Wireless Network Summary Data Overview

Cisco© Prime Infrastructure 3.1

Job Aid

Copyright Page

Wireless Network Summary Data Overview Job Aid

Contents

Basics **1**
Overview 1
Introduction 1
Skills 1
Network Operator 1
Proficient to Expert *1*
Terms 2
Security Index Score (wireless reporting) 2
Monitoring Summary Wireless Network Data **3**
Summary Data Dashboards 3
Introduction 3
Managing Data Reporting Time Periods *5*
Managing Dashlet Settings and Defining Top N Reporting *6*
Adding Dashboards and Dashlets for Flexible Monitoring *8*
Network Summary Metrics and Aggregate Dashlets 9
Network Summary Metrics Dashlets 9
Network Summary Aggregate Dashlets 10
AP Radio Coverage Status by Site *10*
The Number of Clients Associated To or Authenticated On the Network *11*
Clients or Network Users Generating the Highest Traffic Rates or Volumes *13*
Wireless-Specific Summary Dashlets 14
General Security Monitoring Dashlets *14*
Rogue Access Point Monitoring Dashlets *15*
Adaptive Wireless Intrusion Prevention System (wIPS) Monitoring Dashlets *18*
Security Events and Attacks Monitoring Dashlets *19*
Wireless Mesh Network-Related Data *20*
CleanAir Technology-Related Data *21*
Alarm, Event, and Syslog Data 23
General Summary Data *23*
Mesh Alarms Data *24*
Data Summarized by Site 24
Device 360^0 Views 25
Overview 25
Access to Performance Graphs 28
Access to Access Point (AP) Radio Details 30
Wireless Site Maps 32
Overview 32
Generating Maps Automatically 36
Links **37**
To Product Information 37

To Training 37
To Contact Us..... 37

Basics

Overview

Introduction

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

Tool types include:

- **Dashboards**
  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
- **360^0 View pop-up windows**
  Device- and interface-specific pop-up windows that contain significant amounts of device-information, including listing alarms and providing information about neighboring devices
- **Wireless site maps**
  Which provide a graphical representation that you can use to monitor and interact with the wireless network, 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.

Skills

Network Operator

To perform network monitoring tasks, you need the following experience.

Proficient to Expert

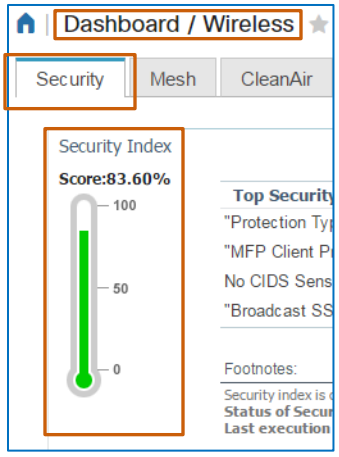
- Prime Infrastructure user interface navigation and behaviors
- Wireless networking concepts and practical knowledge

Terms

Security Index Score (wireless reporting)

The system calculates the security index score by assigning weight to various security configurations. Configuration weighting can vary from 0 to 100 where 0 indicates the least secure status and 100 indicates the most secure status.

The security index score of the Prime Infrastructure managed network is equal to the lowest scoring wireless LAN controller and the lowest scoring location server or Mobility Service Engine (MSE).



Monitoring Summary Wireless Network Data

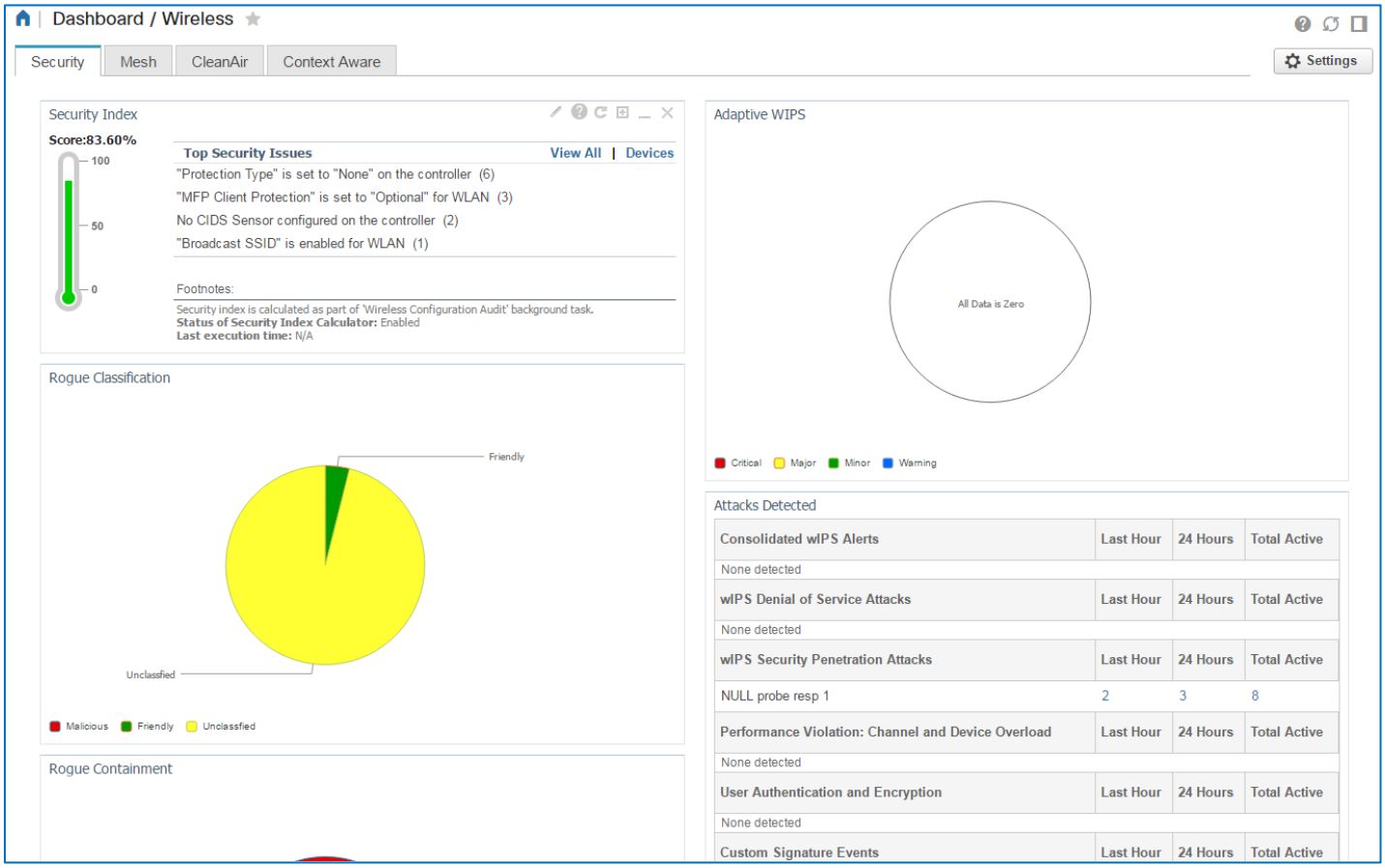
Summary Data Dashboards

Introduction

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.

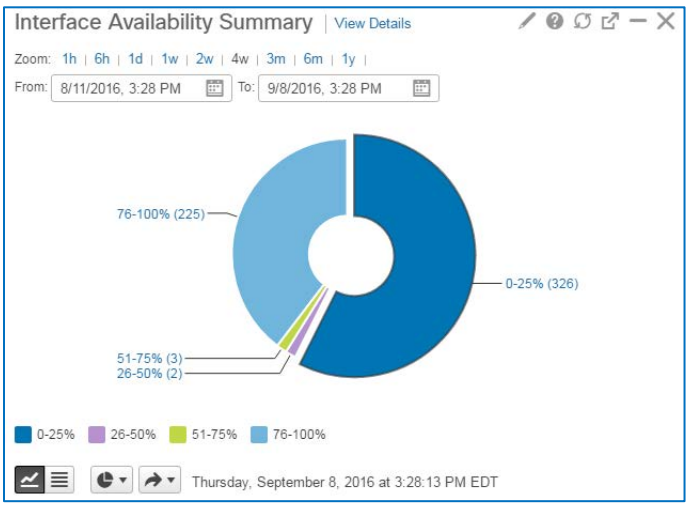
Note: While some dashboards combine reporting on both wired and wireless areas of the network, this job aid focuses on wireless network monitoring.

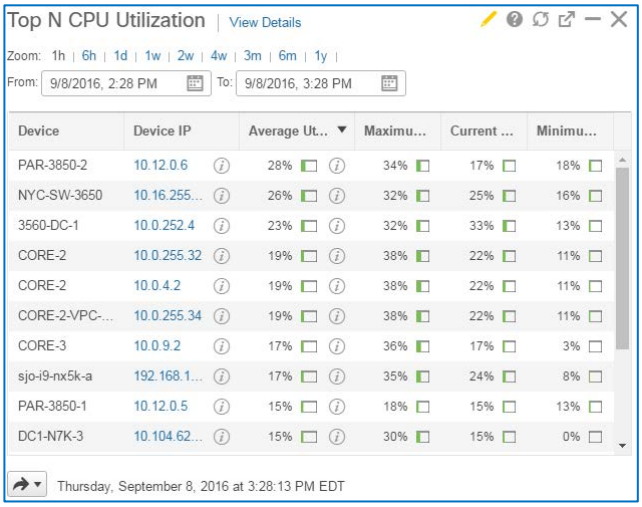
Dashboards can include multiple tabs and dashlets. You can organize dashboards and dashlets and manage the data that they report.

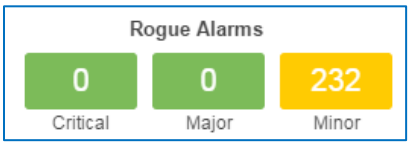


Dashlets are separate data elements that organize and report categories of information, such as alarm summaries, network statuses, and network and system performance metrics, among other information.

Dashlets can present information in charts, in tables, or interactive graphical data representations.







Note: In this job aid, we are presenting dashlets as they appear by default in the Prime Infrastructure.

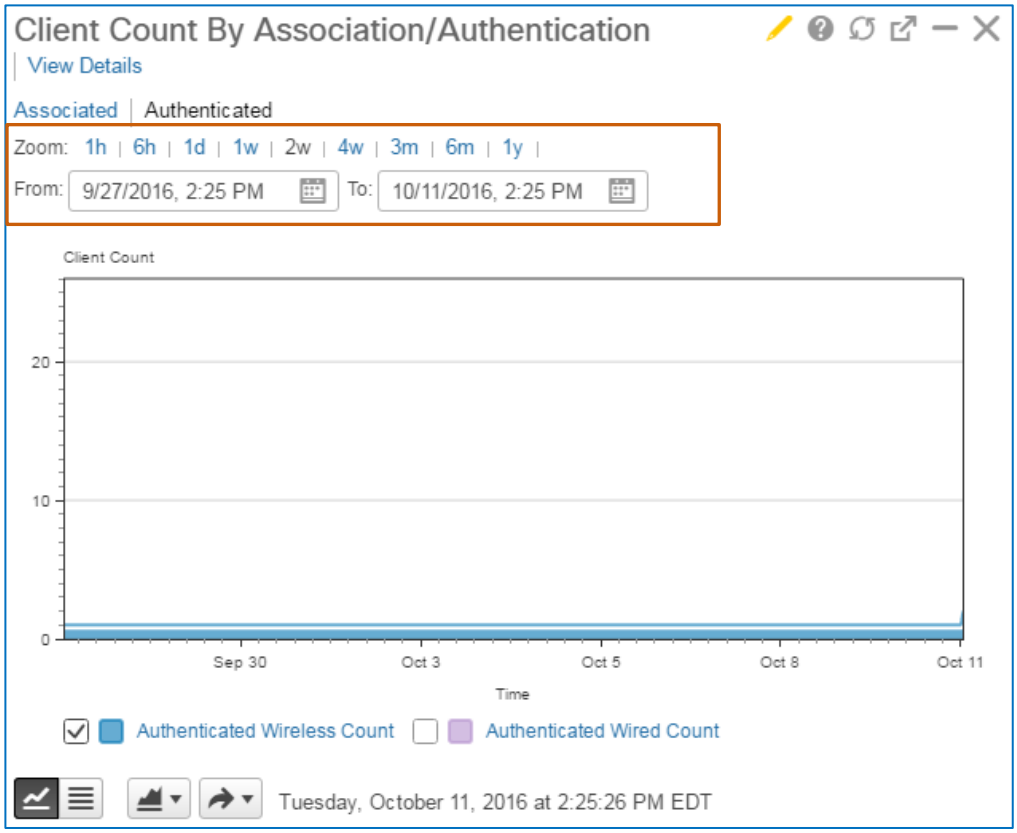
You can add or remove dashlets on existing tabs or configure custom tabs and add the dashlets that support your specific monitoring tasks.

You can add the same dashlet to more than one tab.

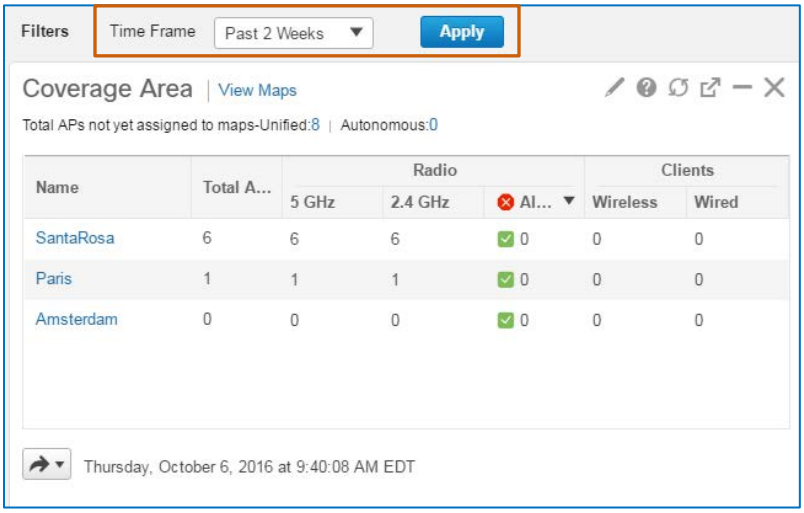
Managing Data Reporting Time Periods

You control dashlet time reporting time periods at a dashlet or dashboard level, depending on the dashlet. Recognizing the time period controls help ensure that you are seeing the data that you need to support your work.

Many dashlets provide dashlet level controls, including the zoom and calendar picker tools.



Some dashlet data reporting time periods are controlled at a dashboard level. The screenshot below illustrates the **Coverage Area** dashlet, which reports data based on the **Time Frame** setting.

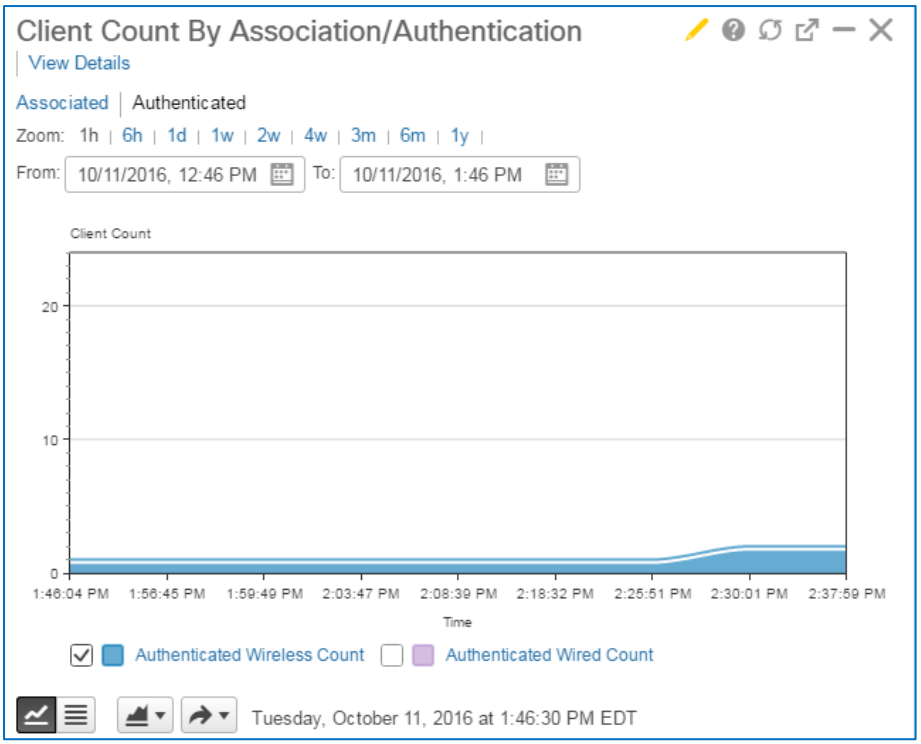


Managing Dashlet Settings and Defining Top N Reporting

At a dashlet level, you have several settings available to manage the data. These settings vary depending on the dashlet.

This way, you can monitor and control data reporting based on your monitoring requirements.

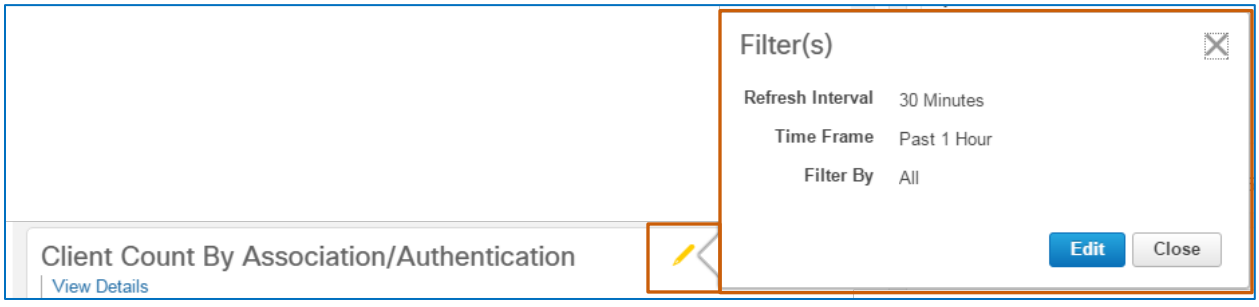
Using the **Client Count by Association/Authentication** dashlet as an example, you can see the types of settings that you can configure.



For wireless dashlets on the Network Summary dashboard, to see the current settings that are applied to the dashlet:

- On the dashlet toolbar, point to **Edit**.

  The **Filter(s)** pop-up window opens, listing the dashlet settings.

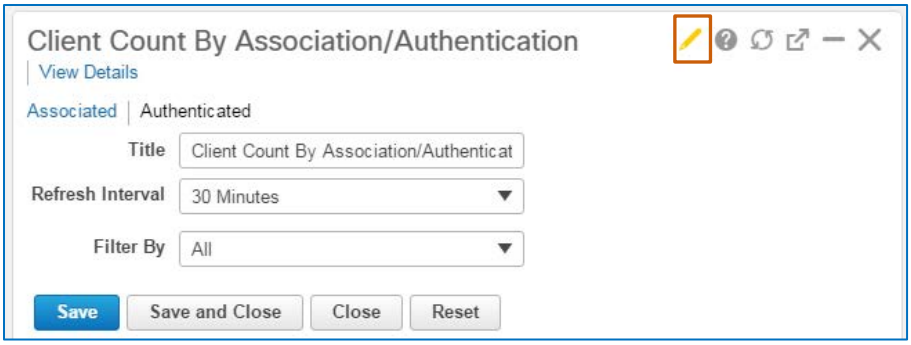


Note: Dashlets available on the **Wireless** dashboard do not provide the point feature.

To configure dashlet settings:

- On the dashlet toolbar, click **Edit**.

  The dashlet expands to display the settings that you can change.



In this example, you can:

- Change the dashlet name.

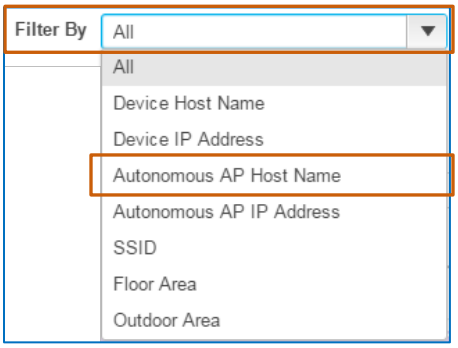
Tip: The naming feature is particularly helpful when you add custom dashlets to a dashboard, providing easier recognition of the data that the dashlet is reporting.

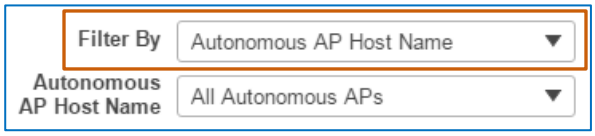
- Apply the optimal data refresh interval.

Note: When setting the data refresh rate, keep in mind that the system reports data based on polling intervals.

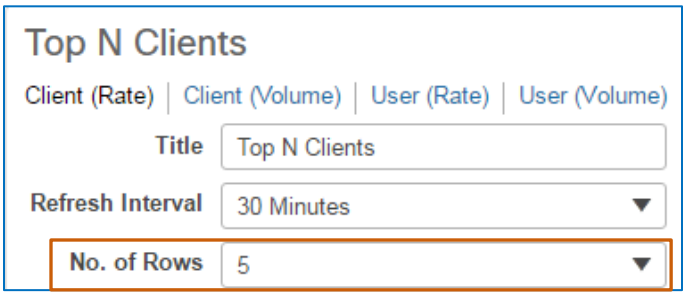
Setting the refresh rate at a shorter time interval than the polling interval causes unnecessary updates.

- Apply a filter on the chart based on the type of client that you need to see. When you select the filter that you want, you can then select specific items in the group on which you want the dashlet to report.





For dashlets that report top number (Top N) metrics, you can select the number of items, up to 15, that the dashlet reports.



Adding Dashboards and Dashlets for Flexible Monitoring

When working with dashlets that provide access to groups, families, or types of items, for example, keep in mind that you can add custom dashlets that report the specific groups of items for which you are responsible.

You also can add custom dashboard tabs. Adding custom dashboard with the system or custom dashlets of interest creates a highly flexible monitoring environment.

This way, you can ensure that you are seeing the metrics that you need so that you can respond to changing conditions most efficiently.

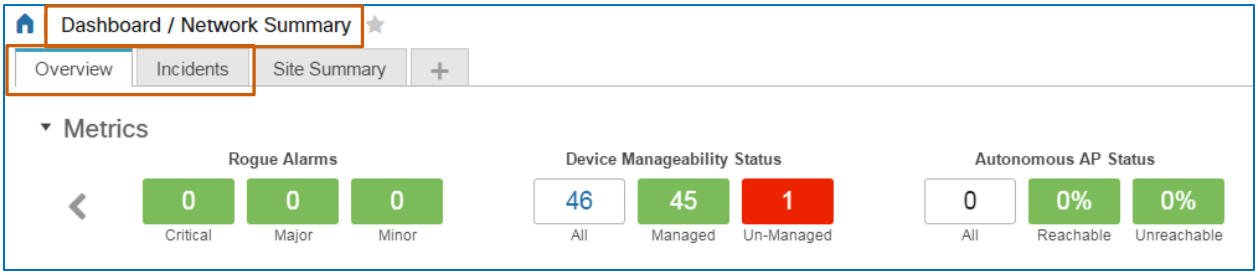
Network Summary Metrics and Aggregate Dashlets

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

Tip: You also can monitor and manage wireless access point health on the **Network Health** dashboard.
For more information, refer the **Network Health Monitoring Overview** job aid.

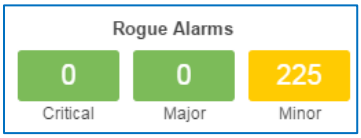
Network Summary Metrics Dashlets

On the **Network Summary** dashboard, the **Overview** and **Incidents** tabs provide **Metrics** dashlets that report key wireless data.

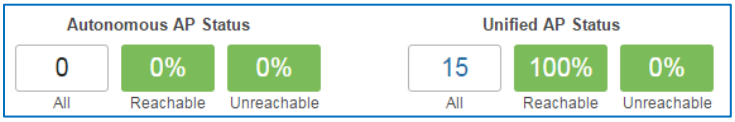


Wireless network specific dashlets report the following:

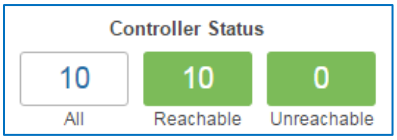
- Numbers of rogue alarms by severity level



- Percentage of reachable and unreachable autonomous and unified access points out of the total number of each that the system is managing

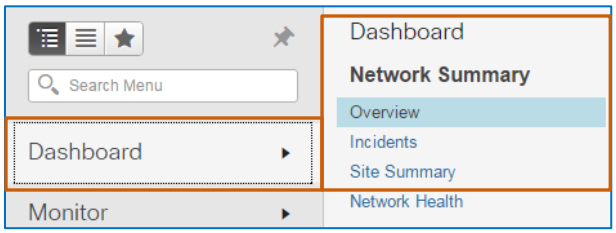


- The number of reachable and unreachable wireless LAN controllers out of the total number of each that the system is managing



Network Summary Aggregate Dashlets

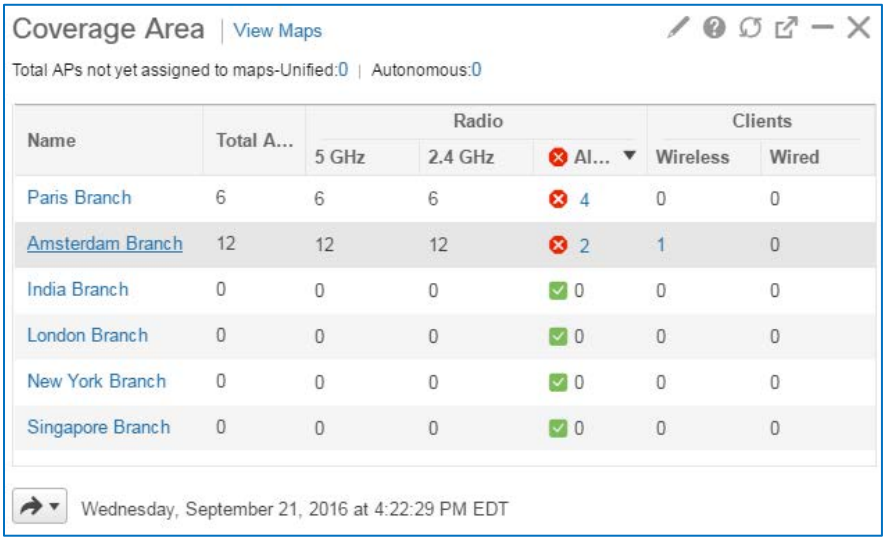
The following network summary and aggregate dashlets, available on the **Network Summary** | **Overview**, **Incidents**, and **Site Summary** tabs, report key wireless data.



Tip: You also can monitor and manage access point device health on the **Network Health** dashboard.
For more information, refer the **Network Health Monitoring Overview** job aid.

AP Radio Coverage Status by Site

The **Coverage Area** dashlet reports radio coverage and indicates the number of AP radios by frequency and any associated alarms by site by wireless site.

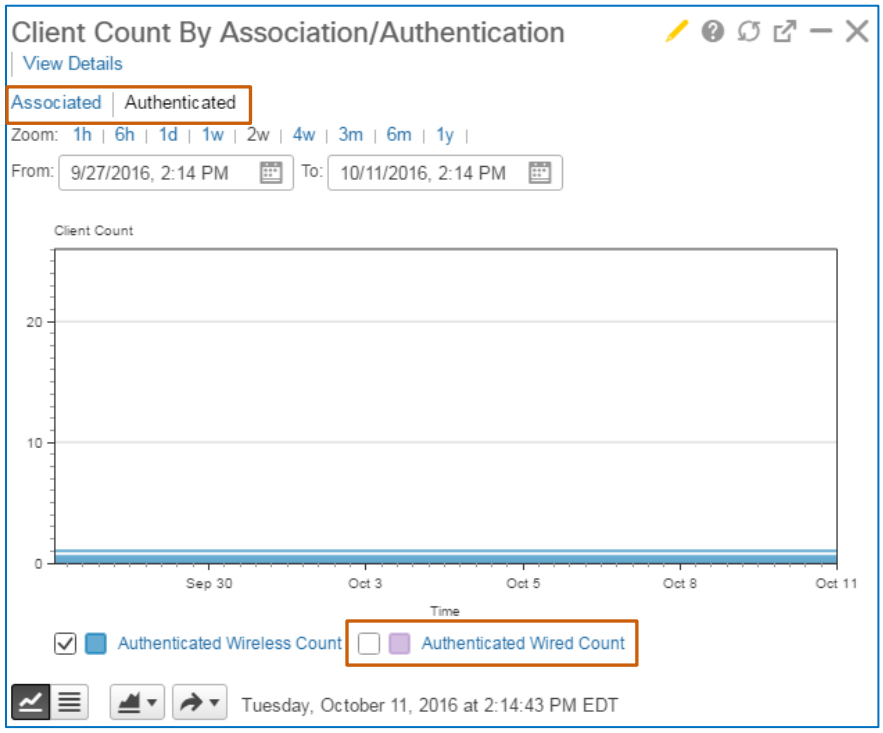


The Number of Clients Associated To or Authenticated On the Network

For the time period indicated in the dashlet, the **Client Count By Association/Authentication** dashlet reports the number of wireless clients that were authenticated on or associated with the network.

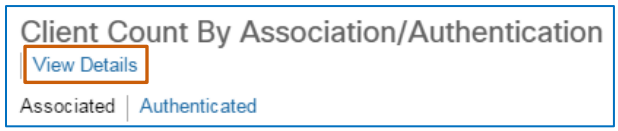
To see the number of wireless client by association or authentication:

- Below the dashlet title, click the **Associated** or **Authenticated**, and then clear the applicable **Wired Count** check box.

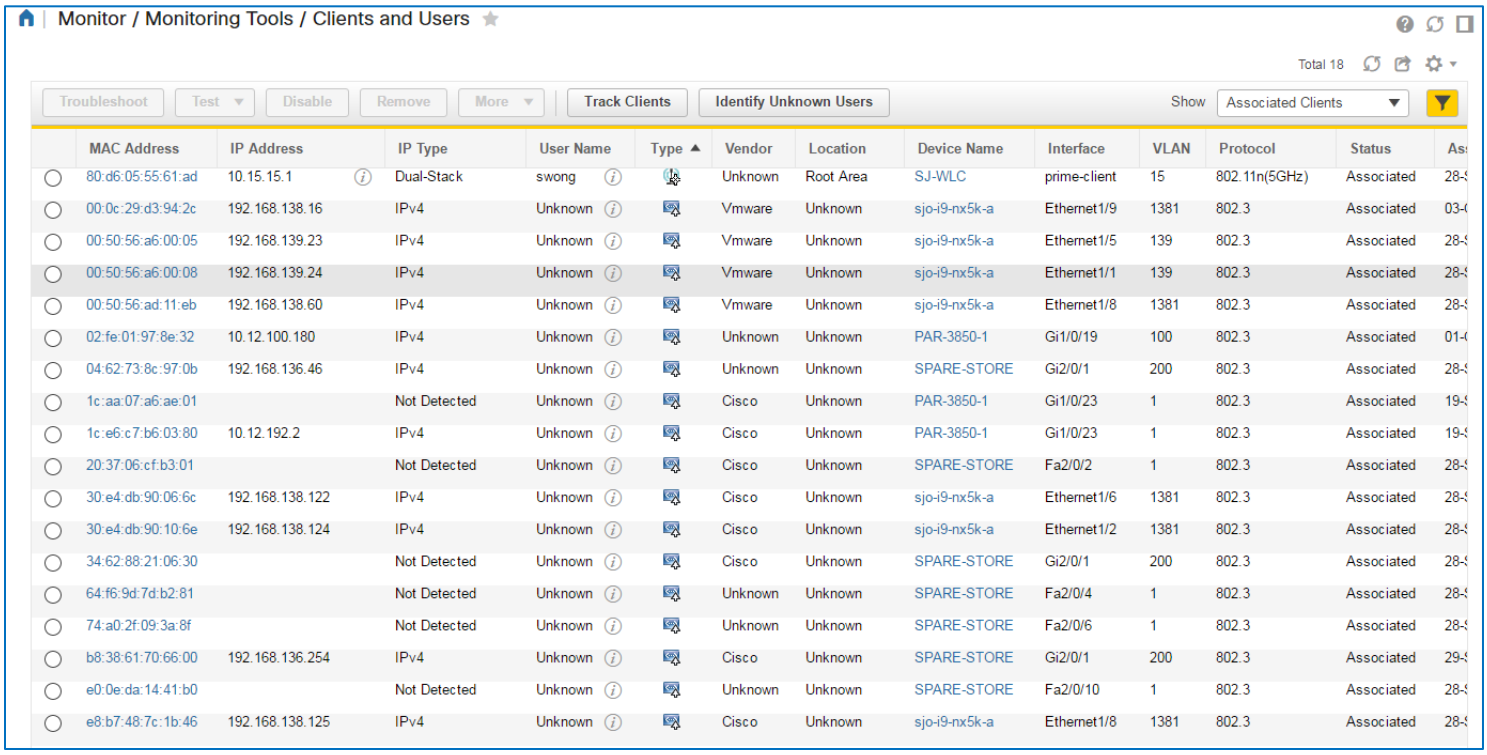


To review a list of clients or access client details:

- Below the dashlet title, click **View Details**.



The **Clients and Users** page opens, where you can access client details or take actions, as needed.



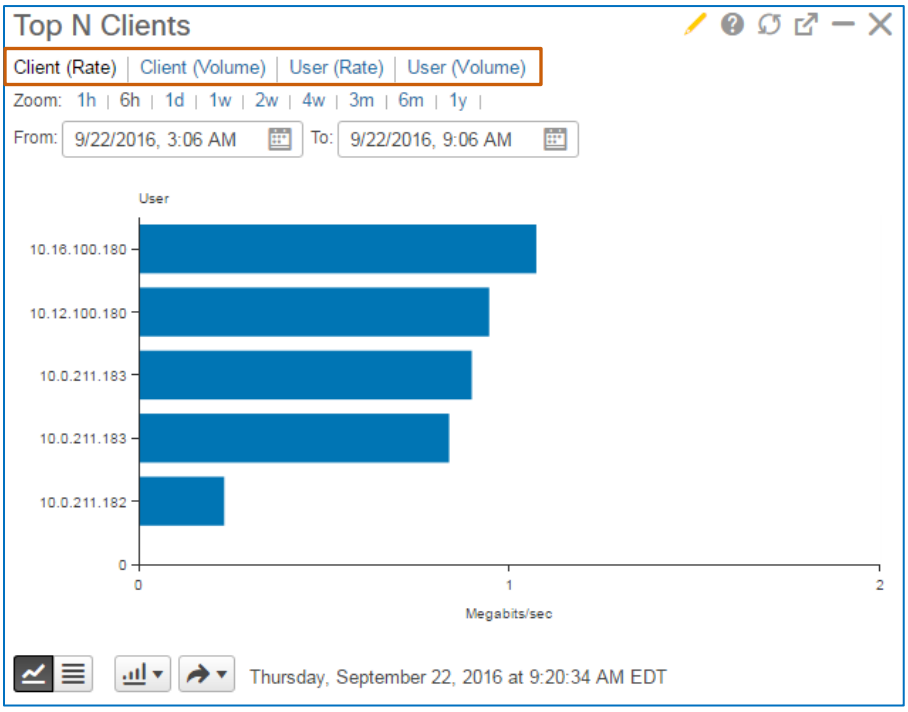
Clients or Network Users Generating the Highest Traffic Rates or Volumes

For the time period indicated in the dashlet, the **Top N Clients** dashlet reports the clients that and end users who are generating the highest traffic rates or volumes.

Monitoring traffic volumes and rates can help you identify clients that are generating excessive traffic compared to other users. This way, you can investigate the type of traffic that the client is generating to mitigate bandwidth or resource usage, and help ensure better user experience on the network.

To see the client rate or volume, or user rate or volume:

- Click the associated link below the dashlet title.

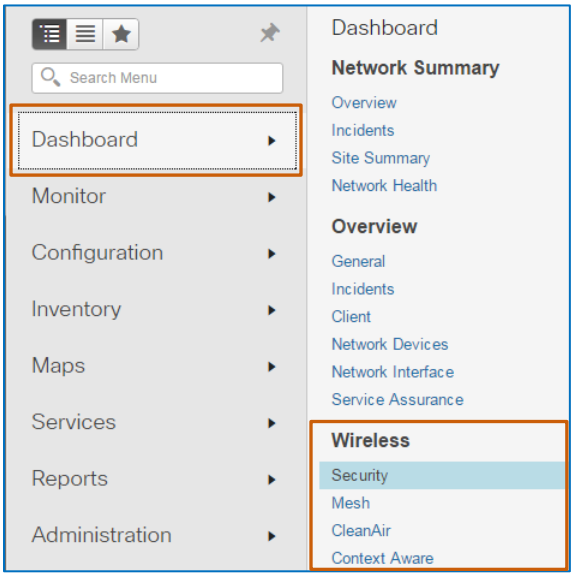


Wireless-Specific Summary Dashlets

The following wireless summary and aggregate dashlets, available on the **Wireless** | **Security**, **Mesh**, **CleanAir** and **Context Aware** tabs, or on custom tabs, report key wireless data.

Note: The **Context Aware** dashboard tab indicates that it is deprecated, which means that the dashboard is active in this release of Prime Infrastructure, but will not be available in the next release.

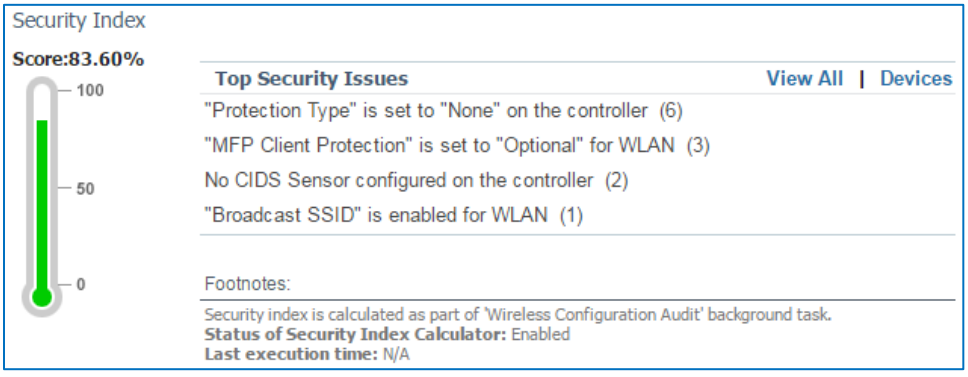
In the next release, the **Context Aware** dashlets will remain available to add to existing or custom dashboards.



General Security Monitoring Dashlets

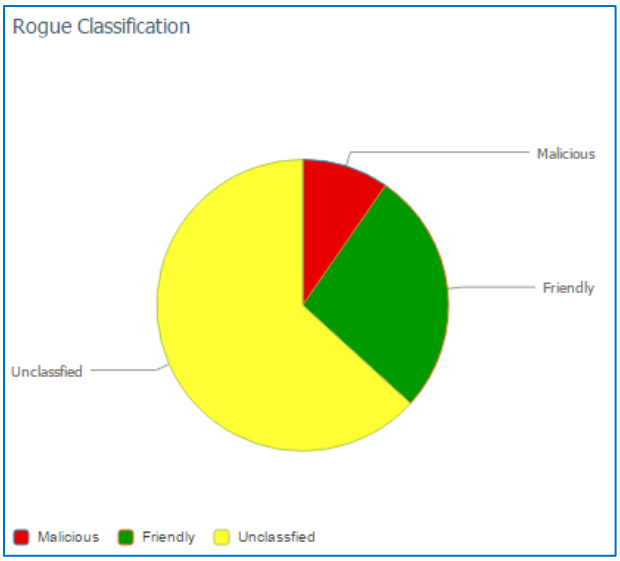
The **Security Index** dashlet reports the current security index score and the most critical security issues that the system has identified when running **Wireless Configuration Audit** jobs in Administration.

You can navigate to devices or issues, as needed, to investigate or mitigate issues.



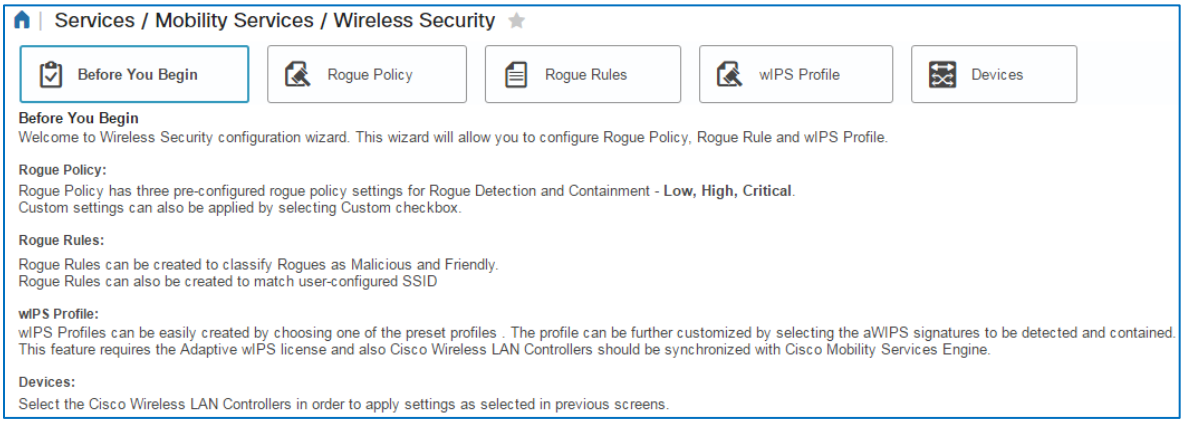
Rogue Access Point Monitoring Dashlets

The **Rogue Classification** dashlet reports friendly, malicious, and unclassified rogue access points that the network is detecting.



When monitoring, the number of malicious rogues should be minimal. Noticing a significant and disproportionate number of malicious rogues can indicate that a serious network attack is in progress.

Tip: System users define the rogue policies and rules that control how the system classifies and reports rogue access point types.



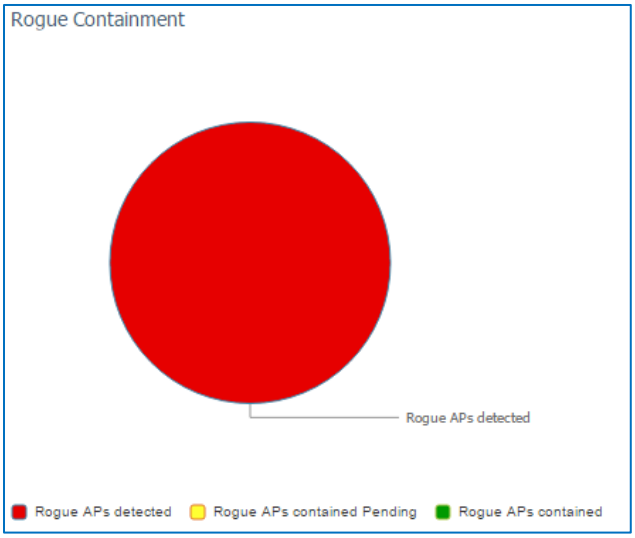
Classifying rogues accurately is a key step when configuring wireless security, which helps avoid misreported rogues or flooding of inaccurate rogue- or security-related alarms.

When you see that the system is reporting disproportinate numbers of unclassified rogue access points, or significant numbers of malicious rogues with no attacks or other issues are occuring, evaluate the rogue rules and policies to help ensure that the system is classifying rogue APs accurately and that the expected rules are in place based on business and operational requirements.

The **Rogue Containment** dashlet reports the number of rogue access points that the system is detecting or that the system is preparing to contain or is containing by using blocking methods.

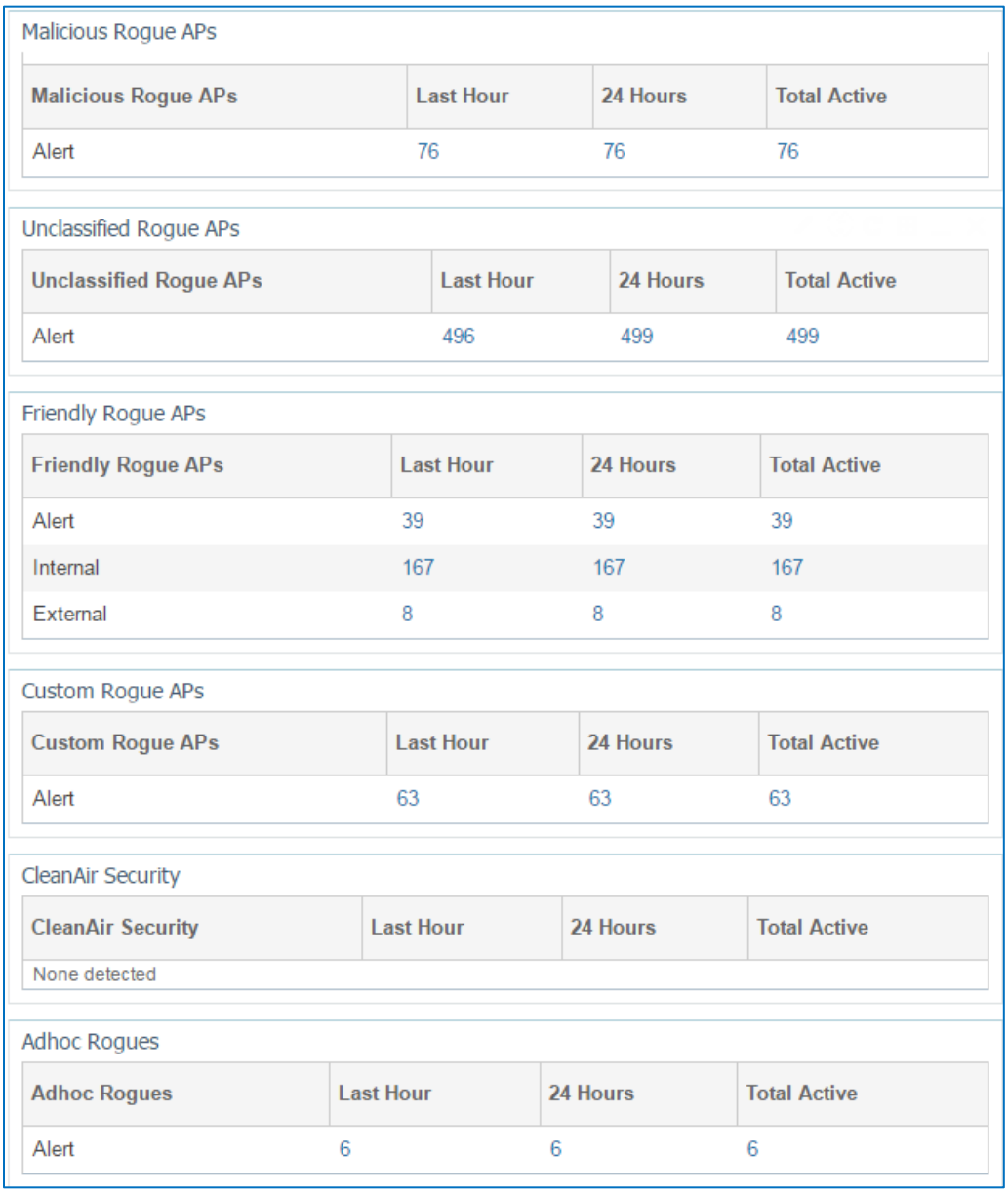
This information helps you determine that malicious rogue containment is occurring as expected.

Seeing a significant number of maliciously classified rogues with only a minimal number contained, for example, can prompt you to investigate the activity that the non-contained rogues are generating.



A series of dashlets report rogue access point types and statuses and ClearAir technology security alerts that the system has identified in the last hour and in the last 24 hours.

You can click the number links to open an **Alarms** page that lists all of the alarm activity associated with the rogue access point for the time frame indicated in the column heading.



Malicious Rogue APs

Malicious Rogue APs	Last Hour	24 Hours	Total Active
Alert	76	76	76

Unclassified Rogue APs

Unclassified Rogue APs	Last Hour	24 Hours	Total Active
Alert	496	499	499

Friendly Rogue APs

Friendly Rogue APs	Last Hour	24 Hours	Total Active
Alert	39	39	39
Internal	167	167	167
External	8	8	8

Custom Rogue APs

Custom Rogue APs	Last Hour	24 Hours	Total Active
Alert	63	63	63

CleanAir Security

CleanAir Security	Last Hour	24 Hours	Total Active
None detected			

Adhoc Rogues

Adhoc Rogues	Last Hour	24 Hours	Total Active
Alert	6	6	6

Adaptive Wireless Intrusion Prevention System (wIPS) Monitoring Dashlets

The Cisco® Adaptive Wireless Intrusion Prevention System (adaptive wIPS) monitors and reports wireless network anomalies, unauthorized access, and network attacks that are occurring by using radio frequencies.

The **Attacks Detected** group of dashlets report wIPS-related issues and attacks.

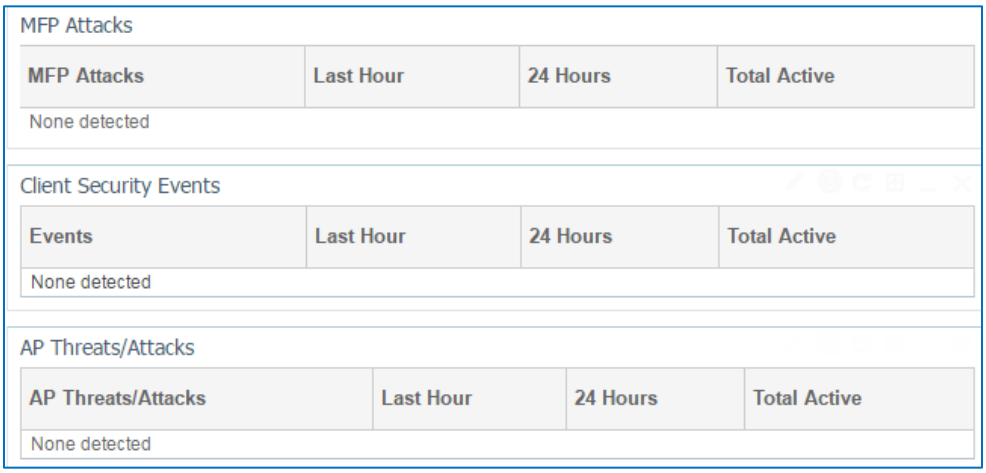
Attacks Detected

Consolidated wIPS Alerts	Last Hour	24 Hours	Total Active
None detected			
wIPS Denial of Service Attacks	**Last Hour**	**24 Hours**	**Total Active**
None detected			
wIPS Security Penetration Attacks	**Last Hour**	**24 Hours**	**Total Active**
NULL probe resp 1	12	12	13
Performance Violation: Channel and Device Overload	**Last Hour**	**24 Hours**	**Total Active**
None detected			
User Authentication and Encryption	**Last Hour**	**24 Hours**	**Total Active**
None detected			
Custom Signature Events	**Last Hour**	**24 Hours**	**Total Active**
None detected			

Security Events and Attacks Monitoring Dashlets

Additional dashlets report:

- **Management Frame Protection (MFP) Attacks**
  Reports the numbers of attacks on 802.11 management messages that are passed among access points and clients, which can indicate attempts to:
  - Invoke denial-of-service attacks.
  - Flood the network with client connection attempts (associations) and client probe requests, which can overwhelm the network and network resources.
  - Interject rogue access points.
  - Attack QoS and radio measurement frames, which can affect network performance.
- **Client Security Events**
  Reports the numbers of client-related security events, including:
  - Excluded client events.
  - Wired equivalent privacy (WEP) decrypt errors.
  - Wi-Fi protected access message integrity check (WPA MIC) errors, which can indicate that someone in the network is trying to replay the message that was sent by the original client or that the client is faulty.
  - Shunned clients, which are suspicious clients that are dynamically excluded from connecting to a wireless mobility group by the group's anchor wireless LAN controller
  - Internet Protocol Security (IPSec) anti-replay check failures, which can indicate attempts to maliciously or fraudulently repeat or delay valid network transmissions in order to impersonate a valid network user or to disrupt or cause negative impact for legitimate connections.
- **AP Threats/Attacks**
  Reports the numbers of various access point threats and attacks, such as denial-of-service (DoS) or security penetration attacks, for example.

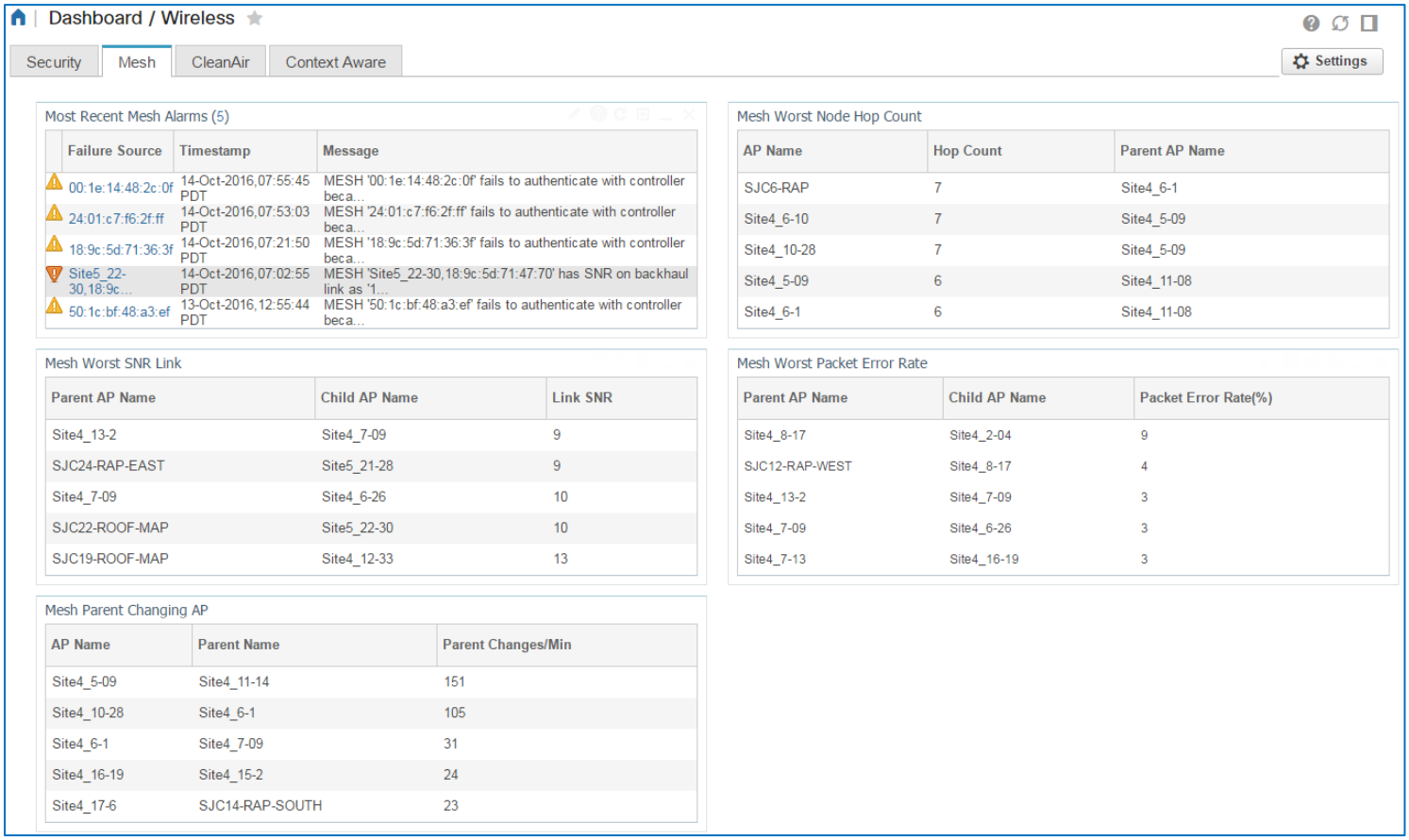


Wireless Mesh Network-Related Data

You can monitor and investigate performance data and potential issues related to the Cisco wireless access points that are configured to support wireless mesh network topologies.

Key mesh-related dashlets report:

- Alarms occurring on mesh access points
- AP radio links that are exhibiting the poorest signal to noise ratios
- The access points experiencing the highest number traffic hops
- Packet error rates on AP radio links
- The AP radio links changing parent access points most often in an attempt to find the optimal route to the root access point (RAP).

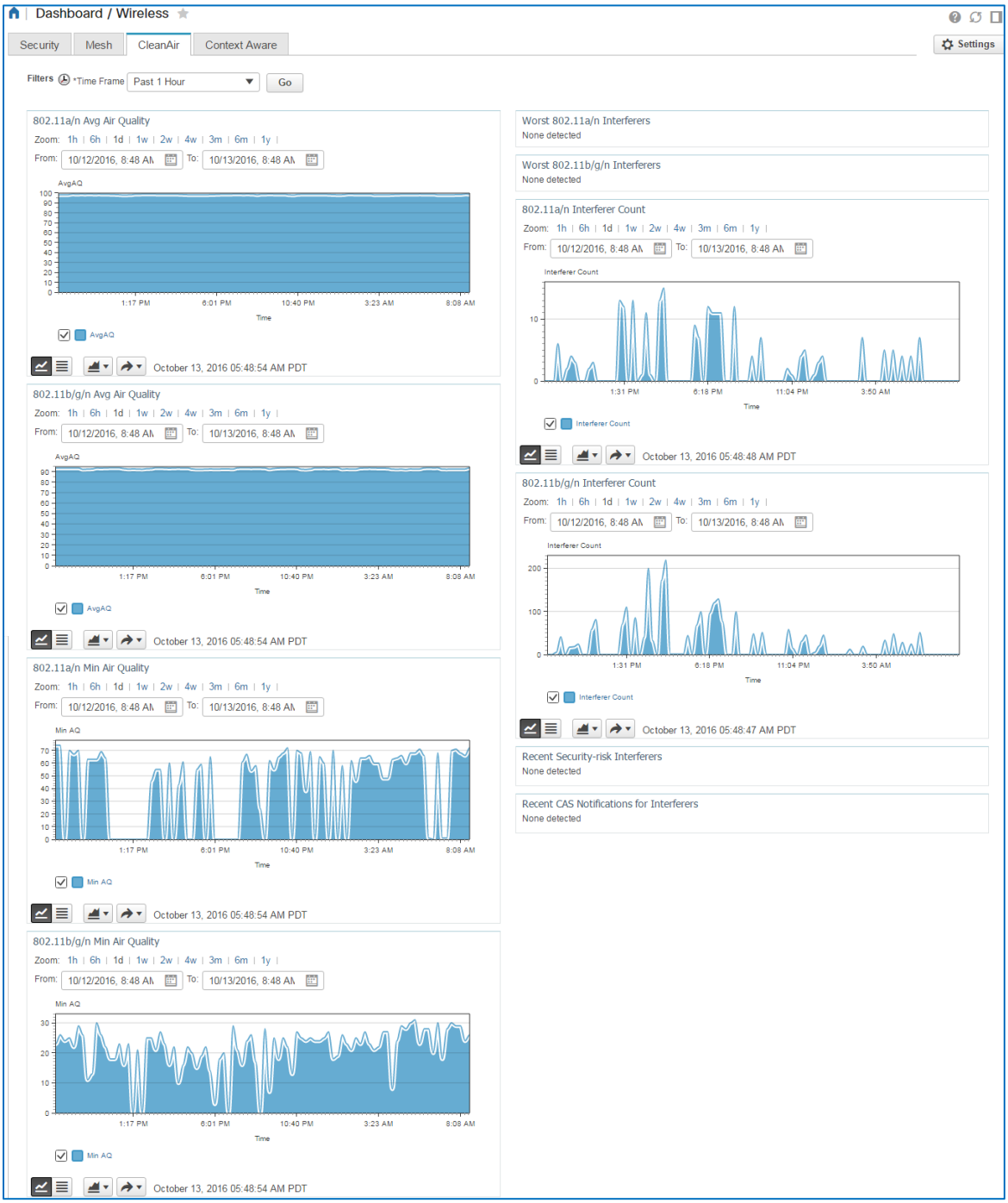


CleanAir Technology-Related Data

Based on the time period that you select, the **CleanAir** dashlets report the air quality for the 802.11 a/n and b/g/n radio protocols and radio frequency interferers, such as microwave ovens or Bluetooth devices, that can affect wireless network performance.

Note: Access points must support CleanAir technology in order to report CleanAir-related data.

For more information on CleanAir technology, you can refer to Cisco documentation that addresses CleanAir deployment and operations.



Based on network policies, interferers can also be designated as security risks. Interferers that breach network policies are reported in the **Recent Security-risk Interferers** dashlet.

By monitoring the **Recent CAS Notification for Interferers** dashlet, you can identify the following items, which helps you to ensure user experience on the network.

- The types of devices that are causing AP radio interference.
- The channels that are being affected by interference.
- The severity of the interference.
- The access point detecting the issue.

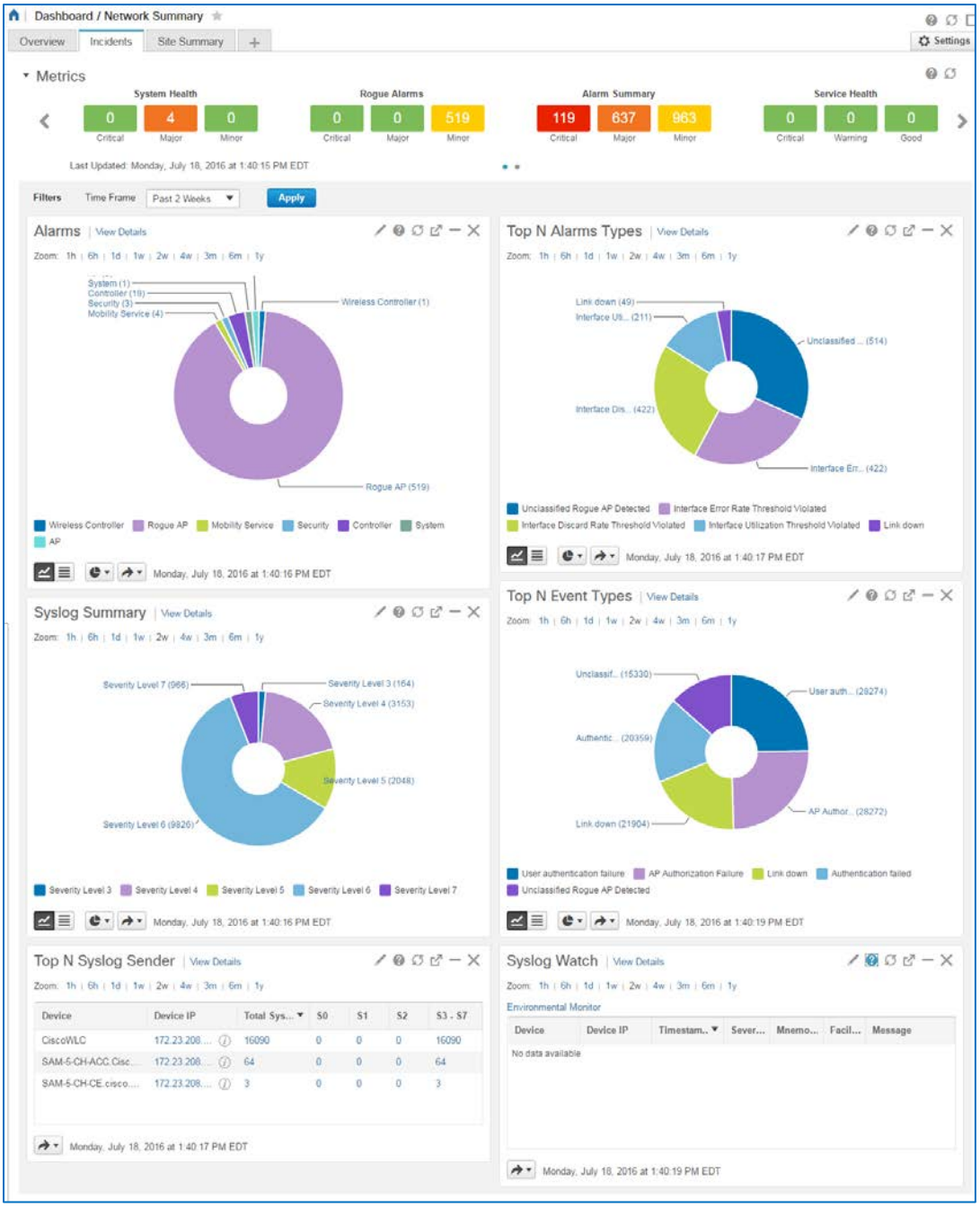
Note: To report CAS notifications, the system must include at least one Cisco© Mobility Services Engine.

Alarm, Event, and Syslog Data

General Summary Data

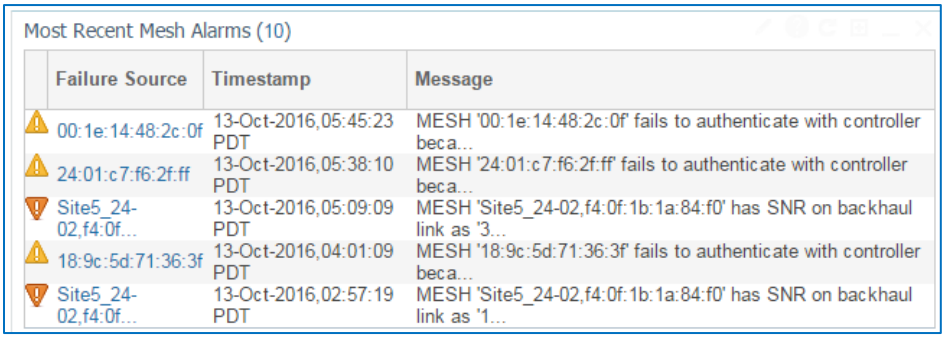
Based on the time frame that you select on the toolbar, the **Incidents** tab summarizes:

- 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 reporting.



Mesh Alarms Data

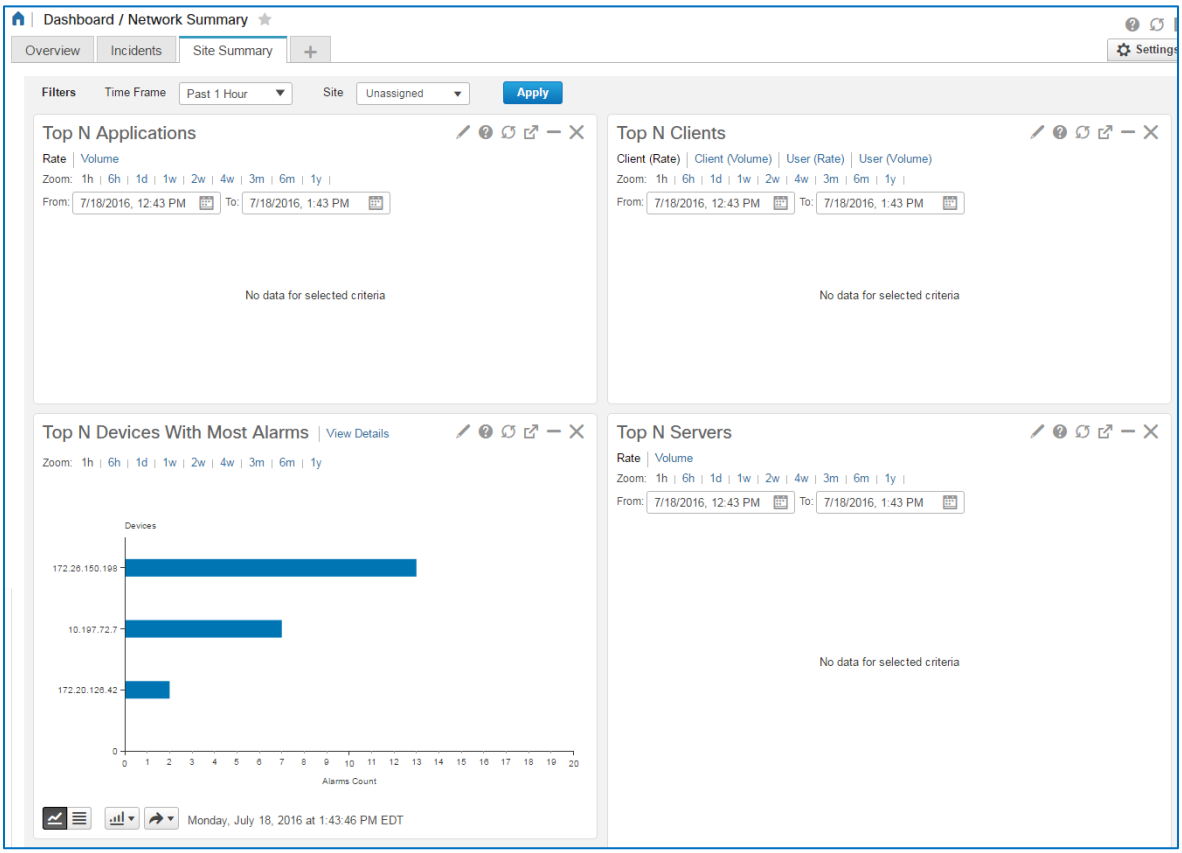
The **Most Recent Mesh Alarms** dashlet reports those alarms occurring on mesh-configured access points during the previous 24 hours at a rolling interval from the current system time.



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 amount (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.



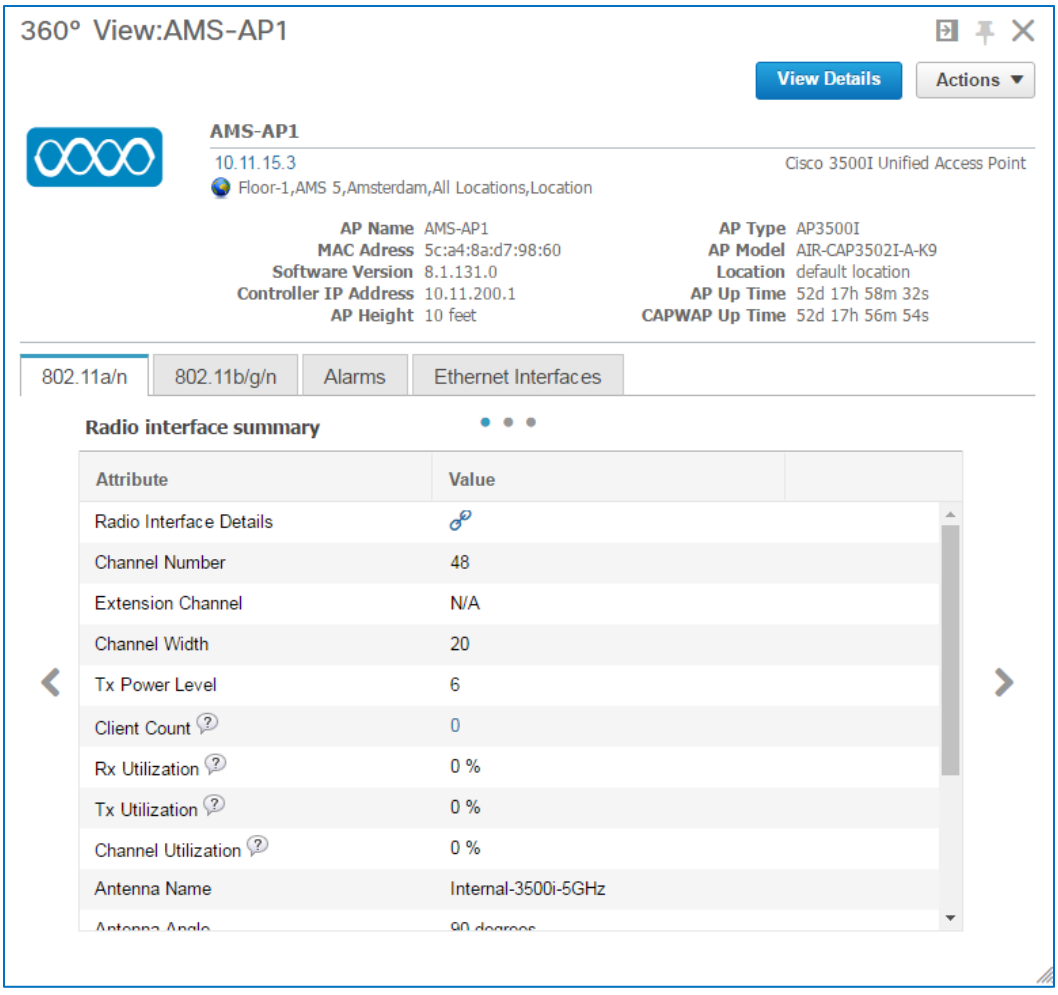
Device 360⁰ Views

Overview

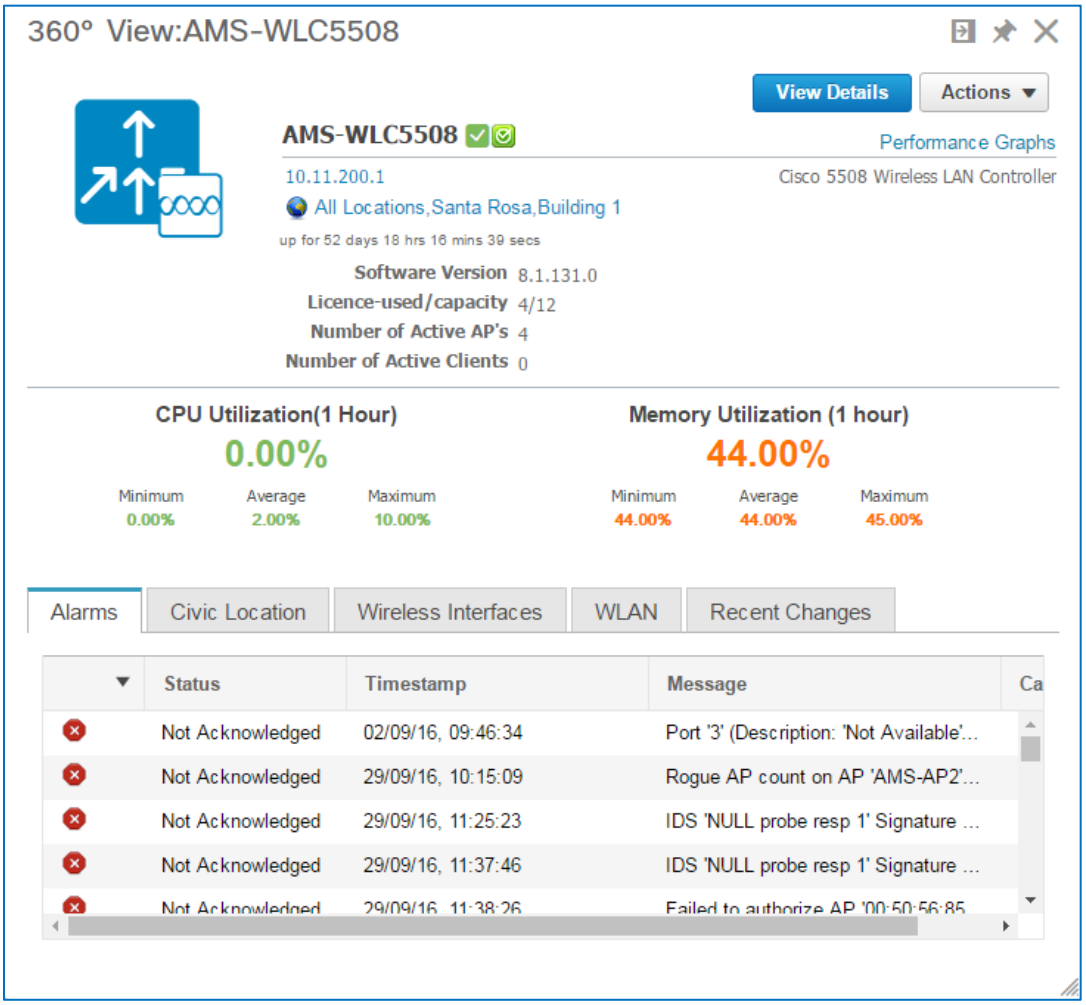
Device **360⁰ View** pop-up windows present significant amounts of device information, report key performance metrics and activities that are occurring on devices, and provide access to take actions on devices, as needed.

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

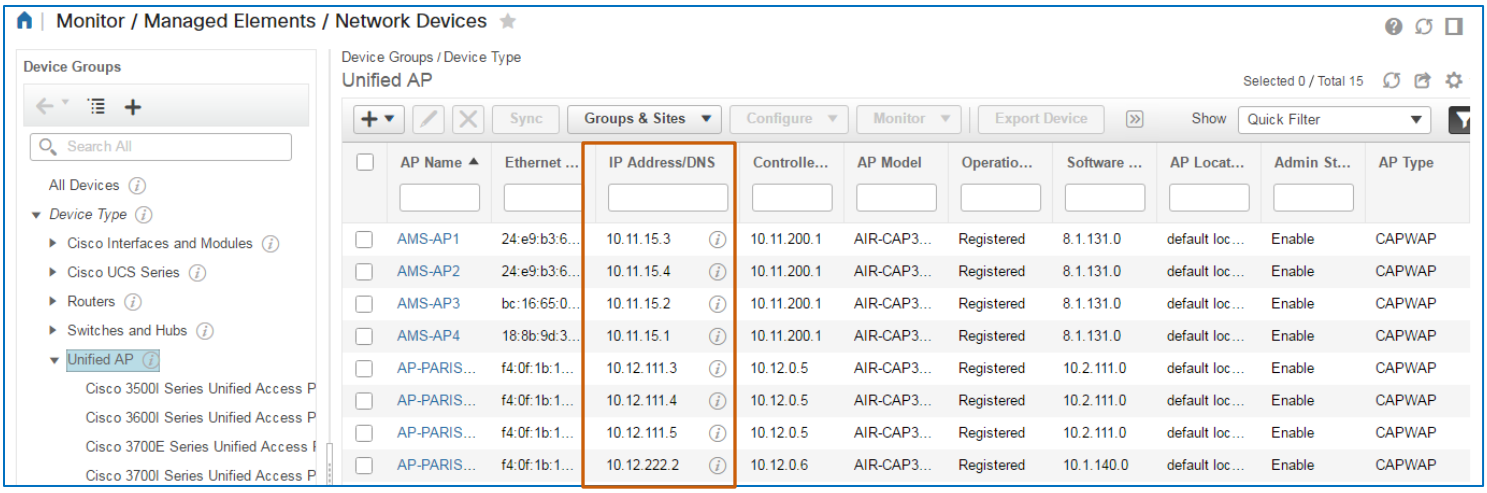
The following screenshot illustrates a unified access point **360⁰ View** pop-up window.



The following screenshot illustrates a wireless LAN controller **360⁰ View** pop-up window.

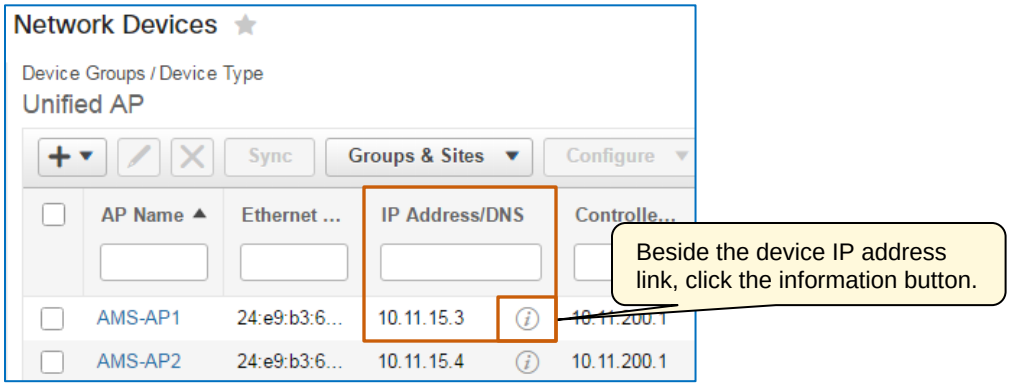


Most tables listing a device IP address provide access to **360⁰ View** pop-up windows by using the information icon.

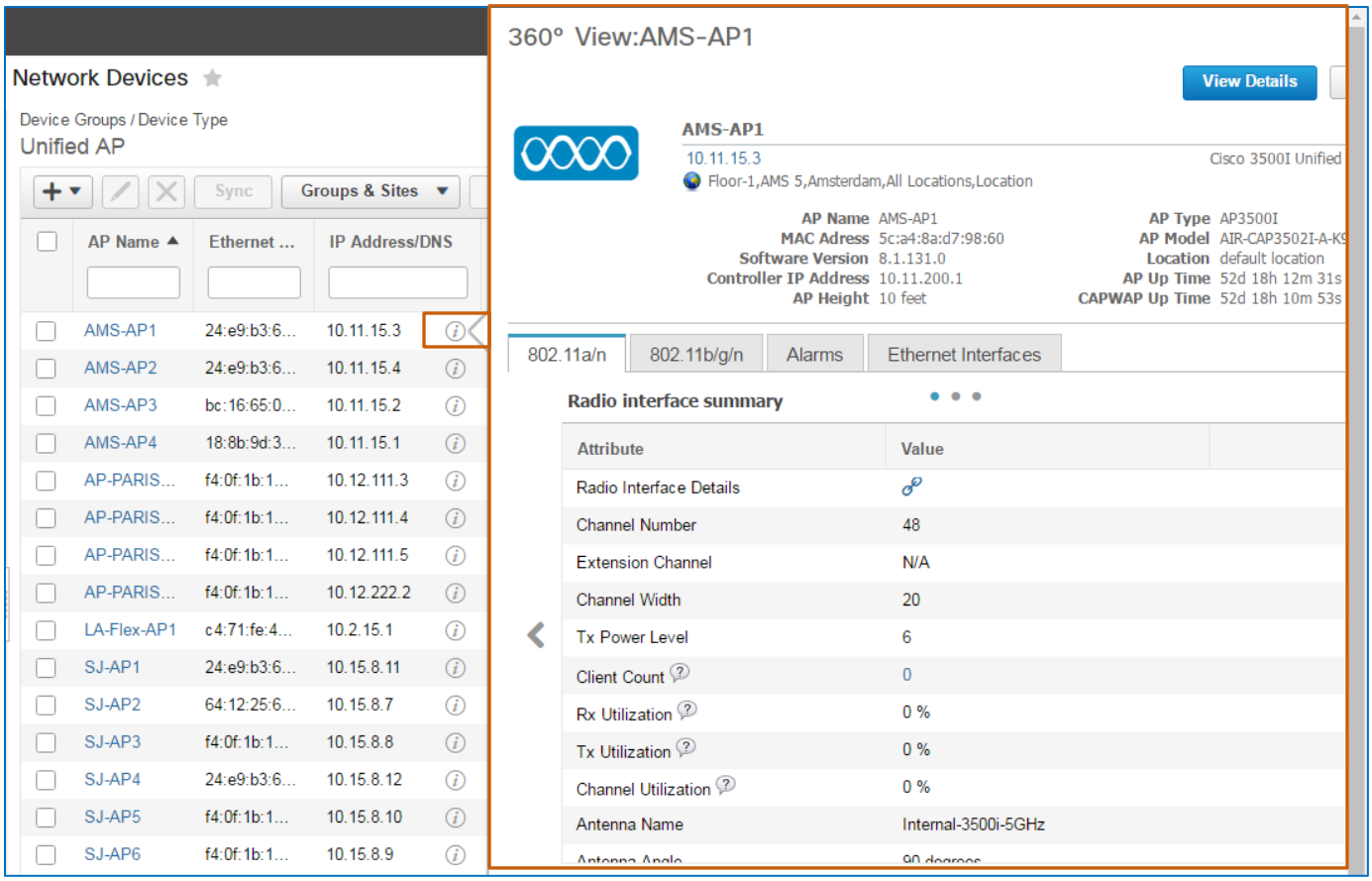


To open a 360⁰ view pop-up window:

- Beside the device IP address link, click the information button.



The associated **360⁰ View** pop up window opens.



When information in the pop-up window prompts you to evaluate a device further, you can take immediate actions on the device, open performance metrics graphs, or open detailed device information based on the specific device type.

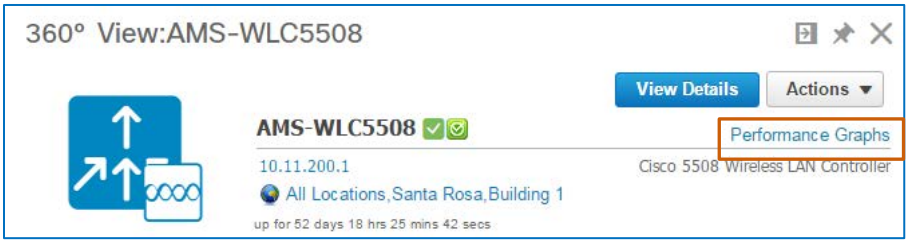
Note: For detailed information on device 360⁰ pop-up window features, refer to the **Cisco Prime Infrastructure 3.1 User Guide**.

In addition to the features addressed in the user guide, pop-up windows can provide access to the following features.

Access to Performance Graphs

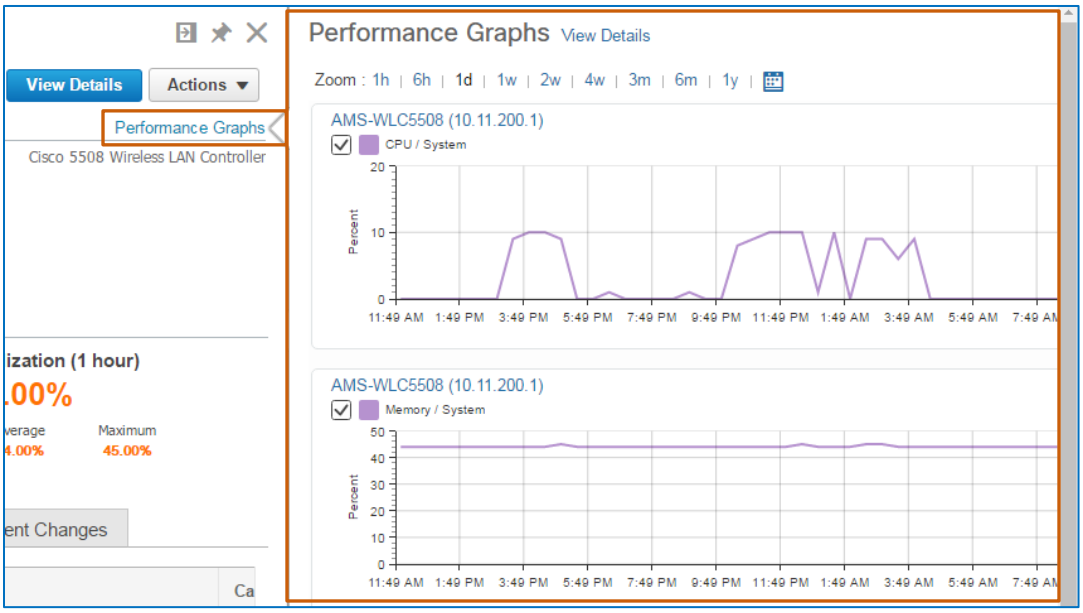
You can review current or evaluate historical performance data for key performance indicators (KPIs) by using the Performance Graphs feature.

Performance graphs illustrate key metrics data over time, which can provide insight to the device's environment and factors that might contribute to potential issues.



To open the Performance Graphs pop-up window:

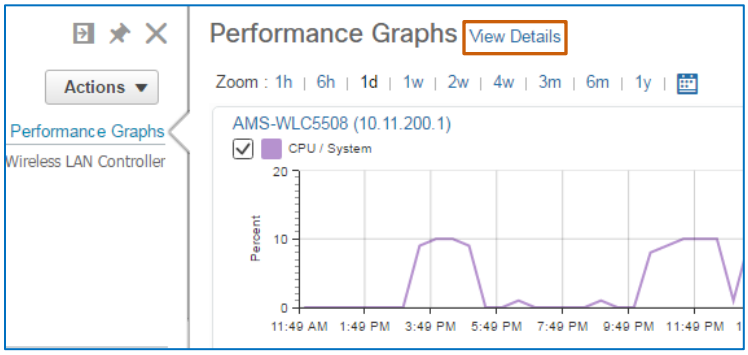
- In the **360⁰ View** pop up window, below the **Actions** drop-down menu, click **Performance Graphs**.



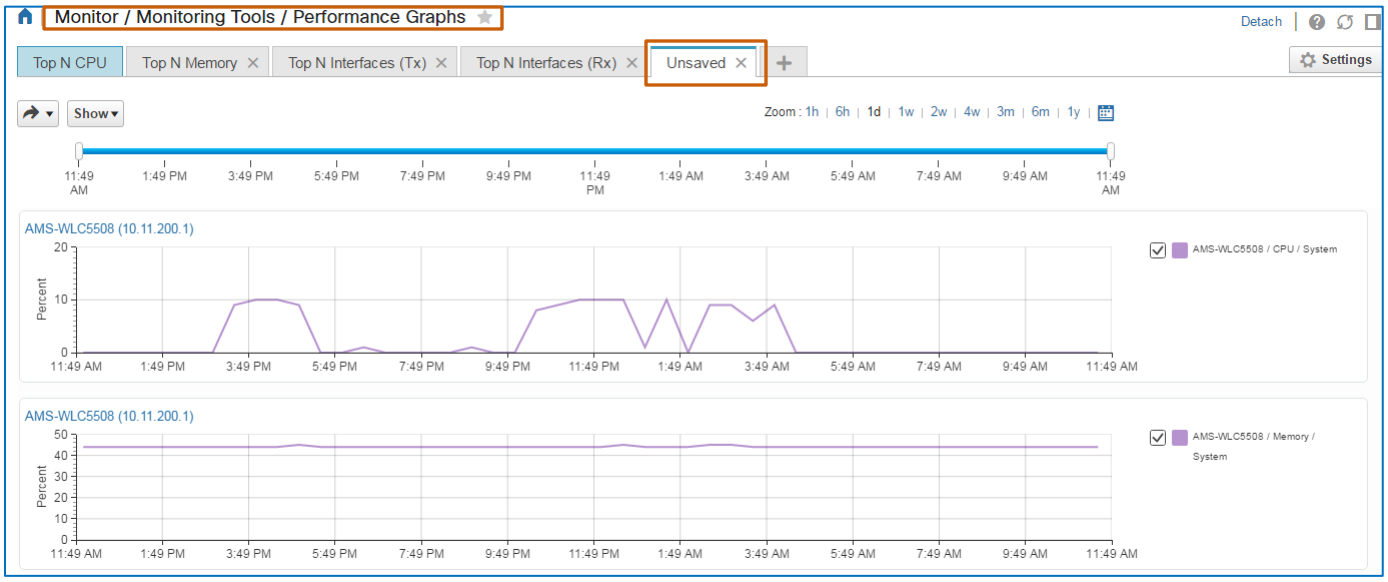
You can also navigate to display alarms and configuration changes in relationship to the KPI values for the component on which a graph is reporting. Correlating changing KPI values to alarm reporting or configuration changes can provide critical insight into possible issues or issue causes.

To navigate to and generate a dedicated list of associated graphs:

- In the **Performance Graph**s pop-up window, click **View Details**.



The system navigates to and generates a tab of associated metrics graphs in the **Performance Graphs** area of the application.



Tip: In this view, you also can display alarms and configuration changes in relationship to the KPI values for the device on which the graph is reporting.

Correlating changing KPI values to alarm reporting or configuration changes can provide critical insight into possible issues or issue causes.

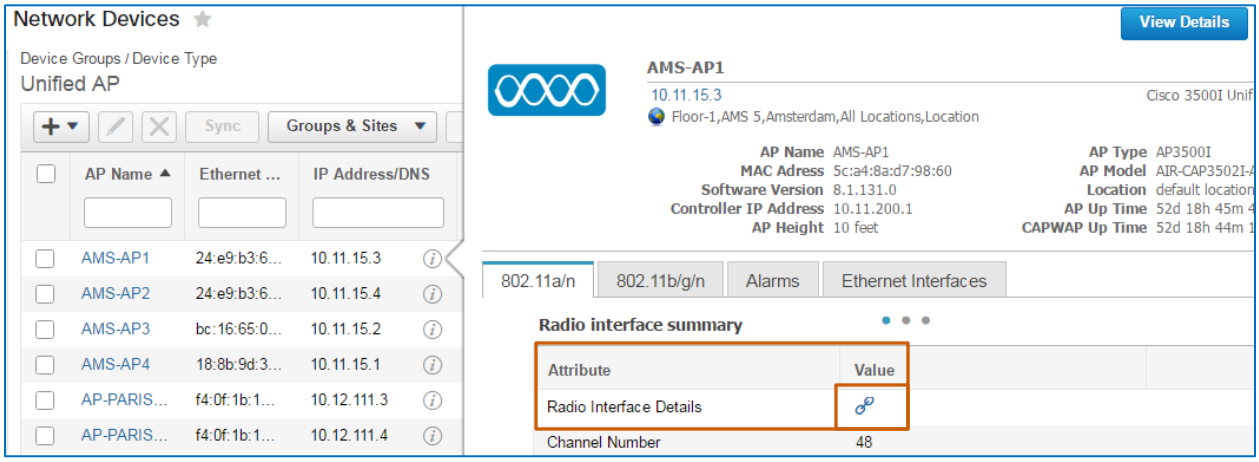
For more information on using performance graphs, refer to the **Network Health Monitoring Overview** job aid.

Access to Access Point (AP) Radio Details

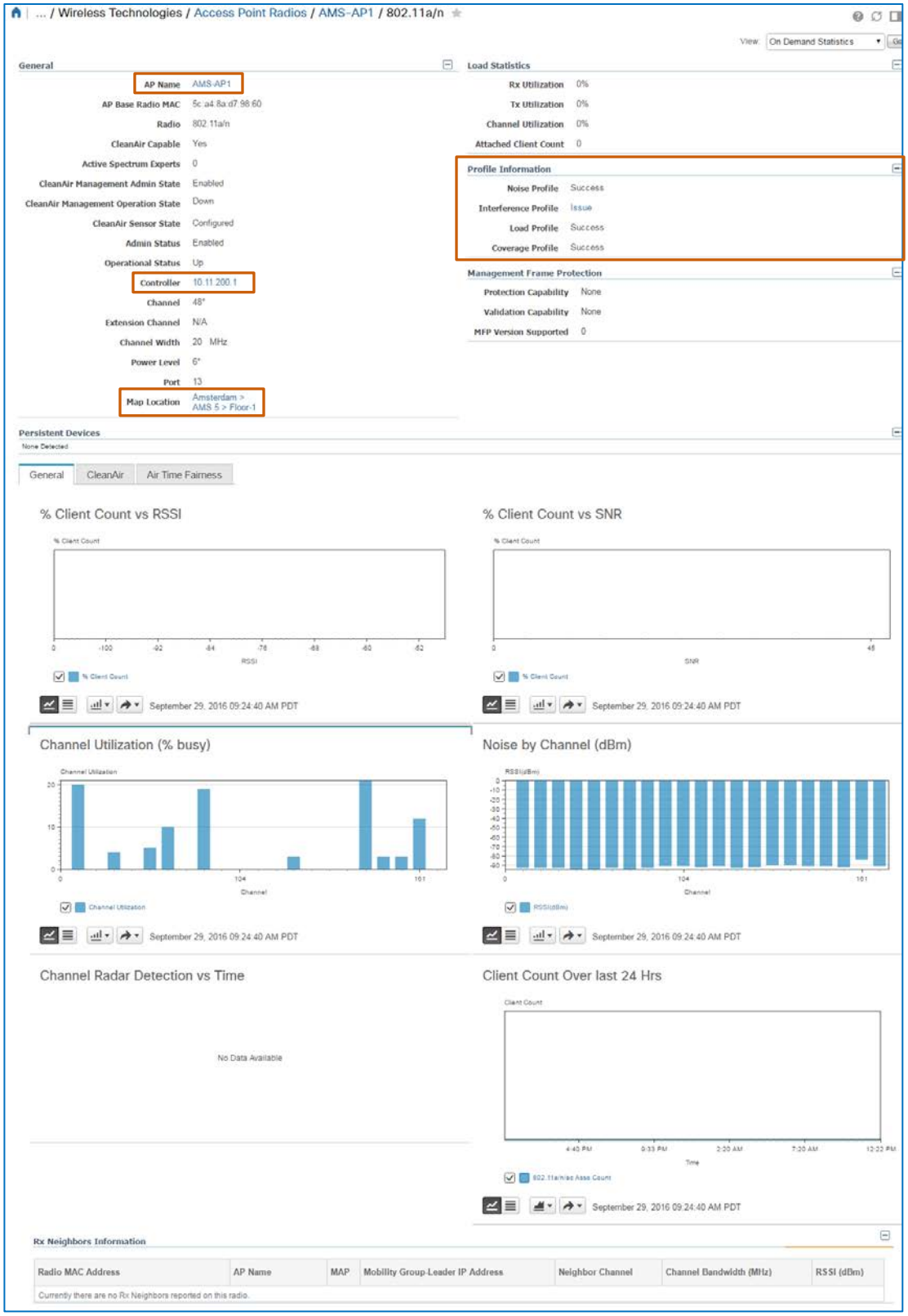
You can review 802.11a/n and 802.11b/g/n access point radio configuration details and performance metrics.

To open AP radio details:

- In the AP radio **360⁰ View** pop-up window, on the applicable tab, click the **Radio Interface Details Value** link.



The system navigates to and opens the AP radio details and provides links to the access point device, associated wireless LAN controller, the wireless site map that contains the AP radio, and the profiles available to apply to the radio.

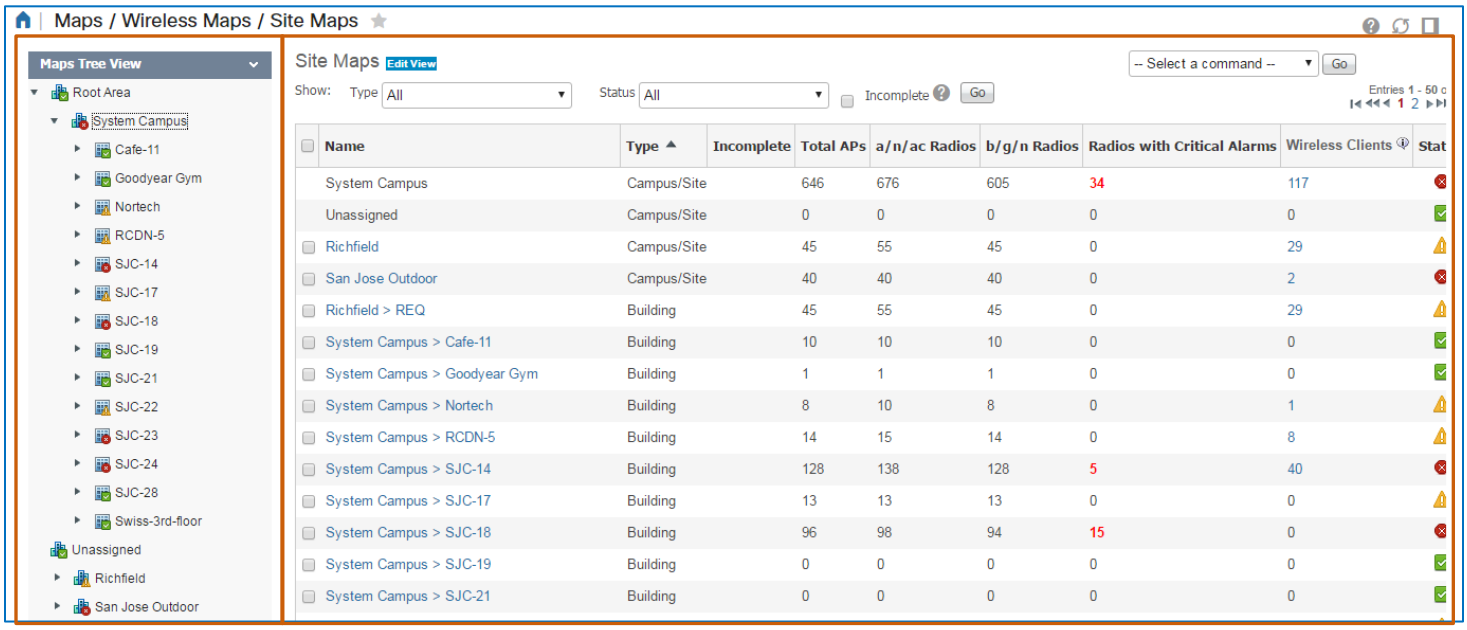


Wireless Site Maps

Overview

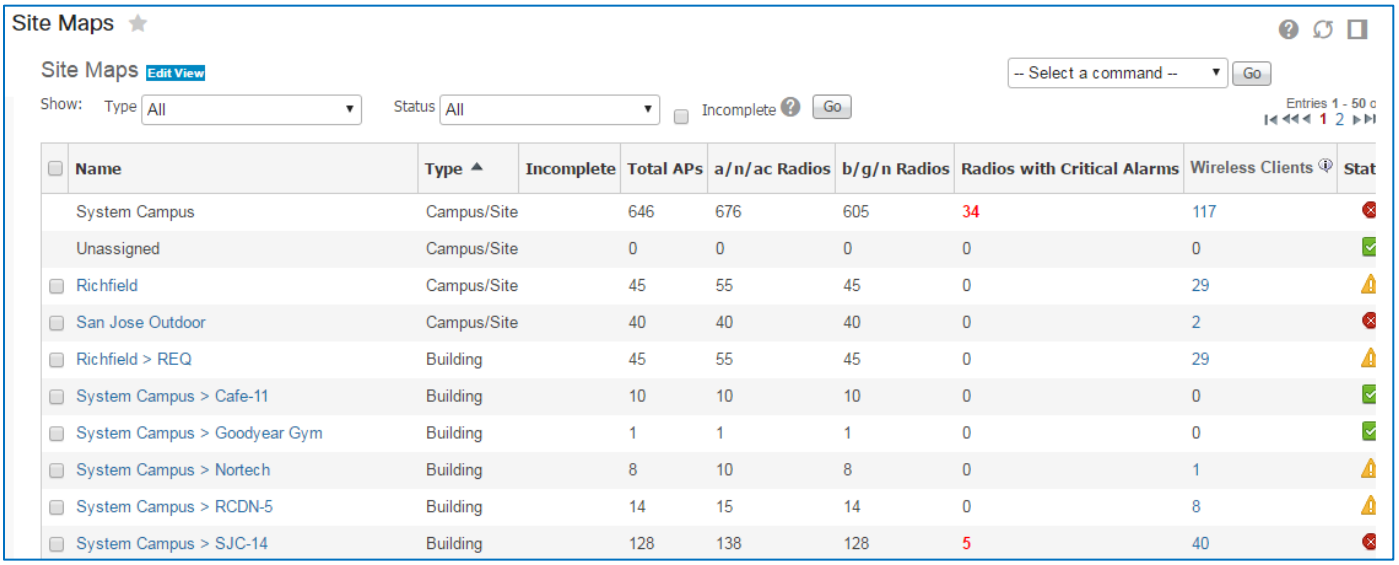
Wireless site maps illustrate the portions of the network that they represent, including device and interface relationships, neighbors, associated alarms, and the circuit and network connections.

System users organize wireless site maps by physical locations, which the system lists in the **Maps Tree View** and in the **Site Maps** list.



Name	Type	Incomplete	Total APs	a/n/ac Radios	b/g/n Radios	Radios with Critical Alarms	Wireless Clients	Stat
System Campus	Campus/Site		646	676	605	34	117	
Unassigned	Campus/Site		0	0	0	0	0	
Richfield	Campus/Site		45	55	45	0	29	
San Jose Outdoor	Campus/Site		40	40	40	0	2	
Richfield > REQ	Building		45	55	45	0	29	
System Campus > Cafe-11	Building		10	10	10	0	0	
System Campus > Goodyear Gym	Building		1	1	1	0	0	
System Campus > Nortech	Building		8	10	8	0	1	
System Campus > RCDN-5	Building		14	15	14	0	8	
System Campus > SJC-14	Building		128	138	128	5	40	
System Campus > SJC-17	Building		13	13	13	0	0	
System Campus > SJC-18	Building		96	98	94	15	0	
System Campus > SJC-19	Building		0	0	0	0	0	
System Campus > SJC-21	Building		0	0	0	0	0	

Physical locations can include an entire site, also referred to as a campus, buildings at the site, floors in a building, and outdoor areas.

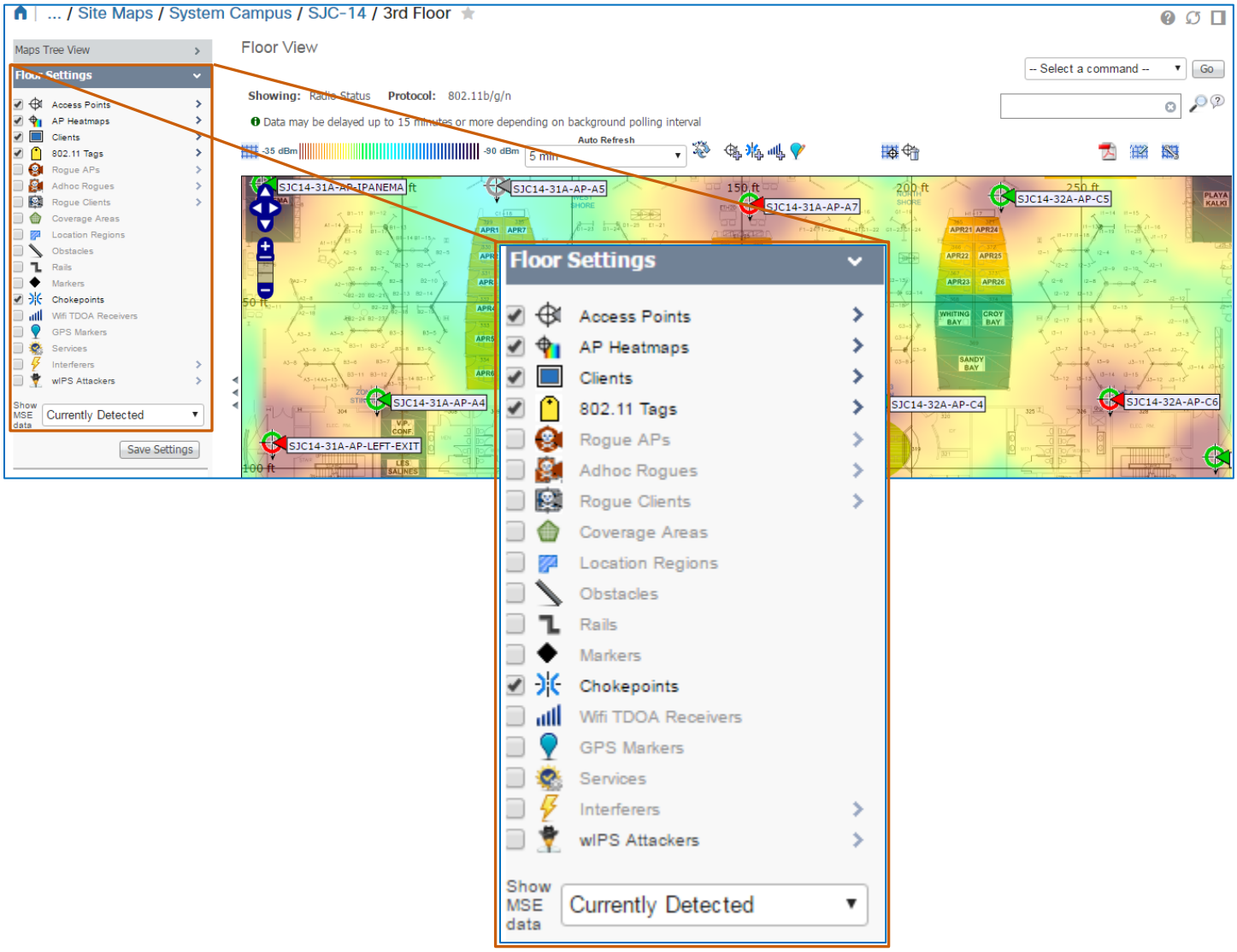


Name	Type	Incomplete	Total APs	a/n/ac Radios	b/g/n Radios	Radios with Critical Alarms	Wireless Clients	Stat
System Campus	Campus/Site		646	676	605	34	117	
Unassigned	Campus/Site		0	0	0	0	0	
Richfield	Campus/Site		45	55	45	0	29	
San Jose Outdoor	Campus/Site		40	40	40	0	2	
Richfield > REQ	Building		45	55	45	0	29	
System Campus > Cafe-11	Building		10	10	10	0	0	
System Campus > Goodyear Gym	Building		1	1	1	0	0	
System Campus > Nortech	Building		8	10	8	0	1	
System Campus > RCDN-5	Building		14	15	14	0	8	
System Campus > SJC-14	Building		128	138	128	5	40	

You can filter the list by location or alarm severity based on what you need to monitor.

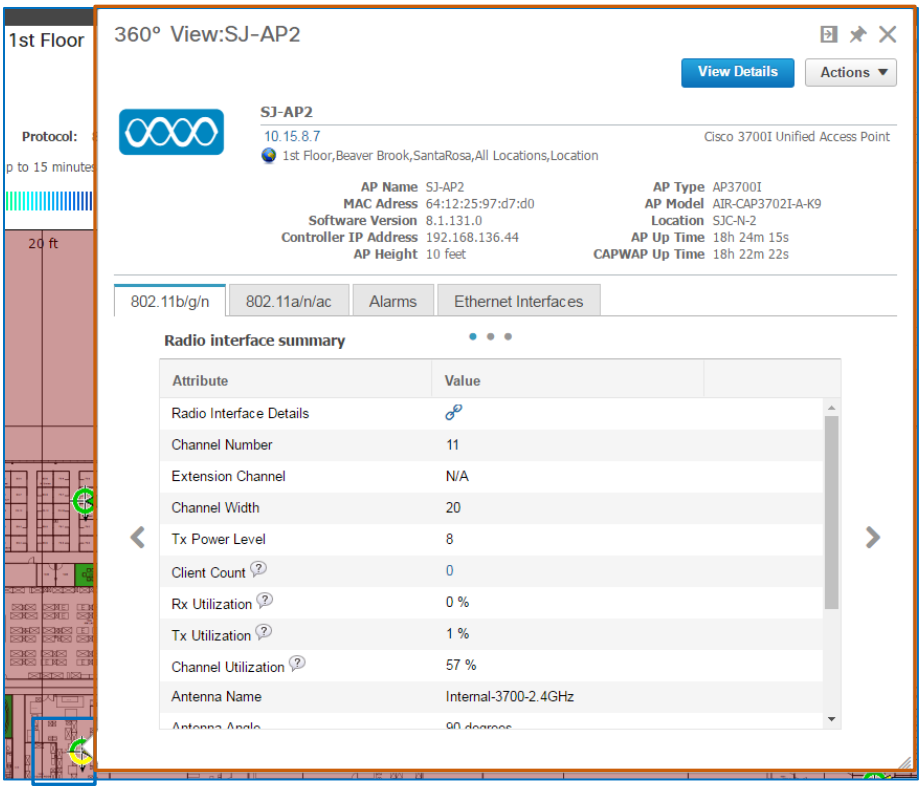
You can add a location map or a building to a location. You also can move, copy, or remove locations or buildings, adjust map properties, import or export maps, or make certain changes at a floor level.

At a floor level, you can select or clear attributes to include or remove them from the map.



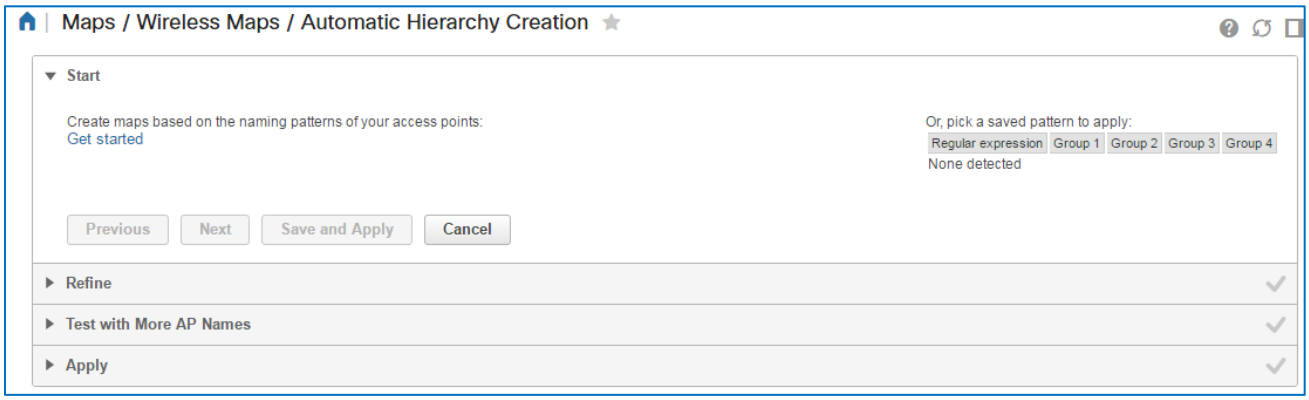
You can manage the floor configuration to a significant level of detail for better accuracy in coverage calculations and in identifying potential points of issues.

At an access point device level, you can open the device's **360⁰ View** pop-up window.



Generating Maps Automatically

System users also can generate maps by using the Automatic Hierarchy Creation tool. The tool follows access point device naming patterns to assign access point devices to floor level maps.



To begin monitoring the devices by using the maps, a user must configure such details as floor height, dimensions, construction materials, and interior objects, all of which can affect access point radio performance.

To filter the list to show maps that system users have not yet configured:

- On the **Site Maps** page, beside the **Go** button, select the **Incomplete** check box.

Links

To Product Information

Visit the Cisco Web site to learn more about Cisco© Prime Infrastructure.

Visit the Cisco Web site to review or download technical documentation.

To Training

Visit the Cisco Web site to access other Cisco© Prime Infrastructure learning opportunities.

Visit the Cisco Web site to access learning opportunities for other Cisco products.

To Contact Us

Send us a message with questions or comments about this job aid.