Wired Clients and Users Monitoring Overview

Cisco© Prime Infrastructure 3.1

Job Aid

Copyright Page

Wired Clients and Users Monitoring Overview Job Aid

Contents

Basics

Overview

Introduction

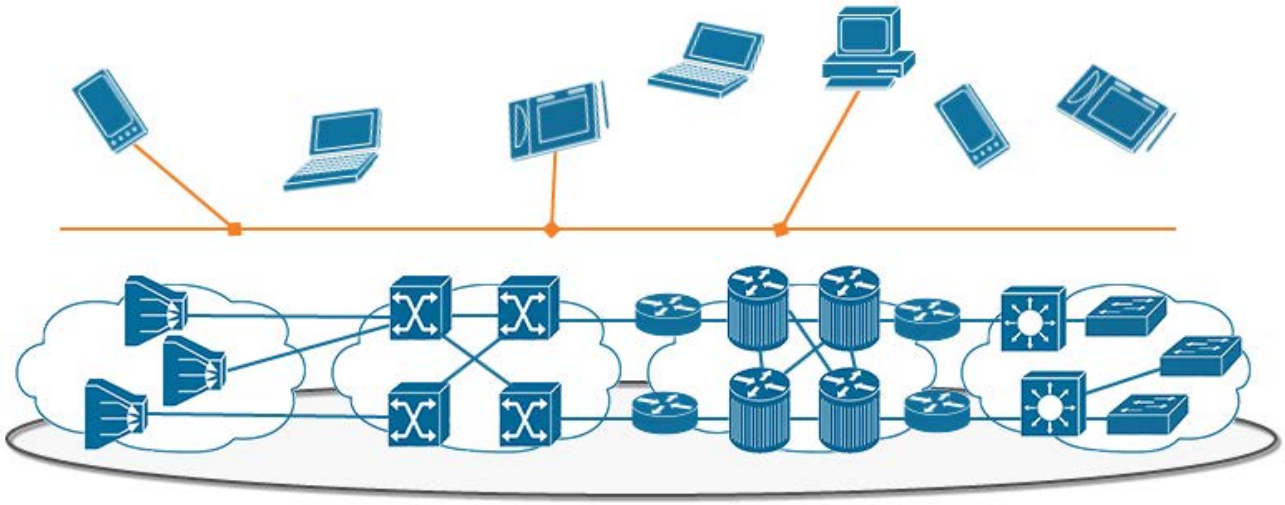
To better ensure the customer experience and meet enterprise goals, you monitor user and network behavior and performance metrics to determine whether users are able to:

- 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

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

Monitoring Clients and Users

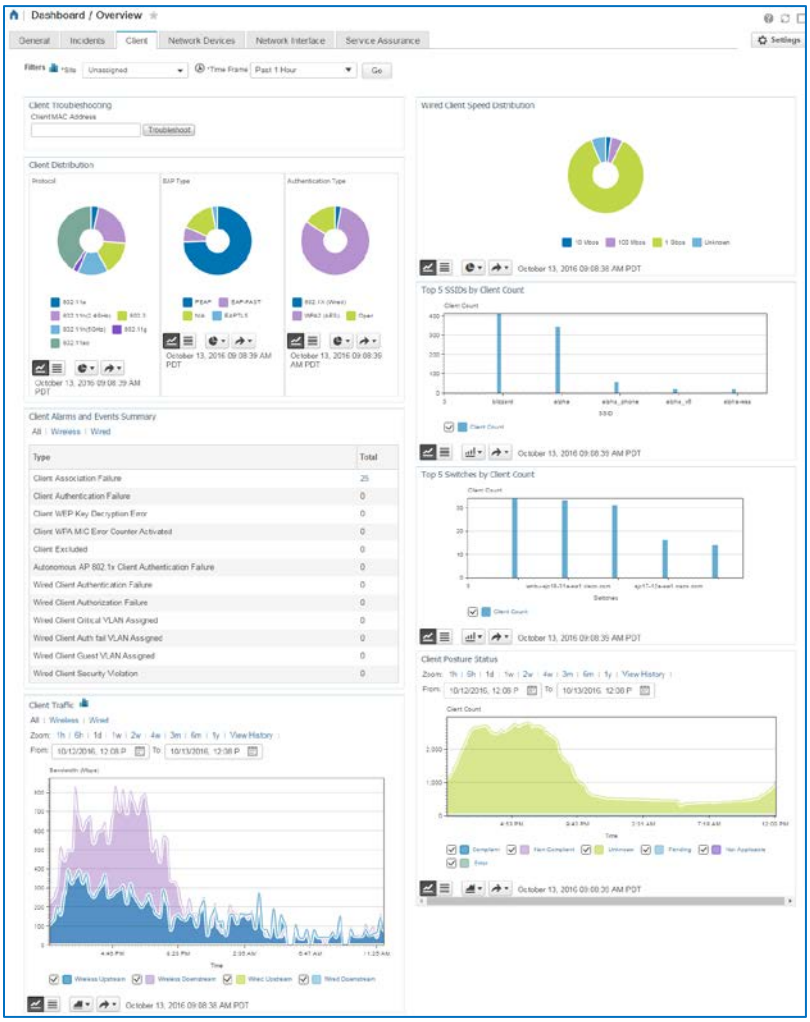
Summary Wired Client and User Data

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 **Wired Network Summary Data Overview** job aid.

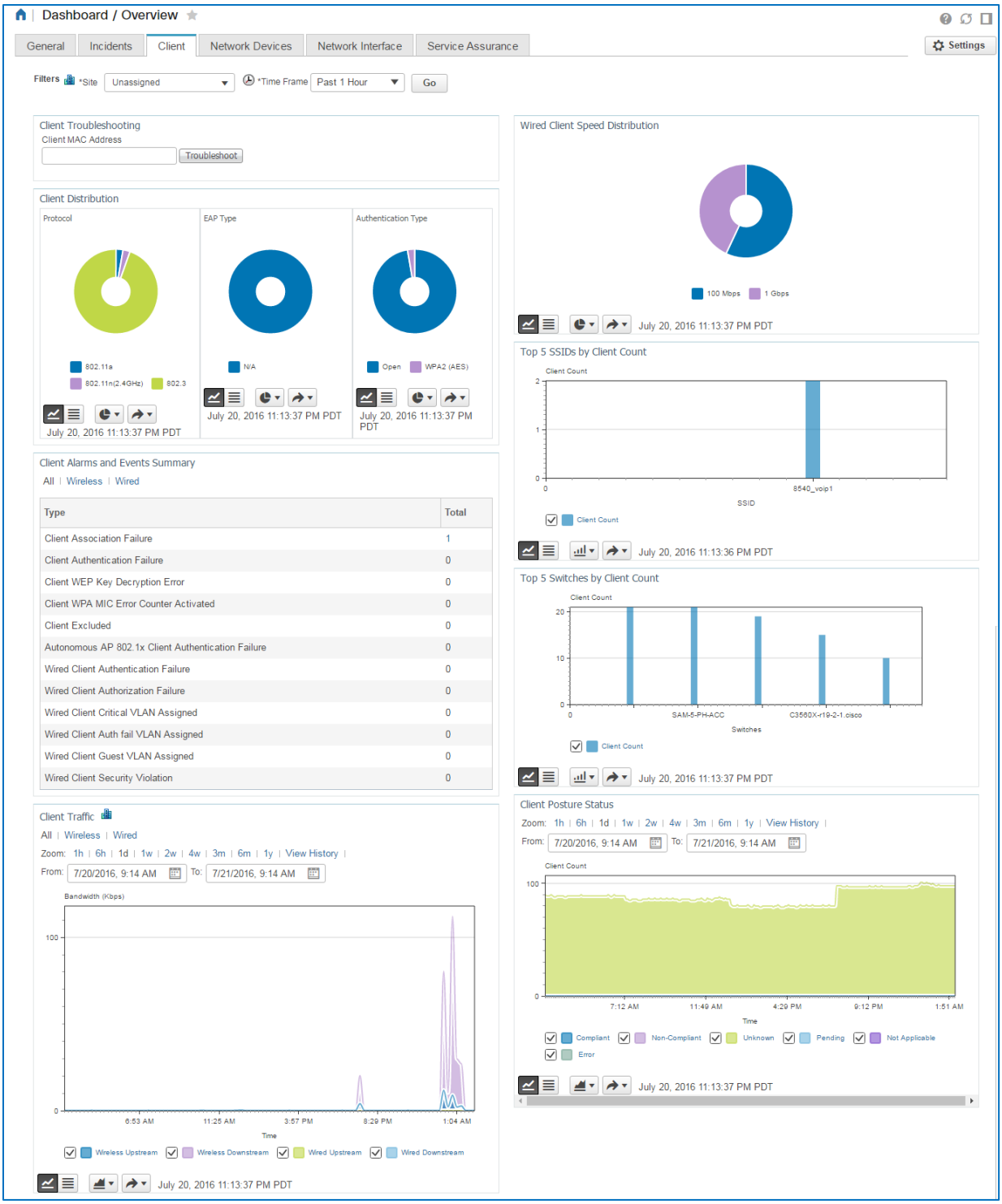
While some dashboards and dashlets combine reporting on both wired and wireless areas of the network, this job aid focuses on wired network monitoring.



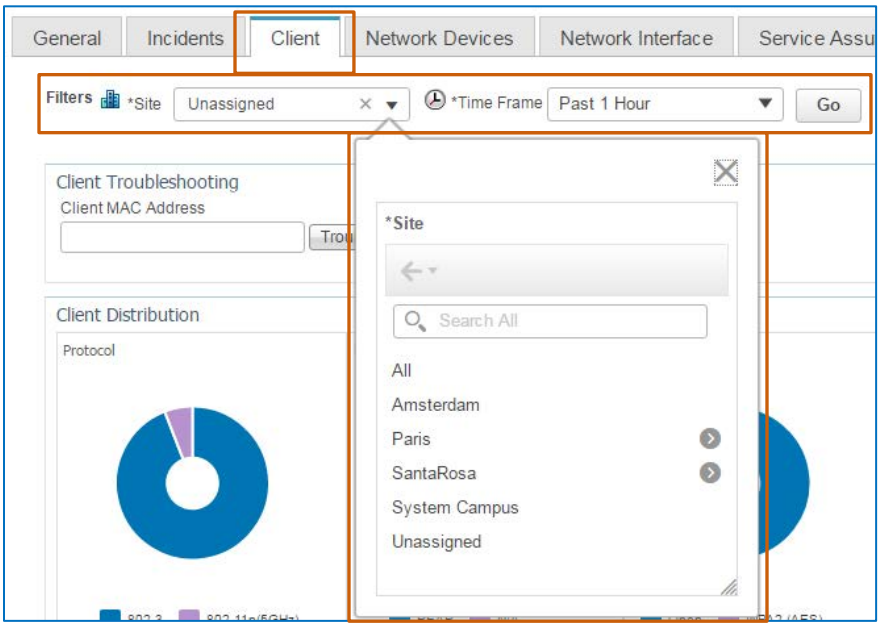
Client Summary Data Dashlets

Overview

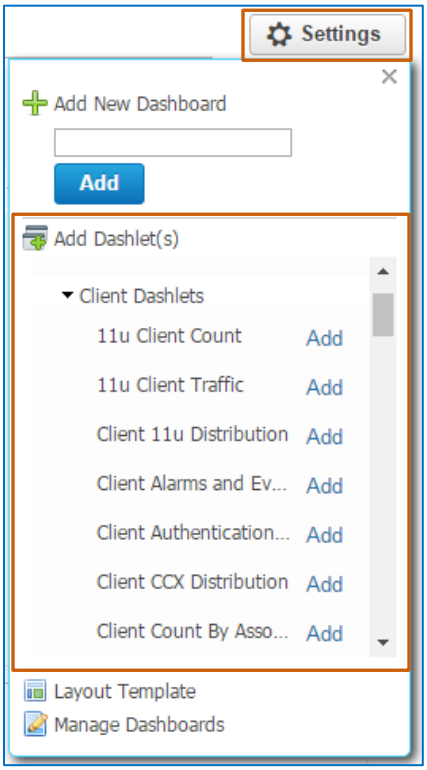
On the **Client** dashboard, you can monitor summary information about the wired clients connected to the network.



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



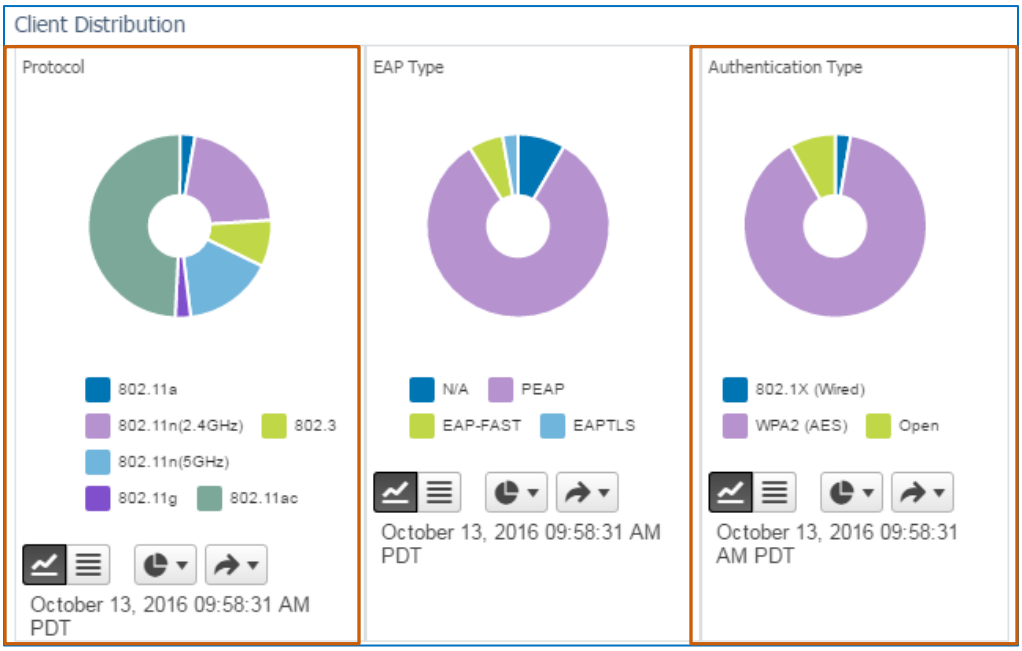
This topic addresses some of the key dashlets that users commonly monitor. The system offers an extensive number of client-related dashlets, which are available on the **Settings** menu.



Connection Protocol and Authentication Data

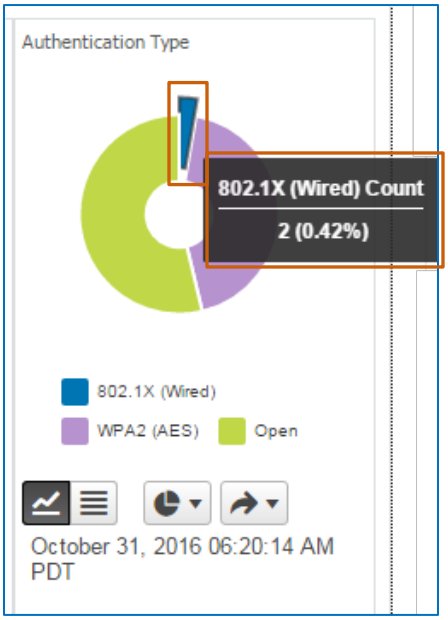
The Client Distribution dashlet reports:

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



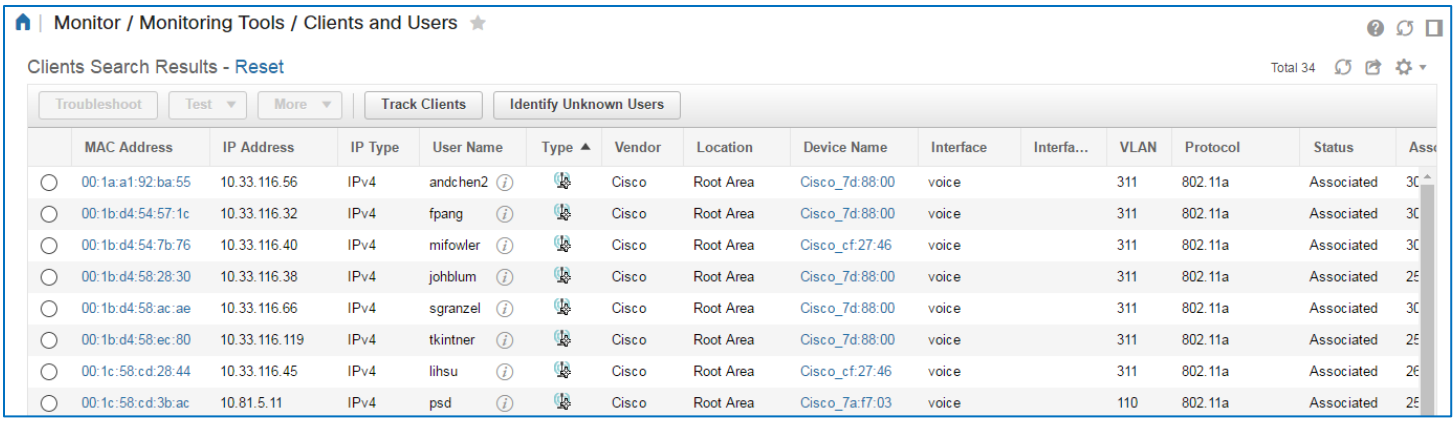
To see the number of clients that a chart element represents:

- 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.

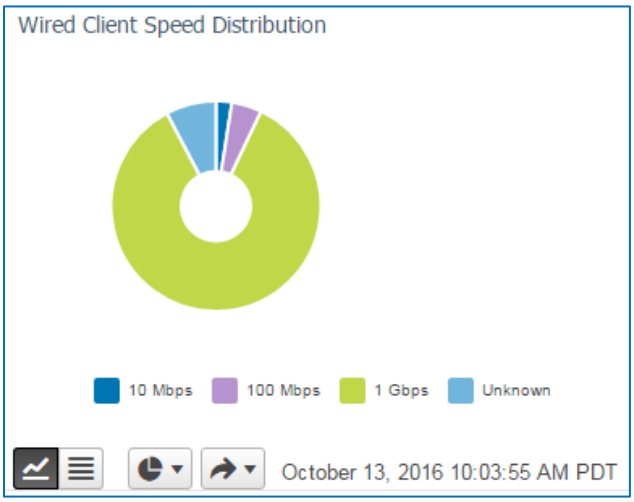


MAC Address	IP Address	IP Type	User Name	Type	Vendor	Location	Device Name	Interface	Interfa...	VLAN	Protocol	Status	Ass
00:1a:a1:92:ba:55	10.33.116.56	IPv4	andchen2		Cisco	Root Area	Cisco_7d:88:00	voice		311	802.11a	Associated	30
00:1b:d4:54:57:1c	10.33.116.32	IPv4	fpang		Cisco	Root Area	Cisco_7d:88:00	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

Client Port Speed Usage Data

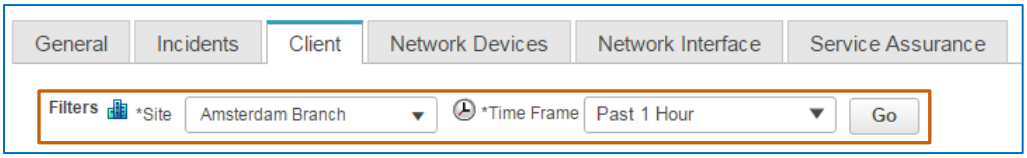
The **Wired Client Speed Distribution** dashlet reports the number and percentage of wired clients that are using various port speeds based on the ports to which the clients are connected.

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



Alarm and Event Data

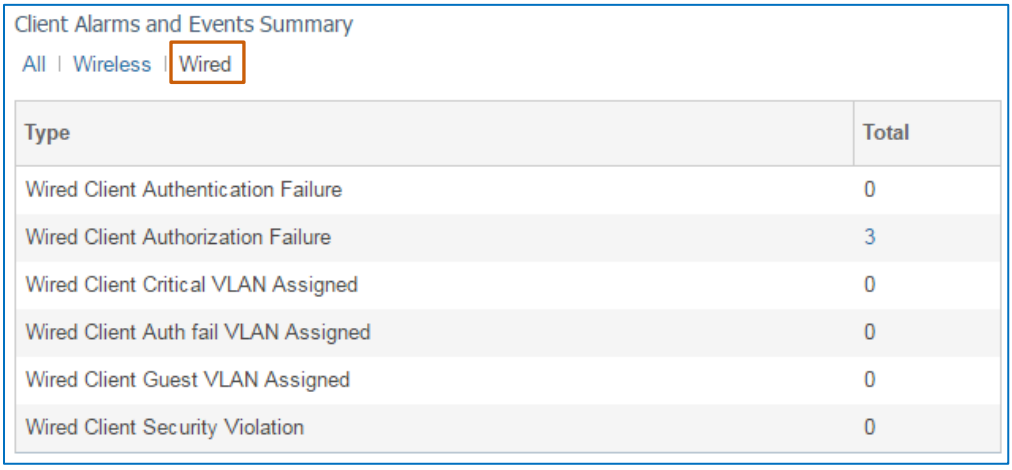
The **Client Alarms and Events Summary** dashlet lists the active, client-related alarms and events for the site and timeline selected on the dashboard.



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

To see alarms related to wired clients:

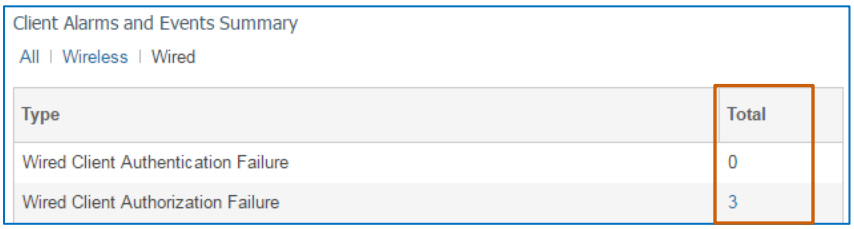
- Below the dashlet title, click **Wired**. The dashlets lists the wired alarm categories only.



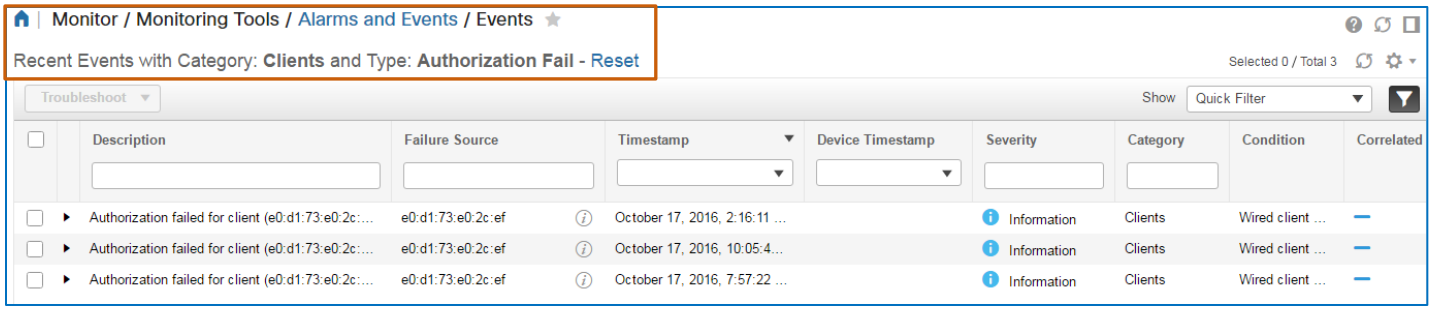
Type	Total
Wired Client Authentication Failure	0
Wired Client Authorization Failure	3
Wired Client Critical VLAN Assigned	0
Wired Client Auth fail VLAN Assigned	0
Wired Client Guest VLAN Assigned	0
Wired Client Security Violation	0

To review the alarms associated with an alarm type:

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



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



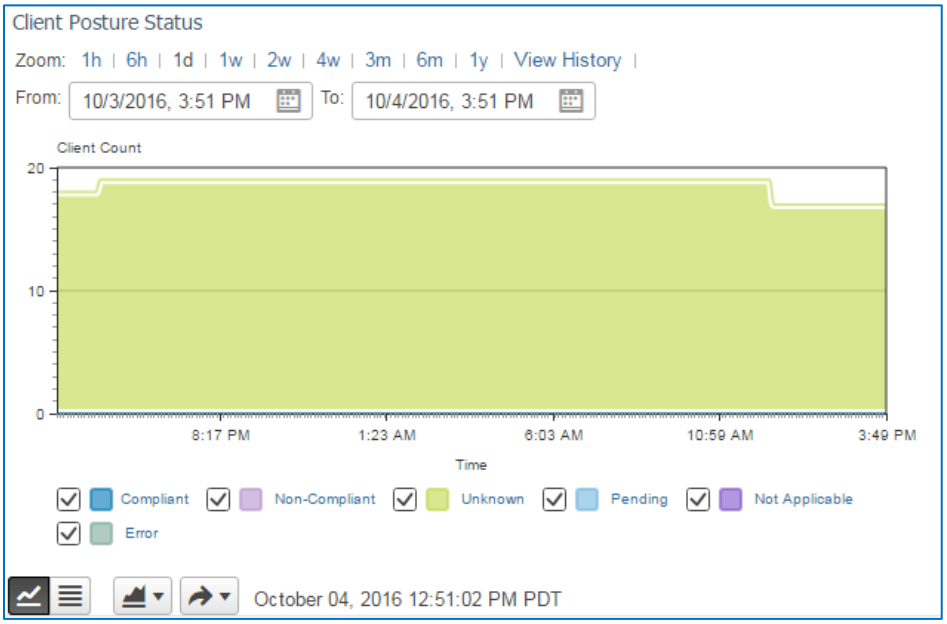
Clients Non-Compliant with ISE Access Authorization Rules

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 that are in or out of compliance with the rules configured on the ISE.

Note: In order for Prime Infrastructure to report ISE rule compliance, the client devices must be integrated with the ISE.

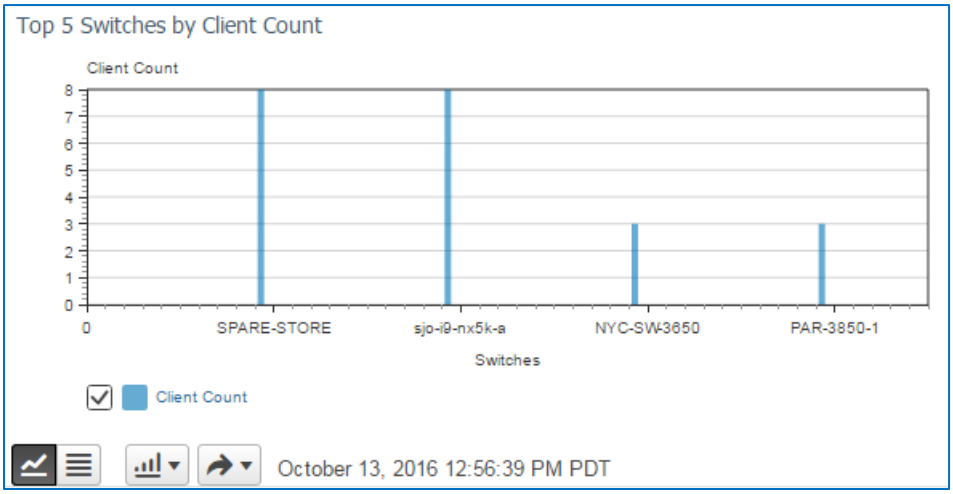
Rules on ISE servers can define such compliance requirements as operating system, browser, or anti-virus minimum standards, for example.

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.



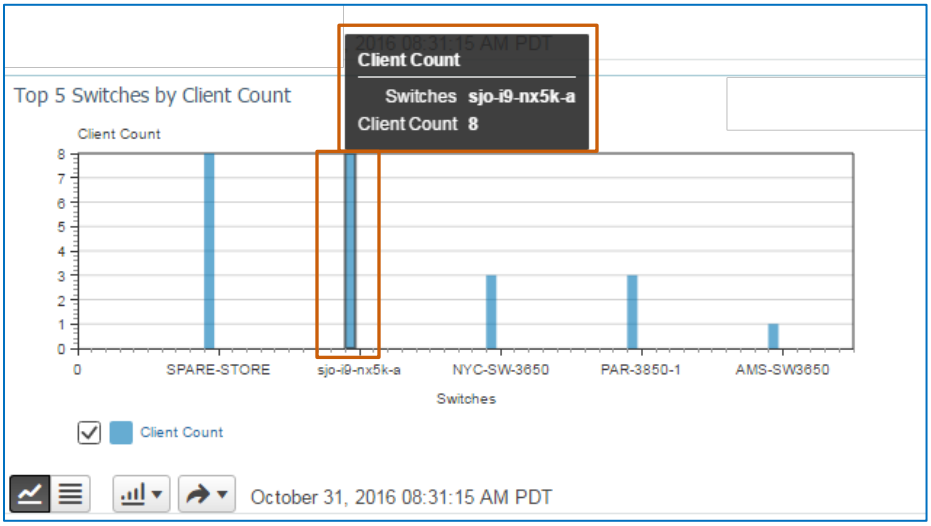
Switches with the Most Connected Clients

The **Top 5 Switches by Client Count** dashlet reports the five network switches with the greatest number of connected clients.



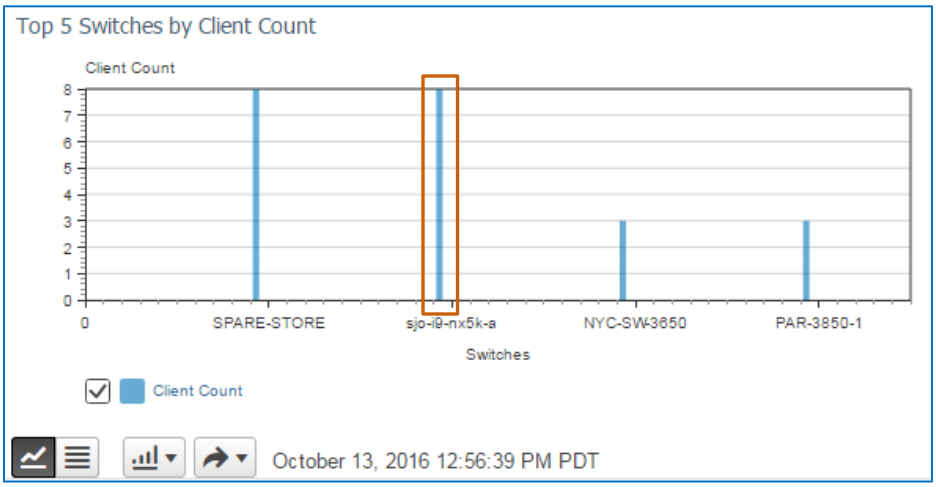
To see the number of clients connected to a switch:

- Point to the chart element. The pop-up window displays the number of clients.

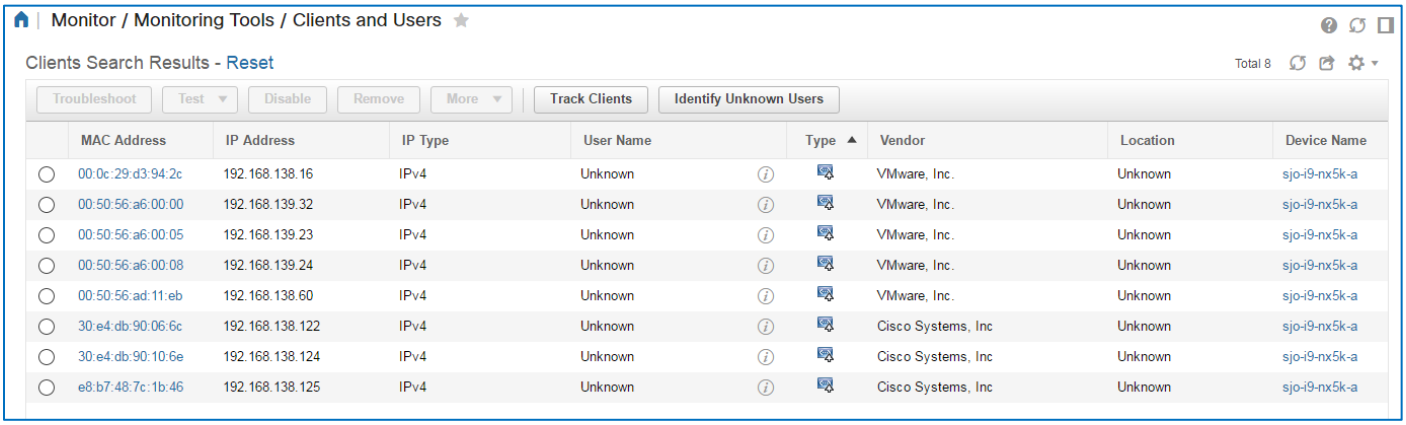


To review the clients connected to a specific switch:

- Click the chart element for the switch.



The system navigates to the **Clients and Users** page and lists the clients that are connected to the switch.



MAC Address	IP Address	IP Type	User Name	Type	Vendor	Location	Device Name
00:0c:29:d3:94:2c	192.168.138.16	IPv4	Unknown		VMware, Inc.	Unknown	sjo-i9-nx5k-a
00:50:56:a6:00:00	192.168.139.32	IPv4	Unknown		VMware, Inc.	Unknown	sjo-i9-nx5k-a
00:50:56:a6:00:05	192.168.139.23	IPv4	Unknown		VMware, Inc.	Unknown	sjo-i9-nx5k-a
00:50:56:a6:00:08	192.168.139.24	IPv4	Unknown		VMware, Inc.	Unknown	sjo-i9-nx5k-a
00:50:56:ad:11:eb	192.168.138.60	IPv4	Unknown		VMware, Inc.	Unknown	sjo-i9-nx5k-a
30:e4:db:90:06:6c	192.168.138.122	IPv4	Unknown		Cisco Systems, Inc	Unknown	sjo-i9-nx5k-a
30:e4:db:90:10:6e	192.168.138.124	IPv4	Unknown		Cisco Systems, Inc	Unknown	sjo-i9-nx5k-a
e8:b7:48:7c:1b:46	192.168.138.125	IPv4	Unknown		Cisco Systems, Inc	Unknown	sjo-i9-nx5k-a

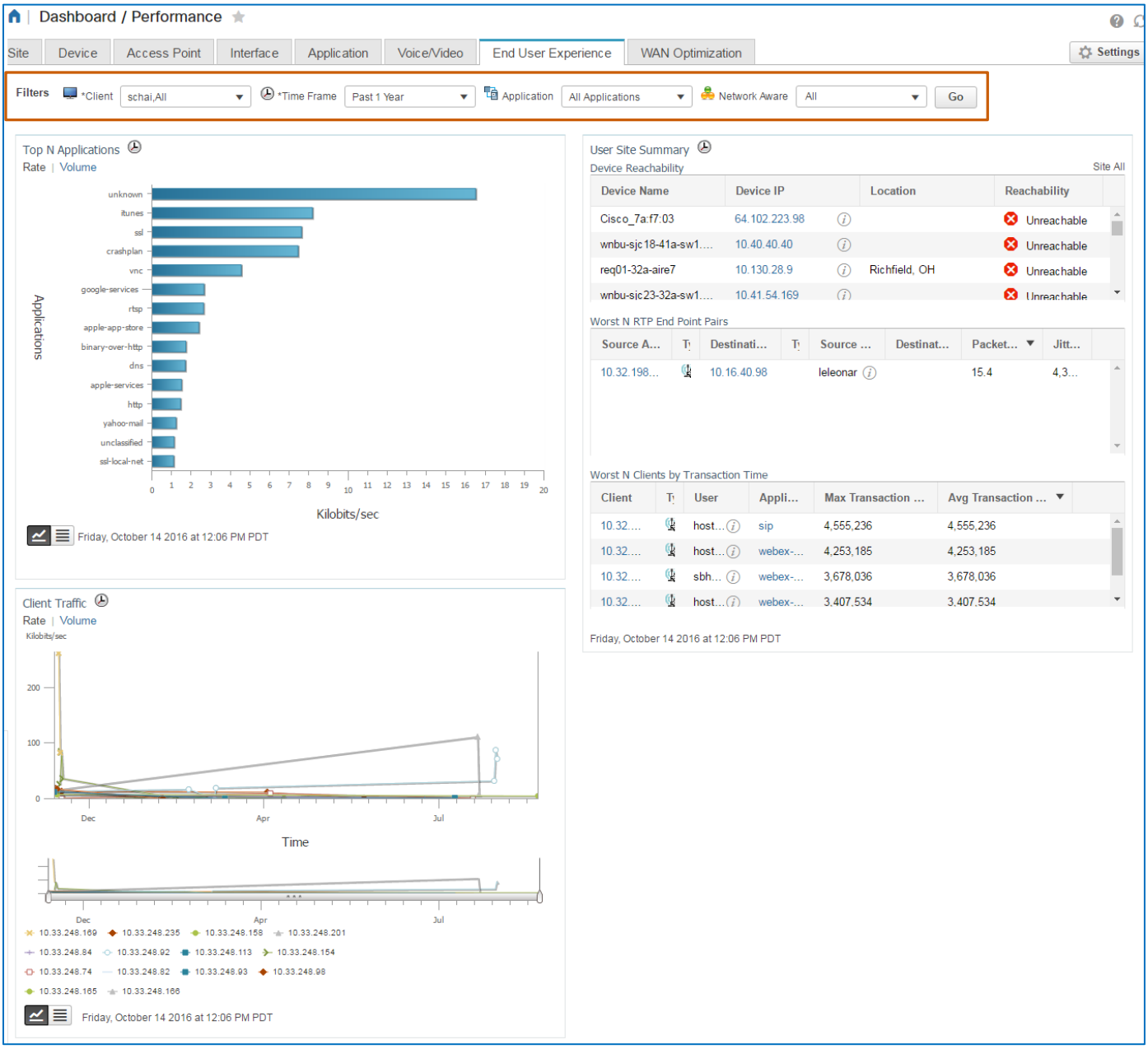
End User Experience Summary Data

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

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

To apply one or more filters:

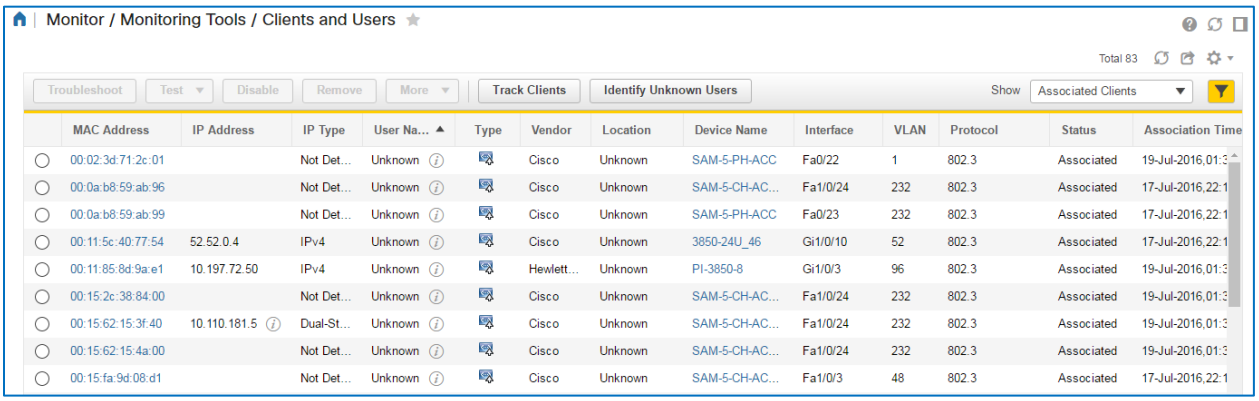
- On the toolbar, make your selections in the drop-down lists, and then click **Go**.



Detailed Client and User Activity

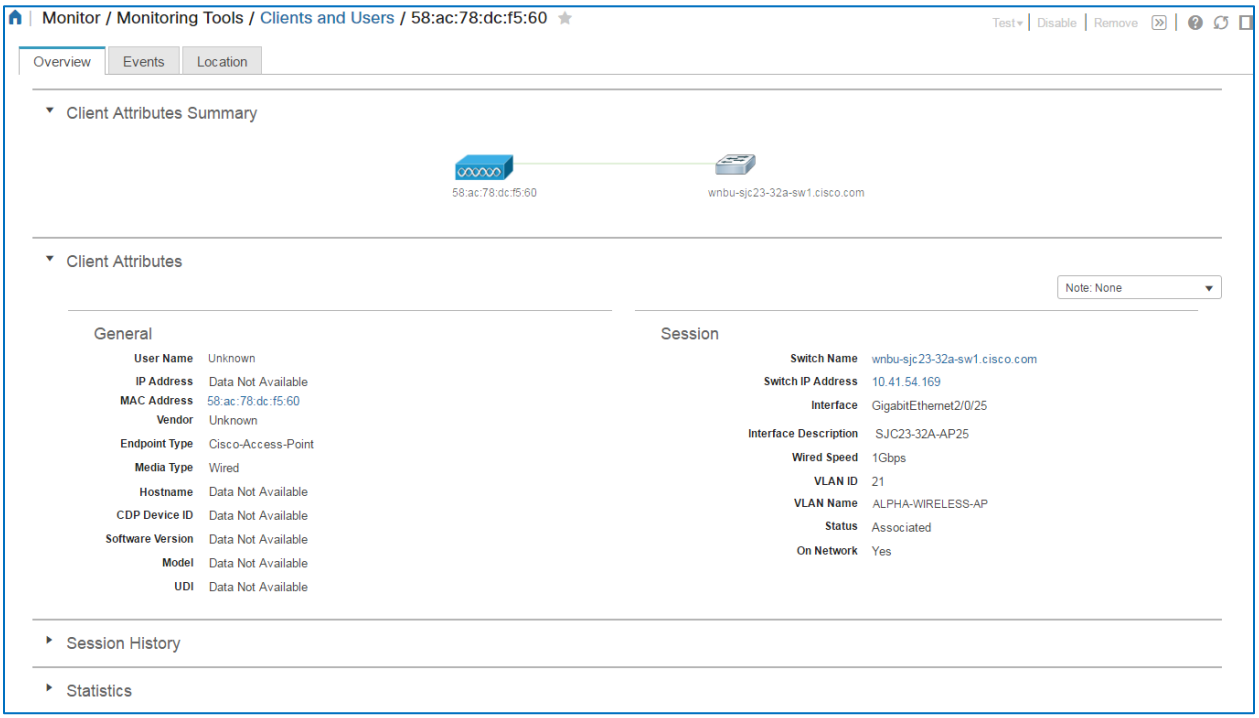
Overview

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



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 data that system users can configure. For example, system users can configure civic (physical address) locations or geographical coordinates for devices, which makes location information available on the **Location** tab.

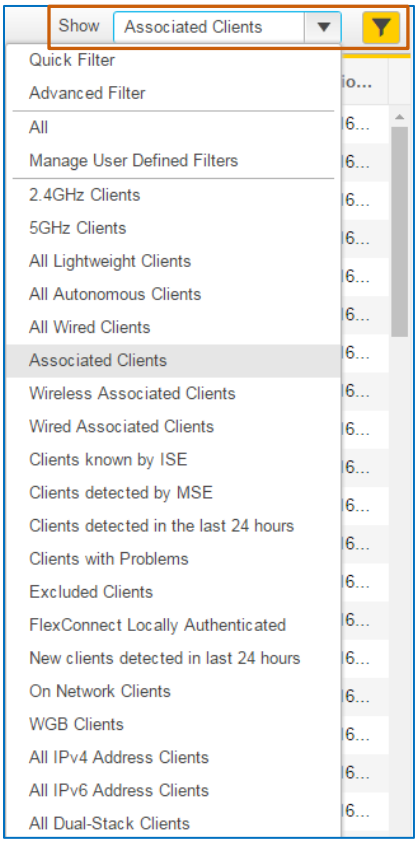


Individual Client Details and Statistics

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

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

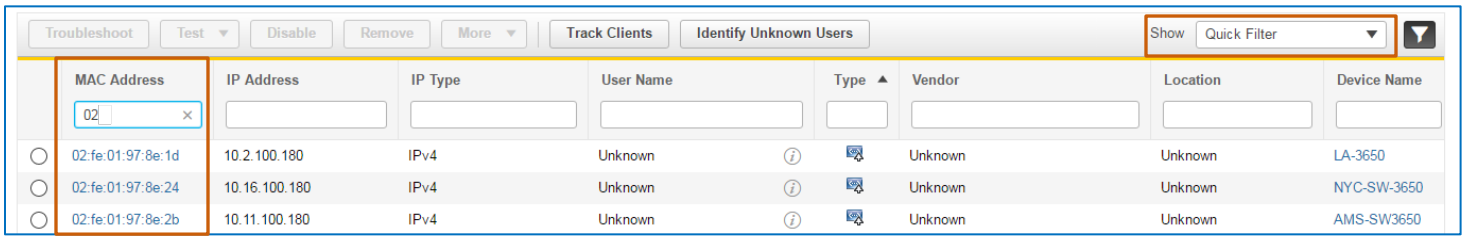
Note: When you do not see the clients that you expect, change the filter criteria to include them.



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

To apply a quick filter:

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



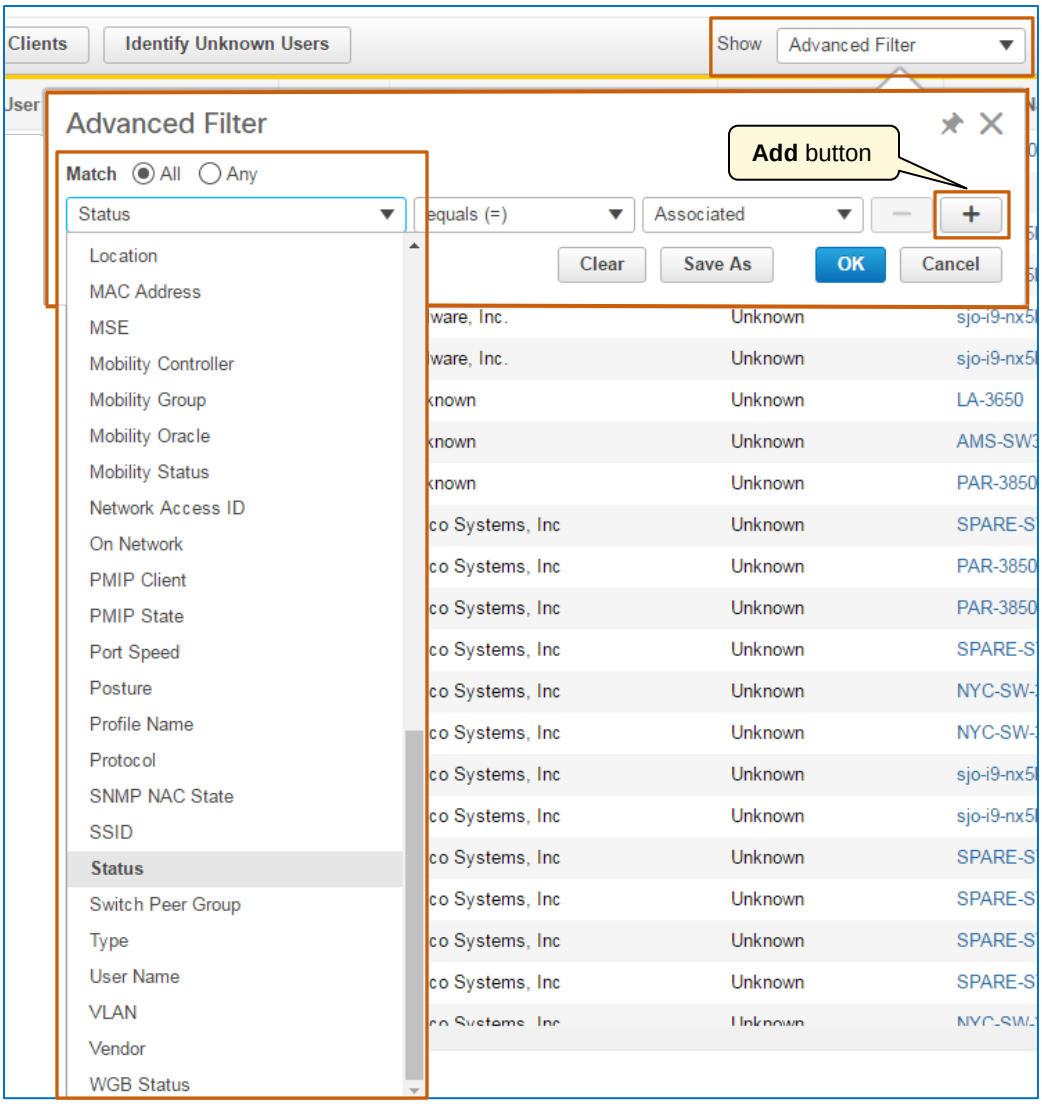
You can configure a series of filter rules to see specific clients by using the **Advanced Filter** feature.

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

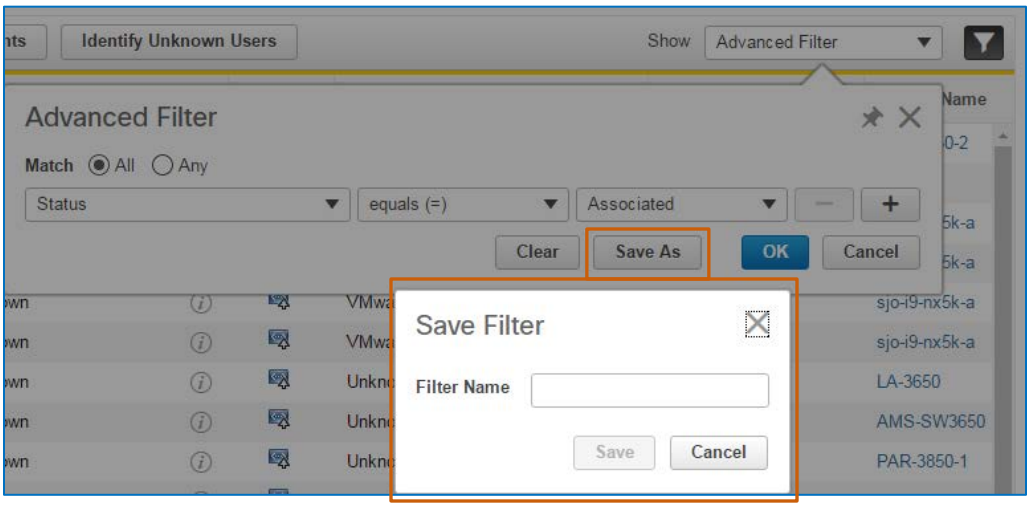
To open the filter rules:

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

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

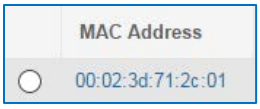


You can configure and save advanced filters for future use.



To review detailed information for a client:

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



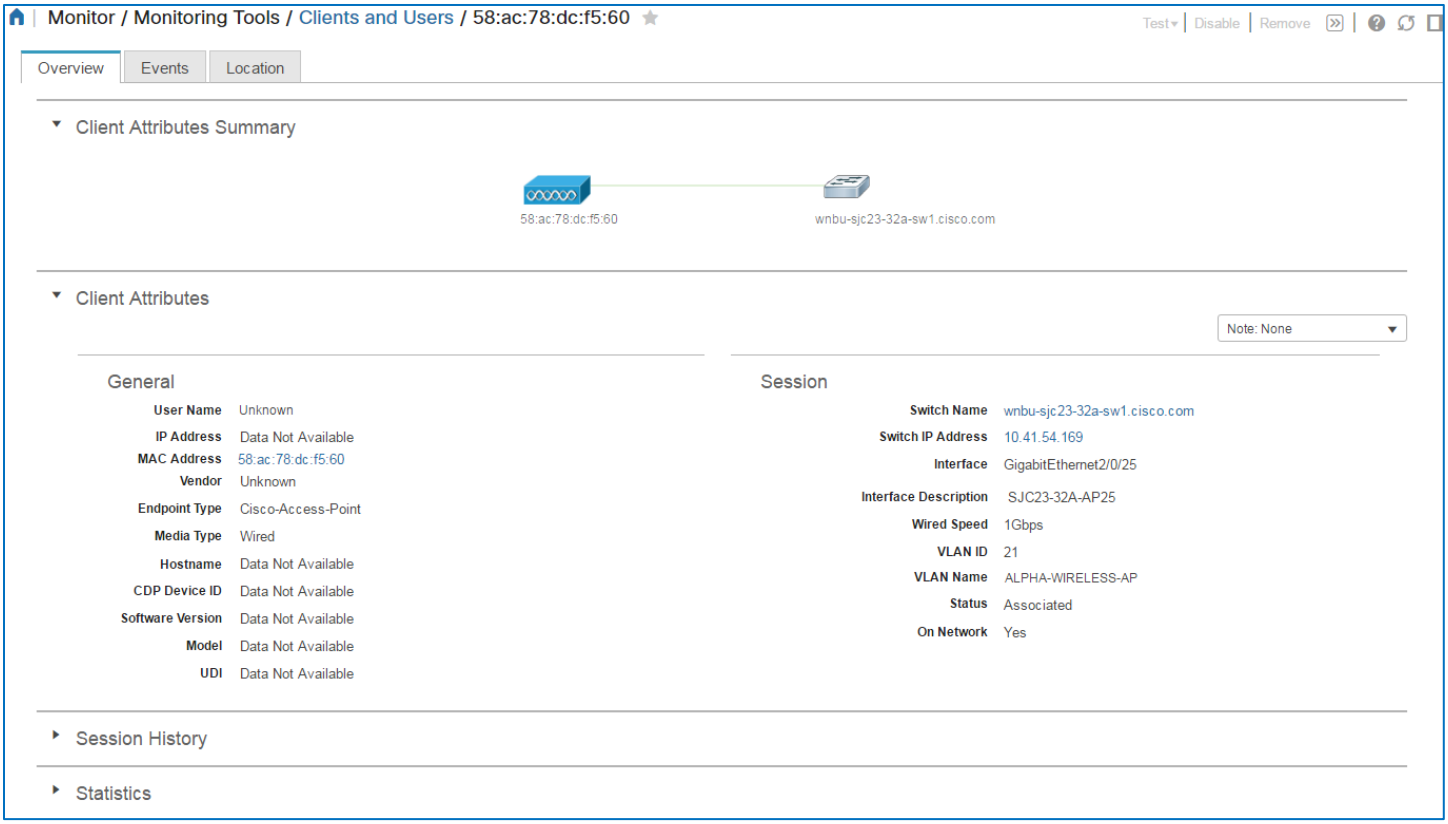
The details page provides summary and additional information based on the client type and whether the network configuration includes other data collection servers, such as Identity Service Engine (ISE) or Mobility Service Engine (MSE) servers.

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:
  - Data exchange rates
  - The applications that the client accesses most often

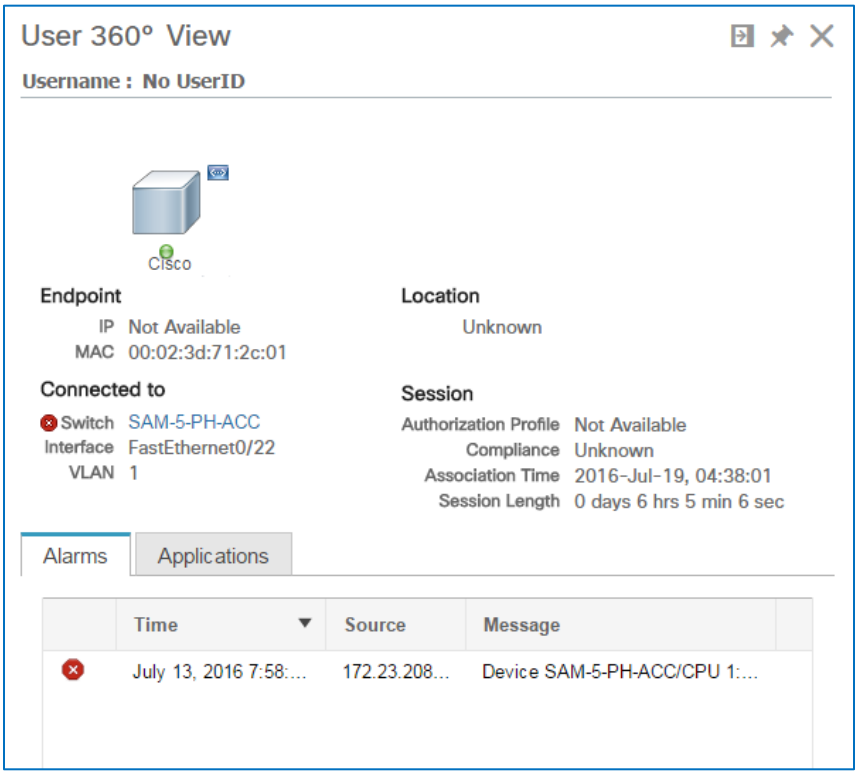


Information and tools available on other tabs can include:

- 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.
- Events that the client is reporting.

Device and User Information

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



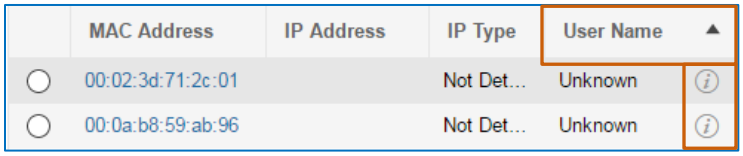
You can see where and how the user is connected, any alarms associated with the session, and the application or applications in use.

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

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

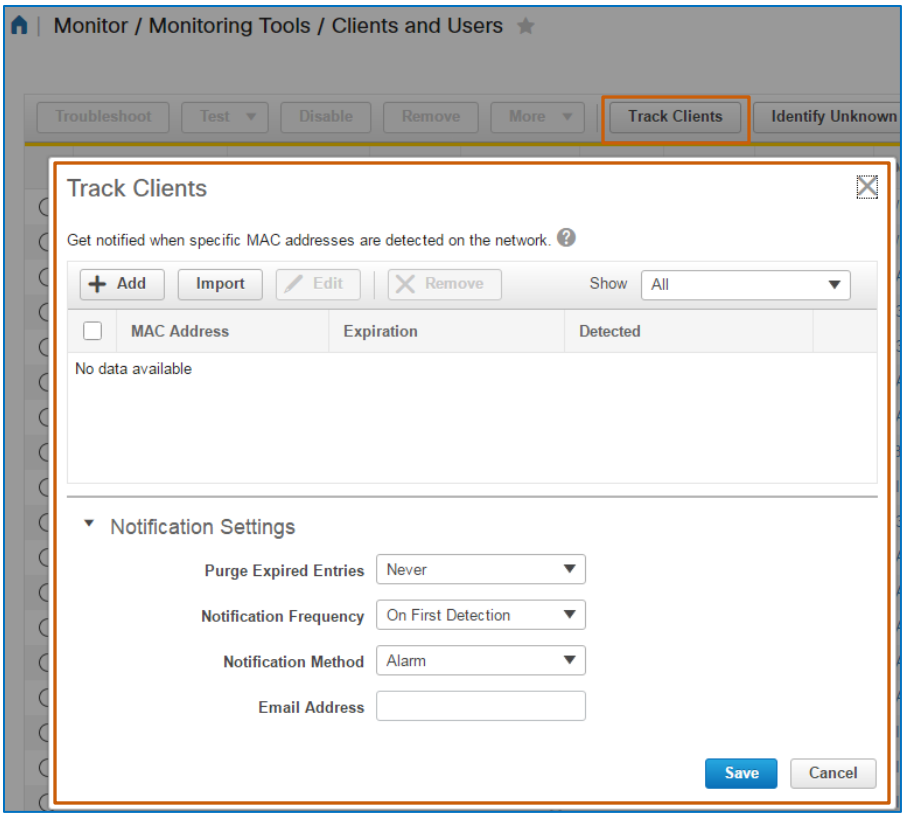
To open a client's User 360⁰ View pop-up window:

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



Ongoing Client Behavior

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



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

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 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.