Network Health Monitoring Overview

Cisco© Prime Infrastructure 3.1

Job Aid

Copyright Page

Network Health Monitoring Overview Job Aid

Contents

Basics

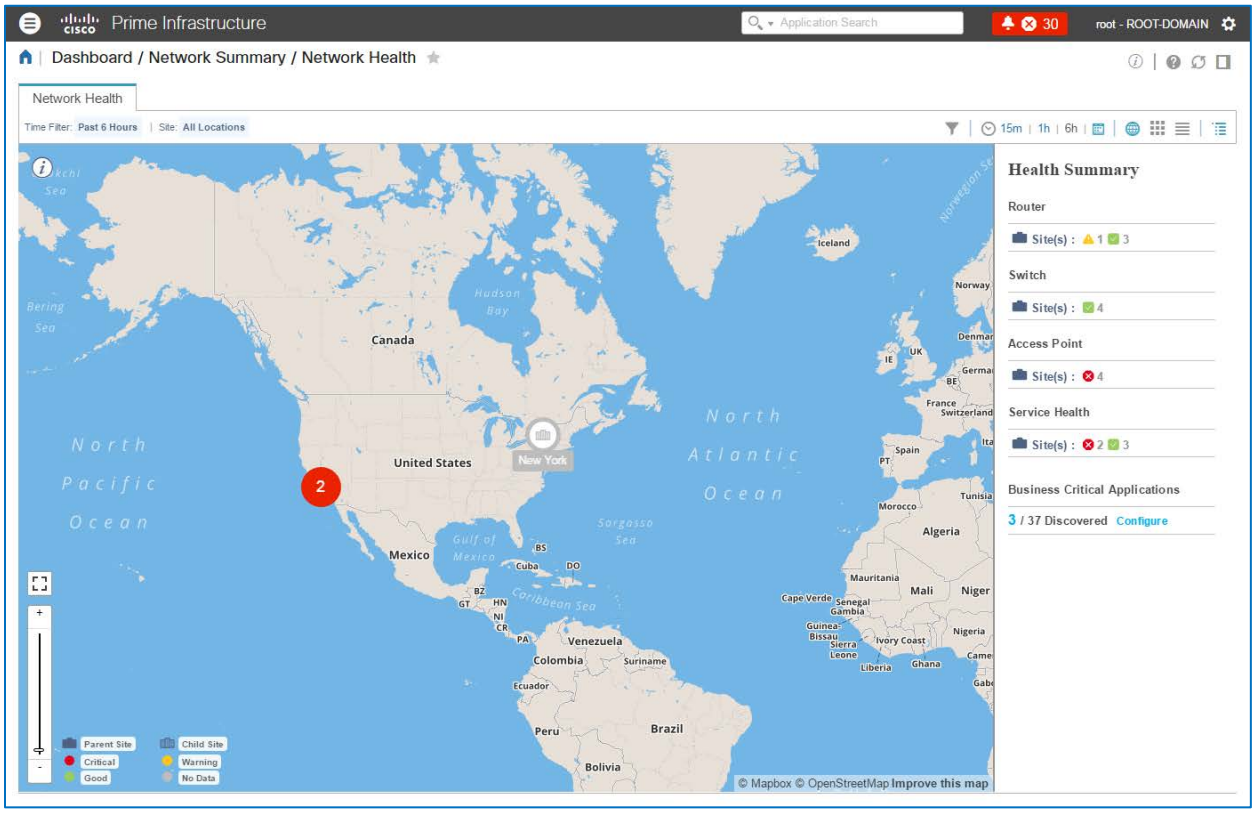
Overview

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

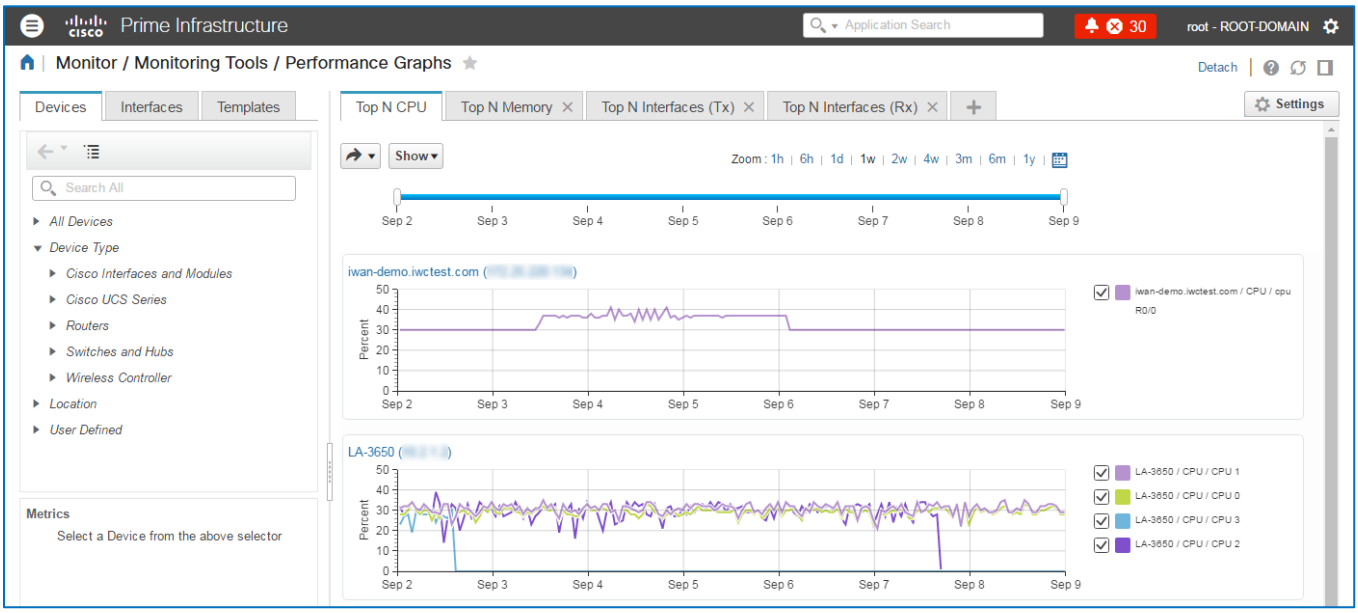
In addition to the dashboards and dashlets that you can use to monitor various targeted aspects of the network, you can monitor and evaluate the overall health of the entire enterprise network efficiently by using these key monitoring tools:

- **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

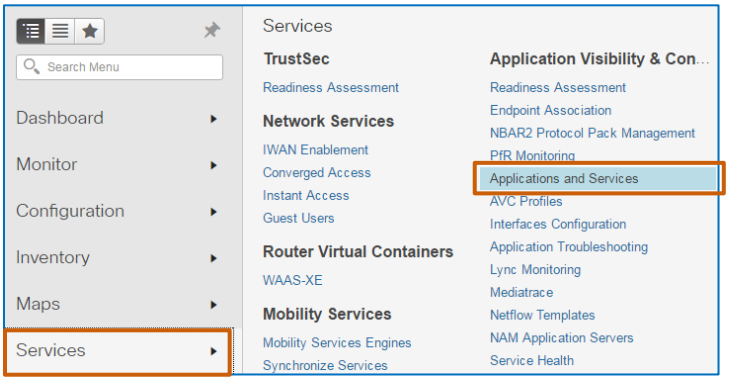
- Correlation of metric, alarm, and configuration data

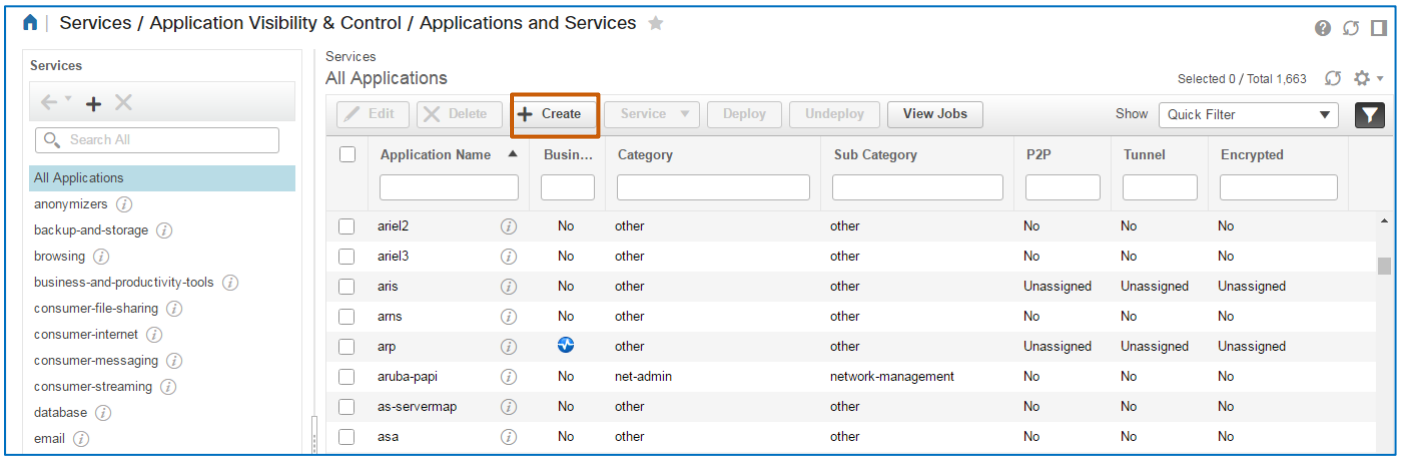
Terms

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 | Application 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.

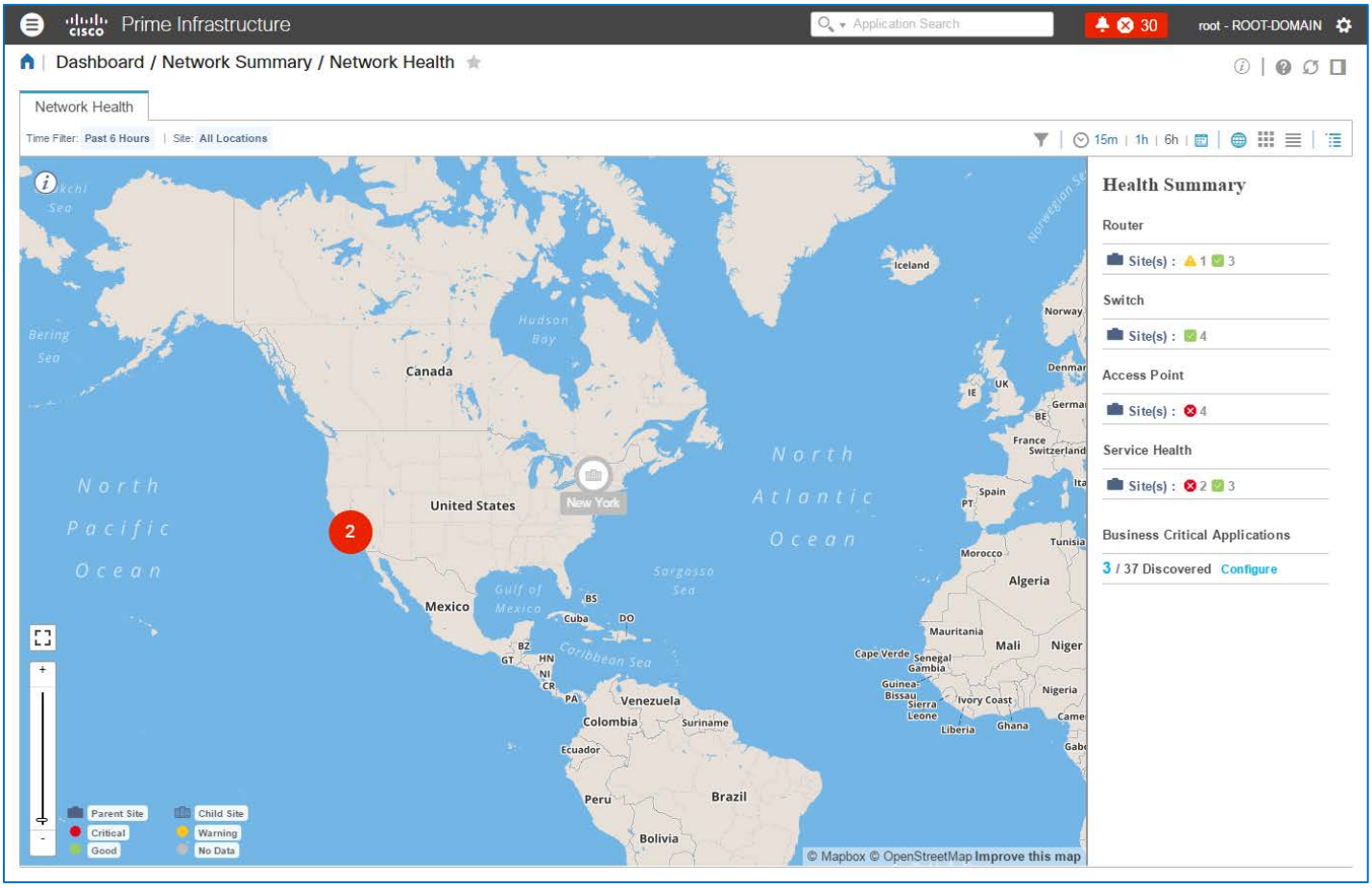
Monitoring Key Network Device and Application Health

Network Health Dashboard Overview

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 locations that system users configure, the **Network Health** dashboard provides map, health index, and table views of configured network location groups and health metrics for the router, switch, and access point devices and interfaces in each group.



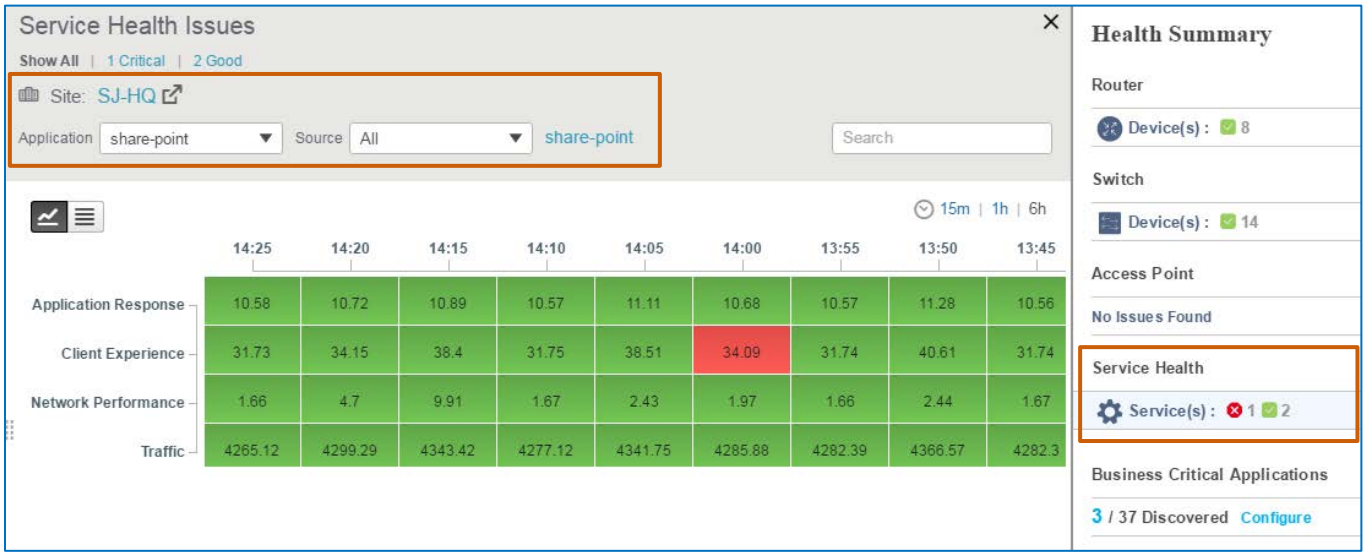
At a site level, router and switch metrics include:

- Site availability.
- CPU usage.
- Memory usage.
- Device temperature.
- Interface availability.
- Interface usage.

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.

The **Service Health** summary reports the health of KPIs for applications by site and source that system users have identified as business-critical.

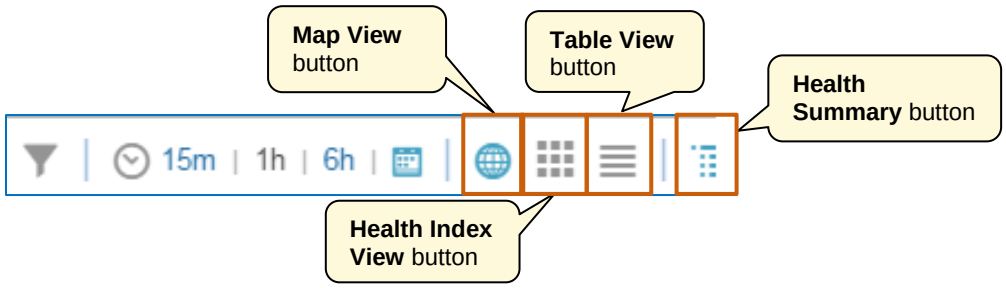


To toggle among the map, health index, and table views, on the toolbar:

- To see the map view, click **Map View**.
- To see the health index view, click **Health Index View**.
- To see the table, click **Table View**.

To toggle the Health Summary navigation on the right of the page open or closed:

- On the toolbar, click **Health Summary**.



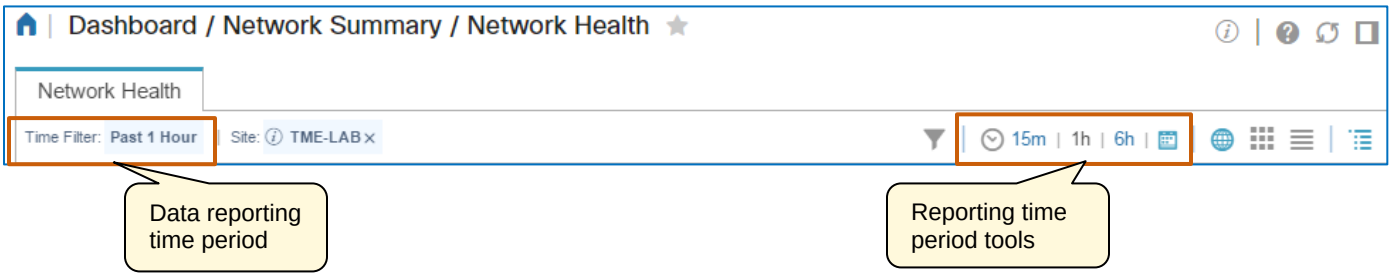
The **Network Health** dashboard provides a proactive monitoring tool that alerts you to potential issues. You then follow business processes to mitigate or correct the root causes of device issues.

Monitoring Tools Overview

Data Reporting Time Periods

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.



Health Reporting 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 has no data to report on the metric.

Note: To review how to configure health rules, refer to the **Configuring Health Rules** topic.

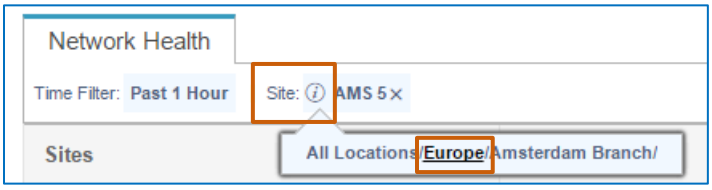
Navigating Among Locations

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.

The Map View

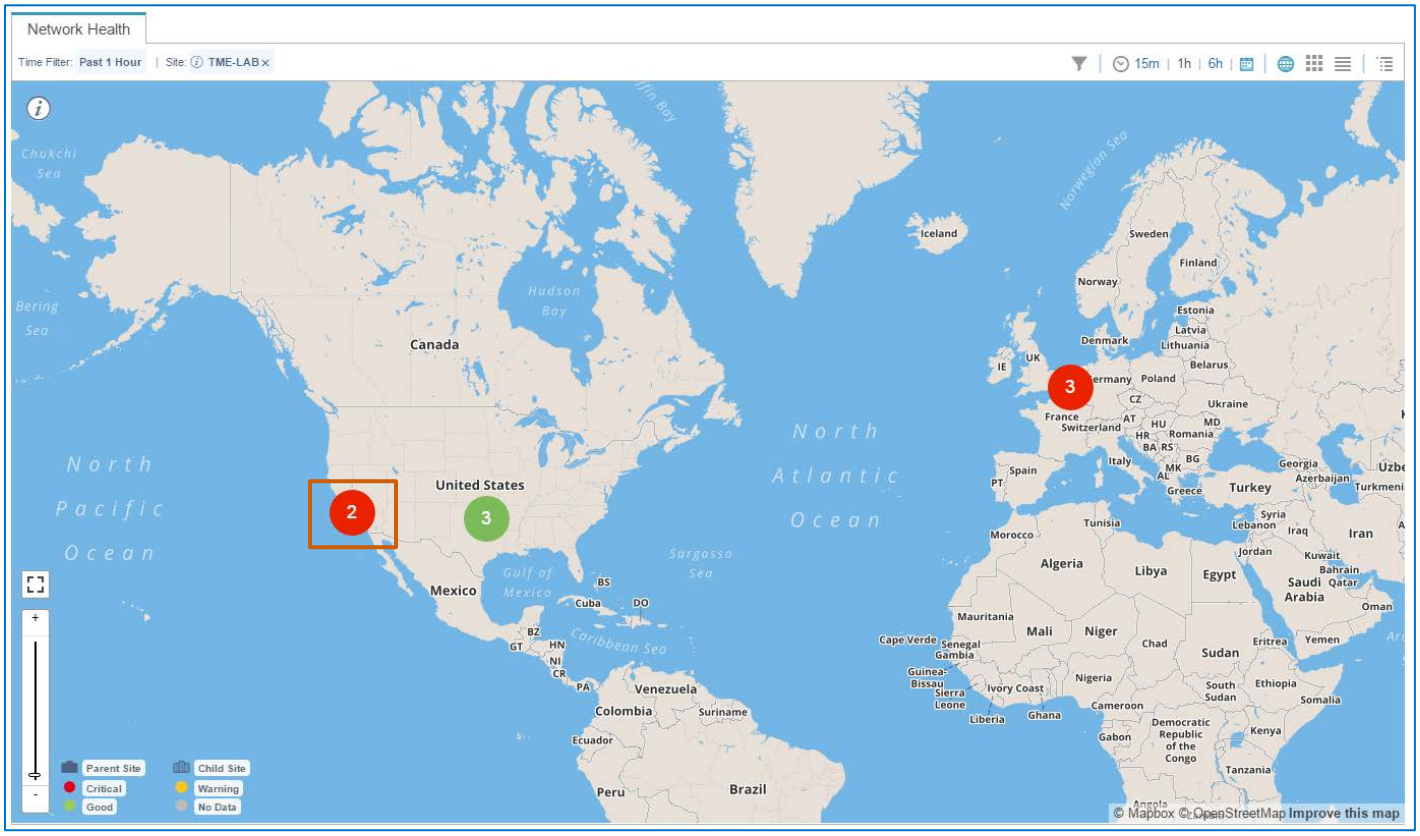
The Map View on the dashboard provides a geographically based overview of network sites and any health issues associated with them. This way, you can identify a problem area efficiently and begin investigating it further.

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

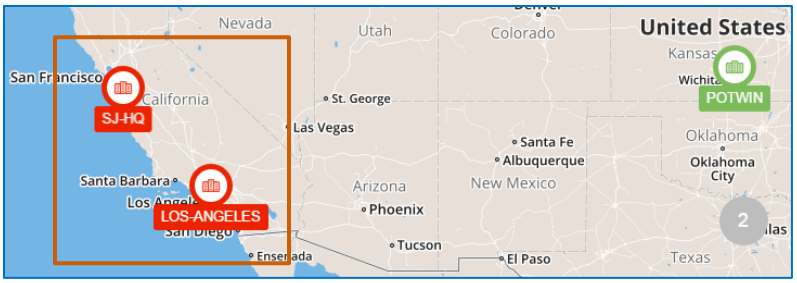
Important Note: Map behavior, including zoom levels, and the sites that you see, are based on how location groups are organized and whether their geographical coordinates are configured.

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.



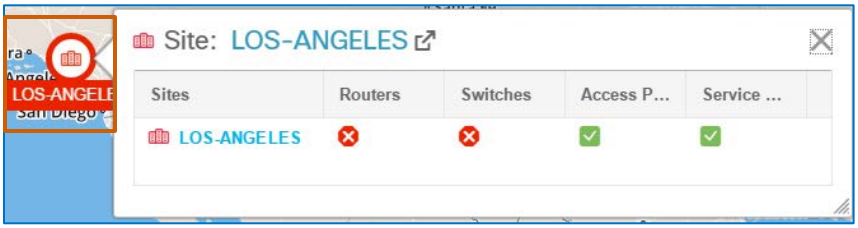
When you zoom in to a specific area, the icons update to represent each site individually. The icon color-code at individual and grouped site levels represents the most critical health issue occurring on one or more devices associated with the site or sites.



To see a summary of the issues a site or site group is reporting:

- Point to the site icon.

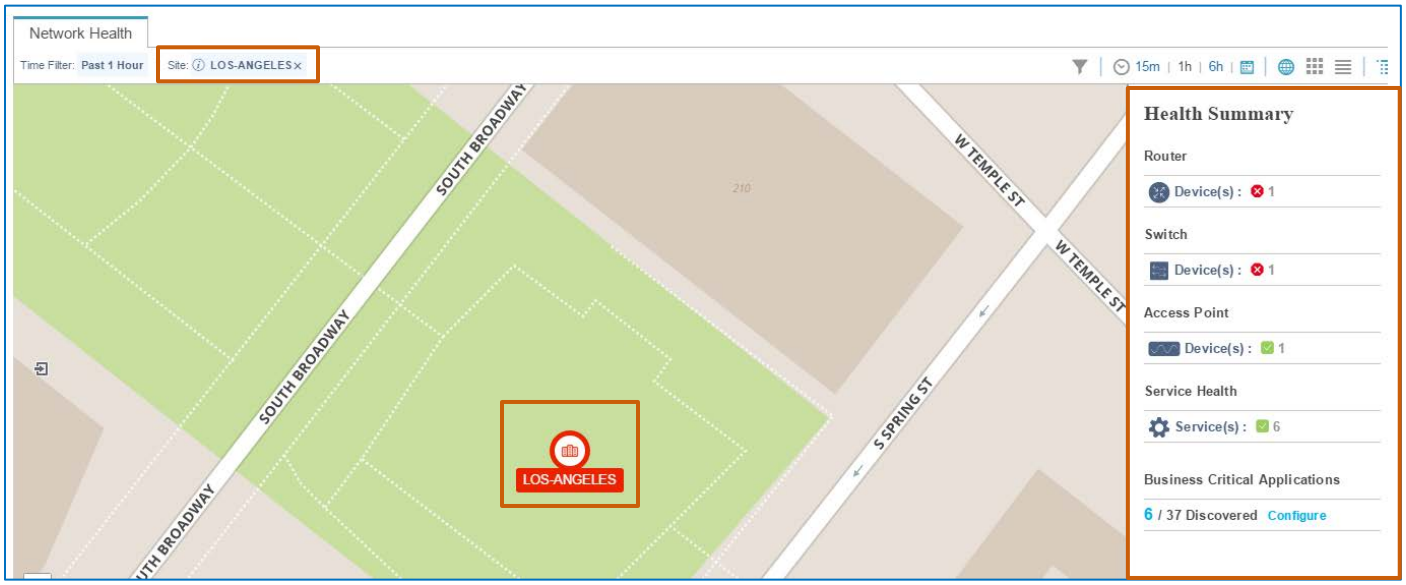
  The **Site** pop-up window opens and, depending on the zoom level, lists the site or sites that the icon represents and the most severe alarm that a key device or service is reporting.



To apply a site level filter to the dashboard data:

- In the pop-up window, click the site name link.

  The map view zooms in and the system applies a filter so that the **Health Summary** panel and the other views report the data for that site 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.

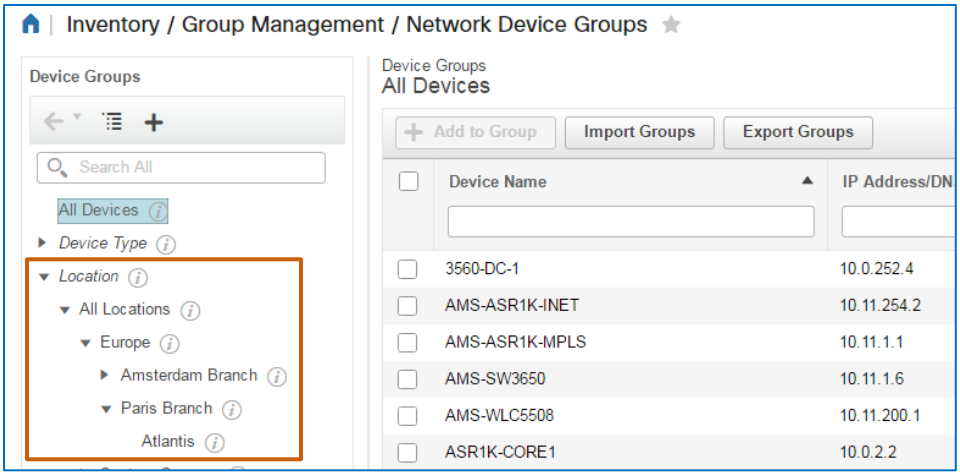
  A dialog box opens and lists the locations without coordinates.

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.

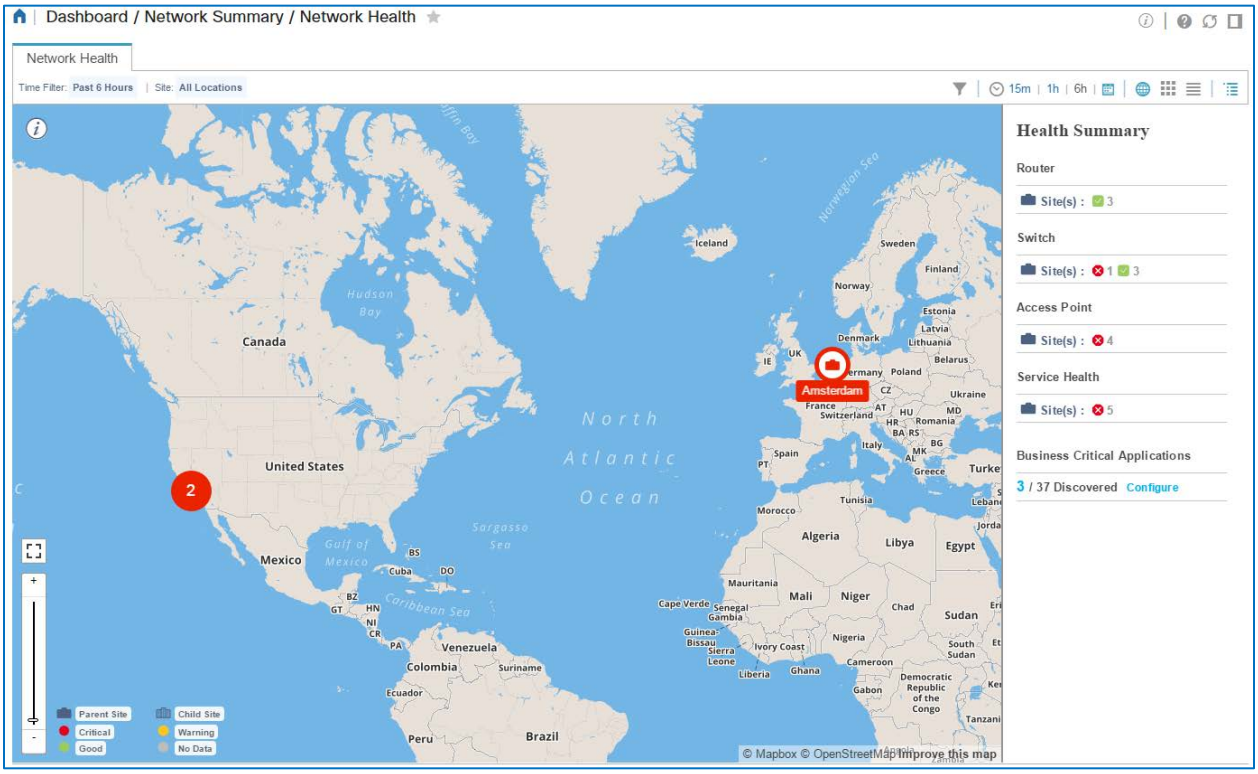
Note: To review how to configure a location group, including adding geographical coordinates, refer to the **Organizing Location Groups** topic.



Investigating a Site Issue

This example illustrates one method that you might use to identify and investigate a site issue by using the Map View.

When you navigate to the **Network Health** dashboard, the Map View opens initially, and displays all of the top level location groups (sites) with geographical coordinates.



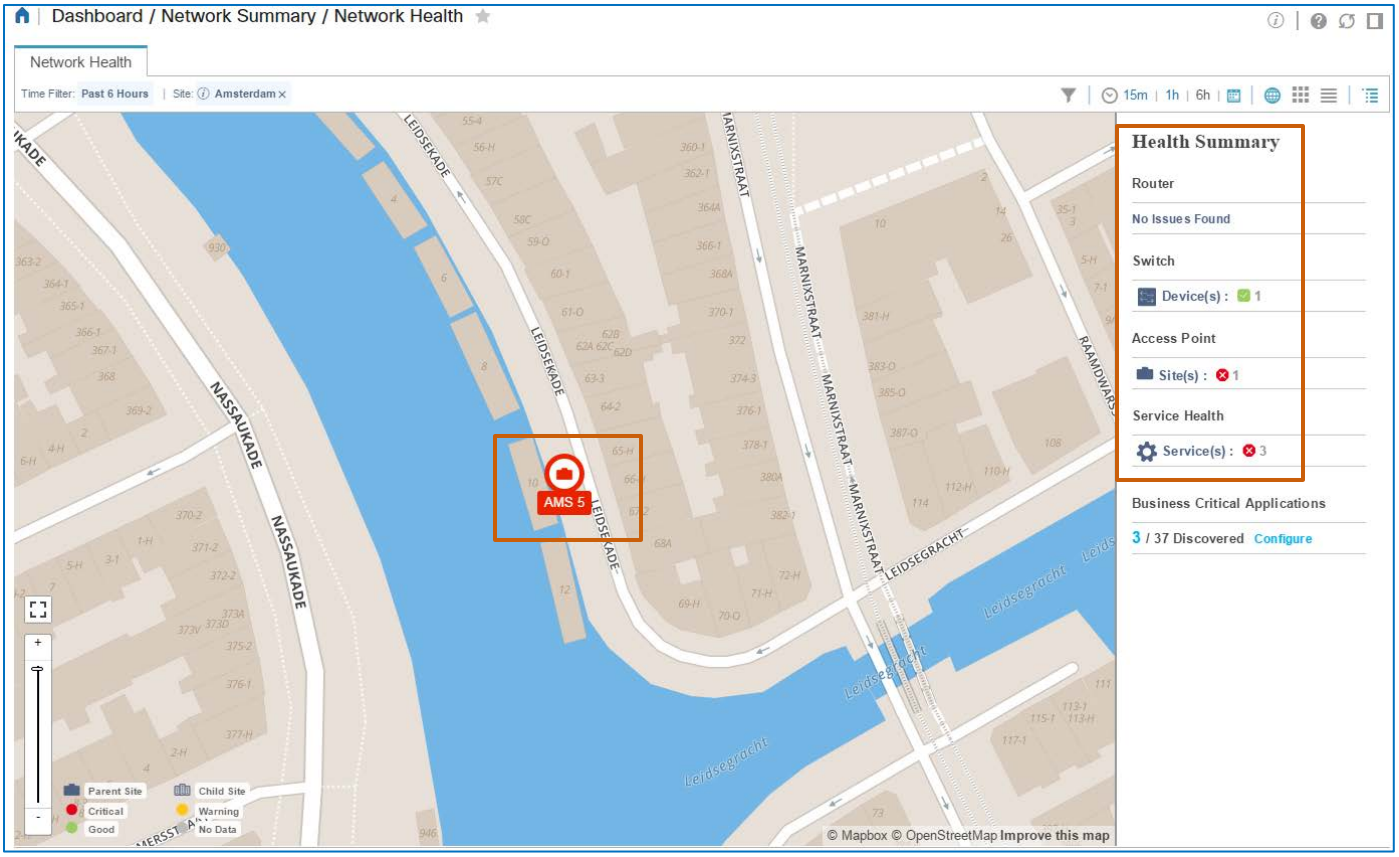
You see a site with color code indicating that the site is reporting a health related issue.

To investigate the issue:

1. On the Map View, click the site icon.

Tip: When you point to the indicator, a pop-up window opens, also. Click the icon for most efficient navigation.

The Map View zooms to a detail level view of the site, and the **Health Summary** panel updates to show what the site is reporting.

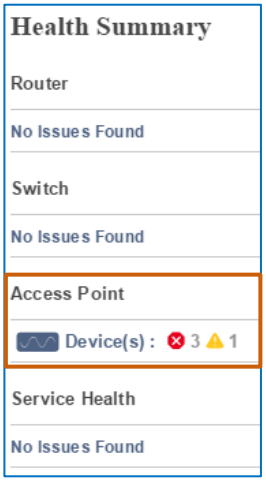


2. To ensure you are at the most detailed site level, click the site icon.

   In this example, the Map View zooms to the floor level, and the **Health Summary** panel updates to show the most critical health issue that devices or services associated with the floor are reporting.

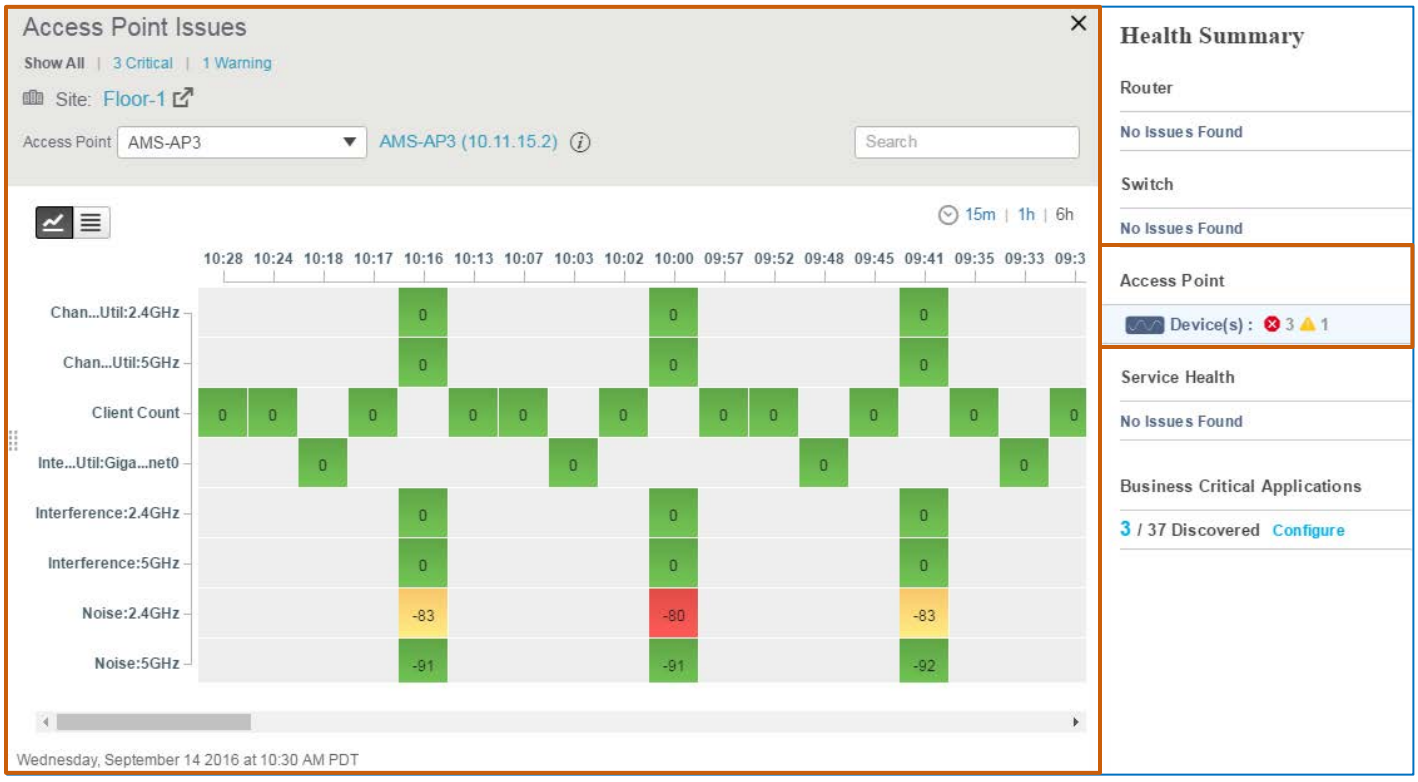
3. In the **Health Summary** panel, identify the devices or service health sections that are indicating metrics outside of threshold parameters.

   In the screenshot below, one or more access points on the floor are reporting minor and critical health issues.

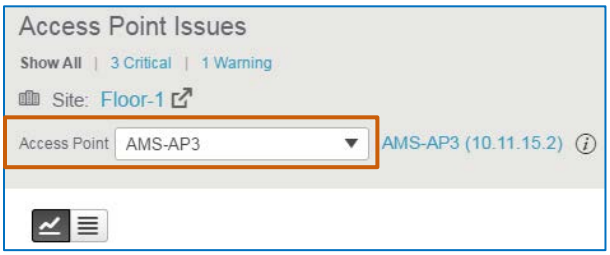


4. To investigate an issue, in the **Health Summary** panel, click the section.

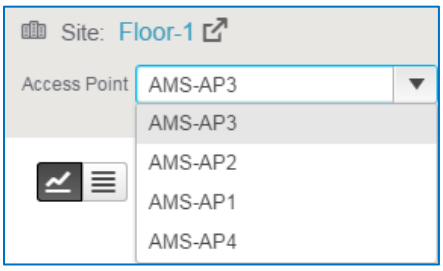
A panel opens and lists the floor level metrics with health indicators…



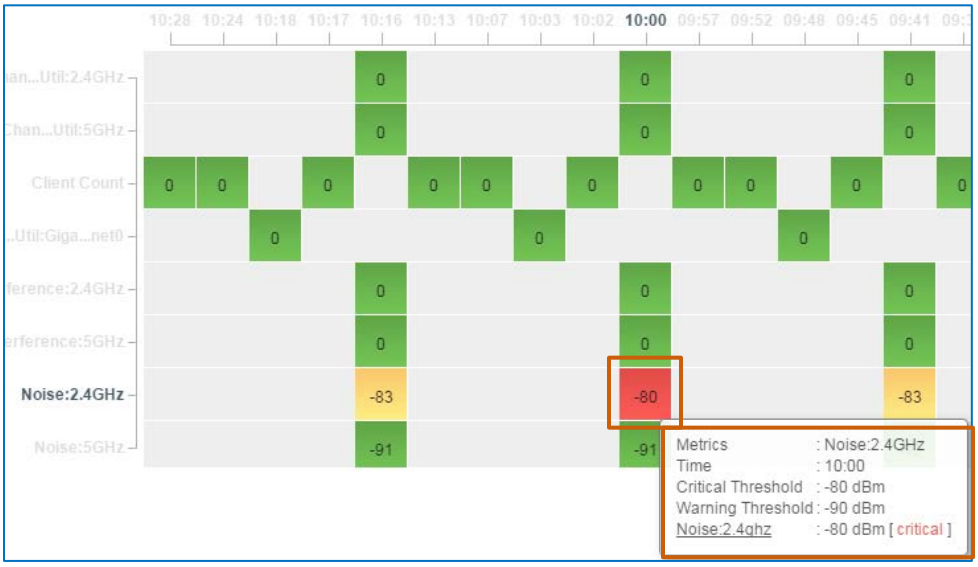
…for the device that is selected in the **Access Point** drop-down list.



You can evaluate the metrics of any access point on the floor by selecting it in the **Access Point** drop-down list.

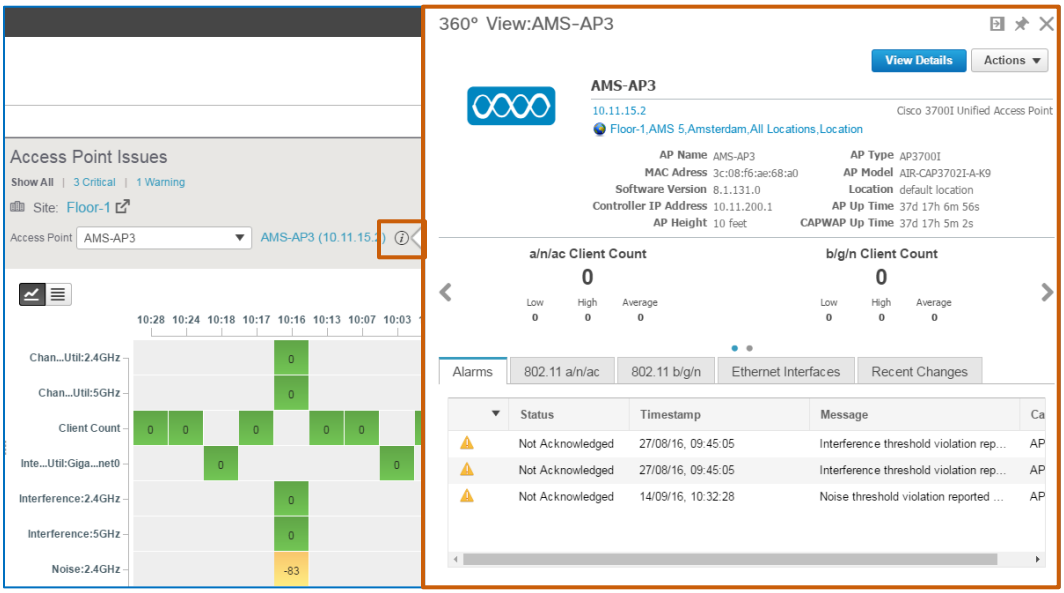


You can point to a metric on the timeline to see details, including the metric thresholds defined in the health rules.



5. To evaluate device level data or take action on the device, beside the device name link, click **Launch Device 360 degree view**.

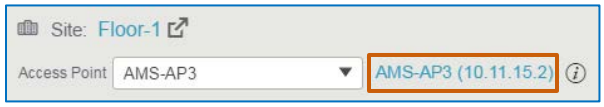
   You can manage the device, as needed, by using the **360⁰ View** pop-up window.



Tip: In some troubleshooting situations, it might be helpful to evaluate summary data for the issue being reported.

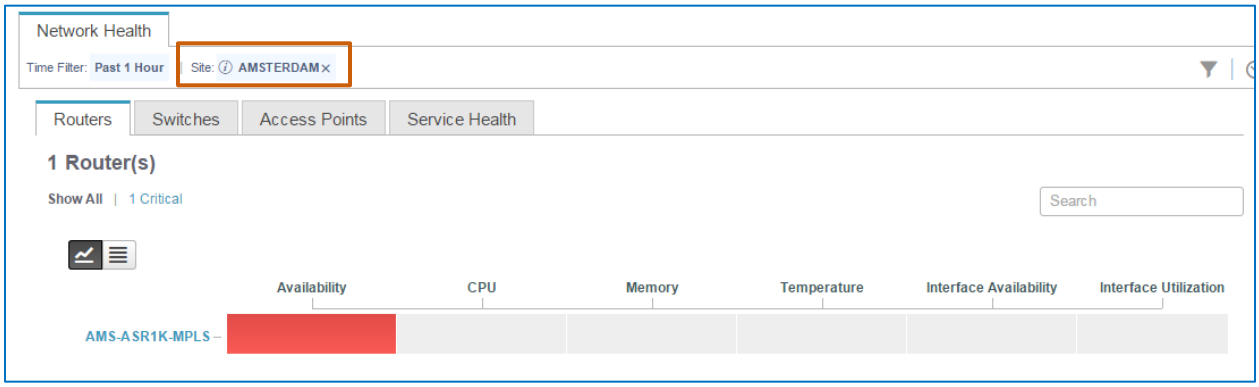
To open another dashboard that summarizes information related to the device type reporting it:

- Click the name link beside the drop-down list.



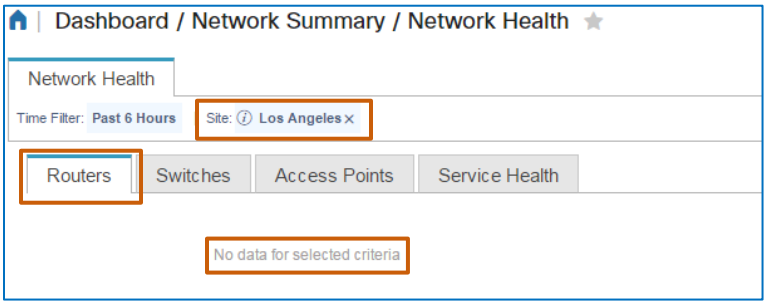
The Health Index View

For the location or group of locations that are applied to the dashboard, the Health Index View displays a graphical representation of device health statuses.



Important Note: The sites that you see listed in the **Health Index View** page depend on the site that is active on the page.

If, at that level, the site does not have assigned devices of the type indicated by the active tab, the tab can appear blank.

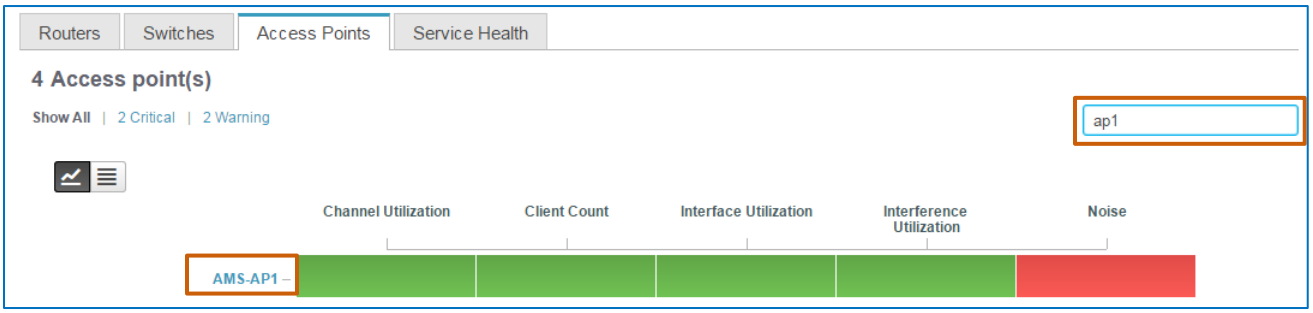


When you have a long list of devices, you can search for a specific device.

To find a specific device:

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

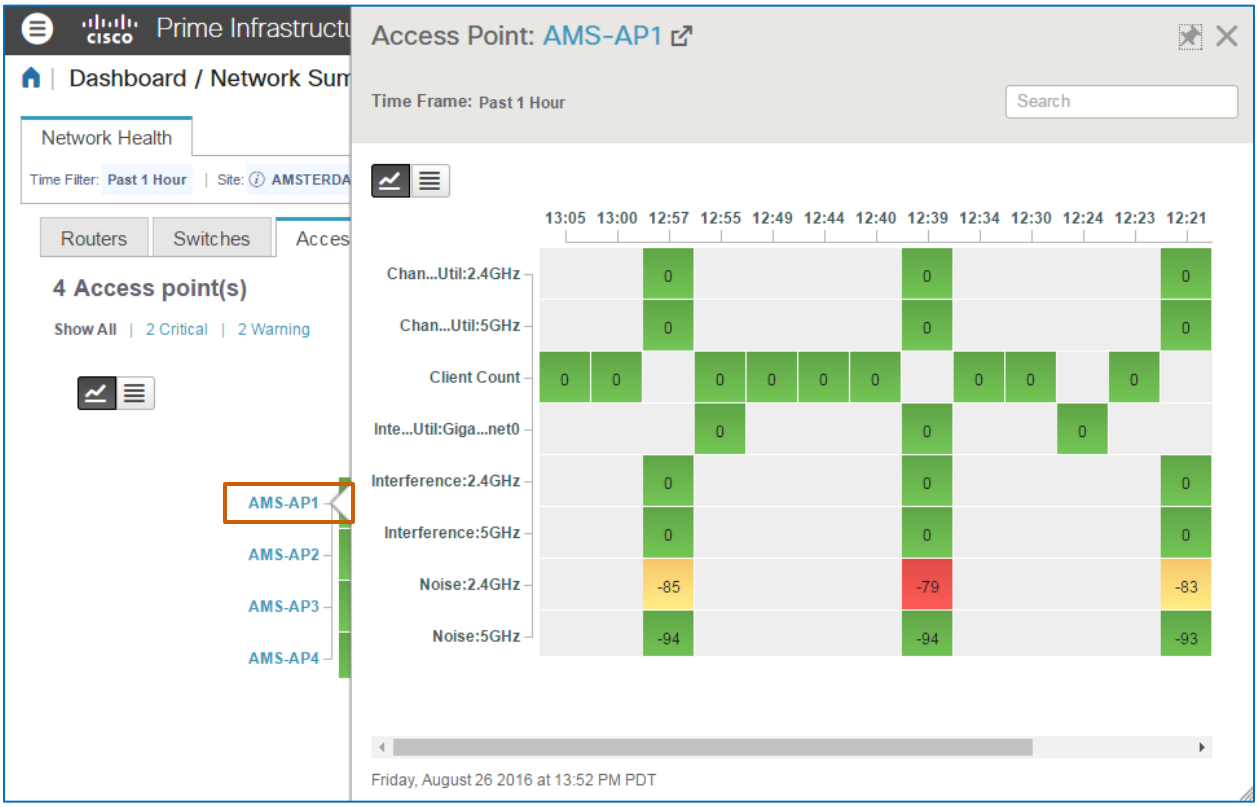
  As you type, the list filters to display all of the devices with names that include the characters that you are typing.



To evaluate health metric details:

- Click a device name link.

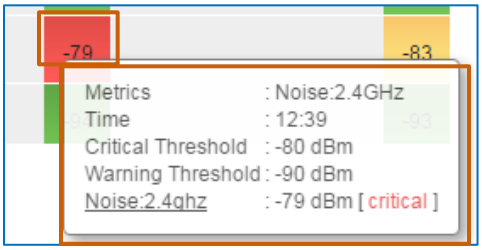
  A pop-window opens and presents detailed metrics along an incremented timeline that reflects the time period applied to the dashboard.



To evaluate a specific metric:

- In the pop-up window, point to the metric of interest.

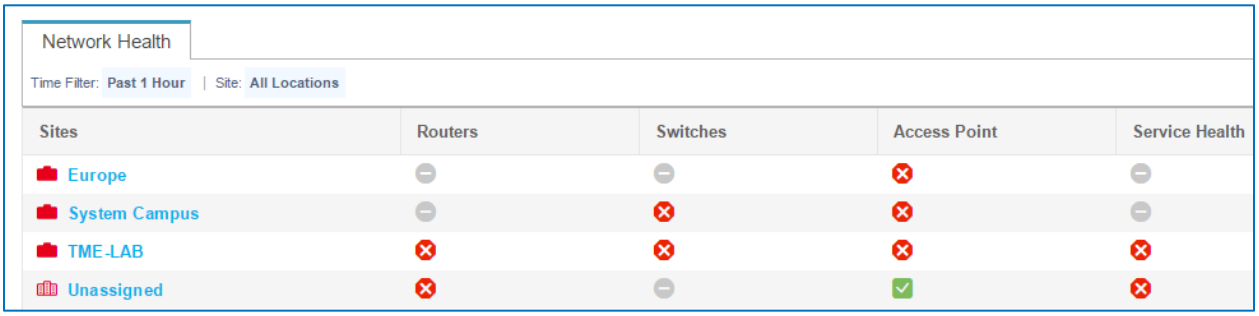
  A second pop-up window opens and indicates the thresholds defined by the health rules in addition to the metric that the device was reporting at that time.



The Table View

For the location or group of locations that are applied to the dashboard, the Table View displays the health metrics in a list.

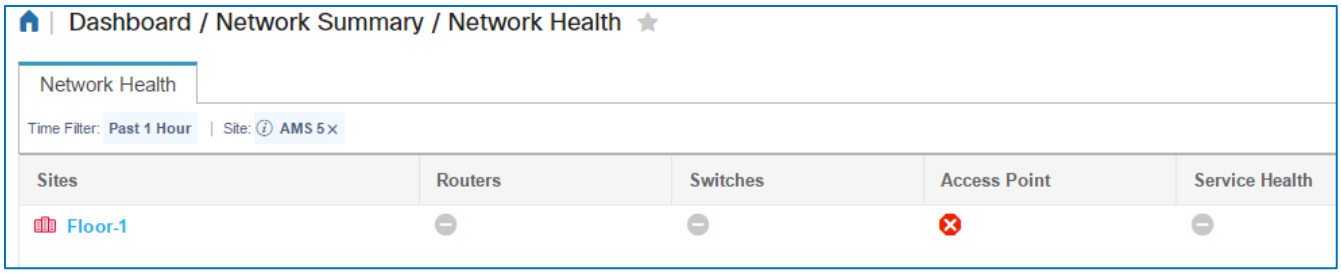
Tip: If you are unsure that you are seeing all of the locations that you need to monitor on the Map View or Health Index View pages, open the **Table View** page, which lists all location groups regardless of whether their geographical coordinates are configured.



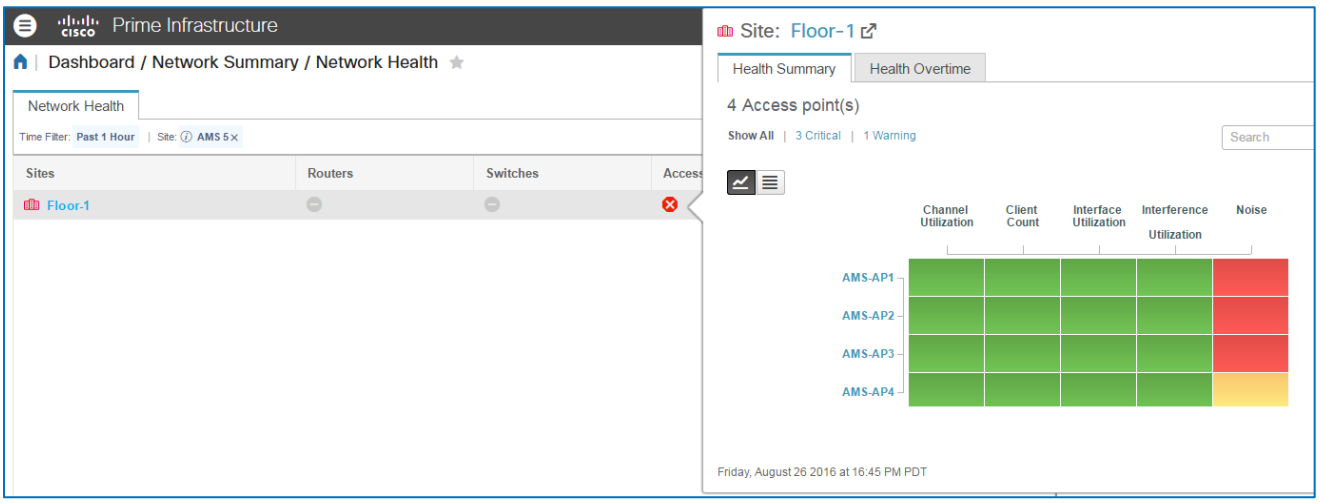
To open a more specific site level:

- Click the location name link.

  The page updates to display the highest severity level that one or more devices or services are reporting.



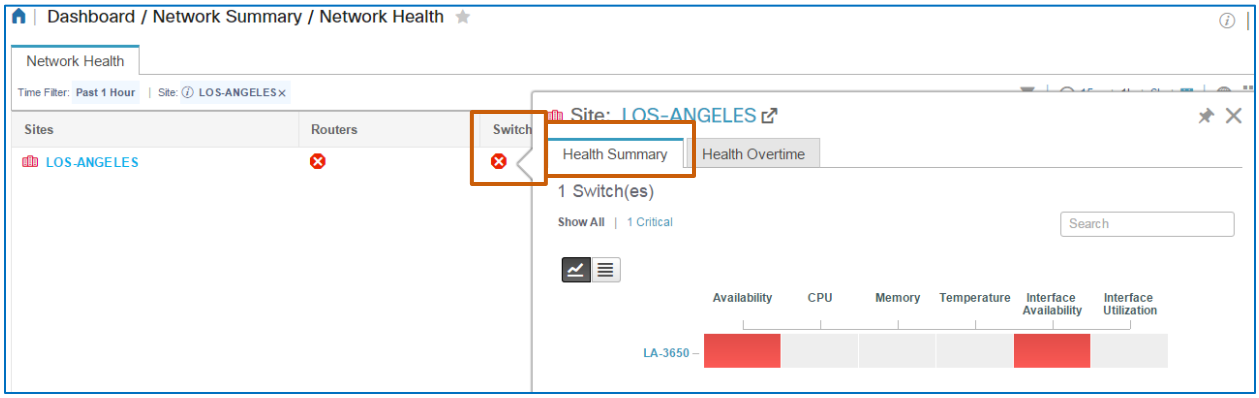
When you reach the device level, you can click a health indicator to review the metrics that the device is reporting.



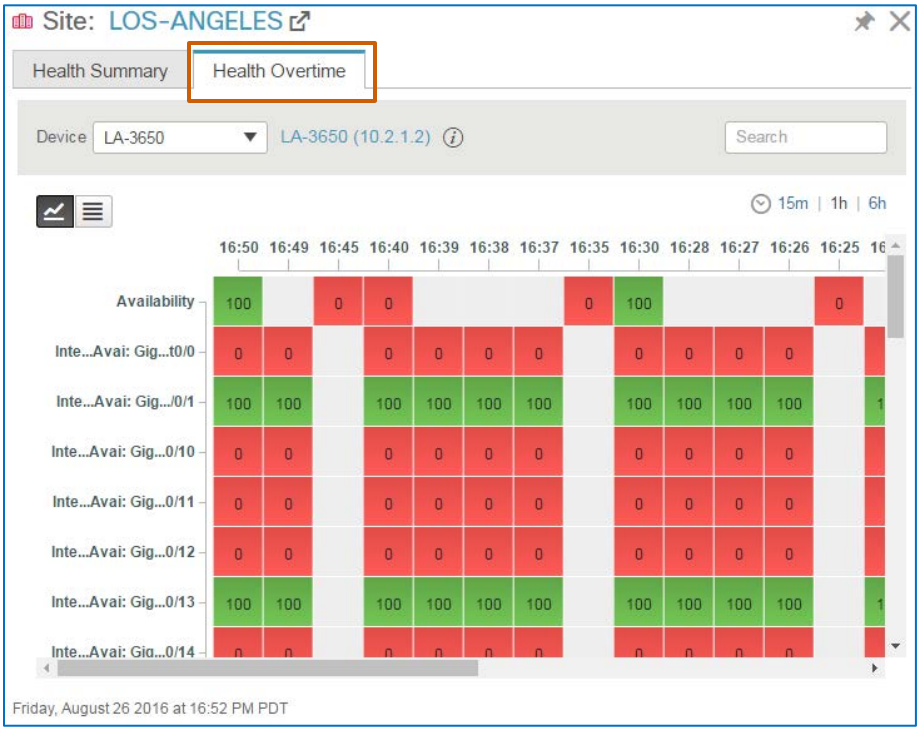
To evaluate a specific metric:

- In the pop-up window, point to the indicator of interest.

  A second pop-up window opens and provides tabs so that you can see a summary of where issues are being reported...



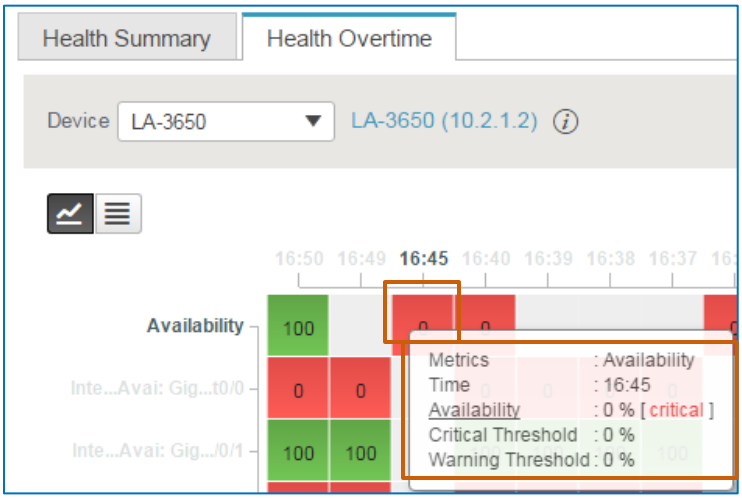
… and detailed metrics over time.



To evaluate a specific metric:

- In the pop-up window, on the **Health Overtime** tab, point to the metric of interest.

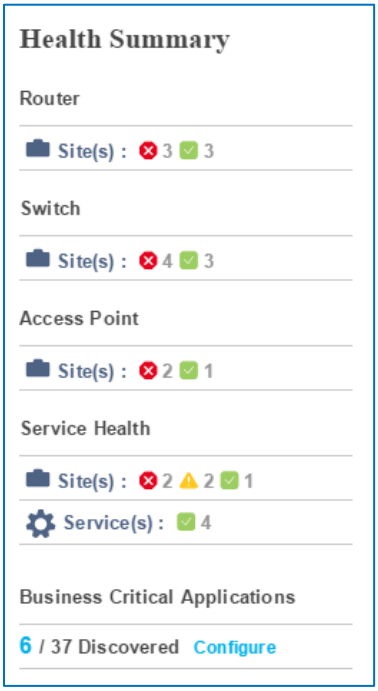
  A third pop-up window opens and indicates the thresholds defined by the health rules in addition to the metric that the device was reporting at that time.



The Health Summary Panel

For the location or group of locations that are applied to the dashboard, the **Health Summary** panel displays all of the health indicators and the number of instances at the location that are reporting each health level, organized by category.

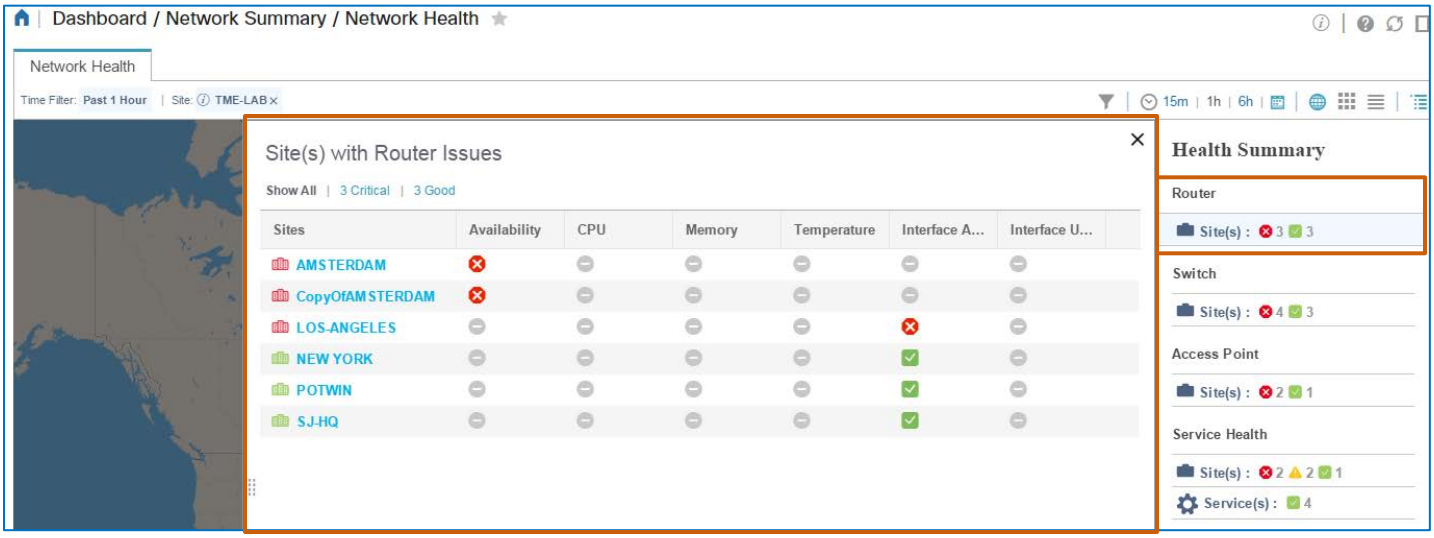
It also provides navigation to review health details for each device type and for services, which are reporting on the health of business critical applications.



To open a list of sites and their health details:

- Below the category of interest, click the **Site(s)** row.

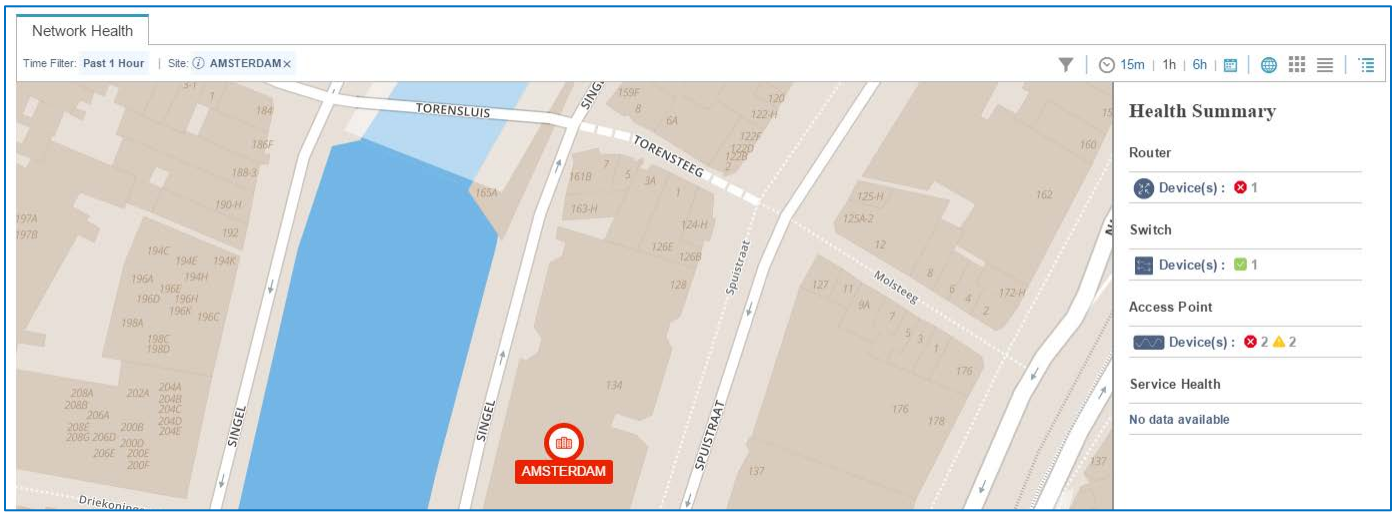
  A **Site(s)** panel opens and lists all of the sites that have the device type or service and the conditions that they are reporting.



To open site level information:

- In the **Site(s)** panel, click a site name link.

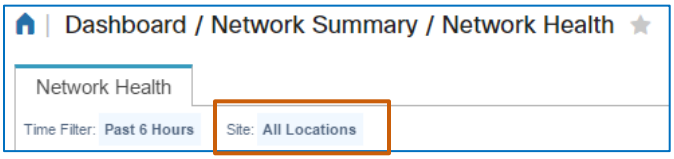
  The panel closes and the location level information updates in the **Health Summary** panel and on the associated view.

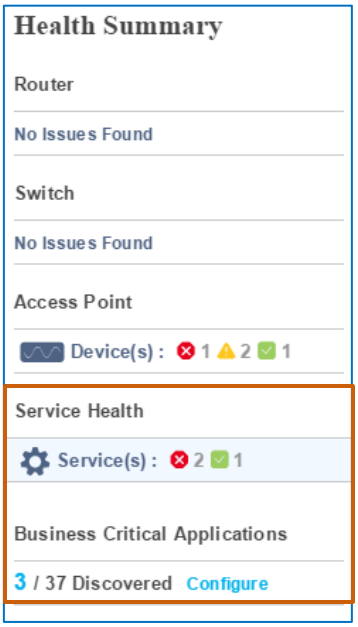


Monitoring Service Health

For those applications identified as business-critical, and that have location groups associated to subnets, you can monitor the health of business critical applications. The health and experience levels that the system reports are defined by the threshold values in the health rules.

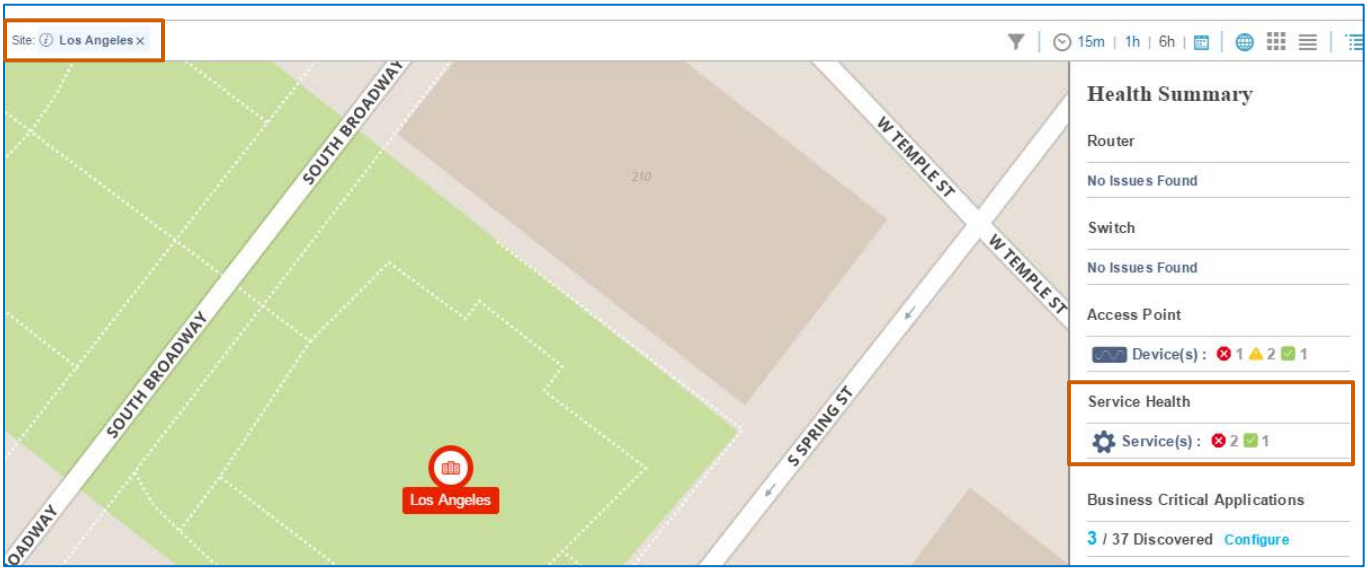
The **Health Summary** panel indicates service health issues based on the site level that you have active, regardless of the view that is visible on the page.



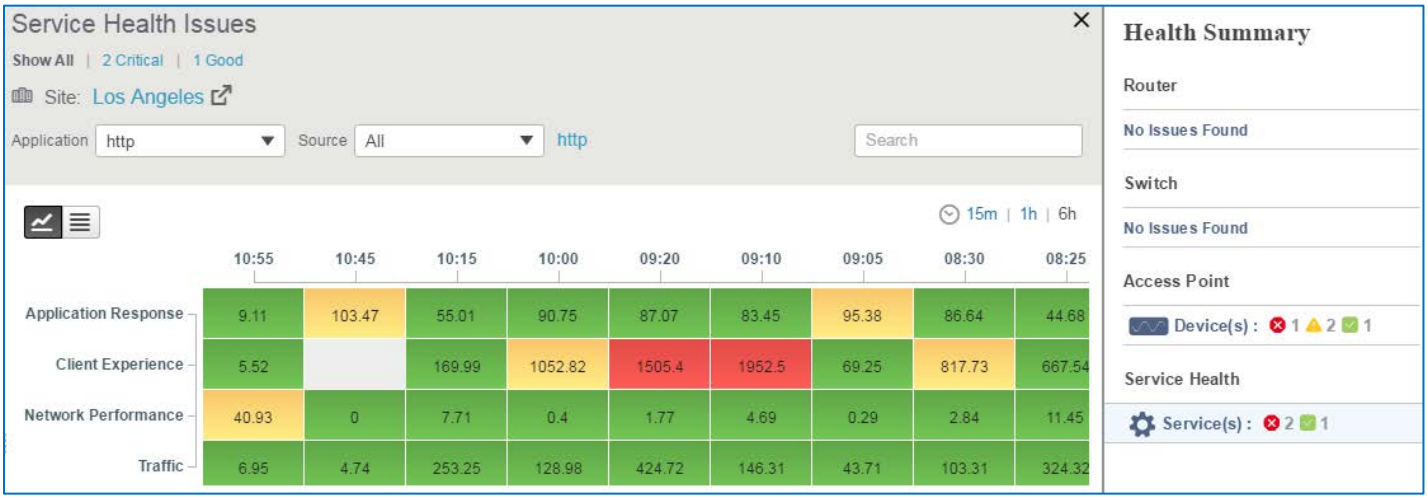


To investigate the site or sites reporting service health issues:

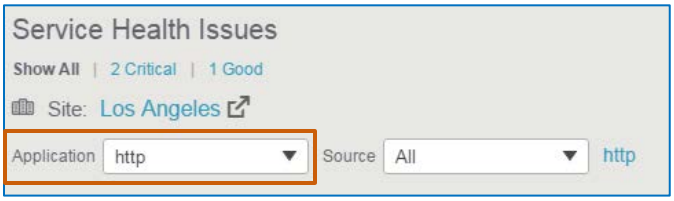
- Navigate to the site level that you want, and then, in the **Health Summary** panel, click the **Service Health** section.



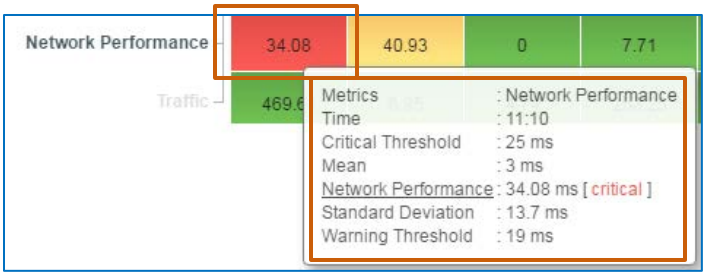
A panel opens and lists the metrics with health indicators…



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

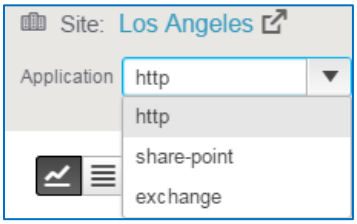


You can point to a metric on the timeline to see details, including the metric thresholds.



To evaluate another application:

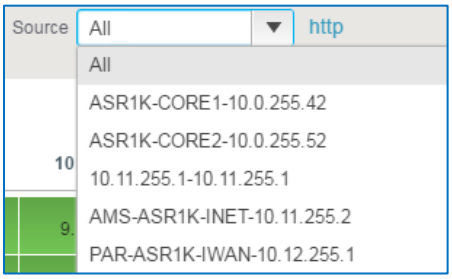
- In the **Application** drop-down list, select the application.



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.

Preparing Network Health Reporting

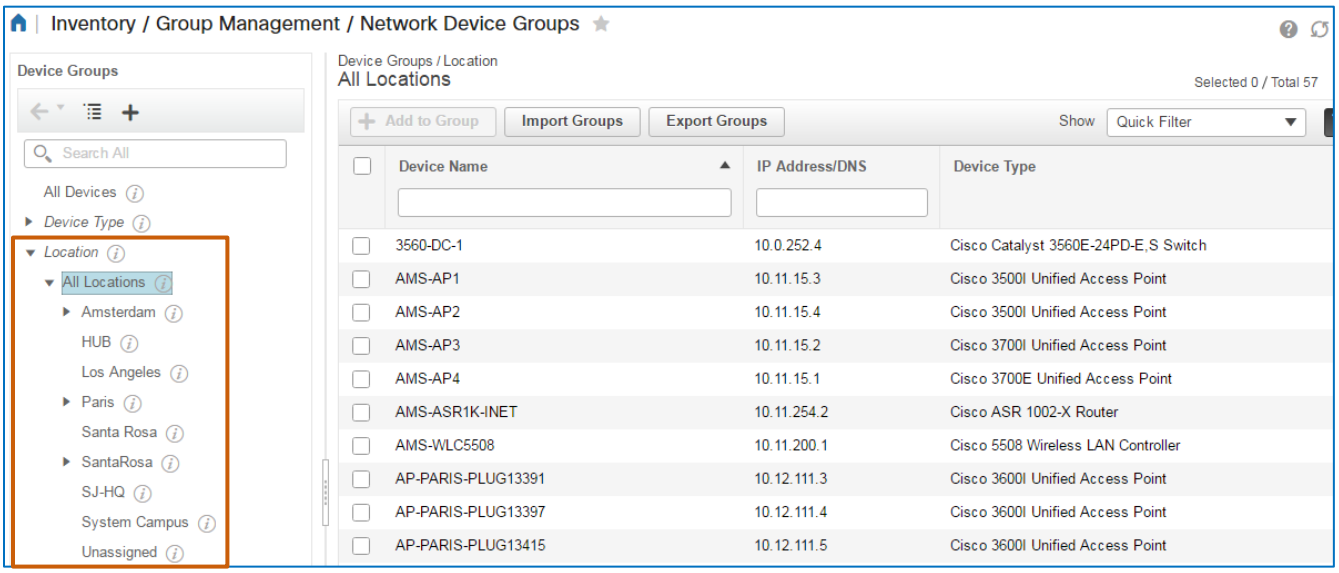
Organizing Location Groups

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.

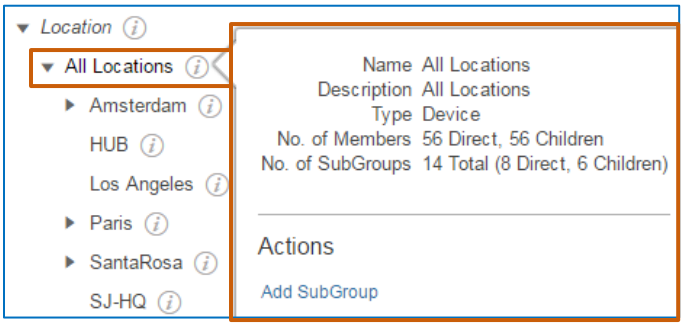
Initially, when you open a map view, the map zoom level applies based on the regions or regions that contain locations with coordinates.

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



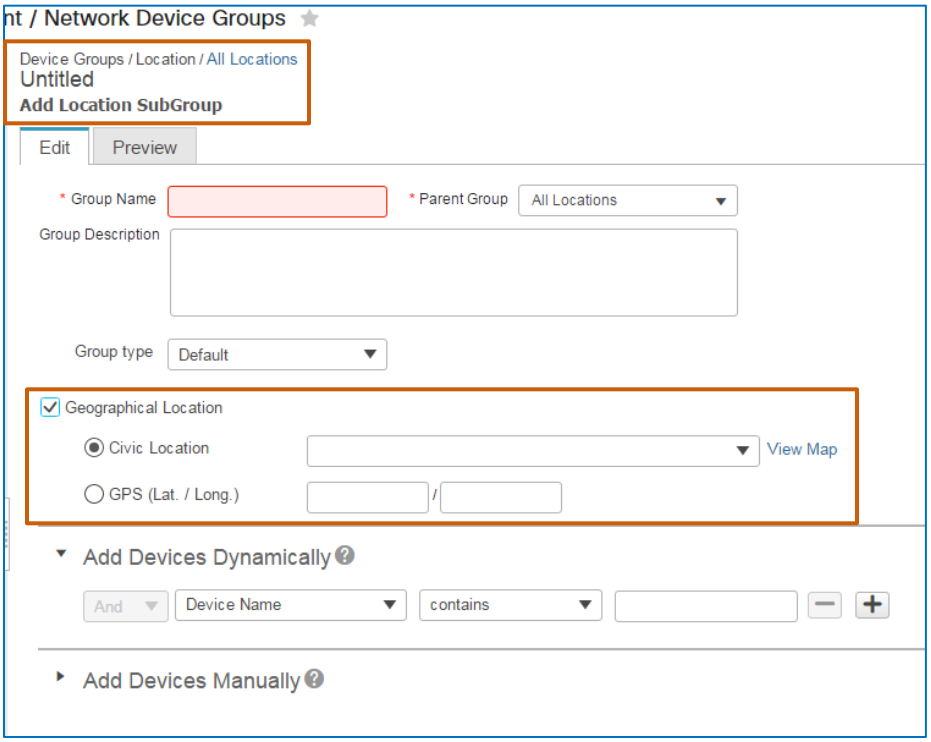
To add a top level location group folder, which equates to the parent site in Network Health views:

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



To make the location group visible in the Network Health views:

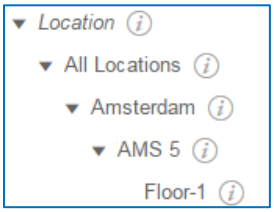
- On the **Add Location SubGroup** page, select the **Geographical Location** check box, and then add the civic location, which is the physical address, or the location's latitude and longitude coordinates.



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 A**dd 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.



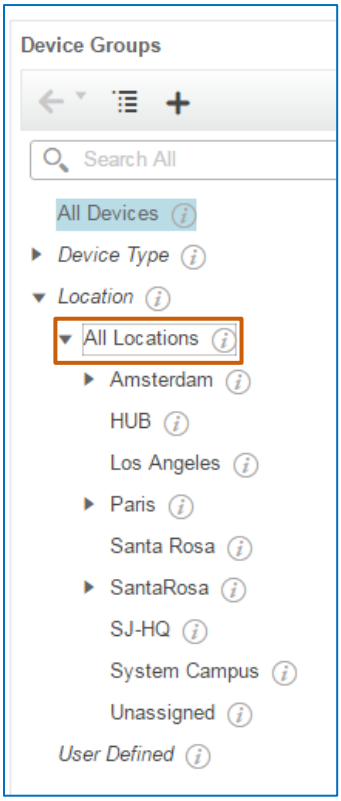
Note: For detailed steps on organizing location groups, refer to the **Cisco Prime Infrastructure 3.1 User Guide**.

How Location Group Organization Affects Views

Recognizing location group organization is critical to understanding what you see when using the Map View 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.



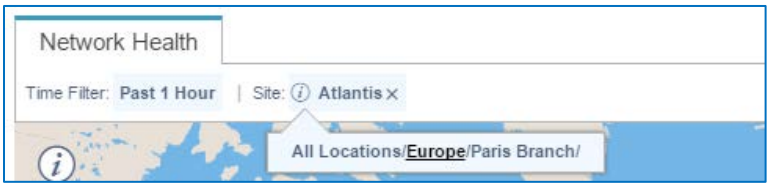
Those top level folders below **All Locations** that have geographical coordinates configured are the parent sites that you see on the map.

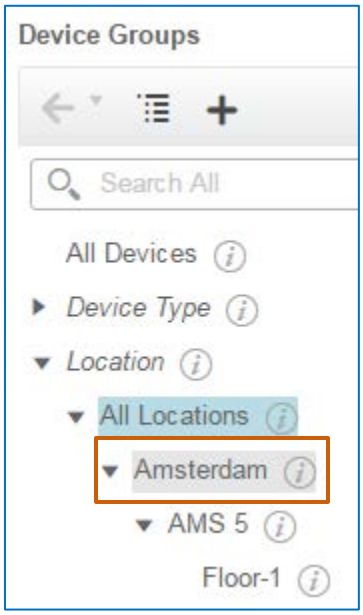
Users can continue to add subgroups of folders under top level location group folders, which define the child sites that belong to each parent site.

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.

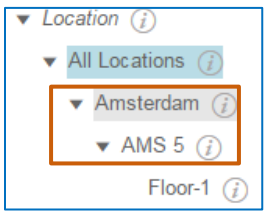
Important Note: In order for users to see the parent site and all of its child sites on the map, the top level folder and each subgroup folder must have its geographical coordinates configured.

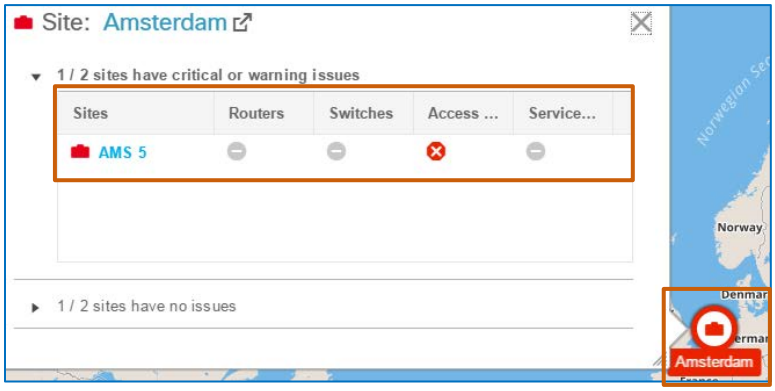
If you do not configure a folder with geographical coordinates, and a user selects that site when navigating a map, that site and its child sites are not visible at that level on the map.





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.

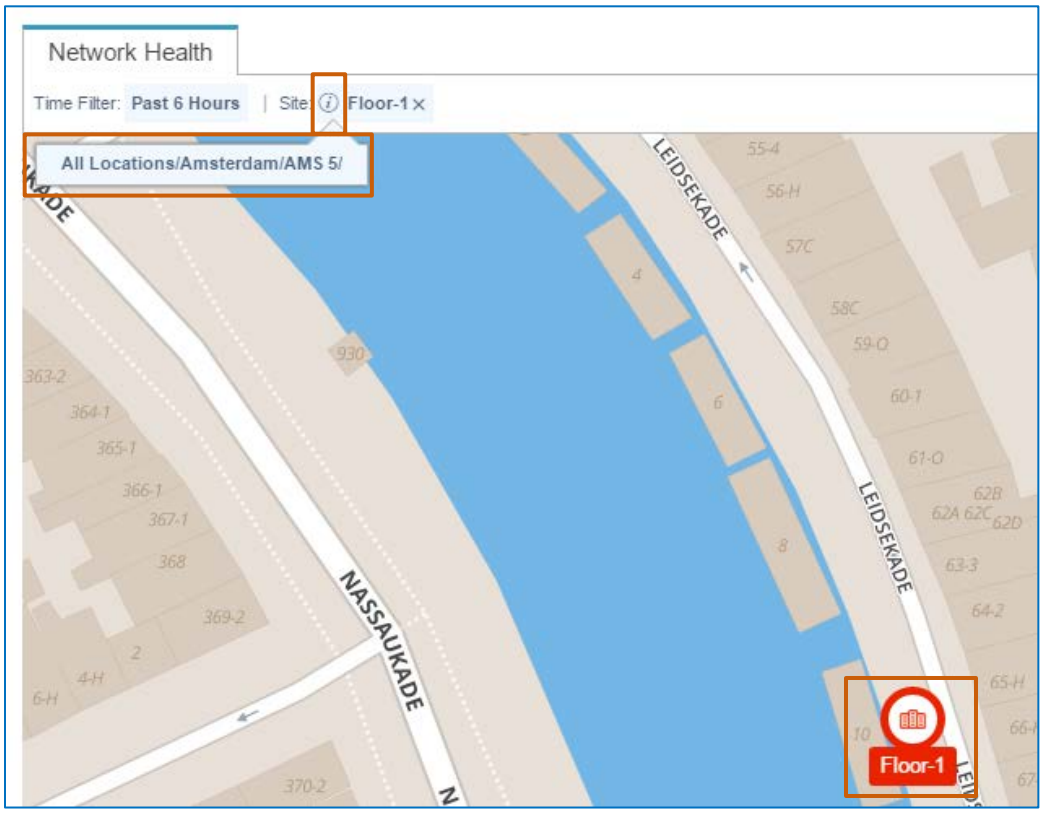


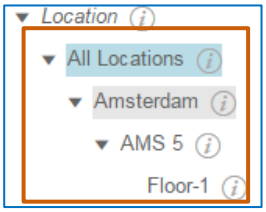


You can click the link in the pop-up window to open the next level of child sites.

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.

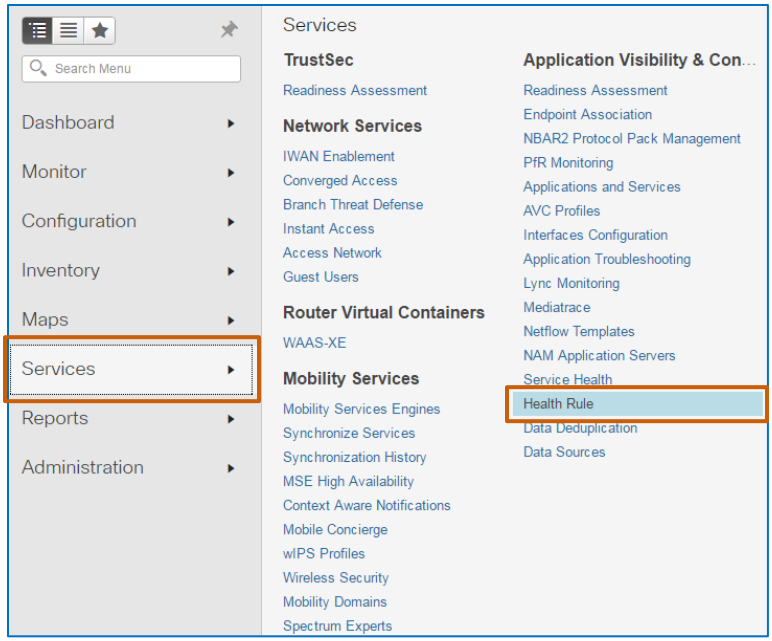
Important Note: On the **Network Devices** or **Network Device Groups** page, when you add location groups and dependent subgroups, ensure that you configure a logical folder hierarchy that reflects enterprise organization, which helps system users navigate the Map View more efficiently.

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.



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

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

- CPU, memory pool, and interface usage
- Environment temperature

On wireless health, the system reports the following metrics:

- Channel and interface usage
- Noise
- Client count

Note: For detailed steps on configuring health rules, refer to the **Cisco Prime Infrastructure 3.1 User Guide**.

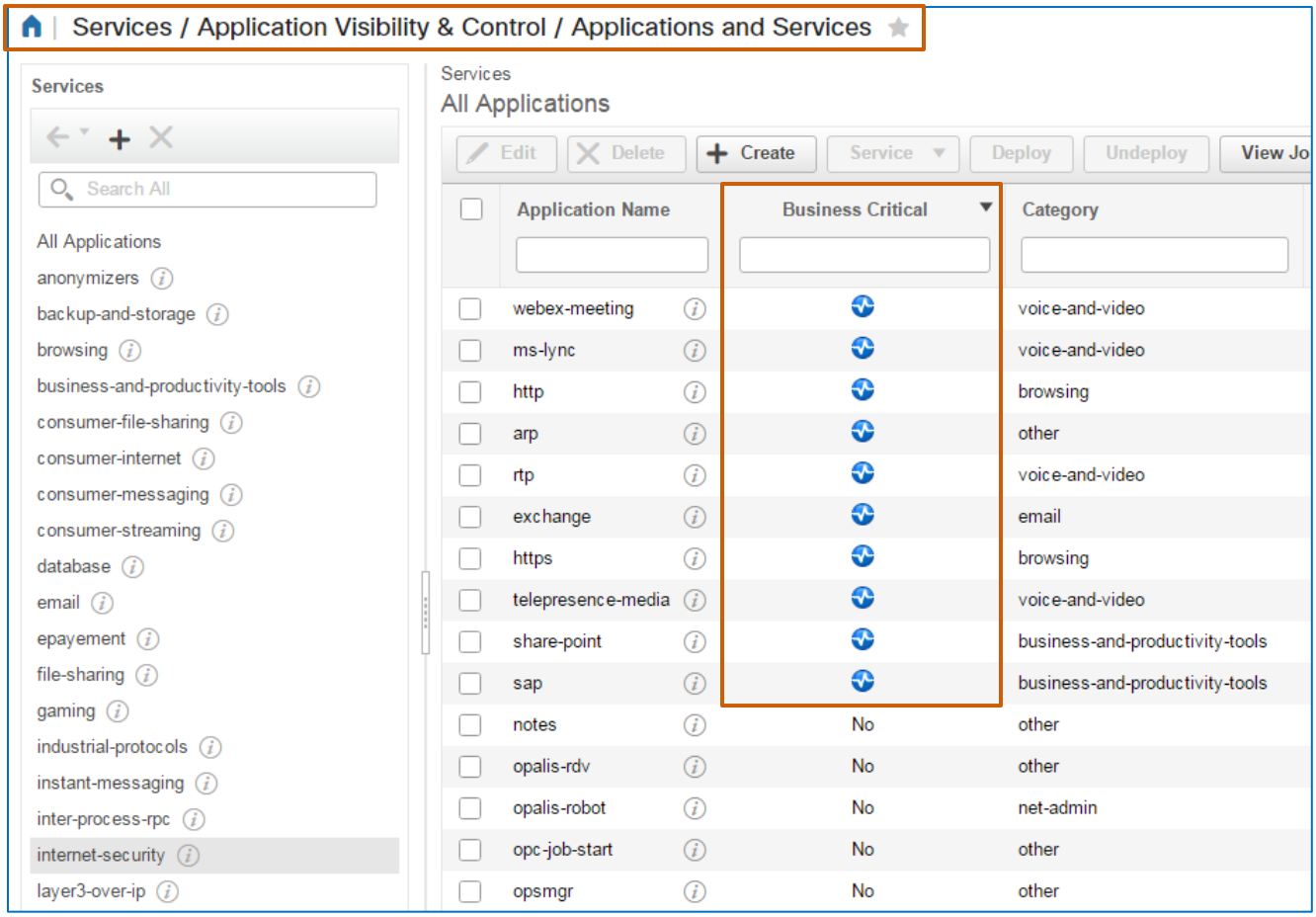
You can configure the critical and warning threshold values for all of the health rule types. You also can configure additional health rules and assign them to specific location groups.

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.

Indicating Business Critical Applications

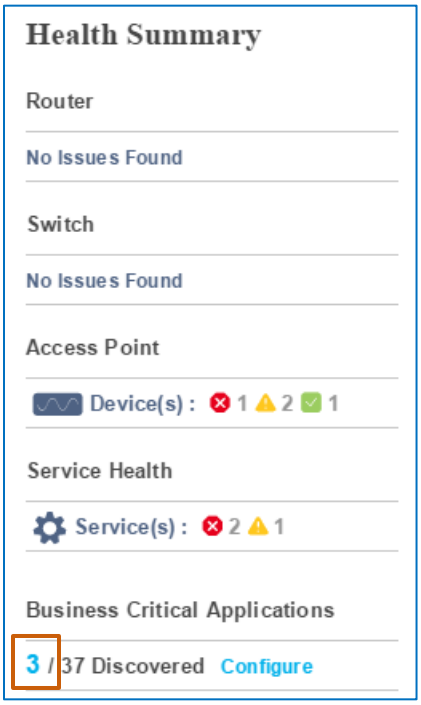
Business critical applications identify those applications that could cause significant operational issues if they experience disruption or downtime.

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



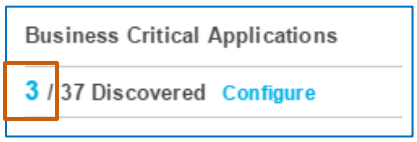
On the **Network Health** dashboard, you can select the business critical applications on which you want the dashboard to report.

On the **Health Summary** panel, under **Business Critical Applications**, the number link indicates the number of applications actively being monitored.

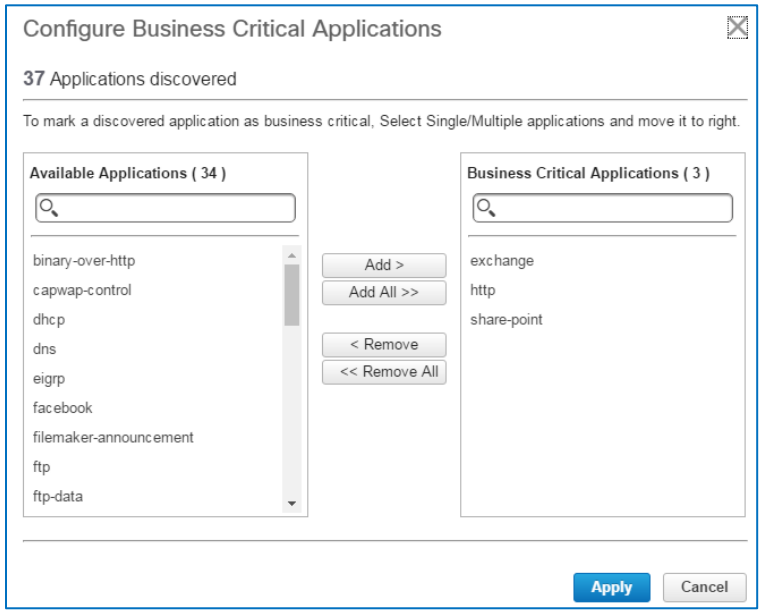


To select business critical applications for or remove them from reporting:

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



The **Configure Business Critical Applications** dialog box opens and lists all of the business critical applications with the NetFlow traffic reporting feature enabled.

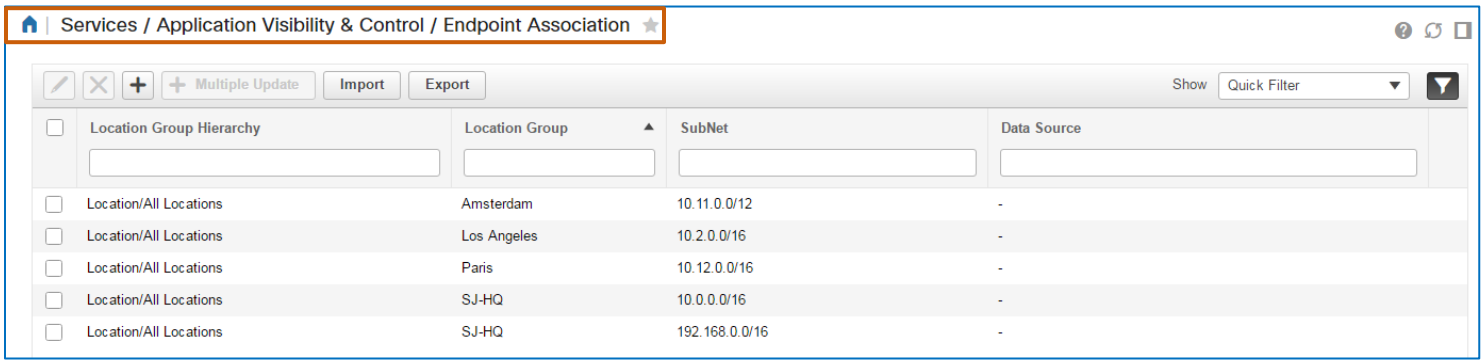


- In the dialog box, to add individual applications, in the **Available Applications** list, select the application or applications, and then click **Add**.
- To add all available applications, click **Add All**.
- To remove individual applications, in the **Business Critical Applications** list, select the application or applications, and then click **Remove**.
- To remove all applications, click **Remove All**.

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.



Monitoring Key Performance Indicators (KPIs)

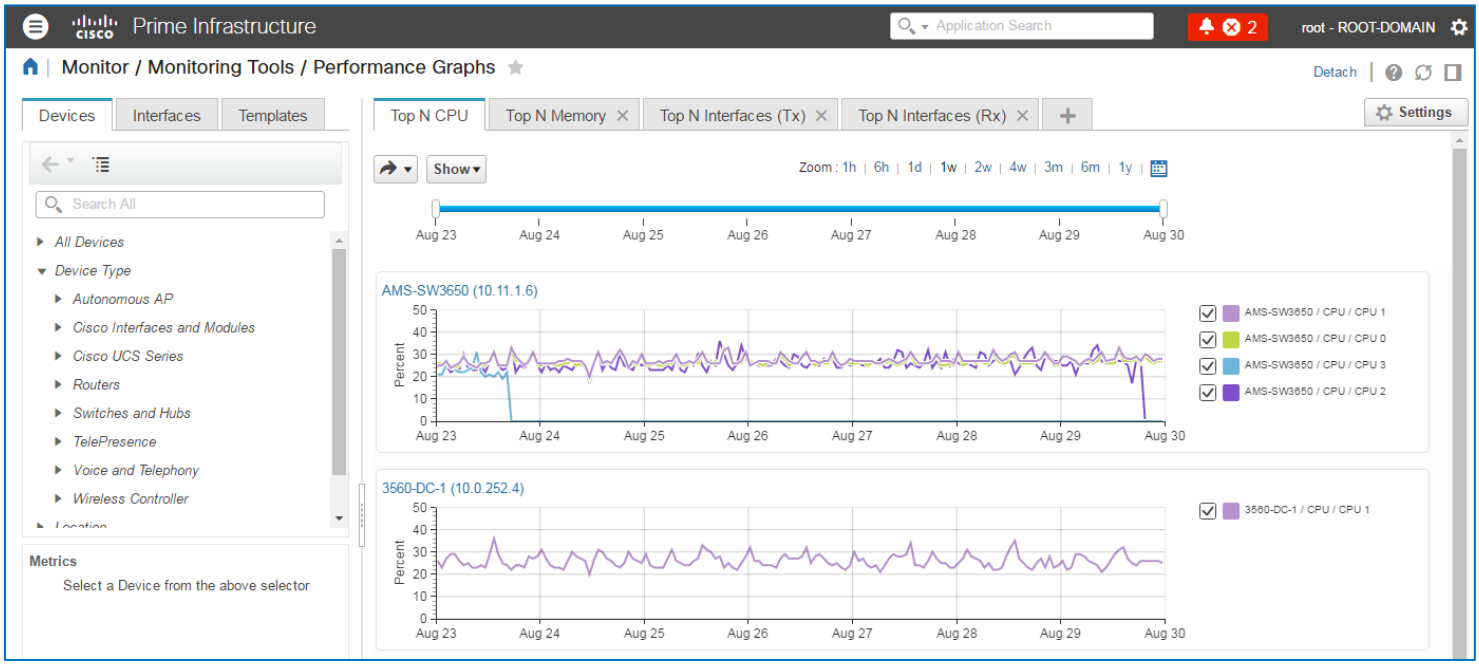
Performance Graphs

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:

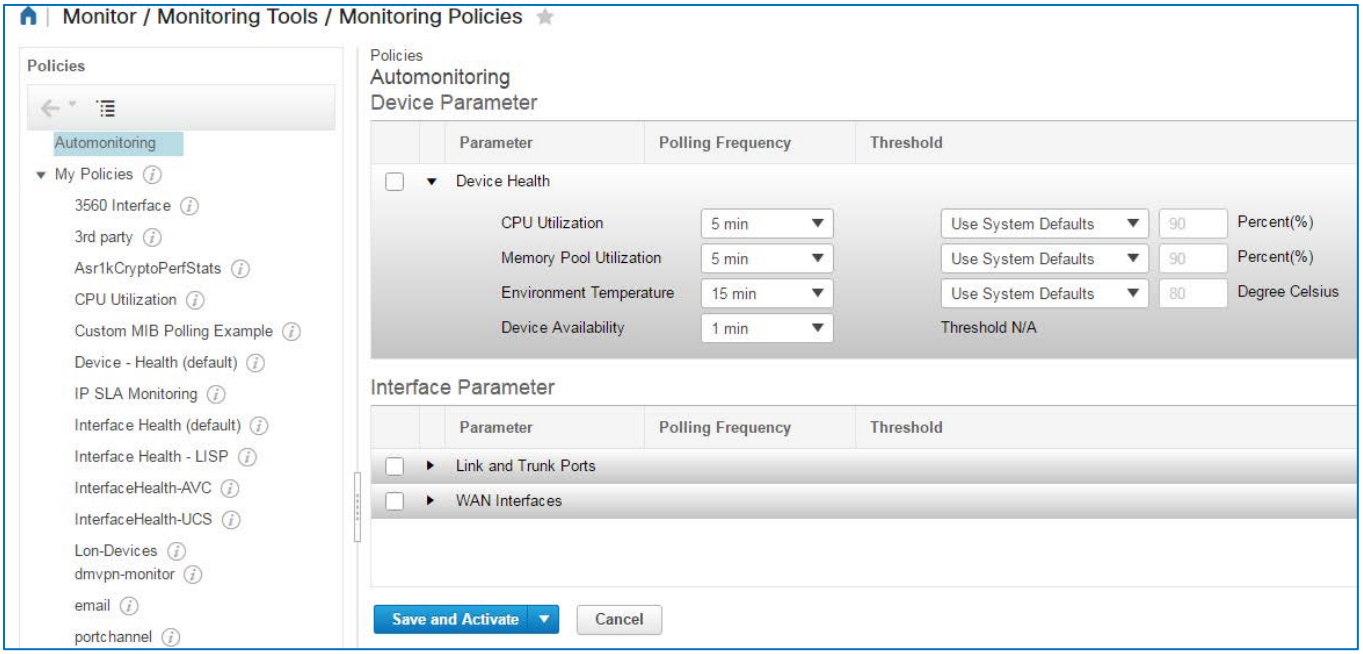
- **Top N CPU**
  Presents graphs for the devices, up to 10, that are experiencing the highest CPU usage
- **Top N Memory**
  Presents graphs for the devices, up to 10, that are experiencing the highest memory usage
- **Top N Interfaces (Tx)**
  Presents graphs for the interfaces, up to 10, that are 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.



Navigating Performance Graphs

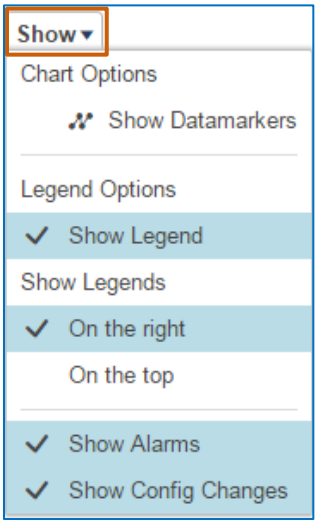
Managing Graph Data Elements

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:

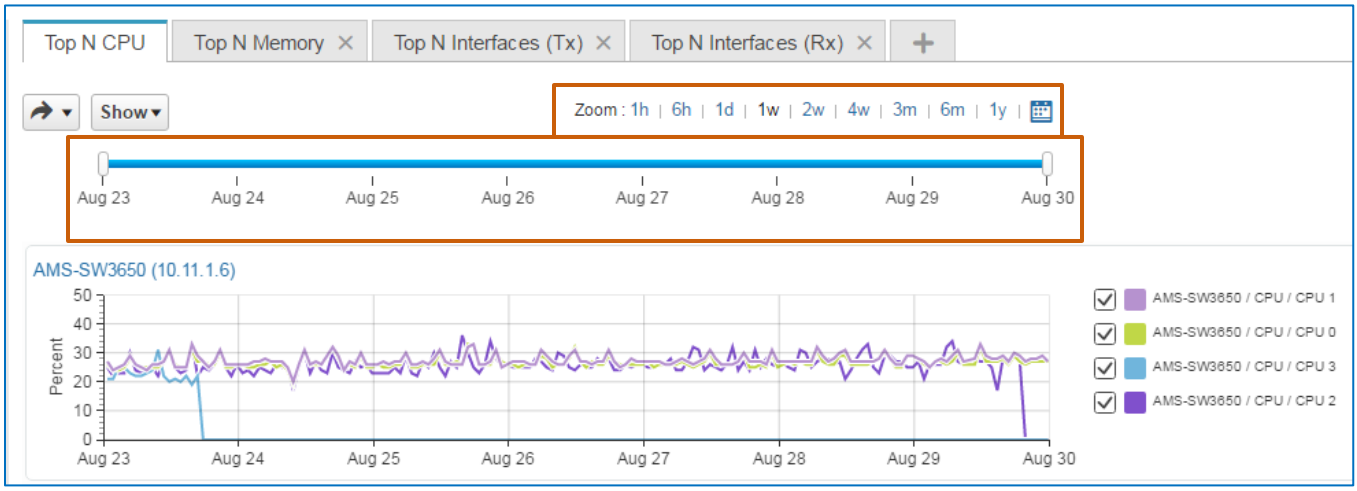
- Select **On the right** or **On the top**.

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.

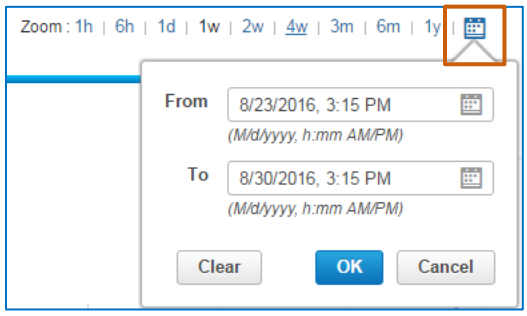


To apply a pre-defined time period by using the zoom tool:

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

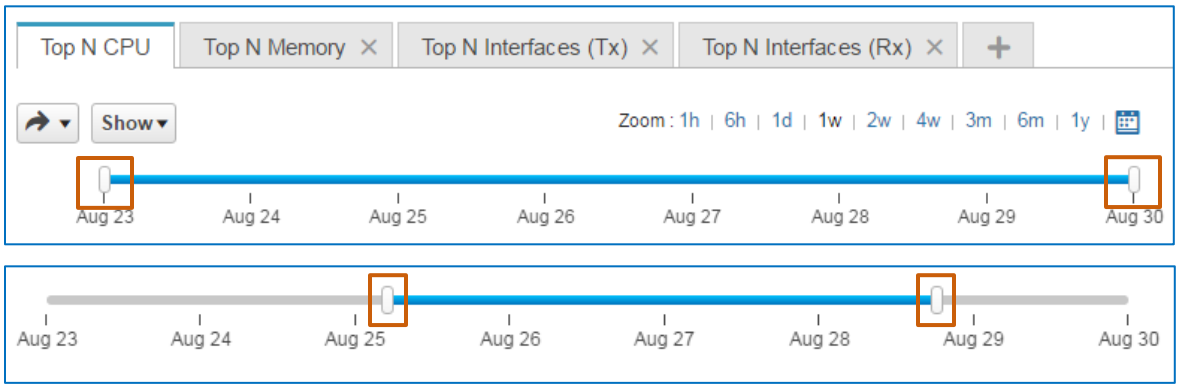
To apply a custom time period:

- 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:

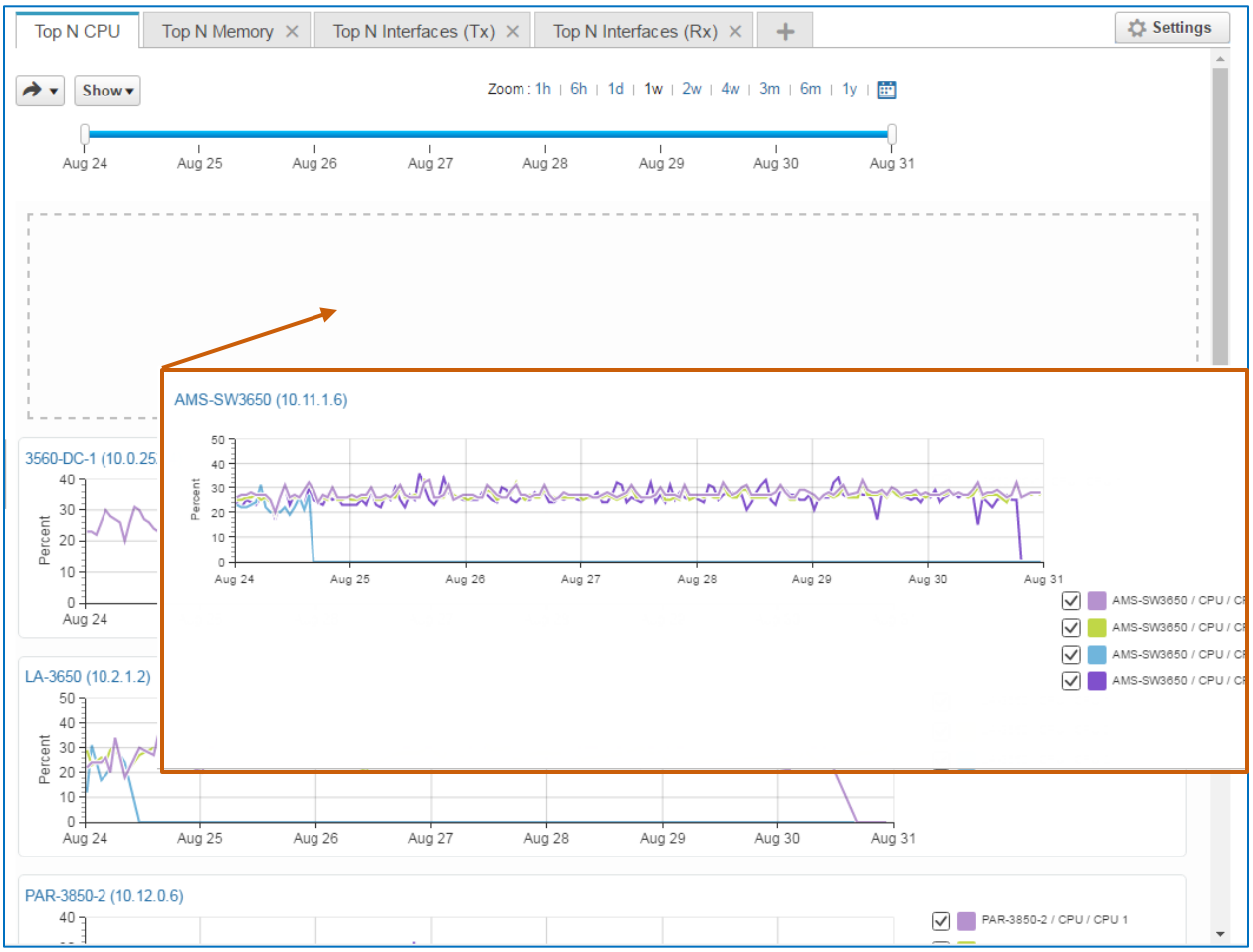
- On either side of the slider, drag the bar.



Changing Graph Layouts

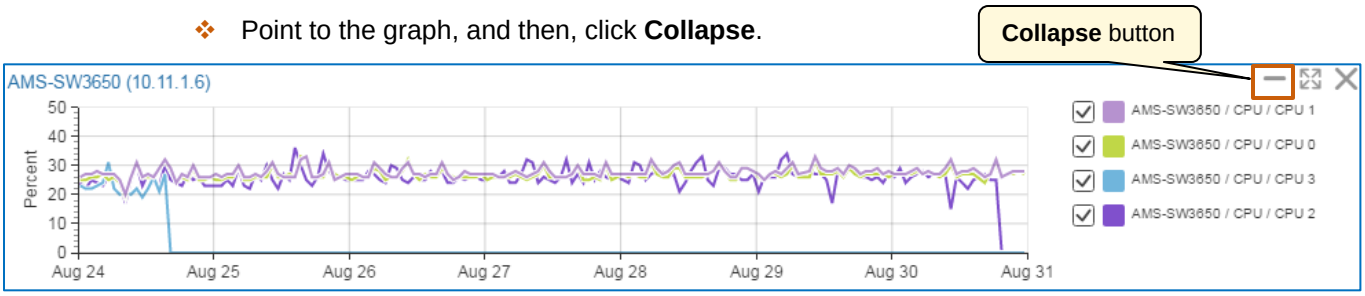
You can move graphs on a tab, maximize graphs for better visibility, or collapse graphs to make a series of graphs easier to see.

You move graphs using the drag and drop operation.

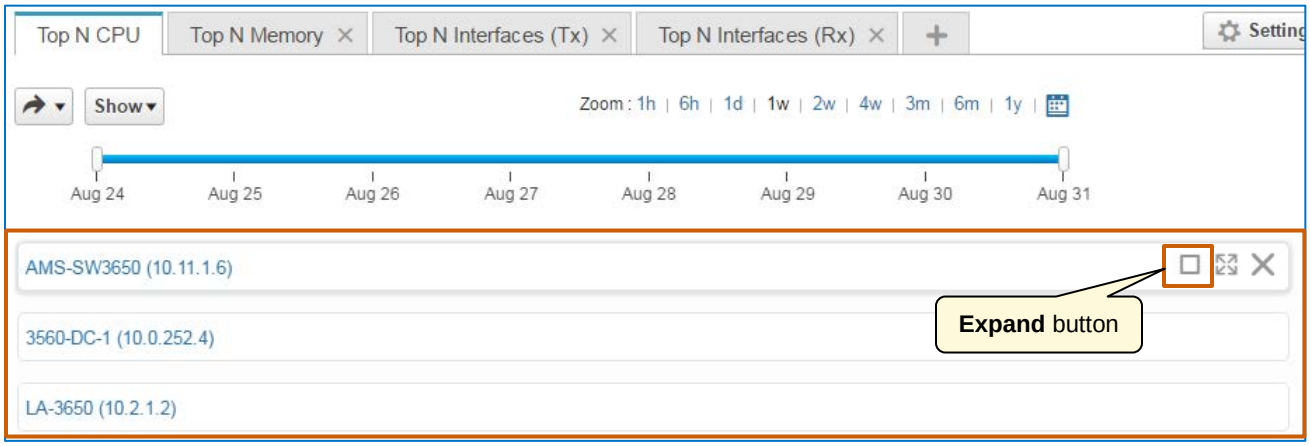


To collapse a graph:

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

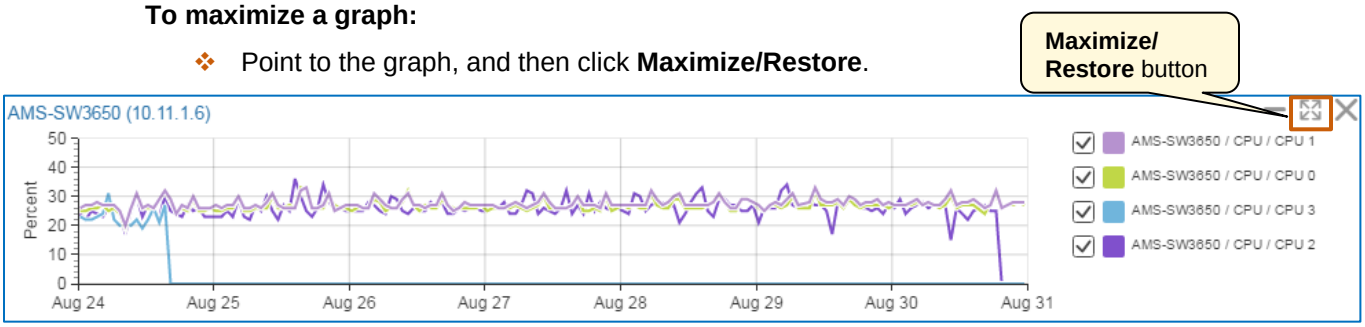


The graph view closes and remains available to expand and view, as needed. The **Collapse** button toggles to the **Expand** button.



To maximize a graph:

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

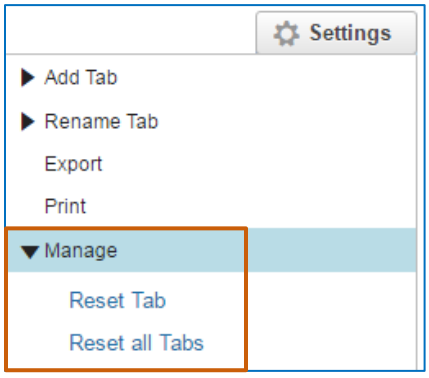


The graph view maximizes and the button icon changes.

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

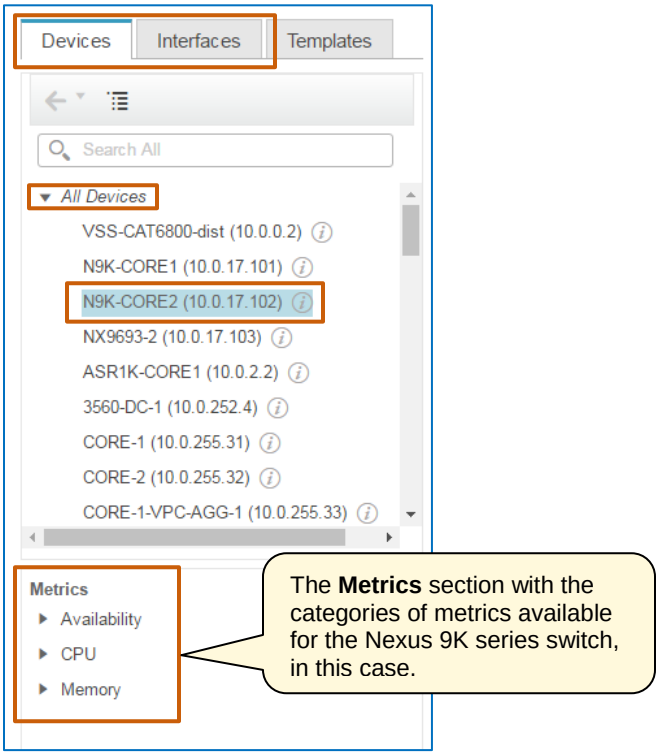
You add graphs by selecting the device or interface of interest, and then selecting the metrics that you need to see.

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

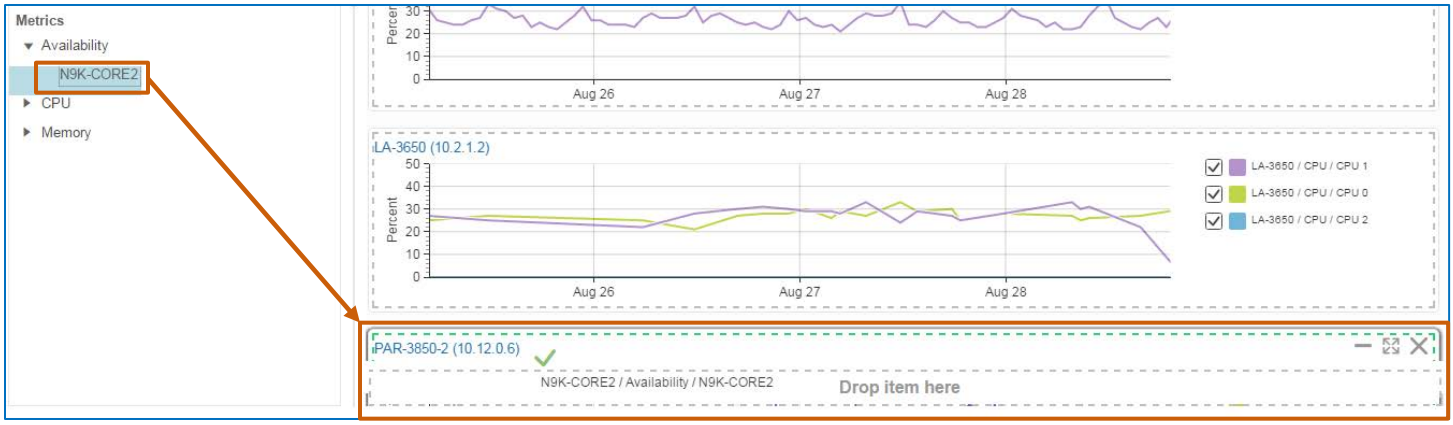
To add a device or interface graph:

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.

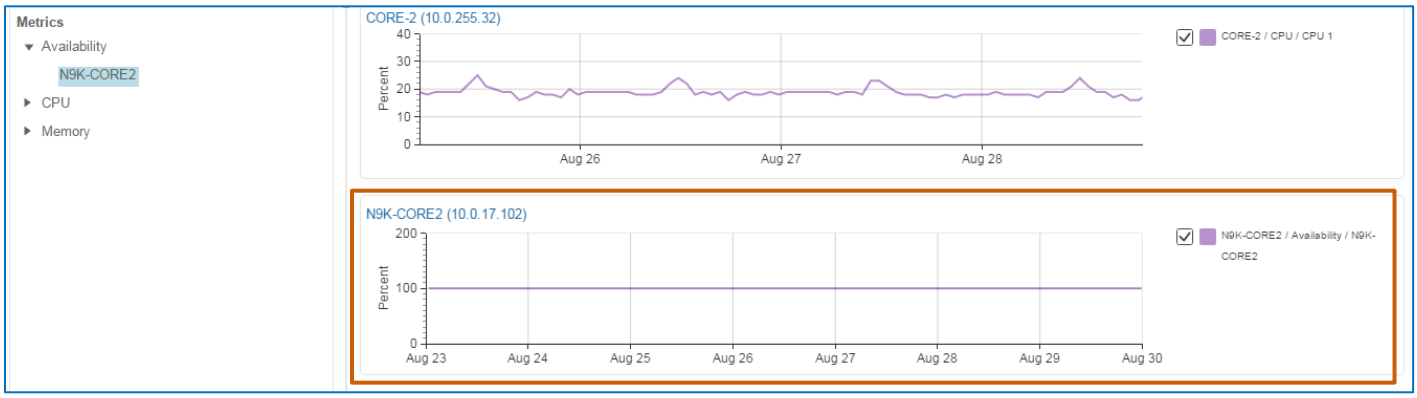
   Below the list, the **Metrics** section populates with the categories of metrics that are available for the element that you selected.



2. 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:

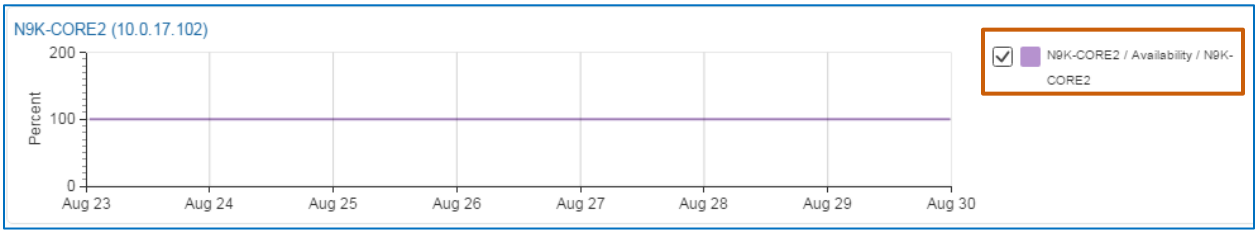
- On the **Show** drop-down menu, select **Show Config Changes**.

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.

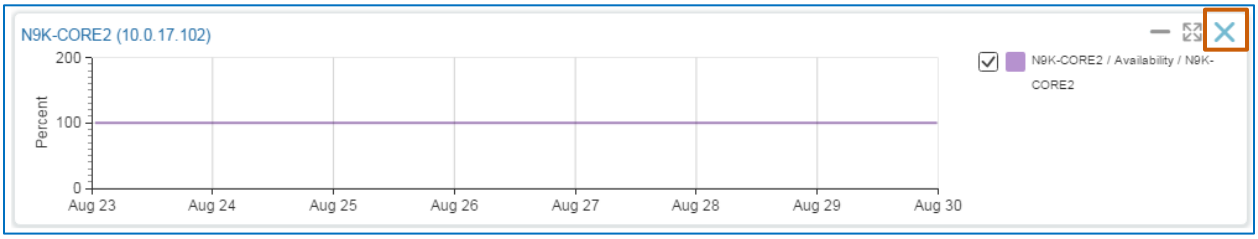


You can remove graphs that do not apply to your task or that you no longer need.

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

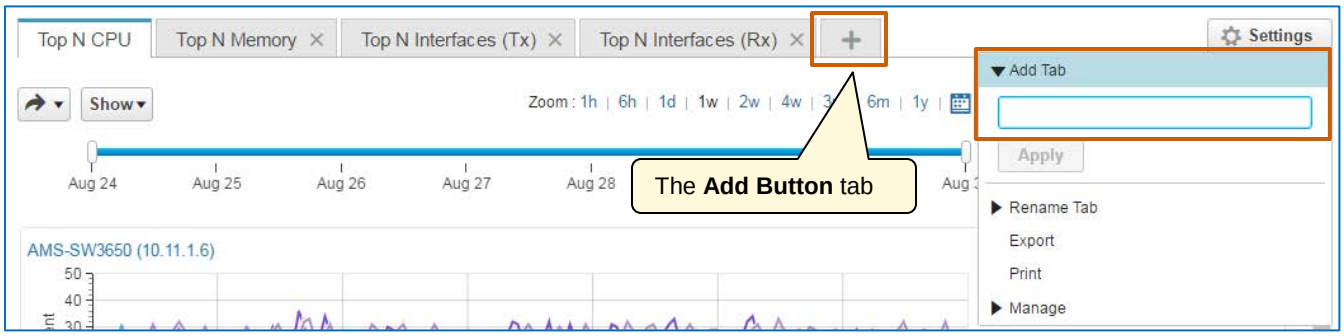
While the **Performance Graphs** page provides default tabs, you can add custom tabs or remove those tabs that you do not need.

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.

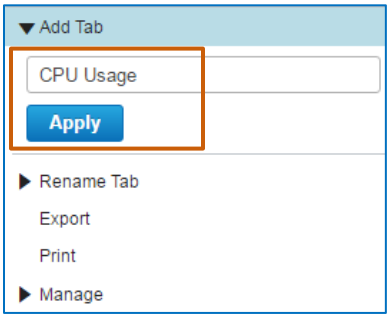
To add a custom tab:

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

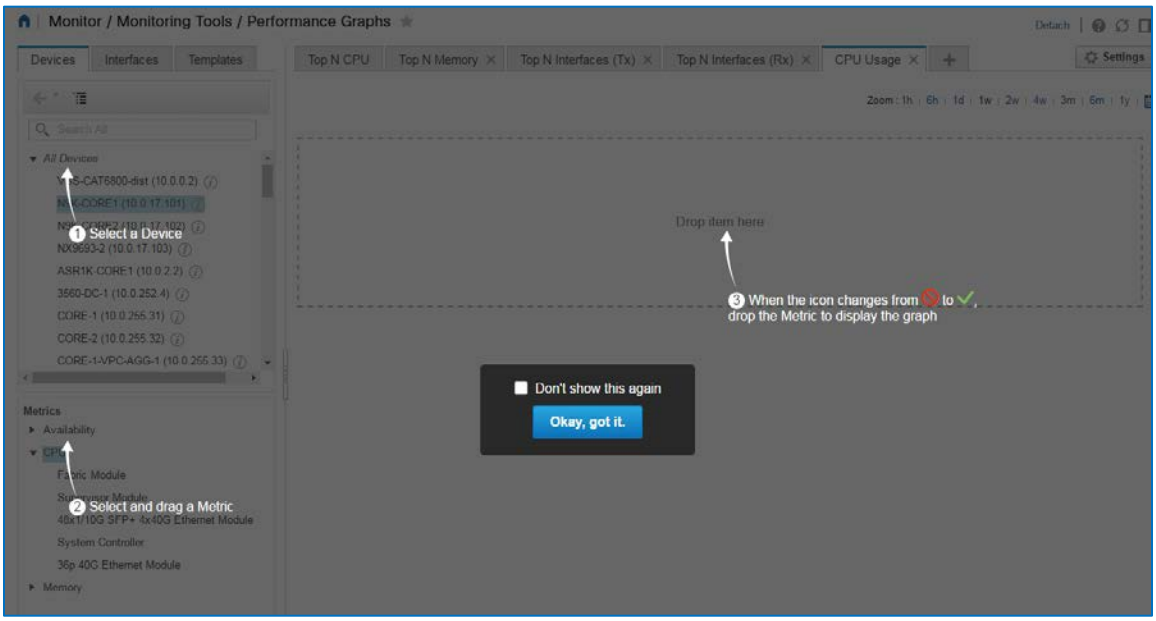
   The **Settings** drop-down menu opens with the **Add Tab** field active.



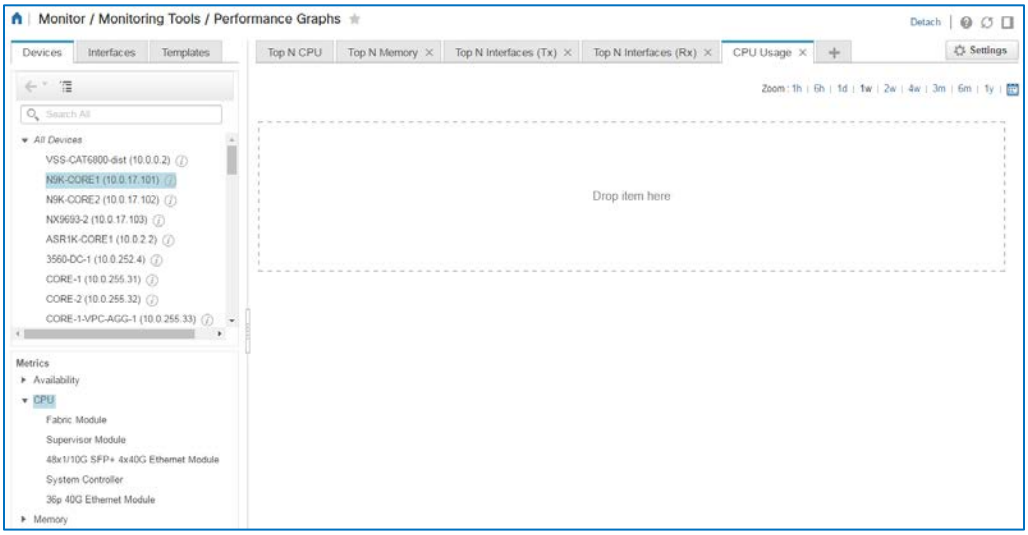
2. In the **Add Tab** field, type the name of the tab as you want it to appear on the page, and then click **Apply**.



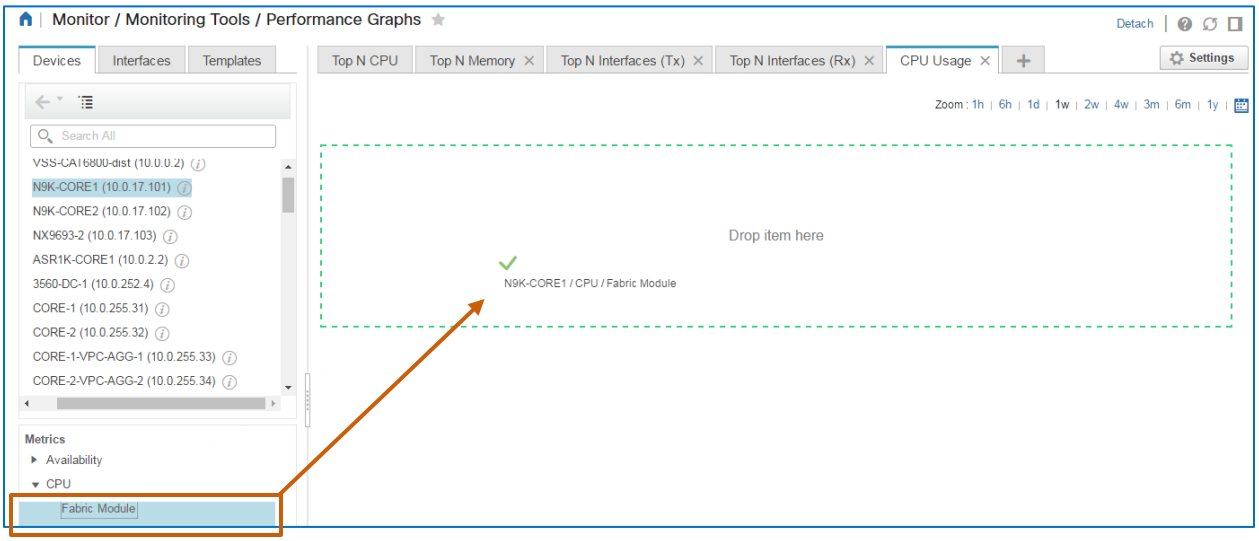
On initial use, a help overlay opens, which you can configure to remain closed when you no longer need it.



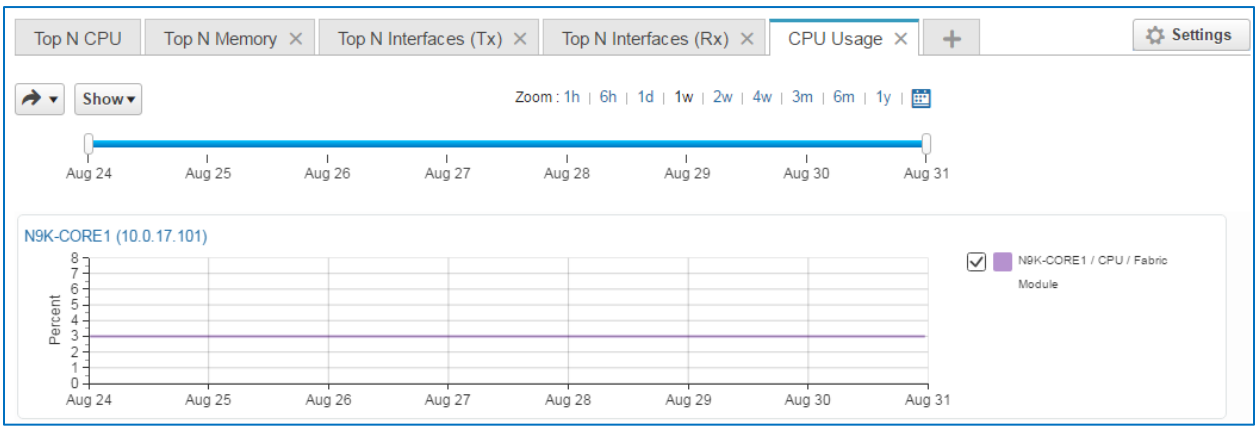
When you clear the overlay, the tab that you added is available for adding graphs.



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.



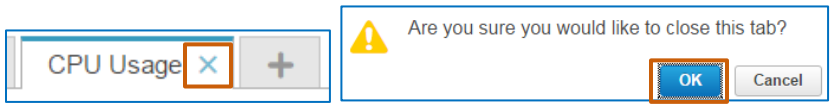
The graph begins reporting data by using the applicable polling interval for the KPI.



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**.



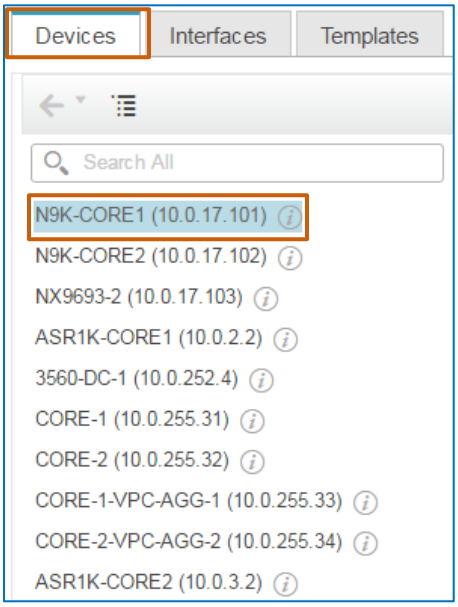
The system removes the tab.

Adding Multiple Metrics to Graphs

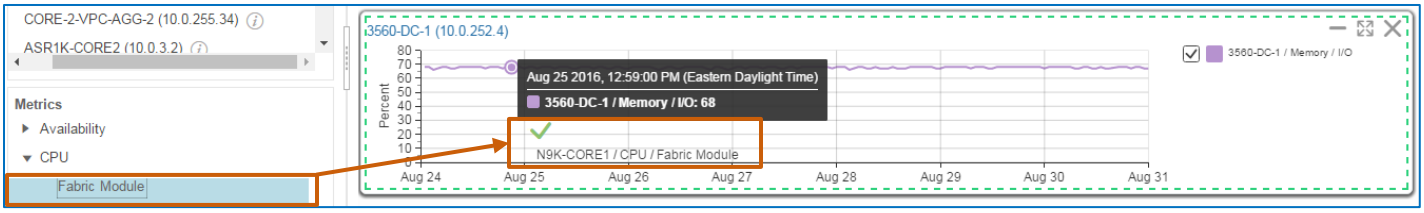
For comparative purposes, you can add multiple metrics to a single graph. For example, you might find it helpful to add CPU and memory metrics for a component on a single graph to determine whether issues related to either metric correlate.

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.

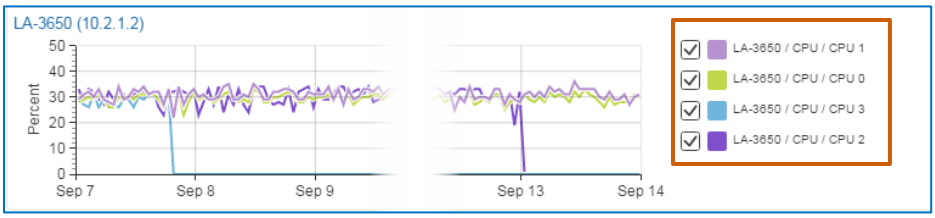


3. To continue adding metrics to the graph, repeat steps 1 and 2.

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.

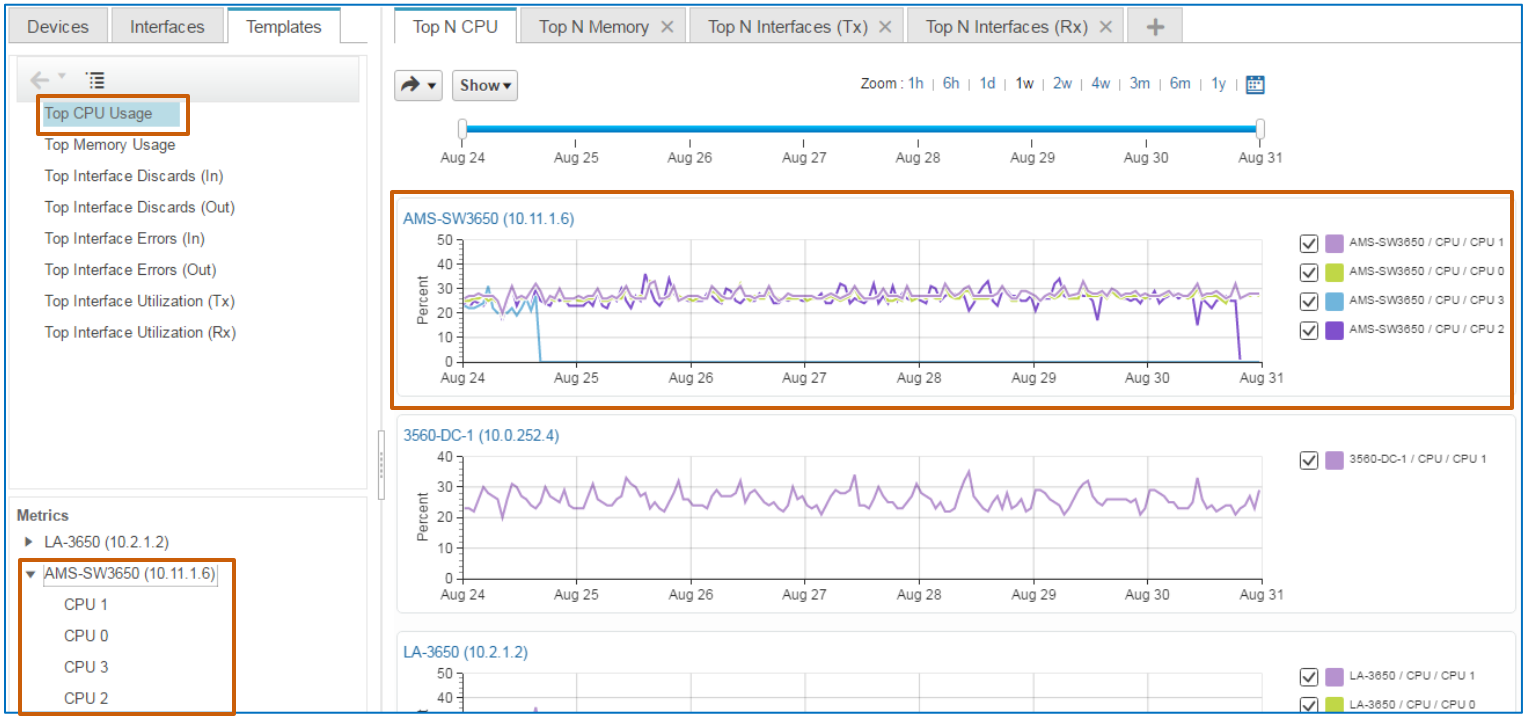
You can evaluate network elements that are experiencing the highest:

- 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.



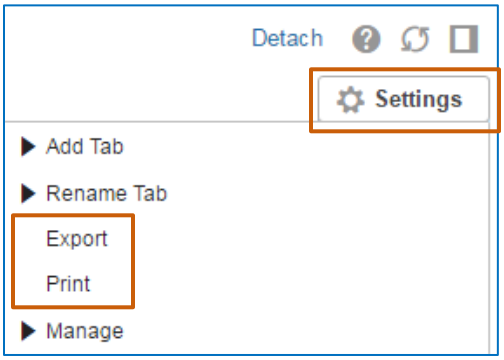
Exporting or Printing Graph Data

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.

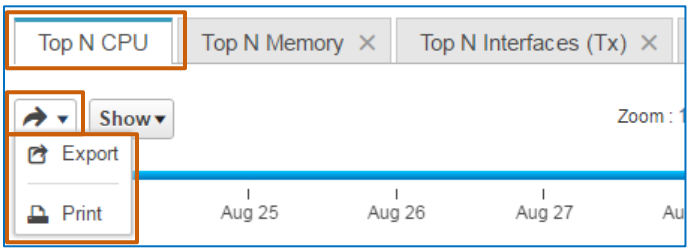
To export or print global level data:

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



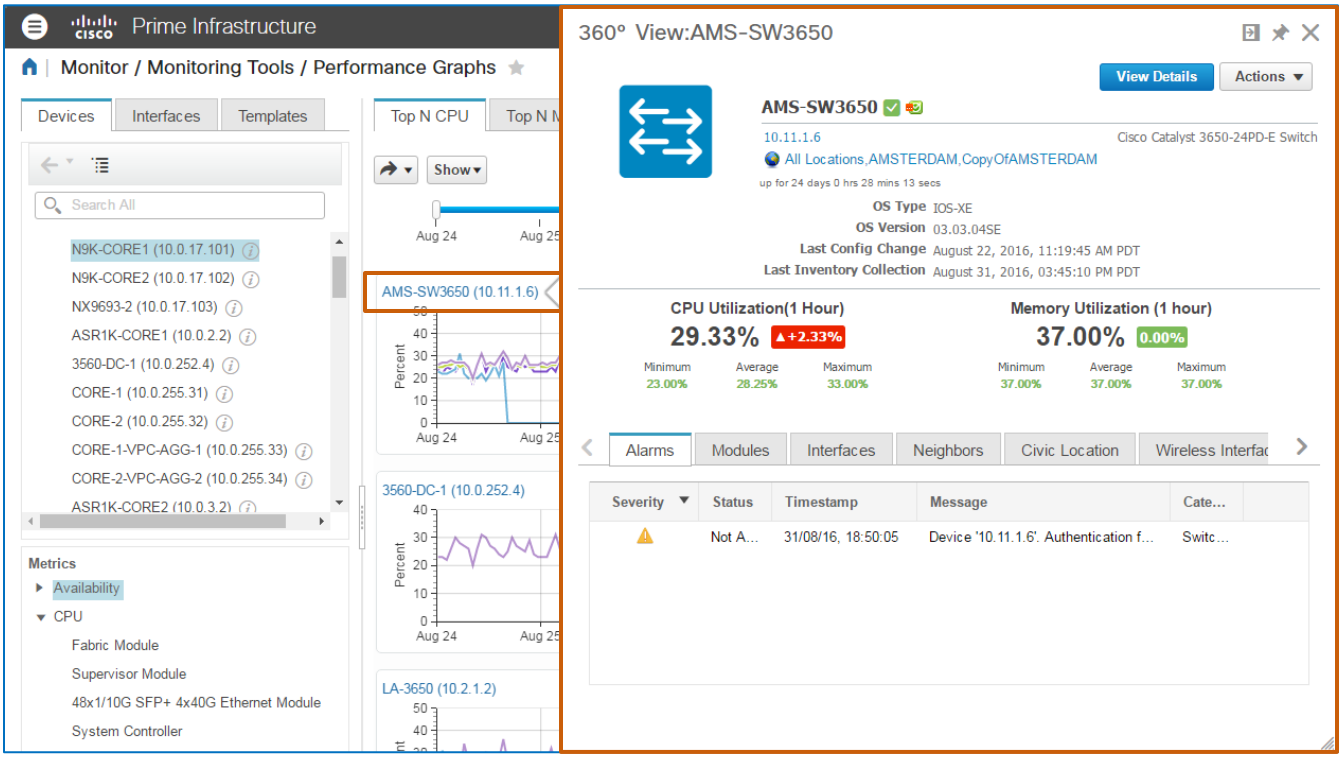
To export or print tab level data:

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



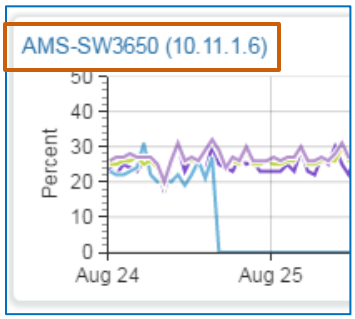
Reviewing Device or Interface Details or Taking Actions

Performance graphs provide direct access to device details in a device **360⁰ 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.

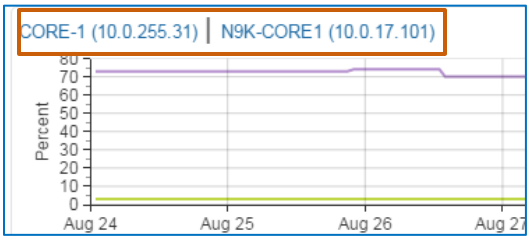


To open a 360⁰ View pop-window:

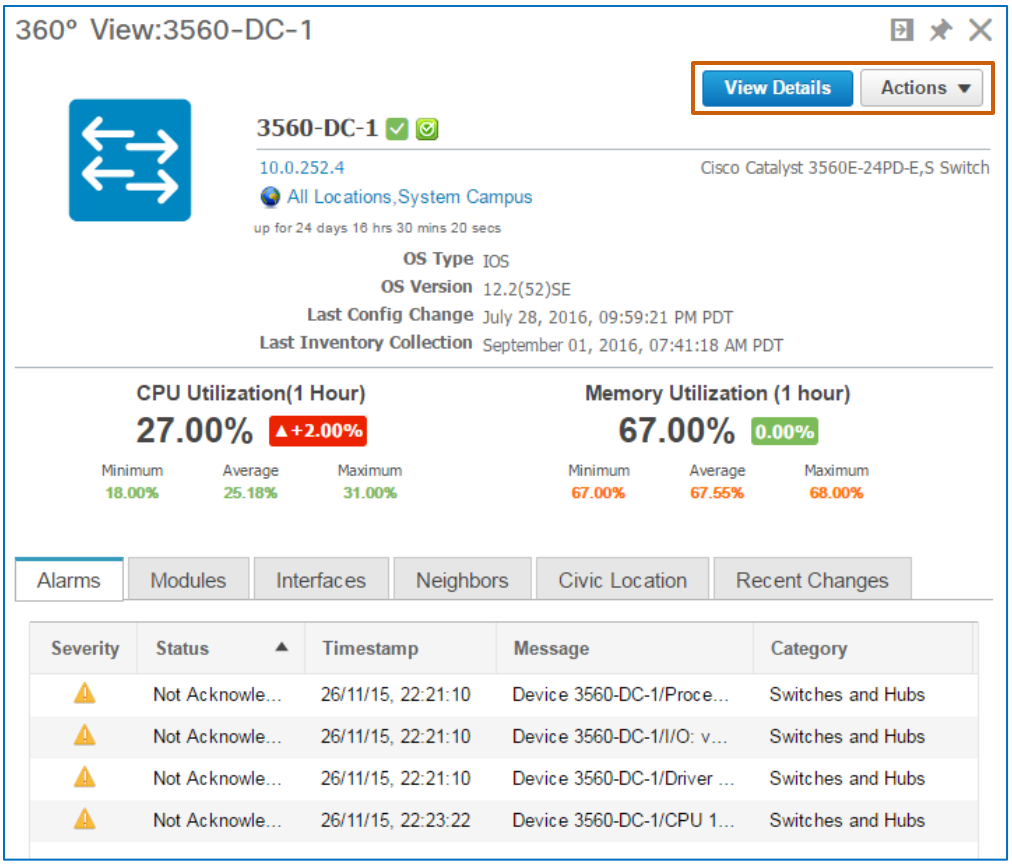
- On a graph, click the name link on the graph.



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



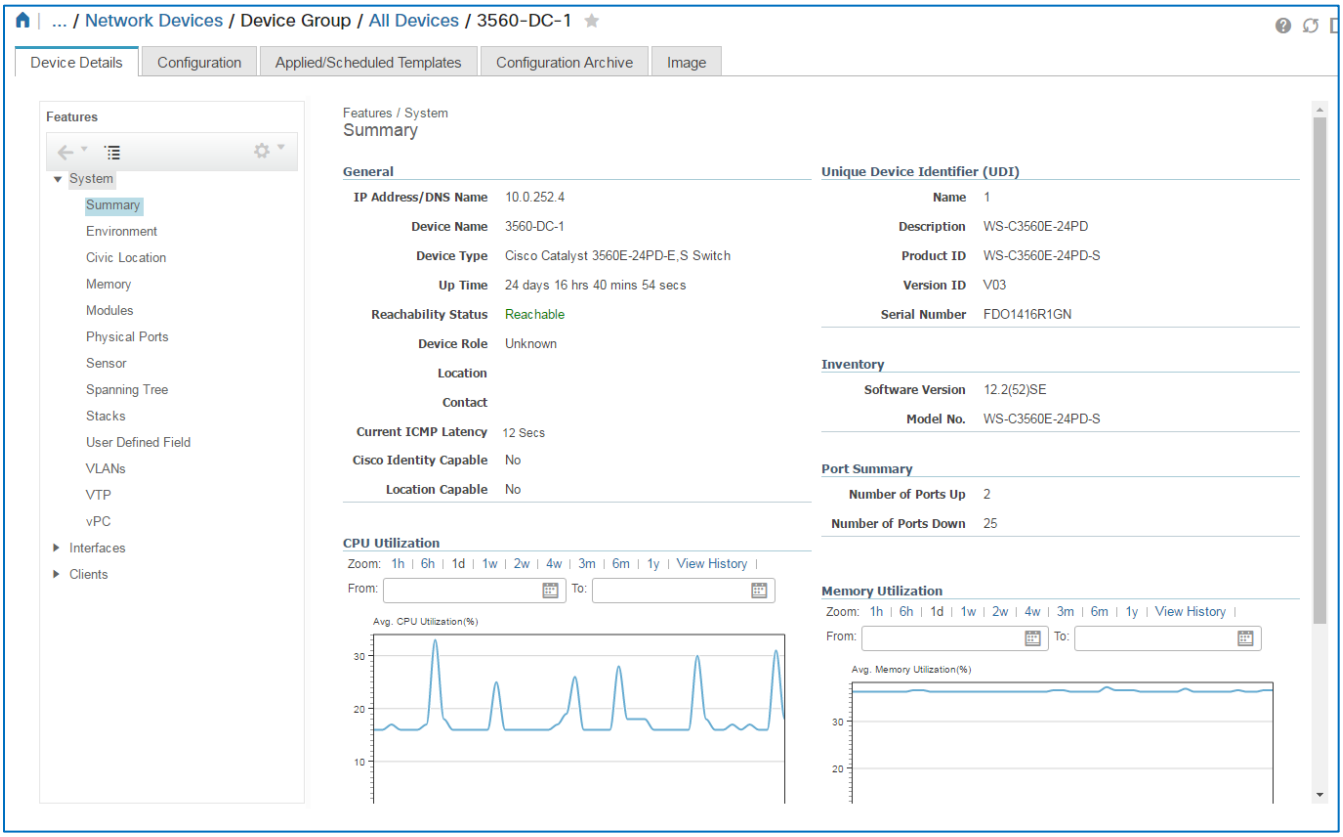
In addition to finding key information about the device, you can open the details and configuration, or take actions, as needed.



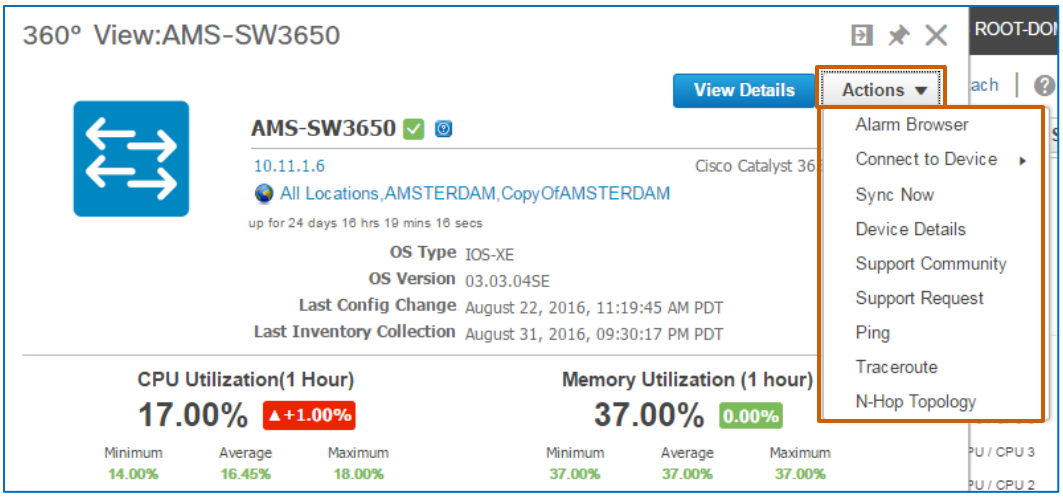
To open device details:

- In the device **360⁰ 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.



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



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.