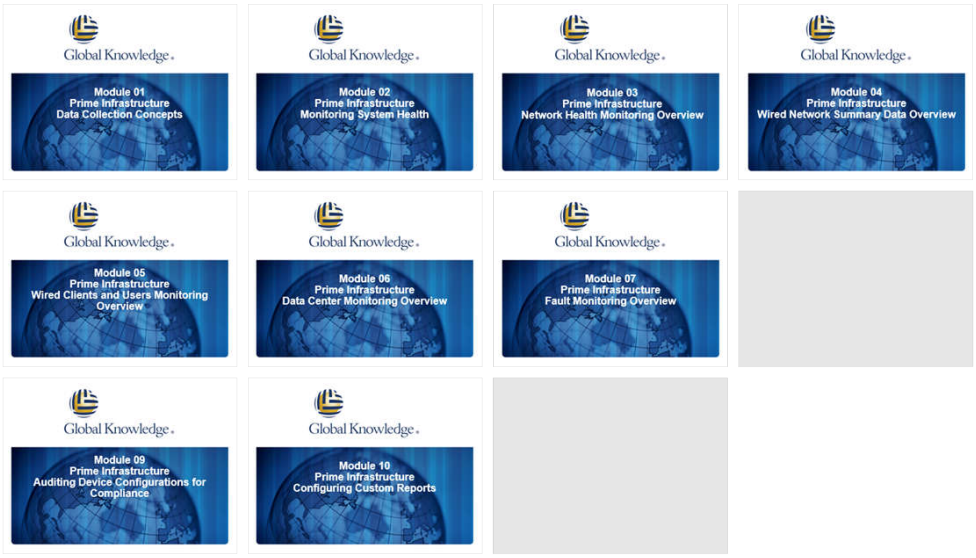
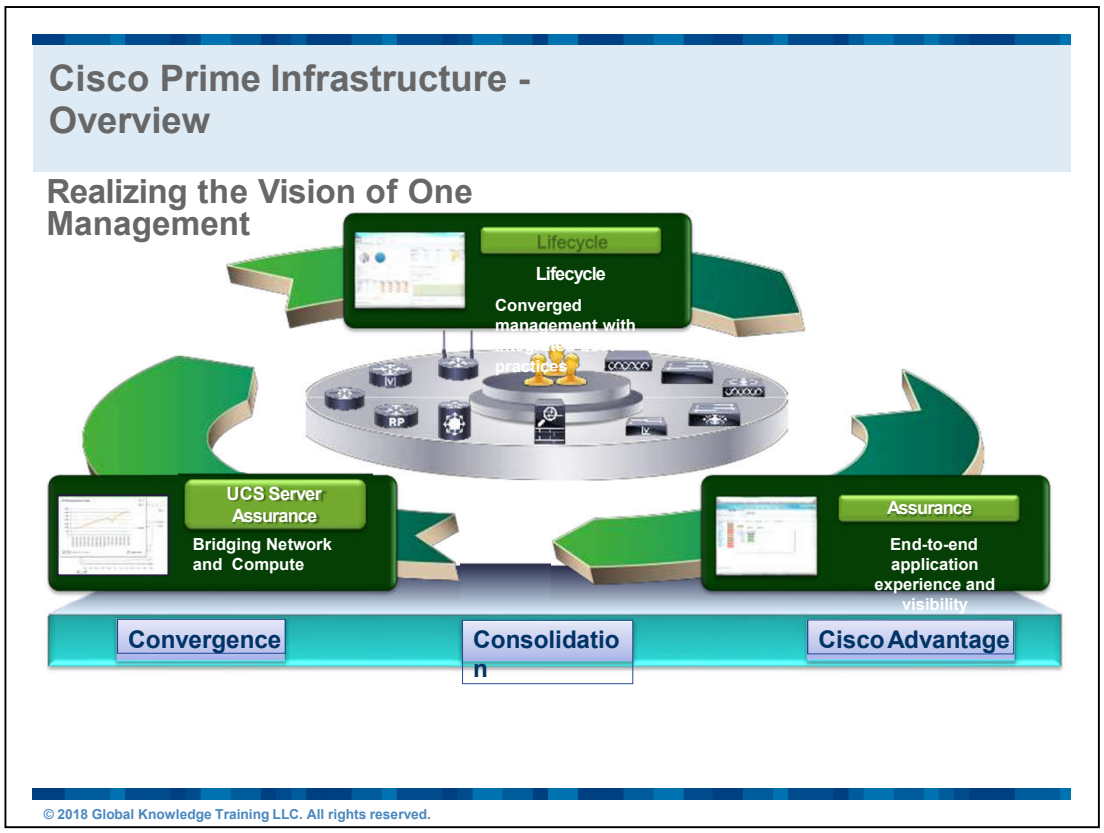
Cisco Prime Infrastructure




Prime Infrastructure Overview



Prime Infrastructure enables you to configure and monitor one or more controllers, switches and associated access points. Prime Infrastructure includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

On Linux, Prime Infrastructure runs as a service, which runs continuously and resumes running after a reboot.

The Cisco Prime Infrastructure user interface requires Mozilla Firefox 11.0 or 12.0 or Internet Explorer 8 or 9 with the Chrome plugin releases or Google Chrome 19.0. The Internet Explorer versions less than 8 are not recommended. The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Note We strongly recommend that you do not enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing **Tools** > **Internet Options** and unselecting the **Enable third-party browser extensions** check box on the Advanced tab.

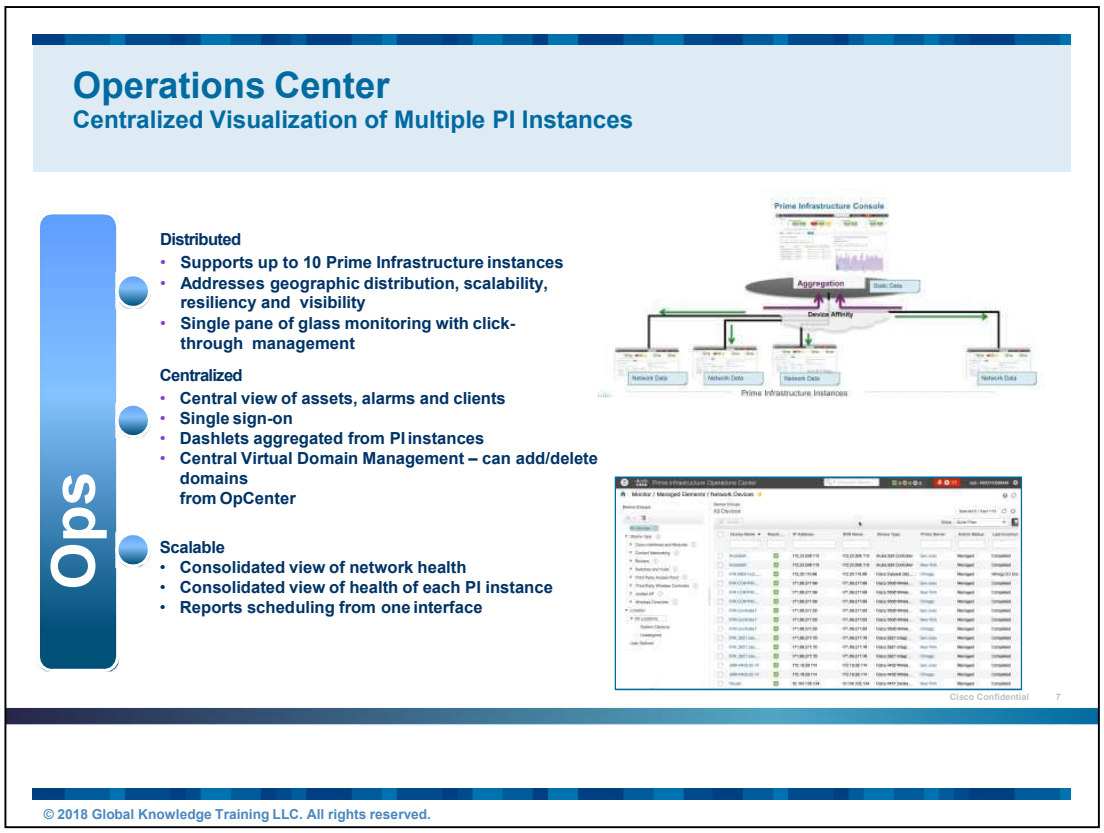
Prime Infrastructure simplifies controller configuration and monitoring and reduces data entry errors. Prime Infrastructure uses the industry-standard SNMP protocol to communicate with the controllers.

Prime Infrastructure also includes the *Floor Plan editor,* which allows you to do the following:

Access vectorized bitmap campus, floor plan, and outdoor area maps.

Add and change wall types.

Import the vector wall format maps into the database.



How to Monitor Multiple Cisco Prime Infrastructure Instances

There are three situations in which you will want to use multiple Cisco Prime Infrastructure server instances to manage your network:

You want to categorize the devices in your network into logical groups, with a different Cisco Prime Infrastructure instance managing each of those groups. For example, you could have one instance managing all of your network's wired devices and another managing all of its wireless devices.

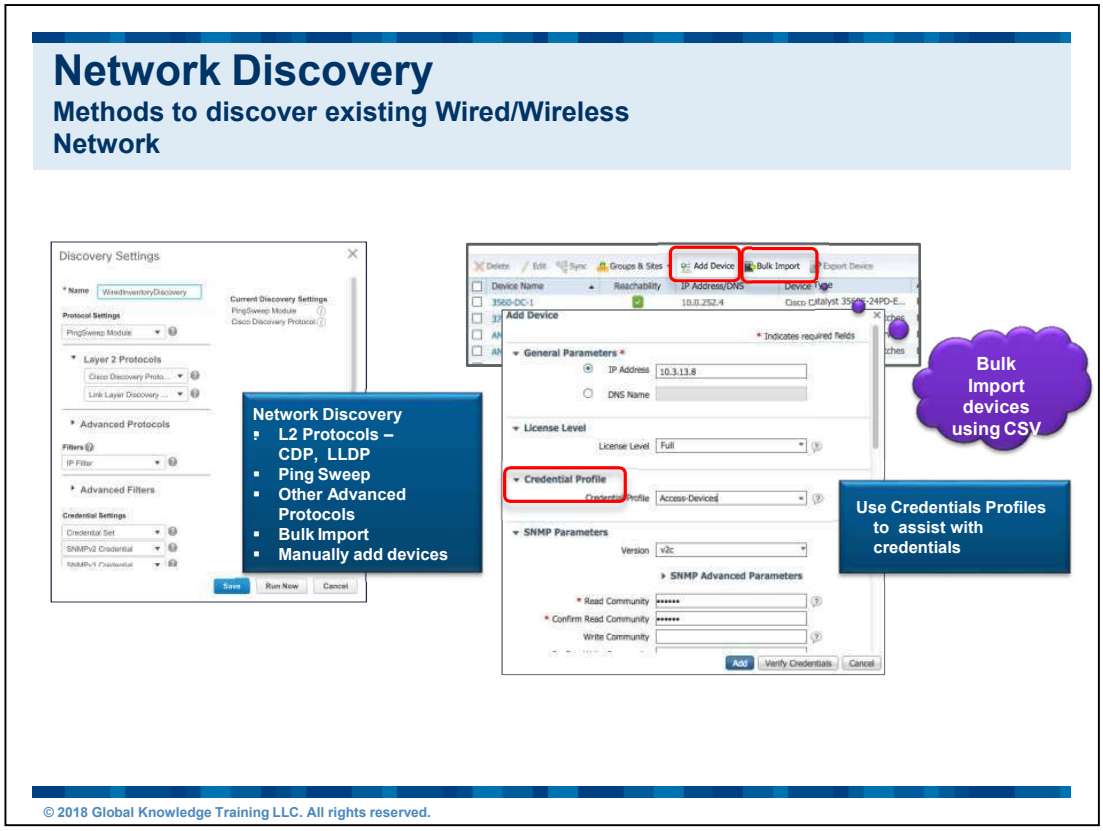
The one Cisco Prime Infrastructure instance you have running is sufficient to manage your network, but the addition of one or more instances would improve Cisco Prime Infrastructure performance by spreading the CPU and memory load among multiple instances.

Your network has sites located throughout the world, and you want a different Cisco Prime Infrastructure instance to manage each of those sites in order to keep their data separate.

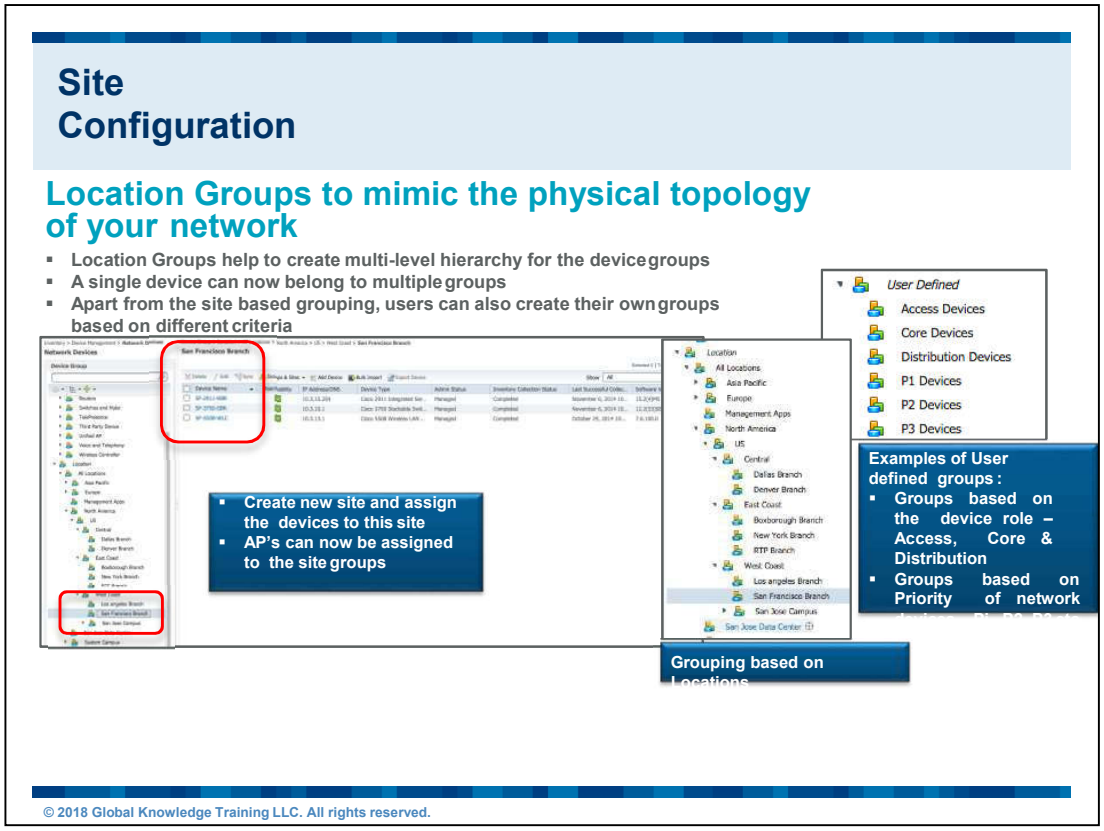
If multiple Cisco Prime Infrastructure instances are running in your network, you can monitor those instances from the Operations Center. In this chapter, we will cover a typical workflow you might employ when using the Operations Center. This workflow consists of the following tasks:

Use the Operations Center Config Dashboard to Manage Multiple Cisco Prime Infrastructure Servers

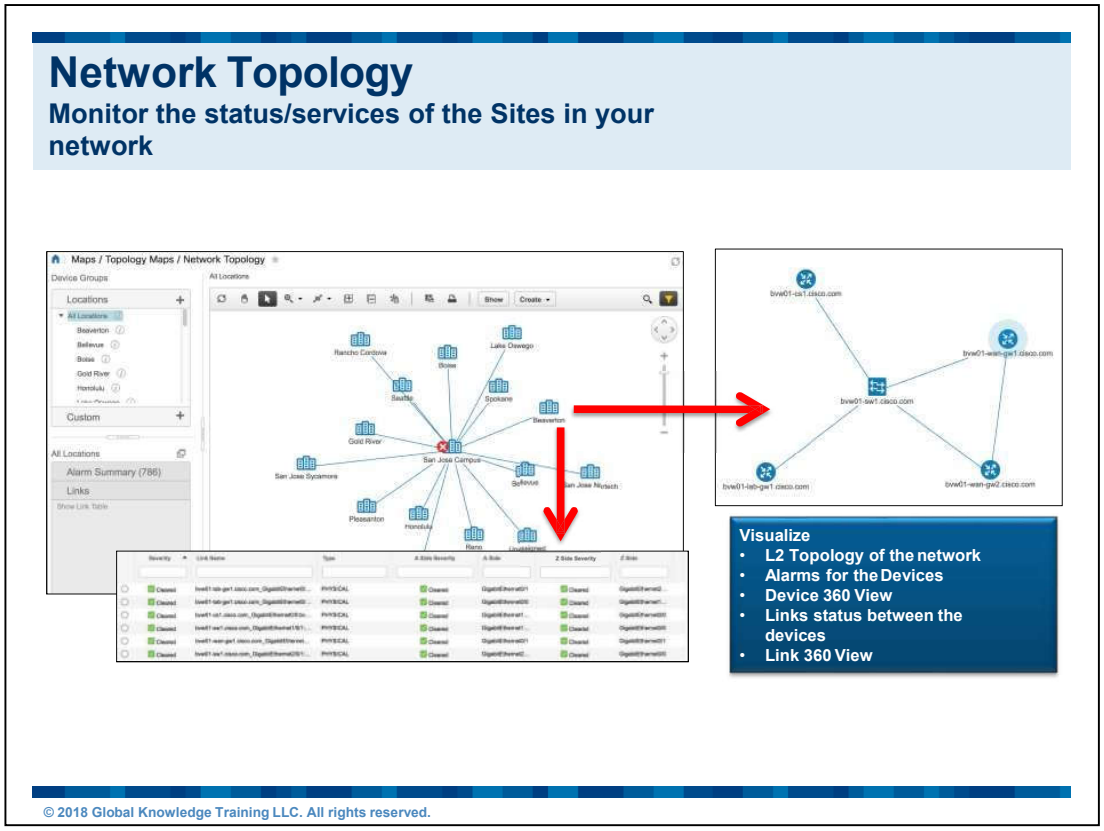
Run Reports on Deployments with Multiple Cisco Prime Infrastructure Servers Using Operations Center



When you run discovery, Prime Infrastructure discovers the devices and, after obtaining access, collects device inventory data. We recommend that you run discovery, when you are initially getting started with Prime Infrastructure. Prime Infrastructure uses SNMP polling to gather information about your network devices within the range of IP addresses you specify. If you have CDP enabled on your network devices, Prime Infrastructure uses the seed device you specify to discover the devices in your network. You can discover your devices by: • Configuring discovery settings—This method is recommended if you want to specify settings and rerun discovery in the future using the same settings. See Running Discovery. • Running Quick Discovery—Quick Discovery quickly ping sweeps your network and uses SNMP polling to get details on the devices. See Running Quick Discovery.



Cisco Prime Infrastructure provides a visual map of your network's physical topology, including the network devices and the links that connect them. The topology maps have indicators that show the current alarm status of network devices and links. Using these network topology maps, you can easily monitor your network by viewing alarms in the context of the interconnection between devices.



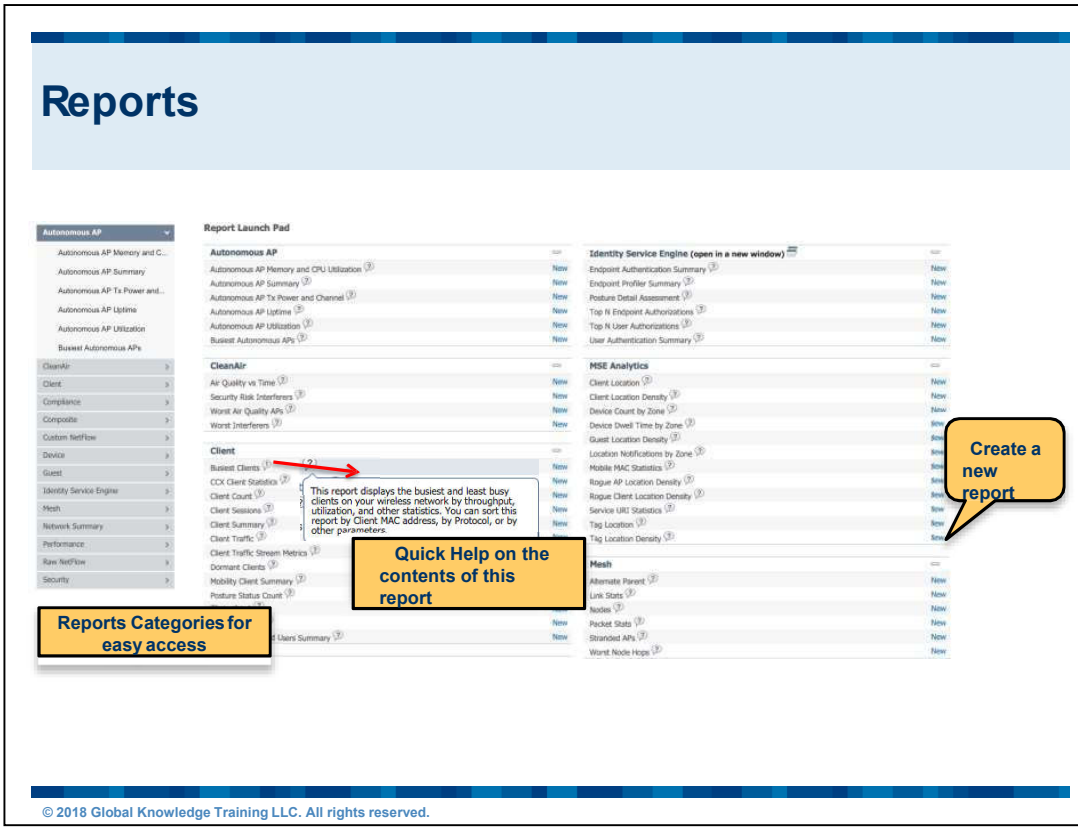
Prime Infrastructure topology maps are based on Location and User Defined groups (see “Types of Groups” in Related Topics). Topology maps show the devices in the group as well as any links between the devices.

The links between devices are discovered using the Cisco Discovery Protocol (CDP). If Prime Infrastructure is unable to discover some links, for example, if CDP is disabled on an interface, you can manually add the link to the topology map, and the associate the link with a specific interface on the appropriate managed device.

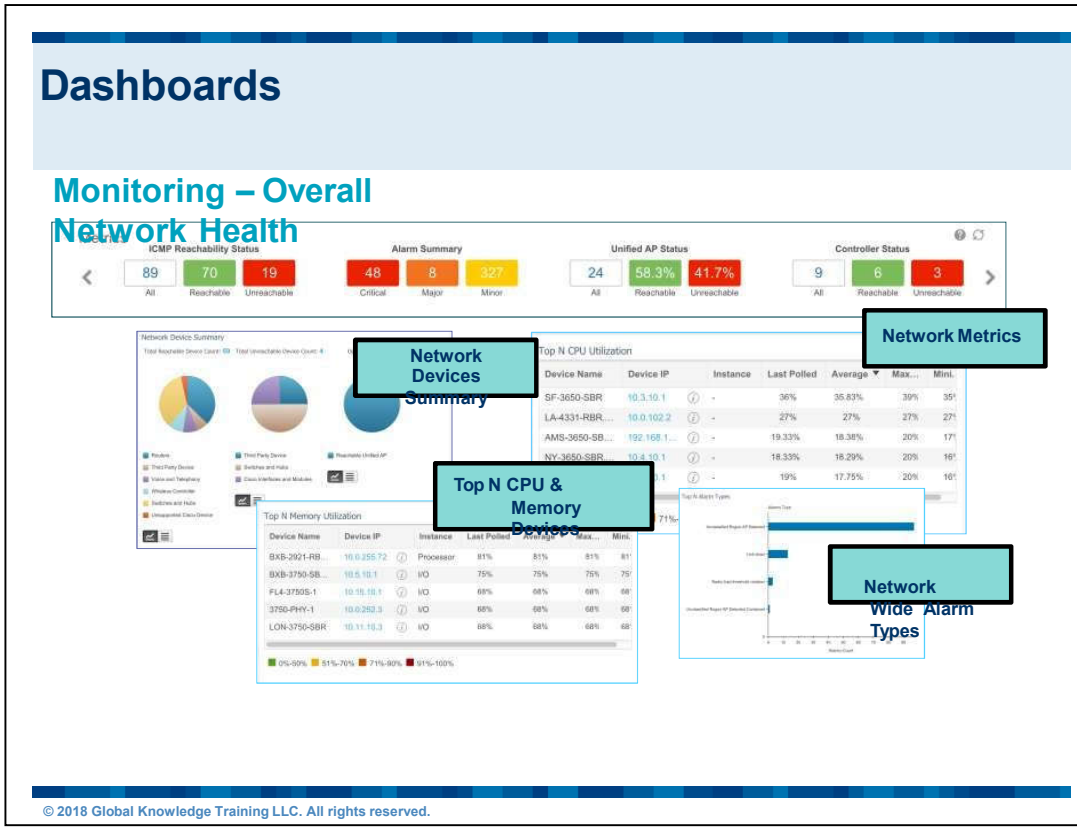
You can also add “unmanaged devices” or “unmanaged network” icons to a topology map and add links between these unmanaged objects and managed devices in the topology map (see “Adding Unmanaged Devices and Links to Topology Maps” in Related Topics).

You can add autonomous APs to Prime Infrastructure topology maps, but you cannot add Unified APs.

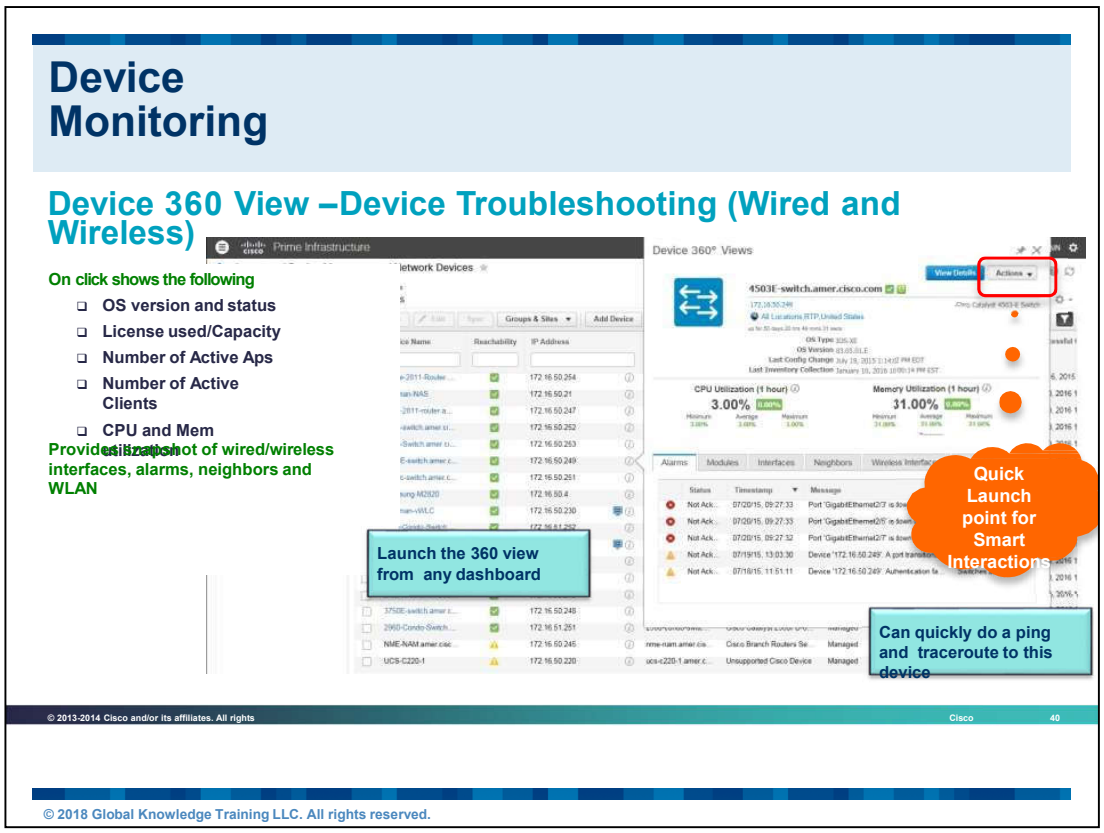
The Network Topology window presents a graphical, topological map view of the devices, the links between them, and the active alarms on the devices or links. The Network Topology window also provides access to information and functions relating to device groups, alarms, and links, and allows you to drill down to get detailed information about the devices displayed in the topology map.



Cisco Prime Infrastructure reporting is necessary to monitor the system and network health as well as troubleshoot network problems. A number of reports can be generated to run on an immediate or a scheduled basis. Reports can also be combined to form composite reports. Each report type has a number of user-defined criteria to aid in defining the reports. The reports can be formatted as a summary, tabular, or combined (tabular and graphical) layout. After they have been defined, the reports can be saved for future diagnostic use or scheduled to run on a regular basis.



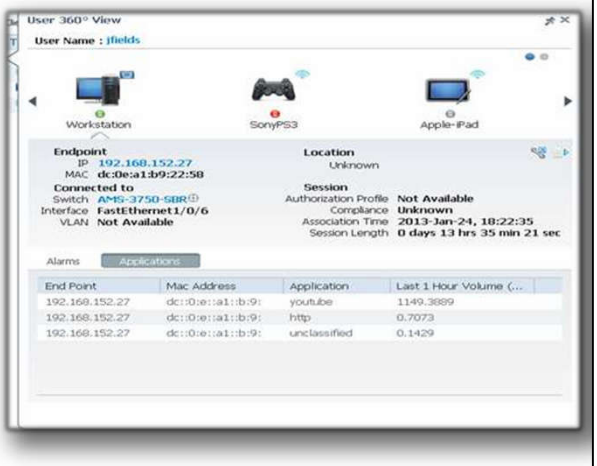
One of PI's biggest strength's is its ability to give you a lot of information in a small amount of real estate. Cisco crams in so much information that I found navigation to be the greatest learning curve of the whole software package. Cisco could probably do a better job of helping the newbie learn where everything is located.



Get Device Details from Device 360° View The Device 360° View provides detailed device information including device status, interface status, and associated device information. You can see the device 360° view from nearly all pages in which device IP addresses are displayed. To launch the 360° view of any device, click the info icon next to the device IP address.

User 360 View

- Concise End-User information about devices from anywhere within the product
- 360 views available for wired and wireless Users
- On click shows the following
  - ✓ OS version and status
  - ✓ License used/Capacity
  - ✓ Number of Active Aps
  - ✓ Number of Active Clients
  - ✓ CPU and Memory utilization
- Provides snapshot of device(s), alarms, and application used per device per user



Getting User Details from the User 360° View

The User 360° View provides detailed information about an end user, including:

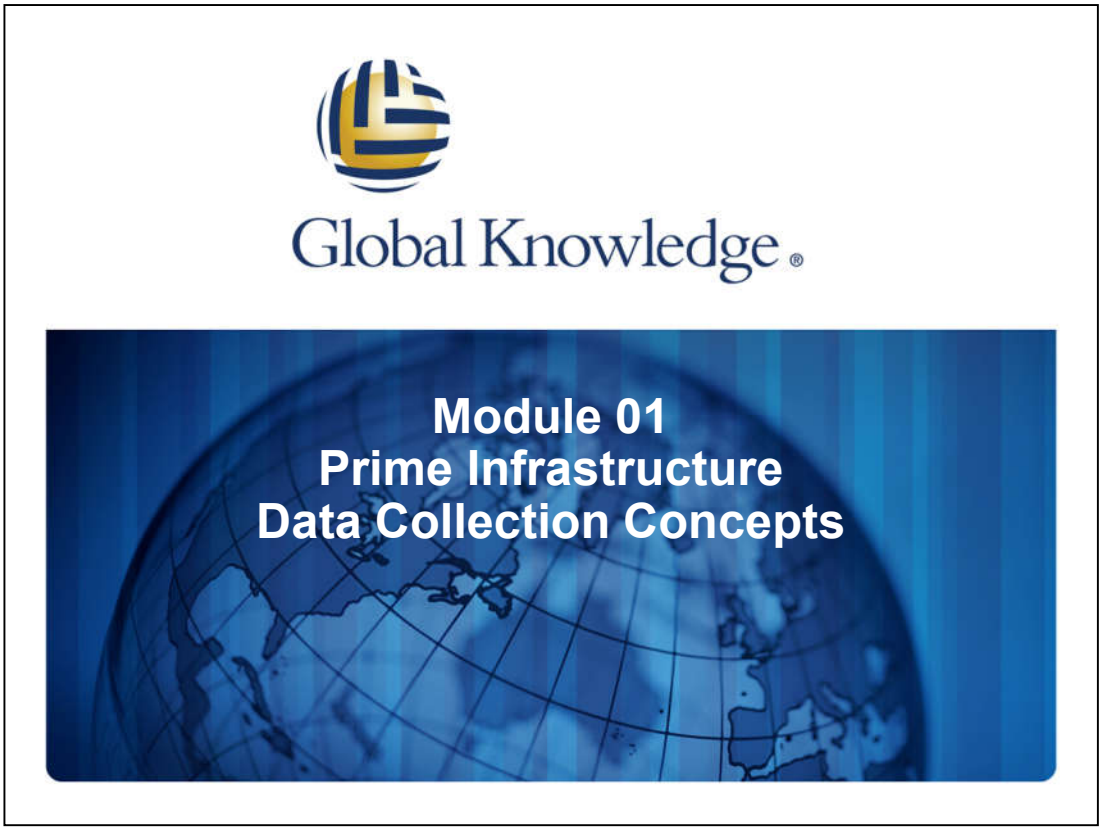
– End user network connection and association

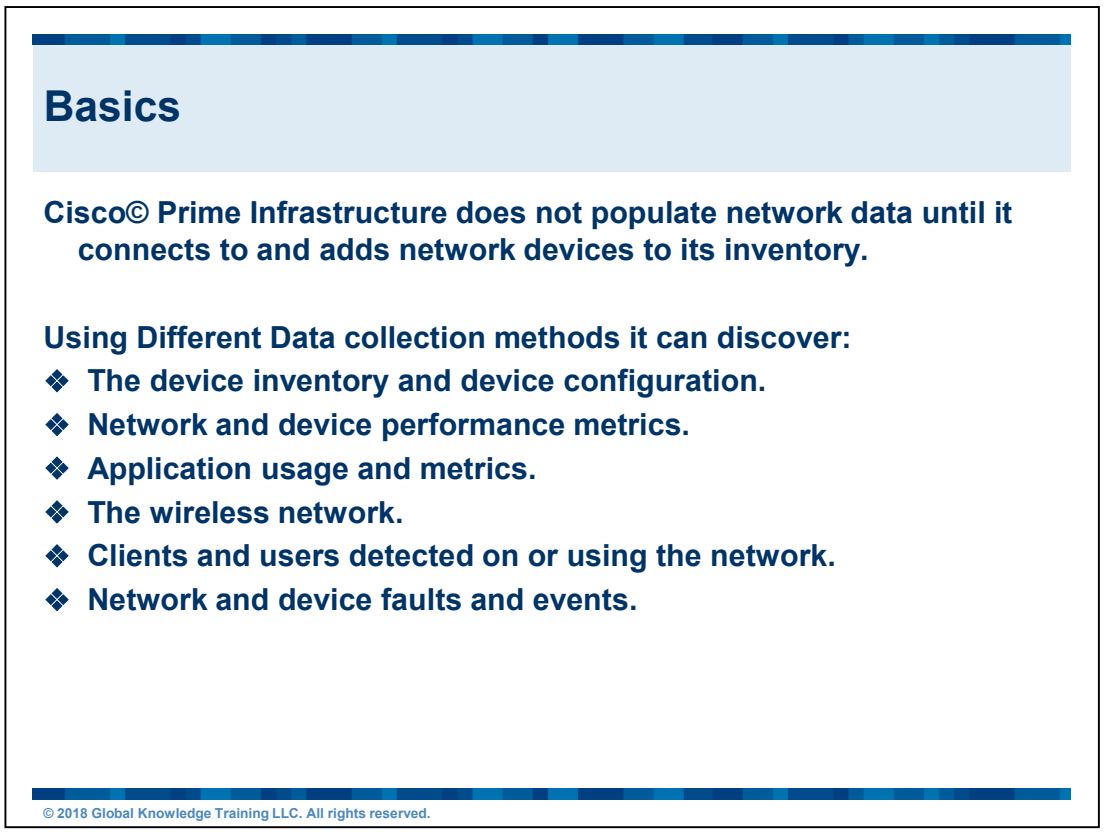
– Authentication and authorization

– Possible problems with the network devices associated with the user's network attachment

– Application-related issues

– Other issues in the broader network


Global Knowledge
Module 01
Prime Infrastructure
Data Collection Concepts



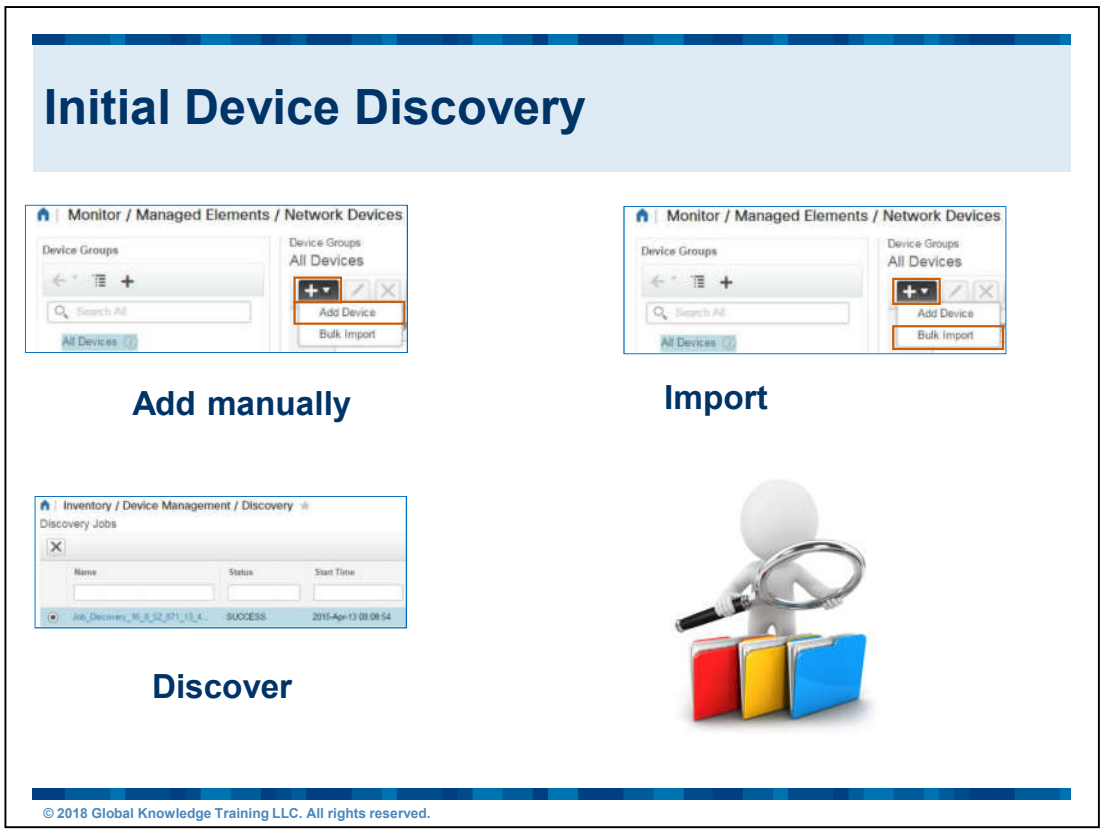
On initial installation, Cisco© Prime Infrastructure does not populate network data until it connects to and adds network devices to its inventory.

The system uses a variety of data collection methods based on data type, licensing, and the data collection functionality that is enabled based on network configuration to report data on:

- The device inventory and device configuration.
- Network and device performance metrics.
- Application usage and metrics.
- The wireless network.
- Clients and users detected on or using the network.
- Network and device faults and events.

This job aid introduces you to Prime Infrastructure data collection processes, which helps you to recognize how the system reports monitoring data, performance metrics, application usage, and faults and events, among other information.

Recognizing these processes also can help configurators and administrators ensure that system users see the data that they need for effective network monitoring and management.



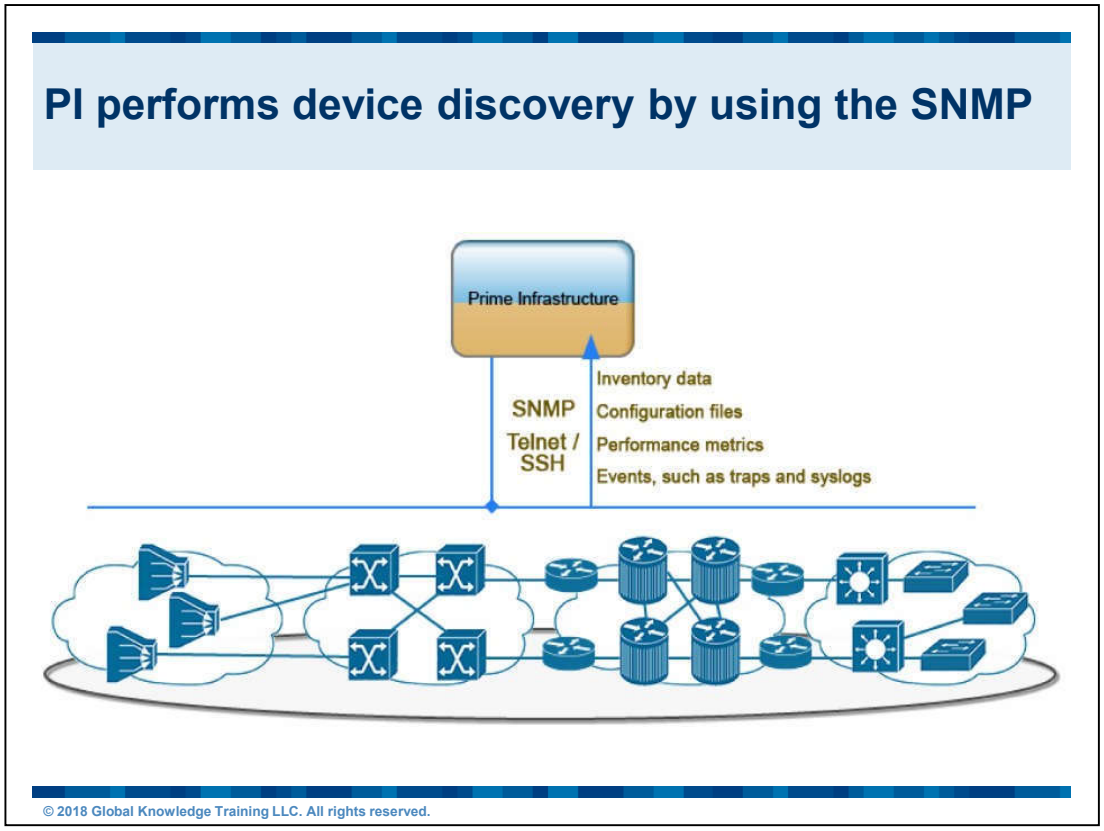
Initial Device Discovery

On initial installation, Prime Infrastructure does not populate network data until it connects to and adds network devices to its inventory. System users can use several methods to perform discovery, including:

- ❖ Running device discovery jobs.
- ❖ Adding devices manually.

- ❖ Importing device information from another system or from a CSV file by using the bulk import feature.

This Photo by Unknown Author is licensed under CC BY-ND



Prime Infrastructure performs device discovery by using the Simple Network Management Protocol (SNMP).

Initial data collection activity occurs after the device discovery process is completed. At that point, Prime infrastructure uses the SNMP and Telnet/SSH protocols to collect:

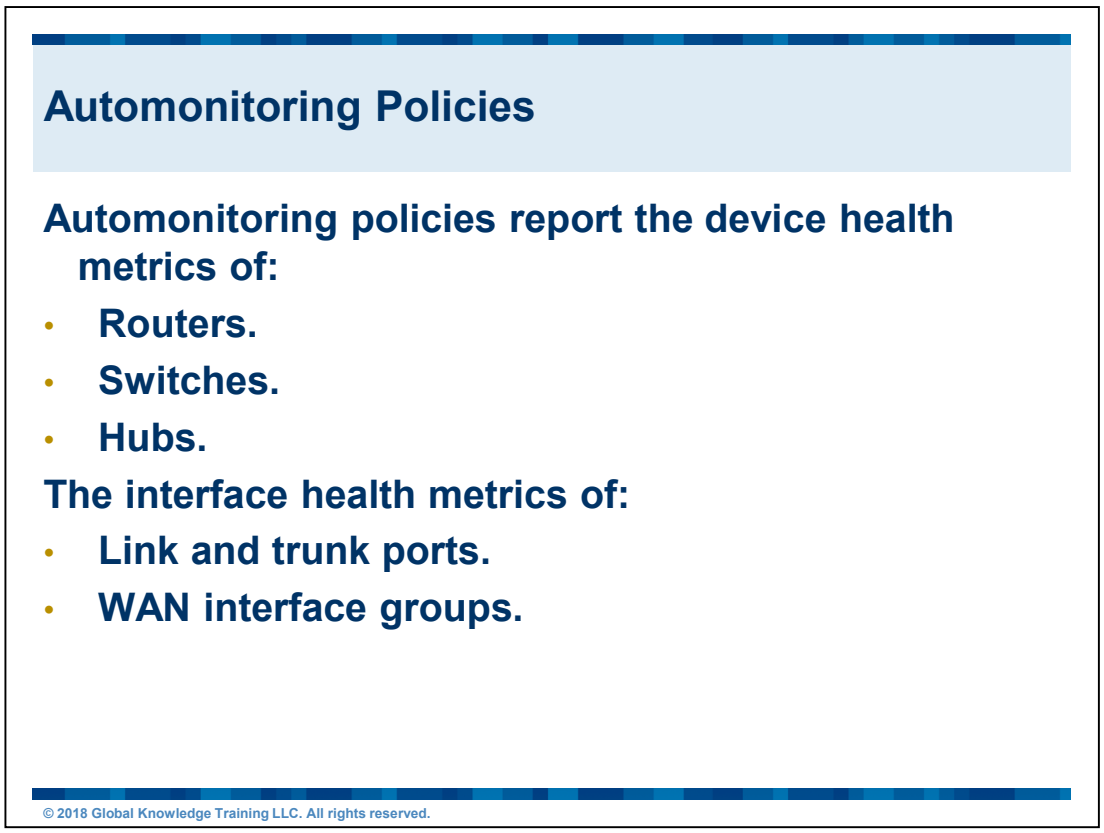
- Inventory data

Including hardware and software components and information on the features and technologies that are active on the device.

- Configuration files

Including the running and startup configurations, and the VLAN database configuration, if applicable.

- Performance metrics.
- Events, such as traps and syslogs.



Automonitoring Policies

After initial inventory data collection, the system begins collecting critical network and system health metrics by using the automated monitoring policies, referred to as automonitoring policies, which come with the system.

These automonitoring policies define the parameters and operational thresholds that the system will follow during data collection. By applying automonitoring policies, Prime Infrastructure does not require configuration to start collecting and reporting key health data.

Automonitoring policies report the device health metrics of:

- Routers.
- Switches.
- Hubs.

The interface health metrics of:

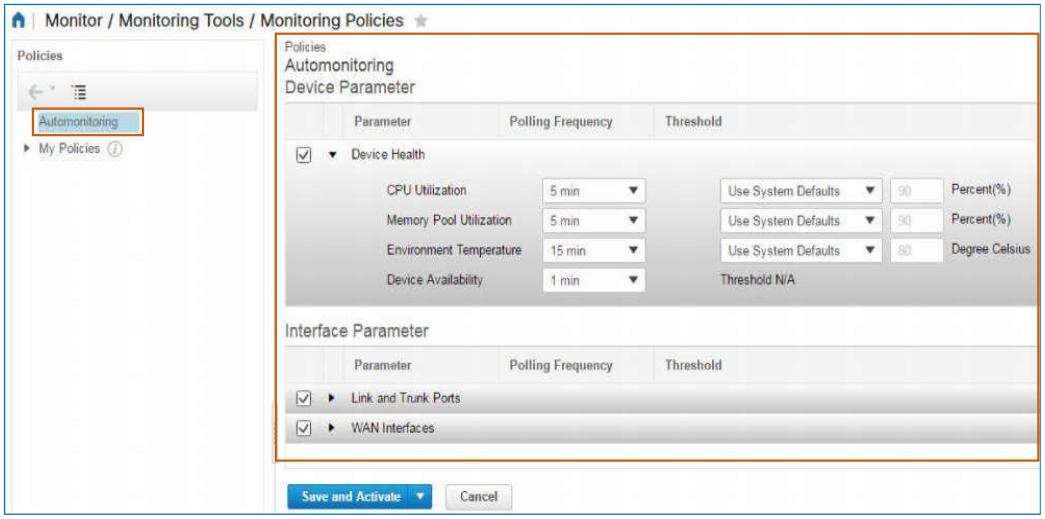
- Link and trunk ports.
- WAN interface groups.

Note: To begin collecting data on wireless LAN controllers, you need to add and activate a custom monitoring policy.

Based on the polling time intervals, or frequencies, defined in the policies, the system begins

reporting the data that it is collecting.

Automonitoring Policies Configuration



System users can change the reporting thresholds and polling frequencies of automonitoring policy parameters to meet business or operational requirements.

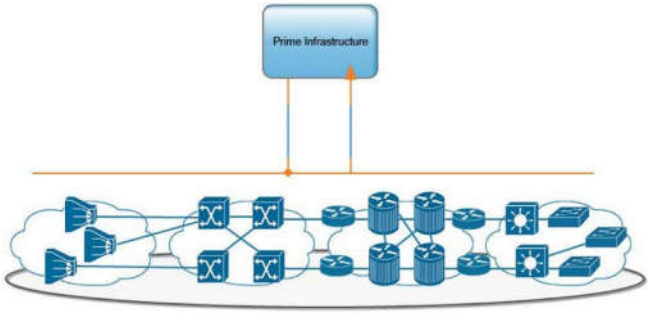
The data that the automonitoring policies collect is available in various areas of the application, including:

- Dashboards.
- Alarms and events.
- Reports.

Ongoing Device Polling

Device polling is the process by which the system continues to collect device data after initial device discovery.

Device polling uses the automated monitoring policies

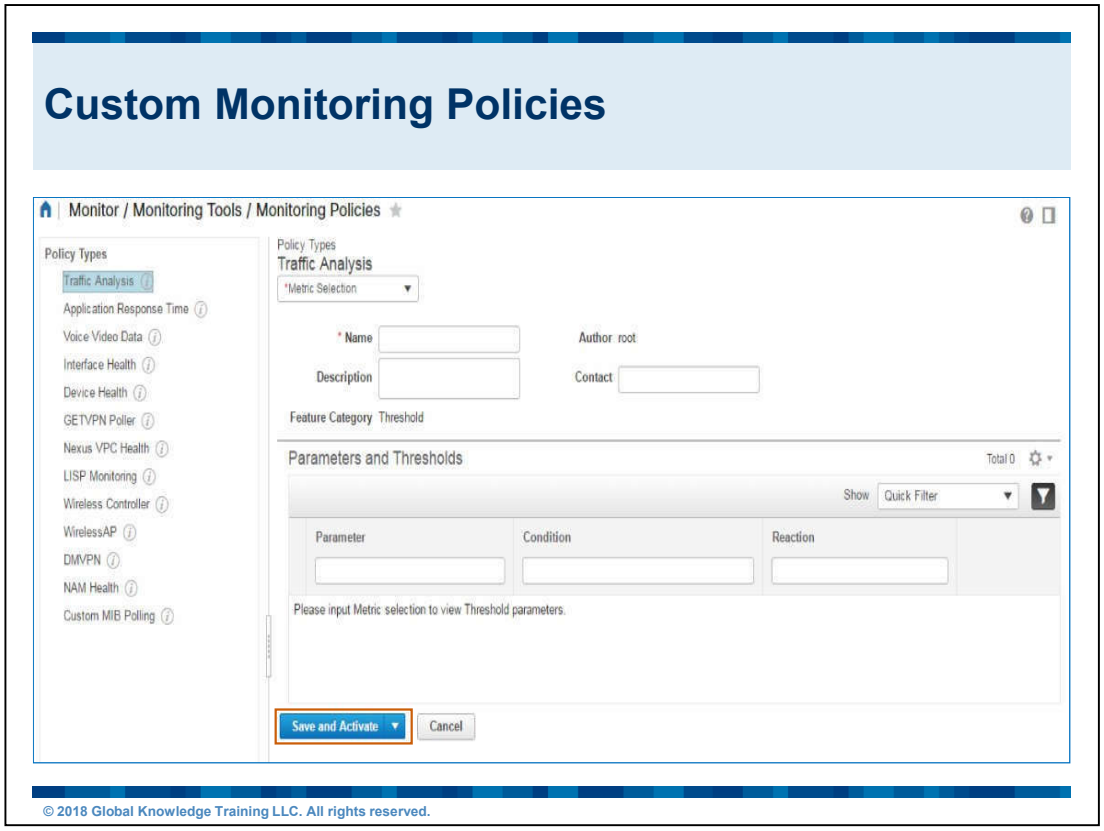


Ongoing Device Polling

Device polling is the process by which the system continues to collect device data after initial device discovery.

Device polling uses the automated monitoring policies that the system activates during the device discovery process for data collection.

Polling also follows the custom monitoring policies that system users must configure to help ensure that Prime Infrastructure is collecting all of the data that is necessary to perform effective network monitoring and management.



Custom Monitoring Policies

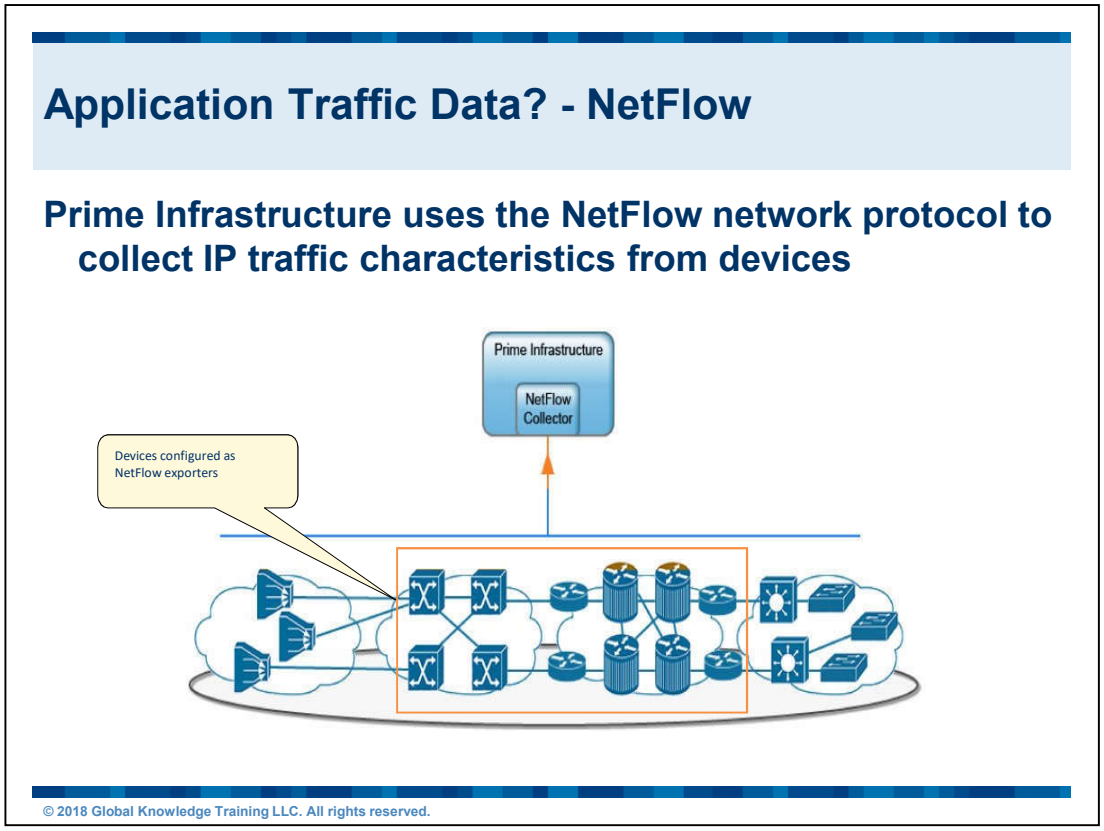
To begin collecting data that meets enterprise requirements, system users need to configure monitoring policies for all of the data categories for which they need information, such as application response time or voice and video data, for example.

Important Note: In addition to the data that automonitoring policies collect, Prime Infrastructure only collects data for custom monitoring polices that a system user has configured and activated.

Note: System users also can save custom monitoring policies and activate them later.

Key monitoring policies that you can configure include:

- Traffic analysis.
- Application response time.
- Voice and video.
- Interface health, in addition to the data that automonitoring policies collect.
- Device health, in addition to the data that automonitoring policies collect.
- Nexus Virtual Port Channel (VPC) health for Nexus, which monitors whether VPCs are configured correctly.
- Wireless LAN controllers.
- Wireless access points.



Application Traffic Data?

The NetFlow Protocol

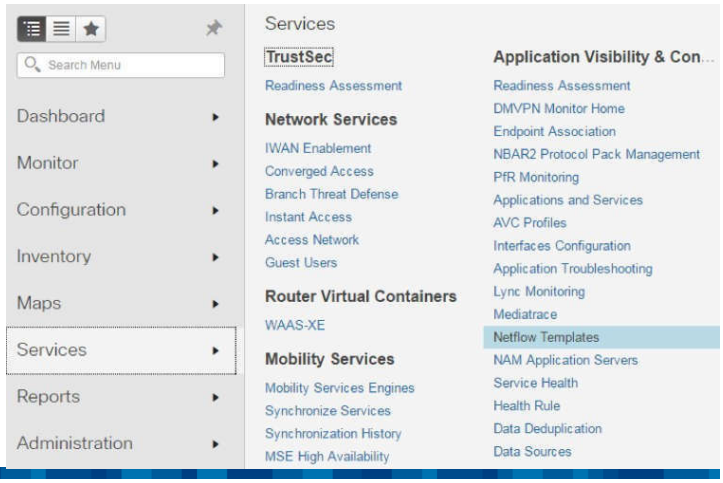
Overview

Prime Infrastructure uses the NetFlow network protocol to collect IP traffic characteristics from devices, which indicate how and where application traffic is traversing the network.

To support NetFlow reporting, devices are configured as NetFlow exporters so that they can send data to Prime Infrastructure. The system then captures the information in its embedded NetFlow collector.

Netflow templates

NetFlow data sources, including devices and interfaces, require NetFlow templates in order for Prime Infrastructure to report application and traffic data successfully.



NetFlow templates define the flow data that the data sources export automatically at defined intervals to Prime Infrastructure's NetFlow collector.

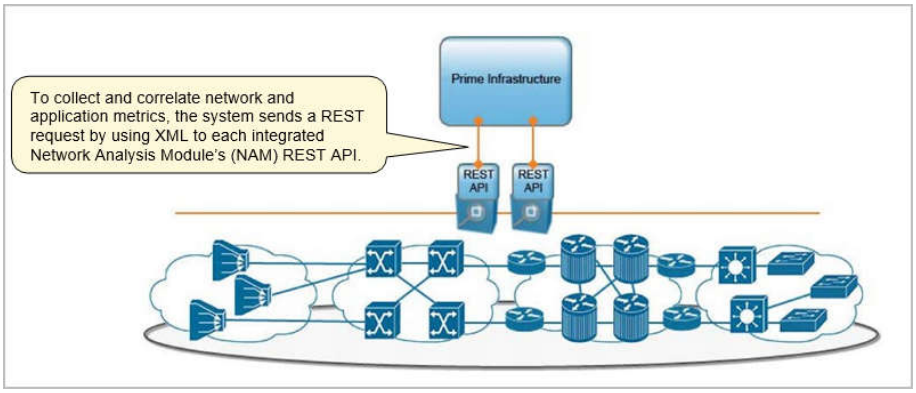
The collector then assembles, combines, and reports the flow data in various dashlets.

Important Note: For successful data reporting in dashlets, data sources must support NetFlow and have NetFlow templates configured for data exporting.

To determine whether a data source supports Netflow, refer to the technical documentation for that specific device.

Application Traffic Data – Integrated Network Analysis Modules (NAMs)

Network Analysis Modules (NAMs) collect detailed traffic movement analysis data,

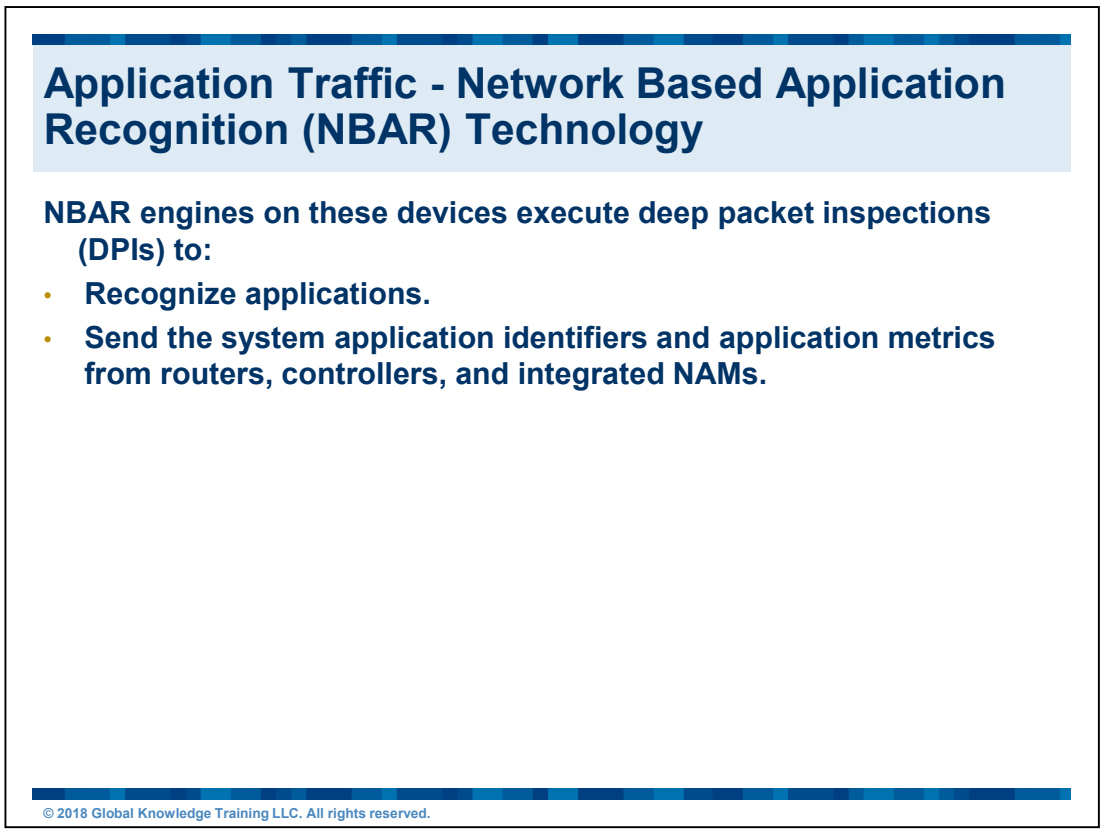


Integrated Network Analysis Modules (NAMs)

Network Analysis Modules (NAMs) collect detailed traffic movement analysis data, including application response time and bandwidth usage metrics, which provides deeper insight into application traffic patterns and changing conditions.

When the network configuration integrates network analysis modules, or NAMs, Prime Infrastructure can collect and correlate network and application metrics calculated by the NAMs.

To collect data, the system sends a REST request by using XML to each NAM's REST API.



Network Based Application Recognition (NBAR) Technology

To recognize applications on which the system is reporting more easily, Prime Infrastructure uses the Network Based Application Recognition (NBAR) technology that is embedded in routers, controllers, and NAMs.

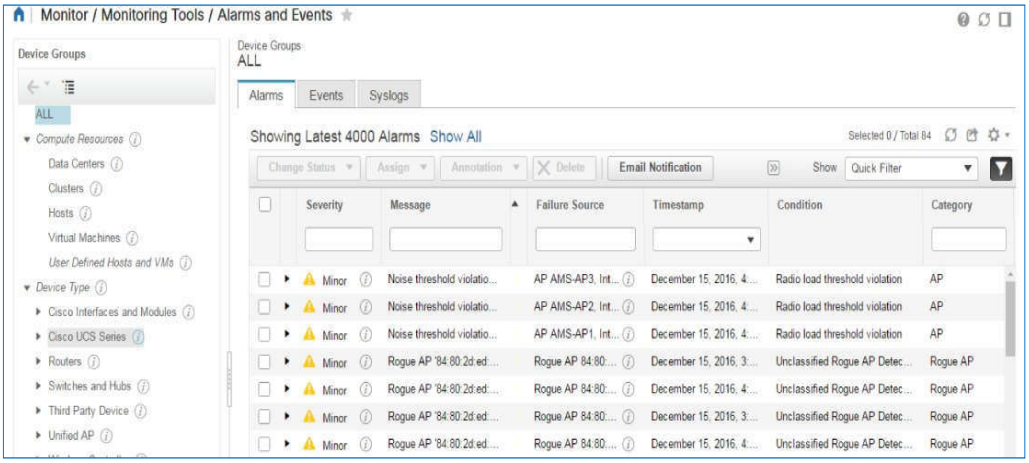
NBAR engines on these devices execute deep packet inspections (DPIs) to:

Recognize applications.

Send the system application identifiers and application metrics from routers, controllers, and integrated NAMs.

Monitoring Policies

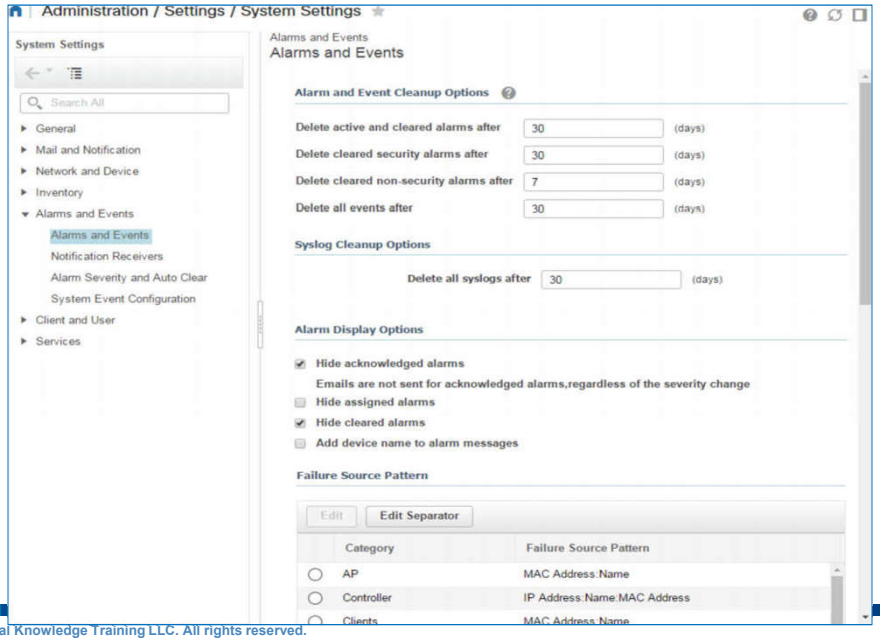
. When conditions fall outside of policy parameters or thresholds, the system can generate and report these conditions as alarms and events.



Monitoring Policies

Automonitoring and custom monitoring policies define the parameters and operational thresholds that the system uses to report data, including faults. When conditions fall outside of policy parameters or thresholds, the system can generate and report these conditions as alarms and events.

Administrative Settings Overview

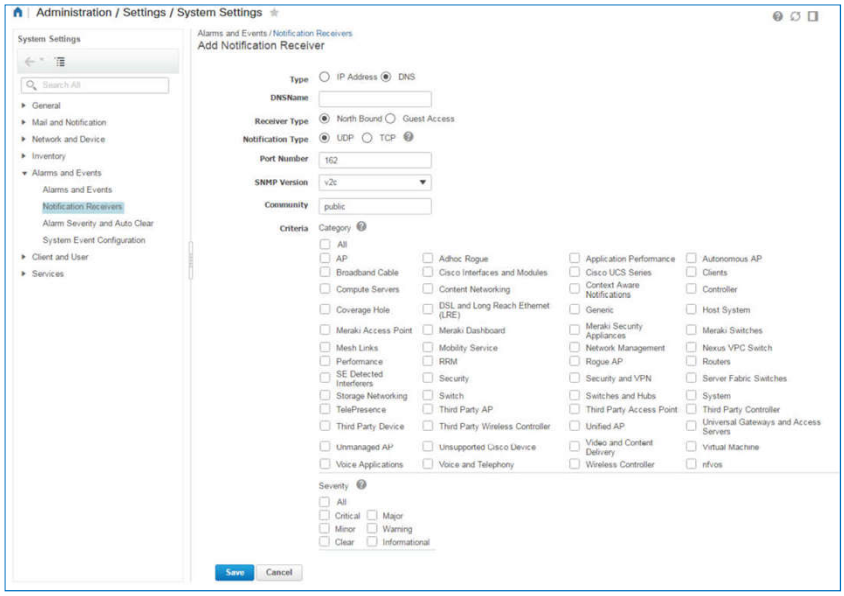


Overview

In Administration, you can configure the system settings that control the management and reporting behaviors of alarms. You also can configure the behaviors of the events and syslogs that form the basis for generating alarms, which provide detailed information.

Configuring these global settings is important for ensuring that the system is escalating issues and managing fault reporting based on operational and business requirements.

Administrative Settings
Collecting Fault Data in Northbound Systems



Collecting Fault Data in Northbound Systems

You can configure notification receivers so that northbound systems can receive data from Prime Infrastructure, including:

Receiving alarms.

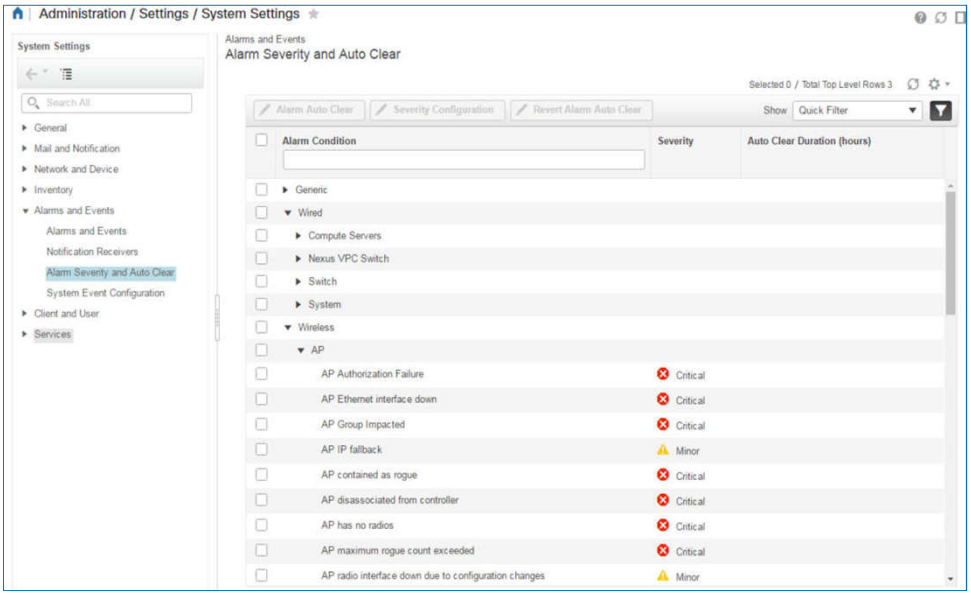
Receiving events that are related to guest access activity, such as guest user accounts that are added, authenticated, or expired.

Forwarding these alarms or events help ensure that you are gathering the data that you need in the systems that you rely on for operational reporting and management activities.

In addition to configuring the forwarding details, you can configure one or more categories of events that you want to forward to the receiving system.

You also can configure the specific severity level or levels of the events that the system is forwarding.

Administrative Settings
Defining Alarm Severities and Behaviors



Defining Alarm Severities and Behaviors

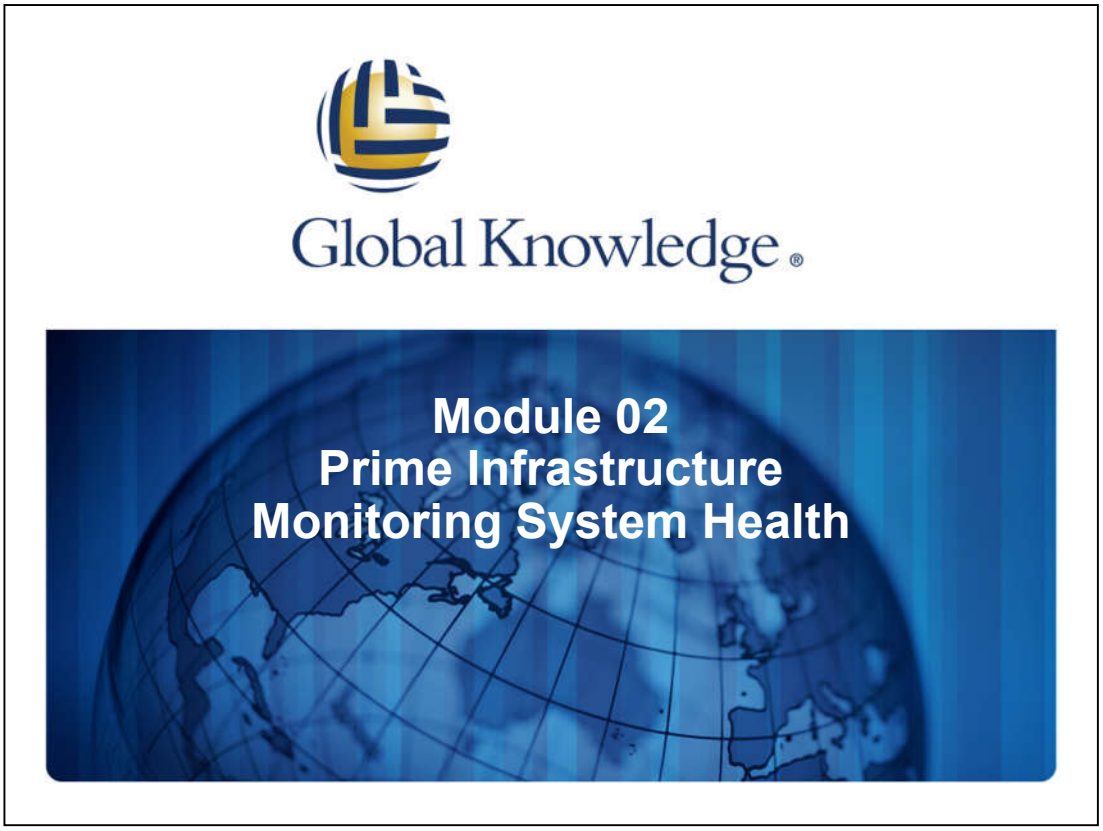
The system applies a default severity level to all of the alarms.

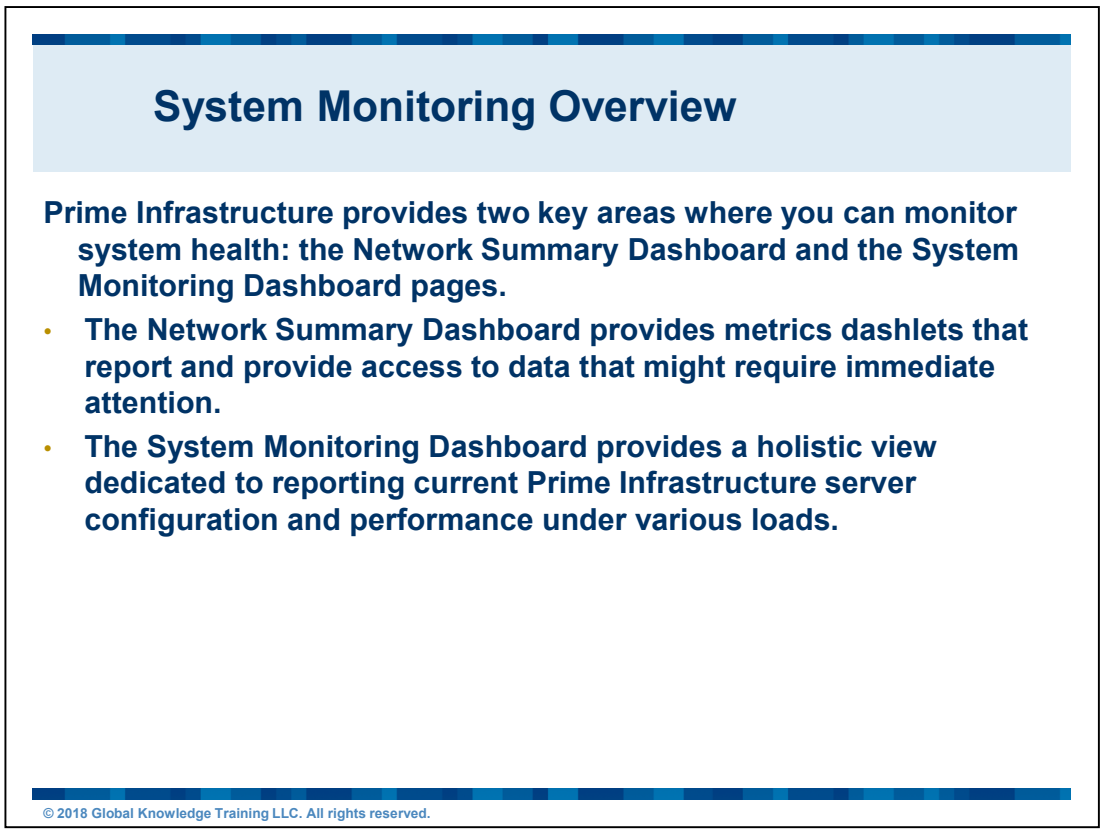
On the **Alarm Severity and Auto Clear** page, you can define the severity levels that the system applies to the alarms that it reports, and the time period that passes before the system automatically clears alarms.

When you change severity levels, you can return the alarm to its system default severity level.

You also can define the time period, in hourly increments, that passes before the system automatically applies a cleared status to an alarm, which overrides the global system default settings.

Note: When you change alarm settings, those changes apply to new alarms that the system generates and do not affect current or cleared alarms.


Global Knowledge
Module 02
Prime Infrastructure
Monitoring System Health



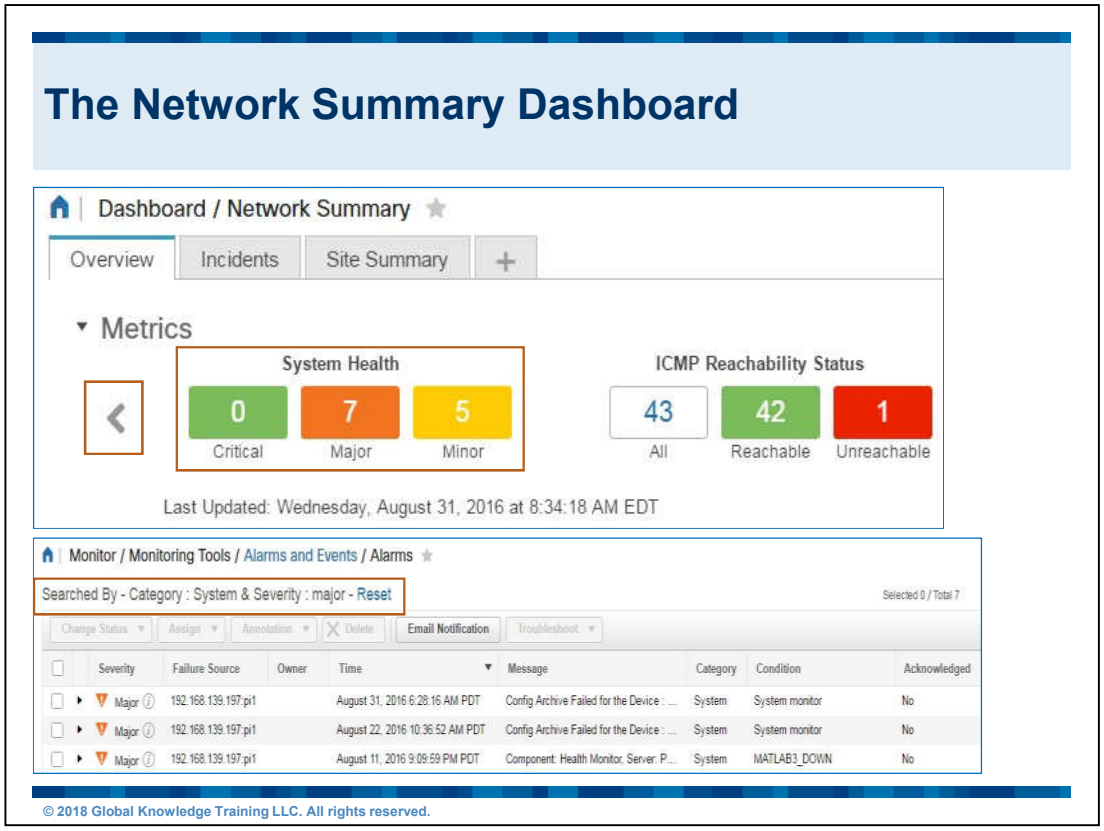
Prime Infrastructure provides two key areas where you can monitor system health: the Network Summary Dashboard and the System Monitoring Dashboard pages.

❖ The Network Summary Dashboard provides metrics dashlets that report and provide access to data that might require immediate attention.

❖ The System Monitoring Dashboard provides a holistic view dedicated to reporting current Prime Infrastructure server configuration and performance under various loads.

Tip: Correlating the data that is available on these dashboards provides a holistic view of system health and can help you to identify and act on potential issues most effectively.

For guidance on where to find data for specific factors that can affect server performance, refer to the Correlating Data thought map.



System Summary Dashlets

On the Network Summary dashboards, you can add and monitor the metrics dashlets, which report summarized system information.

Summary information provides an immediate view of two key system health indicators, system events and device manageability.

The system displays both metrics dashlets by default. You can add the dashlets to custom tabs or remove them.

To see the dashlets:

- ❖ In the Metrics section, scroll left or right to see the dashlet that you want.

Reviewing Summary System Health Metrics

Summary system health information provides an immediate indicator of active system events and their severity levels. That way, you can investigate the root cause of the alarm, and monitor it to help mitigate or avoid potentially emergent problems quickly.

Note: When the system is not reporting current alarms for a severity level, the indicator color-code is green.

When the system is reporting current alarms of a specific severity, the indicator for that severity changes to the applicable severity color code.

For example, the Critical indicator turns red when the system is reporting one or more critical alarms.

Refer to the System Health metrics dashlet to:

- ❖ See the number of critical, major, and minor events that the system is reporting on itself.
- ❖ Open a list of the events by clicking the number link of the category of interest.

Reviewing Device Manageability Status Metrics

Device manageability summary information provides an immediate indicator of the number of devices that the system is or is not managing.

Unmanaged devices might require more attention to determine and resolve the problem that is causing the system's inability to manage them.

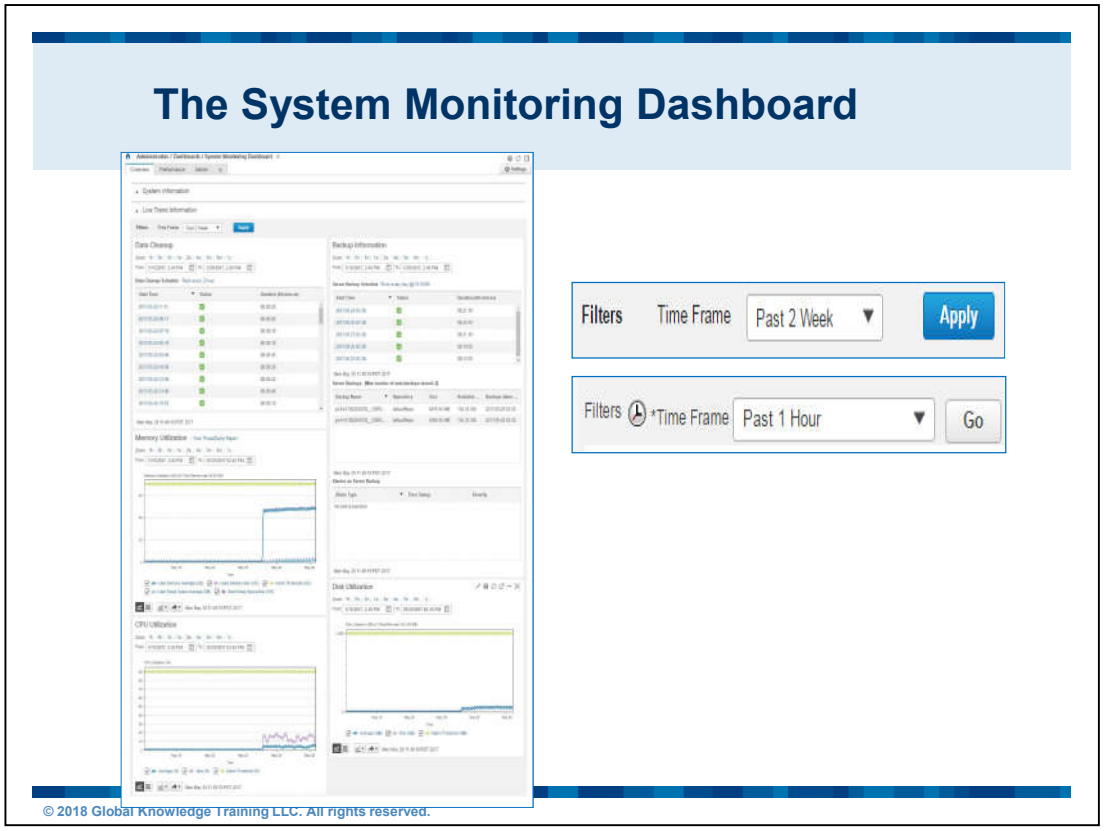
Note: On this dashlet, the indicator color-coded in green reports the number of devices that the system is managing successfully.

The indicator color-coded in red reports the number of devices that the system can communicate with but is not managing successfully. An unmanaged device can indicate that there is a problem, such as a communication issue, that needs to be resolved so that the system can manage the device.

The white All category indicates the total number of network devices that are in the system inventory.

Refer to the Device Manageability Status metrics dashlet to:

- ❖ See the total number of devices in the inventory and the number of those devices in the inventory that the system is or is not managing.
- ❖ Open a list of the devices by clicking the number link of the group of interest.



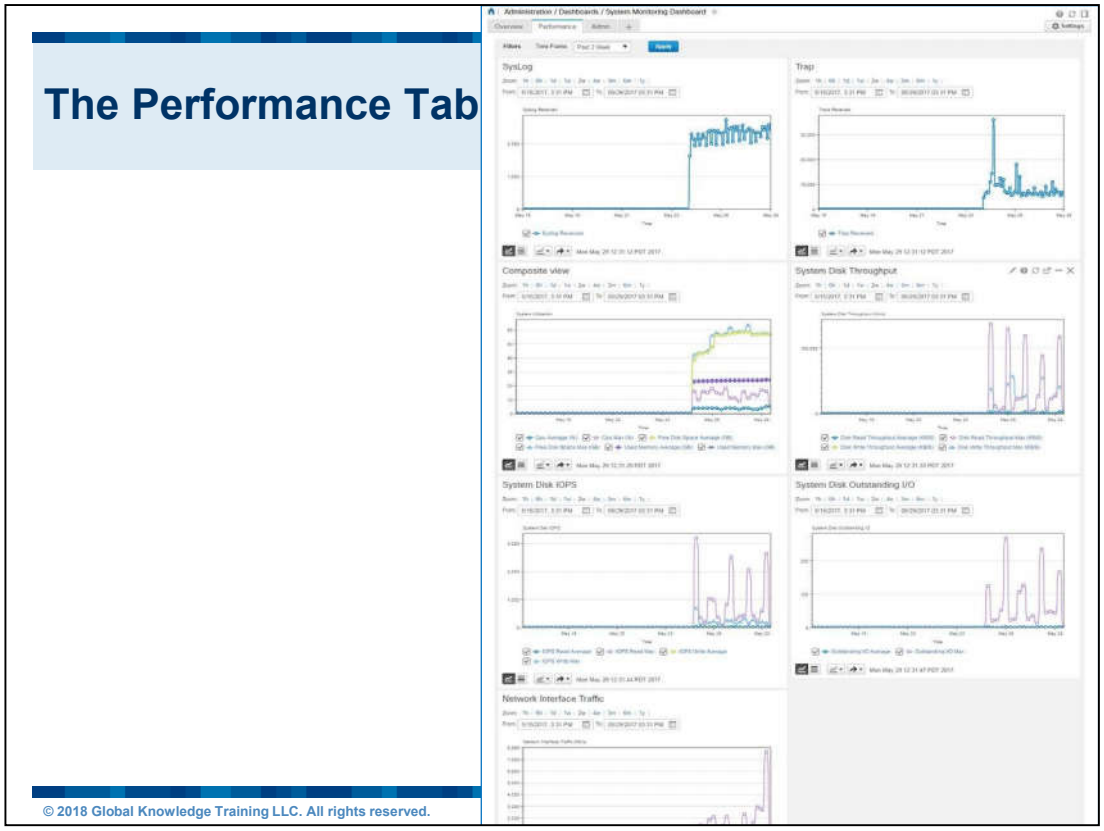
Dashboard Overview

The System Monitoring Dashboard page in Administration provides a holistic view of how the Prime Infrastructure server is performing under various server loads. These loads can originate from the application, such as running data cleanup or backup jobs, or from network activity.

The dashboard provides the Overview, Performance, and Admin tabs by default.

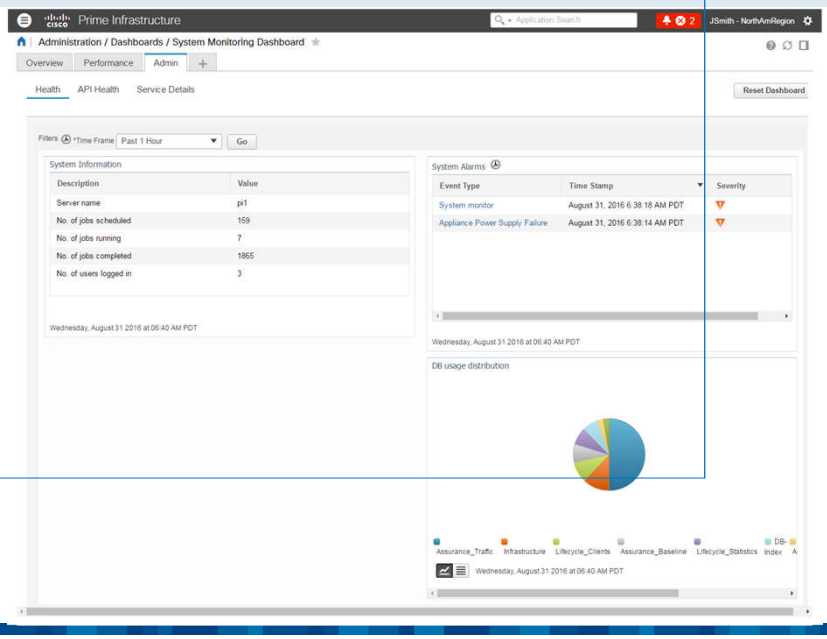
Note: While each tab provides certain data and statistics by default, you can add custom tabs and include the Overview and Performance dashlets that you want. You also can add dashlets to existing tabs.

For more information on organizing dashboards and dashlets



Provides system performance data, including composite and detailed views of system operational statistics

The Admin Tab

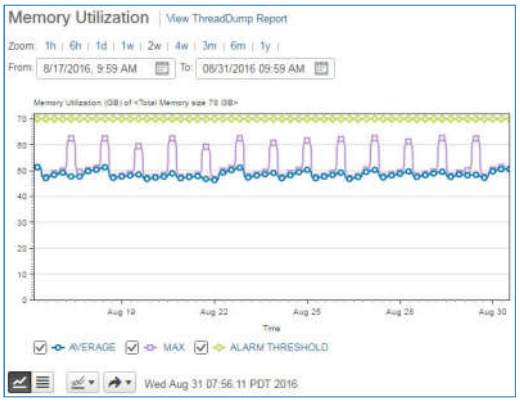


Provides health information on a series of subtabs, including events that are occurring on the system, and API health and API service statistics

Dashlet Basics

What are Dashlets?

Dashlets are data elements that present operational and statistical information on dashboard tabs.



Dashlet Basics

What are Dashlets?

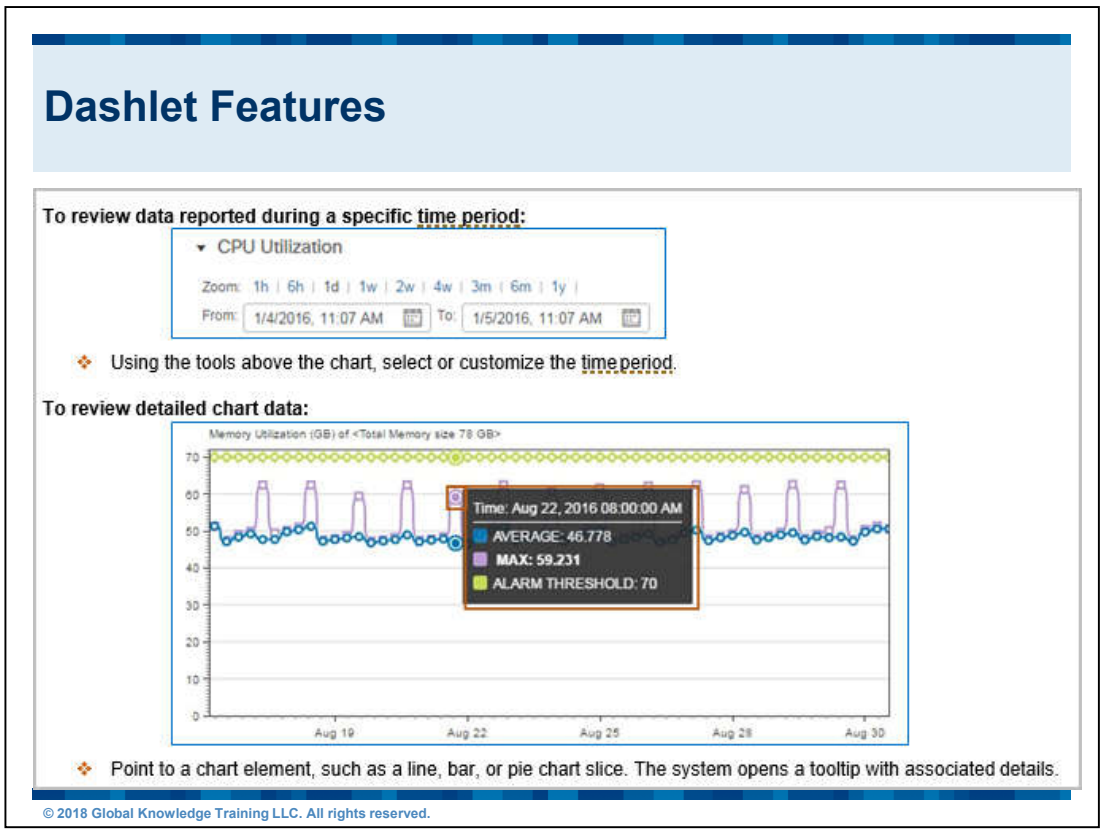
Dashlets are data elements that present operational and statistical information on dashboard tabs.

Following are examples of dashlets.

For system monitoring, Prime Infrastructure provides Overview, Performance, or Admin dashlets based on the active dashboard tab. While the dashboard tabs include specific dashlets by default, you can add dashlets to or remove them from existing tabs.

You also can add custom dashboards and include the Overview or Performance dashlets that you want. This way, you can organize information in a way that is most effective for you.

When dashlets present graphical data in charts, you can open granular levels of detail, which can be helpful when investigating issues.

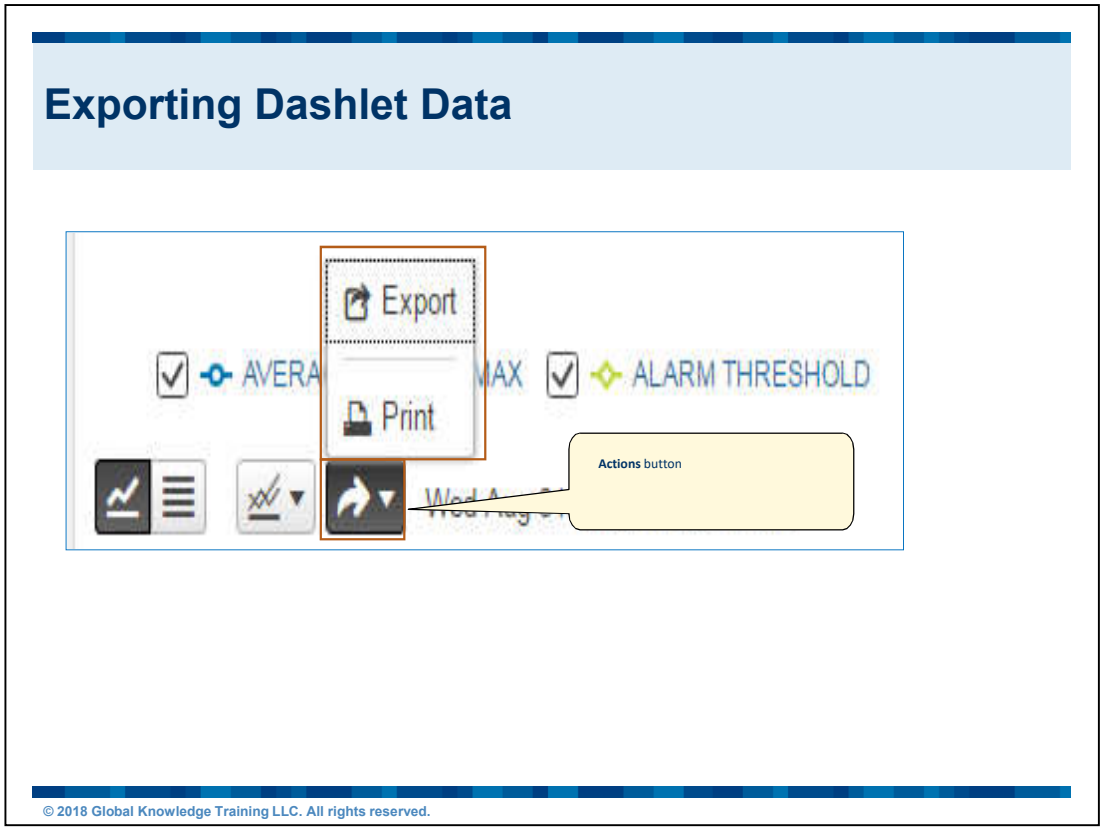


To review data reported during a specific time period:

❖ Using the tools above the chart, select or customize the time period.

To review detailed chart data:

❖ Point to a chart element, such as a line, bar, or pie chart slice. The system opens a tooltip with associated details.



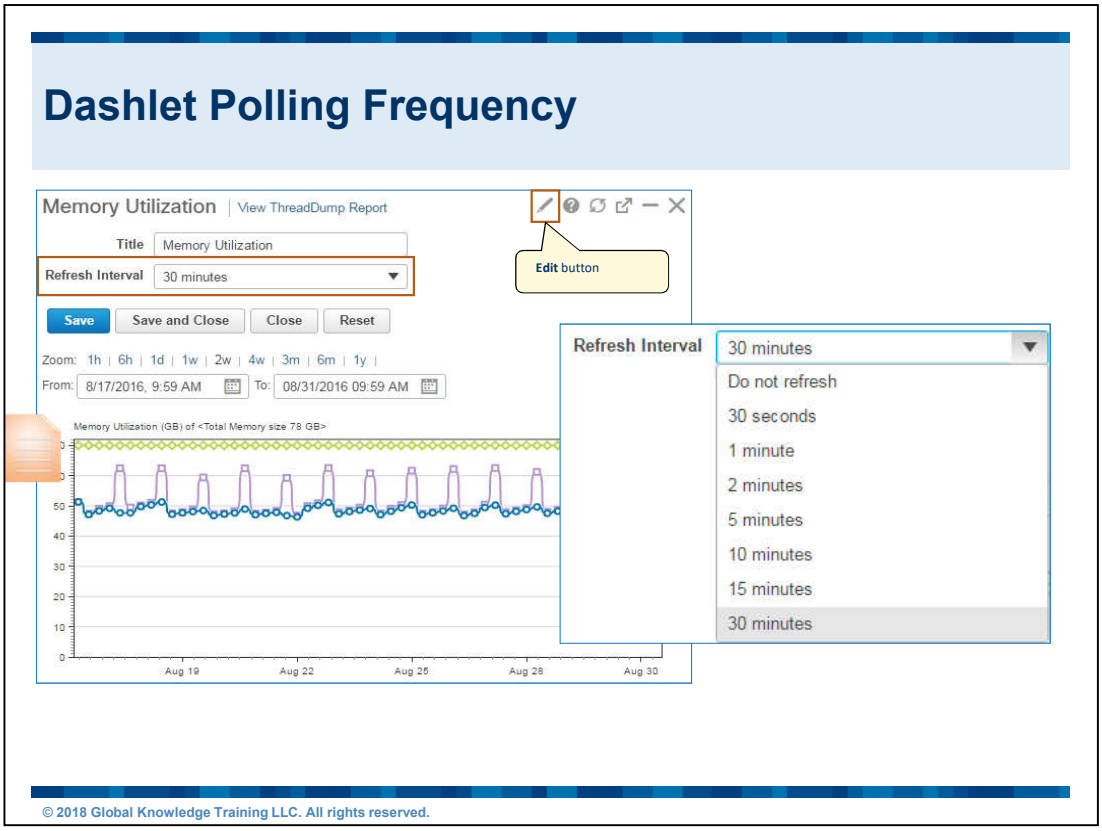
Exporting Dashlet Data

For dashlets that support it, you can export or print the data that they are displaying.

Exporting or printing data captures historical or ongoing information and can be particularly helpful when requesting support from Cisco.

To export or print dashlet data, in the dashlet:

- Click Actions, and then select the Export or Print.



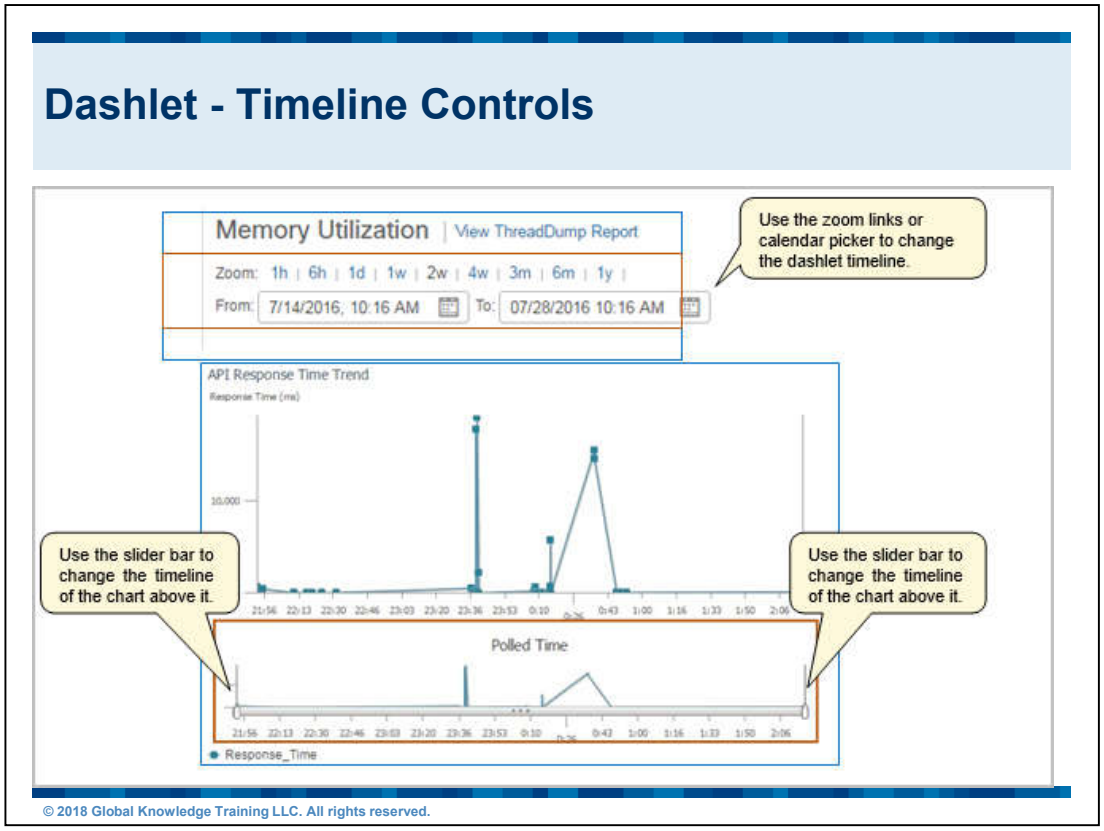
Dashlet Reporting Concepts

Polling Frequency and Timeline Controls

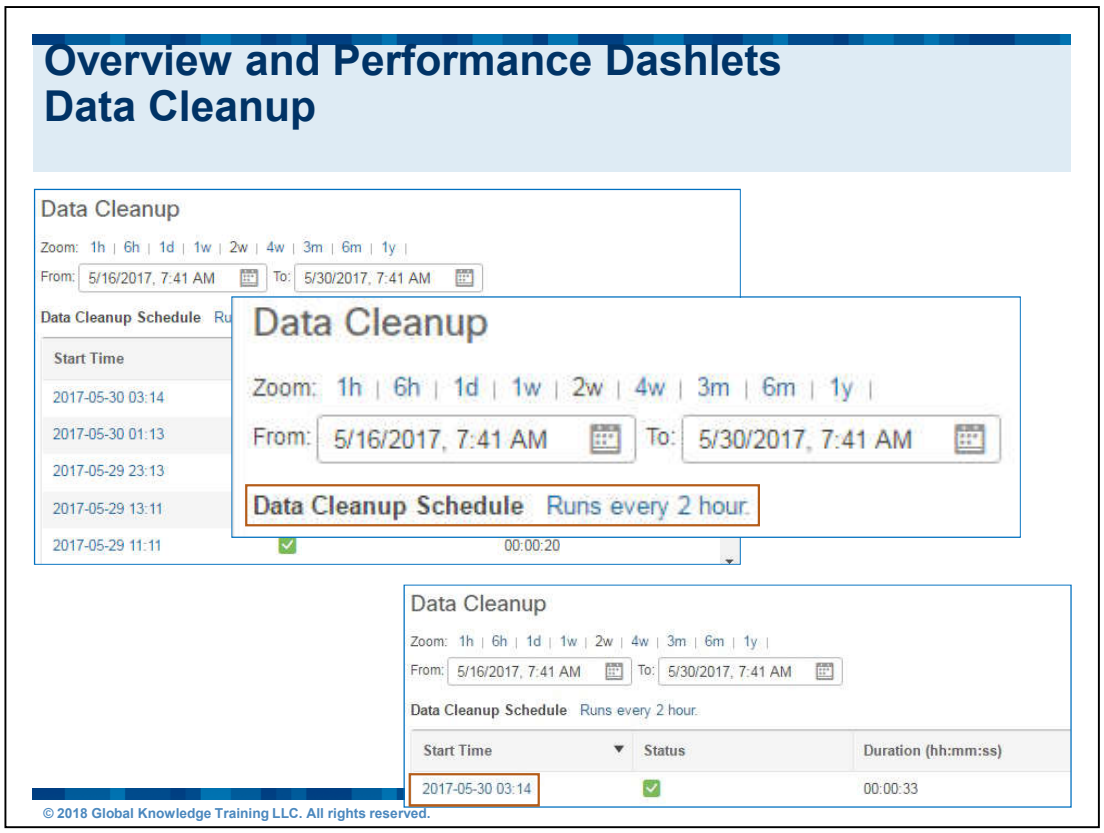
Component polling frequencies, dashlet refresh rates, and dashlet time settings work in combination, which affects how current the dashlet data is.

Important Note: While administrators can change polling frequencies for various components, use caution when changing default settings, which follow best practices.

Increasing polling frequency causes additional server workload, which can affect server performance.



Time period settings are another factor that affects the data that you are seeing. There is a time frame setting at a page level, and for dashlets that offer them, zoom links and a calendar picker or timeline sliders that control the time interval.



In order to reclaim disk space, the system runs jobs that compact the Prime Infrastructure application database, referred to as Data Cleanup jobs.

Data cleanup jobs remove information that system parameters indicate is aged beyond retention periods or as less significant, including:

- Temporary report files and their caches.
- Temporary backup archive directories.
- Aged or orphaned audit reports.
- The in-memory cache.
- Events that have aged beyond the retention period.
- Database tables entries that have aged beyond the retention period.

You can change how often the system runs these jobs.

Refer to the Data Cleanup dashlet to:

- See or change the database clean up job schedule.
- See the last five jobs that have occurred and their statuses.

The system sets the default clean up job schedule to run every two hours. You can change the time

period, as needed, to address specific circumstances.

Important Note: Cisco recommends that you retain the default time period setting, which follows Cisco best practices.

Use caution when changing the time period, particularly if you are reducing the time interval, which causes additional system load and can potentially affect system performance.

To change the time interval that the system performs a cleanup job:

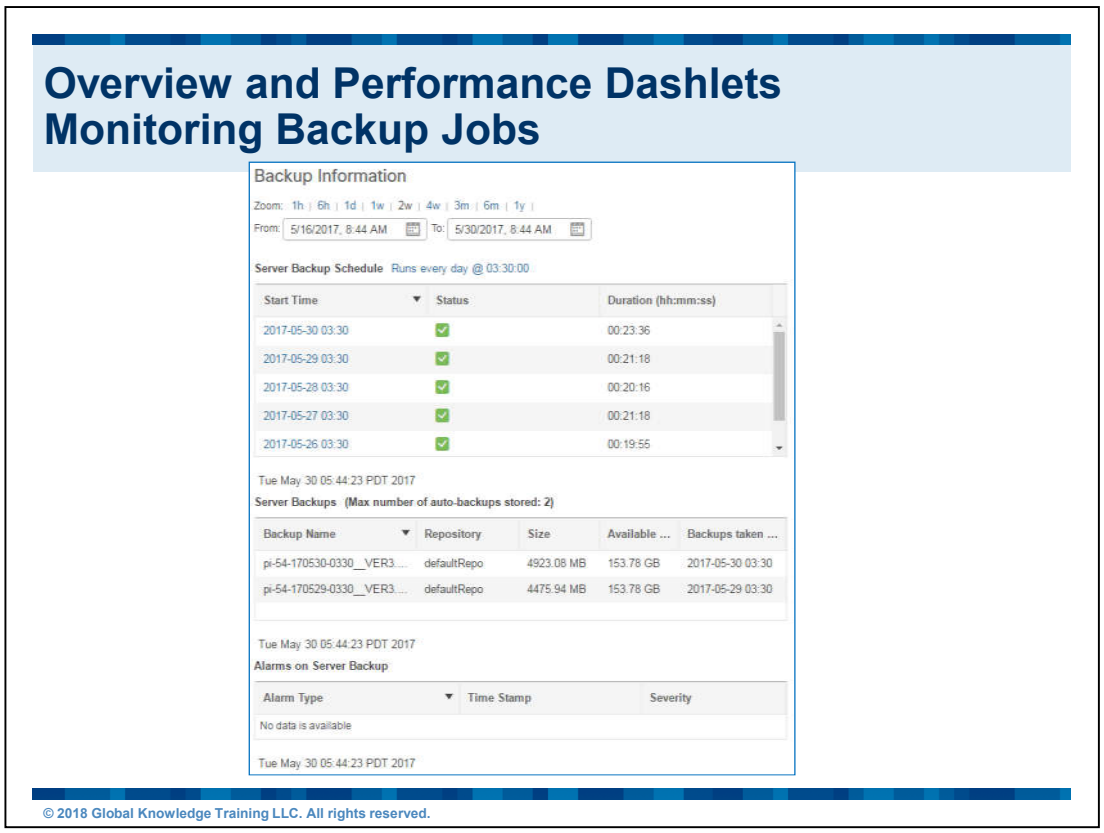
❖ Click the Data Cleanup schedule link that indicates the current time interval, and then configure the time period.

To review job details:

❖ For the job of interest, click the Start Time link.

The system navigates to the Data Cleanup page on the Job Dashboard in Administration, which lists the 5 most recently completed data cleanup jobs and provides a link to see all of the cleanup jobs that have run.

Note: An administrator can define the time period that the system retains jobs in system settings.



Monitoring Backup Jobs

Server backups are critical to ongoing operations and support more efficient system recovery in case of a failure.

Refer to the Backup Information dashlet to:

- ❖ See or change the backup job schedule.
- ❖ See the last five jobs that have occurred and their statuses.
- ❖ See a list of the backups that are available in the repository for restore or recovery processes.

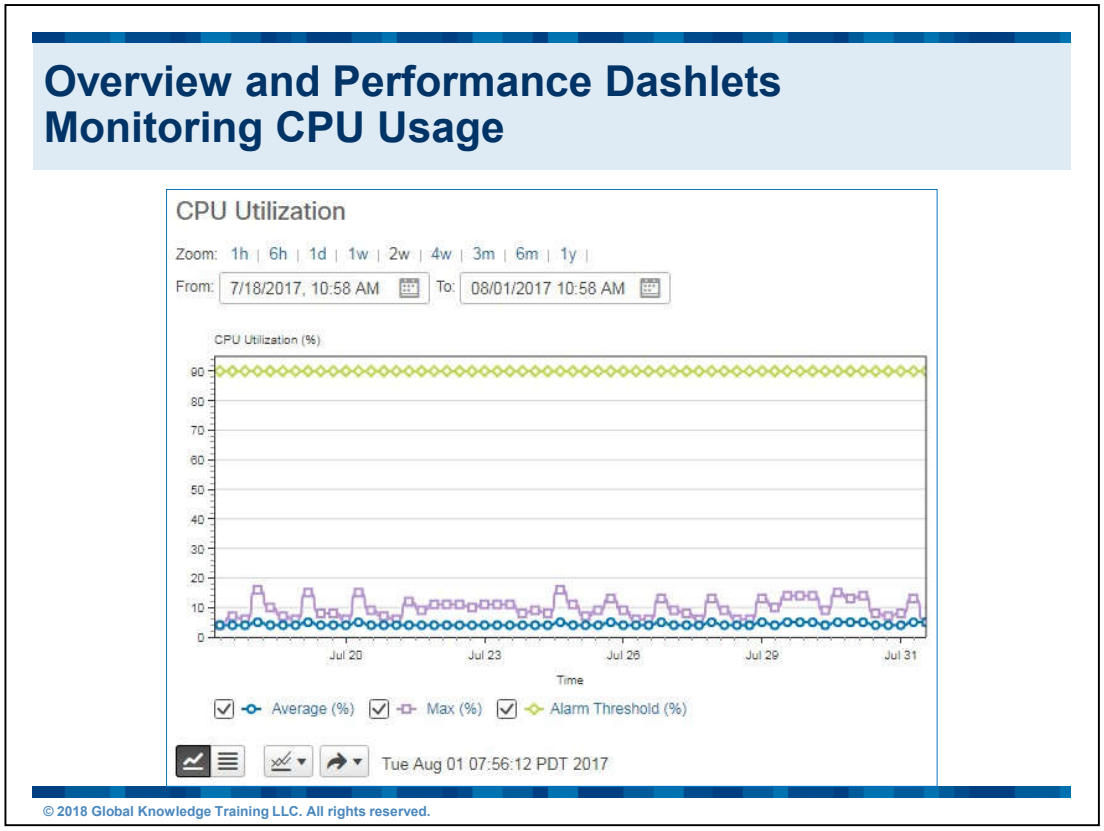
Note: The dashlet only lists available backup files when they are stored in the Prime Infrastructure server repository. When they are stored on another server, the system cannot report on available backup files.

- ❖ See backup-related alarms that the system is reporting.

Tip: While you can monitor all of the system alarms that are occurring on the Alarms dashlet on the Admin tab, the Backup Information dashlet provides a list of alarms specifically generated during server backup jobs.

Important Note: Cisco recommends that you take immediate action on backup job alarms, which can mitigate or avoid data loss.

For more information on managing backup processes, refer to the Prime Infrastructure Administrator Guide.



Monitoring CPU Usage

CPU usage indicates the amount of computing power that processes and jobs running in the system are consuming.

Refer to the CPU Utilization dashlet to see:

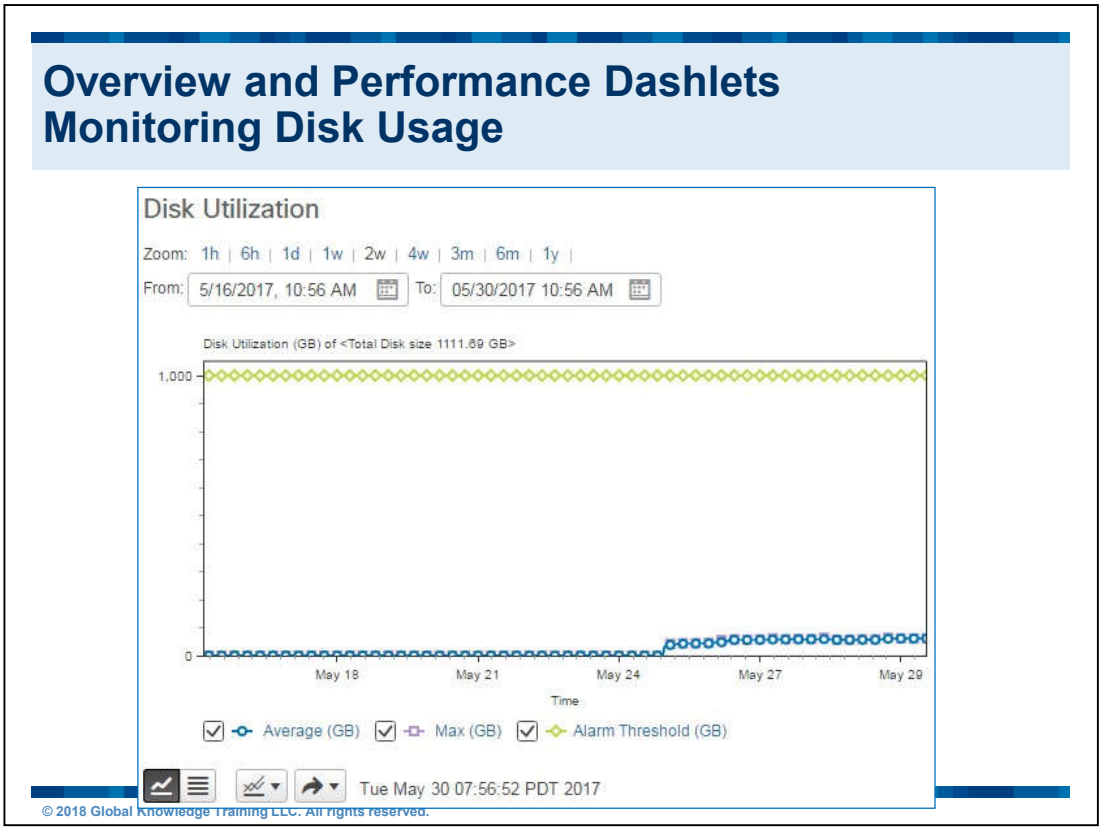
- Average and maximum CPU usage over time, which should remain in a relatively consistent, steady state.
- The relationship of average and maximum statistics to the usage alarm threshold.

Continue monitoring or take action when:

- CPU usage statistics are consistently trending closely or peaking above the alarm threshold.

This situation indicates that one or more processes are consuming a majority of computing power, which can reduce the ability of other processes to run efficiently.

For example, the amount of CPU usage can peak based on the type of activity that is occurring, such as a flood of alarms or jobs that are running frequently.



Monitoring Disk Usage

Refer to the Disk Utilization dashlet to see:

- Related usage statistics during the selected time period.

Continue monitoring or take further action when:

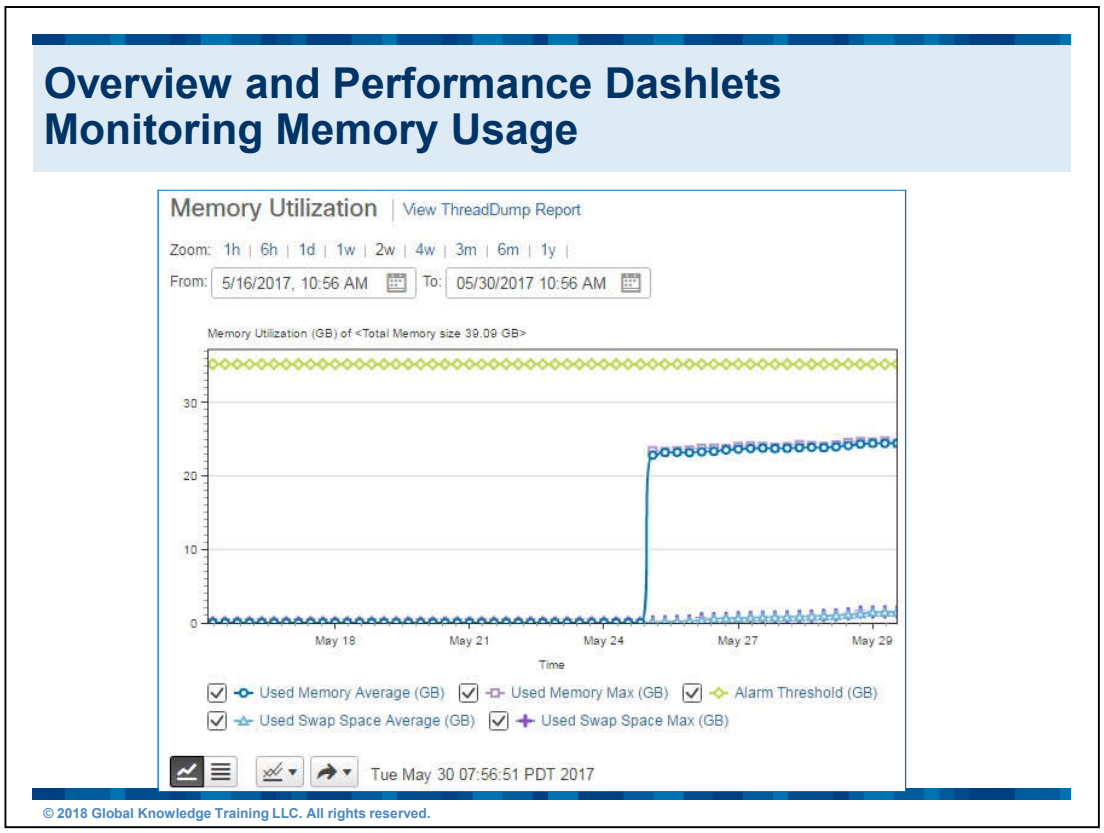
- The Disk Utilization dashlet begins to indicate excessive disk usage or alarms.

To review the volumes and the space they are occupying on the disk, refer to the Disk Statistics dashlet, which can help you determine which volumes might be increasing or are too large.

To see if a backup job failed, which can cause excessive storage, refer to the Backup Information dashlet.

To see if other jobs, including background processes or reports, are failing, which can cause excessive storage, refer to the Jobs Dashboard page.

To review the API call retention periods, which can affect the amount of disk space that the system requires to store call data, refer to the FAQ.



Monitoring Memory Usage

By design, Prime Infrastructure allows the database to consume as much memory as it requires.

Refer to the Memory Utilization dashlet to see:

- ❖ Average and maximum memory usage over time.
- ❖ The relationship of average and maximum statistics to the usage alarm threshold.
- ❖ Average and maximum swap space usage over time.

Continue monitoring or take action when:

- ❖ Memory usage statistics are consistently trending closely or peaking above the alarm threshold.
- ❖ This situation might indicate that threads might not be responding to processing requests.

To evaluate the issue, you can generate a Memory Threshold Breach Report

following the instructions below.

Important Note: If you plan to submit a TAC case to evaluate a memory usage problem, generate a Memory Threshold Breach Report that includes the time period in which the problem occurred.

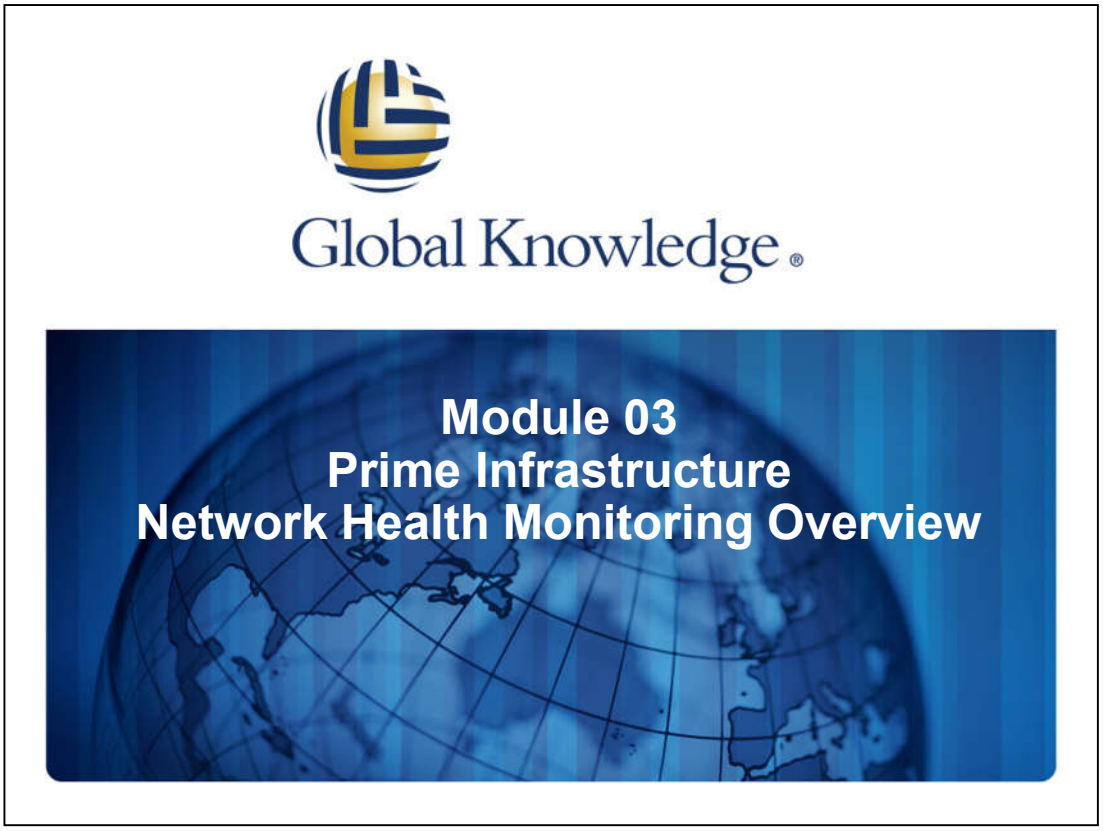
The report lists the details for the thread activity occurring in the time period that you select, which can provide insight into threads that might be causing issues.

- ❖ When running the system in a VM environment, this situation might indicate that a configurator

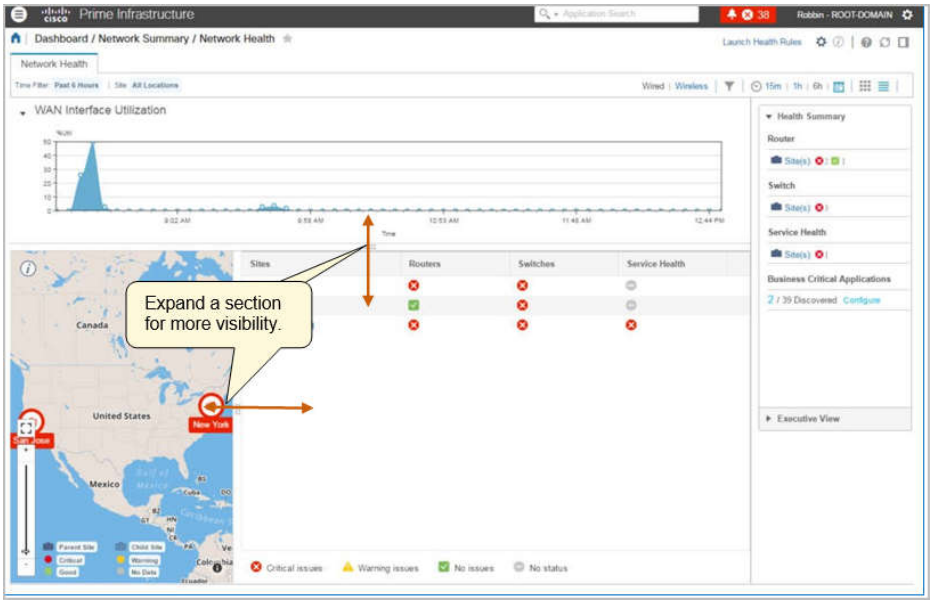
did not set the VM disk allocation to Thick Provision Lazy Zeroed.

It is important to allocate memory for the system and not allow other processes to share it. On initial installation, a configurator should set the VM to apply the Thick Provision Lazy Zeroed disk allocation, which allocates the memory space.

If this setting is not configured correctly, the VM provides memory in 2 gigabyte increments, forcing the system to make ongoing requests for disk space during operations, which can significantly affect performance


Global Knowledge
Module 03
Prime Infrastructure
Network Health Monitoring Overview

Monitoring Network Health



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

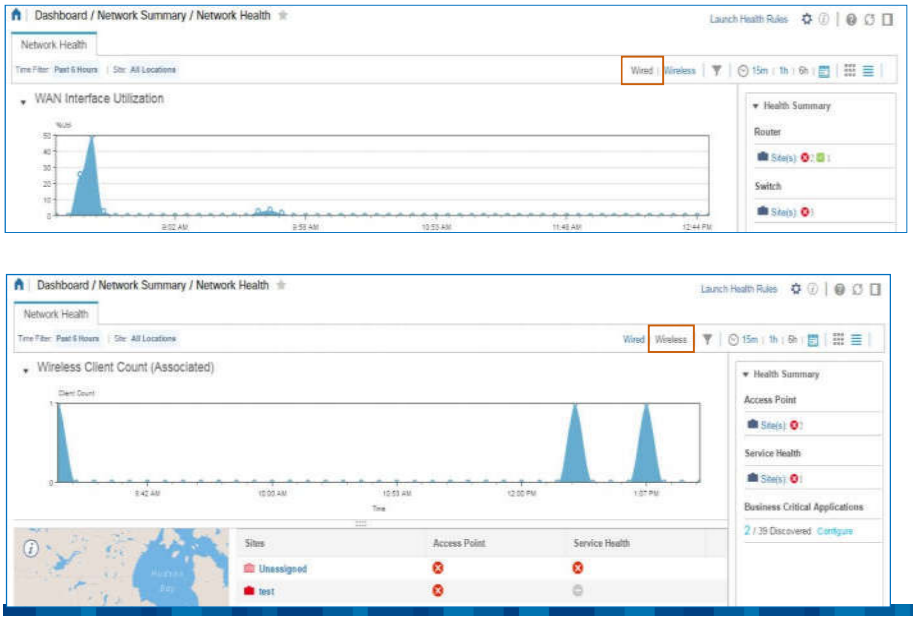
In addition to the dashboards and dashlets that you can use to monitor various targeted aspects of the network, you can monitor and evaluate the overall health of the entire enterprise network efficiently by using these key monitoring tools:.

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.

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**.

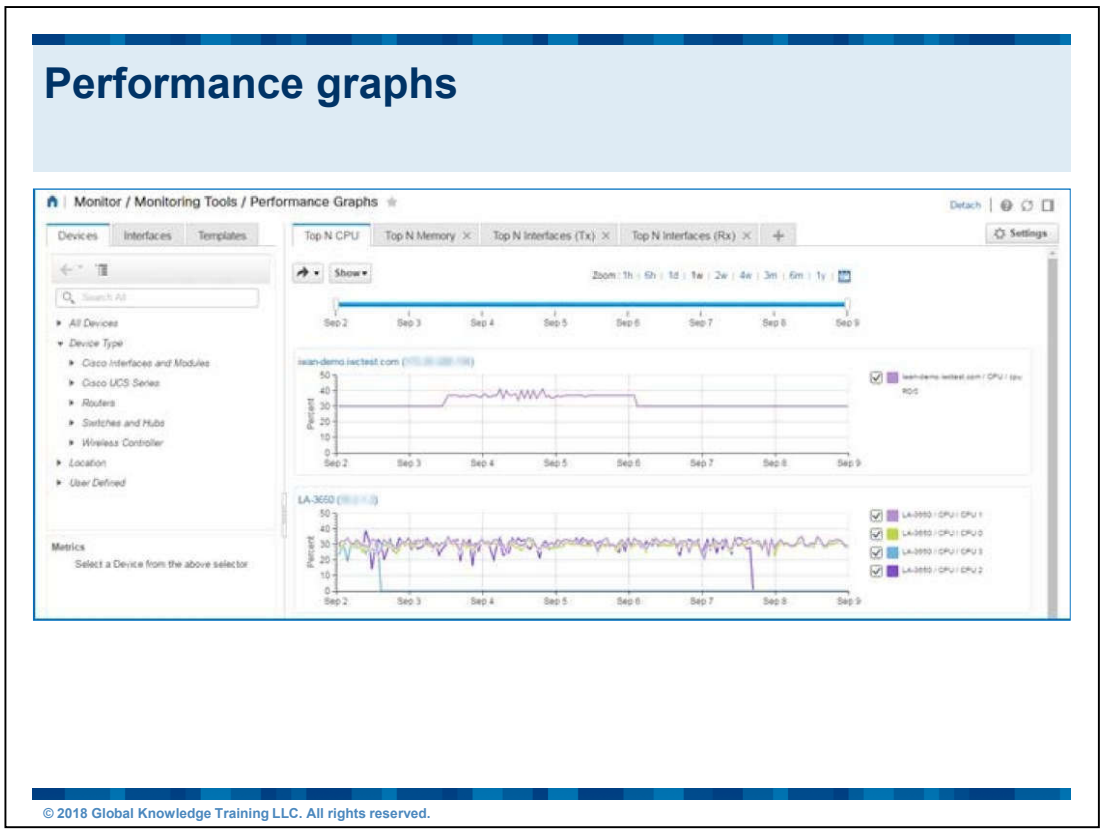
At a site level, access point metrics include:

Channel usage.

Noise.

Interference.

Interface usage.



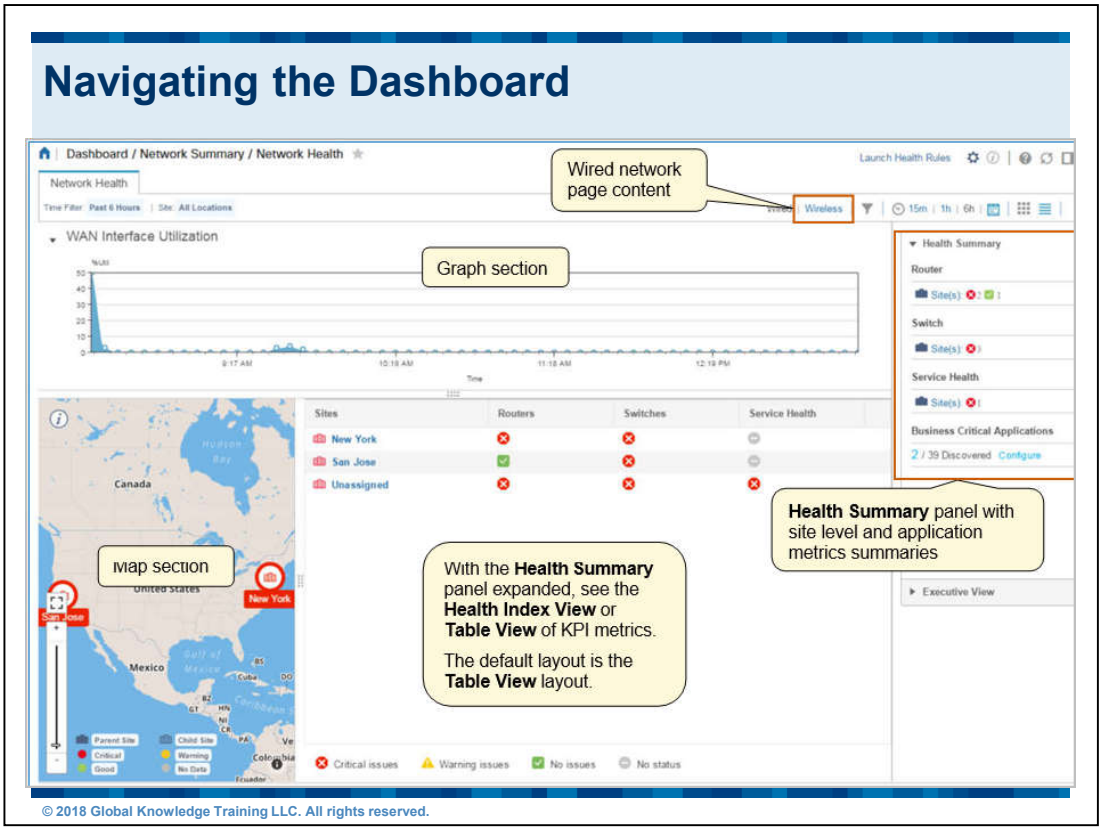
Performance graphs

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.



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.

Metric Health Status Color Codes

Good

The associated metric is reporting below the warning threshold value.

Warning

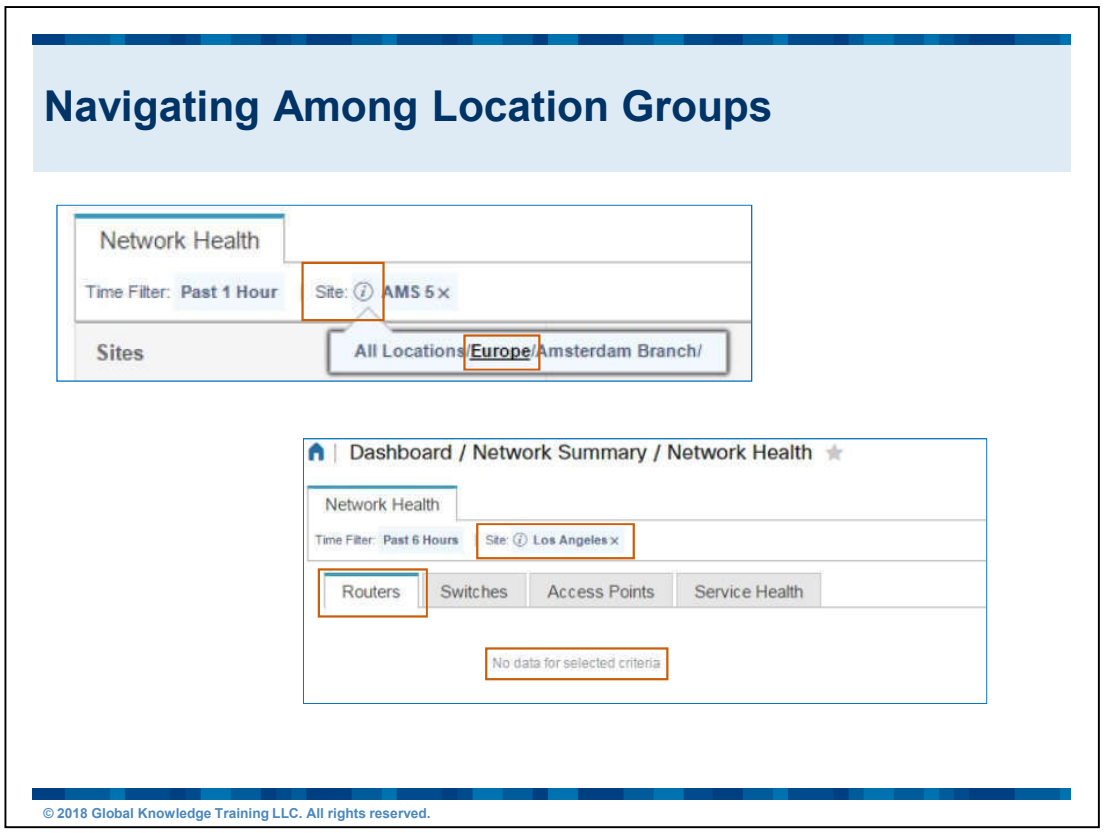
The associated metric is reporting above the warning and below the critical threshold values.

Critical

The associated metric is reporting above the critical threshold value.

No data

The system is not reporting data on the metric.



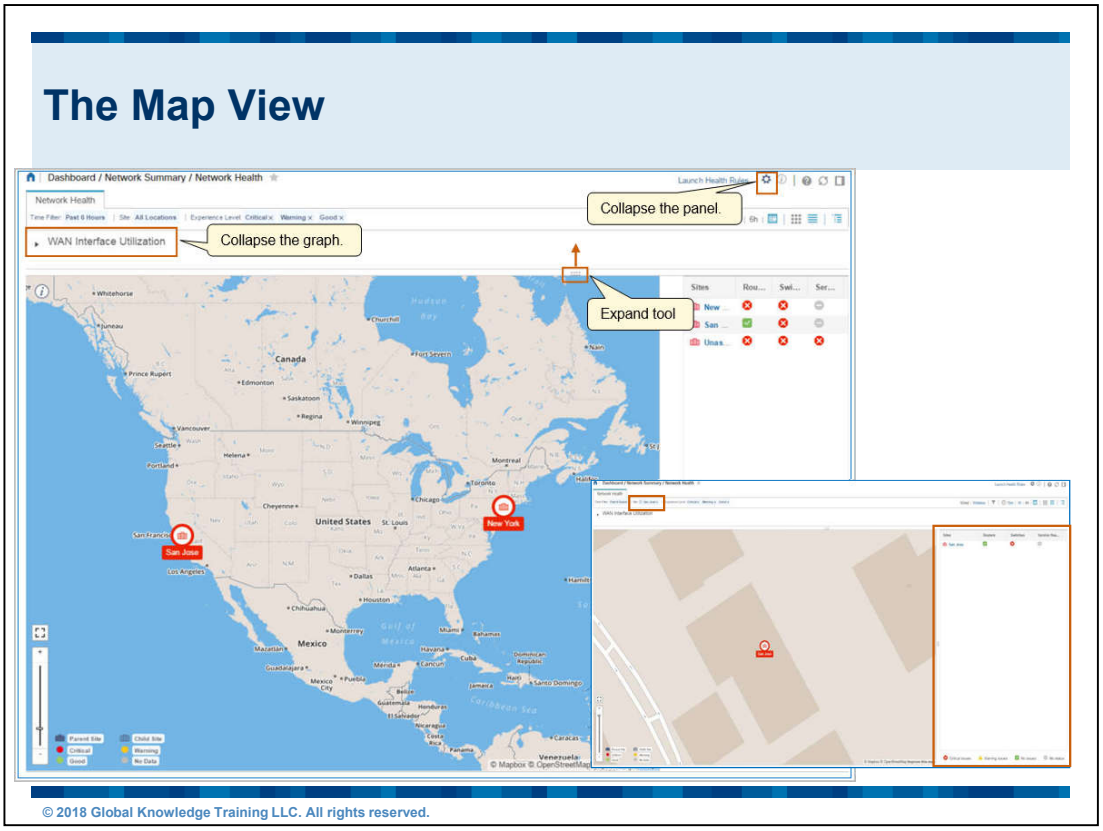
Navigating Among Location Groups

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.



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:

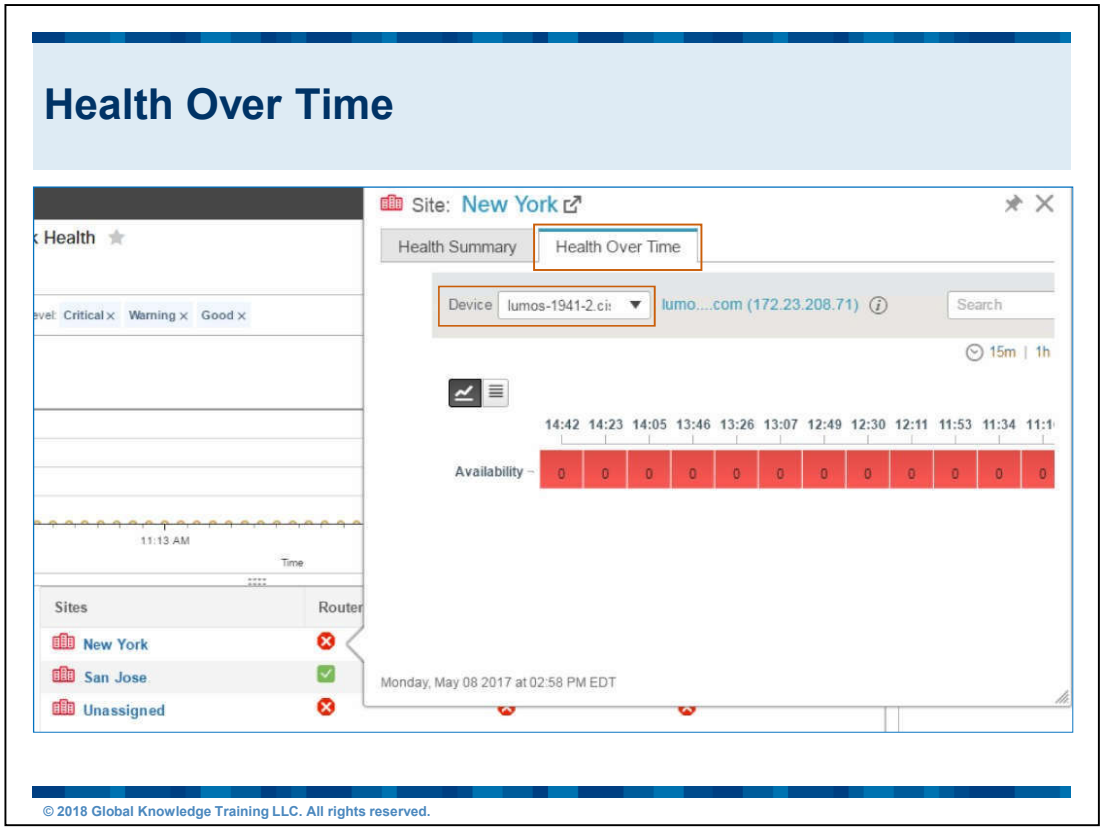
Expand the map area.

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.

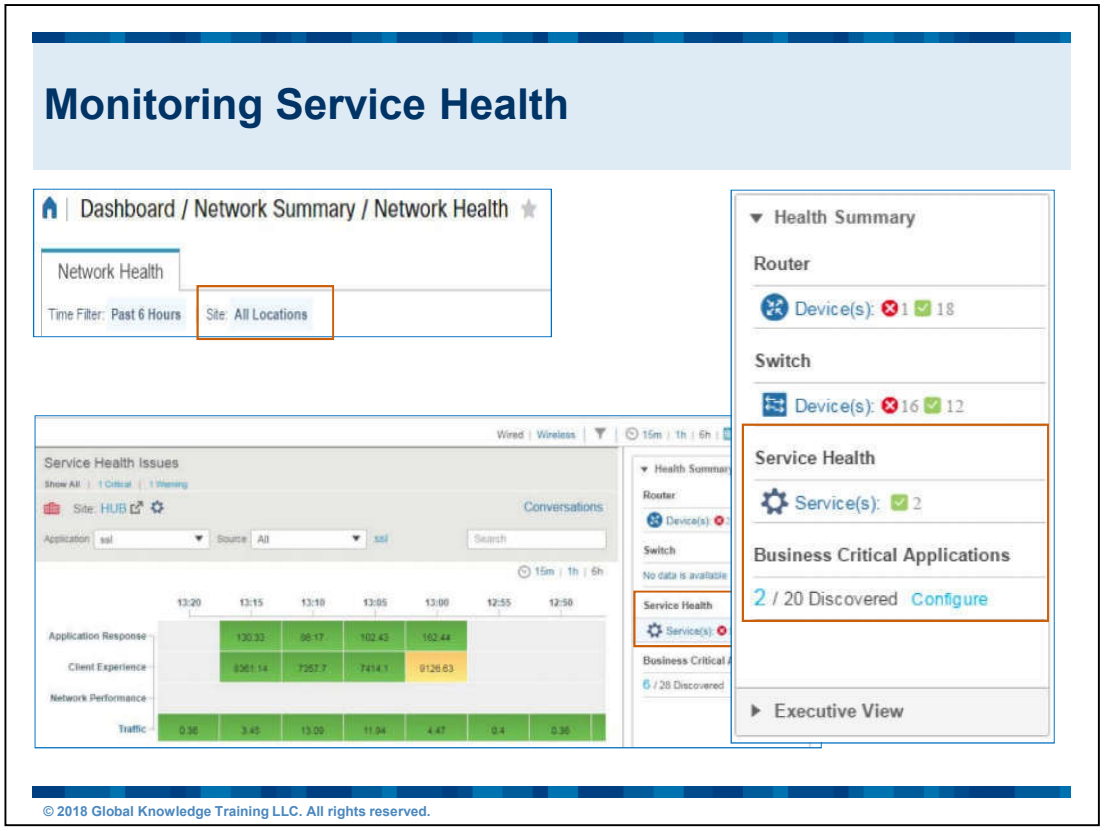


The **Health Over Time** tab illustrates the health of the device indicated in the **Device** drop-down list for the active time period. You can review the health of each device at the location by selecting it in the drop-down list.

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



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.

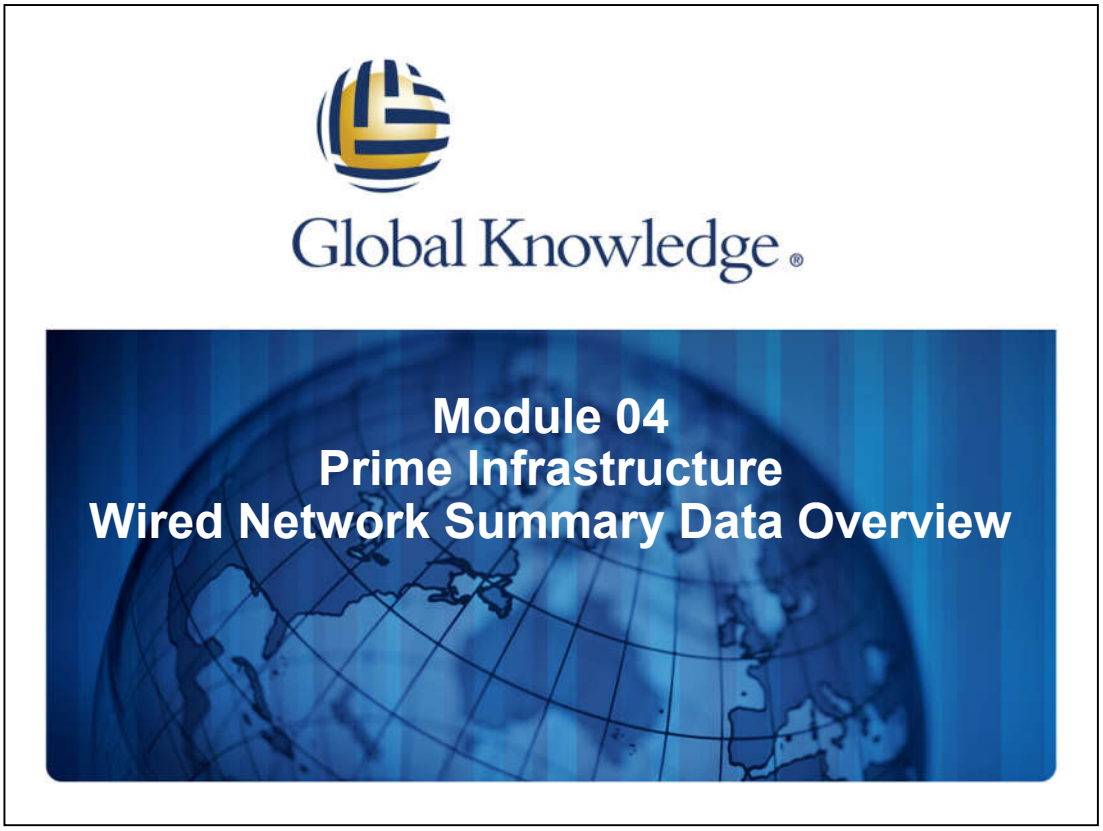
The health statuses that the system reports are defined by the threshold values in the health rules.

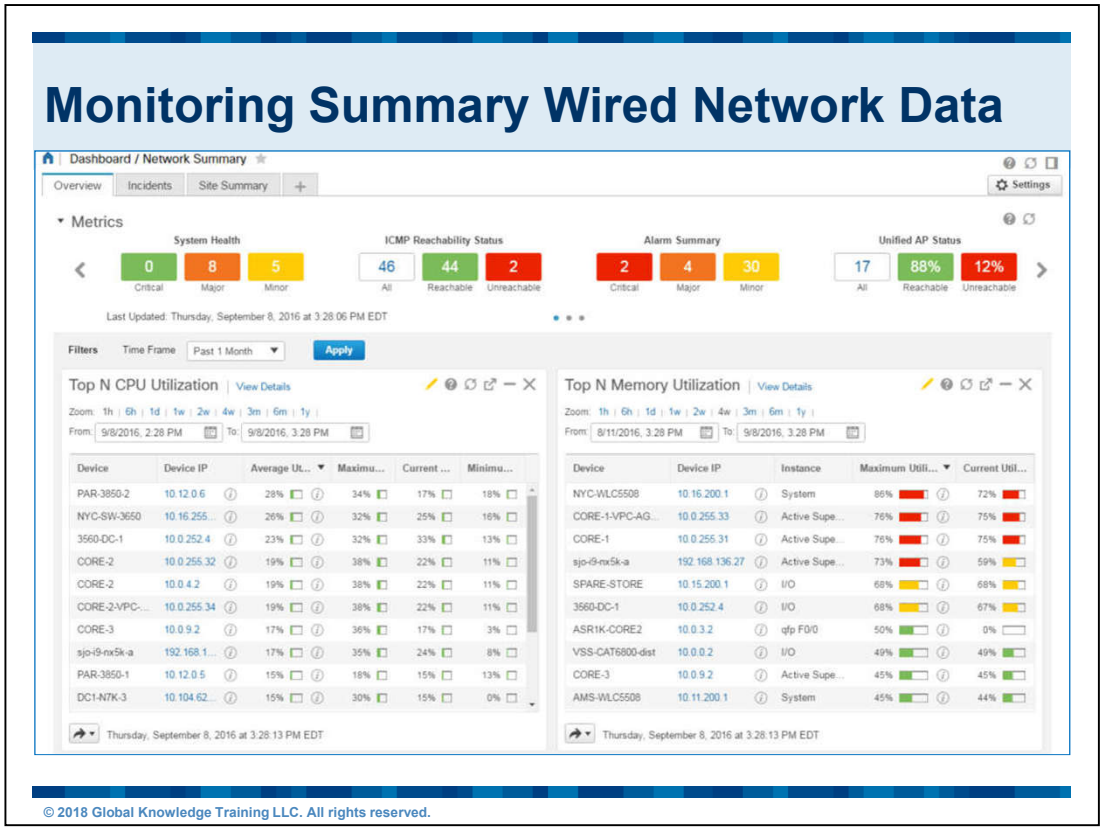
The **Health Summary** feature indicates service health issues based on the site level that you have active in both the wired and wireless views.

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…


Global Knowledge
Module 04
Prime Infrastructure
Wired Network Summary Data Overview



Cisco© Prime Infrastructure provides performance and fault monitoring tools that summarize the network activity and resource usage. Recognizing these tools will help you access the data that you need more efficiently and effectively.

Tool types include:

Dashboards

Which summarize data in concise, organized layouts to provide you with a comprehensive overview of the information that the system is reporting based on various categories

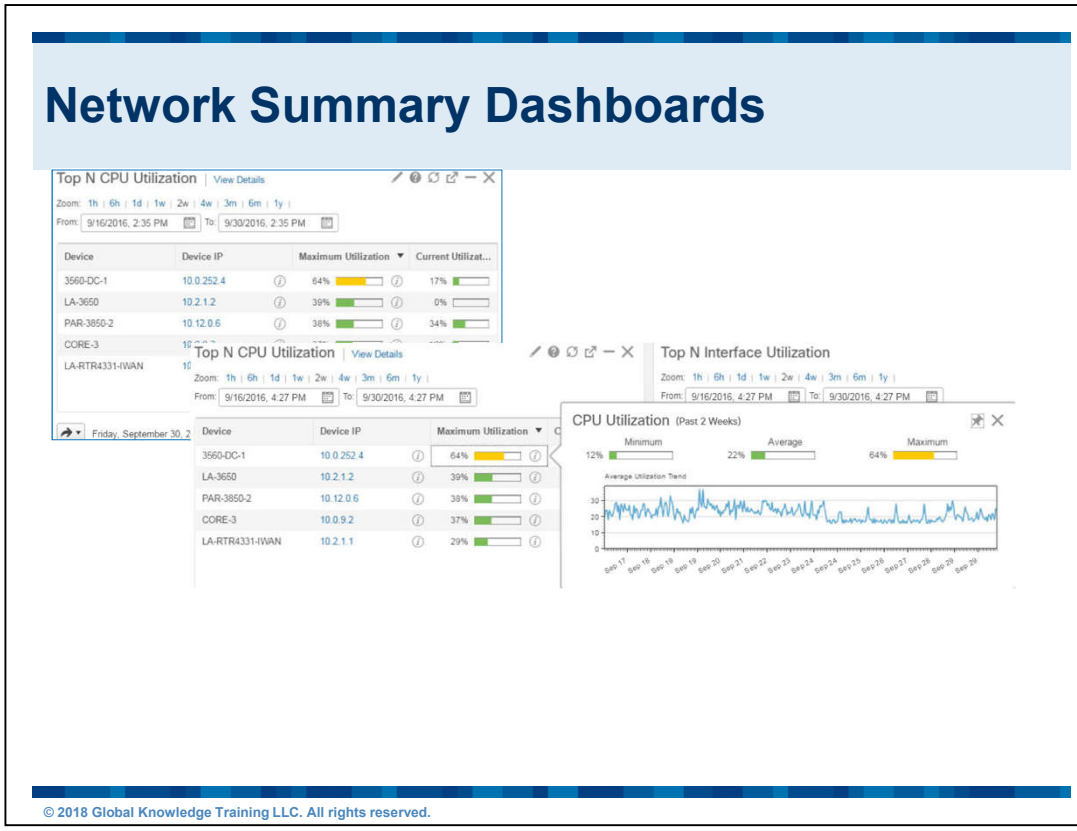
3600 views

Device- and interface-specific pop-up windows that contain significant amounts of - information, including listing alarms and providing information about neighboring devices

Network topology maps

Which provide a graphical representation that you can use to monitor and interact with network or data center devices, and are most often organized by locations, regions, or device types.

This job aid introduces you to Prime Infrastructure monitoring tools that report summary or high-level information and provide efficient navigation to detailed data to support your monitoring tasks.



Network Summary and Aggregate Dashlets

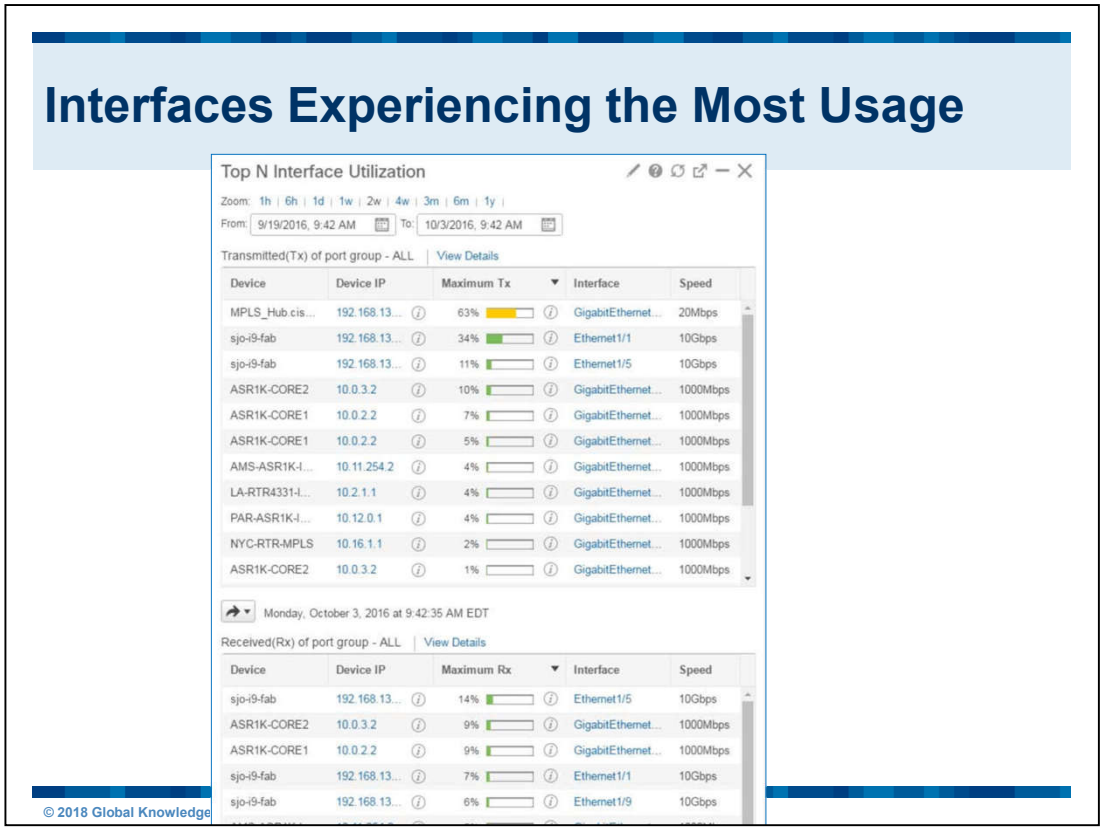
The following network summary and aggregate dashlets, available on the **Network Summary** | **Overview**, **Incidents**, and **Site Summary** tabs, report key wired data.

Tip: You also can monitor and manage wired router and switch health on the **Network Health** dashboard.

For more information, refer the **Network Health Monitoring Overview** job aid.

Device-Related Summary Dashlets

The **Top N CPU Utilization** dashlet lists the device CPUs experiencing the highest usage rates.



Interfaces Experiencing the Most Usage

The **Top N Interface Utilization** dashlet lists the interfaces receiving or transmitting the most data.

The data that you see in the dashlet depends on:

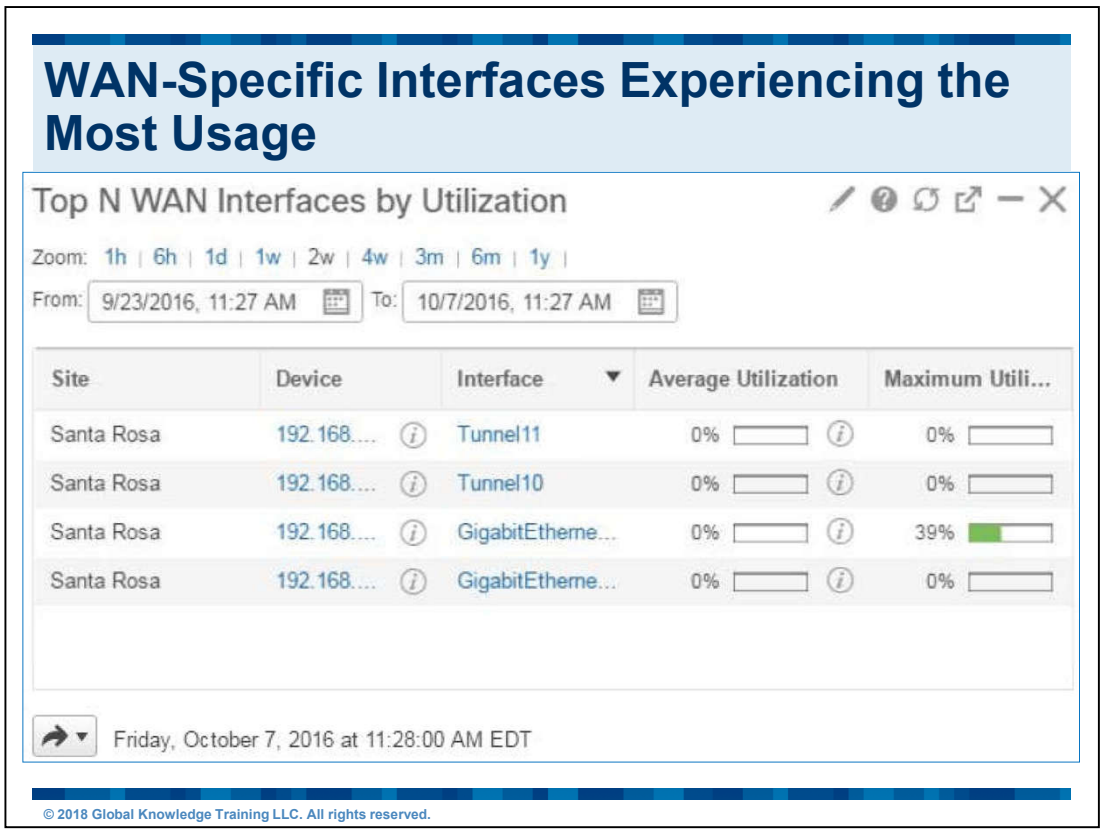
The monitoring policy definitions and reporting thresholds.

The port groups that system users have configured.

The settings that you apply to the dashlet.

How Monitoring Policies and Port Groups Affect Interface Reporting

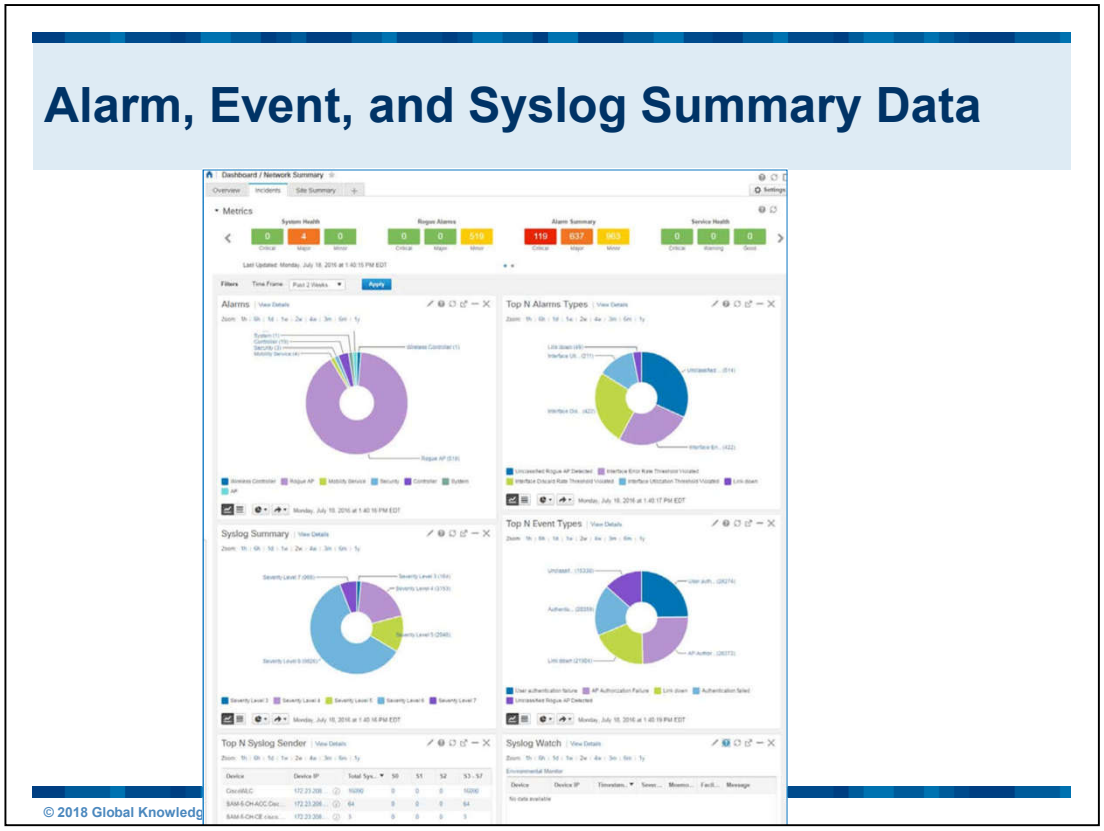
Prime Infrastructure enables standard monitoring policies automatically on installation. The automated policies report on these interfaces system-wide.



WAN-Specific Interfaces Experiencing the Most Usage

Because WAN interface connectivity is critical to ongoing enterprise communication and network support among sites, Prime Infrastructure reports metrics for WAN-specific interfaces separately in the **Top N WAN Interfaces by Utilization** dashlet.

This dashlet provides all of the same features, functions, and management capabilities available to you on the **Top N Interface Utilization** dashlet. In this case, rather than port groups, you can evaluate WAN interfaces at a site level.



Alarm, Event, and Syslog Summary Data

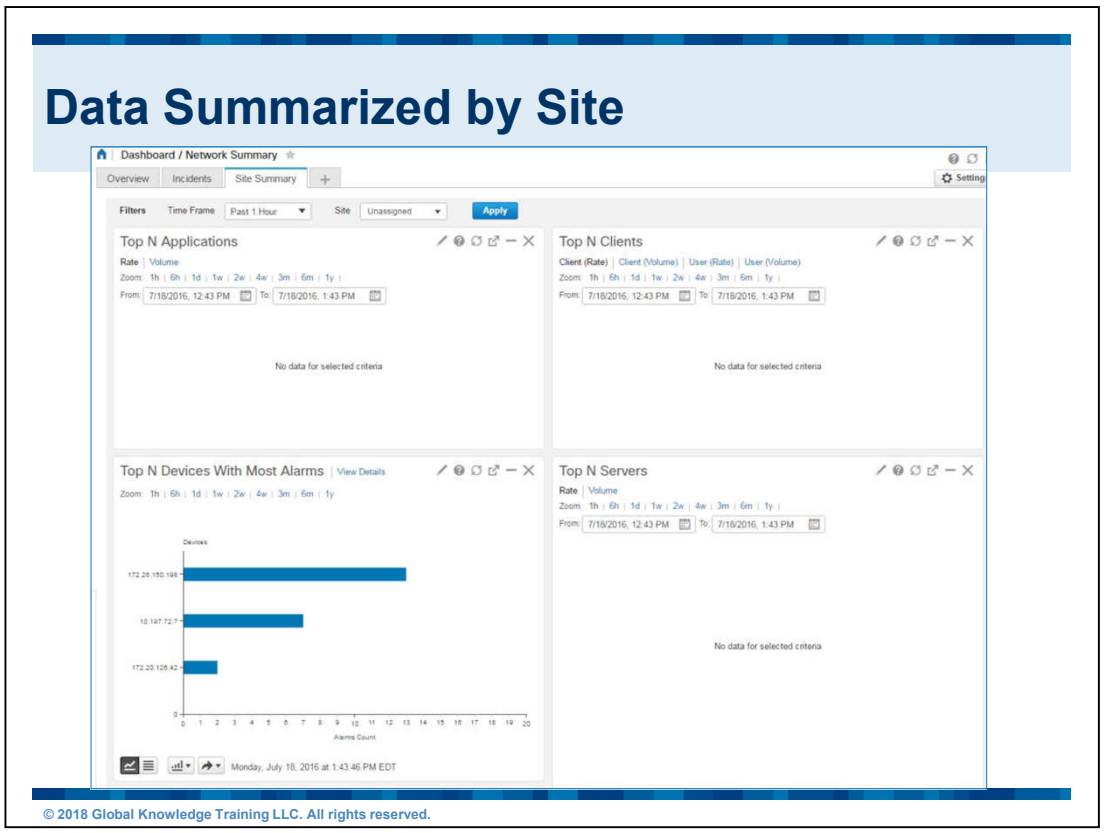
Alarm, event, and syslog summary data combines reporting of incidents occurring on wired and wireless devices.

Based on the time frame that you select on the toolbar, the **Incidents** tab summarizes:

Active network and system alarms and their types.

The types of events the system is reporting.

Syslog types, the devices reporting the most number of syslogs, and the types of messages that devices are re



Data Summarized by Site

Based on the time frame and site that you select on the toolbar, the **Site Summary** tab reports:

The most used applications by volume or rate for that site.

The clients most often accessing the network for that site.

The devices reporting the most alarms at that site.

The servers reporting the highest traffic rates at that site.

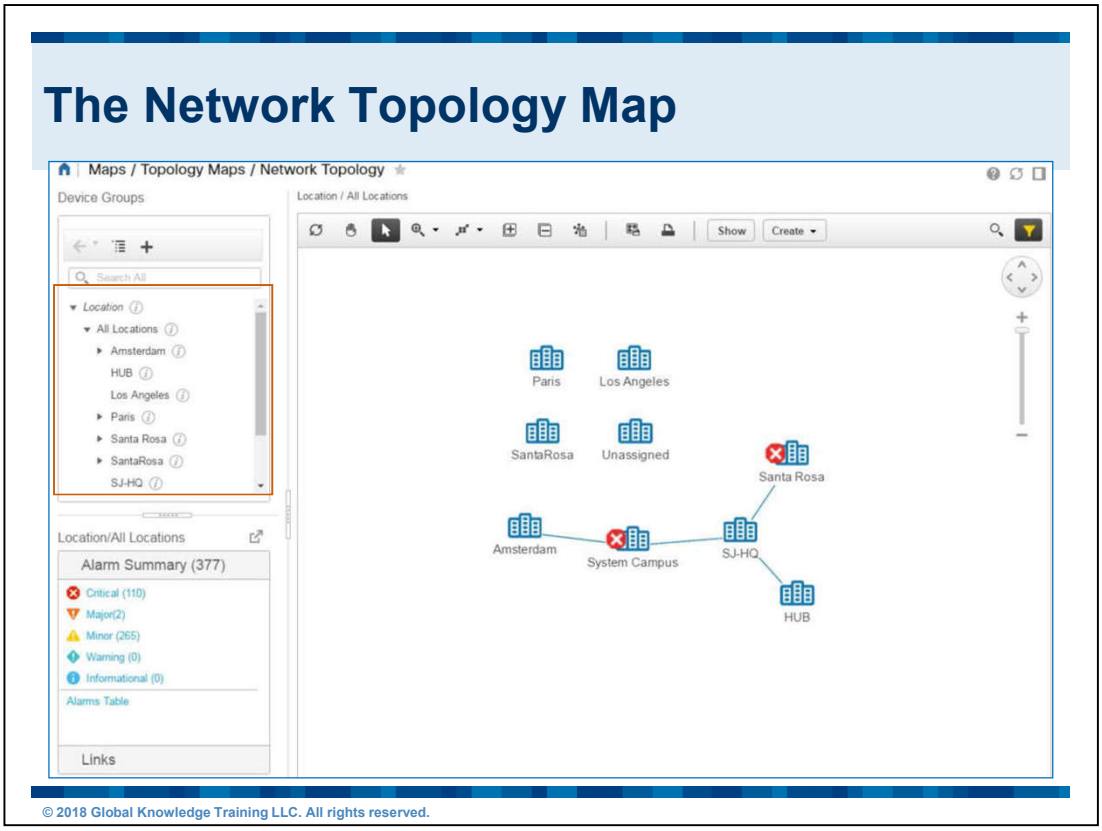
Device 3600 Views

Device **3600 View** pop-up windows present significant amounts of information, report key performance metrics and activities that are occurring on devices, and provide access to take actions on devices, as needed.

The device type determines the information that is available and the actions that you can take in a pop-up window.

The following screenshot illustrates a Cisco Catalyst 3560 series switch **3600 View** pop-up window.

Most tables listing a device IP address provide access to **3600 View** pop-up windows by using the information icon.



Topology Maps

Overview

Topology maps illustrate the portions of the network that they represent, including device and interface relationships, neighbors, associated alarms, and the provisioned circuit and network connections.

You can monitor network or data center devices by using topology maps.

Topology Map Navigation

System users can organize network and data center topology maps logically by using location, device type, or custom groups to reflect the organization of the enterprise.

When organizing groups, users can include dependent subgroups. For example, a regional group, such as Paris, might have 3 building subgroups, and each building subgroup might have several subgroups to reflect the floors in the building.

Logically organizing groups and their dependent hierarchies can help user activities by illustrating key device and network relationships, which can emphasize how issues might affect portions of the network.

The Network Topology Map

Overview

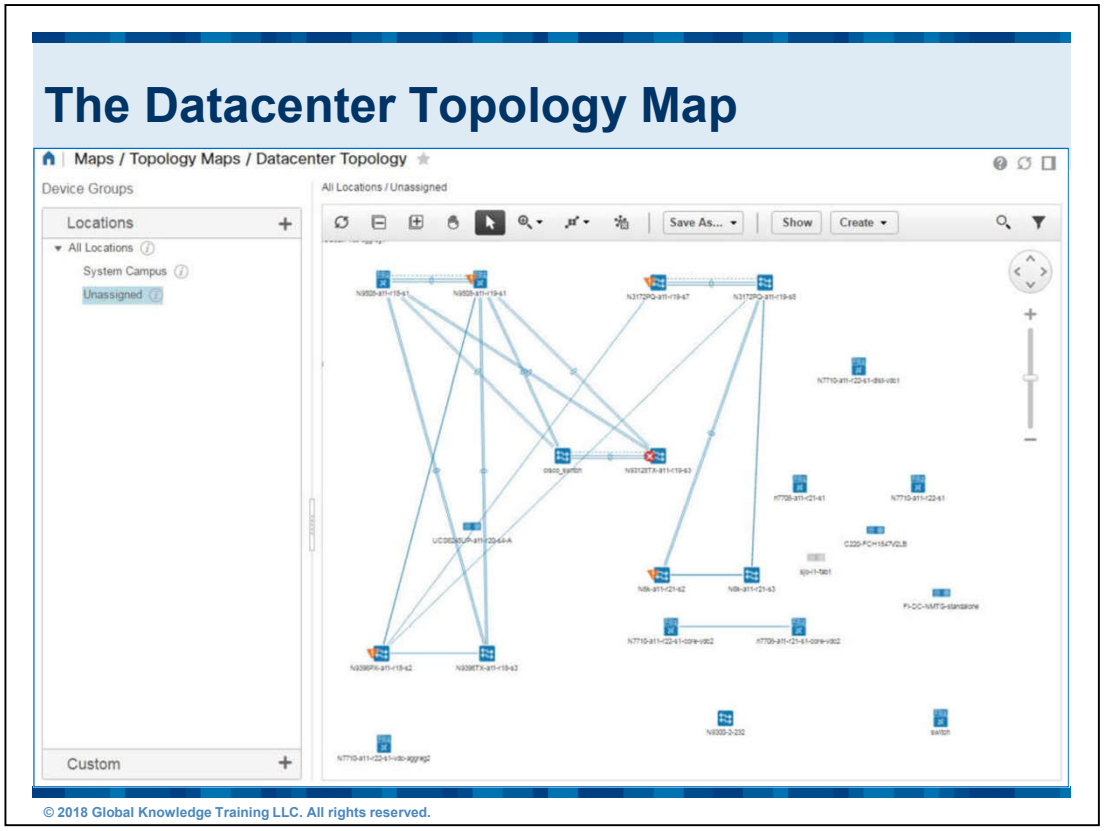
Network topology maps present a graphical view of wired and wireless network devices and their relationships.

You can monitor device groups based on location, device type, or custom groups.

The **Alarm Summary** list reports the number of alarms for each severity level that are active on the current map.

Note: When a series of groups is active on the map, the list reports the number of alarms for all of those groups, inclusively.

As you open specific groups, the list updates to report alarms for the devices included in the group or groups that are visible.



The Datacenter Topology Map

Overview

Datacenter topology maps present a graphical view of the data center devices, including:

Nexus switches.

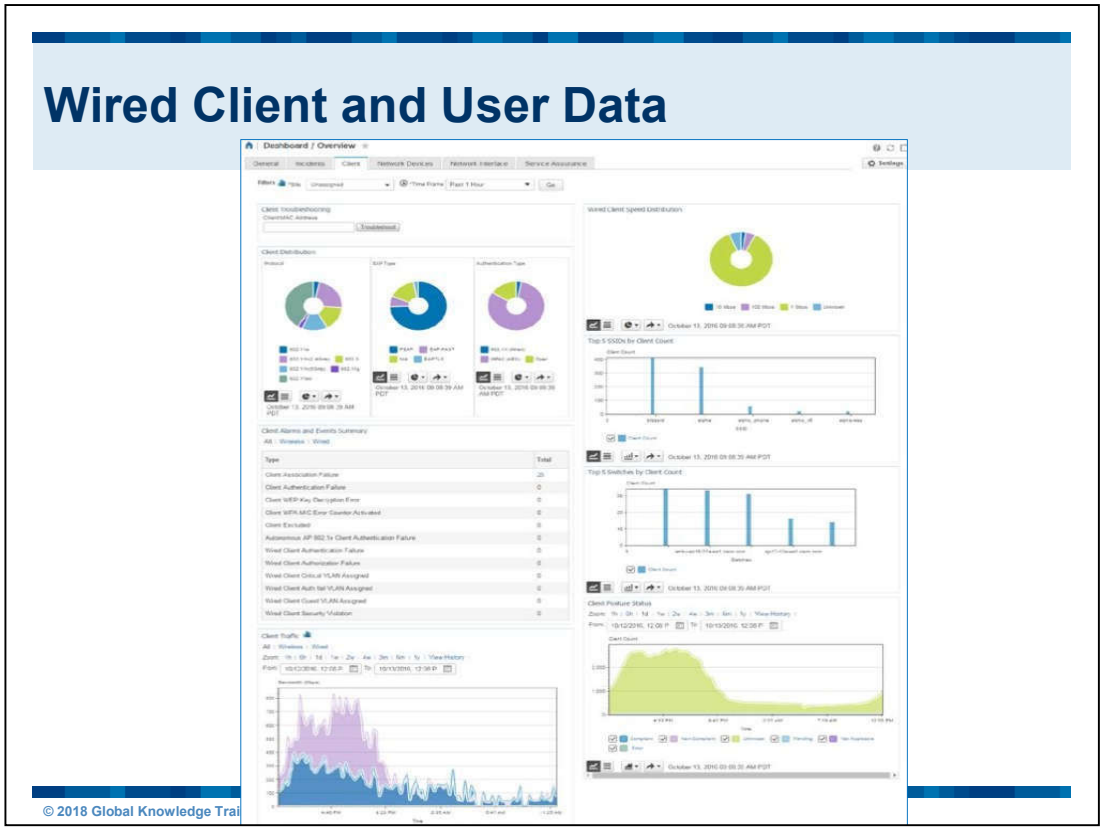
Cisco Unified Computing System (UCS) blade servers.

Fabric interconnect switches.

As on network topology maps, data center topology maps illustrate the relationships among data center devices and indicate the highest severity level alarms occurring on devices, when alarms are occurring.

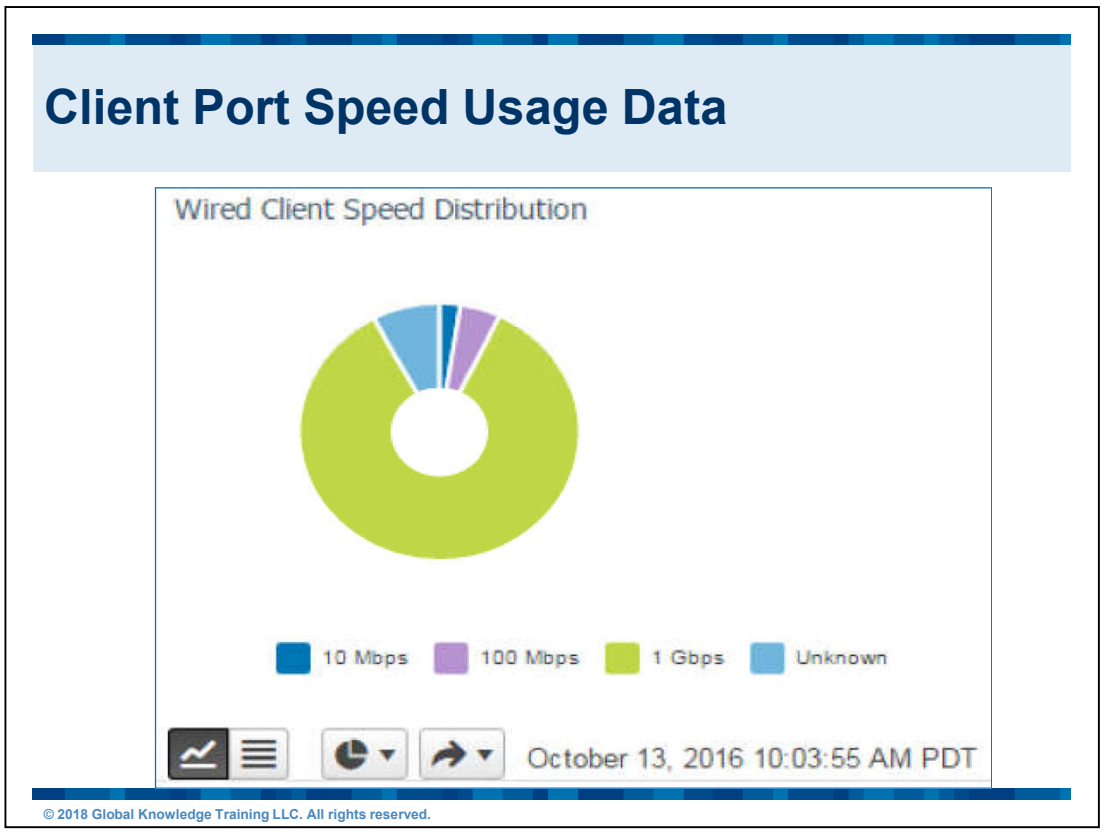
This topic addresses features that are unique to data center devices and monitoring.


Global Knowledge
Module 05
Prime Infrastructure
Wired Clients and Users Monitoring
Overview



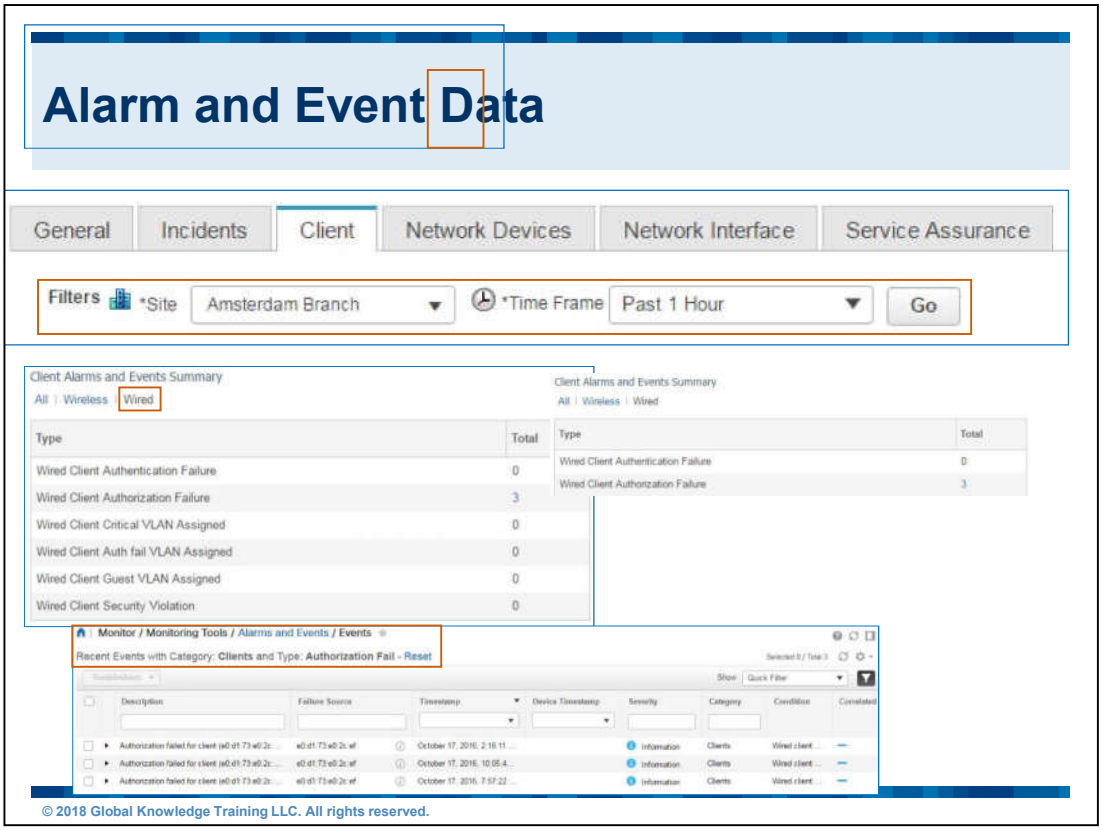
Dashboards present summary and aggregate data in concise, organized layouts to provide you with a comprehensive overview of the information that the system is reporting based on various categories.

While some dashboards and dashlets combine reporting on both wired and wireless areas of the network, this job aid focuses on wired network monitoring.



The Wired Client Speed Distribution dashlet reports the number and percentage of wired clients that are using various port speeds based on the ports to which the clients are connected.

This information provides insight into the type of wired clients that using the network and their bandwidth requirements and also can help administrators size the network appropriately based on port speed usage.



Alarm and Event Data

The Client Alarms and Events Summary dashlet lists the active, client-related alarms and events for the site and timeline selected on the dashboard.

Note: Alarms are current as of the last time that the system refreshed the data.

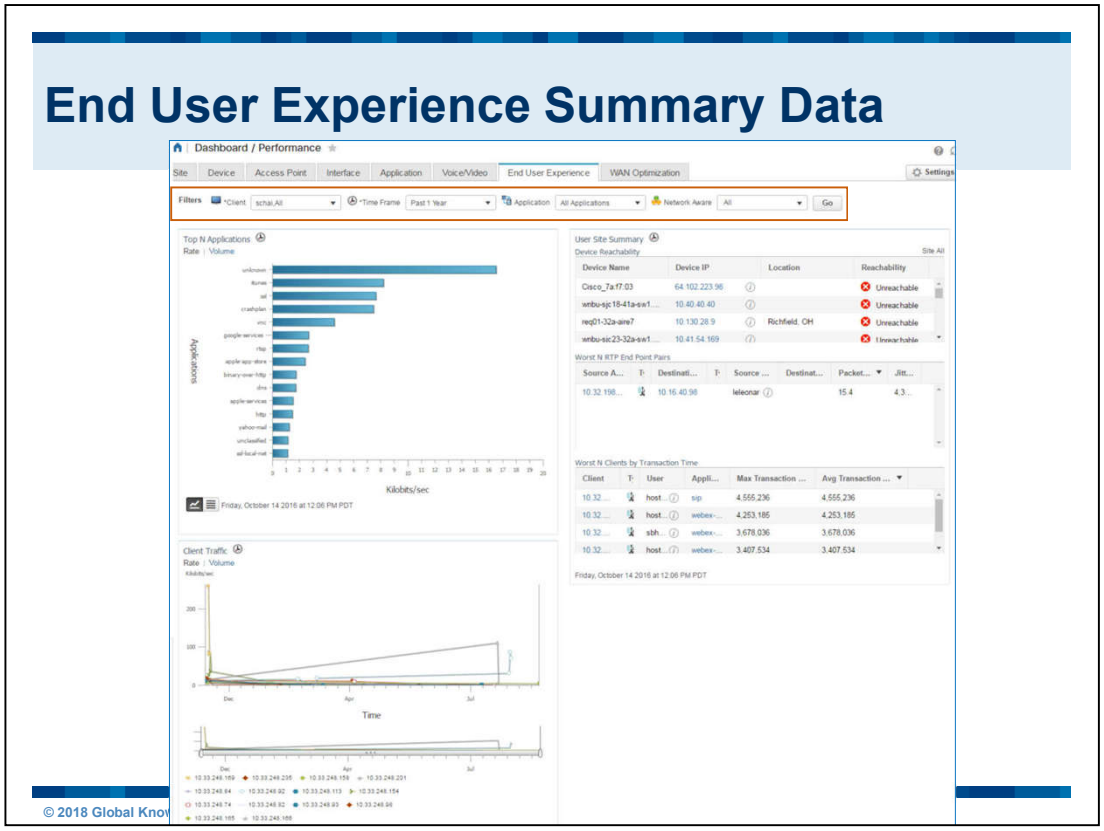
To see alarms related to wired clients:

❖ Below the dashlet title, click Wired. The dashlets lists the wired alarm categories only.

To review the alarms associated with an alarm type:

❖ In the dashlet, in the Total column, click the number link.

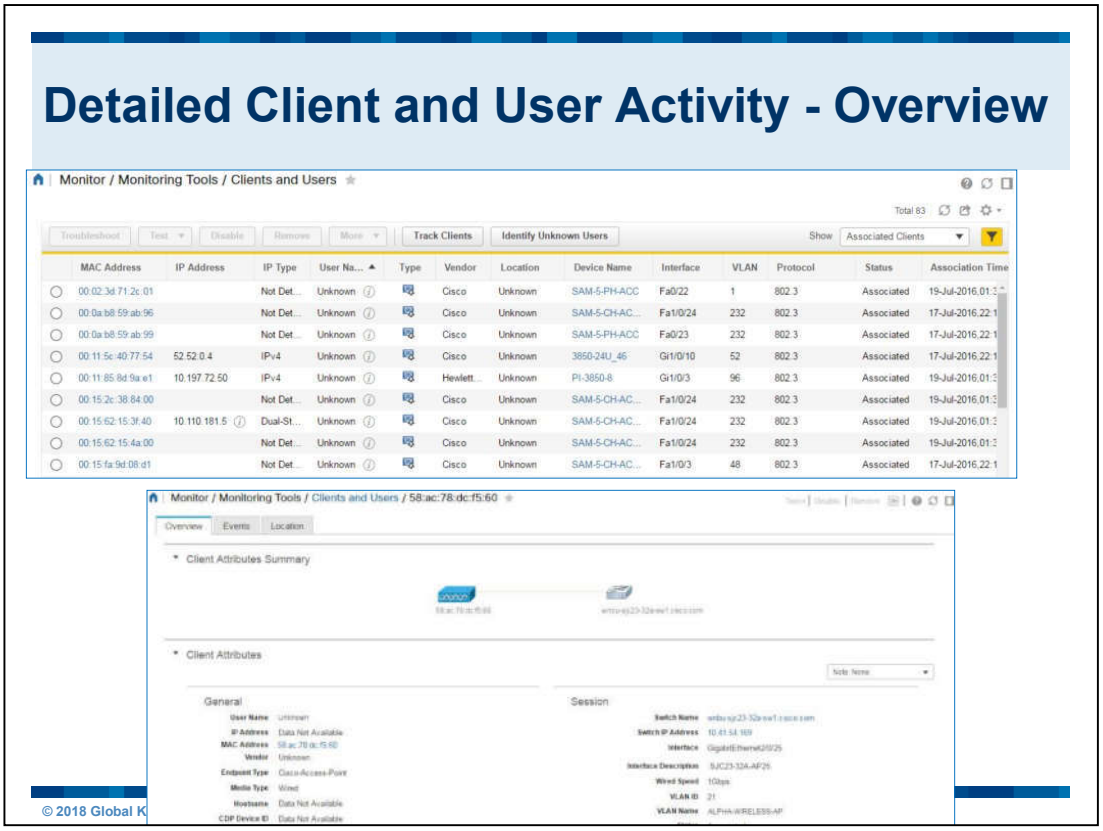
The system navigates to and opens the list of events related to the category.



End User Experience Summary Data

When a system user is reporting, or you see an IP or a MAC address exhibiting, performance-related issues, you can review application, site, traffic, conversation, and packet loss data, which can provide insight into areas that might be affecting a system user's experience.

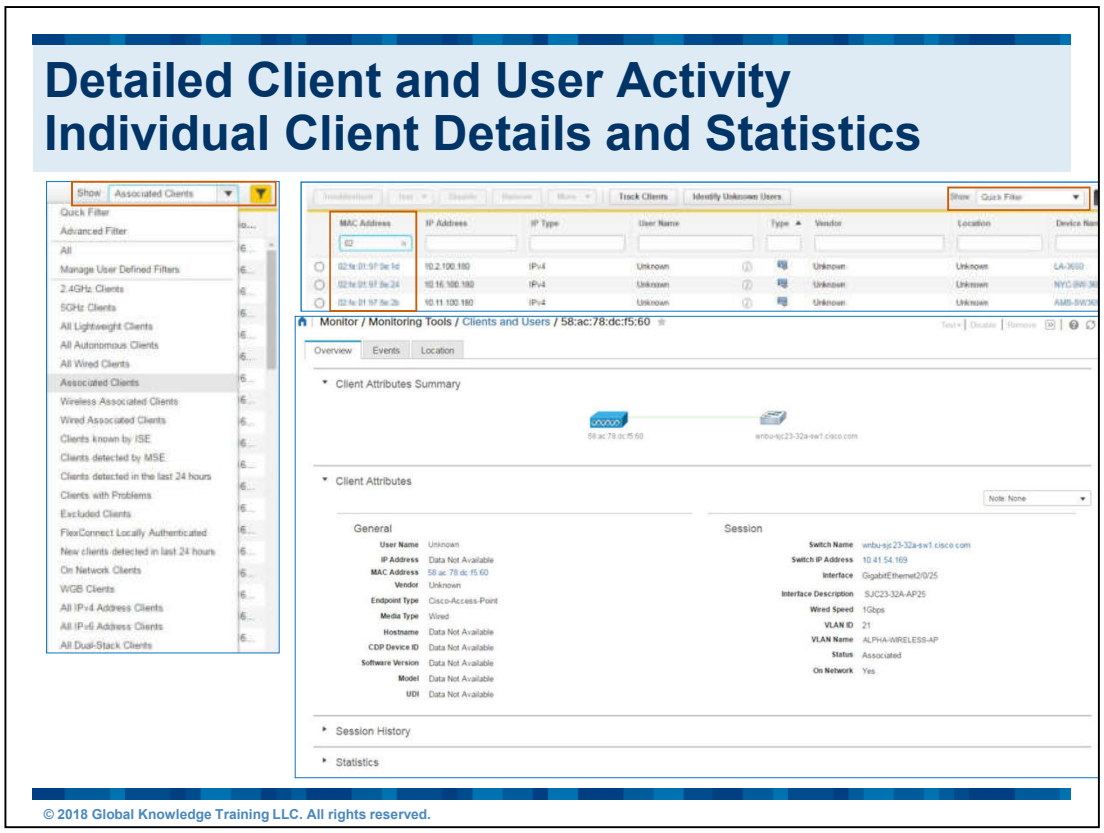
By using the toolbar, you can filter the data in all of the dashlets by a specific client, time period, or application, or by wired or wireless devices.



Overview

The Client and Users page reports the clients that currently are or have been connected to the network.

It also provides detailed user and end user device information based on data that system users can configure. For example, system users can configure civic (physical address) locations or geographical coordinates for devices, which makes location information available on the Location tab.



Individual Client Details and Statistics

When you open the Client and Users page, the system filters the page to display all of the clients associated with the network by default.

The Show drop-down list indicates the criterion currently applied to the list, as emphasized by the active filter indicator .

Note: When you do not see the clients that you expect, change the filter criteria to include them.

When you have a long list of clients, you can use the Quick Filter feature to find the item that you need.

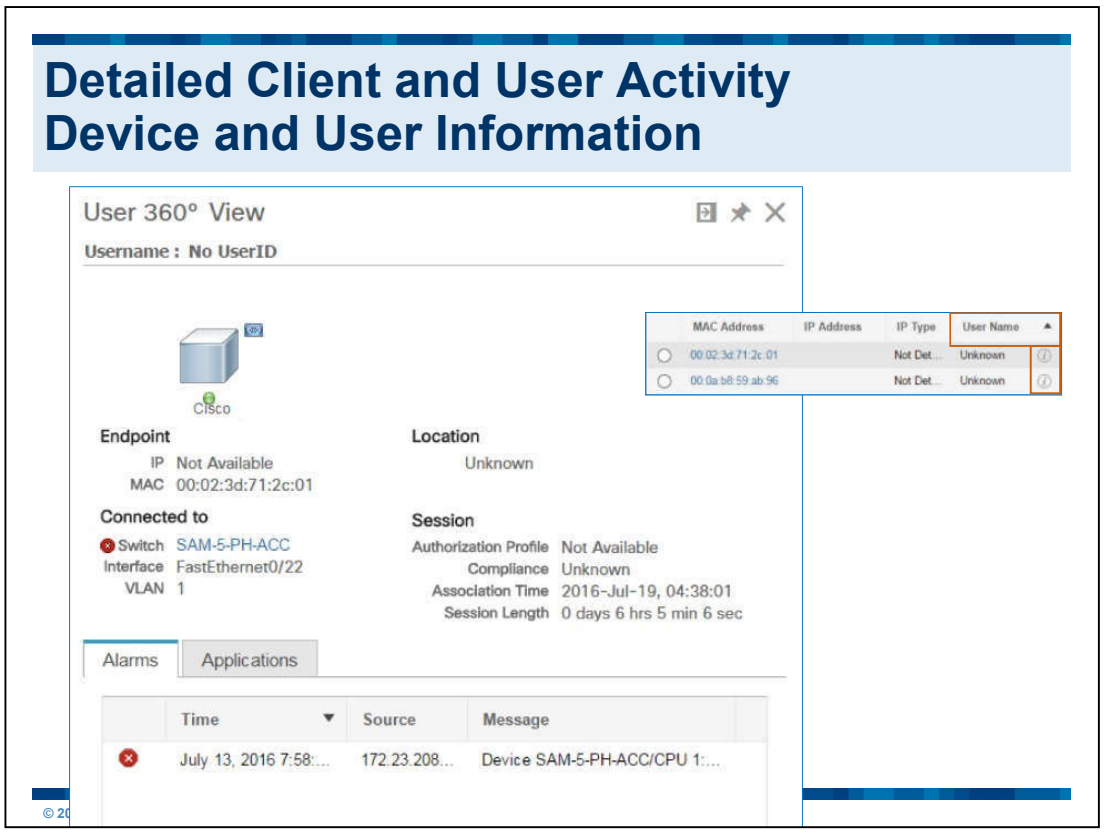
To apply a quick filter:

❖ In the Show drop-down list, select Quick Filter, and then, below the applicable column heading, in the field, type or select item data. The system filters the list to show those items that match the search criteria.

You can configure a series of filter rules to see specific clients by using the Advanced Filter

feature.

Tip: Filtering the list to see specific types of clients can make some



The **User 3600 View** pop-up window provides key information about the client.

You can see where and how the user is connected, any alarms associated with the session, and the application or applications in use.

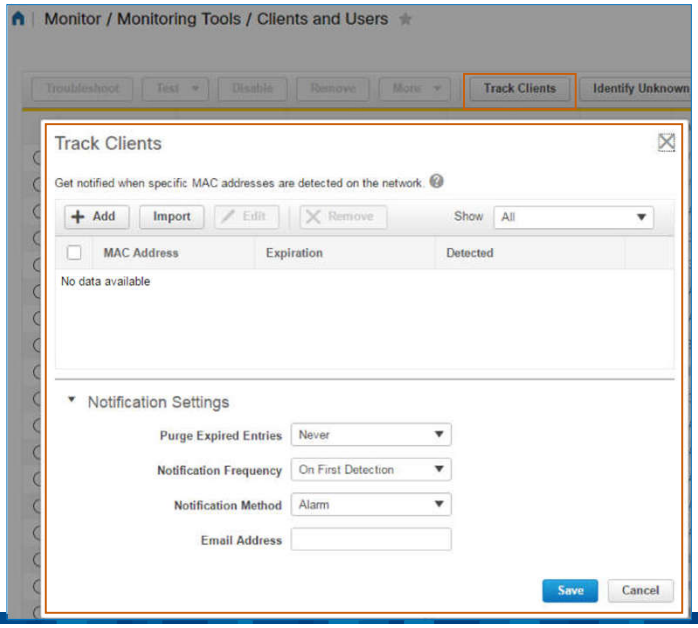
When users are using more than one device, an icon representing each device appears in the window.

To review details about devices, you can click the device icon of interest, which updates the window with the associated details.

To open a client's User 3600 View pop-up window:

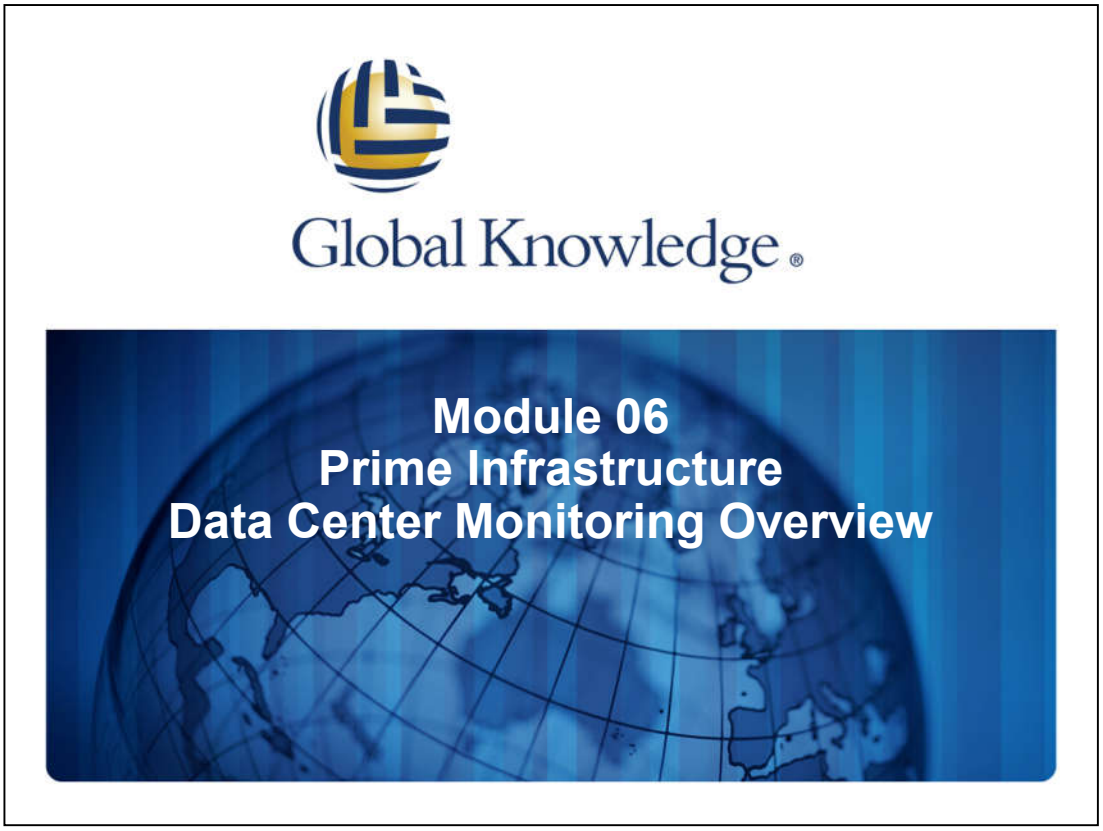
In the client's **User Name** field, click the information icon.

Detailed Client and User Activity
Ongoing Client Behavior



When you want to perform ongoing monitoring of a particular client or clients, you can use the **Track Clients** feature, which generates notifications when it detects that the client that you designate is using the network.

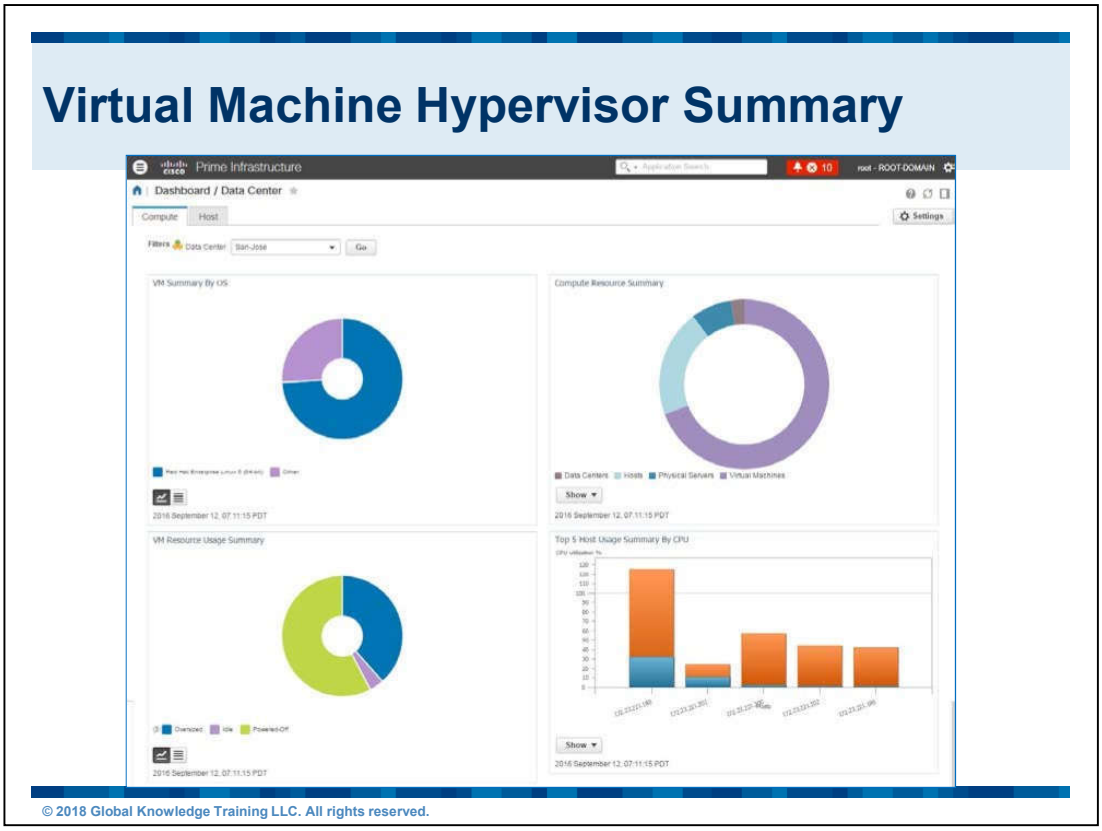
This type of monitoring can be helpful when you need to determine that the network is detecting a specific device.



The data center includes the virtual and physical servers that provide compute resources, including data storage and processing resources, to the enterprise.

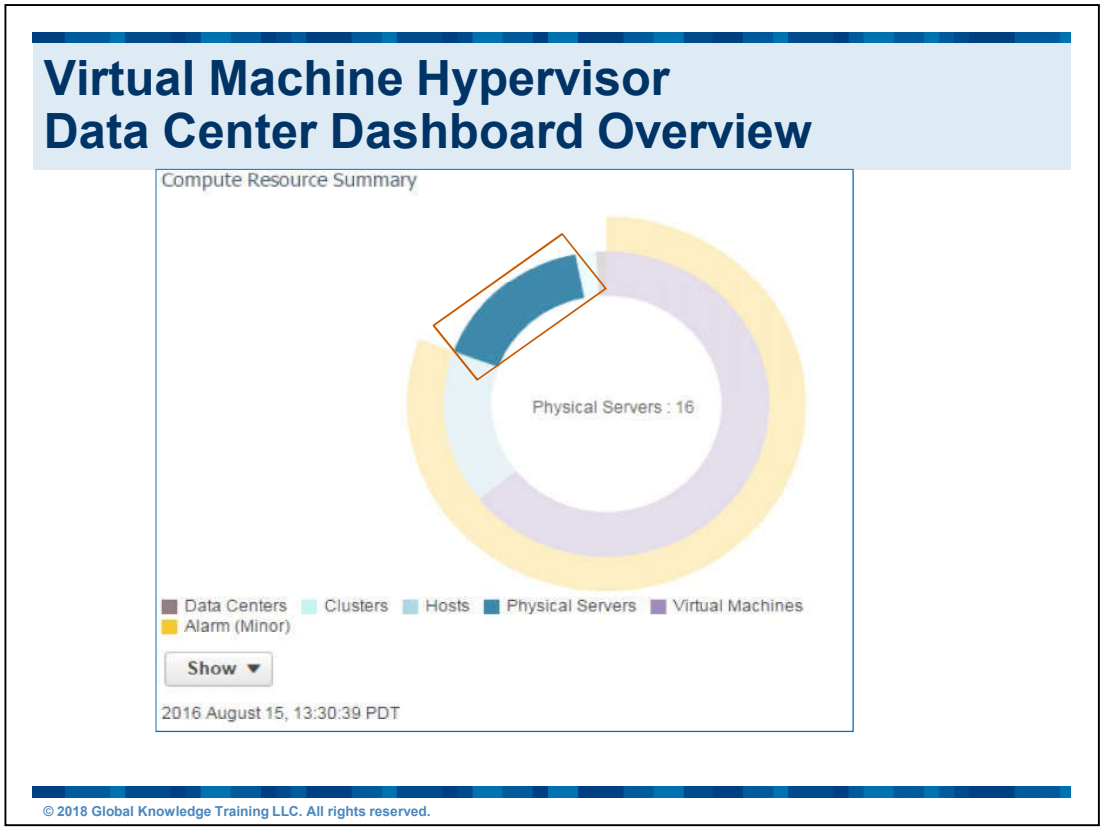
This feature supports end-to-end monitoring of the network among sites and the data center. For example, when investigating an application access issue, you can evaluate the server environment in addition to the network to help determine the root cause of the problem.

Or, if during proactive monitoring you see that a server blade is not operational, you can see the virtual machines (VMs) running on it to determine the operations that might be affected. As an example, consider that you have the Oracle application running on a group of virtual machines and you see that the blade that is running those virtual machines is reporting alarms. You can investigate the alarms and correct associated issues before they affect users' access to the Oracle application.



Data Center Dashboard Overview

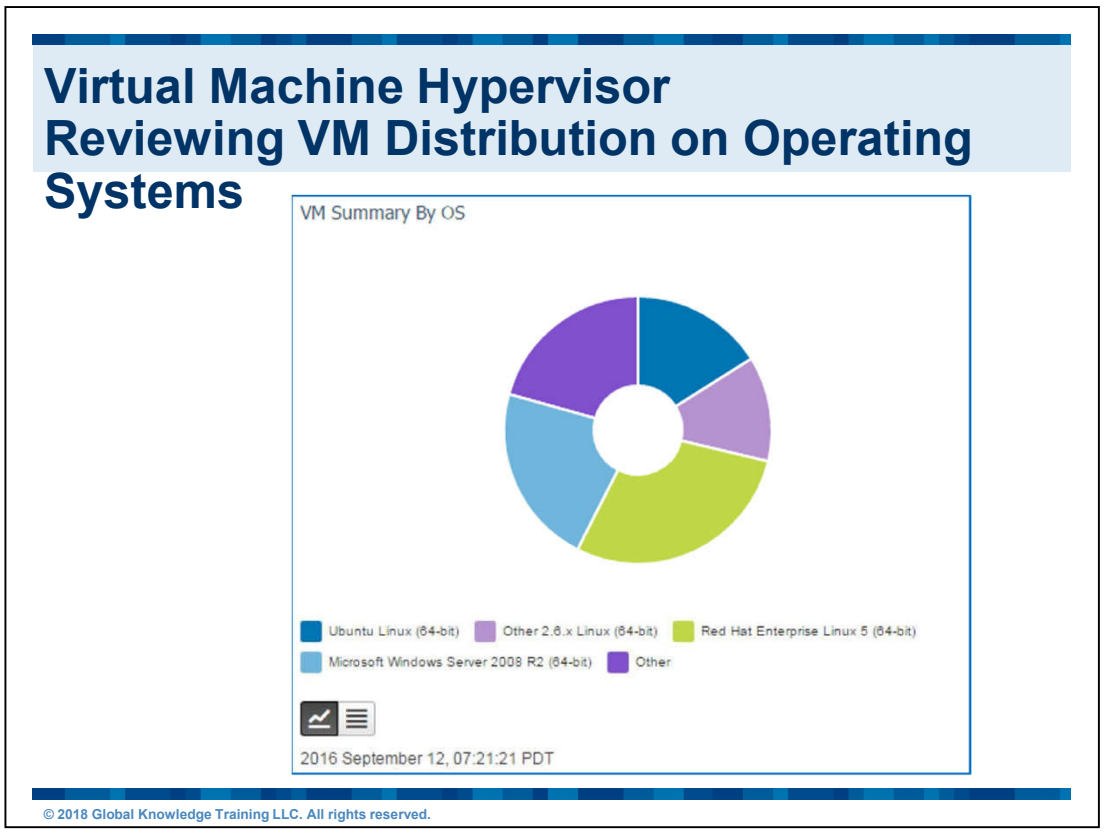
The dashboard provides dashlets that report metrics on hosts, such as host usage by CPUs, and on virtual machines, such as VM statuses and the number of VMs by operating system and resources, the number of compute resources and associated alarms, and host CPU and resource usage.



To navigate to details when reviewing summary data:

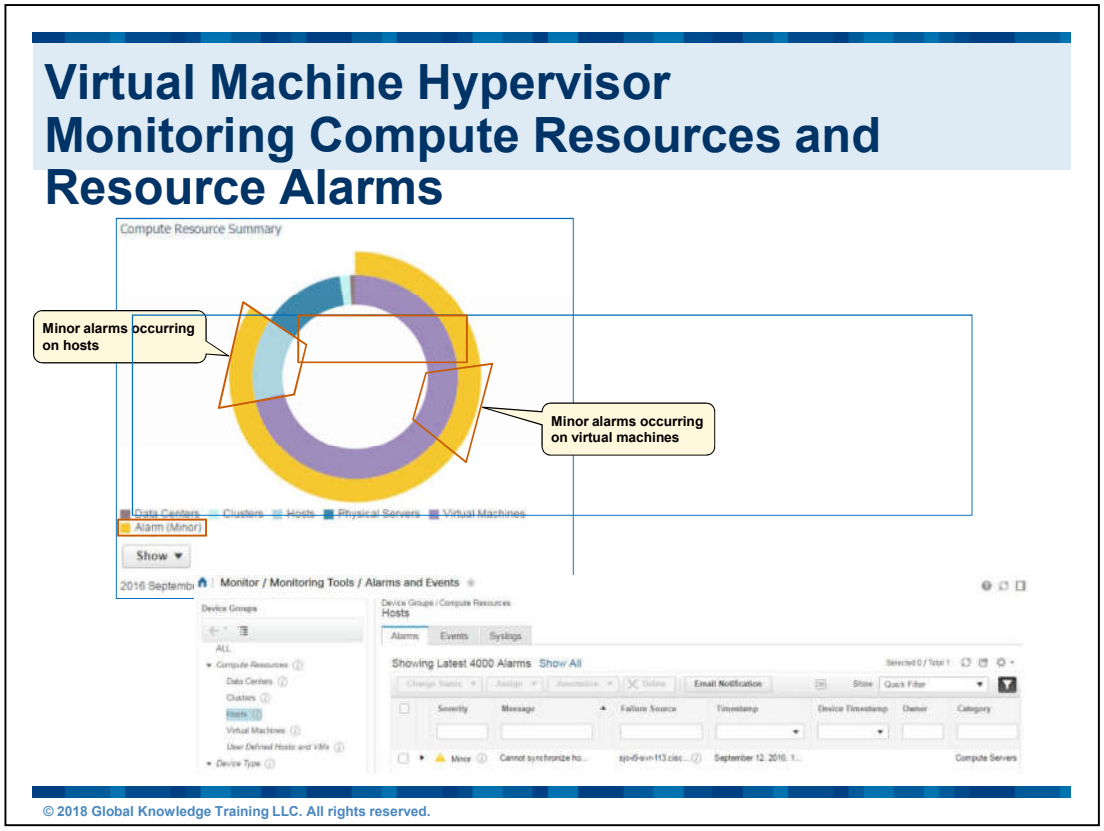
In a chart, click a compute resource data element.

The system opens the page associated with the data element that you clicked. For example, clicking the Physical Servers data element in the chart above opens the Physical Servers page in Compute Devices, illustrated below.



Reviewing VM Distribution on Operating Systems

The **VM Summary By OS** dashlet provides graphical and table views of the number of virtual machines running the operating system.

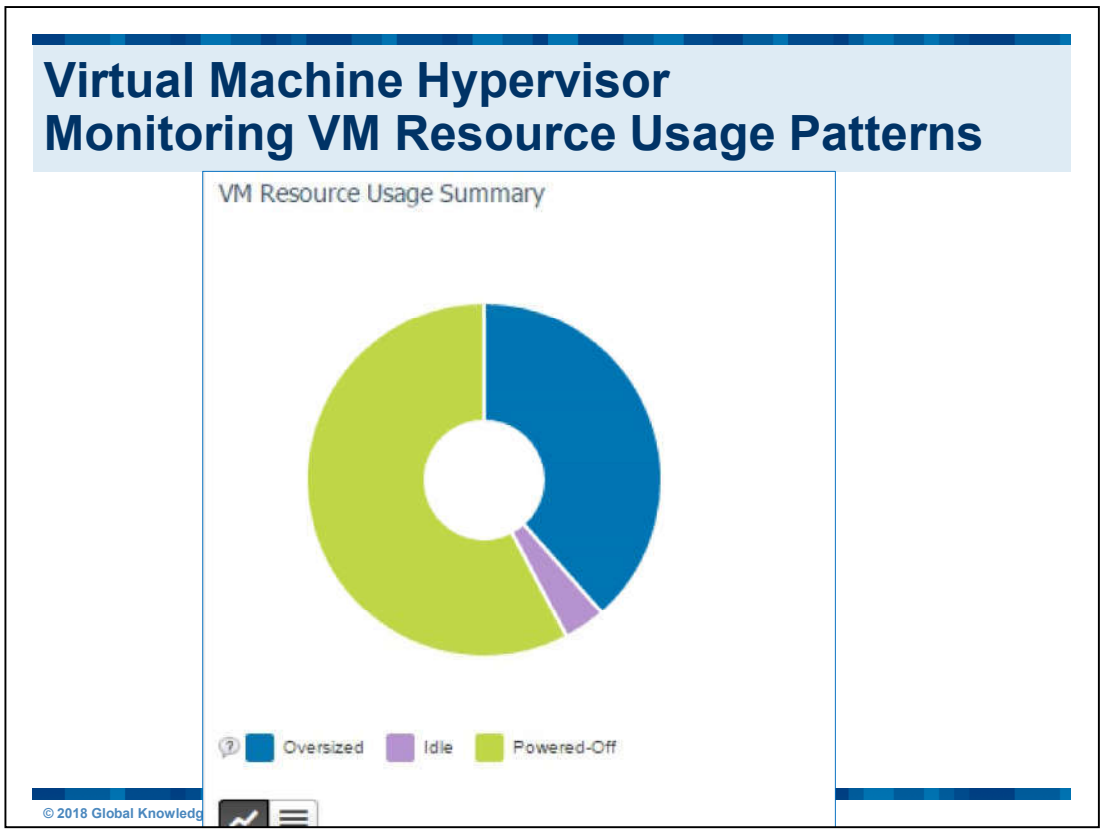


Monitoring Compute Resources and Resource Alarms

The **Compute Resource Summary** dashlet provides graphical and table views of the numbers of compute resource types that the system is managing and the alarms that the system is reporting for a resource type.

When monitoring data center virtual resources, the dashlets provide an effective way to see associated alarms, or take action to manage resources, as needed.

When a compute resource is reporting alarms, the chart associates the highest severity alarm indicator to the resource that is reporting the alarm. The screenshot below illustrates that one or more hosts and one or more virtual machines are reporting one or more minor alarms.



Monitoring VM Resource Usage Patterns

The VM Resource Usage Summary dashlet illustrates the distribution of oversized, idle, and powered off virtual machines. This information helps you determine whether virtual machines are running efficiently or need attention.

Oversized

Oversized virtual machines are consuming less than 30% of their allocated CPU and memory, which means that the machines have a large amount of resources allocated but might not be using them optimally.

Idle

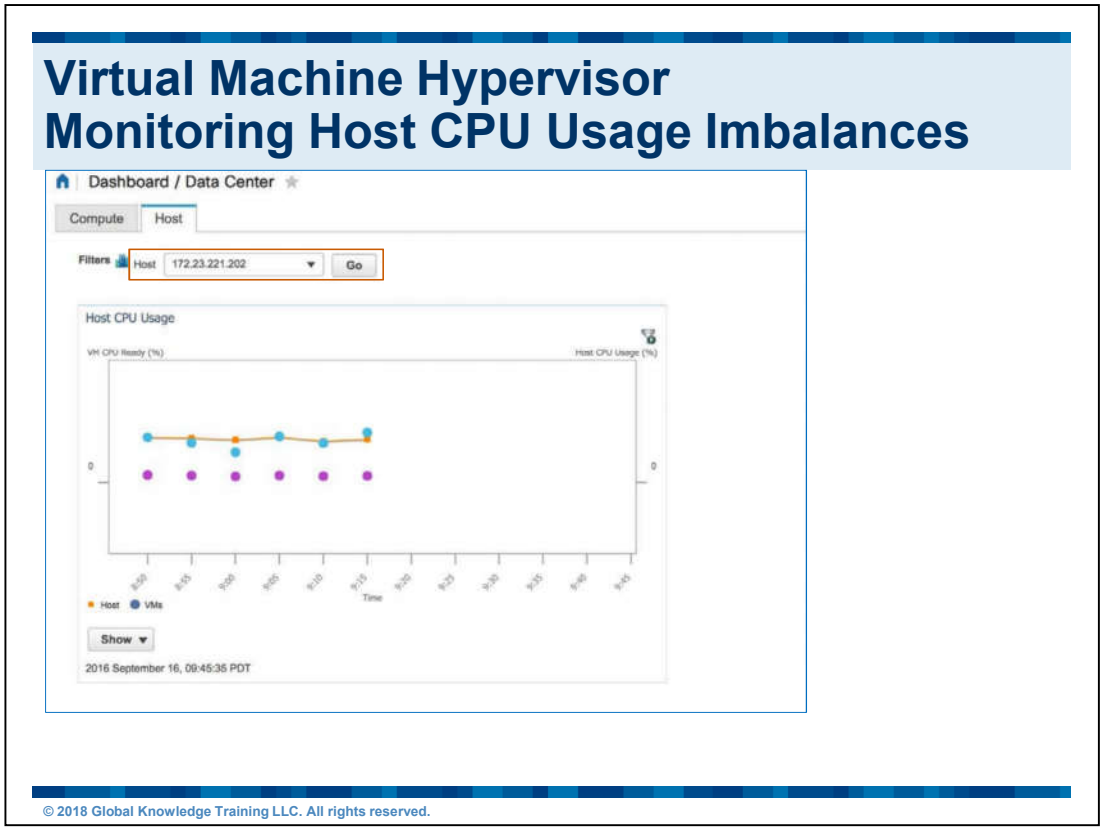
Idle virtual machines are consuming less than 1% of their allocated CPU and memory, which means that the machines are significantly underused.

Powered-Off

Those virtual machines that are not running.

Note: Virtual machines that are consuming more than 30% tend to be running most efficiently and are not reported in the dashlet.

You might consider removing significantly underused virtual machines or virtual machines that are powered off for long time periods from the system, which frees their resource allocations for other uses.

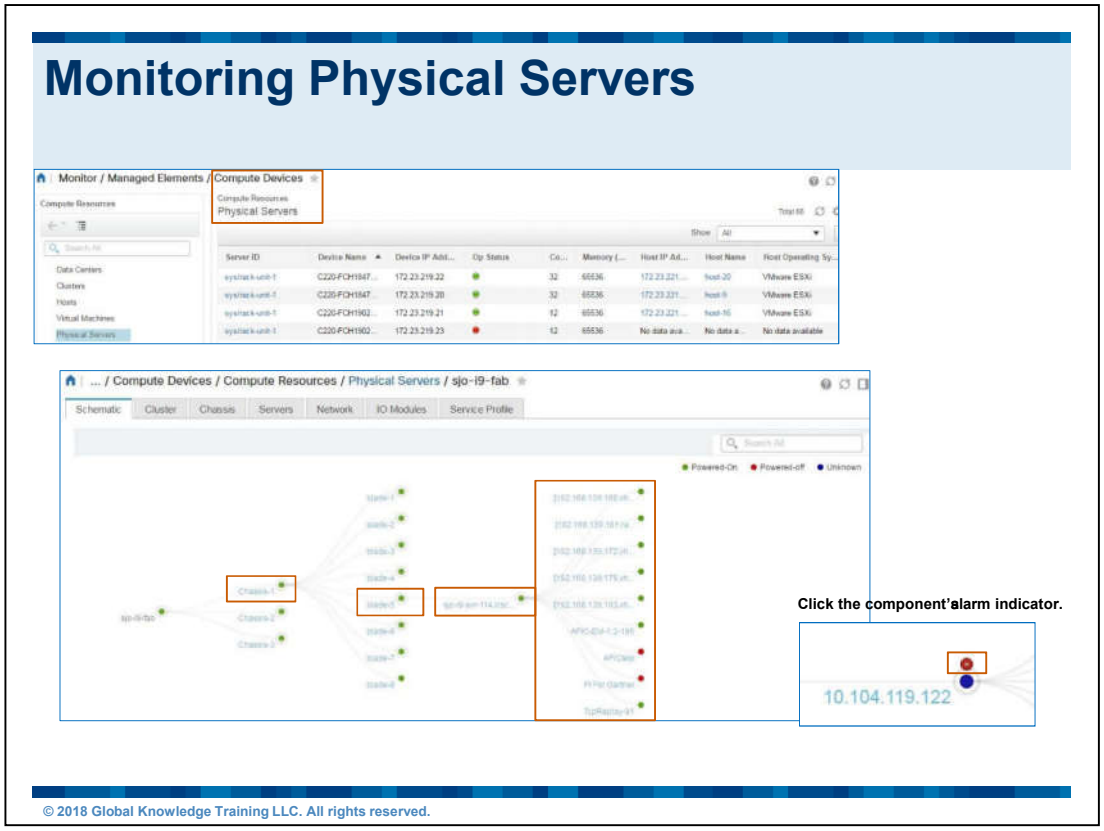


Monitoring Host CPU Usage Imbalances

For the host that you select in the Host drop-down list, the Host CPU Usage dashlet illustrates the percentages of the host CPU that the host is using compared to the percentage of host CPU that the associated virtual machines are using.

The screenshot below illustrates the host percentage in yellow color-coding. The color code of the percentage for each virtual machine varies so that the machines and host are all more easily identifiable.

When there many virtual machines running on a host, you can filter the list to show only the machines that you are evaluating.



Monitoring Physical Servers

The Physical Servers page lists the UCS B-Series and C-series physical servers, their resources, and the vCenter hypervisors that they are running.

Proactive monitoring of the physical servers is critical to help avoid operational disruption or downtime, such as issues that might affect the running of critical business applications.

You can use this page to monitor operational statuses and resource metrics.

failure, you can review detailed chassis, blade server, and fabric interconnect data for each server.

The types of information that you can evaluate include:

Schematic views.

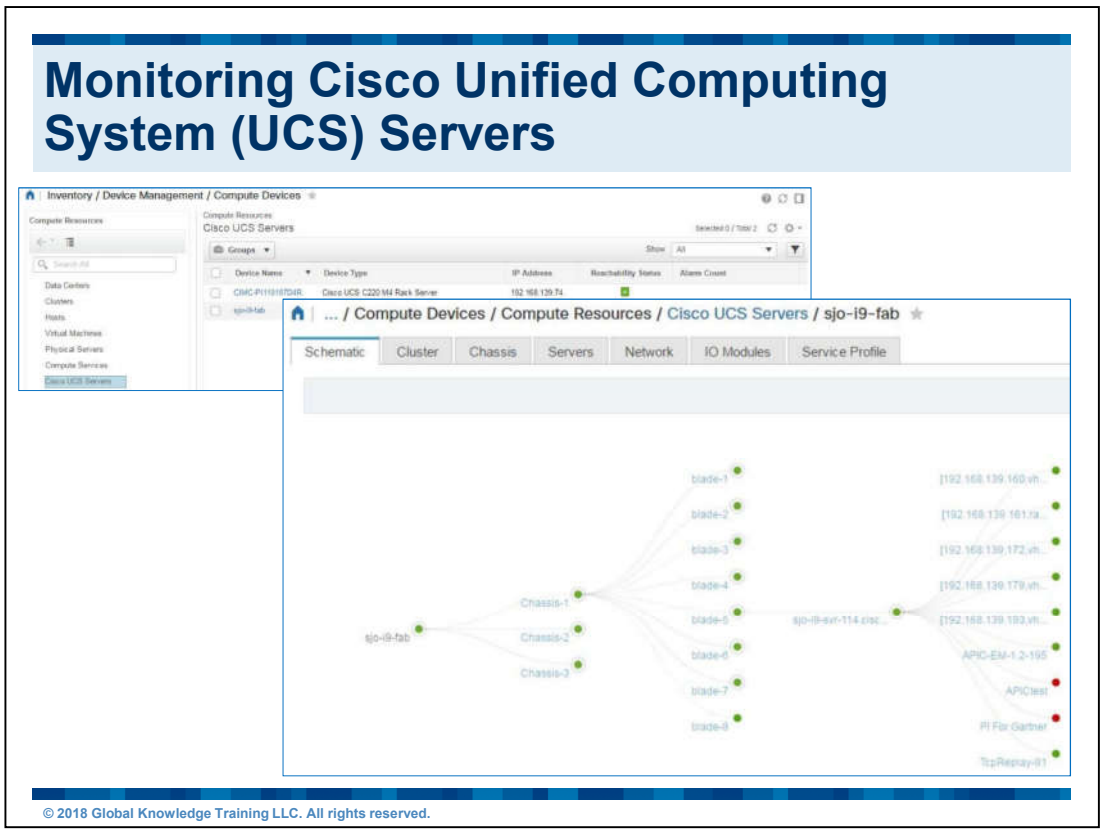
Chassis views with power supply unit and fan statuses.

Blade server memory capacities; adapter, network interface card (NIC), and host bus adapter (HBAs) operational statuses; and service profile associations and overall statuses.

Bandwidth usage on fabric interconnect ports.

When using schematic views, you can expand each dependent group of components to see where alarms might be occuring, and the dependent components that might be affected.

The screenshot below illustrates a fabric interconnect and the chassis that it is managing. Chassis 1 is expanded to display its blades, and blade 5 is expanded to display the associated host. The host is expanded to display its associated virtual machines.

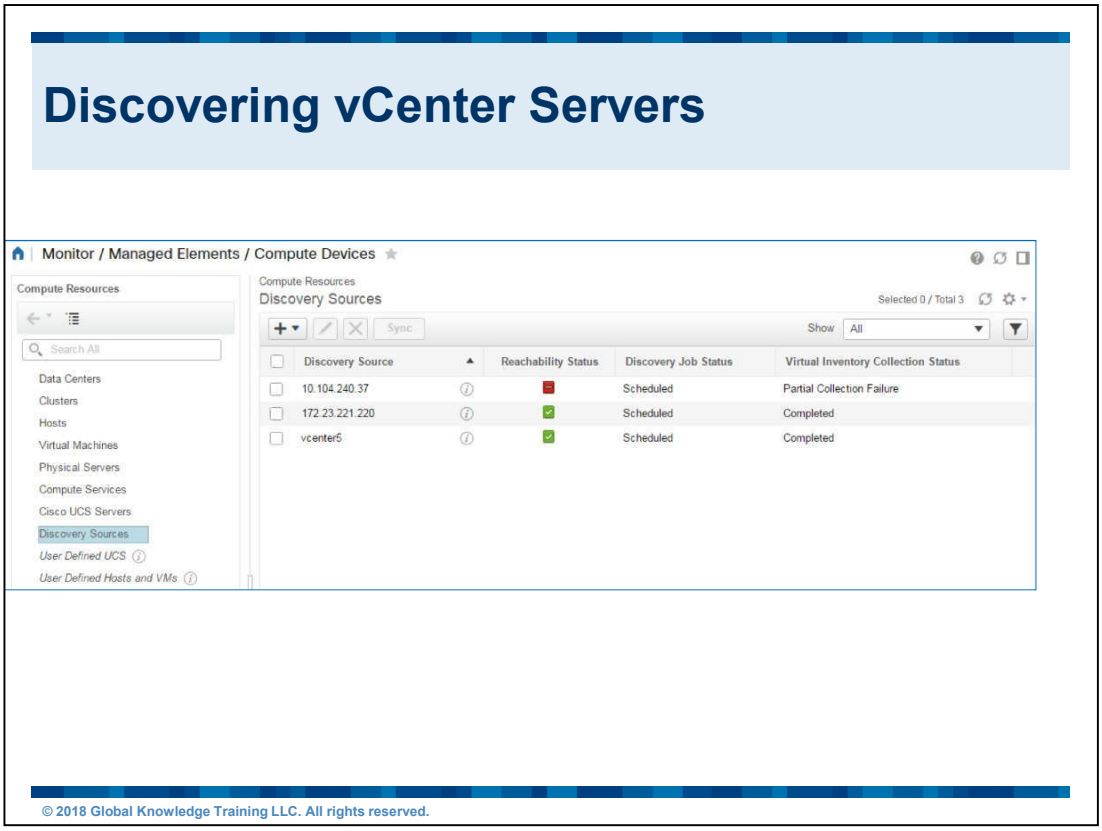


Monitoring Cisco Unified Computing System (UCS) Servers

The Cisco UCS Servers page lists C series standalone and UCS-E servers and the UCS fabric interconnects and reports reachability and any alarms that the hardware is reporting.

You can click a chassis Device Name link to open details about server components, such as component operational and administrative statuses, serial numbers and identifiers, and the service profiles that define the server's storage and networking characteristics.

This information helps you monitor the component level health of a server or fabric interconnect.



Discovering vCenter Servers

The discovery source process is the method by which Prime Infrastructure identifies the VMware vCenter servers on the network and enables data collection on the server components and resources, including all virtual machines.

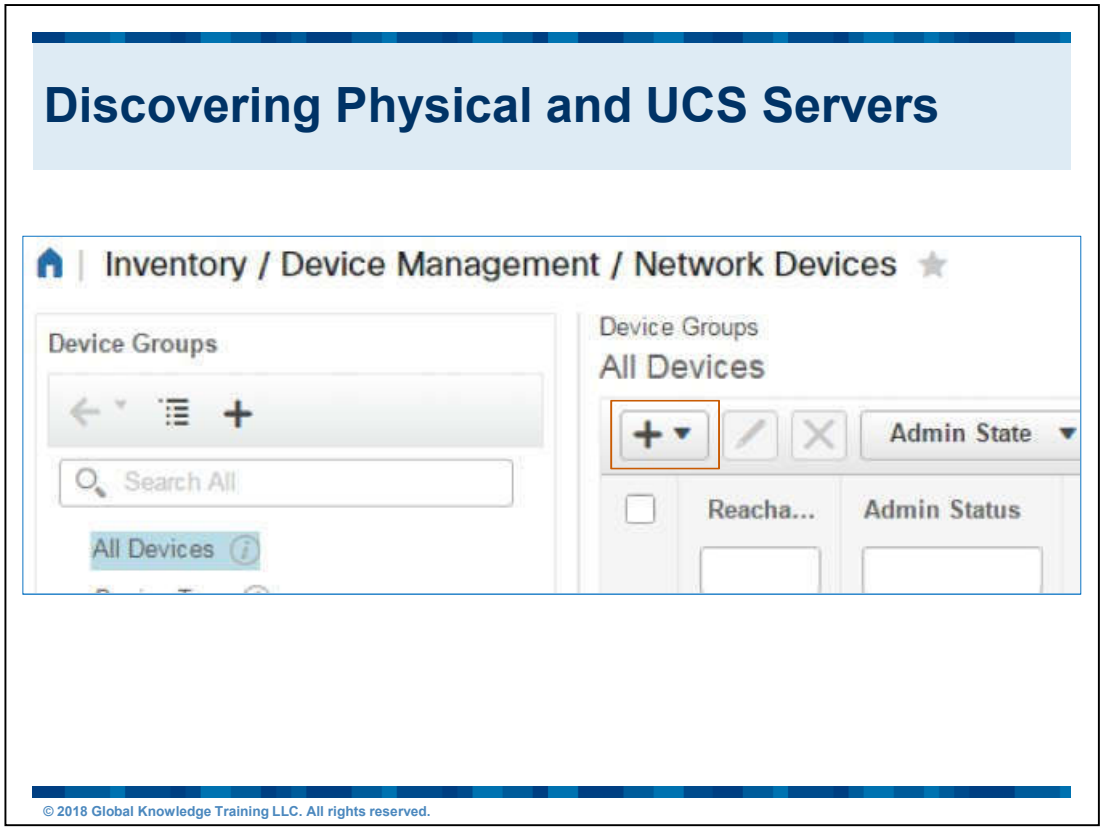
To add a vCenter server, on the Compute Devices page:

In Discovery Sources, click Add Device.

You can add servers individually or import them in bulk by using a .csv file.

When you add the vCenter server, the system starts the discovery process automatically and, when the process is complete, populates the hosts and virtual machine information on the Compute Devices pages.

After discovery, you can synchronize the compute resources inventory manually to help ensure that Prime Infrastructure is reporting current vCenter inventory.



Discovering Physical and UCS Servers

To identify and begin managing the physical and UCS servers, you perform the same discovery process that you do when adding other network devices.

To add a server, on the Network Devices page:

On the toolbar, click **Add Device**.

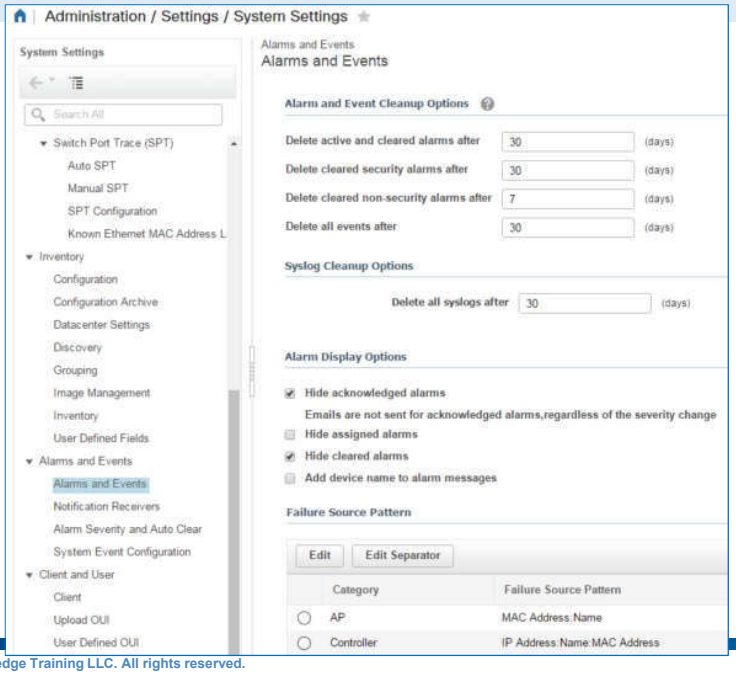
You can add servers individually or import them in bulk by using a .csv file.

When you add a UCS C series server, you need to provide the server's Cisco Integrated Management Controller (CIMC) IP address and the server's SNMP and CLI credentials.

When you add a UCS B series server, you need to provide the IP address of the primary fabric interconnect and the server's SNMP and CLI credentials. With this information, the system can discover all the UCS B Series servers that the fabric interconnect manages.


Global Knowledge
Module 07
Prime Infrastructure
Fault Monitoring Overview

Monitoring Faults



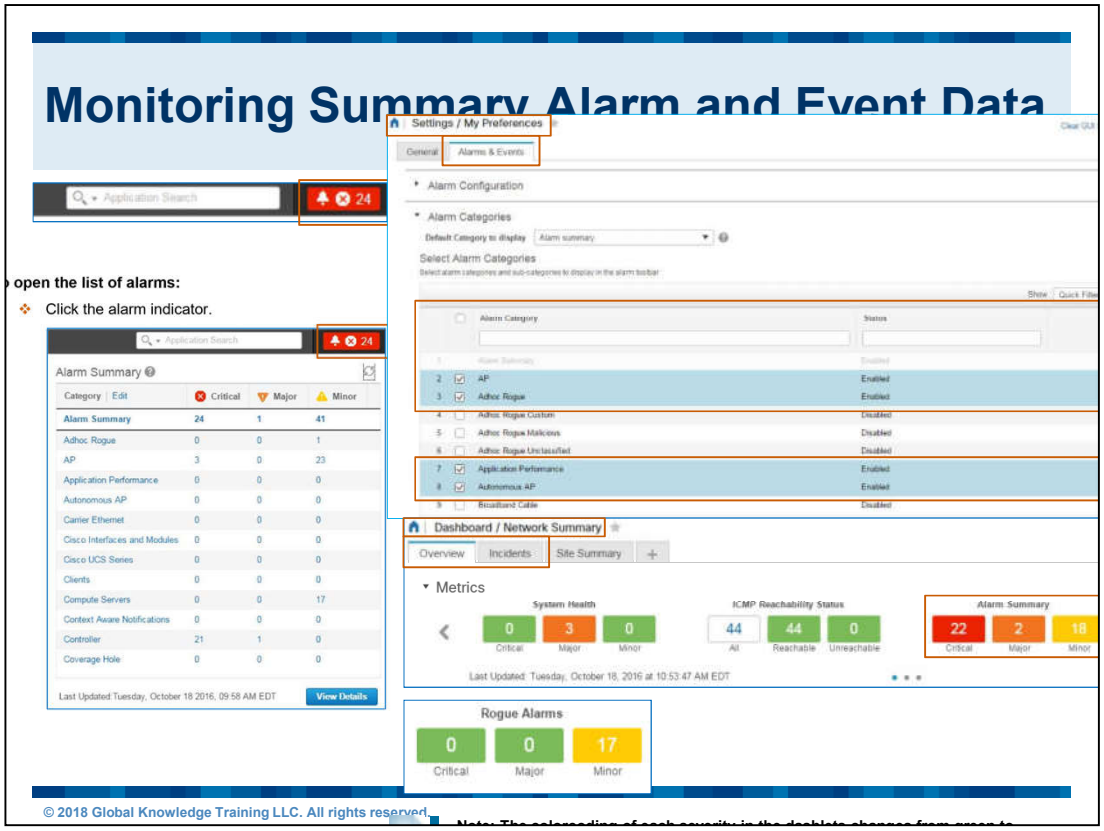
For all of the aspects of the system, Prime Infrastructure reports faults that might be affecting network accessibility, the user experience, or network performance. Network faults include errors, failures, or exceptional conditions on the network or its devices.

Fault monitoring includes collecting all of the syslog events, SNMP trap events, and systemgenerated events during device polling or when conditions prompt devices to send events to the system.

When conditions or series of events require more attention, for example, key performance indicator values moving outside of their operational thresholds, the system reports that information by using alarms.

Because conditions can return to acceptable, or normal, states without manual intervention, a situation might require more intensive monitoring only. Or, when you see more emergent situations, you can respond to alarms to help mitigate or avoid network issues or downtime.

Administrators configure back end alarm, event, and syslog reporting and clearing behaviors and severities in Administration.



Monitoring Summary Alarm and Event Data

Alarm and event reporting is a key method by which Prime Infrastructure alerts you to changing conditions on the network and its devices that might require additional monitoring or more immediate attention.

The system reports summary alarm and event information:

In the Alarm Summary list.

On metrics and dashboard dashlets.

Alarm, Event, and Syslog Summaries

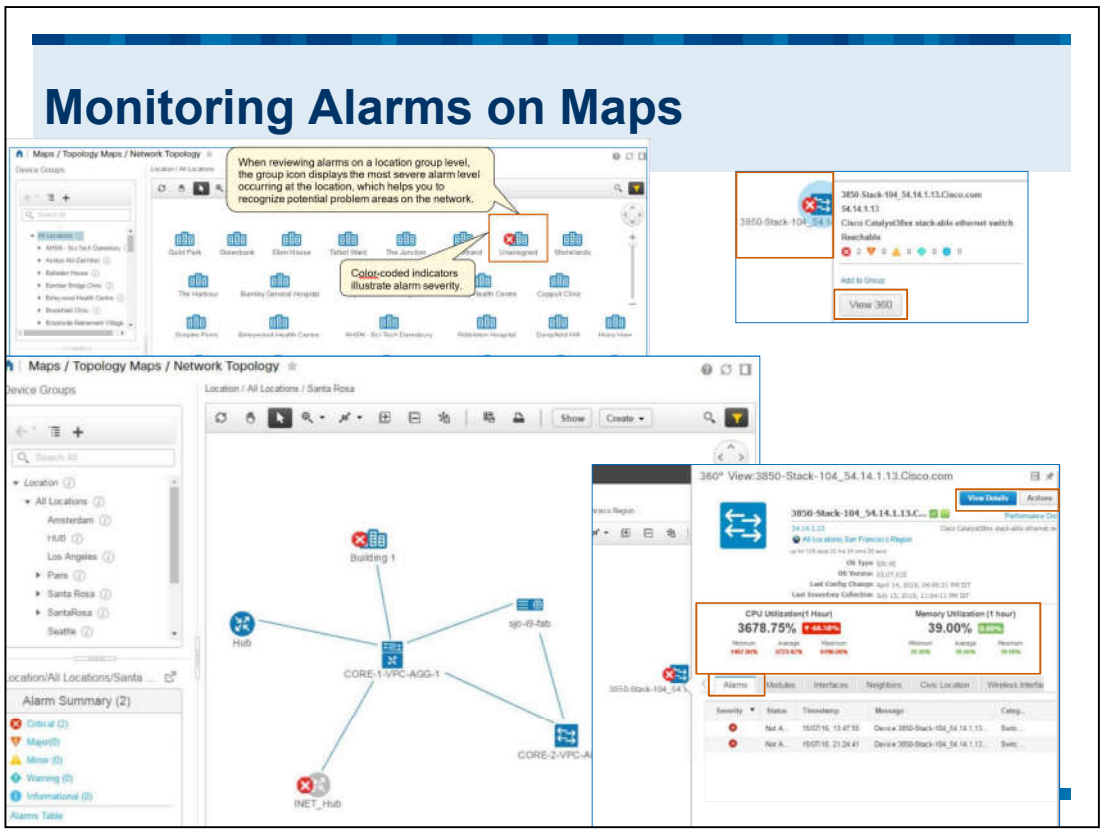
Application Banner Alarm Summary

To call attention to alarms that are occurring, the system provides an alarm indicator on the application banner.

The banner indicator displays the total number of alarms of the highest severity that are currently active for the categories that you enabled in your user preferences.

The list contains all of the alarm categories that you have enabled in your preferences and their

associated numbers of alarms based on severity level.



Monitoring Alarms on Maps

Wired Network Alarm Reporting on Topology Maps

Topology maps display alarms that are occurring on the wired portion of the network that the map represents and associates them to the devices or links that are generating the alarms.

On the network topology or data center map, to evaluate alarms that are occurring at a network location:

On the map, click the location icon, and then click Drill Down Group.

The map refreshes to display the devices at the location and their relationships to each other.

To evaluate the alarms that are occurring on a device:

On the map, click the device icon, and then click View 360.

The Alarms and Events page provides an alternate method for monitoring the network for potential issues, providing flexibility to monitor devices by:

Their types or locations.

Categories that system users have organized.

Various application areas, including dashboards and maps, provide navigation to the Alarms pages.

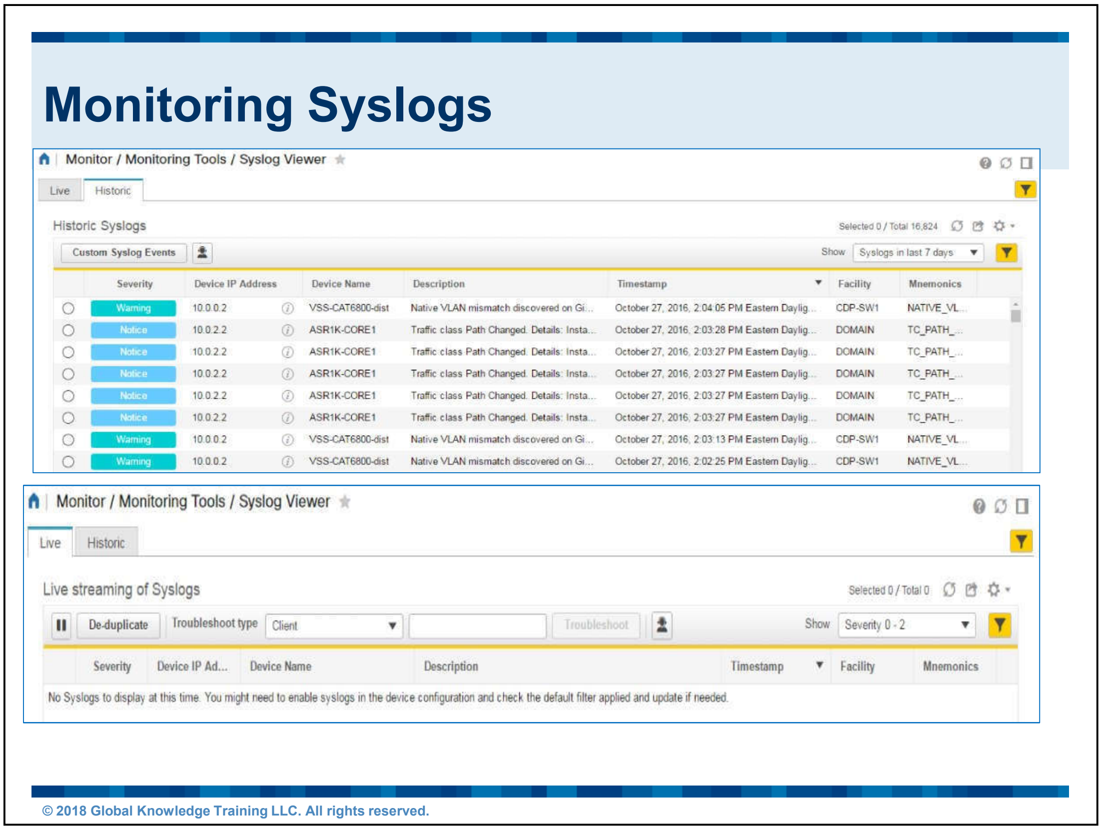
When you use that navigation, the system filters the list based on the category and type of alarm that you clicked to access the page.

When you begin working to resolve conditions causing an alarm, you can acknowledge the alarm, or assign it to yourself or someone else for further investigation.

To assign an alarm to yourself or another system user for monitoring, evaluation, or troubleshooting:

On the Alarms tab, select the alarm that requires attention, and then, in the Assign dropdown list, select the applicable assignment.

You also can define device groups to best support your monitoring tasks. For example, you might define a group that includes all of the devices that you monitor regularly.



Monitoring Syslogs

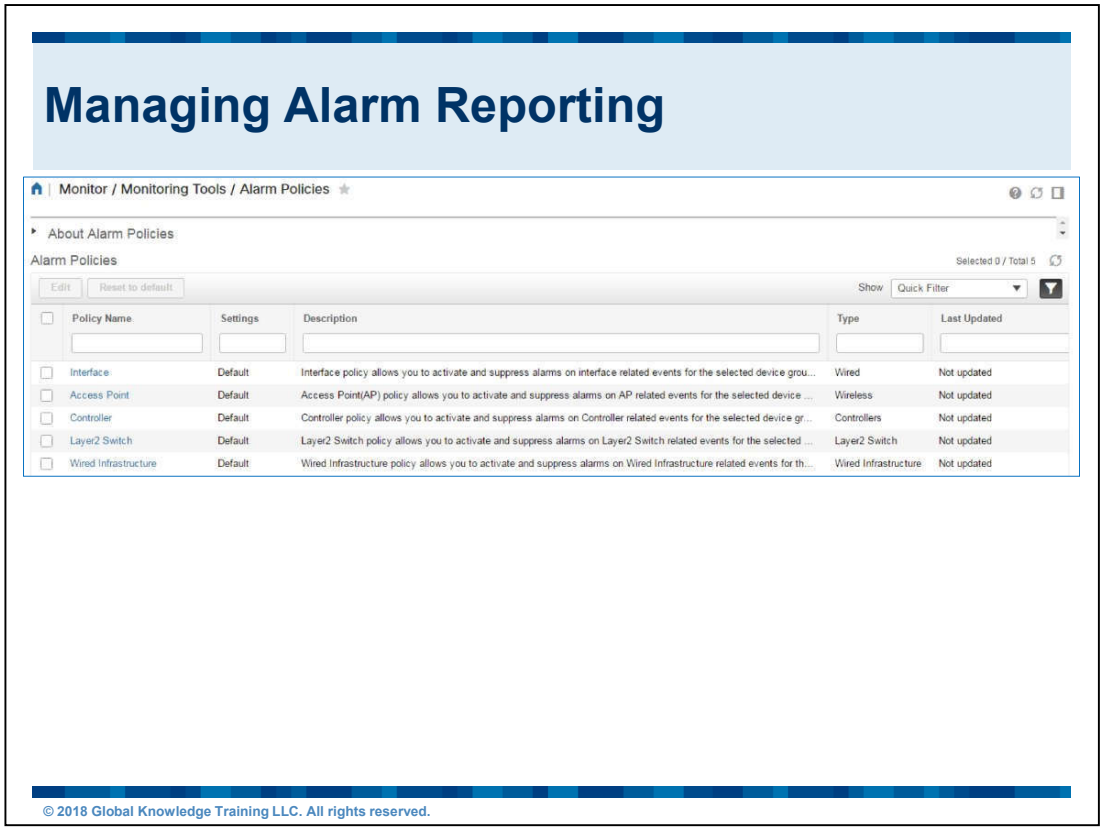
Overview

Devices generate syslog messages to report events and changes that are occurring on them. For certain device syslogs, Prime Infrastructure generates alarms by default.

In most cases, you need to use the syslog viewer to see all of the syslog messages that the system is receiving from devices. Monitoring incoming syslogs can help provide insight into device and network conditions in addition to those that are generating alarms.

You can review incoming syslogs on the **Syslog Viewer** page, which color codes message severity levels.

On the **Historic** tab, you can review asynchronous syslogs that the system captures when device events or changes occur.



Managing Alarm Reporting

Overview

Prime Infrastructure identifies changing network conditions by collecting and evaluating events from network devices. When these events indicate conditions that are falling outside of operational thresholds, the system generates alarms in varying severities to bring attention to these situations.

To manage the alarms that the system reports, Prime Infrastructure provides default alarm policies associated with specific device types or components. These policies manage the types and severities of events that generate alarms and apply to device or port groups that system users can configure.

Note: Administrators can configure global settings that control back end alarm behaviors, such as the time intervals in which the system clears or drops alarms, or alarm display behaviors.

Alarm policies are a separate mechanism that allows you to control whether the system reports or suppresses specific alarms based on device type and device or port group, and applies to all areas of the application that report alarms.

Alarm policies report events that are occurring on the following device components or types:

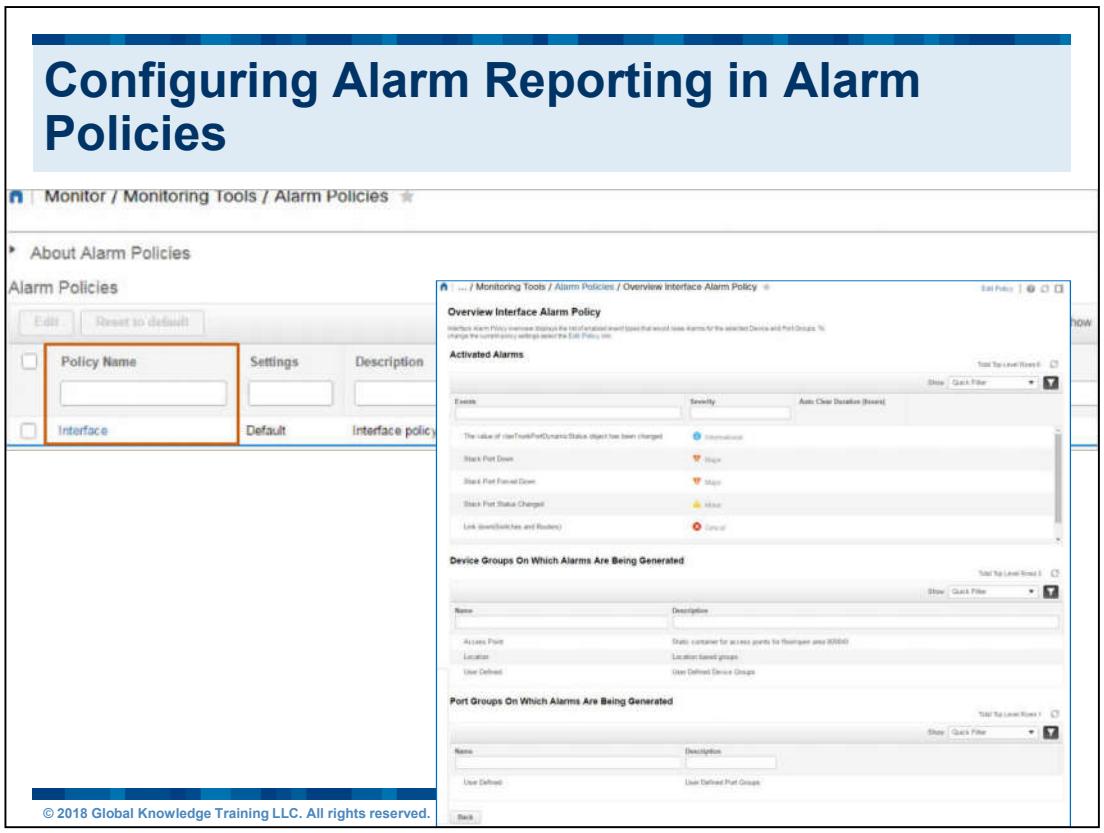
Device interfaces

Wireless access points

Wireless LAN controllers

Layer 2 switches

Wired infrastructure, which reports alarms related to physical component conditions, such as environment temperatures or fan conditions



Configuring Alarm Reporting in Alarm Policies

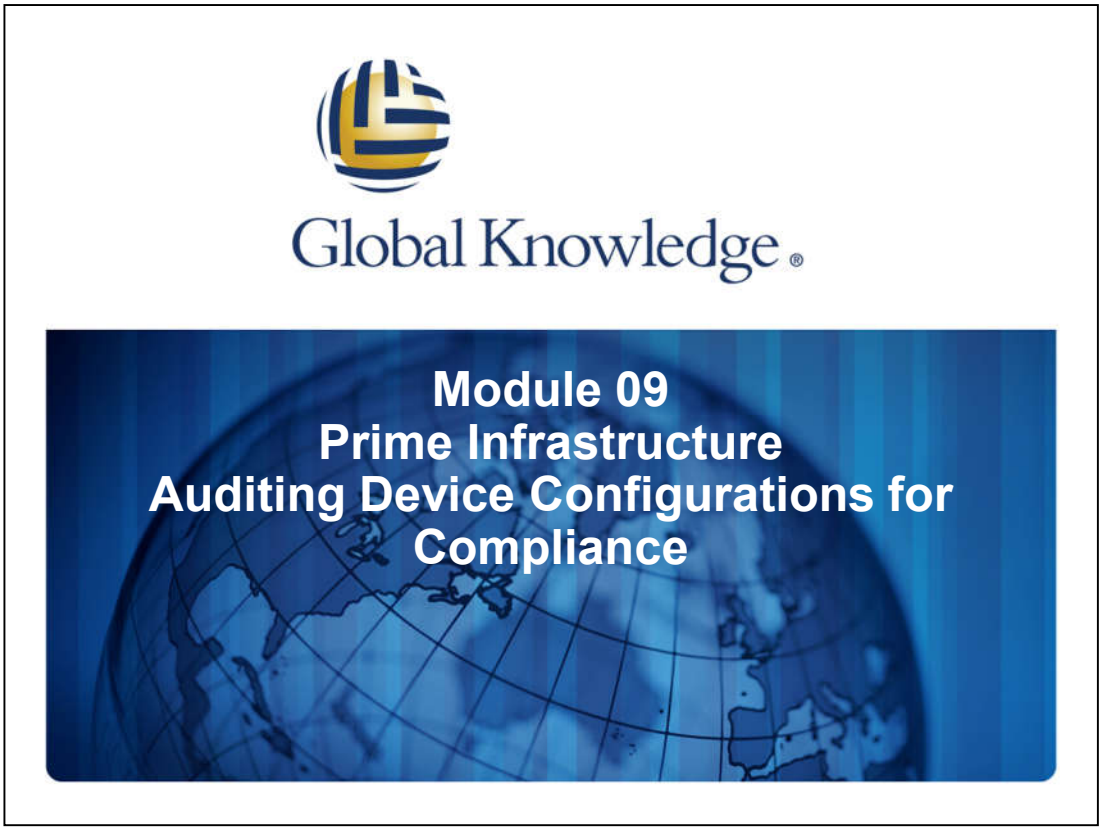
You can review alarm policy details to determine whether you want to make any changes.

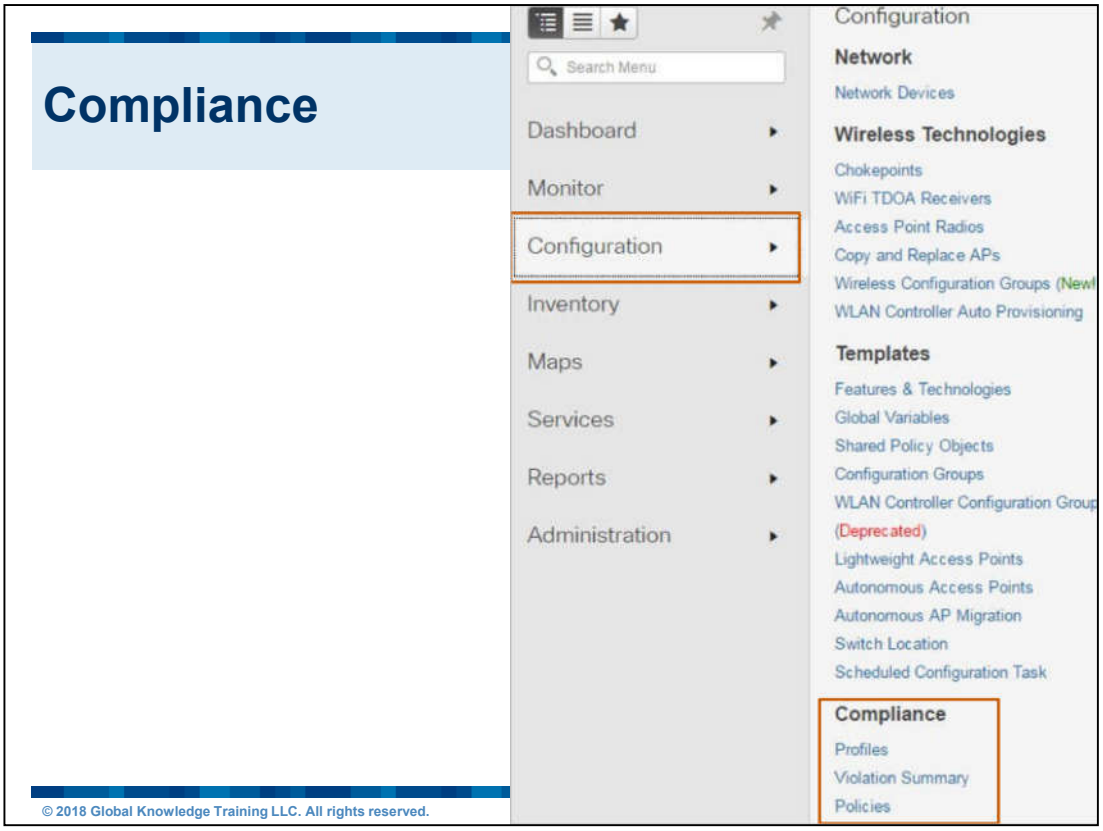
To review alarm policy details:

The policy overview lists:

The events included in the policy and the alarm severity level assigned to each event.

The device or port groups, depending on the policy type, for which the system will generate alarms.


Global Knowledge
Module 09
Prime Infrastructure
Auditing Device Configurations for Compliance



Prime Infrastructure provides compliance features that you can use to perform audits that determine whether devices have configurations that are not compliant with network requirements.

This information helps you to ensure that the network is running securely and as expected.

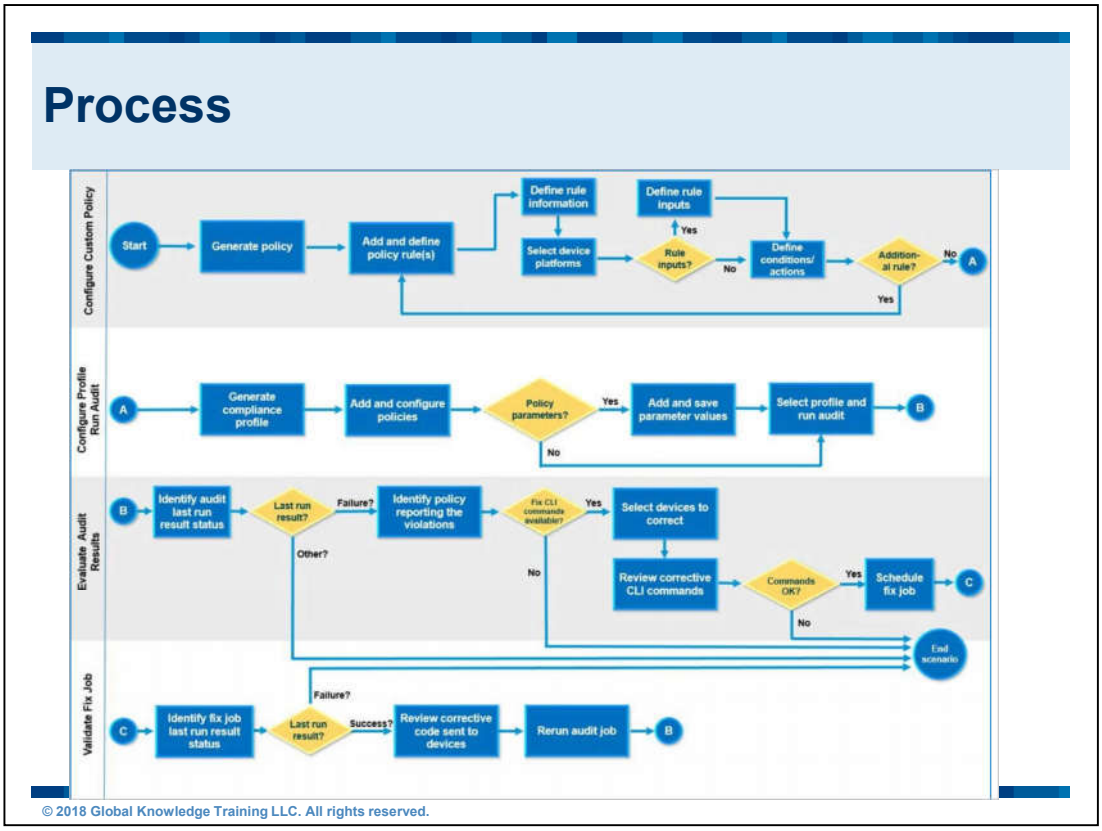
Note: To have the compliance functionality available, an administrator needs to enable the compliance service in the system settings, and then log out and back in to Prime Infrastructure.

For more information on enabling compliance functionality, refer to the FAQ.

The compliance functionality that administrators use to configure policies and network operators use to run audits is available on the Configuration menu, including:

Defining custom compliance policies, as needed.

Network operators also review the audit results, which run as jobs in the system.

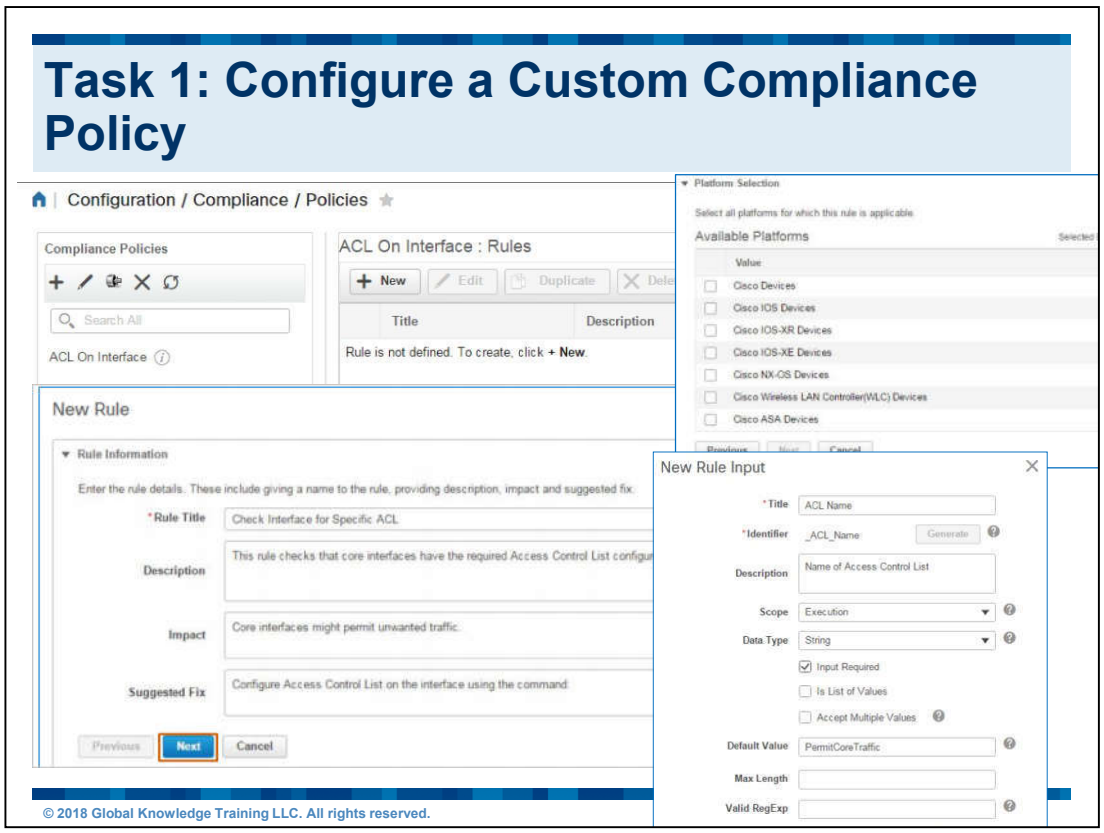


Process Overview

To audit device configurations:

1. Configure a custom compliance policy, as needed, and then define and add policy rules.
2. Configure the compliance profile, including custom and system-provided policies.
3. Run the compliance audit.
4. Evaluate the audit results to determine whether device configurations are compliant with the policy or policies included in the profile.
5. Based on audit results, make corrections, as needed, by running a fix job.
6. After running a fix job, validate that the corrections are successful and the audited devices indicate compliance.

0.



Configuring a compliance policy can include:

Defining the device platforms that the policy can evaluate and on which it can run fix jobs.

Adding placeholder rule inputs that allow users to define auditing values.

Defining conditions to evaluate on the devices and whether the system reports those conditions

Defining CLI commands that can correct conditions that do not comply with the audit definitions.

To determine whether core router and switch device interfaces have Access Control Lists in place to recognize and reject unauthorized traffic, you, as the network administrator, configure a custom compliance policy.

Follow the subtasks and steps below.

Subtask 1: Add the Policy Placeholder

1. On the Configuration menu, navigate to and open the Compliance | Policies page.
2. On the Policies page, in the Compliance Policies list, click Create Compliance Policy

3. In the Create Compliance Policy dialog box, in the Title field, type a straightforward policy name.

Note: The field name requires alphanumeric formatting and can include underscores or symbols.

Example: Policy Name_1(

4. In the Description field, type a brief explanation of the use of the policy, and then click Create.

5. To add and configure rules to the policy, go to subtask 2.

The policy is now available to add rules.

Important Note: Compliance policies must include one rule and can include as many rules as you need to perform a specific audit.

The system does not retain the policy placeholder until you add and save at least one rule to the policy.

0.

Subtask 2: Configure the Policy Rules

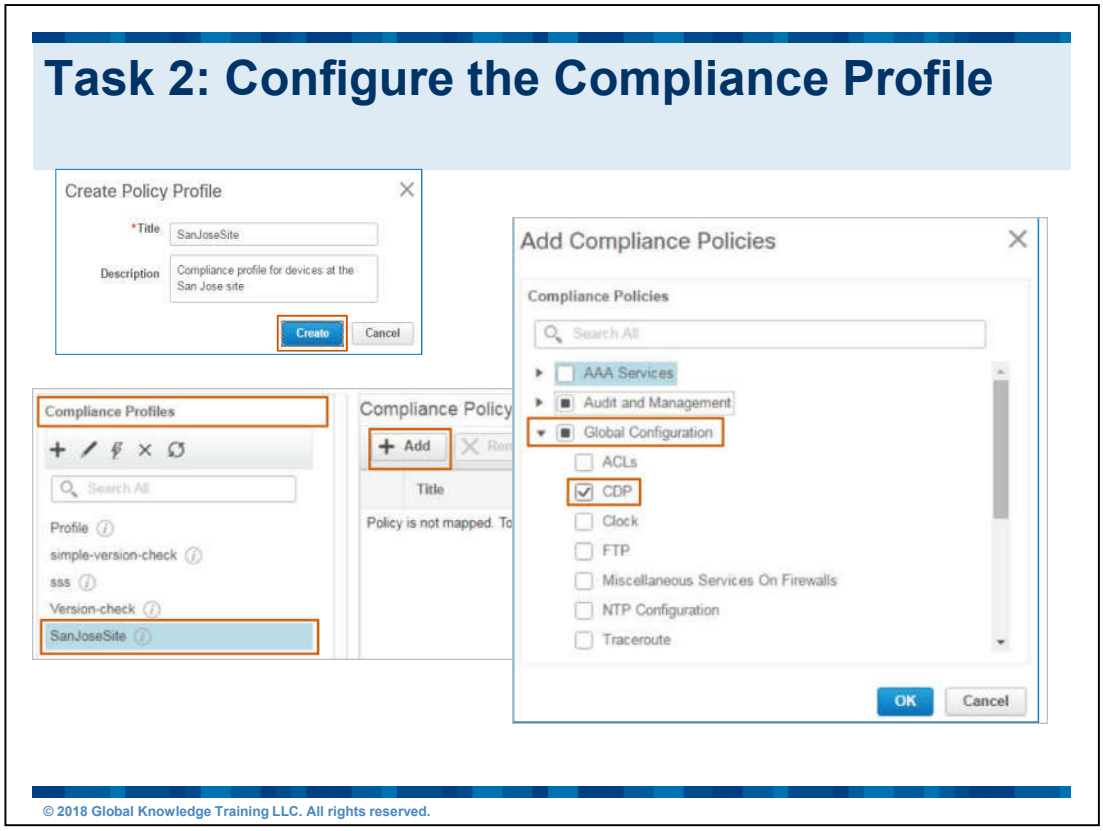
With the policy generated, you, as the network administrator, need to add the rule that defines the auditing, reporting, and correction parameters, including:

Identifying core router and switch device interfaces with IP addresses.

Auditing whether their configurations include the ACL, and on those interfaces that do, auditing whether the ACL is configured.

Raising violations for configurations in which the ACL is not configured on the interface and providing the CLI code that corrects it.

Raising violations for configurations in which the ACL itself is not configured and providing the CLI code that corrects it.



You, as the network operator, need to perform a security audit on network interfaces. You want to configure a profile that performs the security validation that you need in a single audit job.

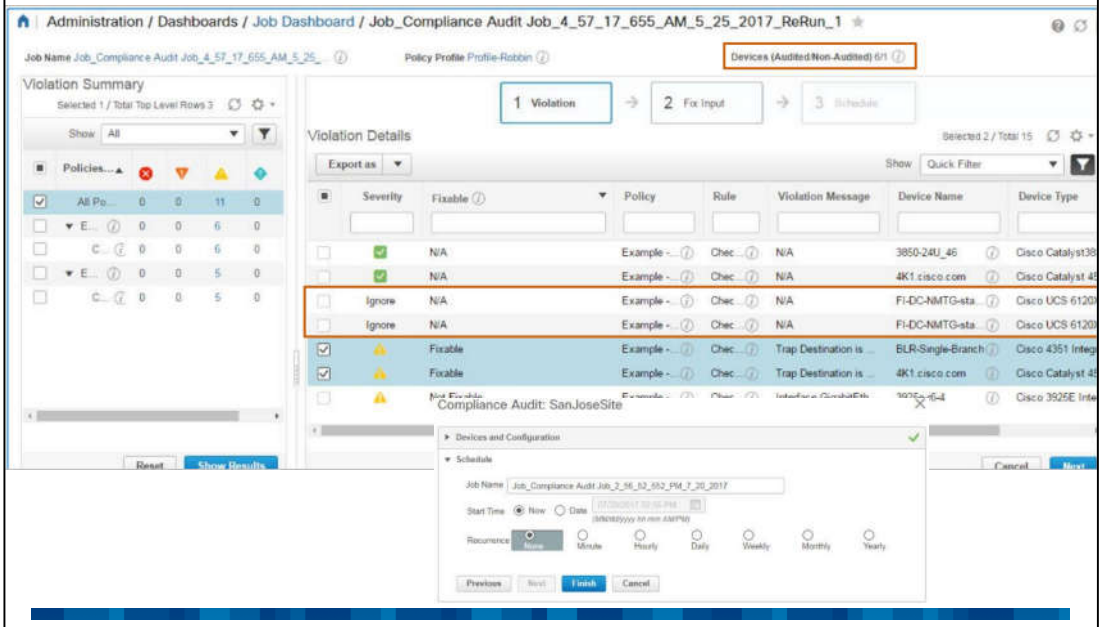
To do so, you configure a profile that includes:

The custom **ACL On Interface** policy, which audits whether device interface configurations include a specific Access Control List and that the list is configured on the interface.

The system-provided **CDP** policy, which audits whether the Cisco Discovery Protocol is disabled on the device, and if enabled, reports a violation.

The system-provided **Host Name** policy, which audits whether each device has a host name, and if not, reports a violation.

Task 3: Run the Compliance Audit

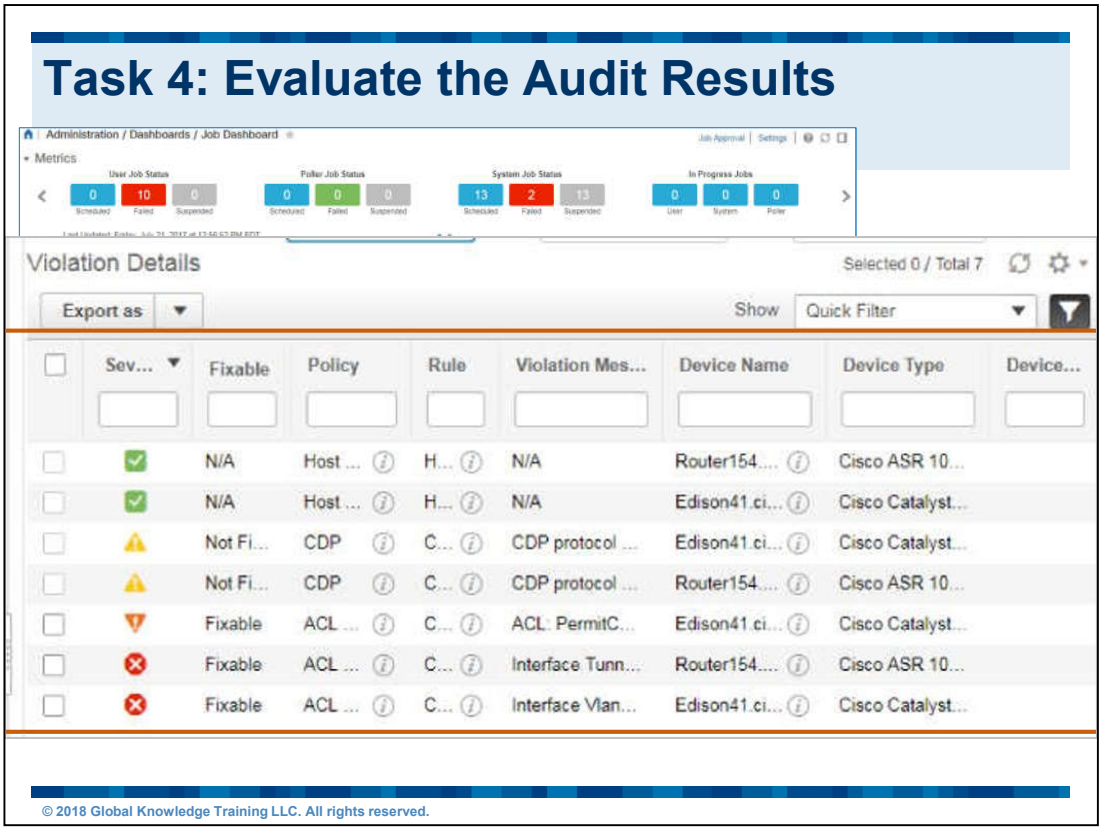


With the policy configured, you run compliance audit. This function is available on the **Profiles** page.

To run the compliance audit:

On the **Compliance | Profiles** page, in the **Compliance Profiles** list, select the profile that you want the audit to run.

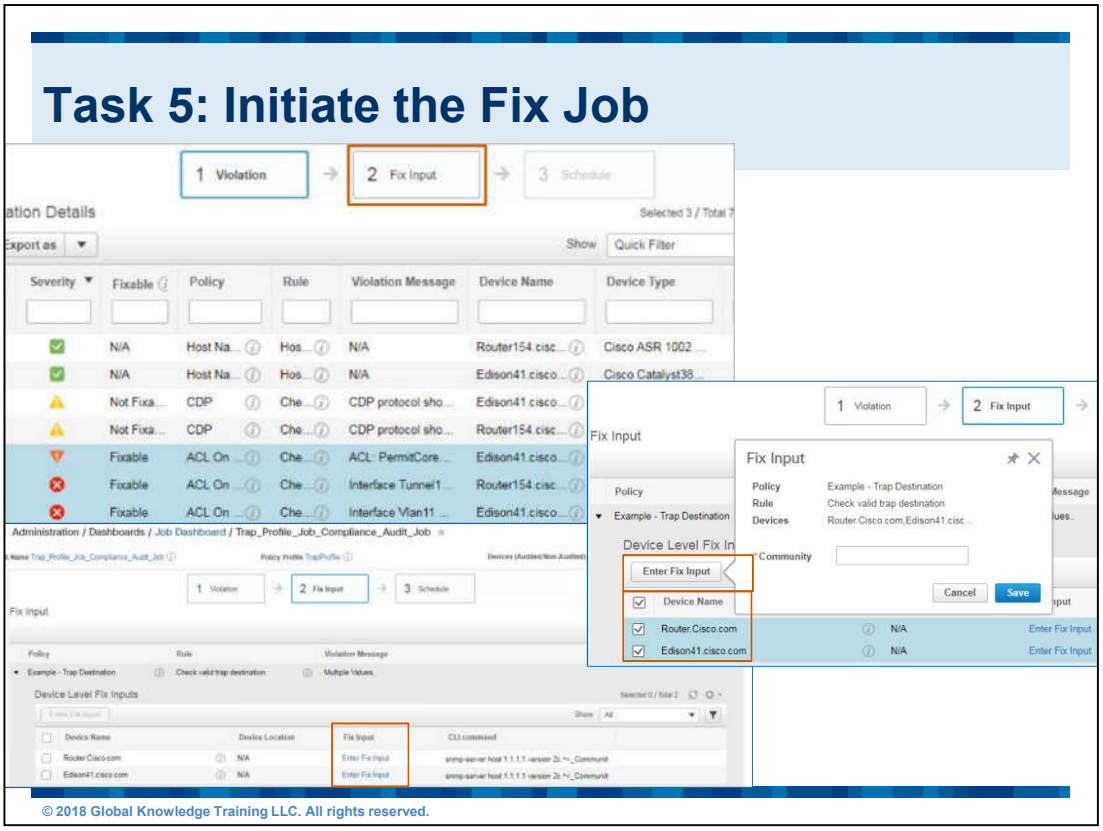
On the toolbar, click **Run Compliance Audit**.



When you evaluate a running job immediately by clicking the job name link in the system message at the end of task 3, the system navigates you to a **Job Dashboard** page in **Administration** that indicates the running job.

When the same job has been run previously, it lists up to 5 of the most recent jobs and their statuses.

When you run audit jobs that you want to evaluate at a later time, you can navigate to the **Job Dashboard** page in **Administration**.

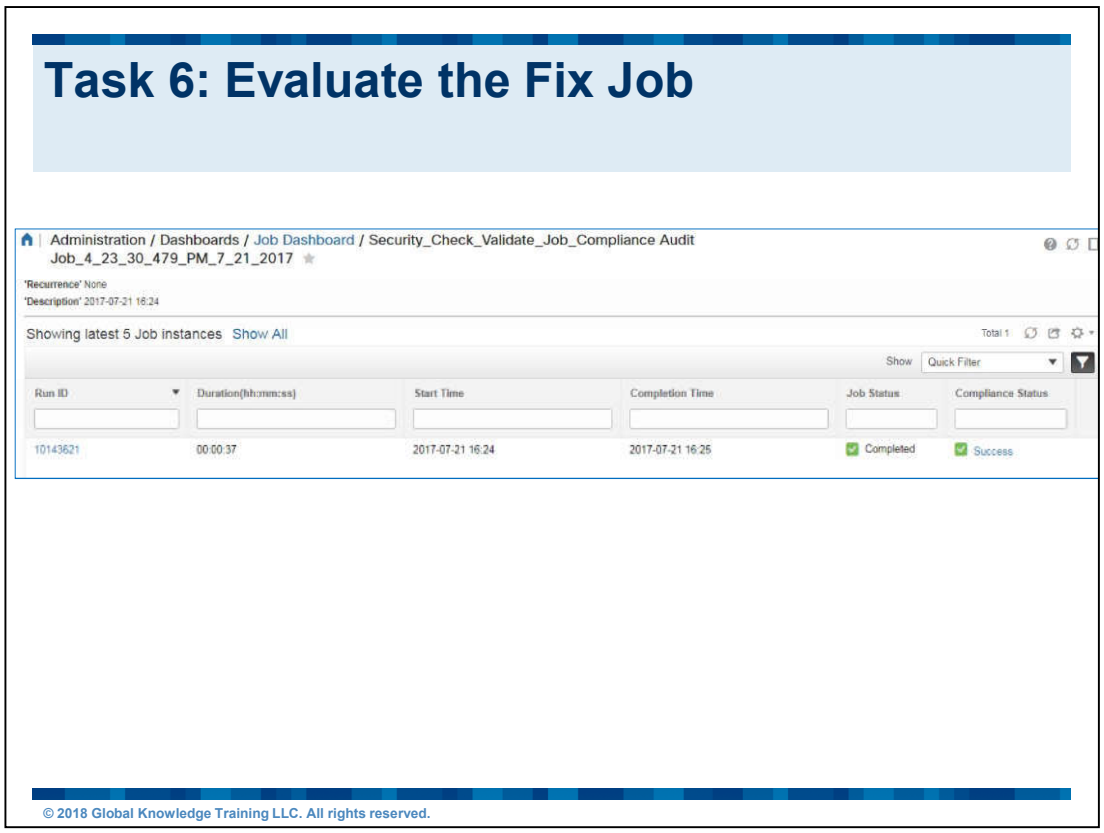


To run the fix job, you select each device that indicates that the compliance issue is fixable. You remain on the job's detailed page to initiate the fix job.

To initiate the fix job, follow these steps:

In the **Violation Details** select each device on which you want to run the fix job.

The **Fix Input** and **Next** button becomes available.



Task 6: Evaluate the Fix Job

The system monitors fix jobs and reports their results on the **Job Dashboard** page. The validation process includes:

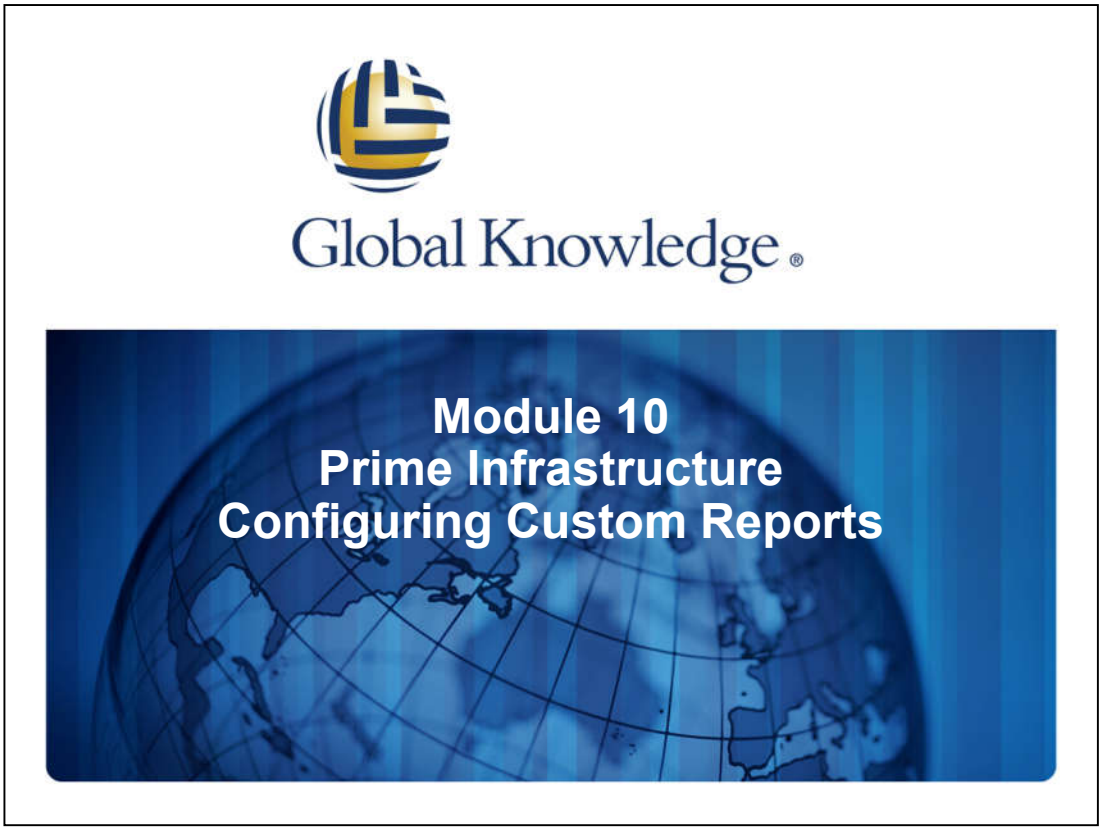
On the **Job Dashboard** page, validating that the fix job is successful.

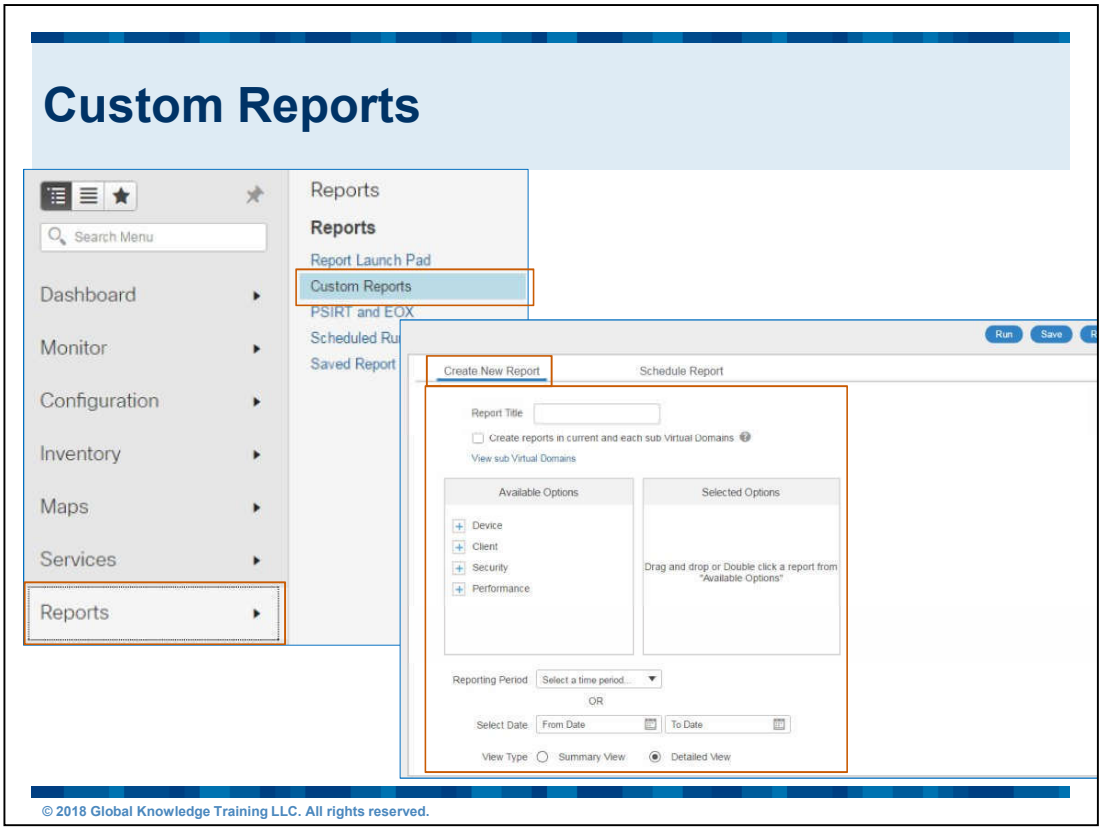
On the **Compliance | Profiles** page, rerunning the audit job and validate that the policy reporting violations is now reporting success.

0.

When you schedule a fix job, the system opens the **Compliance Jobs** dashboard page and a system message opens confirming whether the system scheduled the job.

Since, in this case, the job is running immediately, the entry indicates the running status in the **Last Run Status** field.


Global Knowledge
Module 10
Prime Infrastructure
Configuring Custom Reports



Introduction

To streamline custom report configuration, Prime Infrastructure provides the Custom Reports feature for several report categories, including:

Device

Client

Security

Performance

When you select a report or reports from one or more categories, the associated attributes and metrics included in each report are available for selection. Then, you can select the specific attributes or metrics that you need in the report and organize where the data appear in the report layout.

Note: For users familiar with the capability to customize reports that they access on the **Report Launch Pad**, this feature uses similar functionality.

You can find customization capabilities for additional report categories and types on the **Report Launch Pad**.

Based on the type of data that you select, reports can include tabular data, graphical data, such as pie or bar charts, or both types of data.

You also can control the virtual domain or any sub-domains in which users can access and generate the report.

This job introduces you to the process to configure and generate reports by using the **Custom**

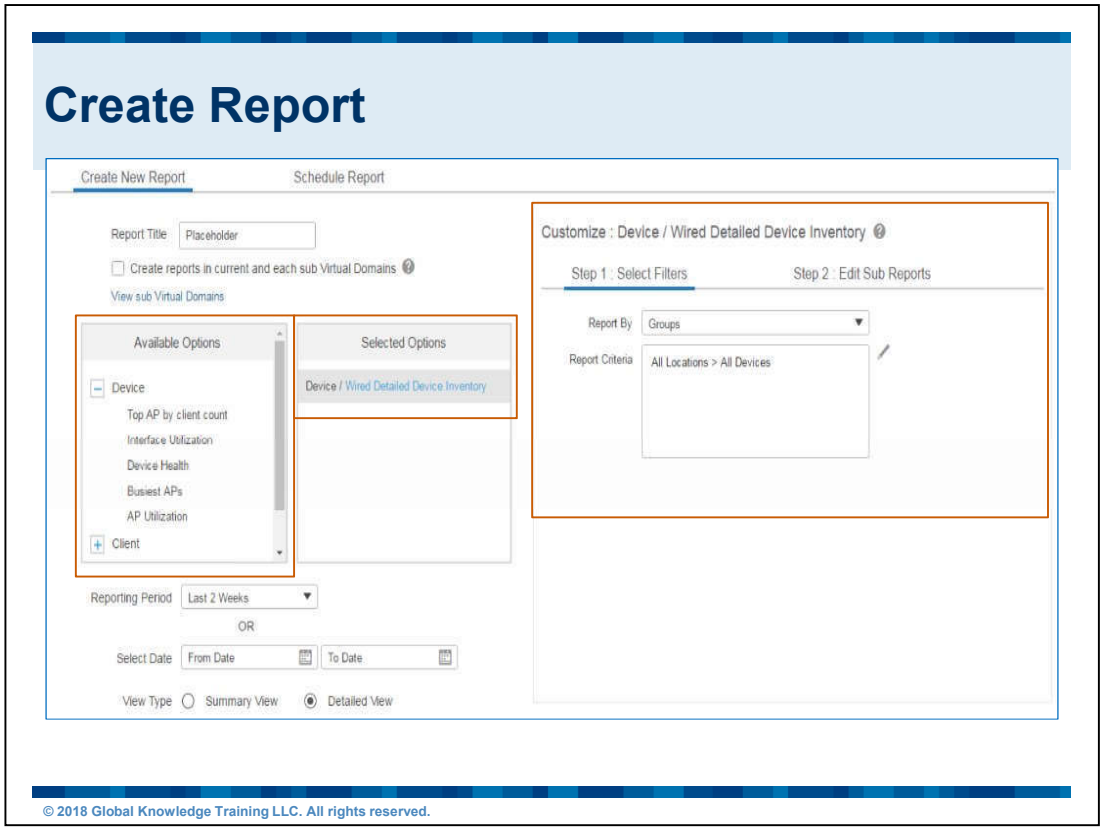
Reports feature.

Tip: To generate effective custom reports, familiarize yourself with the contents of the reports that you plan to use.

That way, you can locate and select the specific data that you want efficiently when selecting report criteria.

Custom Reports Features and Layout

Custom reports provides a more streamlined process for generating custom reports. You access custom reports on the **Reports** menu.

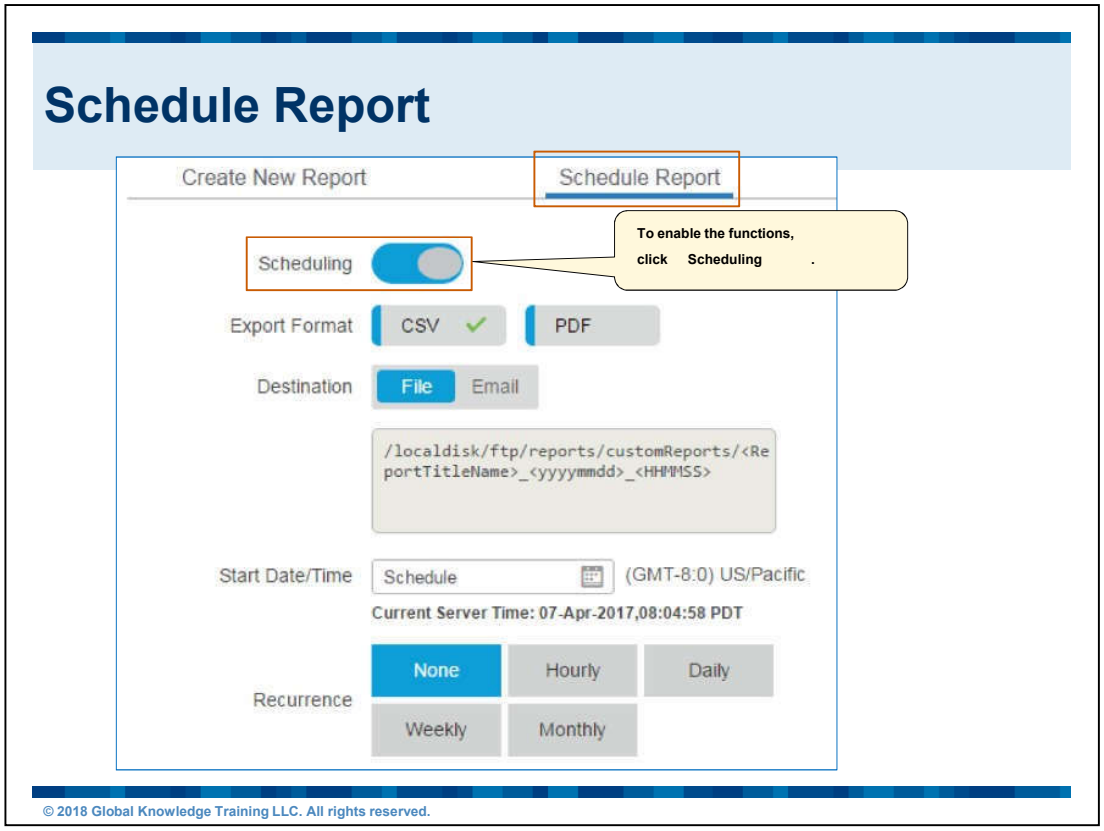


Custom Reports Features and Layout

Custom reports provides a more streamlined process for generating custom reports. You access custom reports on the Reports menu.

You select the reports, reporting period, and report type on the Create New Report tab.

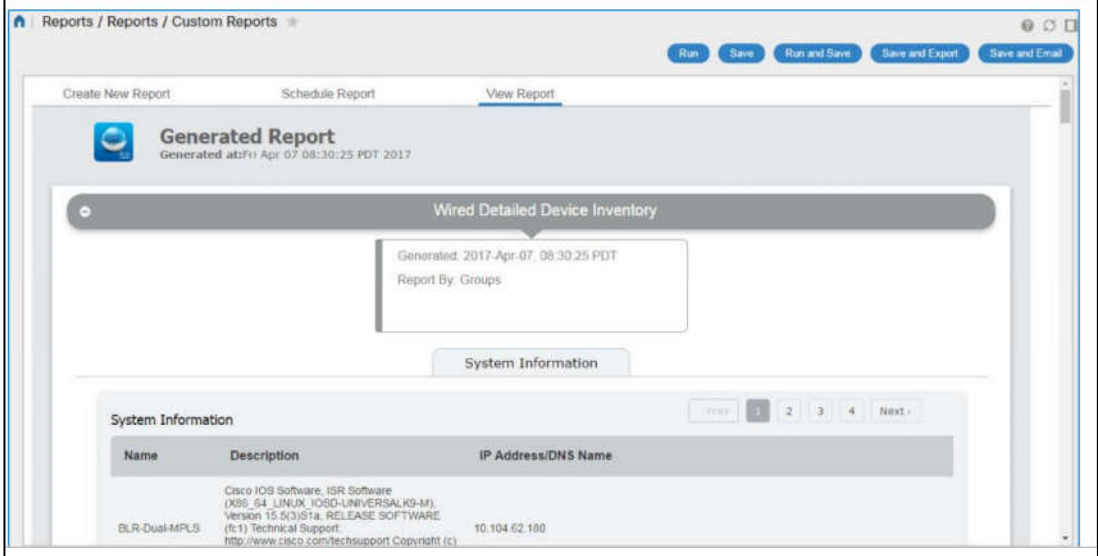
When you expand a report category, and select one or more reports, options to select report filters and details become available.



You configure report schedules, including recurrences, when needed, on the Schedule Report.

To generate or run reports on following a schedule or on an on-demand basis, after you configure the report, you use the toolbar buttons.

View Report



When you generate a report on demand by using the Run or Run and Save buttons on the toolbar, the system opens and navigates you to the View Report tab.

Important Note: If you need to retain the report after running it, click Run