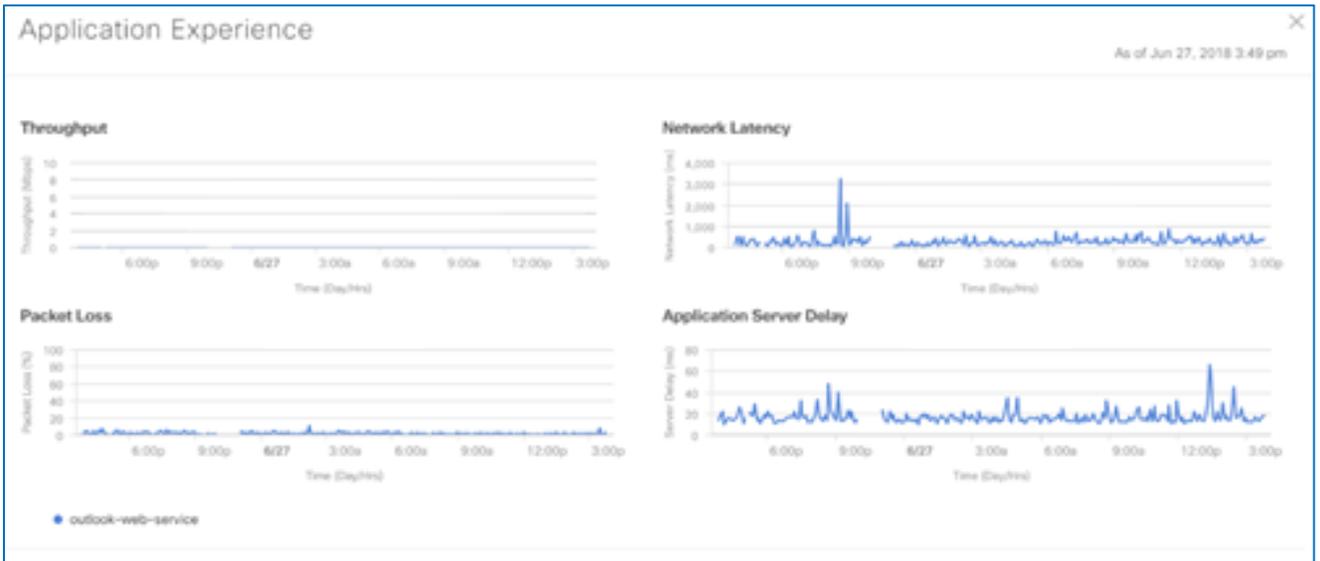
Average Throughput	Traffic Class	DSCP		Packet Loss (%)		Network Latency		Application Server Delay	
		Marking	Preservation	Max	Average	Max	Average	Max	Average
2.86 Mbps	bulk-data	DF	No	72	0.55	16 sec	1 sec	128 ms	0 ms
2.81 Kbps	bulk-data	DF	No	11	2	3 sec	230 ms	112 ms	16 ms

To see application throughput and qualitative metrics charts for a specific application:

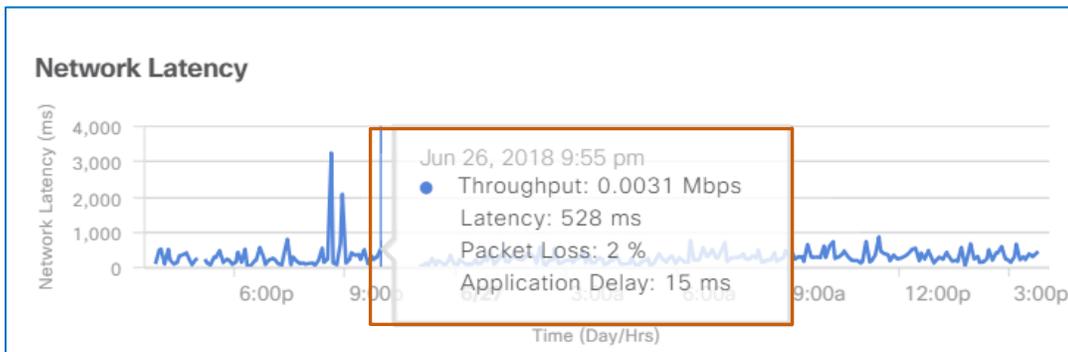
- Beside the application of interest, click the option button.



The **Application Experience** panel opens and overlays the page. The panel provides interactive charts with metrics' behavior over the 24-hour time period.



You can point to any chart to see all of the metrics for a specific time.



Application Experience also provides access to the **Application 360** page for each application that is running on the client.

Name	Host Name	Health	
		Most Recent	Last 24 Hours
outlook-web-service	outlook.live.com	2	View
ntp	--	--	--
dns	--	--	--

Links to open application based 360 pages

...More Metrics and Detailed Information?

The Detail Information Section

Under **Detail Information**, the **Client 360** page includes the following tabs with more device information and metrics.

- [Device Info](#)
Device attributes and connection information
- [Connectivity](#)
Charts that map the number of bytes that the device transmits (Tx) and receives (Rx), and DNS request and response times for the last 24 hours
- [RF](#)
Charts that illustrate the signal strength in relation to noise levels for the last 24 hours
- [iOS Analytics](#)
When the device connected to the endpoint is an Apple® device, additional metrics, connectivity, and dissociation details



Note: iOS Analytics tab availability depends on the combination of the versions of the Apple device's operating system, its hardware, and the Cisco access points.

Detail Information

Device Info Connectivity RF iOS Analytics

Information		Connection Information	
User Name	daphne.blake	Band	5 GHz
Host Name	Daphne-iPhone	Spatial Streams	2
MAC Address	A8:BE:27:36:70:11	Channel Width	20 MHz
IP Address	10.30.100.29	WMM	Supported
Device Type	iPhone 7	U-APSD	Disabled
Operating System	Cisco-Switch iOS11.4		
VLAN ID	100		

Reviewing Device Type and Connectivity Attributes

The **Device Info** tab lists device attributes and device connection information.

Detail Information

Device Info
Connectivity
RF

Information		Connection Information	
User Name	daphne.blake	Band	2.4 GHz
Host Name	Daphne-PC	Spatial Streams	0
MAC Address	B8:27:EB:CA:AA:88	Channel Width	20 MHz
IP Address	10.30.100.20	WMM	Supported
Device Type	Linux-Workstation	U-APSD	Disabled
Operating System	dhcpcd-6.7.1:Linux-4.9.53-v7+:armv7l:BCM2835		
VLAN ID	100		

Reviewing Transmit / Receive Metrics and DNS Request / Response Times

The **Connectivity** tab provides charts that illustrate the following over a 24-hour period.

- The bytes that the device transmits (Tx) and receives (Rx)
- The DNS request and the DNS query response times

Detail Information

Device Info
Connectivity
RF

Tx (bytes)

● Tx (bytes) Threshold: 10

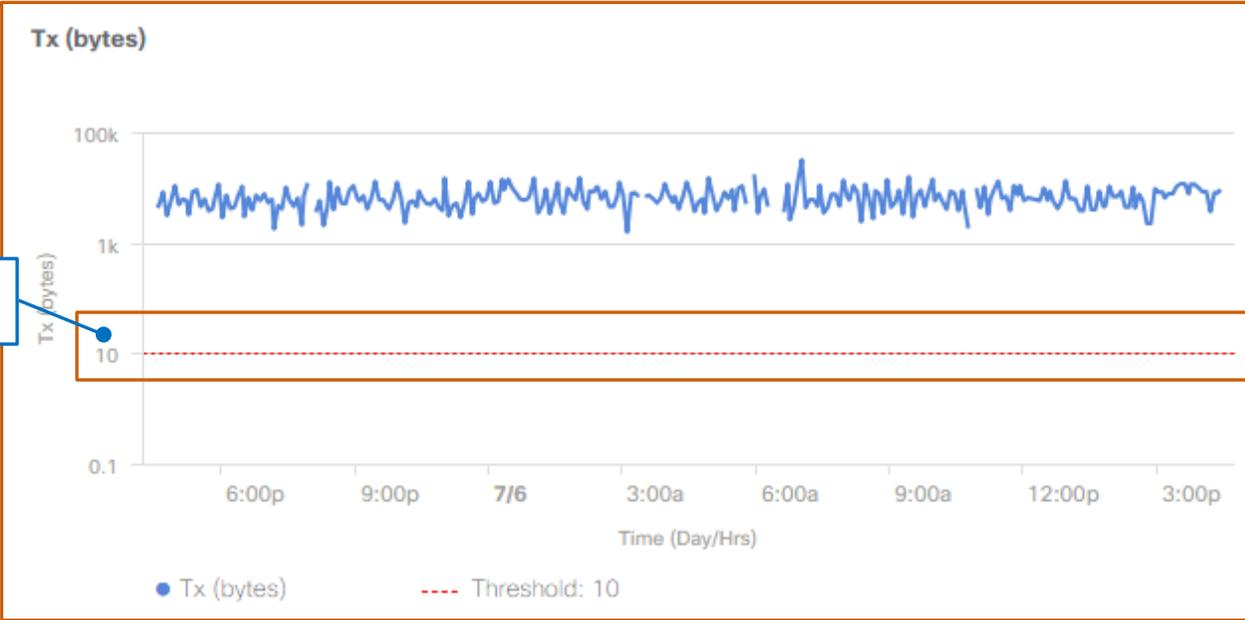
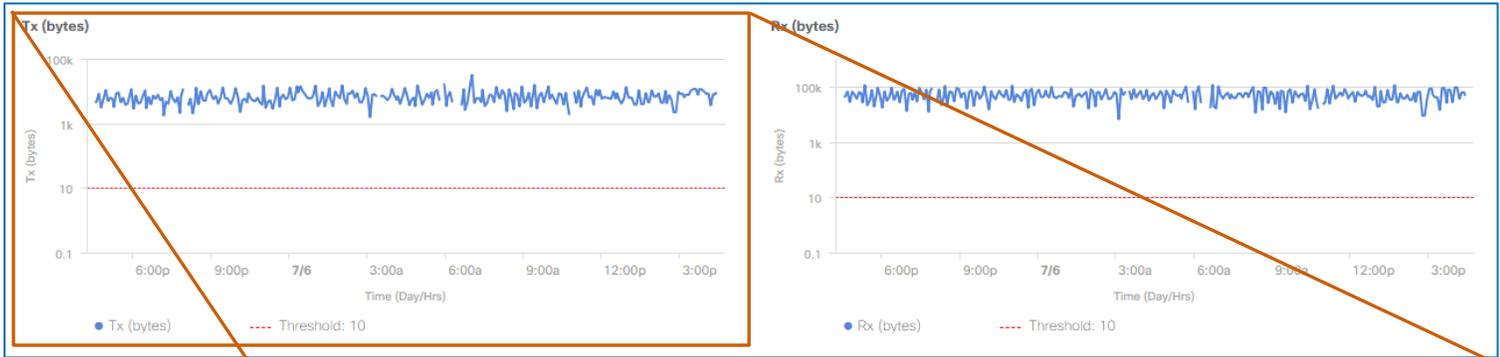
Rx (bytes)

● Rx (bytes) Threshold: 10

DNS Request and Response

● Threshold: 10 (Request) ● Response

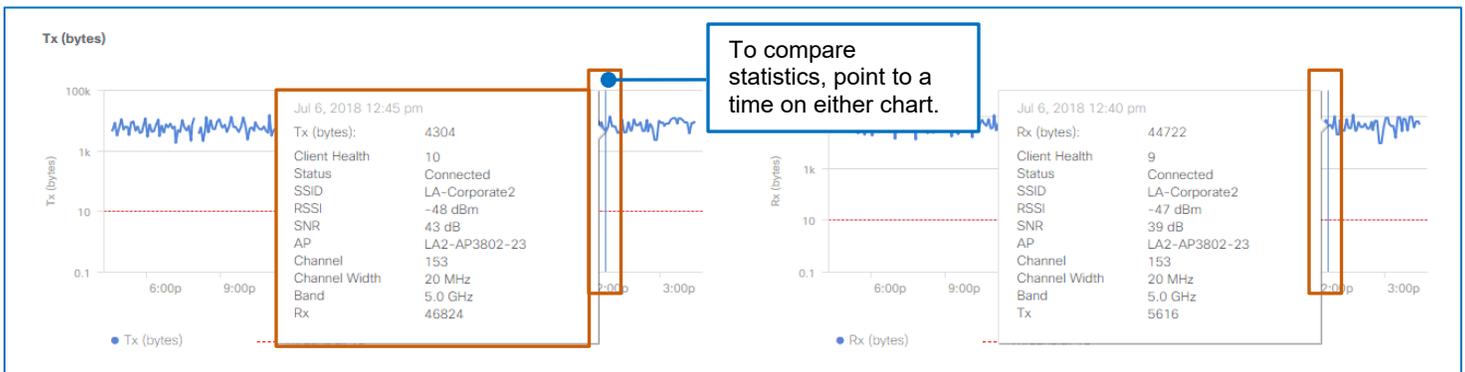
The **Tx (bytes)** and **Rx (bytes)** charts include a threshold line to emphasize when the endpoint is transmitting or receiving packets that are below acceptable levels.



The charts also provide a comparison tool so that you can evaluate the metrics for a specific time side-by-side.

To compare the transmit and receive data for a specific time:

- On either chart, point to the time of interest. You can move the pointer along the timeline to see varying metrics.



Reviewing Signal Strength and Signal to Noise Metrics

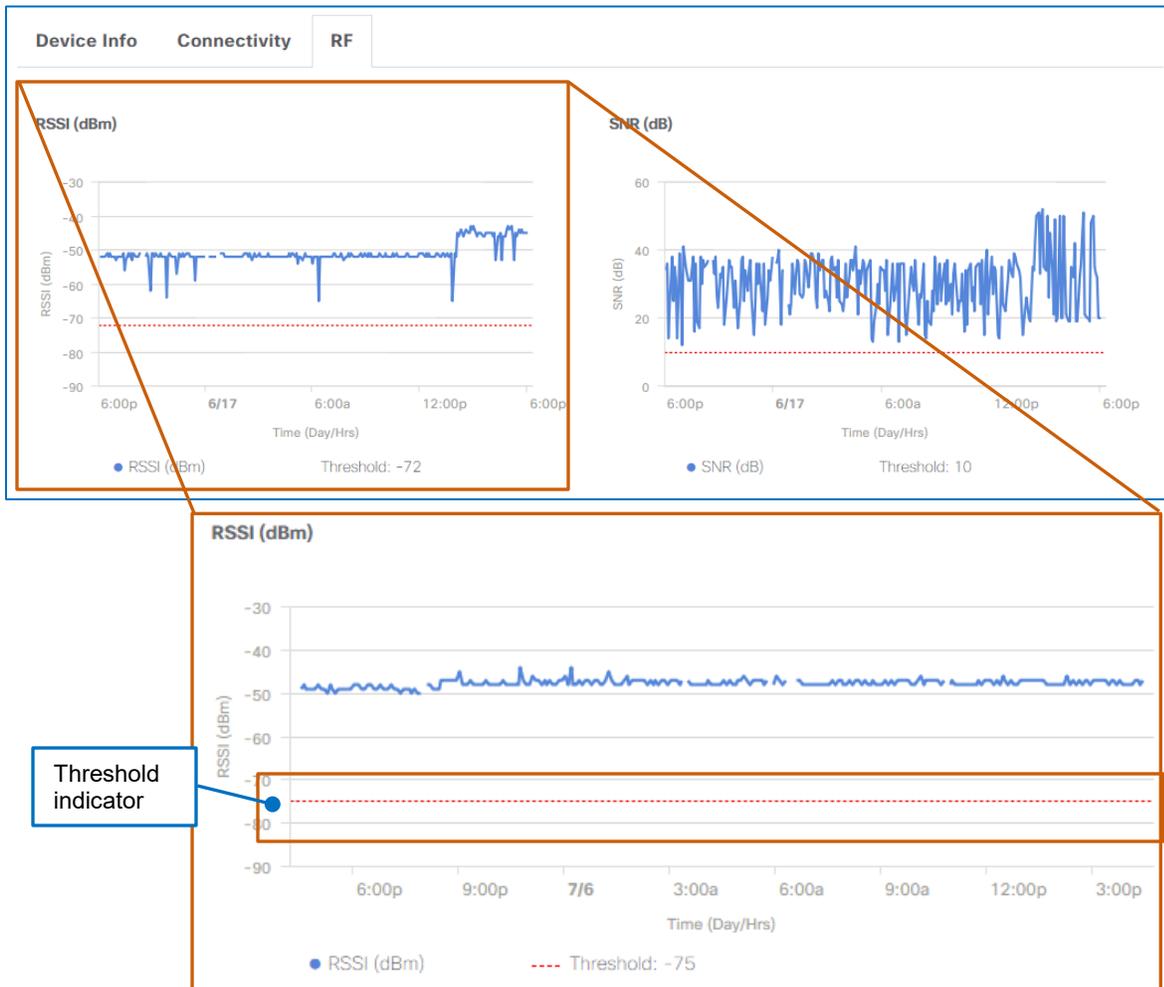
For wirelessly connected clients, the **RF** tab provides charts that illustrate the following measurements over a 24-hour period:

- The signal strength that the endpoint is receiving (**RSSI**)
- The signal-to-noise ratio (**SNR**) that the device is experiencing



This information helps you to determine if the client is experiencing poor RF conditions, such as high noise levels or issues with the radio channel utilization, width, or mode.

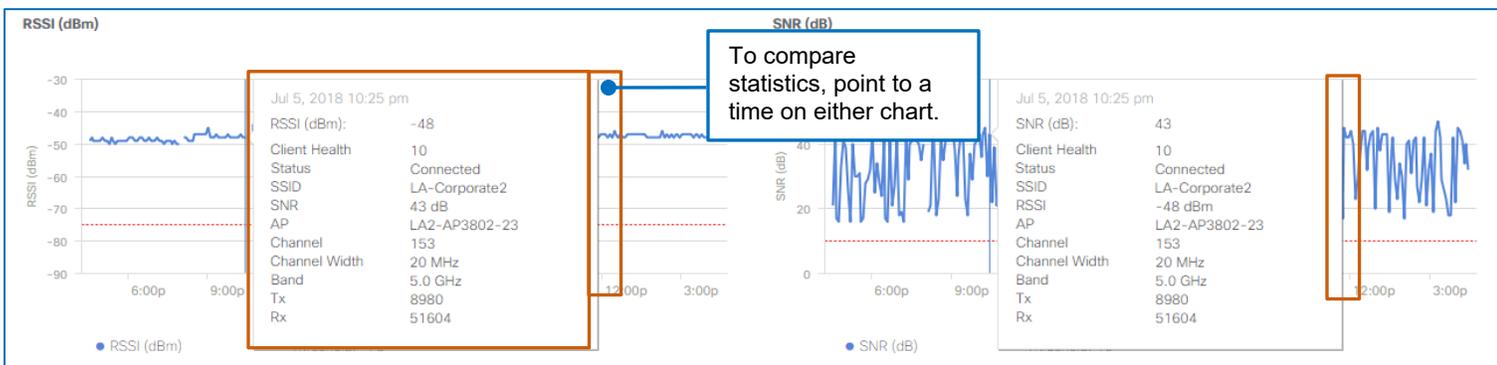
The RSSI and SNR charts include a threshold line so that you can evaluate when the endpoint is experiencing measurements that are below acceptable levels.



The charts also provide a comparison tool so that you can evaluate the metrics for a specific time side-by-side.

To compare the signal strength and signal-to-noise data for a specific time:

- On either chart, point to the time of interest. You can move the pointer along the timeline to see varying metrics.



Reviewing Apple® iOS Client Metrics and Connectivity to APs

When you select an endpoint to which an Apple® device is connected wirelessly, **Detail Information** includes the **iOS Analytics** tab, which displays.

- A list and the topology for the access point to which the device is connected and other available access points.
- A list of device disassociation actions.

iOS Analytics tab for Apple® wireless devices

BSSID	AP Name	Channel	RSSI (dBm)	Location
38:90:A5:CD:69:6F	LA1-AP3802-31	161	-58	Global/USA/LA/Level16

Time	Disassociation Reason	Disassociated AP	Session Duration	AP Location
Friday, July 27, 2018 9:56 AM	User triggered disassociation	LA1-AP3802-31		Level16
Friday, July 27, 2018 9:51 AM	Device idle	LA1-AP3802-31		Level16
Friday, July 27, 2018 9:46 AM	Device idle	LA1-AP3802-31		Level16
Friday, July 27, 2018 9:41 AM	User triggered disassociation	LA1-AP3802-31		Level16



Note: iOS Analytics tab availability depends on the combination of the versions of the Apple device's operating system, its hardware, and the Cisco access points.

Neighbor APs presents the access point list and topology.

In the topology below the list, a solid line indicates the device's active connection to an access point.

Dotted lines indicate access points to which the device also can connect.

Access point available to the device

Device's active connection to an access point

BSSID	AP Name	Channel	RSSI (dBm)	Location
38:90:A5:DF:3B:6F	LA2-AP3802-23	153	-58	Global/USA/SM/Level1
38:90:A5:DF:3B:60	LA2-AP3802-23	6	-39	Global/USA/SM/Level1

In general, when a client connects to an access point, it remains connected until there is reason to connect to a different access point or to disconnect. Devices join the nearest AP with the strongest signal based on the connection's RSSI and SNR measurements.

Client Disassociation Details lists:

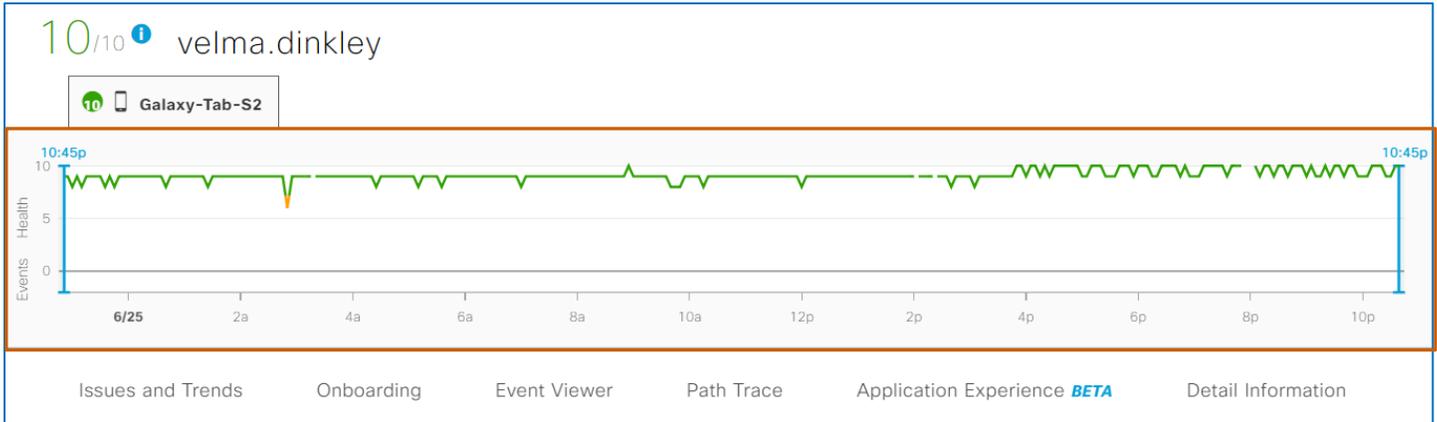
- Each time that the device disconnected from any access point and the reason that it disconnected.
- The access point to which the device was connected.
- The length of time that the device was connected.
- The location of the access point.

Client Disassociation Details (144)				
 Filter				
Time	Disassociation Reason	Disassociated AP	Session Duration	AP Location
Friday, July 27, 2018 9:56 AM	User triggered disassociation	LA1-AP3802-31		Level16
Friday, July 27, 2018 9:51 AM	Device idle	LA1-AP3802-31		Level16
Friday, July 27, 2018 9:46 AM	Device idle	LA1-AP3802-31		Level16

What Was an Endpoint Experiencing at a Certain Time?

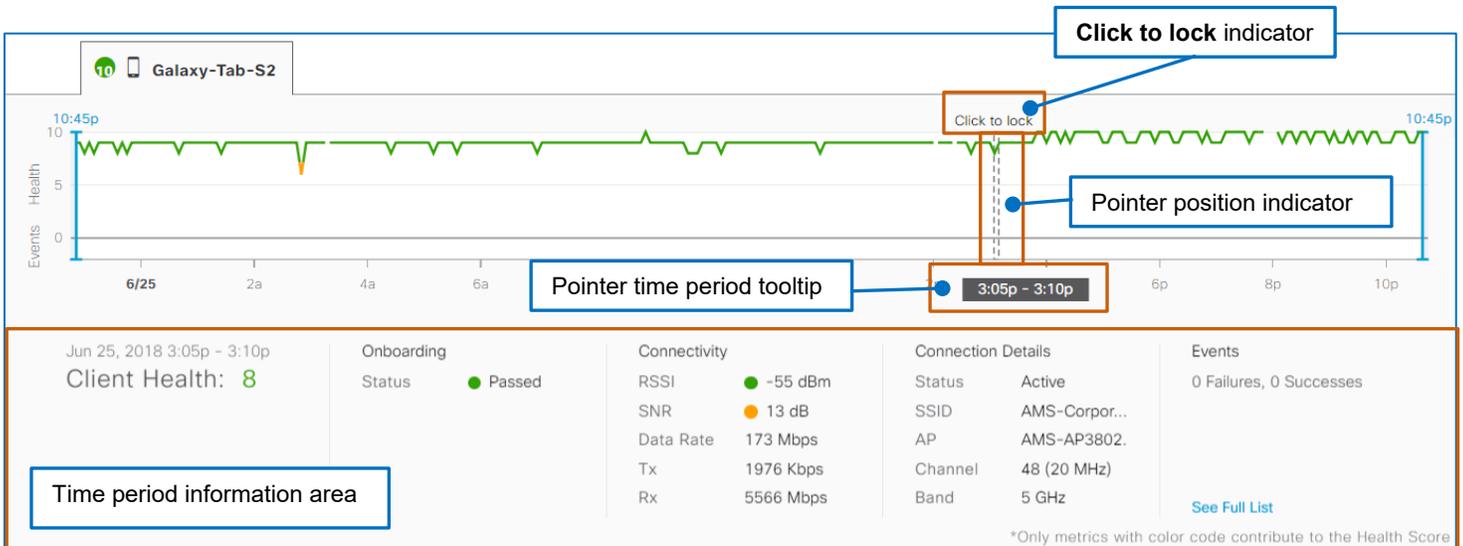
You can evaluate the health of an endpoint at a specific point in time by using the timeline.

This context supports issue troubleshooting, proactive responses to changing conditions, and helps to avoid similar problems in the future.



When you point the timeline:

- A pair of dotted lines indicate the pointer position on the timeline.
- The tooltip indicates the time period on which you are pointing.
- An information area below it expands with details about the state of the endpoint at that specific time.
- A **Click to lock** indicator opens, emphasizing the action that you can take to keep the information area visible when you move the pointer away from the timeline.



When you click a point on the timeline, the information area remains visible on the page when you move the pointer away from the timeline.

The time period information area provides the same information that the **Client 360** page does for the state of the endpoint at that time.



Note: Locking a timeline point does not affect the 24-hour time period that is applied to the overall page.

<p>Jul 03, 2018 4:30a - 4:35a</p> <p>Client Health: 8</p>	<p>Onboarding</p> <p>Status ● Passed</p>	<p>Connectivity</p> <p>RSSI ● -53 dBm</p> <p>SNR ● 13 dB</p> <p>Data Rate --</p> <p>Tx 2392 Kbps</p> <p>Rx 7567 Mbps</p>	<p>Connection Details</p> <p>Status Active</p> <p>SSID AMS-Corpor...</p> <p>AP AMS-AP3802.</p> <p>Channel 48 (20 MHz)</p> <p>Band 5 GHz</p>	<p>Events</p> <p>0 Failures, 0 Successes</p> <p>See Full List</p>
--	---	---	---	---

*Only metrics with color code contribute to the Health Score

The **Client Health** score is based only on those metrics that apply for the time period, which are listed under **Onboarding** and **Connectivity**. The metrics for which the score is reporting display color-code beside them.

<p>Jul 03, 2018 4:30a - 4:35a</p> <p>Client Health: 8</p>	<p>Onboarding</p> <p>Status ● Passed</p>	<p>Connectivity</p> <p>RSSI ● -53 dBm</p> <p>SNR ● 13 dB</p> <p>Data Rate --</p> <p>Tx 2392 Kbps</p> <p>Rx 7567 Mbps</p>
--	---	---

Onboarding metric contributing to health score

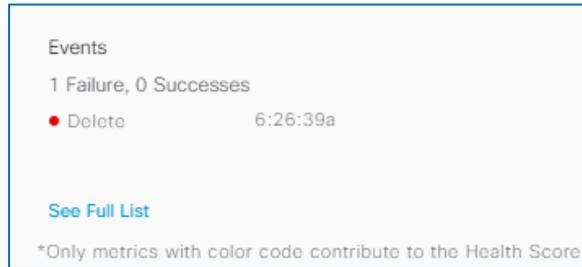
Connectivity metrics contributing to health score

Under **Events**, the information area indicates the number of successful or failed event that occurred at that time.

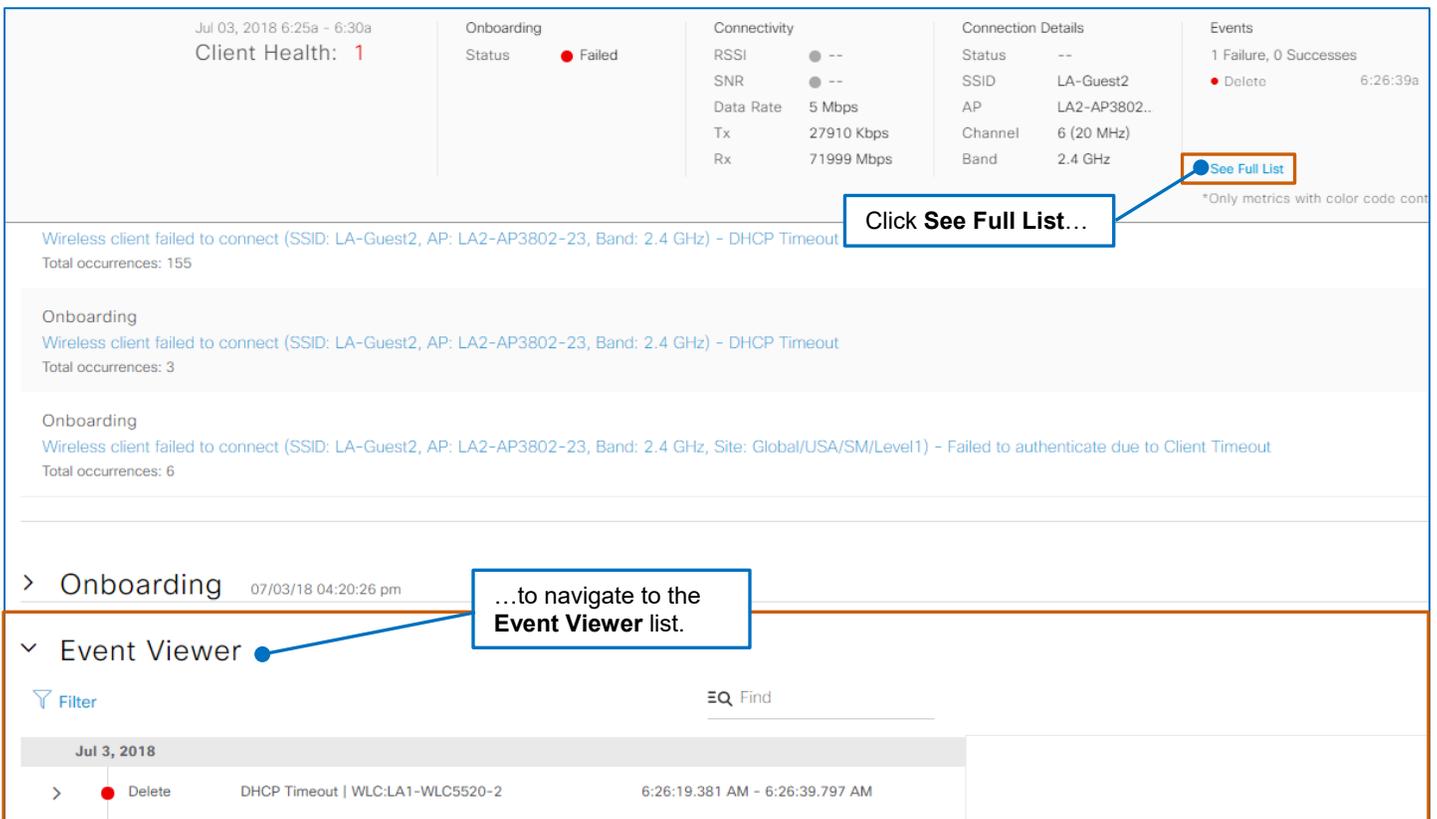
<p>Events</p> <p>1 Failure, 0 Successes</p> <p>● Delete 6:26:39a</p> <p>See Full List</p> <p style="font-size: small;">*Only metrics with color code contribute to the Health Score</p>
--

To see a complete list of events for the time period in the timeline:

- Below **Events**, click **See Full List**.



The link navigates to the **Event Viewer** section on the **Client 360** page.



Jul 03, 2018 6:25a - 6:30a
Client Health: 1

Onboarding
Status ● Failed

Connectivity
RSSI ● --
SNR ● --
Data Rate 5 Mbps
Tx 27910 Kbps
Rx 71999 Mbps

Connection Details
Status --
SSID LA-Guest2
AP LA2-AP3802..
Channel 6 (20 MHz)
Band 2.4 GHz

Events
1 Failure, 0 Successes
● Delete 6:26:39a

[See Full List](#)

*Only metrics with color code contribute to the Health Score

Wireless client failed to connect (SSID: LA-Guest2, AP: LA2-AP3802-23, Band: 2.4 GHz) - DHCP Timeout
Total occurrences: 155

Onboarding
Wireless client failed to connect (SSID: LA-Guest2, AP: LA2-AP3802-23, Band: 2.4 GHz) - DHCP Timeout
Total occurrences: 3

Onboarding
Wireless client failed to connect (SSID: LA-Guest2, AP: LA2-AP3802-23, Band: 2.4 GHz, Site: Global/USA/SM/Level1) - Failed to authenticate due to Client Timeout
Total occurrences: 6

> Onboarding 07/03/18 04:20:26 pm

...to navigate to the **Event Viewer** list.

Event Viewer

Filter Find

Jul 3, 2018

> ● Delete DHCP Timeout | WLC:LA1-WLC5520-2 6:26:19.381 AM - 6:26:39.797 AM

How Are All of a Single User's Clients Doing?

Get a Holistic View on the User-Based Client 360

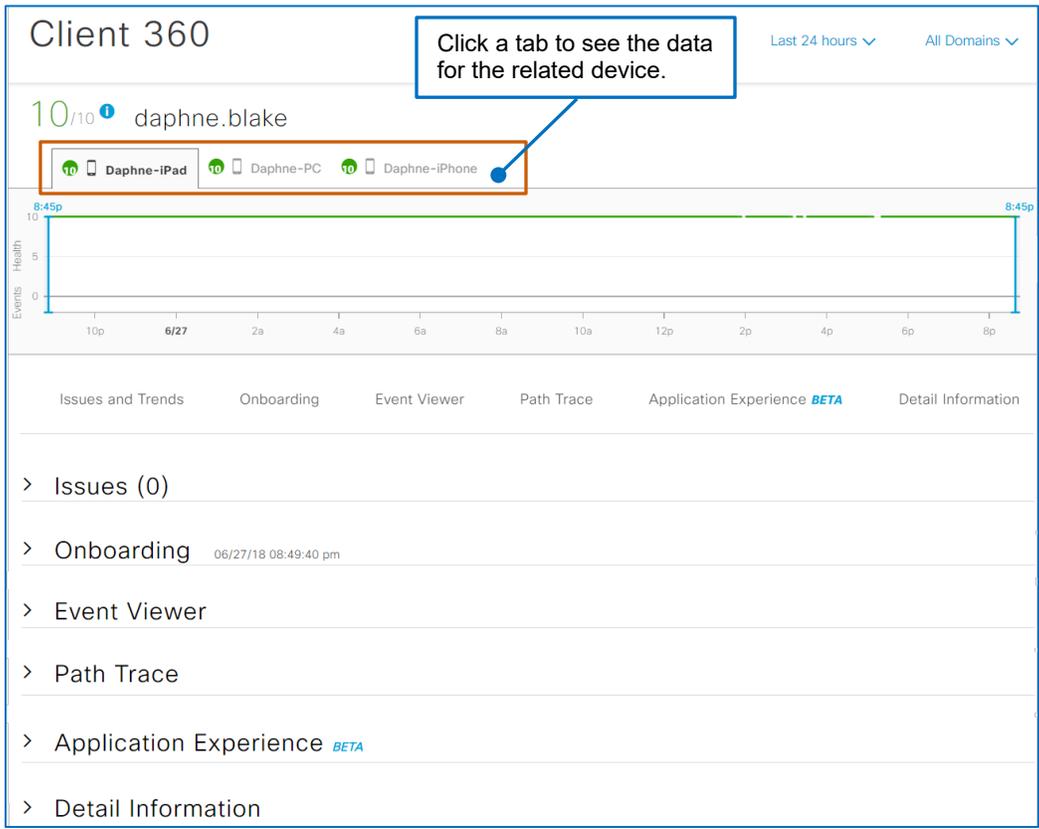
What Will I See?

The user-based **Client 360** page includes all of the devices that are associated with a single network user and provides the same information, features, and functions as [the Client 360 for a specific client endpoint](#).

The system collects end user data from WLCs, and, based on the system configuration, also can:

- In deployments with an Identify Services Engine (ISE), identify the device type.
- In deployments with Cisco Connected Mobile Experiences (CMX), the endpoint device's location.

The page provides tabs for each of the user's connected devices.

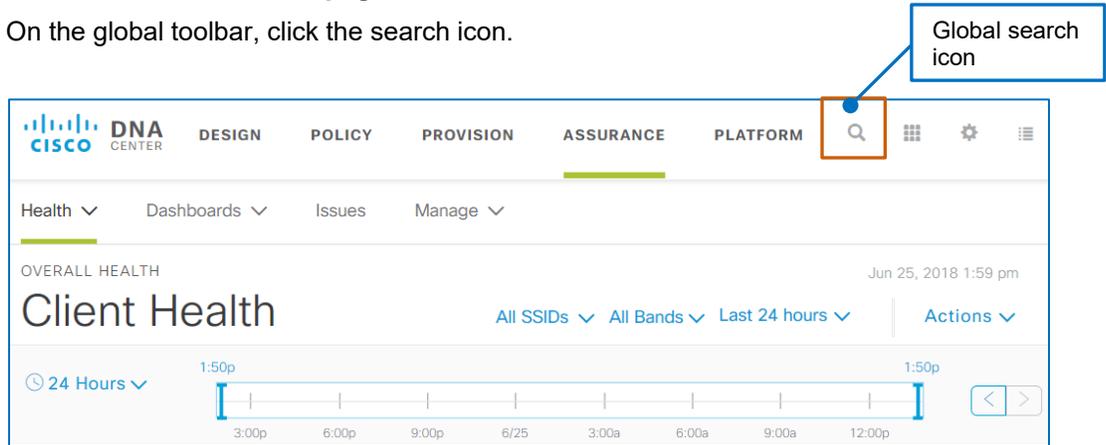


How Do I Open a User-Based Client 360 Page?

You open a user-based **Client 360** page by using the Cisco DNA Center global search feature.

To open a user-based **Client 360** page:

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

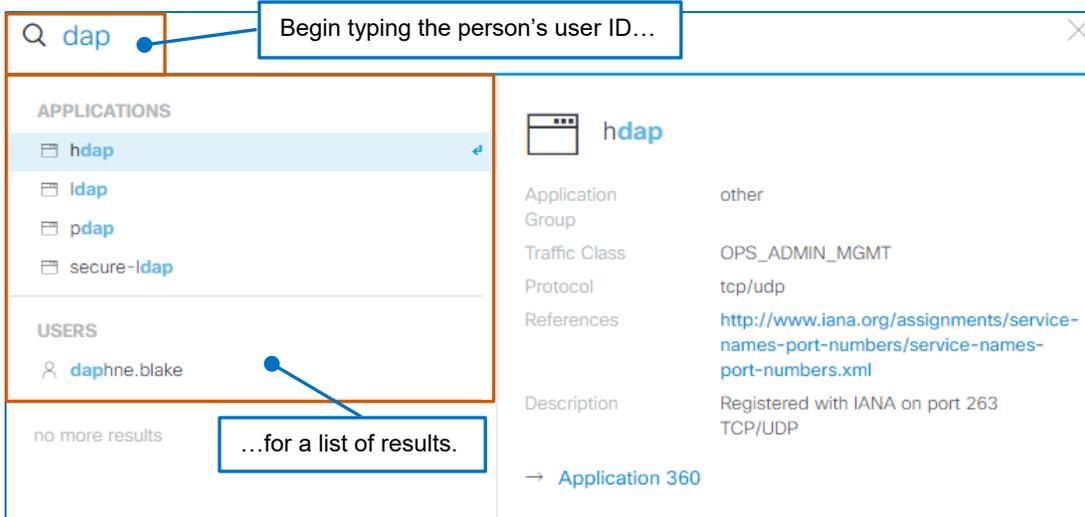


The **Search** dialog box opens.

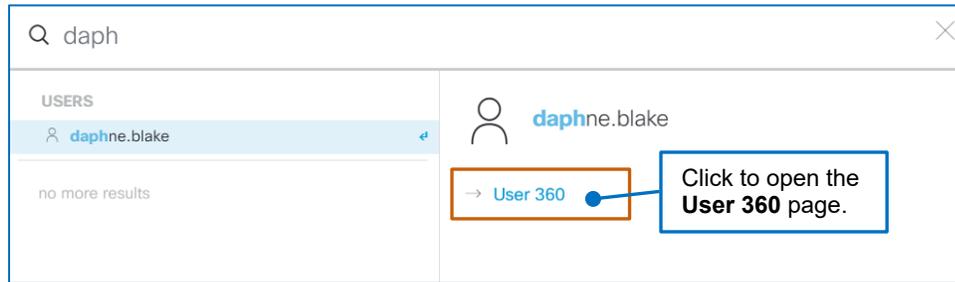


2. In the **Search** field, begin typing the user ID of the person whose client devices you need to see.

A list of results matching the characters that you type begins populating automatically.



- To access the **User 360** link, in the results list, under **Users**, select the person's user ID. The dialog box provides the **User 360** link to the right of the search results.



- To open the user-based **Client 360** page, click **User 360**. The **Client 360** page with tabs for each of the user's devices opens.

Client 360 Last 24 hours ▾ All Domains ▾

10/10 daphne.blake

Daphne-iPad Daphne-PC Daphne-iPhone

7:20a 7:20a

Events Health

Issues and Trends Onboarding Event Viewer Path Trace Application Experience *BETA* Detail Information

Issues (9)

- Onboarding: Wireless client took a long time to connect (SSID: LA-Corporate2, AP: LA2-AP3802-23, Band: 2.4 GHz) - Excessive time for Authentication due to AAA server or Network delays. Total occurrences: 18. 06/25 7:18am
- Application: Network Latency for Application 'outlook-web-service' is Above the Threshold Value of 412ms. Total occurrences: 86. 06/25 3:15am

Onboarding 06/25/18 07:21:58 am

AAA DHCP

Daphne-PC LA-Corporate2 LA2-AP3802-23 LA1-WLC5520-2

Event Viewer

Filter EQ Find

Jun 25, 2018

Re-Authentication 4 way Key Timeout | WLC:LA1-W... 7:45:28.220 AM - 7:45:32.452 AM Select an event to view details

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

Application Experience *BETA* As of Jun 25, 2018 7:21 am Refresh

Detail Information

Device Info		Connectivity		RF	
Information					
User Name	daphne.blake	Connection Information			
Host Name	Daphne-PC	Band	2.4 GHz		
MAC Address	BB:27:EB:CA:AA:88	Spatial Streams	0		
IP Address	10.30.100.20	Channel Width	20 MHz		
Device Type	Linux-Workstation	WMM	Supported		
Operating System	dhcpd-6.7.1:Linux-4.9.53-v7+:armv7l:BCM2835	U-APSD	Disabled		
VLAN ID	100				

Watch It Happen in Cisco DNA Center

Video

This step-by-step instructional video demonstrates all of the steps that you can take to complete the task.

And, it includes the context that you need for a deeper understanding of system processes, best practices, and considerations for optimal system usage and results.



[Evaluating a System User's Printer Connection \(8:00\)](#)

Watch as we use the Assurance Path Trace tool to map the complete path that traffic is taking from its source IP address to its destination.

The results provide insight into ongoing or potential issues that might be affecting network traffic.

How To Watch a Video

To watch a video:

- Click the video's title link, which opens an MP4 file.

Based on your system and configuration, you might need to start the video manually.



Note: Video download and streaming times can vary.

Want More?

Find 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.](#)

Find Training

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

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

Contact Us About This Training

[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.