



Wireless Network Summary Data Overview

Cisco® Prime Infrastructure 3.1

Job Aid

Copyright Page

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

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

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

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

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

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

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

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

Wireless Network Summary Data Overview Job Aid

© Copyright 2016 Cisco Systems, Inc. All rights reserved.



Contents

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



Core Software Group

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° 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

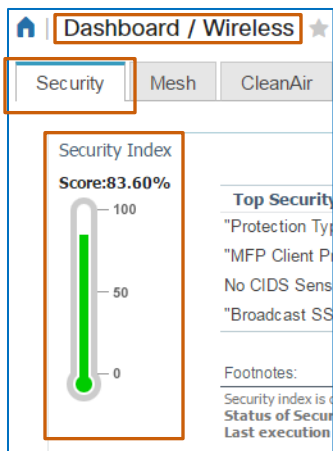
- ❖ Prime Infrastructure user interface navigation and behaviors
- ❖ Wireless networking concepts and practical knowledge

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

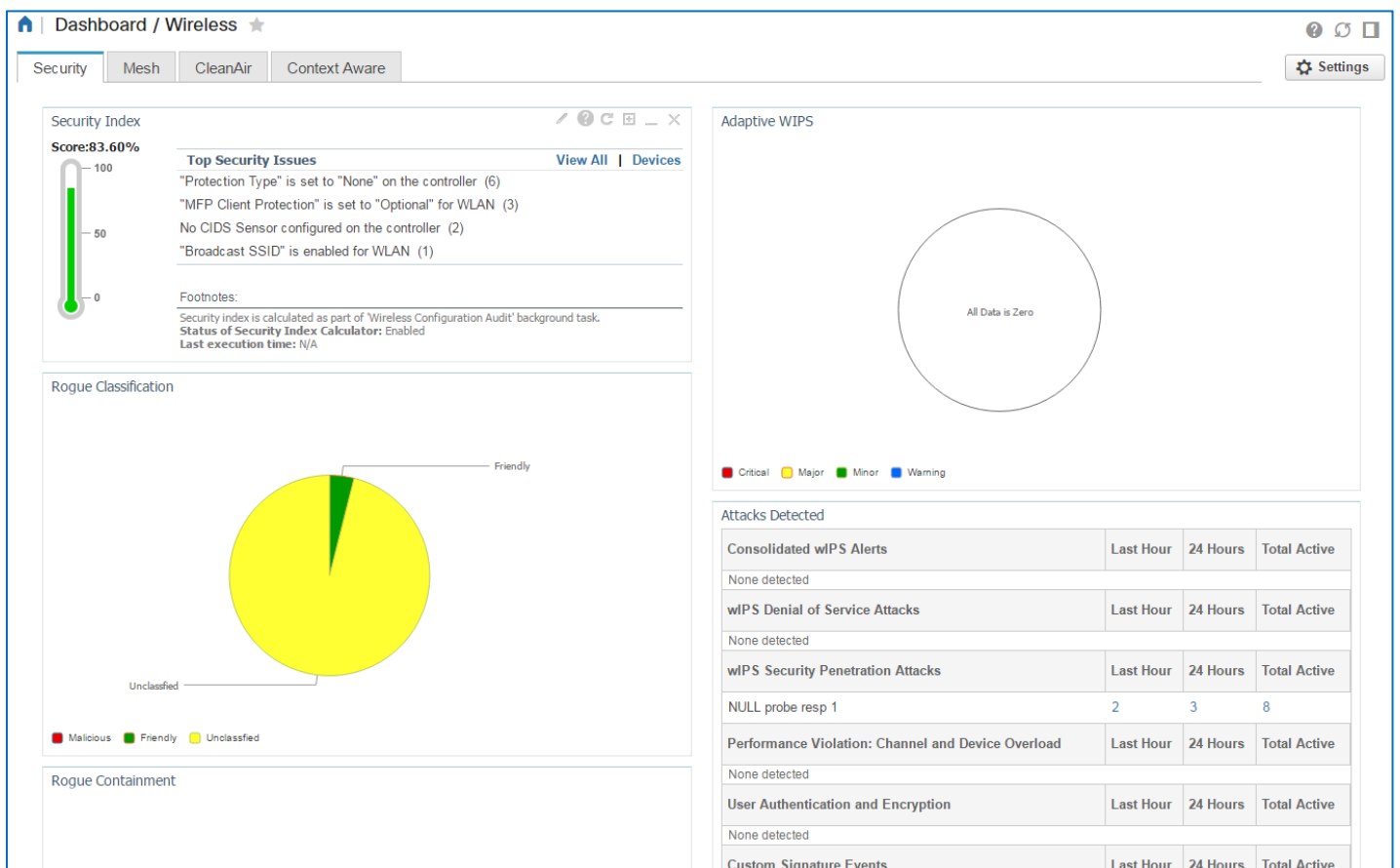
Introduction

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.



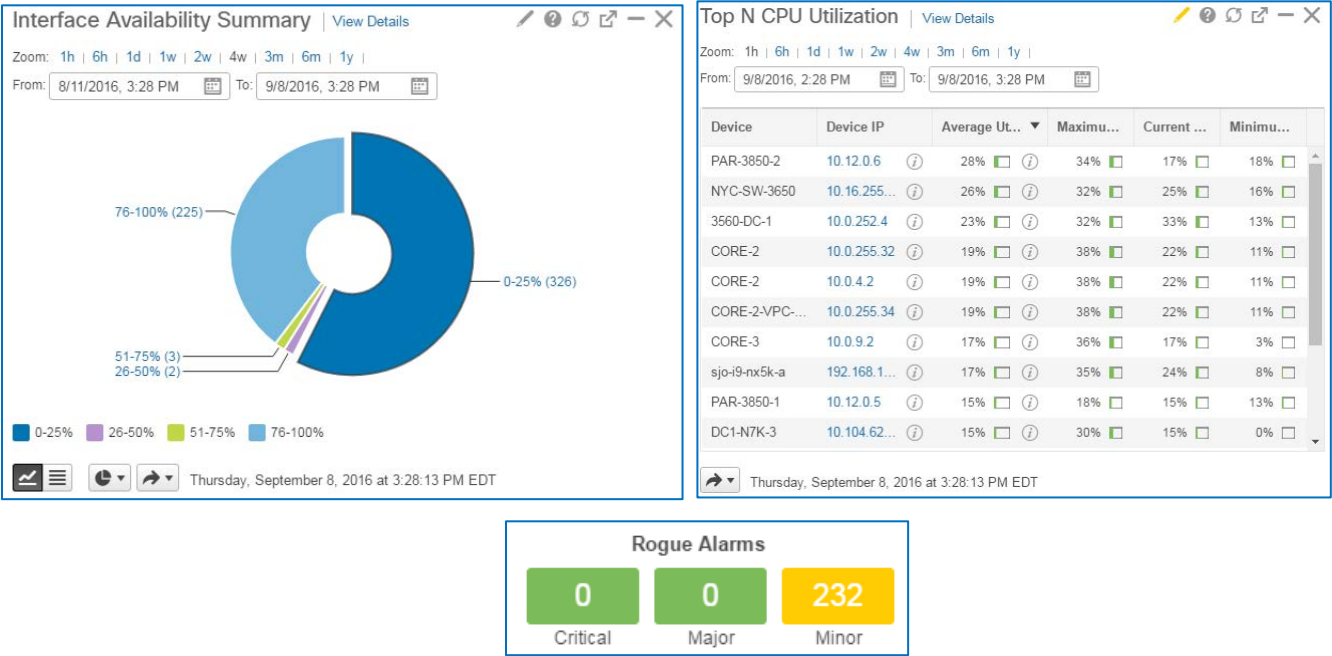
Note: While some dashboards combine reporting on both wired and wireless areas of the network, this job aid focuses on wireless network monitoring.

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.

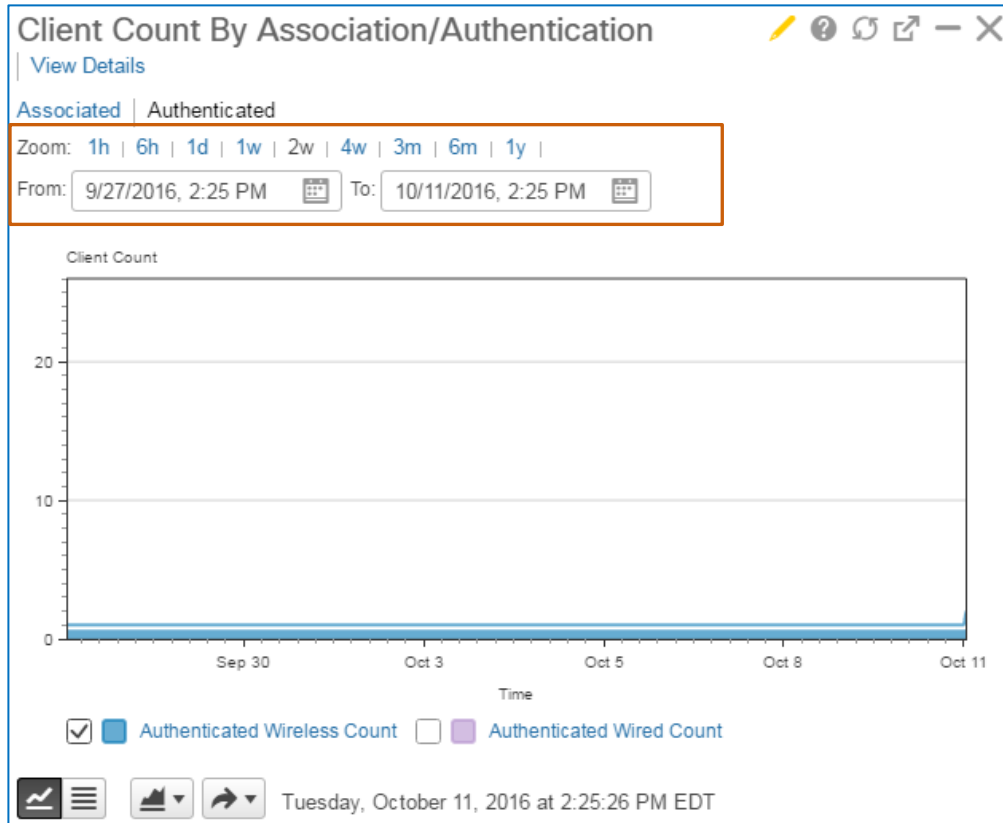
You can add or remove dashlets on existing tabs or configure custom tabs and add the dashlets that support your specific monitoring tasks.

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

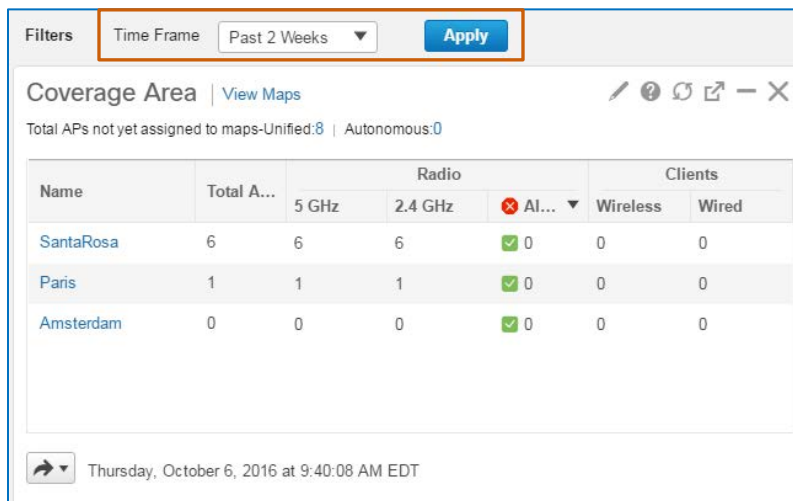
Managing Data Reporting Time Periods

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.



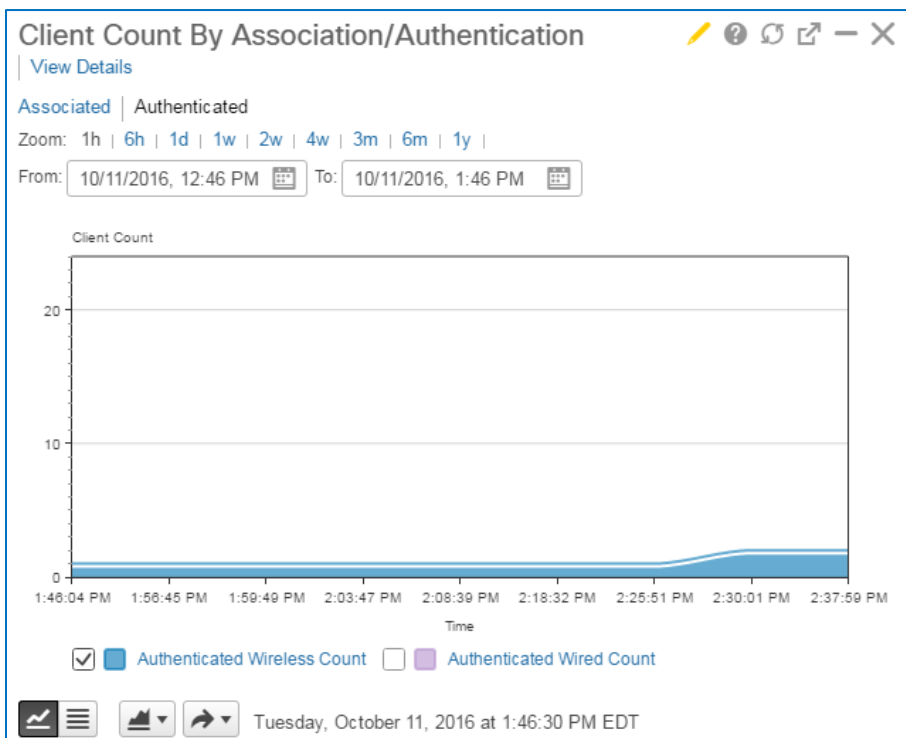
Name	Total A...	Radio			Clients	
		5 GHz	2.4 GHz	AI...	Wireless	Wired
SantaRosa	6	6	6	0	0	0
Paris	1	1	1	0	0	0
Amsterdam	0	0	0	0	0	0

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.

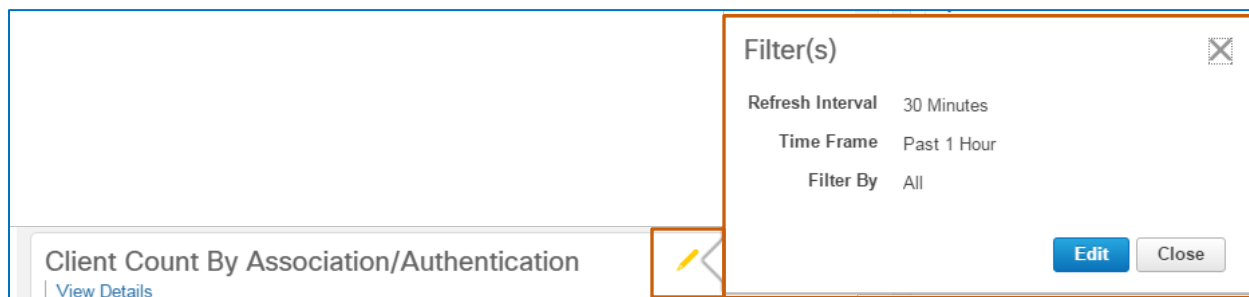
Using the **Client Count by Association/Authentication** dashlet as an example, you can see the types of settings that you can configure.



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.

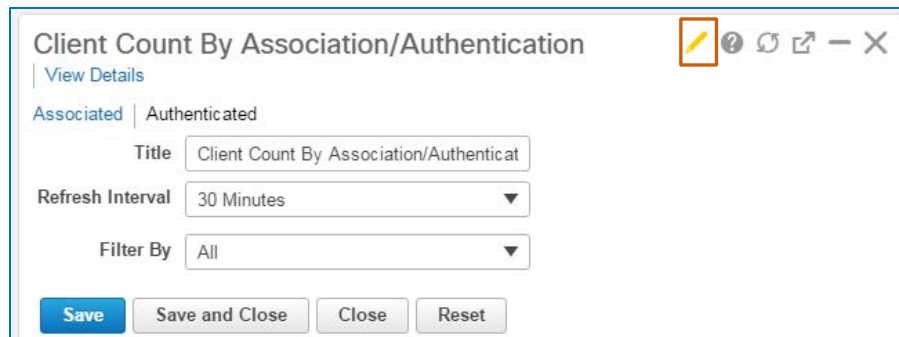


Note: Dashlets available on the **Wireless** dashboard do not provide the point feature.

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.

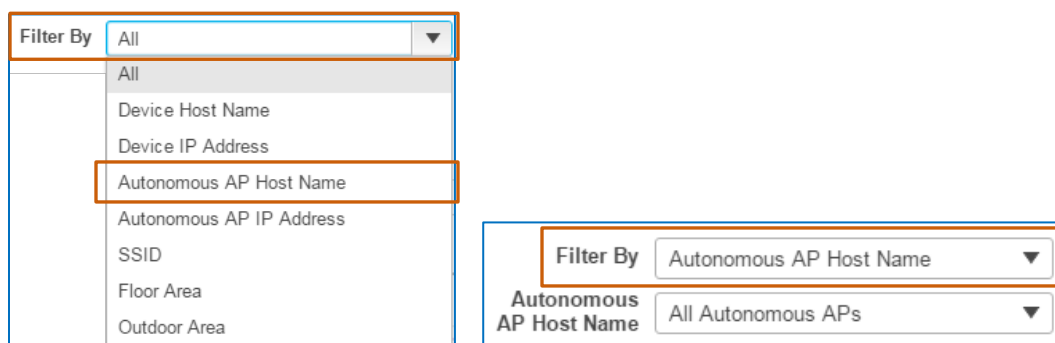
- ❖ Apply the optimal data refresh interval.



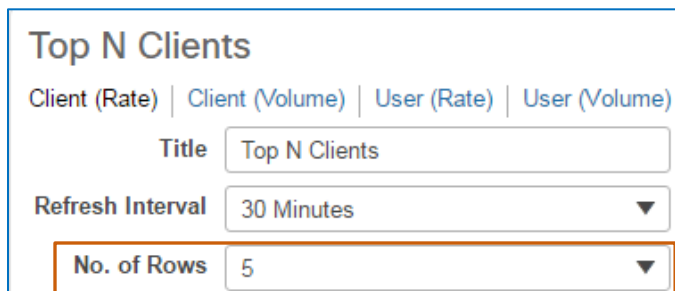
Note: When setting the data refresh rate, keep in mind that the system reports data based on polling intervals.

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.



Top N Clients

Client (Rate) | Client (Volume) | User (Rate) | User (Volume)

Title Top N Clients

Refresh Interval 30 Minutes ▼

No. of Rows 5 ▼

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.

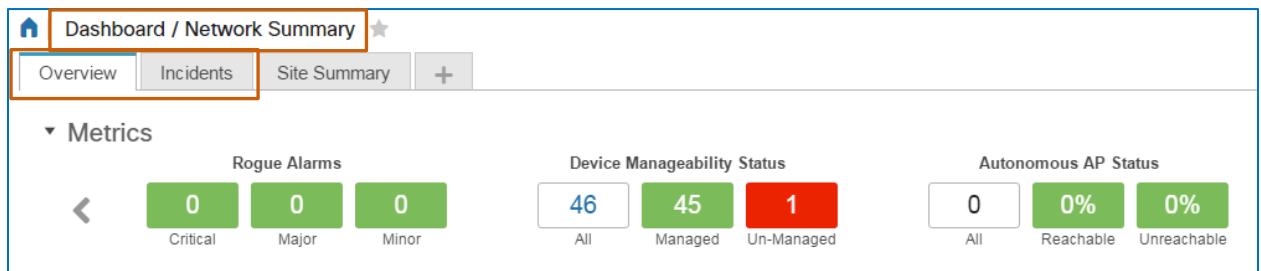


Tip: You also can monitor and manage wireless access point health on the **Network Health** dashboard.

For more information, [refer the Network Health Monitoring Overview job aid](#).

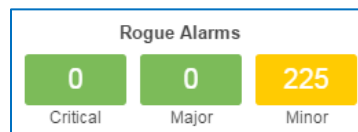
Network Summary Metrics Dashlets

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:

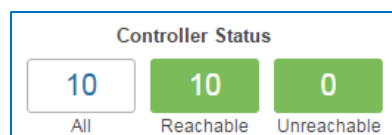
- ❖ Numbers of rogue alarms by severity level



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

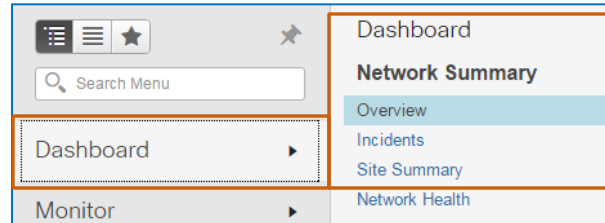


- ❖ The number of reachable and unreachable wireless LAN controllers out of the total number of each that the system is managing



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](#).

Coverage Area View Maps						
Total APs not yet assigned to maps-Unified:0 Autonomous:0						
Name	Total A...	Radio			Clients	
		5 GHz	2.4 GHz	Al...	Wireless	Wired
Paris Branch	6	6	6	4	0	0
Amsterdam Branch	12	12	12	2	1	0
India Branch	0	0	0	0	0	0
London Branch	0	0	0	0	0	0
New York Branch	0	0	0	0	0	0
Singapore Branch	0	0	0	0	0	0



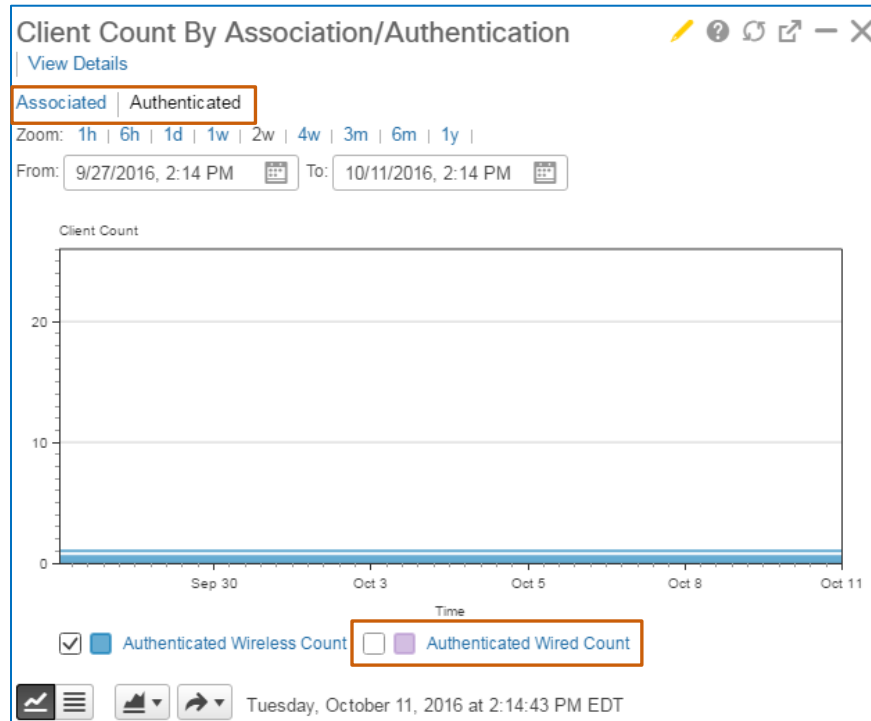
Wednesday, September 21, 2016 at 4:22:29 PM EDT

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.

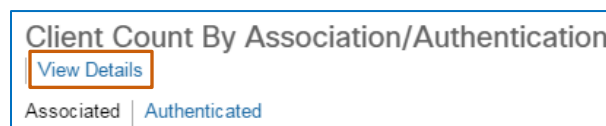
To see the number of wireless client by association or authentication:

- ❖ 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.

Monitor / Monitoring Tools / Clients and Users

TroubleshootTestDisableRemoveMoreTrack ClientsIdentify Unknown Users

Total 18

ShowAssociated Clients

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Location	Device Name	Interface	VLAN	Protocol	Status	As
	80:d6:05:55:61:ad	10.15.15.1	Dual-Stack	swong		Unknown	Root Area	SJ-WLC	prime-client	15	802.11n(5GHz)	Associated	28-5
	00:0c:29:d3:94:2c	192.168.138.16	IPv4	Unknown		Vmware	Unknown	sjo-i9-nx5k-a	Ethernet1/9	1381	802.3	Associated	03-4
	00:50:56:a6:00:05	192.168.139.23	IPv4	Unknown		Vmware	Unknown	sjo-i9-nx5k-a	Ethernet1/5	139	802.3	Associated	28-5
	00:50:56:a6:00:08	192.168.139.24	IPv4	Unknown		Vmware	Unknown	sjo-i9-nx5k-a	Ethernet1/1	139	802.3	Associated	28-5
	00:50:56:ad:11:eb	192.168.138.60	IPv4	Unknown		Vmware	Unknown	sjo-i9-nx5k-a	Ethernet1/8	1381	802.3	Associated	28-5
	02:fe:01:97:8e:32	10.12.100.180	IPv4	Unknown		Unknown	Unknown	PAR-3850-1	Gi1/0/19	100	802.3	Associated	01-4
	04:62:73:8c:97:0b	192.168.136.46	IPv4	Unknown		Unknown	Unknown	SPARE-STORE	Gi2/0/1	200	802.3	Associated	28-5
	1c:aa:07:a6:ae:01		Not Detected	Unknown		Cisco	Unknown	PAR-3850-1	Gi1/0/23	1	802.3	Associated	19-5
	1c:e6:c7:b6:03:80	10.12.192.2	IPv4	Unknown		Cisco	Unknown	PAR-3850-1	Gi1/0/23	1	802.3	Associated	19-5
	20:37:06:cf:b3:01		Not Detected	Unknown		Cisco	Unknown	SPARE-STORE	Fa2/0/2	1	802.3	Associated	28-5
	30:e4:db:90:06:6c	192.168.138.122	IPv4	Unknown		Cisco	Unknown	sjo-i9-nx5k-a	Ethernet1/6	1381	802.3	Associated	28-5
	30:e4:db:90:10:6e	192.168.138.124	IPv4	Unknown		Cisco	Unknown	sjo-i9-nx5k-a	Ethernet1/2	1381	802.3	Associated	28-5
	34:62:88:21:06:30		Not Detected	Unknown		Cisco	Unknown	SPARE-STORE	Gi2/0/1	200	802.3	Associated	28-5
	64:f6:9d:7d:b2:81		Not Detected	Unknown		Unknown	Unknown	SPARE-STORE	Fa2/0/4	1	802.3	Associated	28-5
	74:a0:2f:09:3a:8f		Not Detected	Unknown		Unknown	Unknown	SPARE-STORE	Fa2/0/6	1	802.3	Associated	28-5
	b8:38:61:70:66:00	192.168.136.254	IPv4	Unknown		Cisco	Unknown	SPARE-STORE	Gi2/0/1	200	802.3	Associated	29-5
	e0:0e:da:14:41:b0		Not Detected	Unknown		Unknown	Unknown	SPARE-STORE	Fa2/0/10	1	802.3	Associated	28-5
	e8:b7:48:7c:1b:46	192.168.138.125	IPv4	Unknown		Cisco	Unknown	sjo-i9-nx5k-a	Ethernet1/8	1381	802.3	Associated	28-5

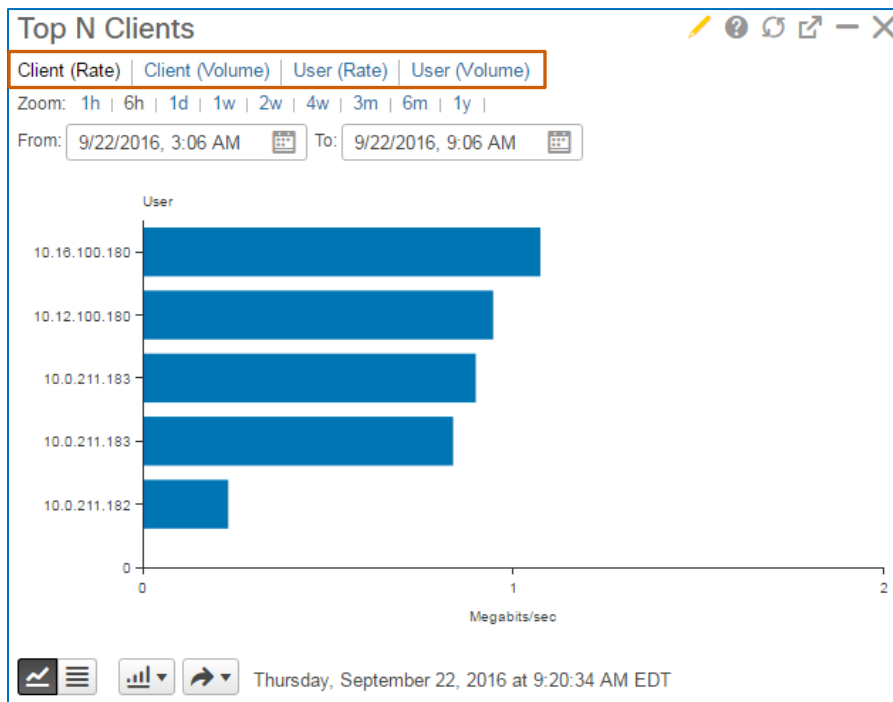
Clients or Network Users Generating the Highest Traffic Rates or Volumes

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.



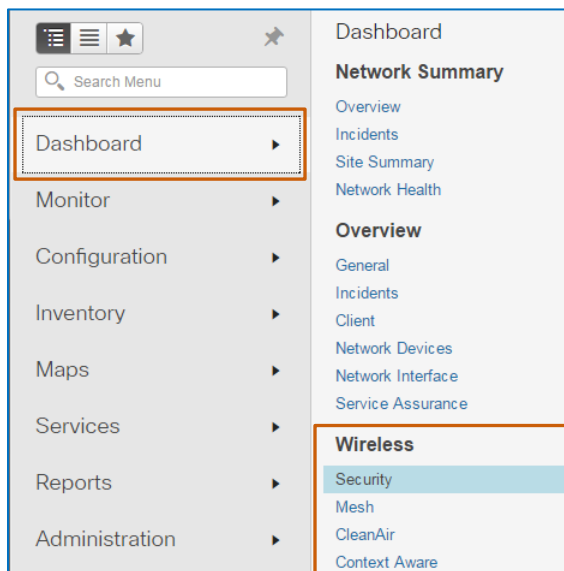
Wireless-Specific Summary Dashlets

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.

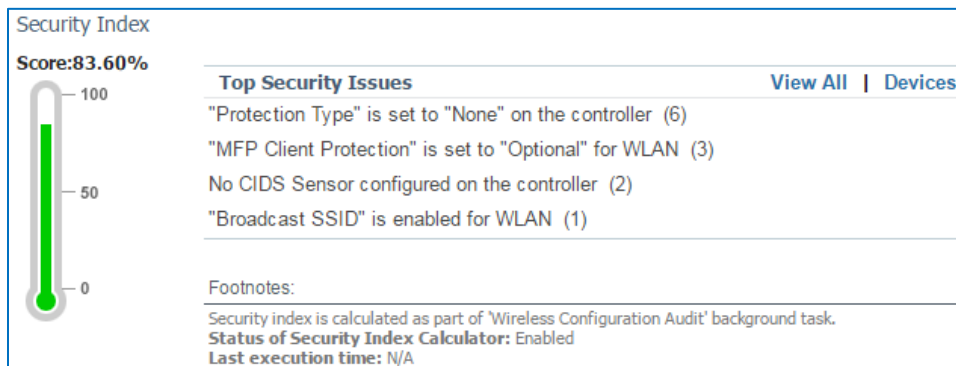
In the next release, the **Context Aware** dashlets will remain available to add to existing or custom dashboards.



General Security Monitoring Dashlets

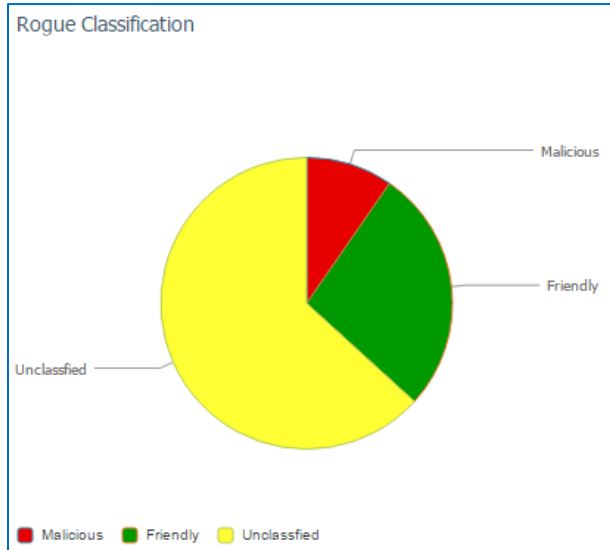
The **Security Index** dashlet reports the current [security index score](#) and the most critical security issues that the system has identified when running **Wireless Configuration Audit** jobs in Administration.

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.

Services / Mobility Services / Wireless Security

Before You Begin

Rogue Policy

Rogue Rules

wIPS Profile

Devices

Before You Begin
Welcome to Wireless Security configuration wizard. This wizard will allow you to configure Rogue Policy, Rogue Rule and wIPS Profile.

Rogue Policy:
Rogue Policy has three pre-configured rogue policy settings for Rogue Detection and Containment - **Low, High, Critical**. Custom settings can also be applied by selecting Custom checkbox.

Rogue Rules:
Rogue Rules can be created to classify Rogues as Malicious and Friendly. Rogue Rules can also be created to match user-configured SSID

wIPS Profile:
wIPS Profiles can be easily created by choosing one of the preset profiles. The profile can be further customized by selecting the wIPS signatures to be detected and contained. This feature requires the Adaptive wIPS license and also Cisco Wireless LAN Controllers should be synchronized with Cisco Mobility Services Engine.

Devices:
Select the Cisco Wireless LAN Controllers in order to apply settings as selected in previous screens.

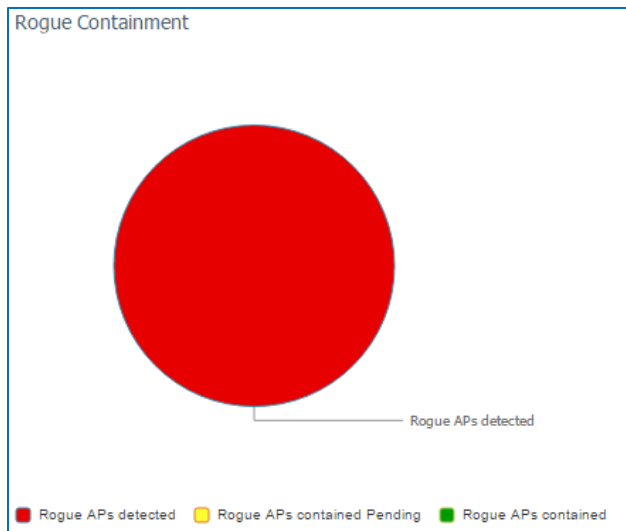
Classifying rogues accurately is a key step when configuring wireless security, which helps avoid misreported rogues or flooding of inaccurate rogue- or security-related alarms.

When you see that the system is reporting disproportionate numbers of unclassified rogue access points, or significant numbers of malicious rogues with no attacks or other issues are occurring, 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.

MFP Attacks			
MFP Attacks	Last Hour	24 Hours	Total Active
None detected			
Client Security Events			
Events	Last Hour	24 Hours	Total Active
None detected			
AP Threats/Attacks			
AP Threats/Attacks	Last Hour	24 Hours	Total Active
None detected			

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).

Dashboard / Wireless

Security
Mesh
CleanAir
Context Aware
Settings

Most Recent Mesh Alarms (5)

Failure Source	Timestamp	Message
00:1e:14:48:2c:0f	14-Oct-2016,07:55:45 PDT	MESH '00:1e:14:48:2c:0f' fails to authenticate with controller beca...
24:01:c7:f6:2f:ff	14-Oct-2016,07:53:03 PDT	MESH '24:01:c7:f6:2f:ff' fails to authenticate with controller beca...
18:9c:5d:71:36:3f	14-Oct-2016,07:21:50 PDT	MESH '18:9c:5d:71:36:3f' fails to authenticate with controller beca...
Site5_22-30,18:9c:...	14-Oct-2016,07:02:55 PDT	MESH 'Site5_22-30,18:9c:5d:71:47:70' has SNR on backhaul link as '1...
50:1c:bf:48:a3:ef	13-Oct-2016,12:55:44 PDT	MESH '50:1c:bf:48:a3:ef' fails to authenticate with controller beca...

Mesh Worst SNR Link

Parent AP Name	Child AP Name	Link SNR
Site4_13-2	Site4_7-09	9
SJC24-RAP-EAST	Site5_21-28	9
Site4_7-09	Site4_6-26	10
SJC22-ROOF-MAP	Site5_22-30	10
SJC19-ROOF-MAP	Site4_12-33	13

Mesh Parent Changing AP

AP Name	Parent Name	Parent Changes/Min
Site4_5-09	Site4_11-14	151
Site4_10-28	Site4_6-1	105
Site4_6-1	Site4_7-09	31
Site4_16-19	Site4_15-2	24
Site4_17-6	SJC14-RAP-SOUTH	23

Mesh Worst Node Hop Count

AP Name	Hop Count	Parent AP Name
SJC6-RAP	7	Site4_6-1
Site4_6-10	7	Site4_5-09
Site4_10-28	7	Site4_5-09
Site4_5-09	6	Site4_11-08
Site4_6-1	6	Site4_11-08

Mesh Worst Packet Error Rate

Parent AP Name	Child AP Name	Packet Error Rate(%)
Site4_8-17	Site4_2-04	9
SJC12-RAP-WEST	Site4_8-17	4
Site4_13-2	Site4_7-09	3
Site4_7-09	Site4_6-26	3
Site4_7-13	Site4_16-19	3

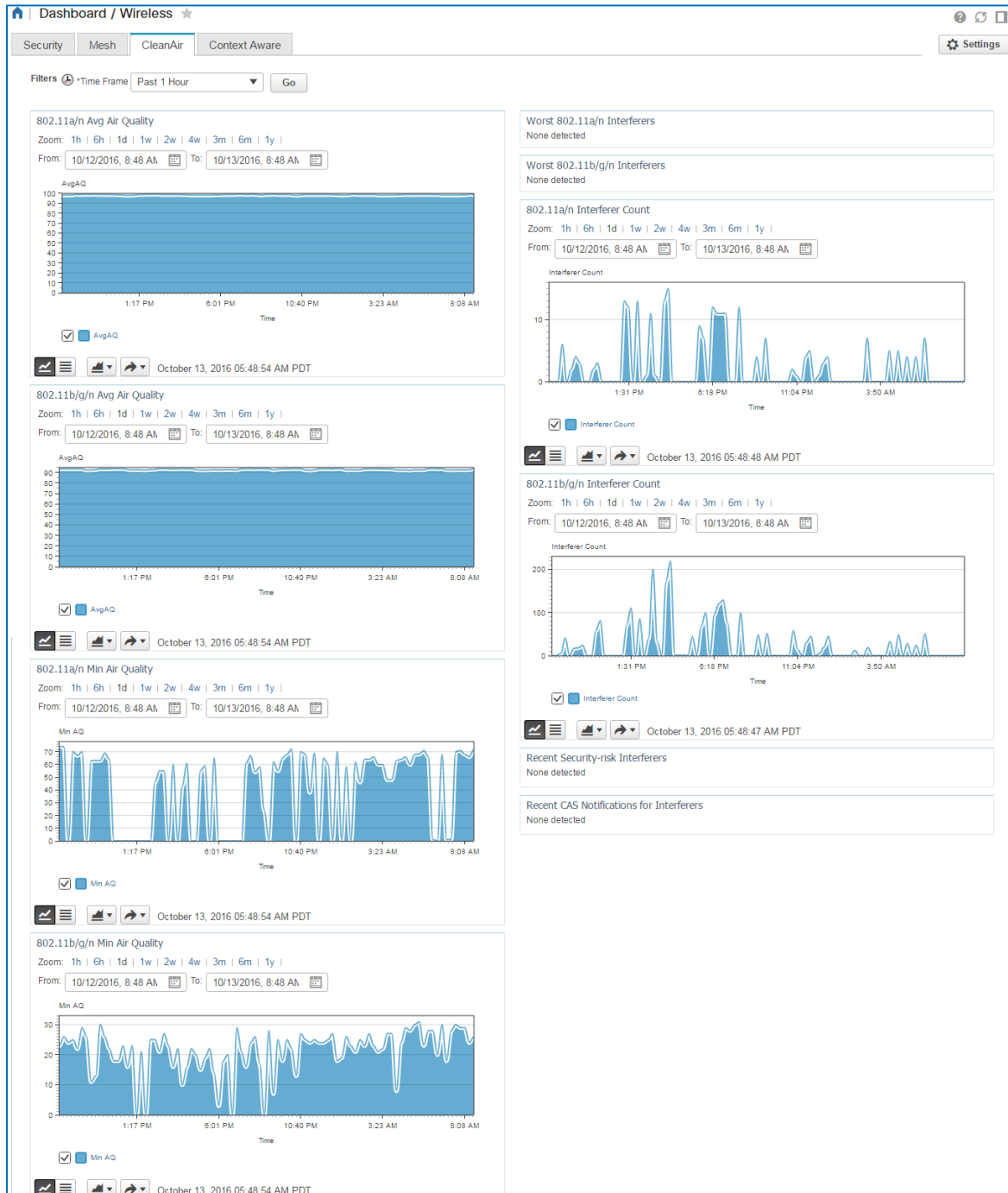
CleanAir Technology-Related Data

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.



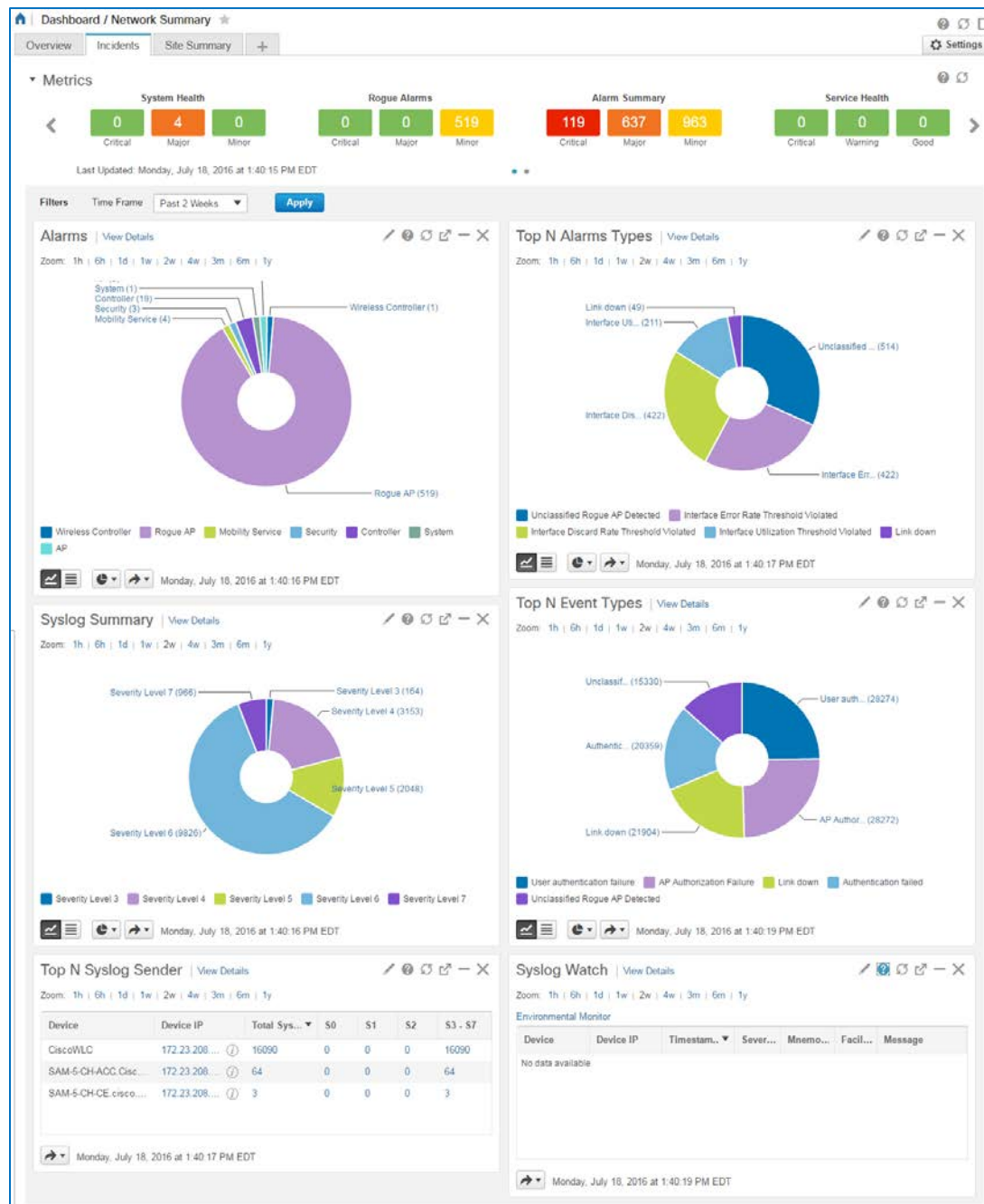
Note: To report CAS notifications, the system must include at least one Cisco® Mobility Services Engine.

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

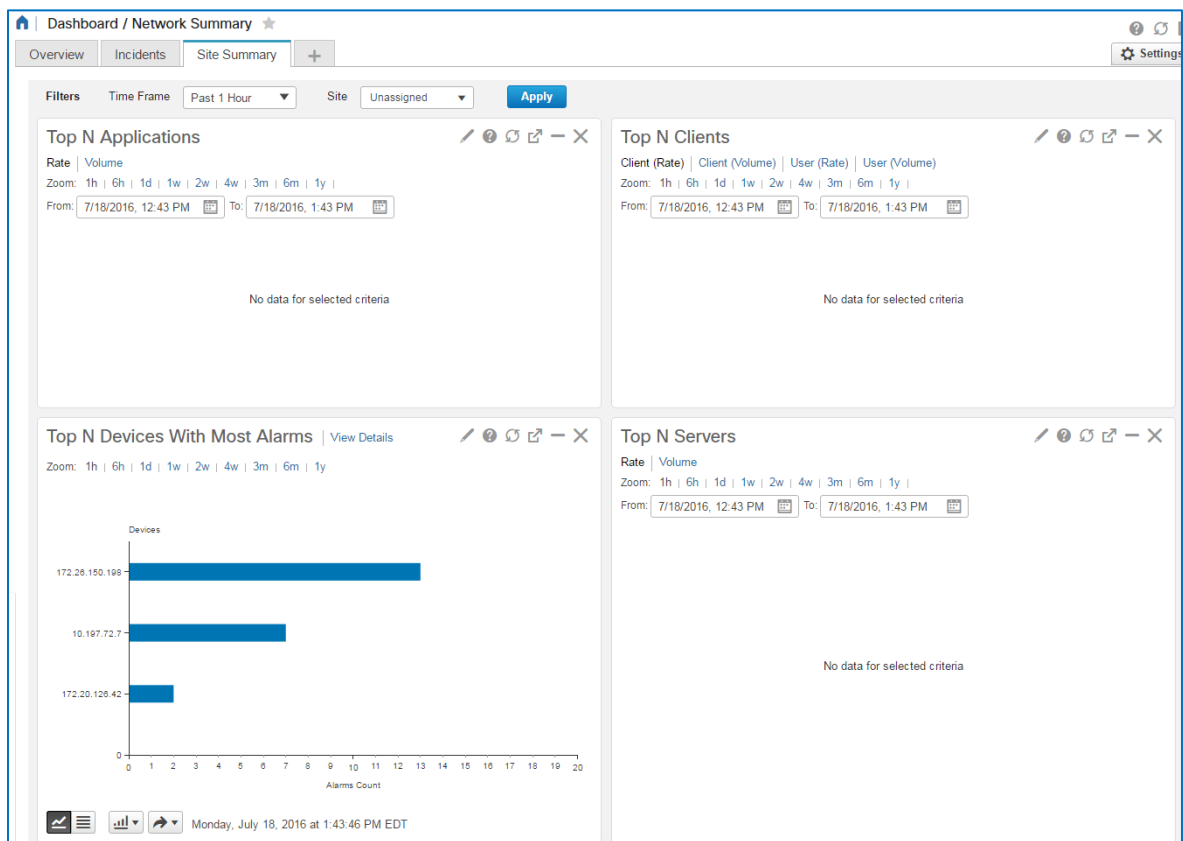
The **Most Recent Mesh Alarms** dashlet reports those alarms occurring on mesh-configured access points during the previous 24 hours at a rolling interval from the current system time.

Most Recent Mesh Alarms (10)			
Failure Source	Timestamp	Message	
00:1e:14:48:2c:0f	13-Oct-2016,05:45:23 PDT	MESH '00:1e:14:48:2c:0f' fails to authenticate with controller beca...	
24:01:c7:f6:2f:ff	13-Oct-2016,05:38:10 PDT	MESH '24:01:c7:f6:2f:ff' fails to authenticate with controller beca...	
Site5_24-02,f4:0f...	13-Oct-2016,05:09:09 PDT	MESH 'Site5_24-02,f4:0f...' has SNR on backhaul link as '3...	
18:9c:5d:71:36:3f	13-Oct-2016,04:01:09 PDT	MESH '18:9c:5d:71:36:3f' fails to authenticate with controller beca...	
Site5_24-02,f4:0f...	13-Oct-2016,02:57:19 PDT	MESH 'Site5_24-02,f4:0f...' has SNR on backhaul link as '1...	

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 360° Views


Overview

Device **360° 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 **360° View** pop-up window.

360° View:AMS-AP1



AMS-AP1

10.11.15.3

Floor-1,AMS 5,Amsterdam,All Locations,Location

Cisco 3500I Unified Access Point

View Details

Actions

AP Name

AMS-AP1

AP Type

AP3500I

MAC Address

5c:a4:8a:d7:98:60

AP Model

AIR-CAP3502I-A-K9

Software Version

8.1.131.0

Location

default location

Controller IP Address

10.11.200.1

AP Up Time

52d 17h 58m 32s

AP Height

10 feet

CAPWAP Up Time

52d 17h 56m 54s


802.11a/n

802.11b/g/n

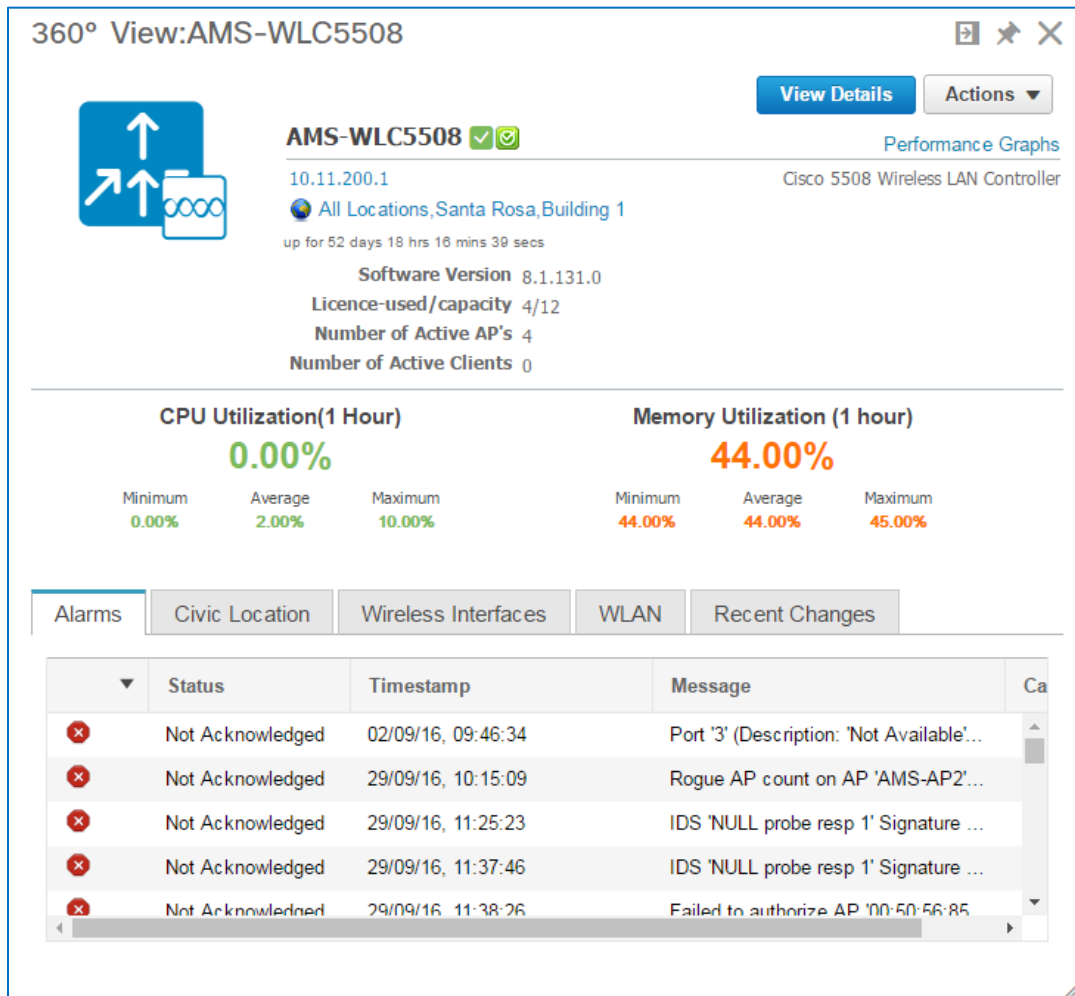
Alarms

Ethernet Interfaces


Radio interface summary

Attribute	Value
Radio Interface Details	
Channel Number	48
Extension Channel	N/A
Channel Width	20
Tx Power Level	6
Client Count	0
Rx Utilization	0 %
Tx Utilization	0 %
Channel Utilization	0 %
Antenna Name	Internal-3500i-5GHz
Antenna Angle	90 degrees

The following screenshot illustrates a wireless LAN controller **360° View** pop-up window.



360° View:AMS-WLC5508

AMS-WLC5508  [View Details](#) [Actions](#) [Performance Graphs](#)






10.11.200.1
All Locations, Santa Rosa, Building 1
Cisco 5508 Wireless LAN Controller
up for 52 days 18 hrs 16 mins 39 secs

Software Version 8.1.131.0
Licence-used/capacity 4/12
Number of Active AP's 4
Number of Active Clients 0

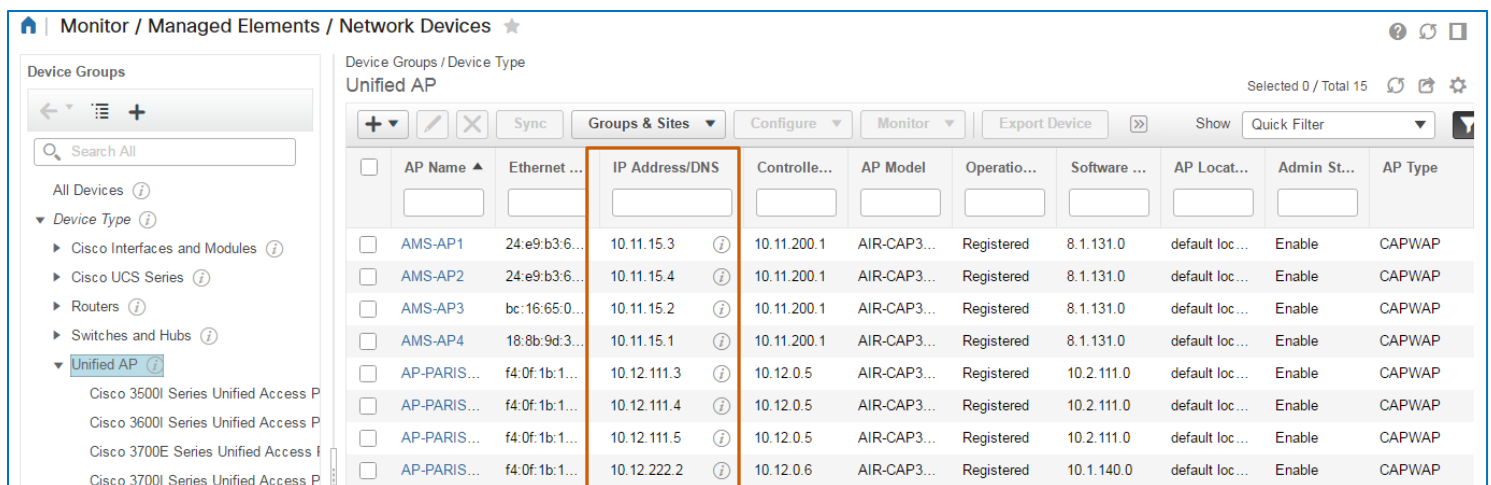
CPU Utilization(1 Hour) **0.00%**
Minimum 0.00% Average 2.00% Maximum 10.00%

Memory Utilization (1 hour) **44.00%**
Minimum 44.00% Average 44.00% Maximum 45.00%

Alarms Civic Location Wireless Interfaces WLAN Recent Changes

▼	Status	Timestamp	Message	Ca
	Not Acknowledged	02/09/16, 09:46:34	Port '3' (Description: 'Not Available'...	
	Not Acknowledged	29/09/16, 10:15:09	Rogue AP count on AP 'AMS-AP2'...	
	Not Acknowledged	29/09/16, 11:25:23	IDS 'NULL probe resp 1' Signature ...	
	Not Acknowledged	29/09/16, 11:37:46	IDS 'NULL probe resp 1' Signature ...	
	Not Acknowledged	29/09/16, 11:38:26	Failed to authorize AP '00-50-56-85'	

Most tables listing a device IP address provide access to **360° View** pop-up windows by using the information icon.



Monitor / Managed Elements / Network Devices

Device Groups / Device Type: Unified AP

Selected 0 / Total 15

AP Name	Ethernet ...	IP Address/DNS	Controlle...	AP Model	Operatio...	Software ...	AP Locat...	Admin St...	AP Type
AMS-AP1	24:e9:b3:6...	10.11.15.3	10.11.200.1	AIR-CAP3...	Registered	8.1.131.0	default loc...	Enable	CAPWAP
AMS-AP2	24:e9:b3:6...	10.11.15.4	10.11.200.1	AIR-CAP3...	Registered	8.1.131.0	default loc...	Enable	CAPWAP
AMS-AP3	bc:16:65:0...	10.11.15.2	10.11.200.1	AIR-CAP3...	Registered	8.1.131.0	default loc...	Enable	CAPWAP
AMS-AP4	18:8b:9d:3...	10.11.15.1	10.11.200.1	AIR-CAP3...	Registered	8.1.131.0	default loc...	Enable	CAPWAP
AP-PARIS...	f4:0f:1b:1...	10.12.111.3	10.12.0.5	AIR-CAP3...	Registered	10.2.111.0	default loc...	Enable	CAPWAP
AP-PARIS...	f4:0f:1b:1...	10.12.111.4	10.12.0.5	AIR-CAP3...	Registered	10.2.111.0	default loc...	Enable	CAPWAP
AP-PARIS...	f4:0f:1b:1...	10.12.111.5	10.12.0.5	AIR-CAP3...	Registered	10.2.111.0	default loc...	Enable	CAPWAP
AP-PARIS...	f4:0f:1b:1...	10.12.222.2	10.12.0.6	AIR-CAP3...	Registered	10.1.140.0	default loc...	Enable	CAPWAP

To open a 360° view pop-up window:

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

Network Devices ★

Device Groups / Device Type
Unified AP

	AP Name ▲	Ethernet ...	IP Address/DNS	Controlle...
<input type="checkbox"/>	AMS-AP1	24:e9:b3:6...	10.11.15.3	10.11.200.1
<input type="checkbox"/>	AMS-AP2	24:e9:b3:6...	10.11.15.4	10.11.200.1

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

The associated 360° View pop up window opens.

360° View:AMS-AP1

AMS-AP1
10.11.15.3
Cisco 3500I Unified

Floor-1,AMS 5,Amsterdam,All Locations,Location

AP Name AMS-AP1
MAC Address 5c:a4:8a:d7:98:60
Software Version 8.1.131.0
Controller IP Address 10.11.200.1
AP Height 10 feet

AP Type AP3500I
AP Model AIR-CAP3502I-A-K9
Location default location
AP Up Time 52d 18h 12m 31s
CAPWAP Up Time 52d 18h 10m 53s

802.11a/n | 802.11b/g/n | Alarms | Ethernet Interfaces

Radio interface summary

Attribute	Value
Radio Interface Details	🔗
Channel Number	48
Extension Channel	N/A
Channel Width	20
Tx Power Level	6
Client Count	0
Rx Utilization	0 %
Tx Utilization	0 %
Channel Utilization	0 %
Antenna Name	Internal-3500i-5GHz
Antenna Angle	90 degrees

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.



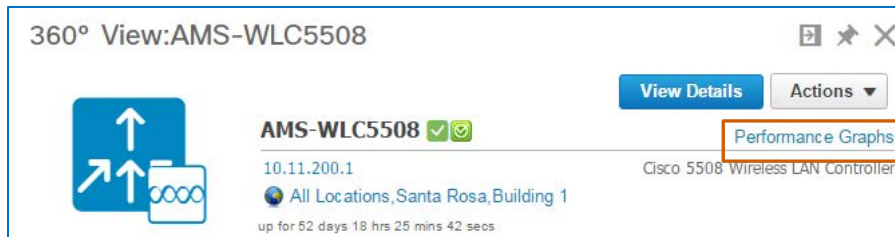
Note: For detailed information on device 360° pop-up window features, [refer to the Cisco Prime Infrastructure 3.1 User Guide](#).

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

Access to Performance Graphs

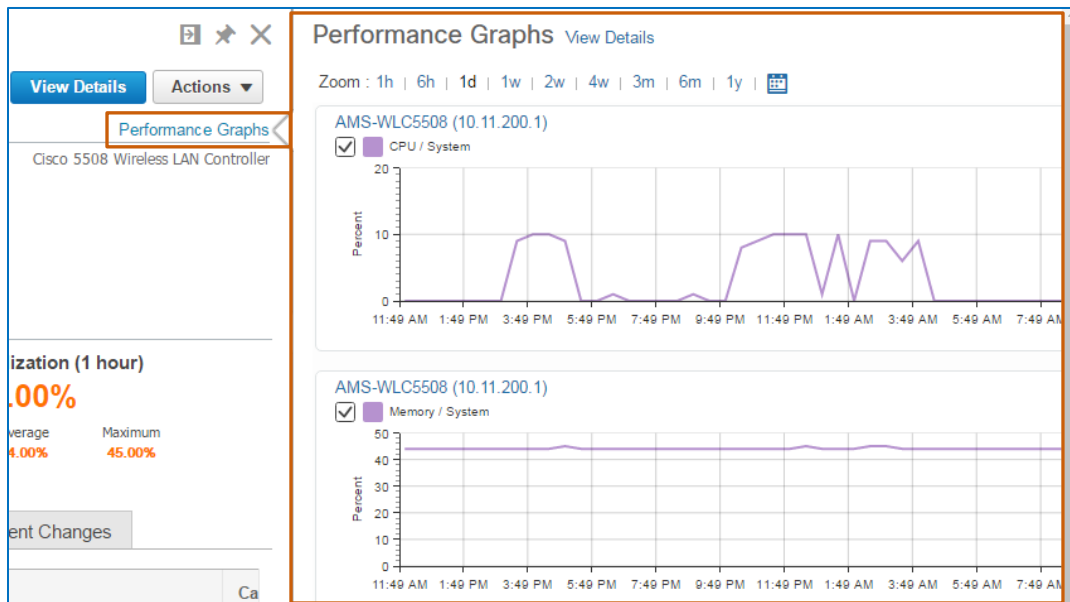
You can review current or evaluate historical performance data for key performance indicators (KPIs) by using the Performance Graphs feature.

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:

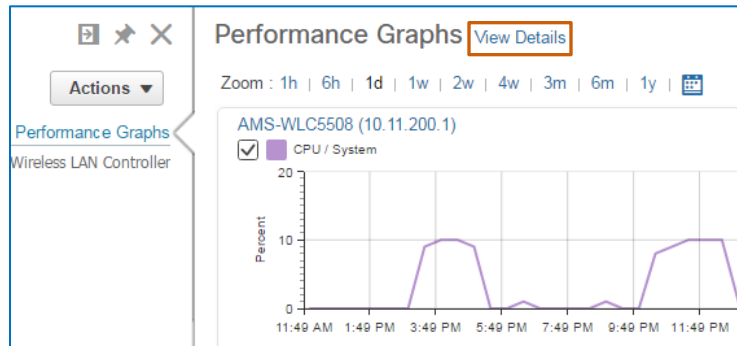
- ❖ In the **360° View** pop up window, below the **Actions** drop-down menu, click **Performance Graphs**.



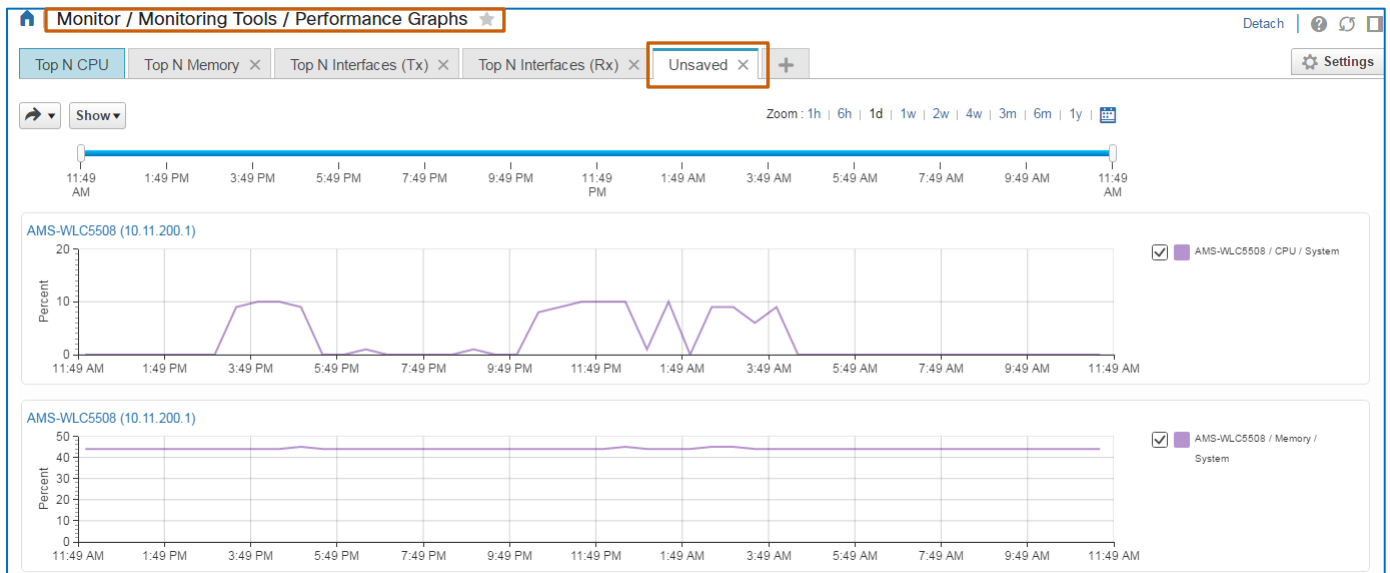
You can also navigate to display alarms and configuration changes in relationship to the KPI values for the component on which a graph is reporting. Correlating changing KPI values to alarm reporting or configuration changes can provide critical insight into possible issues or issue causes.

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

- ❖ In the **Performance Graphs** 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.



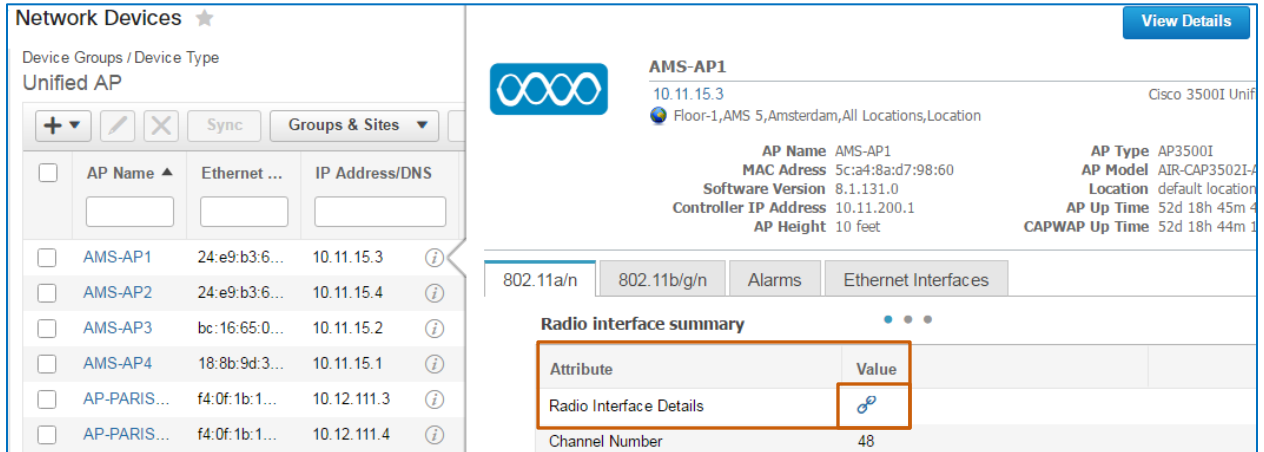
Tip: In this view, you also can display alarms and configuration changes in relationship to the KPI values for the device on which the graph is reporting. Correlating changing KPI values to alarm reporting or configuration changes can provide critical insight into possible issues or issue causes. For 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:

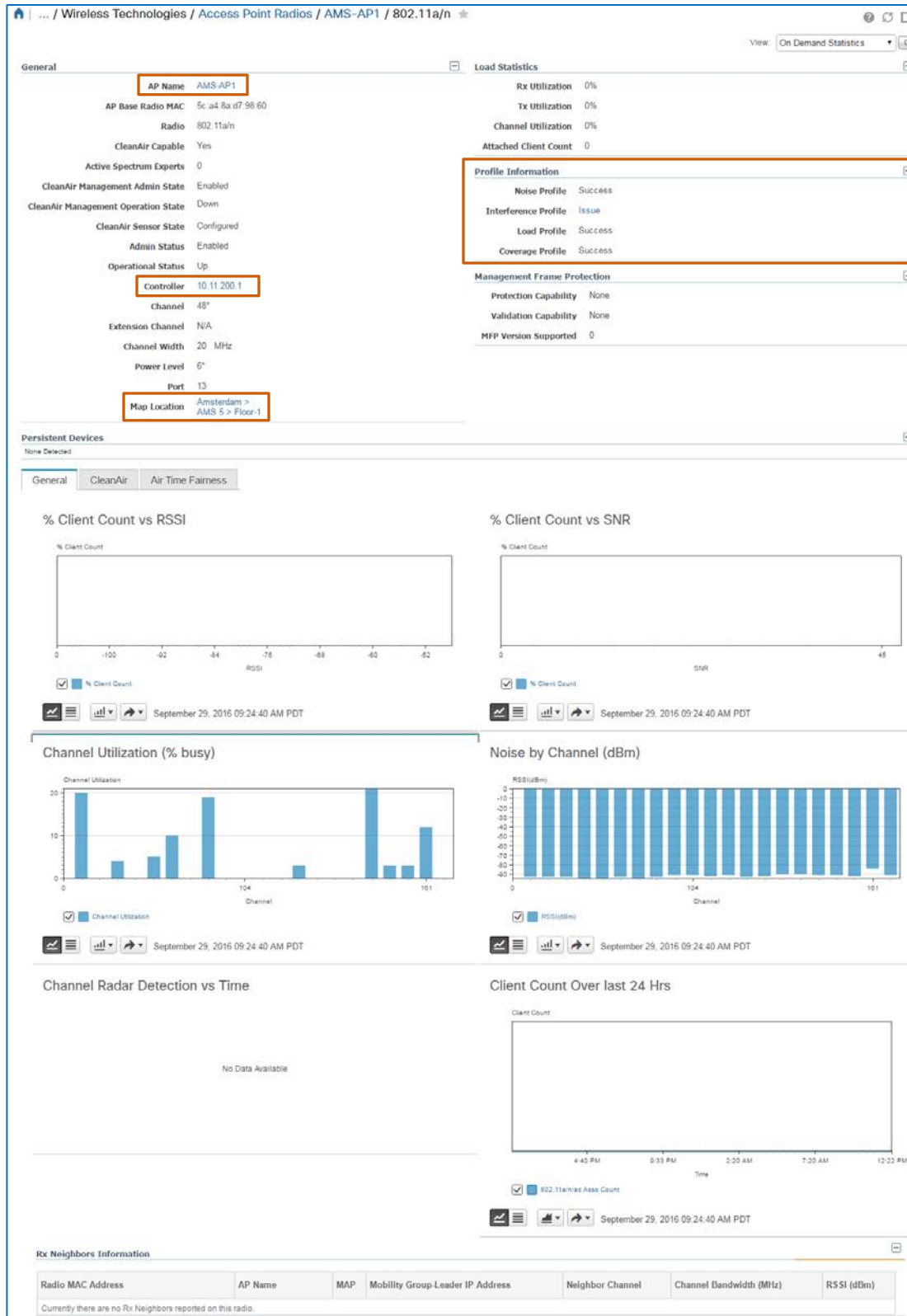
- ❖ In the AP radio **360° View** pop-up window, on the applicable tab, click the **Radio Interface Details Value** link.



The screenshot displays the Cisco Network Devices interface. On the left, a table lists several Unified APs. The main panel shows details for 'AMS-AP1' (10.11.15.3), including its location and various configuration parameters. Below this, the 'Radio interface summary' section is visible, with tabs for 802.11a/n, 802.11b/g/n, Alarms, and Ethernet Interfaces. The 802.11a/n tab is active, showing a table with 'Attribute' and 'Value' columns. A red box highlights the 'Radio Interface Details' row, which contains a link icon. Below this, the 'Channel Number' is listed as 48.

Attribute	Value
Radio Interface Details	Link Icon
Channel Number	48

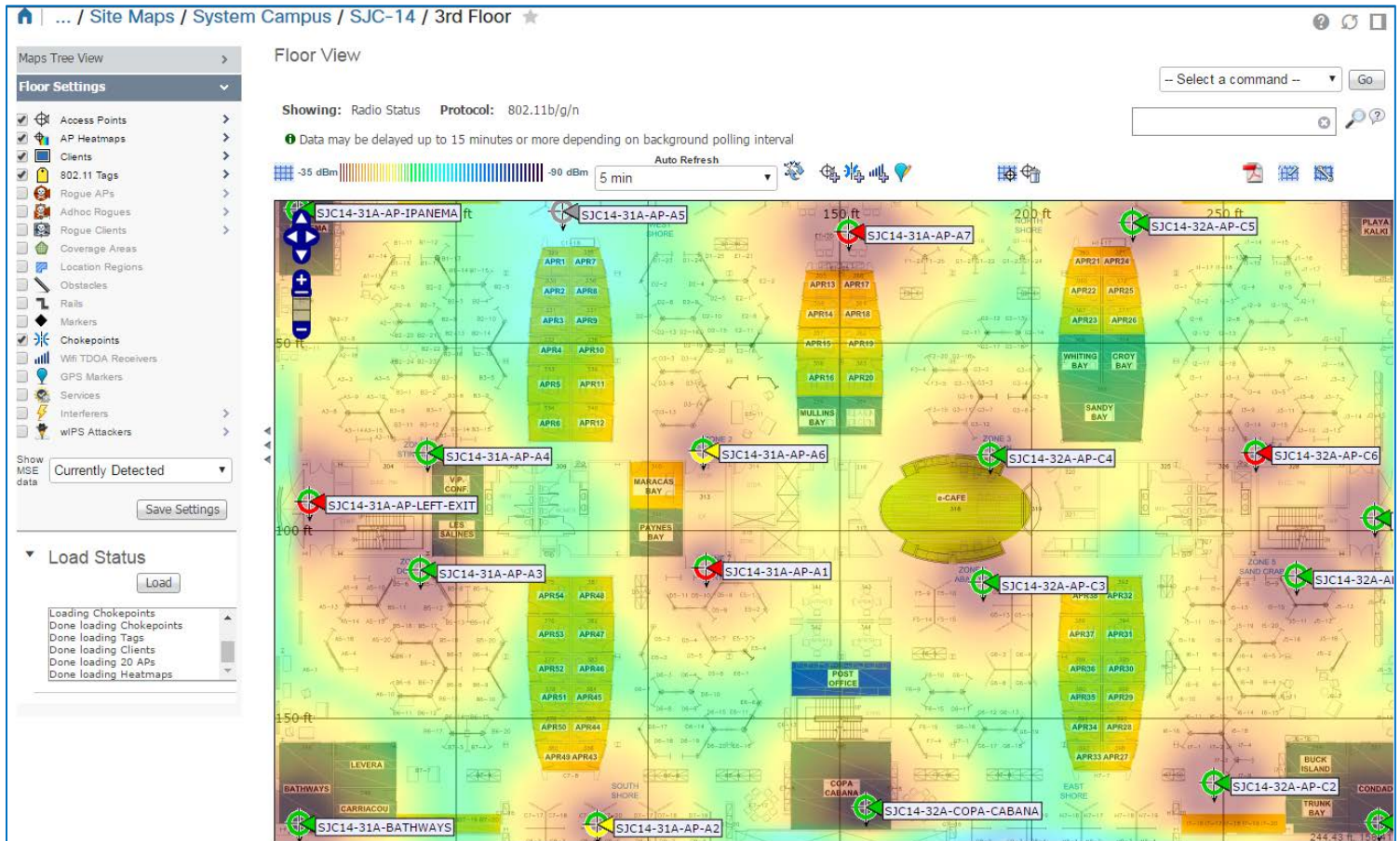
The system navigates to and opens the AP radio details and provides links to the access point device, associated wireless LAN controller, the wireless site map that contains the AP radio, and the profiles available to apply to the radio.



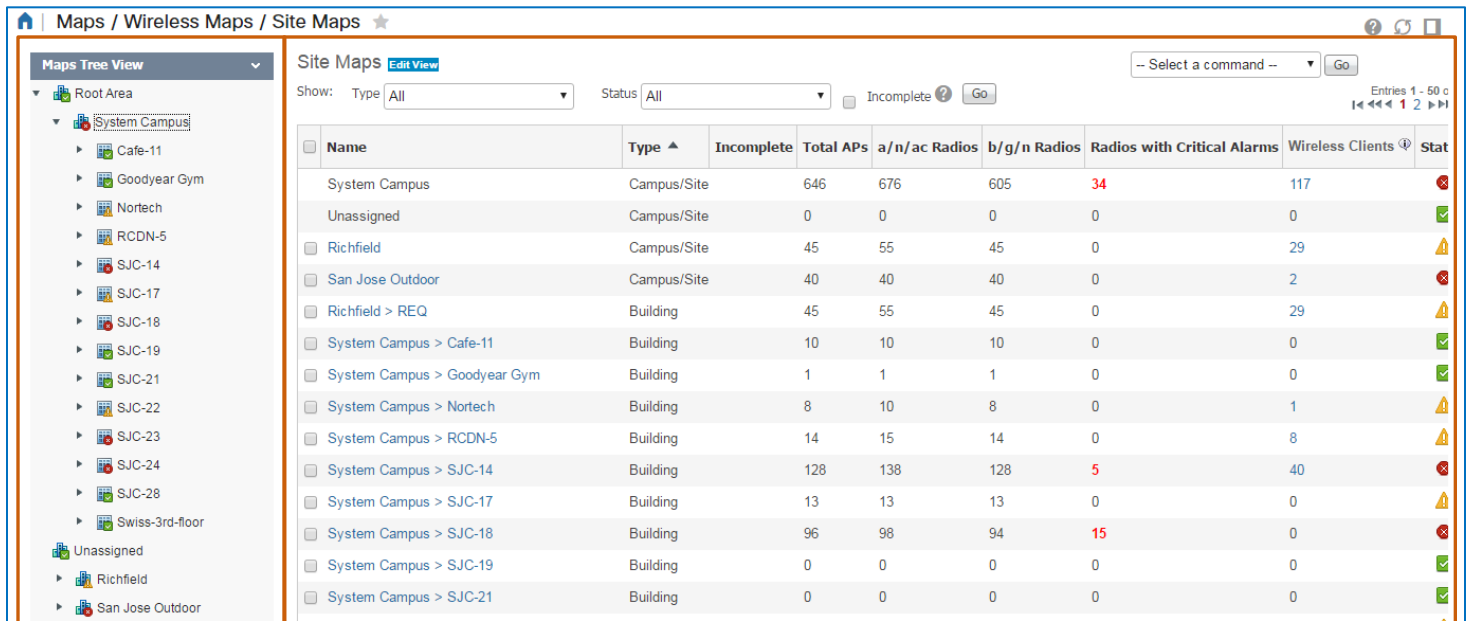
Wireless Site Maps

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.

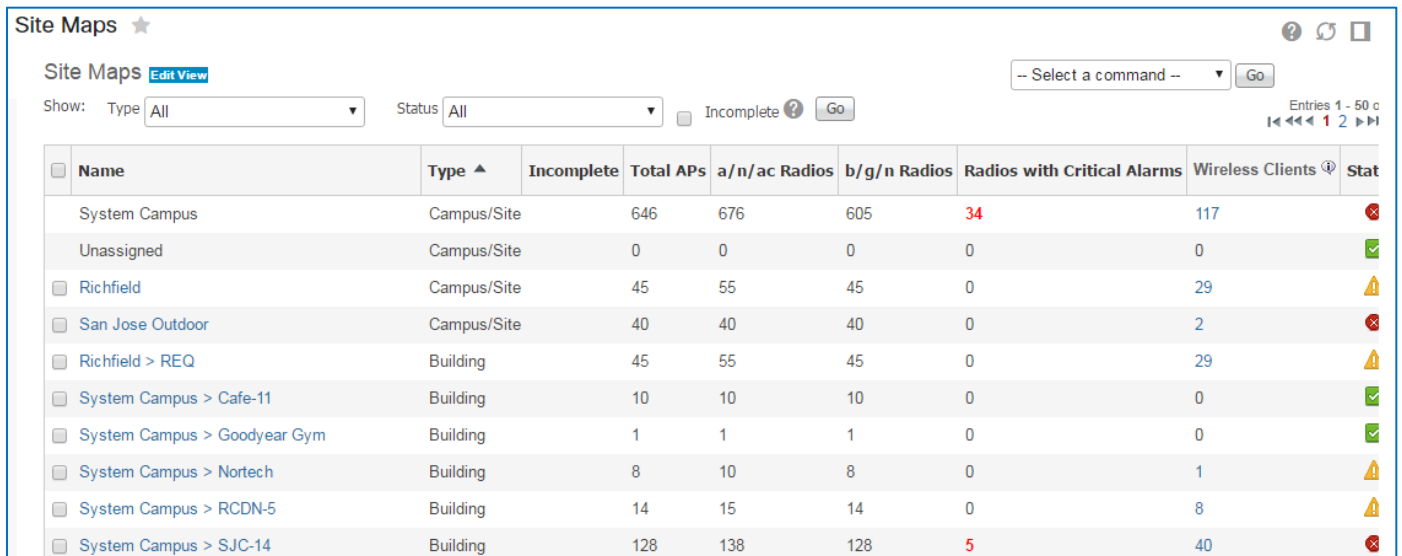


System users organize wireless site maps by physical locations, which the system lists in the **Maps Tree View** and in the **Site Maps** list.



The screenshot shows the Cisco Wireless Network Summary Data Overview interface. On the left, the **Maps Tree View** displays a hierarchical structure of locations, including **System Campus** (with sub-locations like Cafe-11, Goodyear Gym, Nortech, RCDN-5, SJC-14, SJC-17, SJC-18, SJC-19, SJC-21, SJC-22, SJC-23, SJC-24, SJC-28, and Swiss-3rd-floor) and **Unassigned** (with sub-locations like Richfield and San Jose Outdoor). The main area displays the **Site Maps** list, which is a table of site maps with columns for Name, Type, Incomplete, Total APs, a/n/ac Radios, b/g/n Radios, Radios with Critical Alarms, Wireless Clients, and Status. The table shows various site maps, including **System Campus**, **Unassigned**, **Richfield**, **San Jose Outdoor**, and various buildings within these locations. The **System Campus** entry shows 646 Total APs, 676 a/n/ac Radios, 605 b/g/n Radios, 34 Radios with Critical Alarms, and 117 Wireless Clients. The **Unassigned** entry shows 0 Total APs, 0 a/n/ac Radios, 0 b/g/n Radios, 0 Radios with Critical Alarms, and 0 Wireless Clients. The **Richfield** entry shows 45 Total APs, 55 a/n/ac Radios, 45 b/g/n Radios, 0 Radios with Critical Alarms, and 29 Wireless Clients. The **San Jose Outdoor** entry shows 40 Total APs, 40 a/n/ac Radios, 40 b/g/n Radios, 0 Radios with Critical Alarms, and 2 Wireless Clients. The **Richfield > REQ** entry shows 45 Total APs, 55 a/n/ac Radios, 45 b/g/n Radios, 0 Radios with Critical Alarms, and 29 Wireless Clients. The **System Campus > Cafe-11** entry shows 10 Total APs, 10 a/n/ac Radios, 10 b/g/n Radios, 0 Radios with Critical Alarms, and 0 Wireless Clients. The **System Campus > Goodyear Gym** entry shows 1 Total AP, 1 a/n/ac Radio, 1 b/g/n Radio, 0 Radios with Critical Alarms, and 0 Wireless Clients. The **System Campus > Nortech** entry shows 8 Total APs, 10 a/n/ac Radios, 8 b/g/n Radios, 0 Radios with Critical Alarms, and 1 Wireless Client. The **System Campus > RCDN-5** entry shows 14 Total APs, 15 a/n/ac Radios, 14 b/g/n Radios, 0 Radios with Critical Alarms, and 8 Wireless Clients. The **System Campus > SJC-14** entry shows 128 Total APs, 138 a/n/ac Radios, 128 b/g/n Radios, 5 Radios with Critical Alarms, and 40 Wireless Clients. The **System Campus > SJC-17** entry shows 13 Total APs, 13 a/n/ac Radios, 13 b/g/n Radios, 0 Radios with Critical Alarms, and 0 Wireless Clients. The **System Campus > SJC-18** entry shows 96 Total APs, 98 a/n/ac Radios, 94 b/g/n Radios, 15 Radios with Critical Alarms, and 0 Wireless Clients. The **System Campus > SJC-19** entry shows 0 Total APs, 0 a/n/ac Radios, 0 b/g/n Radios, 0 Radios with Critical Alarms, and 0 Wireless Clients. The **System Campus > SJC-21** entry shows 0 Total APs, 0 a/n/ac Radios, 0 b/g/n Radios, 0 Radios with Critical Alarms, and 0 Wireless Clients.

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

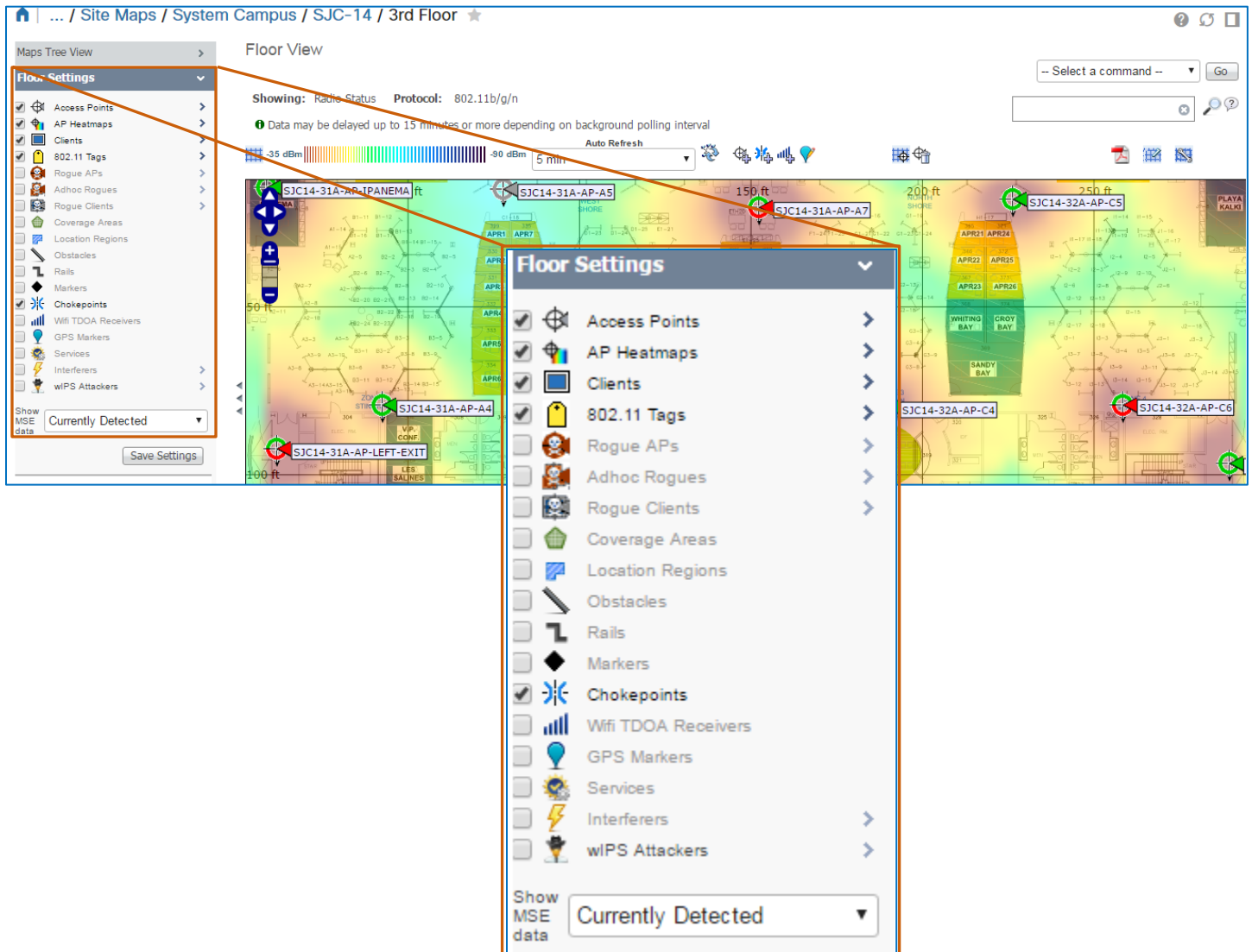


The screenshot shows the Cisco Wireless Network Summary Data Overview interface, specifically the **Site Maps** list. The list is a table of site maps with columns for Name, Type, Incomplete, Total APs, a/n/ac Radios, b/g/n Radios, Radios with Critical Alarms, Wireless Clients, and Status. The table shows various site maps, including **System Campus**, **Unassigned**, **Richfield**, **San Jose Outdoor**, and various buildings within these locations. The **System Campus** entry shows 646 Total APs, 676 a/n/ac Radios, 605 b/g/n Radios, 34 Radios with Critical Alarms, and 117 Wireless Clients. The **Unassigned** entry shows 0 Total APs, 0 a/n/ac Radios, 0 b/g/n Radios, 0 Radios with Critical Alarms, and 0 Wireless Clients. The **Richfield** entry shows 45 Total APs, 55 a/n/ac Radios, 45 b/g/n Radios, 0 Radios with Critical Alarms, and 29 Wireless Clients. The **San Jose Outdoor** entry shows 40 Total APs, 40 a/n/ac Radios, 40 b/g/n Radios, 0 Radios with Critical Alarms, and 2 Wireless Clients. The **Richfield > REQ** entry shows 45 Total APs, 55 a/n/ac Radios, 45 b/g/n Radios, 0 Radios with Critical Alarms, and 29 Wireless Clients. The **System Campus > Cafe-11** entry shows 10 Total APs, 10 a/n/ac Radios, 10 b/g/n Radios, 0 Radios with Critical Alarms, and 0 Wireless Clients. The **System Campus > Goodyear Gym** entry shows 1 Total AP, 1 a/n/ac Radio, 1 b/g/n Radio, 0 Radios with Critical Alarms, and 0 Wireless Clients. The **System Campus > Nortech** entry shows 8 Total APs, 10 a/n/ac Radios, 8 b/g/n Radios, 0 Radios with Critical Alarms, and 1 Wireless Client. The **System Campus > RCDN-5** entry shows 14 Total APs, 15 a/n/ac Radios, 14 b/g/n Radios, 0 Radios with Critical Alarms, and 8 Wireless Clients. The **System Campus > SJC-14** entry shows 128 Total APs, 138 a/n/ac Radios, 128 b/g/n Radios, 5 Radios with Critical Alarms, and 40 Wireless Clients.

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.

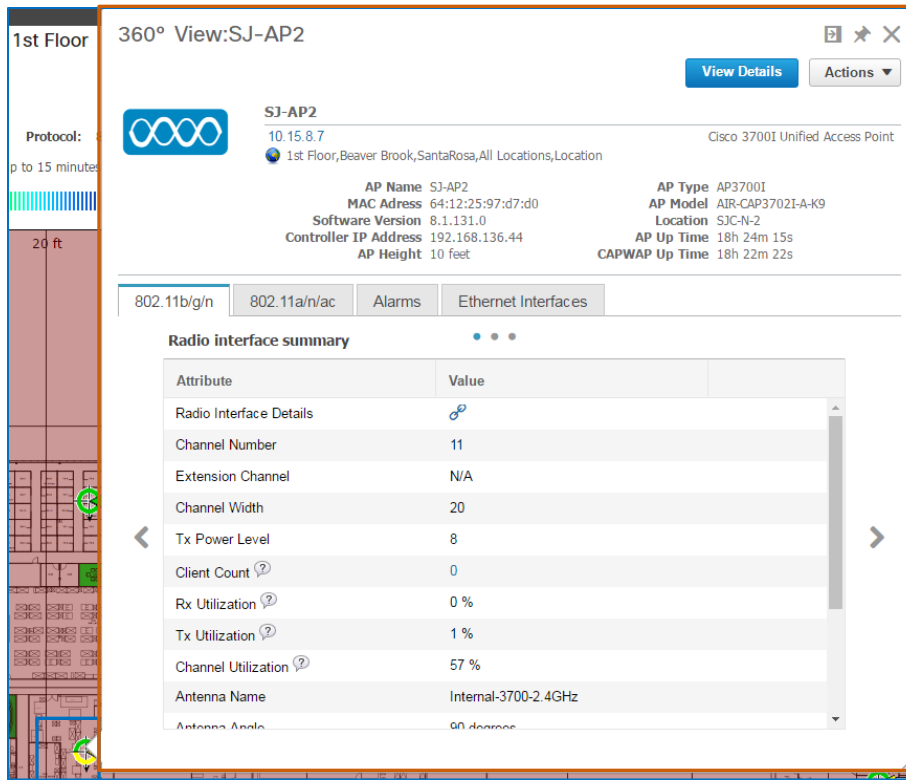


The screenshot displays the Cisco Wireless Network Summary Data Overview interface, specifically the Floor View for the 3rd Floor of SJC-14. The interface is divided into several sections:

- Maps Tree View:** Located on the left, it shows a hierarchy of maps. The 'Floor Settings' section is expanded, listing various attributes that can be displayed on the map.
- Floor Settings:** A central panel that allows users to select or clear attributes to include or remove from the map. The attributes listed include:
 - Access Points
 - AP Heatmaps
 - Clients
 - 802.11 Tags
 - Rogue APs
 - Adhoc Rogues
 - Rogue Clients
 - Coverage Areas
 - Location Regions
 - Obstacles
 - Rails
 - Markers
 - Chokepoints
 - Wifi TDOA Receivers
 - GPS Markers
 - Services
 - Interferers
 - wIPS Attackers
- Map View:** The right side of the interface shows a map of the 3rd Floor. The map displays various access points (e.g., SJC14-31A-AP-A4, SJC14-31A-AP-A5, SJC14-31A-AP-A7, SJC14-32A-AP-C4, SJC14-32A-AP-C6) and coverage areas. The map is color-coded to represent signal strength, with a legend at the top showing a range from -35 dBm to -90 dBm.

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 360° View pop-up window](#).



360° View: SJ-AP2

View Details Actions

SJ-AP2
10.15.8.7
Cisco 3700I Unified Access Point
1st Floor, Beaver Brook, Santa Rosa, All Locations, Location

AP Name: SJ-AP2
MAC Address: 64:12:25:97:d7:d0
Software Version: 8.1.131.0
Controller IP Address: 192.168.136.44
AP Height: 10 feet

AP Type: AP3700I
AP Model: AIR-CAP3702I-A-K9
Location: SJ-C-N-2
AP Up Time: 18h 24m 15s
CAPWAP Up Time: 18h 22m 22s

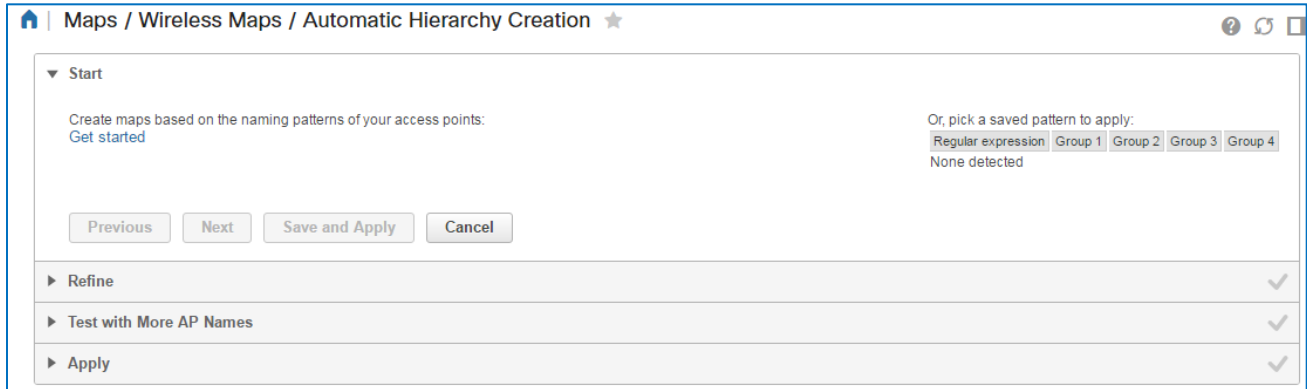
802.11b/g/n 802.11a/n/ac Alarms Ethernet Interfaces

Radio interface summary

Attribute	Value
Radio Interface Details	Details
Channel Number	11
Extension Channel	N/A
Channel Width	20
Tx Power Level	8
Client Count	0
Rx Utilization	0 %
Tx Utilization	1 %
Channel Utilization	57 %
Antenna Name	Internal-3700-2.4GHz
Antenna Angle	00 degrees

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.

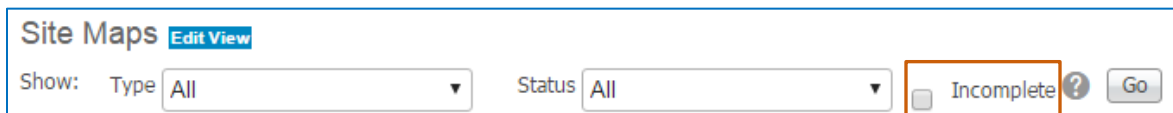


The screenshot shows the 'Automatic Hierarchy Creation' tool interface. At the top, there's a breadcrumb trail: 'Maps / Wireless Maps / Automatic Hierarchy Creation'. Below this, the 'Start' section contains instructions: 'Create maps based on the naming patterns of your access points:' with a 'Get started' link. To the right, there's a section 'Or, pick a saved pattern to apply:' with buttons for 'Regular expression', 'Group 1', 'Group 2', 'Group 3', and 'Group 4'. Below these buttons, it says 'None detected'. At the bottom of the 'Start' section, there are four buttons: 'Previous', 'Next', 'Save and Apply', and 'Cancel'. Below the 'Start' section, there are three expandable sections: 'Refine', 'Test with More AP Names', and 'Apply', each with a checkmark icon on the right.

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.



The screenshot shows the 'Site Maps' filter interface. At the top, there's a 'Site Maps' label and an 'Edit View' button. Below this, there's a 'Show:' label followed by a 'Type' dropdown menu set to 'All'. To the right of the 'Type' dropdown is a 'Status' dropdown menu set to 'All'. To the right of the 'Status' dropdown is a checkbox labeled 'Incomplete' with a question mark icon next to it. To the right of the 'Incomplete' checkbox is a 'Go' button.

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.](#)