Wireless Clients and Users Monitoring Overview

Cisco© Prime Infrastructure 3.1

Job Aid

Copyright Page

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 Clients and Users Monitoring Overview Job Aid

Contents

Basics **1**

Overview 1

Introduction 1

Skills 2

Network Operator 2

Proficient to Expert 2

Monitoring Clients and Users **3**

Summary Wireless Client and User Data 3

Overview 3

Client Summary Data Dashlets 4

Overview 4

Connection Protocol and Authentication Data 6

Alarm and Event Data 7

Client Traffic Protocol Usage Data 9

Clients Non-Compliant with ISE Access Authorization Rules 13

Wireless LAN Service Set Identifiers (SSIDS) Usage 14

End User Experience Data 15

Detailed Client and User Activity 16

Overview 16

Introduction 16

Configuring Mobility Services for Client and User Reporting 17

Individual Client Details and Statistics 19

Device and User Information 23

Ongoing Client Behavior 24

Links **25**

To Product Information 25

To Key Concepts 25

To Training 25

To Contact Us 25

Basics

Overview

Introduction

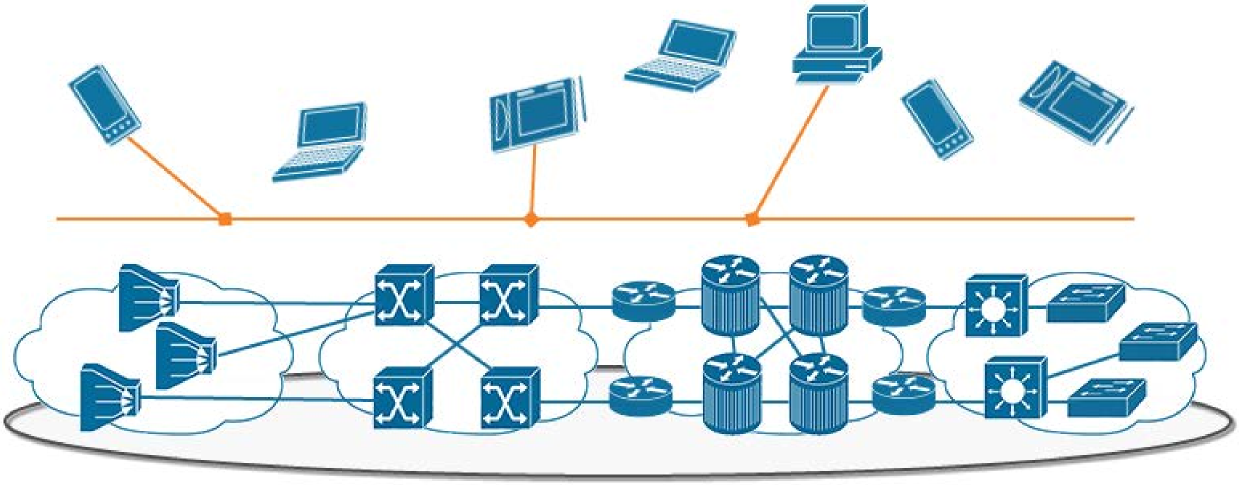
To better ensure the customer experience and meet enterprise goals, you monitor user and network behavior and performance metrics to determine whether users are able to:

- Connect to the network efficiently and successfully.
- Access the applications that they need.
- Have the experience that they expect while using the network.

You also need to monitor:

- Whether the network is meeting enterprise quality of service and other usage policies.
- Client connections or connection attempts, which helps you to mitigate possible attacks or to identify malicious rogue devices.

This job aid introduces you to key tools that Cisco© Prime Infrastructure provides to support your client and user monitoring activities.



Skills

Network Operator

To perform client and user monitoring tasks, you need the following experience.

Proficient to Expert

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

Monitoring Clients and Users

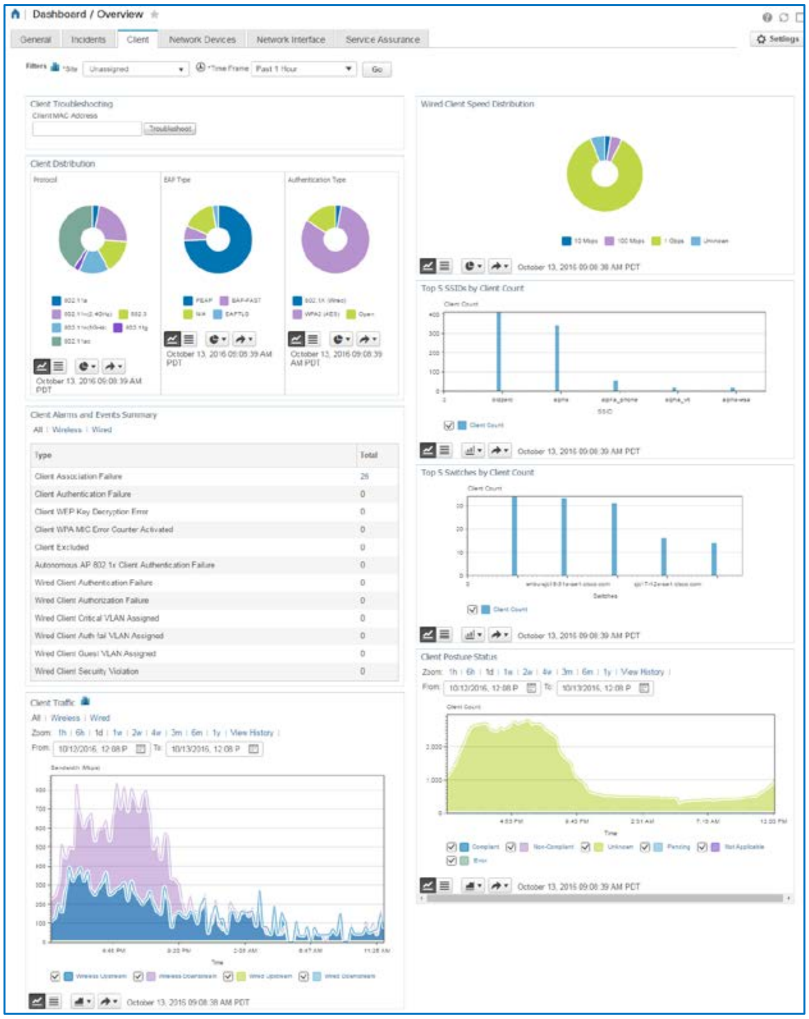
Summary Wireless Client and User Data

Overview

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

Note: For an overview on the general dashboard and dashlet functions, refer to the **Wireless Network Summary Data Overview** job aid.

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



Client Alarms and Events Summary

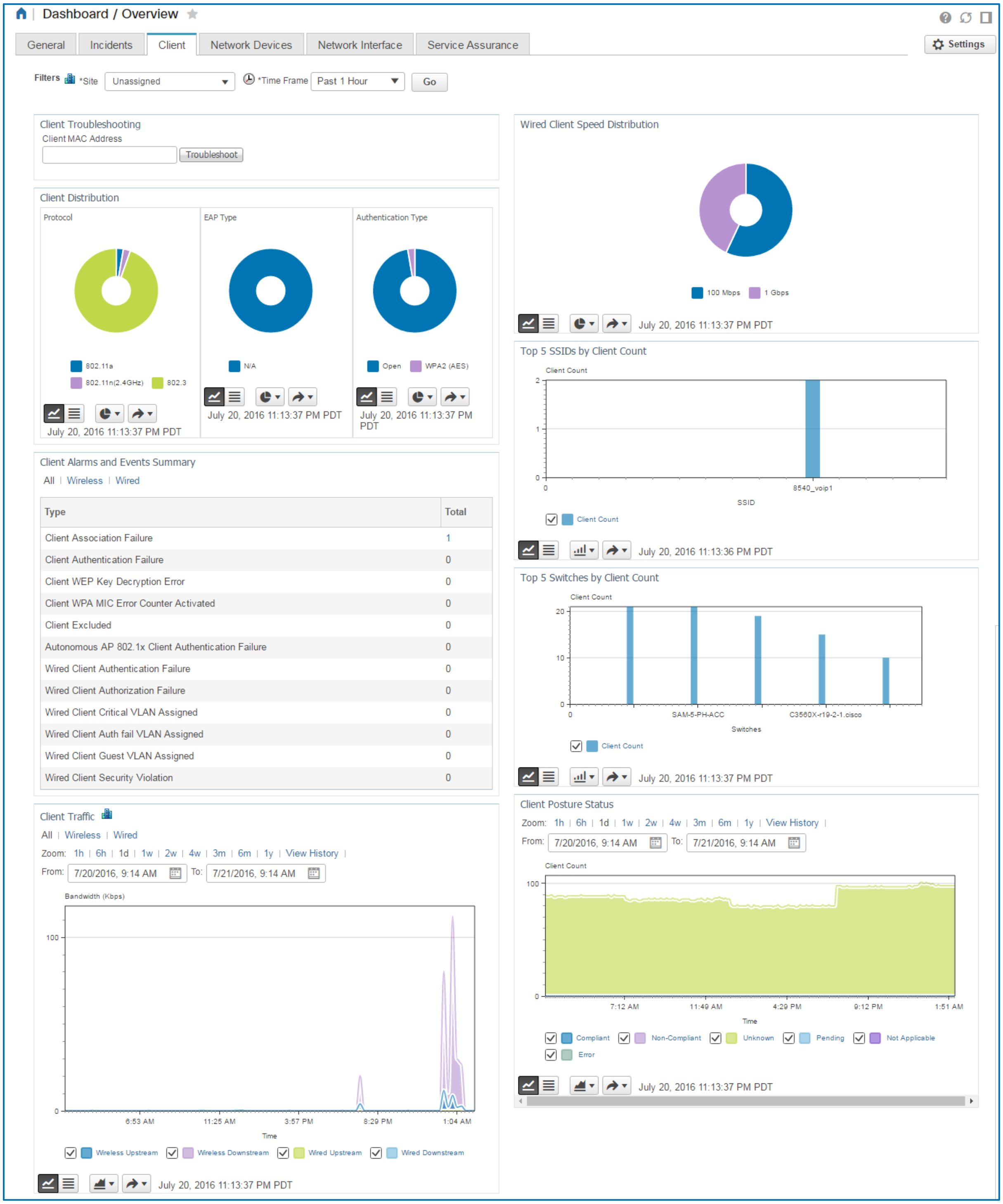
All | Wireless | Wired

Type	Total
Client Association Failure	26
Client Authentication Failure	0
Client WEP Key Decryption Error	0
Client WPA MIC Error Counter Activated	0
Client Excluded	0
Autonomous AP 802.1x Client Authentication Failure	0
Wired Client Authentication Failure	0
Wired Client Authorization Failure	0
Wired Client Critical VLAN Assigned	0
Wired Client Auth fail VLAN Assigned	0
Wired Client Guest VLAN Assigned	0
Wired Client Security Violation	0

Client Summary Data Dashlets

Overview

On the **Client** dashboard, you can monitor summary information about the wireless clients connected to the network.



Filters *Site Unassigned *Time Frame Past 1 Hour

Client Troubleshooting

Client MAC Address

Client Distribution — July 20, 2016 11:13:37 PM PDT

Wired Client Speed Distribution — July 20, 2016 11:13:37 PM PDT

Top 5 SSIDs by Client Count — July 20, 2016 11:13:36 PM PDT

Top 5 Switches by Client Count — July 20, 2016 11:13:37 PM PDT

Client Alarms and Events Summary

All | Wireless | Wired

Type	Total
Client Association Failure	1
Client Authentication Failure	0
Client WEP Key Decryption Error	0
Client WPA MIC Error Counter Activated	0
Client Excluded	0
Autonomous AP 802.1x Client Authentication Failure	0
Wired Client Authentication Failure	0
Wired Client Authorization Failure	0
Wired Client Critical VLAN Assigned	0
Wired Client Auth fail VLAN Assigned	0
Wired Client Guest VLAN Assigned	0
Wired Client Security Violation	0

Client Traffic

From: 7/20/2016, 9:14 AM To: 7/21/2016, 9:14 AM

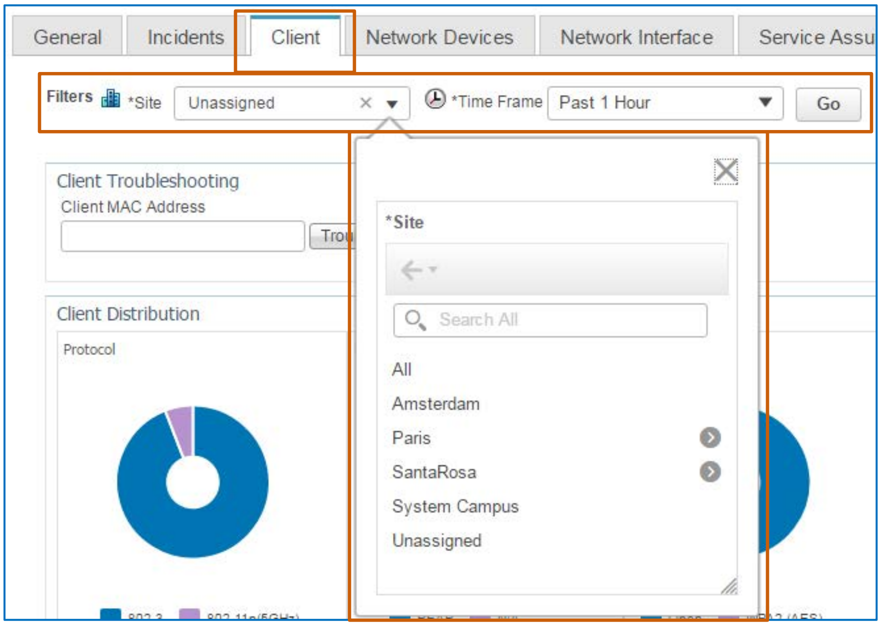
July 20, 2016 11:13:37 PM PDT

Client Posture Status

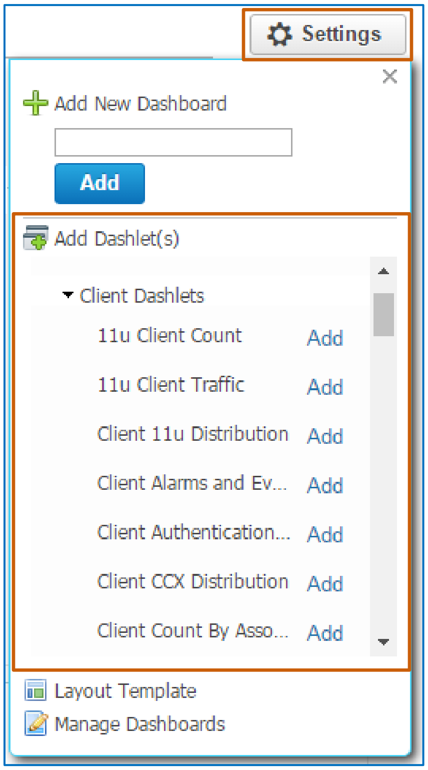
From: 7/20/2016, 9:14 AM To: 7/21/2016, 9:14 AM

July 20, 2016 11:13:37 PM PDT

The data that the dashlets report is based on the location group and the time period that you select.



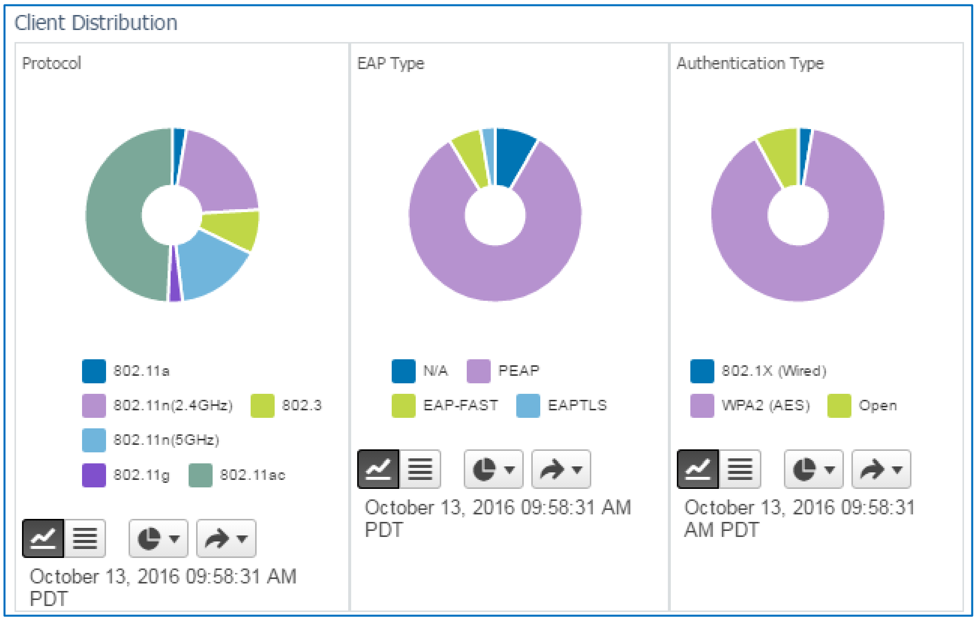
This topic addresses some of the key dashlets that users commonly monitor. The system offers an extensive number of client-related dashlets, which are available on the **Settings** menu.



Connection Protocol and Authentication Data

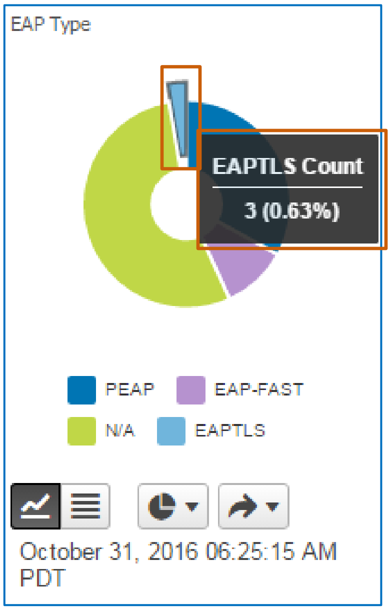
The **Client Distribution** dashlet reports:

- The distribution of associated clients based on the protocols that they use to connect, including wired and wireless protocols
- The number of clients using the Extensible Authentication Protocol, or EAP, for network authentication and the type of protocol.
- The number of clients using authentication methods other than EAP.



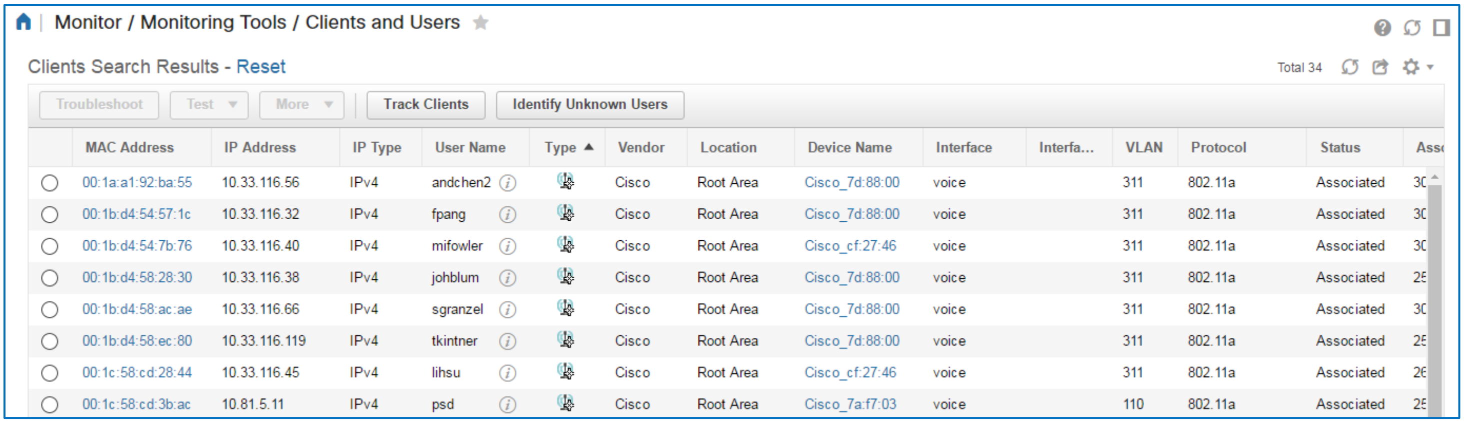
To see the number of clients that a chart element represents:

- Point to the chart element. A pop-up window opens with the number and percentage of clients using the protocol or authentication method.



To review the list of clients that are using the protocol or authentication method:

- Click a chart element. The system navigates to the **Clients and Users** page and lists the clients that are using the protocol or authentication method.



Monitor / Monitoring Tools / Clients and Users

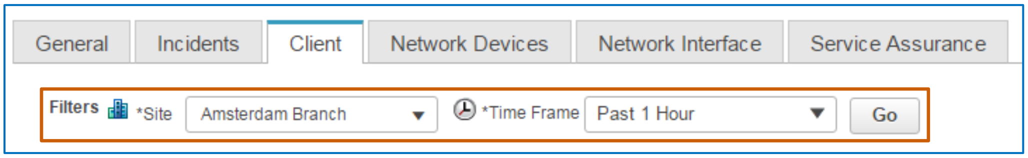
Clients Search Results - Reset   Total 34

Troubleshoot | Test | More | Track Clients | Identify Unknown Users

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Location	Device Name	Interface	Interfa...	VLAN	Protocol	Status	Ass
○	00:1a:a1:92:ba:55	10.33.116.56	IPv4	andchen2		Cisco	Root Area	Cisco_7d:88:00	voice		311	802.11a	Associated	30
○	00:1b:d4:54:57:1c	10.33.116.32	IPv4	fpang		Cisco	Root Area	Cisco_7d:88:00	voice		311	802.11a	Associated	30
○	00:1b:d4:54:7b:76	10.33.116.40	IPv4	mifowler		Cisco	Root Area	Cisco_cf:27:46	voice		311	802.11a	Associated	30
○	00:1b:d4:58:28:30	10.33.116.38	IPv4	johblum		Cisco	Root Area	Cisco_7d:88:00	voice		311	802.11a	Associated	25
○	00:1b:d4:58:ac:ae	10.33.116.66	IPv4	sgranzel		Cisco	Root Area	Cisco_7d:88:00	voice		311	802.11a	Associated	30
○	00:1b:d4:58:ec:80	10.33.116.119	IPv4	tkintner		Cisco	Root Area	Cisco_7d:88:00	voice		311	802.11a	Associated	25
○	00:1c:58:cd:28:44	10.33.116.45	IPv4	lihsu		Cisco	Root Area	Cisco_cf:27:46	voice		311	802.11a	Associated	26
○	00:1c:58:cd:3b:ac	10.81.5.11	IPv4	psd		Cisco	Root Area	Cisco_7a:f7:03	voice		110	802.11a	Associated	25

Alarm and Event Data

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

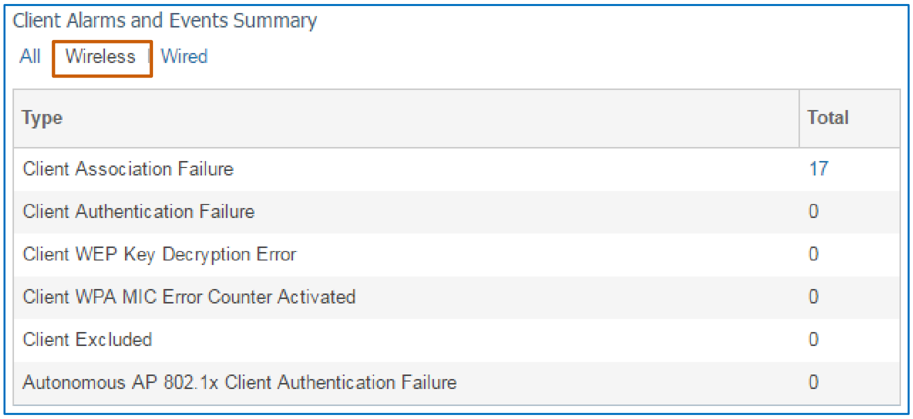


Filters *Site Amsterdam Branch *Time Frame Past 1 Hour

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

To see alarms related to wireless clients:

- Below the dashlet title, click **Wireless**. The dashlets lists the wireless alarm categories only.

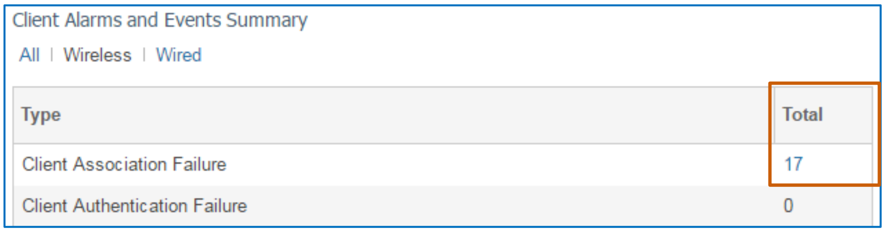


Client Alarms and Events Summary

Type	Total
Client Association Failure	17
Client Authentication Failure	0
Client WEP Key Decryption Error	0
Client WPA MIC Error Counter Activated	0
Client Excluded	0
Autonomous AP 802.1x Client Authentication Failure	0

To review the alarms associated with an alarm type:

- In the dashlet, in the **Total** column, click the number link.

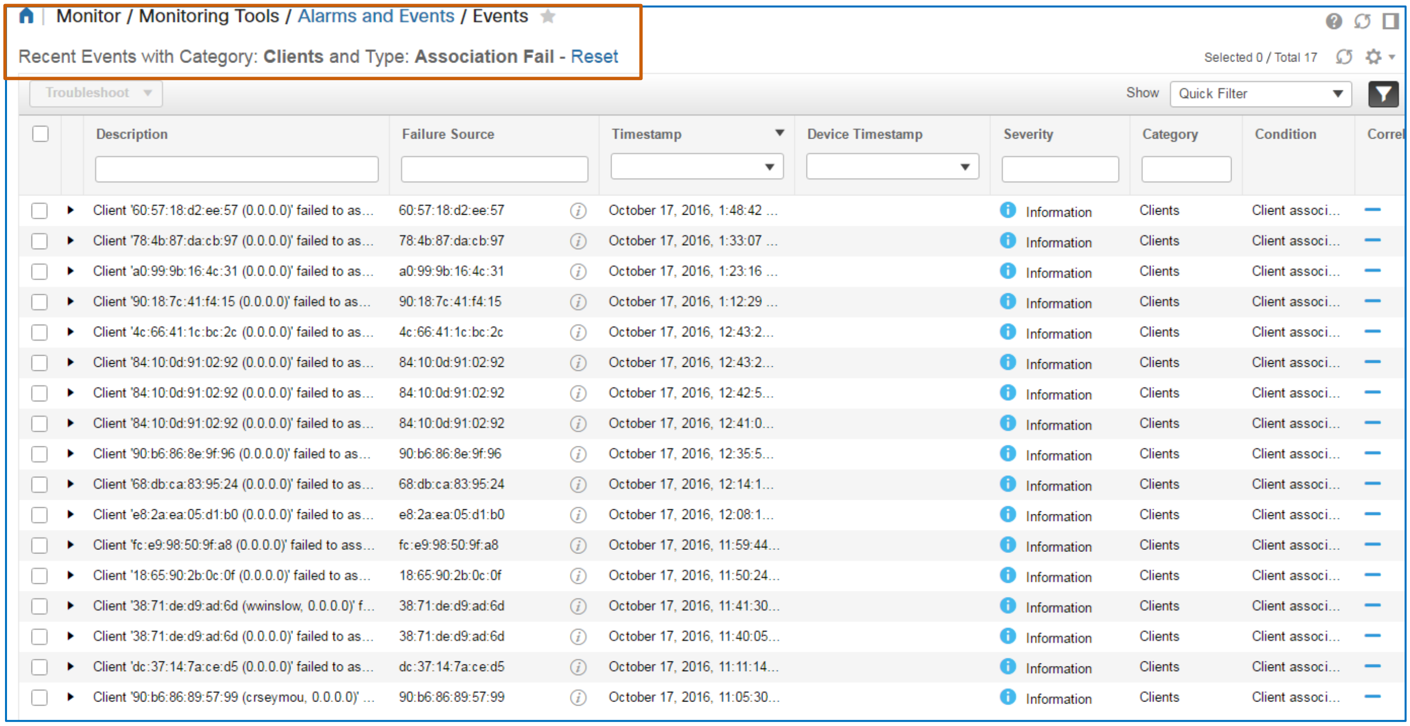


Client Alarms and Events Summary

All | Wireless | Wired

Type	Total
Client Association Failure	17
Client Authentication Failure	0

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



Monitor / Monitoring Tools / Alarms and Events / Events

Recent Events with Category: **Clients** and Type: **Association Fail** - Reset

Selected 0 / Total 17

☐		Description	Failure Source	Timestamp	Device Timestamp	Severity	Category	Condition	Correl
☐	▸	Client '60:57:18:d2:ee:57 (0.0.0.0)' failed to as...	60:57:18:d2:ee:57	October 17, 2016, 1:48:42 ...		Information	Clients	Client associ...	—
☐	▸	Client '78:4b:87:da:cb:97 (0.0.0.0)' failed to as...	78:4b:87:da:cb:97	October 17, 2016, 1:33:07 ...		Information	Clients	Client associ...	—
☐	▸	Client 'a0:99:9b:16:4c:31 (0.0.0.0)' failed to as...	a0:99:9b:16:4c:31	October 17, 2016, 1:23:16 ...		Information	Clients	Client associ...	—
☐	▸	Client '90:18:7c:41:f4:15 (0.0.0.0)' failed to as...	90:18:7c:41:f4:15	October 17, 2016, 1:12:29 ...		Information	Clients	Client associ...	—
☐	▸	Client '4c:66:41:1c:bc:2c (0.0.0.0)' failed to as...	4c:66:41:1c:bc:2c	October 17, 2016, 12:43:2...		Information	Clients	Client associ...	—
☐	▸	Client '84:10:0d:91:02:92 (0.0.0.0)' failed to as...	84:10:0d:91:02:92	October 17, 2016, 12:43:2...		Information	Clients	Client associ...	—
☐	▸	Client '84:10:0d:91:02:92 (0.0.0.0)' failed to as...	84:10:0d:91:02:92	October 17, 2016, 12:42:5...		Information	Clients	Client associ...	—
☐	▸	Client '84:10:0d:91:02:92 (0.0.0.0)' failed to as...	84:10:0d:91:02:92	October 17, 2016, 12:41:0...		Information	Clients	Client associ...	—
☐	▸	Client '90:b6:86:8e:9f:96 (0.0.0.0)' failed to as...	90:b6:86:8e:9f:96	October 17, 2016, 12:35:5...		Information	Clients	Client associ...	—
☐	▸	Client '68:db:ca:83:95:24 (0.0.0.0)' failed to as...	68:db:ca:83:95:24	October 17, 2016, 12:14:1...		Information	Clients	Client associ...	—
☐	▸	Client 'e8:2a:ea:05:d1:b0 (0.0.0.0)' failed to as...	e8:2a:ea:05:d1:b0	October 17, 2016, 12:08:1...		Information	Clients	Client associ...	—
☐	▸	Client 'fc:e9:98:50:9f:a8 (0.0.0.0)' failed to ass...	fc:e9:98:50:9f:a8	October 17, 2016, 11:59:44...		Information	Clients	Client associ...	—
☐	▸	Client '18:65:90:2b:0c:0f (0.0.0.0)' failed to as...	18:65:90:2b:0c:0f	October 17, 2016, 11:50:24...		Information	Clients	Client associ...	—
☐	▸	Client '38:71:de:d9:ad:6d (wwinslow, 0.0.0.0)' f...	38:71:de:d9:ad:6d	October 17, 2016, 11:41:30...		Information	Clients	Client associ...	—
☐	▸	Client '38:71:de:d9:ad:6d (0.0.0.0)' failed to as...	38:71:de:d9:ad:6d	October 17, 2016, 11:40:05...		Information	Clients	Client associ...	—
☐	▸	Client 'dc:37:14:7a:ce:d5 (0.0.0.0)' failed to as...	dc:37:14:7a:ce:d5	October 17, 2016, 11:11:14...		Information	Clients	Client associ...	—
☐	▸	Client '90:b6:86:89:57:99 (crseymou, 0.0.0.0)' ...	90:b6:86:89:57:99	October 17, 2016, 11:05:30...		Information	Clients	Client associ...	—

Client Traffic Protocol Usage Data

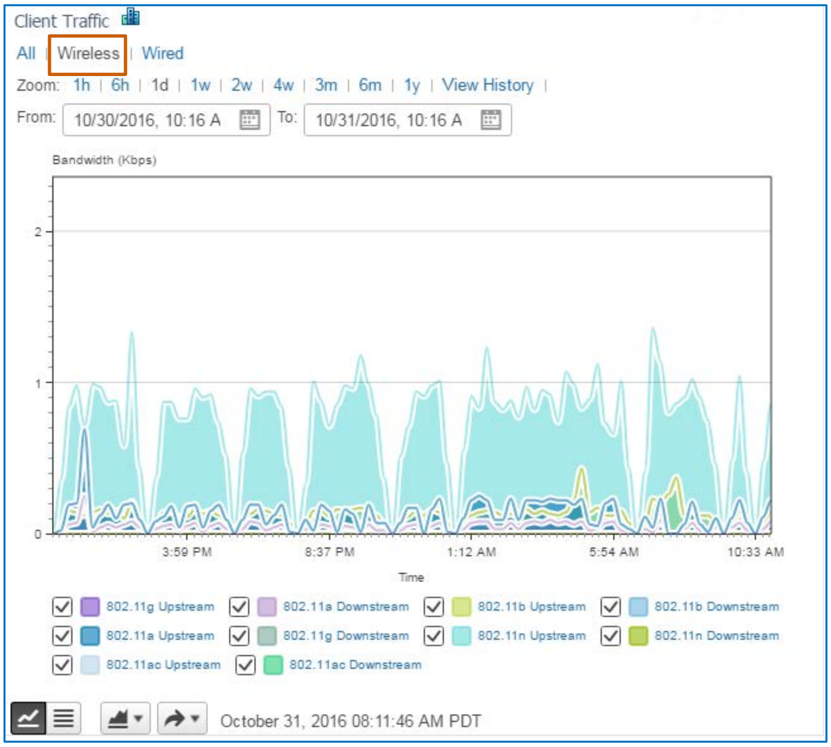
The **Client Traffic** dashlet reports the amount of bandwidth that client traffic is consuming for each network protocol that clients are using to connect to the network.

Recognizing the most heavily consumed protocols can provide insight into the types of infrastructure that the system requires to manage traffic effectively and into future expansion requirements.

To see the amount of bandwidth that wireless clients are consuming by protocol:

- Below the dashlet title, click **Wireless**.

  The dashlet illustrates the wireless bandwidths that are being consumed and their consumption levels.

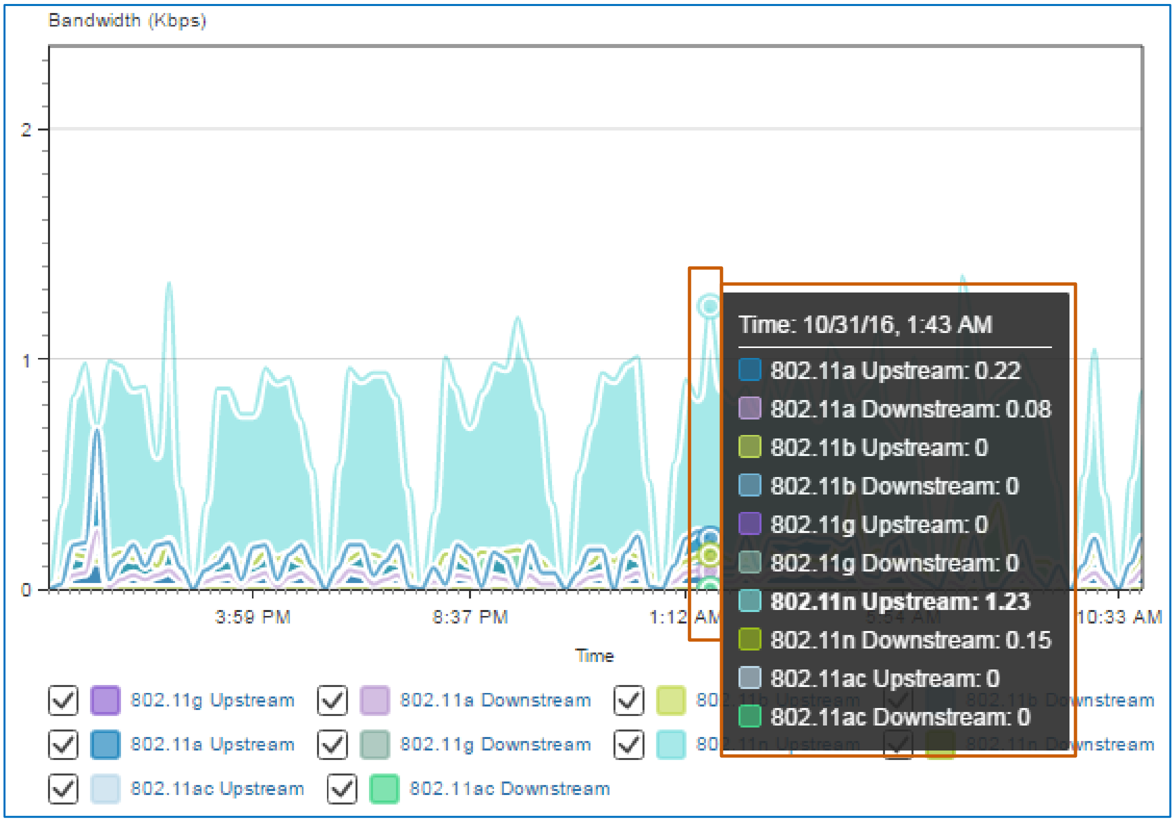


From: 10/30/2016, 10:16 A To: 10/31/2016, 10:16 A

October 31, 2016 08:11:46 AM PDT

To see specific bandwidth consumption with its timestamp:

- Point to a chart element. The chart applies data points to indicate where on the timeline the pop-up window is reporting the bandwidth statistics.



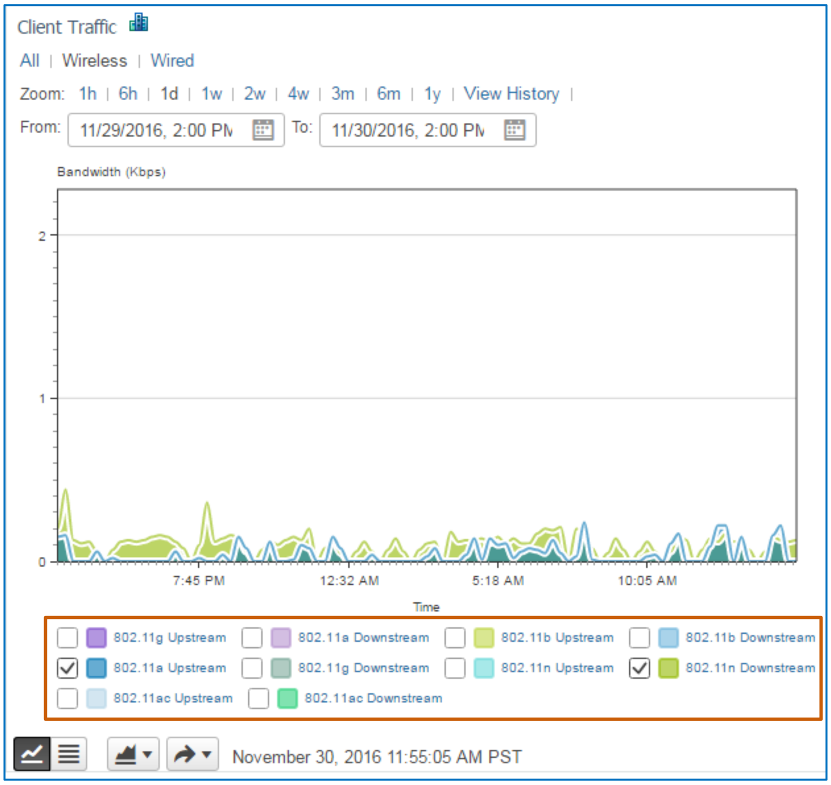
Time: 10/31/16, 1:43 AM

802.11a Upstream: 0.22
802.11a Downstream: 0.08
802.11b Upstream: 0
802.11b Downstream: 0
802.11g Upstream: 0
802.11g Downstream: 0
802.11n Upstream: 1.23
802.11n Downstream: 0.15
802.11ac Upstream: 0
802.11ac Downstream: 0

The dashlet displays the upstream and downstream metrics for all available protocols by default. You can select only those protocols that you need for your monitoring tasks.

To exclude protocols from the chart:

- Clear the check box of each protocol that you do not need to see.



From: 11/29/2016, 2:00 PM To: 11/30/2016, 2:00 PM

☐ 802.11g Upstream ☐ 802.11a Downstream ☐ 802.11b Upstream ☐ 802.11b Downstream
☑ 802.11a Upstream ☐ 802.11g Downstream ☐ 802.11n Upstream ☑ 802.11n Downstream
☐ 802.11ac Upstream ☐ 802.11ac Downstream

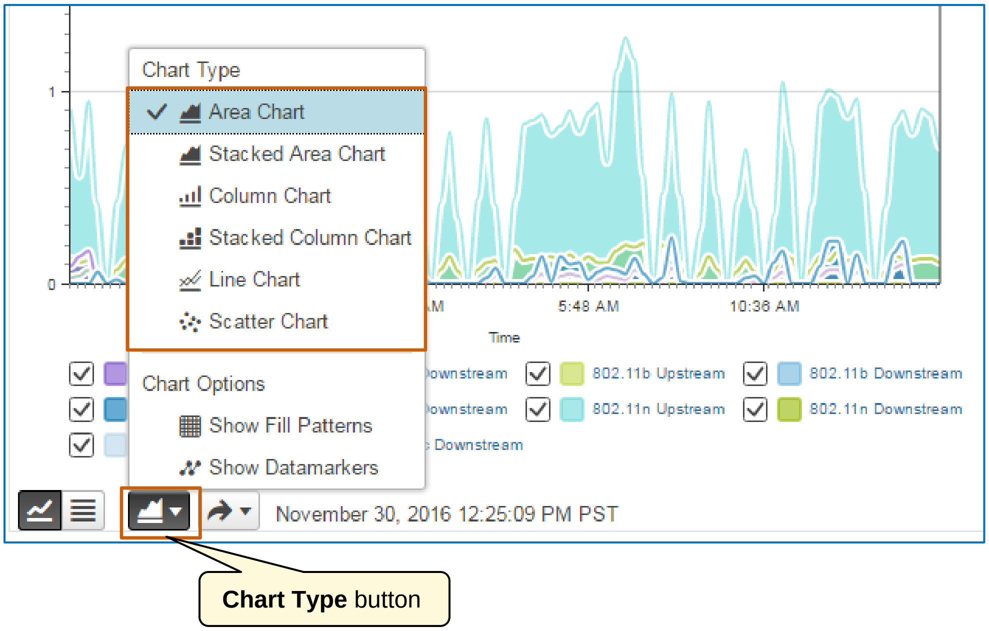
November 30, 2016 11:55:05 AM PST

You also can apply the chart layout most effective for you, including:

- Area, which is the default chart layout
- Stacked Area
- Column
- Stacked Column
- Line
- Scatter

To apply a different chart layout:

- Below the chart, click **Chart Type**, and then select the layout that you prefer.

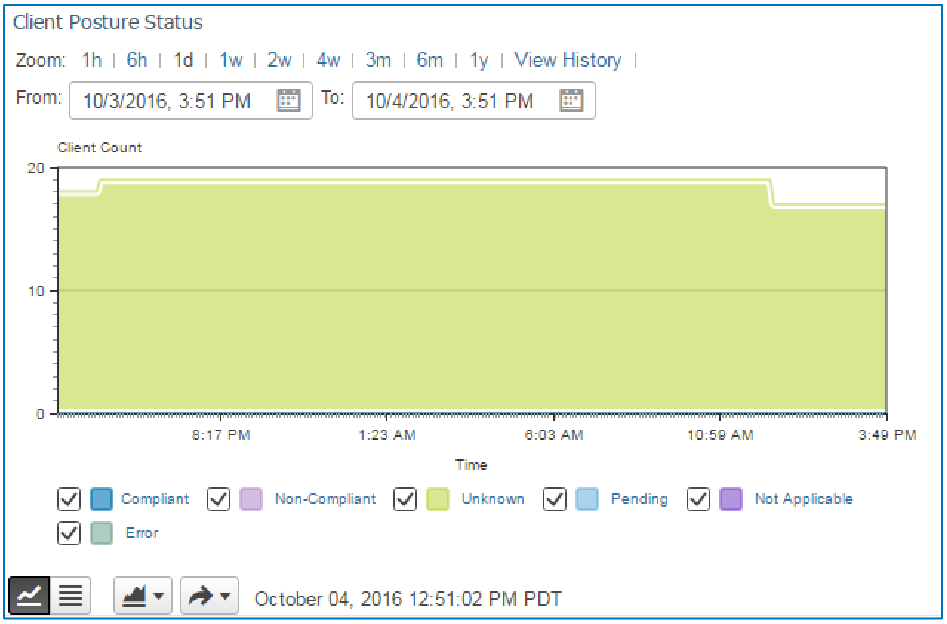


Clients Non-Compliant with ISE Access Authorization Rules

In systems that use an Identity Services Engine (ISE) server to authorize client access to the network, the **Client Posture Status** dashlet reports the number of clients, for those client devices that are integrated with an ISE, that are in or out of compliance with the rules configured on the ISE.

Rules on ISE servers can define such compliance requirements as operating system, browser, or anti-virus minimum standards, for example.

When you see a large number of clients that are non-compliant for various reasons, this information indicates that you need to review the ISE server to evaluate rule configuration, device integration, or device configuration details to determine what might be causing non-compliance.



Client Posture Status

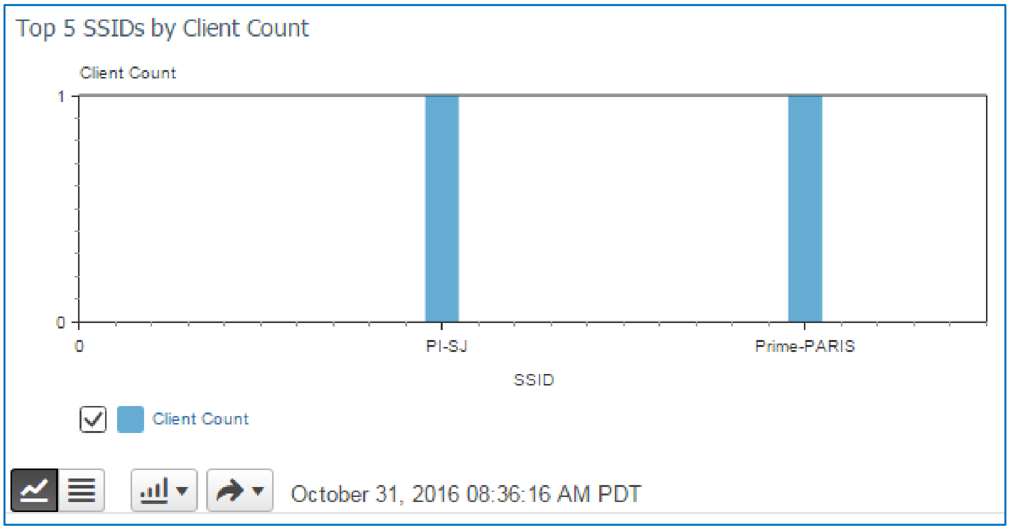
From: 10/3/2016, 3:51 PM To: 10/4/2016, 3:51 PM

October 04, 2016 12:51:02 PM PDT

Wireless LAN Service Set Identifiers (SSIDS) Usage

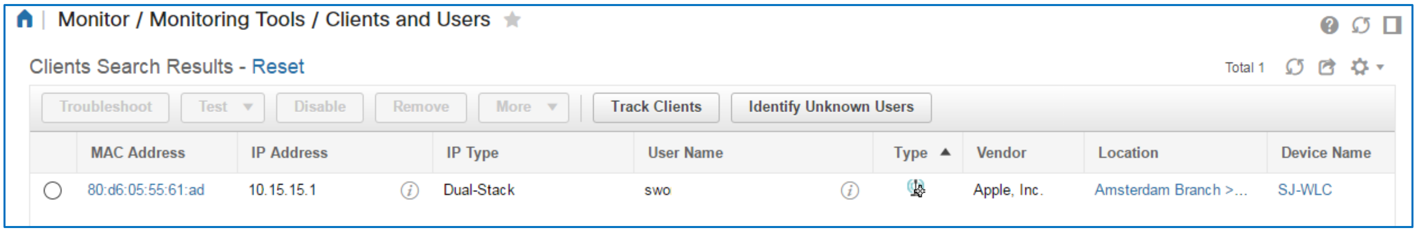
The **Top 5 SSIDs by Client Count** dashlet reports the wireless LAN service set identifiers (SSIDs) that clients are using the most, up to five.

Recognizing the number of users accessing the network on various SSIDs can provide insight into whether system users tend to be logging on to primary SSIDs or secondary SSIDs such as guest or test SSIDs, for example.



To review the clients logging on to a specific SSID:

- Click the SSID's chart element. The system navigates to the **Clients and Users** page listing the clients that are connected to the SSID.


Monitor / Monitoring Tools / Clients and Users
Clients Search Results - Reset
Total 1
Troubleshoot
Test
Disable
Remove
More
Track Clients
Identify Unknown Users

	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Location	Device Name
○	80:d6:05:55:61:ad	10.15.15.1	Dual-Stack	swo		Apple, Inc.	Amsterdam Branch >...	SJ-WLC

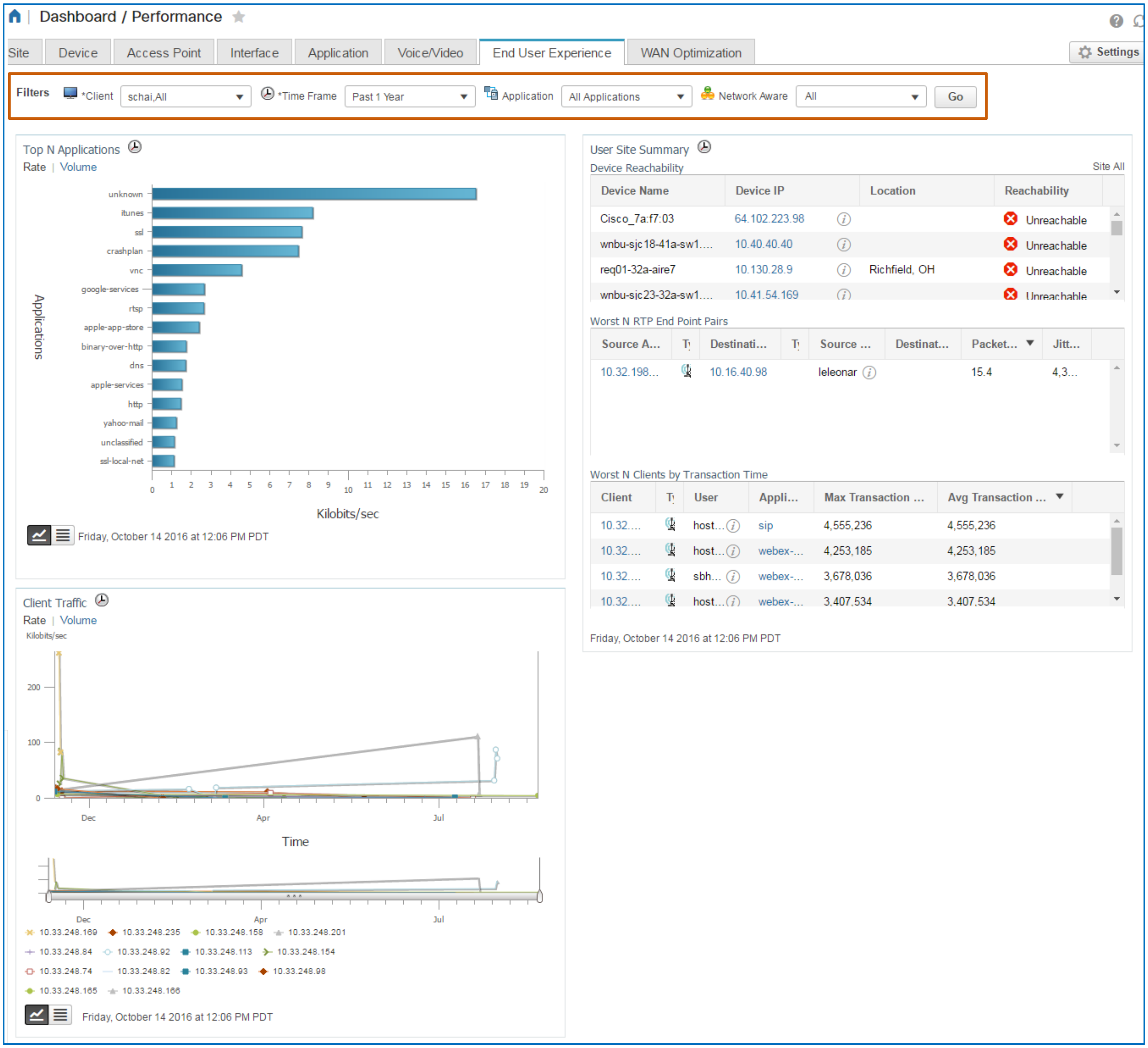
End User Experience Data

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

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

To apply one or more filters:

- On the toolbar, make your selections in the drop-down lists, and then click **Go**.



Filters: *Client: schai,All; *Time Frame: Past 1 Year; Application: All Applications; Network Aware: All

Top N Applications: Friday, October 14 2016 at 12:06 PM PDT

Client Traffic: Friday, October 14 2016 at 12:06 PM PDT

User Site Summary

Device Reachability — Site All

Device Name	Device IP	Location	Reachability
Cisco_7a:f7:03	64.102.223.98		Unreachable
wnbu-sjc18-41a-sw1....	10.40.40.40		Unreachable
req01-32a-aire7	10.130.28.9	Richfield, OH	Unreachable
wnbu-sjc23-32a-sw1....	10.41.54.169		Unreachable

Worst N RTP End Point Pairs

Source A...	Ty	Destinati...	Ty	Source ...	Destinat...	Packet...	Jitt...
10.32.198...		10.16.40.98		leleonar		15.4	4,3...

Worst N Clients by Transaction Time

Client	Ty	User	Appli...	Max Transaction ...	Avg Transaction ...
10.32....		host...	sip	4,555,236	4,555,236
10.32....		host...	webex-...	4,253,185	4,253,185
10.32....		sbh...	webex-...	3,678,036	3,678,036
10.32....		host...	webex-...	3,407,534	3,407,534

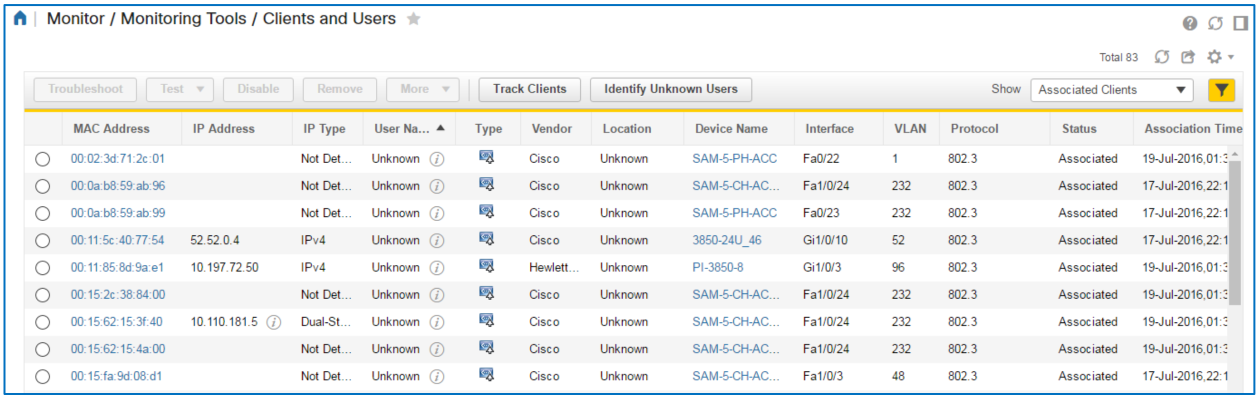
Friday, October 14 2016 at 12:06 PM PDT

Detailed Client and User Activity

Overview

Introduction

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



Monitor / Monitoring Tools / Clients and Users

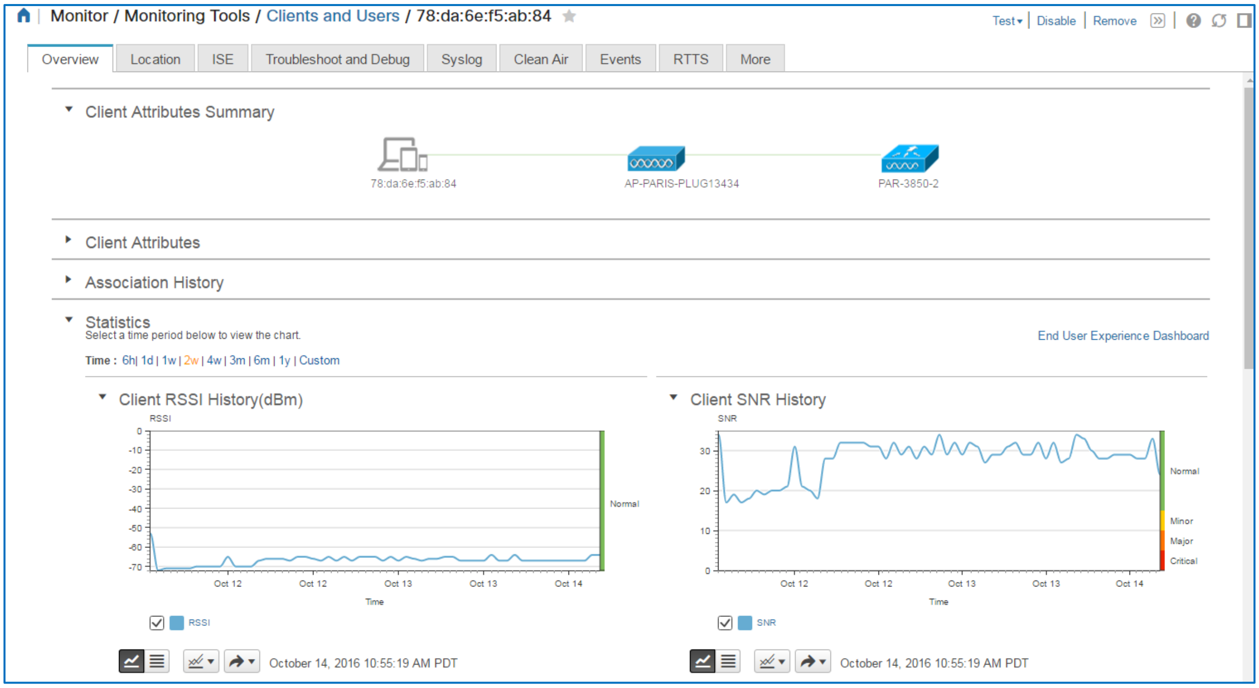
Total 83

Troubleshoot | Test ▾ | Disable | Remove | More ▾ | Track Clients | Identify Unknown Users

Show: Associated Clients ▾

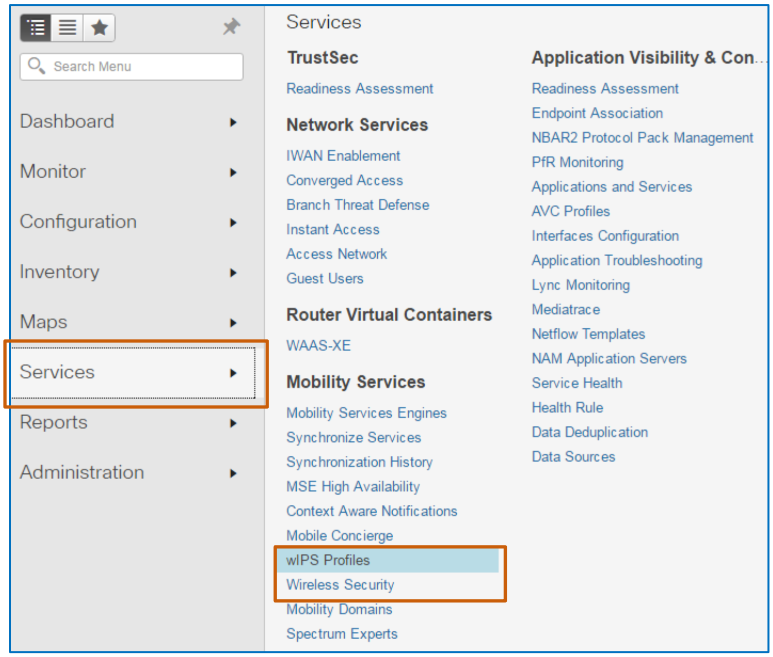
	MAC Address	IP Address	IP Type	User Na... ▲	Type	Vendor	Location	Device Name	Interface	VLAN	Protocol	Status	Association Time
○	00:02:3d:71:2c:01		Not Det...	Unknown ⓘ		Cisco	Unknown	SAM-5-PH-ACC	Fa0/22	1	802.3	Associated	19-Jul-2016,01:3
○	00:0a:b8:59:ab:96		Not Det...	Unknown ⓘ		Cisco	Unknown	SAM-5-CH-AC...	Fa1/0/24	232	802.3	Associated	17-Jul-2016,22:1
○	00:0a:b8:59:ab:99		Not Det...	Unknown ⓘ		Cisco	Unknown	SAM-5-PH-ACC	Fa0/23	232	802.3	Associated	17-Jul-2016,22:1
○	00:11:5c:40:77:54	52.52.0.4	IPv4	Unknown ⓘ		Cisco	Unknown	3850-24U_46	Gi1/0/10	52	802.3	Associated	17-Jul-2016,22:1
○	00:11:85:8d:9a:e1	10.197.72.50	IPv4	Unknown ⓘ		Hewlett...	Unknown	PI-3850-8	Gi1/0/3	96	802.3	Associated	19-Jul-2016,01:3
○	00:15:2c:38:84:00		Not Det...	Unknown ⓘ		Cisco	Unknown	SAM-5-CH-AC...	Fa1/0/24	232	802.3	Associated	19-Jul-2016,01:3
○	00:15:62:15:3f:40	10.110.181.5 ⓘ	Dual-St...	Unknown ⓘ		Cisco	Unknown	SAM-5-CH-AC...	Fa1/0/24	232	802.3	Associated	19-Jul-2016,01:3
○	00:15:62:15:4a:00		Not Det...	Unknown ⓘ		Cisco	Unknown	SAM-5-CH-AC...	Fa1/0/24	232	802.3	Associated	19-Jul-2016,01:3
○	00:15:fa:9d:08:d1		Not Det...	Unknown ⓘ		Cisco	Unknown	SAM-5-CH-AC...	Fa1/0/3	48	802.3	Associated	17-Jul-2016,22:1

It also provides detailed user and end user device information based on the network configuration. For example, in systems that include a Cisco© Mobility Services Engine, detailed location information is available.



Configuring Mobility Services for Client and User Reporting

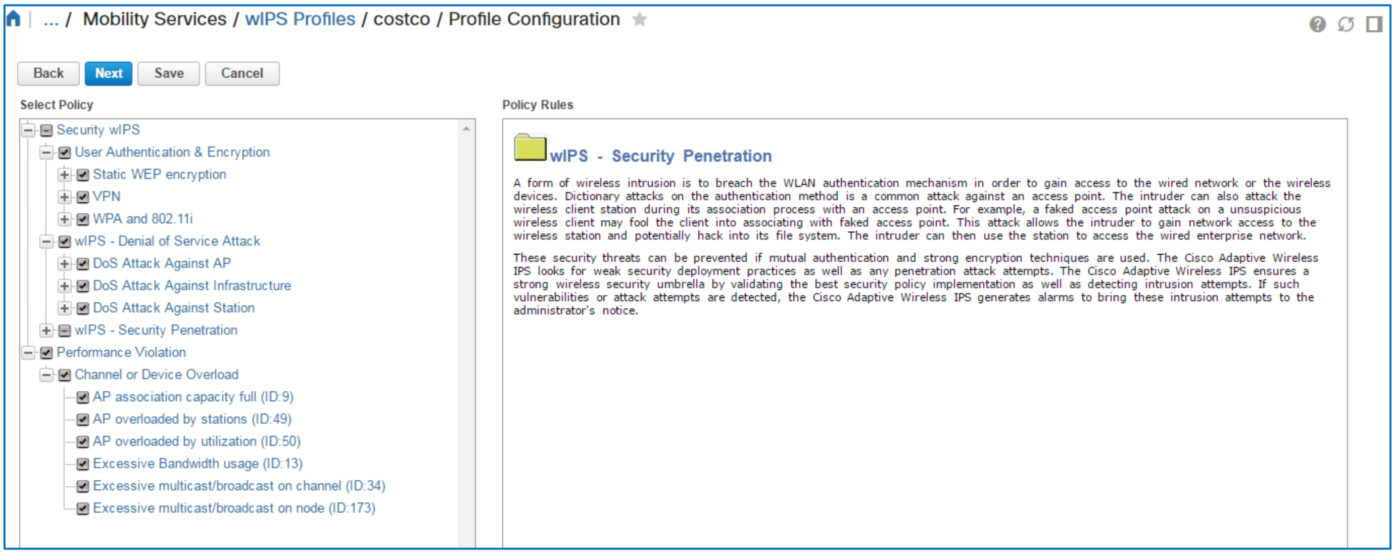
System users can configure two key mobility services, available on the **Services** menu, that define wireless client and user data reporting.



In systems that include a Mobility Services Engine (MSE), the Wireless Intrusion Protection System (wIPS) profiles define security reporting policies, such as user authentication and encryption, denial of service attacks, and security penetration; and performance violations, such as channels or devices that are exceeding usage or capacity thresholds.

User authentication and denial-of-service rules and policies help ensure that you identify and address potentially malicious clients and users.

Note: To learn more about adaptive wIPS technology and concepts, refer to the **Cisco Adaptive wIPS Deployment Guide**.


... / Mobility Services / wIPS Profiles / costco / Profile Configuration
Back
Next
Save
Cancel
Select Policy
Security wIPS
User Authentication & Encryption
Static WEP encryption
VPN
WPA and 802.11i
wIPS - Denial of Service Attack
DoS Attack Against AP
DoS Attack Against Infrastructure
DoS Attack Against Station
wIPS - Security Penetration
Performance Violation
Channel or Device Overload
AP association capacity full (ID:9)
AP overloaded by stations (ID:49)
AP overloaded by utilization (ID:50)
Excessive Bandwidth usage (ID:13)
Excessive multicast/broadcast on channel (ID:34)
Excessive multicast/broadcast on node (ID:173)
Policy Rules

wIPS - Security Penetration

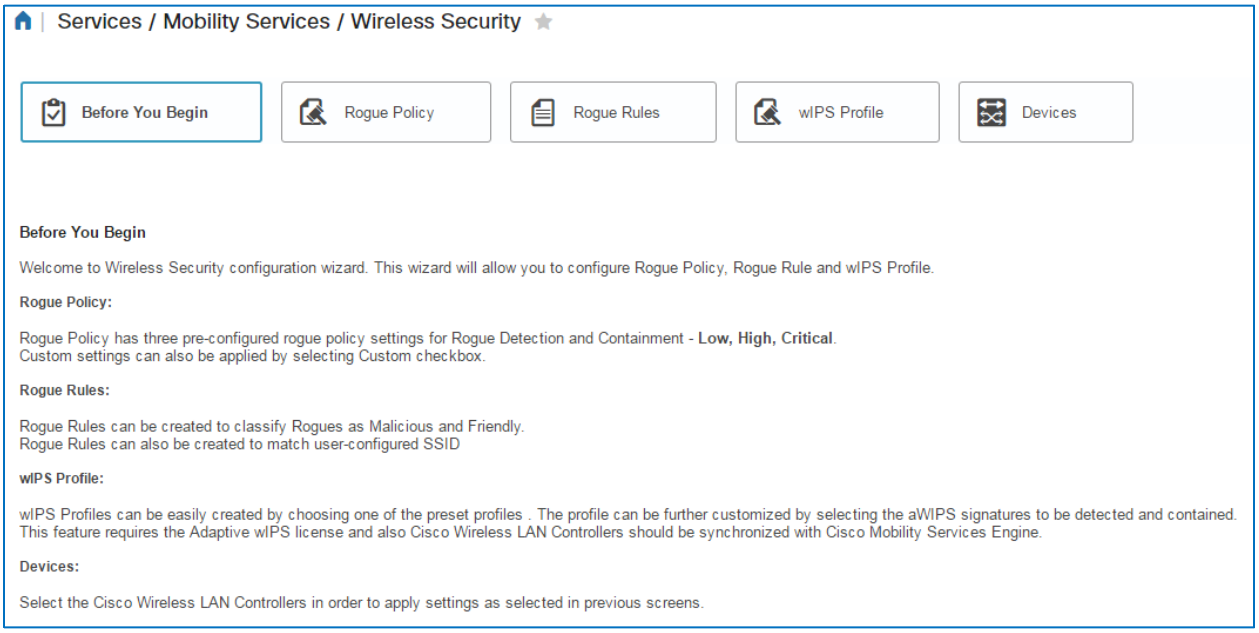
A form of wireless intrusion is to breach the WLAN authentication mechanism in order to gain access to the wired network or the wireless devices. Dictionary attacks on the authentication method is a common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked access point attack on a unsuspicious wireless client may fool the client into associating with faked access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

These security threats can be prevented if mutual authentication and strong encryption techniques are used. The Cisco Adaptive Wireless IPS looks for weak security deployment practices as well as any penetration attack attempts. The Cisco Adaptive Wireless IPS ensures a strong wireless security umbrella by validating the best security policy implementation as well as detecting intrusion attempts. If such vulnerabilities or attack attempts are detected, the Cisco Adaptive Wireless IPS generates alarms to bring these intrusion attempts to the administrator's notice.

By configuring wireless security rogue access point (AP) policies and rules, system users define how the system detects and contains rogue access points and the parameters that determine whether rogue APs are friendly or malicious.

System users apply rogue AP policies and rules to wIPS profiles.

These policies and rules also help you to identify users and clients associated with rogue APs.



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 aWIPS 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:

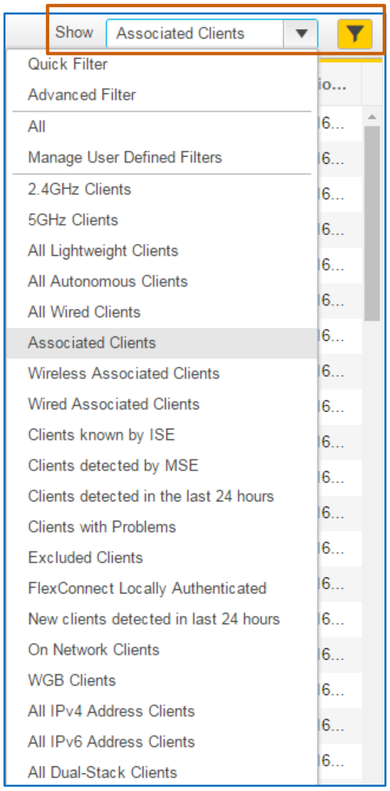
Select the Cisco Wireless LAN Controllers in order to apply settings as selected in previous screens.

Individual Client Details and Statistics

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

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

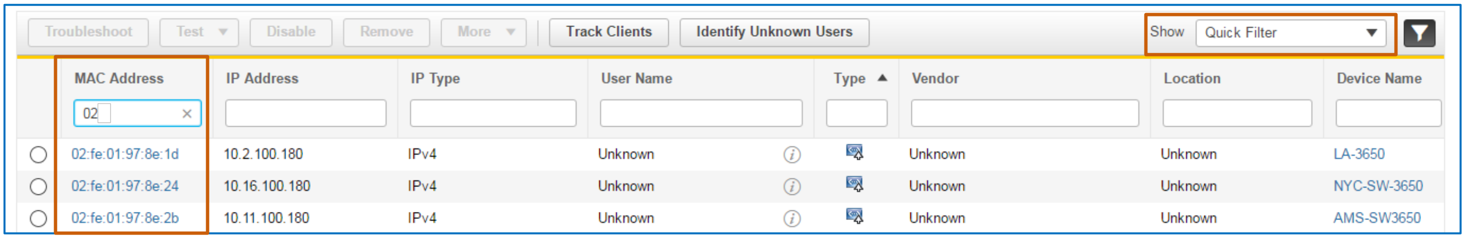
Note: When you do not see the clients that you expect, change the filter criteria to include them.



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

To apply a quick filter:

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



	MAC Address	IP Address	IP Type	User Name	Type	Vendor	Location	Device Name
	02							
○	02:fe:01:97:8e:1d	10.2.100.180	IPv4	Unknown		Unknown	Unknown	LA-3650
○	02:fe:01:97:8e:24	10.16.100.180	IPv4	Unknown		Unknown	Unknown	NYC-SW-3650
○	02:fe:01:97:8e:2b	10.11.100.180	IPv4	Unknown		Unknown	Unknown	AMS-SW3650

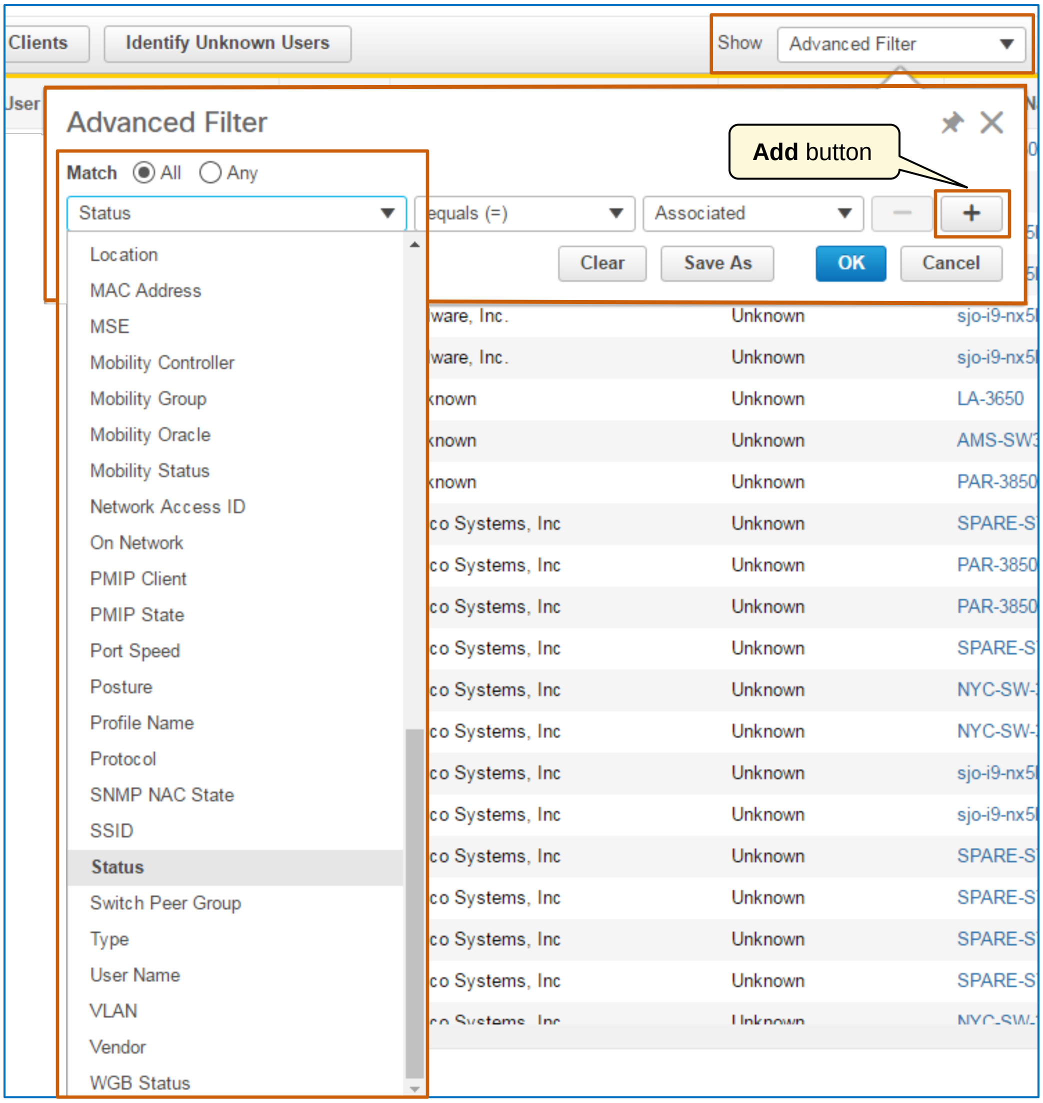
You can configure a series of filter rules to see specific clients by using the **Advanced Filter** feature.

Tip: Filtering the list to see specific types of clients can make some troubleshooting tasks easier.

To open the filter rules:

- In the **Show** drop-down list, select **Advanced Filter**.

You can configure a series of rules by clicking the **Add** button.

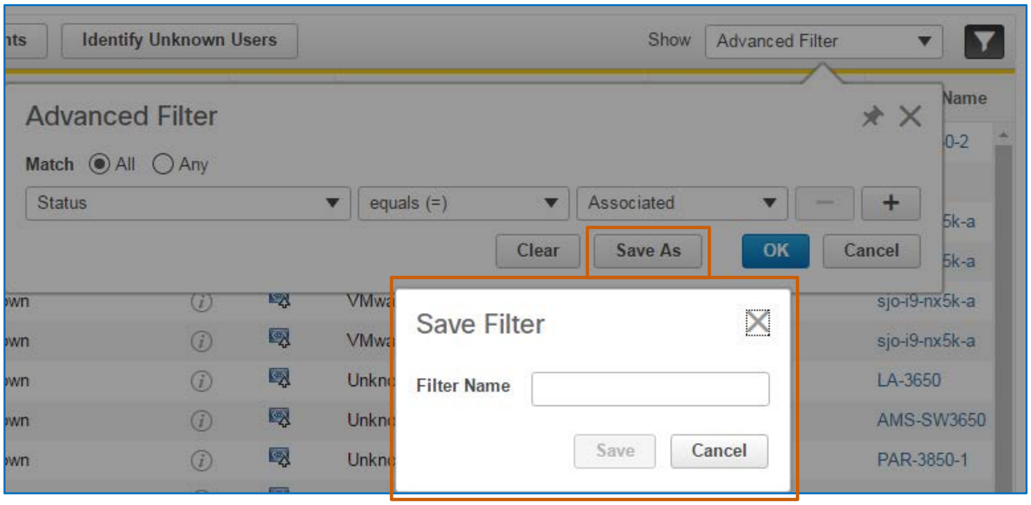


Match ● All ○ Any

Status | equals (=) | Associated

ware, Inc.	Unknown	sjo-i9-nx5
ware, Inc.	Unknown	sjo-i9-nx5
known	Unknown	LA-3650
known	Unknown	AMS-SW3
known	Unknown	PAR-3850
co Systems, Inc	Unknown	SPARE-S
co Systems, Inc	Unknown	PAR-3850
co Systems, Inc	Unknown	PAR-3850
co Systems, Inc	Unknown	SPARE-S
co Systems, Inc	Unknown	NYC-SW-
co Systems, Inc	Unknown	NYC-SW-
co Systems, Inc	Unknown	sjo-i9-nx5
co Systems, Inc	Unknown	sjo-i9-nx5
co Systems, Inc	Unknown	SPARE-S
co Systems, Inc	Unknown	SPARE-S
co Systems, Inc	Unknown	SPARE-S
co Systems, Inc	Unknown	SPARE-S
co Systems, Inc	Unknown	NYC-SW-

You can configure and save advanced filters for future use.



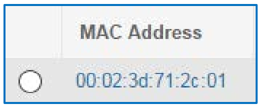
Show: Advanced Filter

Match: ● All ○ Any

Status | equals (=) | Associated

To review detailed information for a client:

- On the **Clients and Users** page, click the **Mac Address** link of the client of interest.



	MAC Address
○	00:02:3d:71:2c:01

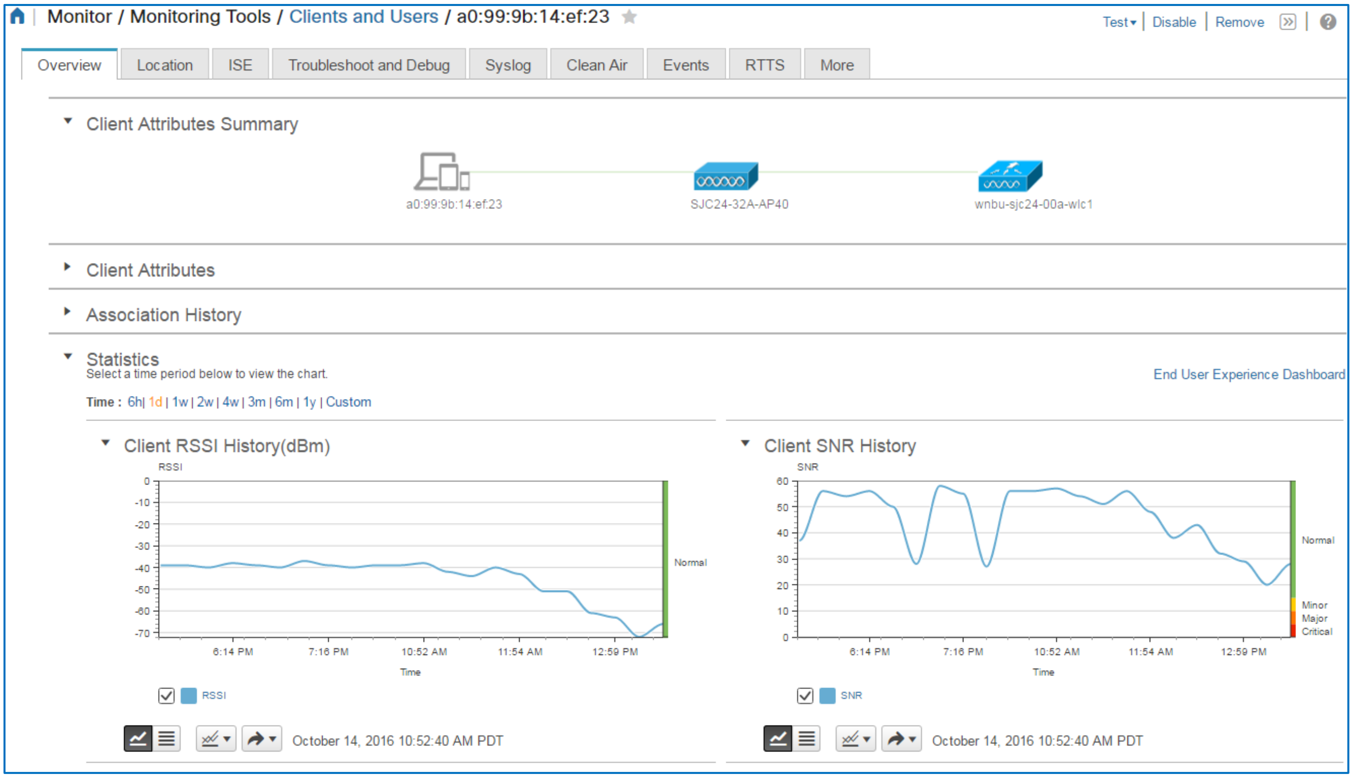
The details page provides summary and additional information based on the client type and whether the network configuration includes other data collection servers, such as Identity Service Engine (ISE) or Mobility Service Engine (MSE) servers.

Tip: The data that you see in client details is populated from the database.

To ensure that you are seeing current information, refresh the page.

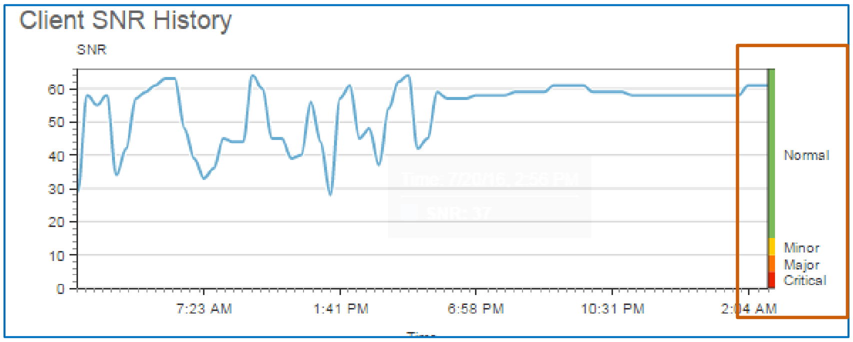
On the **Overview** tab, you can review:

- Client attributes
- Client session history
- Statistics over time for:
  - Received signal strength indicator (RSSI) history
  - Signal to noise ratio (SNR) history
  - Data exchange rates
  - The applications that the client accesses most often
- Site maps, when an MSE sever is included in the system configuration.



Select a time period below to view the chart.

Note: The RSSI and SNR charts provide color-coding on their y axes based on Cisco best practices. That way, you can recognize more easily those statistics that are in normal ranges and those that are crossing or remaining in thresholds that Cisco considers of minor, major, or critical concern.

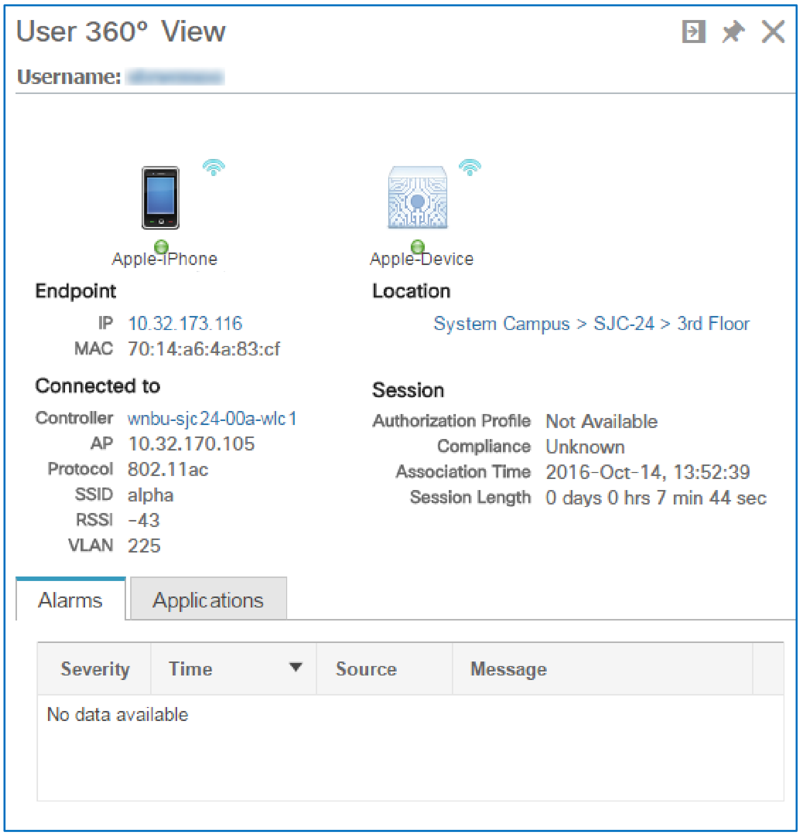


Information and tools available on other tabs can include:

- The client’s current location and location history, when the configuration includes at least one Mobility Services Engine.
- The client’s identification, onboarding, posture, and policy, when the configuration includes at least one Identity Services Engine.
- Troubleshooting analysis tools.
- RF interference and air status, when the configuration includes specific types of wireless access points.
- Events that the client is reporting.
- Additional IP and testing tools.

Device and User Information

The **User 360^0 View** pop-up window provides key information about the client.



User 360° View

Username: [redacted]

Endpoint

IP 10.32.173.116
MAC 70:14:a6:4a:83:cf

Location

System Campus > SJC-24 > 3rd Floor

Connected to

Controller wnbu-sjc24-00a-wlc1
AP 10.32.170.105
Protocol 802.11ac
SSID alpha
RSSI -43
VLAN 225

Session

Authorization Profile Not Available
Compliance Unknown
Association Time 2016-Oct-14, 13:52:39
Session Length 0 days 0 hrs 7 min 44 sec

Severity	Time	Source	Message
No data available			

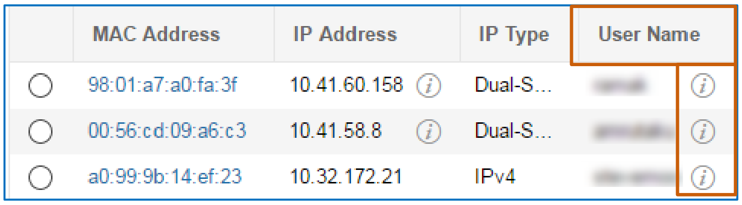
You can see where and how the user is connected, any alarms associated with the session, and the application or applications in use.

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

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

To open a client's User 360^0 View pop-up window:

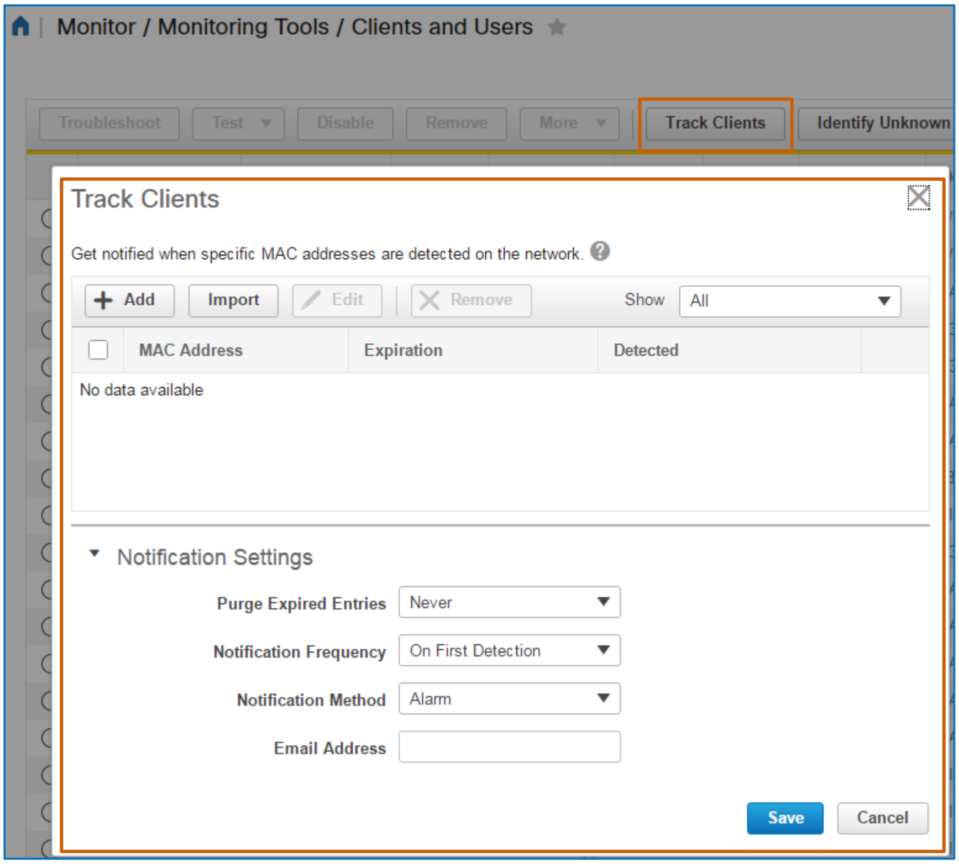
- In the client's **User Name** field, click the information icon.



	MAC Address	IP Address	IP Type	User Name
○	98:01:a7:a0:fa:3f	10.41.60.158 ⓘ	Dual-S...	[redacted] ⓘ
○	00:56:cd:09:a6:c3	10.41.58.8 ⓘ	Dual-S...	[redacted] ⓘ
○	a0:99:9b:14:ef:23	10.32.172.21	IPv4	[redacted] ⓘ

Ongoing Client Behavior

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



Track Clients

Get notified when specific MAC addresses are detected on the network.

Show: All

□	MAC Address	Expiration	Detected
No data available			

Notification Settings

Purge Expired Entries: Never

Notification Frequency: On First Detection

Notification Method: Alarm

Email Address:

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

You can configure the system to generate alarms or generate and send e-mail notifications to you or to the users that you designate when the network detects the client.

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 Key Concepts

To learn more about adaptive wIPS technology and concepts, refer to the **Cisco Adaptive wIPS Deployment Guide**.

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.