



# Network Health Monitoring Overview

---

Cisco Prime Infrastructure 3.2

Job Aid

## Copyright Page

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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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

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

*Network Health Monitoring Overview Job Aid*

© Copyright 2017 Cisco Systems, Inc. All rights reserved.

## Contents

|   |           |
|---|-----------|
| <b>Basics.....</b>  | <b>1</b>  |
| Overview.....   | 1         |
| Skills .....  | 2         |
| Basic .....   | 2         |
| Proficient .....  | 2         |
| Expert.....   | 2         |
| Terms.....  | 3         |
| Business Critical Applications .....                                      | 3         |
| Parent and Child Sites.....   | 3         |
| Sites or Locations.....   | 3         |
| <b>Monitoring Key Network Device and Application Health Metrics .....</b> | <b>4</b>  |
| Network Health Dashboard Overview .....                                   | 4         |
| Introduction .....  | 4         |
| Viewing Wired or Wireless Metrics .....                                   | 5         |
| Navigating the Dashboard.....   | 6         |
| <i>Layout Overview .....</i>  | <i>6</i>  |
| <i>Metric Health Status Color Codes .....</i>                             | <i>10</i> |
| <i>Changing the Page Layout.....</i>                                      | <i>11</i> |
| <i>Applying Time Reporting Filters .....</i>                              | <i>12</i> |
| <i>Applying Location, Metrics, and Health Status Filters .....</i>        | <i>13</i> |
| <i>Navigating Among Location Groups.....</i>                              | <i>14</i> |
| Map Navigation Overview.....  | 15        |
| The Map View .....  | 15        |
| Unmapped Locations .....  | 18        |
| Accessing Metrics Overview.....   | 19        |
| Additional Navigation Features .....                                      | 28        |
| Opening Metrics Dashboards.....   | 28        |
| Monitoring Service Health .....   | 31        |
| Reviewing Key Graphs .....  | 34        |
| Preparing Network Health Reporting.....                                   | 35        |
| Organizing Location Groups.....   | 35        |
| <i>Location Groups Overview.....</i>                                      | <i>35</i> |
| <i>How Location Group Organization Affects Views.....</i>                 | <i>37</i> |
| Configuring Health Rules .....  | 40        |
| Service Health Metrics Reporting.....                                     | 42        |
| Infrastructure Metrics Reporting .....                                    | 43        |
| Wireless Health Metrics Reporting .....                                   | 44        |
| Indicating Business Critical Applications .....                           | 45        |



|  |           |
|--|-----------|
| Identifying Subnets for Site Level Service Health Reporting .....    | 47        |
| <b>Monitoring Key Performance Indicators (KPIs).....</b>             | <b>48</b> |
| Performance Graphs .....   | 48        |
| Navigating Performance Graphs .....                                  | 50        |
| Managing Graph Data Elements .....                                   | 50        |
| Changing Graph Timelines.....  | 51        |
| Changing Graph Layouts .....   | 52        |
| Managing Performance Graphs .....                                    | 55        |
| Seeing the Data That You Need .....                                  | 55        |
| Adding or Removing Device or Interface Graphs to Tabs .....          | 56        |
| Adding or Removing Tabs.....   | 58        |
| Adding Multiple Metrics to Graphs.....                               | 61        |
| Monitoring Devices or Interfaces Reporting the Highest Metrics ..... | 62        |
| Exporting or Printing Graph Data .....                               | 63        |
| Opening Graph Tabs in Separate Windows .....                         | 64        |
| Reviewing Device or Interface Details or Taking Actions.....         | 65        |
| <b>Links.....</b>  | <b>68</b> |
| To Product Information .....   | 68        |
| To Training .....  | 68        |
| To Contact Us.....   | 68        |

# Basics

## Overview

Monitoring overall network health helps you to avoid or mitigate potential operational disruptions or downtime.

In addition to the dashboards and dashlets that you can use to monitor various targeted aspects of the network, you can monitor and evaluate the overall health of the entire enterprise network efficiently by using these key monitoring tools:

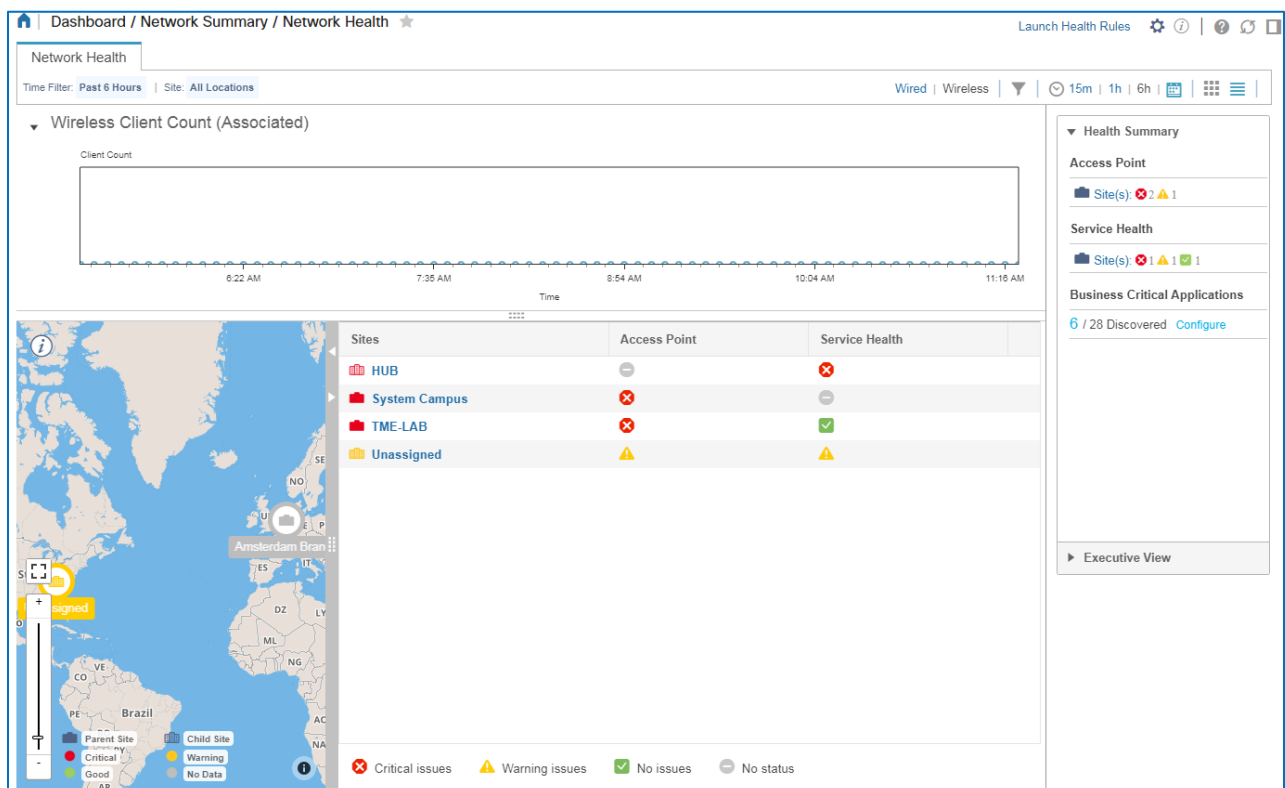
### ❖ The Network Health dashboard

Which provides summary views of all of the sites that comprise the enterprise network, and reports on the health of:

- ◆ Network routers, switches, and access points, including whether the devices' key performance indicators (KPIs) are within or outside of normal ranges.
- ◆ Business critical application metrics, such as application response or client experience.

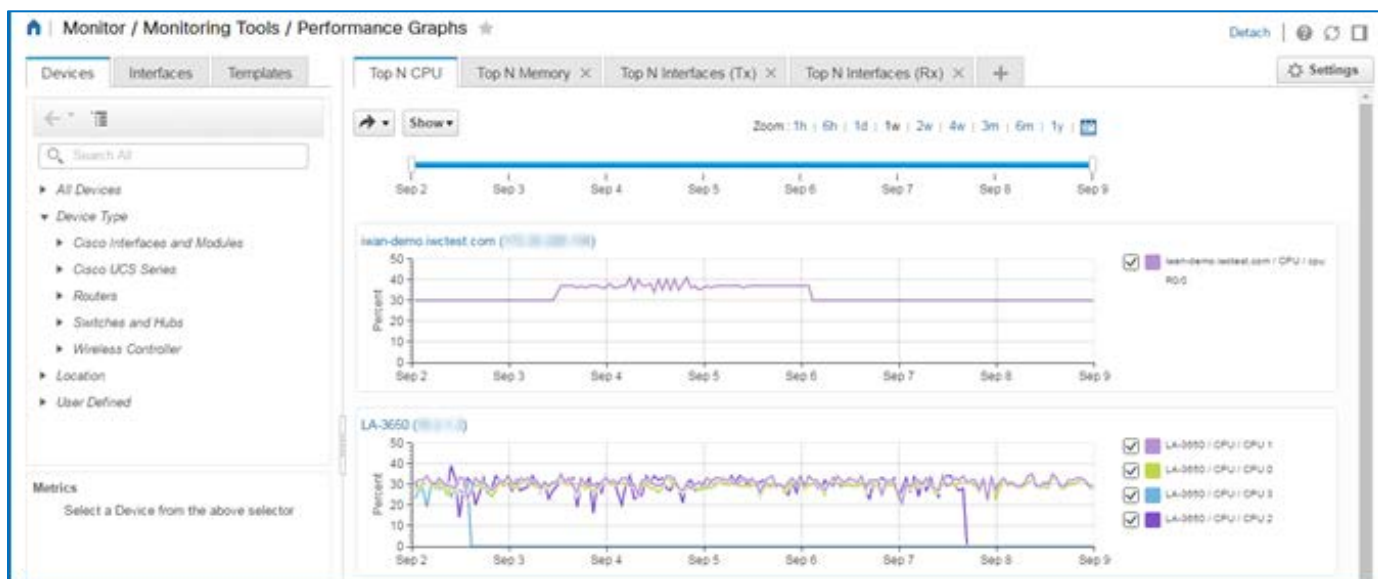


**Note:** Prime Infrastructure requires an Assurance license to support the Network Health dashboard and functionality.



### ❖ Performance graphs

Which report device and interface metrics over time for the KPIs that you indicate.



When you see that a device is reporting KPIs outside of normal ranges on the **Network Health** dashboard, you can investigate the issue further by using performance graphs.

For example, if you see that a device indicates critical health issues, you can review a performance graph for the component with the metrics of interest to compare their behaviors. You also can display alarms and configuration changes to see if either of those activities correlate to time periods in which metrics are exceeding metric thresholds.

This job aid introduces you to the types of information that you can see when using the **Network Health** dashboard and performance graphs to monitor overall network health.

## Skills

To monitor overall network health, you need the following experience.

### Basic

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

### Proficient

- ❖ Prime Infrastructure user interface and navigation
- ❖ OSI model
- ❖ Network hardware design and concepts
- ❖ Networking concepts

### Expert

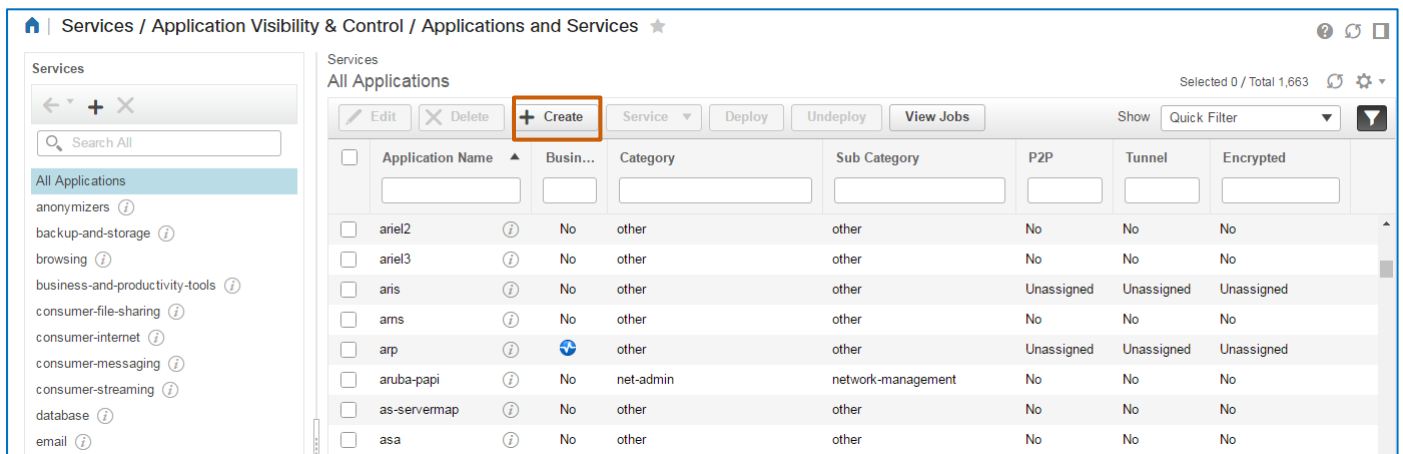
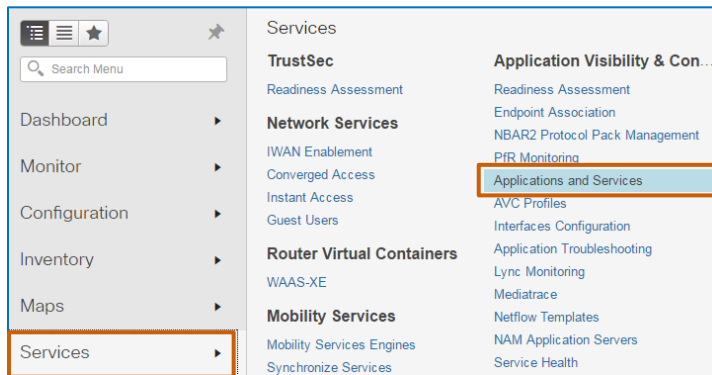
- ❖ Correlation of metric, alarm, and configuration data

## Terms

### Business Critical Applications

Those applications that system users or administrators have identified in Prime Infrastructure as critical to business operations

System users or administrators indicate business critical applications when adding applications and services on the **Services | Application Visibility & Control | Applications and Services** page.



### Parent and Child Sites

When organizing locations groups, users can add child locations, also referred to as sites, under a parent site, so that the devices associated with those locations are organized logically to reflect how the enterprise manages device groups.

When you are investigating issues, it can be helpful to recognize location dependencies to avoid or mitigate potential network disruptions or downtime across larger regions.

### Sites or Locations

In Prime Infrastructure, the terms site and location are used interchangeably.

# Monitoring Key Network Device and Application Health Metrics

## Network Health Dashboard Overview

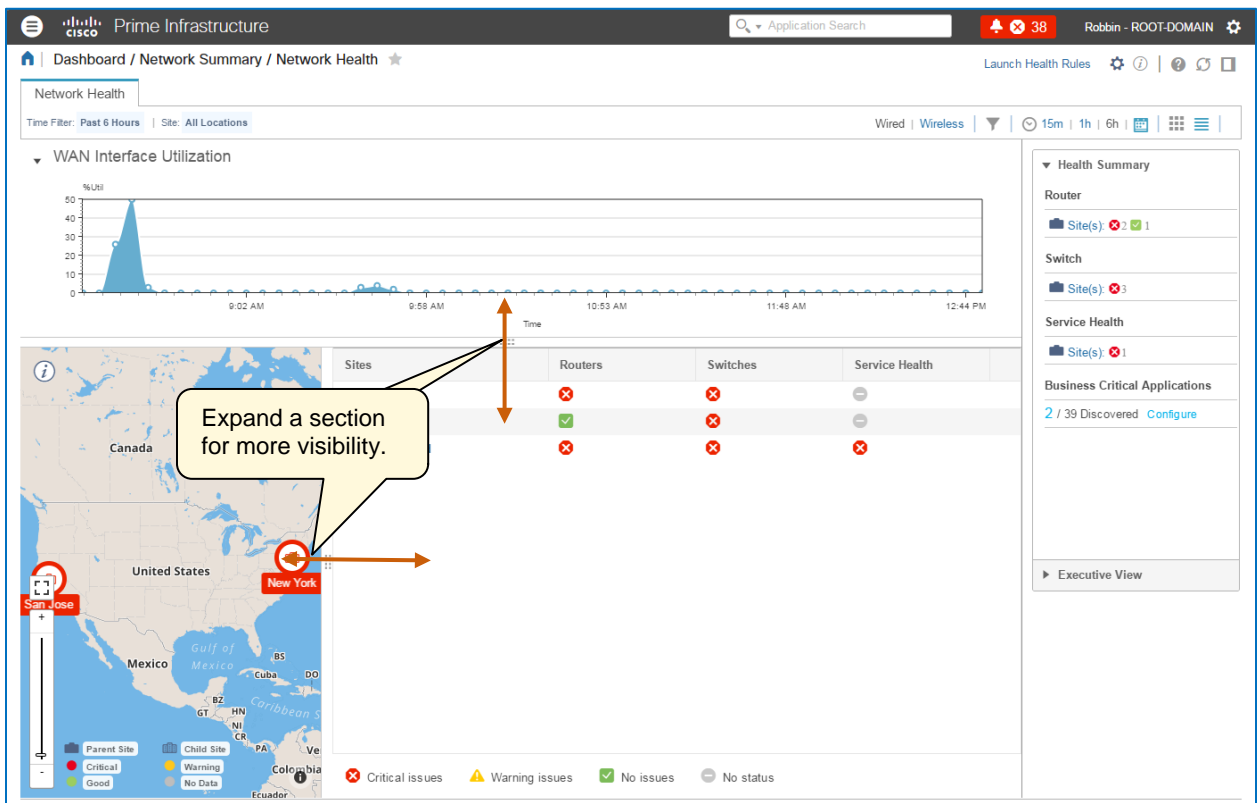
### Introduction

You can monitor key device and application health proactively on the **Network Health** dashboard. By using color-coded indicators, the dashboard alerts you to sites and devices that are reporting KPI values that are outside of operational ranges.

When monitoring network health proactively, you can investigate potential issues and take corrective actions, as needed, to avoid or mitigate problems.

[Based on the health rules](#) and device location groups, referred to as sites, that system users configure, the **Network Health** dashboard reports the health metrics for router, switch, and access point devices and interfaces.

The flexible layout that includes a map and readily accessible views at the site and device levels.

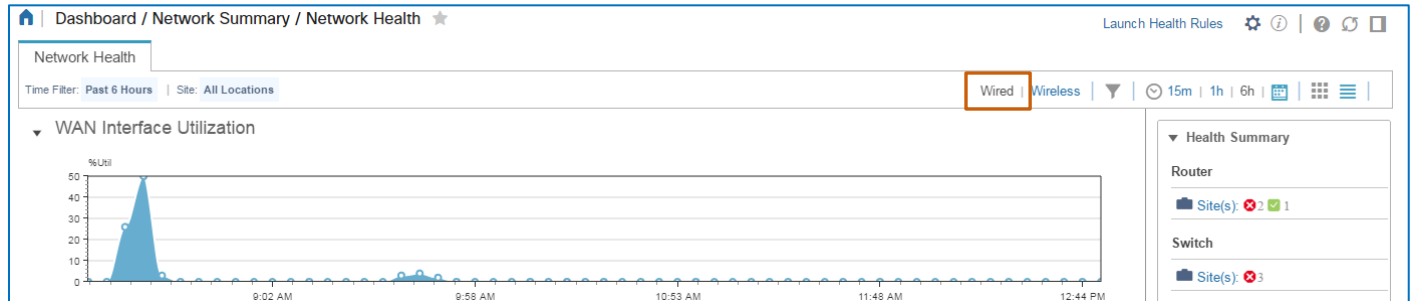




## Viewing Wired or Wireless Metrics

To see router and switch metrics:

- ❖ On the toolbar, click **Wired**.

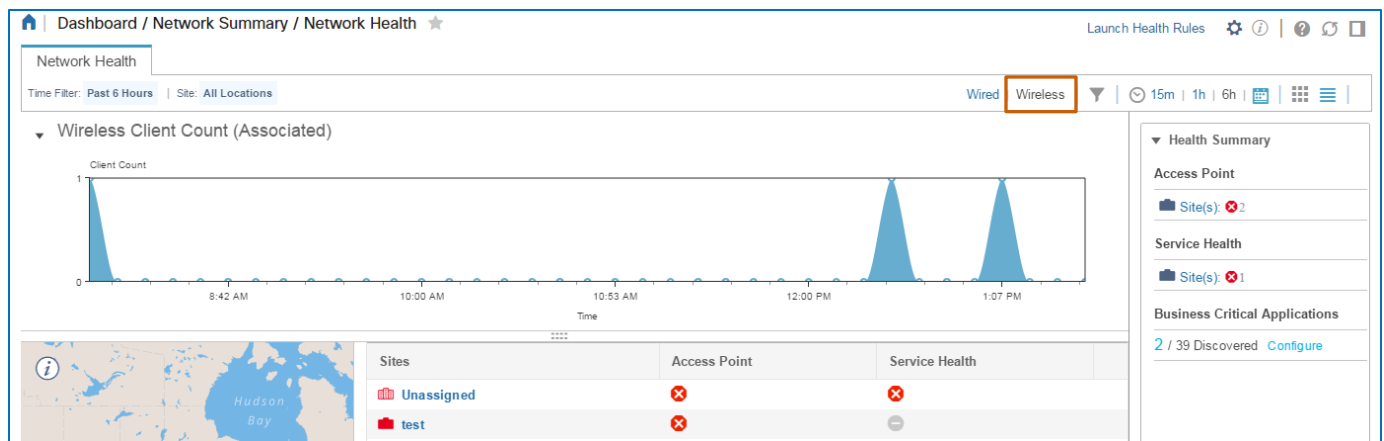


At a site level, router and switch metrics include:

- ❖ Site availability.
- ❖ CPU usage.
- ❖ Memory usage.
- ❖ Device temperature.
- ❖ Interface availability.
- ❖ Interface usage.
- ❖ Quality of service (QoS) for the classes of traffic that system users can indicate.

To see access points:

- ❖ On the toolbar, click **Wireless**.



At a site level, access point metrics include:

- ❖ Channel usage.
- ❖ Noise.
- ❖ Interference.
- ❖ Interface usage.

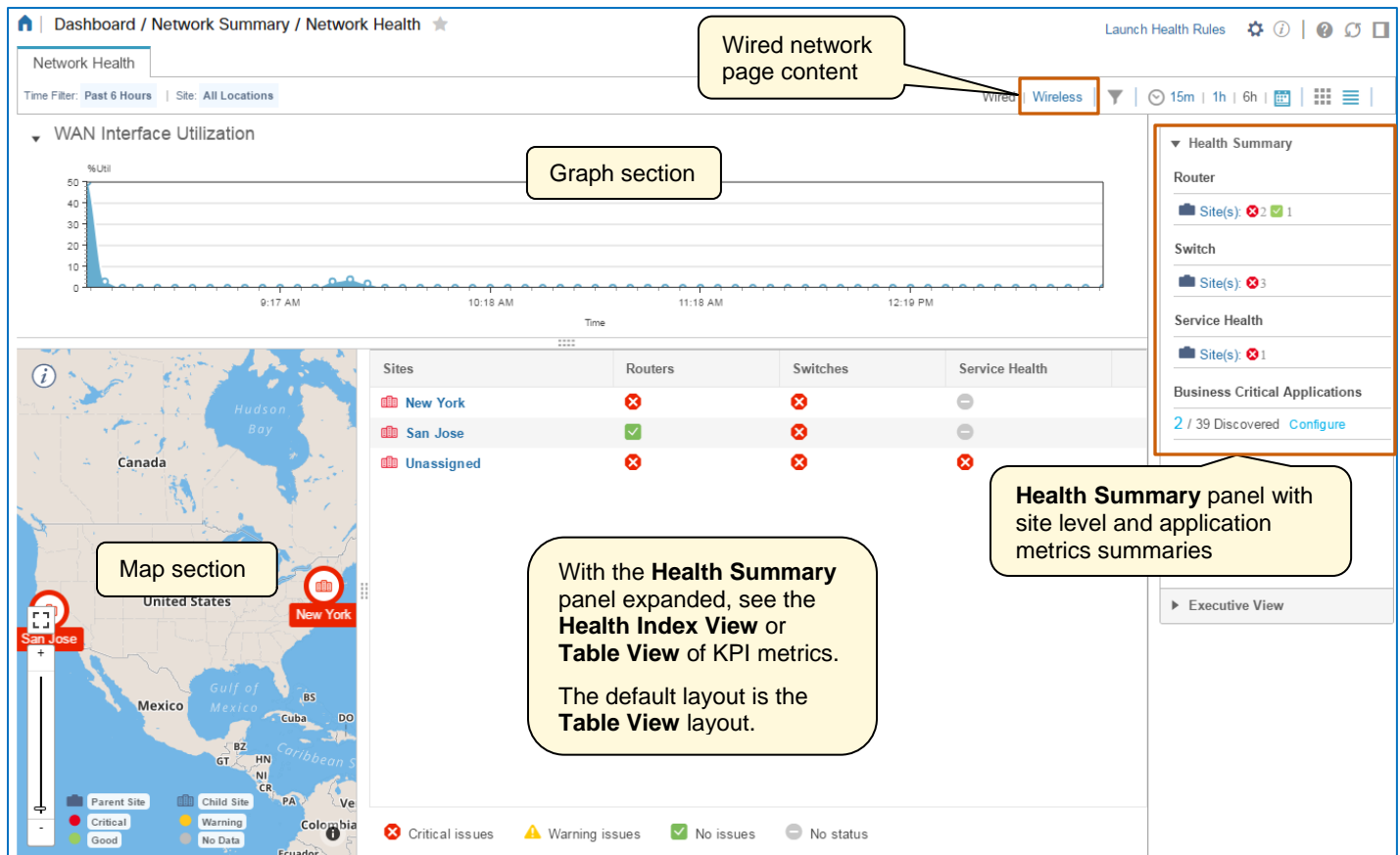
- ❖ The number of clients currently connected to access points at the site.

## Navigating the Dashboard

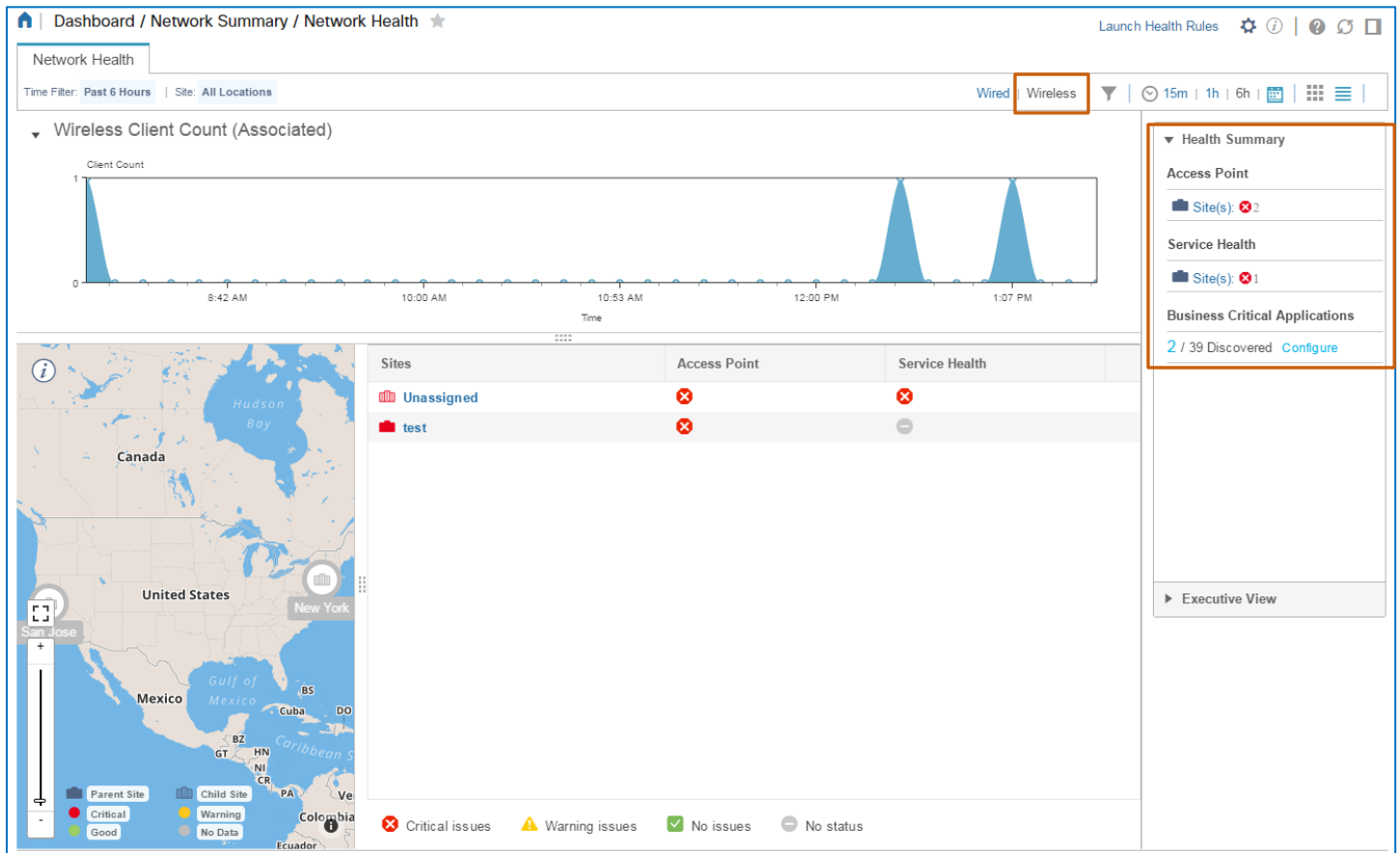
### Layout Overview

The **Network Health** page layout is the same in the wired and wireless views. You select whether to monitor the wired or wireless network based on your monitoring tasks.

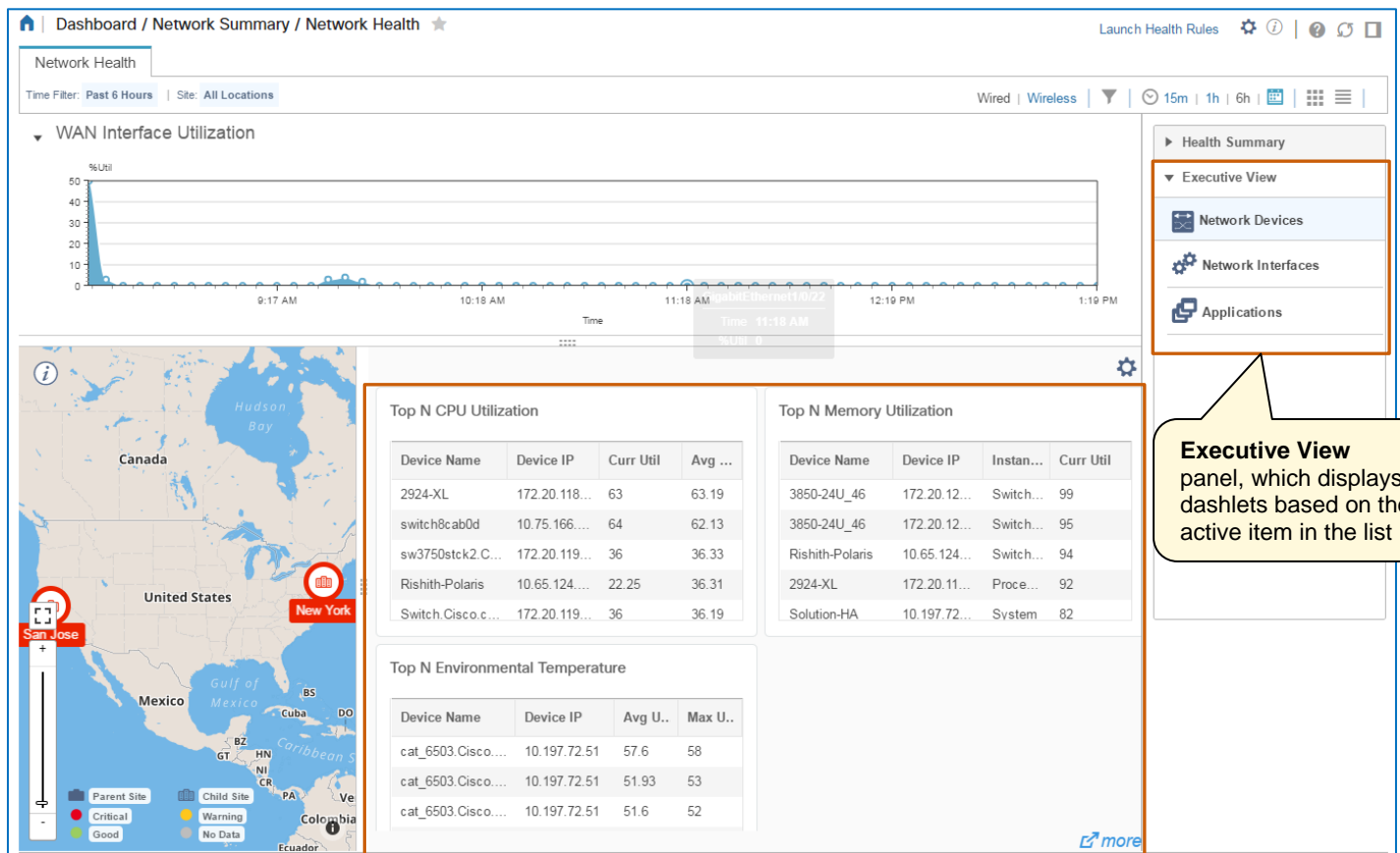
The following screenshot illustrates available wired network information when the **Health Summary** panel is active.



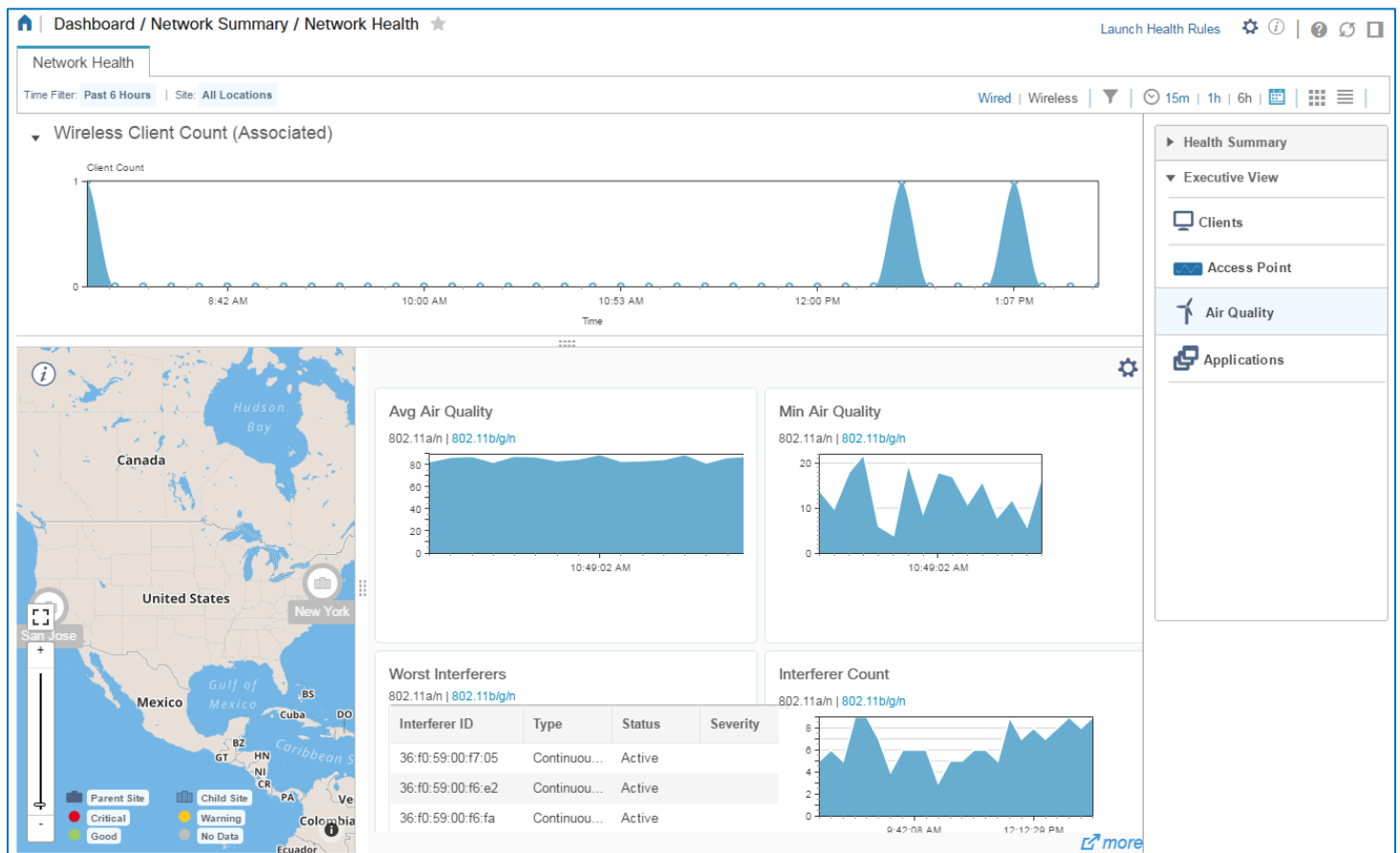
The following screenshot illustrates the available wireless network information when the **Health Summary** panel is active.



The following screenshot illustrates the available wired network information when the **Executive View** panel is active and an option selected in the list.



The following screenshot illustrates the available wireless network information when the **Executive View** panel is active and an option selected in the list.



## Metric Health Status Color Codes

In all views, the system applies color codes to alert you to areas that might require attention. The health and experience levels that the system reports are defined by the threshold values in the health rules.

### Good

The associated metric is reporting below the warning threshold value.

### Warning

The associated metric is reporting above the warning and below the critical threshold values.

### Critical

The associated metric is reporting above the critical threshold value.

### No data

The system is not reporting data on the metric.



**Note:** In most cases, you can configure health rules so that the page reports the data that you need to see.

To review how to configure health rules, [refer to the \*\*Configuring Health Rules\*\* topic](#).

## Changing the Page Layout

The system default selections are that the graph appear at the bottom of the window and the panel containing the **Health Summary** and **Executive View** opens automatically.

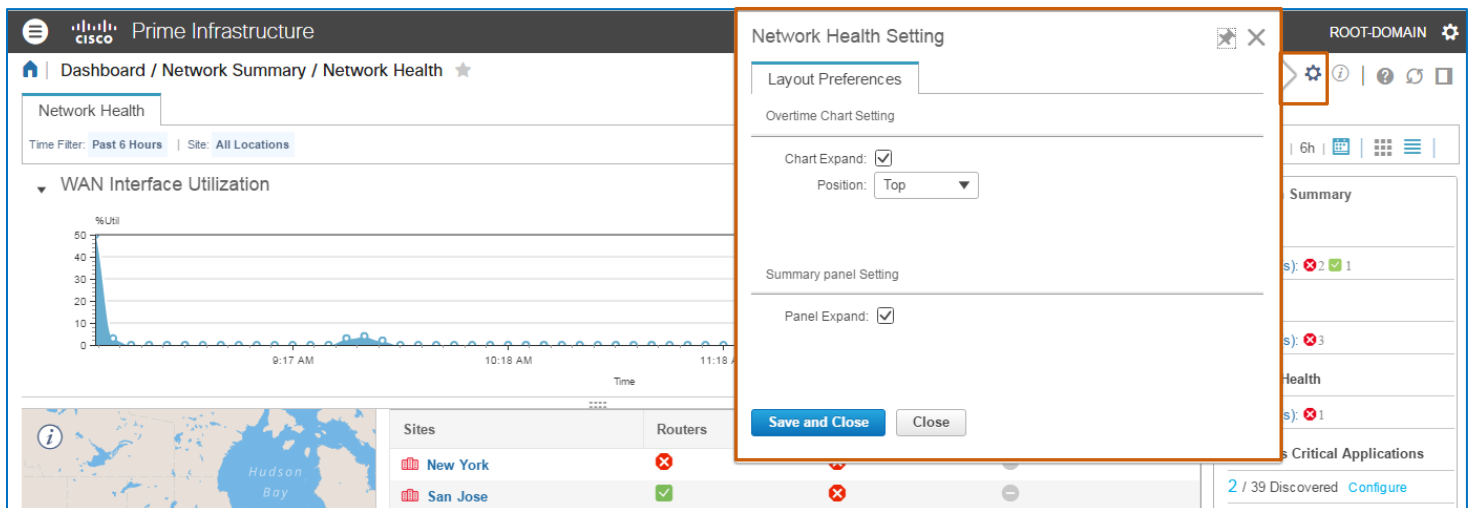
You can control panel visibility and the graph location based on your preferences.

### To make changes:

- ❖ Below the application banner, point to the **Setting** icon.

The **Network Health Setting** pop-up window opens. The default settings include:

- ❖ The graph section visible and at the top of the page on page entry.
- ❖ The **Health Summary / Executive View** panel expanded on the right side of the page.

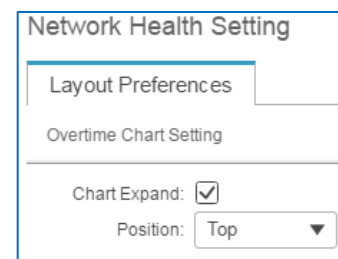


### To set the graph section to a collapsed state when you open the page:

- ❖ Clear the **Chart Expand** check box, and then click **Save and Close**.

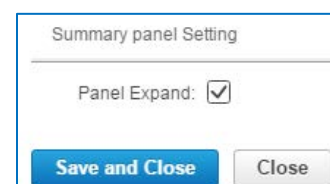
### To set the graph section to appear at the bottom of the page:

- ❖ In the **Position** drop-down list, select **Bottom**, and then click **Save and Close**.



### To set the panel to a collapsed state when you open the page:

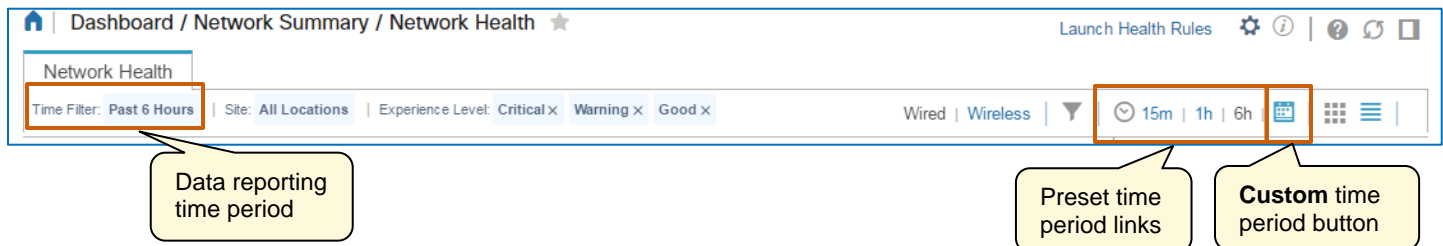
- ❖ Clear the **Panel Expand** check box, and then click **Save and Close**.



## Applying Time Reporting Filters

The dashboard reports data for the past hour by default, and indicates the data reporting time period below the **Network Health** tab.

You can change the reporting time period by using the tools on the toolbar.

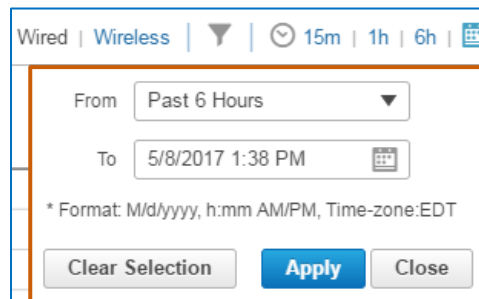


### To select a preset time period:

- ❖ On the toolbar, click a time period link.

### To configure a custom time period:

1. On the toolbar, click the **Custom** time period button.
2. In the pop-up window, select a time period, click **Apply**, and then click **Close**.



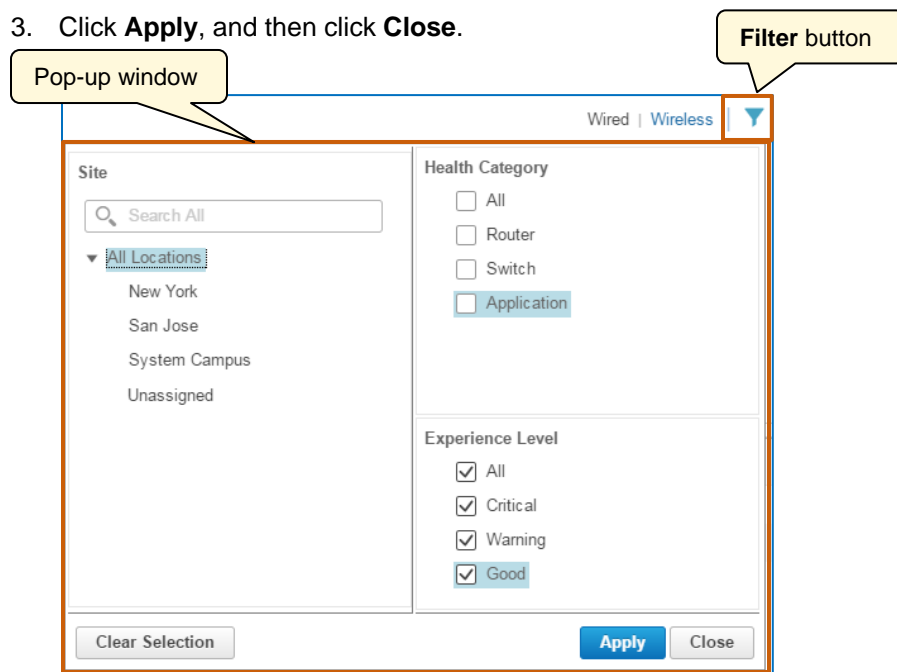


## Applying Location, Metrics, and Health Status Filters

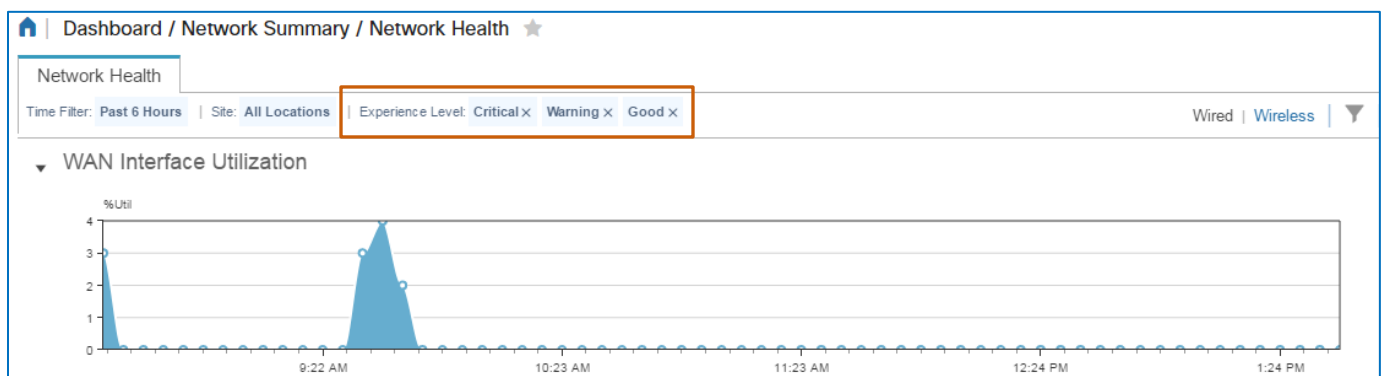
You can configure the location metrics, including device type or application metrics, and health statuses that you want to see on the dashboard.

**To configure the location, device type or application metrics, or health statuses:**

1. On the toolbar, click **Filter**.
2. In the pop-up window:
  - ❖ To select a location, expand the applicable locations headings, and then select the location entry.
  - ❖ To select all or specific device types or applications, under **Health Category**, select the applicable check boxes.
  - ❖ To select all or specific health statuses, under **Experience Level**, select the applicable check boxes.
3. Click **Apply**, and then click **Close**.



The page refreshes automatically and displays the data based on the filters that you selected.



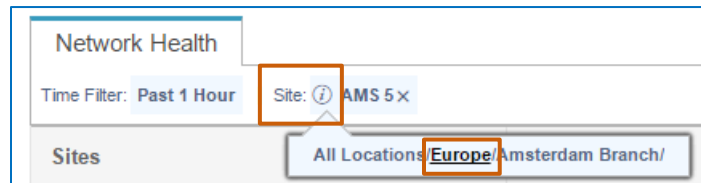
## Navigating Among Location Groups

When you click location name links in lists or pop-up windows, the system opens the next level of site detail. For example, you can navigate from a site with several locations to a single location, then to a building at the location, and then to a floor in the building.

When you navigate to a more detailed site view, you can return to higher level views by using the breadcrumbs available by using the **Show Parent** button.

### To return to a higher level view on a page:

- ❖ On the toolbar, beside **Site**, click the **Show Parent** button, and then, in the list of breadcrumb links, click the level of view that you want.



**Important Note:** The top level folder and each subgroup folder must have its geographical coordinates configured in order to appear in map or health index views.

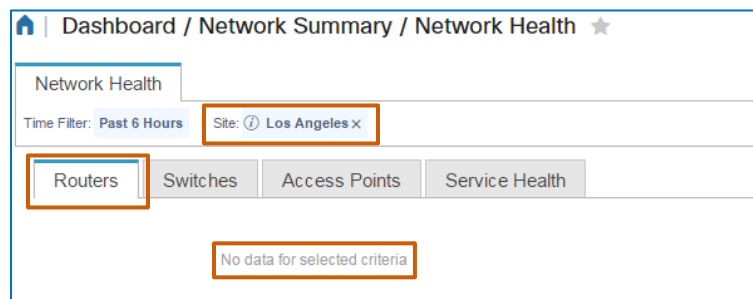
If coordinates are not configured for a view that users select in the breadcrumb links, they will not see those sites in the view.

For more information, [refer to the How Location Group Organization Affects Views topic](#).



**Important Note:** The information that you see on the page depend on the site that is active on the page.

If, at the particular parent or child level location level, the location does not have assigned devices of the type indicated, the system prompts that no data is applicable based on filter criteria.



## Map Navigation Overview

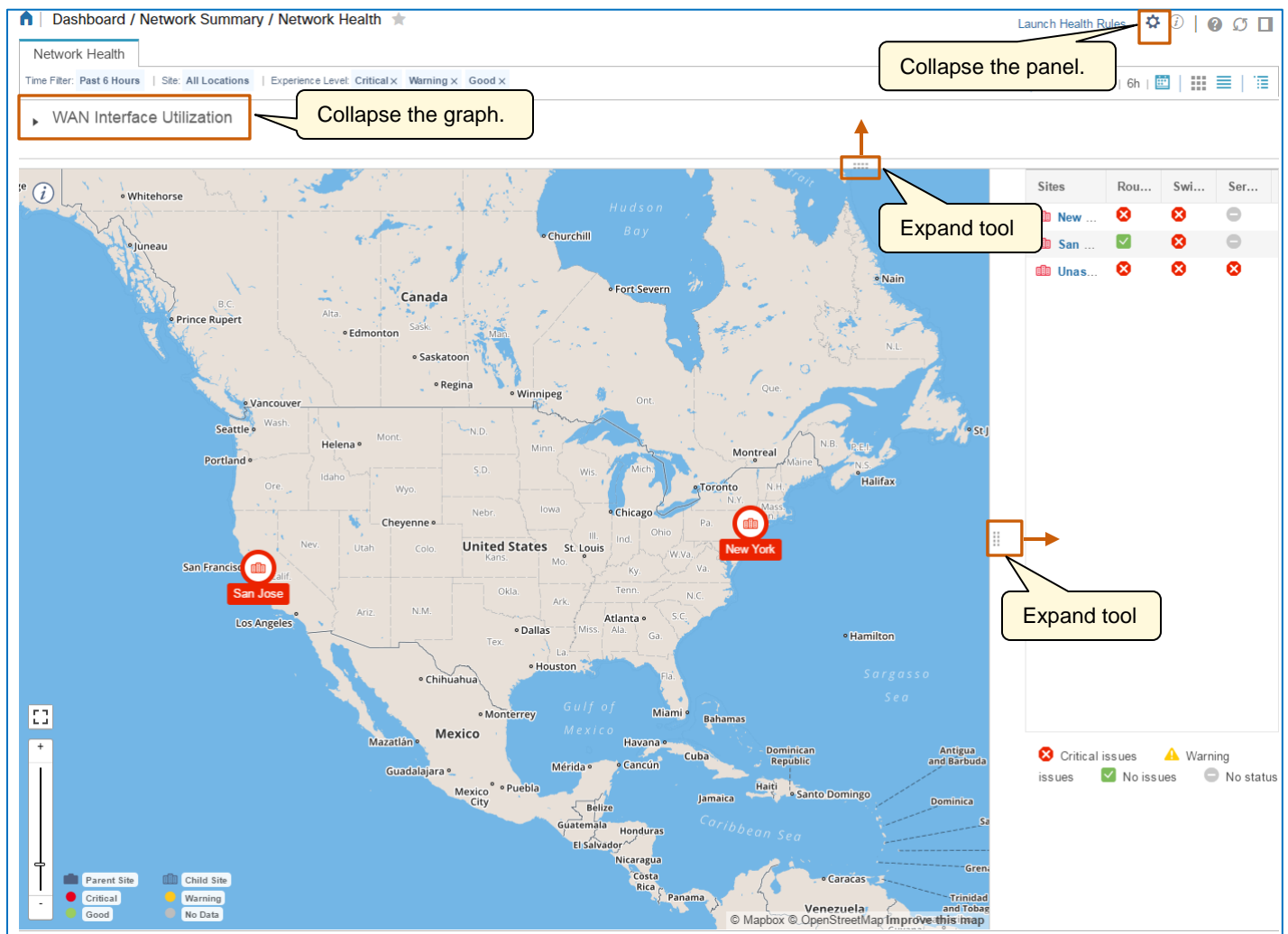
### The Map View

Network Health provides a map that you can use to monitor the network in its geographical context. This way, you can identify problem areas and their network relationships to determine the effects of issues more efficiently.



**Tip:** For optimal visibility, you can:

- ❖ Expand the map area.
- ❖ Collapse the graph area.
- ❖ Close the **Health Summary / Executive View** panel.
- ❖ Maximize the browser window.



For the location or group of locations that have geographical coordinates, the map displays icons for those groups and their associated devices, which system users configure.



**Important Note:** Map behavior, including zoom levels, and the sites that you see, are based on how location groups are organized and whether their geographical coordinates are configured.

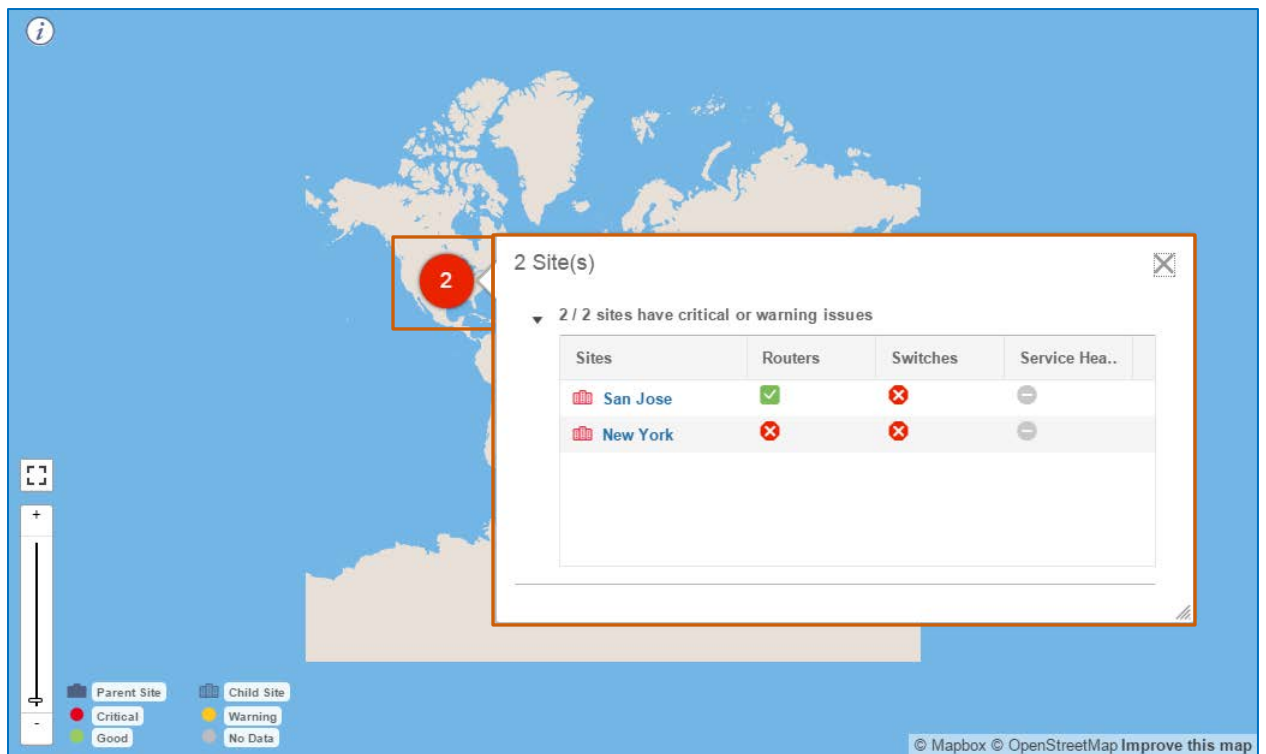
For more information and key concepts on organizing and configuring location groups, which define parent and child sites and map behaviors, [refer to the Organizing Location Groups topic](#).

Depending on the zoom level of the map, the map presents location groups that are geographically close together in a single icon. In broader views, the icon indicates the number of sites that the icon represents.

When you zoom in to a specific area, the icons update to represent each site individually.

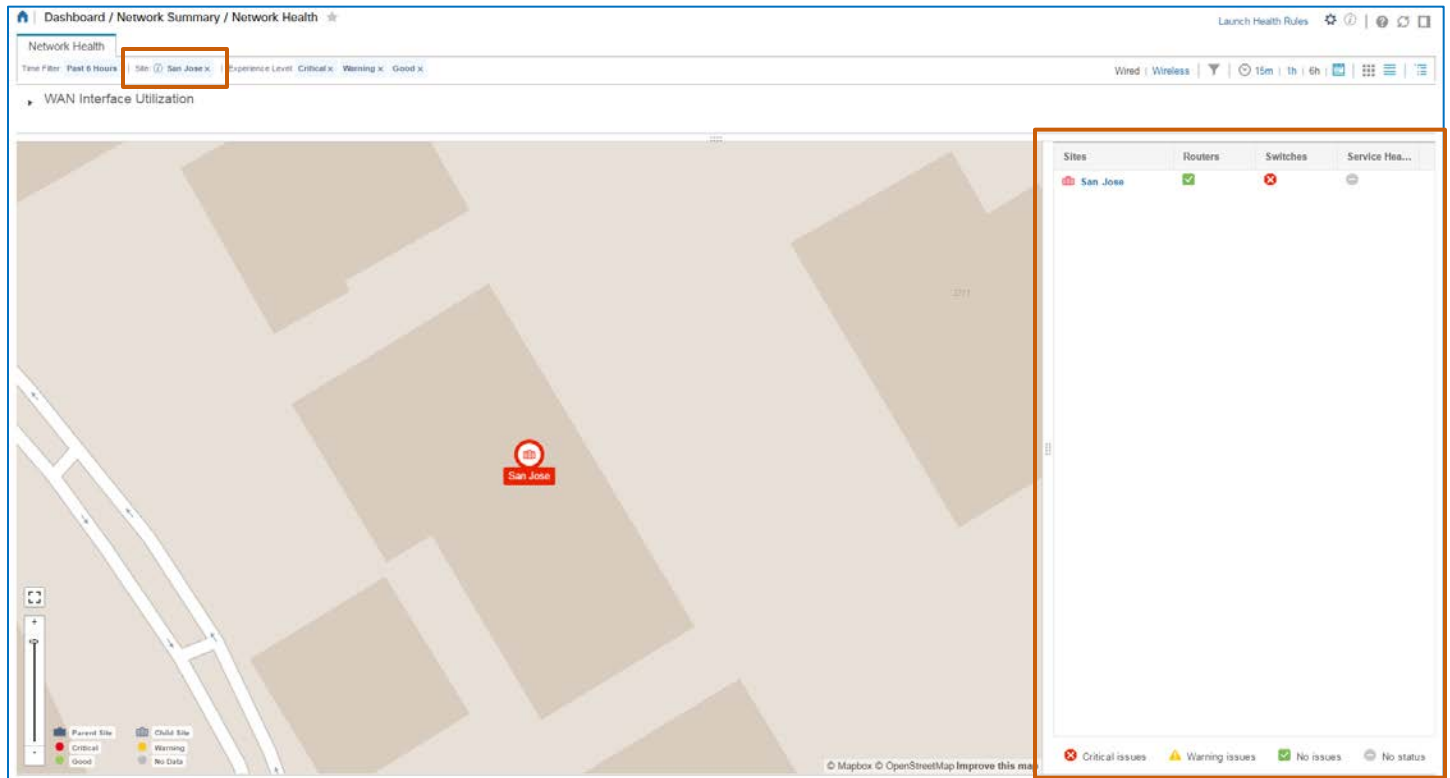
The icon color-code at individual and grouped site levels represents the most critical health issue occurring on one or more devices associated with the site or sites.

You can point to the icon to see the sites that are included in the grouped location.



To zoom to a more detailed view, you can click the location icon on the map or by using one of the name links in the pop-up window.

The map view zooms in and the system applies a filter so that the dashboard reports the data for that location only. The system indicates the site level filter below the **Network Health** tab.



## Unmapped Locations

When system users have configured location groups but not applied geographical coordinates to those groups, they will not appear in the map view.

To help ensure that you are seeing the sites that you need to monitor:

- ❖ Click the **Sites with no Geo coordinates** button.

A dialog box opens and lists the locations without coordinates.



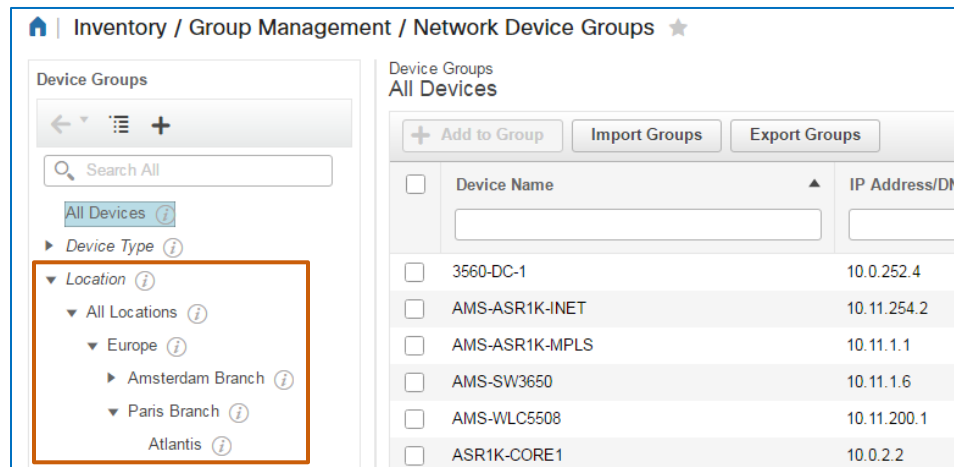
To apply geographical coordinates to a location group:

- ❖ In the dialog box, click the location name link.

This system navigates to and opens the **Network Devices** page where you can find and configure the location group coordinates.





**Note:** To review how to configure a location group, including adding geographical coordinates, [refer to the Organizing Location Groups topic](#).



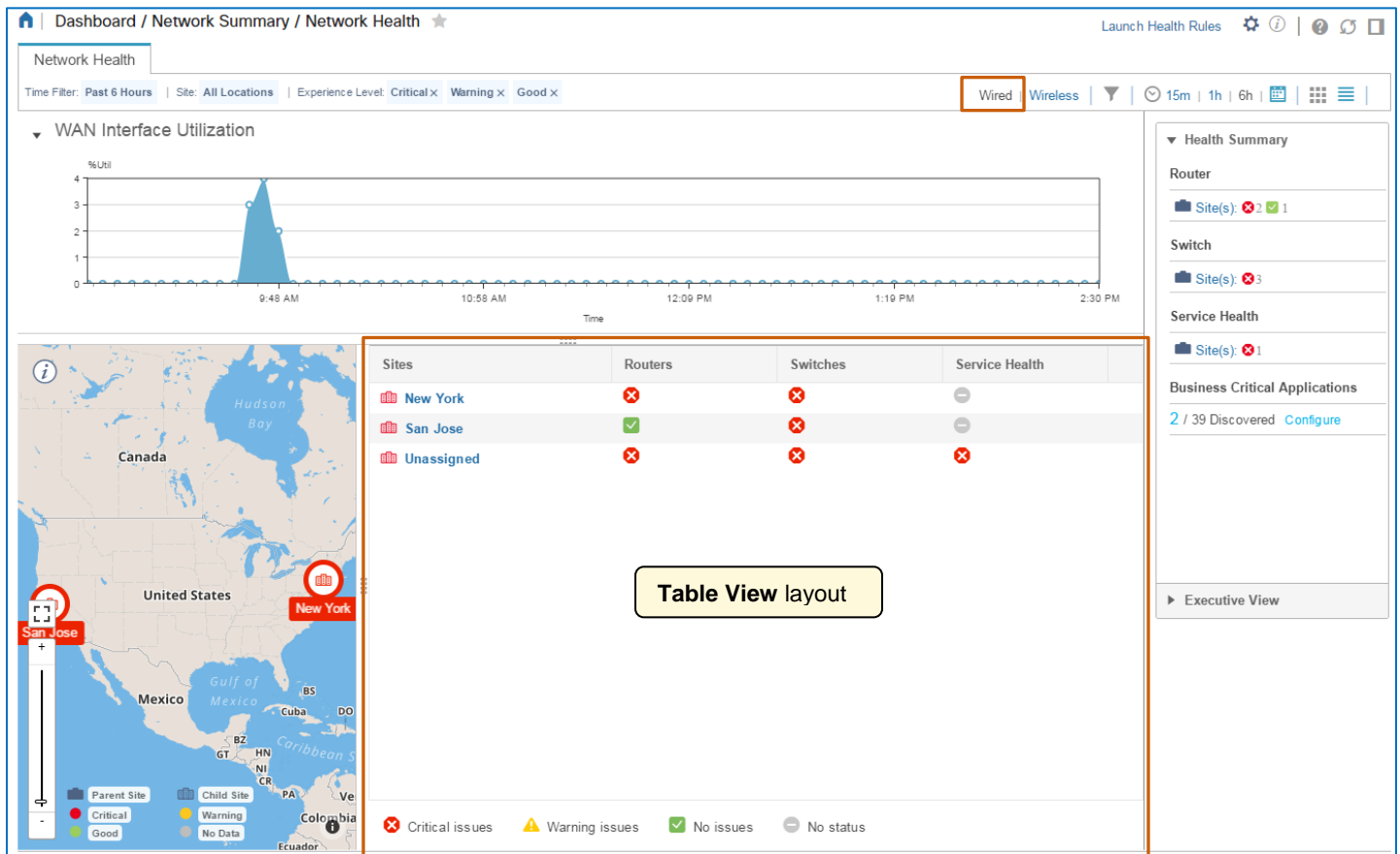
## Accessing Metrics Overview

By default, the page displays the **Table View** layout. At the highest level, the layout lists all of the parent and child location groups that include geographical coordinates.

Sites that contain child locations are indicated by solid icons that are color-coded to indicate the highest reported severity level. 

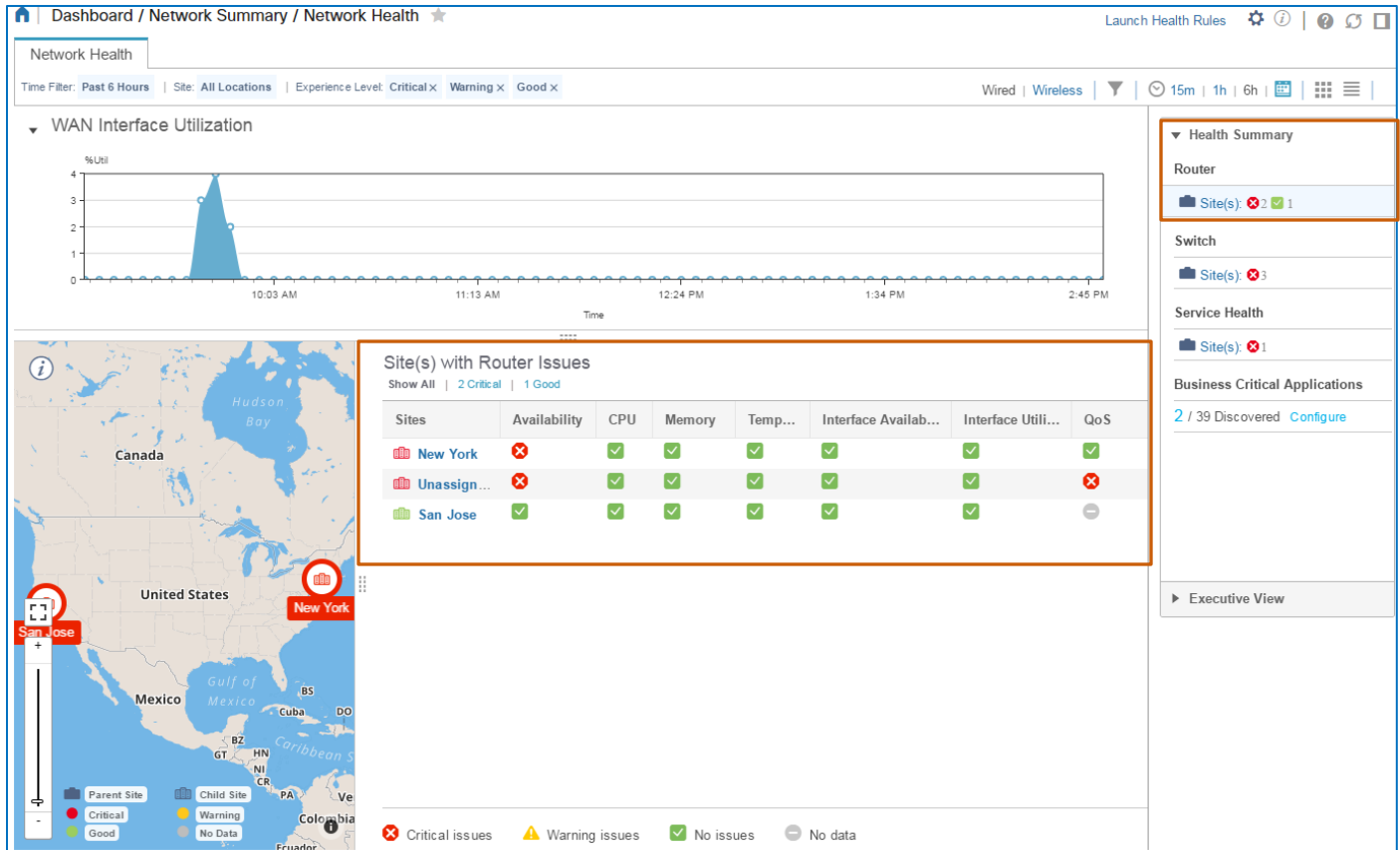
When a site is at its lowest child level in the location group hierarchy, the icon is not solid. 

The **Table View** displays the health metrics in a list by site and device type, and indicates the most critical alarm type that is occurring at the location level.



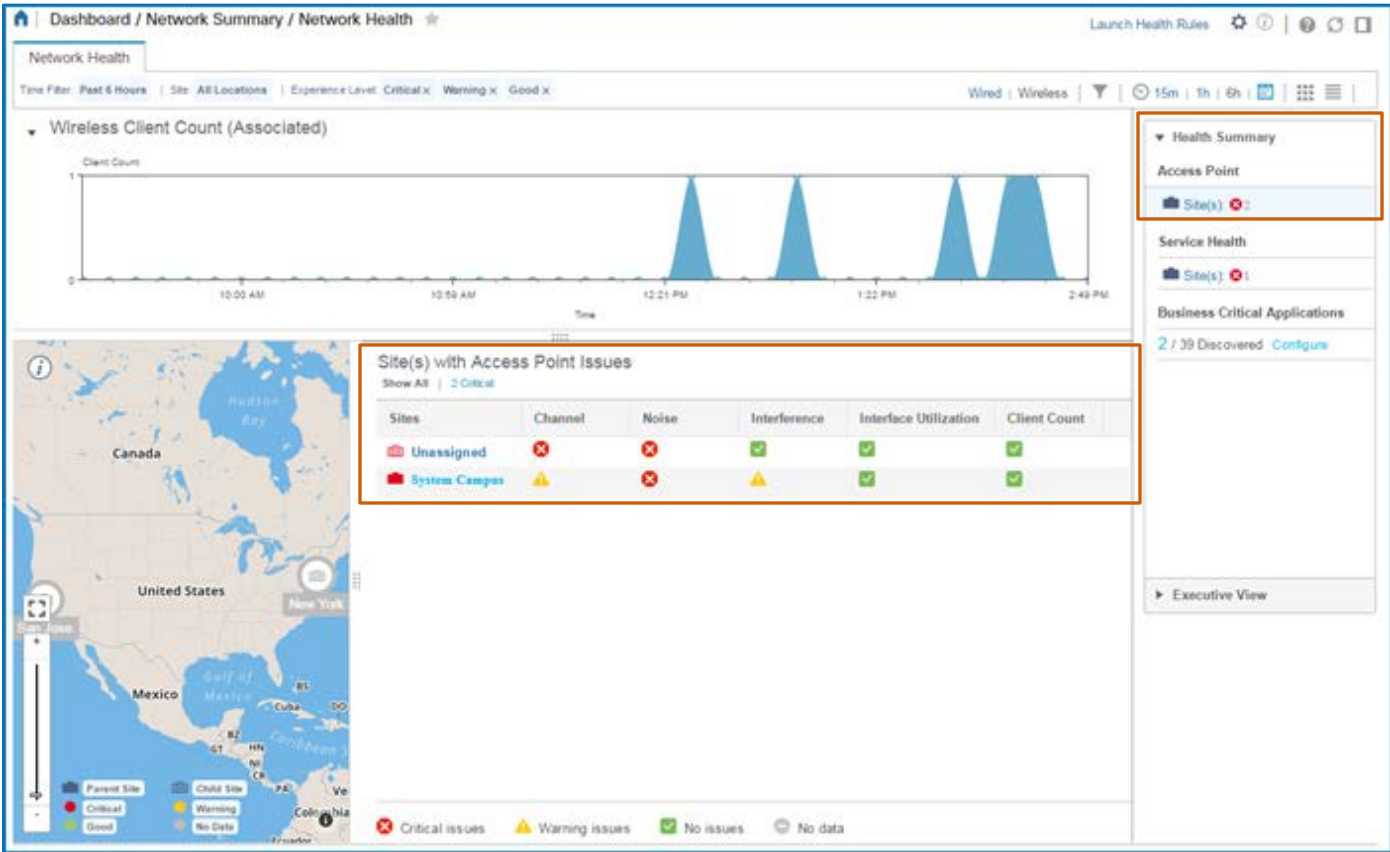
In the **Health Summary** panel, you can click a device type or service health item. The view section updates to list the sites and show their related metrics, screenshots below.

This screenshot illustrates the metrics for the view of the wired network for multiple locations.

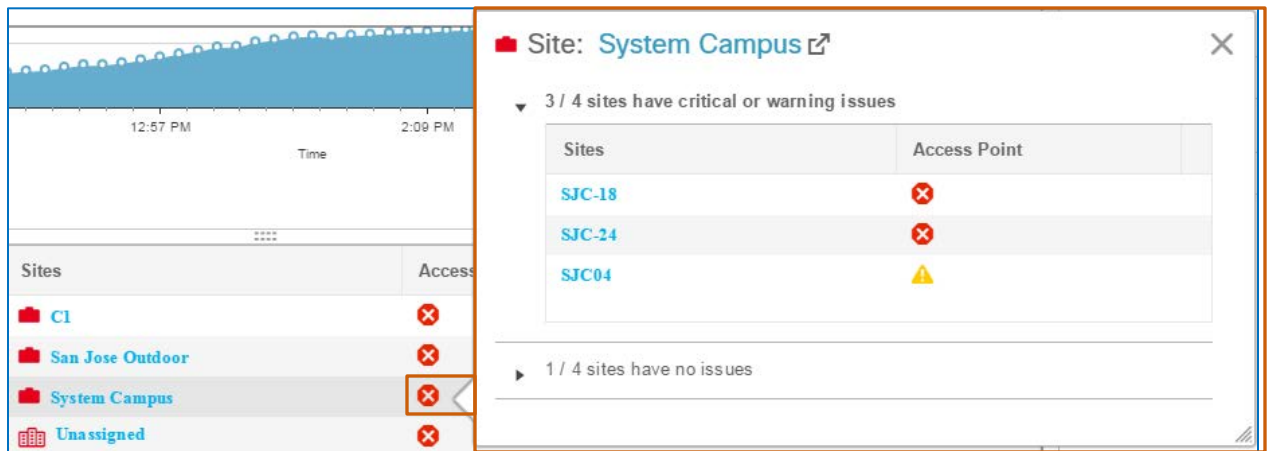




This screenshot illustrates the metrics for the view of the wireless network.

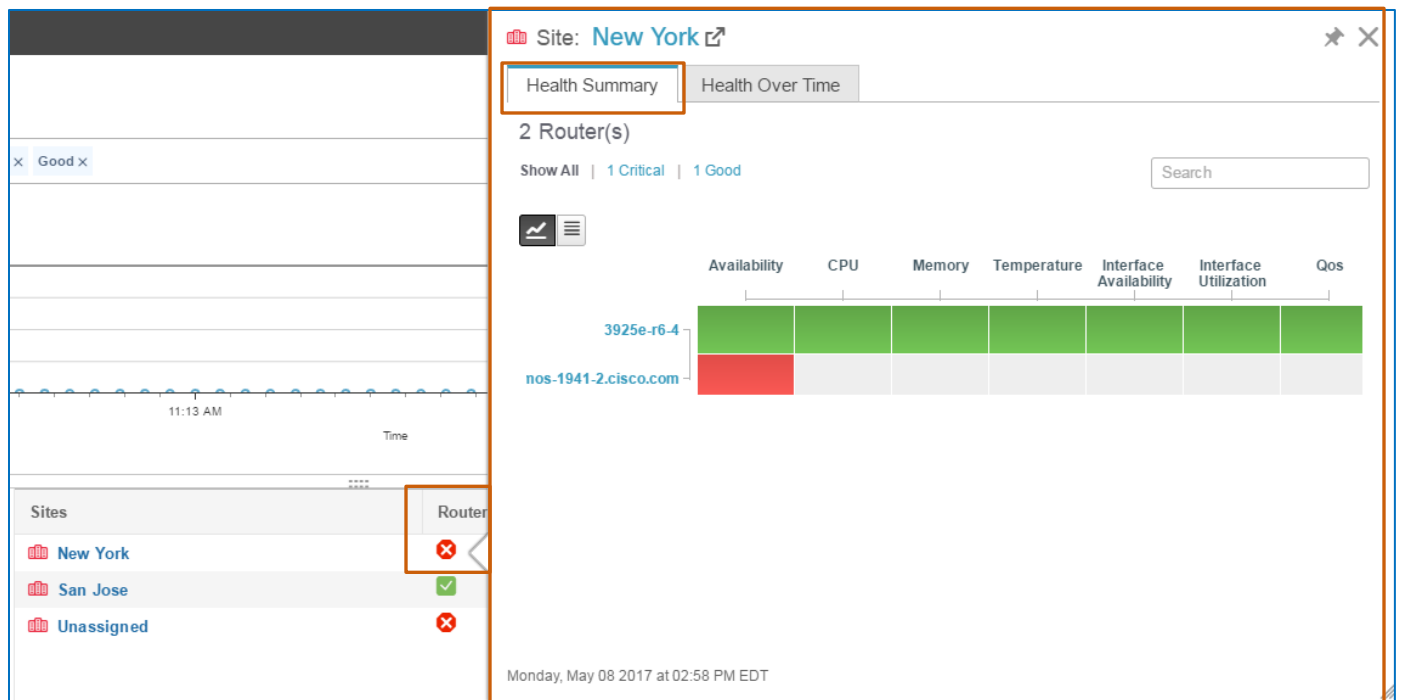


In the table view, when you click a metric in the row of a parent site, a pop-up window opens provides navigation to its child sites.



When an item is at its lowest child level in the location group hierarchy, you can click a device type status indicator to open a pop-up window, which lists the metrics for each device of that type at the location.

The **Health Summary** tab illustrates the status of each metric.

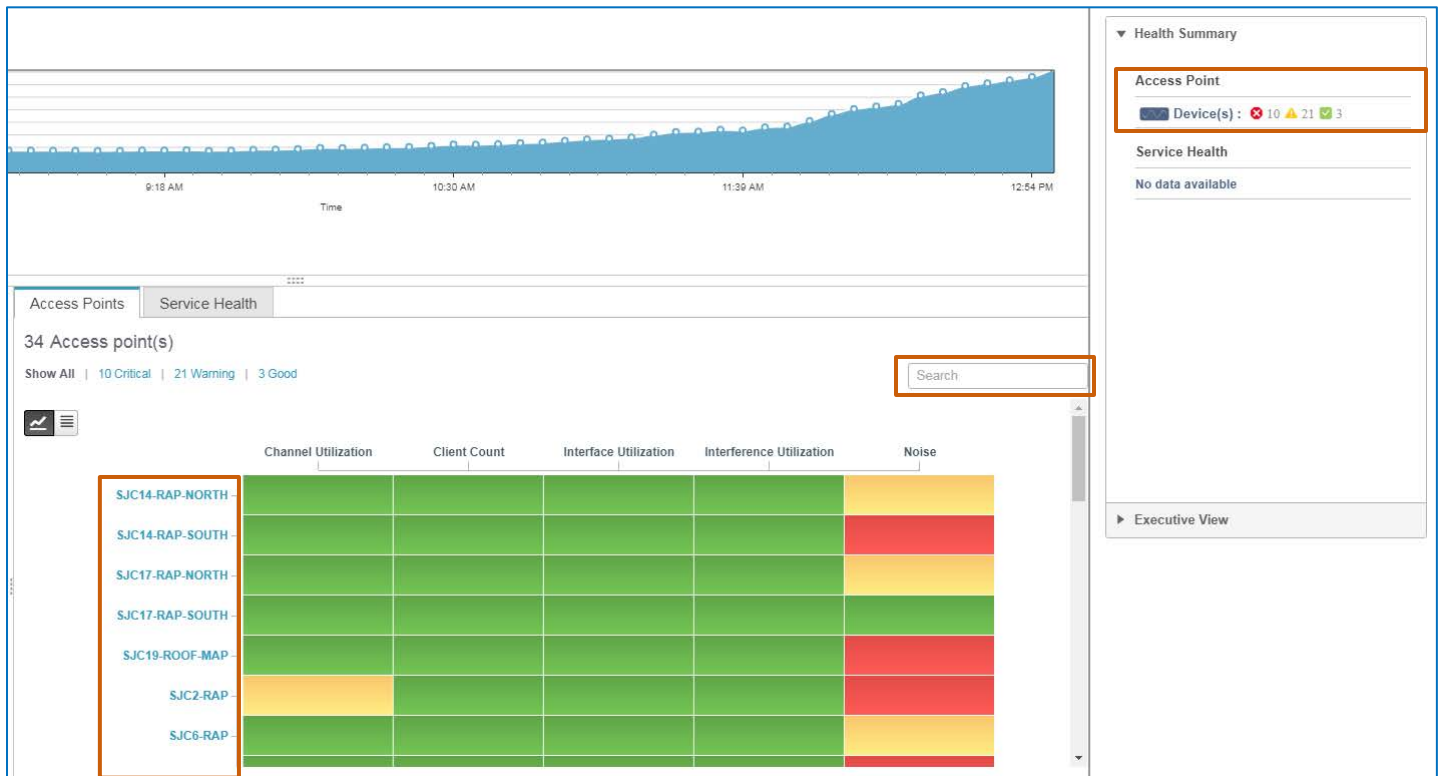


When you have a long list of devices, you can search for a specific device.

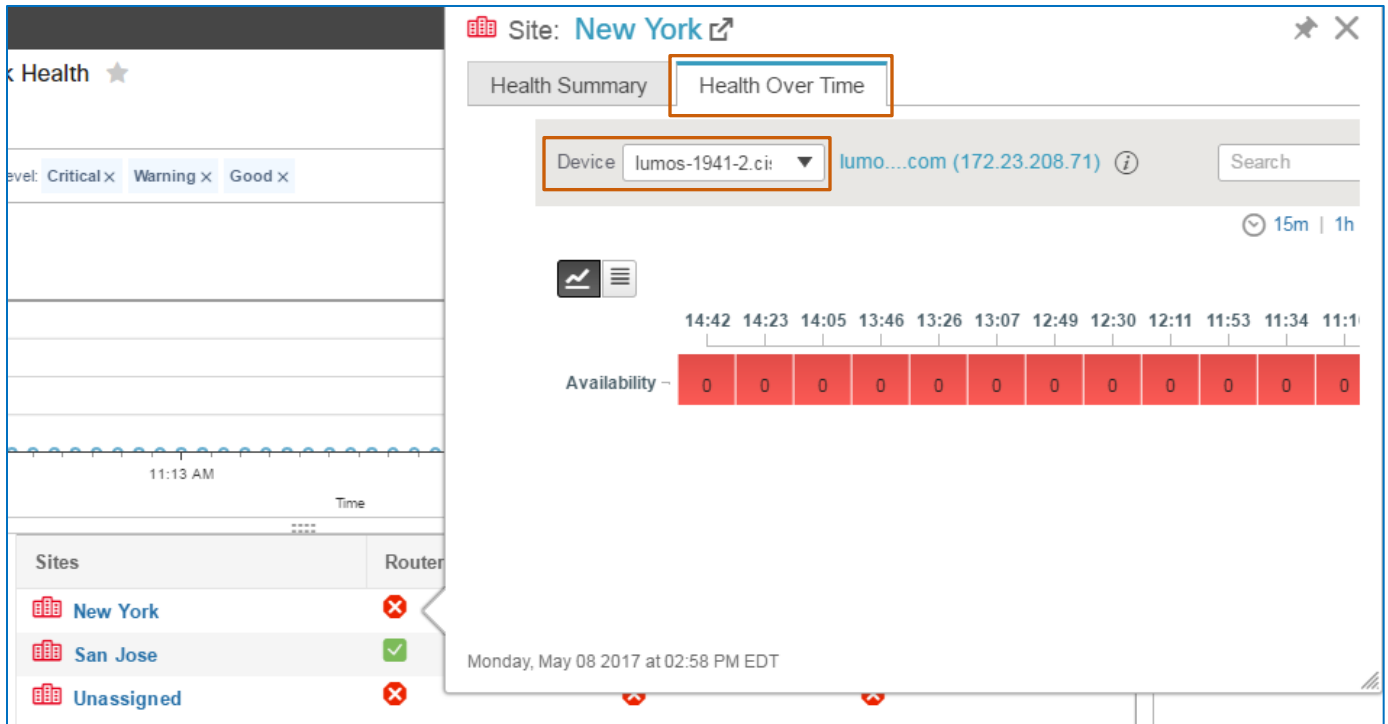
**To find a specific device:**

- ❖ In the **Search** field, begin typing the characters that are included in the device name.

As you type, the list filters to display all of the devices with names that include the characters that you are typing.



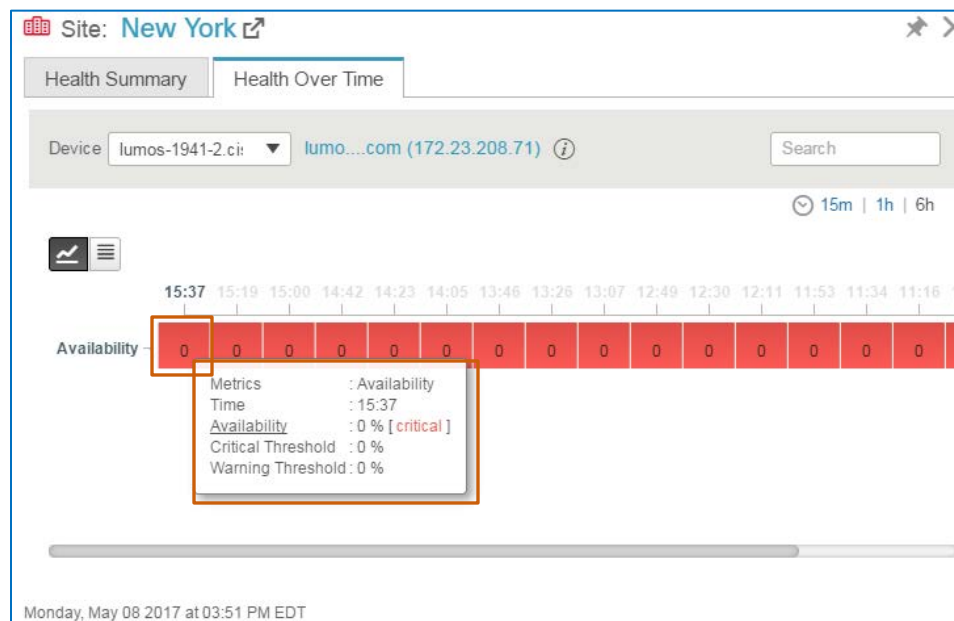
The **Health Over Time** tab illustrates the health of the device indicated in the **Device** drop-down list for the active time period. You can review the health of each device at the location by selecting it in the drop-down list.



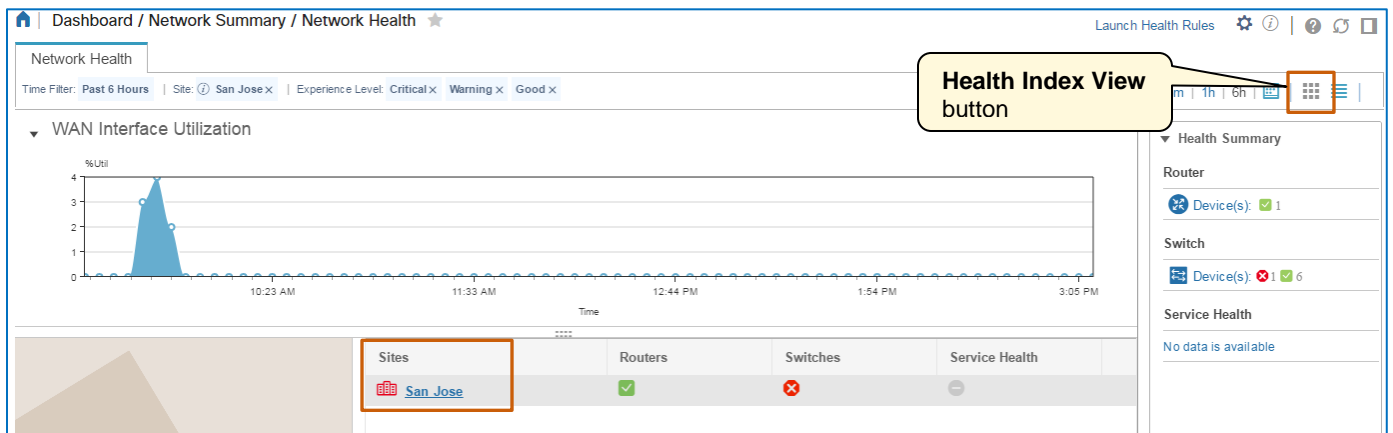
To evaluate a specific metric, on the Health Over Time tab:

- ❖ Point to the metric of interest.

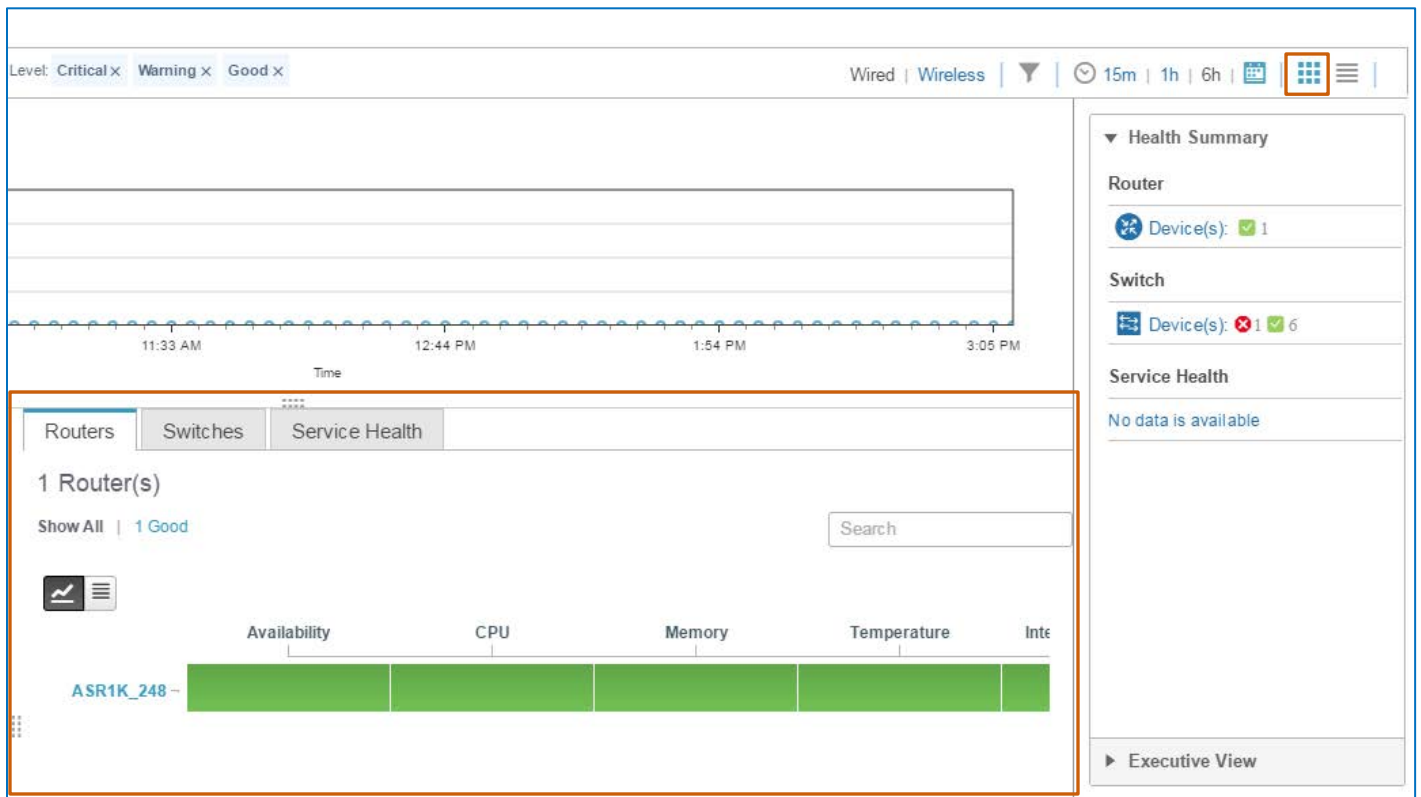
A third pop-up window opens and indicates the thresholds defined by the health rules in addition to the metric that the device was reporting at that time.



When you are accessing metrics at the lowest child level of a site (a site with no dependencies), you can apply the **Health Index View**.



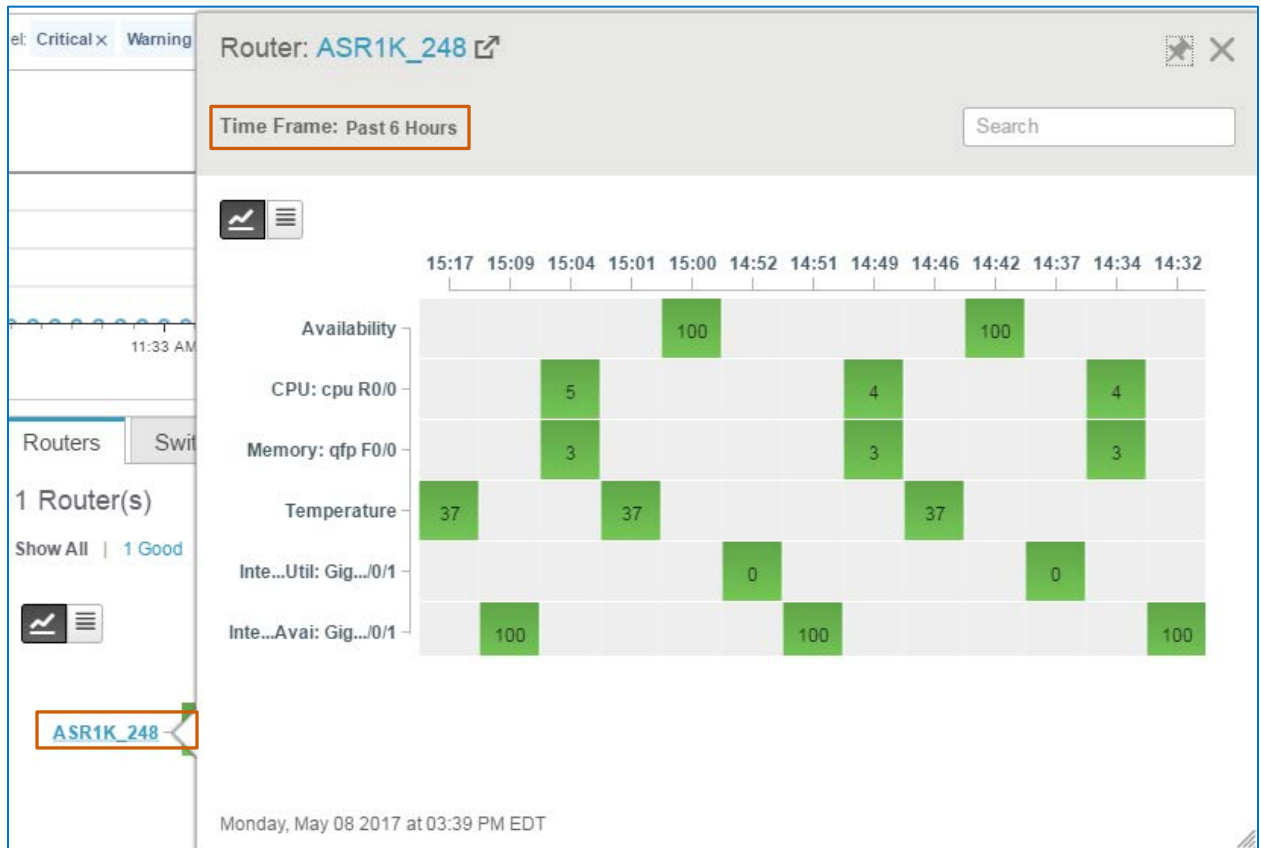
In this view, you see all of the devices in the location group and the highest severity level of each metric.



To access the metrics for a specific device in the list:

- ❖ Click the device name link beside the graph.

The pop-up window reports metrics based on the global time frame configured on the dashboard.



You also can click a device type in the **Health Summary** panel to display the health metrics for the device indicated in the **Device** drop-down list.



## Additional Navigation Features

Various dashboard elements provide navigation to detailed information, including links to:

- ❖ Summary and detailed performance metrics.
- ❖ Device information.

This way, when the information that you see on dashlets prompts you to get more information, you can access more information efficiently.

### Opening Metrics Dashboards

When reviewing metrics by using the **Health Summary** feature, you can navigate directly to:

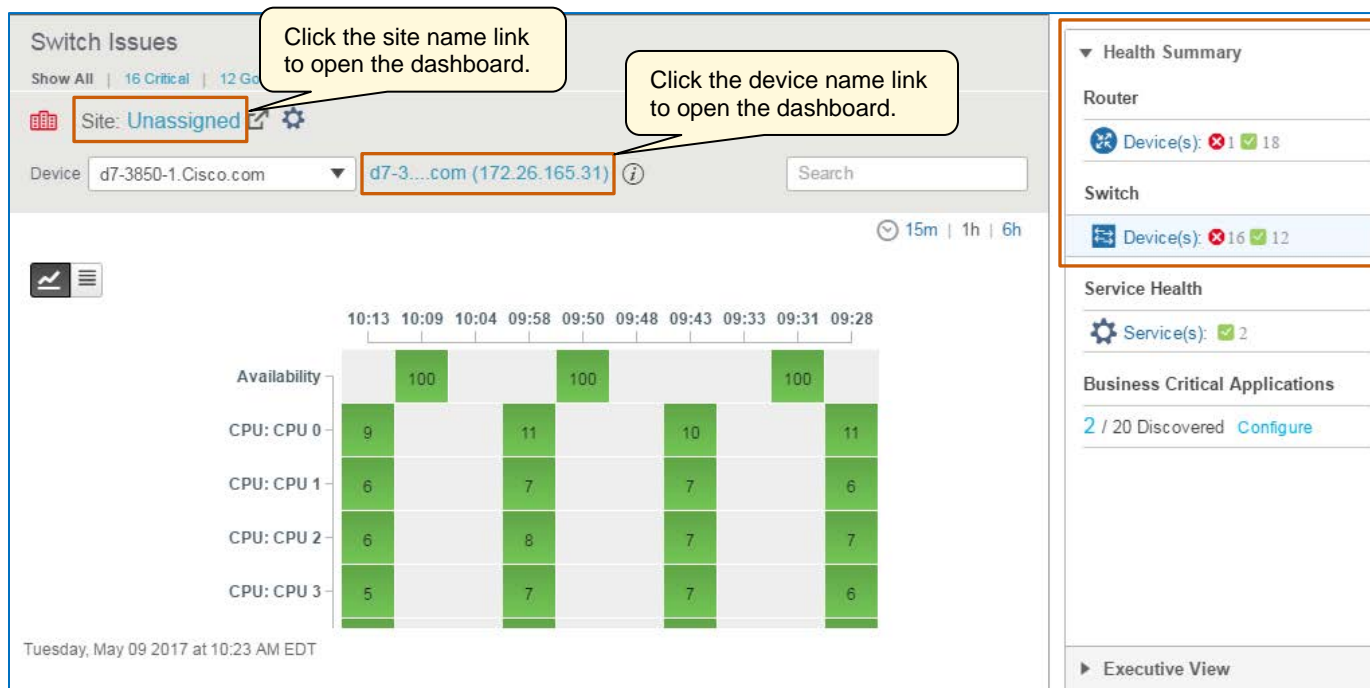
- ❖ The **Performance | Site** dashboard tab to see a summary of location performance metrics.
- ❖ The **Performance | Device** dashboard tab to see a summary of device performance metrics.

**To open the Performance | Site dashboard tab:**

- ❖ In the metrics area, beside **Site**, click the site name link.

**To open the Performance | Device dashboard tab:**

- ❖ In the metrics area, beside the **Device** drop-down list, click the device name link.

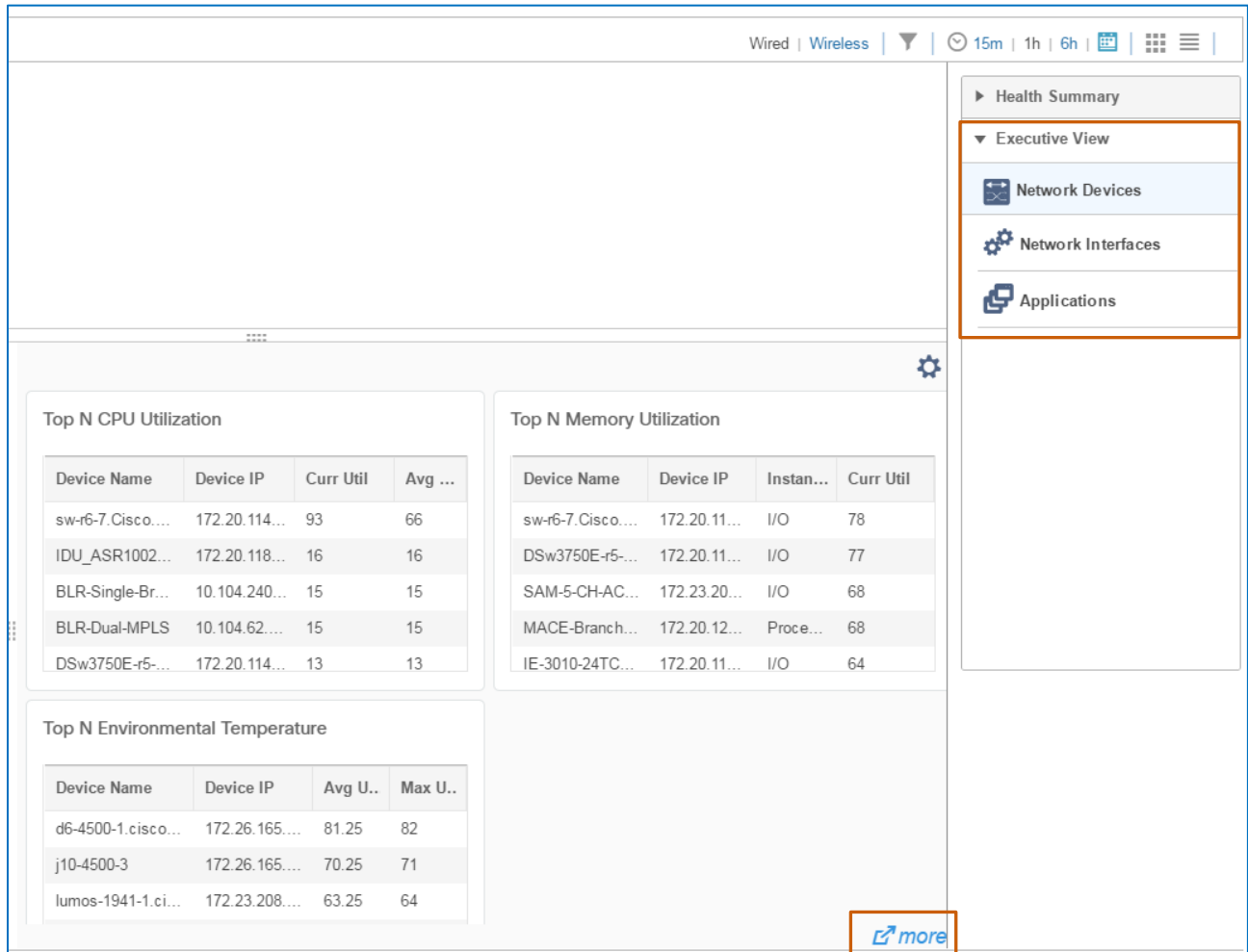




When reviewing metrics by using the **Executive View**, you can navigate directly to the dashboard.

**To navigate to a dashboard:**

- ❖ Below the dashlets, click the **more** link.



The screenshot shows the Cisco Network Health Monitoring dashboard. The top navigation bar includes links for 'Wired' and 'Wireless' views, a filter icon, and time range selectors for '15m', '1h', and '6h'. The main content area displays three dashlets: 'Top N CPU Utilization', 'Top N Memory Utilization', and 'Top N Environmental Temperature'. Each dashlet contains a table of device metrics. On the right side, there is a sidebar with a 'Health Summary' section and an 'Executive View' section. The 'Executive View' section is highlighted with an orange border and contains three sub-sections: 'Network Devices', 'Network Interfaces', and 'Applications'. At the bottom right of the main content area, there is a 'more' link with an external link icon, also highlighted with an orange border.

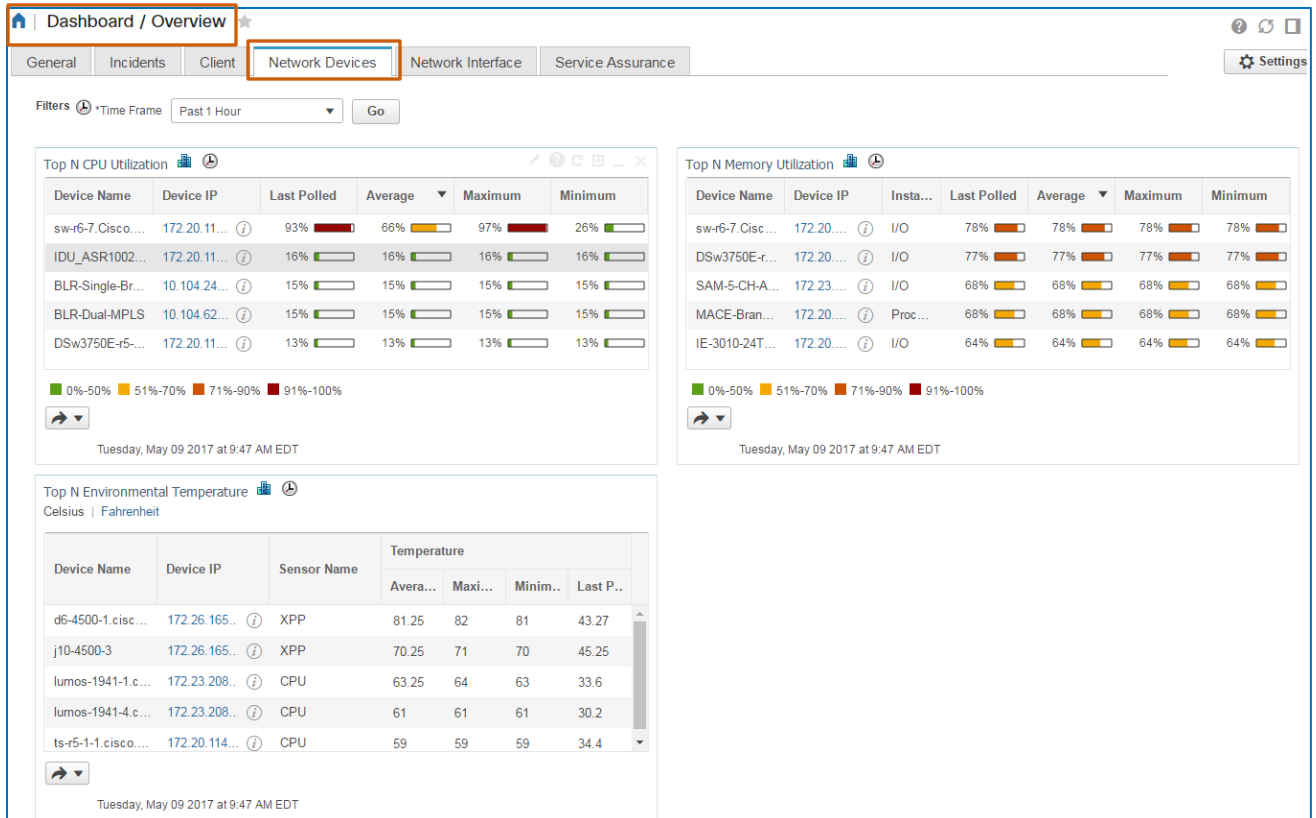
| Device Name       | Device IP     | Curr Util | Avg ... |
|-------------------|---------------|-----------|---------|
| sw-r6-7.Cisco.... | 172.20.114... | 93        | 66      |
| IDU_ASR1002...    | 172.20.118... | 16        | 16      |
| BLR-Single-Br...  | 10.104.240... | 15        | 15      |
| BLR-Dual-MPLS     | 10.104.62.... | 15        | 15      |
| DSw3750E-r5...    | 172.20.114... | 13        | 13      |

| Device Name       | Device IP    | Instan... | Curr Util |
|-------------------|--------------|-----------|-----------|
| sw-r6-7.Cisco.... | 172.20.11... | I/O       | 78        |
| DSw3750E-r5...    | 172.20.11... | I/O       | 77        |
| SAM-5-CH-AC...    | 172.23.20... | I/O       | 68        |
| MACE-Branch...    | 172.20.12... | Proce...  | 68        |
| IE-3010-24TC...   | 172.20.11... | I/O       | 64        |

| Device Name        | Device IP      | Avg U.. | Max U.. |
|--------------------|----------------|---------|---------|
| d6-4500-1.cisco... | 172.26.165.... | 81.25   | 82      |
| j10-4500-3         | 172.26.165.... | 70.25   | 71      |
| lumos-1941-1.ci... | 172.23.208.... | 63.25   | 64      |

The system navigates to and opens the related **Overview** dashboard tab.

For example, when you click the more link below the **Network Devices** dashlets, the system navigates to the **Network Devices** dashboard tab, screenshot below.

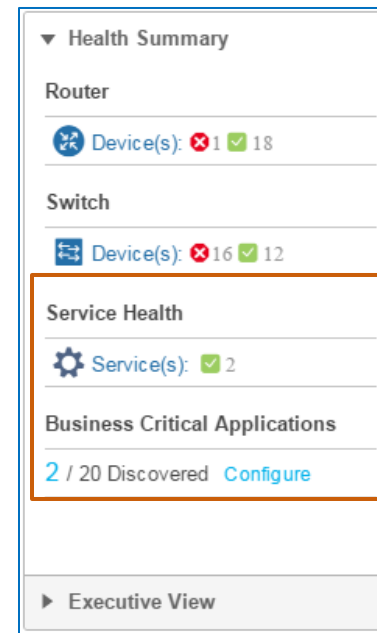
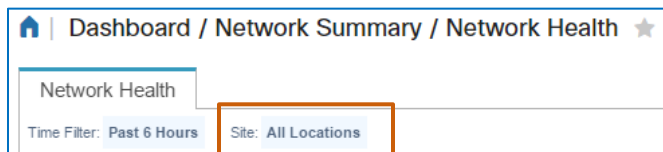


## Monitoring Service Health

The **Service Health** summary feature also reports the service health of KPIs for applications by site and source that system users have [identified as business-critical](#) and that have [location groups associated to subnets](#).

The health statuses that the system reports are defined by the threshold values in the [health rules](#).

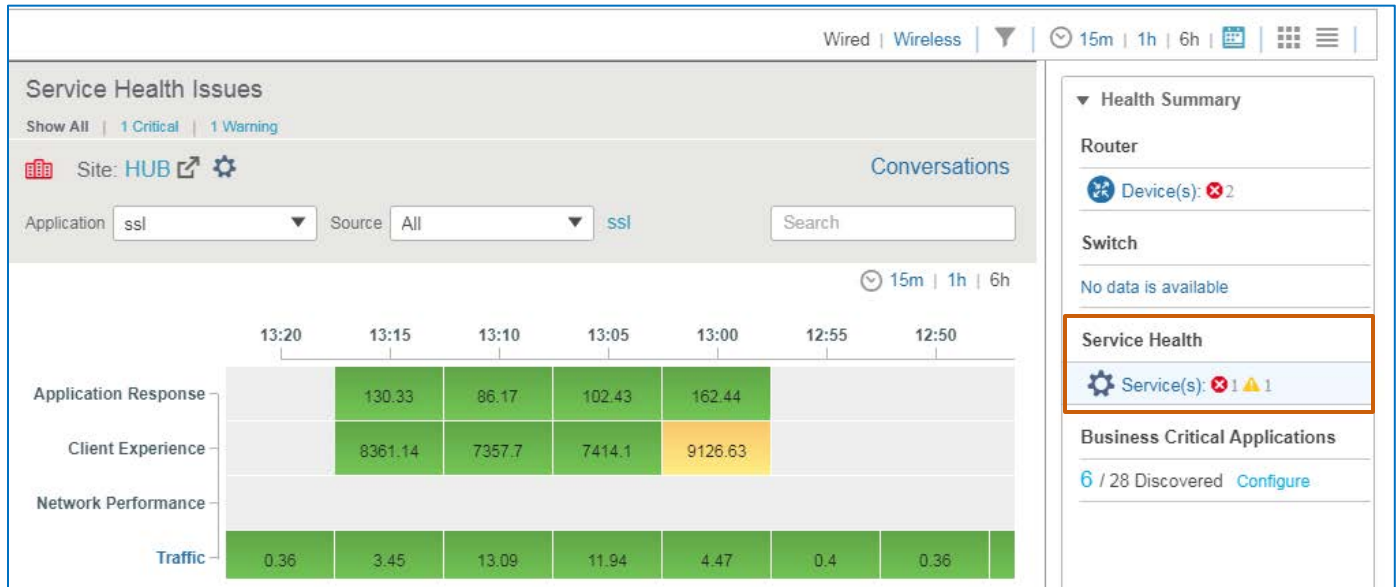
[The Health Summary feature](#) indicates service health issues based on the site level that you have active in both the wired and wireless views.



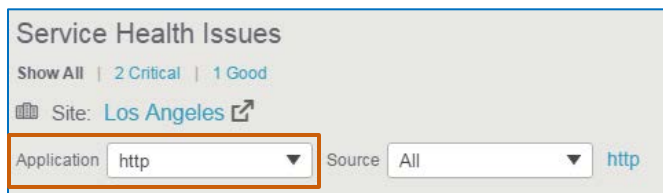
To investigate the location or locations reporting service health issues:

- ❖ Navigate to the location level that you want, and then, in the **Health Summary** feature, under **Service Health**, click **Service(s)**.

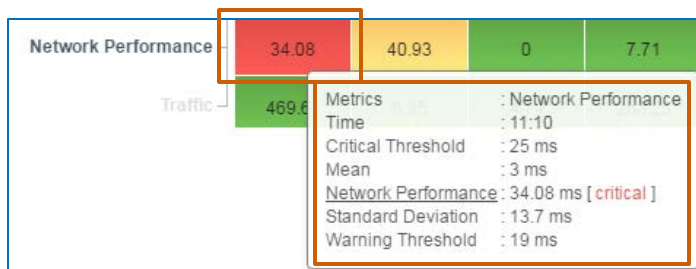
A panel opens and lists the metrics with health indicators...



...for the business critical application that is selected in the **Application** drop-down list.

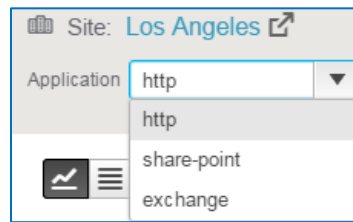


You can point to a metric on the timeline to see details, including the metric thresholds.



**To evaluate another application:**

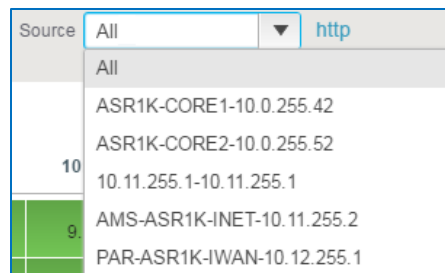
- ❖ In the **Application** drop-down list, select the application.



By default, the system reports the combined metrics for all of the devices with the NetFlow feature enabled, which collects IP network traffic flow.

**To evaluate the metrics of a specific device:**

- ❖ In the **Source** drop-down list, select the device.

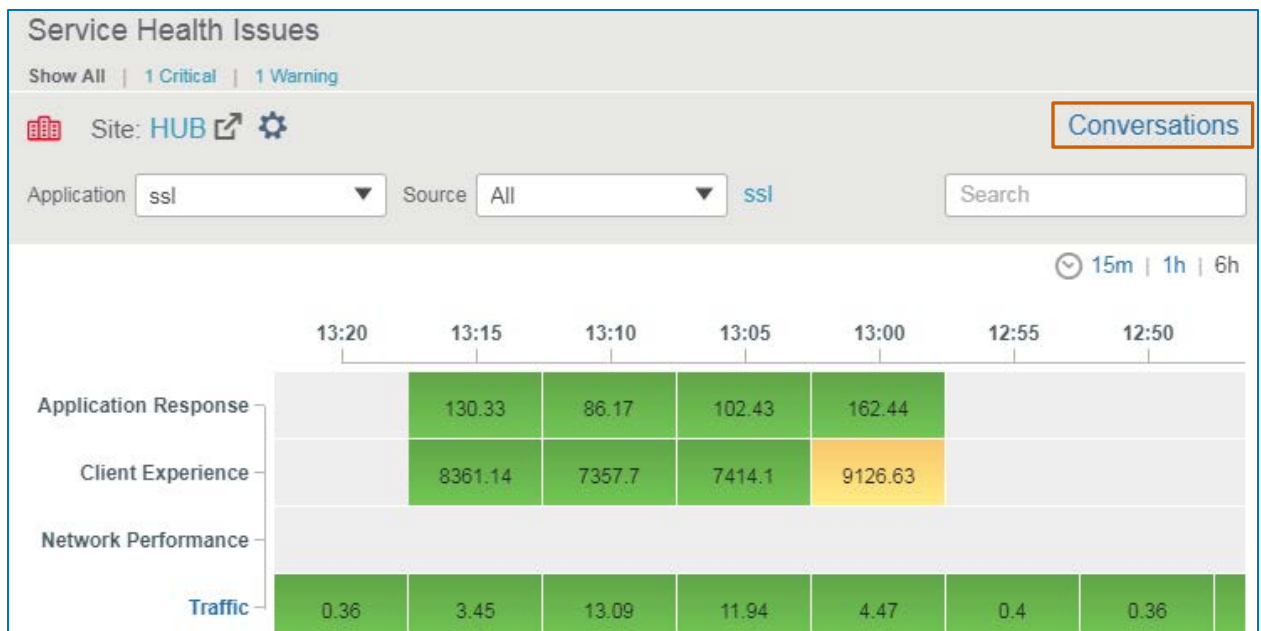


You can indicate the business critical applications on which you want the system to report service health.



**Note:** For more information, [refer to the Indicating Business Critical Applications topic](#).

You also can evaluate and monitor NetFlow traffic by interface or site by using the Conversations feature, available by using the **Conversations** link.

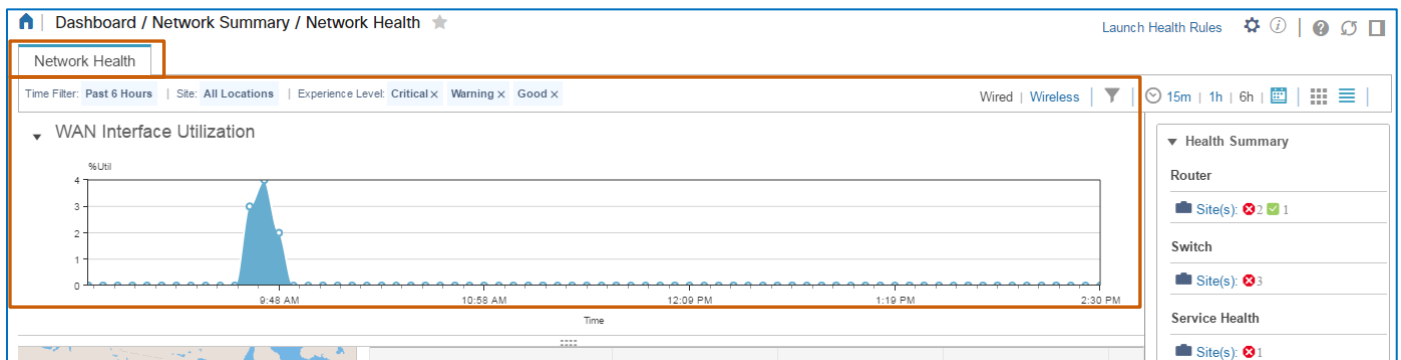


## Reviewing Key Graphs

The **Network Health** dashboard page also provide a key graph based on the view type, either wired or wireless.

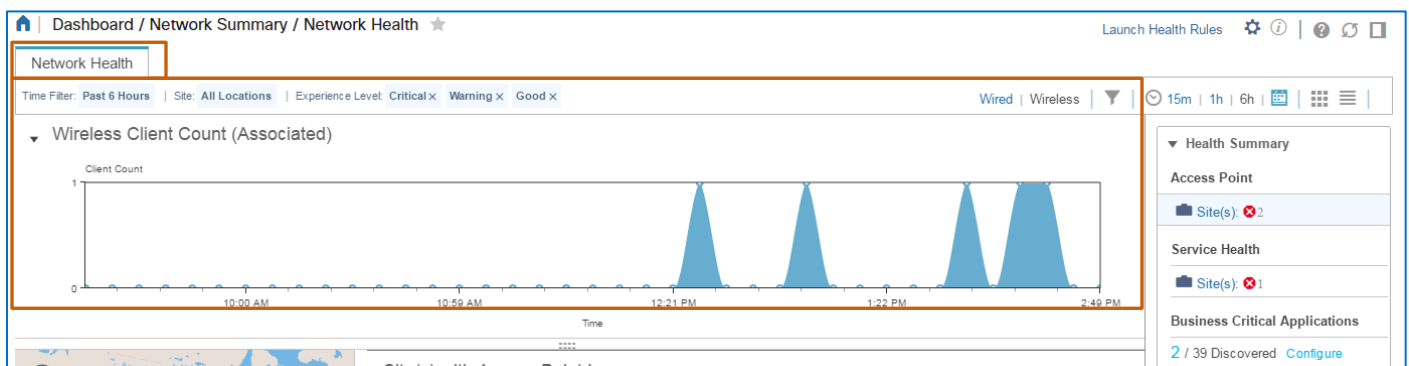
When monitoring the wired network, the page displays the **WAN Interface Utilization** graph.

Knowing how heavily interfaces are being used at the location provides insight into whether, for example, you might consider adding links to distribute traffic more evenly or reduce network congestion.



When monitoring the wireless network, the page displays the **Wireless Client Count** graph.

Knowing the number of wireless clients that are accessing the network at the location provides insight into whether, for example, you might consider adding access points to support network access more efficiently or improve the end user experience.



## Preparing Network Health Reporting

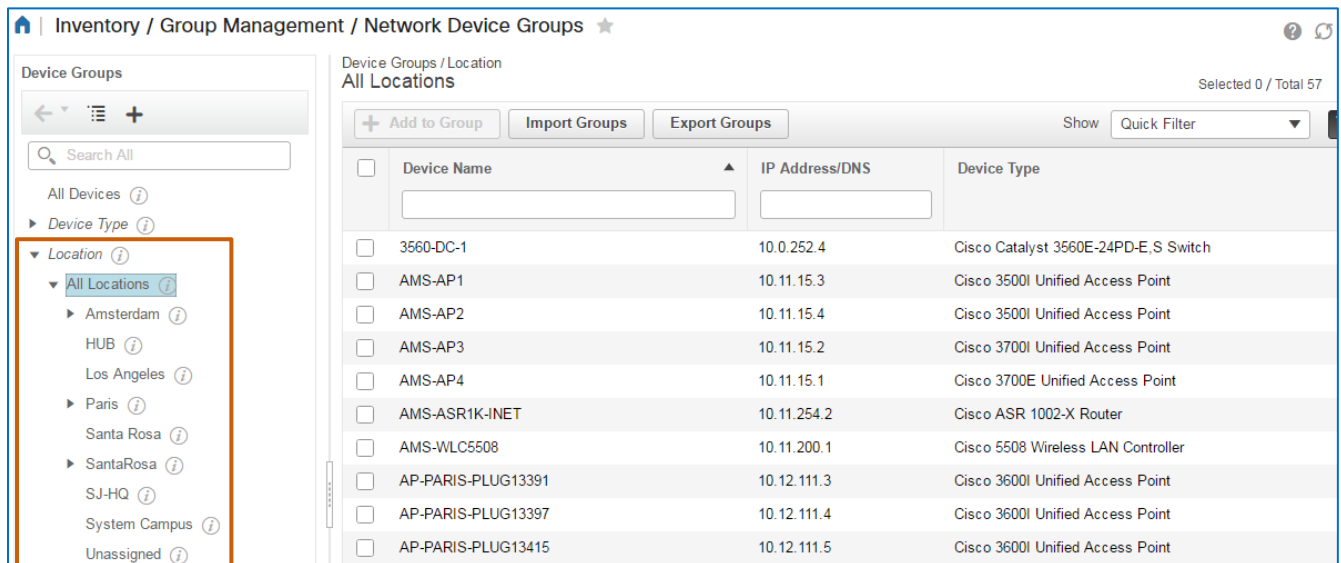
### Organizing Location Groups

#### Location Groups Overview

Location groups are a method of logically organizing devices based on the locations (sites), that they support. System users must configure location groups and include geographical coordinates so that the **Network Health** dashboard can display and report the locations (sites) accurately and report location (site) level health data.

Initially, when you open a map view, the map zoom level applies based on the regions or regions that contain locations with coordinates.

You can organize location groups on the **Network Devices** or **Network Device Groups** page.

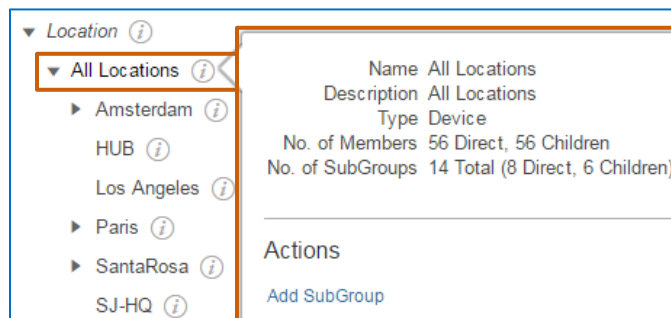


The screenshot shows the 'Inventory / Group Management / Network Device Groups' page. On the left, the 'Device Groups' sidebar shows a hierarchy: 'All Devices' > 'Device Type' > 'Location' > 'All Locations' (highlighted with an orange box). Below 'All Locations' are sub-locations: 'Amsterdam', 'HUB', 'Los Angeles', 'Paris', 'Santa Rosa', 'SantaRosa', 'SJ-HQ', 'System Campus', and 'Unassigned'. The main panel shows 'Device Groups / Location All Locations' with a table of devices. The table has columns for 'Device Name', 'IP Address/DNS', and 'Device Type'. The table lists 14 devices, including switches, access points, and routers.

| Device Name        | IP Address/DNS | Device Type                           |
|--------------------|----------------|---------------------------------------|
| 3560-DC-1          | 10.0.252.4     | Cisco Catalyst 3560E-24PD-E, S Switch |
| AMS-AP1            | 10.11.15.3     | Cisco 3500I Unified Access Point      |
| AMS-AP2            | 10.11.15.4     | Cisco 3500I Unified Access Point      |
| AMS-AP3            | 10.11.15.2     | Cisco 3700I Unified Access Point      |
| AMS-AP4            | 10.11.15.1     | Cisco 3700E Unified Access Point      |
| AMS-ASR1K-INET     | 10.11.254.2    | Cisco ASR 1002-X Router               |
| AMS-WLC5508        | 10.11.200.1    | Cisco 5508 Wireless LAN Controller    |
| AP-PARIS-PLUG13391 | 10.12.111.3    | Cisco 3600I Unified Access Point      |
| AP-PARIS-PLUG13397 | 10.12.111.4    | Cisco 3600I Unified Access Point      |
| AP-PARIS-PLUG13415 | 10.12.111.5    | Cisco 3600I Unified Access Point      |

To add a top level location group folder, which equates to the parent site in Network Health views:

- ❖ Under **Location**, point to the information button beside the **All Locations** category, and in the pop-up window, click **Add SubGroup**.

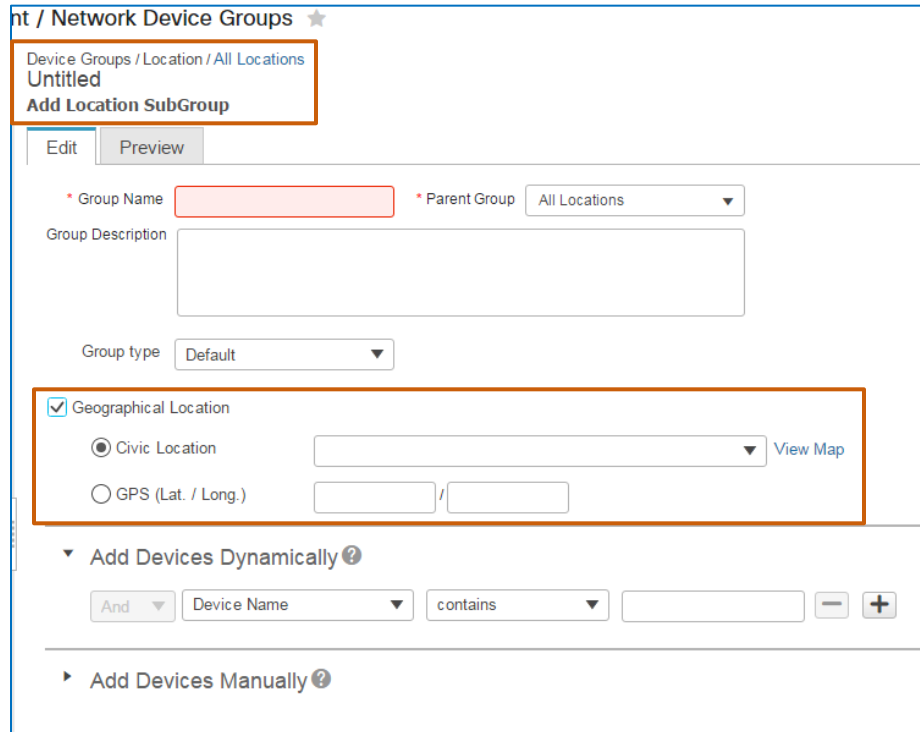


The screenshot shows the 'All Locations' information pop-up window. The window displays the following information:

- Name: All Locations
- Description: All Locations
- Type: Device
- No. of Members: 56 Direct, 56 Children
- No. of SubGroups: 14 Total (8 Direct, 6 Children)
- Actions: Add SubGroup

To make the location group visible on the Network Health dashboard page:

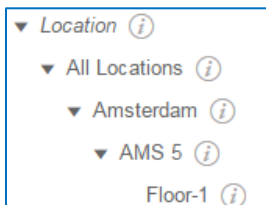
- ❖ On the **Add Location SubGroup** page, select the **Geographical Location** check box, and then add the civic location, which is the physical address, or the location's latitude and longitude coordinates.



To add a child location group (child site) to a top level location group (parent site):

- ❖ Under the **All Locations** heading, point to the information button beside the top level folder (parent site) name, and then, in the pop-up window, click **Add SubGroup**.

You can continue to add child sites, as needed, to represent location and device relationships. When system users can recognize device and location relationships, they can more readily identify the parts of the network and enterprise that potential disruption or health issues might affect.



**Note:** For detailed steps on organizing location groups, [refer to the Cisco Prime Infrastructure 3.2 User Guide](#).

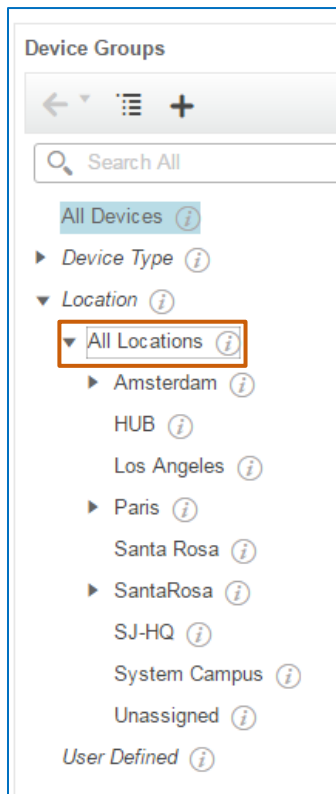


## How Location Group Organization Affects Views

Recognizing location group organization is critical to understanding what you see on the **Network Health** dashboard.

The dashboard uses parent and child site relationships to illustrate where network devices are located globally and in relationship to the larger enterprise. The relationships are defined by, and the same as, the location groups and their folder organizations on the **Network Devices** or **Network Device Groups** page.

When you add location groups, the system automatically places them in the **All Locations** category.



Those top level folders below **All Locations** that have geographical coordinates configured are the parent sites that you see on the map.

Users can continue to add subgroups of folders under top level location group folders, which define the child sites that belong to each parent site.

System users can monitor access points at a floor level only. To make access points visible on the **Network Health** dashboard page, you need to configure the following top down location group hierarchy:

- ❖ A campus location
  - ◆ A building or buildings in the campus location
    - Outdoor areas at the location
    - The floor or floors in the building location on which you place the access points

You can configure as many buildings and floors at a campus level location as you need to support monitoring requirements.

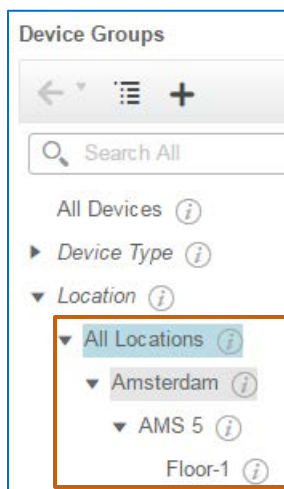
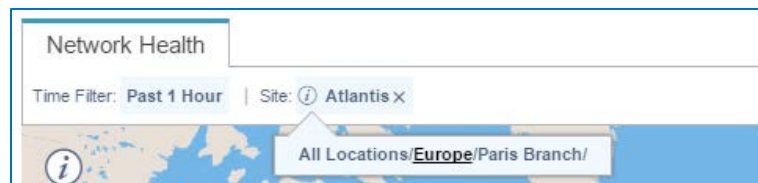
As with all location groups, you need to apply the geographical coordinates at each location level.

The screenshots below illustrate the Amsterdam location group, which has two subgroup levels, and the Amsterdam parent site, which appears on the map. The icon above the site label is solid, which indicates that the site has child sites associated with it.

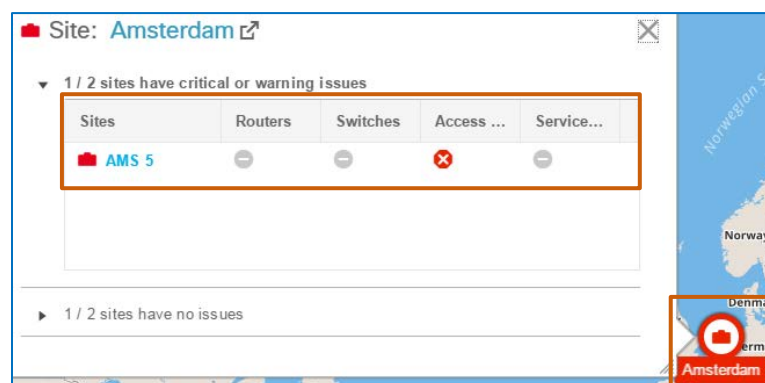
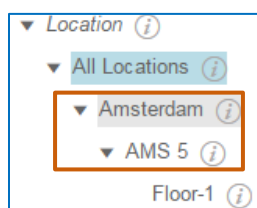


**Important Note:** In order for users to see the parent site and all of its child sites on the map, the top level folder and each subgroup folder must have its geographical coordinates configured.

If you do not configure a folder with geographical coordinates, and a user selects that site when navigating a map, that site and its child sites are not visible at that level on the map.



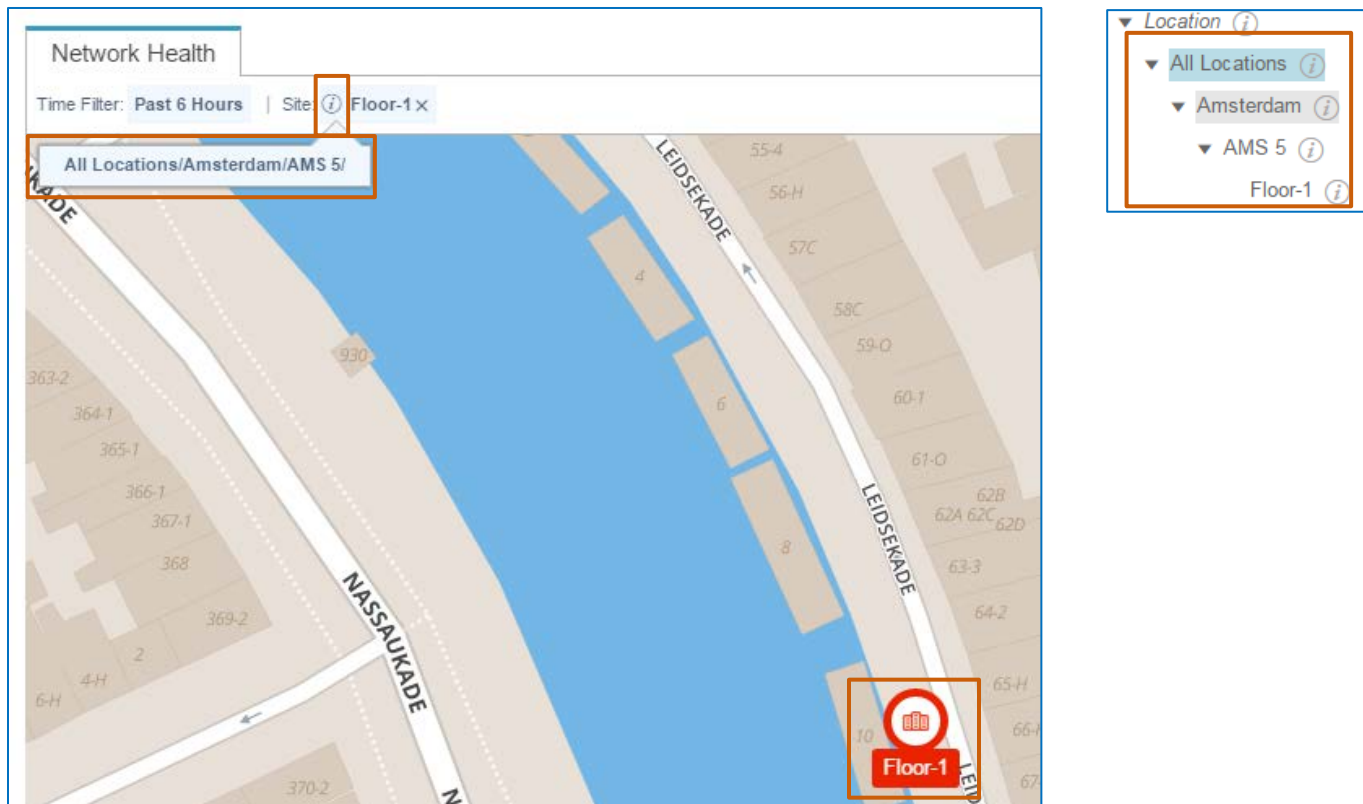
When you point to the site on the map, the pop-up window lists each next level child site based on the site level that is active on the map.



In the list of sites, you can click the name link to open the next level of child sites in the pop-up window.

When you open child sites on the map, you can navigate to higher level folders by clicking the **Show Parent** button on the toolbar, and then clicking a site link.

The screenshots below illustrate the same hierarchy in the navigation pop-up window that you see in the location group list, when you have the **Floor-1** child site open on the map.



Keep in mind that the active parent or child level affects the map view.



**Tip:** If you do not see the site or site level that you expect, ensure that:

- ❖ You are in the applicable parent site.
- ❖ On the **Network Devices** or **Network Device Groups** page, the site's geographical coordinates are configured, or
- ❖ The site that you expect to see is organized under the location group folder that you expect.



**Important Note:** On the **Network Devices** or **Network Device Groups** page, when you add location groups and dependent subgroups, ensure that you configure a logical folder hierarchy that reflects enterprise organization, which helps system users navigate the Map View more efficiently.

## Configuring Health Rules

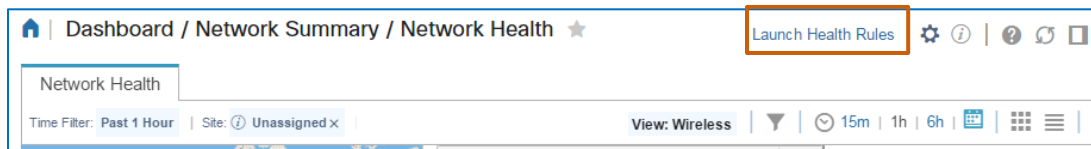
Health rules define the thresholds that the **Network Health** dashboard applies when reporting health issues in its views and on the **Health Summary**.

Health rules define the warning and critical reporting thresholds based on operationally acceptable values for service, infrastructure, and wireless health statuses.

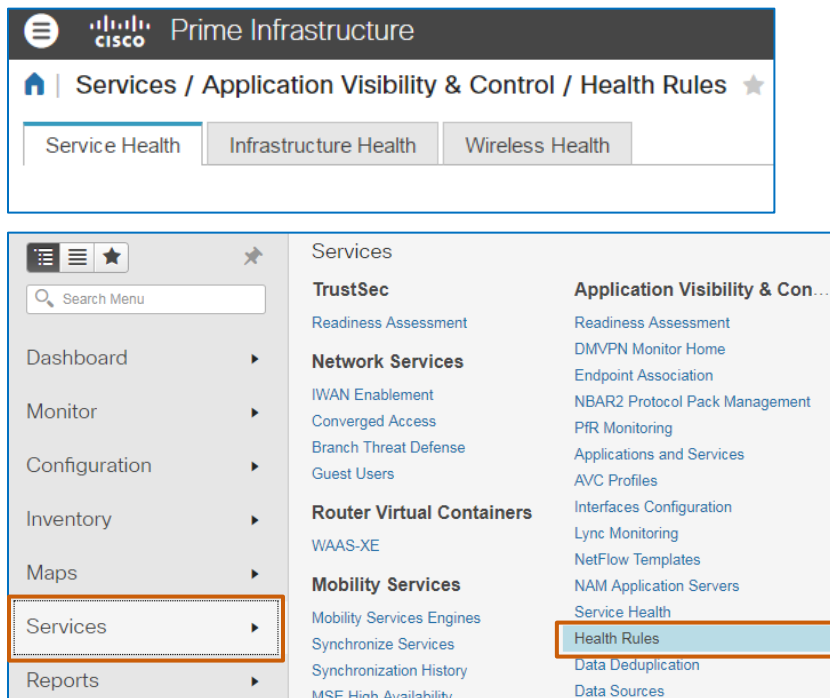
You configure health rules on the **Services | Application Visibility & Control | Health Rules** page.

To navigate to the Health Rule page, on the Network Health page, below the toolbar:

- ❖ Click **Launch Health Rules**.



This action navigates you to the **Health Rules** page, which you also can access on the **Service** menu.

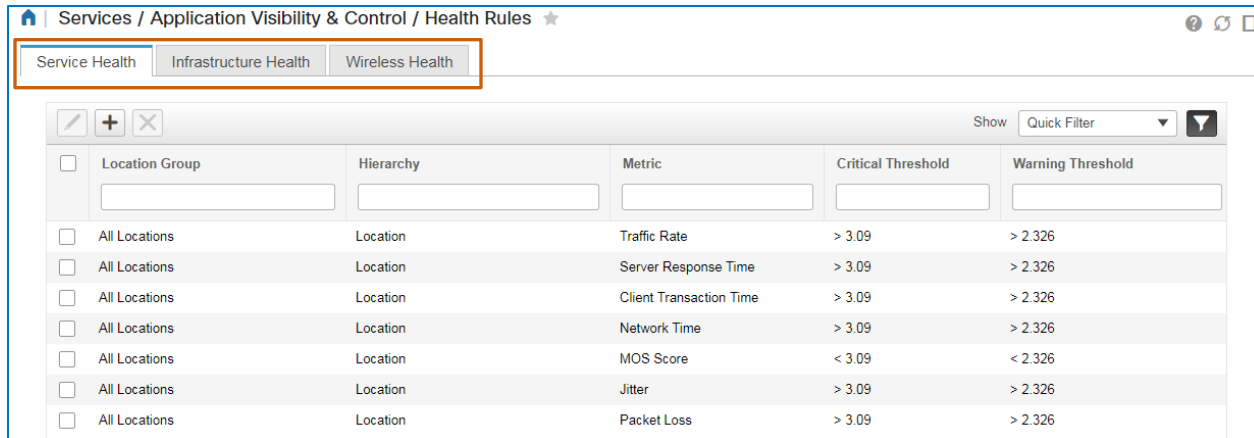


By default, Prime Infrastructure defines the key performance metric baselines, each with two severity level thresholds, critical and warning, which are based on the standard deviation of each metric from its baseline.

It then calculates the baseline values against the threshold values to help determine abnormal deviations in the metrics.

When a health metric exceeds either a warning or critical threshold, it displays a color-coded severity level indicator on the Network Health dashboard page.

The **Health Rule** page includes service, infrastructure, and wireless health metrics thresholds.



| Location Group | Hierarchy | Metric                  | Critical Threshold | Warning Threshold |
|----------------|-----------|-------------------------|--------------------|-------------------|
| All Locations  | Location  | Traffic Rate            | > 3.09             | > 2.326           |
| All Locations  | Location  | Server Response Time    | > 3.09             | > 2.326           |
| All Locations  | Location  | Client Transaction Time | > 3.09             | > 2.326           |
| All Locations  | Location  | Network Time            | > 3.09             | > 2.326           |
| All Locations  | Location  | MOS Score               | < 3.09             | < 2.326           |
| All Locations  | Location  | Jitter                  | > 3.09             | > 2.326           |
| All Locations  | Location  | Packet Loss             | > 3.09             | > 2.326           |

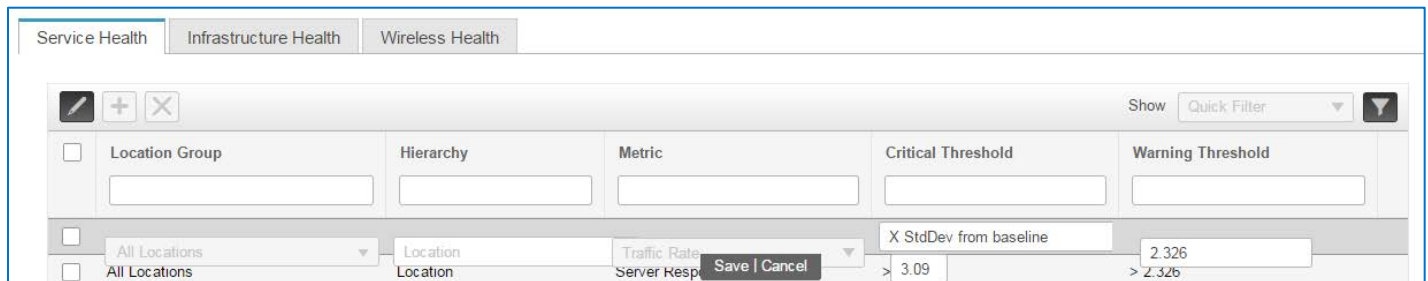
You can configure the critical and warning threshold values for all of the health rule types. You also can configure additional health rules and assign them to specific location groups.



**Note:** For detailed steps on configuring health rules, [refer to the Cisco Prime Infrastructure 3.2 User Guide](#).



**Tip:** When configuring location-specific infrastructure and wireless health rules, you can define varying warning or critical thresholds, which provides flexibility to monitor network health against discrete operational or business requirements.



| Location Group | Hierarchy | Metric               | Critical Threshold     | Warning Threshold |
|----------------|-----------|----------------------|------------------------|-------------------|
| All Locations  | Location  | Traffic Rate         | X StdDev from baseline | 2.326             |
| All Locations  | Location  | Server Response Time | > 3.09                 | > 2.326           |

## Service Health Metrics Reporting

On service health, the system reports the following metrics:

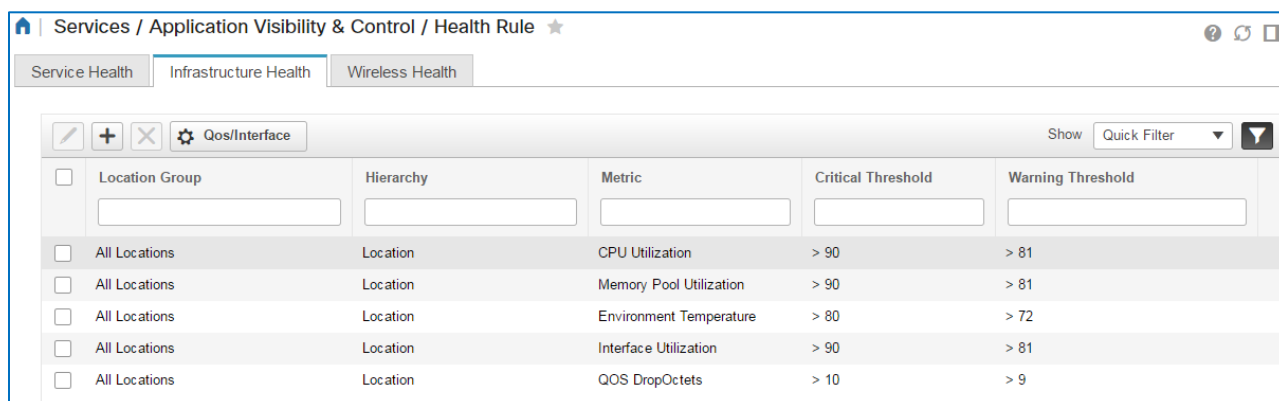
- ❖ Client transaction time
- ❖ Jitter
- ❖ Mean opinion score (MOS) of the telephony experience
- ❖ Network time, which reports the time that it takes for packets to traverse the network between the client and server
- ❖ Packet loss
- ❖ Server response time
- ❖ Traffic rate

| Service Health    Infrastructure Health    Wireless Health   |                |           |                         |                    |           |
|--|----------------|-----------|-------------------------|--------------------|-----------|
| <div> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <div>Show Quick Filter</div> </div> |                |           |                         |                    |           |
| <input type="checkbox"/>   | Location Group | Hierarchy | Metric                  | Critical Threshold | Warning T |
| <input type="checkbox"/>   | All Locations  | Location  | Traffic Rate            | > 3.09             | > 2.326   |
| <input type="checkbox"/>   | All Locations  | Location  | Server Response Time    | > 3.09             | > 2.326   |
| <input type="checkbox"/>   | All Locations  | Location  | Client Transaction Time | > 3.09             | > 2.326   |
| <input type="checkbox"/>   | All Locations  | Location  | Network Time            | > 3.09             | > 2.326   |
| <input type="checkbox"/>   | All Locations  | Location  | MOS Score               | < 3.09             | < 2.326   |
| <input type="checkbox"/>   | All Locations  | Location  | Jitter                  | > 3.09             | > 2.326   |
| <input type="checkbox"/>   | All Locations  | Location  | Packet Loss             | > 3.09             | > 2.326   |

## Infrastructure Metrics Reporting

On infrastructure health, the system reports the following metrics on wired devices:

- ❖ CPU, memory pool, and interface usage
- ❖ Environment temperature
- ❖ The amount of quality of service (QoS) octets that the network is dropping for various classes of network traffic

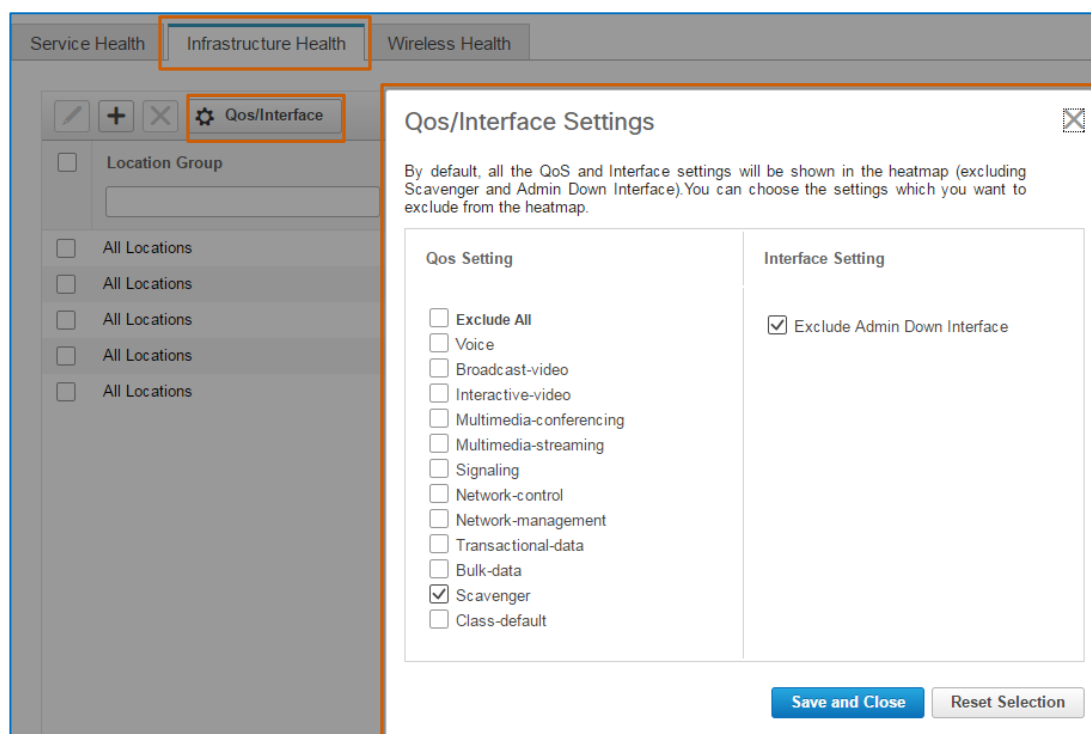


| Services / Application Visibility & Control / Health Rule |                |           |                         |                    |                   |
|---|----------------|-----------|-------------------------|--------------------|-------------------|
| Service Health Infrastructure Health Wireless Health      |                |           |                         |                    |                   |
| Qos/Interface   |                |           |                         |                    |                   |
|   | Location Group | Hierarchy | Metric                  | Critical Threshold | Warning Threshold |
| <input type="checkbox"/>                                  | All Locations  | Location  | CPU Utilization         | > 90               | > 81              |
| <input type="checkbox"/>                                  | All Locations  | Location  | Memory Pool Utilization | > 90               | > 81              |
| <input type="checkbox"/>                                  | All Locations  | Location  | Environment Temperature | > 80               | > 72              |
| <input type="checkbox"/>                                  | All Locations  | Location  | Interface Utilization   | > 90               | > 81              |
| <input type="checkbox"/>                                  | All Locations  | Location  | QOS DropOctets          | > 10               | > 9               |

By default, the system reports on all network traffic classes, except for the Scavenger class of traffic, which includes the least important business applications.

**To exclude other classes of traffic that you do not need users to monitor:**

- ❖ On the toolbar, click **Qos/Interface**, and in the dialog box, under **Qos Setting**, select the check box beside each class of traffic that you do not need to monitor, and then click **Save and Close**.



Service Health
Infrastructure Health
Wireless Health

Qos/Interface

Location Group

All Locations

All Locations

All Locations

All Locations

All Locations

Qos/Interface Settings

By default, all the QoS and Interface settings will be shown in the heatmap (excluding Scavenger and Admin Down Interface). You can choose the settings which you want to exclude from the heatmap.

Qos Setting

☐ Exclude All
☐ Voice
☐ Broadcast-video
☐ Interactive-video
☐ Multimedia-conferencing
☐ Multimedia-streaming
☐ Signaling
☐ Network-control
☐ Network-management
☐ Transactional-data
☐ Bulk-data
☒ Scavenger
☐ Class-default

Interface Setting

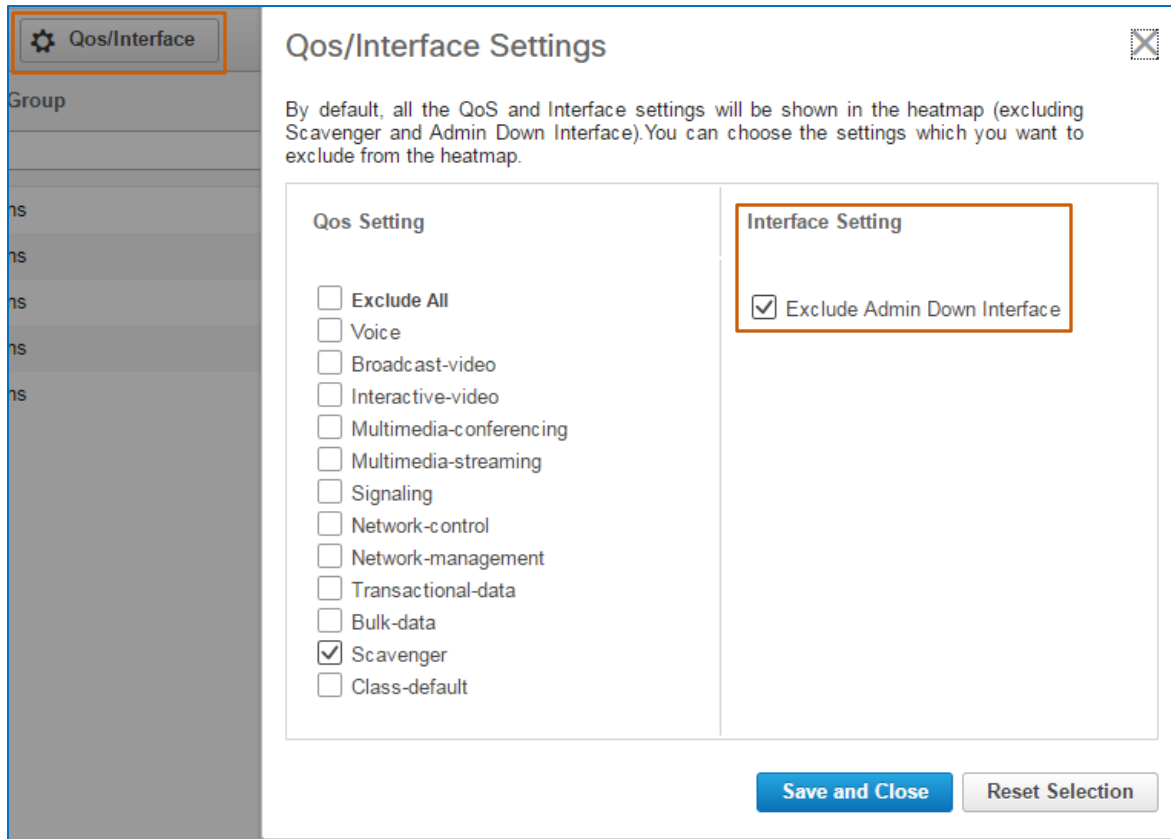
☒ Exclude Admin Down Interface

Save and Close

Reset Selection

In the **Qos/Interface** dialog box, in the **Interface Settings** section, the system excludes reporting that an administrative interface is reporting a down condition by default.

You can clear the check box and save the change to include reporting for that metric.



The image shows the 'Qos/Interface Settings' dialog box. On the left is a sidebar with a 'Group' section and a list of items. The main area is titled 'Qos/Interface Settings' and contains a text block explaining that by default, all QoS and Interface settings are shown in the heatmap, except for Scavenger and Admin Down Interface. Below this are two sections: 'Qos Setting' and 'Interface Setting'. The 'Qos Setting' section has a list of checkboxes: 'Exclude All', 'Voice', 'Broadcast-video', 'Interactive-video', 'Multimedia-conferencing', 'Multimedia-streaming', 'Signaling', 'Network-control', 'Network-management', 'Transactional-data', 'Bulk-data', 'Scavenger' (checked), and 'Class-default'. The 'Interface Setting' section has a single checked checkbox: 'Exclude Admin Down Interface'. At the bottom right are 'Save and Close' and 'Reset Selection' buttons.

## Wireless Health Metrics Reporting

On wireless health, the system reports the following metrics:

- ❖ Channel and interface usage
- ❖ Noise
- ❖ Client count
- ❖ Interferers on wireless channels that are peaking above usage thresholds.

Services / Application Visibility & Control / Health Rule

Service Health Infrastructure Health **Wireless Health**

|                          | Location Group | Hierarchy | Metric                   | Critical Threshold | Warning Thr |
|--------------------------|----------------|-----------|--------------------------|--------------------|-------------|
| <input type="checkbox"/> | All Locations  | Location  | Channel Utilization      | > 90               | > 80        |
| <input type="checkbox"/> | All Locations  | Location  | Interference Utilization | > 60               | > 50        |
| <input type="checkbox"/> | All Locations  | Location  | Noise                    | < 80               | < 90        |
| <input type="checkbox"/> | All Locations  | Location  | Client Count             | > 40               | > 30        |
| <input type="checkbox"/> | All Locations  | Location  | Interface Utilization    | > 90               | > 80        |



## Indicating Business Critical Applications

Business critical applications identify those applications that could cause significant operational issues if they experience disruption or downtime.

System users can [identify applications as business critical](#) when adding or editing services on the **Applications and Services** page.

[Home](#) | [Services / Application Visibility & Control / Applications and Services](#)

Services

←

+

×

All Applications

anonymizers

backup-and-storage

browsing

business-and-productivity-tools

consumer-file-sharing

consumer-internet

consumer-messaging

consumer-streaming

database

email

epayment

file-sharing

gaming

industrial-protocols

instant-messaging

inter-process-rpc

internet-security

layer3-over-ip

Services

All Applications

Edit

Delete

Create

Service

Deploy

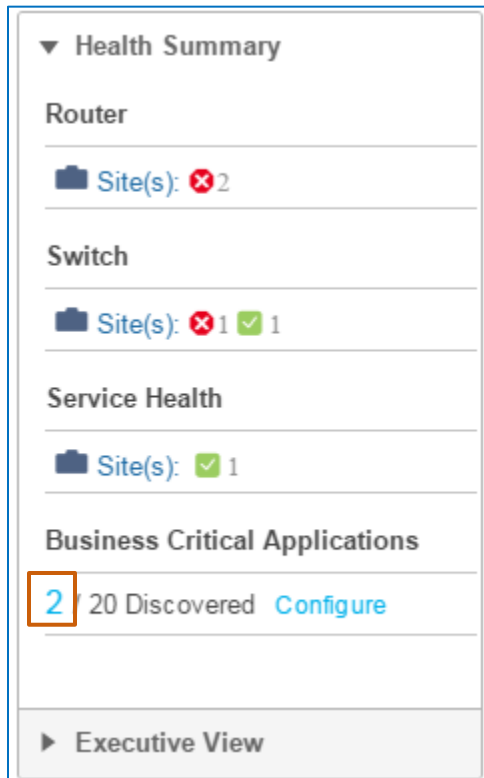
Undeploy

View Jo

| <input type="checkbox"/> | Application Name   | Business Critical | Category                        |
|--------------------------|--------------------|-------------------|---------------------------------|
| <input type="checkbox"/> | webex-meeting      |                   | voice-and-video                 |
| <input type="checkbox"/> | ms-lync            |                   | voice-and-video                 |
| <input type="checkbox"/> | http               |                   | browsing                        |
| <input type="checkbox"/> | arp                |                   | other                           |
| <input type="checkbox"/> | rtp                |                   | voice-and-video                 |
| <input type="checkbox"/> | exchange           |                   | email                           |
| <input type="checkbox"/> | https              |                   | browsing                        |
| <input type="checkbox"/> | telepresence-media |                   | voice-and-video                 |
| <input type="checkbox"/> | share-point        |                   | business-and-productivity-tools |
| <input type="checkbox"/> | sap                |                   | business-and-productivity-tools |
| <input type="checkbox"/> | notes              | No                | other                           |
| <input type="checkbox"/> | opalis-rdv         | No                | other                           |
| <input type="checkbox"/> | opalis-robot       | No                | net-admin                       |
| <input type="checkbox"/> | opc-job-start      | No                | other                           |
| <input type="checkbox"/> | opsmgr             | No                | other                           |

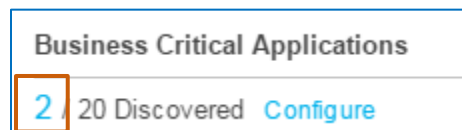
On the **Network Health** page, you can select the business critical applications on which you want the dashboard to report.

Under the **Health Summary | Business Critical Applications**, the number link indicates the number of applications actively being monitored.



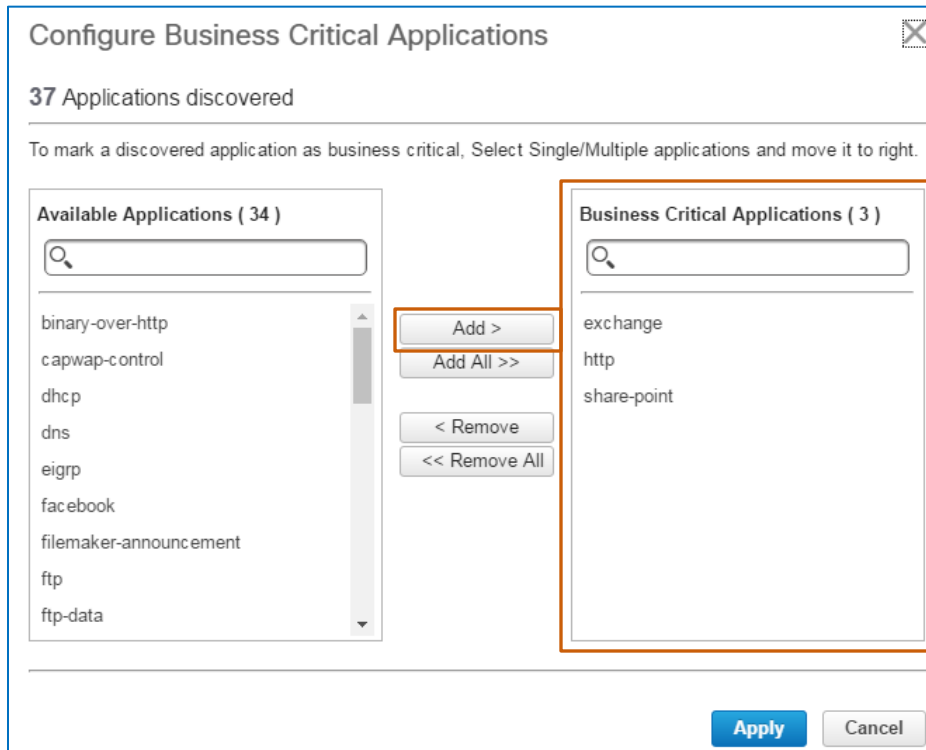
To select business critical applications for or remove them from reporting:

- ❖ On the **Health Summary** panel, under **Business Critical Applications**, click the number link.



The **Configure Business Critical Applications** dialog box opens.

The **Available Applications** section lists all of the business critical applications with the NetFlow traffic reporting feature enabled. You can add applications to **Business Critical Applications** list to enable the system to report their related metrics.



**Configure Business Critical Applications**

37 Applications discovered

To mark a discovered application as business critical, Select Single/Multiple applications and move it to right.

**Available Applications ( 34 )**


- binary-over-http
- capwap-control
- dhcp
- dns
- eigrp
- facebook
- filemaker-announcement
- ftp
- ftp-data

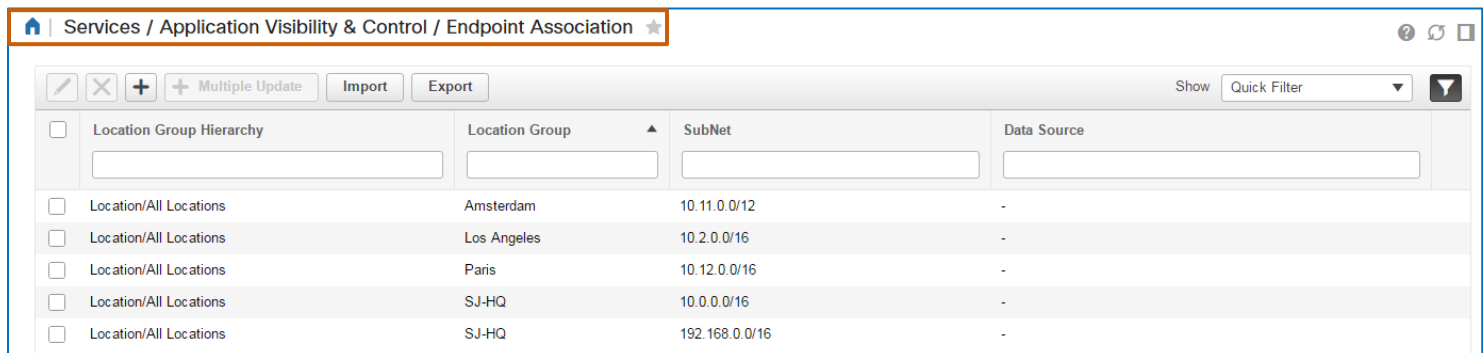
**Business Critical Applications ( 3 )**


- exchange
- http
- share-point

## Identifying Subnets for Site Level Service Health Reporting

By using the endpoint association function, you can relate devices on specific subnets to location groups. Then, the **Network Health** dashboard can report service health issues on the location groups (sites on the **Network Health** dashboard) that system users have added and configured with geographical coordinates.

System users can perform endpoint association on the **Endpoint Association** page on the **Services** menu.



Services / Application Visibility & Control / Endpoint Association

Show

| <input type="checkbox"/> | Location Group Hierarchy | Location Group | SubNet         | Data Source |
|--------------------------|--------------------------|----------------|----------------|-------------|
| <input type="checkbox"/> | Location/All Locations   | Amsterdam      | 10.11.0.0/12   | -           |
| <input type="checkbox"/> | Location/All Locations   | Los Angeles    | 10.2.0.0/16    | -           |
| <input type="checkbox"/> | Location/All Locations   | Paris          | 10.12.0.0/16   | -           |
| <input type="checkbox"/> | Location/All Locations   | SJ-HQ          | 10.0.0.0/16    | -           |
| <input type="checkbox"/> | Location/All Locations   | SJ-HQ          | 192.168.0.0/16 | -           |

# Monitoring Key Performance Indicators (KPIs)

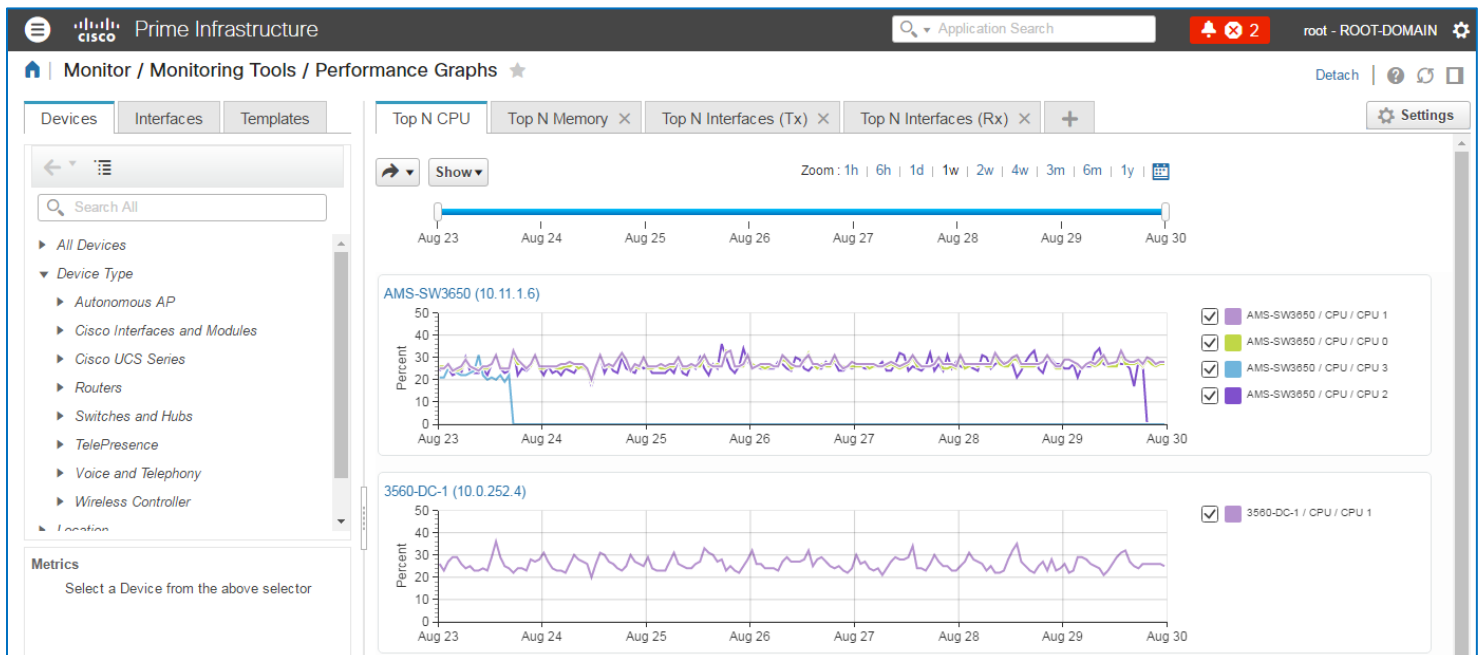
## Performance Graphs

You can monitor current or evaluate historical device- or interface-level performance data for key performance indicators (KPIs) by using the Performance Graphs feature.

You can display alarms and configuration changes in relationship to the KPI values for the component on which a graph is reporting. Correlating changing KPI values to alarm reporting or configuration changes can provide critical insight into possible issues or issue causes.

You have the flexibility to select the device or interface metrics of interest, remove those that do not apply, add custom tabs, and include a series of metrics in a single graph, which provides you with a highly flexible monitoring environment.

Depending on the situation that you are monitoring, you can organize tabs and graphs so that you see the data that you need when you need it.



On initial entry, the **Performance Graphs** page provides four tabs by default, including:

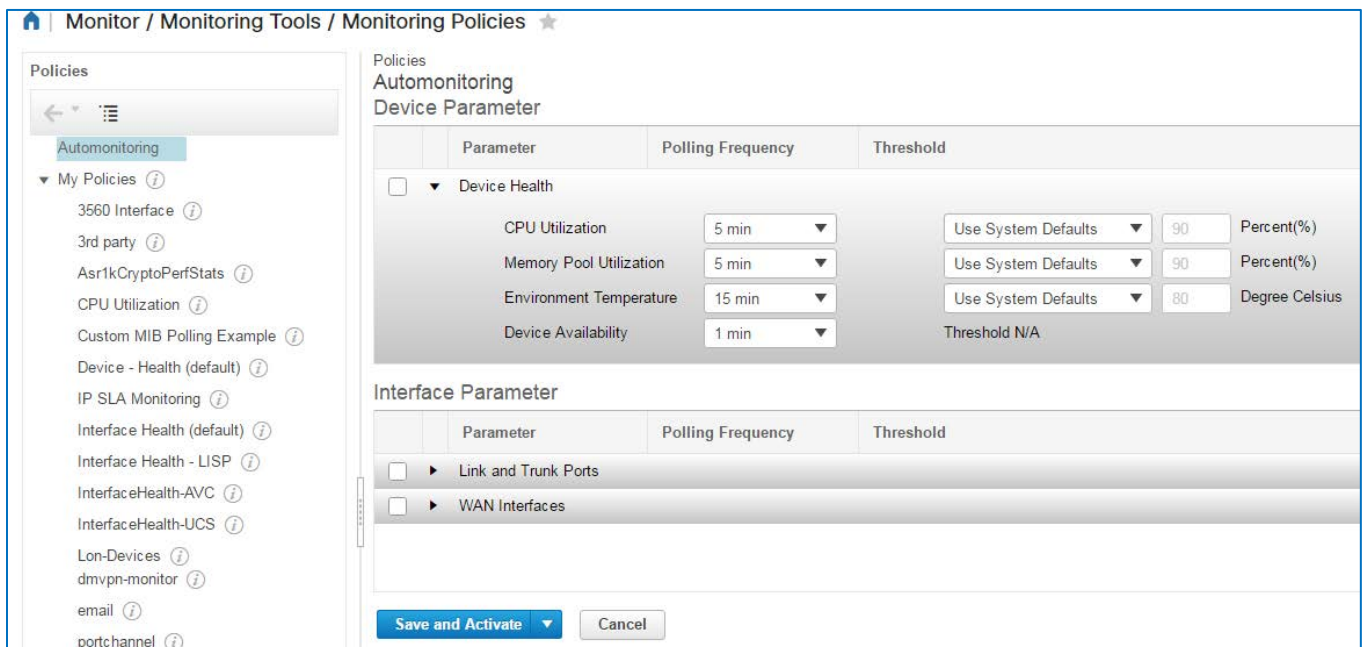
- ❖ **Top N CPU**  
Presents graphs for the devices, up to 10, that are experiencing the highest CPU usage
- ❖ **Top N Memory**  
Presents graphs for the devices, up to 10, that are experiencing the highest memory usage
- ❖ **Top N Interfaces (Tx)**  
Presents graphs for the interfaces, up to 10, that are experiencing the highest bandwidth usage for data that they are transmitting
- ❖ **Top N Interfaces (Rx)**  
Presents graphs for the interfaces, up to 10, that are experiencing the highest bandwidth usage for data that they are receiving

To collect and report the data that you see in performance graphs, the system uses monitoring policies, which indicate the KPIs on which to report, and define the threshold reporting values and polling intervals on the KPI parameters.

On initial startup, Prime Infrastructure enables several policies automatically, referred to as automonitoring policies, which report:

- ❖ Device health metrics.
- ❖ Link port, trunk port, and WAN interface and quality of service (QoS) metrics.

System users also can configure and activate custom monitoring policies to support operational and business monitoring requirements.



Monitor / Monitoring Tools / Monitoring Policies

Policies

Automonitoring

My Policies

- 3560 Interface
- 3rd party
- Asr1kCryptoPerfStats
- CPU Utilization
- Custom MIB Polling Example
- Device - Health (default)
- IP SLA Monitoring
- Interface Health (default)
- Interface Health - LISP
- InterfaceHealth-AVC
- InterfaceHealth-UCS
- Lon-Devices
- dmvpn-monitor
- email
- portchannel

Policies

Automonitoring

Device Parameter

| Parameter               | Polling Frequency | Threshold                             |
|-------------------------|-------------------|---------------------------------------|
| Device Health           |                   |                                       |
| CPU Utilization         | 5 min             | Use System Defaults 90 Percent(%)     |
| Memory Pool Utilization | 5 min             | Use System Defaults 90 Percent(%)     |
| Environment Temperature | 15 min            | Use System Defaults 80 Degree Celsius |
| Device Availability     | 1 min             | Threshold N/A                         |

Interface Parameter

| Parameter            | Polling Frequency | Threshold |
|----------------------|-------------------|-----------|
| Link and Trunk Ports |                   |           |
| WAN Interfaces       |                   |           |

Save and Activate Cancel

## Navigating Performance Graphs

### Managing Graph Data Elements

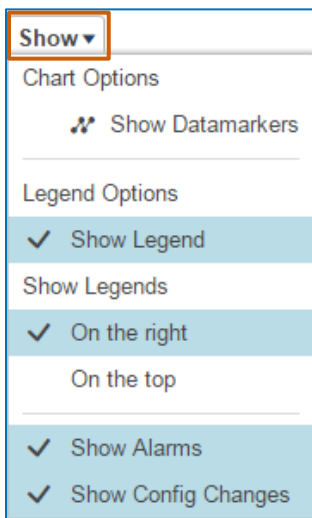
By default, graphs report the KPI metrics that you select for the device or interface. In addition, you can show:

- ❖ Data points, referred to as datamarkers.
- ❖ Alarms.
- ❖ Configuration changes.

You also can control the placement of the legend. On the **Show** drop-down menu, the visible elements are emphasized with a check mark and highlight.



**Note:** The choices you make by using a **Show** drop-down menu apply only to the active tab.



**To show or hide what you see on a graph, on the Show drop-down menu:**

- ❖ Select or clear any **Show** drop-down menu item.

You can indicate your preference of legend placement, either above the graph or on the right side of the graph.

**To indicate legend placement, on the Show drop-down menu:**

- ❖ Select **On the right** or **On the top**.



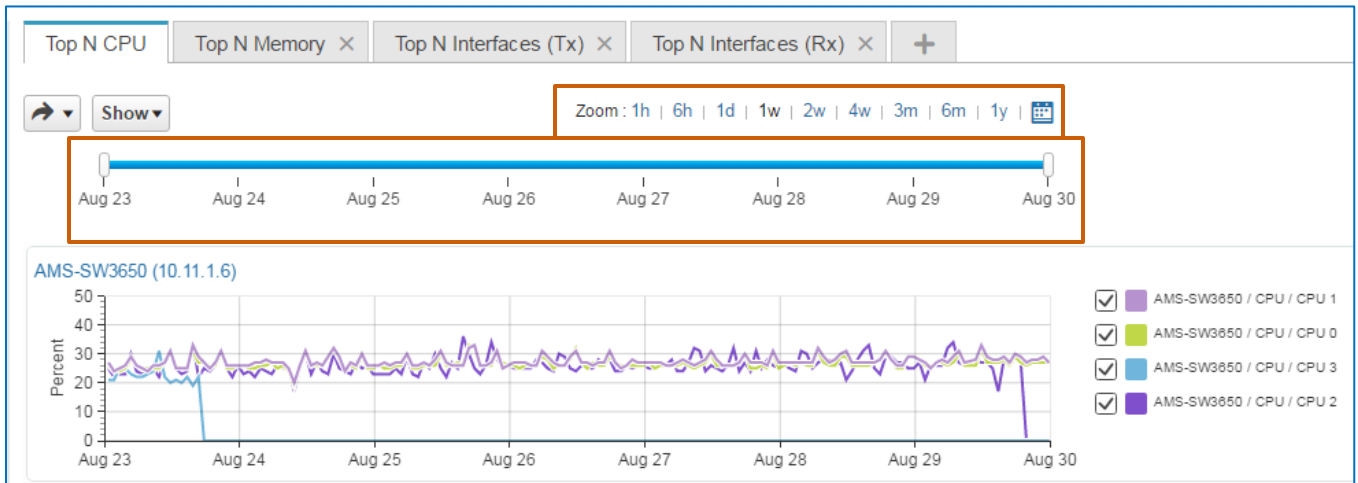
**Note:** You cannot remove the legend from view.

## Changing Graph Timelines

Each tab provides zoom, date range, and horizontal timeline slider tools so that you can control the time period for which the graphs on that tab are displaying data. These tools are available above the tab graphs.



**Note:** The timeline that you indicate applies only to the active tab.



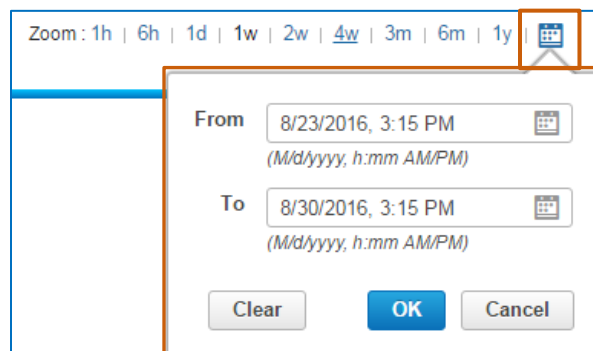
### To apply a pre-defined time period by using the zoom tool:

- ❖ In the **Zoom** field, click the hourly, daily, weekly, monthly, or annual time period link that you want.



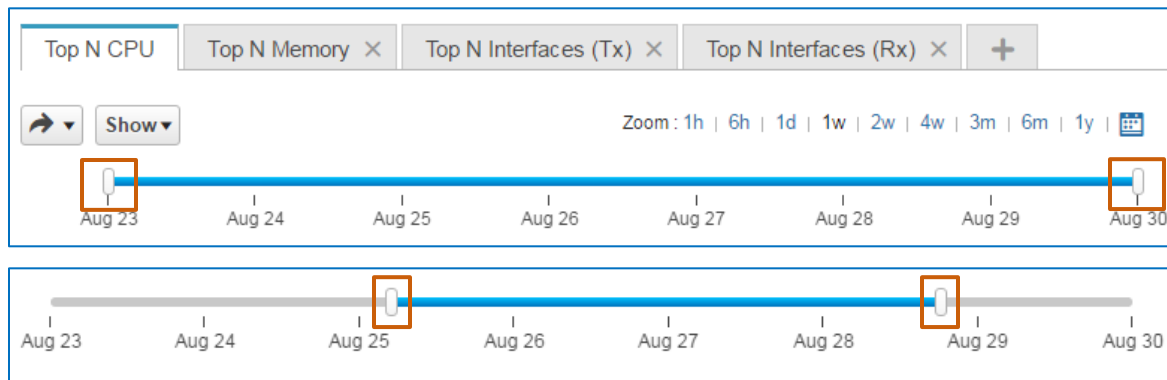
### To apply a custom time period:

- ❖ To the right of the **Zoom** time period link, click **Select a custom date range**, indicate the range that you want, and then click **OK**.



To apply a time period by using the horizontal timeline slider:

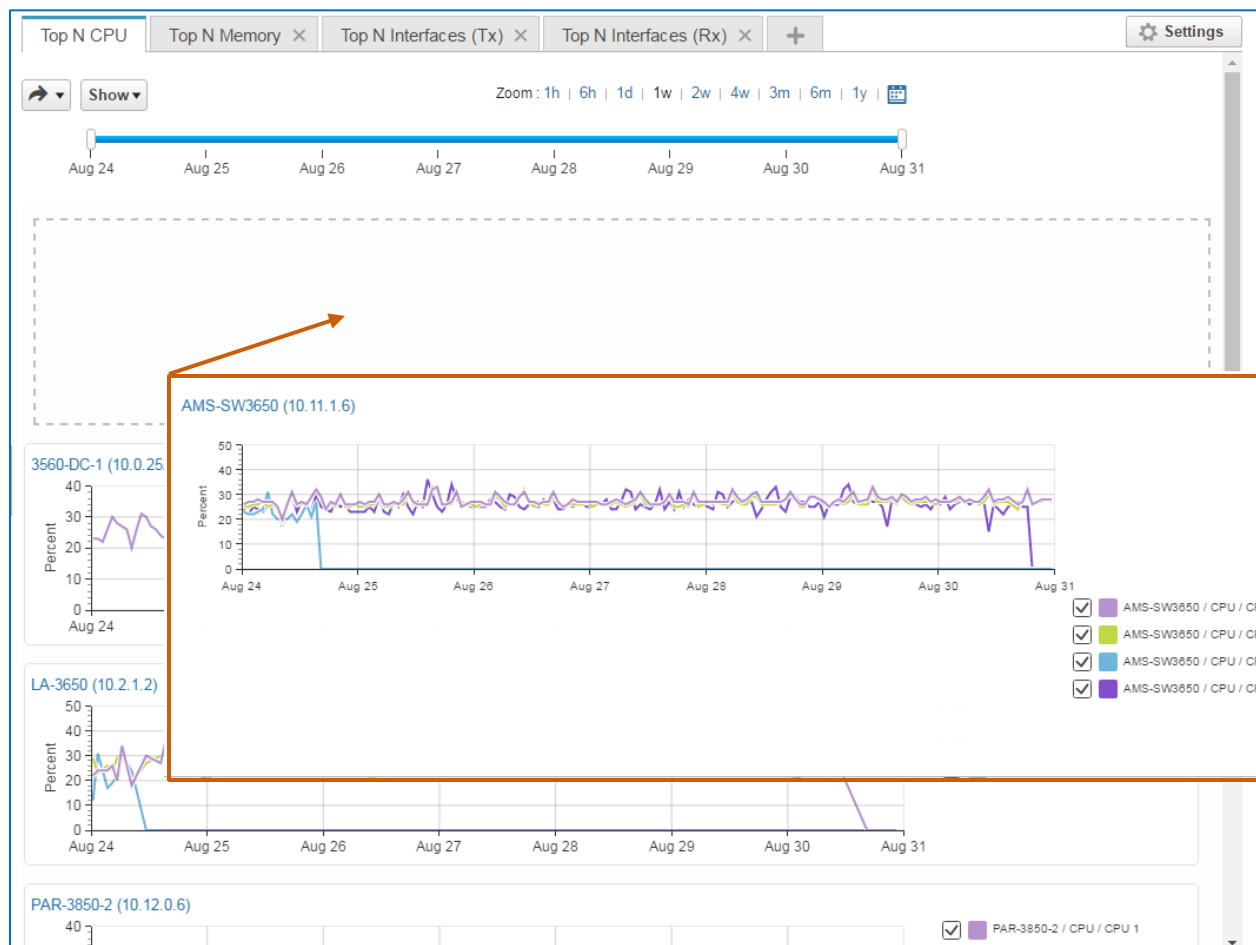
- ❖ On either side of the slider, drag the bar.



## Changing Graph Layouts

You can move graphs on a tab, maximize graphs for better visibility, or collapse graphs to make a series of graphs easier to see.

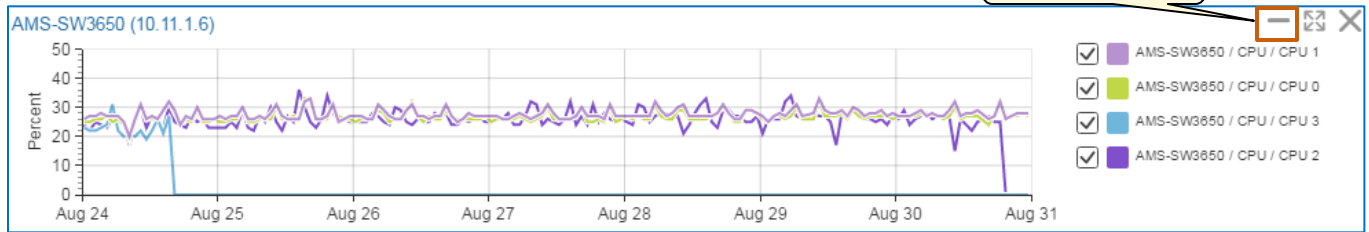
You move graphs using the drag and drop operation.



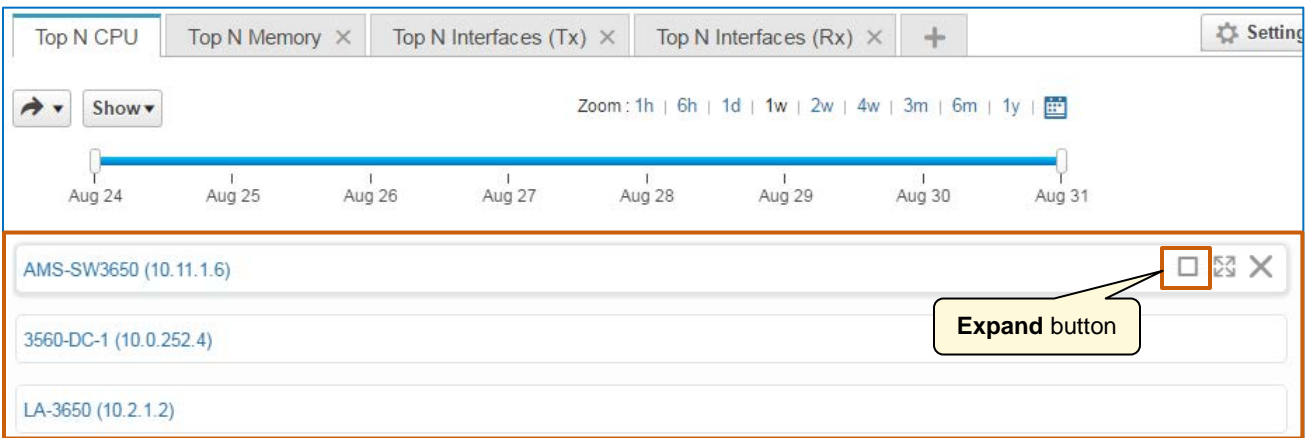


### To collapse a graph:

- ❖ Point to the graph, and then, click **Collapse**.

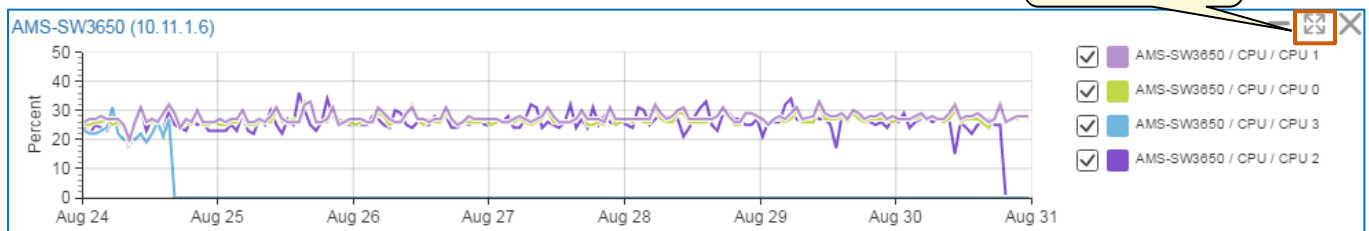


The graph view closes and remains available to expand and view, as needed. The **Collapse** button toggles to the **Expand** button.

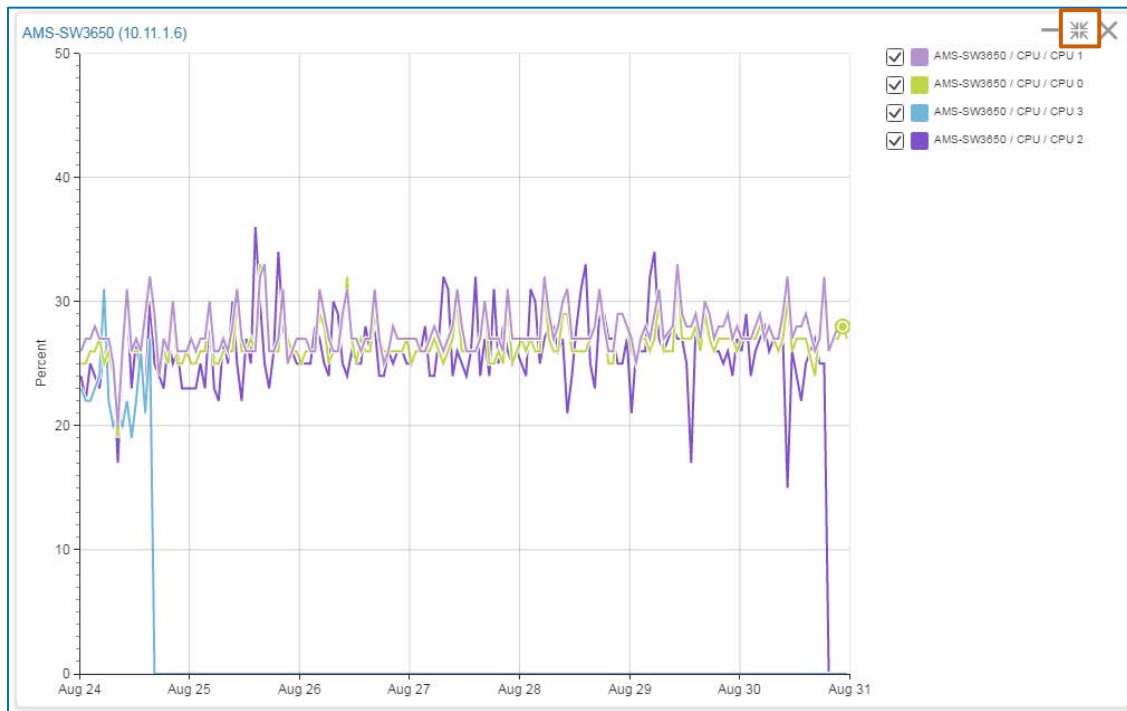


### To maximize a graph:

- ❖ Point to the graph, and then click **Maximize/Restore**.



The graph view maximizes and the button icon changes.

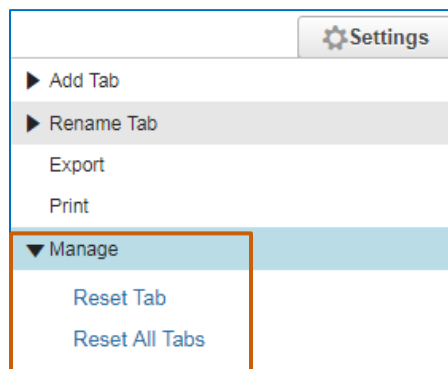


To return the Performance Graphs page or tabs to their default layouts:

- ❖ On the **Settings** menu, under **Manage**:
  - ◆ To return the active tab on the page to its default layout, click **Reset Tab**.
  - ◆ To return all of the tabs to their default layouts, click **Reset all Tabs**.



**Important Note:** When you reset all of the tab layouts, this action removes any custom tabs that you have added, also.



## Managing Performance Graphs

### Seeing the Data That You Need

---

When you first use performance graphs, the system [provides four default tabs with graphs](#).

Depending on the metrics that you need to monitor the network or evaluate potential issues, you might consider organizing performance graphs by:

- ❖ Adding or removing the default tabs.
- ❖ Adding or removing graphs from default tabs.
- ❖ Adding custom tabs with the graphs that you need.

For example, you might add a custom tab that includes key metrics for devices that you need to monitor regularly. That way, you can have the information available in a single view.

- ❖ Layering several metrics on a single graph for comparative or data correlation purposes.
- ❖ Layering configuration changes and alarm reporting over device metrics for comparison purposes.

For example, while evaluating a device reporting CPU values that are exceeding critical thresholds, you can display alarms or configuration changes to determine if there is any relationship between those activities and the excessive CPU values.

## Adding or Removing Device or Interface Graphs to Tabs

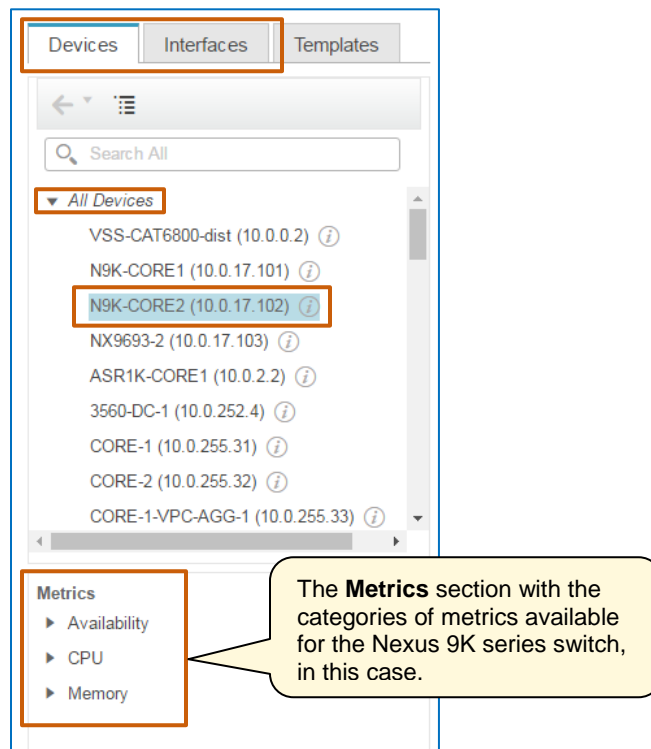
You add graphs by selecting the device or interface of interest, and then selecting the metrics that you need to see.

You select device or interface related metrics by following the same steps.

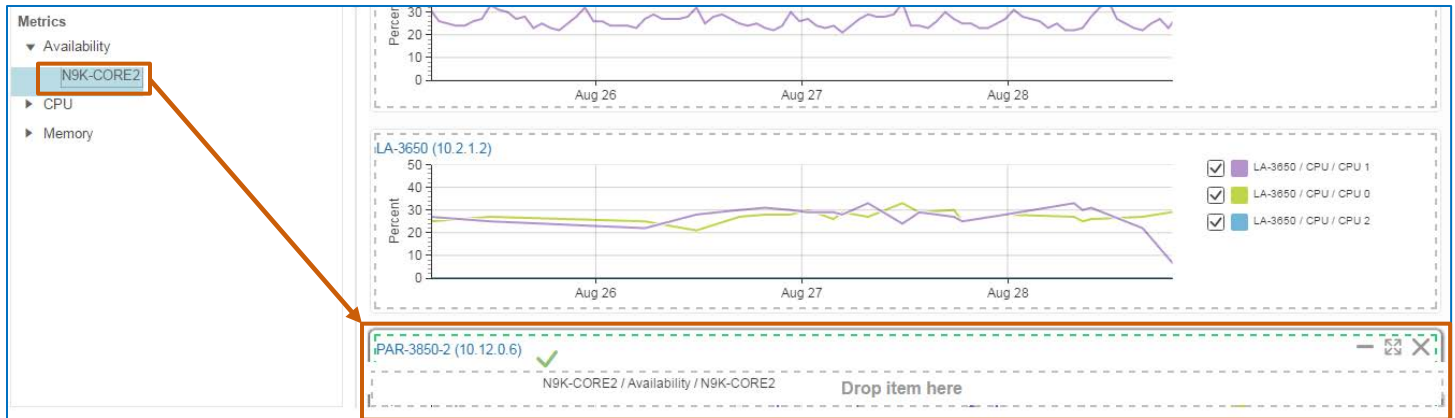
### To add a device or interface graph:

1. On the **Devices** or **Interfaces** tab, in the devices list, expand the category of interest, and then locate and select the device or device interface.

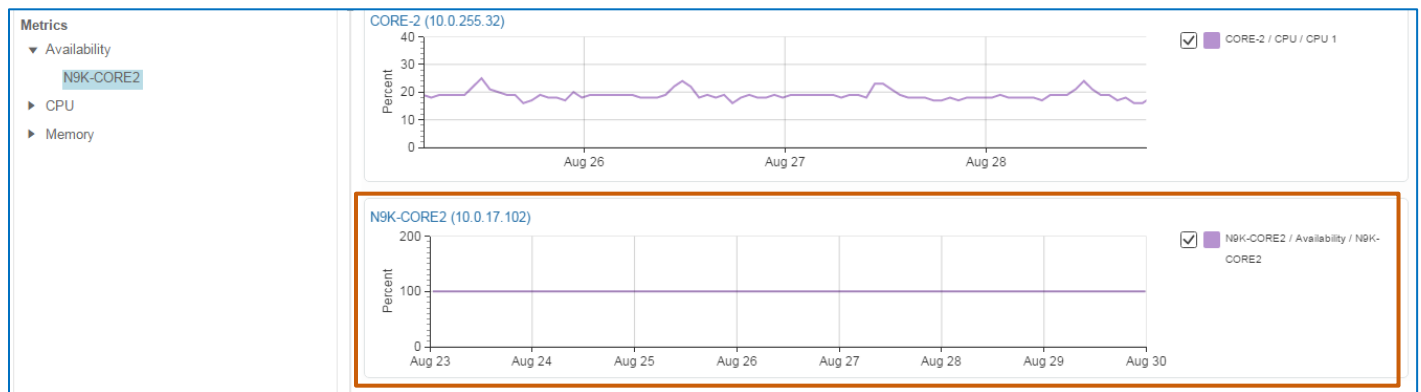
Below the list, the **Metrics** section populates with the categories of metrics that are available for the element that you selected.



- In the **Metrics** section, expand the category of interest, and then drag the entry toward the bottom right of the window until you see a green highlight and check mark, and a message to drop the item in the highlighted location...



...and then drop the item. The graph appears below all of the other graphs that are visible on the tab.



To see any configuration changes that occurred during the time period:

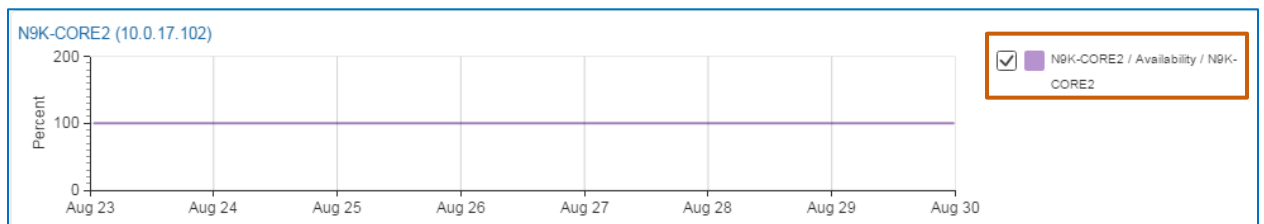
- ❖ On the **Show** drop-down menu, select **Show Config Changes**.

To see any alarms that the system is reporting during the time period:

- ❖ On the **Show** drop-down menu, select **Show Alarms**.

To see alarms or configuration changes without the metric that you selected:

- ❖ In the legend, clear the metric's check box.

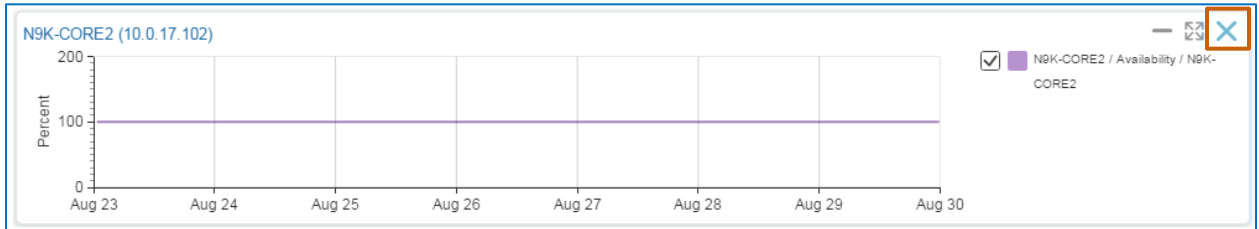


You can remove graphs that do not apply to your task or that you no longer need.

### To remove a graph:

- ❖ Point to the graph, and then, on the toolbar that appears in the upper right corner, click **Close**.

The system removes the graph.



## Adding or Removing Tabs

While the **Performance Graphs** page provides default tabs, you can add custom tabs or remove those tabs that you do not need.

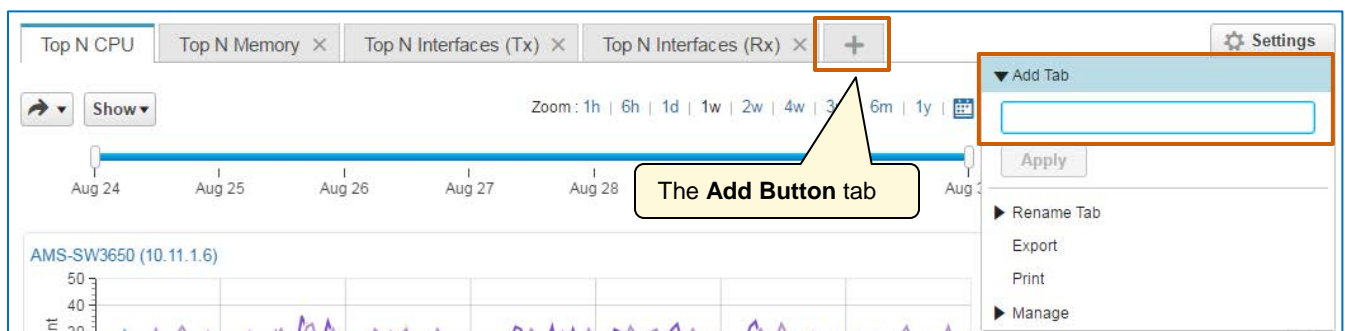


**Note:** The custom tabs that you add are only available to you in the virtual domain in which you add them. If you work in another virtual domain to which you have access, you will not see the tab.

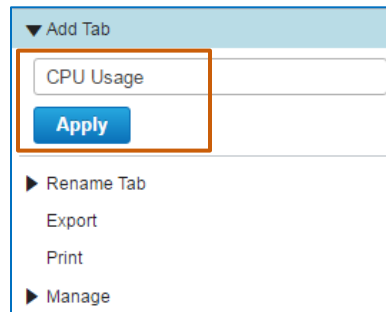
### To add a custom tab:

1. In the tab row, click **Add Button**.

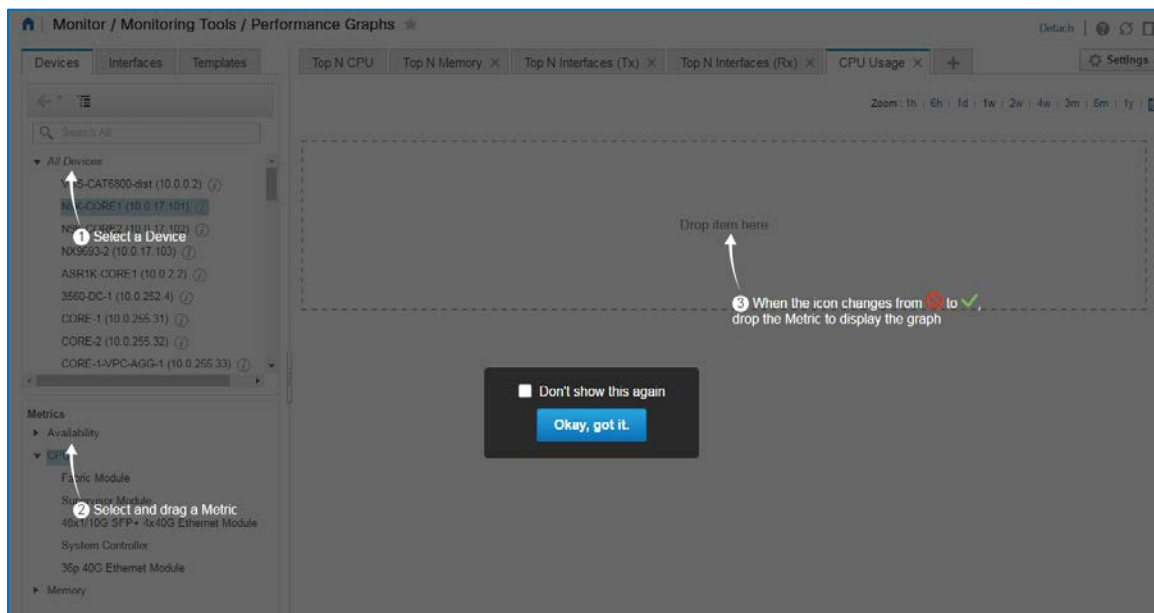
The **Settings** drop-down menu opens with the **Add Tab** field active.



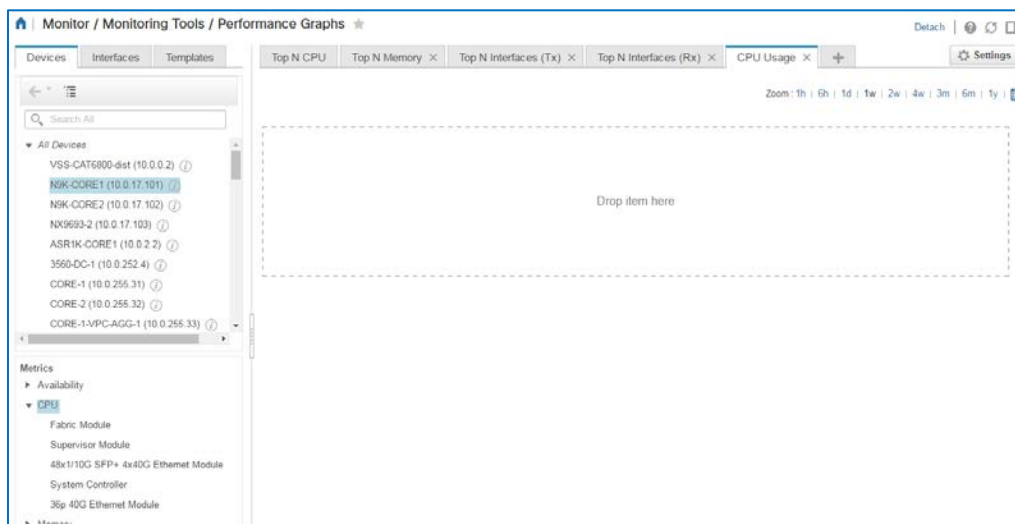
- In the **Add Tab** field, type the name of the tab as you want it to appear on the page, and then click **Apply**.



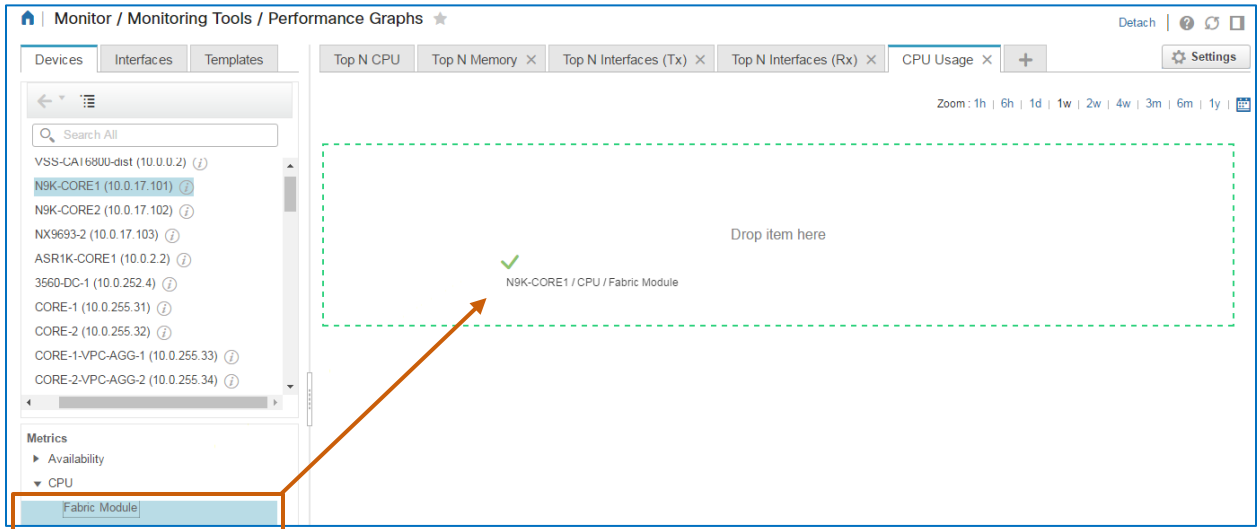
On initial use, a help overlay opens, which you can configure to remain closed when you no longer need it.



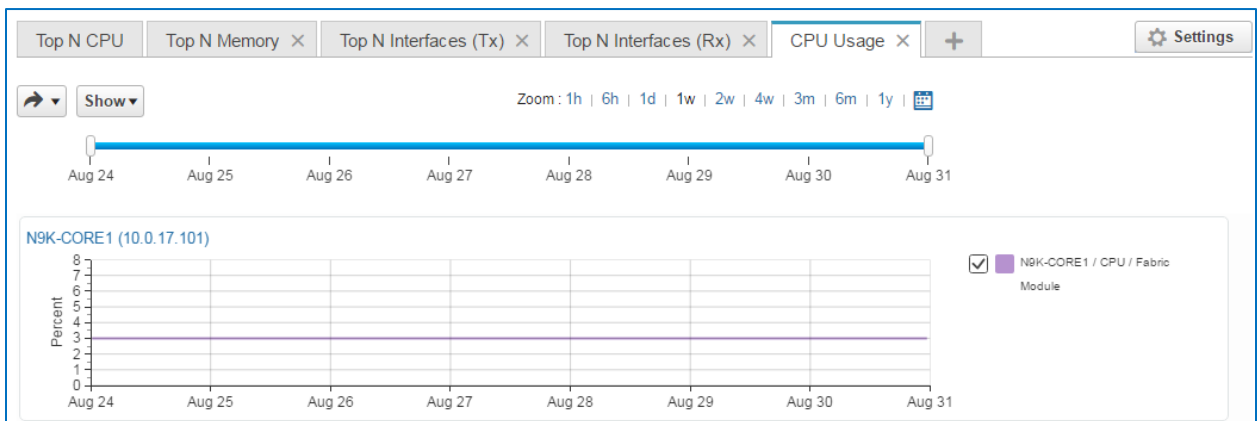
When you clear the overlay, the tab that you added is available for adding graphs.



3. In the device list, select the device that you need.
4. In the **Metrics** list, expand the category, and then drag the metric for the device element that you want and drop it in the container.



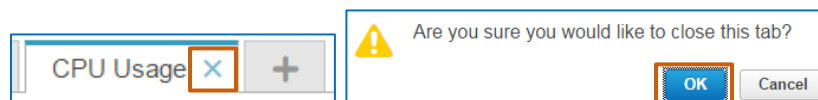
The graph begins reporting data by using the applicable polling interval for the KPI.



5. To continue adding graphs to the tab, repeat steps 3 and 4.

#### To remove a tab:

- ❖ On the tab, click **Close**, and then, in the system message, click **OK**.



The system removes the tab.

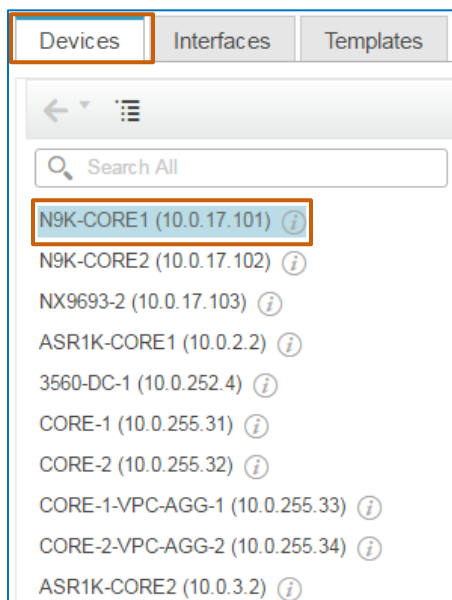


## Adding Multiple Metrics to Graphs

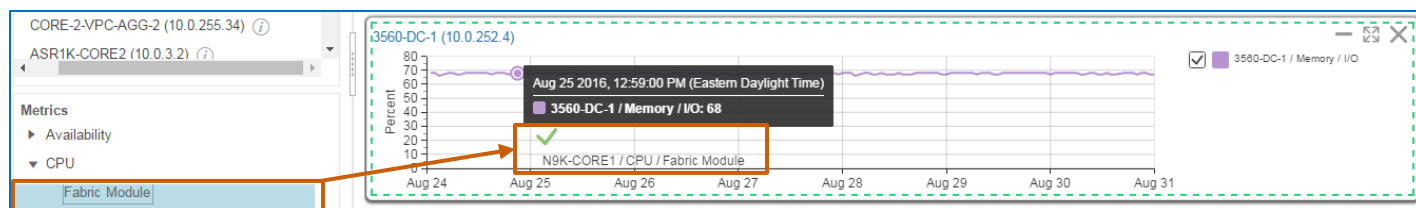
For comparative purposes, you can add multiple metrics to a single graph. For example, you might find it helpful to add CPU and memory metrics for a component on a single graph to determine whether issues related to either metric correlate.

**To add multiple metrics to a graph:**

1. In the device or interface list, select the device or interface.



2. Under **Metrics**, drag the metric, and then drop it on the graph.



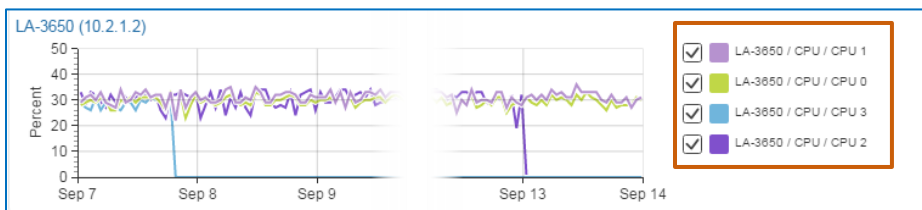
3. To continue adding metrics to the graph, repeat steps 1 and 2.



**Note:** You can add up to 10 metrics on a single graph.

**To remove a metric on a graph from view:**

- ❖ Beside the graph, clear the check box of the metric.



## Monitoring Devices or Interfaces Reporting the Highest Metrics

You can select metrics of interest, which can help you identify devices or interfaces that might be nearing or peaking above operational limits. This information can help you mitigate or avoid potential issues.

You can evaluate network elements that are experiencing the highest:

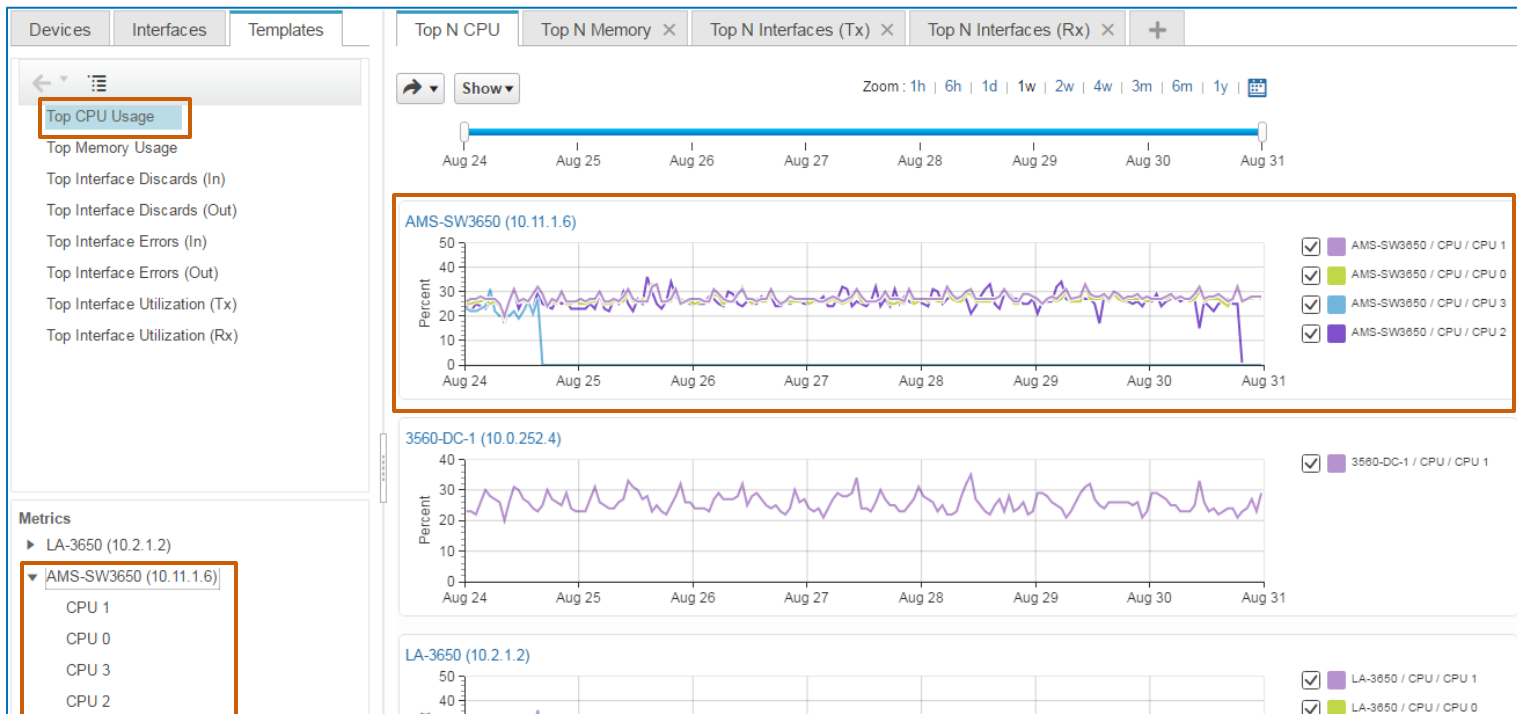
- ❖ CPU usage
- ❖ Memory usage
- ❖ Interface inbound or outbound packet discards
- ❖ Interface inbound or outbound packet processing errors
- ❖ Interface transmitting (Tx) or receiving (Rx) bandwidth usage

When you select a metric, the system lists all of the devices reporting the metric as trending with higher values than other devices.

You select metrics on the **Templates** tab, then, under **Metrics**, it lists those devices reporting the highest levels of the metric.



You can [follow the steps to add graphs with single device or interface metric](#); or [follow the steps to add multiple metrics on a single graph](#), as needed.



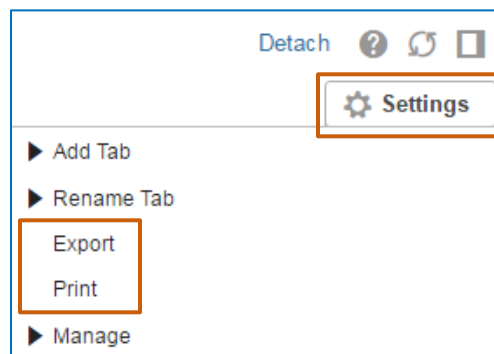
## Exporting or Printing Graph Data

You can export or print graph data at a global or tab level.

When you use the export function, the system generates a PDF-formatted file. When you use the print function, the system opens the print functions that are available to you.

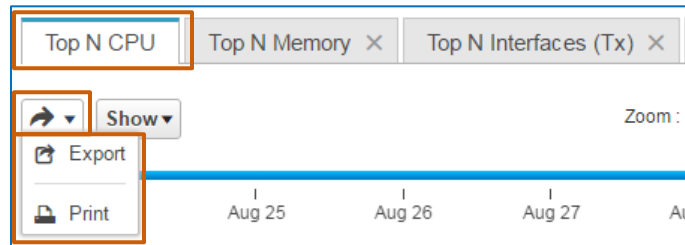
**To export or print global level data:**

- ❖ On the **Settings** menu:
  - ◆ To export the data, click **Export**.
  - ◆ To use print functions to capture the data, click **Print**.



### To export or print tab level data:

- ❖ On the active tab, click the arrow button, and then click the action that you want.

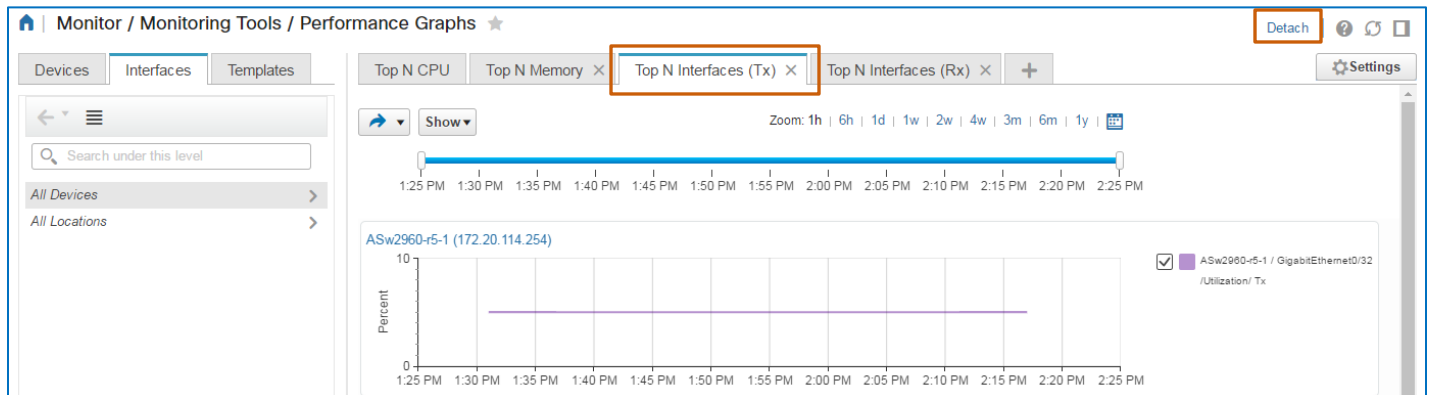


### Opening Graph Tabs in Separate Windows

You can open graph tabs in separate windows so that data is readily accessible for ongoing monitoring or troubleshooting.

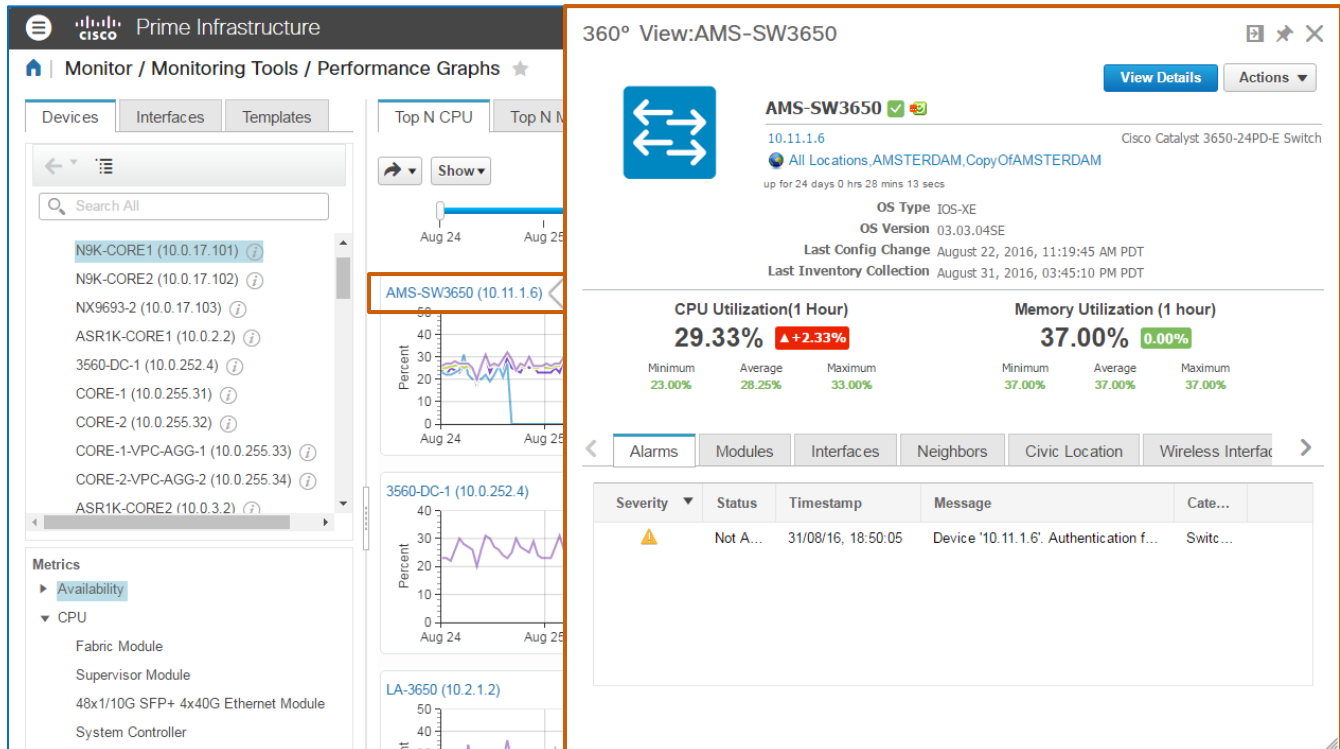
### To open a tab in a separate window:

- ❖ Select the tab containing the data that you want, and then click **Detach**.



## Reviewing Device or Interface Details or Taking Actions

Performance graphs provide direct access to device details in a device **360° View** pop-up window, such as device type and location, performance metrics, alarms, and neighboring devices among other information, which is based on device type.

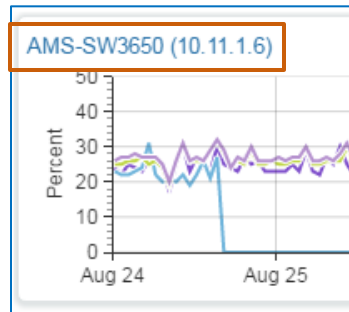


The screenshot displays the Cisco Prime Infrastructure interface. On the left, the 'Monitor / Monitoring Tools / Performance Graphs' section is active, showing a list of devices under the 'Devices' tab. The device 'AMS-SW3650 (10.11.1.6)' is highlighted. The main area shows the '360° View:AMS-SW3650' pop-up window. This window provides detailed information about the device, including its IP address, location, OS type, version, and configuration changes. It also displays performance metrics for CPU and Memory utilization over a 1-hour period. Below the metrics, there are tabs for 'Alarms', 'Modules', 'Interfaces', 'Neighbors', 'Civic Location', and 'Wireless Interfaces'. The 'Alarms' tab is currently selected, showing a table of active alarms.

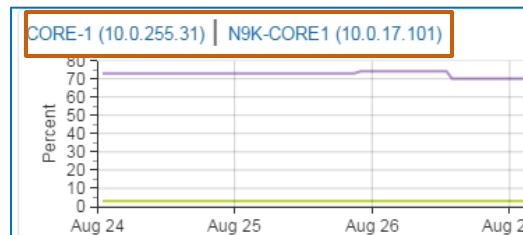
| Severity | Status   | Timestamp          | Message                                 | Cate...  |
|----------|----------|--------------------|---|----------|
| Warning  | Not A... | 31/08/16, 18:50:05 | Device '10.11.1.6'. Authentication f... | Switc... |

**To open a 360° View pop-window:**

- ❖ On a graph, click the name link on the graph.





**Note:** When a graph includes more than one device or interface, links are available for each device at the top of the graph.



In addition to finding key information about the device, you can open the details and configuration, or take actions, as needed.

360° View:3560-DC-1



3560-DC-1 

10.0.252.4

Cisco Catalyst 3560E-24PD-E,S Switch

All Locations, System Campus

up for 24 days 16 hrs 30 mins 20 secs

OS Type IOS

OS Version 12.2(52)SE


Last Config Change July 28, 2016, 09:59:21 PM PDT

Last Inventory Collection September 01, 2016, 07:41:18 AM PDT

View Details

Actions

CPU Utilization(1 Hour)

27.00%  +2.00%

Minimum

18.00%


Average

25.18%

Maximum

31.00%

Memory Utilization (1 hour)

67.00%  0.00%

Minimum

67.00%

Average

67.55%

Maximum

68.00%

Alarms





Modules

Interfaces

Neighbors

Civic Location

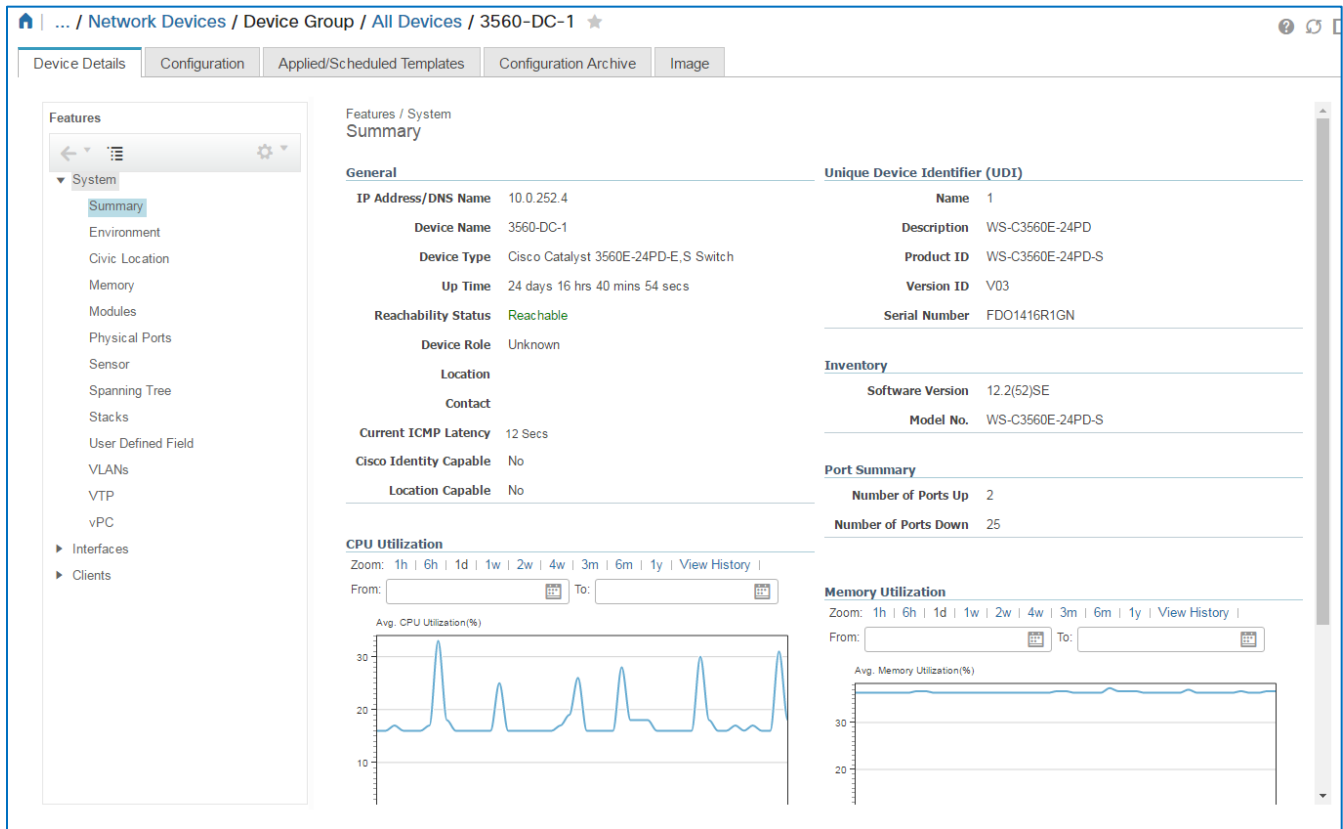
Recent Changes

| Severity  | Status             | Timestamp          | Message                     | Category          |
|---|--------------------|--------------------|-----------------------------|-------------------|
|  | Not Acknowledge... | 26/11/15, 22:21:10 | Device 3560-DC-1/Proce...   | Switches and Hubs |
|  | Not Acknowledge... | 26/11/15, 22:21:10 | Device 3560-DC-1/I/O: v...  | Switches and Hubs |
|  | Not Acknowledge... | 26/11/15, 22:21:10 | Device 3560-DC-1/Driver ... | Switches and Hubs |
|  | Not Acknowledge... | 26/11/15, 22:23:22 | Device 3560-DC-1/CPU 1...   | Switches and Hubs |

**To open device details:**

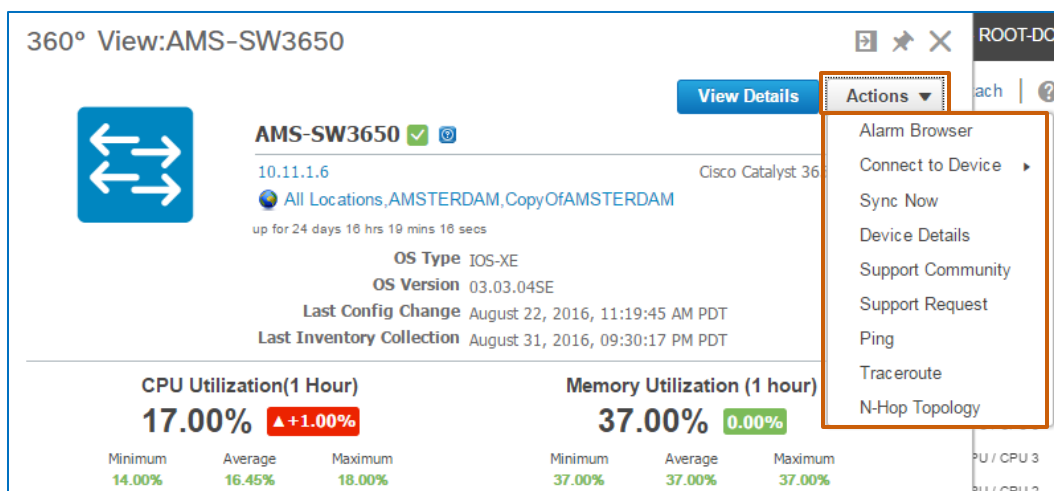
- ❖ In the device **360° View** pop-up window, click **View Details**.

The system navigates to the device details, which provide access to device components, configurations and configuration history, and the device software image information.



The screenshot displays the 'Device Details' page for a Cisco Catalyst 3560E-24PD-E switch. The interface includes a left-hand navigation menu with categories like System, Interfaces, and Clients. The main content area is divided into several sections: General (IP Address/DNS Name, Device Name, Device Type, Up Time, Reachability Status, Device Role, Location, Contact, Current ICMP Latency, Cisco Identity Capable, Location Capable), Unique Device Identifier (UDI) (Name, Description, Product ID, Version ID, Serial Number), Inventory (Software Version, Model No.), Port Summary (Number of Ports Up, Number of Ports Down), CPU Utilization (line graph showing average CPU utilization over time), and Memory Utilization (line graph showing average memory utilization over time).

By using the **Actions** drop-down menu, you can take direct actions, access support, or open alarm or device details.



The screenshot shows the '360° View:AMS-SW3650' interface. It displays the device name 'AMS-SW3650' with a status icon, IP address '10.11.1.6', and location 'All Locations, AMSTERDAM, CopyOfAMSTERDAM'. The device is up for 24 days 16 hrs 19 mins 16 secs. The OS Type is IOS-XE and the OS Version is 03.03.04SE. The last configuration change was on August 22, 2016, at 11:19:45 AM PDT, and the last inventory collection was on August 31, 2016, at 09:30:17 PM PDT. The CPU Utilization (1 Hour) is 17.00% (up 1.00% from 14.00% minimum to 18.00% maximum). The Memory Utilization (1 hour) is 37.00% (0.00% change from 37.00% minimum to 37.00% maximum). An 'Actions' dropdown menu is open, showing options: Alarm Browser, Connect to Device, Sync Now, Device Details, Support Community, Support Request, Ping, Traceroute, and N-Hop Topology.

# Links

## To Product Information

[Visit the Cisco Web site to learn more about Cisco® Prime Infrastructure.](#)

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

## To Training

[Visit the Cisco Web site to access other Cisco® Prime Infrastructure learning opportunities.](#)

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

## To Contact Us

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



**Note:** Please send messages that address the content of this job aid or other training questions only.

Please follow your regular business process to request technical support or address technical or application-related questions.