

# RUCKUS Analytics User Guide, 2.3

# Copyright, Trademark and Proprietary Rights Information

© 2021 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

## Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

*These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.*

## Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

## Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

## Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

---

<b>Preface</b> .....	<b>9</b>
Document Conventions.....	9
Notes, Cautions, and Safety Warnings.....	9
Command Syntax Conventions.....	9
Document Feedback.....	10
RUCKUS Product Documentation Resources.....	10
Online Training Resources.....	10
Contacting RUCKUS Customer Services and Support.....	11
What Support Do I Need?.....	11
Open a Case.....	11
Self-Service Resources.....	11
<b>RUCKUS Analytics Overview</b> .....	<b>13</b>
RUCKUS Analytics Introduction.....	13
<b>Logging In to RUCKUS Analytics</b> .....	<b>15</b>
<b>Navigating the RUCKUS Analytics User Interface</b> .....	<b>17</b>
Header Panel.....	17
Search Field .....	18
Using the Navigation Bar.....	19
<b>Feature Support Matrix</b> .....	<b>21</b>
<b>RUCKUS Analytics Dashboard</b> .....	<b>23</b>
Dashboard Overview.....	23
Melissa AI Assistant.....	24
Time Selection Field.....	26
Incident Selection.....	26
Scrolling Data Tile.....	26
Incident Types Tile.....	27
Critical Incidents Tile.....	27
Network History Tile.....	28
Incident Summary Tile.....	28
Interactive Network Hierarchy.....	29
Interactive Network Topology.....	29
Settings.....	30
Accounts.....	33
<b>Analytics</b> .....	<b>35</b>
Analytics Page.....	35
Network Filter Menu.....	36
Date and Time Filter.....	36
Network Node Details.....	36
Severity Filter.....	37
Incident Timeline.....	38
Incidents List Table.....	38
Incident Details Page.....	40
Network Impact Tile.....	41

Insights Tile.....	46
Incident Info Tile.....	47
Health Page.....	48
Unique Connected Clients Graph.....	49
Overview Tab.....	51
Connection Tab.....	52
Performance Tab.....	53
Infrastructure Tab.....	54
Configuration Change Page.....	55
Configuration Change Tile.....	56
Configuration Change Listing Tile.....	57
Health Tile.....	57
Client Troubleshooting Page.....	58
Occupancy Page.....	60
Utilization Tile.....	61
Total In-Site Visitors Tile.....	61
Avg. Dwell Time Tile.....	62
Sites Overview Chart.....	62
Sites Listing Table.....	62
Site Report.....	63
<b>Network Health.....</b>	<b>67</b>
Testing Client Services.....	67
Network Health Test Report.....	70
Overview Tab.....	70
Details Tab.....	72
<b>Testing Video Call Quality.....</b>	<b>75</b>
Video Call QoE Workflow.....	75
Creating a Test Call.....	76
Video Call Test Report.....	78
Participants Details Tile.....	78
Zoom Call Statistics Tile.....	78
<b>Report.....</b>	<b>81</b>
Using the Overview Dashboard: Content Panel.....	81
Wireless Network Report.....	83
Overview Tile.....	84
Traffic Distribution Tile.....	85
Top APs by Traffic Tile.....	86
Top APs by Client Count Tile.....	87
Traffic Trend Graphs.....	87
Traffic Over Time Table.....	88
Wired Network Report.....	89
Overview Tile.....	90
Traffic Distribution by Switch Model and Port Speed Chart.....	90
Top Switches by Traffic Tile.....	91
Top Switches by PoE Usage Tile.....	92
Top Switches by Errors Tile.....	93
Traffic Trend Graph.....	94
Error Trend Graph.....	94
Inventory - APs Report.....	94

Overview Tile.....	95
Top APs by Offline Duration Tile.....	96
AP Count Trend Graph.....	97
AP Status Trends Tile.....	97
Top AP Models.....	98
Top AP Software Versions Tile.....	99
Top 10 AP Reboot Reasons Tile.....	100
Top APs by Reboot Count Tile.....	100
Top 10 AP Alarm Types Tile.....	101
APs Configured in Multiple Systems Tile.....	102
AP Details for Online/Offline Status Table.....	102
AP Details for Other Statuses Table.....	103
Inventory - Controllers Report.....	103
Overview Tile.....	104
Resource Utilization Table .....	104
License Utilization Table.....	105
KRACK Assessment Table.....	105
Inventory - Switches Report.....	106
Overview Tile .....	107
Switch Count Trend Graph.....	107
Top Switch Software Versions Tile.....	108
Top Switch Models Tile .....	109
Port Status Trends Tile.....	110
WLAN Report .....	110
Overview Tile.....	111
SSID Changes Over Time Tile.....	112
Top SSIDs by Traffic Table.....	112
Top SSIDs by Client Count Tile.....	113
Active SSIDs Trend Graphs.....	114
Clients Report.....	115
Overview Tile.....	116
Top 10 Unique Clients by Traffic Chart.....	116
Clients Details.....	117
Unique Clients Trend Over Time Graphs.....	117
Top 10 OS by Client Count Tile.....	118
Top 10 Manufacturers by Client Count Tile .....	118
Top 10 Authentication Methods by Client Count Tile.....	119
Client Health Dashboard.....	119
Client Health Report.....	119
Applications Report.....	123
Overview Tile.....	123
Top Applications by Traffic.....	124
Top Applications by Client Count Tile.....	124
Airtime Utilization Report.....	125
Overview Tile.....	126
Top 10 APs by Airtime Utilization Chart.....	126
Top APs by Airtime Utilization for 2.4 GHz Table.....	127
Top APs by Airtime Utilization for 5 GHz Table.....	127
Airtime Utilization Trend Graph.....	128
Airtime Utilization Over Time Table.....	129

AP Details Report.....	129
Summary Tile.....	130
Performance Tile .....	130
Details Tile.....	131
Stats Tile .....	131
Uptime History Graph.....	132
Traffic Trend Graphs.....	132
Unique Clients Trend Over Time Graphs .....	133
Top 10 Clients by Traffic Volume Tile .....	134
Top 10 Applications by Traffic Volume Tile.....	134
Top SSIDs by Traffic Table.....	135
Sessions Table .....	135
RSS Trend Graph.....	135
SNR Trend Graph.....	136
Airtime Utilization Trend Graphs.....	136
Clients Details Table .....	137
Alarms Table.....	138
Events Table.....	138
Anomalies Graph.....	139
Client Details Report.....	139
Summary Tile.....	139
Stats Tile.....	140
Client Details Stats.....	140
Traffic Trend Tile.....	141
RSS Trend Tile.....	141
SNR Trend Tile.....	142
Sessions tile.....	142
Switch Details Report Dashboard.....	143
Switch Details Report.....	143
Comparison Reports Dashboard.....	147
Compare Filters .....	147
PCI Profiles.....	150
Creating a PCI Profile.....	152
Opening and Downloading a PCI Profile.....	154
Editing or Deleting a PCI Profile.....	155
<b>Data Explorer.....</b>	<b>157</b>
Data Explorer and Data Cubes.....	157
Data Exploration.....	157
Applications.....	158
AP Airtime and Hardware.....	159
AP Wired Device.....	159
AP Info and Statistics.....	160
Airtime Utilization.....	160
Client Info and Statistics.....	161
Client Sessions.....	161
Switch Inventory.....	162
AP Events.....	162
Impacted Clients.....	163
AP Inventory .....	163
AP Metrics.....	164

AP Connection Failures.....	164
Client Connection Counts.....	165
Client Connection Events .....	165
Client Time to Connect .....	166
AP Alarms.....	166
Controller Inventory.....	167
Controller Metrics.....	167
AP Rogues.....	168
Switch Network.....	168
AP Wi-Fi Calling.....	169
Data Cube Filters.....	170
Dimensions Filter.....	170
Measures Filter.....	177
Filter.....	181
Explore Filter.....	183
View Outputs Filter.....	185
Add to Dashboard Icon.....	185
Share Link Icon.....	186
Options Icon.....	186
Pinboard Pane.....	187
Comparisons.....	187
Creating a Data Comparison.....	188
Removing the Compare Feature.....	191
Creating a Data Explorer Dashboard.....	193
Actions You Can Perform on an Existing Dashboard.....	198
Opening a Dashboard.....	198
Editing a Dashboard.....	199
<b>Administration.....</b>	<b>203</b>
Viewing Onboarded Systems.....	203
Onboarding the controller to RUCKUS Analytics.....	203
Managing Users.....	204
Managing Resource Groups.....	205
Contacting Ruckus Support.....	208
Managing Licenses and Assigning APs.....	209
Viewing Schedules.....	212
Creating Webhooks.....	212
Integrating RUCKUS Analytics Incident Webhook with ServiceNow Application.....	214
Create a New Salesforce Case for RUCKUS Analytics Incident using Zapier Application.....	217
Updating an Existing Salesforce Case for RUCKUS Analytics Incident using Zapier Application.....	219





# Preface

- Document Conventions..... 9
- Command Syntax Conventions..... 9
- Document Feedback..... 10
- RUCKUS Product Documentation Resources..... 10
- Online Training Resources..... 10
- Contacting RUCKUS Customer Services and Support..... 11

## Document Conventions

The following table lists the text conventions that are used throughout this guide.

**TABLE 1** Text Conventions

Convention	Description	Example
monospace	Identifies command syntax examples	<code>device(config)# interface ethernet 1/1/6</code>
<b>bold</b>	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the <b>Start</b> menu, click <b>All Programs</b> .
<i>italics</i>	Publication titles	Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information.

## Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

### NOTE

A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

### ATTENTION

An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



### CAUTION

A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



### DANGER

A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

## Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
<b>bold text</b>	Identifies command names, keywords, and command options.

## Preface

### Document Feedback

Convention	Description
<i>italic text</i>	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional.  Default responses to system prompts are enclosed in square brackets.
{ x   y   z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x   y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member</i> [ <i>member</i> ...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

## Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at [#Ruckus-Docs@commscope.com](mailto:#Ruckus-Docs@commscope.com).

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

## RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at <https://support.ruckuswireless.com/documents>. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at <https://www.ruckuswireless.com>.

## Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at <https://training.ruckuswireless.com>.

# Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using <https://support.ruckuswireless.com>, or go to <https://www.ruckuswireless.com> and select **Support**.

## What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

## Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at <https://support.ruckuswireless.com/contact-us> and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

## Self-Service Resources

The RUCKUS Support Portal at <https://support.ruckuswireless.com> offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—[https://support.ruckuswireless.com/#products\\_grid](https://support.ruckuswireless.com/#products_grid)
- Security Bulletins—<https://support.ruckuswireless.com/security>

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at [https://support.ruckuswireless.com/case\\_management](https://support.ruckuswireless.com/case_management).



# RUCKUS Analytics Overview

---

- [RUCKUS Analytics Introduction.....](#) 13

## RUCKUS Analytics Introduction

RUCKUS Analytics is a cloud-native data analytics and machine-assisted software service designed to help network operators become more proactive in network management, operation, reporting, and troubleshooting. RUCKUS Analytics supports RUCKUS Cloud as well as SmartZone controllers and access points (APs). Access points and controllers serve as data sources, which measure and collect various key performance indicators (KPIs), connectivity status and flows, traffic, applications, and more. The data is packaged by the AP or controller as lightweight streaming telemetry and sent to the cloud through a secure transport. Once in the cloud, the data is ingested into a scalable and efficient data warehouse, analyzed using machine learning algorithms, and presented for your consumption in several different formats, for a variety of use cases.

RUCKUS Analytics provides several valuable resources for network administrators:

- **Dashboard:** Summarizes the network health and provides a quick focus on top problem areas.
- **Analytics:** Provides a detailed analysis on incidents, client impact, reasons, root causes, and recommendations.
- **Client Troubleshooting page:** Provides granular details about specific client experiences, connectivity issues, and quality.
- **Reports:** Leverages and displays pre-built reports and charts to understand network usage and inventory.
- **Data Explorer:** Explores all the data in your database with a customizable UI-driven tool to help answer questions about your network, usage, inventory, operating environment, and potential problems.
- **Service Validation:** Provides comprehensive end-to-end testing mechanism to validate LAN, WAN and connectivity to application servers.



# Logging In to RUCKUS Analytics

---

Before logging in to RUCKUS Analytics, ensure that you have configured the Northbound Data Streaming to enable data transfer from the controller, and configure the controller to enable historical connection failures and client events.

To access on-prem SmartZone RUCKUS Analytics and RUCKUS Analytics from RUCKUS Cloud, refer <https://support.ruckuswireless.com/articles/000011818>.

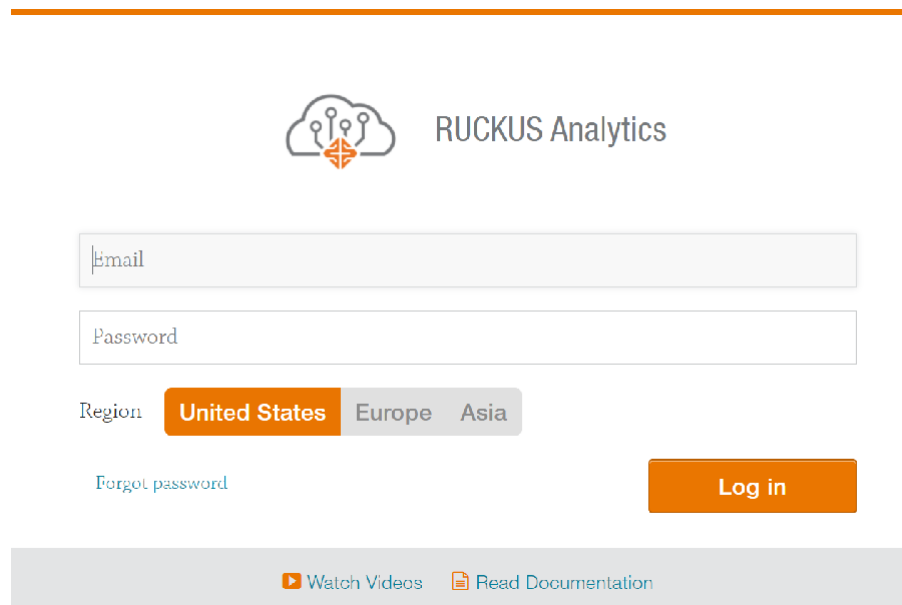
Complete the following steps to log in:

1. Open your web browser, and enter <https://ruckus.cloud/analytics> (for US users) in the address bar.
2. Enter your RUCKUS Analytics email address and password.
3. Click **Log In**.

The RUCKUS Analytics dashboard loads in your browser.

**FIGURE 1** RUCKUS Analytics Login Page

---



The image shows the RUCKUS Analytics login page. At the top center is the RUCKUS Analytics logo, which consists of a cloud icon with three stylized human figures inside, and the text "RUCKUS Analytics" to its right. Below the logo are two input fields: "Email" and "Password". Underneath the "Password" field is a "Region" selector with three buttons: "United States" (highlighted in orange), "Europe", and "Asia". To the left of the "Log in" button is a link for "Forgot password". The "Log in" button is a solid orange rectangle. At the bottom of the page, there is a grey bar containing two links: "Watch Videos" with a play icon and "Read Documentation" with a document icon.

Log in to RUCKUS Analytics at <https://ruckus.cloud/analytics> (US cloud hosting), <https://eu.ruckus.cloud/analytics> (EU cloud hosting) or <https://asia.ruckus.cloud/analytics> (Asia cloud hosting) with your Ruckus Support credentials.



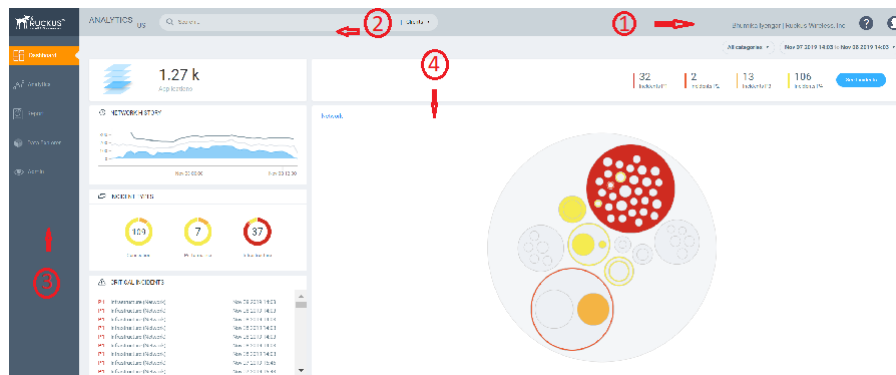


# Navigating the RUCKUS Analytics User Interface

- Header Panel..... 17
- Search Field ..... 18
- Using the Navigation Bar..... 19

The RUCKUS Analytics user interface (UI) consists of four major components: a header panel (top right), a search field (top left), a navigation bar (left), and a main content panel. The following figure shows the four main components of the RUCKUS Analytics UI. Refer to the following table for descriptions.

**FIGURE 2** RUCKUS Analytics Web Interface Components



**TABLE 2** Identifying RUCKUS Analytics Web Interface Components

No	Name
1	Header panel
2	Search field
3	Navigation bar
4	Main content panel

## Header Panel

Provides links for documentation help, support, and displays the currently logged-in user profile

When you click the user icon (👤), a menu displays two options:

- **My Account** : Launches the My Account page to enter user information.
- **Logout** : Logs you out of RUCKUS Analytics.







## Search Field

The search field allows for quick and easy exploration of devices and navigation to device- or asset-specific pages. You can search the system on three levels:

1. **Clients:** The client search displays a list of users or devices matching the search input. The following client and device fields are supported by search:
  - MAC Address
  - Hostname
  - Username
  - IP Address (IPv4 and IPv6)
  - Operating System (OS) Type
2. **Access Points:** AP search displays a list of access points matching the search input. The following AP fields are supported by search:
  - AP Name
  - MAC Address
  - IP Address (IPv4 and IPv6)
  - AP Model
3. **AP Hierarchy:** AP Hierarchy search displays a list of system hierarchies (Zone/Venue, AP group and so on) matching the search input. The following AP Hierarchy fields are supported by search:
  - Cluster Name
  - Domain Name
  - Zone Name
  - AP Group Name
  - AP Name

The results of each search displays a table, which has links that take you to a different portion of the RUCKUS Analytics system.

**TABLE 3** Search Types

Search Type	Link Icon	Link Destination
Client		The <b>Client Details Report</b> shows information about the total traffic received and transmitted, and the total number of clients over the selected time period.
		The <b>Client troubleshooting</b> page provides a holistic summary of the client connectivity, events, and health.
Access Points		The <b>AP Details Report</b> focuses on the usage and health details.
		The <b>AP Analytics</b> page shows incidents and health-related data for the AP.
Network Hierarchy		The <b>APs and Controllers</b> page provides a general overview of the APs on the network.
		The <b>Network Analytics</b> page shows incidents and health-related data for the network hierarchy.

## Using the Navigation Bar

The navigation bar highlights the main pages of the system:

- **Dashboard:** Summarizes network status and health, helping you focus on top problem areas. For more information, refer to [RUCKUS Analytics Dashboard](#) on page 23.
- **Analytics:** Allows exploration and drill-down on incidents, client impact areas, and network health requirements. For more information, refer to [Analytics Page](#) on page 35.
- **Report:** Provides pre-built reports and charts to understand network usage and inventory. For more information, refer to [Report](#) on page 81.
- **Data Explorer:** Explores the database with a customizable UI-driven tool to answer core questions. For more information, refer to [Data Explorer](#) on page 157.
- **Service Validation:** Provides ability to create comprehensive end-to-end tests to validate LAN, WAN and connectivity to application servers. For more information, refer to [Network Health](#) on page 67



# Feature Support Matrix

---

The following table lists the features supported in various SmartZone controllers and ICX switch models.

**TABLE 4** Feature-Software Compatibility Matrix

Feature	Supported SZ Release	Supported ICX FastIron Release
Switch Insights	5.2.1 and later	8.0.95 and later
Service Validation	5.2.1+KSP (MLISA_SERVICE_VALIDATION_5_2_1_811419.ksp) + AP patch (5.2.1.0.1038)	
CPU Insight	5.2.1 and later	
TTG Insight	5.2.1 and later	
All Released RUCKUS Analytics Features	5.1.2 and later	



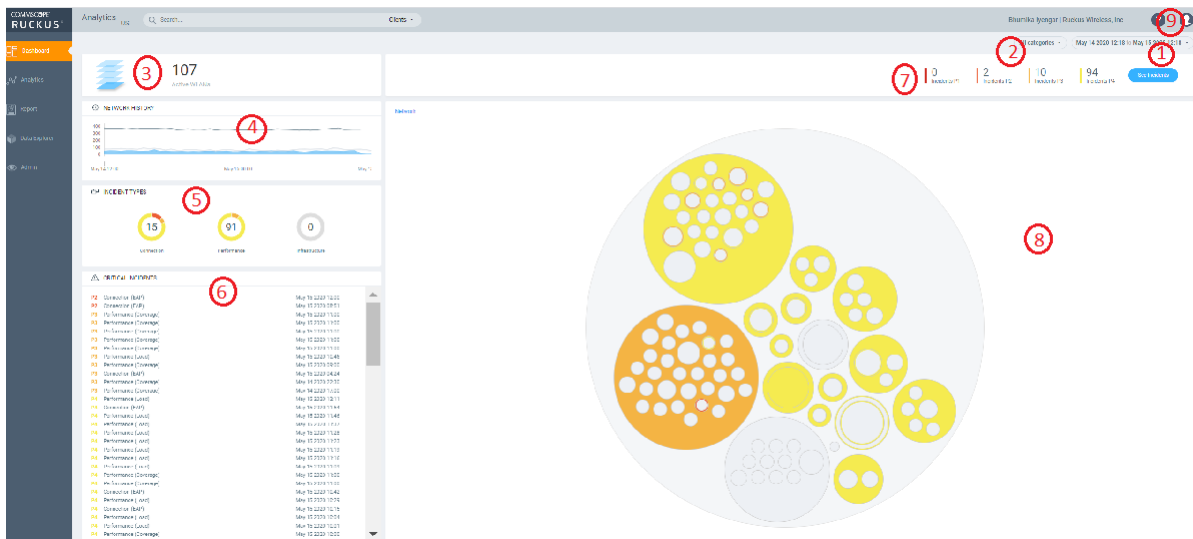
# RUCKUS Analytics Dashboard

- Dashboard Overview..... 23

## Dashboard Overview

The RUCKUS Analytics dashboard provides a summary of the network health and incident occurrences across the system. The dashboard is a starting point for network administrators seeking specific work-flows and issues that may require attention. Refer to [Navigating the RUCKUS Analytics User Interface](#) on page 17 more information.

FIGURE 3 RUCKUS Analytics Dashboard



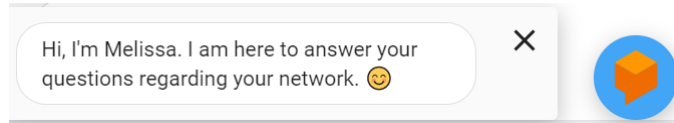
The dashboard comprises a number of components that provide a summary of network health:

TABLE 5 Dashboard Elements

Callout Number	Dashboard Elements
1	Time Selection field
2	Incident Selection
3	Scrolling Data tile
4	Incident Types tile
5	Critical Incidents tile
6	Network History tile
7	Incident Summary tile
8	Interactive Network Hierarchy
9	Settings

## Melissa AI Assistant

FIGURE 4 Melissa AI Assistant



The RUCKUS Analytics also offers a beta version of our virtual network assistant Melissa, which provides a conversational AI interface for you to interact with and understand more about your network. It provides intelligent and helpful answers to your questions. This feature is especially helpful for IT administrators as it reduces the effort to manually navigate through the user interface to analyze information about the network. Based on the questions asked, Melissa interprets user intent and provides responses, thereby providing a logical flow to the conversation and enhancing user experience; much like talking to an administrator for support. Additionally, all the intents and the training phases are enhanced so that it can understand, interact and provide better answers to questions. It also has the capability to now directly navigate to the required link in the page while you continue your conversation. The Melissa AI assistant is available throughout the application. Following are some questions (not limited to) that you can use to converse with Melissa.

- How's my network today?
- What are the top applications?
- How is client Rob doing?
- How many incidents are there in Zone Lobby yesterday?
- Is Zone Boardroom meeting expectations?
- Which WLAN is the busiest?
- Show me client office-laptop at 2pm.

Using key identification words like **client**, **zone**, **system**, etc. before the name will ensure a faster response from Melissa as names are often non-unique strings. Full names are not necessary as Melissa has the capabilities for partial search. You could also indicate the time periods by using terms like **today**, **yesterday**, **last week**, **3pm**, etc.

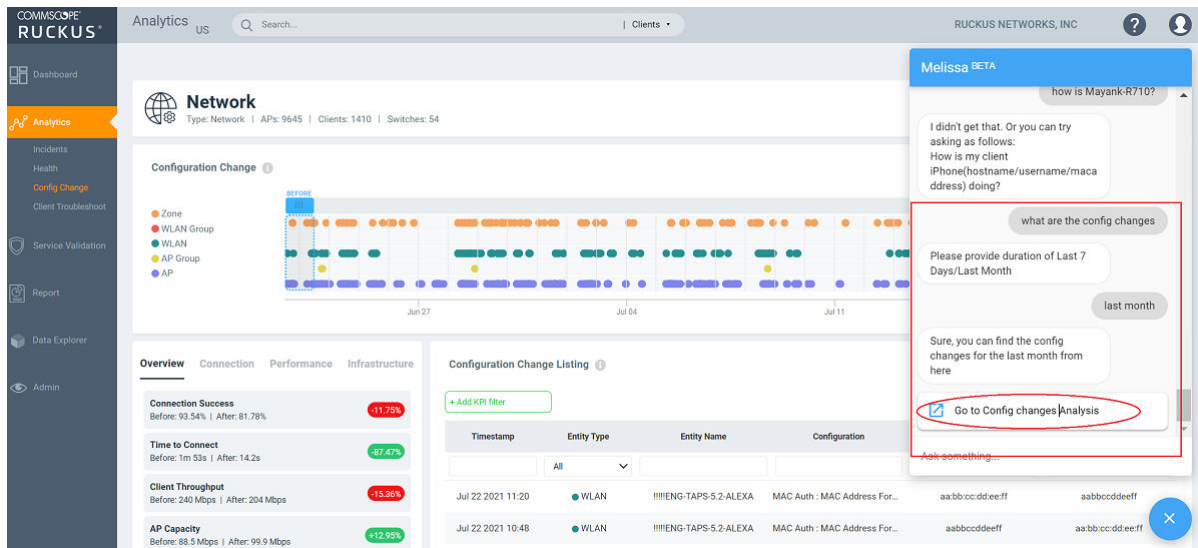
The current release of the product also has improved support for queries from Melissa AI. You can now:

- Check the status of devices (APs, clients, and switches) and troubleshoot issues
- Check the status of incidents and nodes
- Check network SLAs, traffic load on the network, and status of Zoom video call tests
- Create a support ticket through the chat box and also track it. You can review the status of the ticket by entering the ticket number in the chat box.
- Verify top applications, SSIDs, APs, zones and clients, configuration changes

Here is an example to find out the configuration changes that have occurred in the last month. The assistant also provides a link to the **Config Change** page for further analysis.

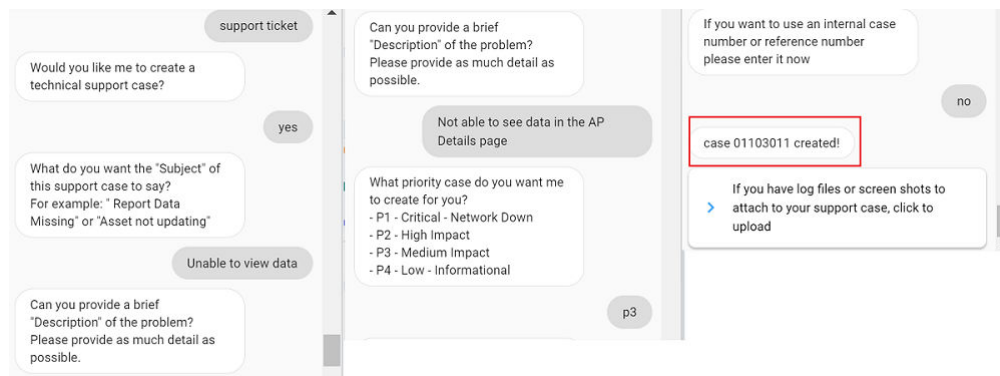


FIGURE 5 Example: Viewing Config Changes for the Last Month



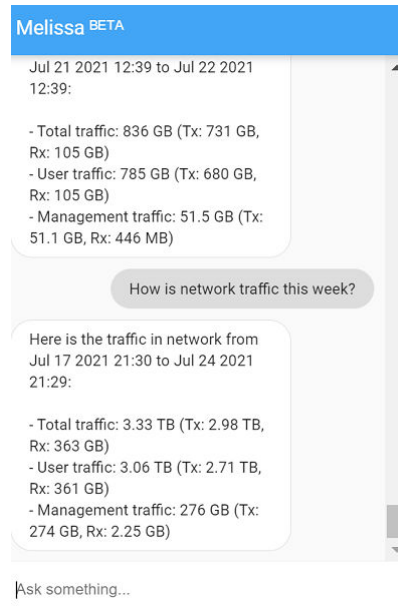
Here is an example to create a support case from the assistant:

FIGURE 6 Creating a Support Case Using the Assistant



Here is an example to find the traffic trend in the network for the past week:

FIGURE 7 Traffic Trend for the Specified Week



Melissa is still in beta phase and we are constantly training the algorithm to interpret more intents and increase the breadth of coverage.

## Time Selection Field

The **Time Selection** field is located in the upper-right corner of the dashboard. You can view elements within the dashboard based on predefined time periods, such as the last hour, the last 24 hours, and the last 7 days. The default view is the last 24 hours.

### NOTE

Time selection is a global option that affects all the measurements shown on the dashboard.

## Incident Selection

The dashboard data is displayed based on the type of incident category selected. You can choose to view incidents based on **Connections**, **Performance**, and **Infrastructure**. You can select one or more of these options at a time. Select the incident category and click **Apply** to view the relevant data reflected on the dashboard.

### NOTE

Category selection is a global option that affects all the measurements shown on the dashboard.

## Scrolling Data Tile

The scrolling data tile is located in the upper-left corner of the dashboard and provides a scrolling summary of key usage metrics.

**FIGURE 8** Scrolling Data Tile



The scrolling data tile maintains five layers of data, as shown in the following table. The scroll mechanism displays a different layer of data every two seconds. If you click one of the tiered layers, the data for that layer of data is displayed. If you click the displayed data result, the relevant data report in the **Reports** menu is displayed.

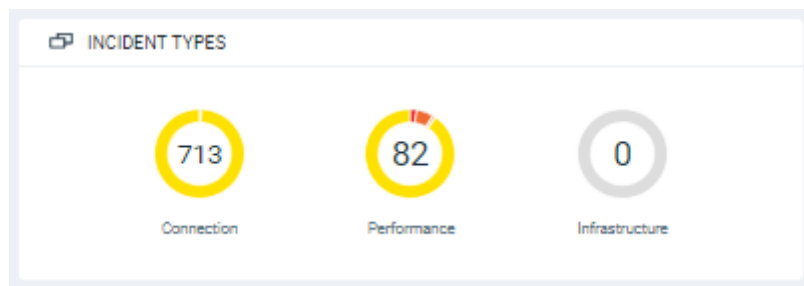
**TABLE 6** Layers of Scrolling Data Tile

Tile Data	Description	Link Destination
AP Count	Shows the number of unique APs supported by, and reporting data into, the system.	The <b>AP Inventory</b> report focuses on AP details and inventory.
Unique Clients	Shows the number of unique clients that have connected in the displayed time window.	The <b>Client</b> report focuses on client, device, and user details.
Traffic	Shows a sum of traffic sent and received by all APs in the displayed time window.	The <b>Network</b> report focuses on network and traffic usage.
Applications	Shows the total number of detected applications in the displayed time window.	The <b>Application</b> report focuses on application consumption.
Active WLANs	Shows the total number of WLANs that have been active on APs (client has connected) in the displayed time window.	The <b>WLANs</b> report focuses on WLAN traffic, client, and usage details.

## Incident Types Tile

The incident types tile shows the types of incidents, the number of incidents of each type, and the relative severity of the incidents. Incidents are categorized into three primary incident types: Connection, Performance, and Infrastructure. Each incident type contains many subtypes.

**FIGURE 9** Incident Types Tile

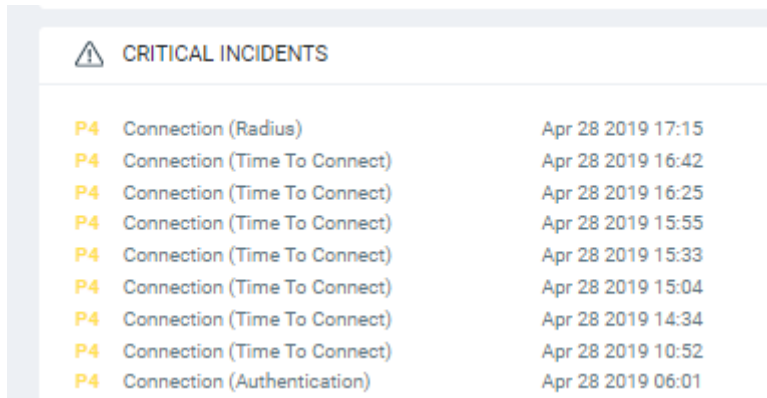


## Critical Incidents Tile

The critical incidents tile list the severity of the incident, the type of the incident, and the time the incident occurred.

If you click one of the incidents, the specific incident is displayed on the **Incident Details** page.

FIGURE 10 Critical Incidents Tile



## Network History Tile

The network history tile represents the number of clients serviced by the network (the gray lines in the chart), and the number of clients affected by incidents (the blue area in the chart).

The client count value in the chart includes all unique clients that attempted to connect to the network, including both failed and successful connections. The data depicts a large number of clients that may be impacted by incidents, even if a large number were not able to connect.

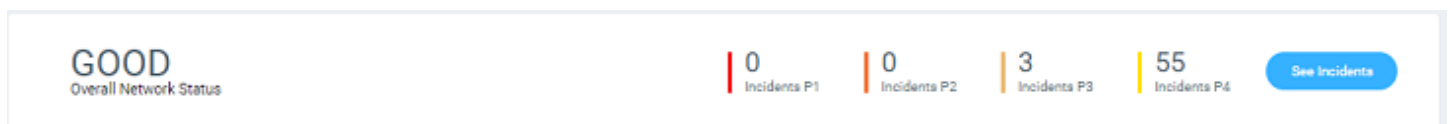
FIGURE 11 Network History Tile



## Incident Summary Tile

The incident summary tile offers a summation of the overall network status and compares the severity levels of each incident on the selected network. Each severity level is identified by priority and color. To explore the analytics details or view incidents of a specific layer of hierarchy, click **See Incidents**.

FIGURE 12 Incident Summary Tile



The following table lists the incident severity level, the priority, and the color assigned to the incident severity level.

**TABLE 7** Severity Levels of an Incident

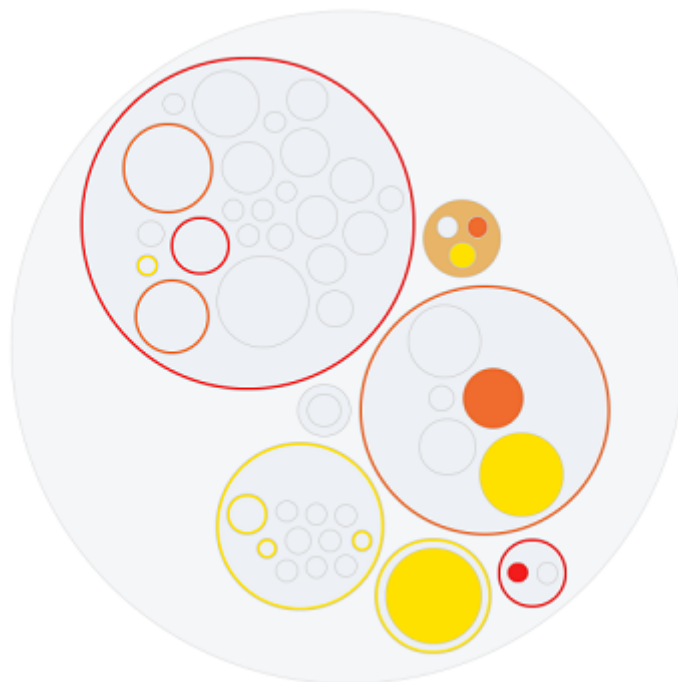
Incident	Priority	Color
P1	Critical	Red
P2	High	Dark Orange
P3	Medium	Orange
P4	Low	Yellow

## Interactive Network Hierarchy

The interactive network hierarchy is introduced by using *circle packing*. Circle packing is a hierarchical representation of the network that illustrates the controller clusters, domains, zones, AP groups, and individual APs visually. You can identify the areas of the network that are impacted by issues or showing problems.

The size of a circle depends on the number of APs. You can navigate within each circle, exploring layers within the hierarchy by clicking the circles themselves. The boundary of a circle indicates that there are incidents occurring within it. To view the analytics details or the incidents of a specific hierarchical layer, click **See Incidents** in the incident summary tile.

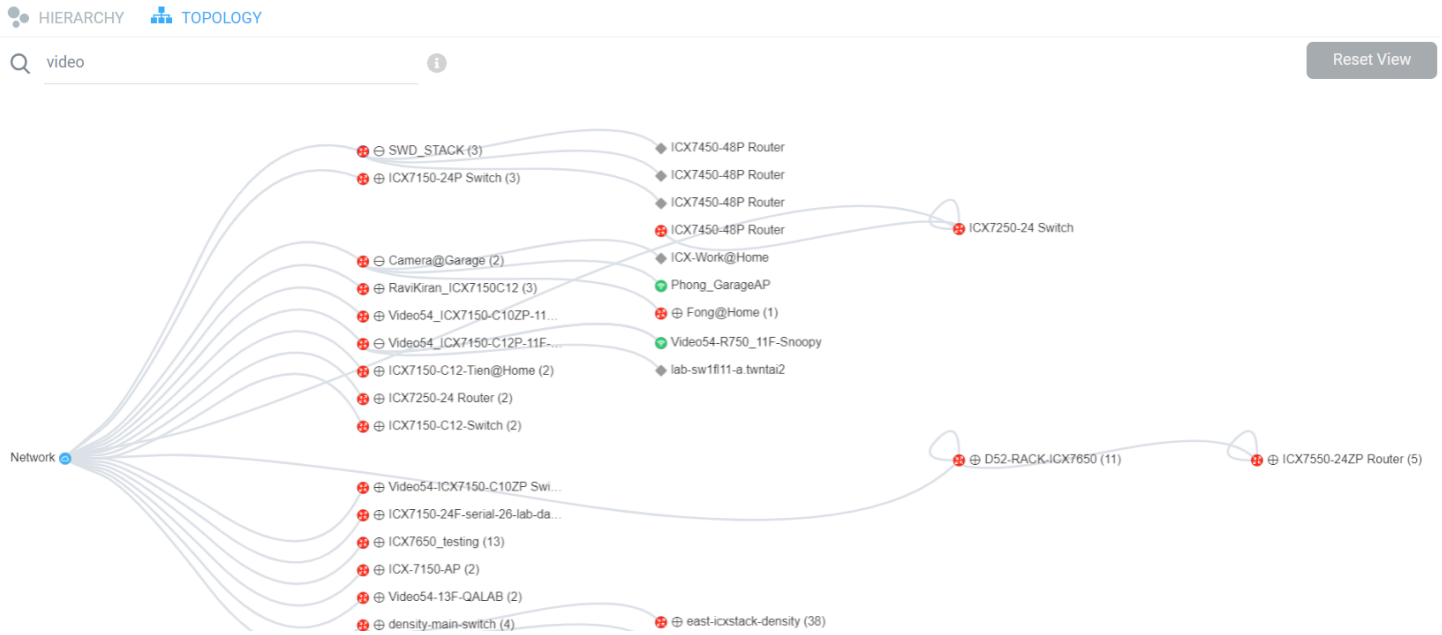
**FIGURE 13** Circle Packing Example



## Interactive Network Topology

The network topology page is interactive and displays the arrangement of various types of elements within the network such as switches, routers, port connections and so on.

FIGURE 14 Interactive Network Topology



You can also use the search bar to look for devices (AP or switch) within the network topology diagram either with their name or MAC address. By clicking on the switch group icon (+), you can expand and view the devices within the group such as routers, APs (●). The switch group can have a stack of switches as well. If the network contains devices other than ICX switches and RUCKUS APs, the device is displayed against this icon - ◆. Pause the pointer over the icons for more information about the devices and over the lines for more information about the port connections. For example, the port connections are displayed as **Connection Port: 1/1/35 <-> eth1** which implies that the ports **1/1/35** of the switch are connected to the **eth1** port of the AP. In the switch ports representation, the first number represents the first switch in the group or stack, the next number represents the switch module, and the last number the switch port. Clicking **Reset View** collapses all the device views and resets the network topology connection diagram.

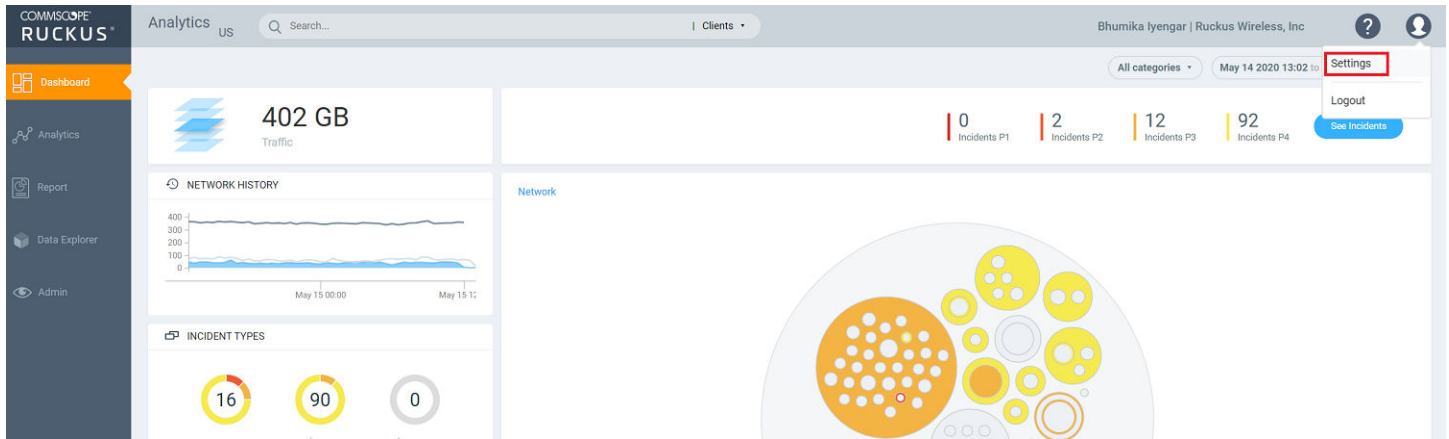
You can zoom-in or zoom-out the **Topology** page and also click on the page to move it.

You can also use the **Auto Update** feature to update the dashboard data, every 3 minutes.

## Settings

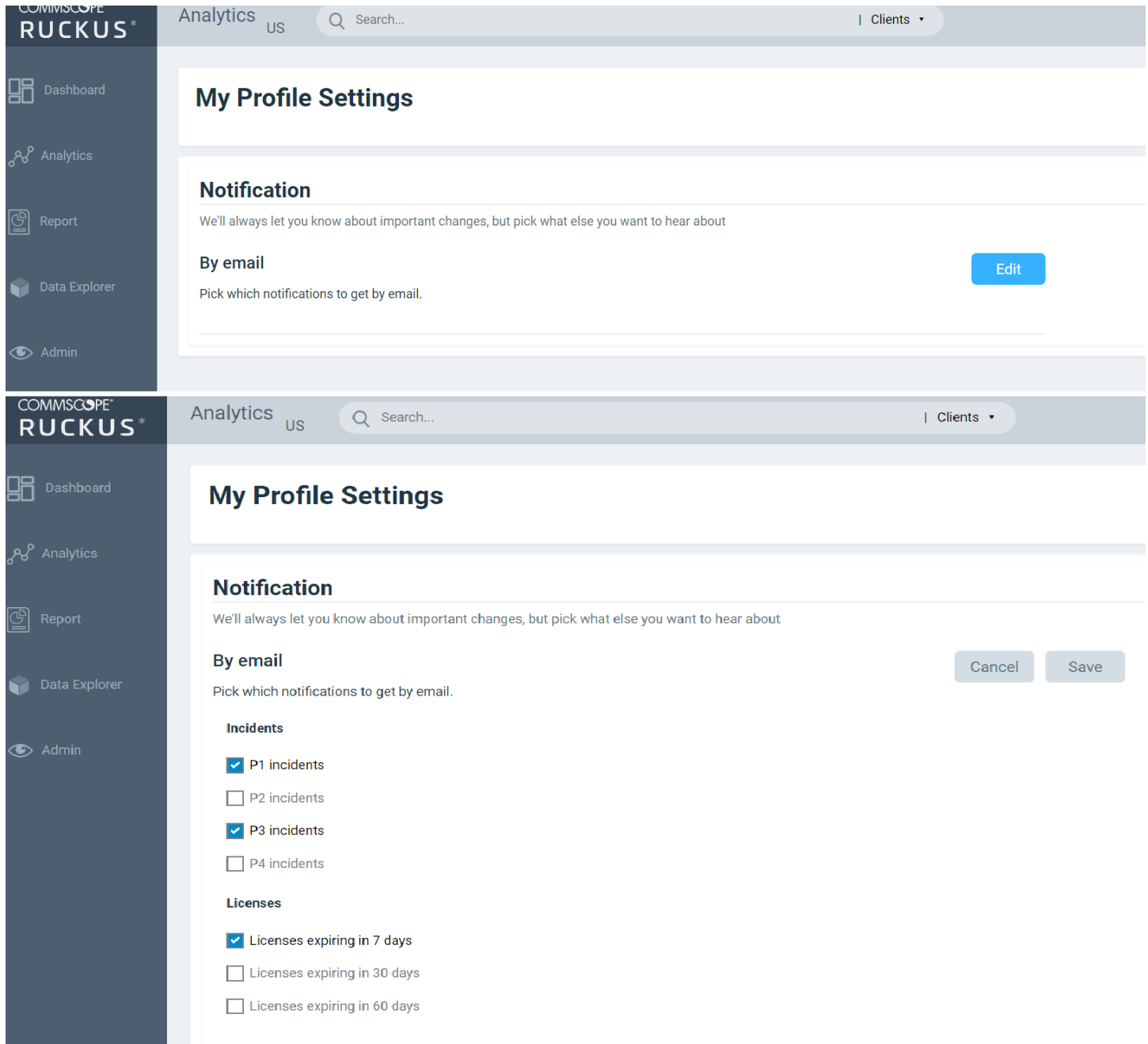
You can modify the user profile from the **My Profile Settings** page and enable the option to receive notification email alerts for incidents of varying severity ranging from P1 to P4.

FIGURE 15 Accessing Settings



Click **Edit** and select the check boxes to indicate the incident severity range or license expiration time for which you want to receive email notifications.

FIGURE 16 Enabling Email Notifications



An email notification typically contains a short description about the incident and also provides a summary with the following details:

- Client Impact: Displays the estimated percentage of clients impacted due to the incident.
- Category: Displays the type of issue impacting the client. For example, if the time to connect to the network is high, the Category would be displayed as "Connection". Other options include "Infrastructure" and "Performance".
- Sub Category: Displays the subcategory of the incident. For example, if the time to connect to the network is high, the Subcategories would vary based on the three categories (Connection, Infrastructure, and Performance). For more information, refer to the "Incidents List Table" and "Incidents Details Page" in [Analytics Page](#) on page 35.



- Network Path: Displays the location of the client within the network.
- Event Start Time: Displays the timestamp of the event when it occurred.

A link to view the incident details is also available in the email notification.

FIGURE 17 Sample Email Notification

Hi there,  
Ruckus Analytics has detected the following **P1 incident** in your network.  
**Description:** The controller cluster is sending data with an incorrect past timestamp. To avoid false or misleading data analysis, past timestamped data is not analyzed for incidents.  
**Summary:**

- Client Impact (Approximately): -
- Category: Infrastructure
- Sub Category: Network
- Network Path: Alphanet-BDC (system)
- Event Start Time: Mar 11, 2020, 6:22:30 AM

Please click this [link](#) to view the incident.  
Thanks  
The Ruckus Analytics Team

## Accounts

The Accounts page displays the total number of third-party user accounts, role associated with the user account, name of the inviter and the status of the invitation. Users can **Accept** or **Reject** the invitation. If an invitation is rejected, it is immediately removed from the account. Invitations that are accepted are included to the account.

FIGURE 18 Accounts Page

Account Name	Role	Inviter	
Dog Company 1008	Admin	First Name 1008 LastNam...	<input type="button" value="Reject"/> <input type="button" value="Accept"/>
Aricent_10000	Admin	-	<input type="radio"/>
Erugg Dev 3	Admin	-	<input type="radio"/>
ruckus internal	Admin	-	<input type="radio"/>
Ruckus Wireless, Inc	Admin	-	<input checked="" type="radio"/>

### NOTE

Registered users can have multiple accounts and can toggle between these accounts to operate. The user interface changes based on the account selection.

Users with one account will be directed to the Dashboard view of the RUCKUS Analytics user interface, by default. Those with multiple accounts will be directed to the **Accounts** page soon after logging into the RUCKUS Analytics user interface so they can choose the account to operate from.



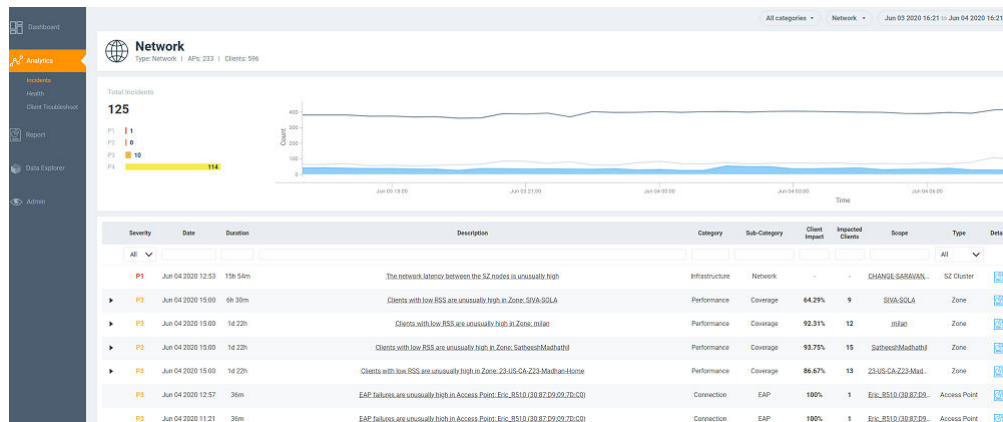
# Analytics

- Analytics Page..... 35
- Health Page..... 48
- Configuration Change Page..... 55
- Client Troubleshooting Page..... 58
- Occupancy Page..... 60

## Analytics Page

The **Analytics** page provides a breakdown of incidents by severity and category, allowing you to focus on incidents of interest, for which they can view details. For any given incident, you can view the severity, client impact, root cause, and recommendations, as well as the events, anomalies, data, or problems that were used to identify the incident.

**FIGURE 19** Analytics Page



The analytics page consists of different sections which are described as follows:

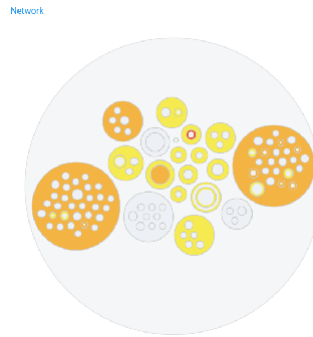
The Analytics page contains a number of components:

- Network Filter menu
- Date and Time filter
- Network Node Details tile
- Severity Filter tile
- Incident Timeline
- Incident List table
- Incident Details
- Network Impact tile
- Insights
- Incident Info tile

## Network Filter Menu

Click the **Network** menu to select a network node within the circle packing representation. By default, **Network** is selected, which displays a circle packing view of all the systems in the network. A network node can be a cluster, domain, zone, AP group, or access point in the network. After selecting a node, click **X** to close the circle packing representation.

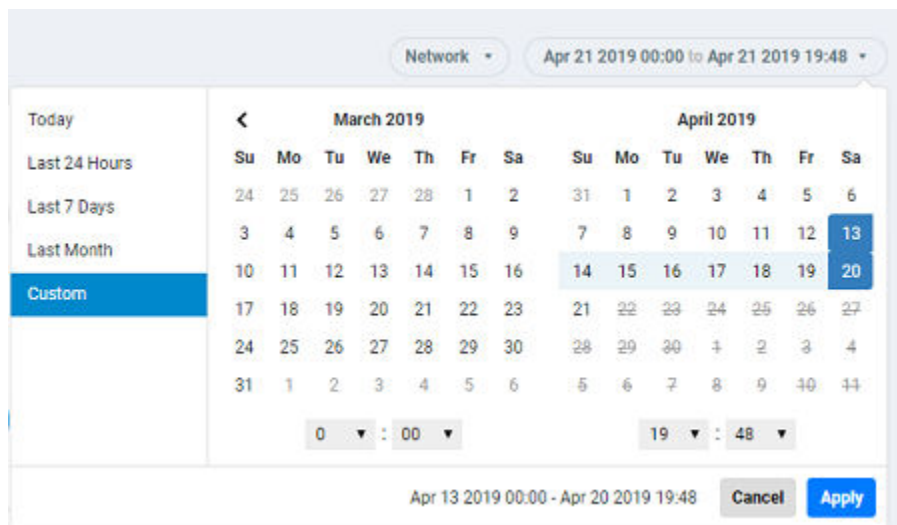
FIGURE 20 Nodes on the Network



## Date and Time Filter

The date and time filter is used to plot the date and time for a specific time period, including such as **Today**, **Last 24 hours**, **Last 7 days**, or **Last Month**. Use the Custom option to select the dates and times for a specific customized time period.

FIGURE 21 Custom Mode



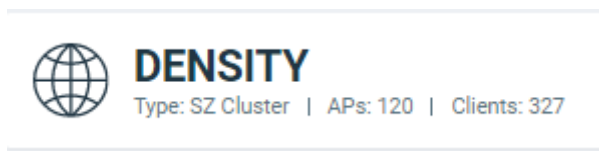
Click **Apply** to save the specified date and time filters and update the Analytics page.

## Network Node Details

The Network Node Details tile displays the name of the selected node from the **Network** Filter menu as a header.

For example, the following figure shows the Density network node and its attributes (Type, APs, and Clients).

FIGURE 22 Density Network Node



The following table lists the various network nodes and their attributes.

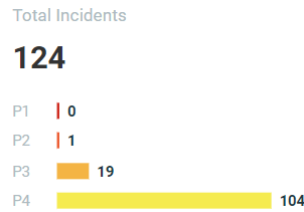
TABLE 8 Network Nodes and Attributes

Node	Attributes
Cluster	<ul style="list-style-type: none"> <li>Type: SZ Cluster</li> <li>Firmware</li> <li>Cluster: Cluster Name</li> <li>SZ Type: SZ104, SZ124, viz.-E, viz.-H, SZ300</li> </ul>
Domain	<ul style="list-style-type: none"> <li>Type: Domain</li> <li>Zone Count</li> <li>AP Count</li> <li>Client Count</li> <li>Cluster</li> </ul>
Zone	<ul style="list-style-type: none"> <li>Type: Zone</li> <li>Firmware: Zone firmware</li> <li>AP Count</li> <li>Client Count</li> <li>Cluster</li> </ul>
AP Group	<ul style="list-style-type: none"> <li>Type: AP Group</li> <li>Zone Firmware</li> <li>AP Count</li> <li>Client Count</li> </ul>
AP	<ul style="list-style-type: none"> <li>Type Access point</li> <li>AP Firmware</li> <li>AP Name</li> <li>Model</li> <li>MAC Address</li> <li>IP Address</li> <li>Client</li> </ul>
Client	<ul style="list-style-type: none"> <li>Type: Client</li> <li>MAC Address</li> <li>Last IP Address</li> <li>OS Type</li> <li>Hostname</li> <li>Username</li> </ul>

## Severity Filter

The severity filter tallies the total number of incidents on the network node, and lists the number of incidents by severity.

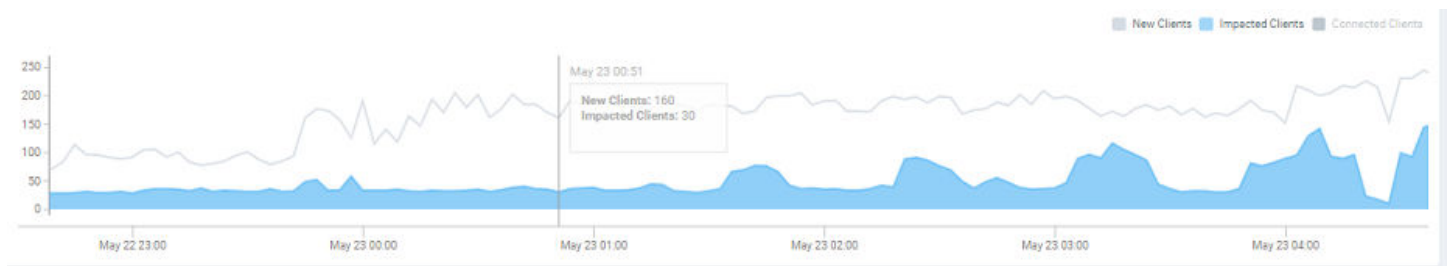
FIGURE 23 Severity Filter



## Incident Timeline

The Incident Timberline is a graphical representation of the number of new clients connecting to the network (the light gray line), the number of clients actively connected to the network (the dark gray line) and the number of clients affected by the network incidents (the blue area in the chart).

FIGURE 24 Incident Timberline



Pausing the pointer at any instance on the timeline displays an information box that shows the number of new clients, impacted clients, and connected clients. You can modify the information displayed in the information box by selecting the **New Clients**, **Impacted Clients**, and **Connected Clients** check boxes.

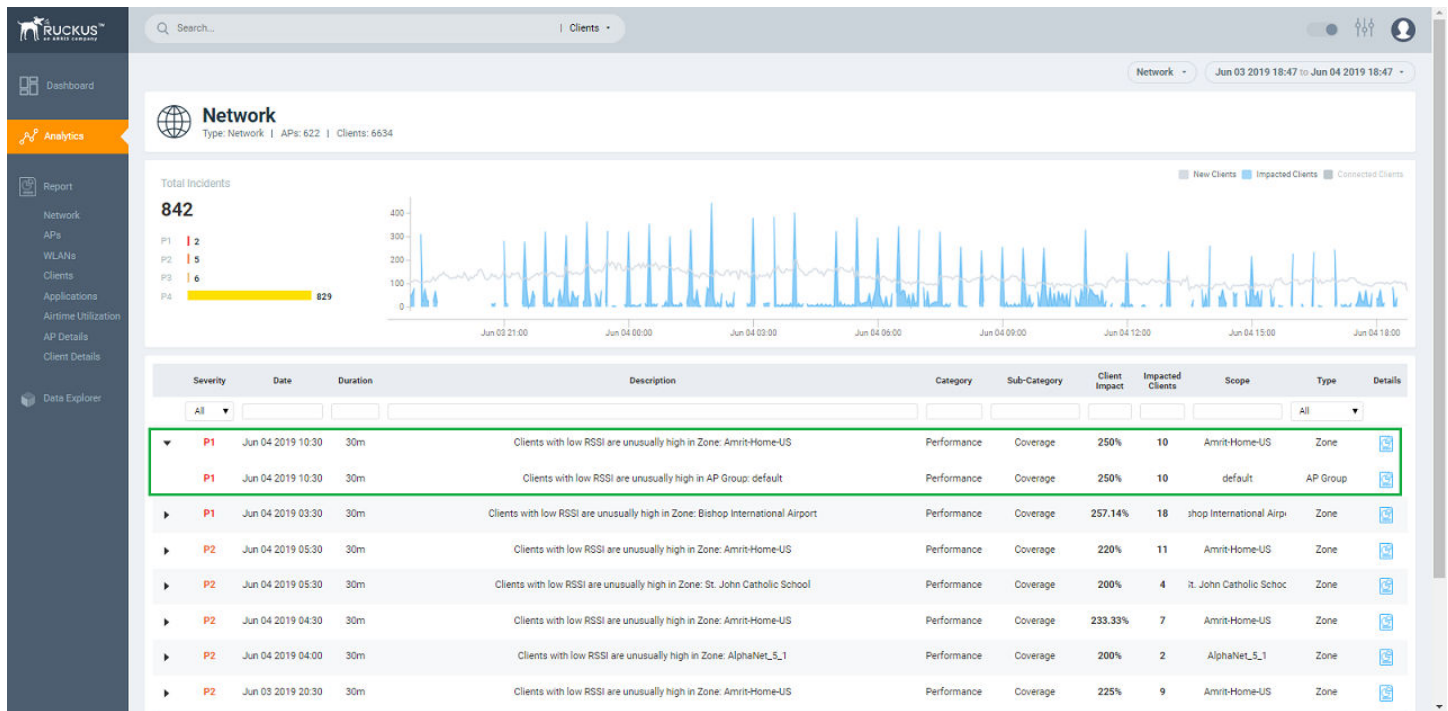
### NOTE

On computers running Windows, press **Ctrl** and rotate the wheel button to zoom in and zoom out of the Incident Timeline.

## Incidents List Table

The Incidents List table offers a summary of each incident.

FIGURE 25 Incidents List Table



Each incident is made up of a number of attributes. Under each attribute is a search field to limit the incident list based on the search criteria. Click the right arrow button to view more information about other incidents that contribute to the selected incident and information about the parent incident to which the selected incident contributes.

TABLE 9 Attributes of the Incidents List Table

Attribute	Description
Severity	The severity of an incident ranges from P1 to P4; P1 being the highest priority and P4 the lowest. The severity of an incident is determined by the client impact, duration, and other factors. You can see the severity score when you hover the mouse over the number. The severity score of the incident takes into account the scope of the incident, duration of the incident, and the severity of the incident; giving equal consideration to all the mentioned parameters to arrive at the severity score.
Date	The date and time when the incident started.
Duration	The measure of how long the incident lasted.
Description	A short description of the incident. Pausing the pointer over the description displays more information about the incident.
Category	The type of incident, for example: Connection, Performance, and Infrastructure.

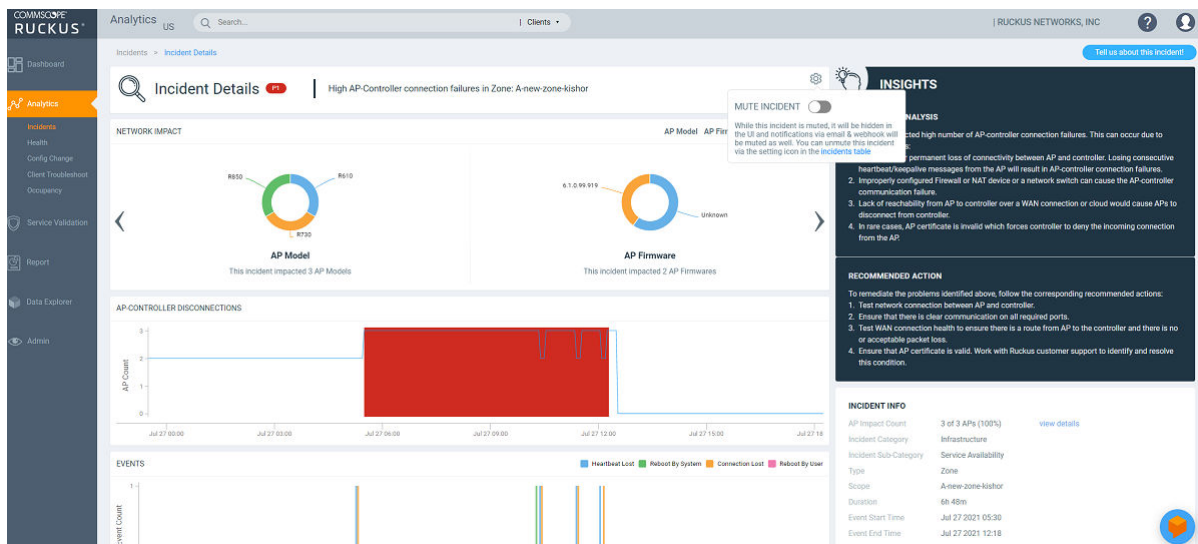
**TABLE 9** Attributes of the Incidents List Table (continued)

Attribute	Description
Sub-Category	<p>Connection incidents consist of the following categories:</p> <ul style="list-style-type: none"> <li>• Association</li> <li>• User Authentication</li> <li>• DHCP</li> <li>• EAP</li> <li>• RADIUS</li> <li>• Time to Connect</li> </ul> <p>Performance incidents consist of the following categories:</p> <ul style="list-style-type: none"> <li>• RSSI</li> <li>• Memory</li> <li>• Coverage</li> </ul> <p>Infrastructure incidents consist of the following categories:</p> <ul style="list-style-type: none"> <li>• VLAN Mismatch</li> <li>• Service Availability</li> </ul>
Client Impact	The percentage of clients impacted by the incident.
Impacted Clients	The number of clients impacted by the incident.
Type	The type of incident that occurred. You can view this by selecting the options from the drop-down menu. Options include SZ Cluster, Domain, Zone, AP Group and Access Point.
Scope	The area of the network in which the incident was detected. Pausing the pointer over the scope displays the entire path of the network node.
Details	Clicking the Details icon displays the <b>Incident details</b> page to find more details about the incident such as impacted areas, root cause, and recommendations.

## Incident Details Page

The header of the **Incident details** page displays the severity level of a selected incident and the description of the incident.

**FIGURE 26** Incident Details Page



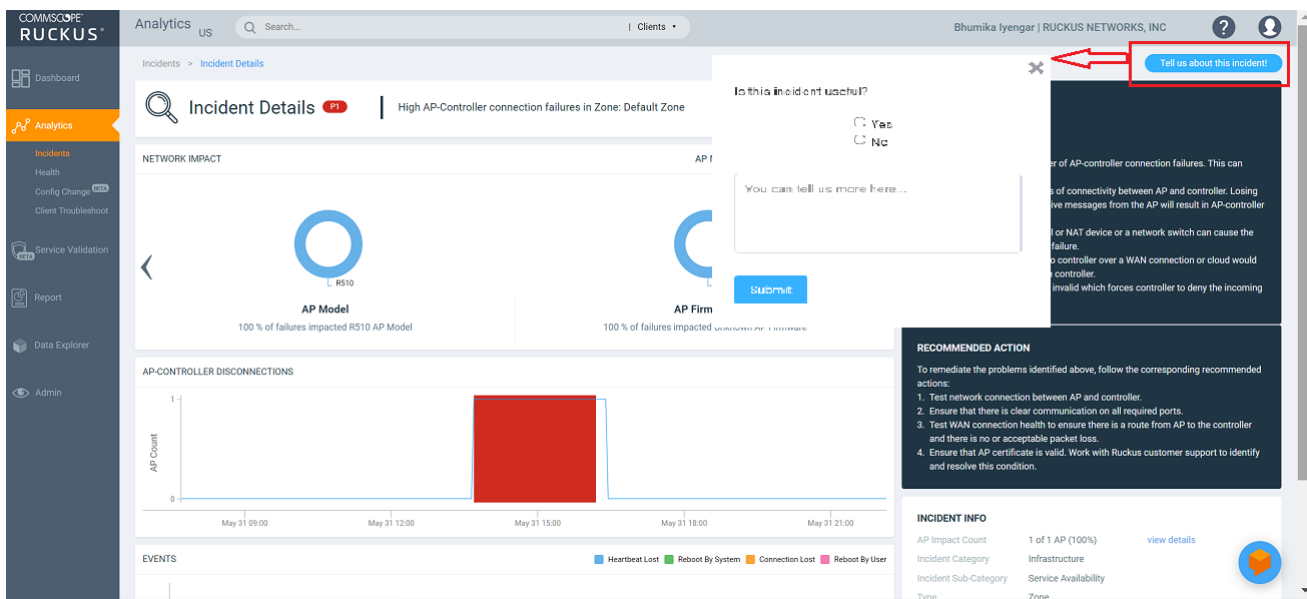


You can also fix the thresholds for health parameters using the **Set Threshold** option to validate the health of your network. Clicking **Set Threshold** takes you to the **Health** page where you can set the threshold for a parameter. For instance, if you set the threshold for the Time to Connect (TTC) parameter as 2 seconds, the TTC graph displays the number of connections that are able to connect to the network within 2 seconds. It also displays the average time to connect to the network in general, and the total connections attempting to connect to the network. Every time a new threshold is set, the graph trends simultaneously change as the computing changes. Similarly, thresholds can be set for various parameters to evaluate network health such as ROSSI, AP Capacity, AP Service Uptime, AP-to-SZ Service Latency, and Cluster Latency. The threshold will apply to the incident related to the metric.

The **Tell us about this incident!** option allows users to provide feedback about how useful the incident information is based on their production environment. In general, an incident is assigned a severity based on various factors but as a user you can also provide feedback as to what severity best fits the incident.

You can mute or unmute an incident via the setting icon in the Incident table or from the Incident page. When an incident is muted, it is hidden in the user interface and notifications via email and webhook are also muted.

FIGURE 27 Incident Feedback Option



## Network Impact Tile

The Network Impact tile consists of various donut charts that represent the areas of the network that were impacted by the incident. Each incident type and subtype has a different set of network impact donut charts, but it is common to see WLANs, Client OS Types, AP Models, Radio Bands, and Reason Codes, which all help to explain some of the common questions: who is impacted, which devices are contributing, what are the reason codes, and more. Every donut chart is divided into donut charts of different colors. If you pause the pointer over any portion of the donut chart, an information box displays the impacted area of the incident and the clients affected by this the incident. Beneath each donut chart is a summary line. Two donut charts are shown by default. You can click the right arrow and left arrow to navigate to other donut charts, or click Radio, WLAN, Client Manufacturers, or Reason to access a specific donut chart.

FIGURE 28 Network Impact Tile

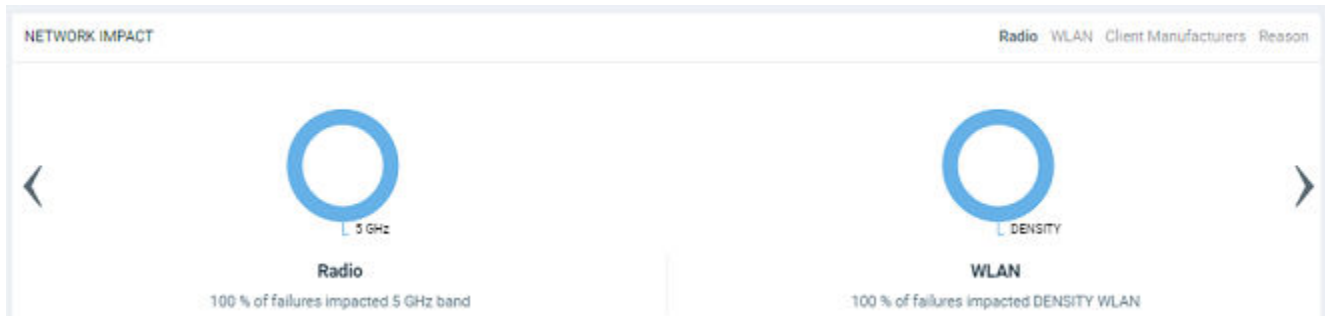


TABLE 10 Attributes of Network Impact Table

Incident Type	Donut Charts	Chart Elements
User Authentication	<ul style="list-style-type: none"> <li>Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios.</li> <li>WLAN: The different WLANs to which the impacted clients are connected.</li> <li>Client Manufacturers: The distribution of device manufacturers.</li> <li>Reason: The breakdown of various failure reasons experienced by the impacted clients.</li> </ul>	<ul style="list-style-type: none"> <li>Authentication Failure Ratio: A time series chart that shows the failure ratio over time. The chart includes data for 6 hours before and 6 hours after (if available) the incident.</li> <li>Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients.</li> <li>Failure counts: A time series chart with three types of raw failure counts: Authentication Failures, Authentication Attempts, and Total Failures, which includes the total of all types of connection failures (authentication, association, EAP, DHCP, and so on) that were observed during this period.</li> </ul>
EAP	<ul style="list-style-type: none"> <li>Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios.</li> <li>WLAN: The different WLANs to which the impacted clients are connected.</li> <li>Client Manufacturers: The distribution of device manufacturers.</li> <li>Reason: The breakdown of various failure reasons experienced by the impacted clients.</li> </ul>	<ul style="list-style-type: none"> <li>EAP Failure Ratio: A time series chart that shows the failure ratio over time. The chart includes data for 6 hours before and 6 hours after (if available) the incident.</li> <li>Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients.</li> <li>Failure counts: A time series chart with three types of raw failure counts: EAP Failures, EAP Attempts, and Total Failures, which includes the total of all types of connection failures (authentication, association, EAP, DHCP, and so on) that were observed during this period.</li> </ul>

**TABLE 10** Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
Association	<ul style="list-style-type: none"> <li>● Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios.</li> <li>● WLAN: The different WLANs to which the impacted clients are connected.</li> <li>● Client Manufactures: The distribution of device manufacturers.</li> <li>● Reason: The breakdown of various failure reasons experienced by the impacted clients.</li> </ul>	<ul style="list-style-type: none"> <li>● Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident.</li> <li>● Association Failure Ratio: A time series chart that shows the failure ratio over time. The chart includes data for 6 hours before and 6 hours after (if available) the incident.</li> <li>● Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients.</li> <li>● Failure counts: A time series chart with three types of raw failure counts: Association Failures, Association Attempts, and Total Failures, which includes the total of all types of connection failures (authentication, association, EAP, DHCP, and so on) that were observed during this period.</li> </ul>
DHCP	<ul style="list-style-type: none"> <li>● Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios.</li> <li>● WLAN: The different WLANs to which the impacted clients are connected.</li> <li>● Clients Manufactures: The distribution of device manufacturers.</li> <li>● Reason: The breakdown of various failure reasons experienced by the impacted clients.</li> </ul>	<ul style="list-style-type: none"> <li>● Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident.</li> <li>● DHCP Failure Ratio: A time series chart that shows the failure ratio over time. The chart includes data for 6 hours before and 6 hours after (if available) the incident.</li> <li>● Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients.</li> <li>● Failure counts: A time series chart with three types of raw failure counts: DHCP Failures, DHCP Attempts, and Total Failures, which includes the total of all types of connection failures (authentication, association, EAP, DHCP, and so on) that were observed during this period.</li> </ul>

**TABLE 10** Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
RADIUS	<ul style="list-style-type: none"> <li>Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios.</li> <li>WLAN: The different WLANs to which the impacted clients are connected.</li> <li>Client Manufactures: The distribution of device manufacturers.</li> <li>Reason: The breakdown of various failure reasons experienced by the impacted clients.</li> </ul>	<ul style="list-style-type: none"> <li>Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident.</li> <li>Radius Failure Ratio: A time series chart that shows the failure ratio over time. The chart includes data for 6 hours before and 6 hours after (if available) the incident.</li> <li>Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients.</li> <li>Failure counts: A time series chart with three types of raw failure counts: RADIUS Failures, RADIUS Attempts, and Total Failures, which includes the total of all types of connection failures (authentication, association, EAP, DHCP, and so on.) that were observed during this period.</li> </ul>
Time to Connect	<ul style="list-style-type: none"> <li>Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios.</li> <li>WLAN: The different WLANs to which the impacted clients are connected.</li> <li>Client Manufactures: The distribution of device manufacturers.</li> <li>Reason: The breakdown of various failure reasons experienced by the impacted clients.</li> </ul>	<ul style="list-style-type: none"> <li>Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident.</li> <li>Time to Connect Failure Ratio: A time series chart that shows the failure ratio over time. The chart includes data for 6 hours before and 6 hours after (if available) the incident.</li> <li>Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients.</li> <li>Time to Connect (By stage): A time series chart that displays the time to connect based on various stages of the connection such as authentication, association, EAP, Radius, and DHCP. Pause the pointer over the graph for more information.</li> </ul>
RSSI	<ul style="list-style-type: none"> <li>Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios</li> <li>WLAN: The different WLANs to which the impacted clients are connected.</li> <li>Client Manufactures: The distribution of device manufacturers.</li> <li>Reason: The breakdown of various failure reasons experienced by the impacted clients.</li> </ul>	<ul style="list-style-type: none"> <li>Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident.</li> <li>RSSI Quality by Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients.</li> <li>RSSI Distribution: The RSSI distribution over a period of time.</li> </ul>

**TABLE 10** Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
Network Latency		<ul style="list-style-type: none"> <li>● Ping Latency: Average time, in milliseconds, for the controller nodes to transmit and receive the packets. Maximum, average, and minimum latency trends are plotted on the graph.</li> <li>● Controller-1: CPU, memory and input-output usage of the controller node over time is displayed.</li> <li>● Controller-2: CPU, memory and input-output usage of the other controller node over time is displayed.</li> </ul>
Reboot	<ul style="list-style-type: none"> <li>● AP Model: distribution of impacted AP models.</li> <li>● AP Firmware: distribution of impacted AP versions.</li> <li>● Reason by AP: distribution of reasons for failure that caused the AP reboot.</li> <li>● Reason by Event: distribution of reasons for failure that caused the AP reboot and triggered related events.</li> </ul>	<ul style="list-style-type: none"> <li>● Reboot by System: a time series chart that displays the number reboot events.</li> <li>● Connected Clients: a time series chart that displays the number of clients connected at that point in time.</li> <li>● Rebooted APs: a time series chart that displays the number of APs that were rebooted at a point in time.</li> </ul>
SmartZone CPU overload insight	<ul style="list-style-type: none"> <li>● SZ Applications: distribution of CPU usage by individual SmartZone applications.</li> <li>● SZ Applications Group: distribution of CPU usage by individual SmartZone application groups.</li> </ul>	<ul style="list-style-type: none"> <li>● Normalized CPU Usage: a time series chart that displays the CPU usage in percentage.</li> <li>● Memory and I/O Usage: a time series chart that displays the memory and I/O usage in percentage. You can select the check-box to displays only one or both of the usage metrics.</li> <li>● CPU Usage by Application Groups: a time series chart that displays the CPU usage in percentage, for the various SmartZone application groups. You can select the check-box to displays only one or more of the usage metrics.</li> </ul>
High AP-controller connection failures	<ul style="list-style-type: none"> <li>● AP Model: displays the percentage of failure that impacted various AP models</li> <li>● AP Firmware: displays the number of failures that impacted various AP firmware versions</li> <li>● Event Type: displays the percentage of failures that were caused by various events</li> <li>● Reason: lists the reasons that caused the incident</li> </ul>	<ul style="list-style-type: none"> <li>● AP-Controller Disconnections: a time series chart that displays the number of disconnections between the AP and controller over time.</li> <li>● Event Count: a time series chart that displays the total event count for the following events: Heartbeat Lost, Connection Lost, Reboot By System, and Reboot By User. When an event is generated for the above mentioned conditions, it is plotted in this graph. You can select the check-box to displays only one or more of the events.</li> </ul>
Channel Distribution		<ul style="list-style-type: none"> <li>● AP Distribution by Channel: heatmap that displays the AP count over time, across channels.</li> <li>● Rogue Distribution by Channel: a time series chart that displays the number of rogue APs across channels.</li> </ul>

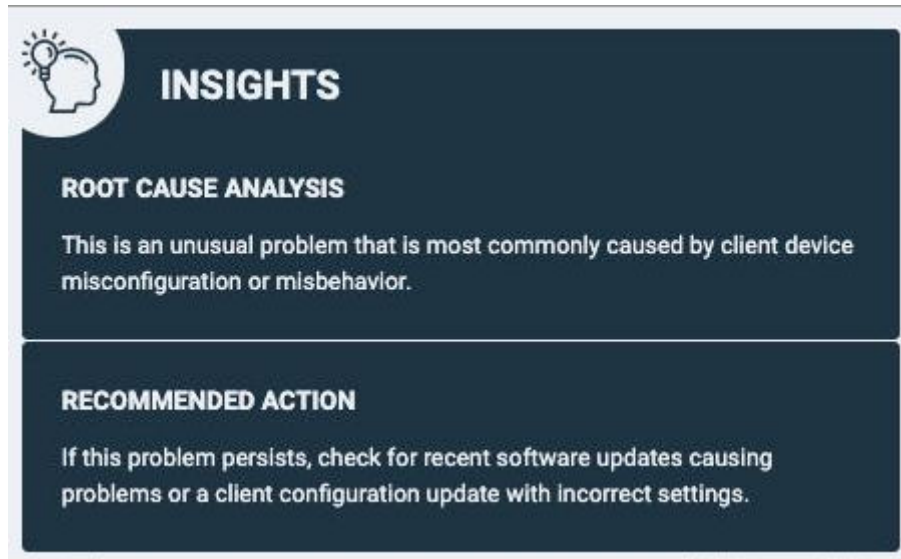
**TABLE 10** Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
VLAN Mismatch	<ul style="list-style-type: none"> <li>Impacted Switch: displays the number of switches impacted by VLAN mismatch</li> <li>Impacted VLANs: displays the number of VLANs that are missing</li> </ul>	<p>Incident identifies incorrect VLAN configurations between switches and wired devices due to which data transmission could be impaired.</p> <ul style="list-style-type: none"> <li>Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident.</li> <li>The <b>Impacted Switches</b> table displays detailed information about the switch name, MAC address, mismatched VLANs, mismatched ports, and mismatched device information where the VLAN mismatch occurred.</li> </ul> <p>Mismatched VLAN numbers are highlighted red.</p>
Memory Utilization		<p>Incident identifies memory leaks within the switch. The time series chart displays high memory utilization by a switch against the threshold set. Pause the pointer over the graph to determine the switch memory used against the threshold set, at a time.</p> <p>The <b>Detected Time</b> identifies when the memory leak happened and based on the threshold set, a <b>Projected Time</b> is calculated and plotted on the graph. Projected time is predicted; it is the time by when the switch will run out of available memory. Contact RUCKUS Support for assistance. You can select the check-box to displays only <b>Memory Used</b> or <b>Threshold</b> graphs.</p>
PoE Power	<ul style="list-style-type: none"> <li>Impacted Switch: displays the number of switches impacted by the denial of PoE power</li> <li>Impacted PoE port: displays the number of PoE ports that are impacted by the denial of PoE power.</li> </ul>	<p>The <b>Impacted Switches</b> table displays detailed information about the switch (name, MAC address, port) for which PoE power was denied.</p>
AP PoE Underpowered	<ul style="list-style-type: none"> <li>AP Model: displays the percentage of failure due to insufficient PoE power that impacted an AP model</li> <li>AP Firmware: displays the percentage of failure due to insufficient PoE power that impacted an AP firmware version</li> </ul>	<ul style="list-style-type: none"> <li>AP POE impact: displays the number of APs impacted at a time, due to insufficient power available on the PoE port</li> <li>Impacted AP: displays the list of APs impacted by failure due to insufficient PoE power within the network</li> </ul>
AP Ethernet Auto-negotiation	<ul style="list-style-type: none"> <li>AP Model: displays the percentage of failure due to Ethernet WAN link mismatch that impacted an AP model</li> <li>AP Firmware: displays the percentage of failure due to Ethernet WAN link mismatch that impacted an AP firmware version</li> </ul>	<ul style="list-style-type: none"> <li>APs WAN Throughput Impact: displays the number of APs impacted at a time, due to Ethernet WAN link mismatch</li> <li>Impacted AP: displays the list of APs impacted by failure due to Ethernet WAN link mismatch within the network</li> </ul>

## Insights Tile

The Insight tile of the **Incident Details** page provides a summary of the root cause and recommended action for the incident. The root cause varies based on the incident type, impacted area, data events, and reason codes.

FIGURE 29 Insights Tile



The Insights tile features a lightbulb icon in a circle at the top left. The main heading is "INSIGHTS". Below this, there are two sections: "ROOT CAUSE ANALYSIS" and "RECOMMENDED ACTION".

**INSIGHTS**

**ROOT CAUSE ANALYSIS**

This is an unusual problem that is most commonly caused by client device misconfiguration or misbehavior.

**RECOMMENDED ACTION**

If this problem persists, check for recent software updates causing problems or a client configuration update with incorrect settings.


## Incident Info Tile

The **Incident Info** tile lets you know the client impact count, the category and sub-category of the incident, the type, scope, duration, and date and time of the incident.. To explore more about the impacted clients, click **Client Impact Count**.

FIGURE 30 Incident Info Tile

INCIDENT INFO		
Client Impact Count	3 of 4 clients (75%)	<a href="#">view details</a>
Incident Category	Connection	
Incident Sub-Category	EAP	
Type	Access Point	
Scope	Eric_R510 (30:87:D9:09:7...	
Duration	1h 45m	
Event start time	Jul 23 2020 17:24	
Event end time	Jul 23 2020 19:09	

Click **view details** for more information about the impacted clients. The **Impacted Clients** page displays the user name, host name, client MAC

address, SSID, and manufacturer of the client. To troubleshoot the client, click the Client Troubleshooting icon (  ) to generate the client


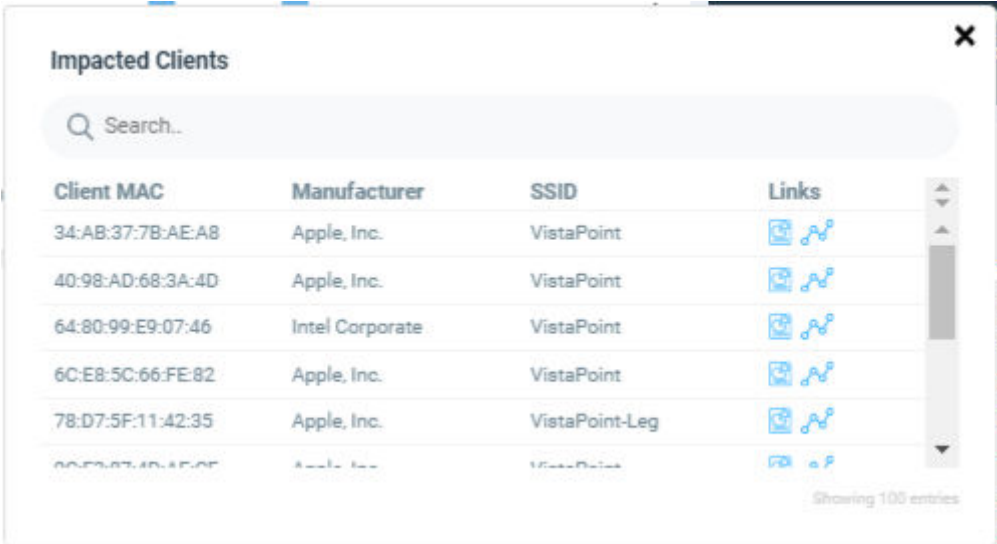
details report, click the Client Details icon (  ) on the **Impacted Clients** page. You can search for impacted clients by the client MAC address and manufacturer.

FIGURE 31 Clients page



Client MAC	Manufacturer	SSID	Links
34:AB:37:7B:AE:A8	Apple, Inc.	VistaPoint	
40:98:AD:68:3A:4D	Apple, Inc.	VistaPoint	
64:80:99:E9:07:46	Intel Corporate	VistaPoint	
6C:E8:5C:66:FE:82	Apple, Inc.	VistaPoint	
78:D7:5F:11:42:35	Apple, Inc.	VistaPoint-Leg	
8C:27:4B:15:0F	Apple, Inc.	VistaPoint	

## Health Page

The **Health** page provides information about network health by giving insights about key performance indicators (KPIs) of the network. The information provided by the **Health** page allows you to analyze the network health and behavior in real time.

You can evaluate network health based on a variety of thresholds that you are allowed to set, called *goals*. For example, you can set the goal (or threshold) to five seconds for all clients to connect to the network, and confirm the number of clients accomplishing the five-second goal in real time. You can thereby determine the metric to understand the number of clients that connect within or before time, and the ones that are delayed. The success rate of network elements meeting each of the goals is typically displayed as a percentage of the metric.

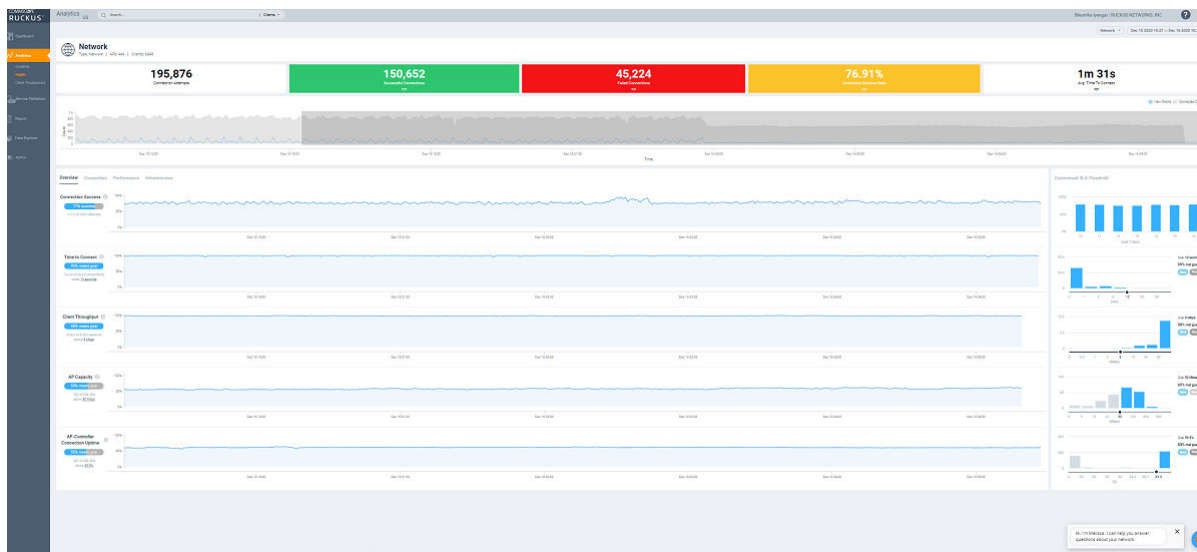
At a high level, the **Health** page also displays the number of connection attempts, successful connections, failed connections, the connection status, and the average time to connect.

### NOTE

You can only view and manage network data for the domains to which you have access, based on the resource group creation and the role assigned to you as a user. For more information, refer to [Managing Users](#) on page 204 and [Managing Resource Groups](#) on page 205.



FIGURE 32 Health Page

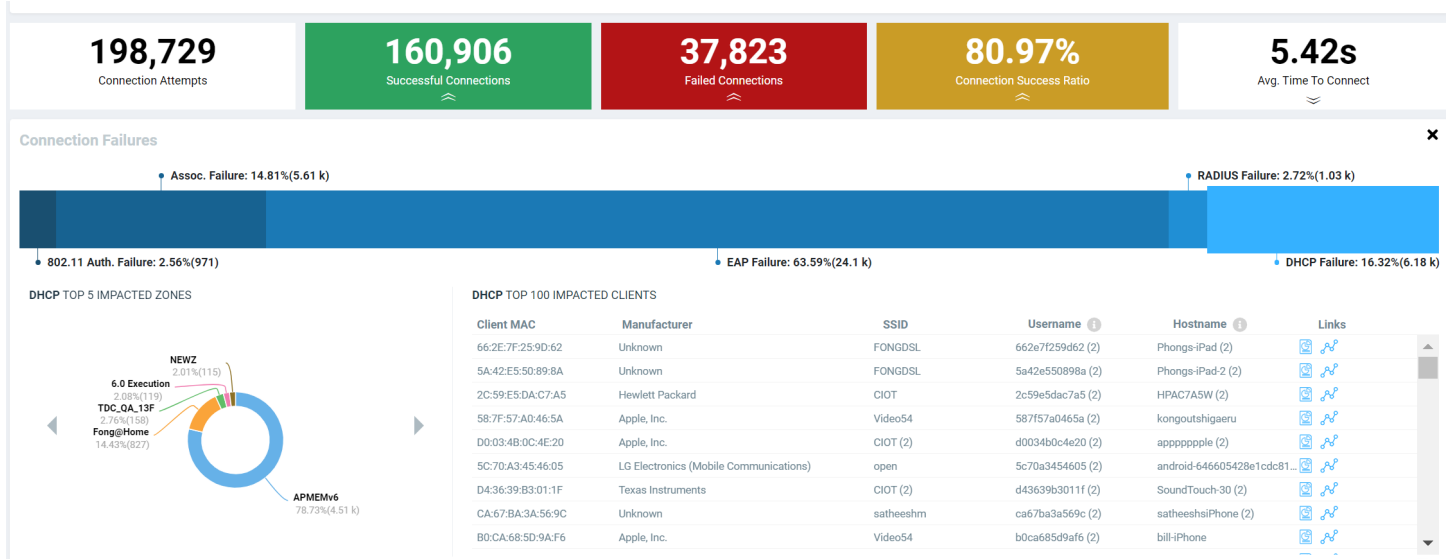


## Unique Connected Clients Graph

The **Unique Connected Clients** graph displays the range of clients attempting to connect to the network. You can modify the range (dark grey area) of clients by moving the scroll bar and this automatically changes the trends displayed in the **Overview**, **Connection**, **Performance** and **Infrastructure** tabs. Pausing the pointer over the graph or placing the pointer at a particular point provides information about the number of connected clients at a time on a given day.

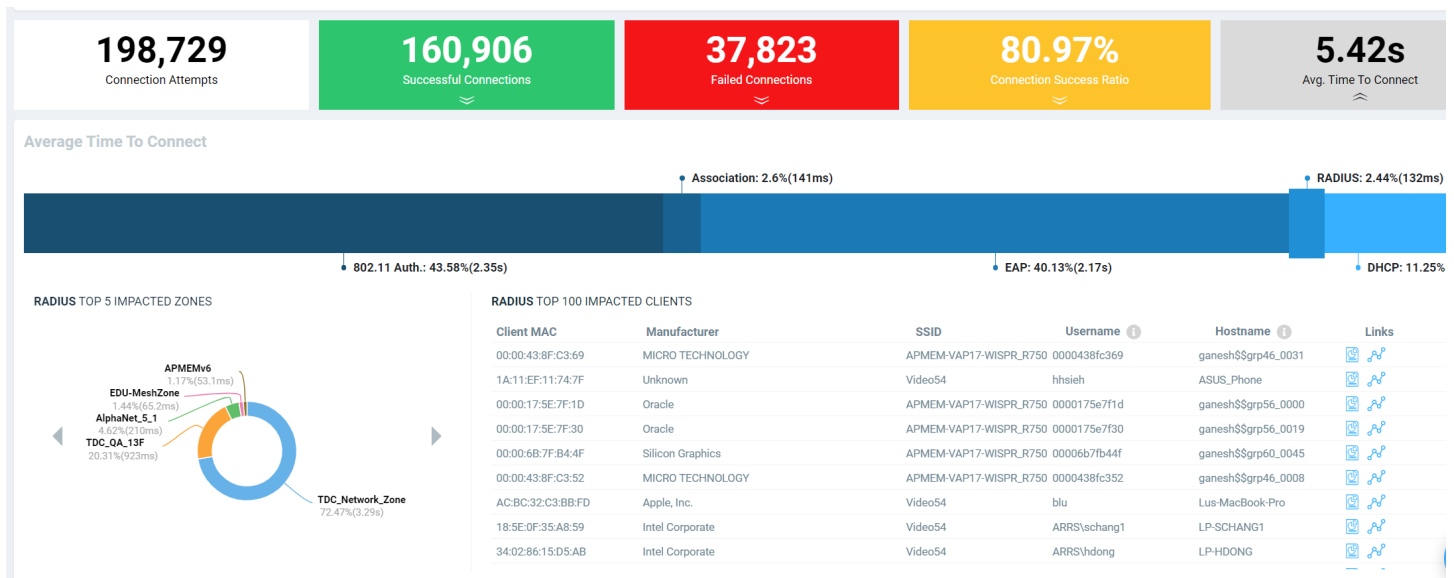
You can also select the drop-down arrows on the coloured bars - Successful Connections, Failed Connections and Connection Success Ratio to display the **Connection Failures** tile. It displays probable reasons for the client to disconnect from the network such as RADIUS failure, EAP failure, DHCP failure and so on. This information is displayed as a bar chart showing the failure percentage in each phase. Clicking the failure types displays more information as a pie chart and table. The pie chart displays the **Top 5 Impacted Zones** and **Top 5 Impacted WLANs**. The table displays **Top 100 Impacted Clients** detailing information such as the client MAC address, manufacturer information, SSID, username, hostname, links to the **Client Details** page and **Client Troubleshooting** page for further analysis.

FIGURE 33 Connection Failures Tile



Similarly, you can also select the drop-down arrow on the **Avg. Time To Connect** bar to display the **Avg. Time To Connect** tile. It displays the average time taken by the client to connect to the network through various authentication mechanisms such as 802.11 Auth, RADIUS authentication, DHCP authentication and so on. This information is displayed as a bar chart showing the percentage of time in each phase of connection. Clicking the authentication types displays more information as a pie chart and table. The pie chart displays the **Top 5 Impacted Zones** and **Top 5 Impacted WLANs**. The table displays **Top 100 Impacted Clients** detailing information such as the client MAC address, manufacturer information, SSID, username, hostname, links to the **Client Details** page and **Client Troubleshooting** page for further analysis.

FIGURE 34 Average Time To Connect Tile



## Overview Tab

The **Overview** tab displays information about successful client connections, time taken by the client to connect to the network, client throughput, AP capacity, and AP service uptime. The area is graphically divided into three sections: a pill-shaped box depicting the metric as percentages, a time series graph depicting the metric as percentages, and a histogram.

The pill-shaped box not only depicts the percentage of successful connections, but also specifies the connections, sessions, and APs meeting a threshold within the larger sample set.

There are two types of histograms: a view-only histogram that provides information about the threshold trends, and another configurable histogram that allows you to set the threshold for a metric. The threshold you set for the metric is the value against the goal. By default, the goal met for the last 7 days is displayed. Click **Apply** to set the new threshold for the metric or click **Reset** to revert to the default threshold value.

The following KPIs are displayed on the tab:

- **Connection Success:** Measures the number of connection attempts that complete successfully. Pausing the pointer over the time series graph at a point displays the percentage of successful connections made and the number of connections attempted by the client at that time and date. Pausing the pointer over the histogram bar graph displays the number of sample clients that attempted to connect to the network.
- **Time to Connect (TTC):** Measures the percentage of connection attempts that completed within the service level agreement (SLA). Pausing the pointer over the time series graph at a point displays the percentage of TTC count and connection count at that time and date. Pausing the pointer over the histogram bar graph displays the number of sample clients that attempted to connect to the network.
- **Client Throughput:** Measures the number of client sessions with the throughput potential that met the SLA. Pausing the pointer over the time series graph at a point displays the percentage of throughput count and session count at that time and date. Pausing the pointer over the histogram bar graph displays the number of sample clients that attempted to connect to the network.
- **AP Capacity:** Measures the number of APs with the average capacity that met the SLA. Pausing the pointer over the time series graph at a point displays the percentage of capacity count at that time and date. Pausing the pointer over the histogram bar graph displays the number of APs that met the SLA.
- **AP Service Uptime:** Measures the percentage of time the radios of an AP are fully available for client service.

**TABLE 11** KPIs Snapshot: Overview Tab

KPI	Pill-Shaped Box	Time Series Graph	Histogram
Connection Success	Displays the percentage of successful connection attempts	Displays the percentage of successful connection attempts	Displays a bar chart of success percentage where the X axis displays time in hours, days, and weeks, and the Y axis displays success percentage
Time to Connect	Displays the percentage of connections that completed within the TTC SLA (for the time range selected)	Displays the percentage of connections meeting the SLA over time	Displays a bar chart of TTC where the X axis displays TTC duration and the Y axis displays the connection count; also displays the percentage of connections that completed within the TTC SLA for the entire time range
Client Throughput	Displays the percentage of client sessions with the average throughput that met the SLA (for the time range selected)	Displays the percentage of client sessions with the throughput that met the SLA	Displays a bar chart of throughput by session where the X axis displays the average throughput per session and the Y axis displays the session count; also displays the percentage of client sessions with the average throughput that met the SLA for the entire time range
AP Capacity	Displays the percentage of APs with average capacity that met the SLA (for the time range selected)	Displays the percentage of AP capacity count that met the SLA	Displays a bar chart of average capacity where the X axis displays average capacity and the Y axis displays AP count; also displays the percentage of APs that met the SLA for the entire time range

**TABLE 11** KPIs Snapshot: Overview Tab (continued)

KPI	Pill-Shaped Box	Time Series Graph	Histogram
AP Service Uptime	Displays the percentage of APs with the uptime that met the SLA (for the time range selected)	Displays the percentage of APs with the uptime that met the SLA	Displays a bar chart of AP service uptime where the X axis displays the percentage of AP service uptime and the Y axis displays the number of APs that meet the goal for the selected time; also displays the percentage of APs with the uptime that met the SLA for the entire time range

## Connection Tab

The **Connection** tab displays information about successful client connections, time taken by the client to connect to the network, association, user authentication, DHCP, RADIUS, and roaming success. The area is graphically divided into three sections: a pill-shaped box depicting the metric as percentages, a time series graph depicting the metric as percentages, and a histogram.

The pill-shaped box not only depicts the percentage of successful connections, authentications, and associations, but also specifies the connections, authentications, and associations meeting a threshold within the larger sample set.

There are two types of histograms: a view-only histogram that provides information about the threshold trends, and another configurable histogram that allows you to set the threshold for a metric. The threshold you set for the metric is the value against the goal. By default, the goal met for the last 7 days is displayed. Click **Apply** to set the new threshold for the metric or click **Reset** to revert to the default threshold value.

The following KPIs are displayed on the page:

- **Connection Success:** Measures the number of connection attempts that complete successfully. Pausing the pointer over the time series graph at a point displays the percentage of successful connections made and the number of connections attempted by the client at that time and date. Pausing the pointer over the histogram bar graph displays the number of sample clients that attempted to connect to the network.
- **Time to Connect (TTC):** Measures the percentage of connection attempts that completed within the service level agreement (SLA). Pausing the pointer over the time series graph at a point displays the percentage of TTC count and connection count at that time and date. Pausing the pointer over the histogram bar graph displays the number of sample clients that attempted to connect to the network.
- **Association:** Measures the number of association attempts that complete successfully. Pausing the pointer over the time series graph at a point displays the percentage of association attempts at that time and date.
- **User (L2) Authentication:** Measures the number of Layer 2 user authentication attempts that complete successfully. Pausing the pointer over the time series graph at a point displays the percentage of successful Layer 2 user authentications at that time and date.
- **DHCP:** Measures the number of DHCP connection attempts that complete successfully. Pausing the pointer over the time series graph at a point displays the percentage of successful DHCP connections at that time and date.
- **RADIUS:** Measures the number of RADIUS connection attempts that complete successfully. Pausing the pointer over the time series graph at a point displays the percentage of successful RADIUS connections at that time and date.
- **Roaming Success:** Measures the number of client roaming attempts that complete successfully.

**TABLE 12** KPIs Snapshot: Connection Tab

KPI	Pill-Shaped Box	Time Series Graph	Histogram
Connection Success	Displays the percentage of successful connection attempts	Displays the percentage of successful connection attempts over time	Displays a bar chart of success percentage where the X axis displays time in hours, days, and weeks, and the Y axis displays success percentage

**TABLE 12** KPIs Snapshot: Connection Tab (continued)

KPI	Pill-Shaped Box	Time Series Graph	Histogram
Time to Connect	Displays the percentage of connections that completed within the TTC SLA (for the selected time range)	Displays the percentage of connections meeting the SLA over time	Displays a bar chart of TTC where the X axis displays TTC duration and the Y axis displays the connection count; also displays the percentage of connections that completed within the TTC SLA for the entire time range
Association	Displays the percentage of successful association attempts	Displays the percentage of successful association attempts over a granular range of time, which is also determined by the time range selected under <b>Unique Connected Clients</b>	Displays a bar chart of successful associations, as a percentage of the sample set, where the X axis displays time in hours, days, and weeks depending upon the time selection made under <b>Unique Connected Clients</b> , and the Y axis displays success percentage
User (L2) Authentication	Displays the percentage of successful Layer 2 user authentication attempts	Displays the percentage of Layer 2 user authentication attempts over a granular range of time, which is also determined by the time range selected under <b>Unique Connected Clients</b>	Displays a bar chart of successful Layer 2 user authentication attempts, as a percentage of the sample set, where the X axis displays time in hours, days, and weeks depending upon the time selection made under <b>Unique Connected Clients</b> , and the Y axis displays success percentage
DHCP	Displays the percentage of successful DHCP attempts	Displays the percentage of successful DHCP attempts over a granular range of time, which is also determined by the time range selected under <b>Unique Connected Clients</b>	Displays a bar chart of successful DHCP attempts, as a percentage of the sample set, where the X axis displays time in hours, days, and weeks depending upon the time selection made under <b>Unique Connected Clients</b> , and the Y axis displays success percentage
RADIUS	Displays the percentage of successful RADIUS attempts	Displays the percentage of successful RADIUS attempts over a granular range of time, which is also determined by the time range selected under <b>Unique Connected Clients</b>	Displays a bar chart of successful RADIUS attempts, as a percentage of the sample set, where the X axis displays time in hours, days, and weeks depending upon the time selection made under <b>Unique Connected Clients</b> , and the Y axis displays success percentage
Roaming Success	Displays the percentage of successful roaming attempts	Displays the percentage of successful roaming attempts over time	Displays a bar chart of roaming percentage where the X axis depicts coarse time and the Y axis displays the success percentage

## Performance Tab

The **Performance** tab displays information about client throughput, AP capacity, and client RSS. The area is graphically divided into three sections: a pill-shaped box depicting the metric as percentages, a time series graph depicting the metric as percentages, and a histogram.

The pill-shaped box not only depicts the percentage of client throughput, AP capacity, and client RSS, but also specifies the client throughput and AP capacity meeting a threshold within the larger sample set.

There are two types of histograms: a view-only histogram that provides information about the threshold trends, and another configurable histogram that allows you to set the threshold for a metric. The threshold you set for the metric is the value against the goal. By default, the goal met for the last 7 days is displayed. Click **Apply** to set the new threshold for the metric or click **Reset** to revert to the default threshold value.

The following KPIs are displayed on the tab:

- **Client Throughput:** Measures the client throughput sessions that met the service level agreement (SLA). Pausing the pointer over the time series graph at a point displays the percentage of successful client throughput values achieved by the client at that time and date. Pausing the pointer over the histogram bar graph displays the number of sample client throughput goals achieved with the network.
- **AP Capacity:** Measures the number of APs with the average capacity that met the SLA. Pausing the pointer over the time series graph at a point displays the percentage of average AP capacity at that time and date. Pausing the pointer over the histogram bar graph displays the number of sample clients that attempted to connect to the network.

- Client RSSI: Measures the number of client sessions with the average RSSI that met the SLA. Pausing the pointer over the time series graph at a point displays the percentage of successful RSSI goals achieved by the client at that time and date. Pausing the pointer over the histogram bar graph displays the number of sample client RSSI goals achieved with the network. This metric defines the signal strength.

**TABLE 13** KPIs Snapshot: Performance Tab

KPI	Pill-Shaped Box	Time Series Graph	Histogram
Client Throughput	Displays the percentage of successful client throughput sessions that met the SLA (for the selected time range)	Displays the percentage of successful client throughput sessions that met the SLA over time	Displays a bar chart of success percentage where the X axis displays the average throughput per session and the Y axis displays the session count; also displays the percentage of successful client throughput sessions that met the SLA for the entire time range
AP Capacity	Displays the percentage of the number of APs with the average capacity that met the SLA (for the selected time range)	Displays the percentage of the number of APs with the average capacity that met the SLA over time	Displays a bar chart of average AP capacity where the X axis displays the average capacity and the Y axis displays the AP count; also displays the percentage of the number of APs with the average capacity that met the SLA for the entire time range
Client RSS	Displays the percentage of client sessions with the average RSSI that met the SLA (for the selected time range)	Displays the percentage of client sessions with the average RSSI that met the SLA over time	Displays a bar chart of average RSSI by session where the X axis displays the average RSSI per session and the Y axis displays the session count; also displays the percentage of client sessions with the average RSSI that met the SLA for the entire time range

## Infrastructure Tab

The **Infrastructure** tab displays information about the time taken for the AP to respond to the controller. The area is graphically divided into three sections: a pill-shaped box depicting the metric as percentages, a time series graph depicting the metric as percentages, and a histogram.

The pill-shaped box not only depicts the percentage of AP controller latency, but also specifies the AP controller latency meeting a threshold within the larger sample set.

The configurable histogram allows you to set the threshold for a metric. The threshold you set for the metric is the value against the goal. By default, the goal met for the last 7 days is displayed. Click **Apply** to set the new threshold for the metric or click **Reset** to revert to the default threshold value.

The following KPIs are displayed on the tab:

- AP-to-SZ-Latency: Measures the number of APs with the SmartZone controller control plane latency that met the service level agreement (SLA). Pausing the pointer over the time series graph at a point displays the percentage of successful latency values achieved by the AP at that time and date. Pausing the pointer over the histogram bar graph displays the number of sample latency goals achieved.
- AP-Controller Connection Uptime: Measures the percentage of time an APs radios are fully available for client service.
- Cluster Latency: Measures the percentage of time the SmartZone cluster latency meets the SLA.
- PoE Utilization: Measures the percentage of PoE utilization by the switches in the network.
- Online APs: Measures the percentage of APs that are online in the network.

**TABLE 14** KPI Snapshot: Infrastructure Tab

KPI	Pill-Shaped Box	Time Series Graph	Histogram
AP-to-SZ-Latency	Displays the percentage of APs with the AP-to-SZ latency that met the SLA (for the selected time range)	Displays the percentage of APs with the AP-to-SZ latency that met the SLA over time	Displays a bar chart of average latency percentage where the X axis displays average AP-to-SZ latency and the Y axis displays the AP count; also displays the percentage of APs with the AP-to-SZ latency that met the SLA for the entire time range
AP-Controller Connection Uptime	Displays the percentage of APs with the uptime that met the SLA (for the selected time range)	Displays the percentage of APs with the uptime that met the SLA over time	Displays a bar chart of AP service uptime where the X axis displays the percentage of AP service uptime and the Y axis displays the number of APs that meet the goal for the selected time; also displays the percentage of APs with the uptime that met the SLA for the entire time range
Cluster Latency	Displays the percentage of time controller cluster latency that met the SLA (for the selected time range)	Displays the percentage of nodes per bin with the latency that met the SLA over time	Displays a bar chart of average cluster latency where the X axis displays the time of latency in ms and the Y axis displays the clusters per bin; also displays the percentage of time controller cluster latency that met the SLA for the entire time range
PoE Utilization	Displays the percentage of Power over Ethernet (PoE) used by the switches that met the SLA (for the selected time range)	Displays the percentage of Power over Ethernet (PoE) used by the switches that met the SLA over time	Displays a bar chart of switches that met the PoE utilization goal where the X axis displays the percentage of PoE utilization and the Y axis displays the number of switches that met the goal for the selected time
Online AP Count	Displays the percentage of APs online (for the selected time range)	Displays the percentage of APs that are online over time	Displays a bar chart of online APs where the X axis displays last 7 days of the week and the Y axis displays the percentage of online APs; the percentage is displayed for each day of the week

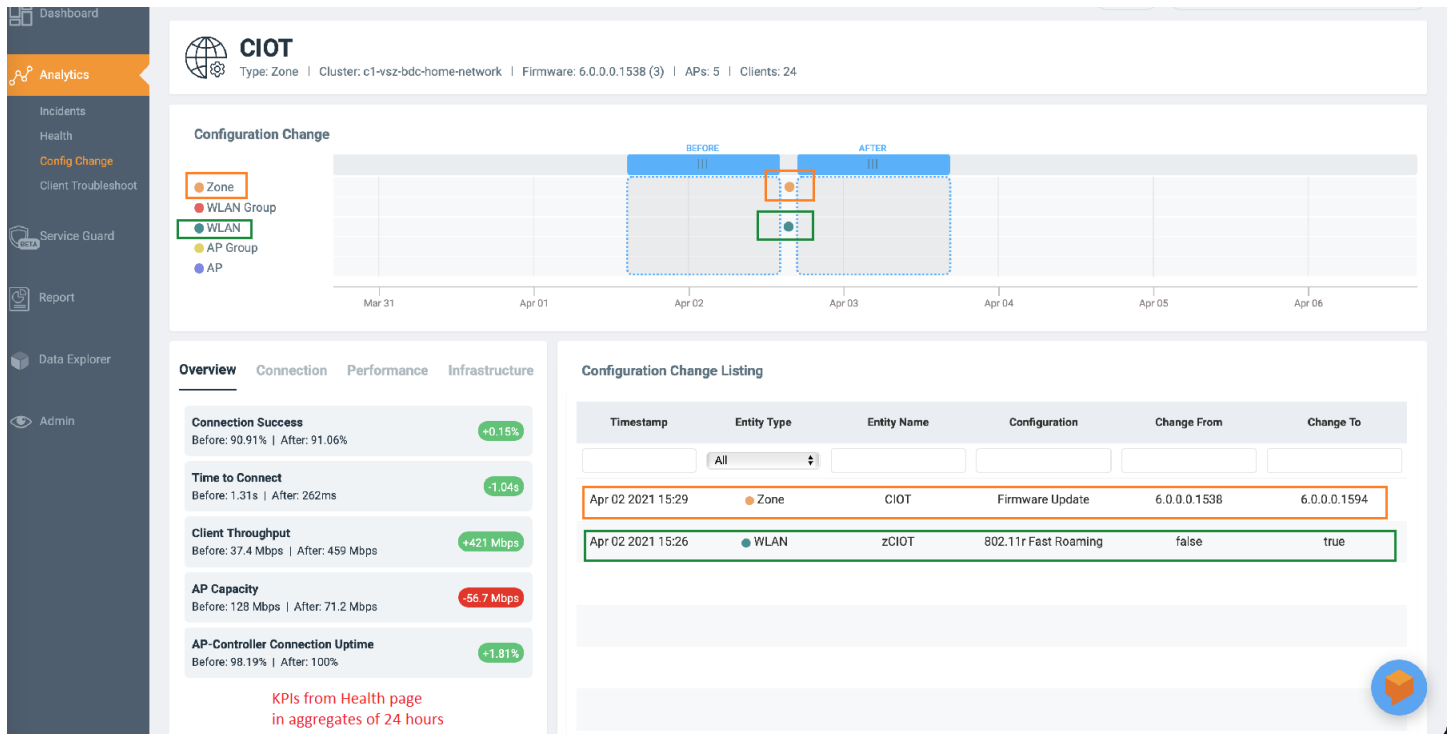
## Configuration Change Page

You can monitor and analyze changes to network KPIs due to configuration changes and software changes from the **Configuration Change** page. Network KPIs can be compared before and after a configuration change is applied to the system, thereby presenting the impact of the configuration changes or software updates on the system and its devices.

**NOTE**

Configuration change analysis is only available for SmartZone controllers.

FIGURE 35 Configuration Change Page



The **Configuration Change** page consists of the following components:

- Configuration Change tile
- Configuration Change Listing table
- Health tile

## Configuration Change Tile

The **Configuration Change** tile displays configuration changes that have been applied at the Zone, WLAN Group, WLAN, AP Group, and AP levels. Every change in configuration or software change is displayed as a dot on the time series graph. Each dot is colored based on the level on which the configuration was applied and is represented by that color. In the example in the figure, an orange dot represents the configuration change applied at the Zone level, and a green dot represents the configuration change applied at the WLAN level. Clicking the dot highlights the configuration change in the **Configuration Change Listing** table and vice versa. The first row of the table pertains to data from the orange dot displaying the firmware updated, and the second row pertains to data from the green dot displaying enabling 802.11r fast roaming. In the time series graph, pause the pointer over a dot to see when the configuration change was applied.

Additionally, there are two scrolling widgets or "lens" that represent a section of time or time slot on the time series graph. They are usually termed "Before" and "After" to indicate the health of the network before and after the configuration change was applied. Scrolling the lenses dynamically computes the KPIs and displays the values on the **Health** tile.

### NOTE

**Health** tile data (before, after, and comparison numbers) is impacted by several factors, including system configuration, Wi-Fi environment, type of clients, number of clients, network back haul, and so on. Therefore, if the scrolling widgets move to an area where there is no visible configuration change (a colored dot), **Health** tile data may still change based on some of the previously mentioned factors.



To determine the network health before and after the firmware update (the orange dot in the figure), scroll the **Before** lens to a time prior to the firmware update and scroll the **After** lens to a time after the firmware update. KPIs on the **Health** tile are computed and displayed immediately, providing clear "before" and "after" values for each KPI. In the example in the figure, **Connection Success**, or the number of clients that attempted to connect to the network, increased by 0.15 percent after the firmware update (the configuration change). **Connection Success** was lower at 90.91 percent before the configuration change than 91.06 percent after the change. Based on this analysis, network administrators can take corrective action to improve the KPI.

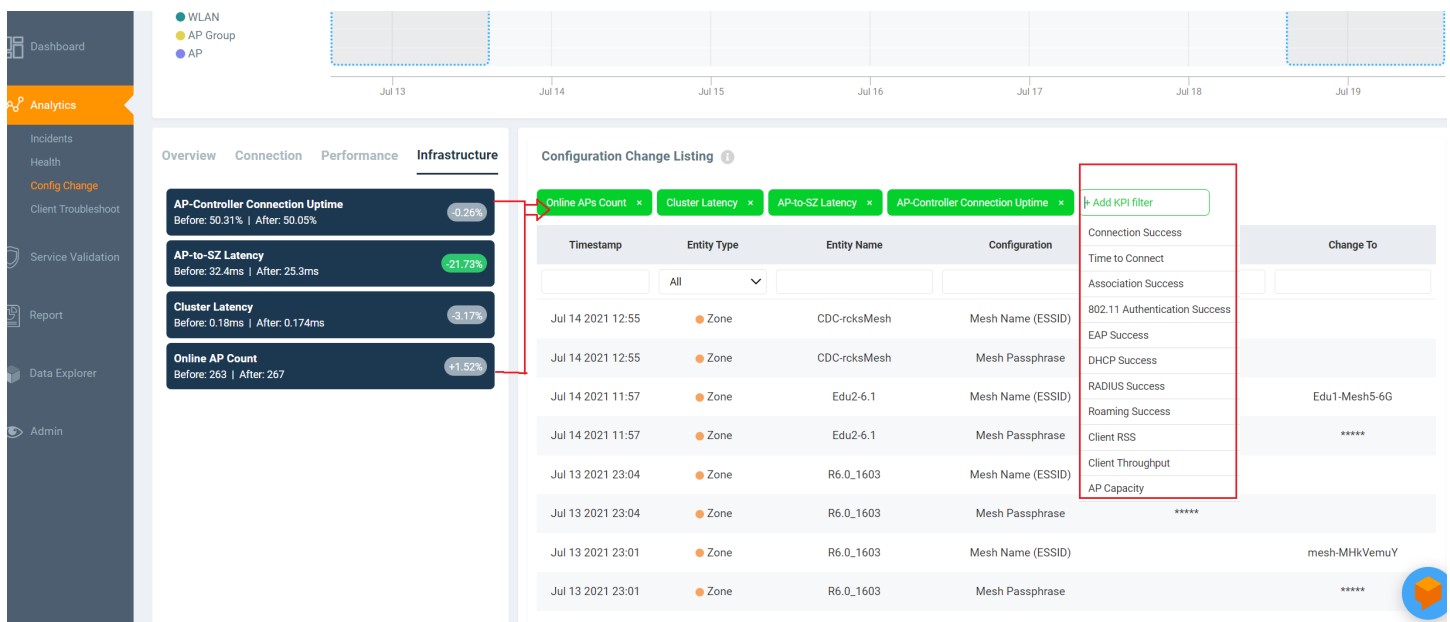
## Configuration Change Listing Tile

The **Configuration Change Listing** table is a tabular representation of all the time series data in the **Configuration Change** tile displaying specific information about what changed after the configuration was applied. It displays information about the timestamp of the configuration change, the entity type for which the configuration was applied (Zone, WLAN, AP, and so on), the entity name, configuration, and information about what specifically changed after the configuration was applied (**Change From** and **Change To** columns).

Additionally, you can also filter for relevant configuration changes that are specific to a particular KPI by simply clicking the KPI in the **Health** tile, or the **Add KPI** filter above the table.

Selecting a row in the **Configuration Change Listing** table highlights the associated dot on the time series graph in the **Configuration Change** tile.

FIGURE 36 Configuration Change Listing Tile: Adding Health KPIs



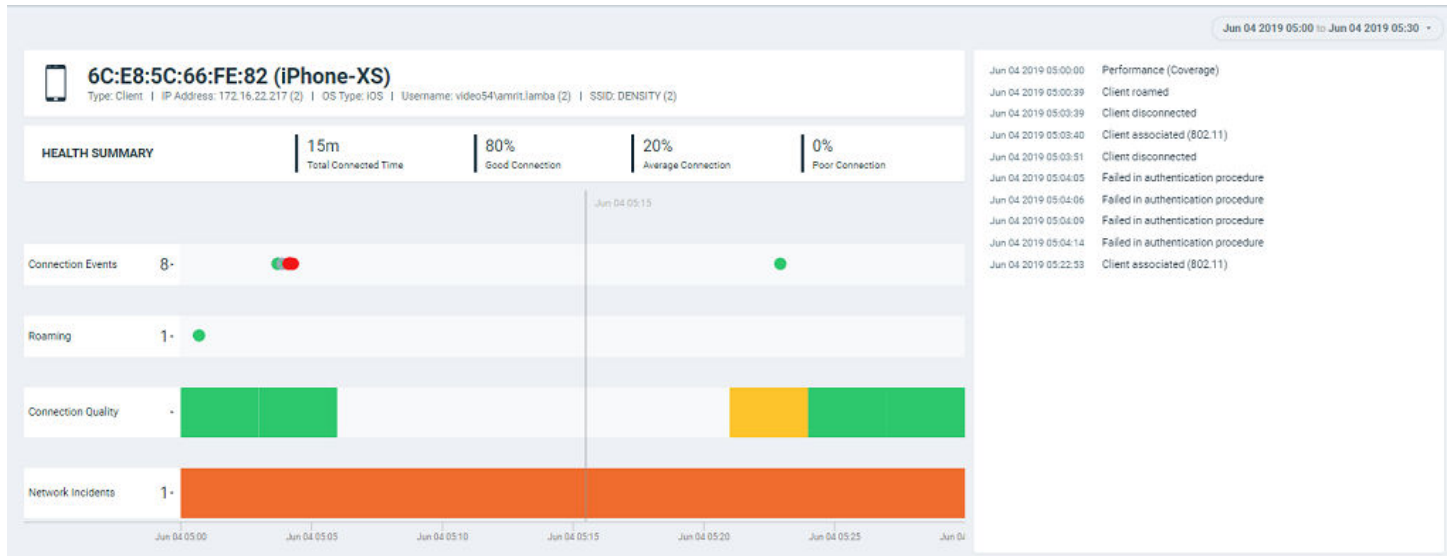
## Health Tile

The **Health** tile displays the same KPIs that are available on the **Health** page, the difference being the **Health** tile displays KPI data aggregated over 24 hours, which is more granular than the Health page with respect to time. For more information, refer to [Health Page](#) on page 48. In the **Health** tile, you can view the before and after values of each KPI impacted by the configuration change. The overall impact of the change is displayed within a red, gray or green capsule based on the percentage change. The capsule appears green if the configuration change positively impacted the KPI or improved the performance by more than 5 percent. It appears red if the change negatively impacted the KPI value and diminished the performance by less than 5 percent. It appears gray if the KPI value is strictly + or - 5%. These granular details enable an administrator to monitor network health continuously and ensure the network performs to its highest capabilities.

# Client Troubleshooting Page

The client troubleshooting page provides you details about the connectivity of a particular client.

**FIGURE 37** Client Troubleshooting Page



The header displays the MAC address of the client followed by its host name. The line underneath the header lists the following client attributes:

- MAC address
- Last IP address
- Host name
- OS type
- Username

For data fields in which there are multiple entries (such as IP address), the system shows a value in parentheses (for example, (2)). Pausing the pointer on this number shows the additional values for the field.

The **Health Summary** shows the total time during which the client was connected to the network. The **Health Summary** highlights the following measurements::

- Total Connected Time
- Percentage of Good Connection
- Percentage of Average Connection
- Percentage of Poor Connection

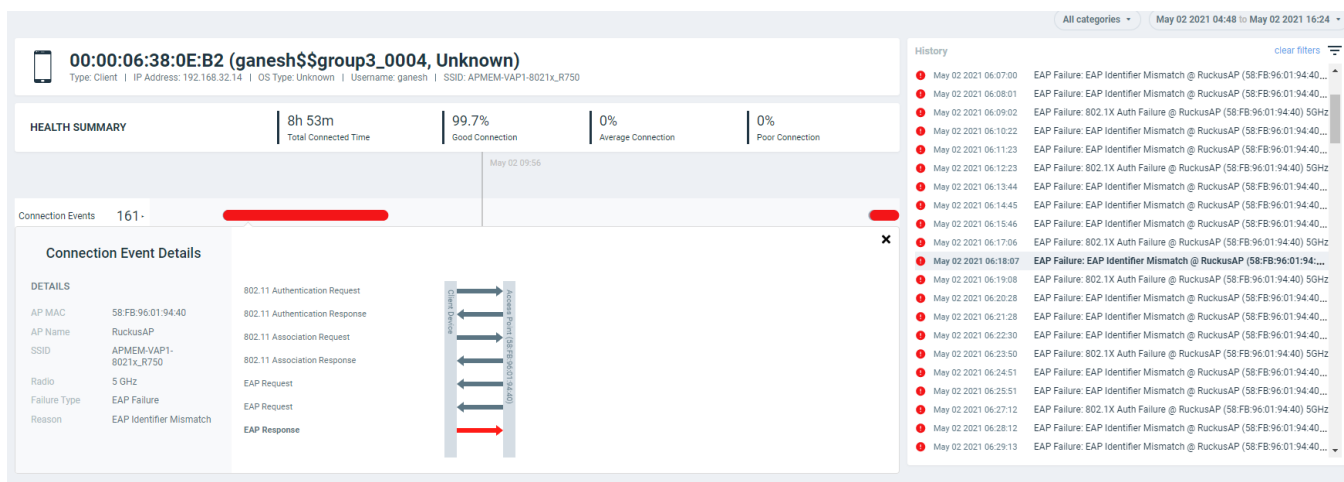
The health classification (good, average, and poor) depends on the **Connection Quality** metrics, which consist of SNR, MCS, and Client Capacity metrics.

The **Connection Events** shows the connection status of the client on the particular WLAN for a specific AP. The connection events are classified (success, failure, slow, and disconnect), and are identified with the following colors:

- Green: Successful connection. Pause the pointer over the green dots to view more information such as the AP MAC address, AP name, SSID and Radio.

- Red circle with exclamation point: Failed connection. You can also click the red circle to view the time of the failure scenario (for example, whether the failure occurred during the EAP request, DHCP discovery, and so on). Pausing the pointer over the circle provides a quick snapshot of information such as the exact time of failure, the type of failure, the client IP address, connection diagram analyzing the point of failure and so on. The failed path is denoted by a red arrow, as shown in the figure. The figure depicts a failure when EAP Identifier Mismatch happens.

FIGURE 38 Failure Due to EAP Identifier Mismatch



- Yellow: Slow (long time to connect to connection)
- Gray: Disconnected

**Roaming** shows the connection status when the client either moves to a different WLAN or a different AP. A roaming event is identified with the following colors:

- Green: Successful roam. Pause the pointer over the dot for more information.
- Red circle with exclamation point: Failed connection. Pause the pointer over the dot for more information.

The **Connection Quality** shows the quality of the service the client experiences throughout of the network. The connection quality is identified with the following colors:

- Green: Good
- Red: Poor
- Yellow: Average

**Network Incidents** shows any incidents that affected the client. The incidents are classified (client connection, performance, and infrastructure), and are identified with the following colors and severities:

- Red: P1
- Dark Orange: P2
- Orange: P3
- Yellow: P4

The Timeline displays the history of events that occurred for this client during the time period displayed on the screen. It shows the client connected and disconnect events, the network incidents, and so on.

**NOTE**

Clicking any network incident in the Timeline directs you to the **Incident Details** Page.

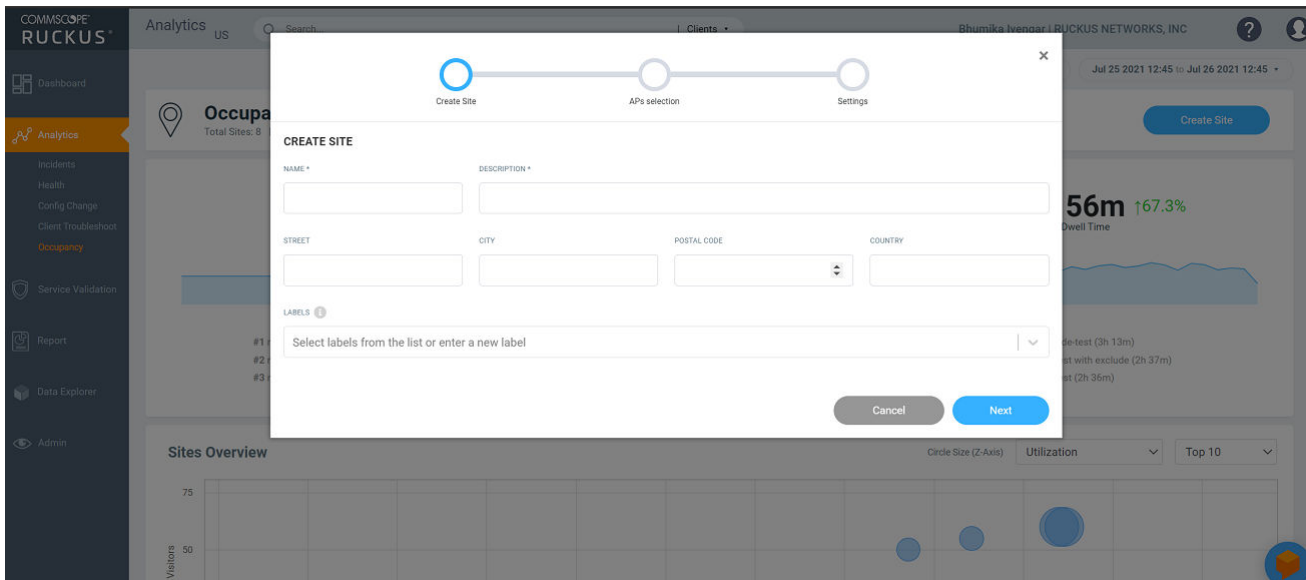
Based on the client access permissions set in the resource group, the client is only able to view the data for APs for which access permission are granted. If the client roams to an AP for which access permissions are not granted, the AP data is not available to view even though the connection between client and AP (roamed to) are established.

## Occupancy Page

Occupancy analytics data provides insights into space utilization within a facility, such as the most heavily used area or the predominantly least-used area within the facility.

The first step to performing the analysis is to divide the facility into sites. A site is a group of APs; a physical unit. Complete the following steps to create a site.

FIGURE 39 Creating a Site



1. From the **Occupancy** page, click **Create Site**.
2. Enter the name of the site, a description (an area of the facility for which you are creating the site, for example, the gym, the lobby, the third floor, or a similar area), and the street, city, postal code, and country of the site. Also, select a label to identify the site or create a new label term.

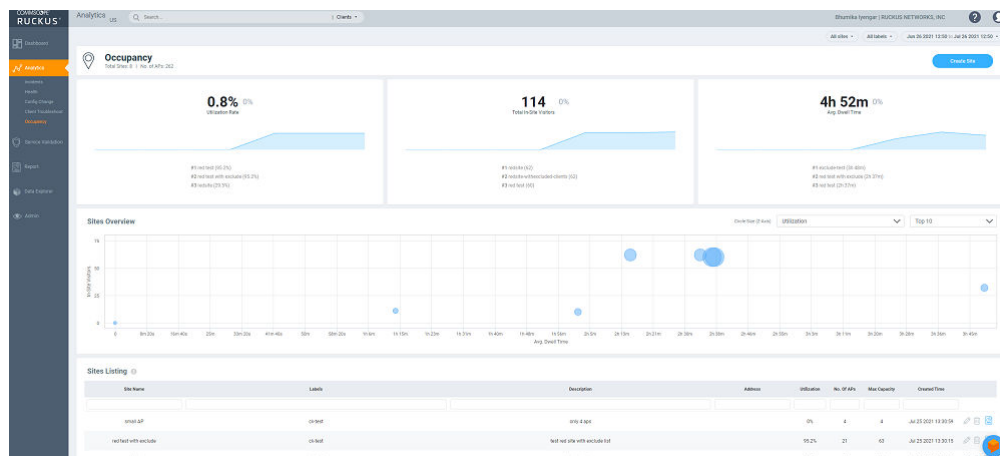
### NOTE

You can include one or more labels for a site. Labels make searching for a particular site easy, especially when there are multiple sites within the network.

3. Click **Next**.
4. Select the APs you want to group within this site.
5. Click **Next**.
6. In the **Settings** page, set the maximum capacity per AP. Based on the APs you selected, the number of APs are populated and the maximum capacity of the site is calculated and displayed.
7. Click **Create**. The site is created and displayed in the **Sites Listing** table.

You can view the occupancy details for specific site(s) with one or more labels from the top-right corner of the **Occupancy** page, using the **All sites** and **All labels** options.

FIGURE 40 Occupancy Page



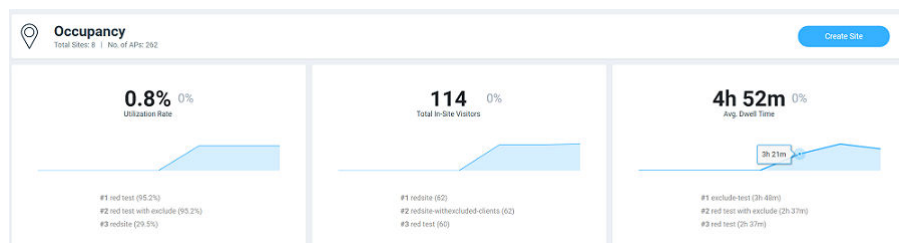
The **Occupancy** page contains a number of components:

- Utilization tile
- Total In-Site Visitors tile
- Avg. Dwell Time tile
- Sites Overview chart
- Sites Listing table

## Utilization Tile

The **Utilization** tile displays the average site utilization percentage and the increase or decrease in utilization percentage from the previous time. An increase in average site utilization is displayed as a green number while a decrease is displayed as a red number. The **Utilization** tile also displays the top three clients utilizing the site.

FIGURE 41 Utilization, Total In-site Visitors, and Avg Dwell Time Tiles



## Total In-Site Visitors Tile

The **Total In-Site Visitors** tile displays the average number of visitors visiting the site and the increase or decrease in the number of in-site visitors from the previous time. An increase in average in-site visitors is displayed as a green number while a decrease is displayed as a red number. The

**Total In-Site Visitors** tile also displays the top three clients visiting the site. A "visitor" is a device connected to an AP in the site with a unique MAC address.

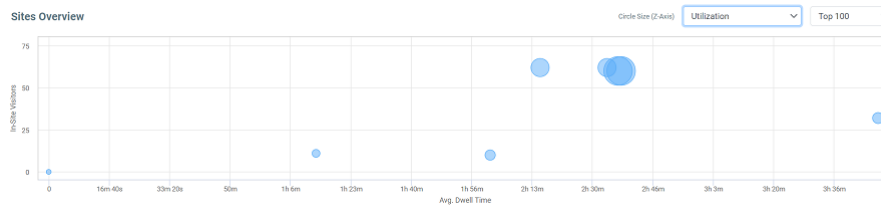
## Avg. Dwell Time Tile

The **Avg. Dwell Time** tile displays the average amount of time in minutes a device is connected to an AP in the site, and the increase or decrease in the dwell time from the previous time. An increase in average dwell time is displayed as a green number while a decrease is displayed as a red number. The **Avg. Dwell Time** tile also displays the top three clients with the highest dwell times in the site.

## Sites Overview Chart

The **Sites Overview** chart provides a graphical representation (bubble chart) of the AP count, average dwell time, and in-site visitors. Selecting one of these parameters from the menu populates data related to the other two in the graph and provides multi-site data for comparison and analysis. For example, selecting **AP Count** from the menu, populates data pertaining to the in-site visitor on the Y-axis and the average dwell time on the X-axis. Pause the pointer over a bubble to view the site rank, average dwell time, AP count, and in-site visitors count. By default, the top 10 sites are displayed, however, you can view up to top 100 sites by using menu options.

FIGURE 42 Sites Overview Chart



## Sites Listing Table

The **Sites Listing** table displays information such as the site name, labels, description, city, country, AP count, and time of site creation. The properties of each site can be edited using the Edit icon (✎). Click the Report icon (📄) to view the [Site Report](#) on page 63.

FIGURE 43 Sites Listing Table

Site Name	Labels	Description	Address	Utilization	No. Of APs	Max Capacity	Created Time	
small AP	ck-test	only 4 aps		0%	4	4	Jul 25 2021 13:30:59	✎ 📄 🗑️
red test with exclude	ck-test	test red site with exclude list		95.2%	21	63	Jul 25 2021 13:30:15	✎ 📄 🗑️
red test	ck-test	test red sites		95.2%	21	63	Jul 25 2021 13:29:15	✎ 📄 🗑️
redsite-withexcluded-clients	test, bangalore, india, bellandur	wfh	bellandur, bangalore, india, 560103	29.5%	21	210	Jul 24 2021 10:45:28	✎ 📄 🗑️
TEST		lobby A desc		1.1%	101	1,010	Jul 24 2021 10:44:53	✎ 📄 🗑️
bigsite	test, bangalore, india, karnataka, bellandur	wfh	doddakanehalli, bangalore, india, 5...	5%	20	200	Jul 24 2021 10:44:40	✎ 📄 🗑️
redsite	marathalli, bangalore, india, karnataka	home	Marathalli, bangalore, India, 560049	29.5%	21	210	Jul 24 2021 10:43:48	✎ 📄 🗑️
exclude-test	test	lobby A desc		6%	53	530	Jul 24 2021 10:43:43	✎ 📄 🗑️

## Site Report

The **Site Report** displays information specific to the selected site such as the site, utilization for a selected period, the average dwell time of visitors, the total number of visitors in the site, and user information in both graphical and tabular formats.

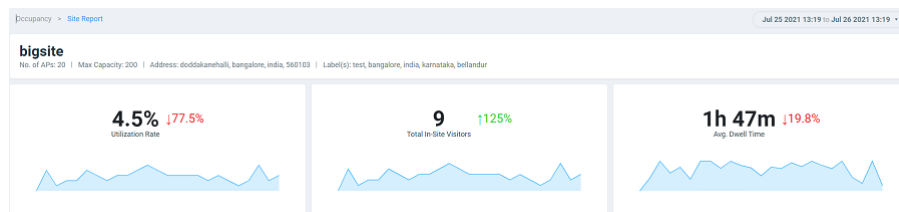
The top portion of the report displays the number of APs grouped into the site and the duration for which you would like to view site data. Options include the last 24 hours and the last 7 days.

The **Site Report** consists of the following components:

- Utilization tile
- Total In-Site Visitors tile
- Avg. Dwell Time tile
- Utilization and Number of Users tile
- Dwell Time tile
- Clients table

### Utilization Tile

FIGURE 44 Utilization, Total In-Site Visitors, and Avg. Dwell Time for a Selected Site



The **Utilization** tile displays the utilization percentage for the selected site and the increase or decrease in utilization percentage from the previous time. An increase in site utilization is displayed as a green number while a decrease is displayed as a red number.

### Total In-Site Visitors Tile

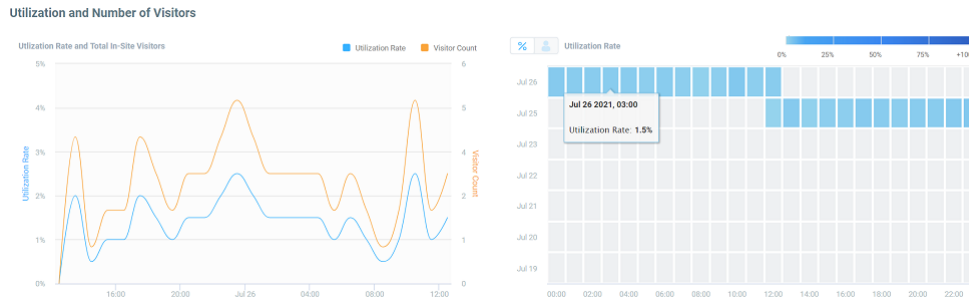
The **Total In-Site Visitors** tile displays the number of visitors visiting the selected site and the increase or decrease in the number of in-site visitors from the previous time. An increase in in-site visitors is displayed as a green number while a decrease is displayed as a red number. A "visitor" is a device connected to an AP in the site with a unique MAC address.

### Avg. Dwell Time Tile

The **Avg. Dwell Time** tile displays the average amount of time in minutes a device is connected to an AP in the selected site, and the increase or decrease in the dwell time from the previous time. An increase in dwell time is displayed as a green number while a decrease is displayed as a red number.

## Utilization and Number of Users Tile

FIGURE 45 Utilization and Number of Users Tile



The **Utilization and Number of Users** tile displays the site utilization and number of users in a time series graph and a heat map. In the time series graph, the utilization rate is displayed as a percentage and the number of users at a time is also displayed. Pause the pointer over the graph for more information. You can choose to view both the utilization rate and user count on the graph or choose only one of them by selecting the check boxes over the graph.

The heat map displays utilization as a percentage and user count per hour, over a 24-hour period, or over a 7-day period, and helps in analyzing these parameters at a glance. You can toggle between the percentage and user count to view either of the parameters. The number of users appears as a set of blue boxes. The depth of the colors for each box can vary and are mapped to the color-range legend atop the heat map. The hour when the user count is high appears as a dark blue box and the hour with the least number of users appears as a light blue box. Pause the pointer over a box to view the corresponding range into which it falls within the color-range legend atop the heat map. Similarly, site utilization appears as a dark red box when at its peak, and the percentage when at its least appears as a light red box.

## Dwell Time Tile

FIGURE 46 Dwell Time Tile



The **Dwell Time** tile displays the dwell time of a client or device for the selected time period as a time series graph, bar graph, and heat map. The time series graph displays the average, maximum, and minimum dwell time information. Pause the pointer over the graph for more information. You can choose to view all the average, maximum, and minimum values on the graph or choose one or two of them by selecting the check boxes over the graph.

The bar graph displays the dwell time distribution over a time range such as the first 15 minutes, the second 15 minutes, from 30 minutes to 60 minutes, from 1 hour to 3 hours, from 3 hours to 8 hours, and 8 hours and longer. Each bar displays the percentage of dwell time for that time period.



The heat map displays the dwell time per hour for the period selected and helps analyze the dwell time of clients at a glance. Dwell time information per hour is displayed as a blue box. The box appears dark blue when dwell time is high and light blue when it is low. Pause the pointer over a box view the corresponding range into which it falls within the color-range legend atop the heat map.

## Clients Table

FIGURE 47 Clients Table

Username	Hostname	MAC Address	IP Address	Total Dwell Time	Max Dwell Time	Min Dwell Time	Avg. Dwell Time	Details	Exclude
185d0f2a6d8	hukas-PC	783d39398c0e	10.174.36.36	33h 15m	23h 15m	23h 15m	23h 15m		
04271902f4	EdvAF-PC	874e119029f0	10.174.36.33	10h 5m	4h 20m	13m	3m		
9e3071589d9	hukas-PC	8870714c0049	10.174.36.28	8h 60m	3h 47m	13m	7h 50m		
2d7fcdad1a9	APDev-PC	2d7fcdad1a9	10.174.36.86	3h 6m	0h 3m	15m	7h 43m		
0830d94515f	SR-V31	0830d94515f	10.174.36.29	2h 20m	1h 8m	2m 46s	37m 16s		
74f5066d6d7	IP-MANAGER	74f5066d6d7	10.174.36.37	22m 51s	15m 23s	7m 20s	11m 28s		
70f909280c5	Unknown	70f909280c5	10.174.36.31	14m 17s	2m 54s	2m 29s	2m 51s		
10481910140	iPhone	10481910140	10.174.36.34	12m 51s	8m 23s	8m 23s	8m 23s		
4284020714d	Android-Phone	4284020714d	10.174.36.32	10m 3s	10m 3s	10m 3s	10m 3s		

MAC Address	Username	Hostname	IP Address	Created At	Include
02015142000c	Unknown	Unknown	10.174.36.65	Jul 04 2021 10:56:05	

The **Clients** table displays information about the top thousand clients. You can use the **Search** field to look for clients by username, hostname, client MAC address, or client IP address. The **Clients** tab displays client information such as the device name, MAC address, IP address, hostname, dwell time (total, average, maximum, and minimum), and contains links to the **Client Details** page and the **Client Troubleshooting** page. Click the Exclude icon (⊖) to remove the selected client from the **Site Report** statistics. After the client is excluded, the client information is removed from the **Clients** tab and populated in the **Excluded Visitors** tab. The list of excluded clients for the site is maintained in this tab. Including or excluding clients updates the graphs, heat maps, bar charts and time series graphs in the tiles of the **Site Report**.

The **Excluded Visitors** tab displays information about the clients that were removed from the analysis, such as the MAC address, username, hostname, and created time. Clicking the Add Back icon (⊕) returns the client back to the **Site Report** for analysis.. The client is also repopulated back into the **Clients** tab by refreshing the information in the charts of the **Site Report**.



# Network Health

---

- [Testing Client Services.....](#) 67
- [Network Health Test Report.....](#) 70

## Testing Client Services

The **Network Health** page allows users to test LAN, WAN and connectivity to application servers with ease. .

APs will emulate as virtual clients and perform the end-to-end connectivity tests (such as EAP, RADIUS, DHCP, DNS, ping, and traceroute) thereby connecting to a Wi-Fi network and the internet thereafter. It also performs speed tests to determine the quality of the connection. This feature therefore offers a comprehensive, end-to-end testing mechanism for users. You can create tests and customize them based on your network requirements. For example, you can create a test to determine network connectivity for a subset of APs within your network. There is no limitation on the number of APs selected to perform these tests. APs continue to serve actual clients while performing these tests. It is important to note that these tests generate test traffic over the wired interface. Mesh APs cannot participate in Network Health tests.

Follow these steps to create a test:

1. From the navigation bar, click **Network Health**.

The **Network Health** page is displayed containing information about the test created earlier such as the test name, number of APs tested, last run time, test results and so on. It also displays the total number of tests created, number of tests that passed and failed, and those that are pending and yet to be run on the network.

**FIGURE 48** Network Health Page

The screenshot shows the 'Network Health' page with a header 'Total Tests: 90' and a 'Learn More' link. A 'Create Test' button is in the top right. The main content is a table with the following columns: Name, APs, Run, Last Run, APs Under Test, and Last Result. The table lists several tests with their respective AP counts and results.

Name	APs	Run	Last Run	APs Under Test	Last Result
dns-check	1 APs		Apr 09 2021 14:05:43	1 APs	0% pass
Offline-check	1 APs		Apr 07 2021 17:54:37	1 APs	0% pass
Offline-unsupported-check	1 APs		Apr 07 2021 14:52:12	1 APs	0% pass
rajiv-hospitality-h550	3 APs		Apr 07 2021 11:10:24	3 APs	0% pass
SV1	1 APs		Apr 05 2021 06:32:57	1 APs	0% pass
SARAVANAN 18 60	1 APs		Mar 31 2021 21:14:22	1 APs	100% pass
597	1 APs		Mar 30 2021 22:59:25	1 APs	0% pass
SARAVANAN-OPEN-2	1 APs		Mar 26 2021 15:25:53	1 APs	0% pass
MLIS33403	3 APs		Mar 24 2021 11:47:49	3 APs	66.67% pass
SARAVANAN-OPEN-CHECK	-		Mar 31 2021 18:21:19	2 APs	0% pass

- **Name:** Displays the name of the test
- **Type:** Select from options such as On-Demand, Daily, Weekly, Monthly. Selecting Daily presents an option to choose the time of the day to run the test. Selecting Weekly presents options to select the day of the week and time for the test while selecting Monthly presents options to select the date of the month and time to run the test.
- **APs:** Displays the number of APs in the zone
- **Run:** Click to run the test
- **Last Run:** Displays the timestamp of the last test run on the AP
- **APs Under Test:** Displays the number of APs that have been tested
- **Last Result:** Displays test success as a percentage. For example, if all the APs within the zone passed the test criteria, then 100% success is displayed as the result. If the test is ongoing, then the status "In progress" is displayed. For example, "In progress... (2 of 16APs tested) "

Click to view the test results.

2. Click **Create Test**.

The **Create Test** page is displayed.

**FIGURE 49** Creating a Test

**CREATE TEST**

TEST NAME

TYPE

On-Demand

Cancel Next

**APs SELECTION**

Network

- 10f-sz07
- 13f-sz07 (All APs selected)
- Alphanet-BDC (All APs selected)
- anindya-vs-z-e-cluster
- BDC-FT-SARAVANAN
- BDC-SARAVANAN-3
- BHN-Scale-SZ300 (All APs selected)
- bugbash
- c1-vs-z-bdc-home-network
- CHANGE-SARAVANAN-FT-100
- CHANGE-SARAVANAN-LET-100

Search... 0 of 0 APs selected

Back Next

**SETTINGS**

WLAN

AUTHENTICATION TYPE

WPA2-Personal

RADIO BAND

2.4 GHz  5 GHz

USERNAME

PRE-SHARED KEY

using configured password

DNS SERVER

Default  Custom

PING DESTINATION ADDRESS

TRACEROUTE DESTINATION ADDRESS

SPEED TEST

Enabled

Back Save

## Network Health

### Network Health Test Report




3. Enter a name for the test
4. Click **Next**. The AP selection page is displayed.
5. Select the APs you want to include to the test from the network.
6. Click **Next**. The **Settings** page is displayed.

Configure the following options:

- **WLAN:** Select the WLAN
  - **Authentication Type:** after the WLAN is created, RUCKUS Analytics automatically selects the authentication method. However, you can still manually select the method as necessary.
  - **Radio Band:** Select the radio frequency that you want to test the APs at - options include 2.4 GHz, 5GHz or both these frequencies
  - **Username:** Enter the username. Some authentication methods such as OpenAuth and WPA2-Personal do not demand entry of login credentials but others such as WISPr and Web Authentication would require you to enter your login credentials. For some authentication methods such as Guest Access, the username is already populated requiring only password entry.
  - **Password:** Enter the password
  - **DNS:** Select one of the options - Default or Custom to assign IP address to APs
  - **Ping Destination Address:** Enter the IP address (internal or external) or URL of the ping destination
  - **Traceroute Destination Address:** Enter the IP address or URL of the traceroute destination
7. Click **Save** to save the test configuration.

After the test is created, it is displayed in the **Network Health** page.

You can click **Run** to run the test to determine the network connectivity. After you run the test, results of the test are displayed under **Last Result**.

Click the **Clone**, **Edit** and **Delete** icons respectively to clone the test, edit test configuration options and to delete it (    ). You can only edit the test that you create.

## Network Health Test Report

The **Network Health** test report provides granular information about the test result which aids in better network analysis. It provides a step-by-step analysis of the various connection stages the AP has to go through before establishing network connectivity, there by, being able to identify the reason for failure or error if there is one.

The **Network Health** Report consists of the following components:

- Overview tab
- Details tab

### NOTE

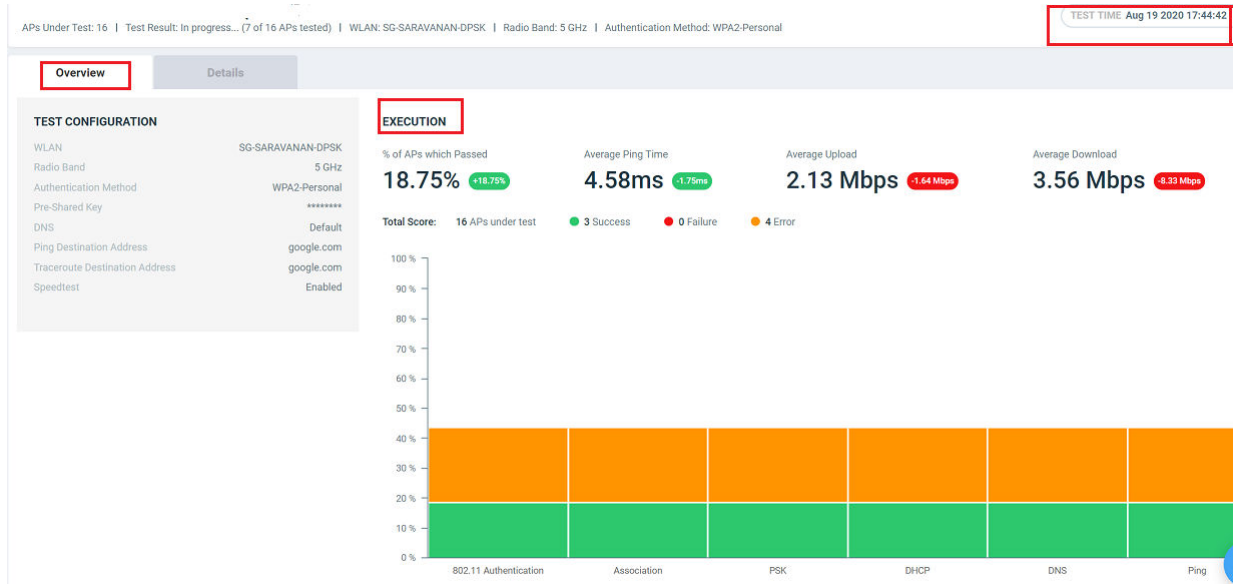
One year is the data retention period for all Network Health tests and reports.

## Overview Tab

The **Overview tab** of the **Network Health** Report displays information about the test configuration that was used while creating the test. The Execution section displays information about the average ping time in ms, upload and download speeds in Mbps, and percentage of APs within that zone that passed the test criteria. In this report, only 3 out of the 16 APs passed the test, therefore the **% of APs which Passed** is displayed as 18.75%. Additionally, a small capsule is displayed next to these values which displays the values derived by comparing current values with the results from the previous test. If the values improved compared to previous test results, the capsule is displayed green and colored red if current

values were lower than the previous one. For example, in this report, we can interpret that the average ping time has reduced by 1.75ms when compared to the previous result. Therefore, the capsule is colored green.

FIGURE 50 Network Health Report: Overview Tab



**Total Score** displays the total number of APs being tested and their status. Following statuses are displayed:

- Success (green)
- Failure (red)
- Error (orange)

**NOTE**

Test success is achieved only when the AP passes all the tests for each connection tests such as 802.11 Authentication, Association, PSK, DHCP, DNS, and Ping.

For example, in this report, only 3 out of 16 APs in the zone passed the test, no APs failed and 4 APs showed errors. An error is usually displayed when the test cannot be performed, for example, when an AP is unavailable or unresponsive.

The **Test Time** field on the top-right corner of the page displays a log of all the previous tests that were executed with details about the test status and a links to the test reports.

FIGURE 51 Test Time Log

TEST TIME Aug 19 2020 17:44:42					
APs Under Test	Success	Failure	Error	Test Time	Links
16	3	0	4	Aug 19 2020 17:44:42	
16	0	1	1	Aug 19 2020 17:40:23	
16	2	1	0	Aug 19 2020 17:35:39	
16	1	1	0	Aug 19 2020 17:20:54	
1	1	0	0	Aug 06 2020 16:46:31	
1	0	1	0	Aug 06 2020 16:46:08	
1	1	0	0	Aug 06 2020 16:45:38	
1	0	1	0	Aug 06 2020 16:40:35	

## Details Tab

The **Details tab** of the **Network Health Report** displays detailed information about the status of the authentication stages.

FIGURE 52 Network Health Report: Details Tab

Overview		Details								
AP Name	AP MAC	802.11 Auth	Association	PSK	DHCP	DNS	Ping	TraceRT	Upload	Download
RuckusAP	0C:F4:D5:07:C2:70	Pending	Pending	Pending	Pending	Pending	Pending		Pending	Pending
RuckusAP	E8:1D:A8:17:62:F0	Error	Error	Error	Error	Error	Error		Error	Error
RuckusAP	EC:58:EA:22:66:20	Pending	Pending	Pending	Pending	Pending	Pending		Pending	Pending
RuckusAP	F0:B0:52:28:B6:90	Pending	Pending	Pending	Pending	Pending	Pending		Pending	Pending
RuckusAP	18:4B:0D:24:5F:50	Pass	Pass	Pass	Pass	Pass	19.3ms		8.21 Kbps	19.1 Kbps
RuckusAP	24:79:2A:1C:12:80	Error	Error	Error	Error	Error	Error		Error	Error
RuckusAP	84:18:3A:09:CF:90	Pending	Pending	Pending	Pending	Pending	Pending		Pending	Pending
RuckusAP	8C:FE:74:27:B4:F0	Pass	Pass	Pass	Pass	Pass	10.9ms		7.17 Kbps	7.94 Kbps
RuckusAP	B4:79:C8:12:8C:50	Error	Error	Error	Error	Error	Error		Error	Error

The **Details Tab** of the **Network Health Report** displays the following:


- AP Name: Displays the name of the AP
- AP MAC: Displays the MAC address of the AP
- 802.11 Auth: Displays that status of the 802.11 authentication test

**NOTE**

For all tests, the status includes Pass, Fail, Error, and Pending. You can pause the pointer over the test status capsule to know more about the reason for success, failure, or error.



- Association: Displays that status of the Association authentication test
- PSK: Displays that status of the PSK authentication test
- DHCP: Displays that status of the DHCP authentication test
- DNS: Displays that status of the DNS authentication test
- Ping: Displays that status of the Ping authentication test. The time taken for the ping response is also recorded in ms in the capsule.
- Traceroute: Displays the traceroute details such as number of network hops, time taken between hops for successful ping operations.

Pause the pointer over the tarceroute icon (  ) for more information. It is enabled only when all authentication stages are passed successfully.

- Upload: Displays the upload speed of the network. **Timeout** is displayed if the speed test times out for some reason.
- Download: Displays the download speed of the network. **Timeout** is displayed if the speed test times out for some reason.



# Testing Video Call Quality

- [Video Call QoE Workflow](#)..... 75
- [Creating a Test Call](#)..... 76
- [Video Call Test Report](#)..... 78

The **Video Call QoE** page allows network administrators to test the quality of video calls made through applications, such as Zoom, over the Wi-Fi network.

Because video calls have high bandwidth requirements, they are susceptible to issues such as latency and jitters which can be analyzed and resolved with the help of video call testing. The test results are captured in a report, which provides insight into various network parameters, pointing to potential corrective action that can enhance video quality.

The **Video Call QoE** page displays information about the test calls created, such as the status of the calls, the number of participants, the creation time and end time of the call, the quality of experience (QoE), and a link to the report. If the QoE of a call is good, a green dot is displayed in the **QoE** column. If the QoE is poor, a red dot is displayed.

**FIGURE 53** Video Call QoE Page

The screenshot shows the RUCKUS Analytics interface for the Video Call QoE page. The page title is "Video Call QoE" with a sub-header "Total Test Calls: 233". A "Create Test Call" button is visible in the top right. The main content is a table with the following columns: Name, Created Time, Start Time, No. of Participants, Status, and QoE. The table contains several rows of test call data.

Name	Created Time	Start Time	No. of Participants	Status	QoE
xyxocm	Apr 22 2021 19:15:07	-	-	Invalid	-
MinimaticTestingforaudio+video	Apr 22 2021 09:34:19	Apr 22 2021 09:35:43	2	Ended	Good
Testingforaudio+video	Apr 22 2021 09:08:53	Apr 22 2021 09:10:22	2	Ended	Good
Z2m7dx-Nocudio+Novideo try	Apr 22 2021 09:32:15	Apr 22 2021 09:34:10	2	Invalid	-
Z2m7dx-Nocudio+Novideo	Apr 22 2021 06:51:21	Apr 22 2021 06:51:10	2	Ended	Good
Sujirya	Apr 22 2021 02:04:10	-	-	Invalid	-
sarawanen-18-18-57:53	Apr 21 2021 23:41:59	-	-	Invalid	-
sara-18-57:53	Apr 21 2021 23:11:24	Apr 21 2021 23:11:38	2	Invalid	-
corovanan 5253	Apr 21 2021 22:46:59	Apr 21 2021 22:47:29	2	Ended	Poor
testingforvideo+audio	Apr 21 2021 18:43:47	Apr 21 2021 18:44:02	2	Ended	Poor

## Video Call QoE Workflow

You can run a video call QoE test by following the steps listed in [Creating a Test Call](#)

After the test call is completed, a test call report is generated after approximately 8 to 10 minutes. For more information, refer to [Video Call Test Report](#) on page 78. You can click the icon to view the report.

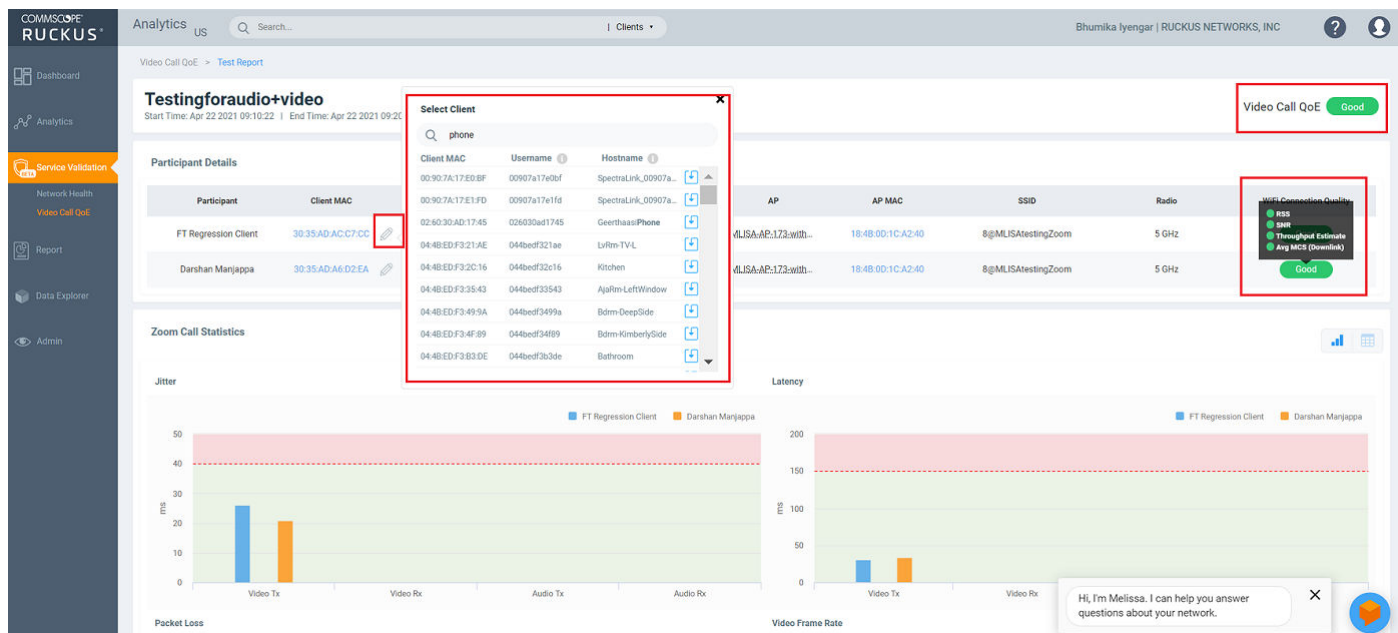
In the report, select the client MAC address of the participants to view the video call QoE. If the call quality is good, the Video Call QoE displays in a green capsule. If the call quality is poor, it appears in a red capsule. Wi-Fi connection quality directly impacts the video call QoE. If the Wi-Fi connection quality of both participants is good, the video call QoE is good, and vice versa. Wi-Fi connection quality is influenced by various factors, such as RSSI, SNR, throughput estimate, and average MCS (downlink).

Selecting the client MAC address displays the [Client Troubleshooting Page](#) on page 58 and clicking the AP MAC address displays the [AP Details Report](#) on page 129.

## Testing Video Call Quality

### Creating a Test Call

FIGURE 54 Selecting the Client MAC Address and Viewing Video Call QoE



## Creating a Test Call

Complete the following steps to create a test call.

1. From the navigation bar, click **Video Call QoE**.
2. Click **Create Test Call**.

### NOTE

Only network administrators can create test calls and these calls can be attended only by clients within the RUCKUS Wi-Fi network.

3. In **Test Name**, enter the name for the test you wish to perform.

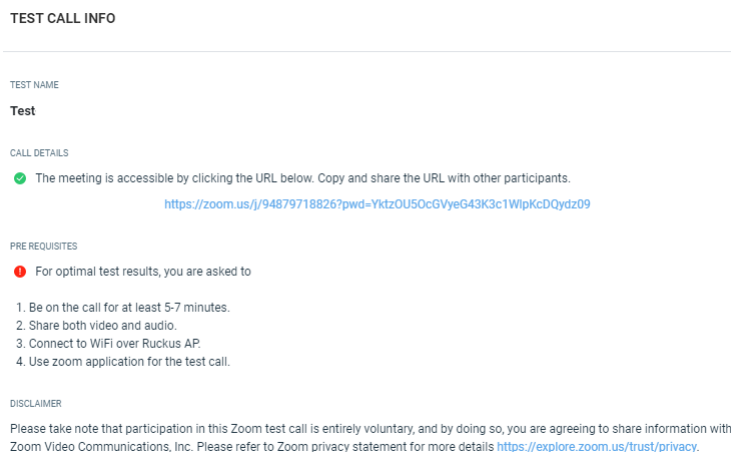
4. Click **Create**.

A **Test Call Info** page is displayed containing information about the test name, a link to make the Zoom call, and prerequisites. Clicking the link takes you to the Zoom Meeting web user interface. As with any Zoom meeting, you can edit the audio and video settings, chat with participants (only two in this case), record the meeting, use the reactions icons, share the screen, and so on.

Only two participants are allowed on the call and they must join the call immediately. For best analysis, both participants must be on the call for at least five minutes, enabling audio and video features on the call.

The MAC address of the participants must be added manually every time a report is generated. Reports are not generated if both participants are connected through a wired network or if no participants join the meeting.

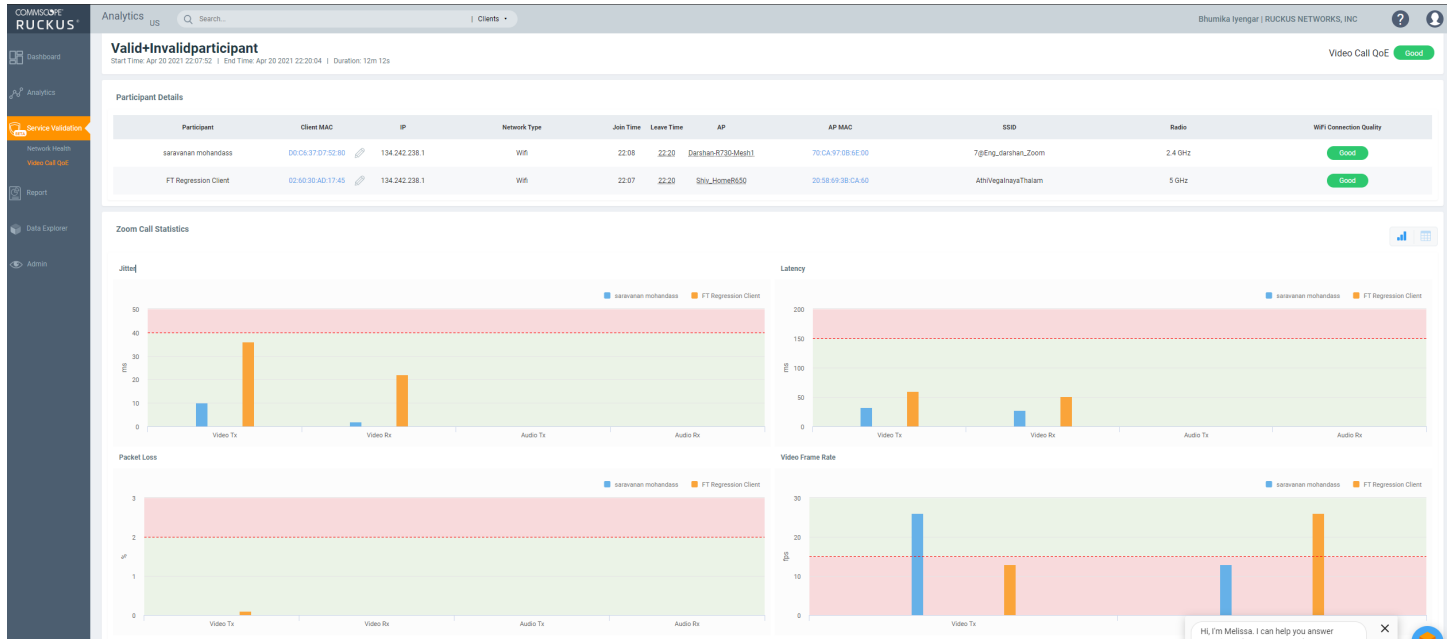
**FIGURE 55** Sample Test Call Info Page



# Video Call Test Report

You can collect video call metrics from the test report and analyze them to improve call quality. Quality metrics such as jitter, latency, packet loss, and video frame rate are displayed in addition to call details. This information is displayed for both participants in the call.


FIGURE 56 Video Call Report



The **Video Call Report** contains the following components:

- Participants Details table
- Zoom Call Statistics tile

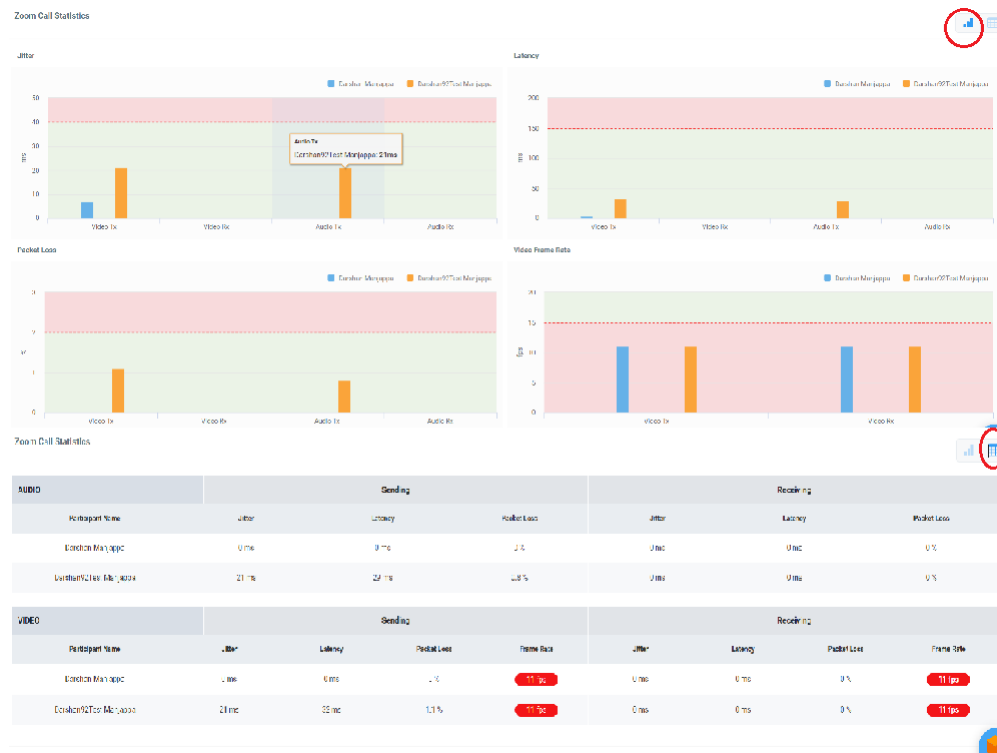
## Participants Details Tile

The **Participants Details** tile displays exhaustive information about the call, such as the participant name, client MAC address, IP address, client MAC address, network type, duration of the call, AP name and MAC address, SSID, radio frequency, Wi-Fi connection quality, and so on. You can select the MAC address of the client by clicking the (edit icon) . You can also pause the pointer over the status capsule in the **Wi-Fi Connection Quality** column for more information about RSS, SNR, throughput estimate, and average MCS (downlink). A video call of good quality is displayed as a green capsule in the **Wi-Fi Connection Quality** column, and a poor quality call is displayed as a red capsule. You must click the edit icon, and select the client for each participant to view the Wi-Fi statistics.

## Zoom Call Statistics Tile

The **Zoom Call Statistics** tile provides a graph or table representation of jitters, latency, packet loss, and video frame rate experience in the call.

FIGURE 57 Zoom Call Statistics: Graph and Table Views



- **Jitter:** This graph displays jitters produced during the call in milliseconds (ms) for both participants for the duration of the call. The participant with lower jitter values experienced better call quality. You can also select the check box next to the participant name to view data only for the selected participant. By default, data pertaining to both participants is displayed.
- **Latency:** This graph displays latency (delay) produced during the call in milliseconds (ms) for both participants for the duration of the call. The participant with lower latency values experienced better call quality because there was minimum or no delay in audio and video transmission. You can also select the check box next to the participant name to view data only for the selected participant. By default, data pertaining to both participants is displayed.
- **Packet Loss:** This graph displays the percentage of data packets lost during video and audio transmission for both participants. The participant with lower values experienced better call quality because there was minimum or no data loss during audio and video transmission. You can also select the check box next to the participant name to view data only for the selected participant. By default, data pertaining to both participants is displayed.
- **Video Frame Rate:** This graph displays the number of video frames transmitted and received between both participants during the call. If the video call was successful for both participants, these values will be the same. The participant with lower frames per second experiences poor video quality. You can also select the check box next to the participant name to view data only for the selected participant. By default, data pertaining to both participants is displayed.





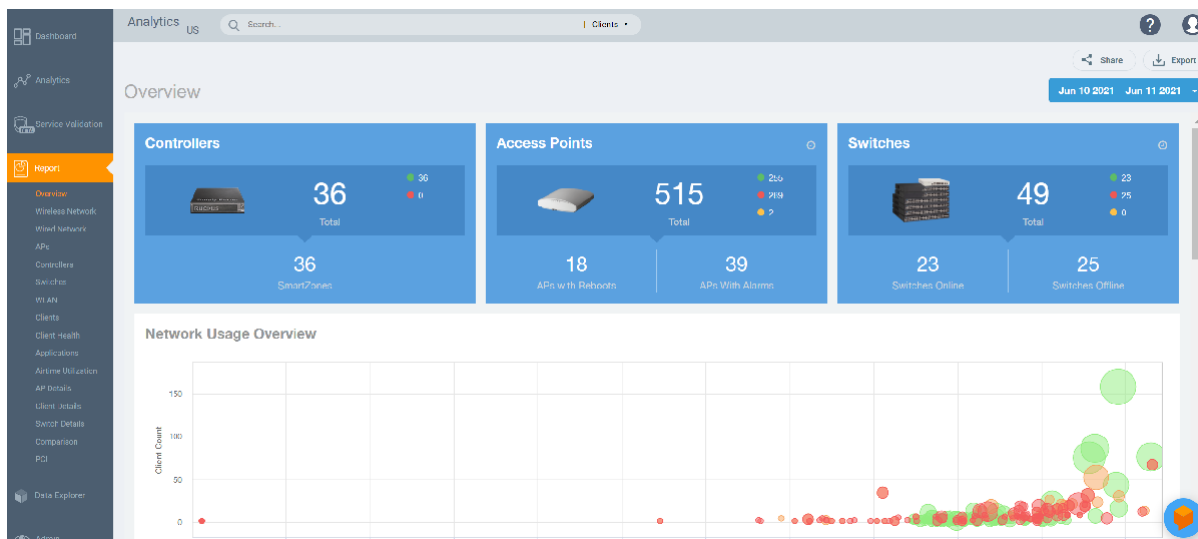
# Report

- Using the Overview Dashboard: Content Panel..... 81
- Wireless Network Report..... 83
- Wired Network Report..... 89
- Inventory - APs Report..... 94
- Inventory - Controllers Report..... 103
- Inventory - Switches Report..... 106
- WLAN Report ..... 110
- Clients Report..... 115
- Client Health Dashboard..... 119
- Applications Report..... 123
- Airtime Utilization Report..... 125
- AP Details Report..... 129
- Client Details Report..... 139
- Switch Details Report Dashboard..... 143
- Comparison Reports Dashboard..... 147
- PCI Profiles..... 150

## Using the Overview Dashboard: Content Panel

The Overview Dashboard is the main page displayed from the **Report** menu. It provides an overview of some important statistics of your Wi-Fi network.

**FIGURE 58** Overview Dashboard : Top Portion



The top right corner of the Reports pages display options to share and export reports in PDF and CSV formats. You can also share them with recipients over e-mails on-demand or periodically by configuring a schedule (daily, weekly and monthly).

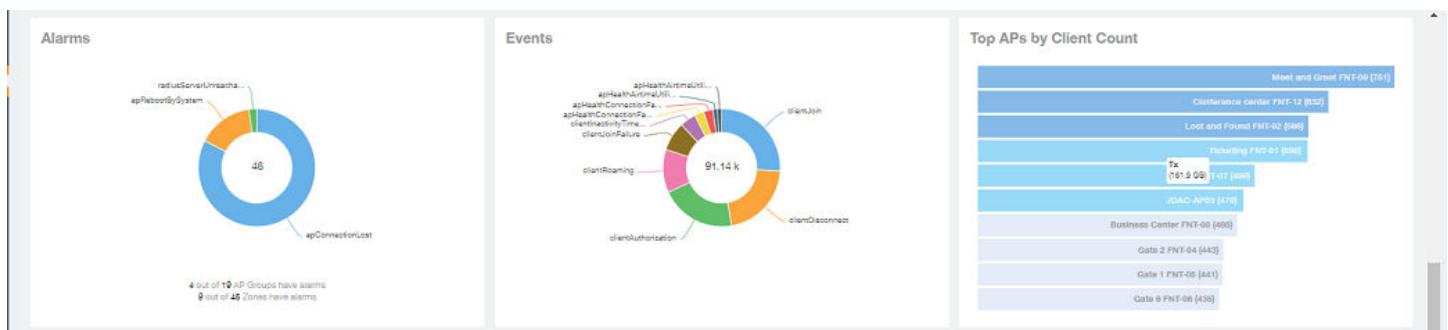
## Report

### Using the Overview Dashboard: Content Panel

The top portion of the **Overview Dashboard** shows the following tiles:

- **Controller:** Displays the number of controllers being used in your Wi-Fi network. The green and red dots show the number of active (green) and inactive (red) controllers.
- **Access Points:** Shows the number of APs in the network. The green, red, and yellow dots show the number of active APs (green), inactive APs (red), and provisioned, in discovery, or rebooting APs (yellow).
- **Switches:** Shows the number of switches in the network. The green, red, and yellow dots show the number of active switches (green), inactive switches (red), and provisioned, in discovery, or rebooting switches (yellow).
- **Network Usage Overview:** Shows the relationship between the number of clients and the total traffic in the network. The bubble chart contains bubbles of different colors that indicate different dimensions of the network, including application, domain, OS type, zone, AP, system, AP group, switch, and SSID. Pause the pointer on an individual bubble to display the number of connected clients and traffic information. Bubble sizes vary depending on their values (except for APs and Switches).

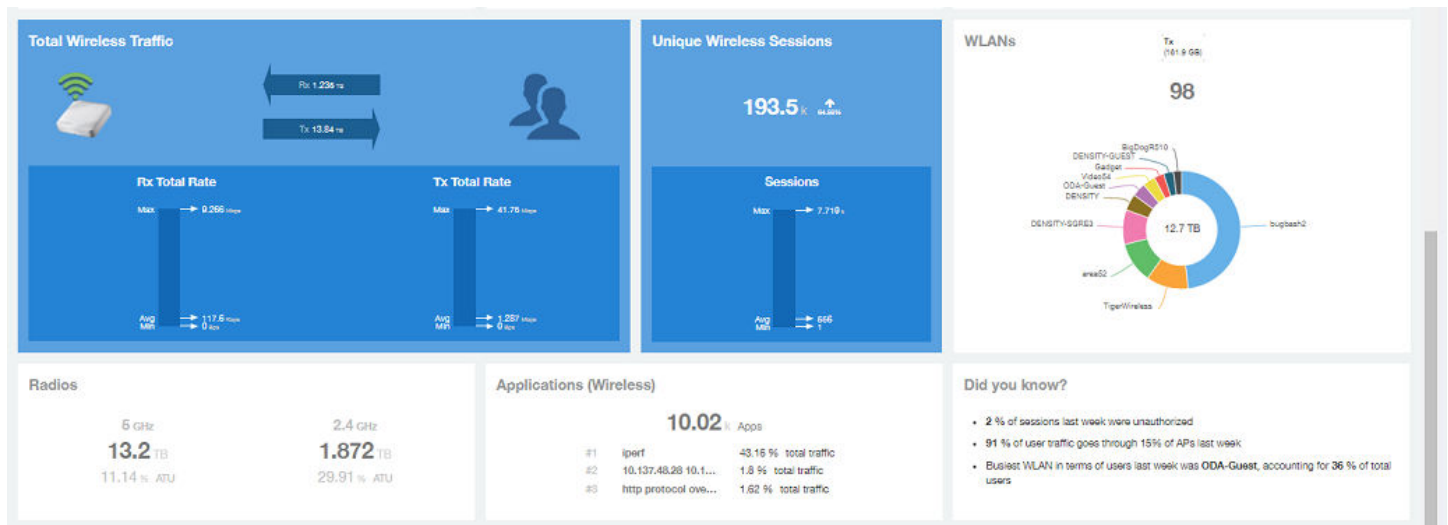
**FIGURE 59** Overview Dashboard: Middle Portion



The middle portion of the **Overview Dashboard** shows the following tiles:

- **Alarms:** Displays the most frequently occurring alarms in the network. Pause the pointer over a color or name to display the full name of the alarm. Go to the Data Explorer dashboard for more information about alarms.
- **Events:** Displays the most frequently occurring events in the network. Pause the pointer over a color or name to display the full name of the event. Go to the Data Explorer dashboard for more information about events.
- **Top APs by Client Count:** Displays the APs being accessed by the most clients. This information is also represented in more detail in the **Wireless Report**.

FIGURE 60 Overview Dashboard: Lower Portion



The lower portion of the **Overview Dashboard** shows the following tiles:

- **Total Traffic:** Shows statistics about traffic received and transmitted by the access points, including the maximum and minimum rates of traffic. Go to the **Wireless Report** for more information about traffic.
- **Total Unique Sessions:** Shows the number of IEEE 802.11 sessions between all clients and APs on the network. Go to the Data Explorer dashboard for more information about sessions.
- **WLANs:** Displays the top SSIDs by traffic, which is also shown in the **WLANs Report**. Pause the pointer over a portion of the donut display to obtain more information about each SSID.
- **Radios:** Displays client data usage, in terabytes, for both the 2.4 GHz and 5.0 GHz networks. For more information about radios, go to the **Airtime Utilization Reports**.
- **Applications:** Shows the applications being used more frequently by the clients in the network. For more information about applications usage, go to the **Applications Reports**.
- **"Did you know?":** Provides a short, bulleted list about your system, such as the average duration of a session for a week, or the busiest SSID. The "Did you know?" section is updated every time you return to the **Overview Dashboard**.

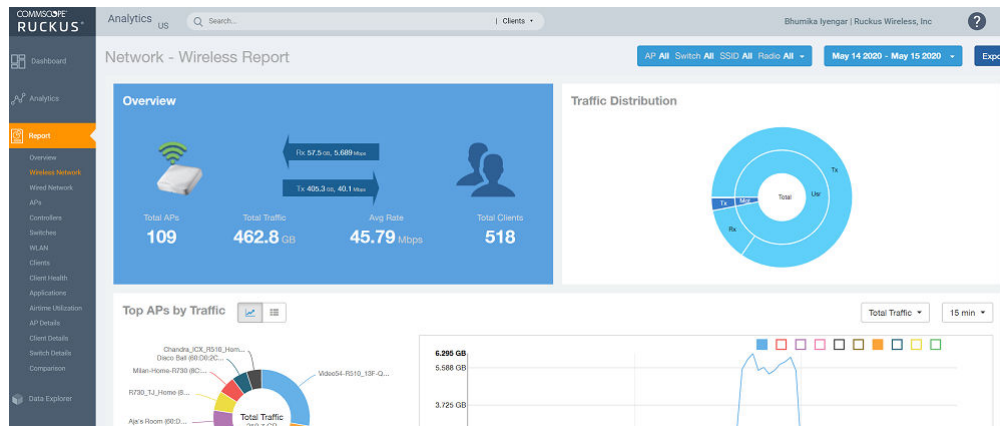
## Wireless Network Report

The **Wireless Network Report** provides details of traffic, clients, and trends by APs, SSIDs, radio, or clients over time.

From the navigation bar, select **Report > Wireless Network**.

The following figure shows only the upper portion of the **Wireless Network Report** update.

FIGURE 61 Wireless Network Report (Upper Portion Only)



The **Wireless Network Report** consists of the following components:

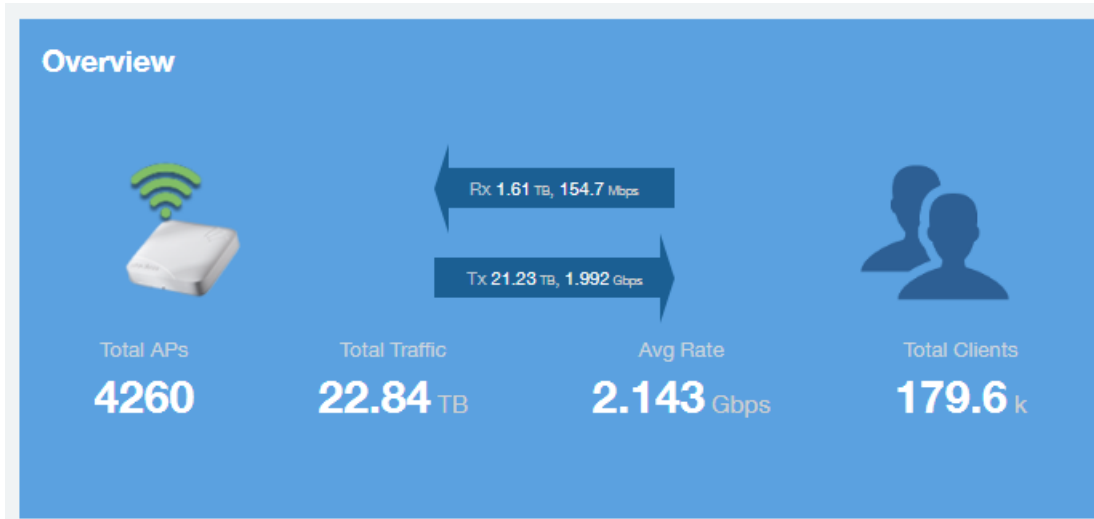
- Overview tile
- Traffic Distribution chart
- Top APs by Traffic tile
- Top APs by Client Count graph
- Traffic Trend graphs
- Traffic Over Time graph

## Overview Tile

The **Overview** tile of the **Wireless Network Report** provides a general overview of the entire network. It displays the following information, based on your selection of APs, SSID, radio, and date range filters.

- Total number of APs
- Total traffic and the average traffic rate
- Total traffic received and transmitted and the average traffic rate
- Total number of clients on the network

FIGURE 62 Wireless Network Report: Overview Tile



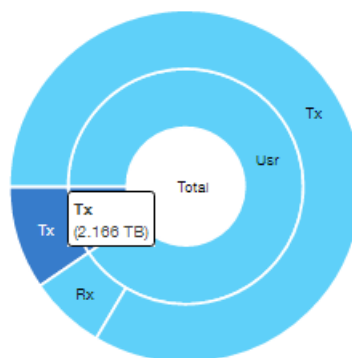
## Traffic Distribution Tile

The **Traffic Distribution** donut chart displays the distribution of traffic types. Use this chart to display management traffic compared to user traffic, for example, based on your selection of APs, SSID, radio, and date range filters.

- Tx = Transmitted traffic
- Rx = Received traffic
- Mgmt = Management traffic
- Usr = User traffic
- Total = Total of all traffic

FIGURE 63 Wireless Network Report: Traffic Distribution Tile

### Traffic Distribution



## Top APs by Traffic Tile

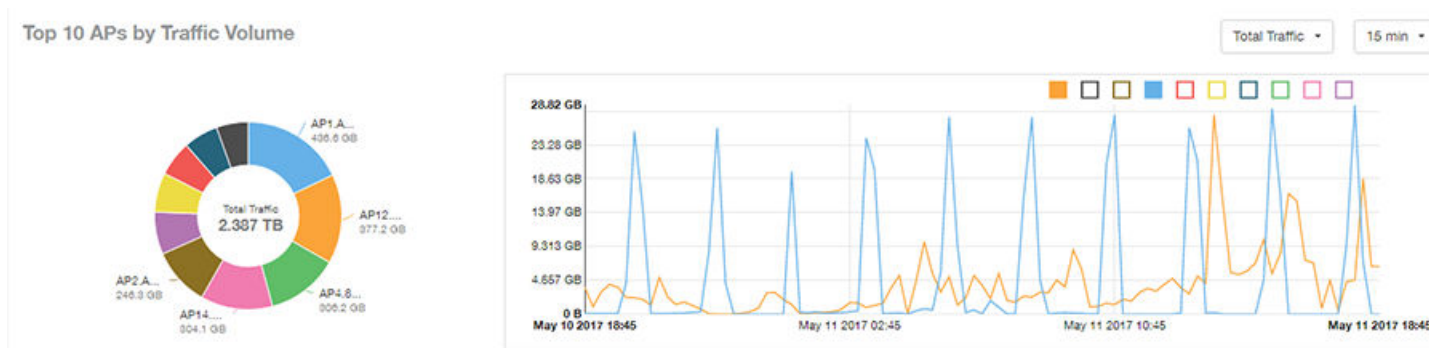
The Top APs by Traffic tile contains a donut chart and a graph. The donut chart and graph displays the APs with the highest traffic volume in the network.

In the tile, use the menus to specify the traffic type (Tx, Rx, or Tx+Rx) and the time period. Click any of the colored squares to display the selected AP details in the line graph.

**NOTE**

The **Traffic Type** menu applies to both the donut chart and the line graph, but the time period applies to the line graph only. This restriction applies to all reports that appear in this format (a donut chart and line graph with the Rx-Tx traffic type and a time period menu).

FIGURE 64 Wireless Network Report: Top APs by Traffic (Chart and Graph)



**NOTE**

If you pause the pointer over the line graph, an information box is displayed containing the selected AP details.

In the **Top APs by Traffic** table, you can view a list of the APs with the highest traffic volume, sorted according to the selected table columns. Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column.

You can select whether to display the top 10, 20, 50, or 100 APs by traffic volume from the filter. The number of rows per page can be defined using the **Rows per page** option in the table settings menu. Use the chart and table icons (📊 📄) to toggle between the chart and table views.

FIGURE 65 Wireless Network Report: Top APs by Traffic (Table)

Top APs by Traffic These APs consume 10.45 % ( 2.387 TB ) of the total traffic ( 22.84 TB ). Top 10 APs

Index	AP Name	AP IP Address	Controller Name	Rx Total	Tx Total	Total Traffic	Clients	⚙️
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	731.1 MB	436.9 GB	436.6 GB	53	
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName2	10.84 GB	366.3 GB	377.2 GB	119	
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName3	20.73 GB	265.5 GB	306.2 GB	42	
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName4	7.841 GB	296.3 GB	304.1 GB	82	
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName5	8.963 GB	237.3 GB	246.3 GB	91	
6	Your_Co_APName6	10.x.y.6	Your_Co_CTName6	4.222 GB	174.5 GB	178.7 GB	255	
7	Your_Co_APName7	10.x.y.7	Your_Co_CTName7	4.47 GB	161.5 GB	166 GB	28	
8	Your_Co_APName8	10.x.y.8	Your_Co_CTName8	10.01 GB	138.7 GB	148.7 GB	67	
9	Your_Co_APName9	10.x.y.9	Your_Co_CTName9	3.707 GB	142.7 GB	146.4 GB	39	
10	Your_Co_APName10	10.x.y.10	Your_Co_CTName10	2.9 GB	131.3 GB	134.2 GB	120	

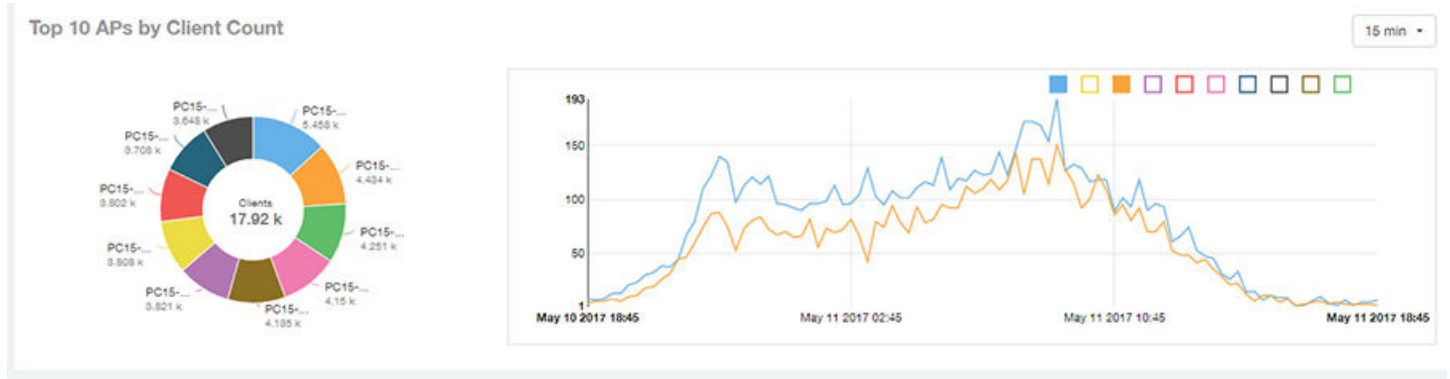
⏪ 1 of 1 ⏩

## Top APs by Client Count Tile

The **Top APs by Client Count** tile contains a donut chart and a graph. The donut chart and graph along display the APs with the most clients on the network.

In the tile, use the menu to specify the time period of 15 minutes, 1 hour, or 1 day. If you pause the pointer over the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected AP details in the line graph.

FIGURE 66 Wireless Network Report: Top APs by Client Count (Chart and Graph)



In the **Top APs by Client Count** table, click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10, 20, 50, or 100 APs count from the table settings menu. The number of rows per page can be defined using the **Rows per page** option in the table settings menu. Use the chart and table icons (📊 📄) to toggle between the chart and table views.

FIGURE 67 Wireless Network Report : Top APs by Client Count (Table)

Top APs by Client Count

These APs consume 0.14 % (32.15 GB) of the total traffic (22.84 TB). Top 10 APs

Index	AP Name	AP IP Address	Controller Name	Clients	Rx Total	Tx Total	Total Traffic
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	5,458 k	288.9 MB	2,416 GB	2,698 GB
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName2	4,434 k	323.9 MB	1,171 GB	1,487 GB
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName3	4,251 k	1,528 GB	989.4 MB	2,474 GB
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName4	4,115 k	190.3 MB	1,961 GB	2,147 GB
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName5	4,135 k	363.1 MB	4,182 GB	4,536 GB
6	Your_Co_APName6	10.x.y.6	Your_Co_CTName6	3,821 k	289.3 MB	826.4 MB	1,092 GB
7	Your_Co_APName7	10.x.y.7	Your_Co_CTName7	3,808 k	569.6 MB	13.12 GB	13.68 GB
8	Your_Co_APName8	10.x.y.8	Your_Co_CTName8	3,802 k	254.3 MB	1,049 GB	1,297 GB
9	Your_Co_APName9	10.x.y.9	Your_Co_CTName9	3,708 k	169.9 MB	583.9 MB	753.8 MB
10	Your_Co_APName10	10.x.y.10	Your_Co_CTName10	3,648 k	155.9 MB	1.85 GB	2,003 GB

## Traffic Trend Graphs

The **Traffic Trend** graphs of the **Wireless Network Report** display the traffic by usage and radio over time.

If you pause the pointer over the line graph, an information box is displayed containing the selected AP details.

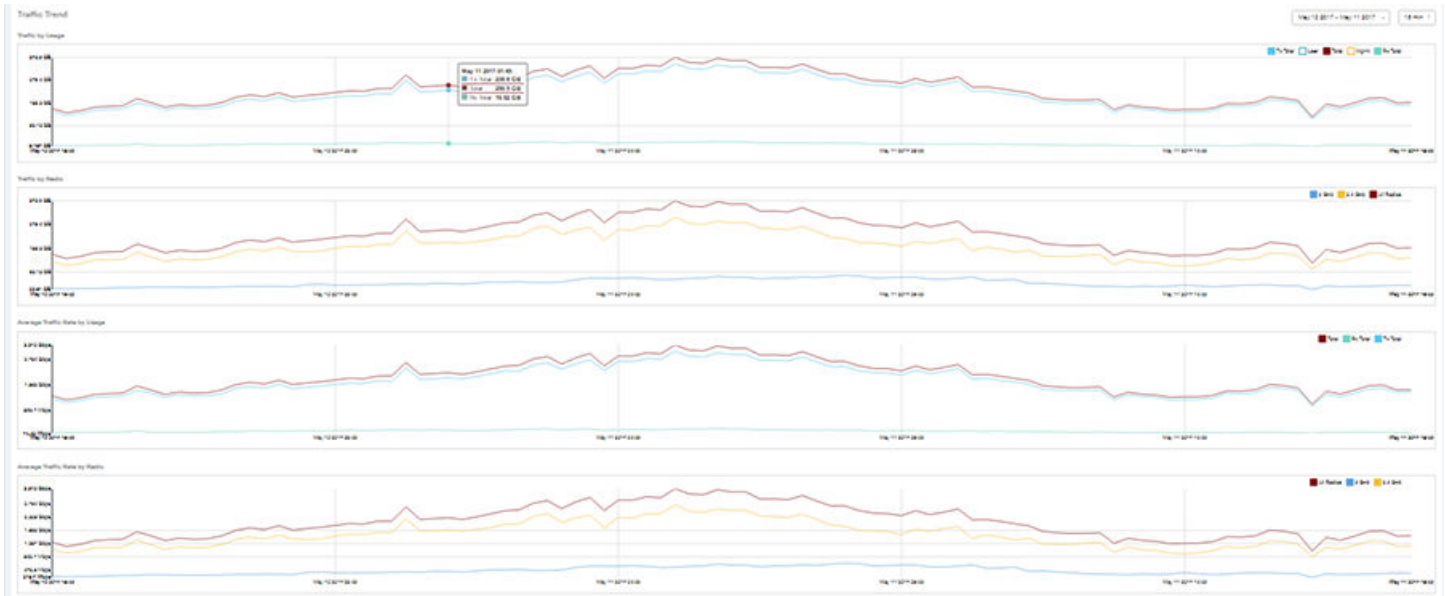
## Report

### Wireless Network Report

**Traffic by Usage:** You can select the traffic by usage details from the check boxes listed in the legend on top of the graph: user, total received traffic, total transmitted traffic, the total received and transmitted traffic, and the management traffic. You can select a date range or a specific date on the line graph. You can specify a time period.

**Traffic by Radio:** You can select the traffic by the following radio details from the check boxes listed in the legend on top of the graph: 5 GHz, 2.4 GHz, and total traffic by radio details. You can select a date range or a specific date on the line graph. These options apply to the corresponding average traffic rate graphs as well.

**FIGURE 68** Wireless Network Report: Traffic Trend Graphs



## Traffic Over Time Table

The **Traffic Over Time** table of the **Wireless Network Report** allows you to compare traffic over multiple time periods.

Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column.



FIGURE 69 Wireless Network Report: Traffic Over Time Table

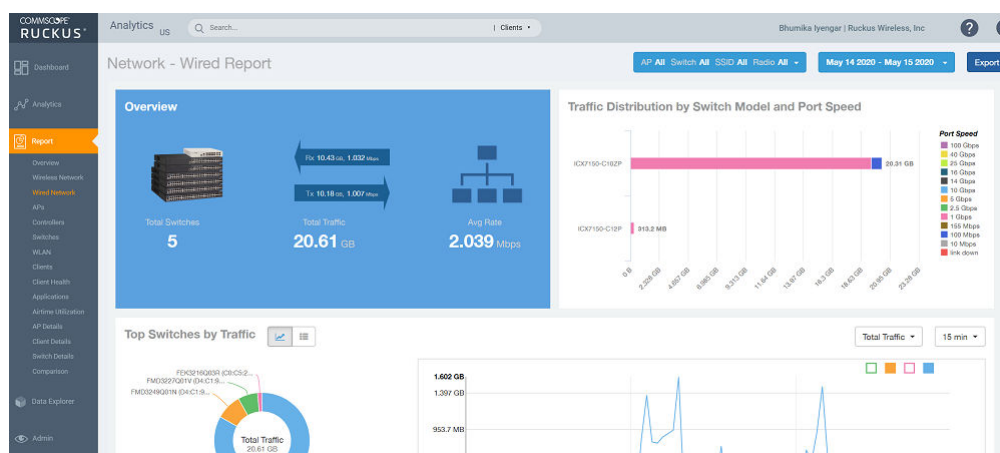
Time Period	2.4 GHz	5 GHz	Rx Total	Tx Total	Total Traffic	Clients
May 10 2017 18:45 - 18:59	134.2 GB	28.65 GB	11.67 GB	151.2 GB	162.9 GB	9,069 k
May 10 2017 19:00 - 19:14	119.6 GB	26.39 GB	11.17 GB	134.8 GB	146 GB	10.22 k
May 10 2017 19:15 - 19:29	126.1 GB	28.09 GB	11.34 GB	142.9 GB	154.2 GB	10.41 k
May 10 2017 19:30 - 19:44	140.5 GB	27.97 GB	12.32 GB	156.1 GB	168.4 GB	10.69 k
May 10 2017 19:45 - 19:59	141.8 GB	30.01 GB	12.89 GB	158.9 GB	171.6 GB	10.78 k
May 10 2017 20:00 - 20:14	142.3 GB	31.95 GB	12.47 GB	161.7 GB	174.2 GB	10.76 k
May 10 2017 20:15 - 20:29	171 GB	32.49 GB	18.18 GB	165.3 GB	203.4 GB	11.15 k
May 10 2017 20:30 - 20:44	151.8 GB	34.87 GB	12.3 GB	174.4 GB	186.7 GB	11.67 k
May 10 2017 20:45 - 20:59	134.5 GB	33.98 GB	11.79 GB	156.7 GB	168.5 GB	12.19 k
May 10 2017 21:00 - 21:14	145.1 GB	33.59 GB	11.84 GB	166.8 GB	178.7 GB	12.37 k

## Wired Network Report

The **Wired Network Report** provides details of total traffic, APs, and clients on the network. It also contains information regarding the received and transmitted traffic between them.

From the navigation bar, select **Report > Wired Network**.

FIGURE 70 Wired Network Report (Upper Portion Only)



The **Wired Network Report** consists of the following components:

- Overview tile
- Traffic Distribution by Switch Model and Port Speed tile
- Top Switches by Traffic tile
- Top Switches by PoE Usage tile
- Top Switches by Errors tile
- Traffic Trend tile

## Report

### Wired Network Report

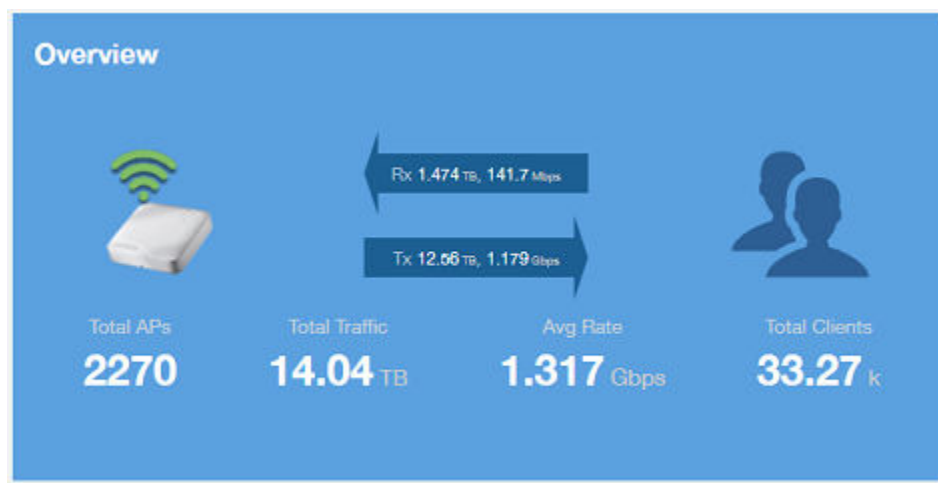
- Error Trend tile

## Overview Tile

The Overview tile of the **Wired Network Report** provides the following information, based on your selection of the AP, SSID, Radio, and Date Range filters:

- Total number of APs
- Total traffic and the average traffic rate
- Total traffic received and transmitted and the average traffic rate
- Total clients on the network

**FIGURE 71** Wired Network Report: Overview Tile

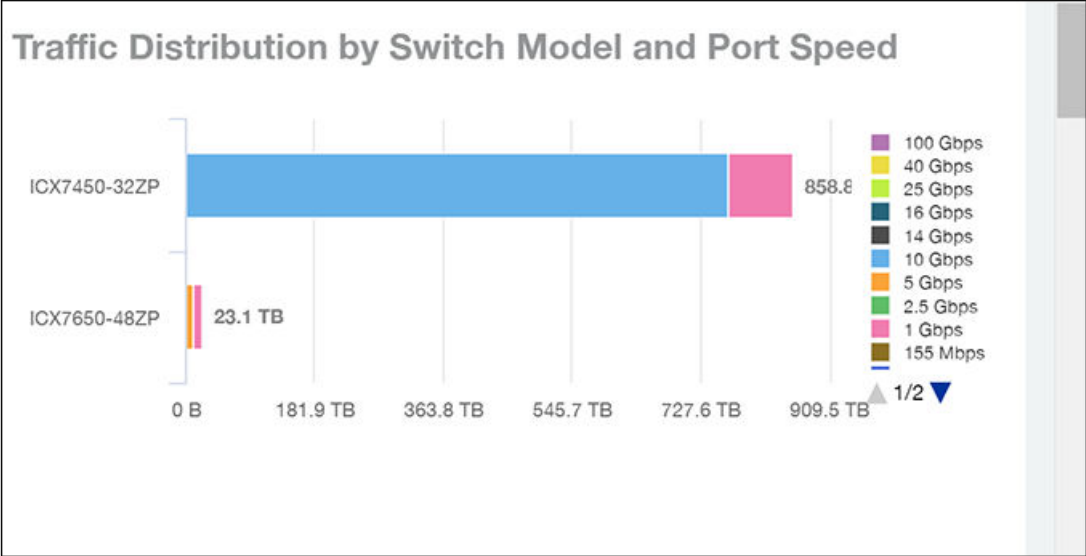


## Traffic Distribution by Switch Model and Port Speed Chart

The **Traffic Distribution by Switch Model and Port Speed** chart of the **Wired Network Report** displays the distribution of traffic by port speed for each switch model being used.

Use this chart to display traffic distribution based on your selection of APs, SSID, Radio, and Date Range filters.

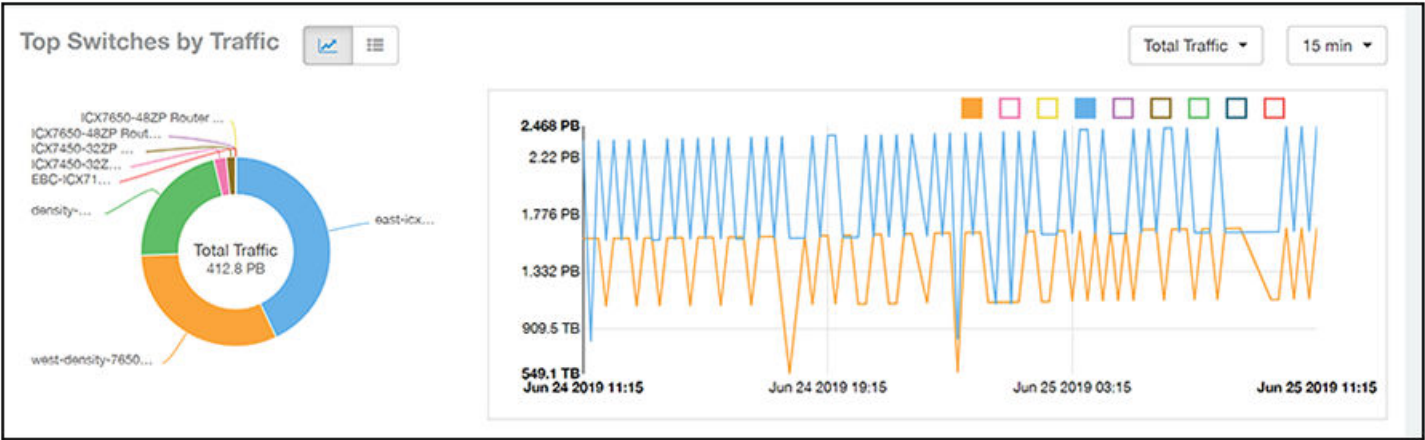
FIGURE 72 Wired NetworkReport: Traffic Distribution by Switch Model and Port Speed Chart



### Top Switches by Traffic Tile

The **Top Switches by Traffic** donut chart and graph of the **Wired Network Report** display which wired switches have the most traffic. You can use the traffic menu to show total traffic, transmitted traffic only, or received traffic only; and use the time menu to specify the time granularity. If you pause the pointer over the donut chart or the line graph, an information box is displayed containing the details on the selected data points. You can click one of the areas of the donut chart to go to the Switch Details dashboard for the corresponding switch. Click any of the colored squares to display the selected switch details in the line graph.

FIGURE 73 Wired Network Report Top Switches by Traffic Tile



Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10 (default value), 20, 50, or 100 switches to display, or display all of the switch models. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 74 Wired Network Report Top Switches by Traffic Table

Top Switches by Traffic 🔍 ☰ These Switches consume 100 % ( 412.8 PB ) of the total traffic ( 412.8 PB ). Top 10 Switches ▾

Index	Switch Name	Rx	Tx	Total Traffic
1	east-icxstack-density	87.61 PB	88.89 PB	177.5 PB
2	west-density-7650-stack	64.17 PB	65.22 PB	129.4 PB
3	density-main-switch	45.06 PB	45.33 PB	90.4 PB
4	ICX7450-32ZP Switch	4.316 PB	4.499 PB	8.815 PB
5	ICX7450-32ZP Router	3.224 PB	3.25 PB	6.474 PB
6	ICX7650-48ZP Router	91.87 TB	91.94 TB	183.8 TB
7	ICX7650-48ZP Router	4.813 TB	2.964 TB	7.776 TB
8	EBC-ICX7150-48ZP-SW01	3.12 TB	3.499 TB	6.619 TB
9	ICX7250-24P Switch	83.22 GB	120.2 GB	203.4 GB

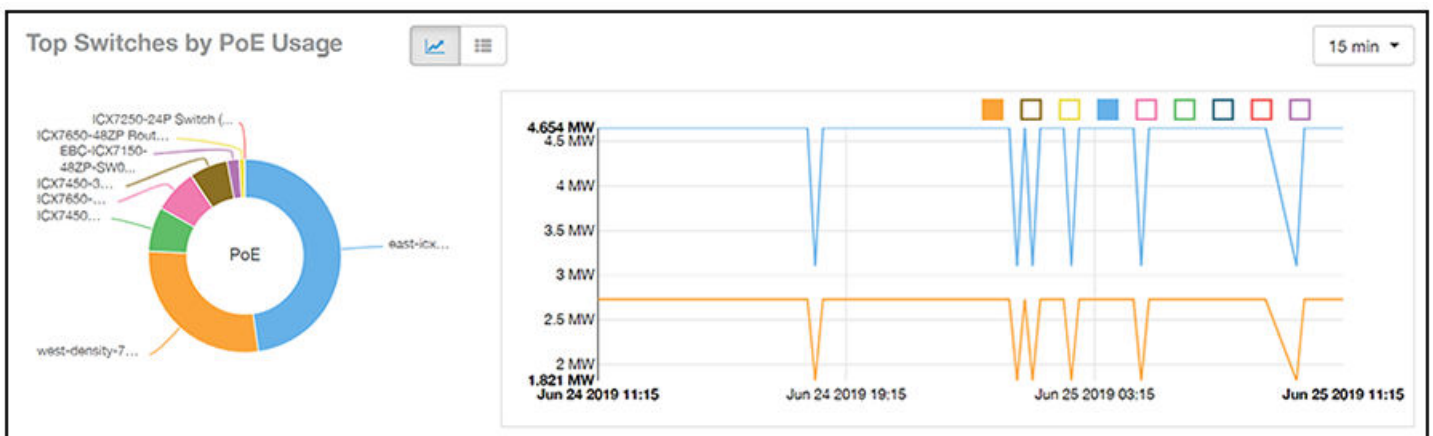
◀ 1 ▾ of 1 ▶

## Top Switches by PoE Usage Tile

The **Top Switches by PoE Usage** donut chart and graph of the **Wired Network Report** display which wired switches are utilizing the most power over the Internet. You can use the menu to specify the time granularity.

If you pause the pointer over the donut chart or the line graph, an information box is displayed containing the details on the selected data points. You can click one of the areas of the donut chart to go to the **Switch Details** dashboard for the corresponding switch. Click any of the colored squares to display the selected switch details in the line graph.

FIGURE 75 Wired Network Report: Top Switches by PoE Usage Tile



Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10 (default value), 20, 50, or 100 switches to display, or display all of the switch models. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

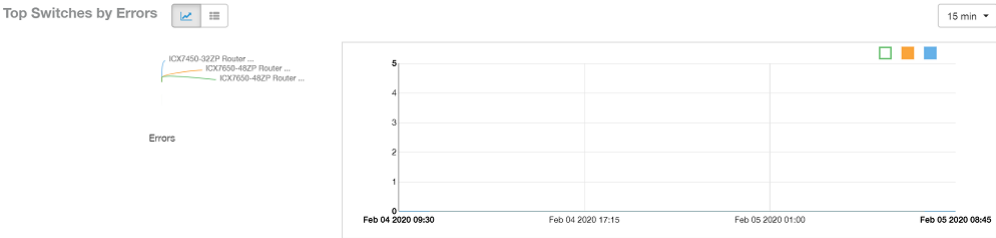
FIGURE 76 Wired Network Report: Top Switches by PoE Usage Table

Index	Switch Name	PoE Utilization	PoE Total	% of PoE Utilized
1	east-icxstack-density	4.654 MW	8.88 MW	52.41 %
2	west-density-7650-stack	2.731 MW	4.488 MW	60.85 %
3	ICX7450-32ZP Router	727.1 KW	2.244 MW	32.4 %
4	ICX7650-48ZP Router	720 KW	4.488 MW	16.04 %
5	ICX7450-32ZP Switch	625.8 KW	4.488 MW	13.94 %
6	EBC-ICX7150-48ZP-SW01	195.9 KW	740 KW	26.48 %
7	ICX7650-48ZP Router	92.4 KW	4.488 MW	2.06 %
8	ICX7250-24P Switch	0 mW	370 KW	0 %
9	density-main-switch	0 mW	2.22 MW	0 %

### Top Switches by Errors Tile

The **Top Switches by Errors** donut chart and graph of the **Wired Network Report** display the error count for switches. If you pause the pointer over the donut chart or the line graph, an information box is displayed containing the details on the selected data points. You can click one of the areas of the donut chart to go to the **Switch Details** dashboard for the corresponding switch. Click any of the colored squares to display the selected switch details in the line graph.

FIGURE 77 Wired Network Report: Top Switches by Errors Tile



Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10 (default value), 20, 50, or 100 errors to display, or display all of the errors. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 78 Wired Network Report: Top Switches by Error Table

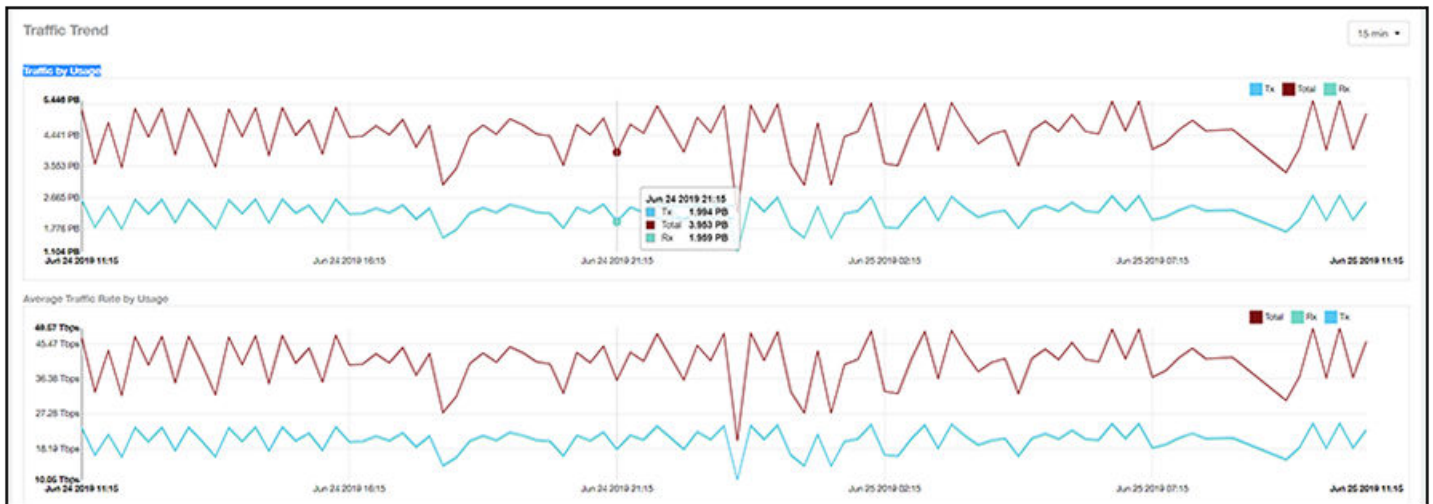
Index	Switch Name	In Errors	Out Errors	Errors
1	ICX7450-32ZP Router	0	0	0
2	ICX7650-48ZP Router	0	0	0
3	ICX7650-48ZP Router	0	0	0

## Traffic Trend Graph

The **Traffic Trend** graph of the **Wired Network Report** contain two line graphs that provide traffic information about the wired switches in the network.

Use the menu to specify the time granularity of the graphs.

FIGURE 79 Wired Network Report: Traffic Trend Graph

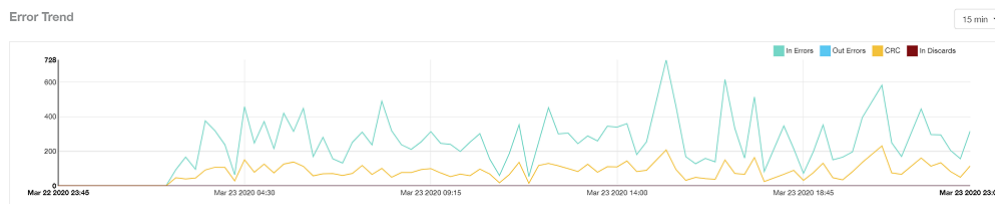


## Error Trend Graph

The **Error Trend** graph of the **Wired Network Report** contains a line graph that provides the error count information over time: In Errors, Out Errors, CRC, and In Discards.

Use the menu to specify the time granularity of the graph.

FIGURE 80 Wired Network: Error Trend Graph

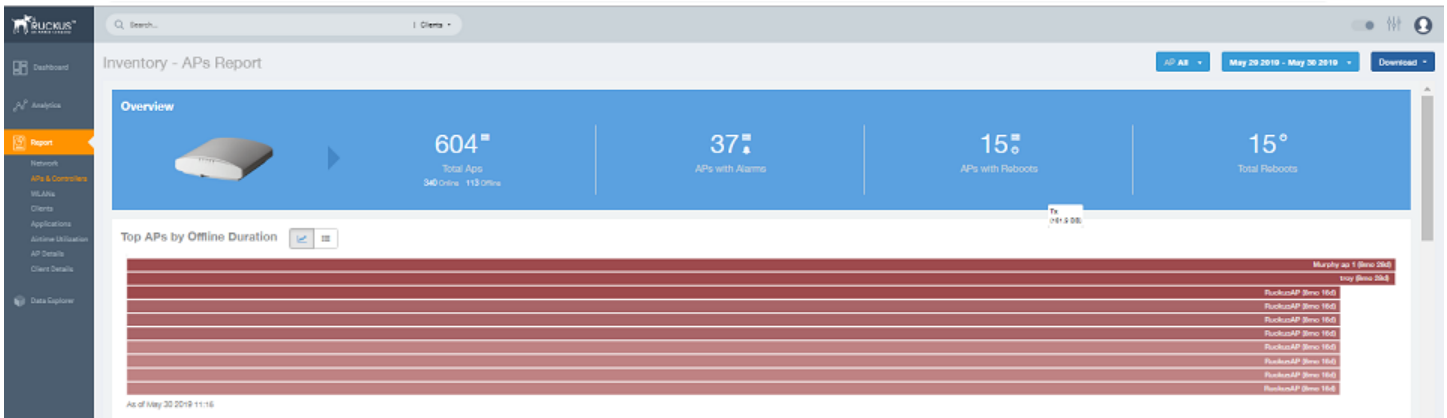


## Inventory - APs Report

The Inventory - APs Report provides details on AP inventory, such as AP reboots, AP software version, AP models and AP Alarms.

From the navigation bar, select **Report > APs**.

FIGURE 81 Inventory - APs Report (Upper Portion Only)



The Inventory - APs Report consists of the following components:

- Overview tile
- Top APs By Offline Duration tile
- AP Count Trend tile
- AP Status Trends tile
- Top AP Models tile
- Top AP Software Versions tile
- Top 10 AP Reboot Reasons tile
- Top APs by Reboot Counts tile
- Top 10 AP Alarm Types tile
- APs Configured in Multiple Systems tile
- AP Details for Online/Offline Status tile
- AP Details for Other Statuses tile

**NOTE**

All counts shown in bar charts, pie charts and tables are exact counts. The counts in trend charts are approximate.

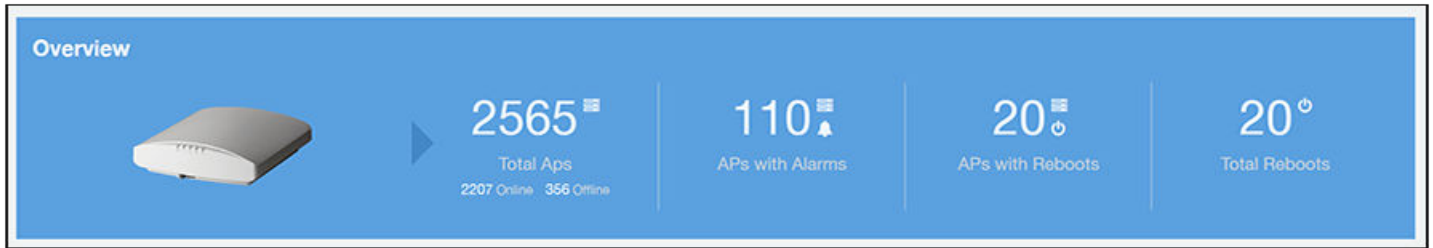
## Overview Tile

The **Overview** tile provides a general overview of the APs on the network.

It displays the following information, based on your selection of APs, radio, and date range filters:

- Total APs
- APs with alarms
- APs with reboots
- Total reboots

FIGURE 82 Inventory - APs Report: Overview Tile

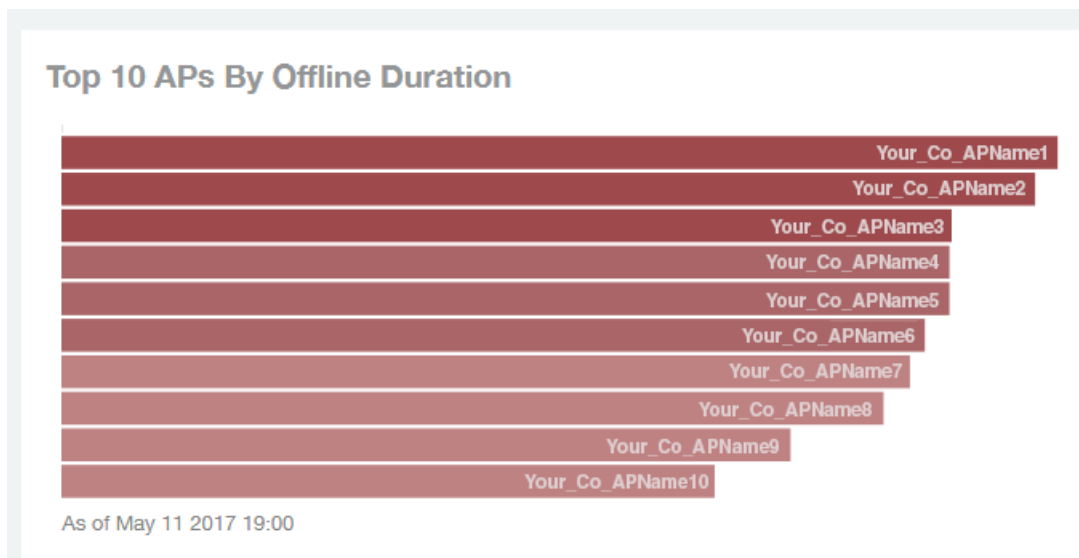




## Top APs by Offline Duration Tile

The **Top APs by Offline Duration** tile contains a bar chart and a table. The chart/table along with the Inventory - APs Report displays the top 10 APs in the network that have been disconnected for the longest duration.

In the bar chart, use the menu to specify the time period. If you pause the pointer over the bar graph, an information box is displayed that allows you to obtain details on the selected data points.

FIGURE 83 Inventory - APs Report: Top APs by Offline Duration (Chart)



Use the chart and table icons (   ) to toggle between the chart and table views.

The table view displays the top APs based on which ones have been offline for the longest time, The APs are listed by AP name, IP address, location, model, controllers, and duration in the table.


Click the gear icon (  ) to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10, 20, 50, or 100 APs by offline duration. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.



FIGURE 84 Inventory - APs Report: Top APs by Offline Duration (Table)

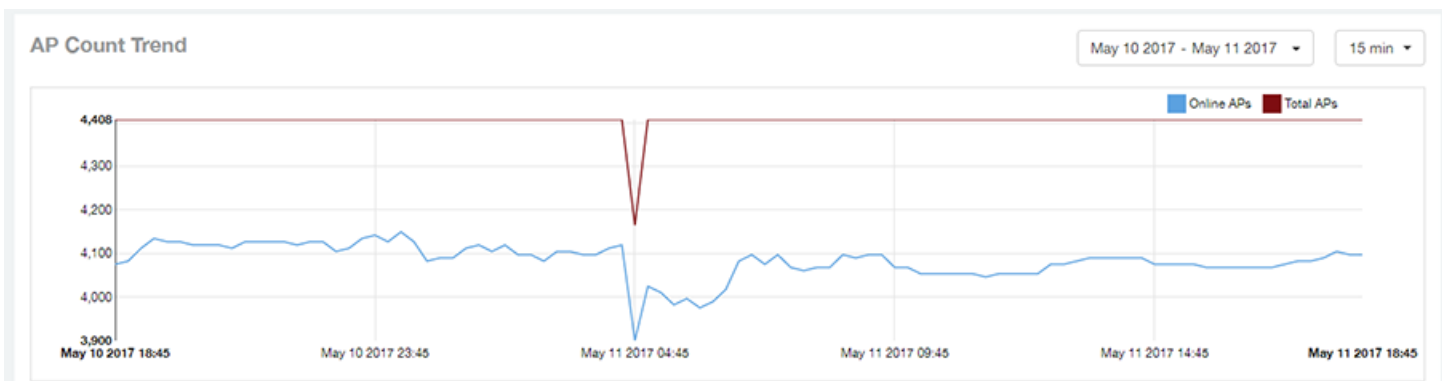
Top APs by Offline Duration							Top 10 APs
Index	AP Name	AP IP Address	AP Location	AP Model	Controller Name	Offline Duration	
1	Your_Co_APName1	10.x.y.1	Your_Co_APSite1	ZF-R710	Your_Co_CTName1	2y	
2	Your_Co_APName2	10.x.y.2	Your_Co_APSite2	ZF-R700	Your_Co_CTName1	1y 11mo	
3	Your_Co_APName3	10.x.y.3	Your_Co_APSite3	ZF-R600	Your_Co_CTName1	1y 9mo	
4	Your_Co_APName4	10.x.y.4	Your_Co_APSite4	ZF-R510	Your_Co_CTName1	1y 9mo	
5	Your_Co_APName5	10.x.y.5	Your_Co_APSite5	ZF-R500	Your_Co_CTName1	1y 9mo	
6	Your_Co_AccessPoint1	172.16.z.1	Your_Co_APLocn1	ZF-T710	Your_Co_Controller2	1y 8mo	
7	Your_Co_AccessPoint2	172.16.z.2	Your_Co_APLocn2	ZF-T301	Your_Co_Controller2	1y 8mo	
8	Your_Co_AccessPoint3	172.16.z.3	Your_Co_APLocn3	ZF-T300	Your_Co_Controller2	1y 7mo	
9	Your_Co_AccessPoint4	172.16.z.4	Your_Co_APLocn4	ZF-P300	Your_Co_Controller2	1y 5mo	
10	Your_Co_AccessPoint5	172.16.z.5	Your_Co_APLocn5	ZF-T610	Your_Co_Controller2	1y 3mo	

## AP Count Trend Graph

The **AP Count Trend** graph depicts how many APs in your network are being utilized over time.

To show APs being used over certain time periods, use the menu to specify the time period. If you pause the pointer over the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected AP details in the line graph..

FIGURE 85 Inventory - APs Report: AP Count Trend Graph



## AP Status Trends Tile

The AP Status Trends tile contains a donut chart and a graph that display the top APs by connection and uptime status, such as online, offline, provisioned, discovery, and other classifications.

Use the drop-down menu to specify the time granularity. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected AP details in the line graph.

## Report

### Inventory - APs Report

**FIGURE 86** Inventory - APs Report: AP Status Trends Tile

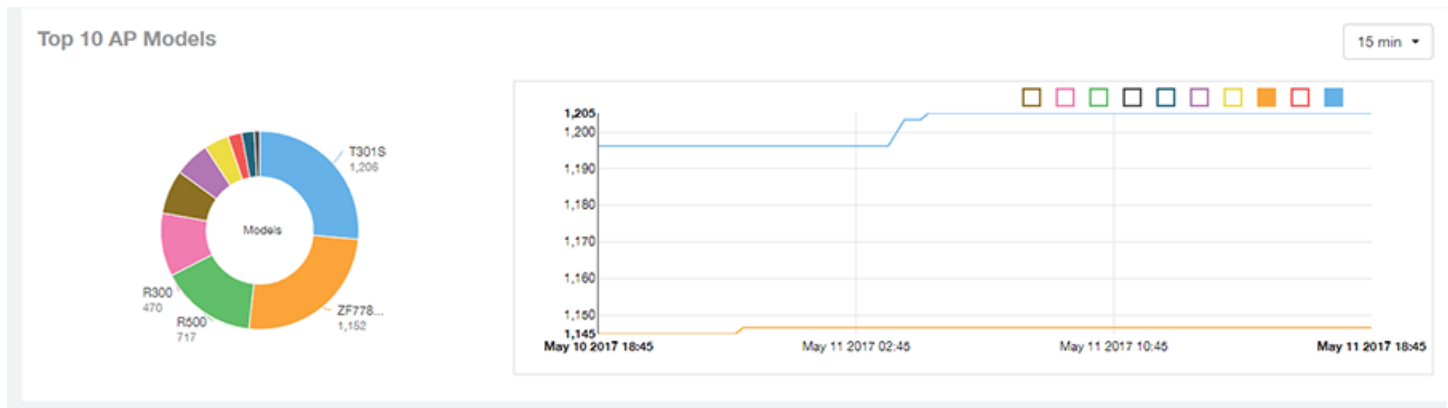




## Top AP Models

The **Top AP Models** tile contains a donut chart and a graph. The donut chart and graph display the model type that is most often used in your network.

In the chart, use the menu to specify the time period. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected AP details in the line graph.

**FIGURE 87** Inventory - APs Report: Top AP Models (Chart and Graph)



Use the chart and table icons (   ) to toggle between the chart and table views.


Click the gear icon (  ) to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10, 20, 50, or 100 models to display. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 88 Inventory - APs Report: Top AP Models (Table)

Top AP Models Top 10 Models ▾

Index	AP Model	Number of APs w/ the Model	% of APs w/ the Model
1	ZF-R710	1,206	25.94 %
2	ZF-R700	1,152	24.77 %
3	ZF-R600	717	15.42 %
4	ZF-R510	470	10.11 %
5	ZF-R500	327	7.03 %
6	ZF-H610	263	5.66 %
7	ZF-H500	184	3.96 %
8	ZF-R310	103	2.22 %
9	ZF-R300	94	2.02 %
10	ZF-R610	40	0.86 %

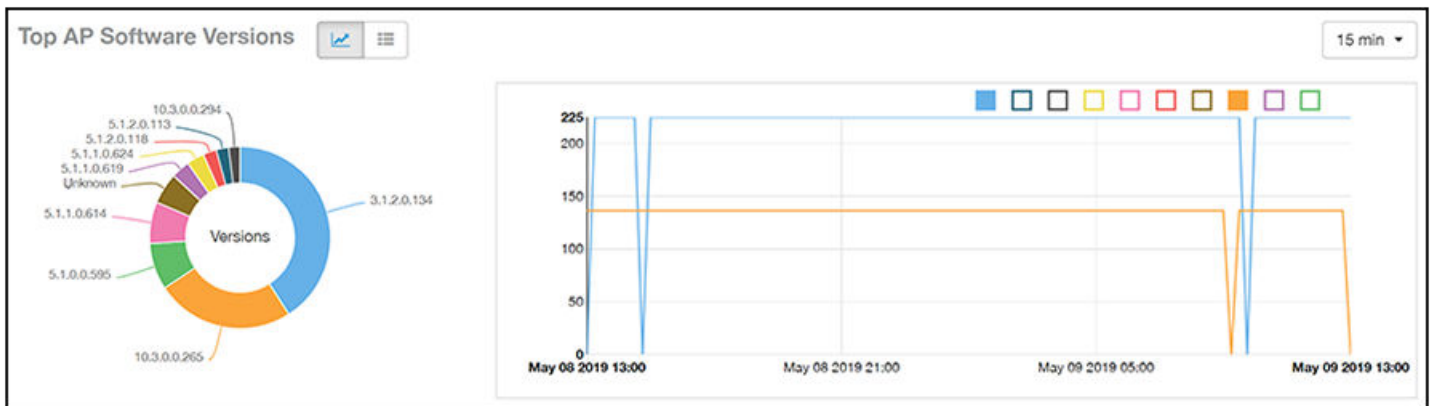
◀ 1 ▾ of 1 ▶

## Top AP Software Versions

The **Top AP Software Versions** tile are represented as a chart and table. The donut chart and graph displays the most-used software versions in your network, and show how many APs are using each version.

In the chart, use the menu to specify the time period. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected AP details in the line graph.

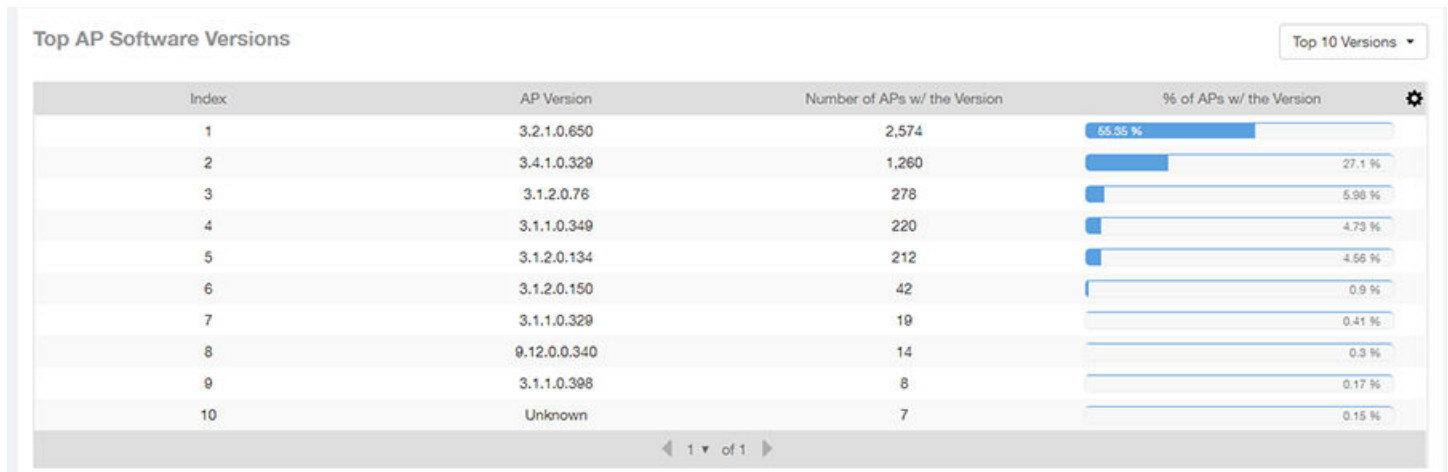
FIGURE 89 Inventory - APs Report: Top AP Software Versions (Graph and Chart)



Use the chart and table icons ( ) to toggle between the chart and table views.

Click the gear icon ( ) to select the columns to display, and click any column heading to sort the table by that column. You can also select the top 10 (default value), 20, 50, or 100 clients to display, or display all AP models. You can select the top 10, 20, 50, or 100 models to display. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 90 Inventory - APs Report: Top AP Software Versions (Table)

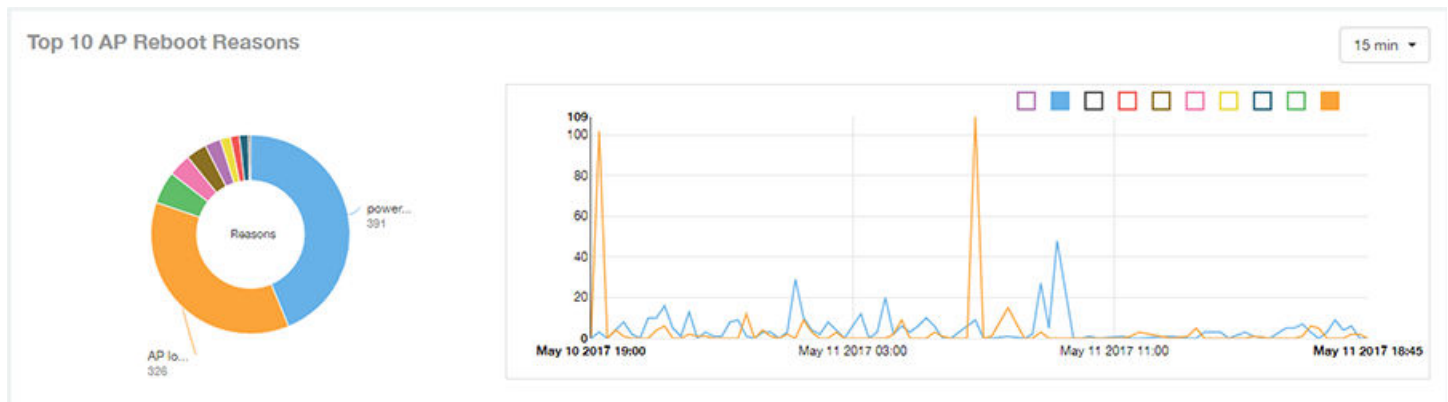


## Top 10 AP Reboot Reasons Tile

The Top 10 AP Reboot Reasons tile contains a donut chart and a graph that display the ten most common reasons why APs in your network have rebooted.

Use the menu to specify the time granularity. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares display the selected AP details in the line graph.

FIGURE 91 Inventory - APs Report: Top 10 AP Reboot Reasons Tile

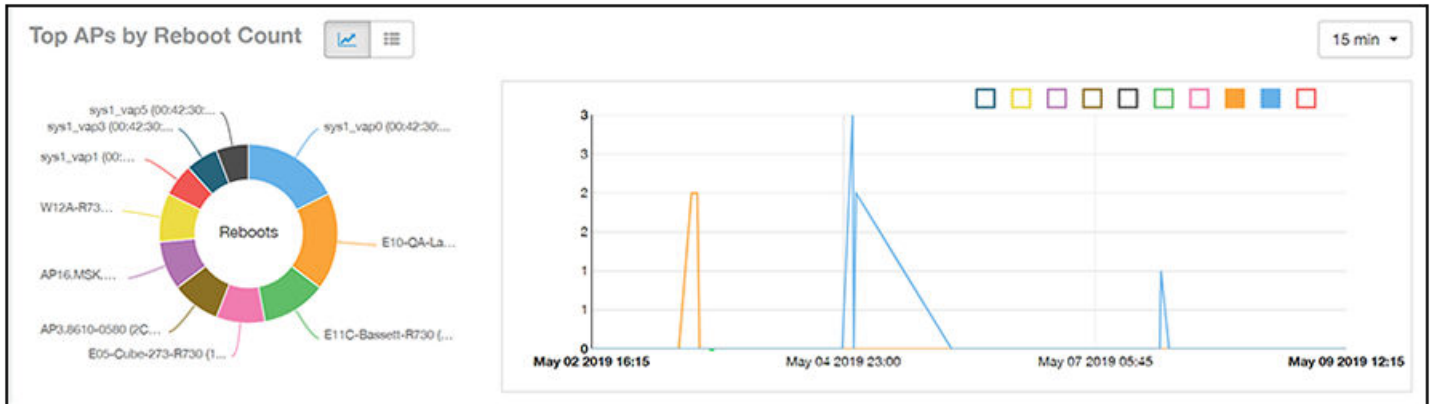


## Top APs by Reboot Count Tile

The **Top APs by Reboot Count** tile contains a donut chart and a graph. The donut chart and graph display the top ten APs in your network that have rebooted most frequently.

Use the menu to specify the time granularity. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected AP details in the line graph.

FIGURE 92 Inventory - APs Report: Top APs by Reboot Count (Chart and Graph)



Use the chart and table icons ( ) to toggle between the chart and table views.

Click the gear icon ( ) to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10, 20, 50, or 100 models to display. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 93 Inventory - APs Report: Top APs by Reboot Count (Table)

Index	AP Name	AP IP Address	AP Location	# of Reboots	Last Reboot Date	Reason for Last Reboot
1	Your_Co_APName1	10.x.y.1	Your_Co_APsite1	16	May 11 2017 18:03	unknown reason
2	Your_Co_APName2	10.x.y.2	Your_Co_APsite2	13	May 11 2017 10:00	unknown reason
3	Your_Co_APName3	10.x.y.3	Your_Co_APsite3	8	May 11 2017 18:17	power cycle
4	Your_Co_APName4	10.x.y.4	Your_Co_APsite4	8	May 11 2017 18:17	power cycle
5	Your_Co_APName5	10.x.y.5	Your_Co_APsite5	8	May 11 2017 18:17	power cycle
6	Your_Co_AccessPoint1	172.16.z.1	Your_Co_APLoon1	6	May 11 2017 08:34	system recovery by wat...
7	Your_Co_AccessPoint2	172.16.z.2	Your_Co_APLoon2	5	May 11 2017 00:28	AP rebooted by control...
8	Your_Co_AccessPoint3	172.16.z.3	Your_Co_APLoon3	5	May 11 2017 15:47	AP lost SCG more than...
9	Your_Co_AccessPoint4	172.16.z.4	Your_Co_APLoon4	4	May 11 2017 00:28	AP rebooted by control...
10	Your_Co_AccessPoint5	172.16.z.5	Your_Co_APLoon5	4	May 10 2017 21:35	power cycle

## Top 10 AP Alarm Types Tile

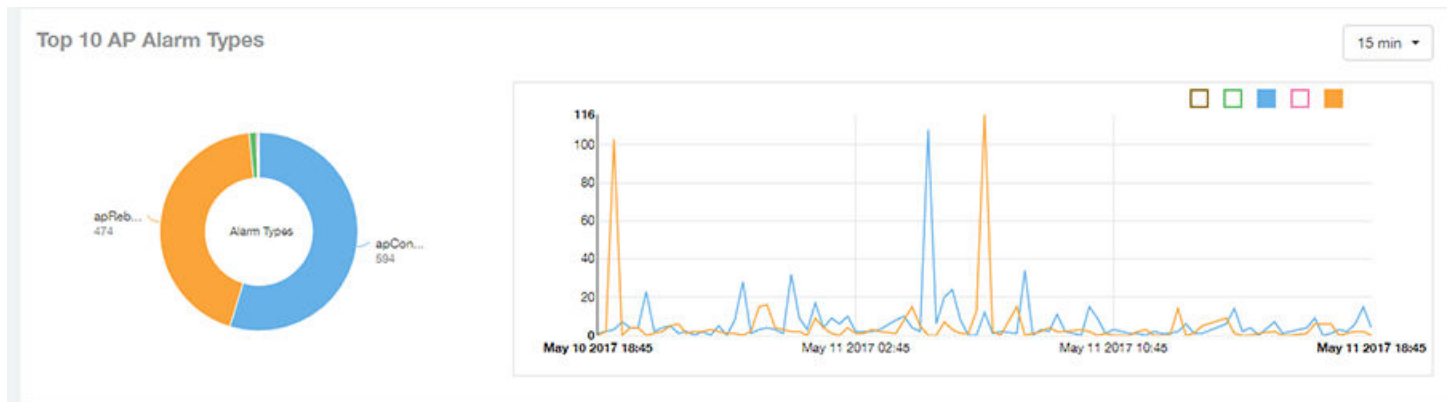
The **Top 10 AP Alarm Types** donut chart and line graph display the ten alarm types that have most frequently occurred to APs in your network.

Use the menu to specify the time period. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected AP details in the line graph.

## Report

Inventory - APs Report

FIGURE 94 Inventory - APs Report: Top 10 AP Alarm Types Tile



## APs Configured in Multiple Systems Tile

The **APs Configured in Multiple Systems** table of the **Inventory - APs Report** shows you information about APs that have been associated with more than one controller.

In the **Controller Name** column, all controllers that the AP has been associated with are listed, separated by commas. The last-known controller that this AP has been associated with is listed in the **Last Controller Name** column.

Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10, 20, 50, or 100 models to display. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 95 Inventory - APs Report: APs Configured in Multiple Systems Table

The screenshot shows a table titled "APs Configured in Multiple Systems" with a "Last Changed 10 APs" dropdown menu. The table has five columns: AP Name, Controller Name, Controller Count, Last Status, and Last Controller Name. A gear icon is visible in the top right corner of the table. The table contains three rows of data.

AP Name	Controller Name	Controller Count	Last Status	Last Controller Name
Your_Co_APName1	Your_Co_CTName1, Your...	2	online	Your_Co_CTName1
Your_Co_APName2	Your_Co_CTName5, Your...	2	online	Your_Co_CTName5
Your_Co_APName3	Your_Co_CTName4, Your...	2	online	Your_Co_CTName4

At the bottom of the table, there is a pagination control showing "1 of 1" with a left arrow and a dropdown arrow.


## AP Details for Online/Offline Status Table

The **AP Details for Online/Offline Status** table of the **Inventory - APs Report** displays its status details based on AP name, IP address, location, model name, controller name, last status, and last status change.

Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10, 20, 50, or 100 models to display. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 96 Inventory - APs Report: AP Details for Online/Offline Status Table

AP Details for Online/Offline Status Last Changed 10 APs ▾

Index	AP Name	AP IP Address	AP Location	AP Model	Controller Name	Last Status	Last Status Change 
1	Your_Co_APName1	10.x.y.1	Your_Co_APsite1	ZF-R710	Your_Co_CTName1	Offline	2d 16h ago
2	Your_Co_APName2	10.x.y.2	Your_Co_APsite2	ZF-R700	Your_Co_CTName1	Offline	2d 16h ago
3	Your_Co_APName3	10.x.y.3	Your_Co_APsite3	ZF-R600	Your_Co_CTName1	Offline	2d 16h ago
4	Your_Co_APName4	10.x.y.4	Your_Co_APsite4	ZF-R510	Your_Co_CTName1	Offline	2d 16h ago
5	Your_Co_APName5	10.x.y.5	Your_Co_APsite5	ZF-R500	Your_Co_CTName1	Offline	2d 16h ago
6	Your_Co_AccessPoint1	172.16.z.1	Your_Co_APLocn1	ZF-T710	Your_Co_Controller2	Offline	2d 16h ago
7	Your_Co_AccessPoint2	172.16.z.2	Your_Co_APLocn2	ZF-T301	Your_Co_Controller2	Offline	2d 16h ago
8	Your_Co_AccessPoint3	172.16.z.3	Your_Co_APLocn3	ZF-T300	Your_Co_Controller2	Offline	2d 16h ago
9	Your_Co_AccessPoint4	172.16.z.4	Your_Co_APLocn4	ZF-P300	Your_Co_Controller2	Offline	2d 16h ago
10	Your_Co_AccessPoint5	172.16.z.5	Your_Co_APLocn5	ZF-T610	Your_Co_Controller2	Offline	2d 16h ago

◀ 1 ▾ of 1 ▶

## AP Details for Other Statuses Table

The **AP Details for Other Statuses** table of the **Inventory - APs Report** displays the details for APs that are currently in a status other than online or offline.



Click the gear icon () to select the columns to display, and click any column heading to sort the table by that column. You can select the top 10, 20, 50, or 100 models to display. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 97 Inventory - APs Report: AP Details for Other Statuses Table

AP Details for Other Statuses Last Changed 10 APs ▾

Index	AP Name	AP IP Address	AP Location	AP Model	Controller Name	Last Status 
1	Your_Co_APName1	10.x.y.1	Your_Co_APsite1	ZF-R710	Your_Co_CTName1	Provisioned
2	Your_Co_APName2	10.x.y.2	Your_Co_APsite2	ZF-R700	Your_Co_CTName1	Provisioned
3	Your_Co_APName3	10.x.y.3	Your_Co_APsite3	ZF-R600	Your_Co_CTName1	Unknown
4	Your_Co_APName4	10.x.y.4	Your_Co_APsite4	ZF-R510	Your_Co_CTName1	Discovery
5	Your_Co_APName5	10.x.y.5	Your_Co_APsite5	ZF-R500	Your_Co_CTName1	Provisioned
6	Your_Co_AccessPoint1	172.16.z.1	Your_Co_APLocn1	ZF-T710	Your_Co_Controller2	Provisioned
7	Your_Co_AccessPoint2	172.16.z.2	Your_Co_APLocn2	ZF-T301	Your_Co_Controller2	Provisioned

◀ 1 ▾ of 1 ▶

## Inventory - Controllers Report

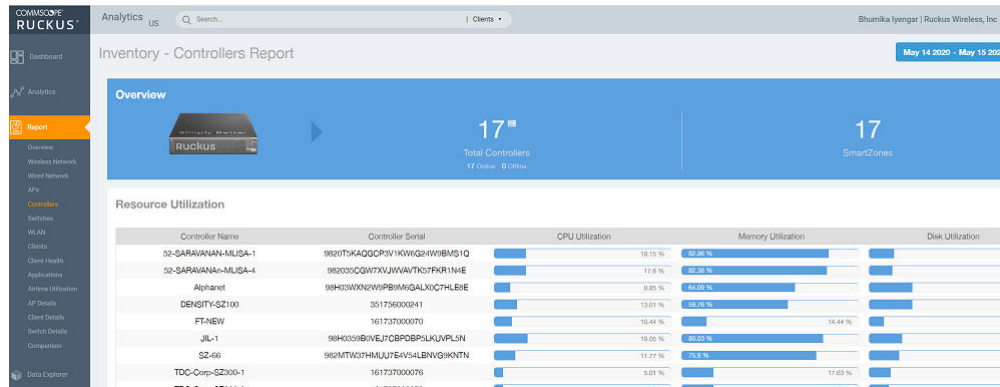
The **Inventory - Controllers Report** provides details on controller inventory, including resource and license utilization.

From the navigation bar, select **Report > Controllers**.

## Report

### Inventory - Controllers Report

FIGURE 98 Inventory - Controllers Dashboard (Upper Portion Only)



The **Inventory - Controllers Report** consists of the following components:

- Overview tile
- Resource Utilization table
- License Utilization table
- KRACK Assessment table

#### NOTE

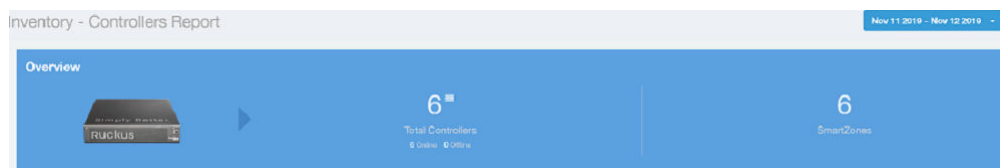
All counts in the **Inventory - Controllers Report** are exact counts.

## Overview Tile

The **Overview** tile of the **Inventory - Controllers Report** provides the following information, based on your selection of AP, Radio, and Date Range filters:

- Total number of controllers (and how many are online and offline)
- Number of SmartZone controllers

FIGURE 99 Inventory - Controllers Report: Overview Tile



## Resource Utilization Table

The **Resource Utilization** table of the **Inventory - Controllers Report** displays the CPU, memory, and disk utilization percentages for each controller in your system.

Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. Click any column heading to sort by that value. You can select the top 10 (default value), 20, 50, or 100 controllers to display, or display all of the controller names. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.



FIGURE 100 Inventory - Controllers Report: Resource Utilization Table

Resource Utilization				
Controller Name	Controller Serial	CPU Utilization	Memory Utilization	Disk Utilization
SCI-PUSH-XML	511408000113	2.36 %	5.9 %	15.58 %
SINLBS-VSZ01	983VF4KRN6UFN00JLL2SV75G...	5.5 %	65.18 %	11.68 %
sci-push-xml-2	501408000926	0.29 %	3.35 %	15.53 %
vSPoT-ZD-CI-RKSGP	481408000086	1.03 %	22.63 %	12.4 %

## License Utilization Table

The **License Utilization** table of the **Inventory - Controllers Report** displays the number of available and consumed licenses for the APs for each system.

Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. Click any column heading to sort by that value. You can select the top 10 (default value), 20, 50, or 100 systems to display, or display all of the system names. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 101 Inventory - Controllers Report: License Utilization Table

License Utilization							
System Name	APs Managed	APs Up	APs Down	AP License Total	License Consumed	License Available	License Utilization
SCI-PUSH-XML-P...	3	2	1	5	2	3	40 %
SCI_14_ZD	14	10	4	50	10	40	20 %
SCI_14_vSZ	1	0	1	10001	1	10000	0.01 %
SCI_PUSH_XML-2	1	1	0	5	1	4	20 %

## KRACK Assessment Table

The **KRACK Assessment** table of the **Inventory - Controllers Report** shows the KRACK vulnerability status of all APs that are filtered to be displayed.

FIGURE 102 Inventory - Controllers Report: KRACK Assessment Table

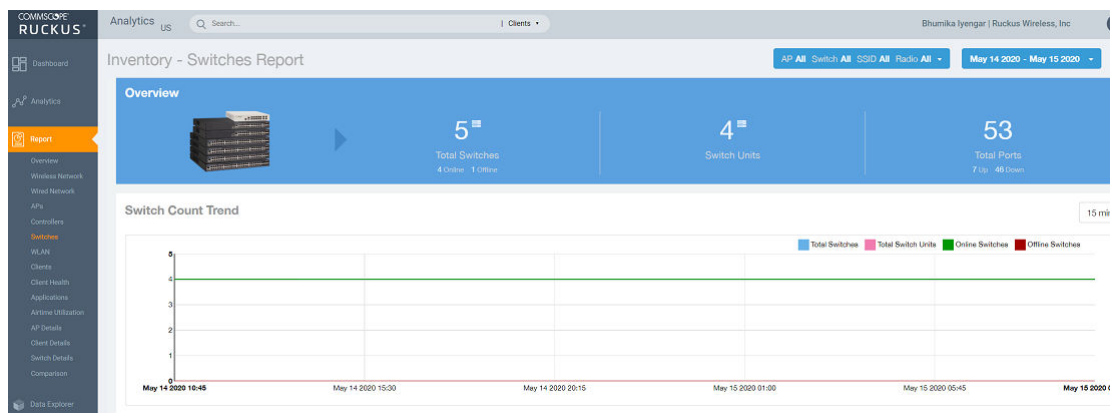
System Name	Zone	APs Patched	APs Patched (%)	Recomm
SYSTEM 1	Zone 1	0/218	0 %	Patch your APs
SYSTEM 2	Zone A	8/8	100 %	Turn on unpatch
SYSTEM 3	Default Zone	0/214	0 %	Patch your APs
SYSTEM 4	Zone A	0/1	0 %	Patch your APs
SYSTEM 5	Default Zone	0/1	0 %	Patch your APs
SYSTEM 6	Zone 1	0/1	0 %	Patch your APs
SYSTEM 7	Default Zone	0/10	0 %	Patch your APs
SYSTEM 8	California Zone	0/1	0 %	Patch your APs
SYSTEM 9	Default Zone	0/3	0 %	Patch your APs
SYSTEM 10	Zone 10	0/1	0 %	Patch your APs

You can follow the recommendations displayed to patch your APs. For information and instructions, refer to: <https://support.ruckuswireless.com/krack-ruckus-wireless-support-resource-center>.

## Inventory - Switches Report

The **Inventory - Switches Report** provides details on switch inventory, including switch models and software versions that are being used the most. From the navigation bar, select **Inventory > Switches**.

FIGURE 103 Inventory - Switches Report (Upper Portion Only)



The **Inventory - Switches Report** consists of the following components:

- Overview tile

- Switch Count Trend Graph
- Top Switch Software Versions tile
- Top Switch Models tile
- Port Status Trend tile

**NOTE**

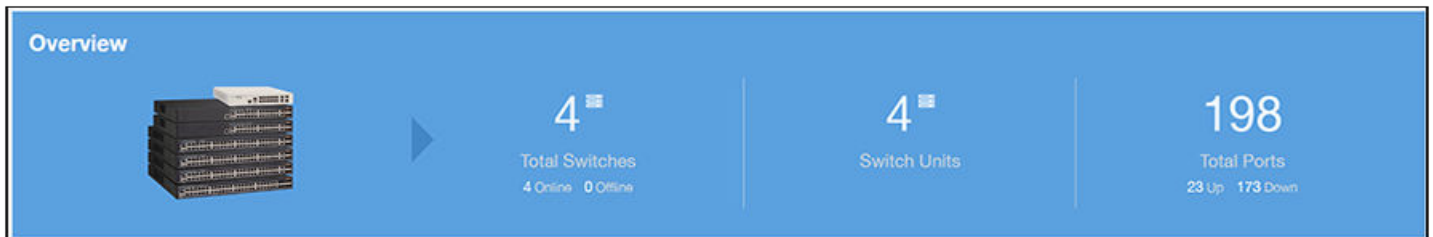
All counts in the line graphs, donut charts, and tables of the **Inventory - Switches Report** are exact counts. The counts in trend graphs are approximate.

## Overview Tile

The **Overview** tile of the **Inventory - Switches Report** provides the following information, based on your selection of filters:

- Total number of switches (and how many are online and offline)
- Number of switch units
- Total number of ports (and how many are up and down)

**FIGURE 104** Inventory - Switches Report: Overview Tile



## Switch Count Trend Graph

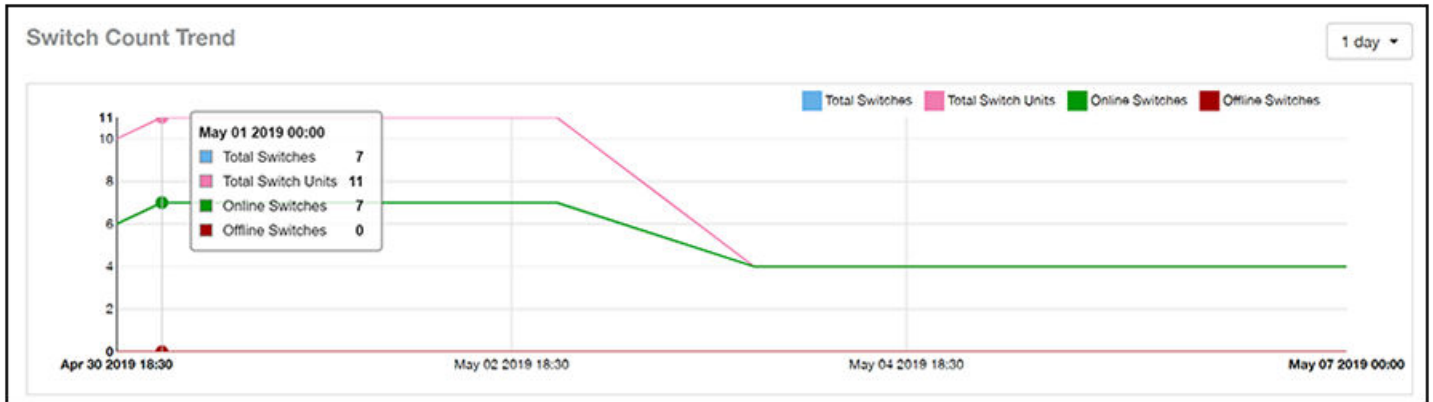
The **Switch Count Trend** graph of the **Inventory - Switches Report** displays the trend of total switches, total switch units, online status, and offline status over specified time intervals.

Use the menu to specify the time granularity. If you pause the pointer over the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected switch details in the line graph.

## Report

### Inventory - Switches Report

FIGURE 105 Inventory - Switches Report: Switch Count Trend Graph

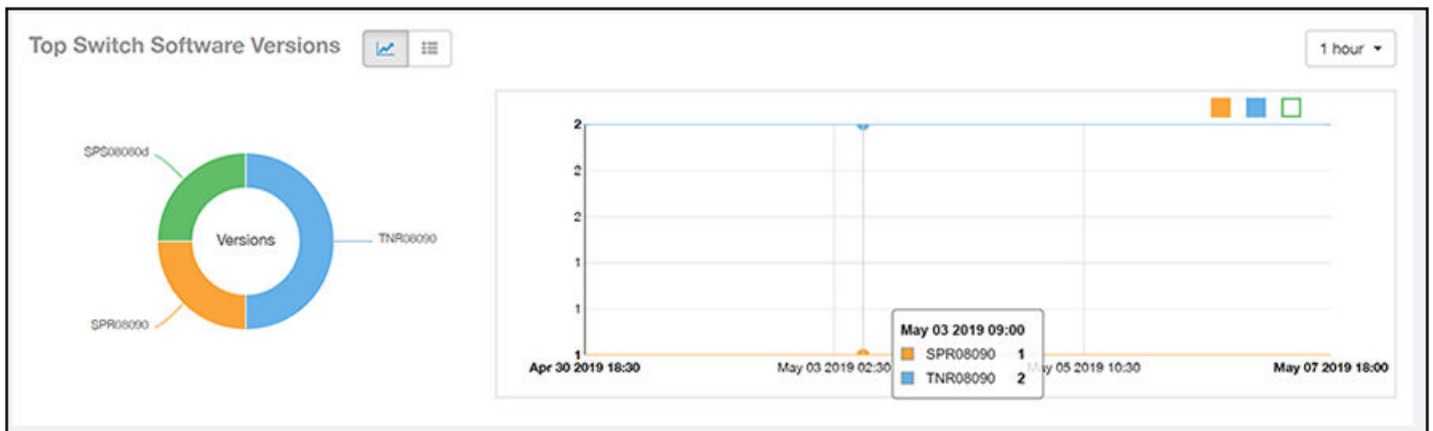


## Top Switch Software Versions Tile

The **Top Switch Software Versions** donut chart and graph of the **Inventory - Switches Report** display the most-used switch software versions in your network, and show the number of switches using each version.

Use the menu to specify the time granularity. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected switch details in the line graph.

FIGURE 106 Inventory - Switches Report: Top Switch Software Versions Tile



Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. The table is sorted on the top switch software version by default. You can select the top 10 (default value), 20, 50, or 100 software versions to display, or display all of the software versions. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 107 Inventory - Switches Report: Top Switch Software Versions Table

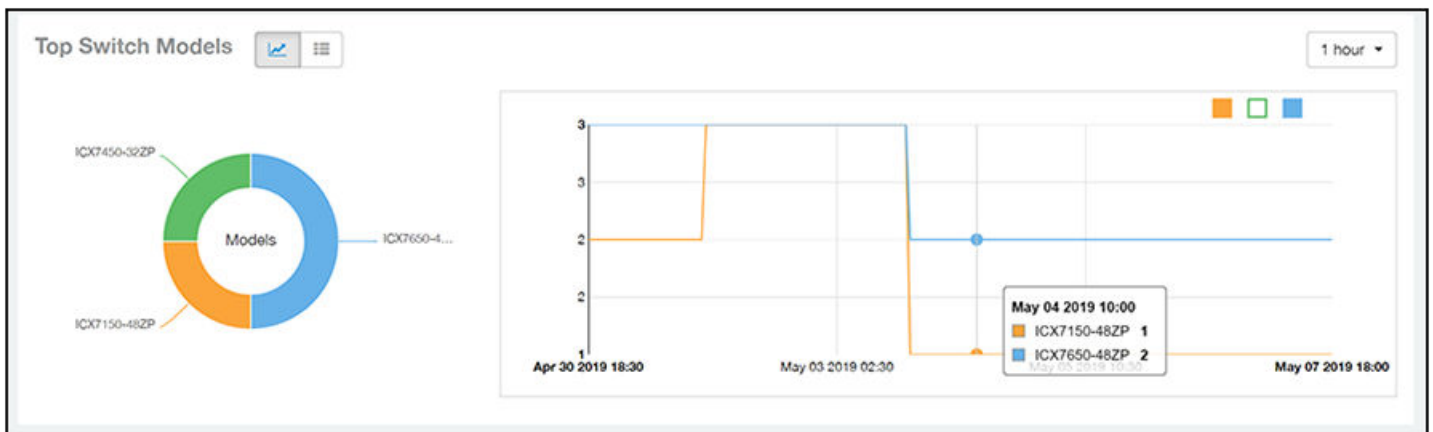
Index	Switch Version	Number of Switches w/ the Version	% of Switches w/ the Version
1	SPS08090b	3	60 %
2	SPS08090a	1	20 %
3	TNS08090b	1	20 %

## Top Switch Models Tile

The **Top Switch Models** donut chart and line graph of the **Inventory - Switches Report** display the model type that is most often used in your network.

Use the menu to specify the time granularity. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected switch details in the line graph.

FIGURE 108 Inventory - Switches Report: Top Switch Models Tile



Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. The table is sorted on the top switch model by default. You can select the top 10 (default value), 20, 50, or 100 models to display, or display all of the switch models. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

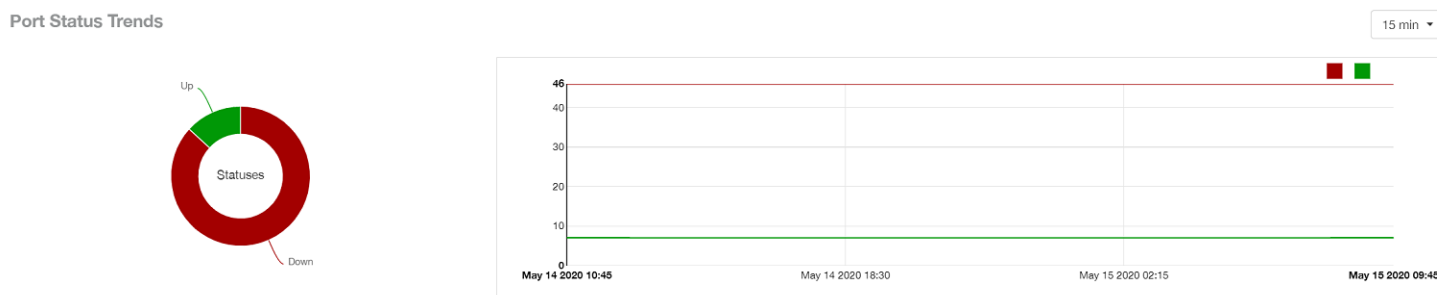
FIGURE 109 Inventory - Switches Report: Top Switch Models Table

Index	Switch Model	Number of Switches w/ the Model	% of switches w/ the Model
1	ICX7150-48ZP	3	60 %
2	ICX7450-32ZP	1	20 %
3	ICX7650-48ZP	1	20 %

## Port Status Trends Tile

The **Port Status Trends** donut chart and line graph of the **Inventory - Switches Report** display the status of the ports as up and down.

FIGURE 110 Inventory - Switches Report: Port Status Trends Tile



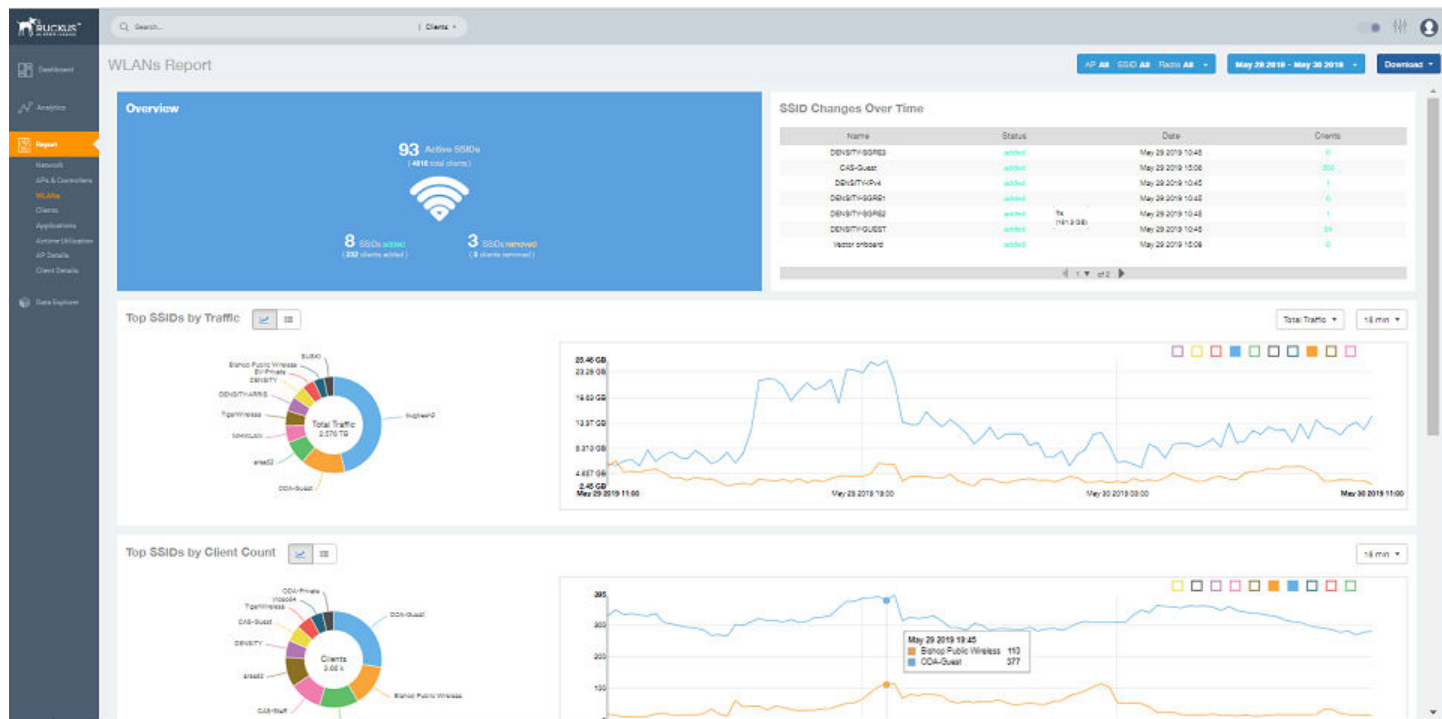
## WLAN Report

The **WLAN Report** contains information about the added SSIDs, including which are active and which have been removed.

The report includes details about SSID changes over time, SSIDs by received and transmitted traffic, the client count over a time range, and the trend of the SSIDs based on traffic count and volume. The **WLAN Report** allows you to filter the information based on APs, SSID and radio, day and date, and receive and transmit (Rx+Tx) filters.

From the navigation bar, select **Report > WLAN**.

FIGURE 111 WLAN Report (Upper Portion Only)



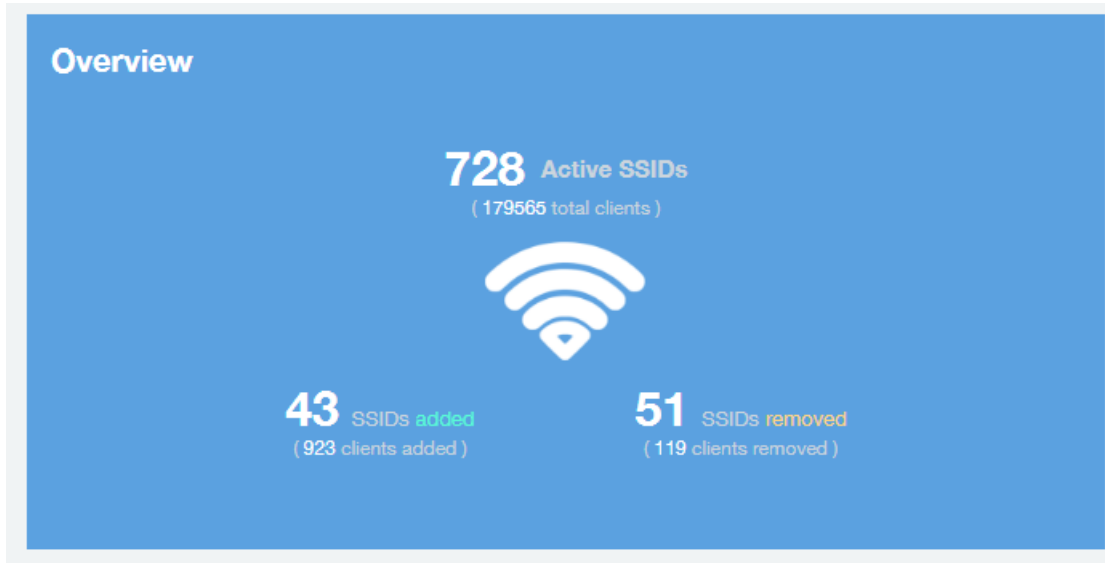
The WLANs Report consists of the following components:

- Overview tile
- SSID Changes Over Time table
- Top 10 SSIDs by Traffic tile
- Top 10 SSIDs by Client Count tile
- Active SSIDs Trend graph

## Overview Tile

The **Overview** tile of the **WLAN Report** shows the total number of active SSIDs, and the number of added and removed SSIDs over the selected period.

FIGURE 112 WLAN: Overview Tile



## SSID Changes Over Time Tile

The **SSID Changes Over Time** table display of the **WLAN Report** shows the most recent SSID changes.

FIGURE 113 WLAN: SSID Changes Over Time Table

Name	Status	Date	Clients
Your_Co_SSIDName1	removed	May 11 2017 14:00	17
Your_Co_SSIDName2	added	May 10 2017 23:45	78
Your_Co_SSIDName3	added	May 10 2017 21:00	25
Your_Co_SSIDName4	added	May 10 2017 23:45	73
Your_Co_SSIDName5	removed	May 10 2017 23:15	1
Your_Co_SSIDName6	removed	May 10 2017 19:15	1
Your_Co_SSIDName6	removed	May 10 2017 19:15	1

1 of 14

## Top SSIDs by Traffic Table

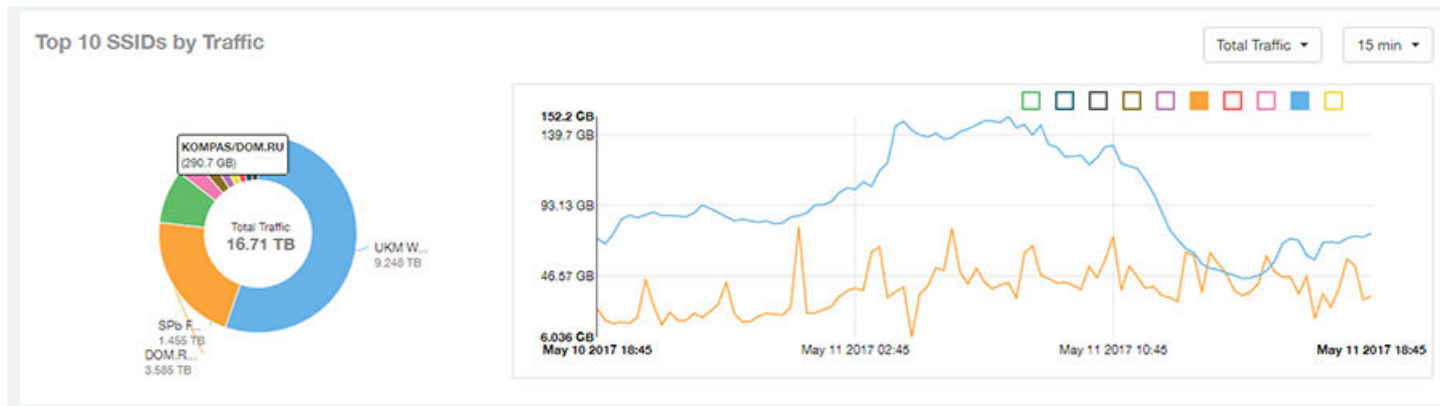
Use the **Top SSIDs by Traffic** donut pie chart and graph of the **WLANs Report** to view which wireless networks are generating the most traffic, to compare usage of the top WLANs over different time periods, and to compare Tx and Rx statistics independently.

The **Top SSIDs by Traffic** tile contains a donut chart and a graph.



In the graph, click any of the colored squares to display the corresponding SSID details in the line graph. You can use the traffic menu to choose whether to display transmitted data only, received data only, or total traffic data.

FIGURE 114 WLAN: Top SSIDs by Traffic Tile



Use the chart and table icons ( ) to toggle between the chart and table views.

In the **Top SSIDs by Traffic** table, you can sort the table by total traffic, clients, AP count, or alphabetically by SSID name. Click the gear icon ( ) to select the columns to display, and click any column heading to sort the table by that column. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

You can select the top 10 (default), 20, 50, or 100 SSIDs by traffic volume, or list all SSIDs.

FIGURE 115 WLAN: Top SSIDs by Traffic (Table)

The table displays the top 10 SSIDs by traffic volume. The total traffic for these SSIDs is 16.71 TB, which is 73.15% of the total traffic (22.84 TB). The table includes columns for Index, SSID Name, Rx Total, Tx Total, Total Traffic, Clients, and APs. The data is as follows:

Index	SSID Name	Rx Total	Tx Total	Total Traffic	Clients	APs
1	Your_Co_SSIDName1	594.3 GB	6,678 TB	9,248 TB	18.45 k	974
2	Your_Co_SSIDName2	151.3 GB	3,437 TB	3,585 TB	44,44 k	1,105 k
3	Your_Co_SSIDName3	157 GB	1,301 TB	1,455 TB	66,74 k	961
4	Your_Co_SSIDName4	61.92 GB	480.3 GB	542.3 GB	11,44 k	213
5	Your_Co_SSIDName5	23.43 GB	374.8 GB	398.2 GB	1,096 k	26
6	Your_Co_SSIDName6	11.38 MB	337.6 GB	337.6 GB	1	959
7	Your_Co_SSIDName7	25.13 GB	299.3 GB	324.5 GB	101	6
8	Your_Co_SSIDName8	26.94 GB	278.2 GB	305.2 GB	3,941 k	50
9	Your_Co_SSIDName9	12.63 GB	278 GB	290.7 GB	288	20
10	Your_Co_SSIDName10	20.05 GB	259.9 GB	279.9 GB	4,754 k	280

## Top SSIDs by Client Count Tile

Use the **Top SSIDs by Client Count** donut chart and graph of the **WLAN Report** to view which wireless networks are most congested in terms of client count, and to compare client counts over different time periods.

The **Top SSIDs by Client Count** tile contains a donut chart and a graph.

In the graph, click any of the colored squares to display the corresponding SSID details in the line graph.

If you pause a pointer over the line graph, an information box is displayed containing the selected SSID names and client counts at the chosen data point.

FIGURE 116 WLAN: Top SSIDs by Client Count Tile



Use the chart and table icons ( ) to toggle between the chart and table views.

In the **Top SSIDs by Client Count** table, you can sort the table by total traffic, clients, AP count, or alphabetically by SSID name. Click the gear icon ( ) to select the columns to display, and click any column heading to sort the table by that column. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

You can select the top 10 (default), 20, 50, or 100 SSIDs by client count, or list all SSIDs.

FIGURE 117 WLAN: Top SSIDs by Client Count (Table)

Index	SSID Name	Clients	Rx Total	Tx Total	Total Traffic	APs
1	Your Co_SSIDName1	66.74 k	157 GB	1.301 TB	1.455 TB	961
2	Your Co_SSIDName2	44.44 k	151.3 GB	3.437 TB	3.585 TB	1,105 k
3	Your Co_SSIDName3	18.45 k	584.3 GB	8.678 TB	9.248 TB	974
4	Your Co_SSIDName4	11.44 k	61.92 GB	480.3 GB	542.3 GB	213
5	Your Co_SSIDName5	4.754 k	20.05 GB	259.9 GB	279.9 GB	280
6	Your Co_SSIDName6	3,941 k	26.94 GB	278.2 GB	305.2 GB	50
7	Your Co_SSIDName7	2,656 k	9.192 GB	100.3 GB	109.5 GB	170
8	Your Co_SSIDName8	1.18 k	2.87 GB	34.78 GB	37.65 GB	5
9	Your Co_SSIDName9	1,096 k	23.43 GB	374.8 GB	398.2 GB	26
10	Your Co_SSIDName10	344	621.7 MB	8.391 GB	8.998 GB	14

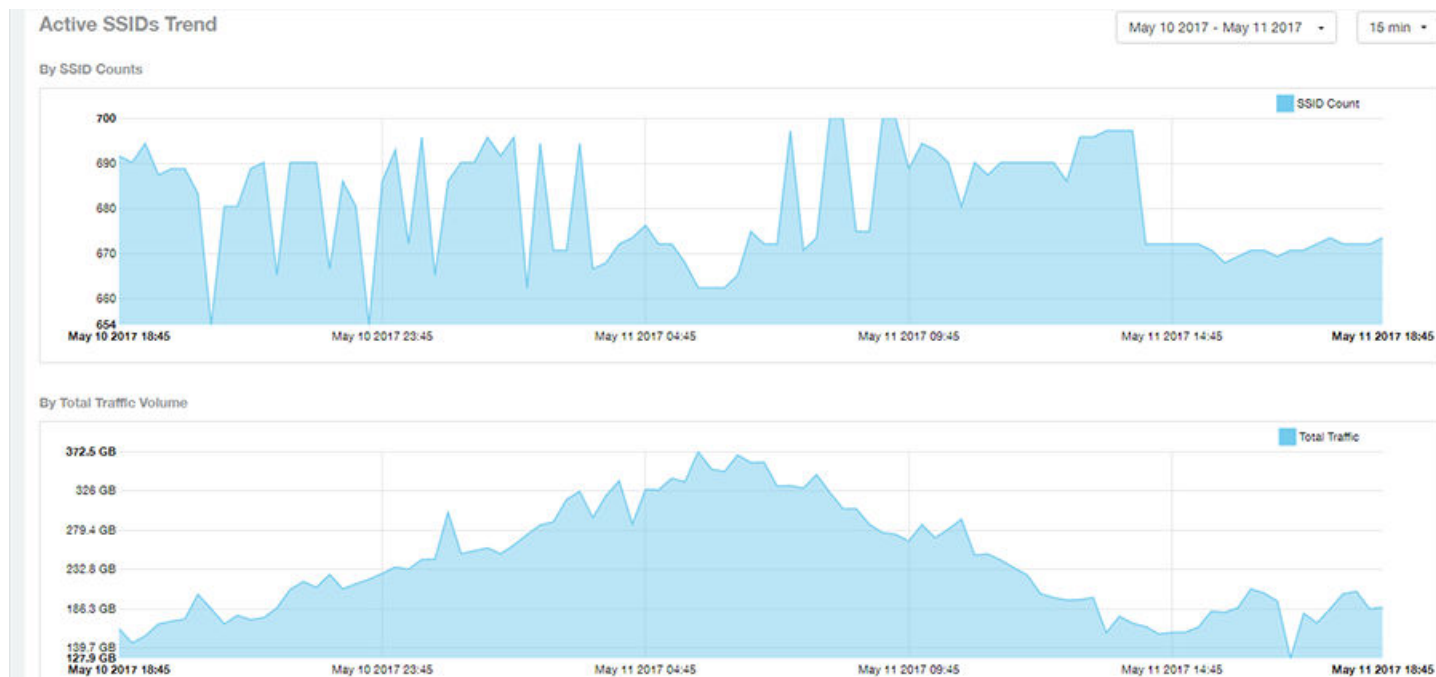
## Active SSIDs Trend Graphs

The **Active SSIDs Trend** graphs of the **WLAN Report** show the: total number of SSIDs over time, and the total traffic volume over time.

Delete this line here. A repeat of the opening paragraph.

Pause the pointer over the graphs to display the total SSID count or total traffic volume at any specific data point.

FIGURE 118 WLAN: Active SSIDs Trend Graphs



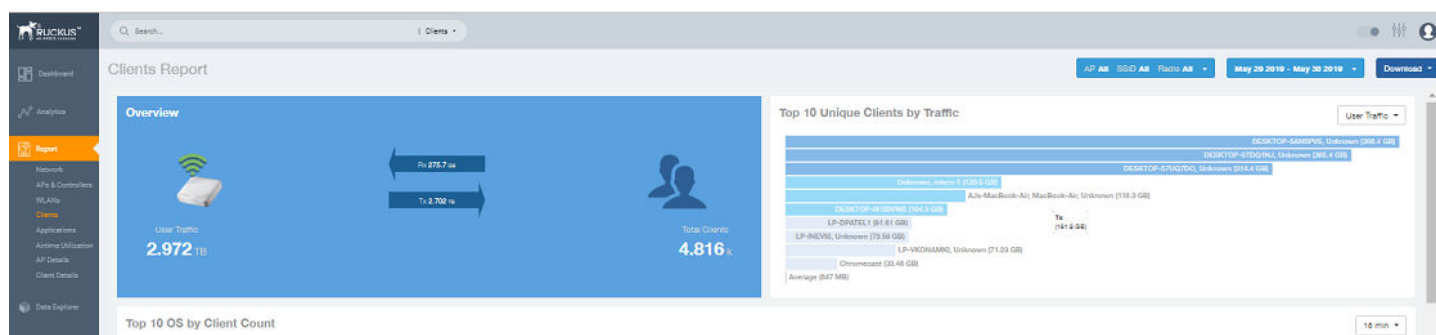
## Clients Report

The **Clients Report** provides you with the details of traffic and trends over time from the client perspective.

The **Clients Report** provides an overview of the total traffic, both received and transmitted, and the total number of clients over time. It also contains details of the top unique clients by traffic, both received and transmitted, and unique client trends over time, by client count and by traffic.

From the navigation bar, select **Report > Clients**.

FIGURE 119 Clients Report (Upper Portion Only)



The Clients Report consists of the following components:

- Overview tile
- Top 10 Unique Clients by Traffic graph
- Top 10 OS by Client Count tile

**Report**  
Clients Report

- Clients Details table
- Unique Clients Trend Over Time graphs

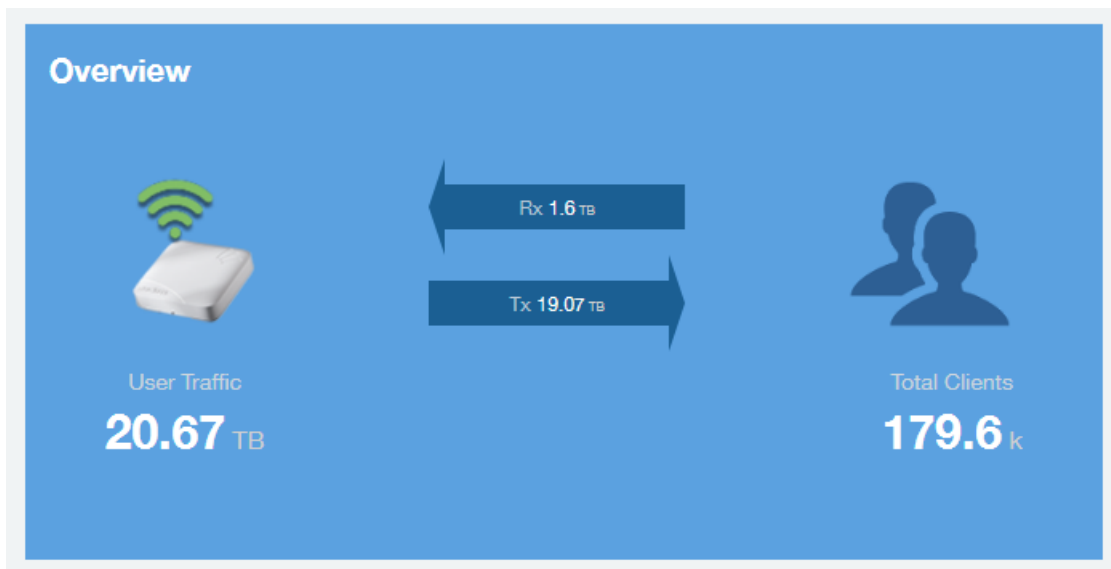
## Overview Tile

The **Overview** tile of the **Clients Report** provides information about the total traffic, both received and transmitted, and the total number of clients over the selected time period.

The **Overview** tile displays the following information, based on your selection of APs, radio, and date range filters:

- Total user traffic
- Total received and transmitted user traffic
- Total number of clients on the network

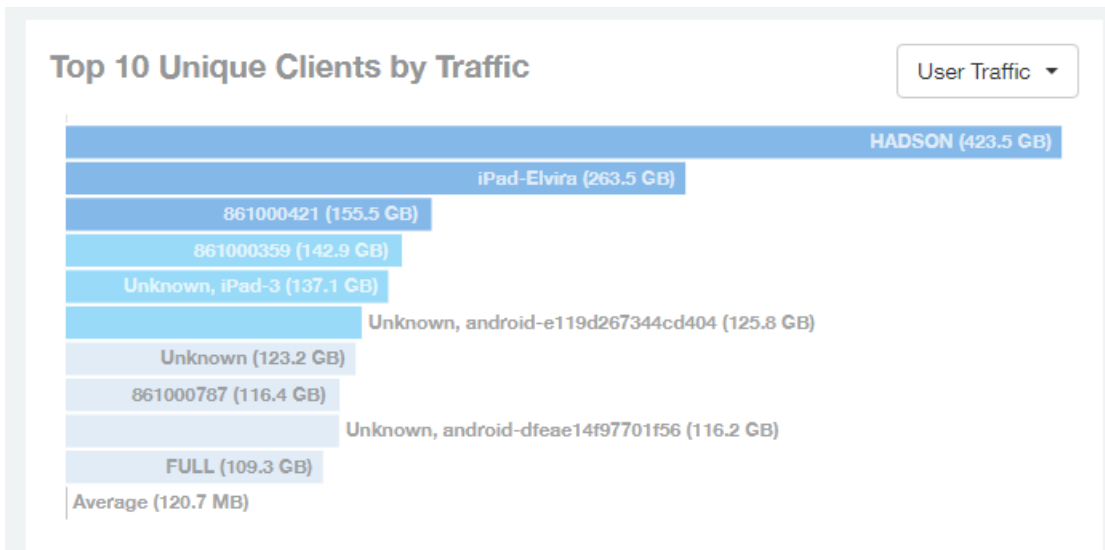
**FIGURE 120** Clients: Overview Tile



## Top 10 Unique Clients by Traffic Chart

The **Top 10 Unique Clients by Traffic** chart of the **Clients Report** provides you with information about the top ten unique clients by traffic, which you can filter on received traffic, transmitted traffic, and total traffic.

FIGURE 121 Clients: Top 10 Unique Clients by Traffic



## Clients Details

The **Clients Details** table of the **Clients Report** shows a list of clients with the highest traffic volume in the network as per the selected components.

Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column. By default, the table is sorted by total traffic (Rx + Tx). You can select the top 10 (default), 20, 50, or 100 clients to display. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 122 Clients: Clients Details Table

Clients Details These clients consume 8.1 % (1.673 TB) of all user traffic (20.67 TB). Top 10 Clients

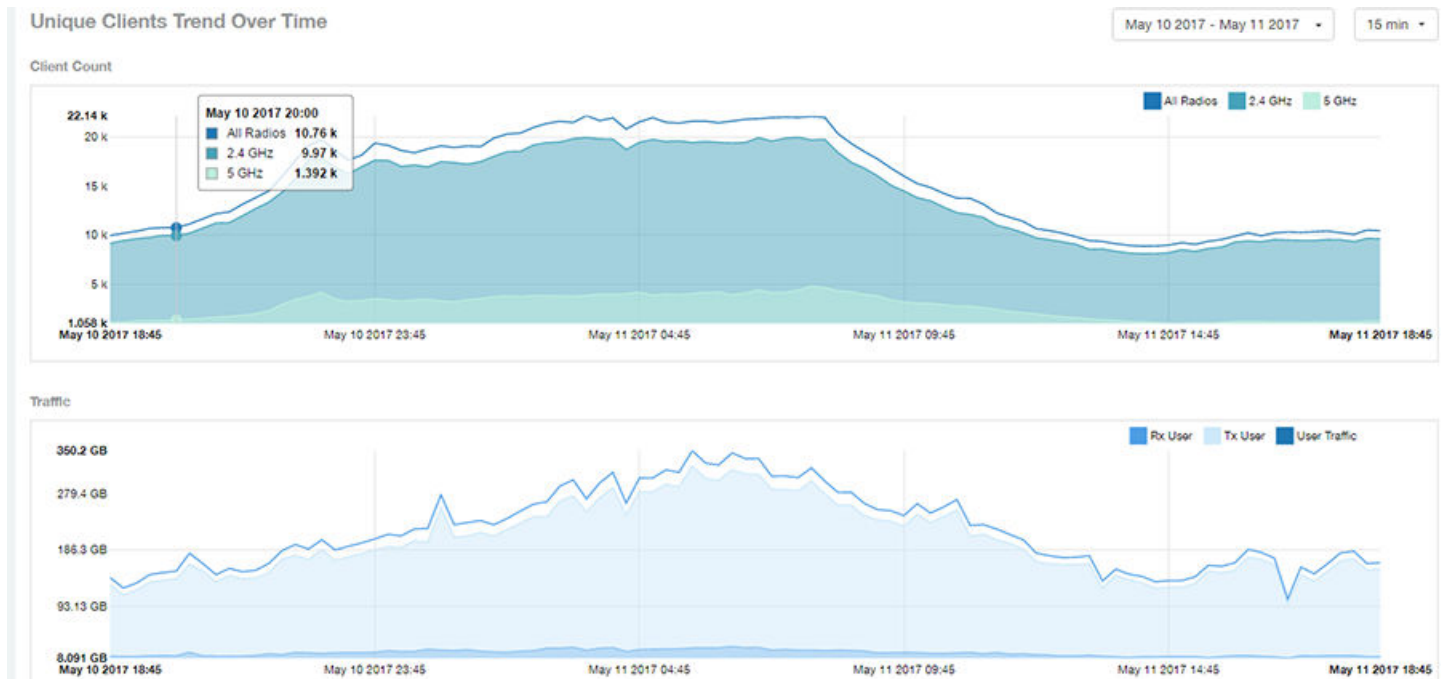
Index	Hostname	MAC Address	IP Address	Username	Sessions	Rx User	Tx User	User Traffic
1	Your_Co_HostName1	FE:DC:BA:89:67:01	10.x.y.1	Your_Co_UserName1	1	190.7 MB	423.3 GB	423.5 GB
2	Your_Co_HostName2	FE:DC:BA:89:67:02	10.x.y.2	Your_Co_UserName2	1	13.8 GB	249.7 GB	263.5 GB
3	Your_Co_HostName3	FE:DC:BA:89:67:03	10.x.y.3	Your_Co_HostName3	9	3.956 GB	151.5 GB	155.5 GB
4	Your_Co_HostName4	FE:DC:BA:89:67:04	10.x.y.4	Your_Co_UserName4	12	3.502 GB	139.4 GB	142.9 GB
5	Your_Co_HostName5	FE:DC:BA:89:67:05	10.x.y.5	Your_Co_UserName5	15	1.066 GB	136 GB	137.1 GB
6	Your_Co_HostName6	FE:DC:BA:89:67:06	10.x.y.6	Your_Co_Username6	41	1.396 GB	124.4 GB	125.8 GB
7	Your_Co_HostName7	FE:DC:BA:89:67:07	10.x.y.7	Your_Co_UserName7	35	645.4 MB	122.6 GB	123.2 GB
8	Your_Co_HostName8	FE:DC:BA:89:67:08	10.x.y.8	Your_Co_UserName8	13	4.239 GB	112.2 GB	116.4 GB
9	Your_Co_HostName9	FE:DC:BA:89:67:09	10.x.y.9	Your_Co_UserName9	7	3.55 GB	112.6 GB	116.2 GB
10	Your_Co_HostName10	FE:DC:BA:89:67:10	10.x.y.10	Your_Co_UserName10	1	1.438 GB	107.9 GB	109.3 GB

◀ 1 of 1 ▶

## Unique Clients Trend Over Time Graphs

Use the **Unique Clients Trend Over Time Graphs** graphs of the **Clients Report** to view a breakdown of unique clients by radio type over time.

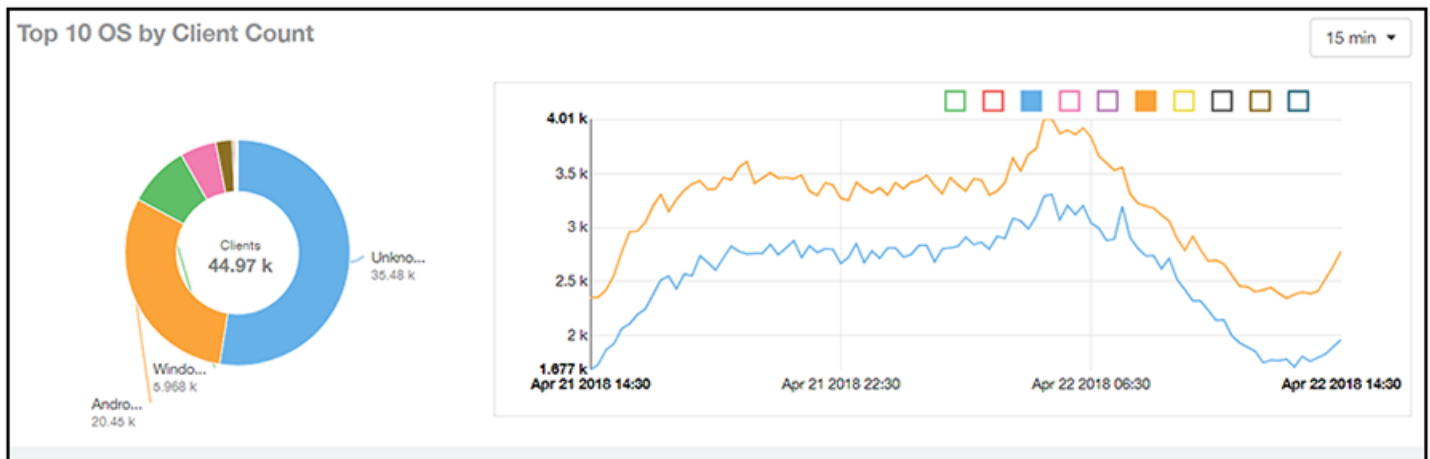
FIGURE 123 Clients: Unique Clients Trend Over Time Graph



## Top 10 OS by Client Count Tile

The **Top 10 OS by Client Count** donut chart and graph of the **Clients Report** provides you with information about the ten operating systems being used the most by the clients in your network.

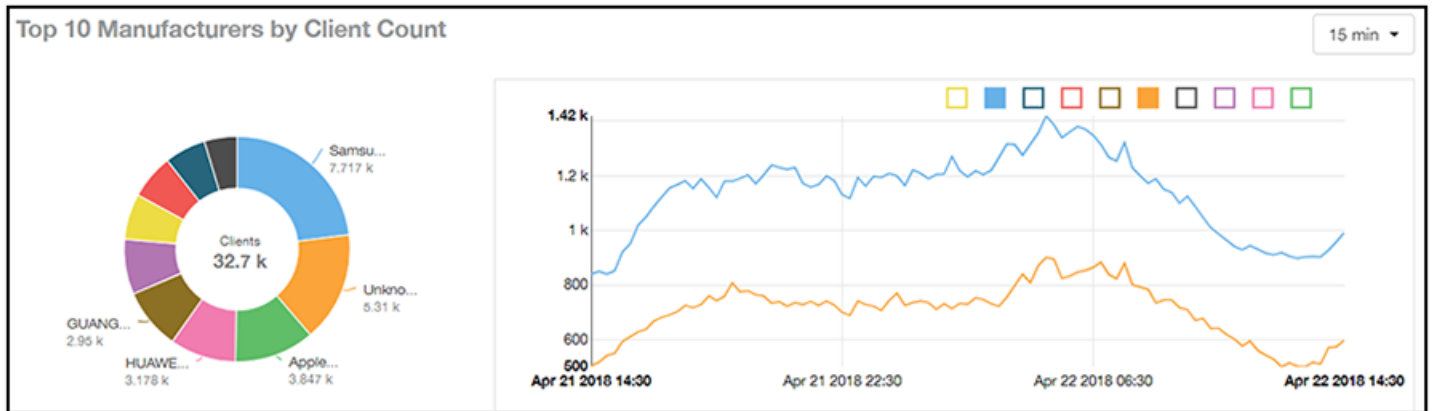
FIGURE 124 Clients: Top 10 OS by Client Count Tile



## Top 10 Manufacturers by Client Count Tile

The **Top 10 Manufacturers by Client Count** donut chart and graph of the **Clients Report** provides you with information about the ten manufacturers of wireless equipment most represented in your network.

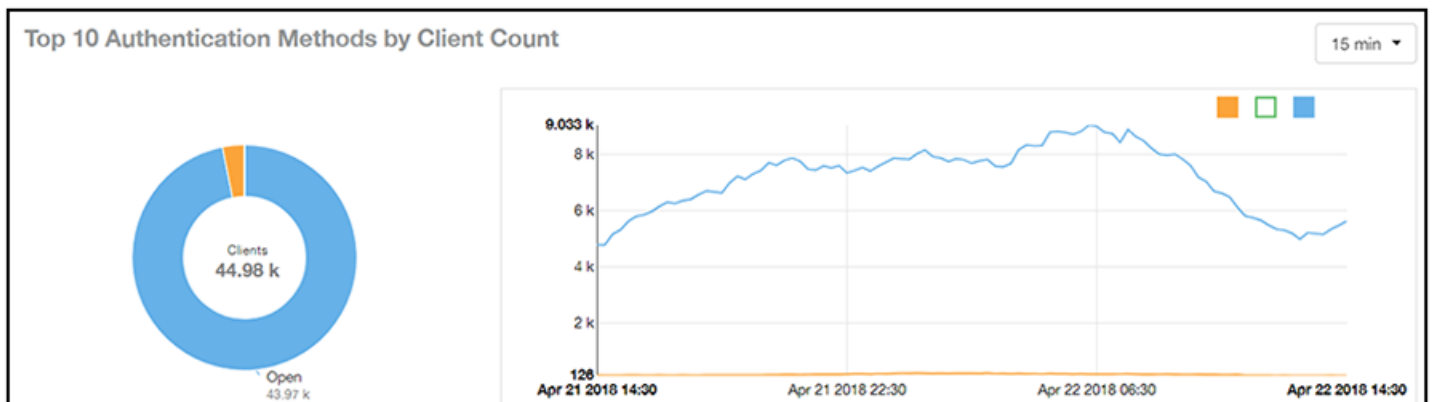
FIGURE 125 Clients: Top 10 Manufacturers by Client Count Tile



## Top 10 Authentication Methods by Client Count Tile

The **Top 10 Authentication Methods by Client Count Tile** donut chart and graph of the **Clients Report** provides you with information about the top ten methods most commonly used in your system to authenticate users.

FIGURE 126 Clients - Top 10 Authentication Methods by Client Count Tile



# Client Health Dashboard

## Client Health Report

The Client Health Report page calculates and displays a client health score to quickly assess the health of client connections.

The score is determined by the following metrics:

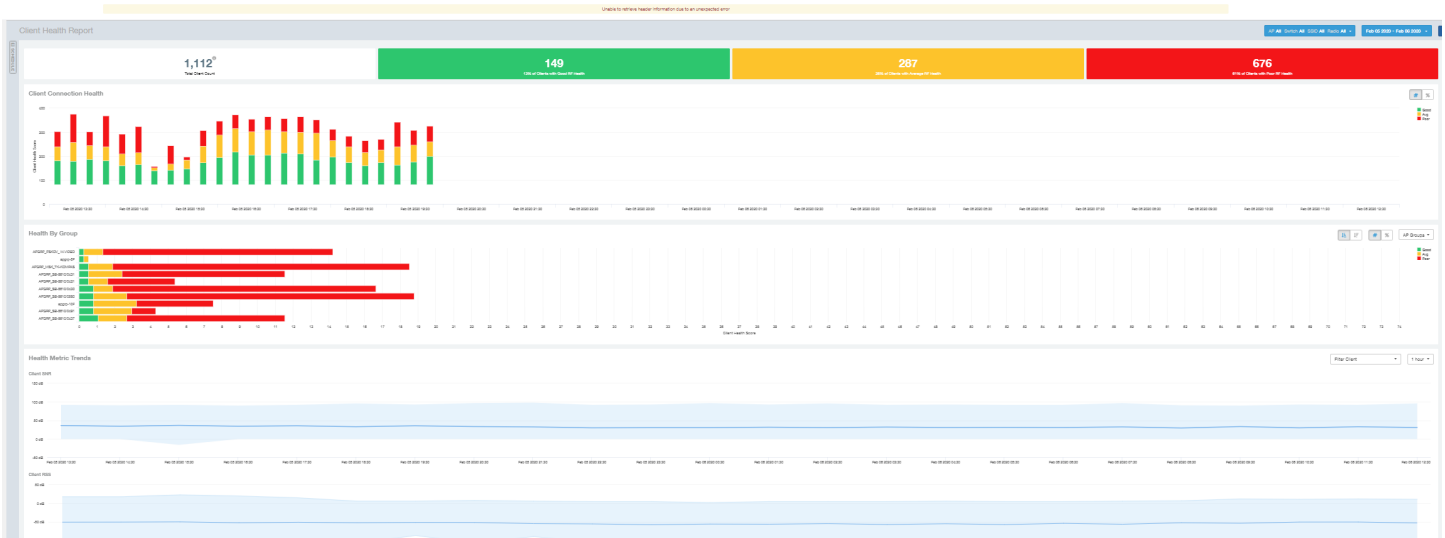
- RSSI
- SNR
- Throughput

## Report

### Client Health Dashboard

- MCS (for transmission)

**FIGURE 127** Client Health Report (Upper Portion Only)

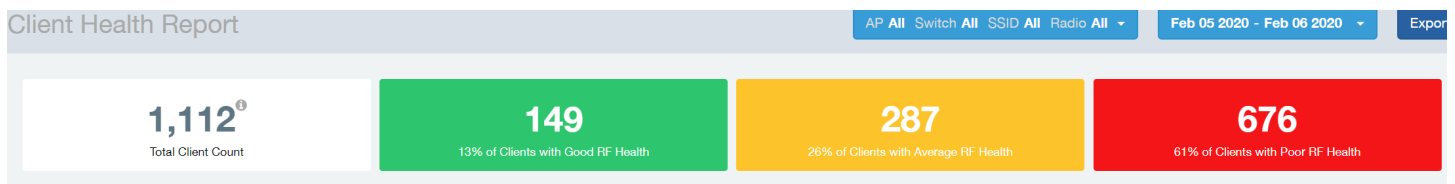


The Client Health Report consists of the following components:

- Header tile
- Client Connection Health tile
- Health by Group tile
- Health Metric Trends graphs

### Header Tile

The header tile shows a summary of client health data for the selected time, by displaying the total clients that have been assigned the client score, and the status of these clients based on their RF health. The RF health is depicted as three colored boxes; each color indicating a status. The client count for each RF health status is also displayed.



The green box shows the number of clients with good RF health. The yellow box shows the number of clients with average RF health and the red box displays the number of clients with poor RF health. The numbers are determined by the threshold that you set as per your expectations of client health in the network.

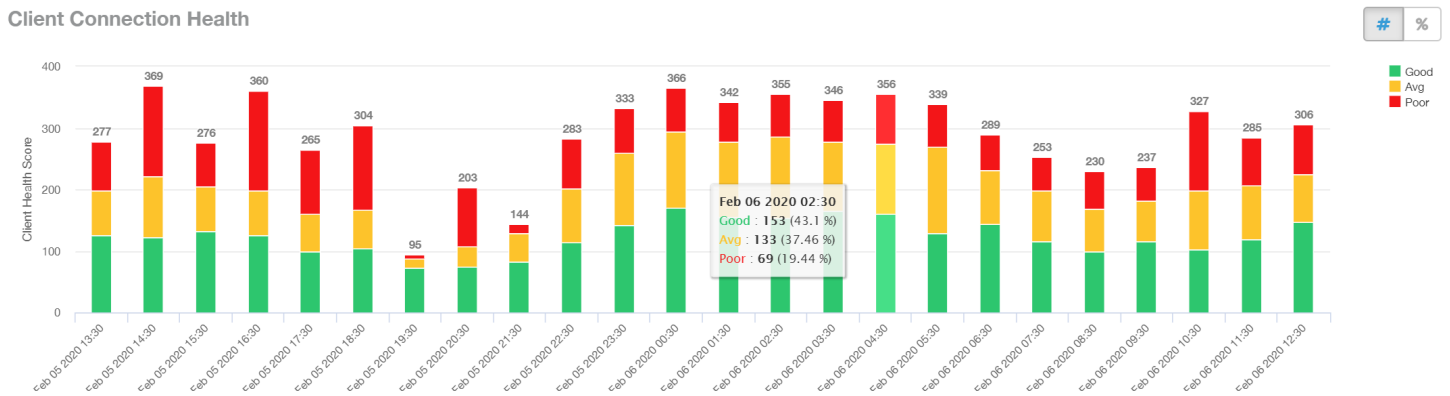
For example, here, out of 1112 clients in total, 149 have good RF health, 287 have average RF health, and 676 clients have poor RF health.



### Client Connection Health Tile

The Client Connection Health chart displays the client health score against a specific time range such as an hour, for example. You can toggle to view the chart in two ways - as (# icon) count, or as (% icon) percentage. Count shows the client health score as good, average, and poor as a stacked color bar, and Percentage shows the percentage of clients at a time (aggregation) as a 100% stacked color bar. You can hover over the bar graph to view more details.

FIGURE 128 Client Health Score: Client Connection Health

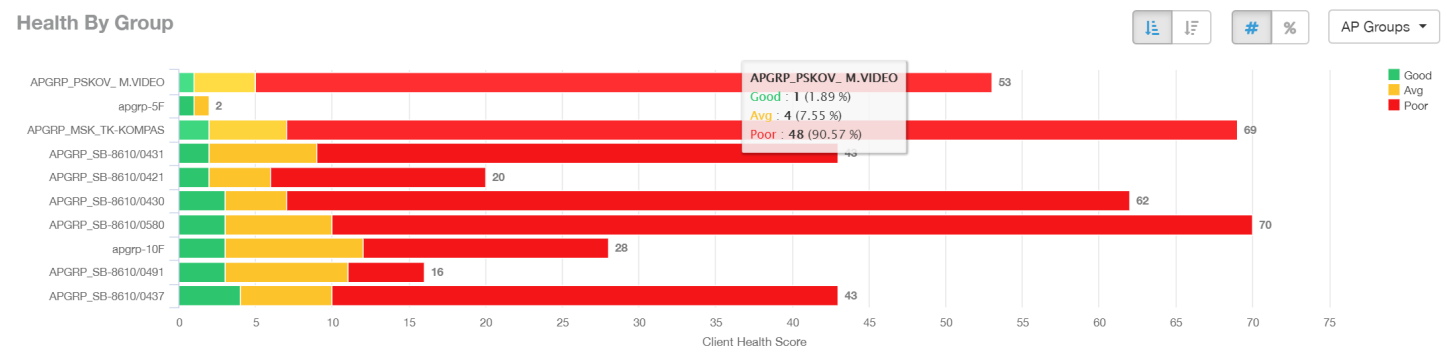


You can toggle the boxes on and off to display or not display clients classified by their score. For example, to only view the clients with a good score, you can disable the yellow and red boxes; you will only see the clients with a good RF health in the graph.

### Health by Group Tile

The Health by Group chart displays the impact of RF health across the group hierarchy, which helps identify top performing and worst performing clients in the network. The group hierarchy level available are System, Domain, Zone, AP, and AP Group. Based on the group selected from the dropdown, stacked color bars are displayed depicting the client score for the group selected.

FIGURE 129 Client Health Score: Health by Group



You can toggle to view the chart in two ways - as (# icon) count, or as (% icon) percentage. Count shows the client health score as good, average, and poor as a stacked color bar, and Percentage shows the percentage of clients at a time (aggregation) as a 100% stacked color bar. You can hover over the bar graph to view more details.

**NOTE**

The top performing values or good scores are used to sort the data.

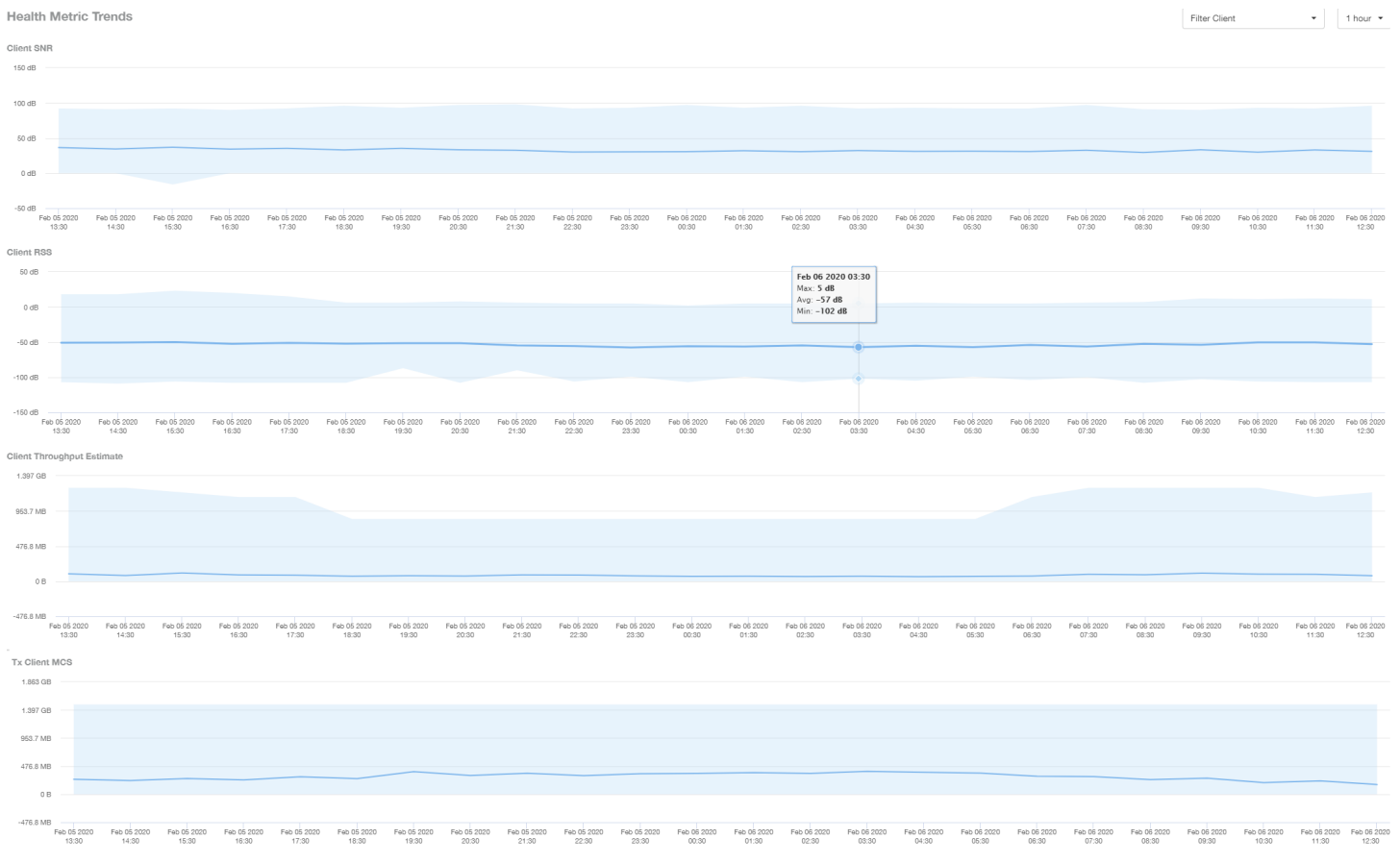
The ascending and descending order icons sort the groups as groups with highest percentage or count of good clients, and highest percentage or count of poor clients, respectively.

You can toggle the boxes on and off to display or not display clients classified by their score.

### Health Metric Trends Graphs

The Health Metric Trend graphs show the raw metrics that are used to compute the client health score; this impacts the header tile, client connection tile, and the health by group tile. The raw metrics used for the computation are RSSI, SNR, MCS (Tx) and client throughput. The graphs are plotted over a range of time. You can also select the time range from the drop-down. Options include 1 hour, 1 day and so on.

FIGURE 130 Client Health Score: Health Metric Trends Graphs



To understand the basis for the health score at a particular date and time, you can view the individual charts for RSSI, SNR, MCS (Tx) and client throughput, at the same date and time. This analysis identifies the raw metric that contributed to the health score computation.

All the four charts display the trends for all the clients that are connected. To view trends for specific clients, you can select the client from the **Filter Client** drop-down. By default, all clients are selected.

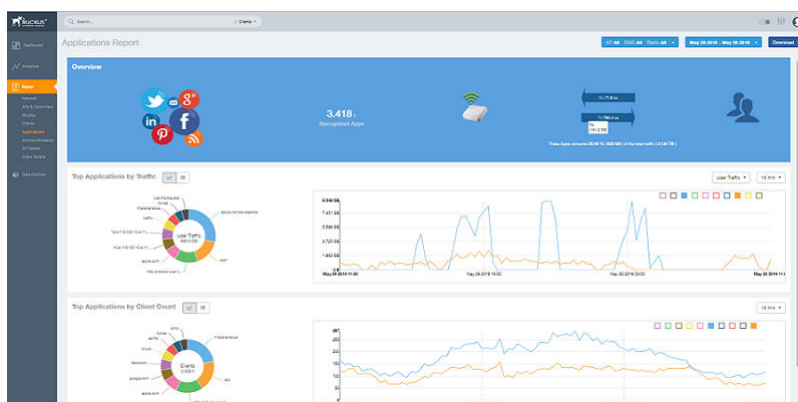
# Applications Report

The **Applications Report** provides the details of the applications accessed by the user.

From the navigation bar, select **Report > Applications**.

The **Applications Report** contains the details of the applications accessed by the user and predefined by RUCKUS Analytics. The overview contains the list of recognized applications. The rest of the report contains the top ten applications by traffic volume received and transmitted over time, client count, traffic, and clients.

**FIGURE 131** Applications Dashboard (Upper Portion Only)



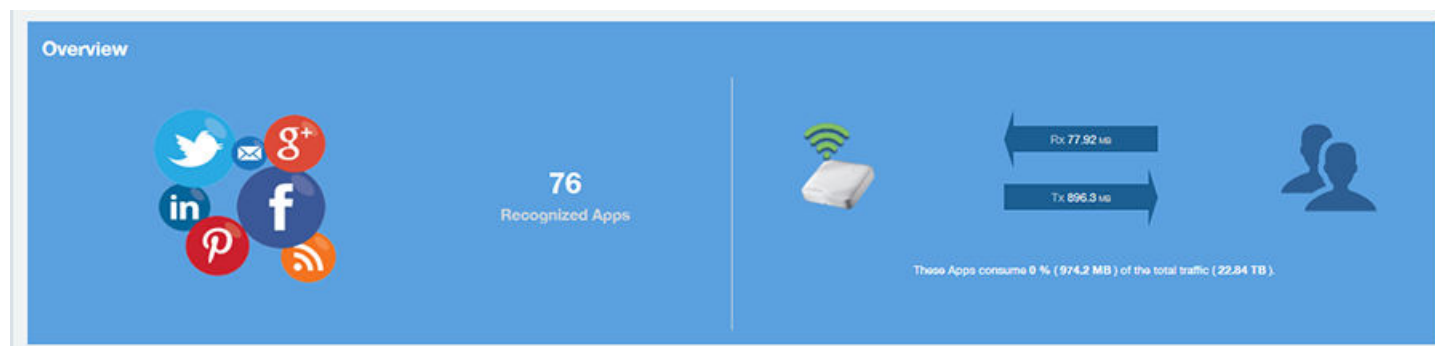
## Overview Tile

The Overview tile of the **Applications Report** provides an overview of all applications recognized by the application-recognition engine and the traffic volumes that these applications consume.

The **Overview** tile displays the following information:

- The number of recognized applications
- Total traffic
- Total number of APs, which also contains the received and transmitted traffic between them
- Total number of clients on the network

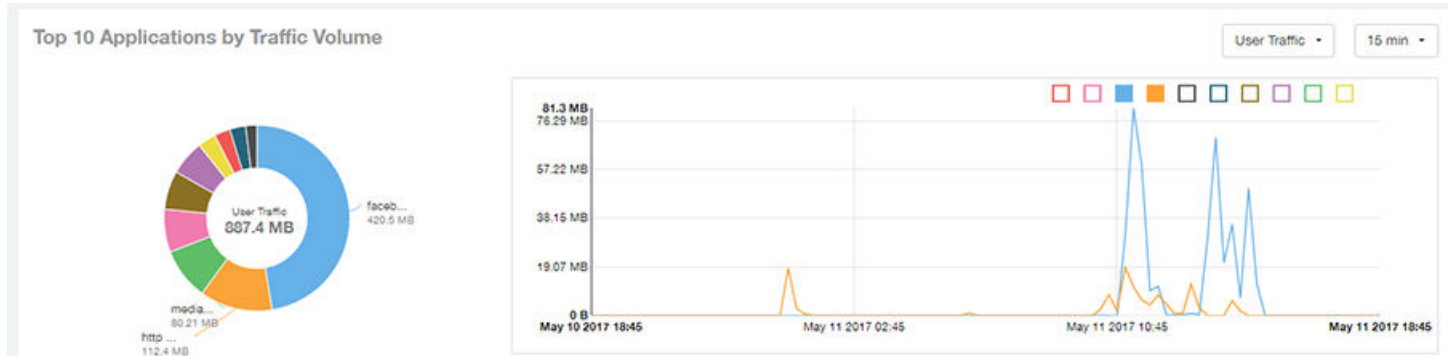
**FIGURE 132** Applications: Overview Tile



## Top Applications by Traffic

The **Top Applications by Traffic** donut chart and graph of the **Applications Report** display the top applications with the largest traffic in the network, along with the received and transmitted traffic.

FIGURE 133 Applications: Top Applications by Traffic Tile





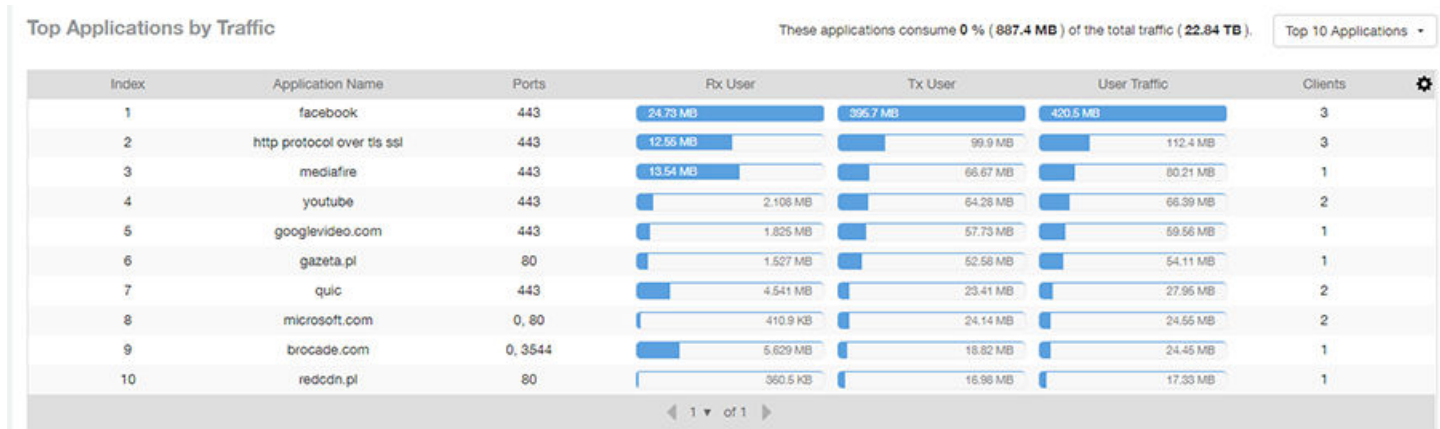
Use the chart and table icons (   ) to toggle between the chart and table views.

FIGURE 134 Applications: Top Applications by Traffic Table

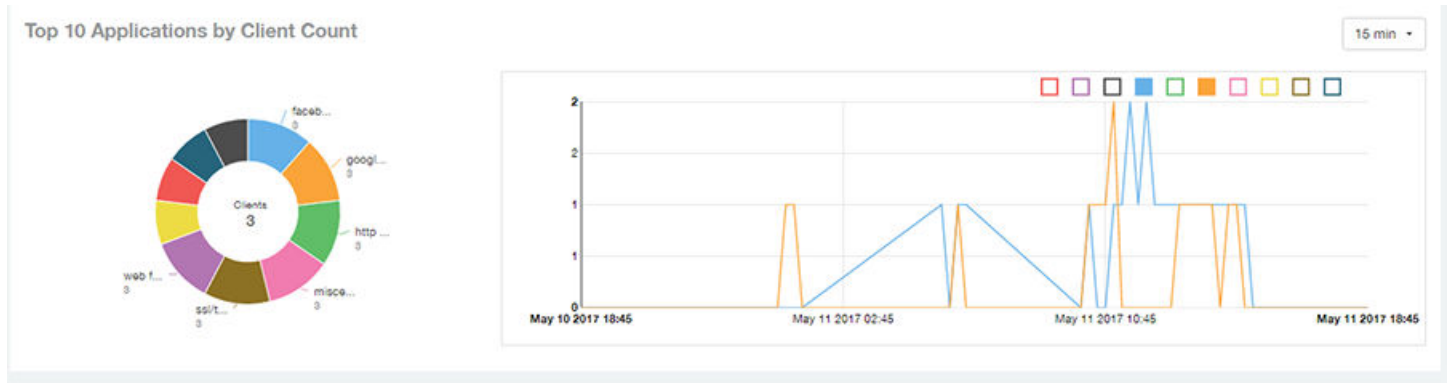


You can view the received and transmitted traffic volumes based on the Rx and Tx filter. In the graph, click any of the colored squares to display the corresponding application details in the line graph. If you pause the pointer over the line graph, an information box is displayed containing the selected details.

## Top Applications by Client Count Tile

The **Top Applications by Client Count** pie chart and graph of the **Applications Report** show the applications that are most frequently being used by the clients in the network over specified time intervals.

FIGURE 135 Applications - Top Applications by Client Count (chart)



Use the chart and table icons ( ) to toggle between the chart and table views.

Click the gear icon ( ) to select the columns to display, and click any column heading to sort the table by that column.

You can select the top 10 (default), 20, 50, or 100 applications to display, or list all applications. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 136 Applications: Top Applications by Client Count Table

Top Applications by Client Count

These applications consume 0% (558.8 MB) of the total traffic (22.84 TB). Top 10 Applications

Index	Application Name	Ports	Clients	Rx User	Tx User	User Traffic
1	facebook	443	3	24.79 MB	395.7 MB	420.5 MB
2	google(ssl)	443	3	70.57 KB	521.2 KB	591.8 KB
3	http protocol over tls ssl	443	3	12.55 MB	99.9 MB	112.4 MB
4	miscellaneous	0, 3544, 443, 5223, 53	3	2.608 MB	3.289 MB	5.896 MB
5	ssl/tls	443, 5223	3	3.032 MB	10.5 MB	13.53 MB
6	web file transfer	0, 80	3	85.6 KB	926.4 KB	1012 KB
7	adkontekst.pl	80	2	62.95 KB	945.2 KB	1008 KB
8	akadns.net	0, 5223	2	3.382 KB	2.291 KB	5.673 KB
9	arp	0	2	29.16 KB	42.6 KB	71.76 KB
10	meteo.pl	80	2	82.4 KB	1.714 MB	1.794 MB

1 of 1

## Airtime Utilization Report

The **Airtime Utilization Report** provides an overview of airtime utilization.

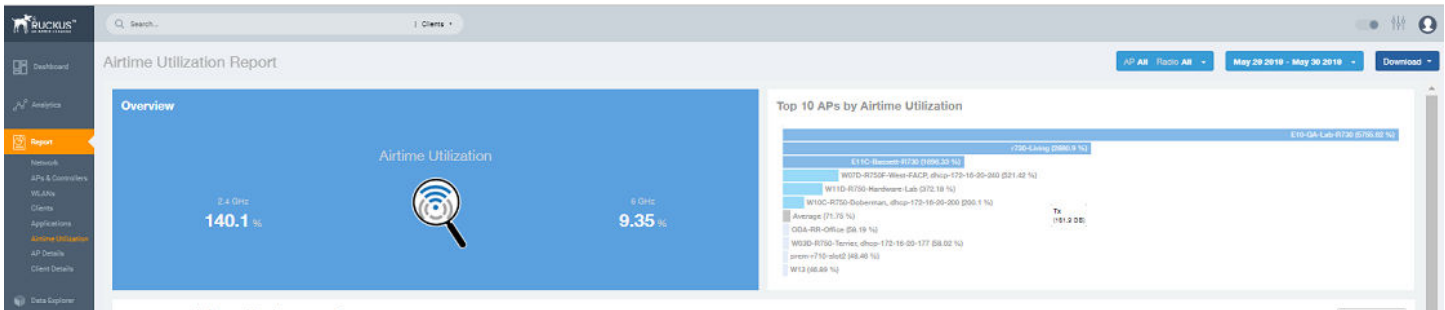
From the navigation bar, select **Report > Airtime Utilization**.

The **Airtime Utilization Report** lists the APs by airtime utilization for radio 2.4 GHz and 5 GHz. It also lists the airtime utilization trend over time based on APs and radio.

## Report

### Airtime Utilization Report

FIGURE 137 Airtime Utilization Report (Upper Portion Only)



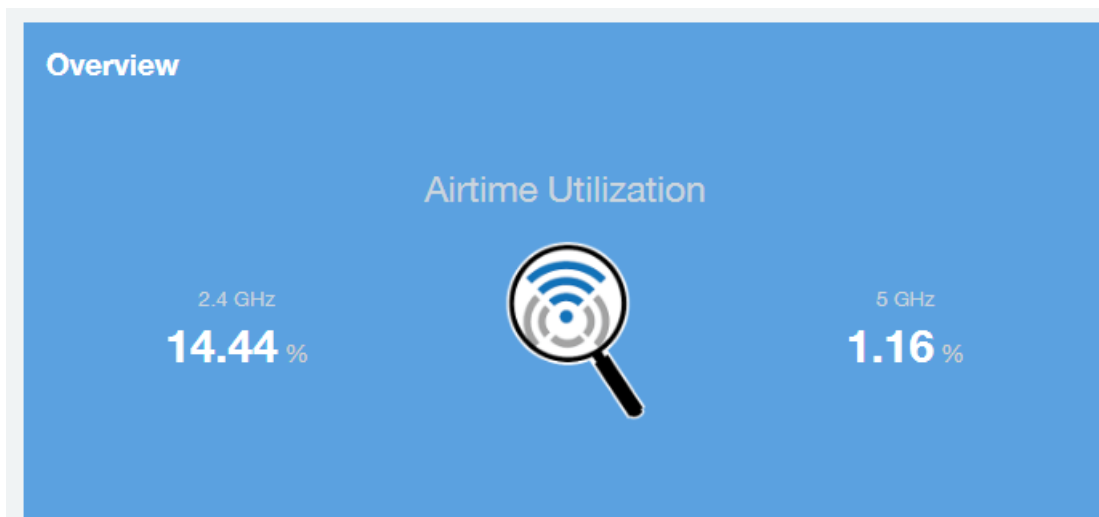
The Airtime Utilization Report consists of the following components:

- Overview tile
- Top 10 APs by Airtime Utilization chart
- Top APs by Airtime Utilization for 2.4 GHz table
- Top APs by Airtime Utilization for 5 GHz table
- Airtime Utilization Trend graphs

## Overview Tile

The **Overview** tile of the **Airtime Utilization Report** displays the aggregate utilization rates for all of the 2.4-GHz and 5-GHz radios on all APs for the selected time period.

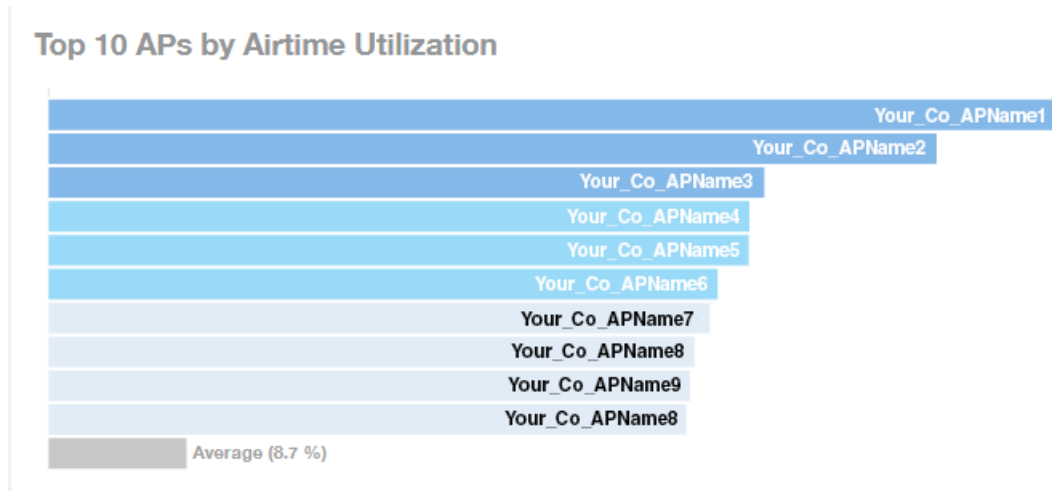
FIGURE 138 Airtime Utilization: Overview Tile



## Top 10 APs by Airtime Utilization Chart

Use the **Top 10 APs by Airtime Utilization** chart to view which APs have the highest airtime utilization percentage rates.

FIGURE 139 Top 10 APs by Airtime Utilization Chart



## Top APs by Airtime Utilization for 2.4 GHz Table

The **Top APs by Airtime Utilization for 2.4 GHz** table displays which APs have the highest utilization on the 2.4 GHz radio.

Use this table to view a list the top APs with the highest airtime utilization sorted according to the selected columns. Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column.

You can select the top 10 (default), 20, 50, or 100 APs by airtime utilization to display. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 140 Top APs by Airtime Utilization for 2.4 GHz Table

Top APs by Airtime Utilization for 2.4 GHz Top 10 APs ▾

Index	AP Name	AP IP Address	Controller Name	Airtime Utilization	Airtime Rx	Airtime Tx	Airtime Busy	⚙️
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	69.07 %	17.04 %	0 %	62.03 %	
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName2	63.56 %	30.74 %	0 %	32.82 %	
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName3	62.14 %	48.92 %	6.86 %	6.37 %	
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName4	59.01 %	47.19 %	4.08 %	7.75 %	
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName5	56.97 %	40.54 %	11.92 %	4.52 %	
6	Your_Co_APName6	10.x.y.6	Your_Co_CTName6	56.39 %	23.04 %	0.03 %	33.32 %	
7	Your_Co_APName7	10.x.y.7	Your_Co_CTName7	56.02 %	26.77 %	0 %	29.25 %	
8	Your_Co_APName8	10.x.y.8	Your_Co_CTName8	53.36 %	42.26 %	3.89 %	7.24 %	
9	Your_Co_APName9	10.x.y.9	Your_Co_CTName9	52.73 %	43.24 %	4.36 %	5.13 %	
10	Your_Co_APName10	10.x.y.10	Your_Co_CTName10	52.64 %	45.71 %	2.45 %	4.48 %	

◀ 1 ▾ of 1 ▶

## Top APs by Airtime Utilization for 5 GHz Table

The **Top APs by Airtime Utilization for 5 GHz** table of the **Airtime Utilization Report** displays which APs have the highest utilization on the 5 GHz radio.

## Report

### Airtime Utilization Report

Use this table to view a list of the top APs with the highest airtime utilization sorted by the selected columns. Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column.

You can select the top 10 (default), 20, 50, or 100 APs by airtime utilization to display. The number of rows in a page is defined by the **Rows per Page** option in the table settings menu.

**FIGURE 141** Top APs by Airtime Utilization for 5 GHz Table

Top APs by Airtime Utilization for 5 GHz Top 10 APs ▾

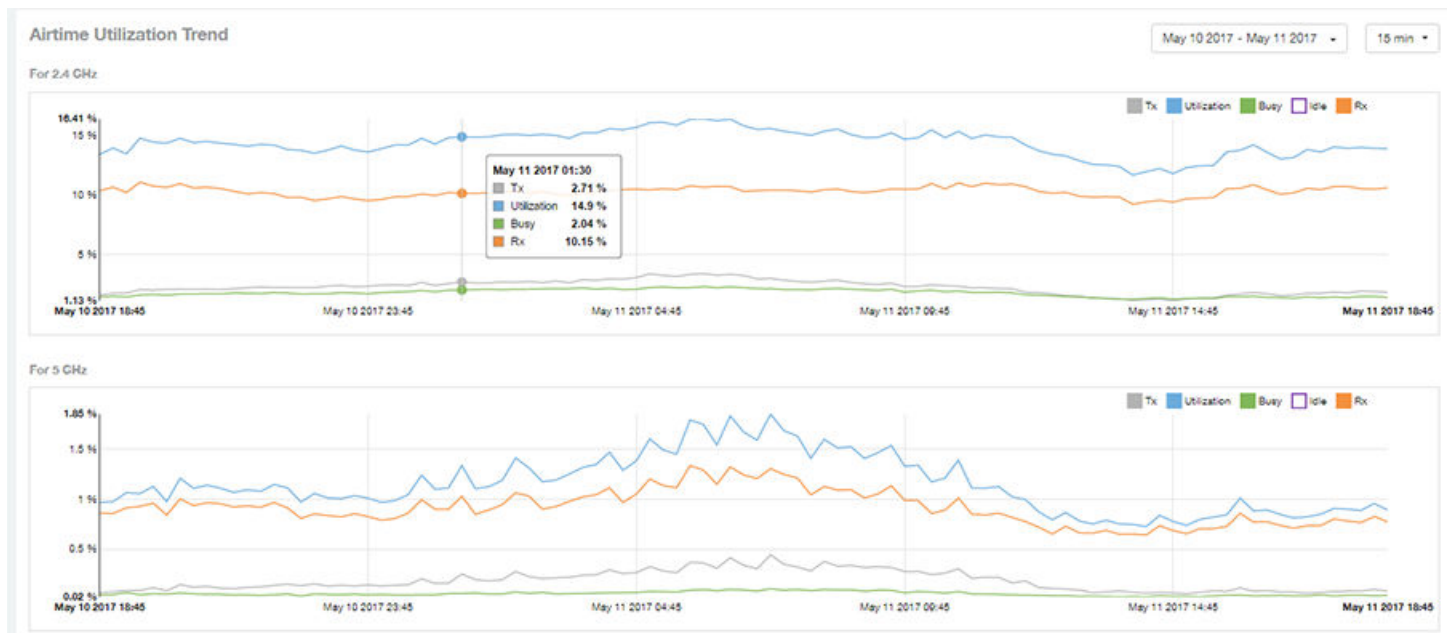
Index	AP Name	AP IP Address	Controller Name	Airtime Utilization	Airtime Rx	Airtime Tx	Airtime Busy
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	74.25 %	72.91 %	0 %	1.34 %
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName1	59.35 %	58.26 %	0 %	1.09 %
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName1	58.29 %	57.54 %	0 %	0.78 %
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName1	55.36 %	53.99 %	0.36 %	1.01 %
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName1	55.08 %	53.78 %	0.45 %	0.85 %
6	Your_Co_AccessPoint1	172.16.z.1	Your_Co_Controller2	54.36 %	54.18 %	0.05 %	0.12 %
7	Your_Co_AccessPoint2	172.16.z.2	Your_Co_Controller2	54.05 %	53.81 %	0 %	0.27 %
8	Your_Co_AccessPoint3	172.16.z.3	Your_Co_Controller2	49.03 %	48.77 %	0.08 %	0.18 %
9	Your_Co_AccessPoint4	172.16.z.4	Your_Co_Controller2	48.88 %	47.47 %	0.95 %	0.45 %
10	Your_Co_AccessPoint5	172.16.z.5	Your_Co_Controller2	46.03 %	45.95 %	0.02 %	0.05 %

◀ 1 of 1 ▶

## Airtime Utilization Trend Graph

The **Airtime Utilization Trend** graph shows the airtime utilization trends for 2.4-GHz and 5-GHz radios in percentages over time.

**FIGURE 142** Airtime Utilization Trend Graph Trends





## Airtime Utilization Over Time Table

Use the **Airtime Utilization Over Time** table to compare utilization rates between time periods, and to examine specific airtime utilization data, such as time spent busy or idle, transmitting or receiving,, and user traffic compared management traffic.

FIGURE 143 Airtime Utilization Over Time Table

Time Period	2.4 GHz Utilization	2.4 GHz Rx	2.4 GHz Tx	2.4 GHz Busy	5 GHz Utilization	5 GHz Rx	5 GHz Tx	5 GHz Busy
May 10 2017 18:45 - 18:59	13.43 %	10.37 %	1.61 %	1.45 %	0.97 %	0.86 %	0.06 %	0.04 %
May 10 2017 19:00 - 19:14	13.96 %	10.67 %	1.76 %	1.62 %	0.98 %	0.86 %	0.07 %	0.04 %
May 10 2017 19:15 - 19:29	13.46 %	10.22 %	1.78 %	1.46 %	1.07 %	0.91 %	0.09 %	0.07 %
May 10 2017 19:30 - 19:44	14.78 %	11.09 %	2.07 %	1.63 %	1.06 %	0.93 %	0.09 %	0.04 %
May 10 2017 19:45 - 19:59	14.46 %	10.76 %	2.04 %	1.66 %	1.13 %	0.96 %	0.11 %	0.06 %
May 10 2017 20:00 - 20:14	14.37 %	10.66 %	2.1 %	1.61 %	0.98 %	0.84 %	0.08 %	0.06 %
May 10 2017 20:15 - 20:29	14.77 %	10.96 %	2.11 %	1.7 %	1.21 %	1 %	0.16 %	0.06 %
May 10 2017 20:30 - 20:44	14.41 %	10.61 %	2.1 %	1.71 %	1.11 %	0.94 %	0.12 %	0.06 %
May 10 2017 20:45 - 20:59	14.62 %	10.67 %	2.11 %	1.73 %	1.14 %	0.96 %	0.13 %	0.06 %
May 10 2017 21:00 - 21:14	14.37 %	10.66 %	2.08 %	1.72 %	1.11 %	0.96 %	0.11 %	0.06 %

## AP Details Report

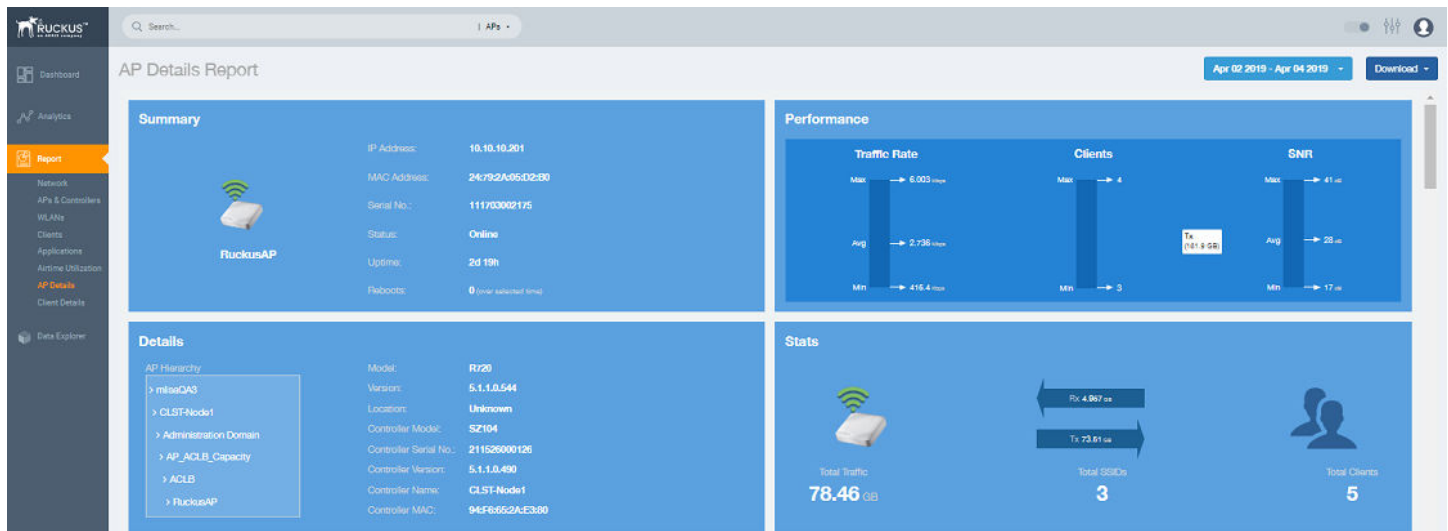
The **AP Details Report** provides details about one specific access point.

From the navigation bar, select **Report > AP Details** and enter the MAC address of the AP for which you want to view the details.

### NOTE

You can reach the **AP Details Report** by clicking the link to an AP name in another report.

FIGURE 144 AP Details Report (Upper Portion Only)



The **AP Details Report** consists of the following components:

- Summary file

## Report

### AP Details Report

- Performance tile
- Details tile
- Stats tile
- Uptime History graph
- Traffic Trend graphs
- Unique Clients Trend Over Time graphs
- Top 10 Clients by Traffic Volume tile
- Top 10 Applications by Traffic Volume tile
- Top SSIDs by Traffic table
- Sessions table
- RSS Trend graph
- SNR Trend graph
- Airtime Utilization Trend graphs
- Clients Details table
- Alarms table
- Events table
- Anomalies graph

## Summary Tile

The **Summary** tile of the **AP Details Report** displays basic information about a specific AP.

**FIGURE 145** AP Details: Summary Tile



## Performance Tile

The **Performance** tile of the **AP Details Report** displays performance data about the specified AP.

FIGURE 146 AP Details: Performance Tile

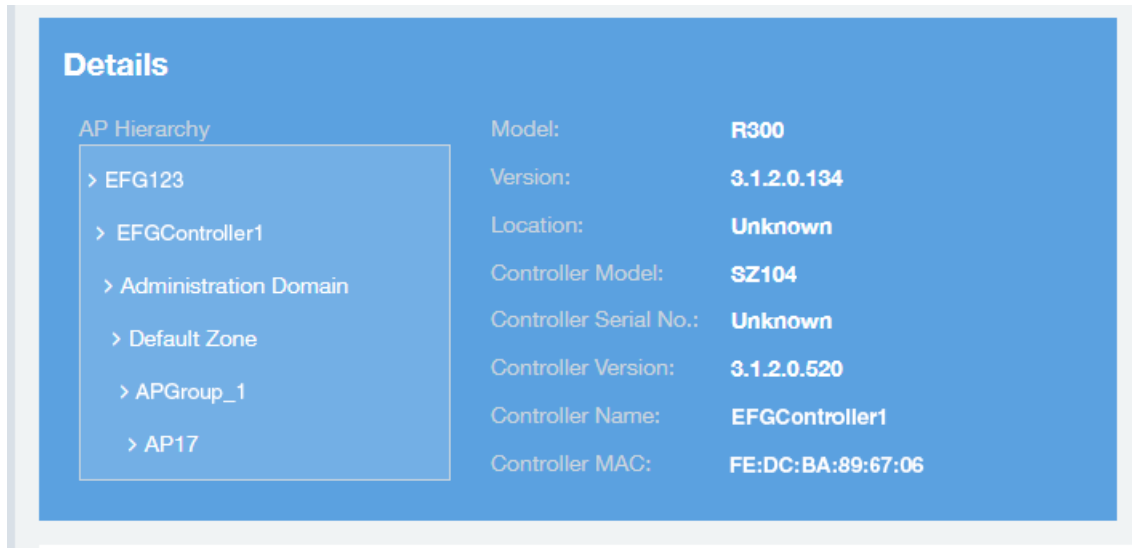


## Details Tile

The **Details** tile of the **AP Details Report** contains some details about the specified AP, including its hierarchy in the network.

The AP shown in this example is named AP17. It belongs to a group of access points that has been named APGroup\_1. EFGController1 in this example is one of the controllers being used on a wireless network named EFG123.

FIGURE 147 AP Details: Details Tile



## Stats Tile

The **Stats** tile of the **AP Details Report** displays some traffic statistics about the specified AP.

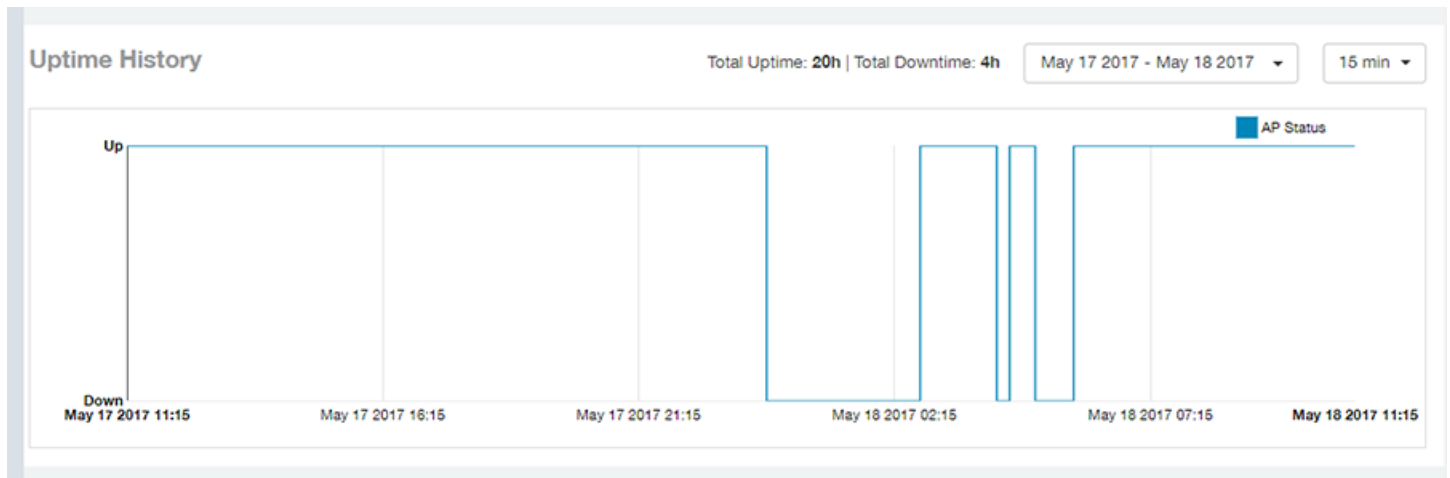
FIGURE 148 AP Details: Stats Tile



## Uptime History Graph

The **Uptime History** graph of the **AP Details Report** shows when this AP has been up or down over different time periods. The blue bar indicates when the AP has been up or down. Use the menus to specify the time frame and the granularity of the graph.

FIGURE 149 AP Details: Uptime History Graph



## Traffic Trend Graphs

The **Traffic Trend** graphs of the **AP Details Report** contain four line graphs that provide information about the specified AP: two types of line graphs that depict traffic by usage and two types of line graphs that depict traffic by radio type for this AP.

Use the menus to specify the time frame and the granularity of the graphs.

FIGURE 150 AP Details: Traffic Trend Graphs



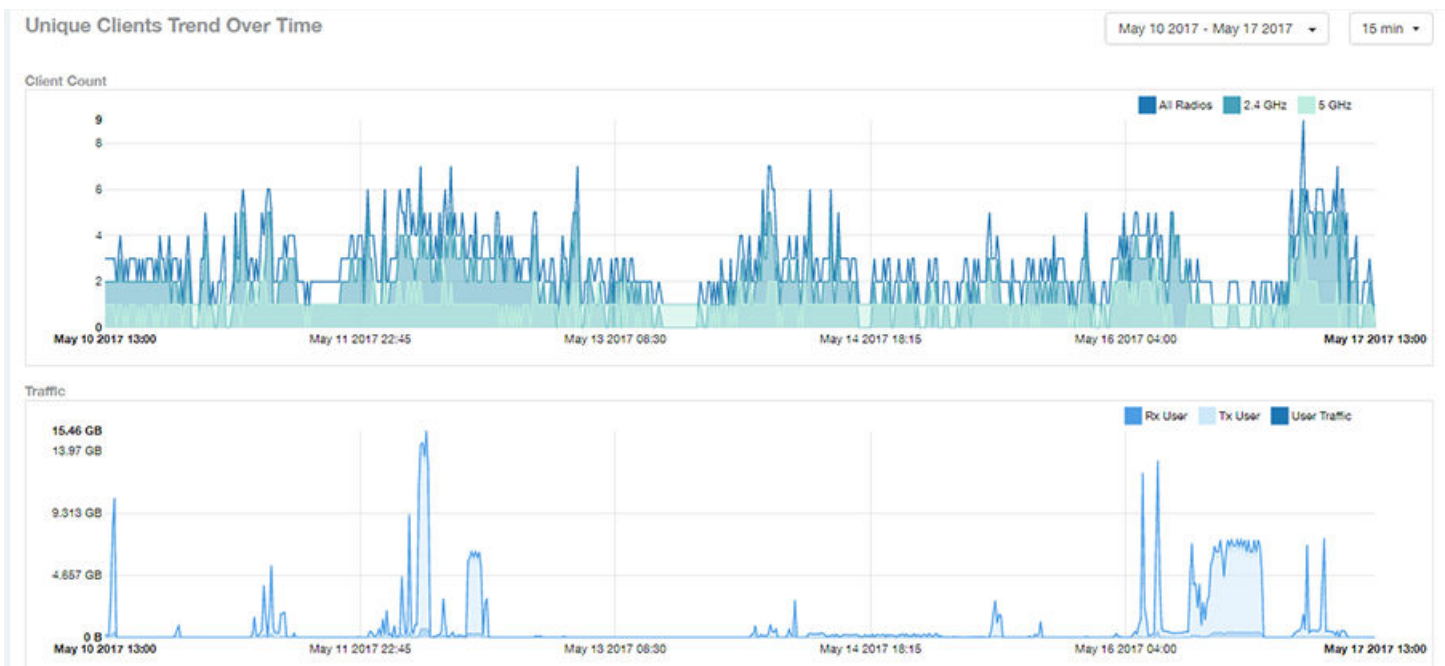
## Unique Clients Trend Over Time Graphs

The **Unique Clients Trend Over Time** graphs of the **AP Details Report** contain two line graphs that provide information about unique clients associated with the specified AP over a certain time period.

One graph shows the number of unique clients and the other shows the traffic generated by unique clients.

Use the menus to specify the time frame and the granularity of the graphs.

FIGURE 151 AP Details: Unique Clients Trend Over Time Graphs



## Top 10 Clients by Traffic Volume Tile

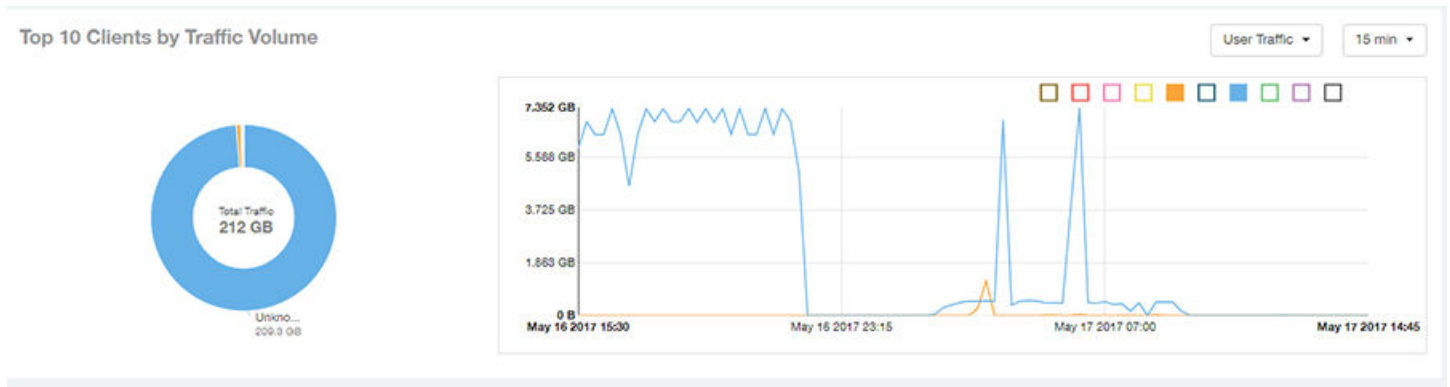
The **Top 10 Clients by Traffic Volume** donut chart and line graph of the **AP Details Report** depict the clients that have generated the largest volume of traffic over this AP for a specified period of time.

Use the menus to specify the time type and the granularity of the graph. In the graph, click any of the colored squares to display the corresponding client details in the line graph.

### NOTE

If you click one of the clients listed in the donut chart, you will be taken to the **Client Details Report** for that client.

FIGURE 152 AP Details: Top 10 Clients by Traffic Volume Tile



## Top 10 Applications by Traffic Volume Tile

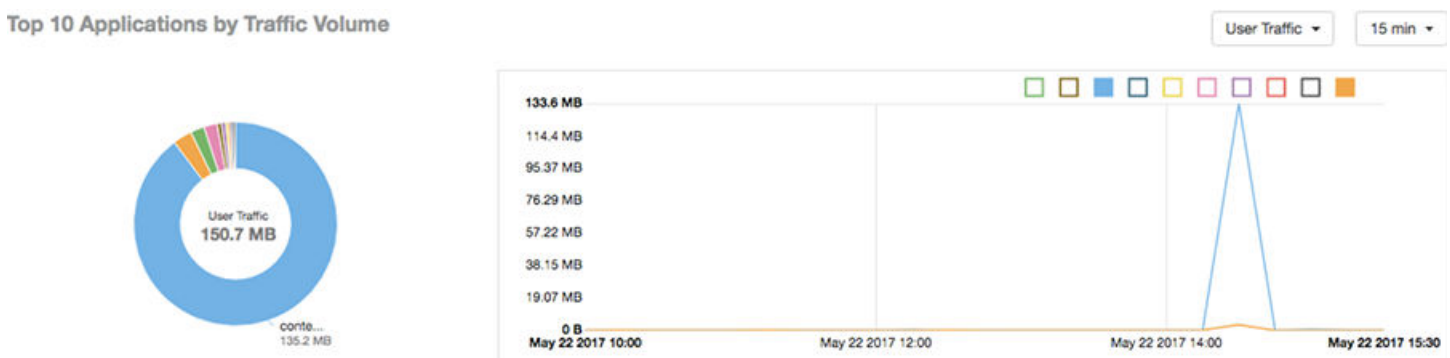
The **Top 10 Applications by Traffic Volume** donut chart and line graph of the **AP Details Report** depict the applications that have generated the largest volume of traffic over this AP for a specified period of time.

Use the menus to specify the traffic type and the granularity of the graph. In the graph, click any of the colored squares to display the corresponding application details in the line graph.

### NOTE

Click the table icon to display a table showing the same information.

FIGURE 153 AP Details: Top 10 Applications by Traffic Volume Tile



## Top SSIDs by Traffic Table

The **Top SSIDs by Traffic** table of the **AP Details Report** lists the SSIDs that have generated the most traffic associated with this AP.

A service set identifier (SSID) is a logical group of APs. An AP can belong to multiple SSIDs. Use the menu to specify the number of SSIDs to display.

FIGURE 154 AP Details: Top SSIDs by Traffic Table

Index	SSID Name	Rx Total	Tx Total	Total Traffic	Clients	APs
1	Your_Co_SSID_Name1	11.02 GB	201.3 GB	212.3 GB	32	1

## Sessions Table

The **Sessions** table of the **AP Details Report** provides details for the number of client sessions that you specify for this AP.

Use the menu to specify how many sessions to display.

If you click one of the client links in the **Hostname** column, you are directed to the **Client Details Report** for that client.

FIGURE 155 AP Details: Sessions Table

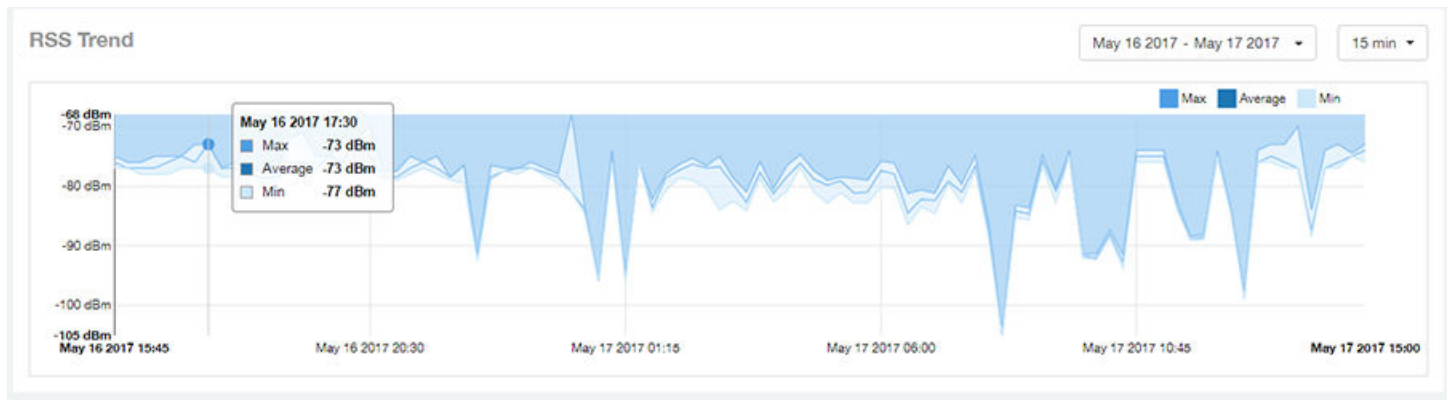
First Connection	Disconnect Time	Session Duration	Hostname	SSID	Radio	Rx User	Tx User	User Traffic
May 17 2017 14:30	May 17 2017 14:46	16m 6s	<a href="#">EFGHost1</a>	EFGSSID1	5 GHz	13.04 KB	13.35 KB	26.38 KB
May 17 2017 13:08	May 17 2017 14:23	1h 14m	<a href="#">EFGHost2</a>	EFGSSID1	5 GHz	39.36 KB	40.04 KB	79.42 KB
May 17 2017 14:02	May 17 2017 14:03	36.27s	<a href="#">EFGHost3</a>	EFGSSID1	2.4 GHz	16.6 KB	15.52 KB	32.12 KB
May 17 2017 12:55	May 17 2017 12:59	3m 57s	<a href="#">EFGHost4</a>	EFGSSID1	2.4 GHz	7.681 KB	14.39 KB	22.07 KB
May 17 2017 12:41	May 17 2017 12:43	2m 33s	<a href="#">EFGHost5</a>	EFGSSID1	5 GHz	13.61 KB	13.41 KB	27.02 KB
May 17 2017 09:19	May 17 2017 12:34	3h 15m	<a href="#">EFGHost6</a>	EFGSSID1	5 GHz	134.7 KB	150.2 KB	285 KB

## RSS Trend Graph

The **RSS Trend** graph of the **AP Details Report** depicts the received signal strength trends over time for this AP.

Use the menus to specify the time frame and the granularity of the graph.

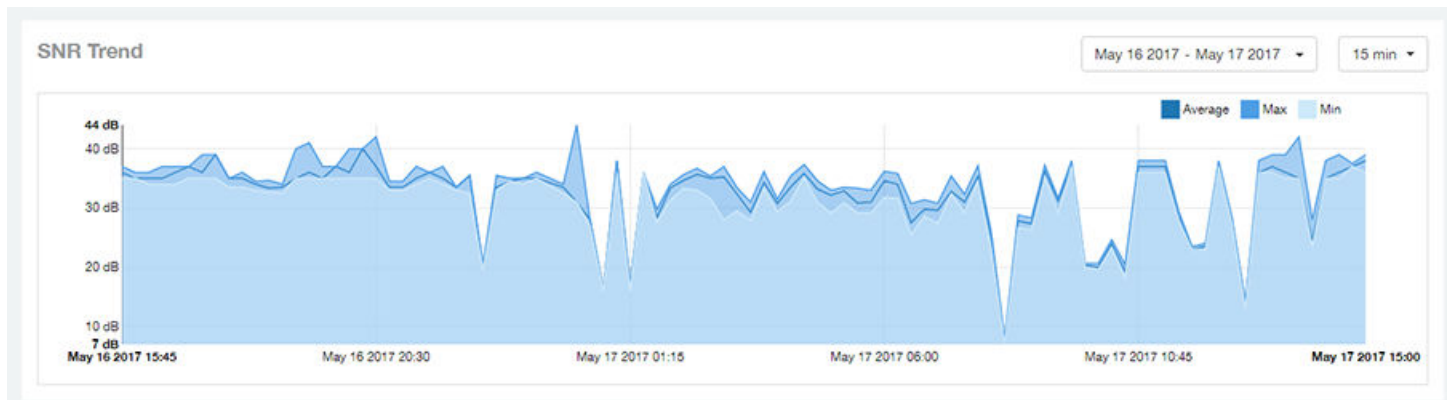
FIGURE 156 AP Details: RSS Trend Graph



## SNR Trend Graph

The SNR Trend graph of the AP Details Report depicts the signal-to-noise ratio over time for this AP. Use the menus to select the time frame and the granularity for the graph.

FIGURE 157 AP Details: SNR Trend Graph

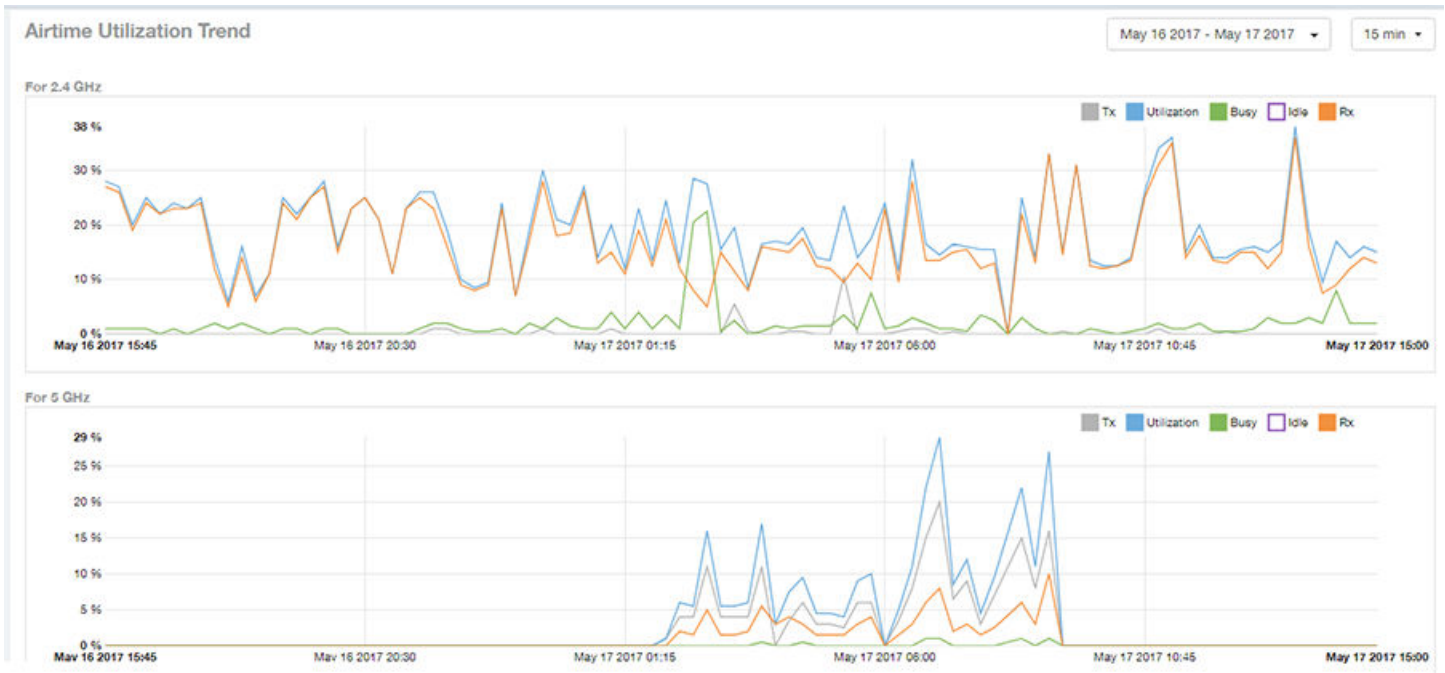


## Airtime Utilization Trend Graphs

The Airtime Utilization Trend graphs of the AP Details Report depict the airtime utilization for this AP, by radio type, over a specified time period. Use the menus to select the time frame and the granularity for the graphs.



FIGURE 158 AP Details: Airtime Utilization Trend Graphs



## Clients Details Table

The **Clients Details** table of the **AP Details Report** provides details for the number of top clients that you specify for this AP.

Use the menu to specify how many top clients to display.

If you click one of the client links in the **Hostname** column, you are directed to the **Client Details Report** for that client.

FIGURE 159 AP Details: Clients Details Table

Clients Details These clients consume 100 % (206.1 GB) of all user traffic (206.1 GB). Top 10 Clients

Index	Hostname	IP Address	Username	Sessions	Rx User	Tx User	User Traffic
1	<a href="#">EFGHost1</a>	10.x.y.1	Your_Co_UserName1	25	10.47 GB	193 GB	203.4 GB
2	<a href="#">EFGHost2</a>	10.x.y.2	Your_Co_UserName2	8	71.58 MB	1.529 GB	1.599 GB
3	<a href="#">EFGHost3</a>	10.x.y.3	Your_Co_UserName3	6	66.91 MB	447.6 MB	514.5 MB
4	<a href="#">EFGHost4</a>	10.x.y.4	Your_Co_UserName4	2	64.17 MB	357 MB	421.2 MB
5	<a href="#">EFGHost5</a>	10.x.y.5	Your_Co_UserName5	6	27.72 MB	63.57 MB	91.29 MB
6	<a href="#">EFGHost6</a>	10.x.y.6	Your_Co_UserName6	62	6.688 MB	53.04 MB	59.73 MB
7	<a href="#">EFGHost7</a>	10.x.y.7	Your_Co_UserName7	9	785.6 KB	810.9 KB	1.559 MB
8	<a href="#">Your_Co_HostName8</a>	10.x.y.8	Your_Co_UserName8	1	140.4 KB	815.2 KB	955.6 KB
9	<a href="#">Your_Co_HostName9</a>	10.x.y.9	Your_Co_UserName9	1	165.3 KB	272.4 KB	457.7 KB
10	<a href="#">Your_Co_HostName10</a>	10.x.y.10	Your_Co_UserName10	3	147.8 KB	174.1 KB	321.8 KB

◀ 1 of 1 ▶

## Alarms Table

The **Alarms** table of the **AP Details Report** lists the alarms generated for this AP for the time period that you specify.

Use the menu to specify how many alarms to display.

Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column.

FIGURE 160 AP Details: Alarms Table

Time	Alarm Code	Alarm Type	Severity	Reason	⚙️
May 18 2017 11:15	302	apRebootBySystem	Major	AP lost Gateway more than 18...	
May 18 2017 10:01	303	apConnectionLost	Major	Unknown	
May 17 2017 22:24	302	apRebootBySystem	Major	AP lost Gateway more than 18...	
May 17 2017 21:21	303	apConnectionLost	Major	Unknown	
May 17 2017 18:54	302	apRebootBySystem	Major	AP lost Gateway more than 18...	

1 of 1

## Events Table

The **Events** table of the **AP Details Report** lists the events generated for this AP for the time period that you specify.

Use the menu to specify how many events to display.

Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column.

FIGURE 161 AP Details: Events Table

Time	Event Code	Event Type	Reason	⚙️
May 17 2017 14:57	202	clientJoin	Unknown	
May 17 2017 14:46	205	clientInactivityTimeout	Unknown	
May 17 2017 14:30	202	clientJoin	Unknown	
May 17 2017 14:23	205	clientInactivityTimeout	Unknown	
May 17 2017 14:03	204	clientDisconnect	Unknown	
May 17 2017 14:02	209	clientRoaming	Unknown	
May 17 2017 13:08	202	clientJoin	Unknown	
May 17 2017 12:59	205	clientInactivityTimeout	Unknown	
May 17 2017 12:55	209	clientRoaming	Unknown	
May 17 2017 12:48	306	apChannelChanged	Unknown	

1 of 33

## Anomalies Graph

The **Anomalies** graph of the **AP Details Report** provides information about any behavior that may be out of the normal range for this AP, such as high reboot count, unusually high or low user traffic, unusually high or low client count, or unusually high or low session count.

## Client Details Report

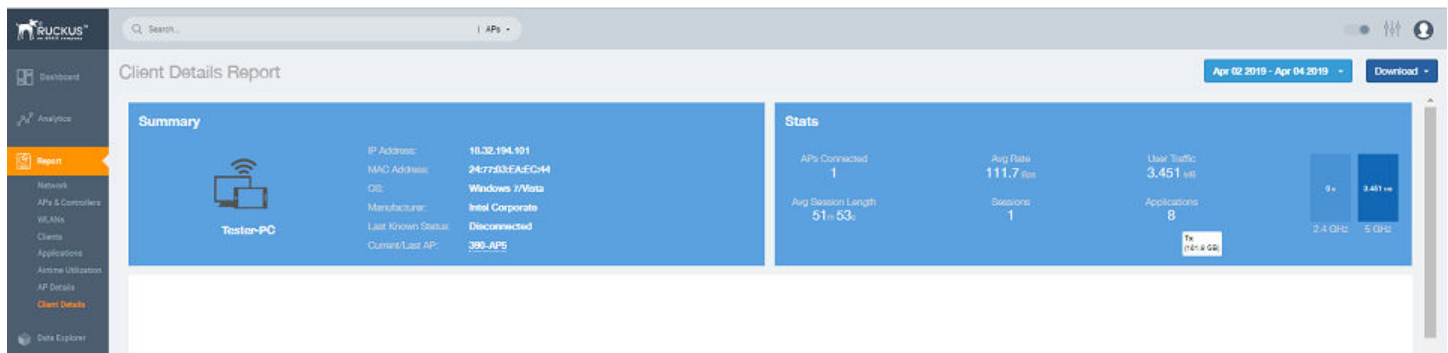
The Client Details report provides details about one specific client.

From the navigation bar, select **Report** > **Client Details** and enter the MAC address of the client for which you want to view the details.

### NOTE

You can reach the **Client Details Report** by clicking the link to a client name in another report.

**FIGURE 162** Client Details Report (Upper Portion Only)



The Wired Report consists of the following components:

- Summary tile
- Stats tile
- Traffic Trend tile
- RSS Trend tile
- SNR Trend tile
- Sessions tile

## Summary Tile

The Summary section of the Client Details report displays basic information about a specific client.

The hostname for the client shown in this example is XYZ123.

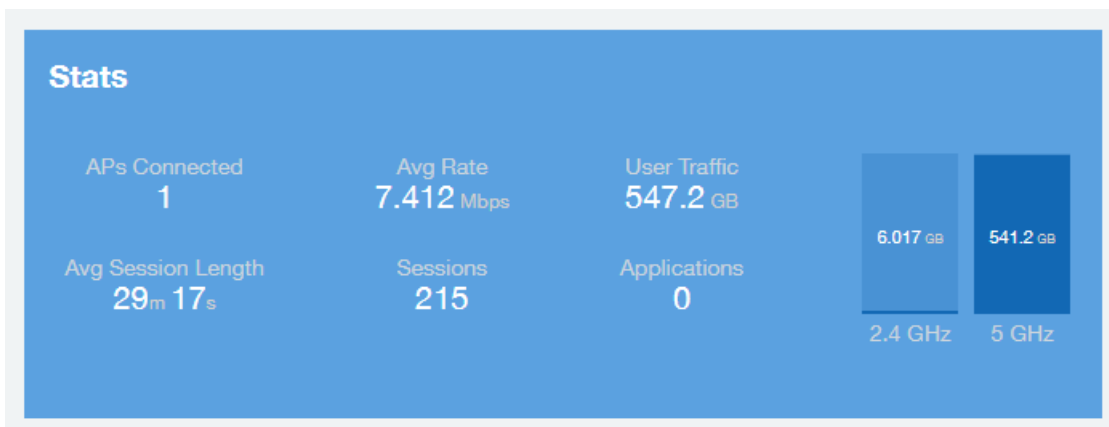
FIGURE 163 Client Details - Summary



## Stats Tile

The Stats section of the Client Details report shows statistics for the specified client.

FIGURE 164 Client Details - Stats



## Client Details Stats

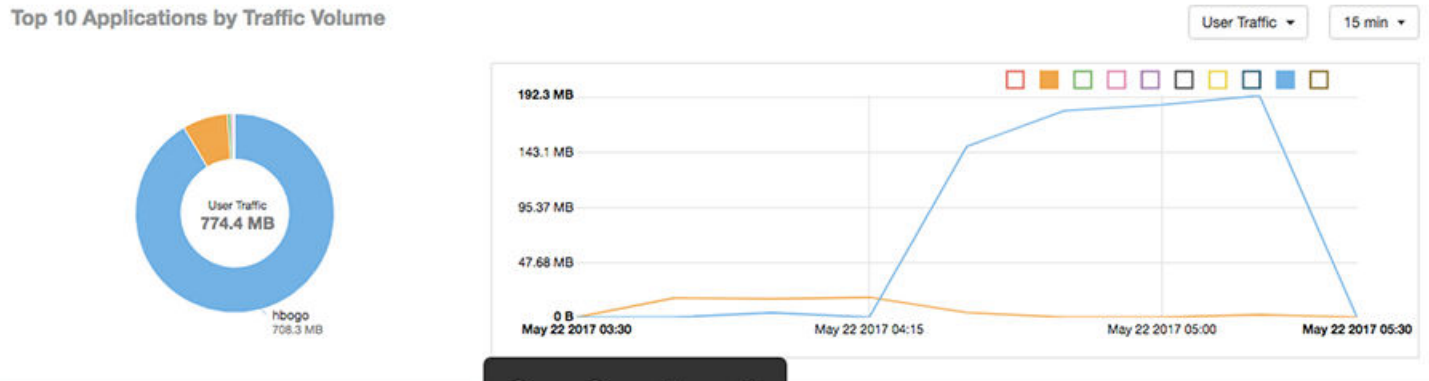
The Client Details - Top 10 Applications by Traffic Volume pie chart and graph show the applications run by this client that have the largest traffic volume.

Use the menus to specify the traffic type and the granularity of the graph. In the graph, click any of the colored squares to display the corresponding application details in the line graph.

**NOTE**

You can click the Table icon to toggle to a table of this same information.

FIGURE 165 Client Details: Top 10 Applications by Traffic Volume Tile

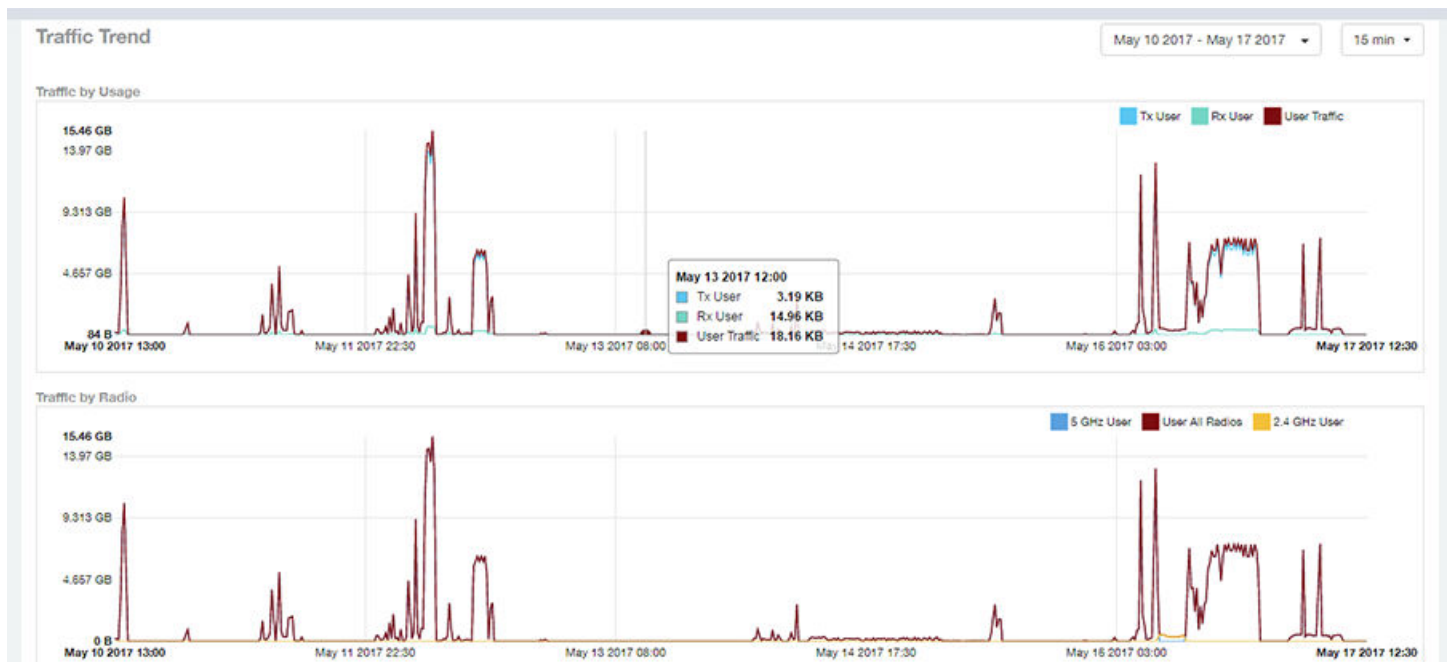


## Traffic Trend Tile

The Traffic Trend graphs of the Client Details report depict traffic by usage and traffic by radio type for the client.

Use the menu to select the time frame and granularity for the graphs.

FIGURE 166 Client Details - Traffic Trend Graphs

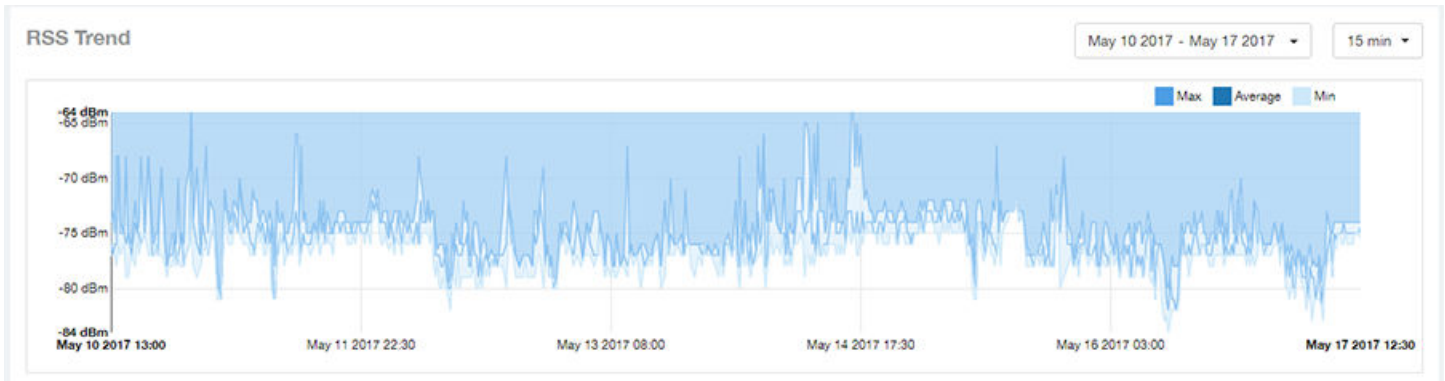


## RSS Trend Tile

The RSS Trend graph of the Client Details report depicts the received signal strength trends over time for this client.

Use the menus to specify the time frame and the granularity of the graph.

FIGURE 167 Client Details - RSS Trend Graph

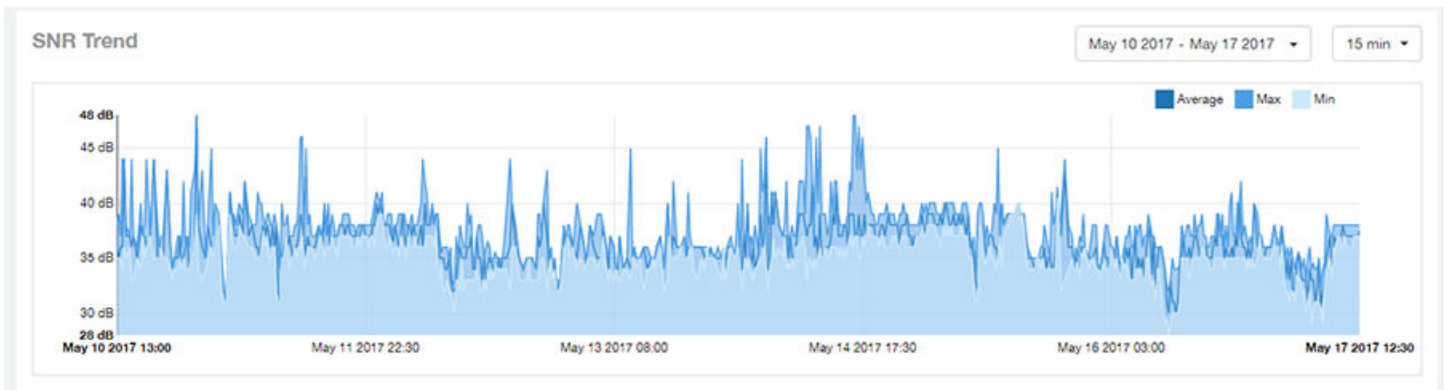


## SNR Trend Tile

The SNR Trend graph of the Client Details report depicts the signal-to-noise ratio over time for this client.

Use the menu to select the time frame and granularity for this graph.

FIGURE 168 Client Details - SNR Trend Graph



## Sessions tile

The Sessions table of the Client Details report provides details for sessions between this client and associated access points.

Use the menu to select the number of sessions you want to display.

Click the gear icon (⚙️) to select the columns to display, and click any column heading to sort the table by that column.

### NOTE

If you click one of the **AP Name** links, you will be taken to the **AP Details Report** for that AP.

FIGURE 169 Client Details: Sessions Table

Sessions									Last 1,000 Sessions ▾
First Connection	Disconnect Time	Session Duration	AP Name	SSID	Radio	Rx User	Tx User	User Traffic	⚙
May 17 2017 12:41	May 17 2017 12:43	2m 33s	AP750	SSID17	5 GHz	13.61 KB	13.41 KB	27.02 KB	
May 17 2017 09:19	May 17 2017 12:34	3h 15m	AP750	SSID17	5 GHz	134.7 KB	150.2 KB	285 KB	
May 17 2017 07:55	May 17 2017 09:19	1h 24m	AP750	SSID17	5 GHz	116.4 MB	2.418 GB	2.532 GB	
May 17 2017 07:19	May 17 2017 07:46	27m 6s	AP750	SSID17	5 GHz	37.69 MB	763.9 MB	801.6 MB	
May 17 2017 06:17	May 17 2017 07:16	58m 59s	AP750	SSID17	5 GHz	113.9 MB	1.714 GB	1.826 GB	
May 17 2017 04:16	May 17 2017 06:17	2h	AP750	SSID17	5 GHz	178.9 MB	3.484 GB	3.669 GB	
May 17 2017 04:13	May 17 2017 04:15	2m 20s	AP750	SSID17	5 GHz	130.8 KB	104.9 KB	235.6 KB	
May 17 2017 04:12	May 17 2017 04:12	16.28s	AP750	SSID17	5 GHz	53.41 KB	145.5 KB	198.9 KB	
May 17 2017 02:17	May 17 2017 04:12	1h 55m	AP750	SSID17	5 GHz	169 MB	3.295 GB	3.46 GB	
May 17 2017 02:15	May 17 2017 02:15	26.6s	AP750	SSID17	5 GHz	66.72 KB	1.41 MB	1.475 MB	

# Switch Details Report Dashboard

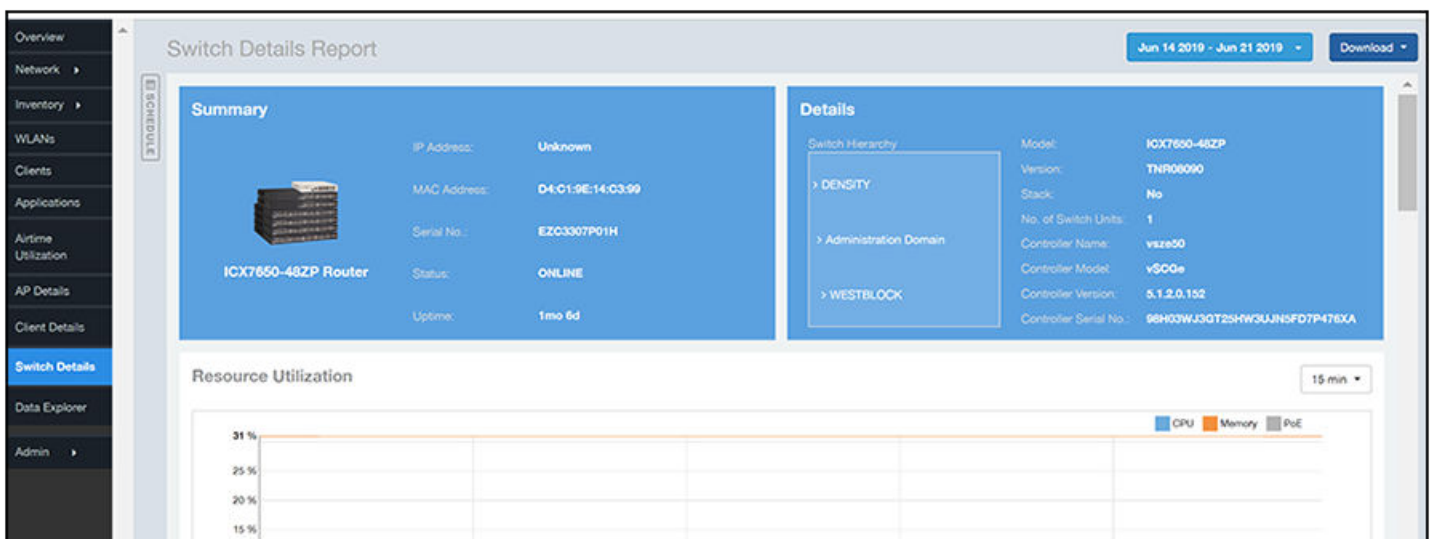
## Switch Details Report

The Switch Details report provides details about one specific switch.

You can reach this report by either clicking on a hyperlink of a switch name from another dashboard, or by clicking **Switch Details** on the navigation bar. If you click **Switch Details** to get to this screen, you then need to enter the MAC address of the switch whose details you want to view.

The following figure shows only the upper sections of the Switch Details report:

FIGURE 170 Switch Details Report (upper portion)



## Report

### Switch Details Report Dashboard

The Switch Details Report consists of the following components:

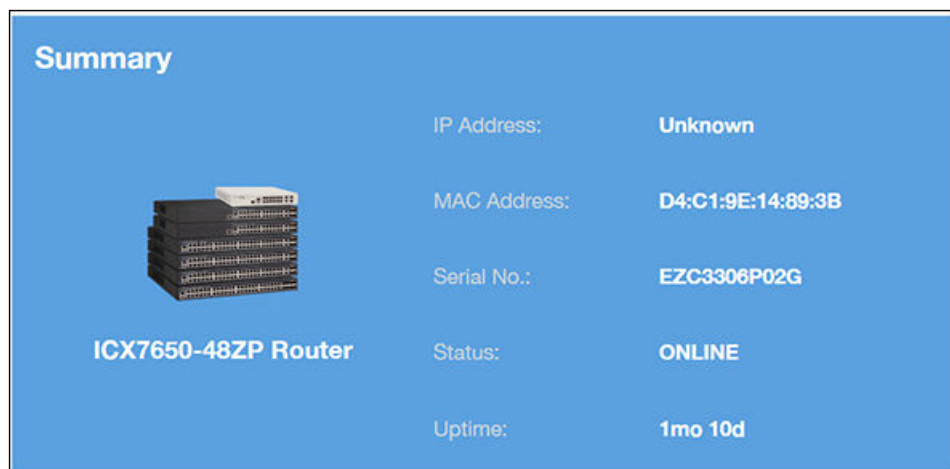
- Summary tile
- Details tile
- Resource Utilization tile
- Top Ports By Traffic tile
- Traffic Trend tile
- LLDP Neighbor List tile
- Uptime History tile

### Summary Tile

The Summary section of the Switch Details report displays basic information about a specific switch.

The switch shown in this example is named ICX7650-48ZP Router.

**FIGURE 171** Switch Details - Summary

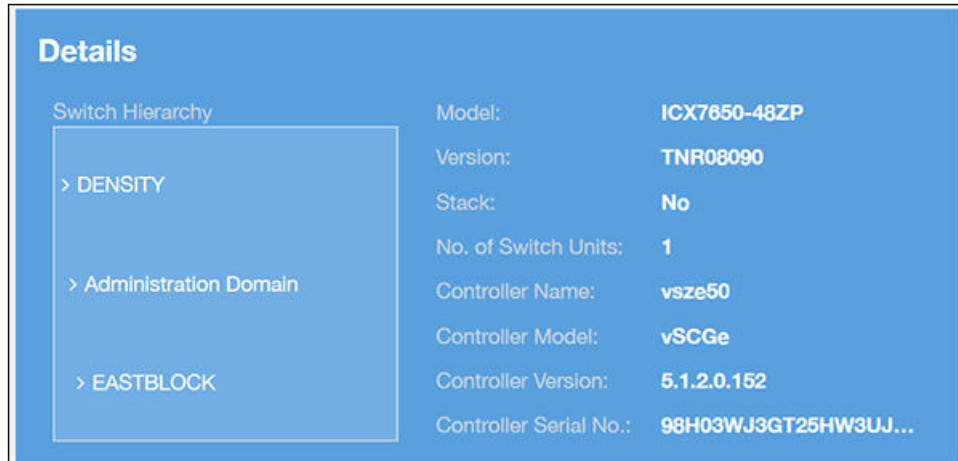


### Details Tile

The Details section of the Switch Details report contains information about the specified switch, including its hierarchy in the network.



FIGURE 172 Switch Details - Details

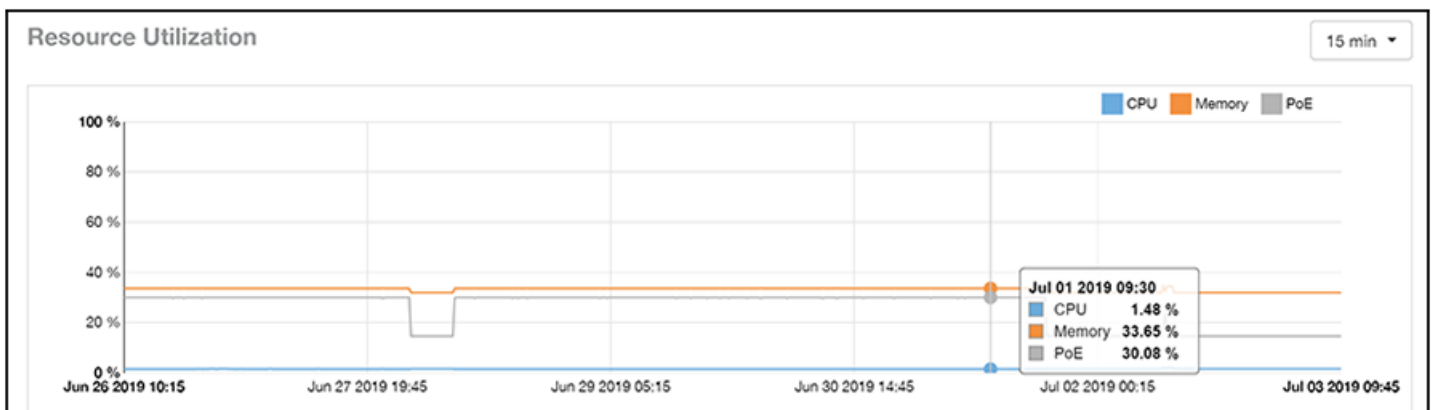


### Resource Utilization Tile

The Resource Utilization table of the Switch Details Report displays the CPU, memory and disk utilization percentages for each switch in your system.

You can hover to view resource utilization at different times; you can toggle the boxes on and off to display or not display the data they represent.

FIGURE 173 Switch Details - Resource Utilization



### Top Ports By Traffic Tile

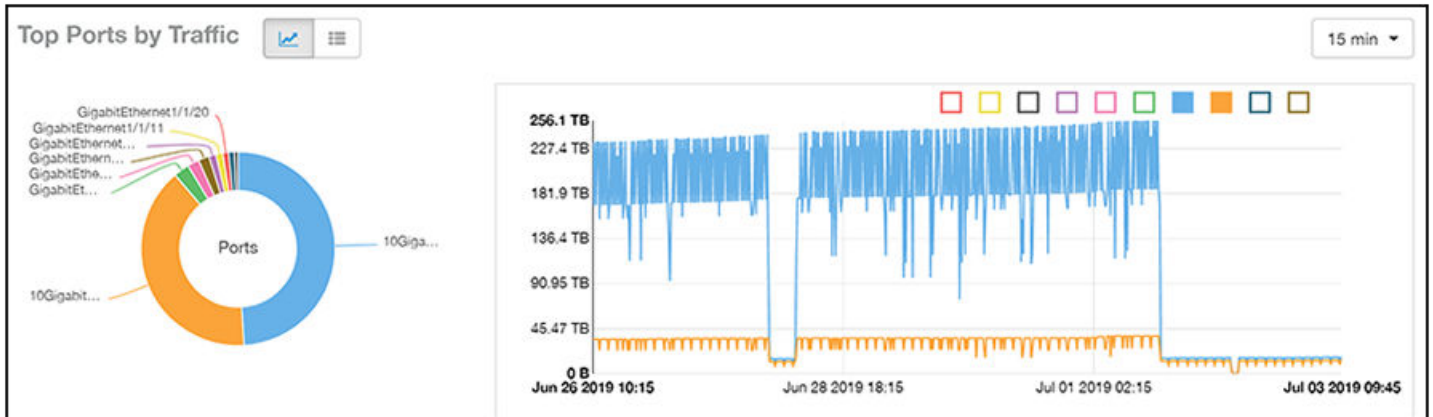
The Top Ports By Traffic pie chart and line graph of the Switch Details report depict the ports that have generated the largest volume of traffic over this switch for a specified period of time.

Use the drop-down menus to specify the time frame and the granularity of the graph. Click any of the colored squares to toggle display of the corresponding ports.

## Report

### Switch Details Report Dashboard

FIGURE 174 Switch Details - Top Ports By Traffic

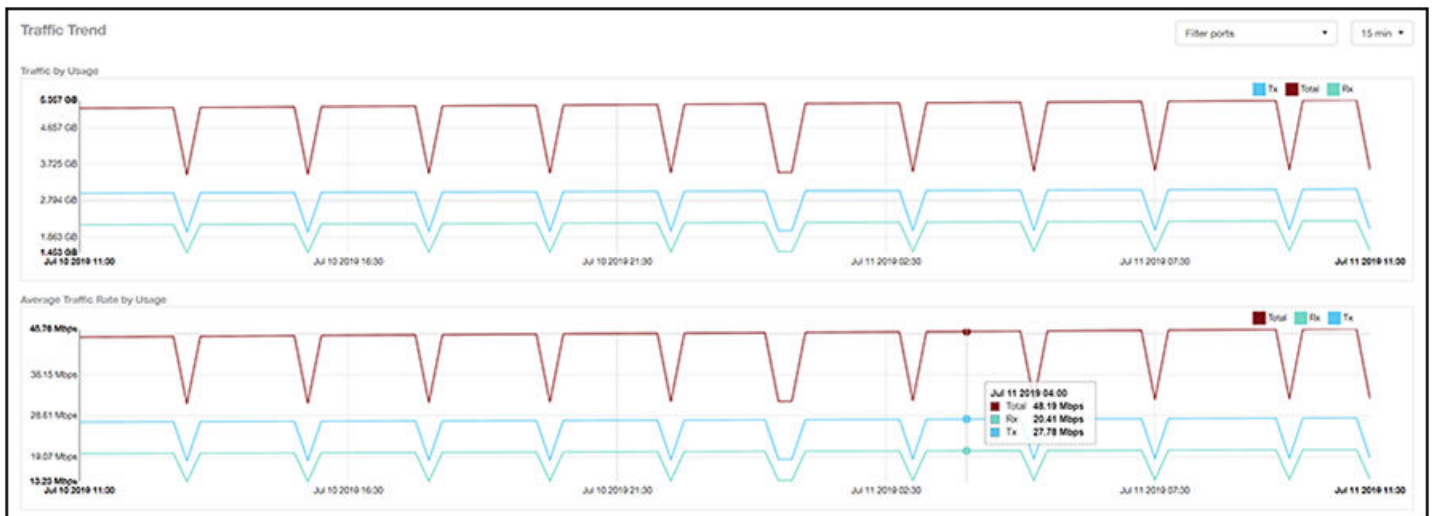


### Traffic Trend Tile

The Traffic Trend section of the Switch Details report contains two line graphs that provide information about the specified switch: one that depicts traffic by usage, and one that shows the average traffic rate by usage.

You can hover over portions of the line graph to view different types of traffic at certain time intervals, and you can click any of the colored squares to toggle display of the corresponding type of traffic.

FIGURE 175 Switch Details - Traffic Trend



### LLDP Neighbor List Tile

The LLDP Neighbor List table of the Switch Details report provides information about all the LLDP neighbors of the specified switch.


Click the gear icon  to select the list of columns to display. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 176 Switch Details - LLDP Neighbor List

LLDP Neighbor List						
Remote Device Name	Remote Port Mac	Remote Port Type	Remote Port	Local Port	Local Port Mac	Remote Port Descr...
EBC-ICX7150-48ZP-SW0	D4:C1:9E:4B:83:E0	Bridge	GigabitEthernet1/1/48	GigabitEthernet1/1/24	60:9c:9f:ab:95:bf	Unknown

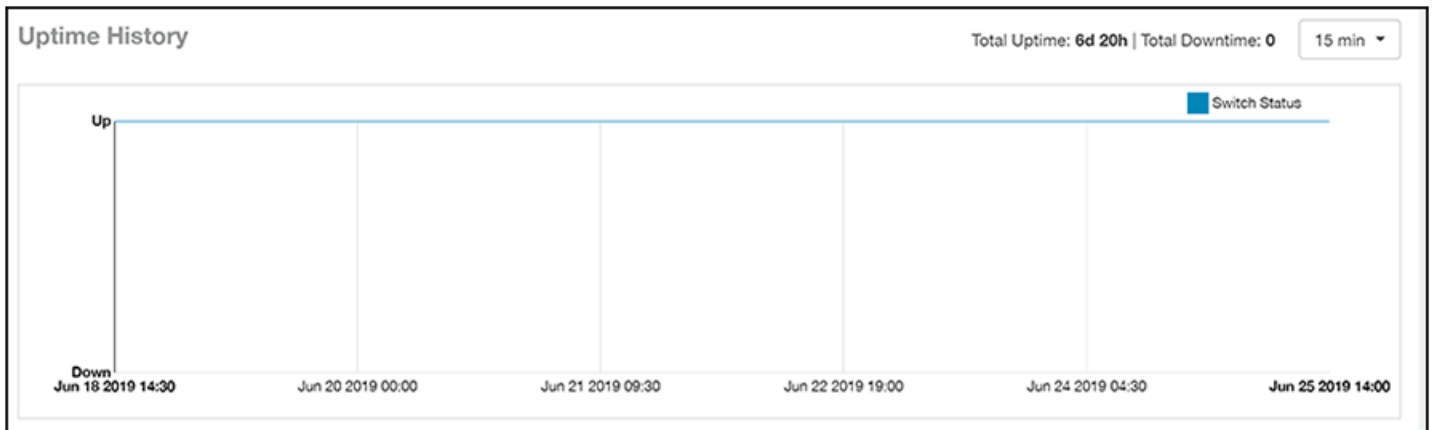
◀ 1 ▼ of 1 ▶

### Uptime History Tile

The Uptime History line graph of the Switch Details report shows when this switch has been up or down over different time periods.

The blue bar indicates when the switch has been up or down. Use the drop-down menu to specify the timeframe and the granularity of the graph.

FIGURE 177 Switch Details - Uptime History



## Comparison Reports Dashboard

### Compare Filters

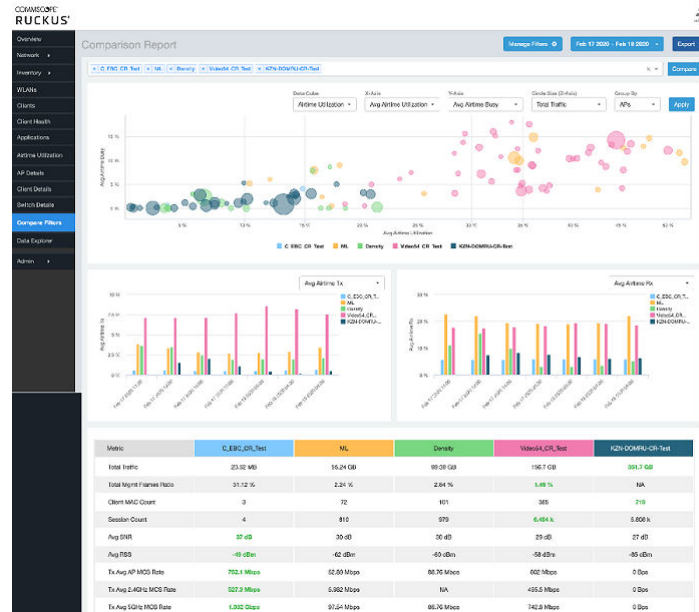
Compare Filters help compare sets of data within the networks against one another to provide a better understanding of network health based on various dimensions such as network deployments, brand, region to name a few.

**NOTE**

Comparison reports are only available for Admin and Super admin users.

The following figure shows only the upper sections of the Compare Filters page:

FIGURE 178 Comparison Report



The Comparison Report consists of the following components:

- Compare Filters tile
- Overview tile
- Metric Over Time tiles
- Comparison table

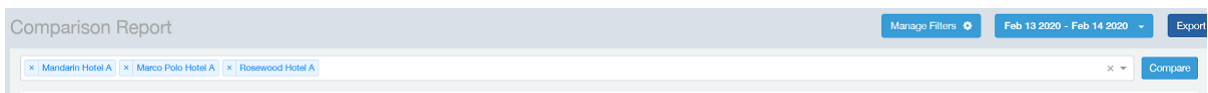
### Compare Filters Tile

You can select the filters you want to compare from the Compare Filter drop-down.

The drop-down displays existing saved filters and those created newly as well, and you can compare up to a maximum five filters at a time. After selecting the filter, click **Compare** to initiate data comparison between the filters selected. The order of the filter selection is maintained across all the graphs and table. This report cannot be scheduled.

The **Compare** button is disabled if you select more than five filters or less than one filter.

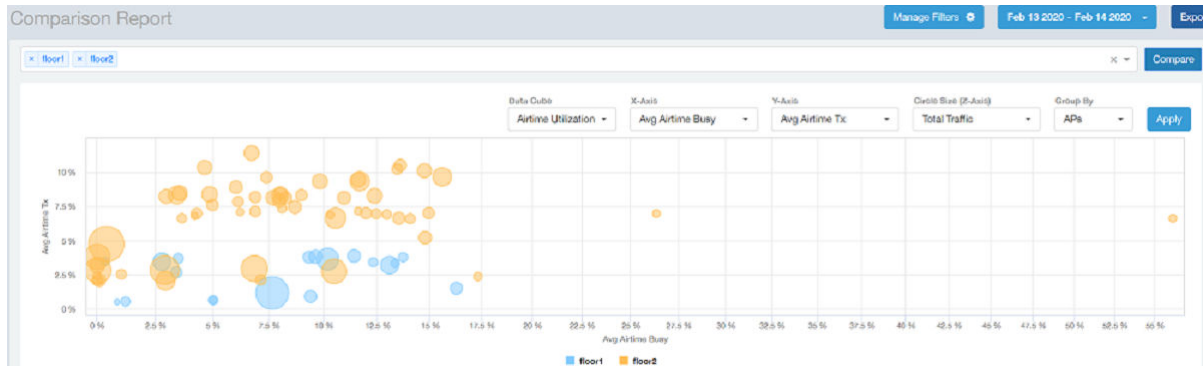
FIGURE 179 Comparison Reports - Compare Filters



### Overview Tile

The Overview section displays a scatter-plot of data being compared from the filters selected. You can select the following parameters to plot the Overview graph:

FIGURE 180 Comparison Report - Overview scatter plot



- DataCube: select from Airtime Utilization, Network, and Clients from the menu.
- X axis and Y axis: select the parameter to display on the axis. The options in these menus change based on the data cube selection. For example, if you selected Airtime Utilization, then some of the parameters you can choose to display in the X and Y axis include Avg Airtime Utilization, Avg Airtime Busy, Avg Airtime Tx/Rx, and Total Traffic.
- Circle Size (Z Axis): displays the data by the size fo the circle. For example, the Total Traffic value in GB is shown as a smaller circle in comparison to the one in TB.

**NOTE**

Each filter data is represented as a circle with a specific color for the filter. For example, in this image the scatter plot circle displays are for the **floor1** filter in blue and **floor2** filter in yellow.

- Group By: this option allows you to group the scatter plots based on the AP, Ap Group, Zone, System, Domain, and WLAN/SSIDs. Pausing the pointer over the circle displays a summary of the data point.

Click **Apply** to apply these parameters. Based on the parameters selected, the Overview graph is refreshed and plotted for your analysis.

You can toggle the circles below the chart (on and off) to display or not display the filters they represent.

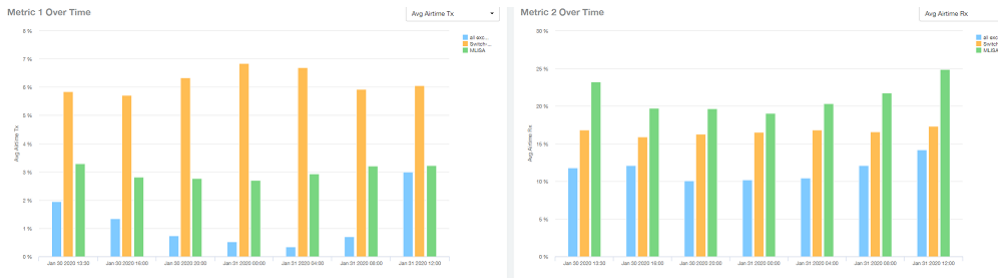
**NOTE**

No two parameters in the X, Y, Z axis fields can be the same.

**Metric Over Time Tiles**

The two Metric charts compare a variety of potential metrics in a historical view, as a bar graph. You can select any two matrices in both the charts to compare. All the metrics are available in the drop-down for comparison. The X axis of the chart displays a time range, and the Y axis parameter can be selected from the drop-down provided. The bar graphs are displayed after the Y axis selection and the colors of the bar pertain to the respective filters selected. Pausing the pointer over the bar displays a summary of the data point. You can toggle the boxes in the chart (on and off) to display or not display the filters they represent.

FIGURE 181 Comparison Report - Metric Over Time



### Comparison Table

The Comparison Table shows columns of comparison filters and rows of all metrics that are compared. You can use the gear icon to select the columns you want to display and also select the number of rows to display. For each metric of a filter, the data comparison is done and data that is top performing is highlighted green as shown in the figure.

FIGURE 182 Comparison Reports - Table

Metric	10 ERTelecom APs	Switch-1	MLISA
Total Traffic	0 B	613.2 GB	54.47 GB
Total Mgmt Frames Ratio	0 %	1.34 %	2.58 %
Client MAC Count	0	1.212 k	77
Session Count	0	14.39 k	934
Client Health Score (Good)	0 %	78.91 %	74.15 %
Avg SNR	0 dB	30 dB	31 dB
Avg RSS	0 dBm	-58 dBm	-59 dBm
Tx Avg AP MCS Rate	0 Bps	486.7 Mbps	75.96 Mbps
Tx Avg 2.4GHz MCS Rate	0 Bps	417.8 Mbps	6.557 Mbps
Tx Avg 5GHz MCS Rate	0 Bps	542.1 Mbps	141 Mbps
Tx Client MCS Rate	0 Bps	318 Mbps	153.5 Mbps
Avg Throughput Estimate	0 Bps	89.95 Mbps	168.7 Mbps

## PCI Profiles

You can generate PCI Profiles in to determine if your WLANs are compliant with the Payment Card Industry (PCI) Data Security Standard v3.2.

When you navigate to **Report > PCI** in the left pane of the user interface, the main PCI Profiles screen appears, as shown in the following example.

FIGURE 183 PCI Profiles Screen

The screenshot shows the 'Admin - PCI Profiles' interface. At the top, there are three buttons: '+ Create', 'Edit', and 'Delete'. Below these is a table with the following columns: Name, SSIDs, Date, and Compliance. The table contains five rows of data. The first row is selected, indicated by a checkmark in the left margin. The 'Compliance' column contains red 'FAIL' buttons for the first four rows and a green 'PASS' button for the last row. A pagination bar at the bottom shows '1 of 1'.

	Name	SSIDs	Date	Compliance
<input checked="" type="checkbox"/>	pci test bed	QA-RaikiH-MSP1-101, QA-...	May 22 2018 04:57	FAIL
<input type="checkbox"/>	density	test-5g	May 17 2018 18:44	FAIL
<input type="checkbox"/>	both	DENSITY, QA-RaikiH-Web-...	May 17 2018 19:17	FAIL
<input type="checkbox"/>	1st density	bugbash, test-5g, qa-pre.k...	May 21 2018 04:00	FAIL
<input type="checkbox"/>	test2	testssid	May 22 2018 11:53	PASS

This screen lists the names of the various profiles that have been run, the SSIDs on which each profile has been run, the date of each profile, and whether the overall profile passed or failed the PCI compliance test. You can click on the red "Fail" or green "Pass" to observe the detailed profile.

## Creating a PCI Profile

You can create a PCI profile to run a report that indicates if a WLAN is in compliance with the PCI Data Security Standard v3.2.

Follow the steps below to create a PCI profile:

1. From **Report > PCI** in the RUCKUS Analytics user interface, click the **Create** button in the upper left of the screen.

The **Create Profile** screen is displayed.

**FIGURE 184** Creating a PCI Profile

**Create Profile**

**Name** Test report 15

**SSIDs to Report**

Search SSID [Q]

All Systems

Index	Question	
1.1.2	Do you maintain a network diagram documenting wireless connections to the CDE?	<input checked="" type="checkbox"/>
1.2.3	Do you have a firewall in place that permits only authorized traffic between the wireless network and CDE?	<input checked="" type="checkbox"/>
2.1.1	Do you change all known encryption keys or passwords when anyone with knowledge about them leaves or changes roles?	<input checked="" type="checkbox"/>
2.4	Do you maintain a system inventory of hardware and software in scope for PCI? (Hint: SZ allows you to export a CSV list of devices)	<input checked="" type="checkbox"/>
6.1	Do you utilize a reputable third-party source to identify and rank security vulnerabilities?	<input checked="" type="checkbox"/>
6.2	Do you monitor and install vendor-supplied security patches in a timely manner?	<input checked="" type="checkbox"/>
7.2	Do you prevent all unnecessary administrative access across systems with a default 'deny-all' policy?	<input checked="" type="checkbox"/>

**Create** **Cancel**



2. Complete the screen configuration as follows:

- **Name:** Enter any descriptive name for your PCI profile.
- **SSIDs to report:** Use the Search area and the + buttons to locate all the SSIDs you want to include in the profile, then click the box next to each desired SSID.

**NOTE**

When an SSID is selected for the PCI profile, this SSID is identified as part of the cardholder data environment (CDE). Unselected SSIDs in the same zone are considered non-CDE SSIDs. The system will compare the security settings of CDE and non-CDE SSIDs to ensure that the network complies with PCI requirements. Only the zone(s) of selected SSIDs are evaluated for each PCI profile.

- **Index/Question:** Check-mark the compliance questions that you want included in your profile which will pull data directly from the controller to check the compliance of each question against the PCI Data Security Standard.

**NOTE**

Not all questions are shown in the screen example above.

3. Click **Create** at the bottom right of the screen.

The result of the profile (Pass or Fail) appears in the list of PCI profiles on the main PCI Profiles screen, an example of which is shown in [Figure 183](#) on page 151.

## Opening and Downloading a PCI Profile

The PCI Profile gives you an overall status (Pass or Fail) as well as a breakdown of all categories you requested when you created the PCI profile.

Follow the steps below to view and download a copy of your PCI profile.

1. From the main PCI Profile screen, an example of which is shown in [Figure 183](#) on page 151, click on either the green "Pass" or red "Fail" button, depending on the report you wish to view.

The profile is displayed, as shown in the following example, where both the overall status is provided (in the upper right) as well as the compliancy of each individual item you chose when you created the PCI profile.

**FIGURE 185** PCI Report Example

The screenshot shows a 'PCI Compliance Report' for 'pci test bed' dated 'May 22 2018 04:57'. The overall status is 'FAIL'. The report contains a table with the following items:

PCI ID	Description	Compliant	Details
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	PASS	
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	PASS	
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	PASS	
2.3	Encrypt all non-console administrative access using strong cryptography.	PASS	
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	PASS	
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	PASS	
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	PASS	
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	PASS	
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	PASS	
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	PASS	
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	PASS	
8.1.3	Immediately revoke access for any terminated users.	PASS	
8.1.4	Remove/disable inactive user accounts within 90 days.	FAIL	TDC-PCI-TESTBED

At the bottom right of the table, there are 'Download' and 'Cancel' buttons.

2. Click the **Download** button (lower right) to obtain a PDF copy of the profile.

## Editing or Deleting a PCI Profile

You can edit or delete any PCI profile, as desired.

To edit or delete a profile, check the box or boxes next to the PCI profile, then click the applicable button - either **Edit** or **Delete** - to perform the desired actions.

**NOTE**

You can select and delete multiple profiles simultaneously if desired.

**FIGURE 186** Edit or Delete PCI Profiles

	Name	SSIDs	Date	Compliance	
<input checked="" type="checkbox"/>	pci test bed	QA-RaikiH-MSP1-101, QA-...	May 22 2018 04:57	FAIL	
<input type="checkbox"/>	density	test-5g	May 17 2018 18:44	FAIL	
<input type="checkbox"/>	both	DENSITY, QA-RaikiH-Web-...	May 17 2018 19:17	FAIL	
<input type="checkbox"/>	1st density	bugbash, test-5g, qa-pre.k...	May 21 2018 04:00	FAIL	
<input type="checkbox"/>	test2	testssid	May 22 2018 11:53	PASS	

1 of 1



# Data Explorer

---

- [Data Explorer and Data Cubes.....](#) 157
- [Data Cube Filters.....](#) 170
- [Creating a Data Explorer Dashboard.....](#) 193
- [Actions You Can Perform on an Existing Dashboard.....](#) 198

## Data Explorer and Data Cubes

Data Explorer and its individual cubes allow you to view, filter, and manipulate data in many different ways .

### Data Exploration

Data exploration is the act of examining the minute details of an Online Analytical Processing (OLAP) cube.

Consider your data to be a three-dimensional cube that you would like to explore, both inside out and outside in, so that you can glean more insights from your data. Of course, most real world data sets will have more than three dimensions, but the concepts from a 3D cube can be directly extended to a multidimensional hypercube.

With an OLAP cube, there are five operations that you can perform:

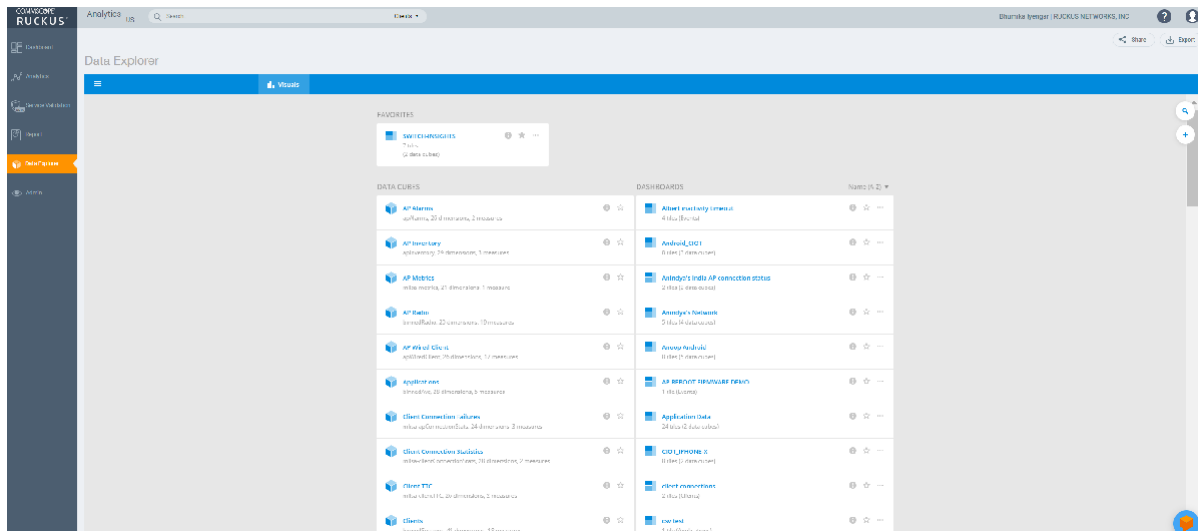
1. **Slice:** Think of slicing a piece of cheese; you make a single cut to the cheese to expose the insides. A typical slice operation is the time slice. Instead of reviewing all the data of the last 30 days, you slice the data to expose only Day 1.
2. **Dice:** Consider dicing a block of cheese; you make multiple cuts and separate the block into a number of smaller pieces. A typical dice operation involves taking a slice of data, such as the Day 1 data, and cutting it further to filter by the controller name and AP group. A smaller piece of the original OLAP cube results from the slice and dice operations.
3. **Drill Up and Drill Down:** In order to delve into the details, you can drill down to a specific AP in an AP group, and drill down further to a specific client host name. Conversely, you could search for a client MAC address and drill up to find the AP and controller to which it belongs.
4. **Roll Up:** The roll up operation typically involves numbers known as measures. After the slice, dice, and drill down of your data, you can roll up the numbers to gain a better understanding of the whole, for example, the total transmit traffic for the selected APs.
5. **Pivot:** The pivot operation allows you to view the data from a different perspective. For example, you have a table showing a list of controllers and the APs belonging to each controller. You may pivot the table to show a list of the APs and the controllers to which they belong. Think of pivoting as changing the hierarchy between the dimensions.

As you use the custom reporting, you can refer to these five operations.

## Data Explorer

### Data Explorer and Data Cubes

FIGURE 187 Data Explorer and Data Cubes



The top right corner of the Data Explorer page displays options to share and export dashboards in PDF and CSV formats. You can also share them with recipients over e-mails on-demand or periodically by configuring a schedule (daily, weekly and monthly).

Data Explorer allows you to explore the data under various categories, using your own permutations and combinations, unlike the other canned reports available.

#### NOTE

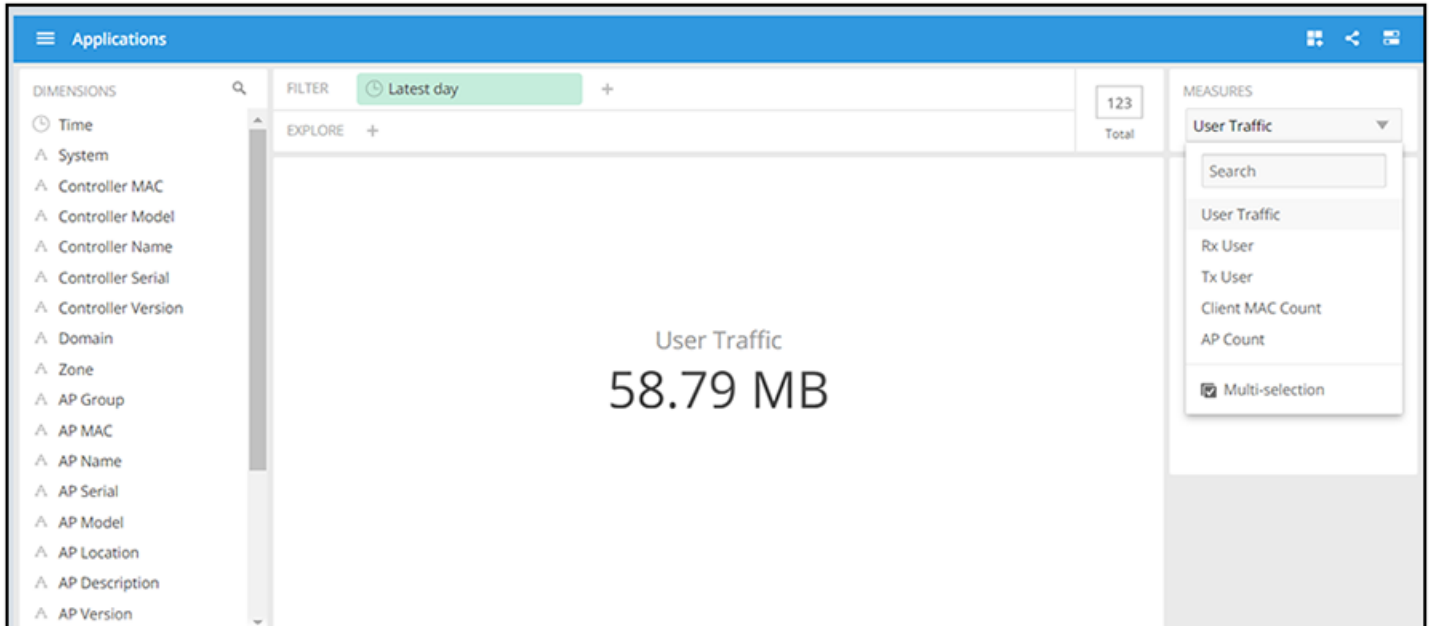
The **Schedule** tab is for use only with dashboards you create, not with data cubes themselves.

For information on how to use data cube filters, which are common to all the data cubes, refer to [Data Cube Filters](#) on page 170. You can also create and save dashboards, which allows you to customize reports by using data from any or all of the data cubes. Refer to [Creating a Data Explorer Dashboard](#) on page 193 and [Actions You Can Perform on an Existing Dashboard](#) on page 198 for more information.

## Applications

The **Applications** cube allows you to explore the application data your system uses.

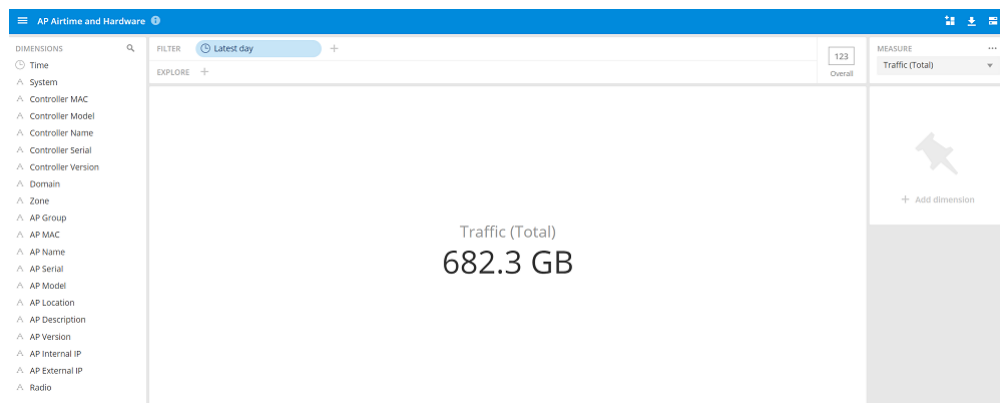
FIGURE 188 Data Explorer: Applications



## AP Airtime and Hardware

The **AP Airtime and Hardware** cube allows you to query, search and aggregate data related to the airtime utilization and CPU/memory/storage utilization of the APs.

FIGURE 189 Data Explorer: AP Airtime and Hardware



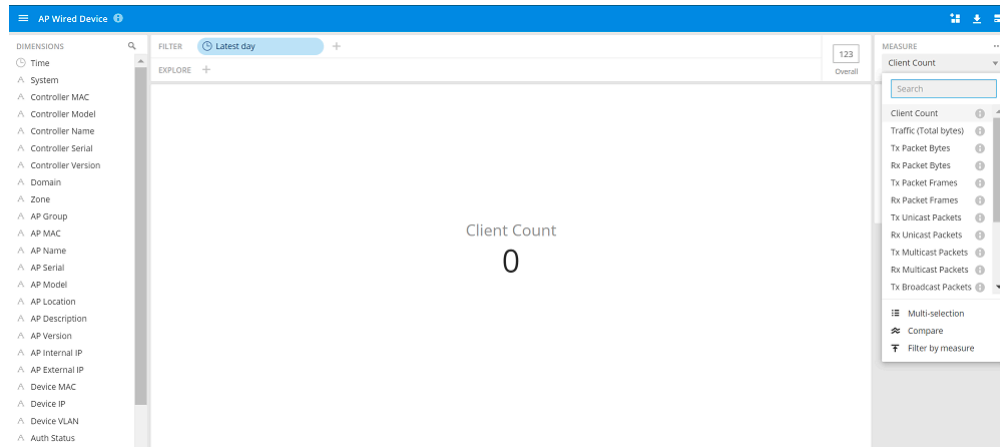
## AP Wired Device

The **AP Wired Device** cube allows you to explore the AP wired clients in the system.

## Data Explorer

### Data Explorer and Data Cubes

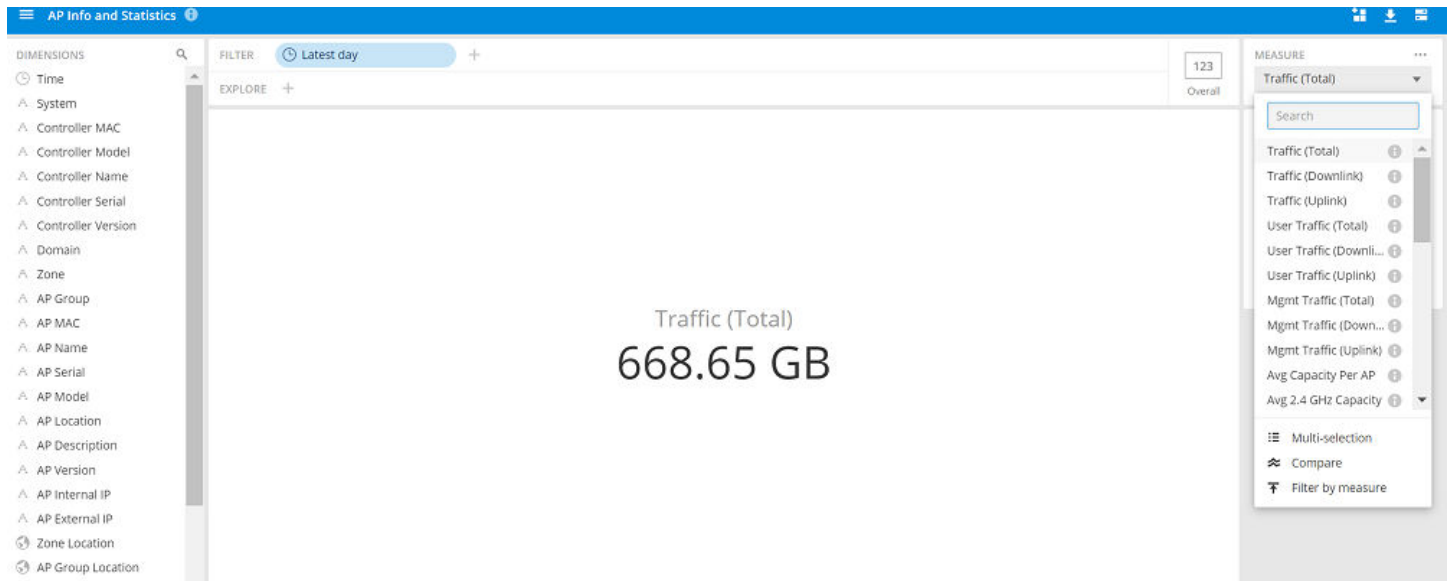
FIGURE 190 Data Explorer: AP Wired Device



## AP Info and Statistics

The **AP Info and Statistics** cube allows you to explore network traffic data and its usage.

FIGURE 191 Data Explorer: AP Info and Statistics

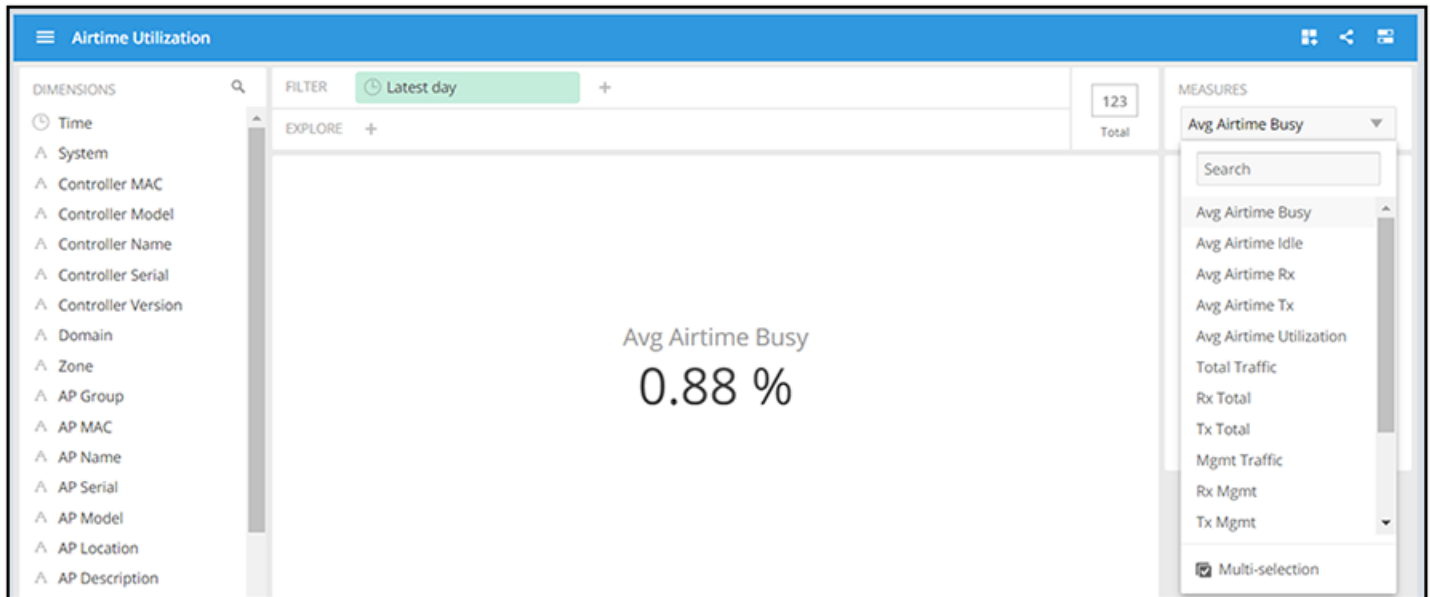


## Airtime Utilization

The **Airtime Utilization** cube allows you to explore the airtime utilization data in your system.



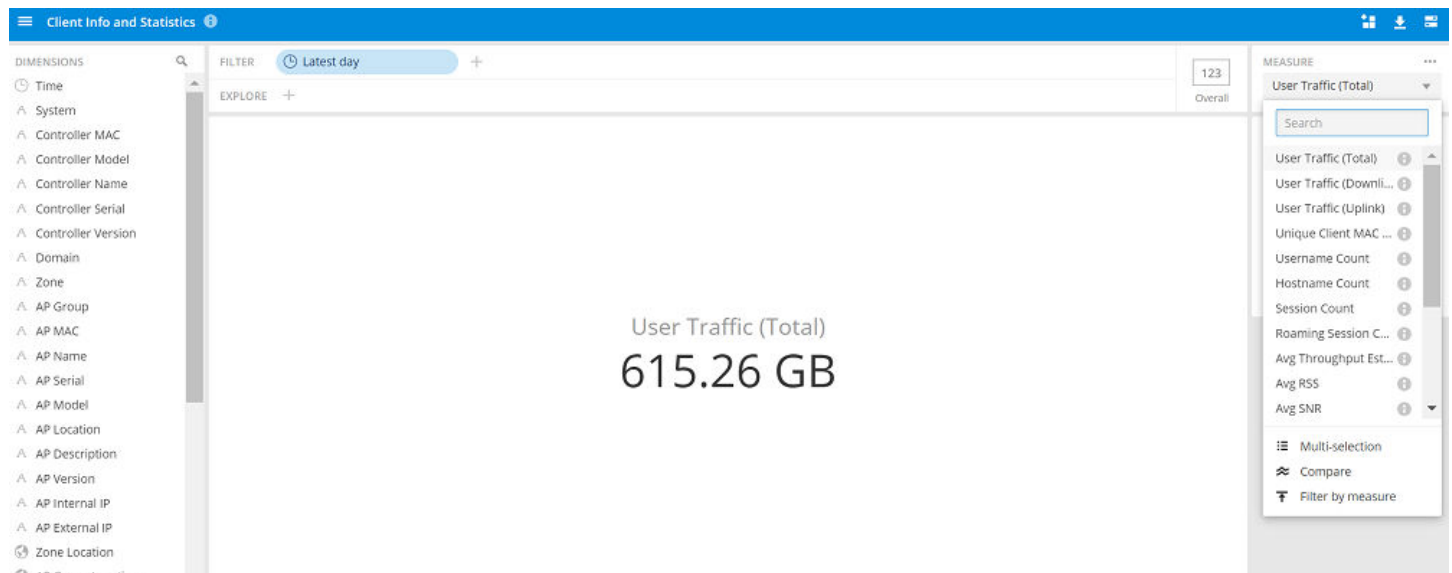
FIGURE 192 Data Explorer: Airtime Utilization



## Client Info and Statistics

The **Client Info and Statistics** cube allows you to explore client data for your system.

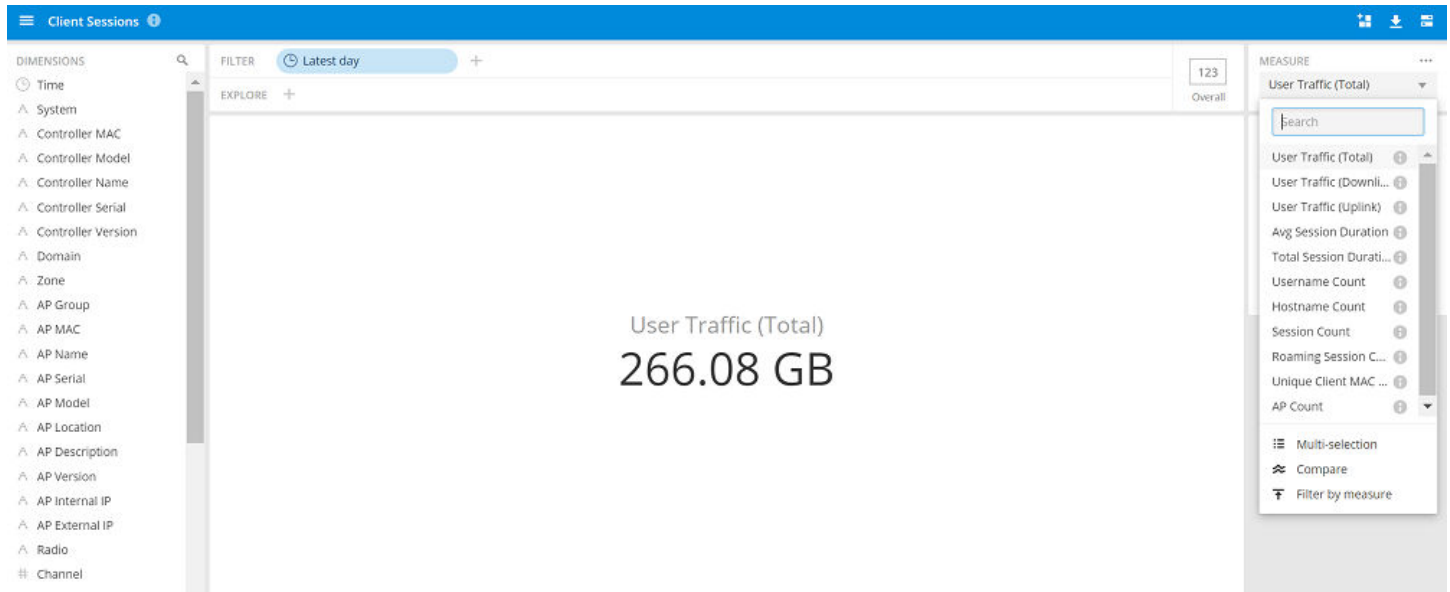
FIGURE 193 Data Explorer: Client Info and Statistics



## Client Sessions

The **Client Sessions** cube allows you to explore data about the various sessions in your system.

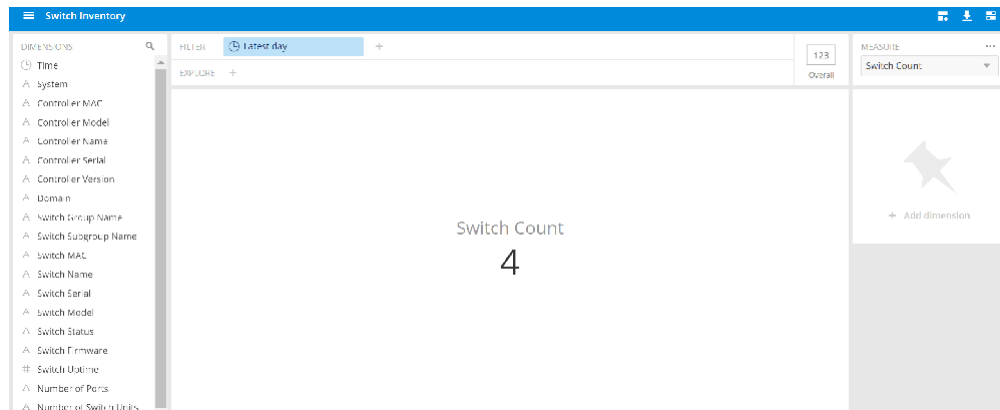
FIGURE 194 Data Explorer: Client Sessions



## Switch Inventory

The **Switch Inventory** cube allows you to view information about the switch configuration data your system uses.

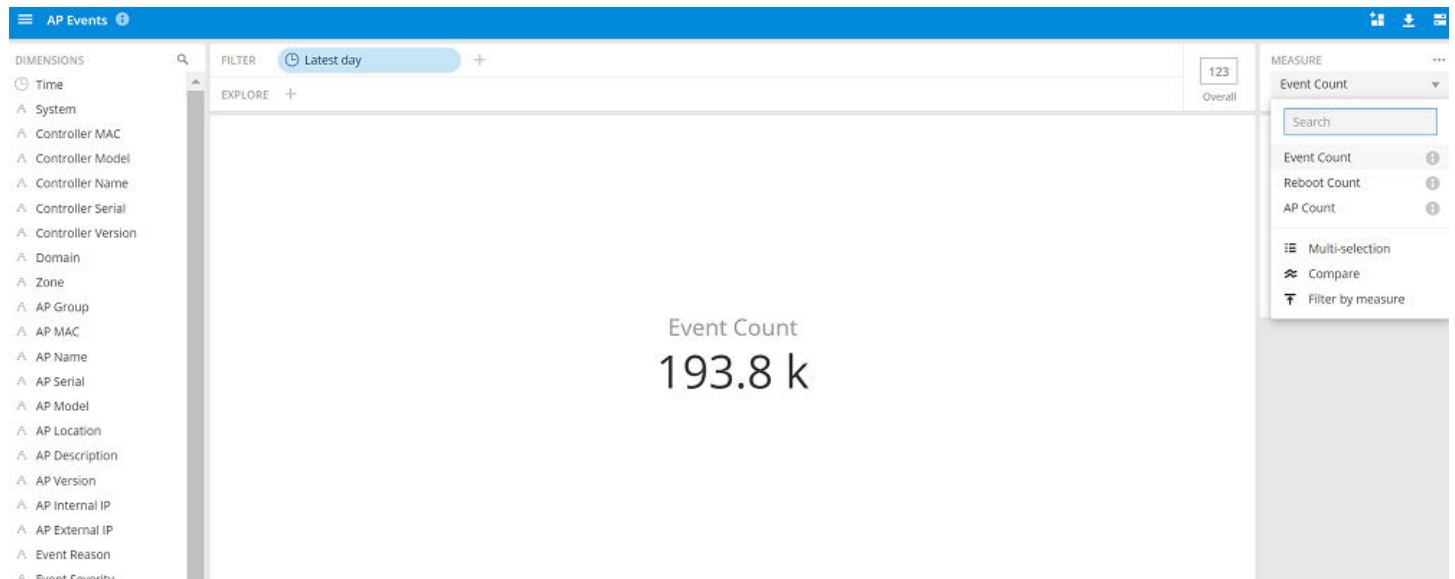
FIGURE 195 Data Explorer: Switch Inventory



## AP Events

The **AP Events** cube allows you to view data about events that have occurred in your system.

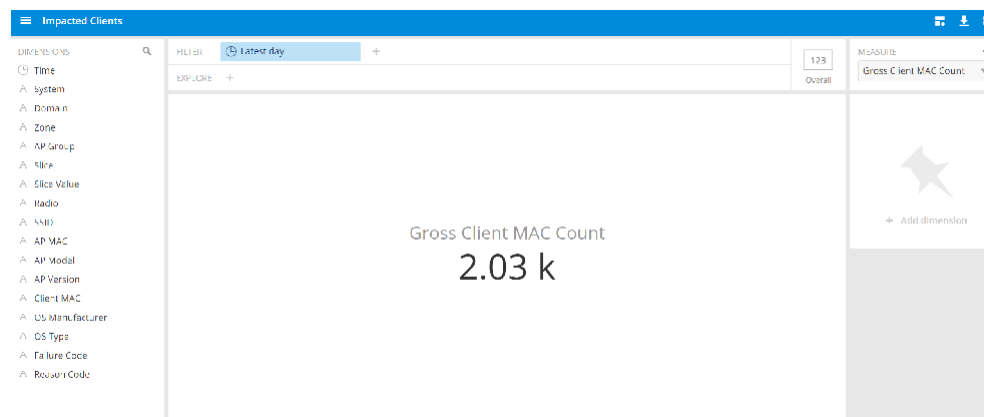
FIGURE 196 Data Explorer: AP Events



## Impacted Clients

The **Impacted Clients** cube allows you to view information about the clients impacted by the incidents.

FIGURE 197 Data Explorer: Impacted Clients



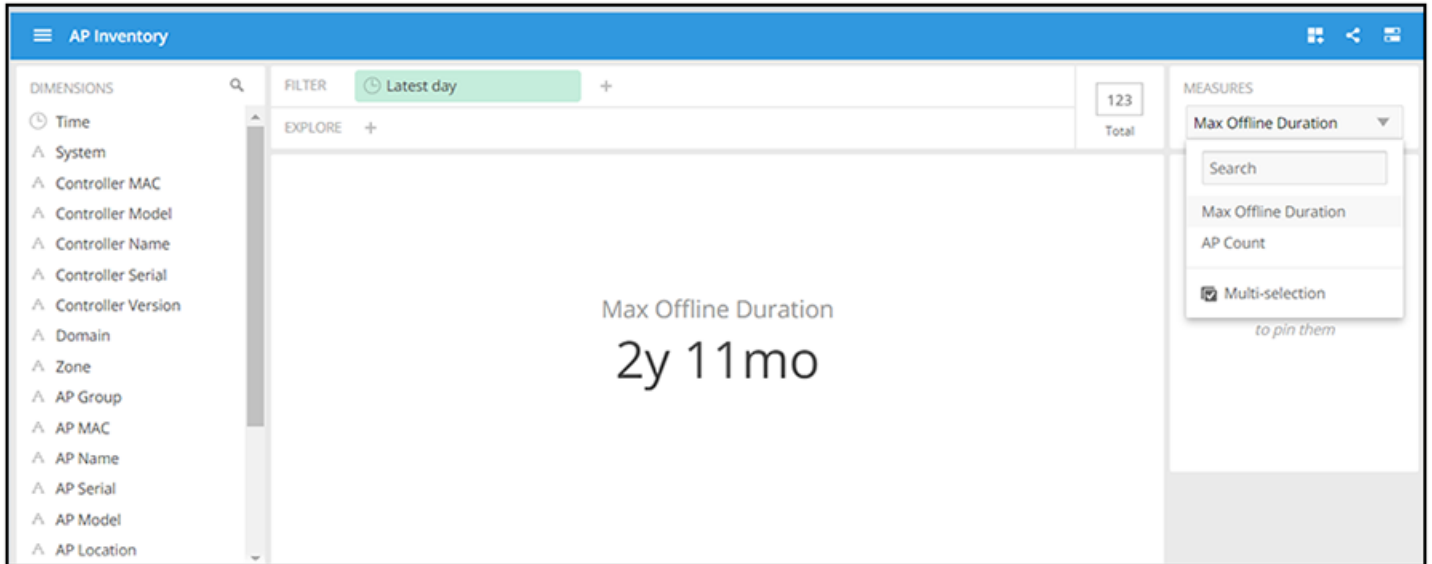
## AP Inventory

The **AP Inventory** cube allows you to view information about the various AP models your system uses.

## Data Explorer

Data Explorer and Data Cubes

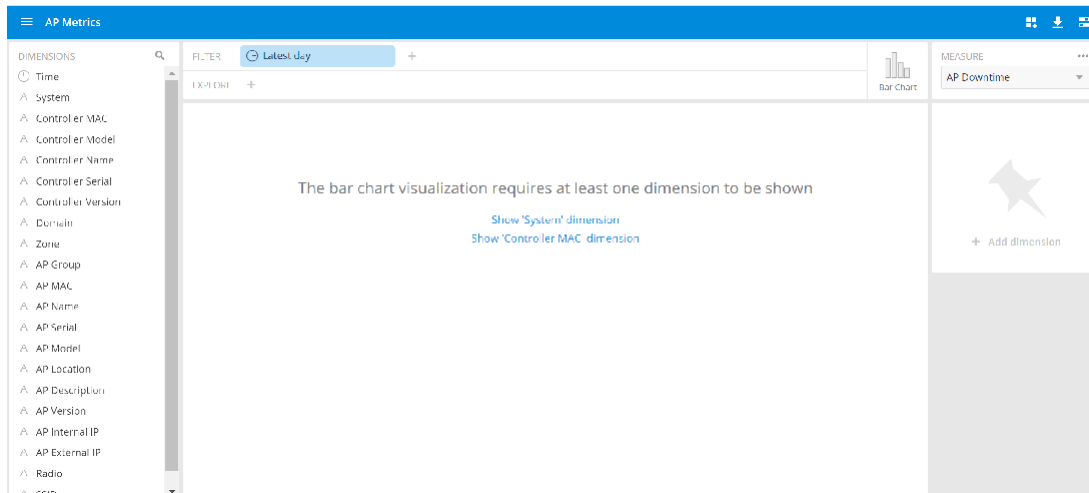
FIGURE 198 Data Explorer: AP Inventory



## AP Metrics

The **AP Metrics** cube allows you to view computed AP metrics (such as AP service downtime) in your system.

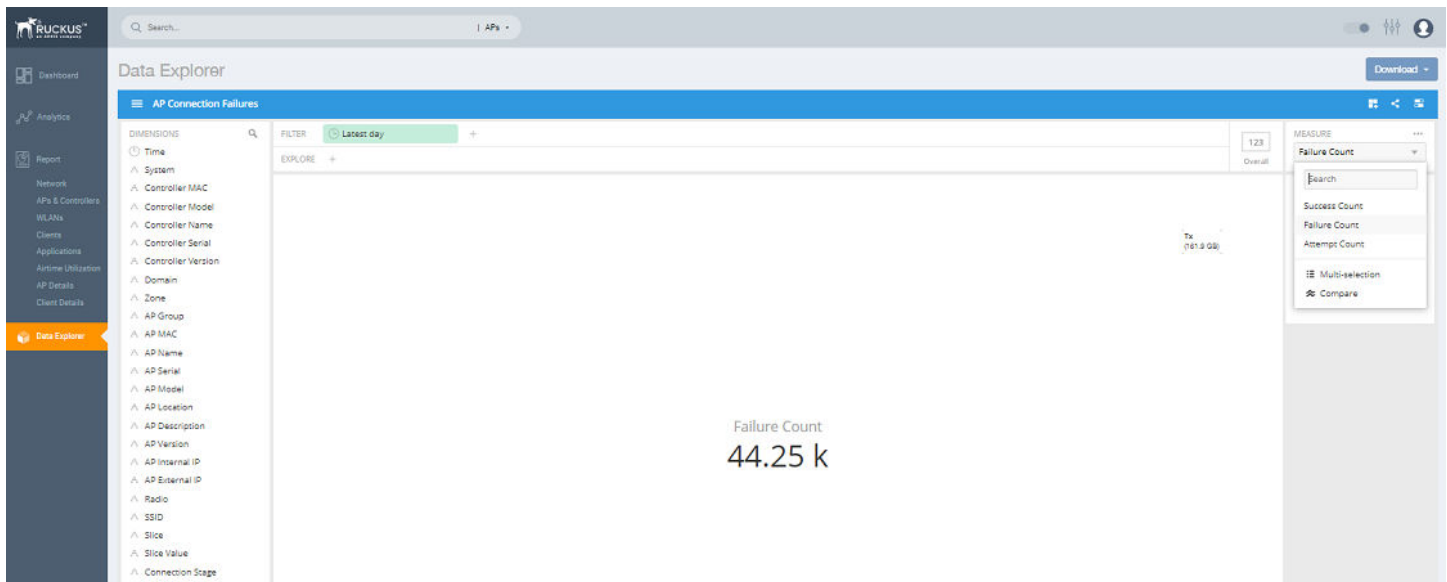
FIGURE 199 Data Explorer: AP Metrics



## AP Connection Failures

The **AP Connection Failures** cube shows all the failures that have occurred in the AP or at any other level in the hierarchy of the AP.

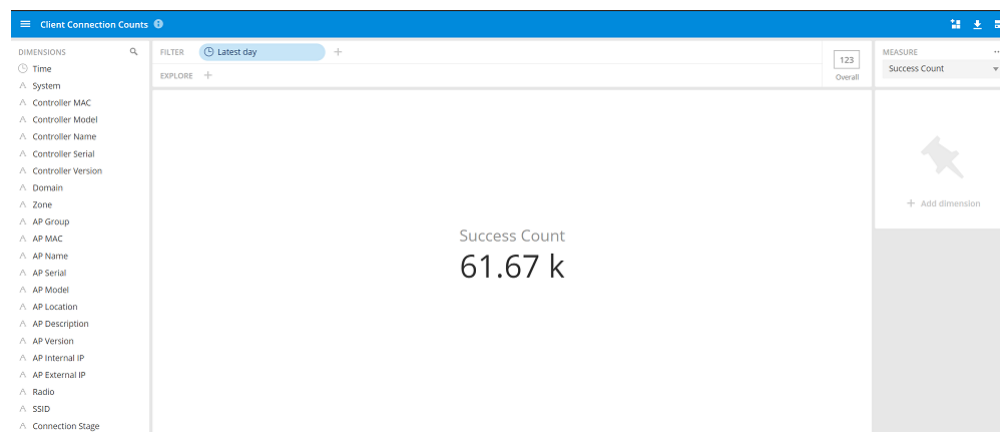
FIGURE 200 Data Explorer: AP Connection Failures



## Client Connection Counts

The **Client Connection Counts** cube shows all client connectivity events, including connectivity failures, client joins and client roams.

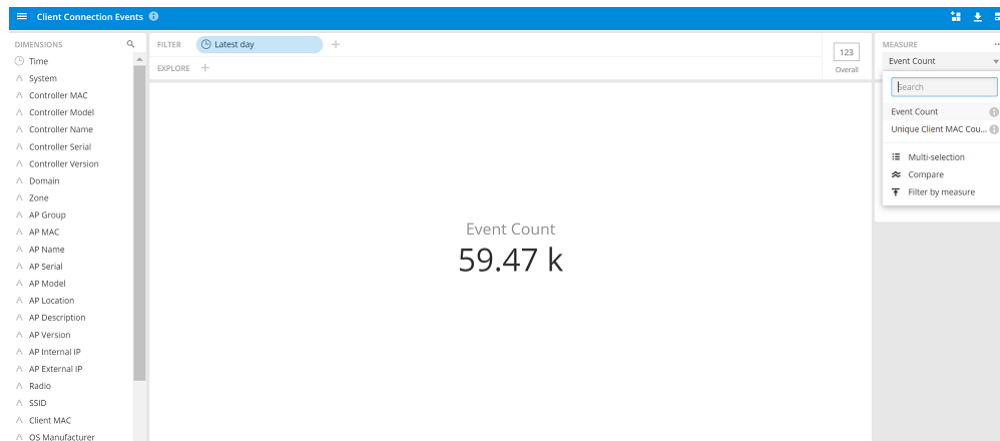
FIGURE 201 Data Explorer: Client Connection Counts



## Client Connection Events

The **Client Connection Events** cube allows you to view any failure- and connection-related data for the client.

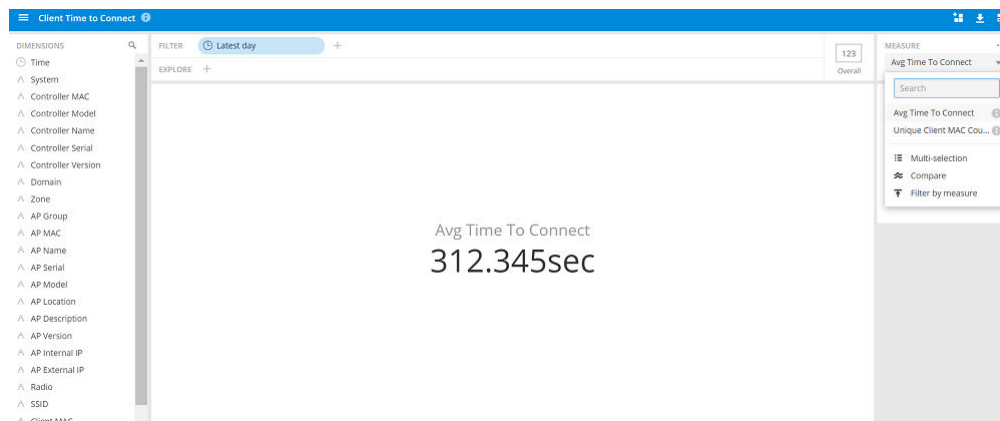
FIGURE 202 Data Explorer: Client Connection Events



## Client Time to Connect

The **Client Time to Connect** cube gives information about the time to connect (TTC) the client to the network.

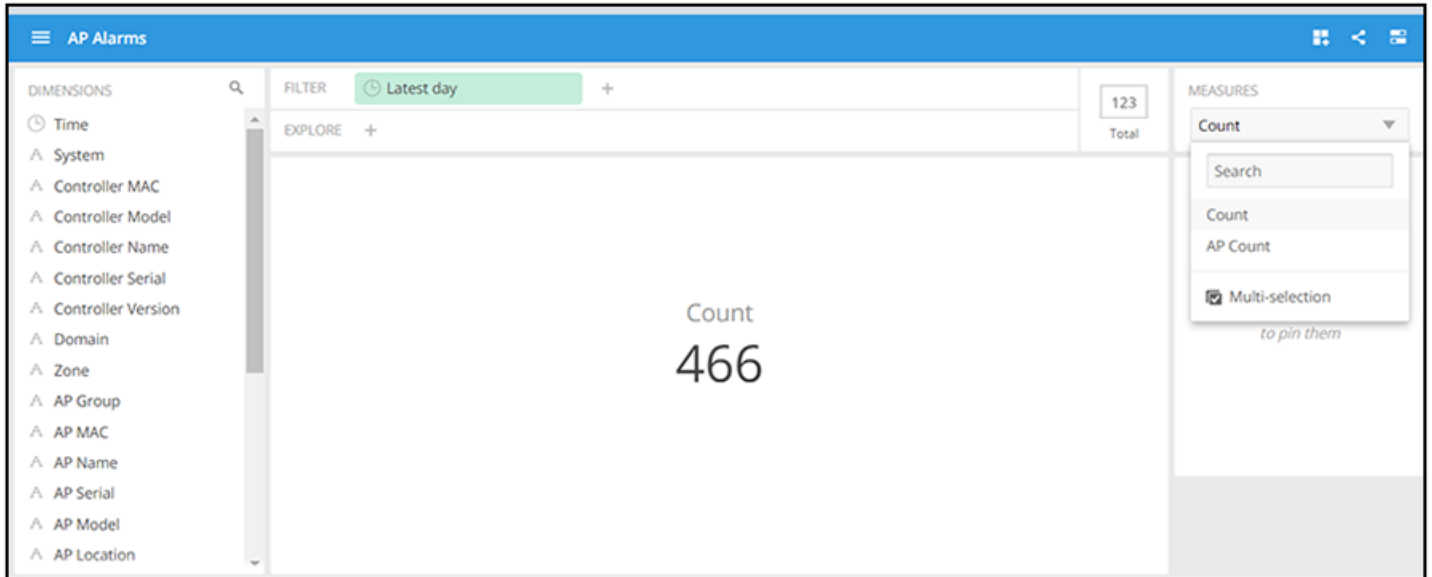
FIGURE 203 Data Explorer: Client Time to Connect



## AP Alarms

The **AP Alarms** cube allows you to view information about alarms in your system.

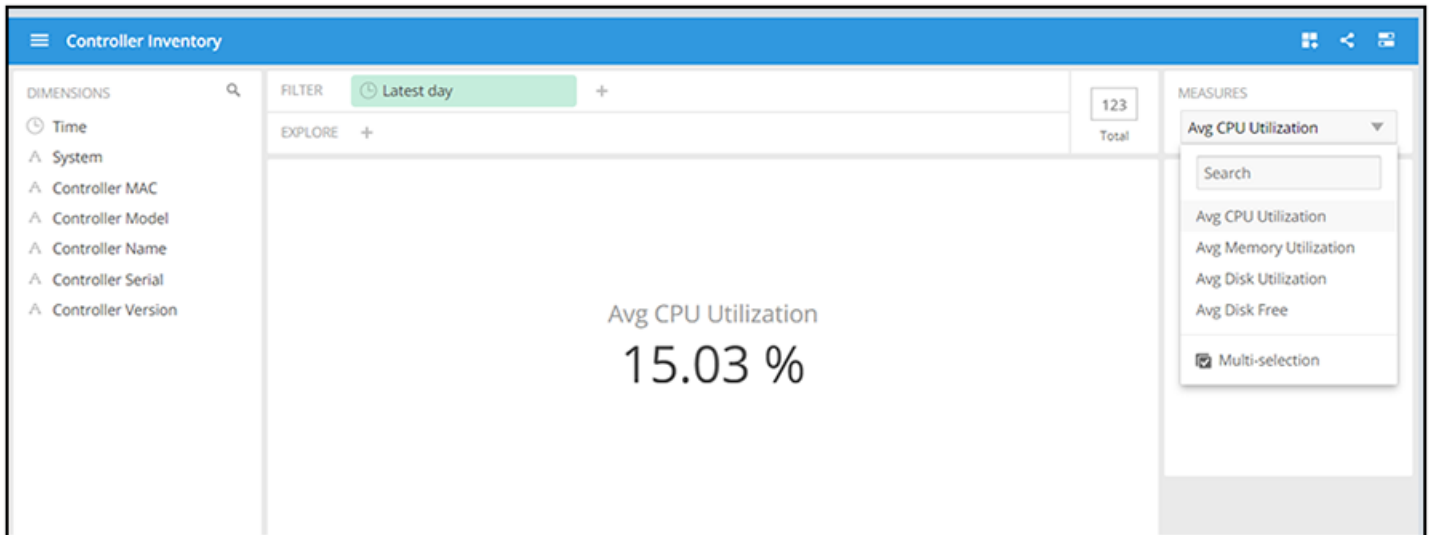
FIGURE 204 Data Explorer: AP Alarms



## Controller Inventory

The **Controller Inventory** cube allows you to view CPU, memory, and disk utilization for the controllers in the system.

FIGURE 205 Data Explorer: Controller Inventory



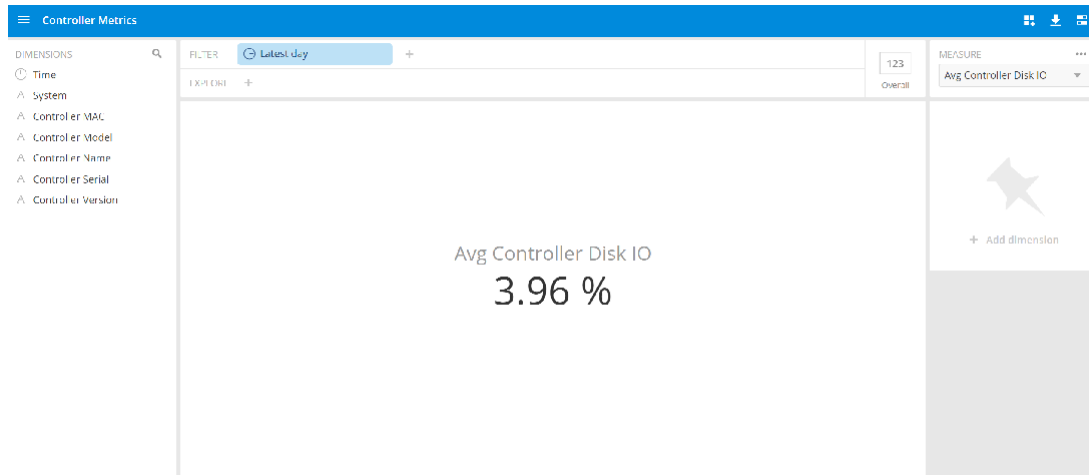
## Controller Metrics

The **Controller Metrics** cube allows you to view the computed client metrics (such as client TTC) in your system.

## Data Explorer

### Data Explorer and Data Cubes

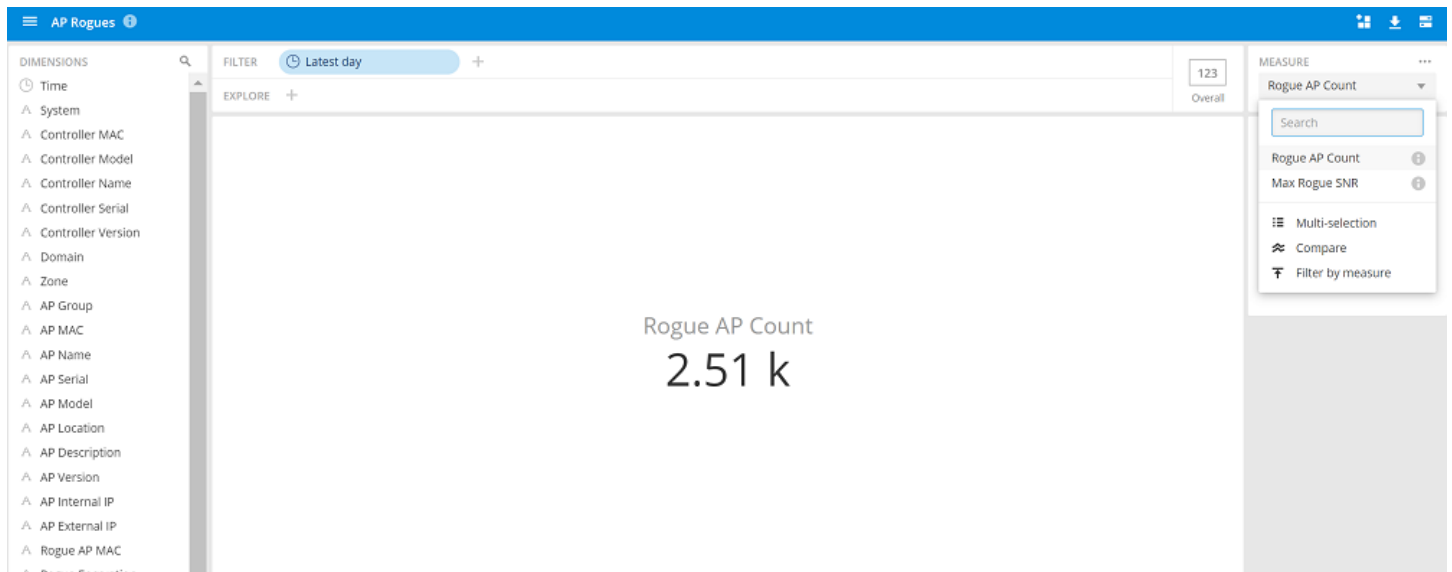
FIGURE 206 Data Explorer: Controller Metrics



## AP Rogues

The **AP Rogues** cube allows you to view information about APs that have been flagged as "Rogue" because they cannot be identified by existing APs in your system.

FIGURE 207 Data Explorer: AP Rogues

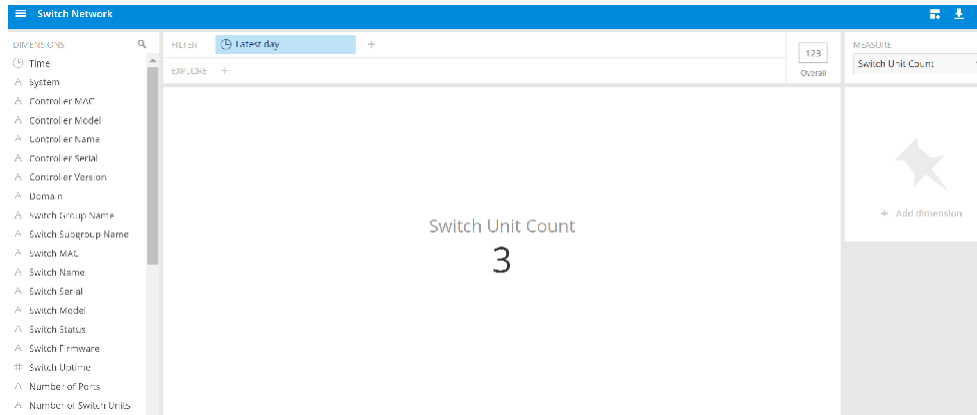


## Switch Network

The **Switch Network** cube allows you to explore switch traffic data and its usage.



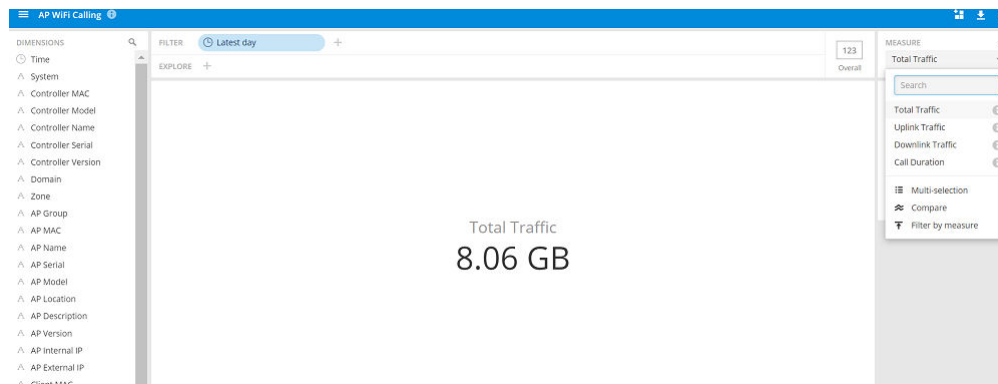
FIGURE 208 Data Explorer: Switch Network



## AP Wi-Fi Calling

The **AP Wi-Fi Calling** cube allows you to view several Wi-Fi Calling KPIs such as the call duration, uplink and downlink bytes and so on.

FIGURE 209 Data Explorer: AP Wi-Fi Calling



# Data Cube Filters

Data cubes contain groups of data sets, some of which exist in multiple cubes. The data cube filters are common to all the data cubes.

FIGURE 210 Data Cube Filters

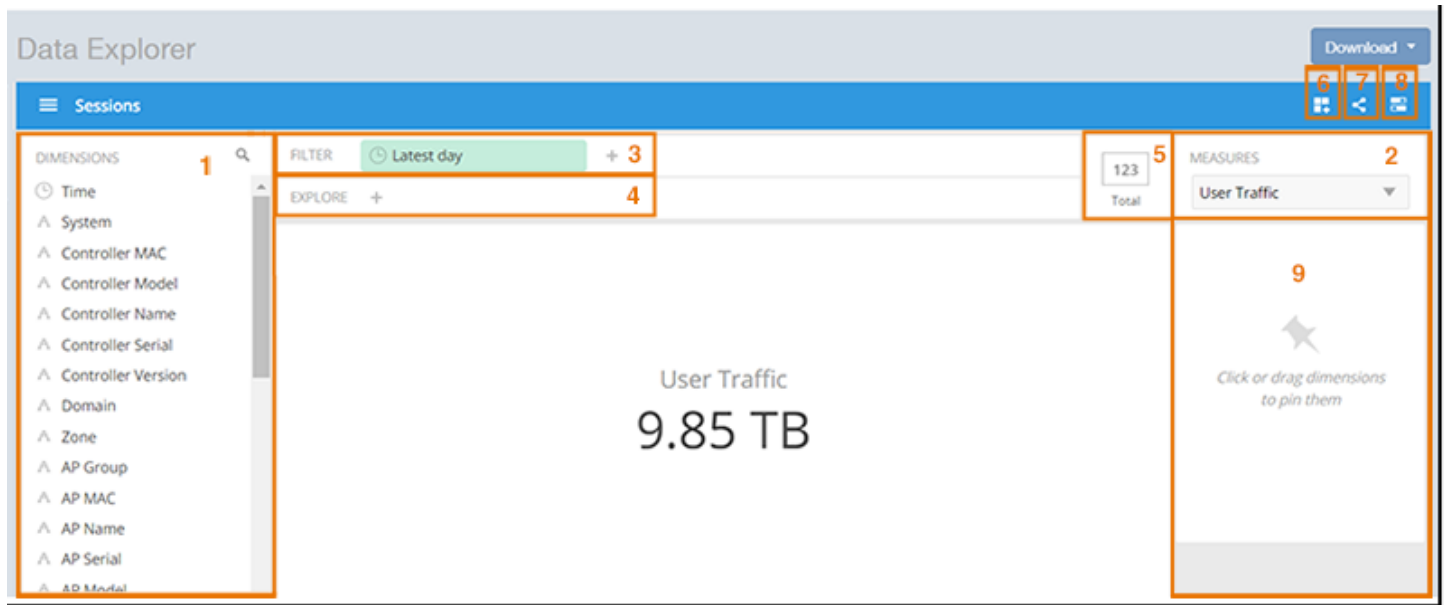


TABLE 15 Identifying Data Explorer Interface Components

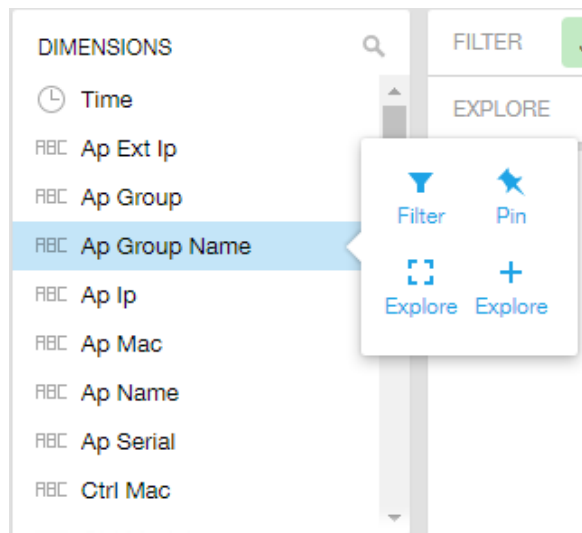
No	Name
1	Dimensions
2	Measures
3	Filter
4	Explore
5	View Outputs
6	Add to Dashboard
7	Share Link
8	Options
9	Pinboard

## Dimensions Filter

The **Dimensions filter** list the industry standard details for radio such as Time, AP name, System, and Zone name. You can apply one or more dimensions to the following:

- Filter: On one or more dimensions. The default dimension is Time.
- Explore: On one or more dimensions. Every dimension used in Explore can be sorted by one or more selected measures, and the number of dimensions to be listed in the table can be selected (5, 10, 25, 50, 100, 500 or 1000). You can also change the sorting order of the dimensions to be explored and pivot or change the hierarchy.
- Pin: One or more dimensions can be attached to the Pinboard for easy reference.

FIGURE 211 Dimensions



You can use the scroll bar for each data cube to view the supported dimensions for that cube. The following table describes all the dimensions that are supported on one or more data cubes in RUCKUS Analytics.

TABLE 16 Dimensions

Dimension Name	Description	Supported Data Cubes
Alarm Code	Unique string assigned by the controller to an alarm.	AP Alarms
Alarm State	Indicates if the alarm is outstanding.	AP Alarms
Alarm Type	Description for access point and controller alarms.	AP Alarms
Alarm UUID	Unique string assigned by the controller to an alarm.	AP Alarms
AP Description	Description string of the access point that is configured in the controller.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>
AP External IP	External IP address of the access point.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>

**TABLE 16** Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
AP Group	AP Groups configured in the controller.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>
AP Internal IP	Internal IP address of the access point.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>
AP Latitude	Latitude of GPS coordinates.	AP Inventory
AP Longitude	Longitude of GPS coordinates.	AP Inventory
AP Location	Location string of the access point that is configured in the controller.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>
AP MAC	Base MAC address of the access point.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>

**TABLE 16** Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
AP Model	Description of the access point model type.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>
AP Name	Name of the access point configured in the controller.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>
AP Serial	Serial number of the access point.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>
AP Version	Firmware version number of the access point.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>
Application Category	Amount of user traffic by category.	Applications
Application Name	Name of the application accessed by the Wi-Fi client.	Applications
Authentication Method	The Wi-Fi encryption and authentication method adopted.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
BSSID	Basic service set identifier.	Network
Cable modem firmware	Firmware version of the cable modem.	AP Inventory
Cable modem IP	IP address of the cable modem.	AP Inventory
Cable modem MAC	MAC address of the cable modem.	AP Inventory

**TABLE 16** Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
Category	Category for access point and controller alarms or events.	<ul style="list-style-type: none"> <li>Events</li> <li>AP Alarms</li> </ul>
Channel	The Wi-Fi channel number used.	<ul style="list-style-type: none"> <li>Network</li> <li>Clients</li> <li>Sessions</li> </ul>
Client IP	Internal IP address of the Wi-Fi client.	<ul style="list-style-type: none"> <li>Clients</li> <li>Sessions</li> </ul>
Client MAC	MAC address of the Wi-Fi client.	<ul style="list-style-type: none"> <li>Applications</li> <li>Clients</li> <li>Sessions</li> </ul>
Client Radio Mode	Possible values are: ac, n, a, g, b, or "unknown" (if SmartZone version is prior to 3.6).	<ul style="list-style-type: none"> <li>Clients</li> <li>Sessions</li> </ul>
Connection Status	Connection status of the access point: Online, Offline, Discovery, Provisioned.	<ul style="list-style-type: none"> <li>AP Inventory</li> </ul>
Controller MAC	MAC address of the controller.	<ul style="list-style-type: none"> <li>Applications</li> <li>Network</li> <li>Airtime Utilization</li> <li>Clients</li> <li>Sessions</li> <li>Events</li> <li>AP Inventory</li> <li>AP Alarms</li> <li>Controller Inventory</li> <li>Rogue APs</li> </ul>
Controller Model	Description of the model of the controller.	<ul style="list-style-type: none"> <li>Applications</li> <li>Network</li> <li>Airtime Utilization</li> <li>Clients</li> <li>Sessions</li> <li>Events</li> <li>AP Inventory</li> <li>AP Alarms</li> <li>Controller Inventory</li> <li>Rogue APs</li> </ul>
Controller Name	Name of the configured controller.	<ul style="list-style-type: none"> <li>Applications</li> <li>Network</li> <li>Airtime Utilization</li> <li>Clients</li> <li>Sessions</li> <li>Events</li> <li>AP Inventory</li> <li>AP Alarms</li> <li>Controller Inventory</li> <li>Rogue APs</li> </ul>

**TABLE 16** Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
Controller Serial	Serial number of the controller.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Controller Inventory</li> <li>• Rogue APs</li> </ul>
Controller Version	Firmware version number of the controller.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Controller Inventory</li> <li>• Rogue APs</li> </ul>
Disconnect Time	Disconnect time of a session.	Sessions
Domain	Domains configured in the controller.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>
Event Code	Code number for access point and controller events.	Events
Event Type	Description for access point and controller events.	Events
First Connection	First connection time of a session.	Sessions
Hostname	Hostname configured in the Wi-Fi client.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
Last Status Change	Date and time of the last change in Connection Status of the access point.	AP Inventory
Manufacturer	Manufacturer information for the Wi-Fi client.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
OS Type	Operating System information for the Wi-Fi client.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
Port	Port of the application accessed by the Wi-Fi client.	Applications

**TABLE 16** Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
Radio	Indicates the radio frequency band: 2.4GHz or 5GHz.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> </ul>
Reason	Additional description for access point and controller alarms or events, if available.	<ul style="list-style-type: none"> <li>• Events</li> <li>• AP Alarms</li> </ul>
Roaming Session ID	A unique session ID that is created when a client roams to multiple APs within a short-enough time span that the client is connected to these APs simultaneously.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
Rogue AP MAC	MAC Address of the detected Rogue AP.	Rogue APs
Rogue Channel	The Wi-Fi channel that the Rogue APs was operating on.	Rogue APs
Rogue Encryption	The Wi-Fi encryption and authentication method adopted by the rogue AP.	Rogue APs
Rogue Radio	The radio band (2.4GHz or 5GHz) that the rogue AP was operating on.	Rogue APs
Rogue SSID	SSID of the detected Rogue AP.	Rogue APs
Rogue Type	Possible types are: ignore, known, rogue, and malicious	Rogue AP
Session ID	ID string assigned to a session.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
Session Type	Indicates whether the session is authorized or unauthorized.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
Severity	Severity level for access point and controller alarms or events.	<ul style="list-style-type: none"> <li>• Events</li> <li>• AP Alarms</li> </ul>
SSID	Service set identifier (SSID) configured in the controller.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Clients</li> <li>• Sessions</li> </ul>
System	System ID of the controller or the SmartZone Cluster.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Controller Inventory</li> <li>• Rogue APs</li> </ul>



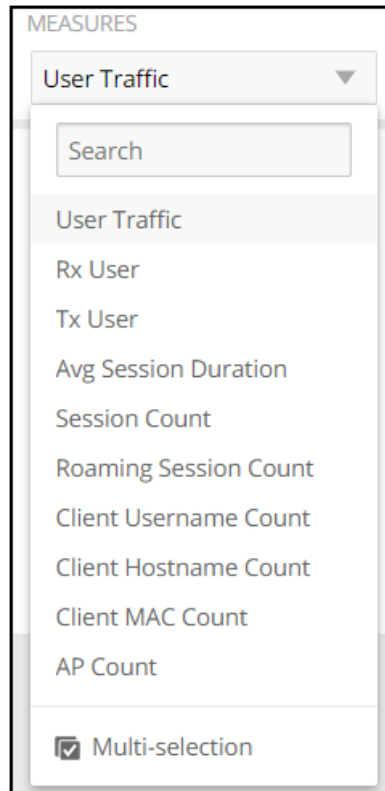
**TABLE 16** Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
Time	Allows the data to be viewed in terms of data points with timestamps. Time granularity of 1 minute, 15 minutes, 1 hour, 1 day, and 1 week can be chosen.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Controller Inventory</li> <li>• Rogue APs</li> </ul>
Username	Username of the user account associated with the Wi-Fi client.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
Zone	Zones configured in the controller.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> <li>• Rogue APs</li> </ul>

## Measures Filter

You can select one or more measures by which you want to sort the selected dimension. Based on the selected cube, measures can vary.

FIGURE 212 Measures



You can use the lists for each data cube to view the supported measures for that cube. The following table describes all the measures that are supported on one or more data cubes in RUCKUS Analytics.

TABLE 17 Measures

Measure Name	Description	Supported Data Cubes
AP Count	Unique number of access points.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> <li>• Events</li> <li>• AP Inventory</li> <li>• AP Alarms</li> </ul>
AP Uptime	Uptime percentage for an access point.	AP Inventory
AP-to-SZ Ping Latency	Average time, in milliseconds, for the AP to transmit a packet to the SZ controller, and receive the packet back.	Network
Avg Airtime Busy	Average of the airtime busy metric.	Airtime Utilization
Avg Airtime Idle	Average of the airtime idle metric.	Airtime Utilization
Avg Airtime Rx	Average of the airtime receive metric.	Airtime Utilization
Avg Airtime Tx	Average of the airtime transmit metric.	Airtime Utilization

**TABLE 17** Measures (continued)

Measure Name	Description	Supported Data Cubes
Avg Airtime Utilization	Average of the total airtime utilization.	Airtime Utilization
Avg CPU Utilization	Average CPU utilization for the controller.	Controller Inventory
Avg Disk Free	Average free disk space for the controller.	Controller Inventory
Avg Disk Utilization	Average disk utilization for the controller.	Controller Inventory
Avg Memory Utilization	Average memory utilization for the controller.	Controller Inventory
Avg Noise Floor	Average noise floor power in dBm.	Clients
Avg RSS	Average received signal strength of the access point in dBm.	Clients
Avg Session Duration	Average time duration for a session.	Sessions
Avg SNR	Average signal to noise ratio at the access point in dB.	Clients
Avg Throughput Estimate	Average throughput estimate for the Wi-Fi client.	Clients
Client Hostname	Name of the client	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
Client MAC Count	Unique number of Wi-Fi clients.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Clients</li> <li>• Sessions</li> </ul>
Client Username	Name of the user	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
Count	Client count	<ul style="list-style-type: none"> <li>• Events</li> <li>• AP Alarms</li> </ul>
Failed Associations	Number of failed associations.	Network
Failed Authentications	Number of failed open authentications	Network
Mgmt Traffic	Traffic volume, which is transmitted and received in IEEE 802.11 control and management frames; this includes all unicast, multicast, and broadcast traffic.	<ul style="list-style-type: none"> <li>• Network</li> <li>• Airtime Utilization</li> </ul>
Max Offline Duration	The maximum offline duration within the selected time range.	AP Inventory
Max Rogue SNR	The maximum detected signal to noise of the rogue AP.	Rogue APs
Max RSS	Maximum received signal strength of the access point in dBm.	Clients
Max SNR	Maximum signal to noise ratio at the access point in dB.	Clients
Min RSS	Minimum received signal strength of the access point in dBm.	Clients
Min SNR	Minimum signal to noise ratio at the access point in dB.	Clients
Reboot Count		Events
Roaming Session Count	The number of roaming sessions for a specific client. A roaming session occurs when a client roams quickly enough to remain connected to multiple APs simultaneously. If you find a client that has a large number of roaming sessions, you can use various dimensions in Data Explorer to obtain details about the APs.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>

**TABLE 17** Measures (continued)

Measure Name	Description	Supported Data Cubes
Rogue AP Count	The number of rogue APs detected by all the APs in your network.	Rogue APs
Rx Failures	Receive packets which failed to be processed due to insufficient buffer in AP.	Network
Rx Management	Traffic volume, which is received by AP (Access Point) in IEEE 802.11 control and management frames; this includes all unicast, multicast, and broadcast traffic.	<ul style="list-style-type: none"> <li>• Network</li> <li>• Airtime Utilization</li> </ul>
Rx Total	Sum of the received user and management traffic.	<ul style="list-style-type: none"> <li>• Network</li> <li>• Airtime Utilization</li> </ul>
Rx User	Traffic volume, which is received by AP in IEEE 802.11 MAC Service Data Unit (MSDU) data frames; this includes all unicast, multicast, and broadcast traffic.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> </ul>
Session Count	Number of unique sessions.	<ul style="list-style-type: none"> <li>• Clients</li> <li>• Sessions</li> </ul>
Successful Associations	Number of successful associations.	Network
Successful Authentications	Number of successful open authentications	Network
Successful Authentication Ratio	Ratio of number of successful open authentications over total number of open authentications.	Network
Total Data Frames Ratio	Percentage of all transmit and receive packets that are data.	Network
Total Management Frames Ratio	Percentage of all transmit and receive packets that are management.	Network
Total Traffic	Sum of the user and management traffic.	<ul style="list-style-type: none"> <li>• Network</li> <li>• Airtime Utilization</li> </ul>
TxBroadcastFrames	Number of broadcast packets transmitted by the network.	Network
TxDropDataFrames	Transmit data frames that are dropped by the message queue.	Network
Tx Failures	Transmit packets which failed to be processed due to insufficient buffer in AP.	Network
Tx Management	Traffic volume, which is transmitted by AP (Access Point) in IEEE 802.11 control and management frames; this includes all unicast, multicast, and broadcast traffic.	<ul style="list-style-type: none"> <li>• Network</li> <li>• Airtime Utilization</li> </ul>
TxMulticastFrames	Number of multicast packets transmitted by the network.	Network
Tx Total	Sum of the transmit user and management traffic.	<ul style="list-style-type: none"> <li>• Network</li> <li>• Airtime Utilization</li> </ul>
TxUnicastFrames	The number of data packets transmitted by the network that are not broadcast or multicast packets.	Network

TABLE 17 Measures (continued)

Measure Name	Description	Supported Data Cubes
Tx User	Traffic volume, which is transmitted by AP (Access Point) in IEEE 802.11 MAC Service Data Unit (MSDU) data frames; this includes all unicast, multicast, and broadcast traffic.	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> </ul>
User Traffic	Traffic volume, which is transmitted and received in IEEE 802.11 MAC Service Data Unit (MSDU) data frames; this includes all unicast, multicast, and broadcast traffic. User Traffic = Rx User + Tx User	<ul style="list-style-type: none"> <li>• Applications</li> <li>• Network</li> <li>• Airtime Utilization</li> <li>• Clients</li> <li>• Sessions</li> </ul>

## Filter

You can use **Filter** to segregate the data by dimensions such as Time Range, and other dimensions. You can filter on one or more dimensions, and change the sorting hierarchy as required. You can also define the dimensions based on specific properties of the dimension, for example, Time has relative and specific settings. The default dimension is Time, because the databases are very large and can crash the system without this filter.

FIGURE 213 Filter

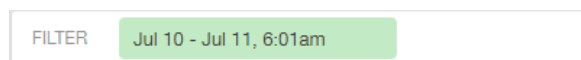
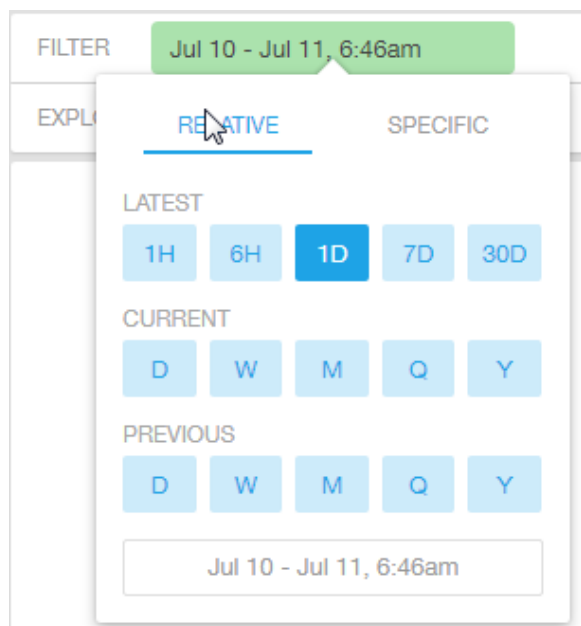


FIGURE 214 Relative Time Settings



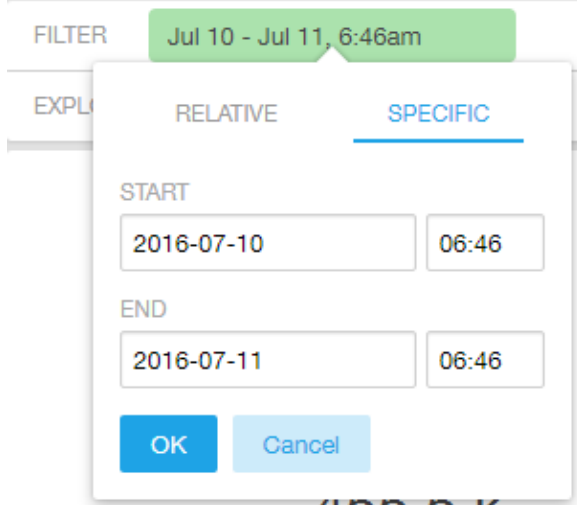
You can specify the following relative time settings:

- Latest time of 1 hour, 6 hours, 1 day, 7 days, or 30 days

**Data Explorer**  
Data Cube Filters

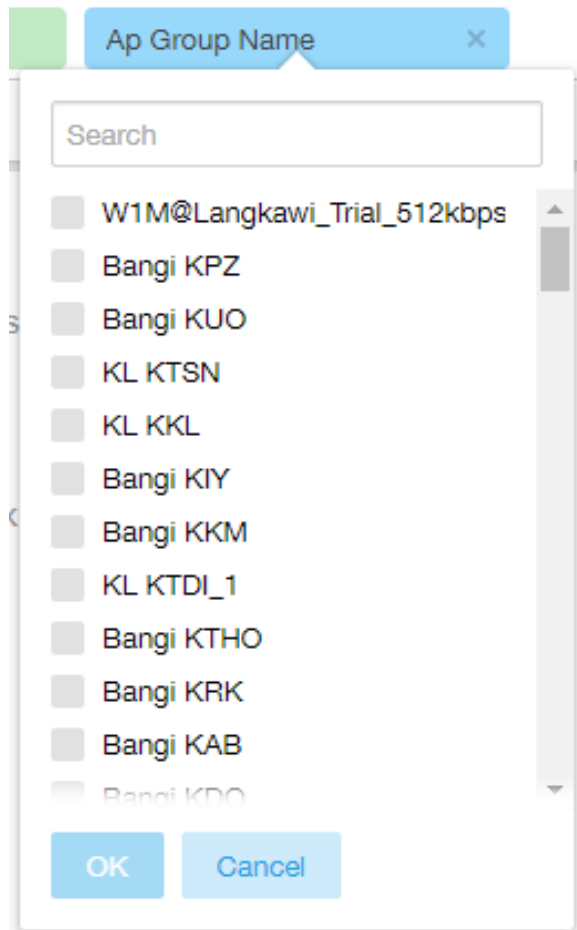
- Current time of day, week, month, quarter, or year
- Previous time of day, week, month, quarter, or year

**FIGURE 215** Specific Time Settings



You can specify the start and end dates and times for the specific time settings.

FIGURE 216 Dimension Options

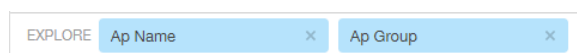


You can search the list of the dimensions and select specific entries. By default, all the data that matches the dimension is listed.

## Explore Filter

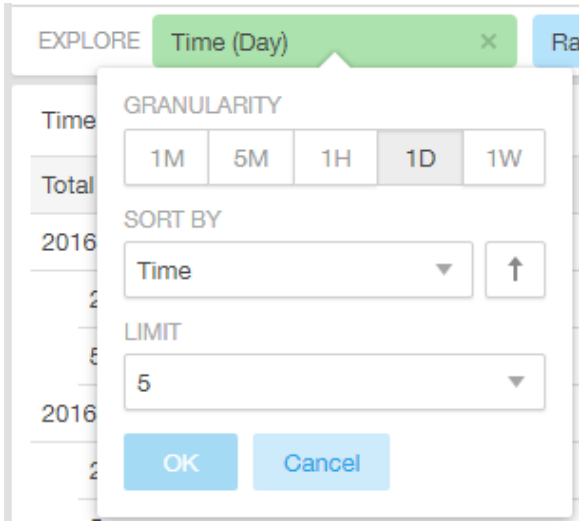
The **Explore filter** enables visualization based on dimensions and time (data granularity).

FIGURE 217 Explore



You can explore one or more dimensions using a methodology similar to pivot tables, and change the sorting hierarchy as required. You can define the number of rows to be listed the screen.

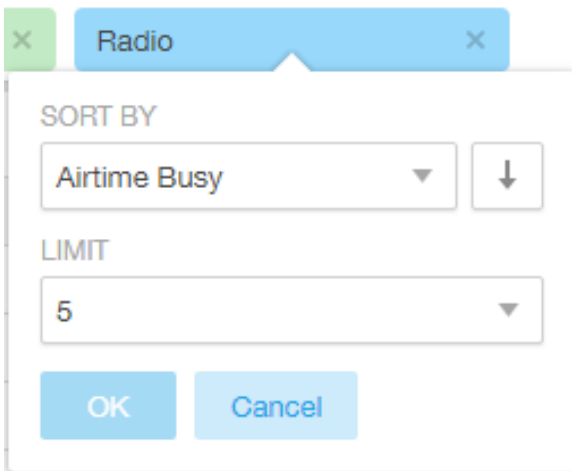
FIGURE 218 Explore Time



You can use the following time filters:

- Set the data granularity to 1 minute, 5 minutes, 1 hour, 1 day, or 1 week.
- Sort by any of the measures related to the dimension.
- Limit the number of rows displayed for the dimension to 5, 10, 25, 50, 100, 500, or 1000.

FIGURE 219 Sort Dimension by Measure



You can use the following measures filters:

- Sort by any of the measures related to the dimension.
- Limit the number of rows displayed for the dimension to 5, 10, 25, 50, 100, 500, or 1000.



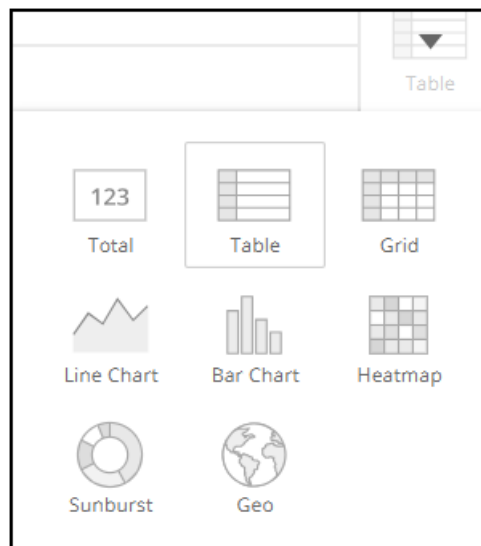
## View Outputs Filter

You can create output views in the following forms:

- Total
- Table
- Grid
- Line Chart
- Bar Chart
- Heatmap
- Sunburst
- Geo

The default view is Total.

FIGURE 220 View Outputs



## Add to Dashboard Icon

The **Add to Dashboard** icon allows you to add a tile you are currently developing to an existing dashboard or to a dashboard that you want to create.

FIGURE 221 Add to Dashboard



## Share Link Icon

You can share the URL, export to various formats, view raw data, or download the information. The following figure shows the various formats you can choose for downloading data. You can also select the number of rows to download.

FIGURE 222 Share Link

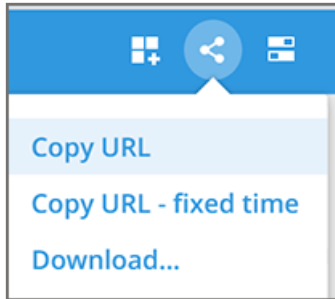
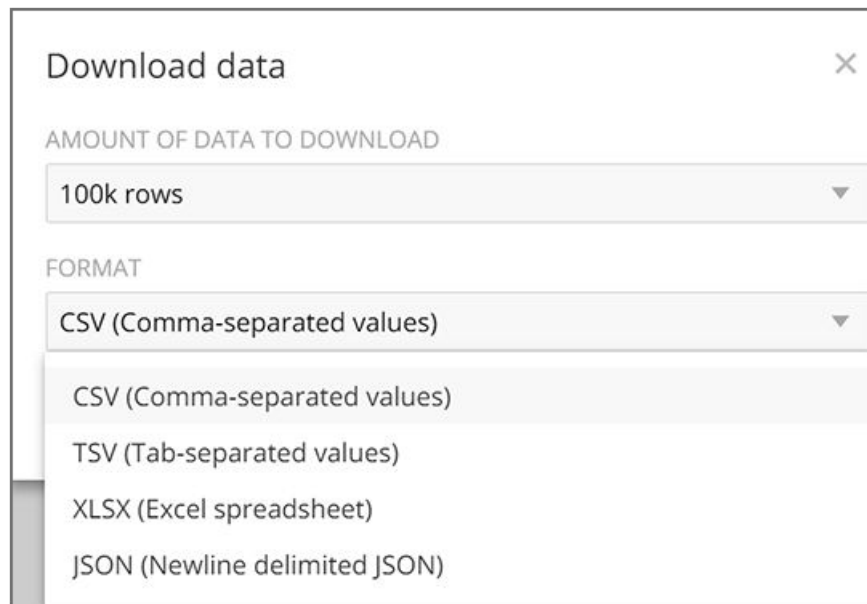


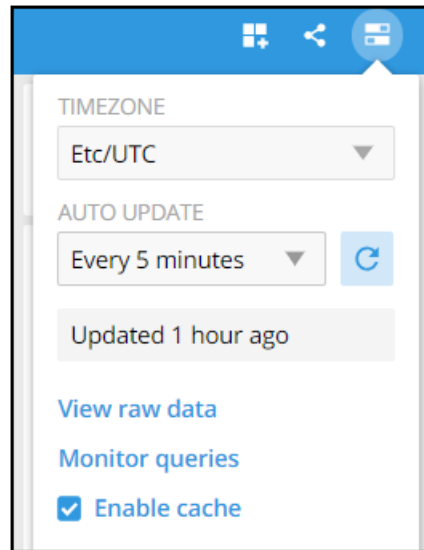
FIGURE 223 Selecting the Amount of Data to Download and the Desired Format



## Options Icon

The **Options** icon allows you to set the time zone, auto update time for the dashboard data, view raw data, monitor queries, and enable cache memory as shown.

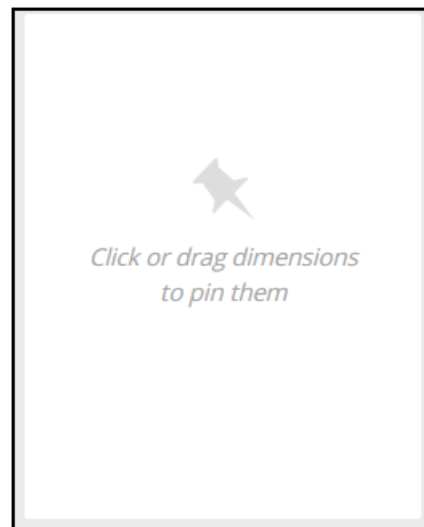
FIGURE 224 Options



## Pinboard Pane

You can click or drag dimensions and pin them on the pinboard. Retain the dimensions for ready reference during visualization.

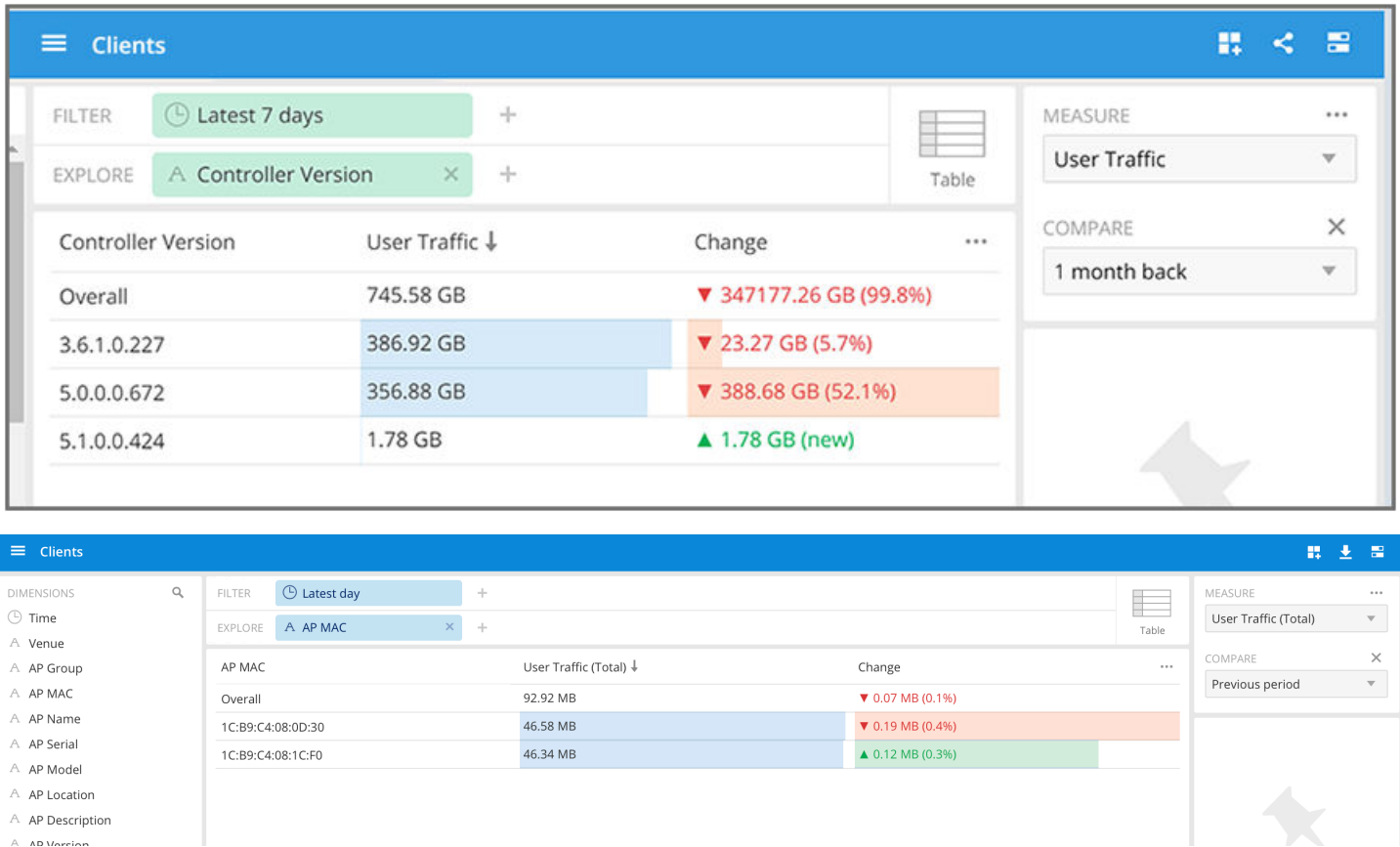
FIGURE 225 Pinboard



## Comparisons

Comparisons allow you to compare the current data of specified dimensions and measures to the same dimensions and measures during previous time periods. For example, the Controller Version dimension and User Traffic measure can be compared over time, as shown in the following figure. The **Change** column indicates how much user traffic has gone up or down for the corresponding controller version over the specified period of time.

FIGURE 226 Comparison Over Time

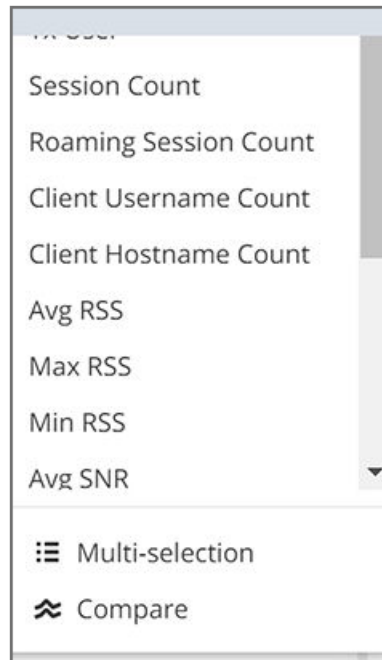


## Creating a Data Comparison

You can create a data comparison using **Data Explorer**.

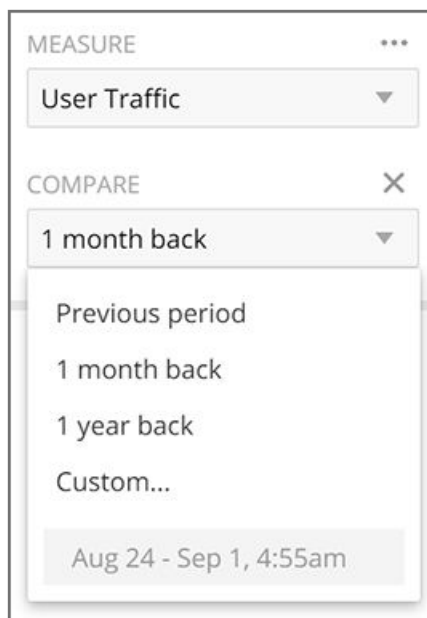
1. From **Data Explorer**, select one of the data cubes.
2. Drag one or more dimensions into the center pane, for example, Controller Version.
3. From the **Measure** list, select one or more measures (use **Multi-Selection** for more than one).
4. From the **Measure** list, select **Compare**.

**FIGURE 227** Selecting Compare from the Measure List



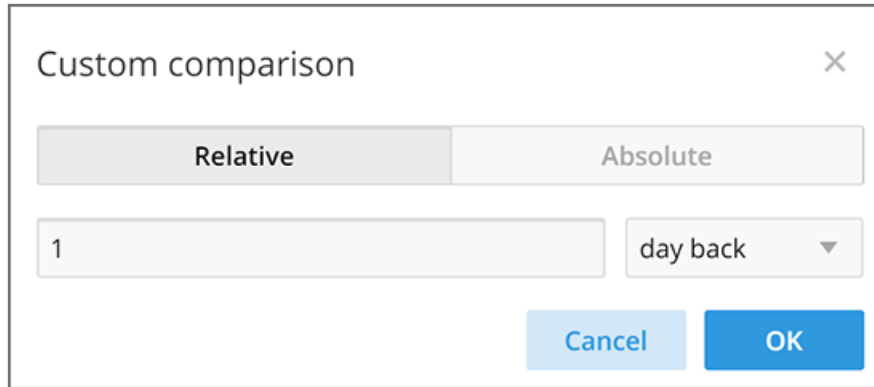
5. If you have already invoked **Compare**, the previous time period you selected is automatically used, and a display such as the one in [Figure 226](#) is displayed. However, if you have not yet used Compare, or if you want to change the current time-period, invoke the **Compare** list:

**FIGURE 228** Using the Compare List



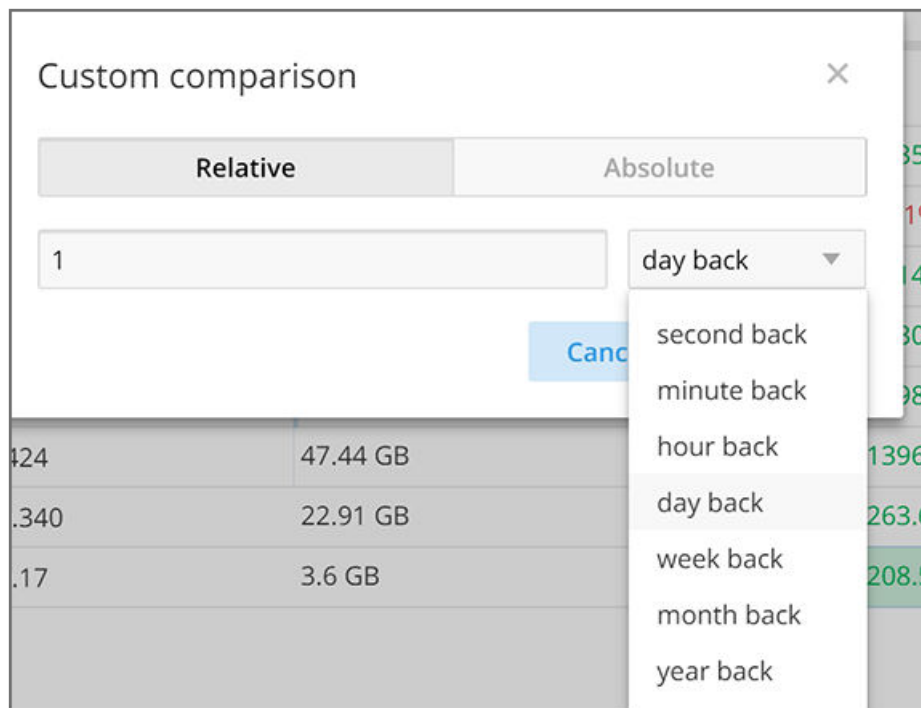
6. (Optional) To customize your choice, click **Custom**. **Custom comparison** dialog box is displayed.

FIGURE 229 Custom Comparison Dialog Box



- To set a relative comparison, click the **Relative** tab and select a measure from the relative measure list.

FIGURE 230 List of Choices from the Relative Measure List



You can change the number of the measure to correspond to your selection in the relative measure list. Click **OK** to create the relative comparison.

- To create a custom time period, click the **Absolute** tab.

FIGURE 231 Custom Comparison: Absolute Tab

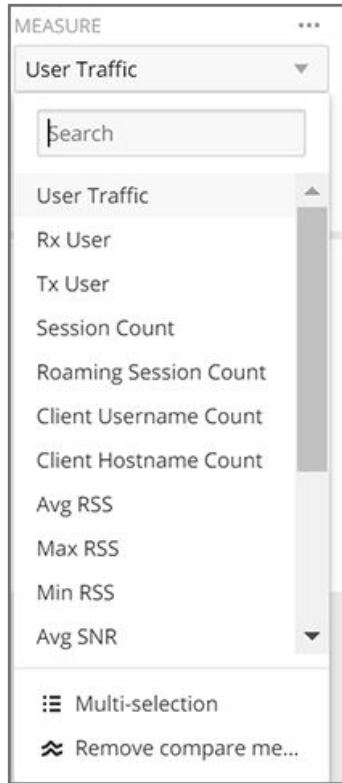
The screenshot shows a dialog box titled "Custom comparison" with a close button (X) in the top right corner. Below the title bar, there are two tabs: "Relative" and "Absolute", with "Absolute" being the active tab. Under the "START TIME" section, there are two input fields: the first contains "2018-09-26" and the second contains "17:46". Below these fields is a checked checkbox labeled "Auto adjust end date". Under the "END TIME" section, there are two input fields: the first contains "2018-09-27" and the second contains "17:46". At the bottom right of the dialog, there are two buttons: "Cancel" and "OK".

You can change the times as desired, and to have the end date automatically adjusted. Click **OK** to set the custom time period.

## Removing the Compare Feature

If you want to remove the **Compare** measure from the data display, go to the **Measure** list, and select **Remove Compare Measure**.

FIGURE 232 Removing the Compare Measure





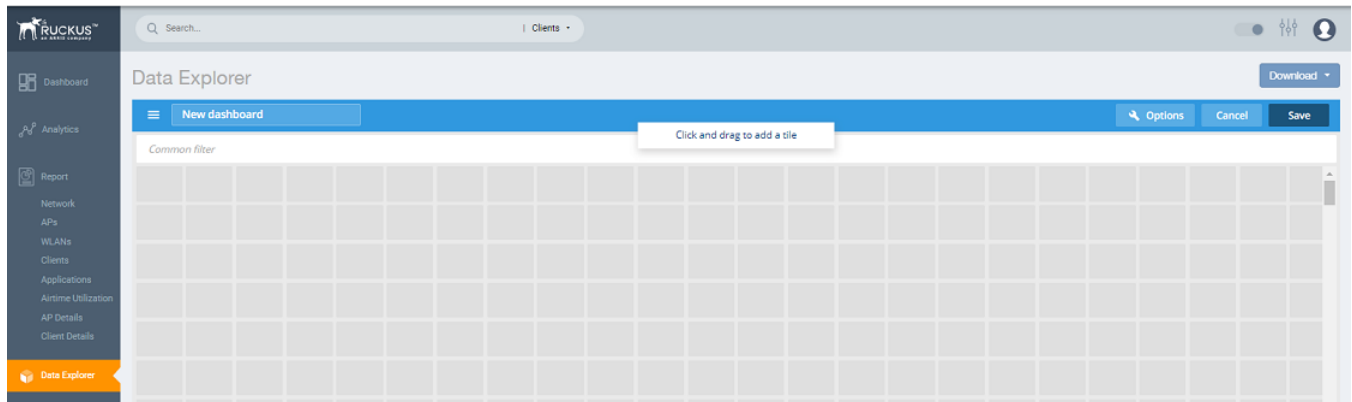
## Creating a Data Explorer Dashboard

You can create custom dashboards in **Data Explorer** portion to focus on data you are interested in that encompasses any or all of the data cubes. These dashboards can be saved so that you can create reports for this unique data set whenever you wish.

1. Click **+ Dashboard** in the upper-right corner of **Data Explorer**.

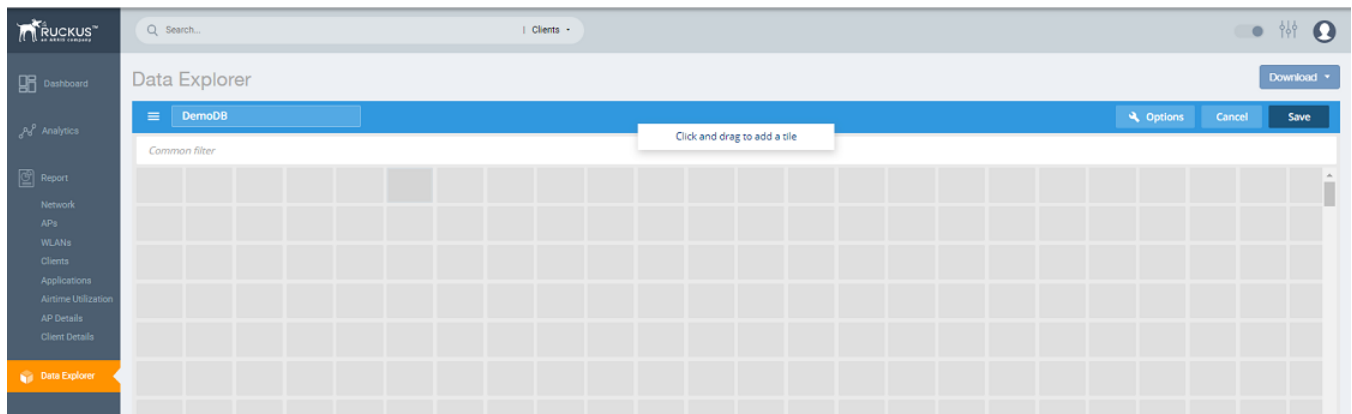
The **New dashboard** screen is displayed.

**FIGURE 233** New Dashboard Screen



2. Highlight **New dashboard** and enter a name for the dashboard (for example, DemoDB, as shown in the following figure).

**FIGURE 234** Naming the New Dashboard

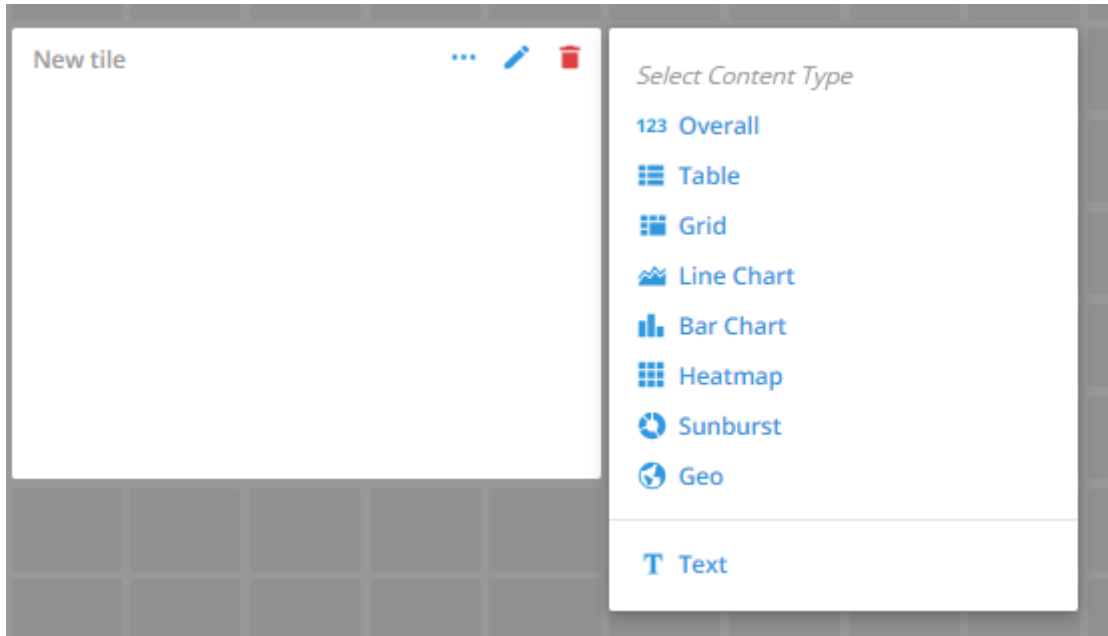


## Data Explorer

### Creating a Data Explorer Dashboard

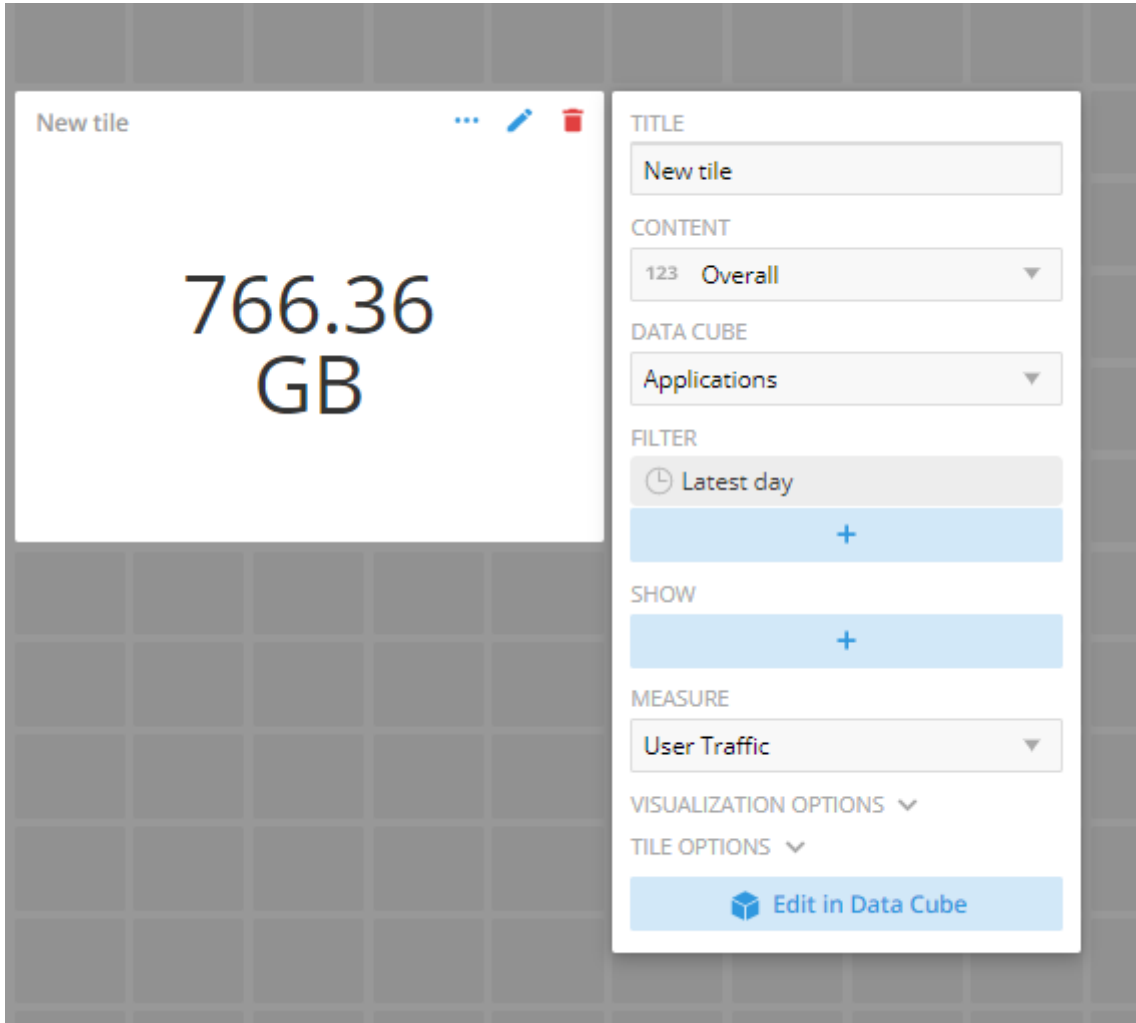
3. Highlight any number of small boxes in the grid on the screen to add a tile to your dashboard. The **Select Content Type** pane is displayed along with the new tile.

**FIGURE 235** Adding a Tile to Your Dashboard



4. Select a content type, for example, 123 Overall, as shown in the following figure

**FIGURE 236** New Tile Options for 123 Overall Content Type



## Data Explorer

### Creating a Data Explorer Dashboard

5. Select options to customize the new tile.

**FIGURE 237** Selecting Options for New Tile

The screenshot displays the 'New tile' configuration interface. On the left, a table lists systems and their total traffic. On the right, a configuration panel allows users to customize the tile's appearance and data source.

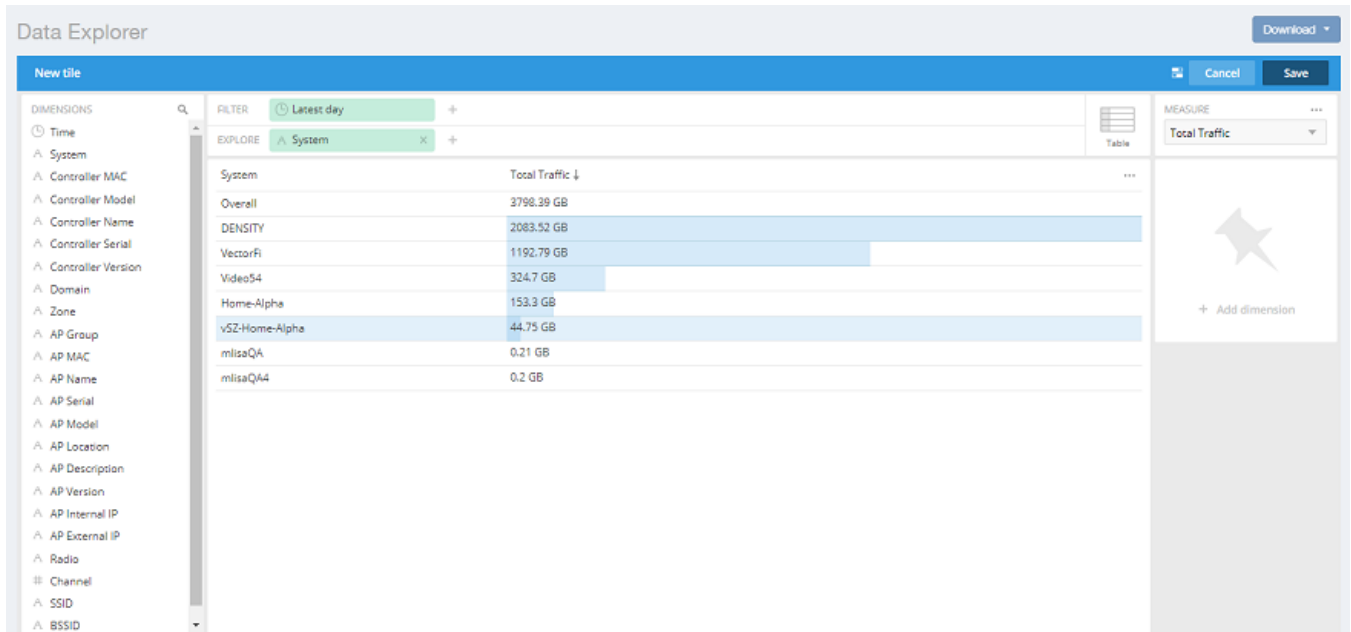
System	Total Traffic ↓
DENSITY	2041.76 GB
VectorFi	1261.78 GB
Video54	208.32 GB
Home-Alpha	163.85 GB
vSZ-Home-Al...	48.74 GB
...	...

**Configuration Panel:**

- TITLE:** New tile
- CONTENT:** Table
- DATA CUBE:** Network
- FILTER:** Latest day
- SHOW:** System
- MEASURE:** Total Traffic
- VISUALIZATION OPTIONS:** (Dropdown)
- TILE OPTIONS:** (Dropdown)
- Buttons:** Edit in Data Cube

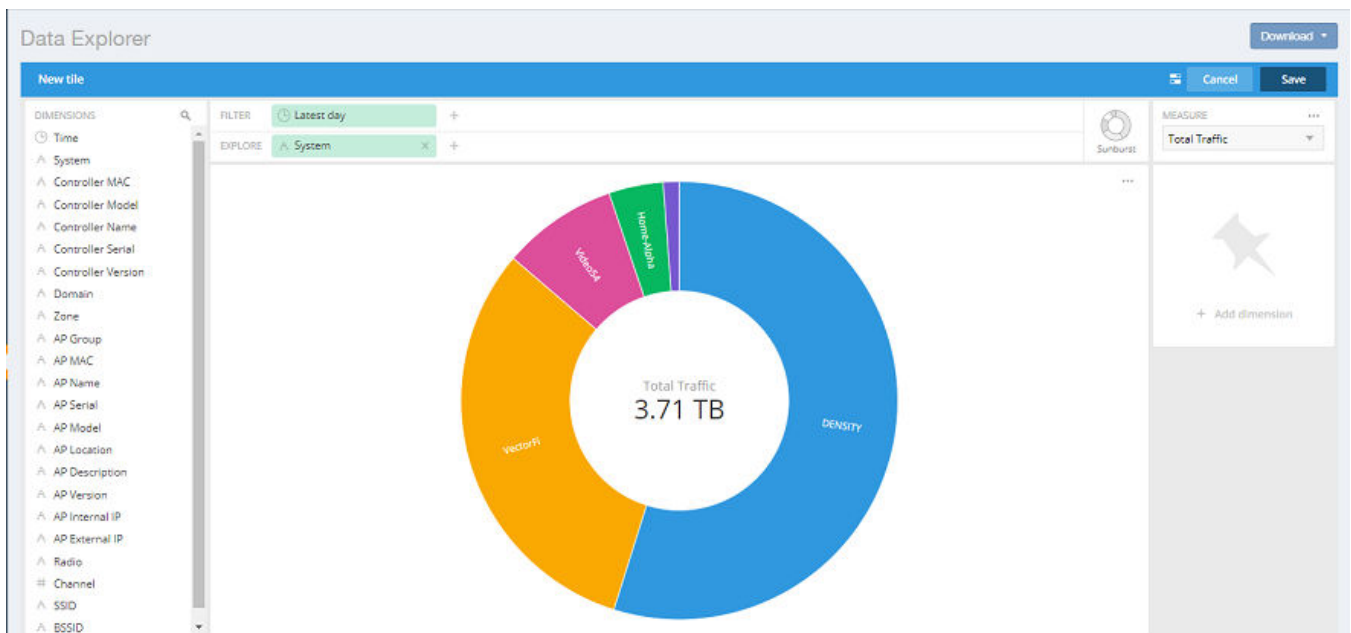
6. Click **Edit in Data Cube** to make changes to the new tile in the data cube.

**FIGURE 238** Editing New Tile in the Data Cube



7. To change the way the data is represented, pause the pointer over the Table icon and select a different content type, for example, Sunburst, as shown in the following figure.

**FIGURE 239** Sunburst Representation of Tile in Data Cube



## Data Explorer

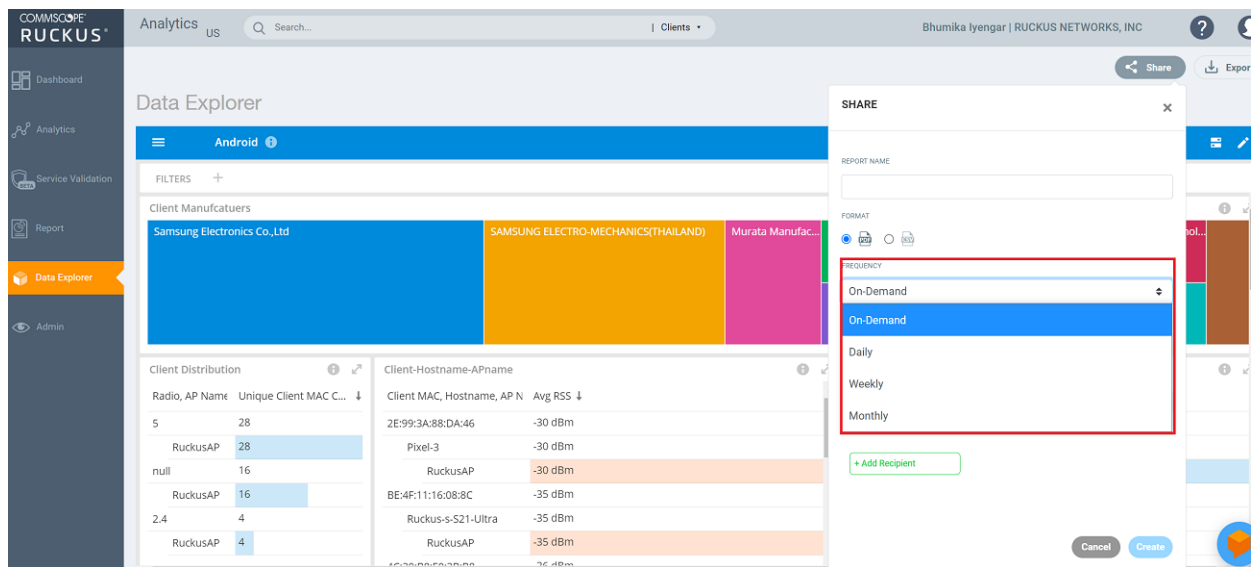
### Actions You Can Perform on an Existing Dashboard

- Click **Save** in the upper-right corner of the screen to save the new tile selections  
You can as many tiles as you want to your dashboard.

#### NOTE

The scheduler is only applicable for custom dashboards in Data Explorer.

**FIGURE 240** Custom Dashboard with Scheduler



## Actions You Can Perform on an Existing Dashboard

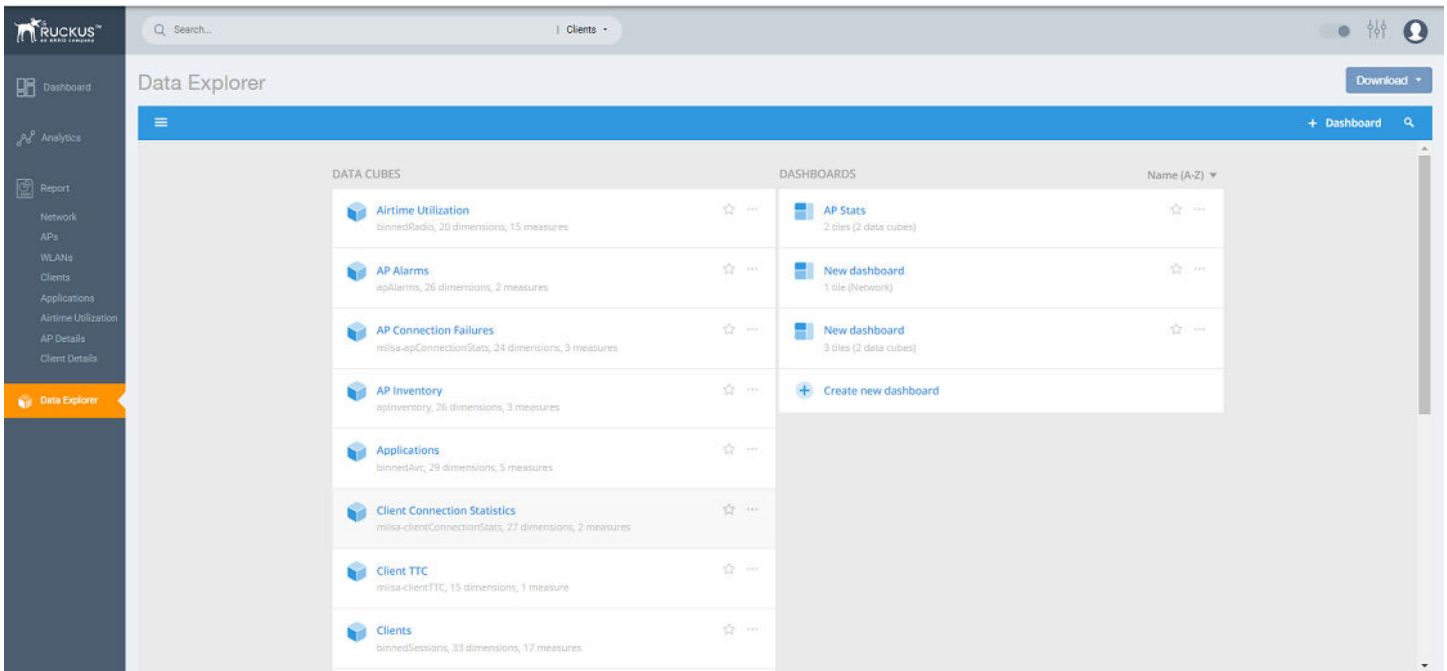
You can perform many actions on an existing dashboard, such as adding or removing tiles, editing existing tiles, deleting tiles and deleting the entire dashboard.

### Opening a Dashboard

When you click the **Data Explorer** in the navigation bar, the data cubes are shown on the left and the existing dashboards are shown on the right of the screen. To open a dashboard, take one of the following actions:

- Click the name of the dashboard you want to open.
- Click the More Options icon (the three horizontal lines in the upper-left corner of the screen), and either use the Search field or locate the desired dashboard to open it.

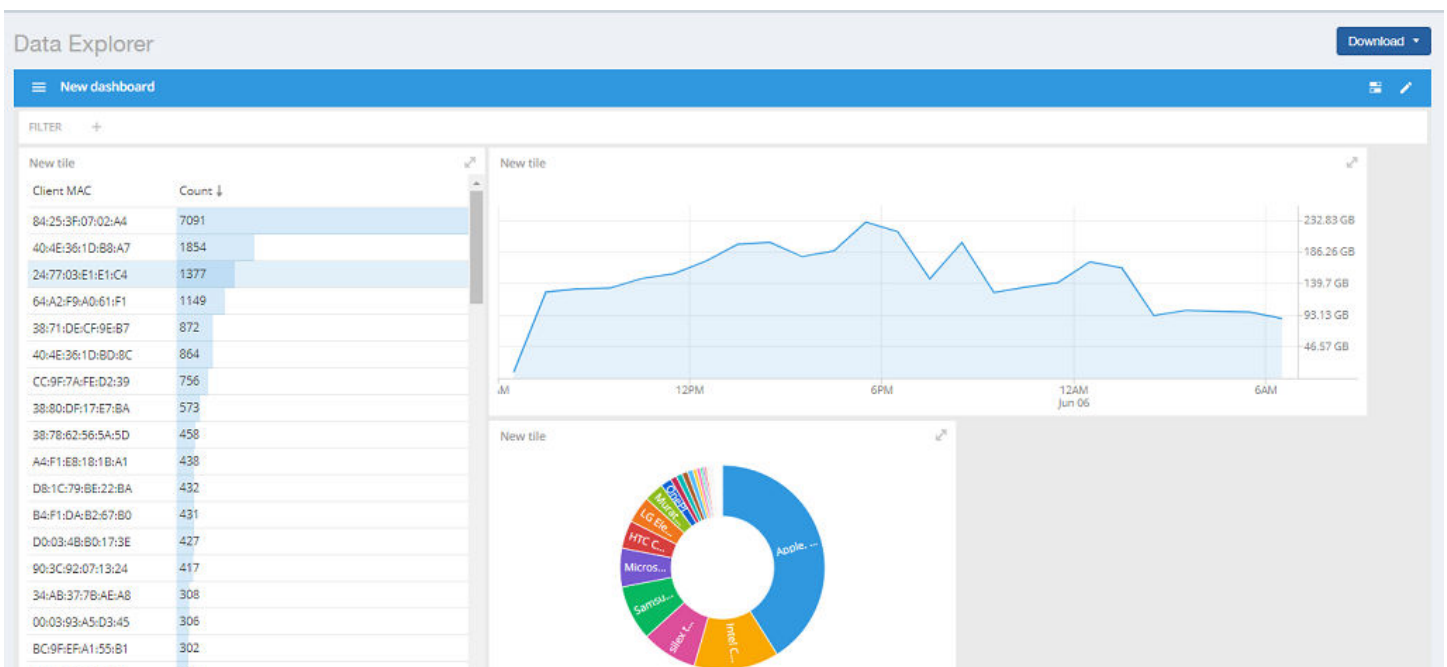
FIGURE 241 Data Cubes and Dashboards in Data Explorer



## Editing a Dashboard

To perform various editing functions on a dashboard, first open the dashboard you want.

FIGURE 242 Dashboard Example with Three Tiles



## Data Explorer

### Actions You Can Perform on an Existing Dashboard




In the upper-right corner of the screen, the dashboard-editing icons are displayed.

**FIGURE 243** Dashboard-Editing Icons



The following table identifies each icon and the actions you can perform.

**TABLE 18** Icons for Editing a Dashboard

Icon	Name of Icon	Actions
	Dashboard options	You can change the following settings: <ul style="list-style-type: none"><li>• Time zone</li><li>• Auto-update interval</li><li>• Enabling or disabling cache</li></ul>
	Edit this dashboard	You can perform the following actions: <ul style="list-style-type: none"><li>• Rearrange or resize the tiles.</li><li>• Make changes to specific tiles within the dashboard by using the icons are displayed for each tile: </li></ul> <ul style="list-style-type: none"><li>- Click the three dots icon to duplicate the tile.</li><li>- Click the pencil icon to add or remove dimensions and measures for the tile, and to change the representation of the data for the tile.</li><li>- Click the garbage can icon to delete the tile from the dashboard.</li></ul>

Click on the **Options** tab in the upper-right corner of the screen. Another screen is displayed containing general information about the dashboard.

Two tabs, **General** and **Access**, are displayed. In the **General** tab, perform the following actions:

- Rename the dashboard
- Add or modify a description of the dashboard
- Change the color theme
- Decide whether to enforce the time filter
- Delete the dashboard

In the **Access** tab, you can set who you want to view and edit the dashboard. Remember to click **Save** to save your changes.



FIGURE 244 General and Access Options to Edit Dashboards

The image shows two screenshots of the 'Dashboard options' interface. The top screenshot shows the 'General' tab selected, with the following fields and options:

- TITLE:** Application Data
- DESCRIPTION:** (empty text field)
- COLOR THEME:** Global default
- PAGES:** Hide pages selector
- GLOBAL FILTERS:** Show global filters
- ENFORCE TIME FILTER:** Do not force a time filter
- DASHBOARD ACTIONS:** Delete, Duplicate

The bottom screenshot shows the 'Access' tab selected, with the following options:

- CAN VIEW:** Only you
- CAN EDIT:** Only you



# Administration

---

- Viewing Onboarded Systems..... 203
- Managing Users..... 204
- Managing Resource Groups..... 205
- Contacting Ruckus Support..... 208
- Managing Licenses and Assigning APs..... 209
- Viewing Schedules..... 212
- Creating Webhooks..... 212

## Viewing Onboarded Systems

You can view the list of your SmartZone controllers that have onboarded to the system and also view additional information regarding their connection status, firmware versions, and so on.

In RUCKUS Analytics, you can access only your account information. If you are a third-party user requiring access to other accounts to manage them, for example, a VAR user requiring access to your customer's account, you can access the customer account only by onboarding the SmartZone controller. After the SmartZone controller is onboarded, a license is attached to the account. The controller data is made available after onboarding. However, access to the controller data is only possible when the license account IDs for the controller and RUCKUS Analytics are the same.

### NOTE

You must enable the **analytics** and **cloud features** in the controller and log in with your RUCKUS customer login details to onboard the controller. For more information, refer to [Onboarding the controller to RUCKUS Analytics](#) on page 203.

From the web interface, go to **Admin > Onboarded Systems**.

The **Onboarded Systems** page displays the following information about the controller:

- **Status:** Displays the connection status of the onboarded controller. If the controller has onboarded and connected successfully, and if data is transmitted to RUCKUS Analytics, the status is displayed in **Green**. If the controller is offboarded and not sending any data, the status is displayed in **Grey**. If the onboarding is in progress, the status is displayed in **Yellow**. If the connection to the controller is lost, or when data is not transmitted, the status is displayed in **Red**.

You can also pause the pointer over the status to read more information about the status from a tooltip.

- **Name:** Displays the name of the controller
- **Firmware version:** Displays the controller firmware version
- **AP Count:** Displays the number of APs from the controller that transmit data
- **External IP Address:** Displays the external IP address of the controller
- **Internal IP Address:** Displays the internal IP address of the controller
- **Added Time:** Displays the time when the controller was onboarded to the RUCKUS Analytics system
- **Last Update Time:** Displays the time stamp of the controller communication

## Onboarding the controller to RUCKUS Analytics

You have to enable the *analytics* and *cloud* features in the controller and login with your (Ruckus customer) login details to onboard the controller.

1. Login to the SmartZone controller web interface with your Ruckus Support user credentials.

2. Go to **General Settings > Cloud Services**, and enable RUCKUS Analytics.

**NOTE**

The SmartZone controller name is retrieved from the controller at the time of onboarding. However, if the name is changed after onboarding the controller, RUCKUS Analytics will not display the updated controller name.

## Managing Users

You can add registered users, associate them to resource groups, and manage users from the RUCKUS Analytics web interface.

The user must be registered with the system.

1. From the web interface, go to **Admin > User**.

**FIGURE 245** User Management

Email	First Name	Last Name	Role	Resource Group	Account	Invited by	Invitation Status
aaron.haggarty@ruckuswireless.com.usat	Aaron	Haggarty	Report Only	default	Ruckus Wireless, Inc	-	-
aaron.lanting@ruckuswireless.com.usat	Aaron	Lanting	Admin	default	Ruckus Wireless, Inc	-	-
aaron.spitz@ruckuswireless.com.usat	Aaron	Spitz	Admin	default	Ruckus Wireless, Inc	-	-
abdul.hameed@ruckuswireless.com.usat	Abdul	Hameed	Admin	default	Ruckus Wireless, Inc	-	-
abhijit.basu@ruckuswireless.com.usat	Abhijit	Basu	Admin	default	Ruckus Wireless, Inc	-	-
adam.ciernicki@ruckuswireless.com.usat	Adam	Ciernicki	Admin	default	Ruckus Wireless, Inc	-	-
altaa.chou@ruckuswireless.com.usat	Altaa	Chou	Admin	test	Ruckus Wireless, Inc	-	-
aj.caplinger@ruckuswireless.com.usat	AJ	Caplinger	Admin	default	Ruckus Wireless, Inc	-	-
akumarhg@ruckuswireless.com.usat	Arjan	Kumar	Admin	default	Ruckus Wireless, Inc	-	-
albert.chuang@ruckuswireless.com.usat	Albert	Chuang	Admin	default	Ruckus Wireless, Inc	-	-

The **Users** page displays the number of registered users and additional information such as the user email address, first and last names, role, associated resource group, and user account.

If a user onboards the controller, that user can be added as a user to the account. However, the user has restricted administrator permissions. For example, the user can access account details but cannot delete other users from the account.

2. Click **Add Internal User**.

The **Create User** page is displayed where you can select the registered users from **Username** and associate the user to a resource group by selecting a group from the **Resource Group** menu. Users are uniquely mapped to Resource Groups. You can assign one of the following roles to the user from the **Role** menu:

- **Admin:** Provides access to all product functionality
- **Network Admin:** Provides access to all product functionality except administrative operations such as users, resource groups, licenses, support, and onboarded systems.
- **Report Only:** Provides access to manage reports

3. You can also add third-party users by clicking **Invite 3rd-Party User**.

A third-party user is a user who does not belong to your organization. By inviting a third-party user, you are explicitly granting access to someone outside your organization to the RUCKUS Analytics service account. Ensure that you have the necessary authorization to do so. A third-party user or a partner can only access a single resource group as defined by the administrator.

**NOTE**

If the **Admin** role is granted, the third-party user will also be able to invite other users into your account. If this is not desired, you can grant the third-party user a **Network Admin** or **Report Only** role.

The **Invite User** dialog box is displayed where you can search for the user by their email ID. After typing the email ID, click **Find**. Select the Resource Group and Role that you want the third-party user to be associated with and click **Invite**.

**NOTE**

The user must have a valid email ID that is registered with RUCKUS support. Else, the third-party account will be rendered invalid.

Information relevant to the invited user is displayed in the **User** page. The user can accept or reject the invitation; the status of which is also displayed on this page as **Accepted**, **Rejected** or **Pending**. The user must also have a registered RUCKUS Analytics account to accept the invitation. Additionally, only users having their own account with RUCKUS Analytics can accept invitations. Else, they will not be granted permission to access the application. If the user wants to use another account to accept invitations, then the new account has to be added and registered with RUCKUS Analytics before the user can accept invitation from that account.

4. Click **Create**.
5. Partners or third party users who are invited to manage multiple customer accounts can take advantage of single sign-on by clicking on **Accounts** in the profile icon (top right). Partners can conveniently switch account views without having to re-login.

## Managing Resource Groups

You can provide Role-Based Access Control (RBAC) to allow an administrator to manage APs and switches organized into resource groups.

A resource group is made up of your selection of APs and switches available in RUCKUS Analytics. There are many roles associated with resource groups with specific functional privileges. The roles available are Admin, Network Admin and Reporting. A resource group allows the Admin to confine access for a group of users to a restricted set of APs and switches. Therefore, a resource group is equivalent to a tenant.

RUCKUS Analytics contains a Default resource group. This group corresponds to the entire set of Wi-Fi assets. The Default resource group cannot be edited or deleted.

The following table lists the functional privileges of each role.

**NOTE**

Only users with Admin privileges can edit a resource group.

**TABLE 19** Roles and their Privileges

Role	View Reports	UI View Mode	Save Filter	Scheduled Reports	Data Explorer	Admin Control	Resource Group	License Management	Enable RUCKUS Support
Admin	Yes	Advanced	Yes	Yes	Create	Yes	Yes	Yes	Yes
Network Admin	Yes	Advanced	Yes	Yes	Create	No	No	No	No

## Administration

### Managing Resource Groups

**TABLE 19** Roles and their Privileges (continued)

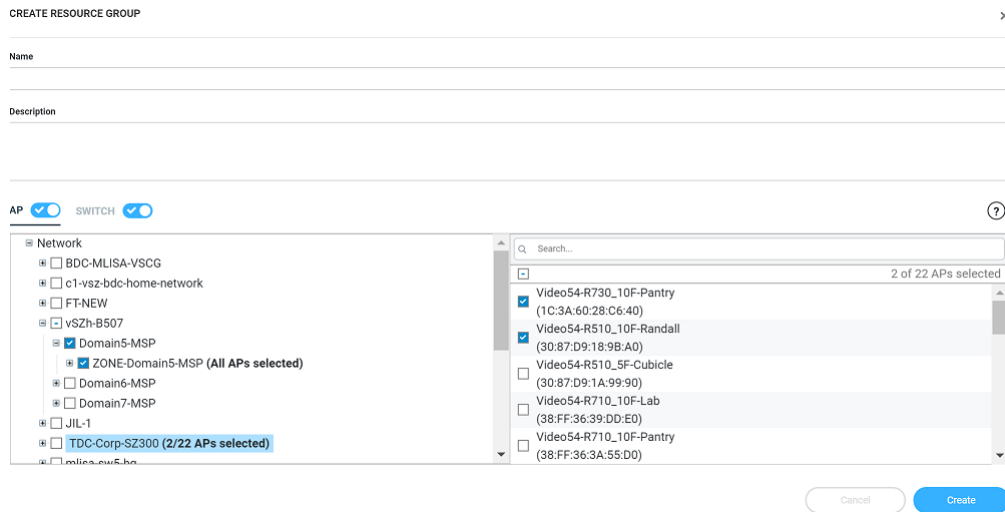
Role	View Reports	UI View Mode	Save Filter	Scheduled Reports	Data Explorer	Admin Control	Resource Group	License Management	Enable RUCKUS Support
Reports	Yes	Report and Data Explorer	Yes	Yes	Create	No	No	No	No

1. To create a resource group of APs and switches, from the web interface, go to **Admin > Resource Groups**. The **Resource Groups** page is displayed.

2. Click **Create Resource Group**.

The **Create Resource Group** page is displayed.

**FIGURE 246** Creating a Resource Group



Configure the following options:

- **Name:** Enter the name of the resource group that you are want to create.
- **Description:** Enter a short description about the group for reference.
- Click the **AP** radio button and **Switch** radio button to view the devices within the network and domains. Choose the devices that you want by selecting the check-boxes, and click **Create**. The resource group with the selected APs and switches is created and displayed in the **Resource Group** page.

**NOTE**

The same set of APs and switches can be part of multiple different resource groups.

You can select or clear all APs and switches by clicking the **AP** radio button and **Switch** radio button. You can also choose to select either an AP or switch to be included in a group. Under the **Network** hierarchy tree, you can select the different domains within the network which in turn display all the APs or switches present in that domain on the right pane. You can search for specific APs or switches by using the device MAC address. It is not mandatory for all APs or switches within a domain to be added to a resource group; you can select specific APs or switches within a domain and add them to the resource group. The number of devices (APs or switches) selected within a domain is displayed on the right pane along with the device name and MAC address, and also displayed within brackets in the **Network** hierarchy tree.

If you want to include all devices within a domain in the resource group, select the domain check-box under the network tree. If you select specific devices within a domain, a hyphen (-) is displayed within the check box to identify that at least one or more devices

## Administration

### Contacting Ruckus Support

within the domain are selected. If all the devices within a domain are selected, the network path to the device is displayed on the right pane.

You can create a resource group at the zone level or at the AP level.

To create a resource group at the AP level, you will not selected all of the APs within a domain and only select specific APs. In addition, if you added new APs to a domain (from the right pane), the new APs will not be automatically added to the resource group. Therefore, creating resource groups at the AP level will not add new APs to the resource group, automatically.

However, if you create a resource group at the zone level, you will select all the APs within a domain by clicking the check box from the left pane. In addition, if you add new APs to the domain, they are automatically included to the resource group. Therefore, creating resource groups at the zone level will also add the new APs to the resource group, automatically.

#### NOTE

A resource group can have up to a maximum of 800 APs. Therefore, RUCKUS recommends that you select devices at the zone-level instead of the APs.

Domains and devices that are no longer part of the network are displayed with their names struck through. These devices or domains can be removed from the resource group. Click the edit (✎) icon to modify the resource group and then save the changes by clicking **Update**.

#### NOTE

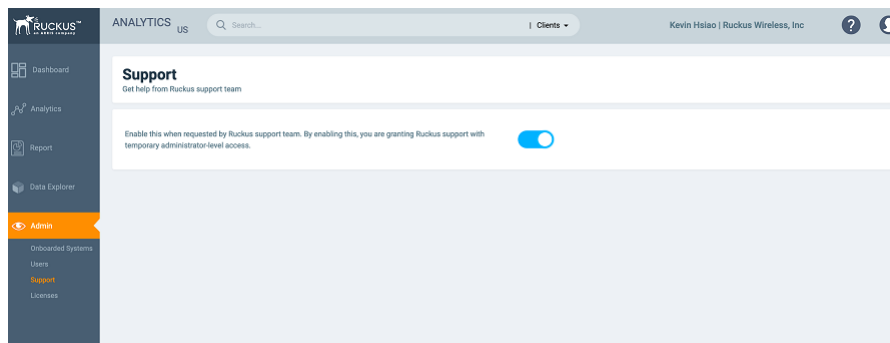
Currently, the entire network cannot be selected and included in a resource group.

## Contacting Ruckus Support

You can request administrator-level access will be provided to Ruckus support personnel to troubleshoot issues for a period of 7 days.

1. From the web interface, go to **Admin > Support**.

**FIGURE 247** Ruckus Support Page



2. Enable to radio button to grant the Ruckus support personnel access to your system to troubleshoot issues.



# Managing Licenses and Assigning APs

You can manage the licenses that you have purchased for Cloud or APs managed by SmartZone controllers.

**NOTE**

Ensure that you have the proper license subscriptions to manage the licenses.

The following table lists the available license subscription packages.

**TABLE 20** License Subscription Packages

License Type	Description
CLD-ANAP-1001	RUCKUS Analytics 1-year subscription for 1 Cloud-or SmartZone-managed AP or ICX switch
CLD-ANAP-3001	RUCKUS Analytics 3-year subscription for 1 Cloud-or SmartZone-managed AP or ICX switch
CLD-ANAP-5001	RUCKUS Analytics 5-year subscription for 1 Cloud-or SmartZone-managed AP or ICX switch
CLR-ANAP-1001	RUCKUS Analytics 1-year subscription for 1 Cloud-or SmartZone-managed AP or ICX switch
CLR-ANAP-3001	RUCKUS Analytics 3-year subscription for 1 Cloud-or SmartZone-managed AP or ICX switch
CLR-ANAP-5001	RUCKUS Analytics 5-year subscription for 1 Cloud-or SmartZone-managed AP or ICX switch
CLD-ANAP-TM60	RUCKUS Analytics 60-day trial subscription for 1 Cloud-or SmartZone-managed AP or ICX switch
CLD-ANAP-TM90	RUCKUS Analytics 90-day trial subscription for 1 Cloud-or SmartZone-managed AP or ICX switch
INT-ANAP-TM90	RUCKUS Analytics 90-day free trial for 100 APs or ICX switches

## Administration

### Managing Licenses and Assigning APs

A notification is sent to the administrator one week before the license expiration is due. A grace period of seven days is available to use the license after the license expiration date. After this grace period, you can only view data populated till the license expiration date and no new data (after license expiration date) will be displayed. You can view old data up to six months after license expiration.

1. From the web interface, go to **Admin > Licenses**.

The **Licenses** page displays the following information:

- **Type:** Displays the type of license package as described in the preceding table
- **Total Count:** Displays the total number of licenses assigned
- **Count Used:** Displays the number of licenses used from the total number assigned
- **Start Date/Time:** Displays the date and time when the license is activated
- **Expiration Date/Time:** Displays the date and time when the license expires or deactivates
- **Days to Expiration:** Displays the number of days available to use the license
- **Description:** Displays a short description about the license type

The **Refresh License** option refreshes this page to display the latest license information.

The **Claim your free 90-day trial** option allows you to use the new built-in 90-day free trial license for 100 APs or ICX switches. Select this option to claim the license immediately. It can only be claimed once. The license is available to all accounts which do not have any paid licenses.

Beneath the **Licenses** page title, **Total Count** displays the sum of all the license allotted, **Licenses Used** displays a sum of all the licenses used from the total number allotted, and **Licenses Left** displays the sum of all the licenses remaining from the total number allotted.

**FIGURE 248** Licenses Page

ID	Type	Total Count	Count Used	Start Date/Time	Expiration Date/Time	Days to Expiration	Description
1	CLD-ANAP-3031	5000	576	Dec 11 2019 05:30	Dec 11 2022 05:30	90+ days	Ruckus Analytics 3 year subscription for 1 Cloud or S2 managed AP
2	CLD-ANAP-1031	5	5	Dec 11 2019 05:30	Dec 11 2020 05:30	90+ days	Ruckus Analytics 1 year subscription for 1 Cloud or S2 managed AP
3	CLD-ANAP-1031	1	1	Mar 19 2020 05:30	Mar 19 2021 05:30	90+ days	Ruckus Analytics 1 year subscription for 1 Cloud or S2 managed AP
4	CLD-ANAP-1031	5000	29	Jan 01 2020 13:30	Jan 01 2021 13:30	90+ days	Ruckus Analytics 1 year subscription for 1 Cloud or S2 managed AP
5	CLD-ANAP-5031	77	8	Jan 14 2020 05:30	Jan 14 2025 05:30	90+ days	Ruckus Analytics 5 year subscription for 1 Cloud or S2 managed AP
6	CLD-ANAP-1031	1	0	Nov 11 2019 05:30	Nov 19 2020 05:30	90+ days	Ruckus Analytics 1 year subscription for 1 Cloud or S2 managed AP
7	CLD-ANAP-5031	77	0	Dec 13 2019 05:30	Dec 13 2024 05:30	90+ days	Ruckus Analytics 5 year subscription for 1 Cloud or S2 managed AP
8	CLD-ANAP-3031	5	0	Nov 11 2019 05:30	Nov 19 2020 05:30	90+ days	Ruckus Analytics 2 year subscription for 1 Cloud or S2 managed AP
9	CLD-ANAP-5031	7	0	Nov 13 2019 05:30	Nov 13 2020 05:30	90+ days	Ruckus Analytics 5 year subscription for 1 Cloud or S2 managed AP
10	CLD-ANAP-5031	1	0	Nov 15 2019 05:30	Nov 15 2020 05:30	90+ days	Ruckus Analytics 5 year subscription for 1 Cloud or S2 managed AP

2. Click the edit icon to assign APs to the license selected.

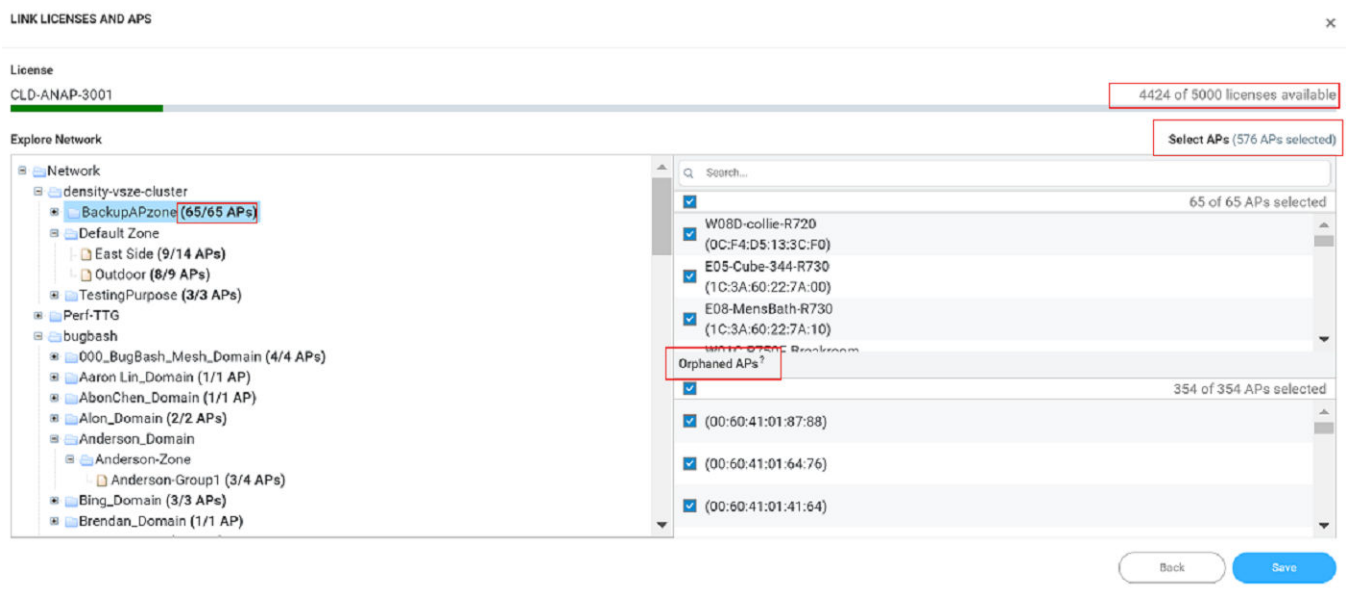
The **Link Licenses and APs** dialog box is displayed.

From the **Network** column on the left, select the system from which you want to assign the APs. The number of APs associated with the system are displayed above the column. After you select the network, the APs within the network are listed in the column on the right. You can manually choose the APs by selecting the check boxes. The number of APs selected from the total APs associated with the network is displayed on top of the column, and also within brackets in the network tree structure. To choose all the APs within the network, select the check box on top of the column.

**NOTE**

If new APs are added to a system, licenses are not automatically assigned to them. You must manually assign licenses to new APs that are added to a system.

**FIGURE 249** Link Licenses and APs Dialog Box



If an AP is already assigned a license, it will be unavailable and you will not be able to select it. A message is also displayed next to the AP stating the license to which it is assigned.

You can use the search bar to find an AP by the AP name or the AP MAC address. You can also see the number of APs matching the search string (name or MAC address) specified in the search bar.

The **Orphaned APs** column displays the APs that are no longer connected to the network. For example, the AP location may have changed or the AP may have lost network connectivity, and therefore there is no account for the AP in the network. You cannot find or search for an orphaned AP within the network. Pause the pointer over the Orphaned APs section for more information about scenarios in which an AP can become orphaned.

The MAC address of the orphaned AP is displayed. The license associated with the orphaned AP is no longer valid, so you can release the license to be assigned to another AP within the network.

A color bar is displayed on top of the columns representing the available licenses for the APs. The bar displays green when the number of licenses consumed is less than 50 percent of the available licenses. It displays yellow when more than 50 percent of the available licenses are consumed, and displays red when more than 75 percent of the available licenses are consumed.

3. Click **Save**.

## Viewing Schedules

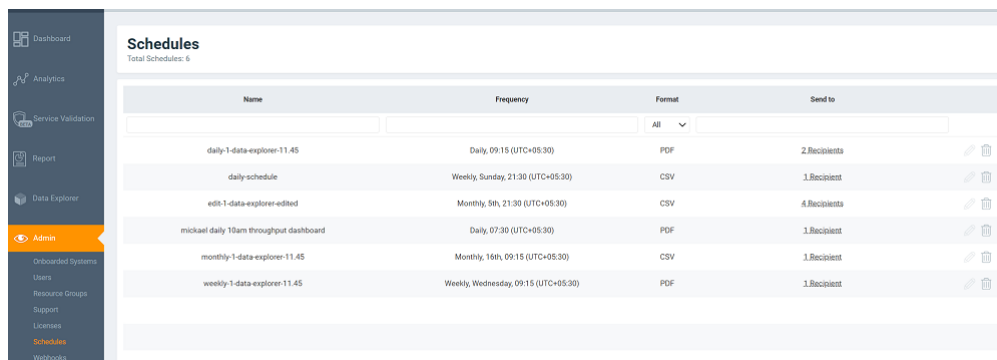
You can view all the schedules created for the reports and custom dashboards in Data Explorer in the **Schedules** page.

The schedule can only be edited by the user who created it, however, schedules can be deleted by any user.

From the web interface, go to **Admin > Schedules Systems**.

The **Schedules** page displays the following information:

**FIGURE 250** Schedules Page



Name	Frequency	Format	Send to
daily-1-data-explorer-11.45	Daily, 09:15 (UTC+05:30)	PDF	2 Recipients
daily-schedule	Weekly, Sunday, 21:30 (UTC+05:30)	CSV	1 Recipient
edit-1-data-explorer-edited	Monthly, 5th, 21:30 (UTC+05:30)	CSV	4 Recipients
mickael daily 10am throughput dashboard	Daily, 07:30 (UTC+05:30)	PDF	1 Recipient
monthly-1-data-explorer-11.45	Monthly, 16th, 09:15 (UTC+05:30)	CSV	1 Recipient
weekly-1-data-explorer-11.45	Weekly, Wednesday, 09:15 (UTC+05:30)	PDF	1 Recipient

- Name: displays the name of the schedule
- Frequency: displays the frequency to which the schedule is set - it can be daily, weekly, monthly, or on-demand
- Format: displays the format in which to save the schedule
- Sent to: displays the email ID of recipients who receive the schedule based on the frequency set

## Creating Webhooks

RUCKUS Analytics allows you to configure Webhook URL addresses to receive real-time notifications when incidents are created or updated in the application - much like e-mail notifications. Webhooks help applications to communicate with each other in real-time and typically use a message or payload to communicate between each other. The message or payload contains real-time information about the incident.

FIGURE 251 Sample Webhook Message with Incident Details

Data structure of incident event from RUCKUS Analytics

```

{ id: string, // Event ID
  type: "incident", // Type of webhook event, will be "incident"
  secret: string, // Webhook secret
  payload: { // incident payload
    status: string, // Incident status, e.g. "new" | "ongoing" |
    "finished"
    id: string, // Unique incident ID
    severity: string, // Incident severity, e.g. "P1" | "P2" | "P3" |
    "P4"
    link: string, // Link to incident,
    title: string, // Title of incident
    category: string, // Category of Incident
    subCategory: string, // Sub-Category of incident
    startTime: string, // Incident start time in ISO 8601 format, e.g.
    "2020-11-01T08:00:00.000Z"
    endTime: string, // Incident end time/last updated time in ISO
    8601 format
    duration: string, // Incident duration, e.g. "4d 10h",
    impactedAreaType: string, // Impacted area type, e.g. "Access Point",
    "Zone" or "Domain"
    impactedAreaName: string, // Impacted area name, e.g. "AP Name
    (AA:AA:AA:AA:AA:AA)"
    impactedAreaHierarchy: string, // Impacted area hierarchy,
    // e.g. "SZ Name (SZ Cluster) > Domain Name
    (Domain) > Zone Name (Zone) > AP Group (AP Group) > AP Name (AA:AA:AA:AA:AA)
    (Access Point)"
    clientCount: number, // Total number of client under current
    hierarchy
    impactedClientCount: number, // Total impacted client under current
    hierarchy
    impactedClientPercentage: string, // Percentage of impacted client over total
    number of client under current hierarchy, e.g. "21.43%"
    rootCauses: string, // Root Causes of current incident
    recommendations: string // Recommendations to resolve current incident
  }
}

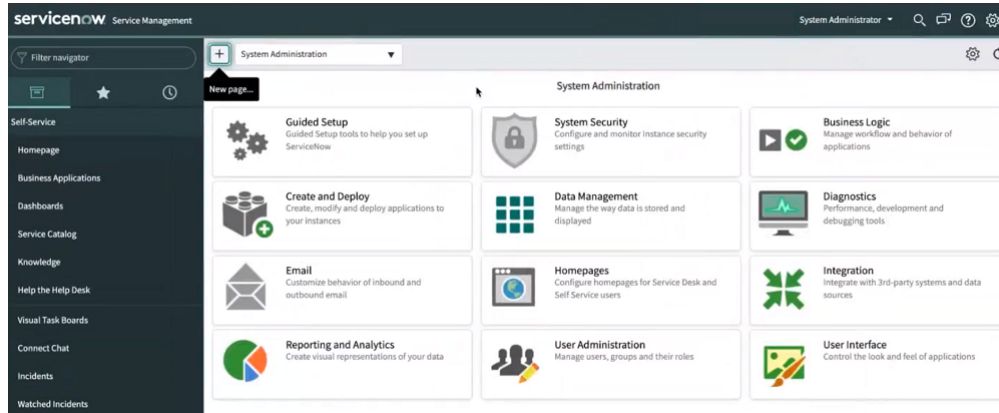
```

For example, RUCKUS Analytics communicates with ticketing applications in ServiceNow and Salesforce (SFDC) via webhooks. Through webhooks, the incidents generated in RUCKUS Analytics appear in the ServiceNow and Salesforce applications, in real-time. Following is a work-flow to configure Webhooks for ServiceNow and SFDC applications.

## Integrating RUCKUS Analytics Incident Webhook with ServiceNow Application

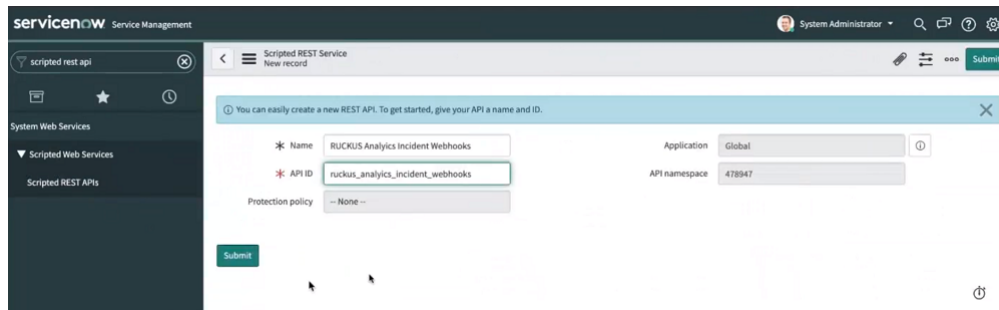
1. Login to the ServiceNow instance

FIGURE 252 Logging into ServiceNow



2. Under **System Web Services**, select **Scripted Rest APIs**

FIGURE 253 Scripted Rest APIs Configuration



A new record to configure the Scripted REST Service is displayed. Configure the following.

- Name: enter the name of the service
  - API ID: enter the API ID
  - Protection Policy: select the appropriate policy from the menu
  - Application: enter the scope of the application. In this example scope is set to Global.
  - API Namespace: a system generated value is populated
3. Click **Submit**.  
The service is created and listed.
  4. Click the service. Under **Resources**, click **New** to provide the endpoint for the service.
  5. Select the **HTTP method** as **POST**

6. In **Script**, enter this code for the endpoint to process the request:**NOTE**

Ensure that the spacing is retained when you copy and paste the code.

```
(function process(/*RESTAPIRequest*/ request, /*RESTAPIResponse*/ response) {
  // Secret shared between Ruckus Analytics (RA) and ServiceNow
  // to ensure the authenticity of data received.
  var secret = "<secret>";

  // Change value to assign incident to specific group,
  // leave as is to not assign to any group
  var assignment_group = "<assignment_group>";

  // Change value to assign incident to specific person,
  // leave as is to not assign to any person
  var assigned_to = "<assigned_to>";

  // Mapping of RA incident severity to
  // ServiceNow incident Impact and Urgency field
  var impactAndUrgencyMap = {
    P1: { impact: 1 /* High */, urgency: 1 /* High */ },
    P2: { impact: 2 /* Medium */, urgency: 1 /* High */ },
    P3: { impact: 2 /* Medium */, urgency: 2 /* Medium */ },
    P4: { impact: 3 /* Low */, urgency: 3 /* Low */ }
  };

  // Mapping of RA incident status to
  // ServiceNow incident State field
  var stateMap = {
    'new': 1 /* New */,
    'ongoing': 1 /* New */,
    'finished': 6 /* Resolved */
  };

  var data = request.body.data;
  // 1. Ensure request uses correct shared secret key
  if (data.secret == secret) {
    var mode; // insert or update
    var event = data.payload;

    var inc = new GlideRecord('incident');

    // 2. Check if incident exists
    inc.addQuery('number', event.id);
    inc.query();

    if (inc.hasNext()) {
      inc.next();
      mode = "update";
    } else {
      inc.initialize();
      mode = "insert";
    }

    // 3. Add/update fields
    inc.number = event.id;
    inc.state = stateMap[event.status];
    inc.impact = impactAndUrgencyMap[event.severity].impact;
    inc.urgency = impactAndUrgencyMap[event.severity].urgency;
    inc.short_description = event.title;
    inc.description = getDescription(event);

    // 4. Assign incident to specific group or person
    if (assigned_to != "<assigned_to>") {
      inc.assigned_to = assigned_to;
    }
    if (assignment_group != "<assignment_group>") {
      inc.assignment_group.setDisplayValue(assignment_group);
    }
  }
}
```

## Administration

### Creating Webhooks

```
// 5. Insert/Update the incident
inc[mode]();

var status = mode + (mode == 'insert' ? 'ed' : 'd');
gs.info('incident ' + event.id + ' ' + status);
} else {
  gs.warn("Invalid secret to run Ruckus Analytics webhook");
}

// Respond to the Webhook
response.setStatus(200);

/**
 * Generate description for incident
 */
function getDescription (event) {
  return [
    'Incident URL: ' + event.link,
    '',
    'Details:',
    '-----',
    'Client Impact Count: ' +
      event.impactedClientCount +
      ' of ' +
      event.clientCount +
      ' (' + event.impactedClientPercentage + '%)',
    'Incident Category: ' + event.category,
    'Incident Sub-Category: ' + event.subCategory,
    'Type: ' + event.impactedAreaType,
    'Scope: ' + event.impactedAreaName,
    'Hierarchy: ' + event.impactedAreaHierarchy,
    'Duration: ' + event.duration,
    'Event Start Time: ' + event.startTime,
    'Event End Time: ' + event.endTime,
    '',
    'ROOT CAUSE ANALYSIS:',
    '-----',
    event.rootCauses,
    '',
    'RECOMMENDED ACTION:',
    '-----',
    event.recommendations
  ].join('\n');
}
})(request, response);
```

7. In **var secret**, set the secret value for data authentication
8. In **var assignment\_group**, assign the RUCKUS Analytics incident to a specific group within ServiceNow
9. In the Security tab, uncheck **Required Authentication**
10. Click **Submit**.
11. From the RUCKUS Analytics web interface, go to **Admin > Webhooks**.

The **Webhooks** page is displayed showing information about the status of the webhook, name, URL and associated resource group.




12. Click **Create Webhooks**.

The **Create Webhook** page is displayed. Configure the following.

- Name: enter the name of the webhook
- Webhook URL: enter the URL by appending the domain URL (for example, <https://dev-123.service-now.com>) and the **Base API Path** from the ServiceNow record (for example, [/api/93874/ruckus\\_analytics\\_incidents](/api/93874/ruckus_analytics_incidents))
- Resource Group: select the resource group that you want to associate with the webhook URL. Any incident created within that resource group will be notified via the webhook URL to the ServiceNow application
- Secret: enter the secret key generated for authentication from the service record
- Enable: If webhook URL is enabled, ServiceNow will receive notifications about the incidents. If webhook URL is enabled, the status appears green and appears grey if it is disabled.
- Event Types: select the event types from severity P1 to P4.

13. Click **Create**. The new webhook is added to the **Webhook** page. This URL will establish communication between ServiceNow and RUCKUS Analytics and reflect incidents generated within resource groups, in real-time.

You can edit the Webhook URL configuration by clicking the  icon. Click **Update** to save edits to the configuration.

## Create a New Salesforce Case for RUCKUS Analytics Incident using Zapier Application

Ensure that you have Zapier account. Also ensure you are logged into Salesforce and RUCKUS Analytics.

Whenever a new incident is triggered in RUCKUS Analytics, a new case is created in Salesforce and updated as an when the incident is updated. Follow these instructions to setup the Zapier application to create a case in Salesforce.

1. Login to the Zapier web interface by clicking <https://zapier.com/shared/0ec3d66a9a6889681fdb83248838d6ca161c90c6>.
2. Click **Try this Zap**.

A page displaying the webhook URL is displayed. This URL is used to integrate Salesforce cases with RUCKUS Analytics incidents, in real-time.

3. From the RUCKUS Analytics web interface, go to **Admin > Webhooks**.

The **Webhooks** page is displayed showing information about the status of the webhook, name, URL and associated resource group.

4. Click **Create Webhooks**.

The **Create Webhook** page is displayed. Configure the following.

- Name: enter the name of the webhook
- Webhook URL: enter the webhook URL from the Zapier interface
- Resource Group: select the resource group that you want to associate with the webhook URL. Any incident created within that resource group will be notified via the webhook URL to the Salesforce application
- Secret: enter secret key for data authentication between RUCKUS Analytics and Zapier
- Enable: If webhook URL is enabled, Salesforce will receive notifications about the incidents. If webhook URL is enabled, the status appears green and appears grey if it is disabled.
- Click **Send a Sample Incident** to continue integration on the Zapier application. When the incident sample has reached Zapier, a success message is relayed on the **Create Webhook** dialog box in the RUCKUS Analytics web interface.

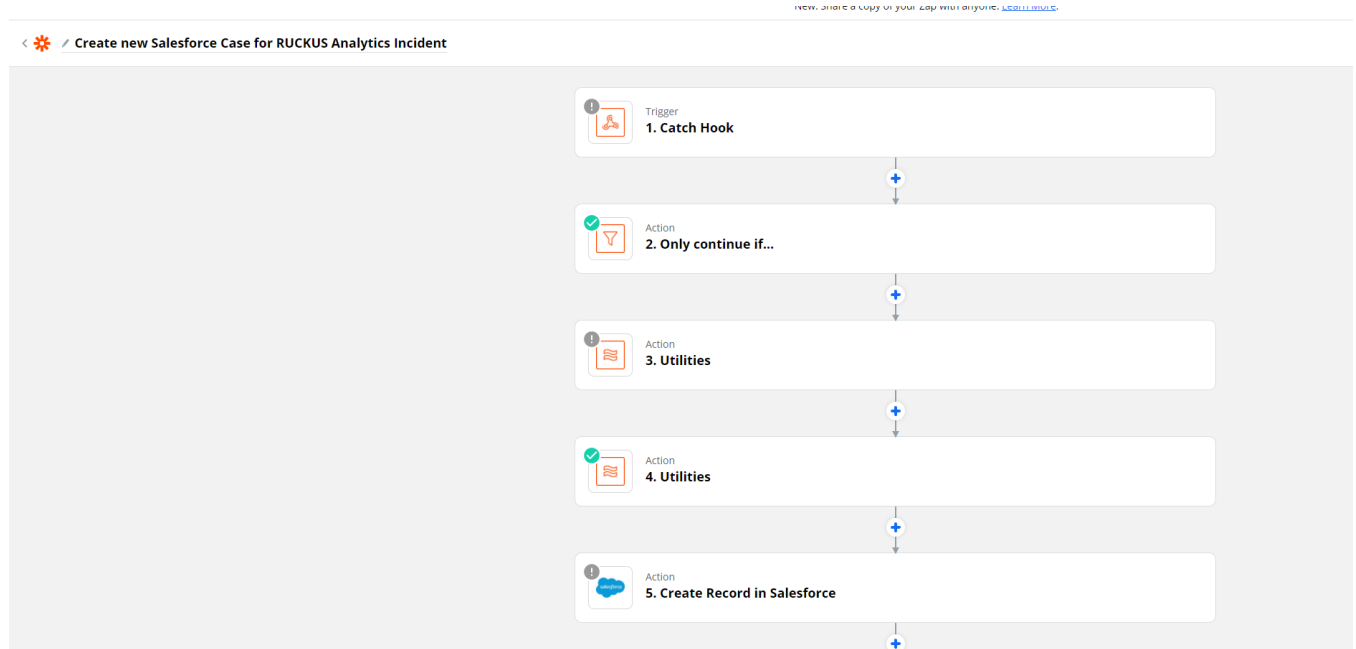
5. Click **Create** to save the configuration.

The new configuration is listed in the **Webhooks** page.

6. In the Zapier web interface, In **Catch Hook**, click **Test Trigger** .

A request message or payload from RUCKUS Analytics is displayed in the Zapier web interface. It contains information about the incident.

**FIGURE 254** Zapier Web Interface



7. Click **Continue**.
8. In **Only Continue if...** , go to **Filter setup & testing** and enter the same secret key that was included in the RUCKUS Analytics web interface for data authentication.
9. Click **Continue**.
10. In **Utilities**, go to **Set up action** and in the lookup table, map the RUCKUS Analytics incidents status with the Case status in Salesforce.
11. Click **Test & Continue**.
12. In **Utilities**, go to **Set up action** and in the lookup table, map the RUCKUS Analytics incidents severity with the priority of cases in Salesforce. For example, P1 incidents will be marked High priority, P2 and P3 as Medium and P3 as Low priority incidents.
13. Click **Test & Continue**.
14. In **Find Record by Query in Salesforce**, go to **Choose account**, and select your Salesforce account or login to your account and authorize Zapier to manage records in Salesforce on your behalf. This step ensures no new cases are recorded when existing cases are present.
15. Click **Continue**.
16. Under **Setup Action**, select Case as the **Salesforce object**.

**NOTE**

Do not change the **WHERE** clause field.

17. Click **Skip Test**.
18. Click **Close**.
19. Click **Continue**
20. Under **Only continue if...** , go to **Filter setup and testing** and click **Continue**

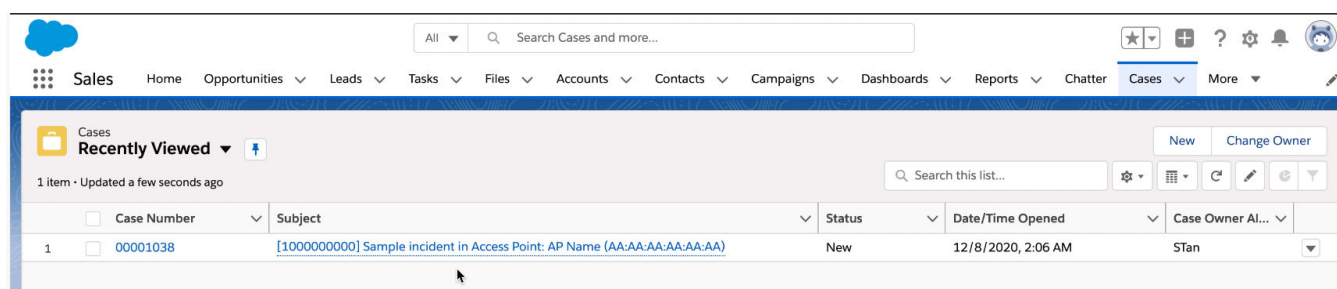
21. In **Create Record in Salesforce**, go to **Choose account** and select your Salesforce account.
22. Under **Setup Action**, select Case as the Salesforce object. Set the other fields as necessary. Modify the fields as required, such as changing the description or assigning the Salesforce case to a particular person or group.

**NOTE**

Do not change the "Subject" as it is used when updating a case.

23. Click **Continue**.  
A Salesforce record is now created.
24. Login to Salesforce Web interface. A new case is created as shown.

**FIGURE 255** New Record in Salesforce



25. In the Zapier web interface, click **Turn on Zap**.  
Whenever an incident occurs in RUCKUS Analytics, the changes will reflect in the Salesforce case as well.  
You can also update existing cases in Salesforce by following the same steps mentioned in the next section.

## Updating an Existing Salesforce Case for RUCKUS Analytics Incident using Zapier Application

1. Setup incident update by clicking <https://zapier.com/shared/6bb3dc515e23d86796c3c70bfcc4121f0d41ae59>
2. Repeat Step 2 to Step 23 from the **Create a New Salesforce Case for RUCKUS Analytics Incident using Zapier Application** section

