USER GUIDE

RUCKUS Analytics User Guide, 2.0

Part Number: 800-72835-001 Rev A
Publication Date: February 2021

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

Preface **9**
- 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

RUCKUS Analytics Overview **13**
- RUCKUS Analytics Introduction 13

Logging In to RUCKUS Analytics **15**

Navigating the RUCKUS Analytics User Interface **17**
- Header Panel 17
- Search Field 18
- Using the Navigation Bar 19

RUCKUS Analytics Dashboard **21**
- Dashboard Overview 21
  - Time Selection Field 22
  - Incident Selection 22
  - Scrolling Data Tile 22
  - Incident Types Tile 23
  - Critical Incidents Tile 23
  - Network History Tile 24
  - Incident Summary Tile 24
  - Interactive Network Hierarchy 25
  - Interactive Network Topology 25
  - Settings 26
  - Accounts 29

Analytics **31**
- Analytics Page 31
  - Network Filter Menu 32
  - Date and Time Filter 32
  - Network Node Details 32
  - Severity Filter 33
  - Incident Timeline 34
  - Incidents List Table 34
  - Incident Details Page 36
  - Network Impact Tile 37
  - Insights Tile 42
  - Incident Info Tile 42
- Health Page 43

Unique Connected Clients Graph 44
Overview Tab 46
Connection Tab 47
Performance Tab 48
Infrastructure Tab 49
Client Troubleshooting Page 50

Service Validation 55
Testing Client Services 55
Service Validation Test Report 58
Overview Tab 58
Details Tab 60

Report 63
Using the Overview Dashboard: Content Panel 63
Wireless Network Report 65
Overview Tile 66
Traffic Distribution Tile 66
Top APs by Traffic Tile 67
Top APs by Client Count Tile 68
Traffic Trend Graphs 69
Traffic Over Time Table 70
Wired Network Report 70
Overview Tile 71
Traffic Distribution by Switch Model and Port Speed Chart 71
Top Switches by Traffic Tile 72
Top Switches by PoE Usage Tile 73
Top Switches by Errors Tile 74
Traffic Trend Graph 75
Error Trend Graph 75
Inventory - APs Report 75
Overview Tile 76
Top APs by Offline Duration Tile 77
AP Count Trend Graph 78
AP Status Trends Tile 78
Top AP Models 79
Top AP Software Versions Tile 80
Top 10 AP Reboot Reasons Tile 81
Top APs by Reboot Count Tile 81
Top 10 AP Alarm Types Tile 82
APs Configured in Multiple Systems Tile 83
AP Details for Online/Offline Status Table 83
AP Details for Other Statuses Table 84
Inventory - Controllers Report 84
Overview Tile 85
Resource Utilization Table 85
License Utilization Table 86
KRACK Assessment Table 86
Inventory - Switches Report 87
Overview Tile 88
Switch Count Trend Graph 88

Top Switch Software Versions Tile 89
Top Switch Models Tile 90
Port Status Trends Tile 91
WLAN Report 91
Overview Tile 92
SSID Changes Over Time Tile 93
Top SSIDs by Traffic Table 93
Top SSIDs by Client Count Tile 94
Active SSIDs Trend Graphs 95
Clients Report 96
Overview Tile 97
Top 10 Unique Clients by Traffic Chart 97
Clients Details 98
Unique Clients Trend Over Time Graphs 98
Top 10 OS by Client Count Tile 99
Top 10 Manufacturers by Client Count Tile 99
Top 10 Authentication Methods by Client Count Tile 100
Client Health Dashboard 100
Client Health Report 100
Applications Report 104
Overview Tile 104
Top Applications by Traffic 105
Top Applications by Client Count Tile 105
Airtime Utilization Report 106
Overview Tile 107
Top 10 APs by Airtime Utilization Chart 107
Top APs by Airtime Utilization for 2.4 GHz Table 108
Top APs by Airtime Utilization for 5 GHz Table 108
Airtime Utilization Trend Graph 109
Airtime Utilization Over Time Table 110
AP Details Report 110
Summary Tile 111
Performance Tile 111
Details Tile 112
Stats Tile 112
Uptime History Graph 113
Traffic Trend Graphs 113
Unique Clients Trend Over Time Graphs 114
Top 10 Clients by Traffic Volume Tile 115
Top 10 Applications by Traffic Volume Tile 115
Top SSIDs by Traffic Table 116
Sessions Table 116
RSS Trend Graph 116
SNR Trend Graph 117
Airtime Utilization Trend Graphs 117
Clients Details Table 118
Alarms Table 119
Events Table 119
Anomalies Graph 120
Client Details Report 120

Summary Tile ... 120
Stats Tile ... 121
Client Details Stats ... 121
Traffic Trend Tile ... 122
RSS Trend Tile ... 122
SNR Trend Tile ... 123
Sessions tile ... 123
Switch Details Report Dashboard ... 124
Switch Details Report ... 124
Comparison Reports Dashboard ... 128
Compare Filters ... 128
PCI Profiles ... 131
Creating a PCI Profile ... 133
Opening and Downloading a PCI Profile ... 135
Editing or Deleting a PCI Profile ... 136

Data Explorer ... 137
Data Explorer and Data Cubes ... 137
Data Exploration ... 137
Applications ... 138
Network ... 139
Airtime Utilization ... 140
Clients ... 140
Sessions ... 141
Switch Inventory ... 142
Events ... 142
Impacted Clients ... 142
AP Inventory ... 143
AP Metrics ... 143
AP Connection Failures ... 144
Client Connection Failures ... 144
Client Connection Statistics ... 145
Client TTC ... 145
AP Alarms ... 146
Controller Inventory ... 146
Controller Metrics ... 147
Rogue APs ... 147
Switch Network ... 148
Wi-Fi Calling ... 148
Data Cube Filters ... 149
Dimensions Filter ... 150
Measures Filter ... 156
Filter ... 160
Explore Filter ... 162
View Outputs Filter ... 164
Add to Dashboard Icon ... 164
Share Link Icon ... 165
Options Icon ... 165
Pinboard Pane ... 166
Comparisons ... 166
Creating a Data Comparison ... 167

Removing the Compare Feature 170
Creating a Data Explorer Dashboard 172
Actions You Can Perform on an Existing Dashboard 177
Opening a Dashboard 177
Editing a Dashboard 177

Administration 181
Viewing Onboarded Systems 181
Onboarding the controller to RUCKUS Analytics 181
Managing Users 182
Managing Resource Groups 183
Contacting Ruckus Support 186
Managing Licenses and Assigning APs 187
Creating Webhooks 190
Integrating RUCKUS Analytics Incident Webhook with ServiceNow Application 191
Create a New Salesforce Case for RUCKUS Analytics Incident using Zapier Application 194
Updating an Existing Salesforce Case for RUCKUS Analytics Incident using Zapier Application 196

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	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* 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
bold text	Identifies command names, keywords, and command options.

Convention	Description
italic text	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, *member*[*member*...].
\	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.

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
- 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.

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

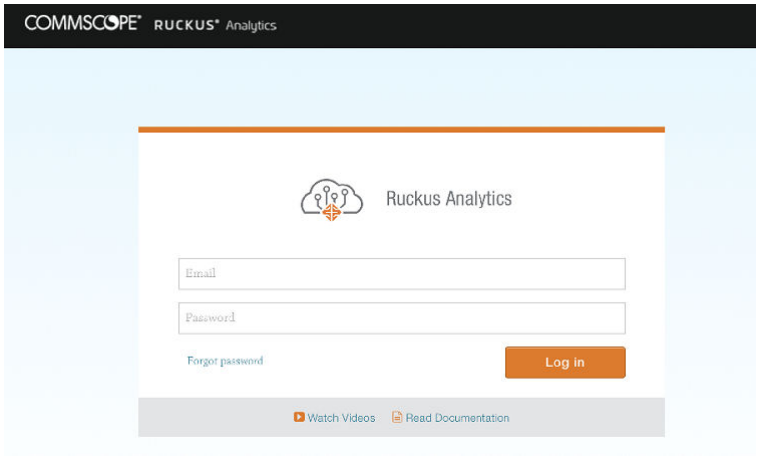
Before logging in to RUCKUS Analytics, ensure that you have configured the Northbound Data Streaming to enable data transfer from the controller, and configure the controller to enable historical connection failures and client events.

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



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

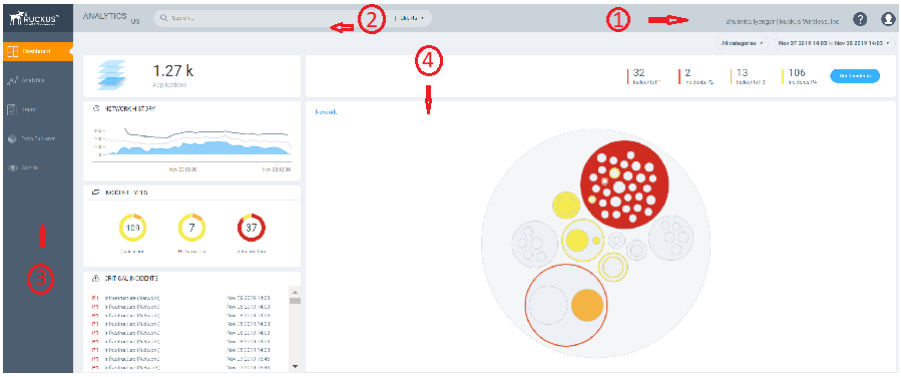


TABLE 2 Identifying RUCKUS Analytics Web Interface Components

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 is 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 **Client Details Report** shows information about the total traffic received and transmitted, and the total number of clients over the selected time period.
		The **Client troubleshooting** page provides a holistic summary of the client connectivity, events, and health.
Access Points		The **AP Details Report** focuses on the usage and health details.
		The **AP Analytics** page shows incidents and health-related data for the AP.
Network Hierarchy		The **APs and Controllers** page provides a general overview of the APs on the network.
		The **Network Analytics** 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 21.
- Analytics: Allows exploration and drill-down on incidents, client impact areas, and network health requirements. For more information, refer to Analytics Page on page 31.
- Report: Provides pre-built reports and charts to understand network usage and inventory. For more information, refer to Report on page 63.
- Data Explorer: Explores the database with a customizable UI-driven tool to answer core questions. For more information, refer to Data Explorer on page 137.
- 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 Service Validation on page 55

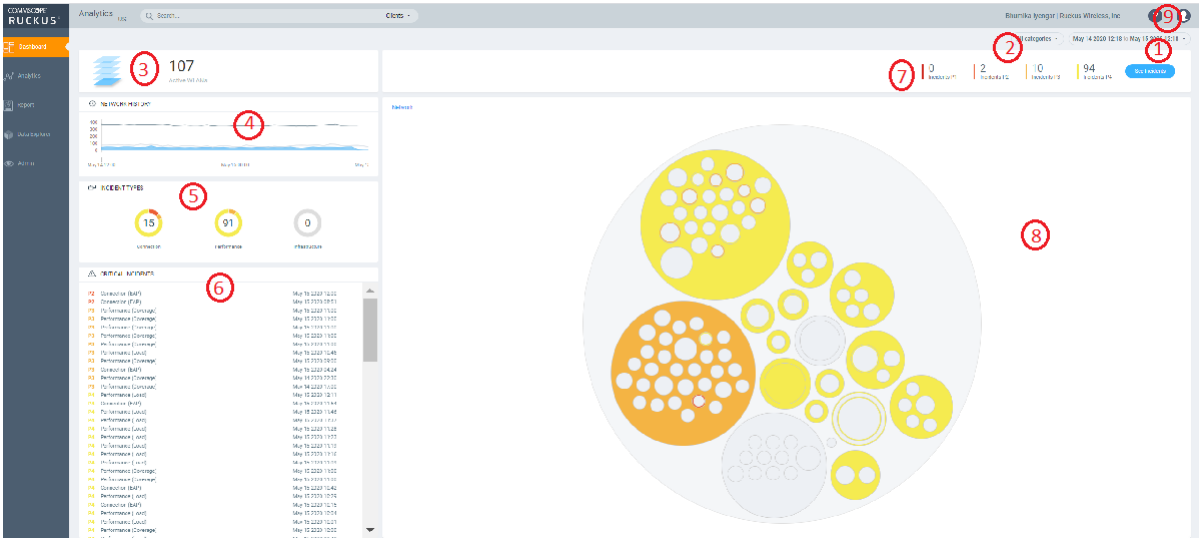
RUCKUS Analytics Dashboard

- Dashboard Overview..... 21

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 4 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

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

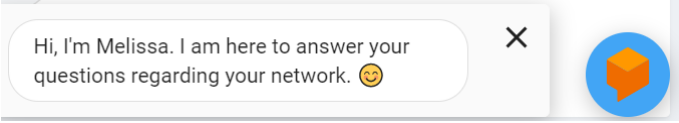
helpful for IT administrators as it reduces the effort to manually navigate through the user interface to analyze information about the network. Based on the questions asked, Melissa interprets user intent and provides responses, thereby providing a logical flow to the conversation and enhancing user experience; much like talking to an administrator for support. 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.

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

FIGURE 4 Melissa AI Assistant



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

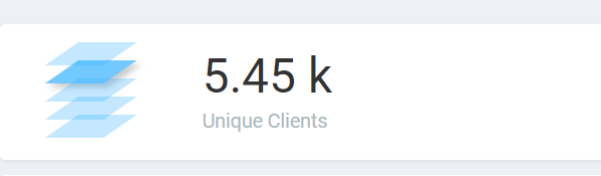
The dashboard data is displayed based on the type of incident category selected. You can choose to view incidents based on **Connections**, **Performance**, and **Infrastructure**. You can select one or more of these options at a time. Select the incident category and click **Apply** to view the relevant 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 5 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.

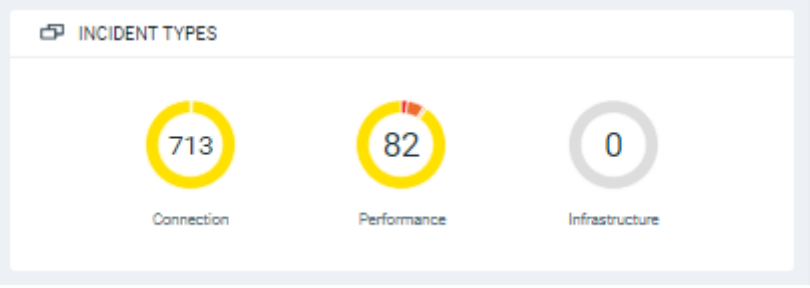
TABLE 5 Layers of Scrolling Data Tile

Tile Data	Description	Link Destination
AP Count	Shows the number of unique APs supported by, and reporting data into, the system.	The **AP Inventory** report focuses on AP details and inventory.
Unique Clients	Shows the number of unique clients that have connected in the displayed time window.	The **Client** 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 **Network** report focuses on network and traffic usage.
Applications	Shows the total number of detected applications in the displayed time window.	The **Application** 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 **WLANs** 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 6 Incident Types Tile

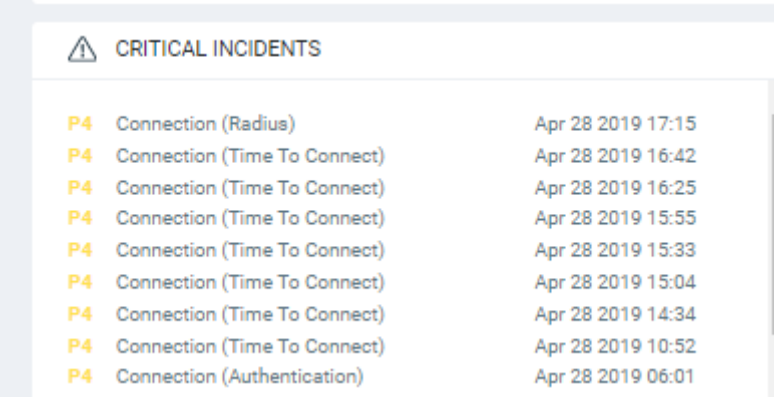


Critical Incidents Tile

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 7 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).

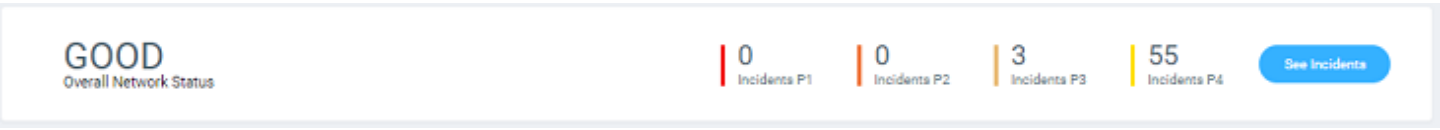
The client count value in the chart includes all unique clients that attempted to connect to the network, including both failed and successful connections. The data depicts a large number of clients that may be impacted by incidents, even if a large number were not able to connect.

FIGURE 8 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 9 Incident Summary Tile



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

TABLE 6 Severity Levels of an Incident

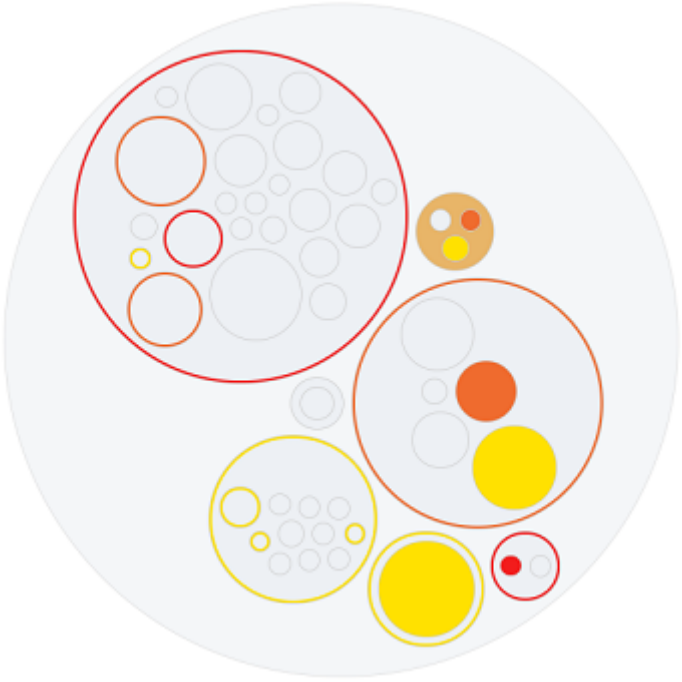
Incident	Priority	Color
P1	Critical	Red
P2	High	Dark Orange
P3	Medium	Orange
P4	Low	Yellow

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.

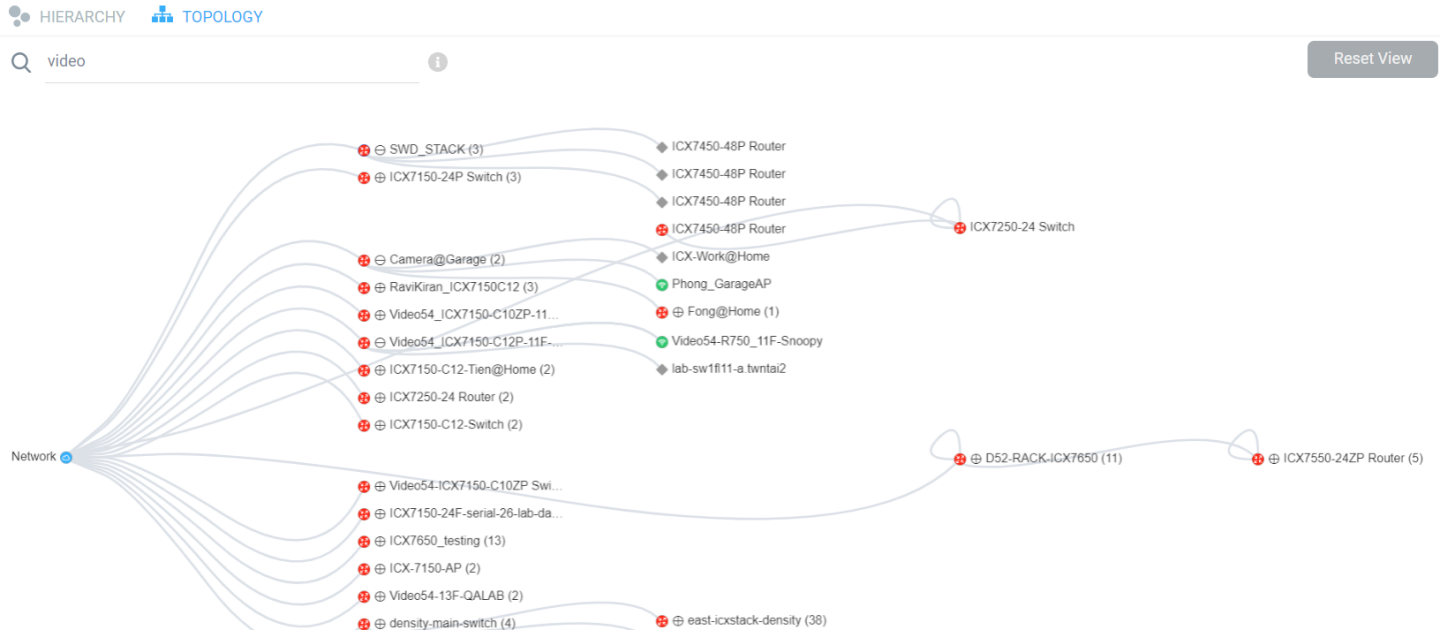
FIGURE 10 Circle Packing Example



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 11 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.

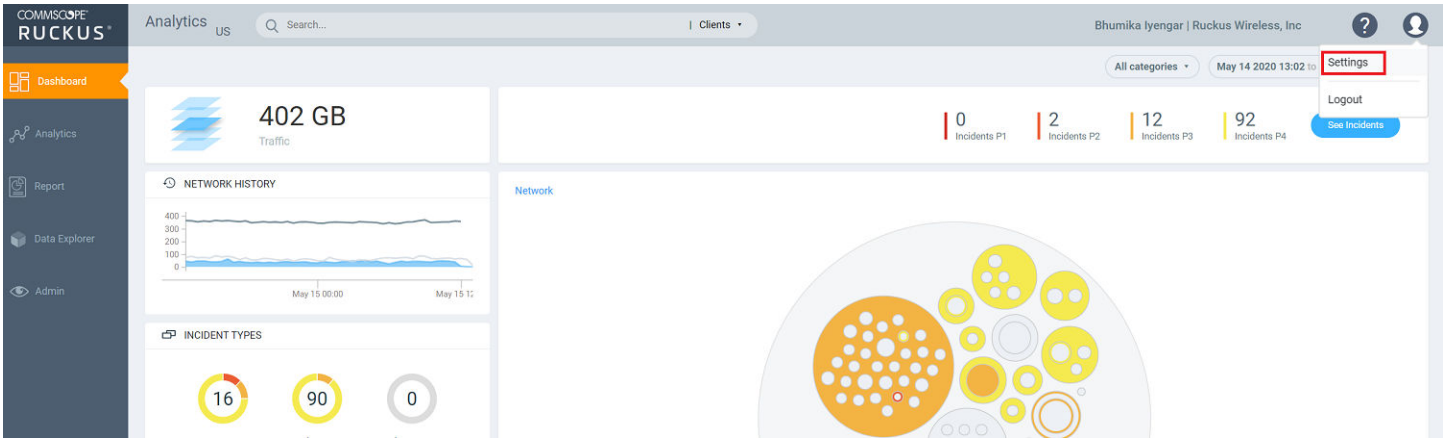
You can zoom-in or zoom-out the **Topology** page and also click on the page to move it.

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

Settings

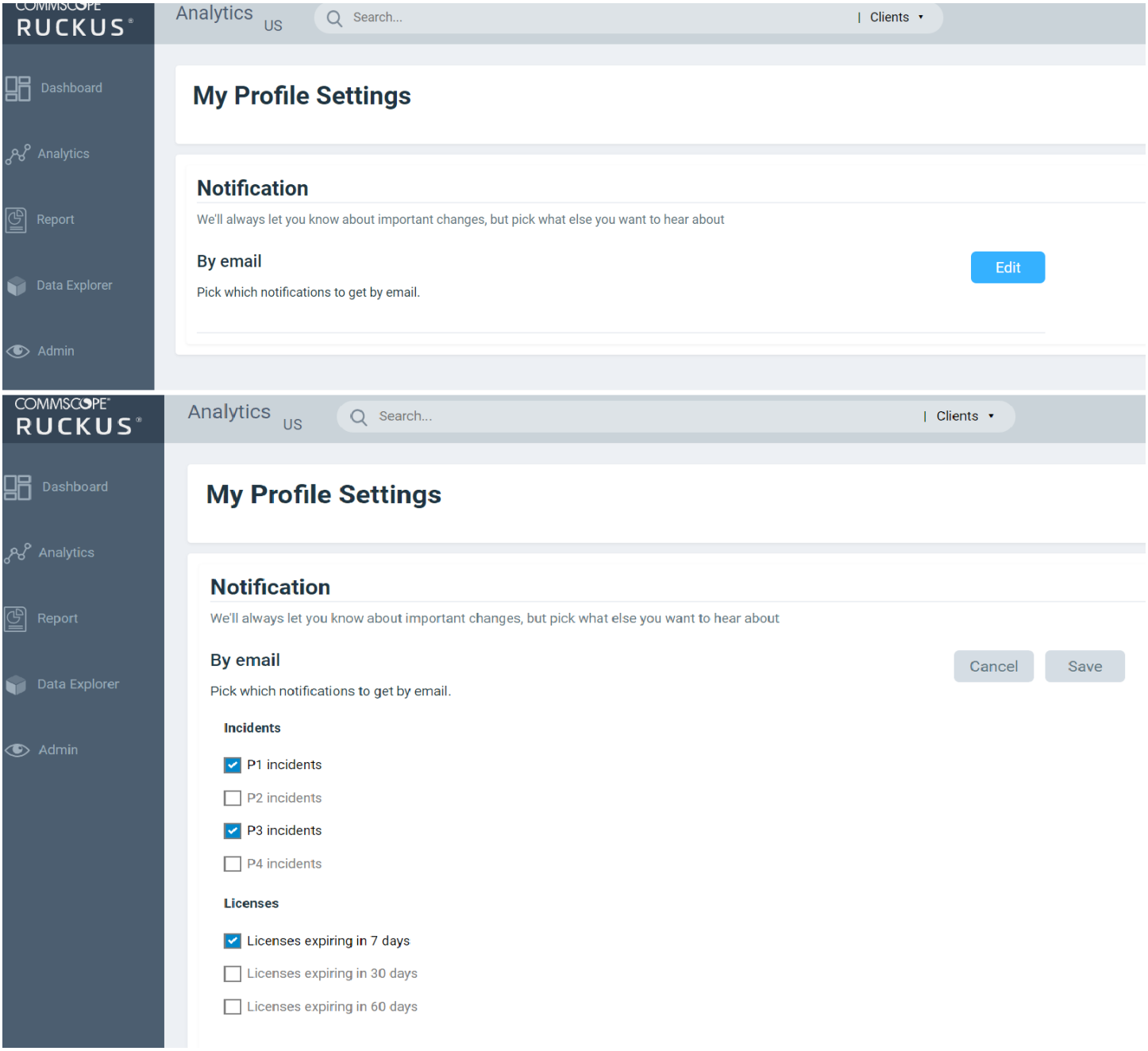
You can modify the user profile from the **My Profile Settings** page and enable the option to receive notification email alerts for incidents of varying severity ranging from P1 to P4.

FIGURE 12 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 13 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 31.

- 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 14 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:

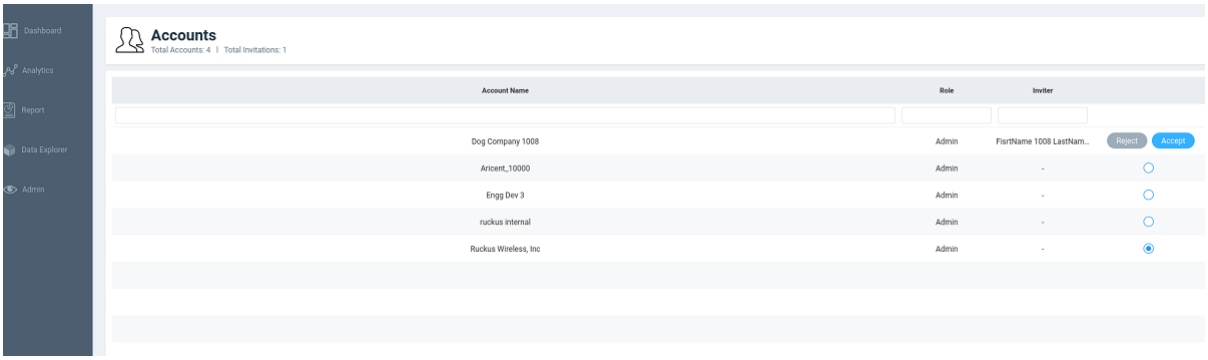
- Client Impact (Approximately): -
- Category: Infrastructure
- Sub Category: Network
- Network Path: Alphanet-BDC (system)
- Event Start Time: Mar 11, 2020, 6:22:30 AM

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 15 Accounts Page



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.

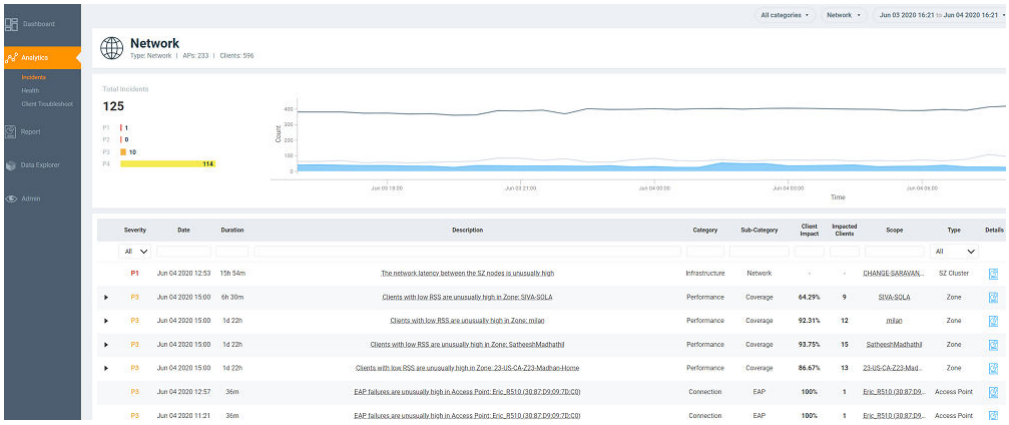
Analytics

- Analytics Page.....31
- Health Page..... 43
- Client Troubleshooting Page.....50

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 16 Analytics Page



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

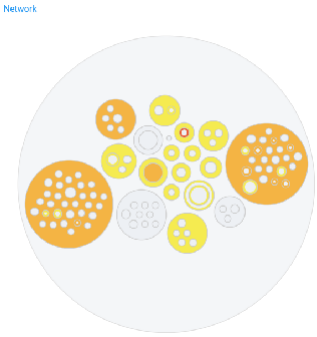
The Analytics page contains a number of components:

- 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.

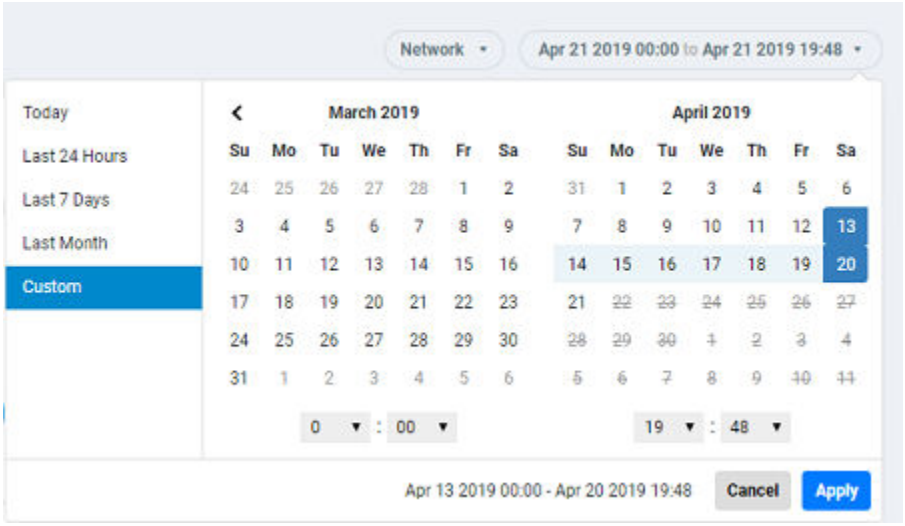
FIGURE 17 Nodes on the Network



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 18 Custom Mode



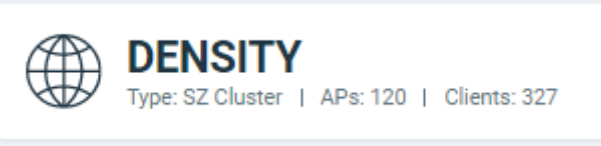
Click **Apply** to save the specified date and time filters and update the Analytics page.

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 19 Density Network Node



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

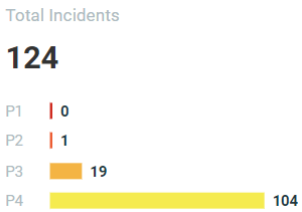
TABLE 7 Network Nodes and Attributes

Node	Attributes
Cluster	• Type: SZ Cluster • Firmware • Cluster: Cluster Name • SZ Type: SZ104, SZ124, viz.-E, viz.-H, SZ300
Domain	• Type: Domain • Zone Count • AP Count • Client Count • Cluster
Zone	• Type: Zone • Firmware: Zone firmware • AP Count • Client Count • Cluster
AP Group	• Type: AP Group • Zone Firmware • AP Count • Client Count
AP	• Type Access point • AP Firmware • AP Name • Model • MAC Address • IP Address • Client
Client	• Type: Client • MAC Address • Last IP Address • OS Type • Hostname • Username

Severity Filter

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

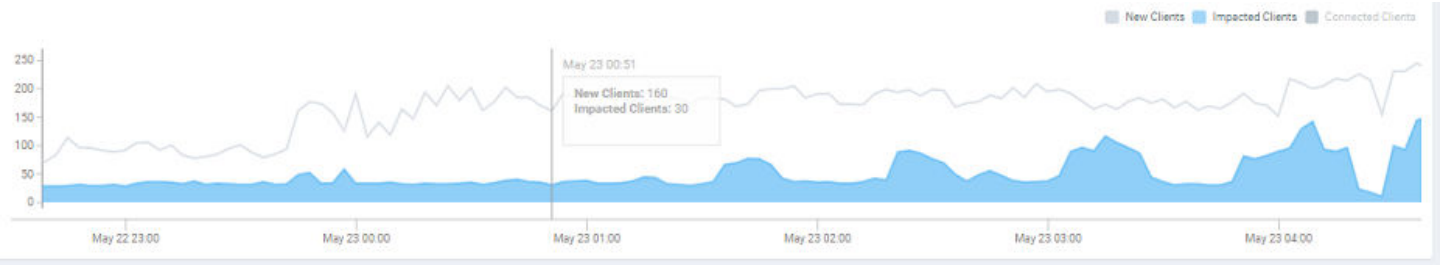
FIGURE 20 Severity Filter



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 21 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.

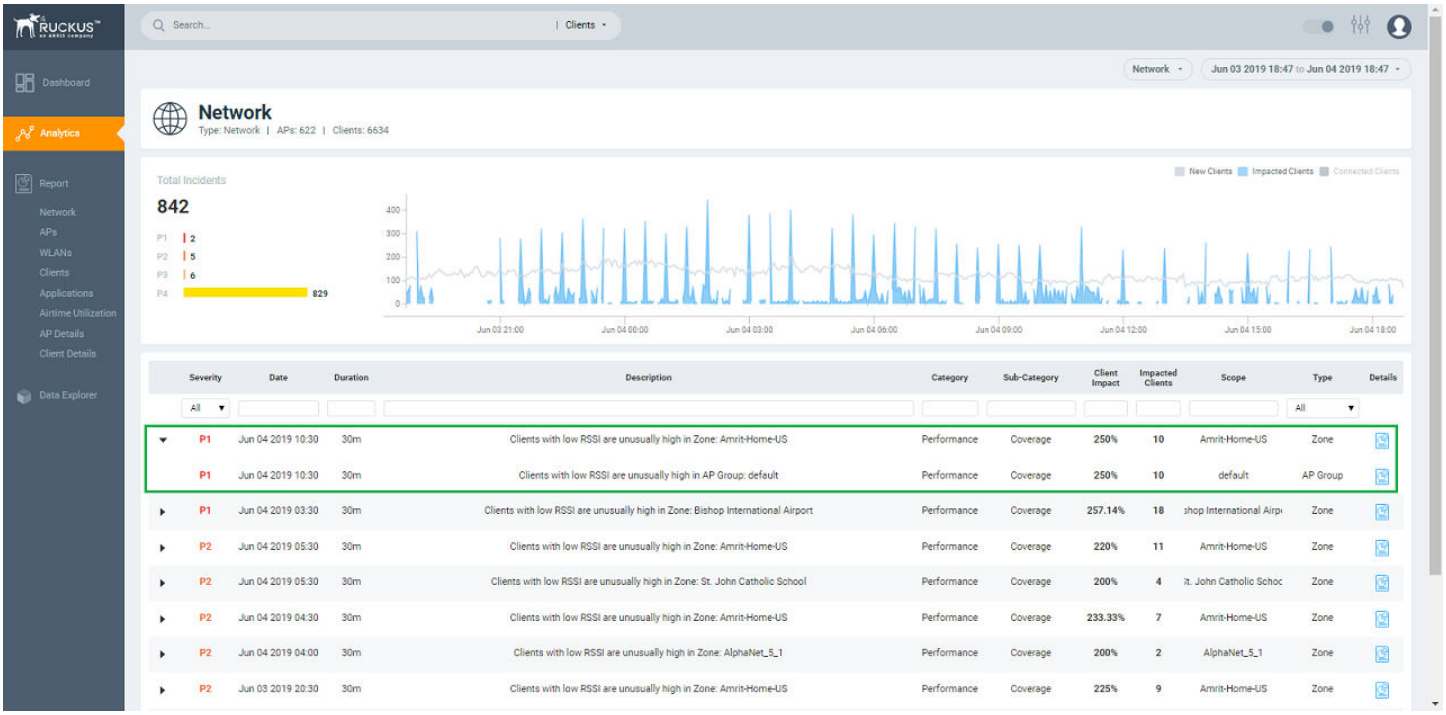
NOTE

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 22 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 8 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.

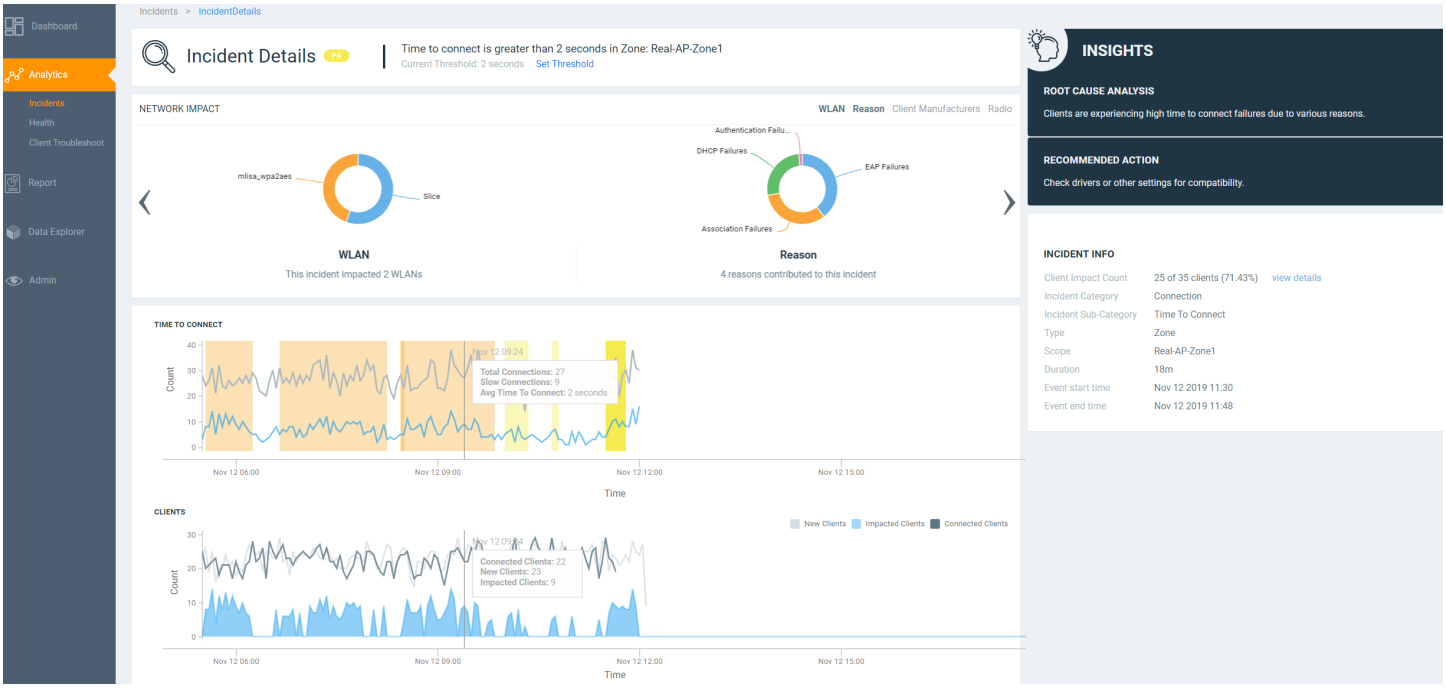
TABLE 8 Attributes of the Incidents List Table (continued)

Attribute	Description
Sub-Category	Connection incidents consist of the following categories: • Association • User Authentication • DHCP • EAP • RADIUS • Time to Connect Performance incidents consist of the following categories: • RSSI • Memory • Coverage Infrastructure incidents consist of the following categories: • VLAN Mismatch • Service Availability
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 **Incident details** 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 23 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 tot he incident related to the metric.

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 24 Network Impact Tile

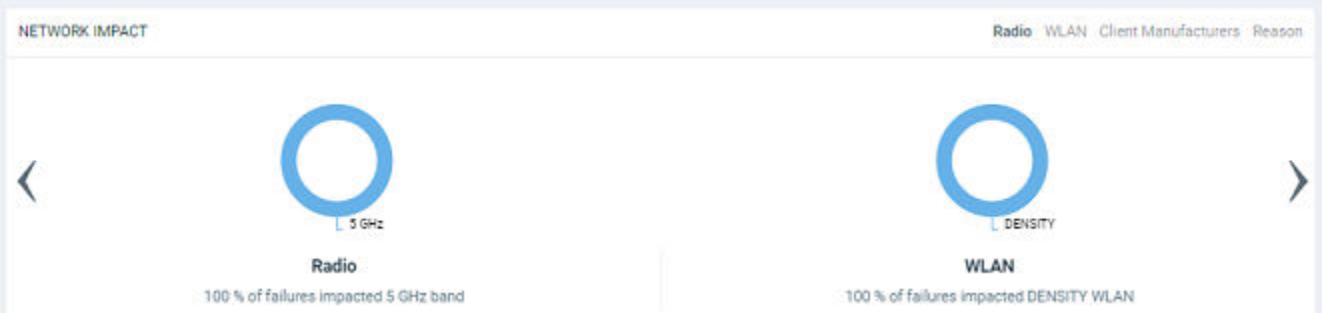


TABLE 9 Attributes of Network Impact Table

Incident Type	Donut Charts	Chart Elements
User Authentication	• Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios. • WLAN: The different WLANs to which the impacted clients are connected. • Client Manufactures: The distribution of device manufacturers. • Reason: The breakdown of various failure reasons experienced by the impacted clients. .	• 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. • Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients. • 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.
EAP	• Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios. • WLAN: The different WLANs to which the impacted clients are connected. • Client Manufactures: The distribution of device manufacturers. • Reason: The breakdown of various failure reasons experienced by the impacted clients.	• 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. • Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients. • 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.

TABLE 9 Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
Association	• Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios. • WLAN: The different WLANs to which the impacted clients are connected. • Client Manufactures: The distribution of device manufacturers. • Reason: The breakdown of various failure reasons experienced by the impacted clients.	• 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. • Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients. • 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.
DHCP	• Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios. • WLAN: The different WLANs to which the impacted clients are connected. • Clients Manufactures: The distribution of device manufacturers. • Reason: The breakdown of various failure reasons experienced by the impacted clients.	• 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. • Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients. • 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.
RADIUS	• Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios. • WLAN: The different WLANs to which the impacted clients are connected. • Client Manufactures: The distribution of device manufacturers. • Reason: The breakdown of various failure reasons experienced by the impacted clients.	• 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. • Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients. • 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.

TABLE 9 Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
Time to Connect	• Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios. • WLAN: The different WLANs to which the impacted clients are connected. • Client Manufactures: The distribution of device manufacturers. • Reason: The breakdown of various failure reasons experienced by the impacted clients.	• 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. • Clients: Three types of time series data: a line for new clients, a line for connected clients, and an area chart for impacted clients. • 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.
RSSI	• Radio: The distribution of impacted clients who connected to 5 GHz and 2.4 GHz radios • WLAN: The different WLANs to which the impacted clients are connected. • Client Manufactures: The distribution of device manufacturers. • Reason: The breakdown of various failure reasons experienced by the impacted clients.	• 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. • RSSI Distribution: The RSSI distribution over a period of time.
Network Latency		• 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. • Controller-1: CPU, memory and input-output usage of the controller node over time is displayed. • Controller-2: CPU, memory and input-output usage of the other controller node over time is displayed.
Reboot	• AP Model: distribution of impacted AP models. • AP Firmware: distribution of impacted AP versions. • Reason by AP: distribution of reasons for failure that caused the AP reboot. • Reason by Event: distribution of reasons for failure that caused the AP reboot and triggered related events.	• Reboot by System: a time series chart that displays the number reboot events. • Connected Clients: a time series chart that displays the number of clients connected at that point in time. • Rebooted APs: a time series chart that displays the number of APs that were rebooted at a point in time.

TABLE 9 Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
SmartZone CPU overload insight	• SZ Applications: distribution of CPU usage by individual SmartZone applications. • SZ Applications Group: distribution of CPU usage by individual SmartZone application groups.	• Normalized CPU Usage: a time series chart that displays the CPU usage in percentage. • 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. • 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.
High AP-controller connection failures	• AP Model: displays the percentage of failure that impacted various AP models • AP Firmware: displays the number of failures that impacted various AP firmware versions • Event Type: displays the percentage of failures that were caused by various events • Reason: lists the reasons that caused the incident	• AP-Controller Disconnections: a time series chart that displays the number of disconnections between the AP and controller over time. • 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.
Channel Distribution		• AP Distribution by Channel: heatmap that displays the AP count over time, across channels. • Rogue Distribution by Channel: a time series chart that displays the number of rogue APs across channels.
VLAN Mismatch	• Impacted Switch: displays the number of switches impacted by VLAN mismatch • Impacted VLANs: displays the number of VLANs that are missing	Incident identifies incorrect VLAN configurations between switches and wired devices due to which data transmission could be impaired. The **Impacted Switches** table displays detailed information about the switch name, MAC address, mismatched VLANs, mismatched ports, and mismatched device information where the VLAN mismatch occurred. Mismatched VLAN numbers are highlighted red.
Memory Utilization		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. The **Detected Time** identifies when the memory leak happened and based on the threshold set, a **Projected Time** 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 **Memory Used** or **Threshold** graphs.

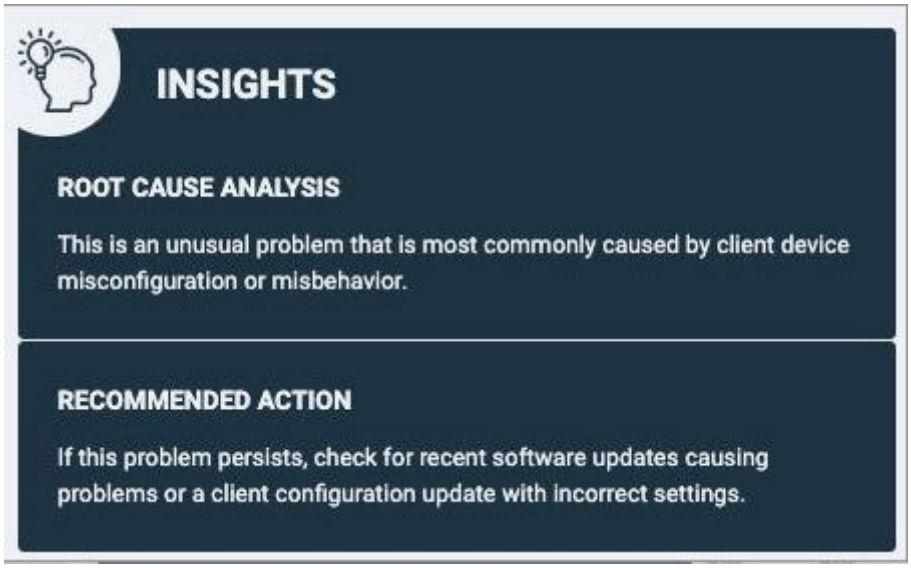
TABLE 9 Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
PoE Power	• Impacted Switch: displays the number of switches impacted by the denial of PoE power • Impacted PoE port: displays the number of PoE ports that are impacted by the denial of PoE power.	The **Impacted Switches** table displays detailed information about the switch (name, MAC address, port) for which PoE power was denied.

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 25 Insights Tile



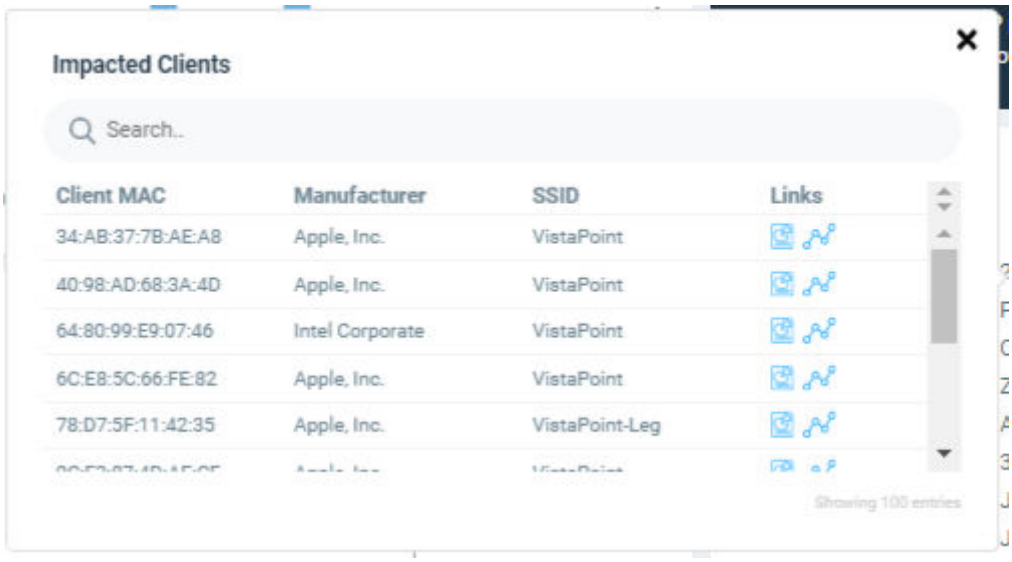
Incident Info Tile

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 26 Incident Info Tile

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 27 Clients page



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 182 and Managing Resource Groups on page 183.

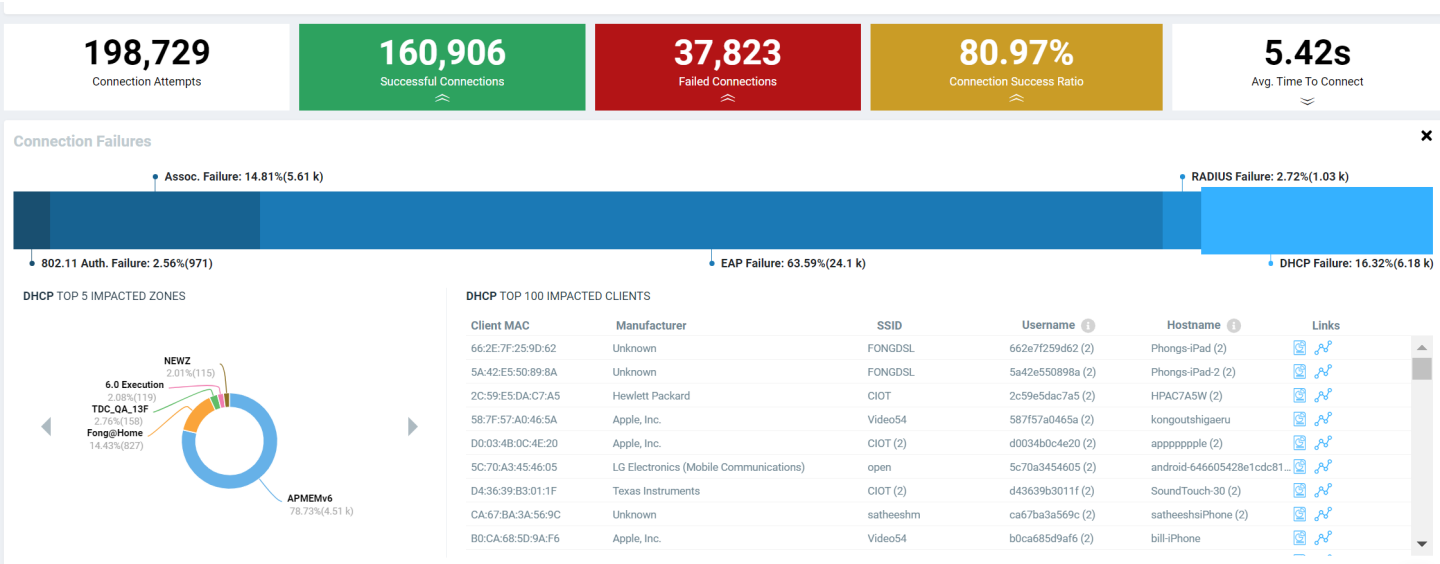
FIGURE 28 Health Page

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.

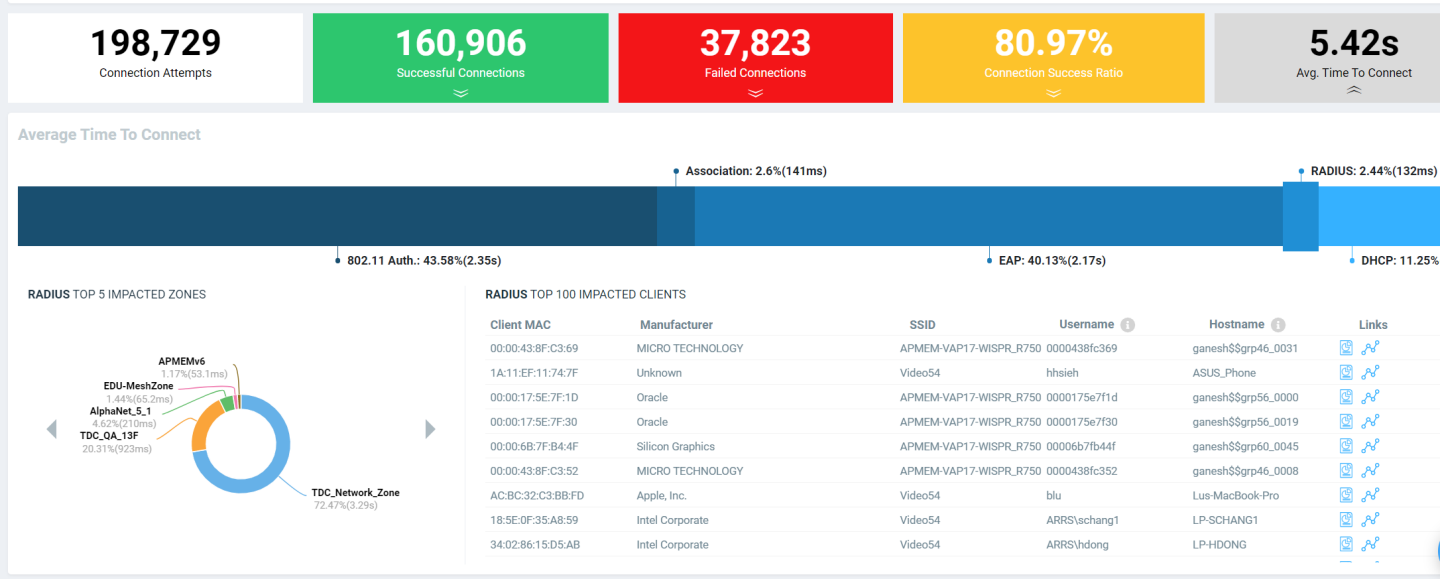
You can also select the drop-down arrows on the coloured bars - Successful Connections, Failed Connections and Connection Success Ratio to display the **Connection Failures** tile. It displays probable reasons for the client to disconnect from the network such as RADIUS failure, EAP failure, DHCP failure 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 29 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 30 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 and AP 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 Service Uptime: Measures the percentage of time the radios of an AP are fully available for client service.

TABLE 10 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

TABLE 10 KPIs Snapshot: Overview Tab (continued)

KPI	Pill-Shaped Box	Time Series Graph	Histogram
AP Capacity	Displays the percentage of APs with the per-bin capacity that met the SLA (for the time range selected)	Displays the percentage of APs with the per-bin capacity 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 with the per-bin capacity that met the SLA for the entire time range
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 11 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
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 **Unique Connected Clients**	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 **Unique Connected Clients**, 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 **Unique Connected Clients**	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 **Unique Connected Clients**, 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 **Unique Connected Clients**	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 **Unique Connected Clients**, 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 **Unique Connected Clients**	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 **Unique Connected Clients**, 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 12 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.

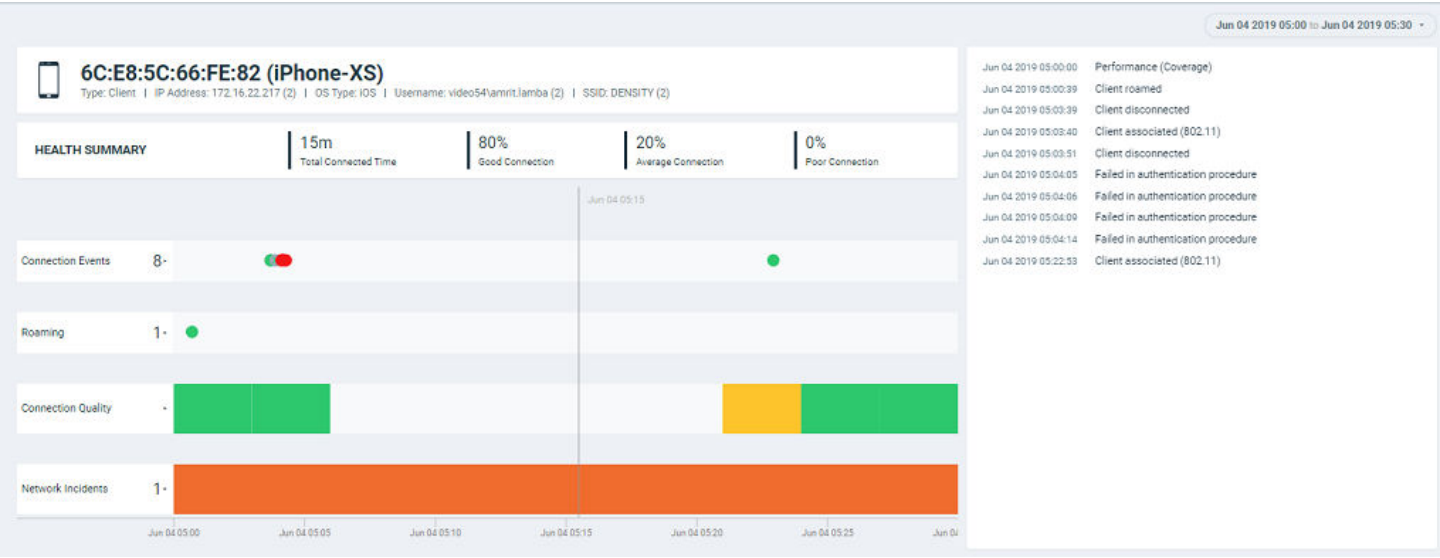
TABLE 13 KPI Snapshot: Infrastructure Tab

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 latency that met the SLA over time	Displays a bar chart of AP service uptime where the X axis displays 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 or 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 percentage of PoE utilization and the Y axis displays the number of switches that meet the goal for the selected time.

Client Troubleshooting Page

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

FIGURE 31 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::

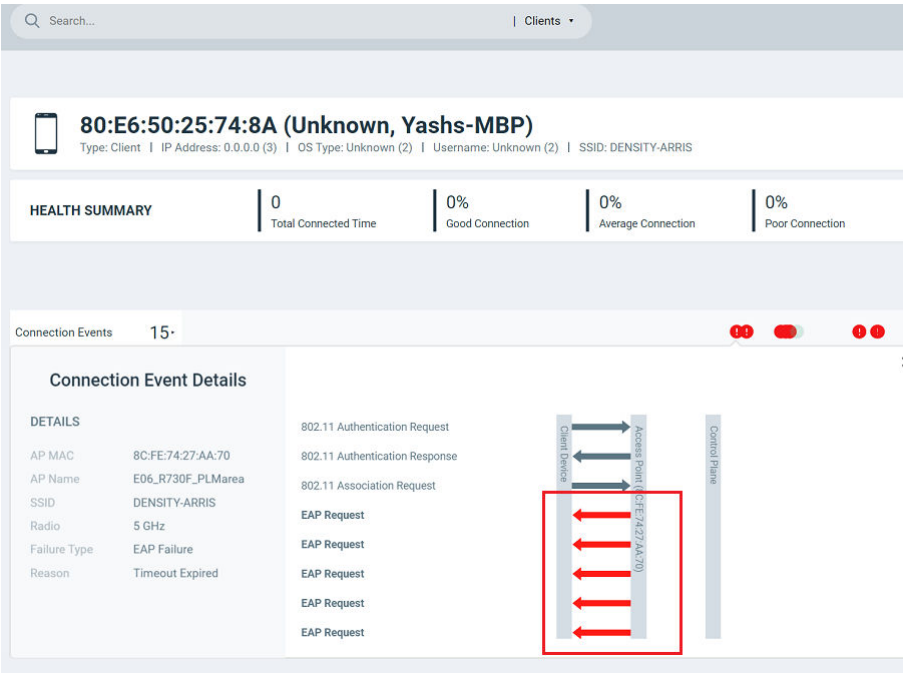
- Total Connected Time
- Percentage of Good Connection
- Percentage of Average Connection
- Percentage of Poor Connection

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 to send EAP requests to the client.

FIGURE 32 Failure to Send EAP Request



- 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.

Service Validation

- Testing Client Services..... 55
- Service Validation Test Report..... 58

Testing Client Services

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

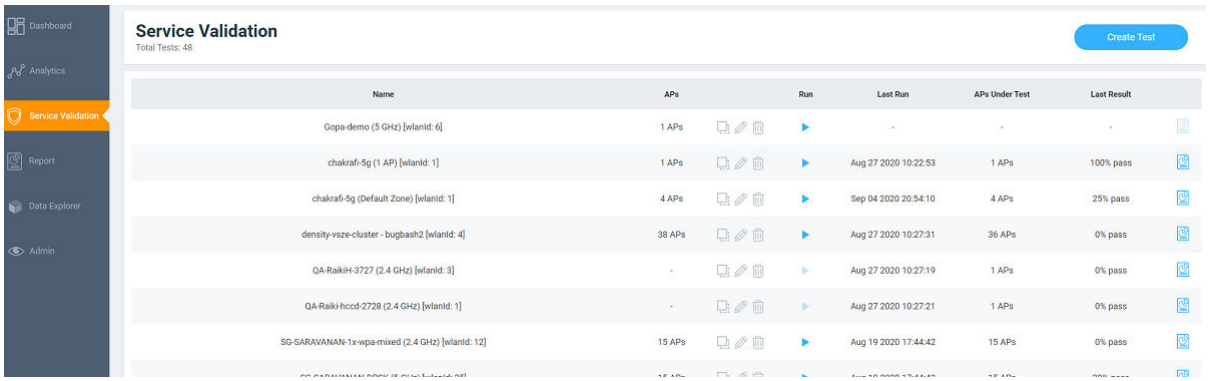
APs will emulate as virtual clients and perform the end-to-end connectivity tests (such as EAP, RADIUS, DHCP, DNS, ping, and traceroute) thereby connecting to a WiFi network and the internet thereafter. It also performs speed tests to determine the quality of the connection. This feature therefore offers 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 service validation tests. It is important to note that service validation tests generate test traffic over the wired interface. Mesh APs cannot participate in service validation tests.

Follow these steps to create a test:

1. From the navigation bar, click **Service Validation**.

   The **Service Validation** 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 33 Service Validation Page



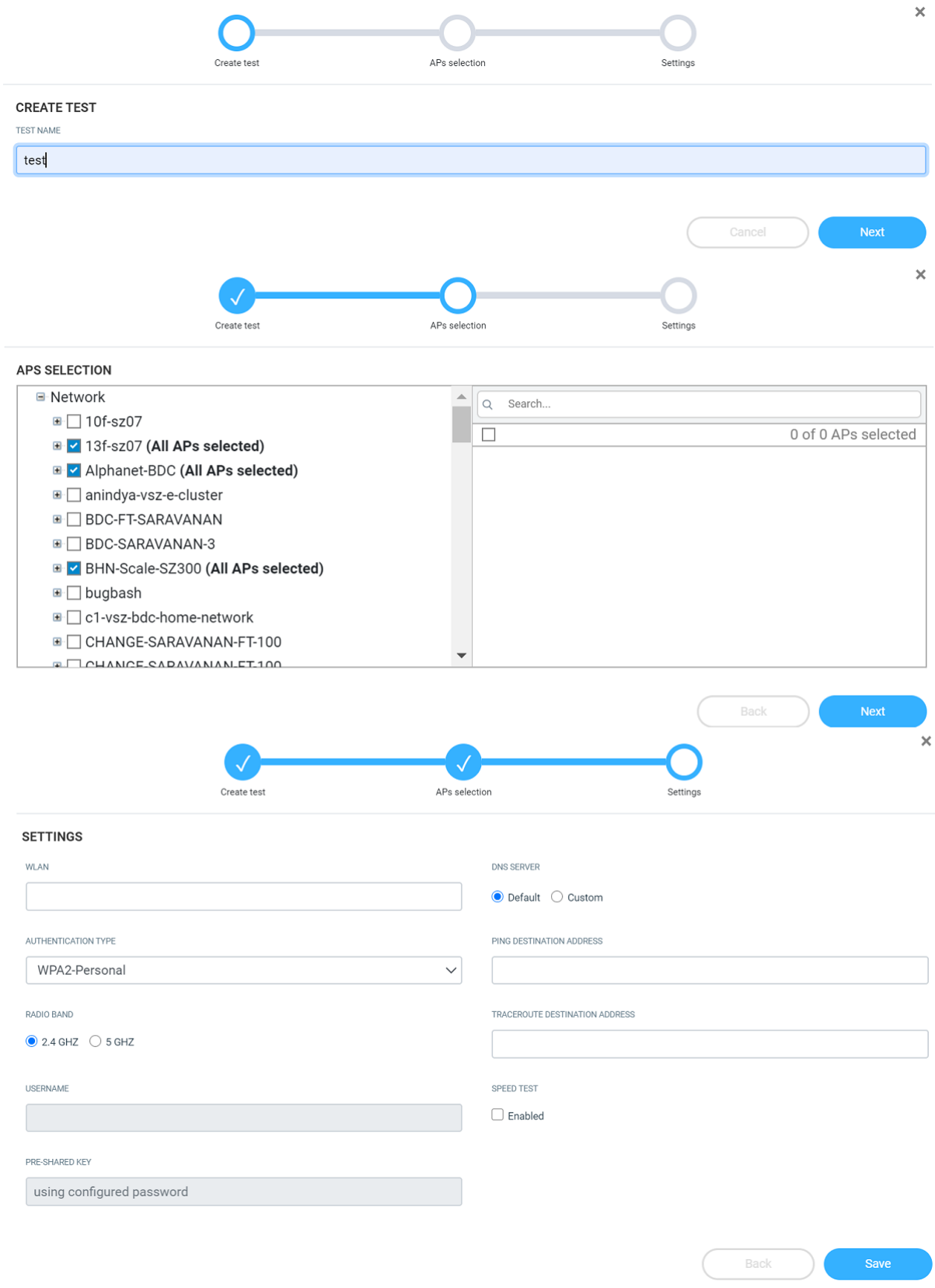
- Name: Displays the name of the test
- APs: Displays the number of APs in the zone
- Run: Click to run the test
- Last Run: Displays the timestamp of the last test run on the AP
- APs Under Test: Displays the number of APs that have been tested
- Last Result: Displays test success as a percentage. For 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 34 Creating a Test



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: Select an authentication method from the menu
   - 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, its is displayed in the **Service Validation** 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.

Service Validation Test Report

The **Service Validation** 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.

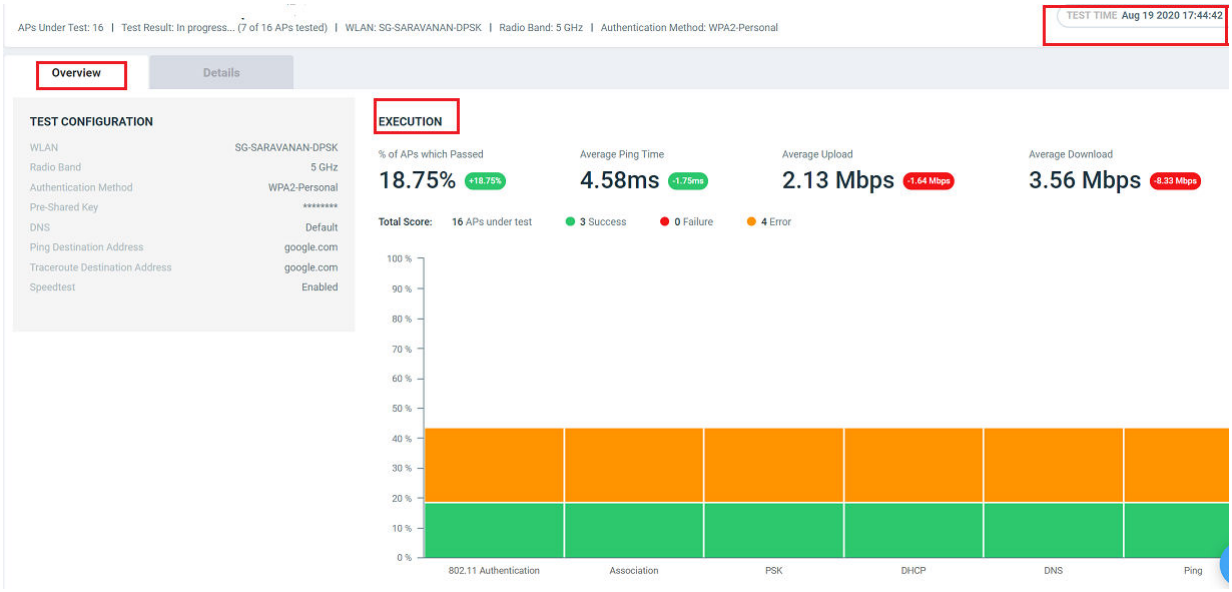
The **Service Validation** Report consists of the following components:

- Overview tab
- Details tab

Overview Tab

The **Overview tab** of the **Service Validation** 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 35 Service Validation 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)

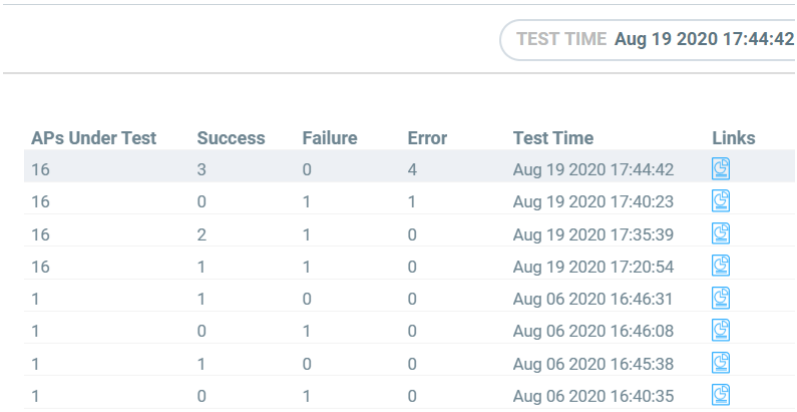
NOTE

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 36 Test Time Log

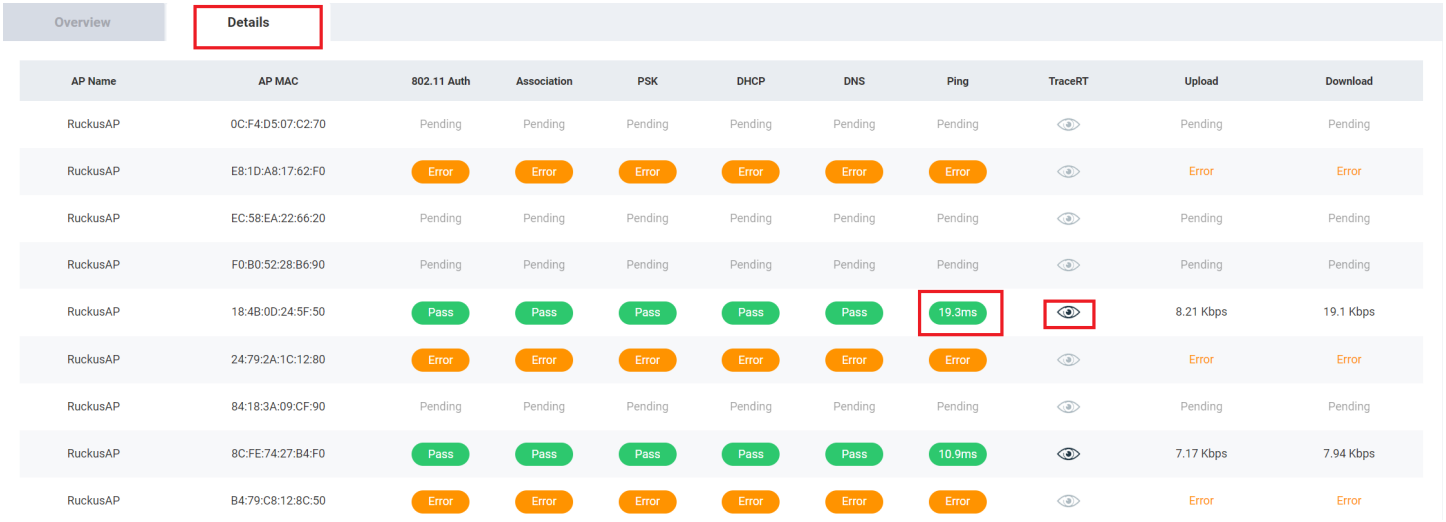


APs Under Test	Success	Failure	Error	Test Time	Links
16	3	0	4	Aug 19 2020 17:44:42	
16	0	1	1	Aug 19 2020 17:40:23	
16	2	1	0	Aug 19 2020 17:35:39	
16	1	1	0	Aug 19 2020 17:20:54	
1	1	0	0	Aug 06 2020 16:46:31	
1	0	1	0	Aug 06 2020 16:46:08	
1	1	0	0	Aug 06 2020 16:45:38	
1	0	1	0	Aug 06 2020 16:40:35	

Details Tab

The **Details tab** of the **Service Validation** Report displays detailed information about the status of the authentication stages.

FIGURE 37 Service Validation Report: Details Tab



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 **Service Validation** 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.

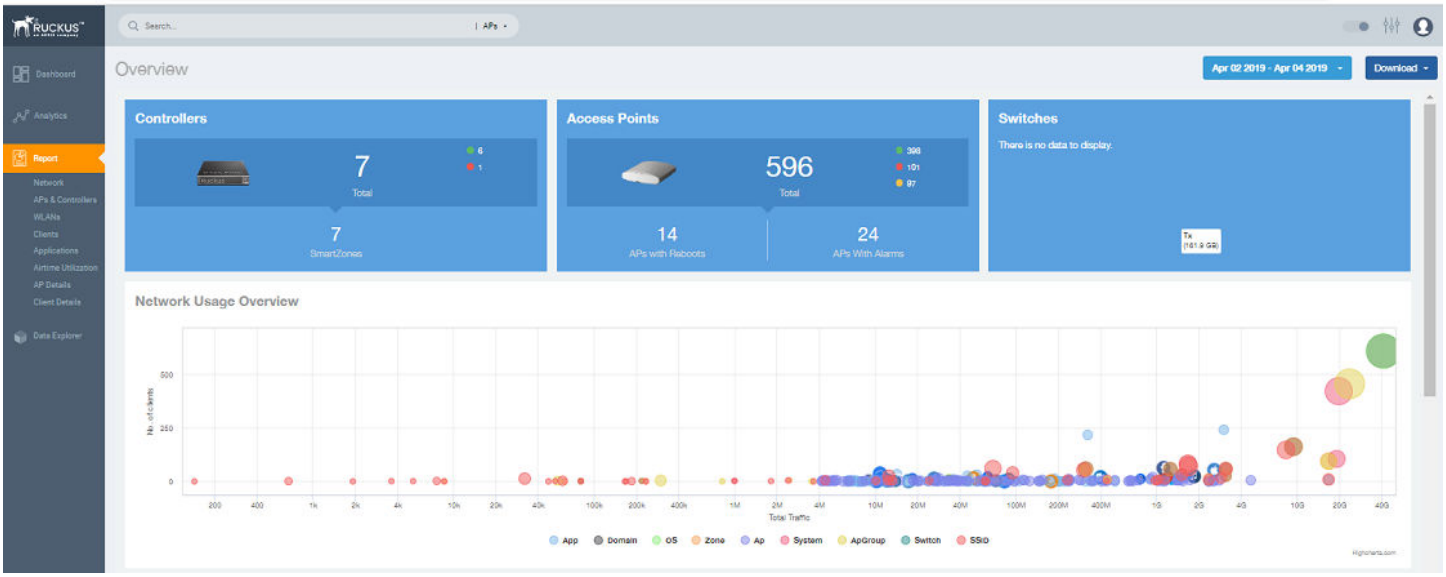
Report

- Using the Overview Dashboard: Content Panel..... 63
- Wireless Network Report..... 65
- Wired Network Report..... 70
- Inventory - APs Report..... 75
- Inventory - Controllers Report..... 84
- Inventory - Switches Report..... 87
- WLAN Report 91
- Clients Report..... 96
- Client Health Dashboard..... 100
- Applications Report..... 104
- Airtime Utilization Report..... 106
- AP Details Report..... 110
- Client Details Report..... 120
- Switch Details Report Dashboard..... 124
- Comparison Reports Dashboard..... 128
- PCI Profiles..... 131

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 38 Overview Dashboard : Top Portion

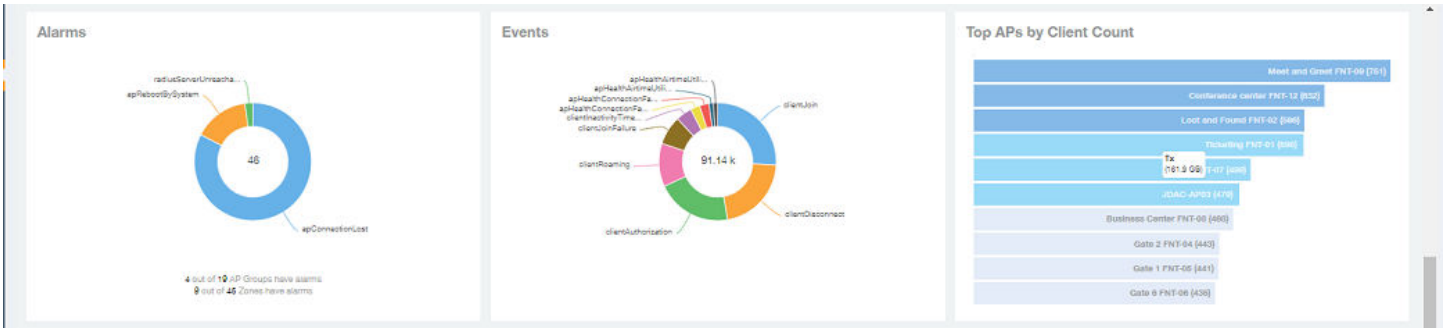


The top portion of the **Overview Dashboard** shows the following tiles:

- 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 39 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 40 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 41 Wireless Network Report (Upper Portion Only)

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

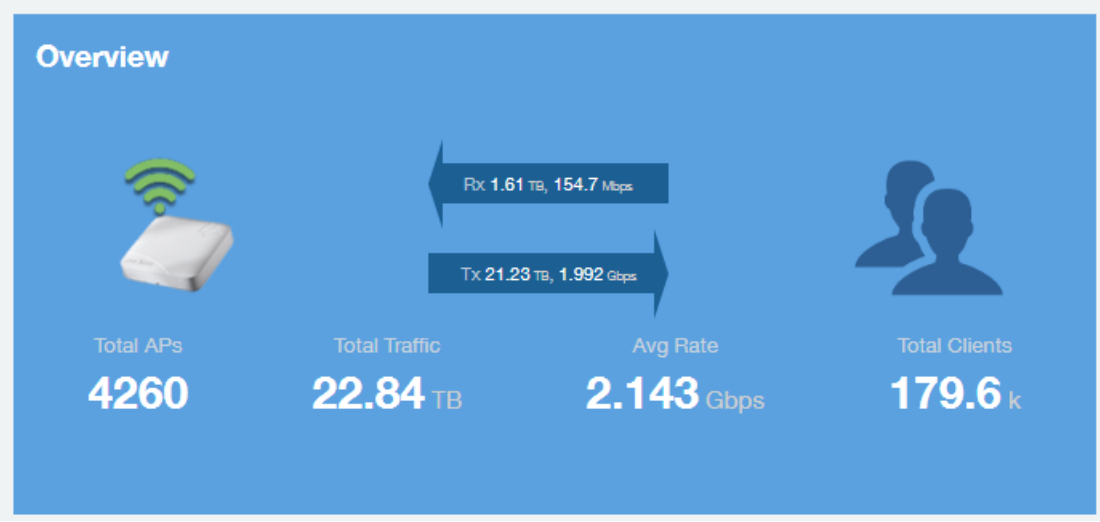
- Overview tile
- Traffic Distribution chart
- Top APs by Traffic tile
- Top APs by Client Count graph
- Traffic Trend graphs
- Traffic Over Time graph

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 42 Wireless Network Report: Overview Tile

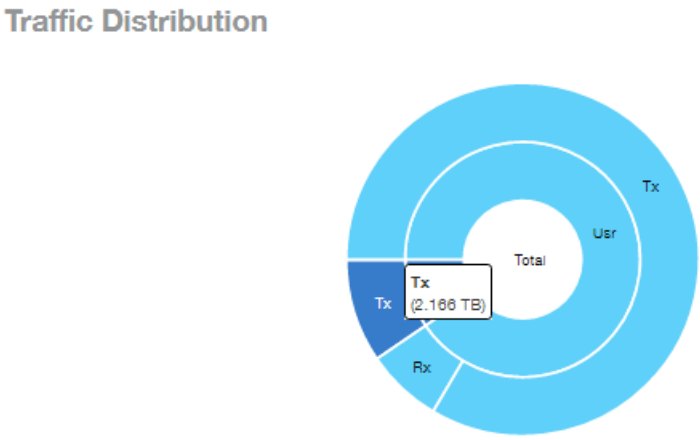


Traffic Distribution Tile

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 43 Wireless Network Report: Traffic Distribution Tile



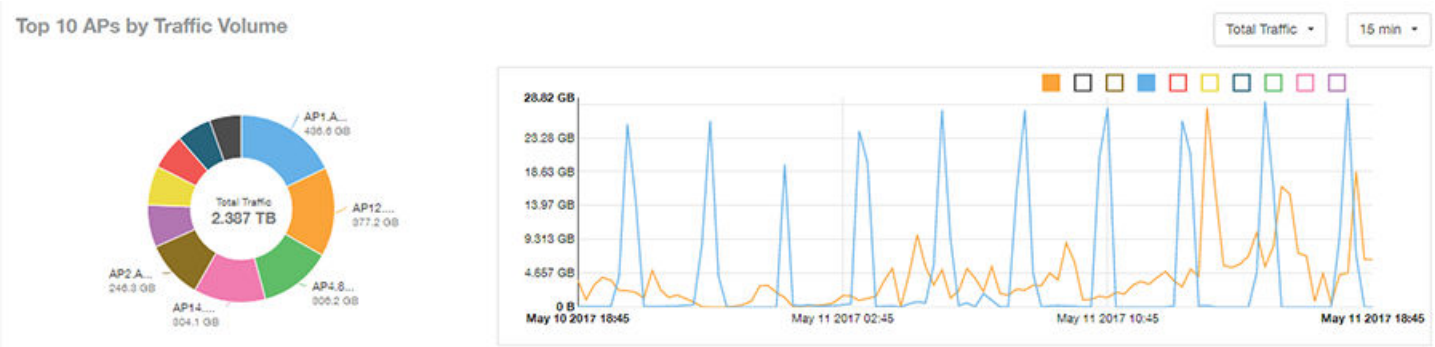
Top APs by Traffic Tile

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

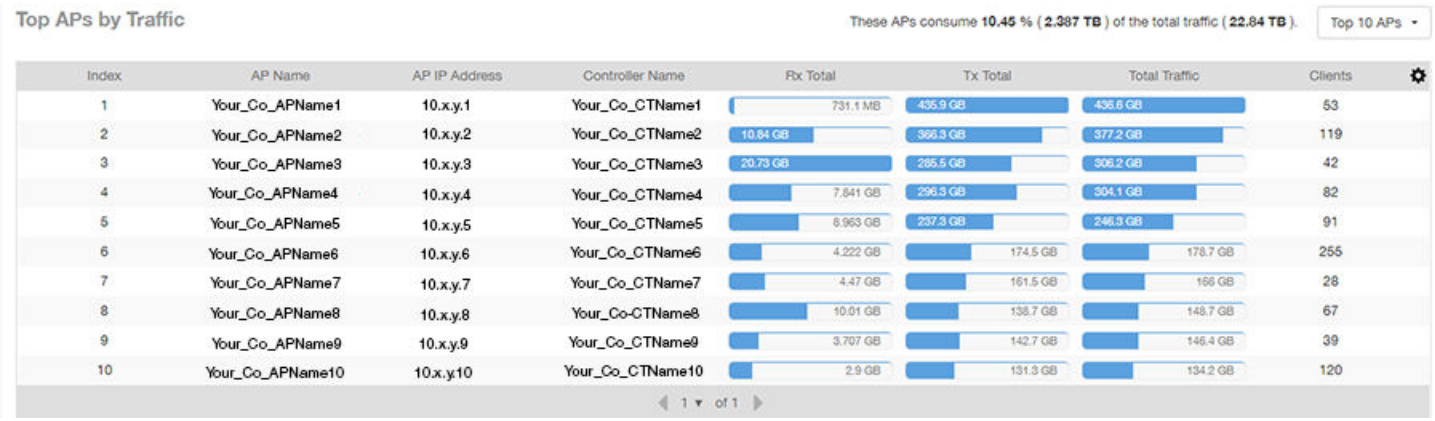


> **NOTE**
> If you pause the pointer over the line graph, an information box is displayed containing the selected AP details.

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 45 Wireless Network Report: Top APs by Traffic (Table)

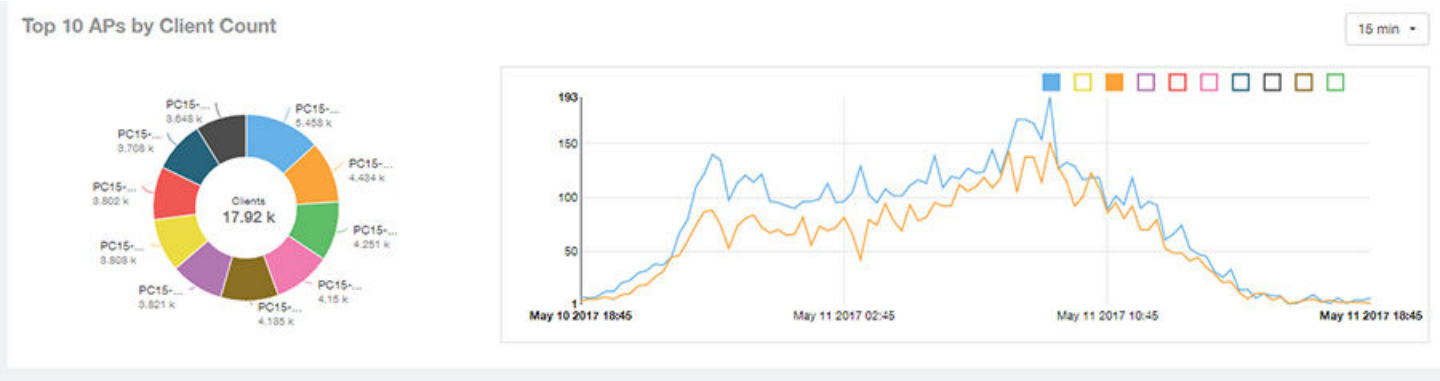


Top APs by Client Count Tile

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.

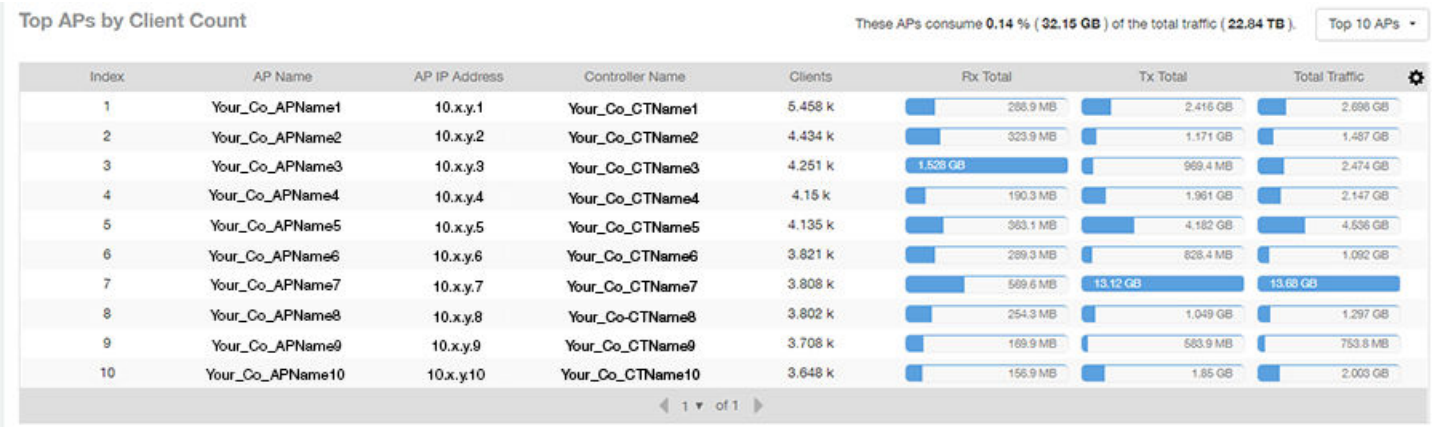
In the tile, use the menu to specify the time period of 15 minutes, 1 hour, or 1 day. If you pause the pointer over the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected AP details in the line graph.

FIGURE 46 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 47 Wireless Network Report : Top APs by Client Count (Table)



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	2.696 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	969.4 MB	2.474 GB
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName4	4.15 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	828.4 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	156.9 MB	1.85 GB	2.003 GB

1 of 1

Traffic Trend Graphs

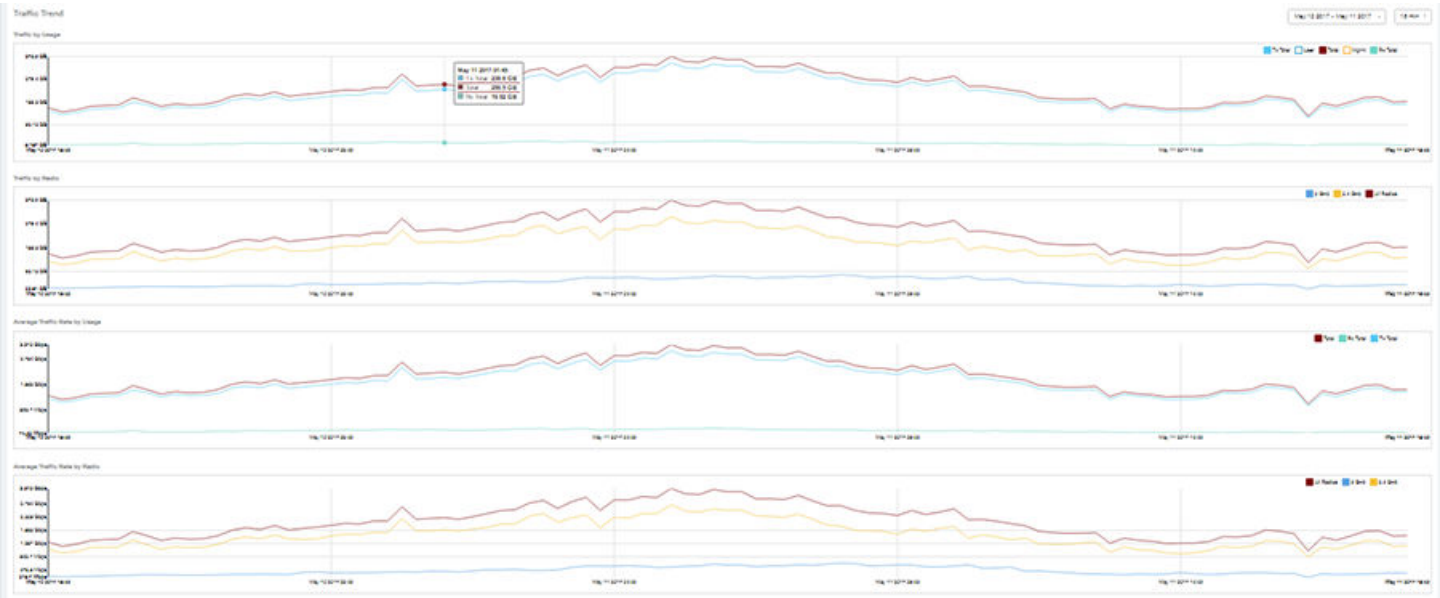
The **Traffic Trend** graphs of the **Wireless Network Report** display the traffic by usage and radio over time.

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

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 48 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.

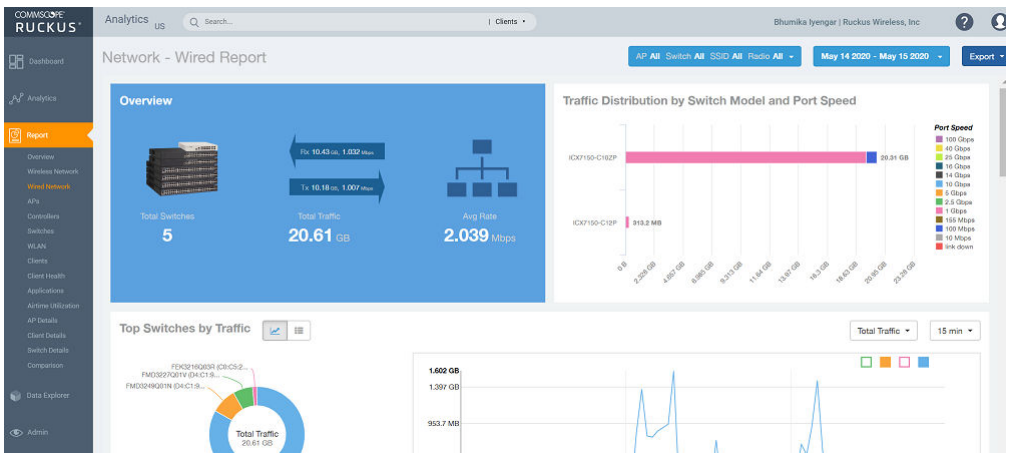
FIGURE 49 Wireless Network Report: Traffic Over Time Table

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 50 Wired Network Report (Upper Portion Only)



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

- Overview tile

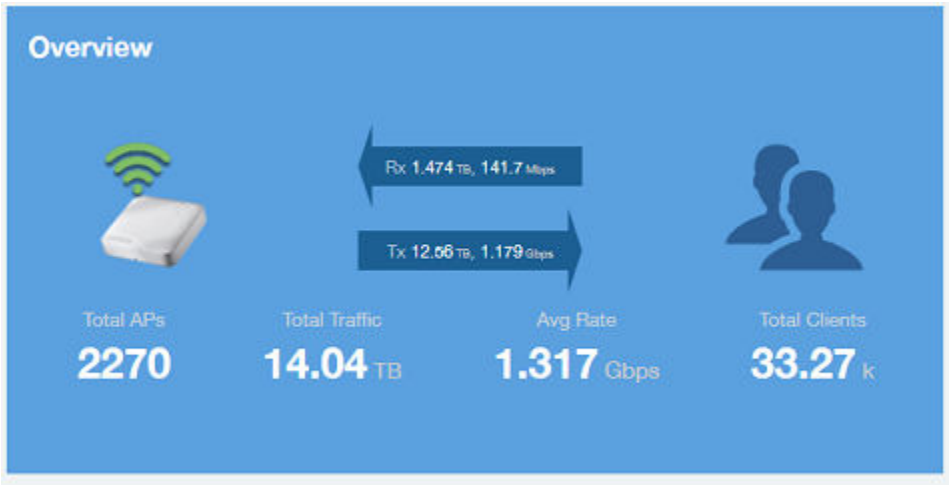
- Traffic Distribution by Switch Model and Port Speed tile
- Top Switches by Traffic tile
- Top Switches by PoE Usage tile
- Top Switches by Errors tile
- Traffic Trend tile
- Error Trend tile

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 51 Wired Network Report: Overview Tile

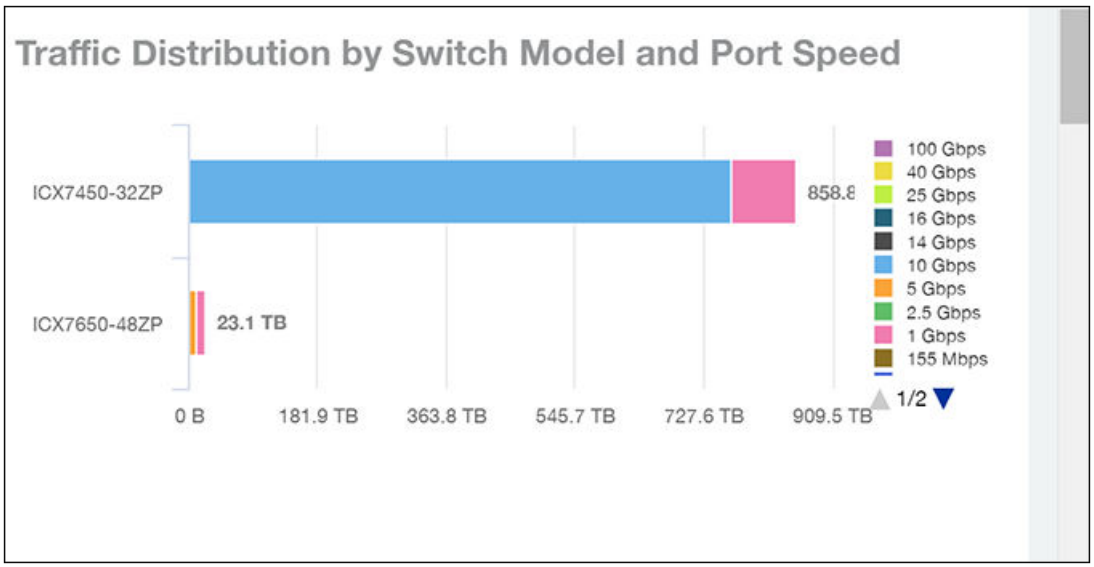


Traffic Distribution by Switch Model and Port Speed Chart

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.

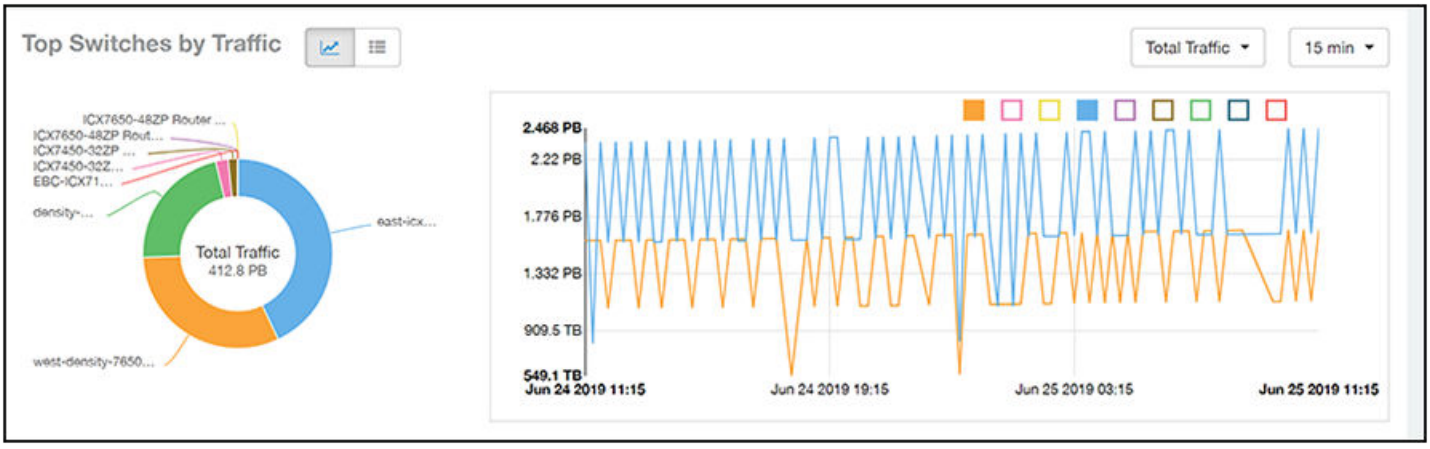
FIGURE 52 Wired NetworkReport: Traffic Distribution by Switch Model and Port Speed Chart



Top Switches by Traffic Tile

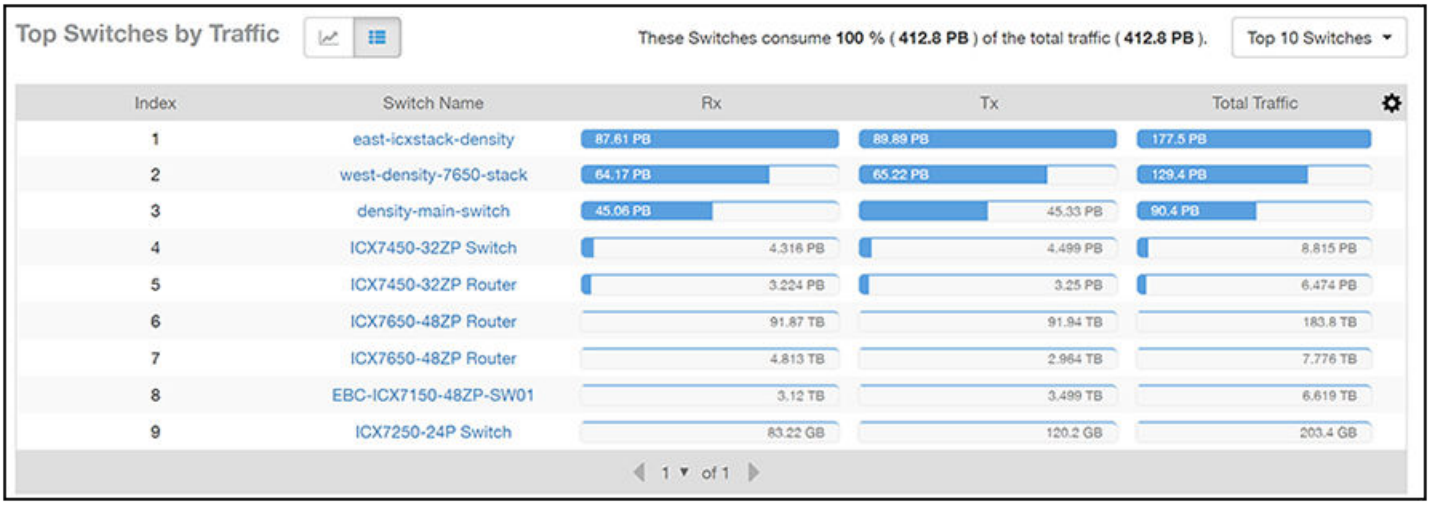
The **Top Switches by Traffic** donut chart and graph of the **Wired Network Report** display which wired switches have the most traffic. You can use the traffic menu to show total traffic, transmitted traffic only, or received traffic only; and use the time menu to specify the time granularity.
If you 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 53 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 54 Wired Network Report Top Switches by Traffic Table

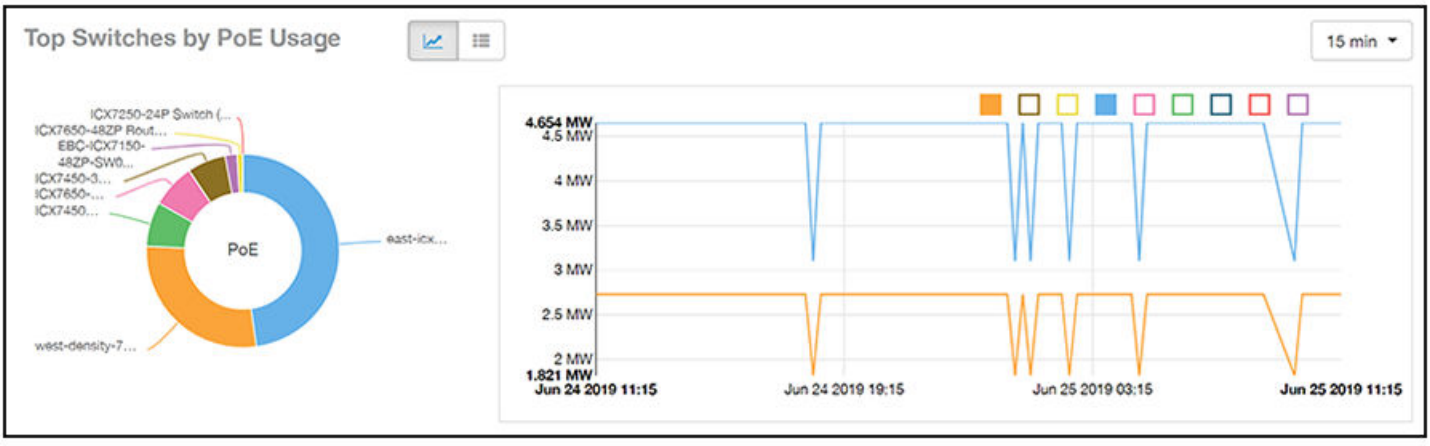


Top Switches by PoE Usage Tile

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.

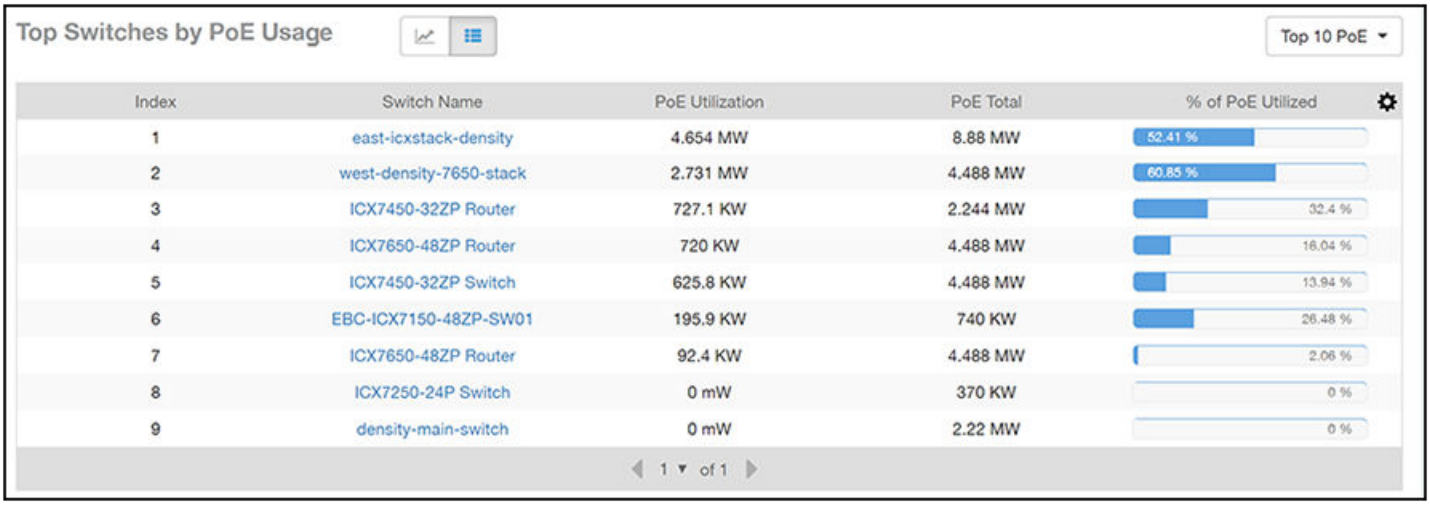
If you pause the pointer over the donut chart or the line graph, an information box is displayed containing the details on the selected data points. You can click one of the areas of the donut chart to go to the **Switch Details** dashboard for the corresponding switch. Click any of the colored squares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

FIGURE 55 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 56 Wired Network Report: Top Switches by PoE Usage Table

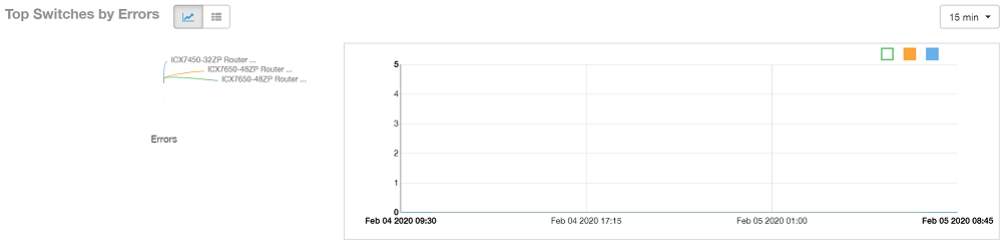


Top Switches by Errors Tile

The **Top Switches by Errors** donut chart and graph of the **Wired Network Report** display the error count for switches.

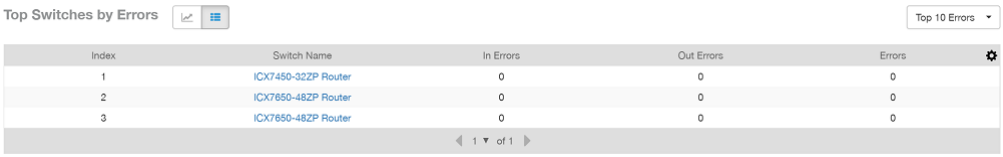
If you pause the pointer over the donut chart or the line graph, an information box is displayed containing the details on the selected data points. You can click one of the areas of the donut chart to go to the **Switch Details** dashboard for the corresponding switch. Click any of the colored squares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

FIGURE 57 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 58 Wired Network Report: Top Switches by Error Table

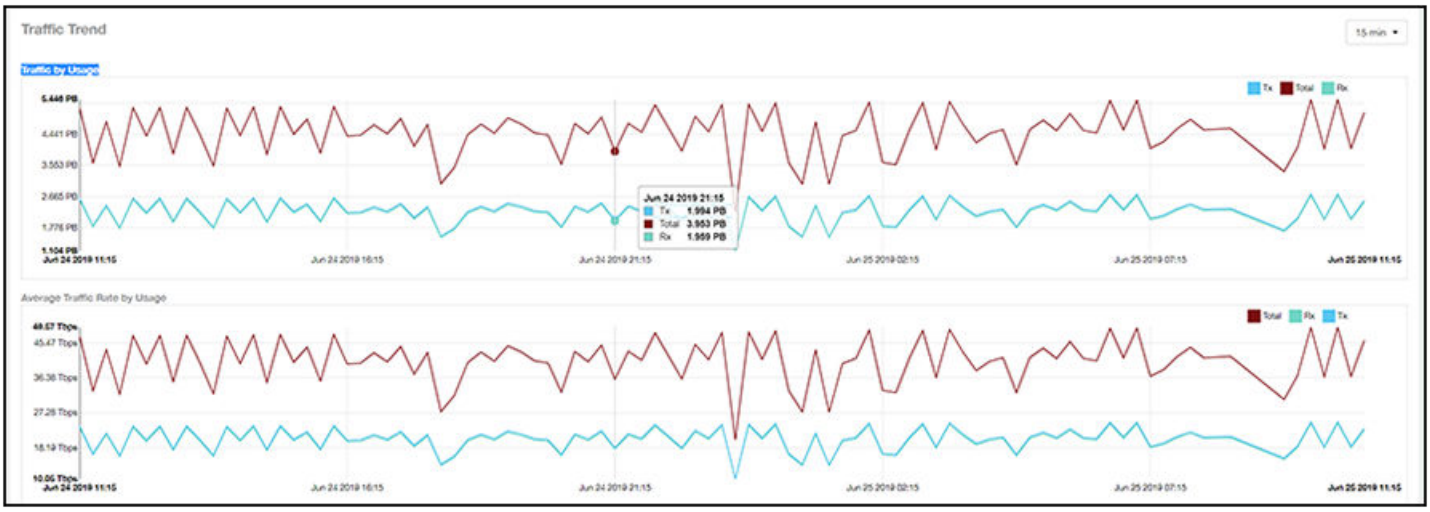


Traffic Trend Graph

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 59 Wired Network Report: Traffic Trend Graph

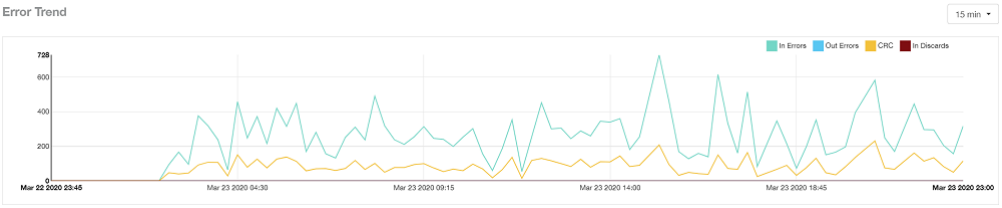


Error Trend Graph

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 60 Wired Network: Error Trend Graph

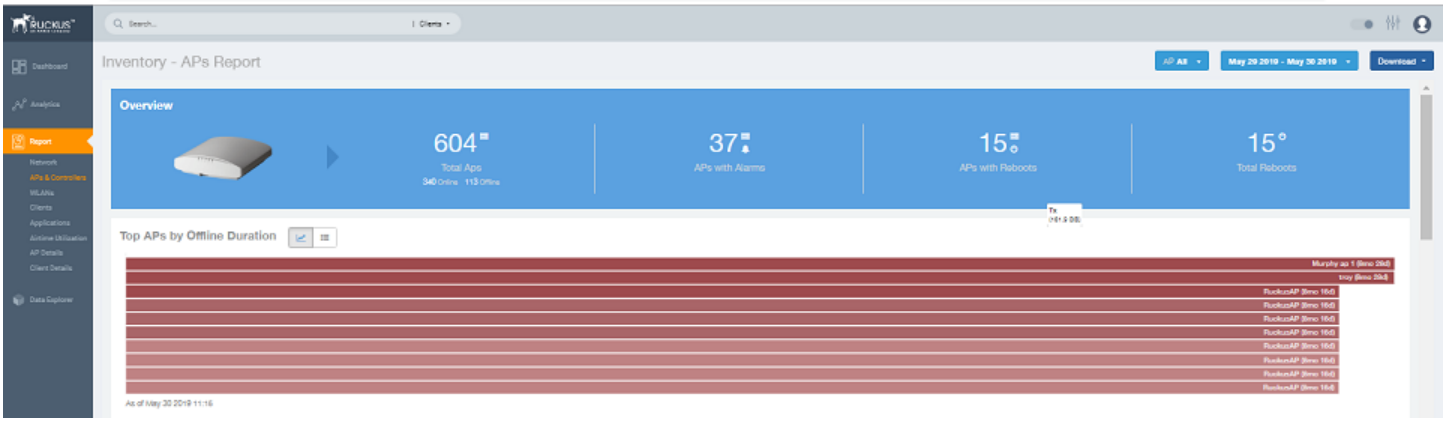


Inventory - APs Report

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 61 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

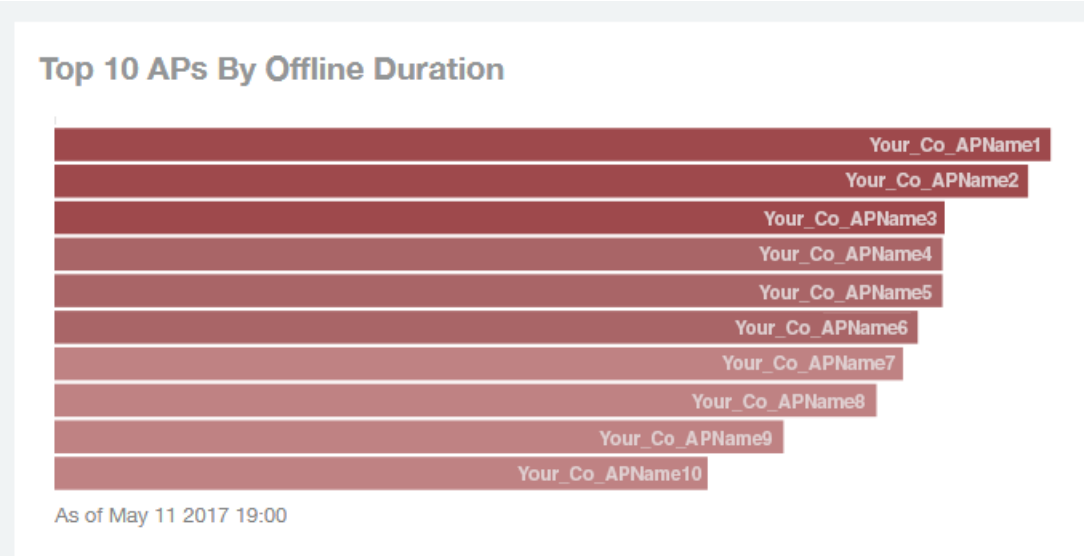
FIGURE 62 Inventory - APs Report: Overview Tile

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

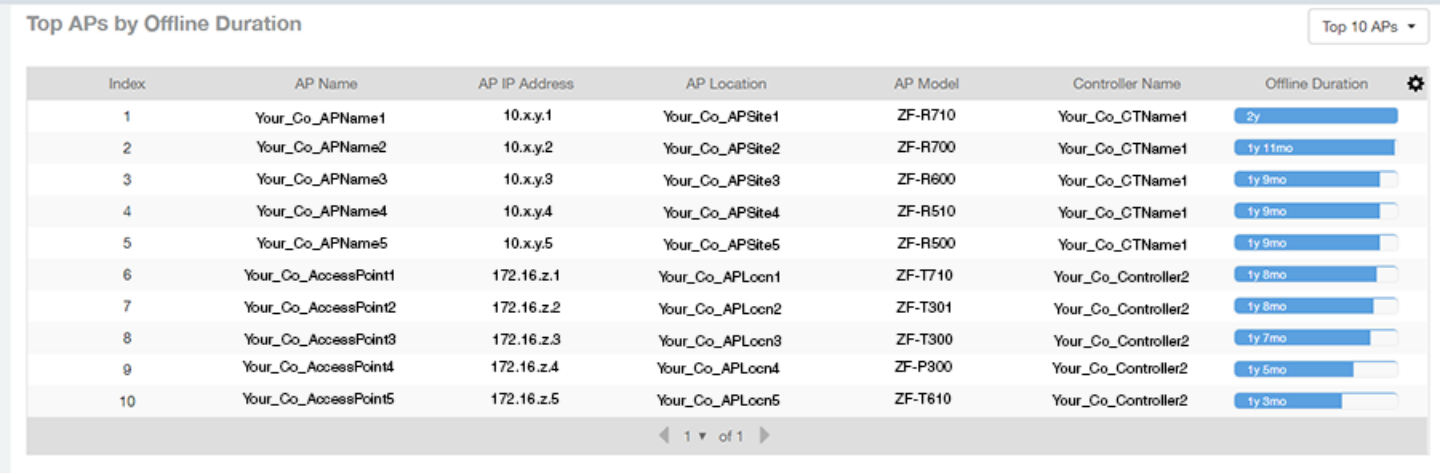


Use the chart and table icons ( ) to toggle between the chart and table views.

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



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

1 of 1

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 65 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.

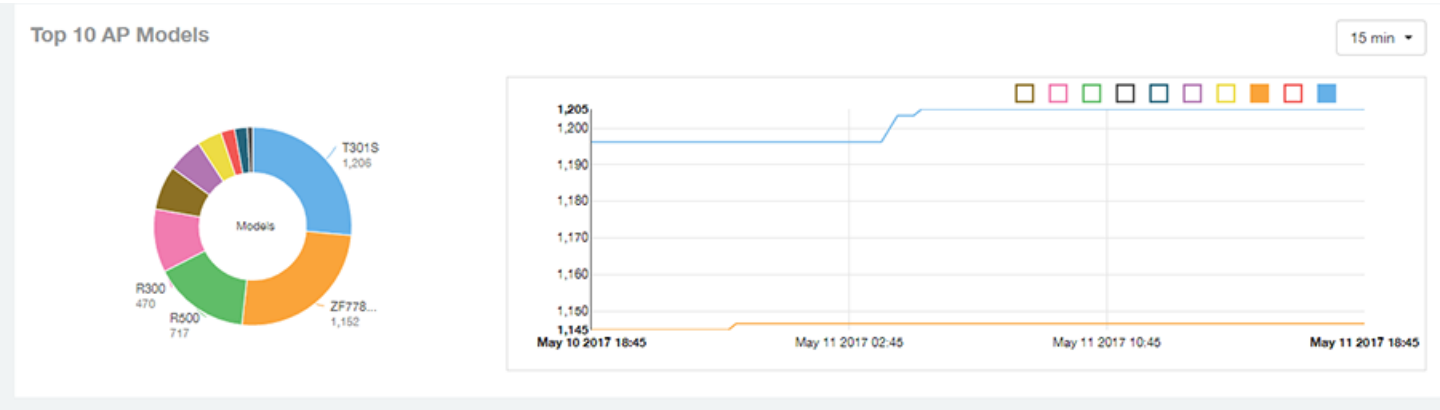
FIGURE 66 Inventory - APs Report: AP Status Trends Tile

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.

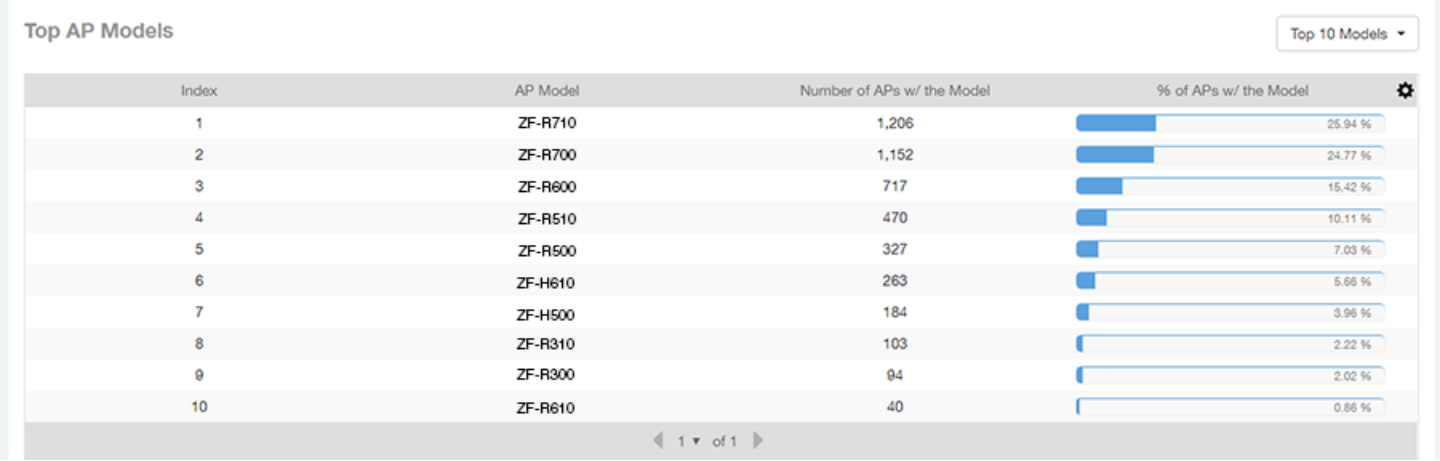
FIGURE 67 Inventory - APs Report: Top AP Models (Chart and Graph)



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 68 Inventory - APs Report: Top AP Models (Table)

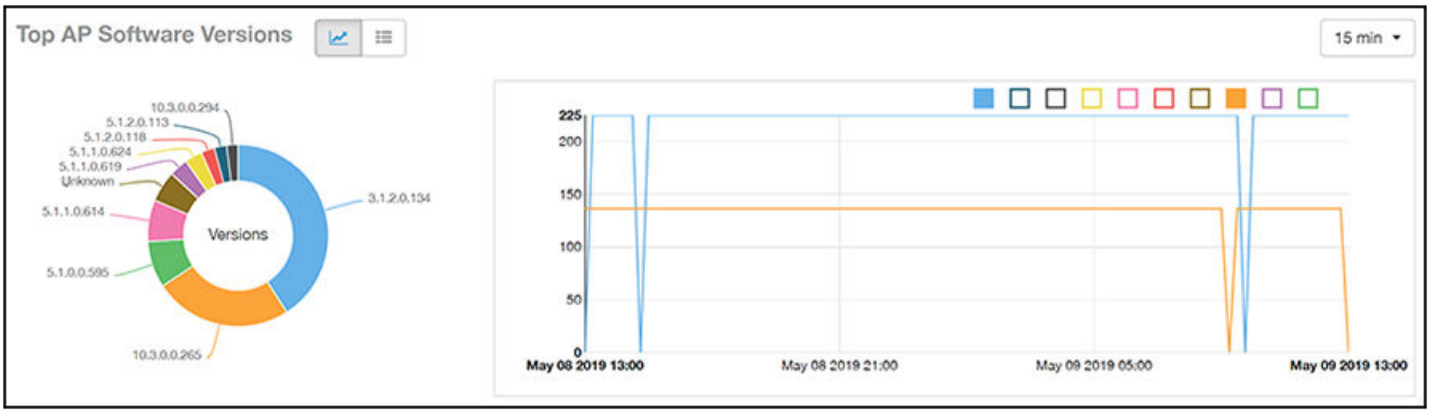


Top AP Software Versions Tile

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.

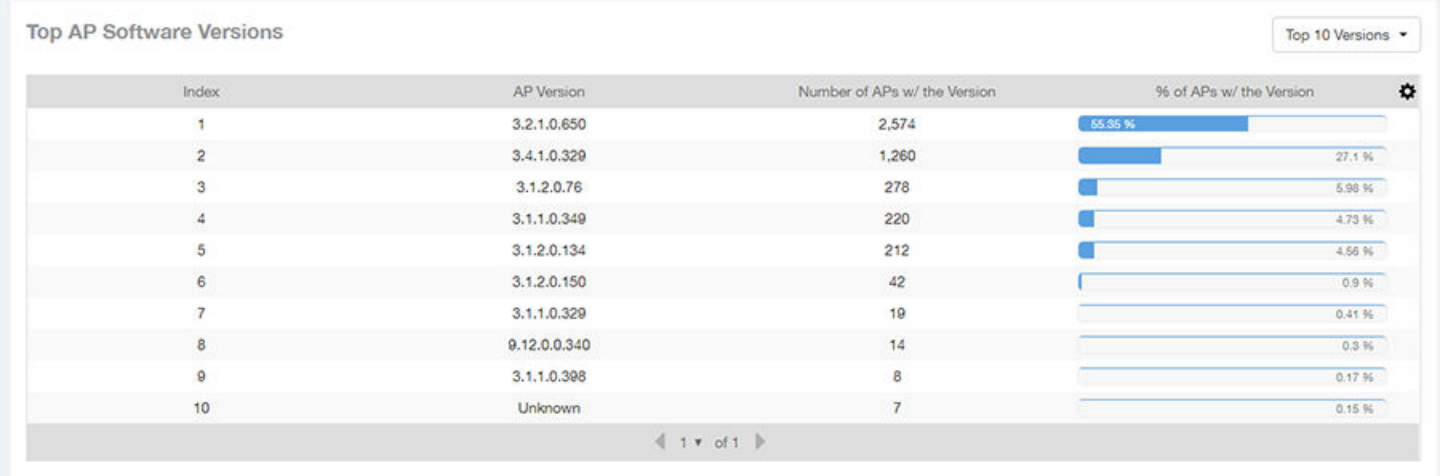
FIGURE 69 Inventory - APs Report: Top AP Software Versions (Graph and Chart)



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

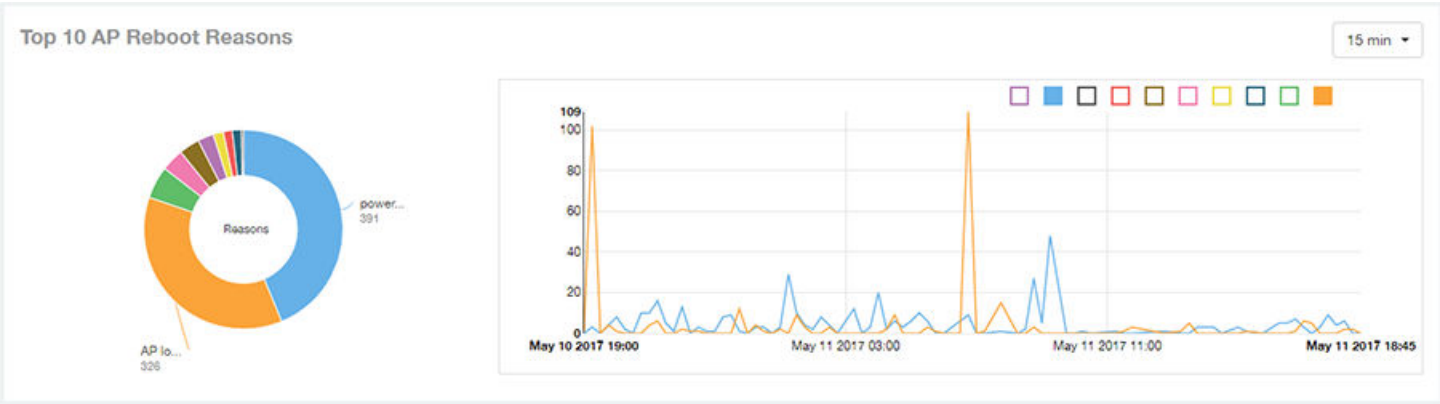


Top 10 AP Reboot Reasons Tile

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 71 Inventory - APs Report: Top 10 AP Reboot Reasons Tile

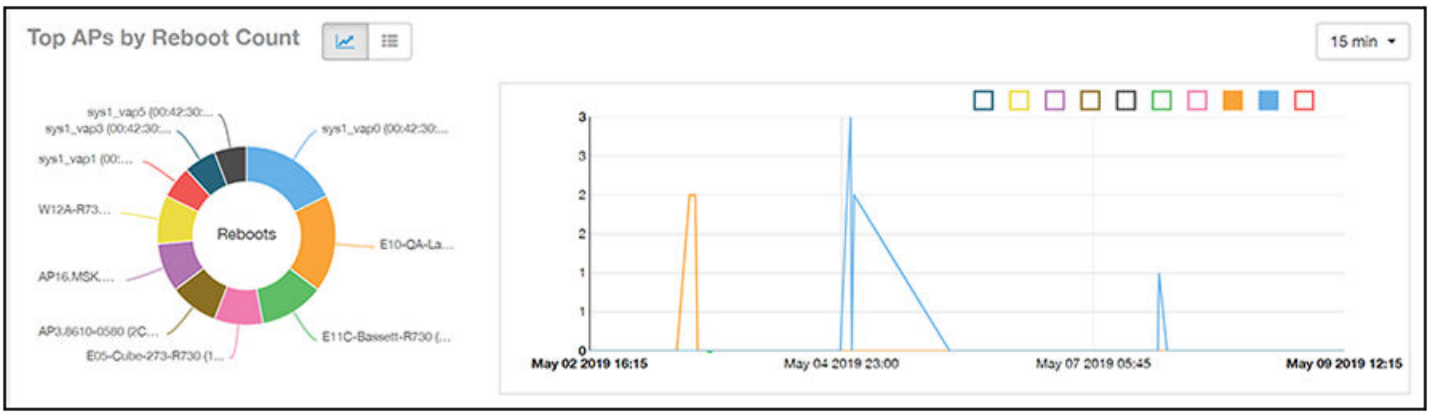


Top APs by Reboot Count Tile

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.

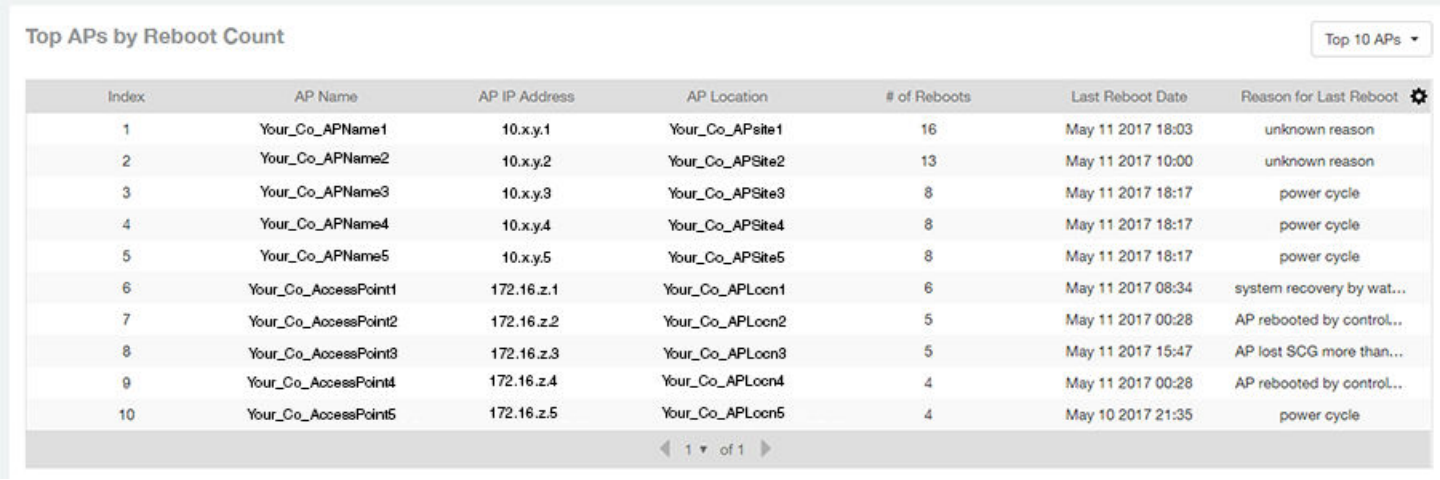
FIGURE 72 Inventory - APs Report: Top APs by Reboot Count (Chart and Graph)



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

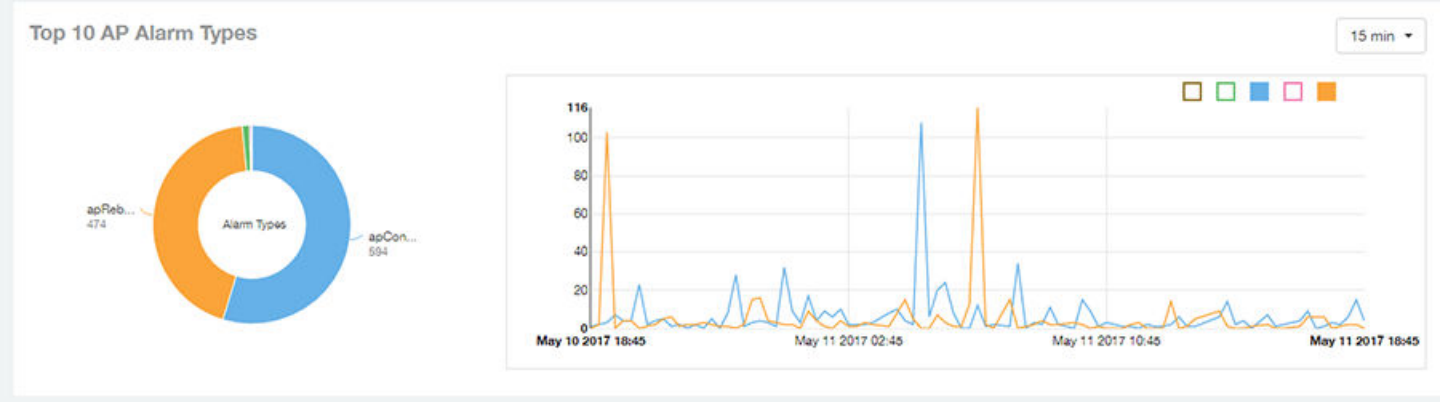


Top 10 AP Alarm Types Tile

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.

FIGURE 74 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.

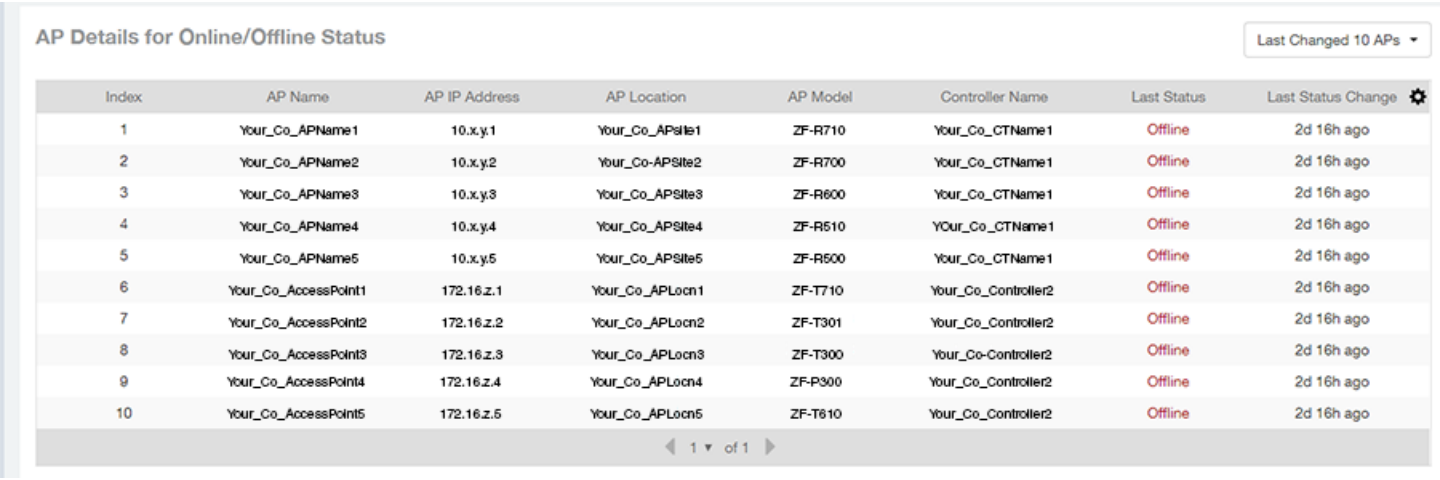
FIGURE 75 Inventory - APs Report: APs Configured in Multiple Systems Table

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



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

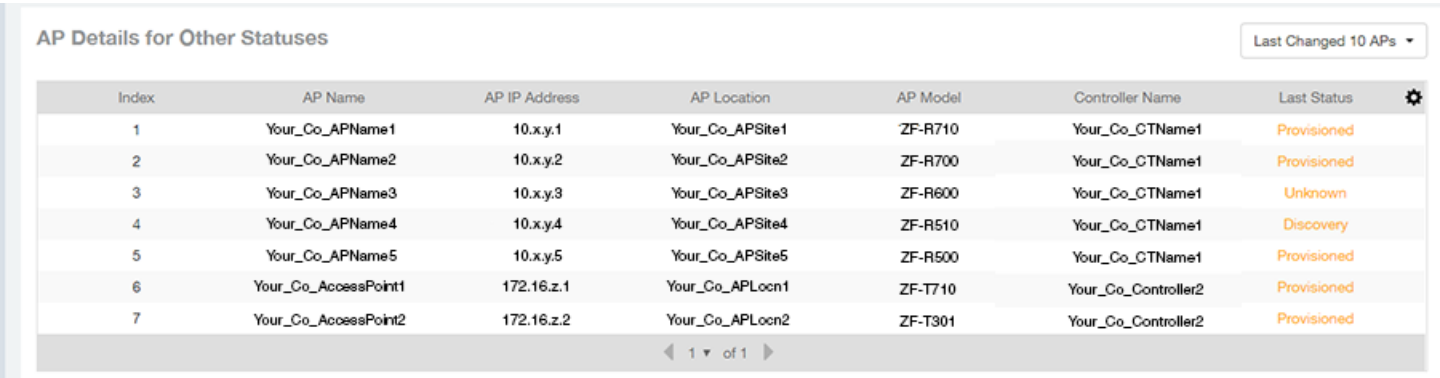
1 of 1

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 77 Inventory - APs Report: AP Details for Other Statuses Table



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

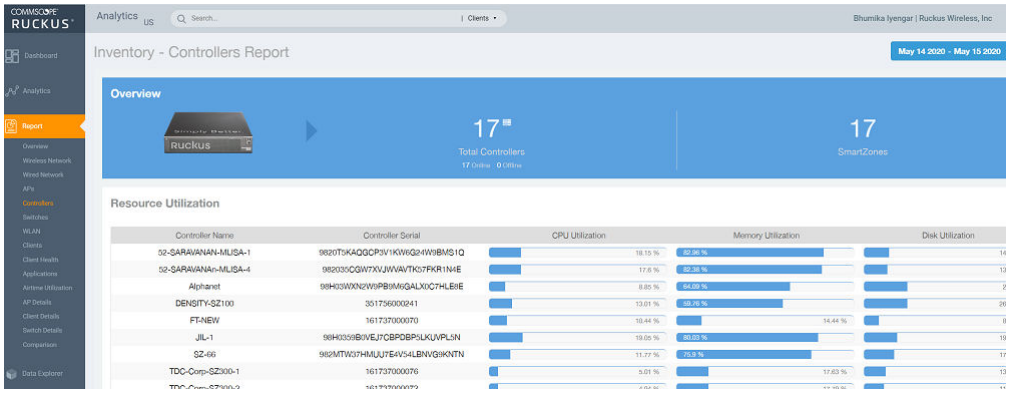
1 of 1

Inventory - Controllers Report

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

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

FIGURE 78 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

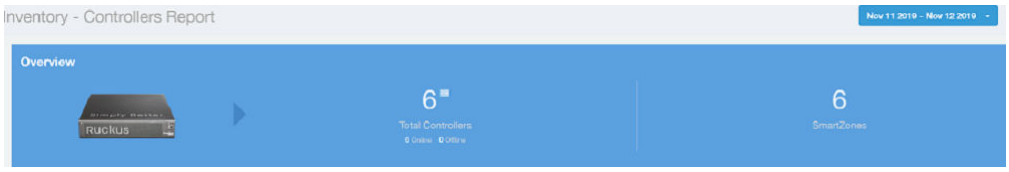
NOTE
All counts in the **Inventory - Controllers Report** are exact counts.

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 79 Inventory - Controllers Report: Overview Tile

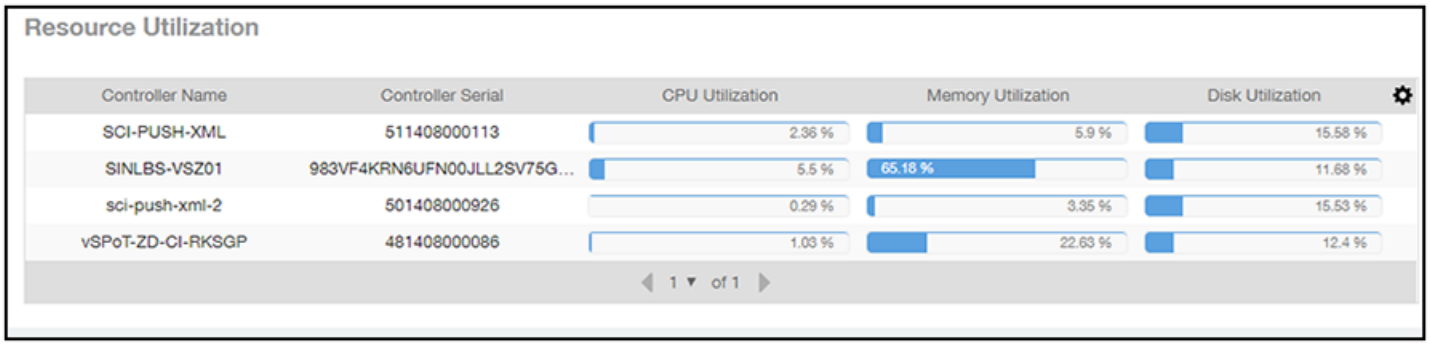


Resource Utilization Table

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 80 Inventory - Controllers Report: Resource Utilization Table

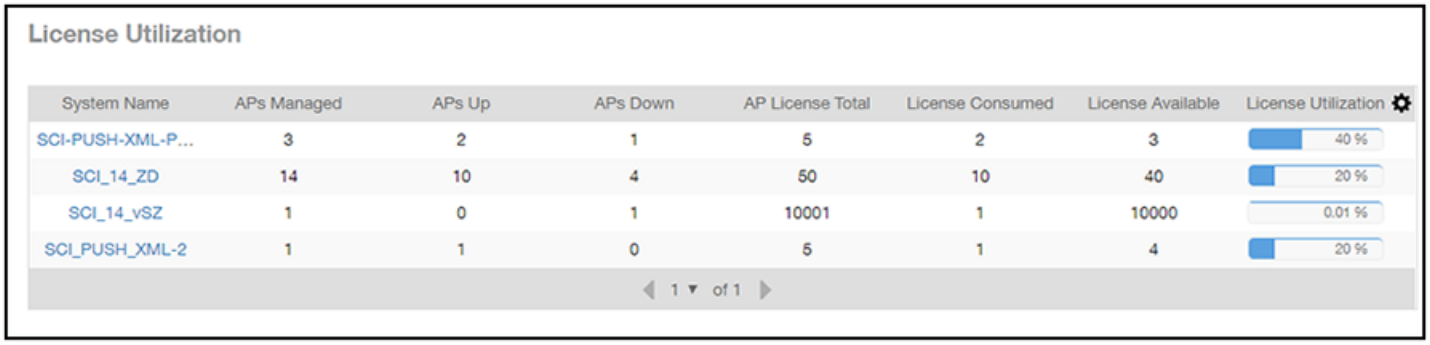


License Utilization Table

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.

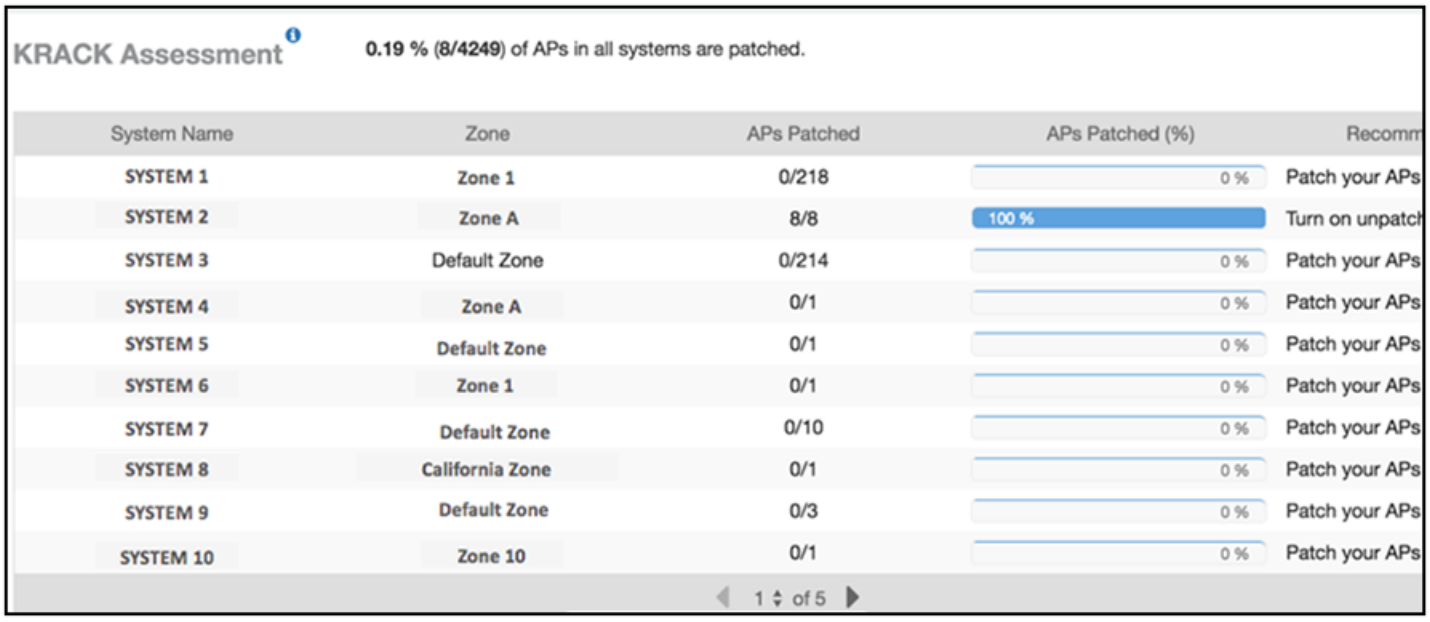
FIGURE 81 Inventory - Controllers Report: License Utilization Table



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 82 Inventory - Controllers Report: KRACK Assessment Table



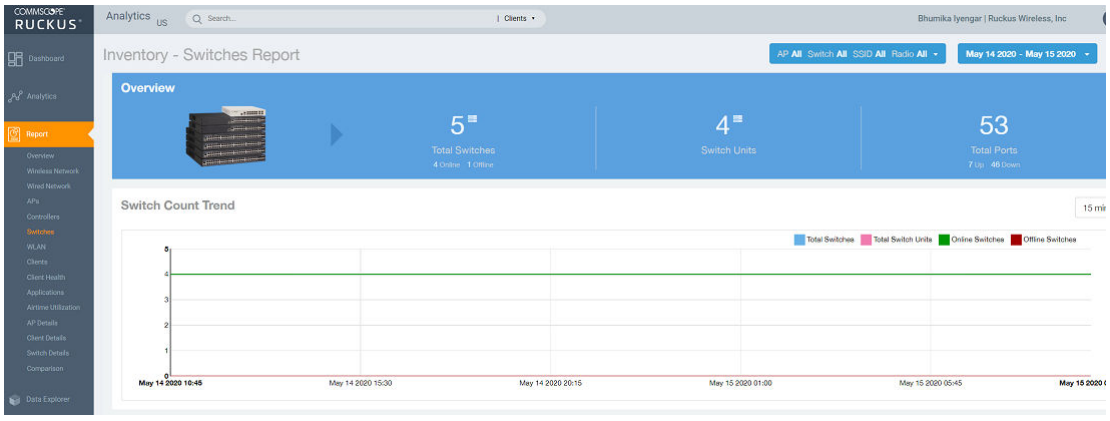
You can follow the recommendations displayed to patch your APs. For information and instructions, refer to: https://support.ruckuswireless.com/krack-ruckus-wireless-support-resource-center.

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 83 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

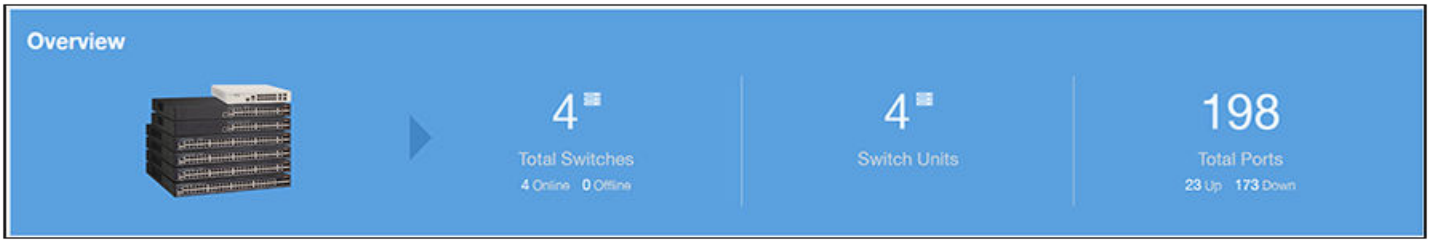
NOTE
All counts in the line graphs, donut charts, and tables of the **Inventory - Switches Report** are exact counts. The counts in trend graphs are approximate.

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 84 Inventory - Switches Report: Overview Tile

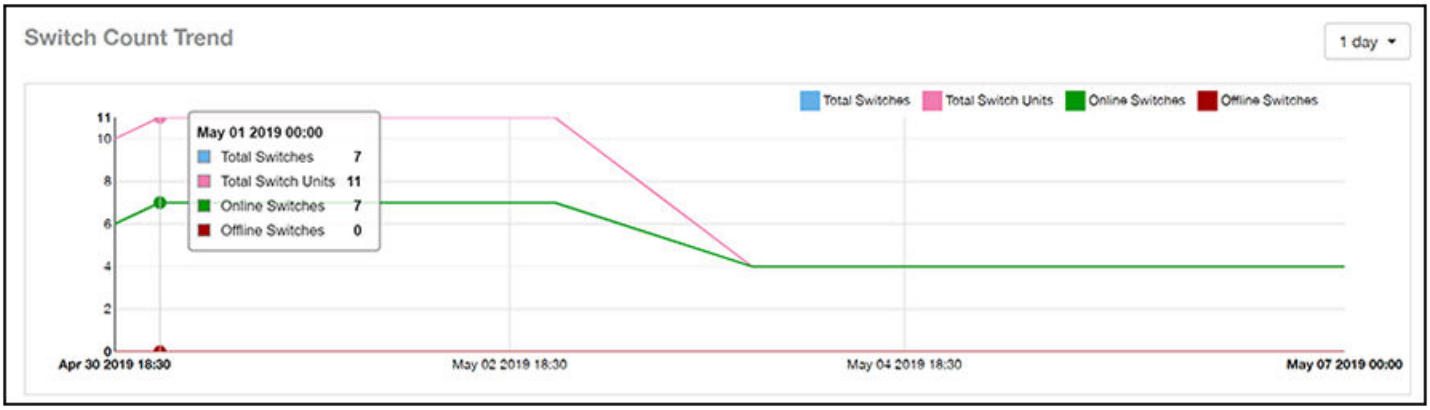


Switch Count Trend Graph

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.

FIGURE 85 Inventory - Switches Report: Switch Count Trend Graph

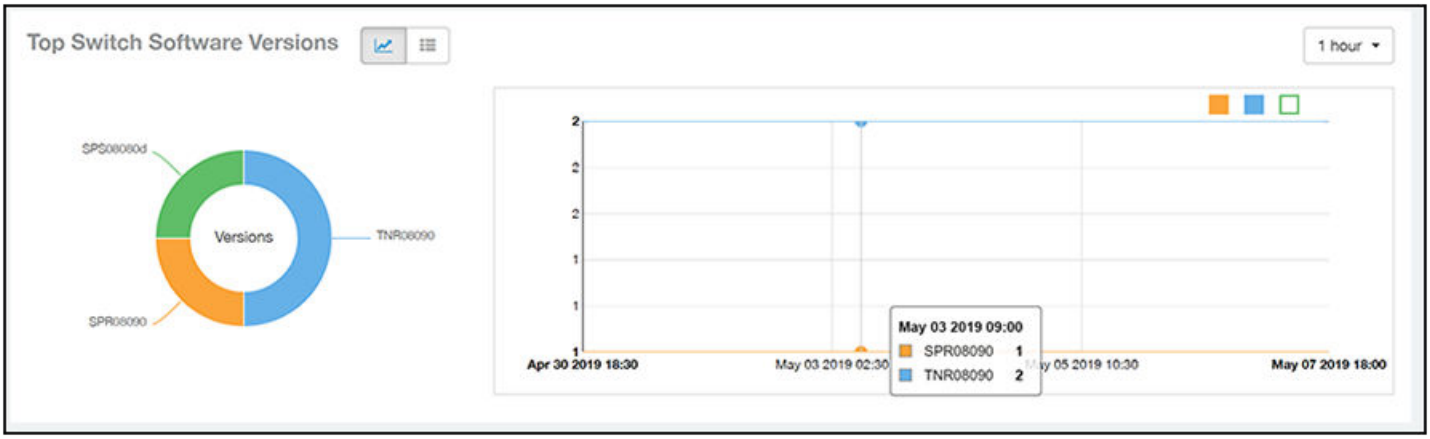


Top Switch Software Versions Tile

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.

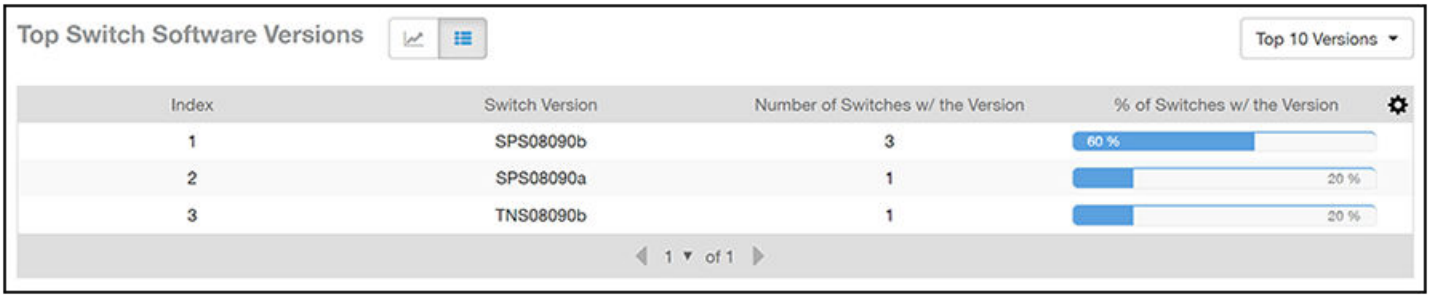
Use the menu to specify the time granularity. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected switch details in the line graph.

FIGURE 86 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 87 Inventory - Switches Report: Top Switch Software Versions Table

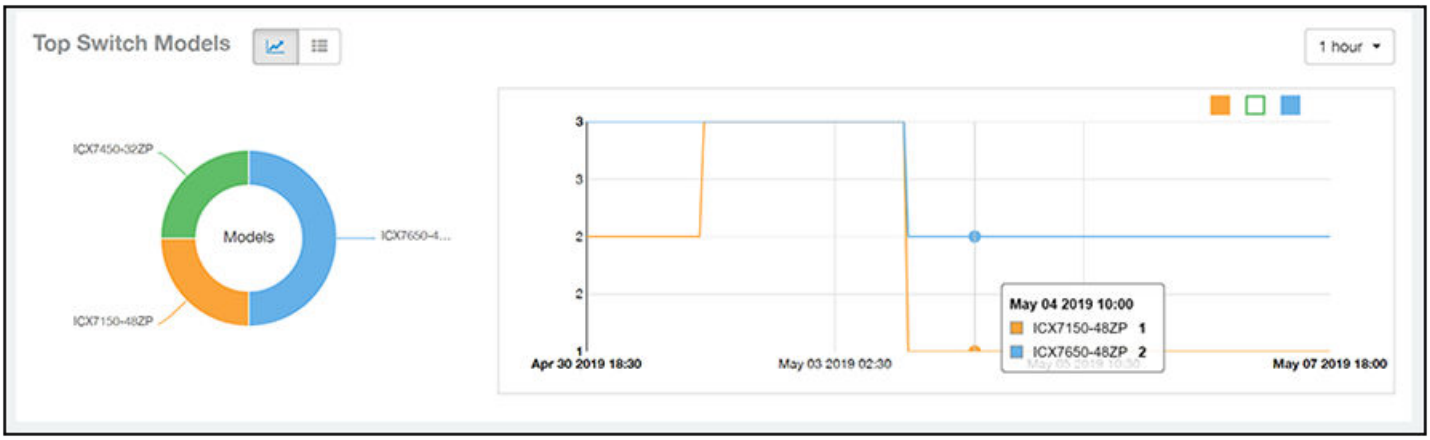


Top Switch Models Tile

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.

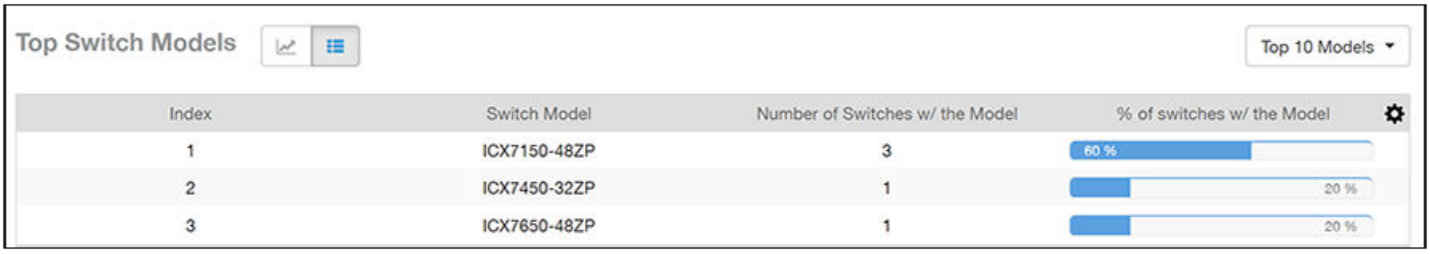
Use the menu to specify the time granularity. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected switch details in the line graph.

FIGURE 88 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.

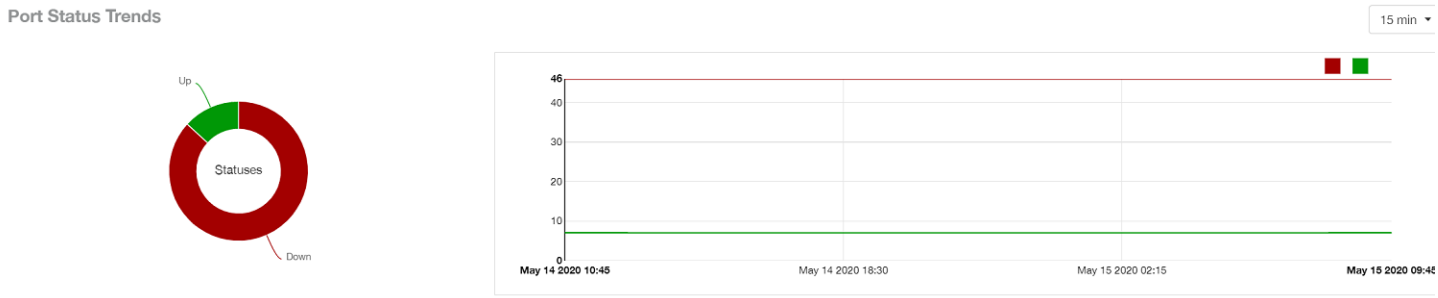
FIGURE 89 Inventory - Switches Report: Top Switch Models Table



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 90 Inventory - Switches Report: Port Status Trends Tile



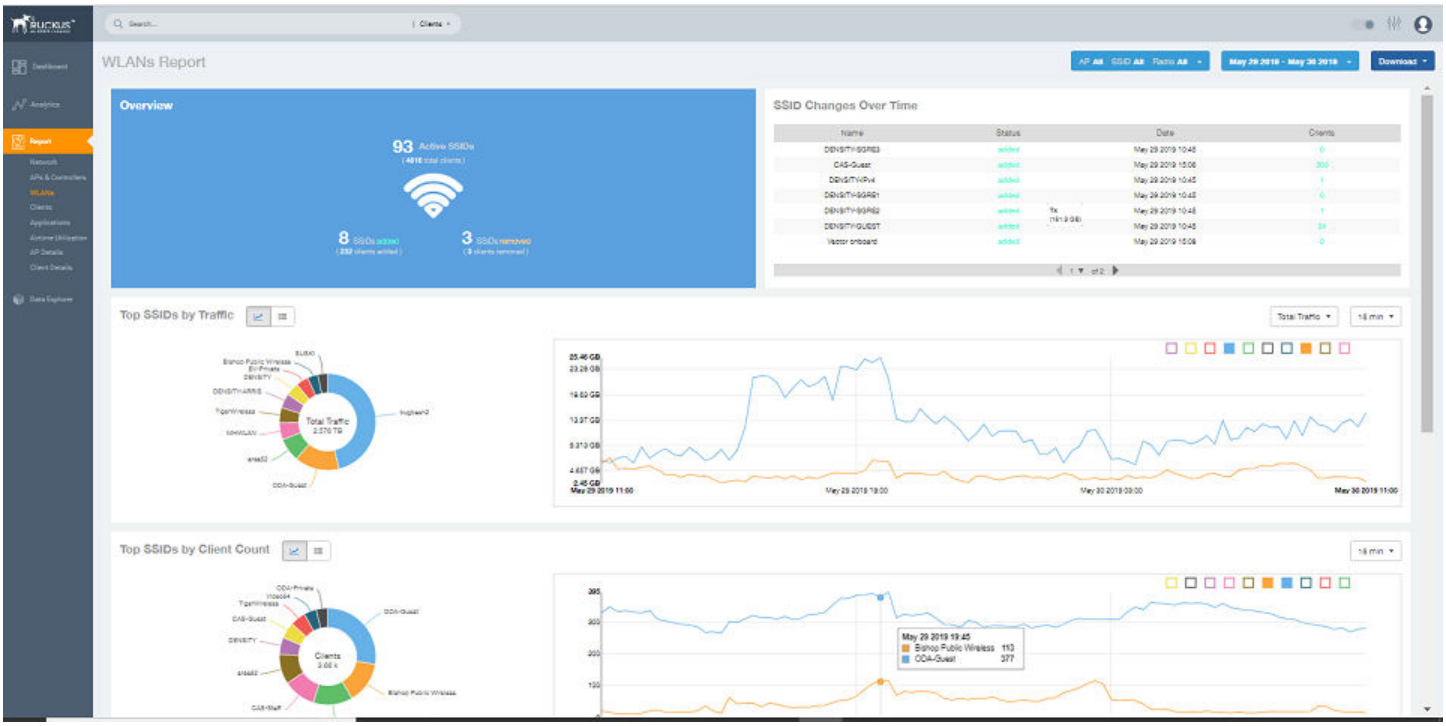
WLAN Report

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 91 WLAN Report (Upper Portion Only)



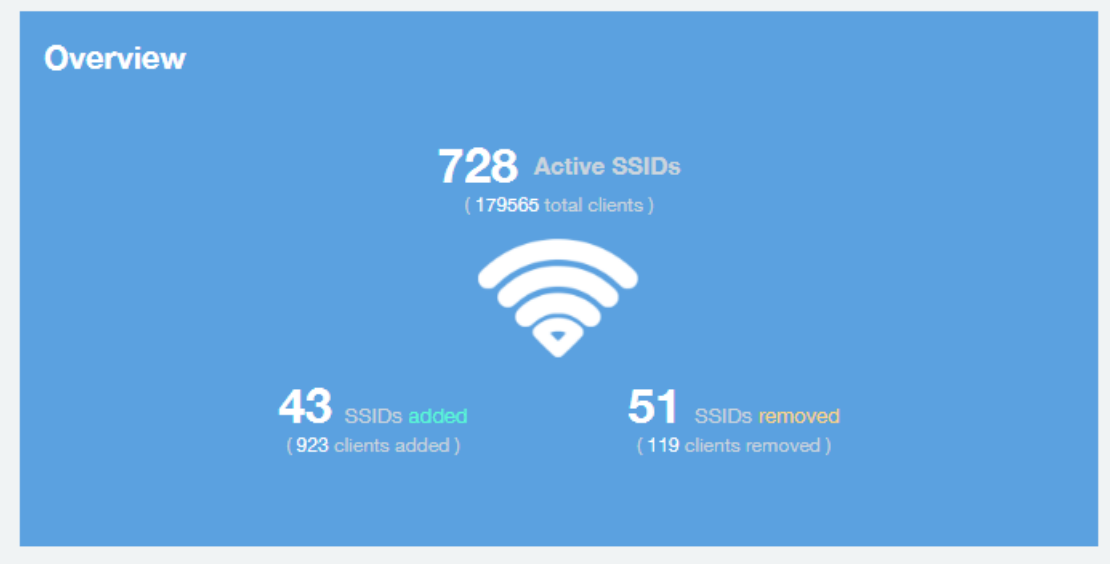
The WLANs Report consists of the following components:

- 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.

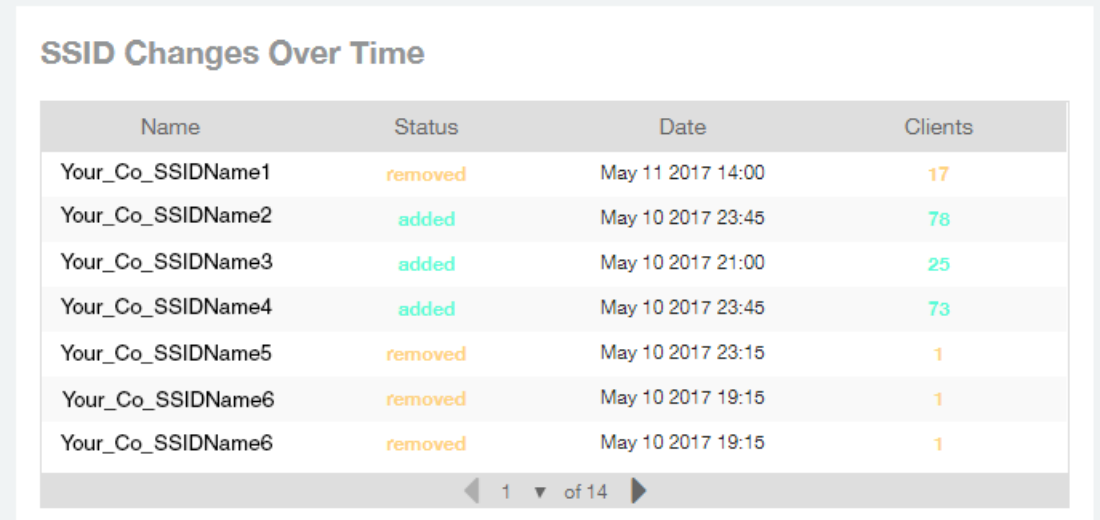
FIGURE 92 WLAN: Overview Tile



SSID Changes Over Time Tile

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

FIGURE 93 WLAN: SSID Changes Over Time Table



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 94 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 95 WLAN: Top SSIDs by Traffic (Table)

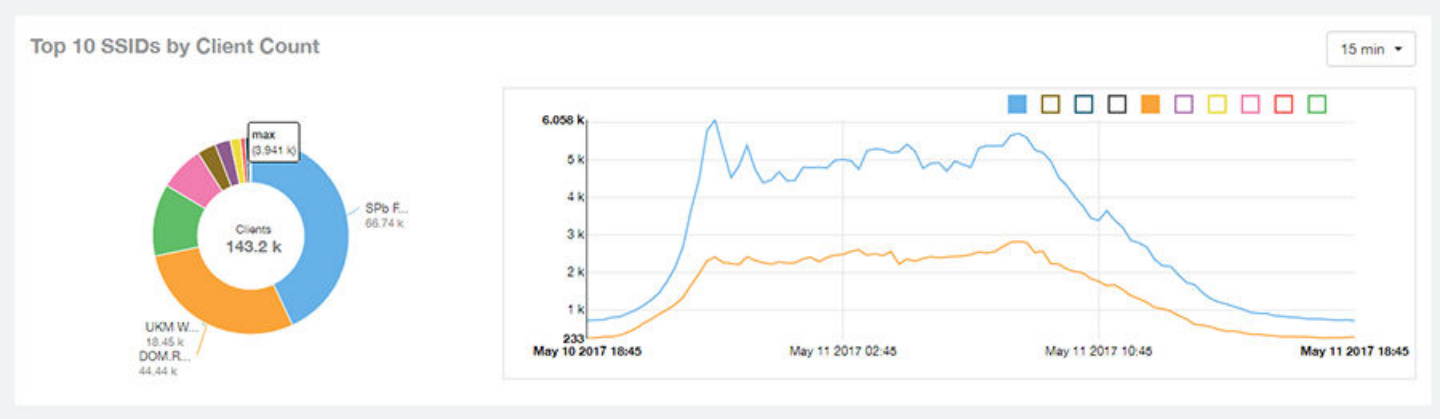
Top SSIDs by Client Count Tile

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 96 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 97 WLAN: Top SSIDs by Client Count (Table)

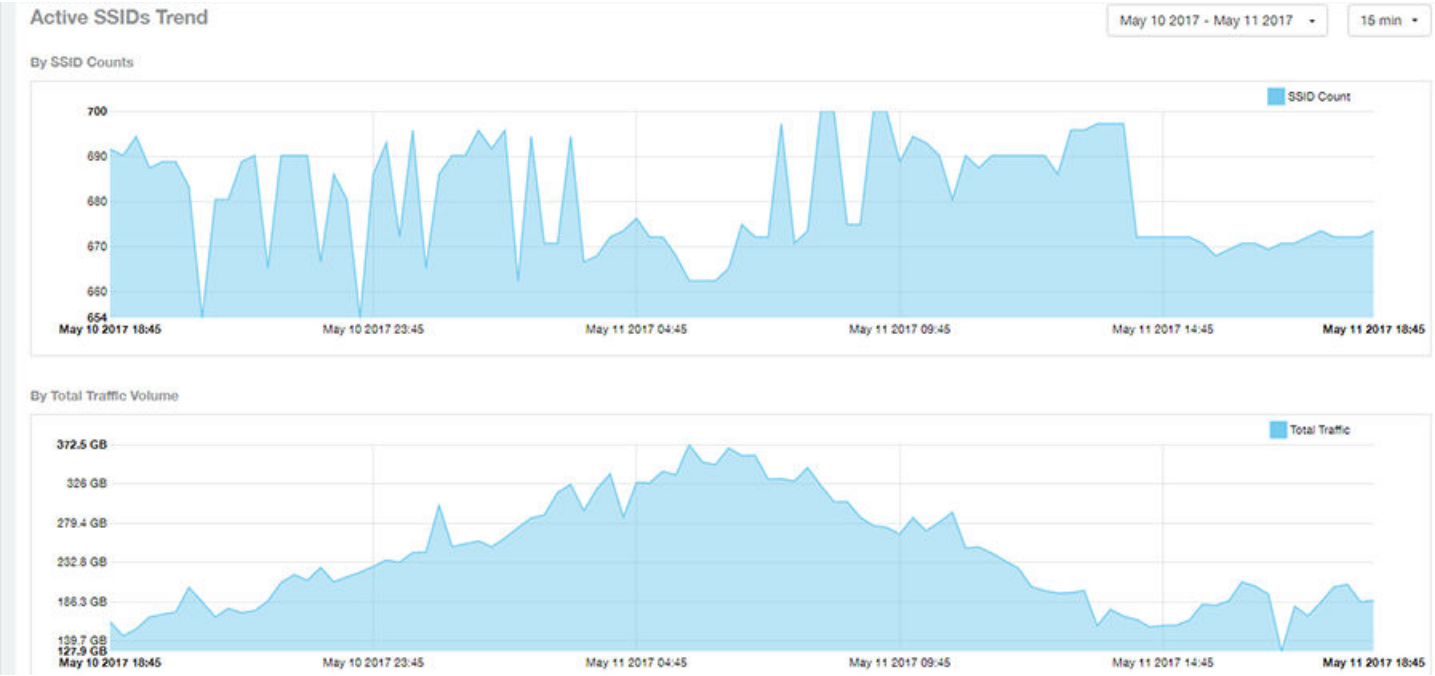
Active SSIDs Trend Graphs

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 98 WLAN: Active SSIDs Trend Graphs



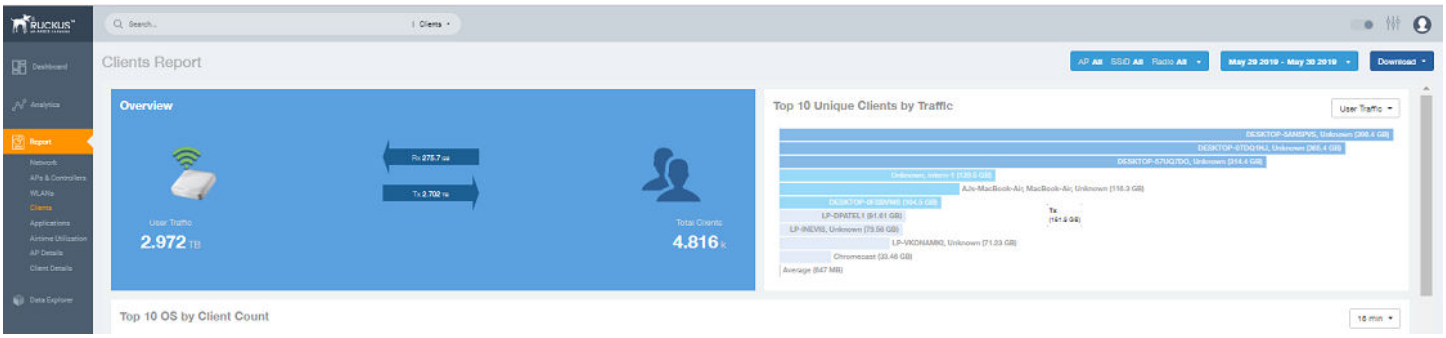
Clients Report

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 99 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

- Clients Details table
- Unique Clients Trend Over Time graphs

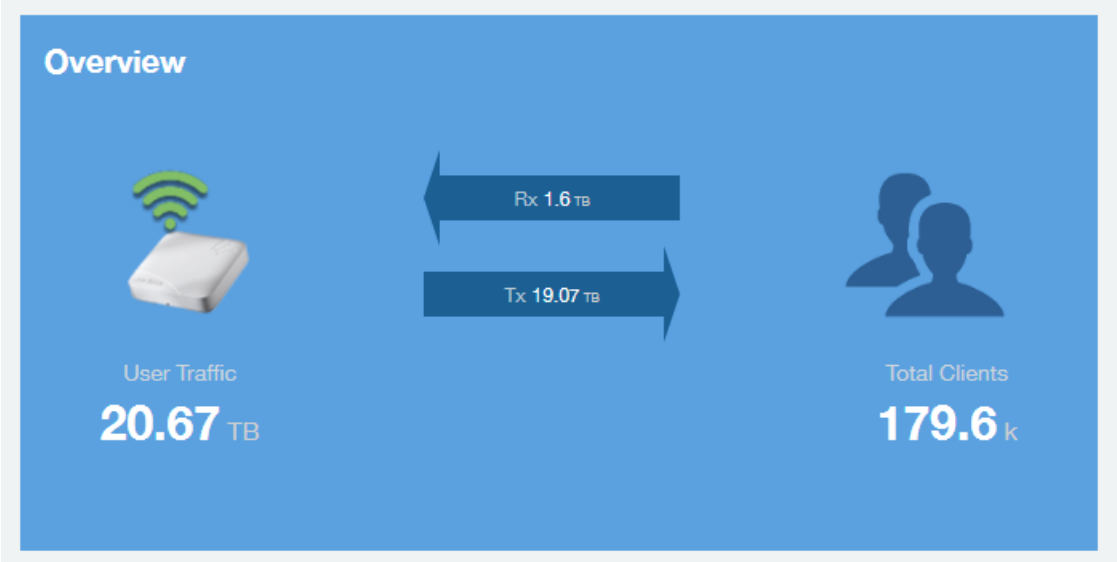
Overview Tile

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

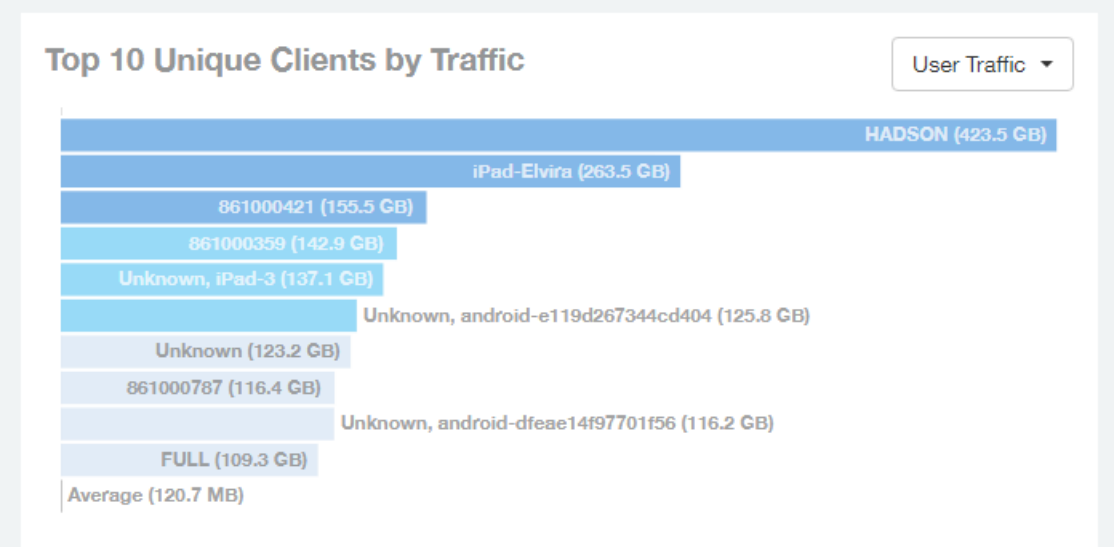
FIGURE 100 Clients: Overview Tile



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 101 Clients: Top 10 Unique Clients by Traffic

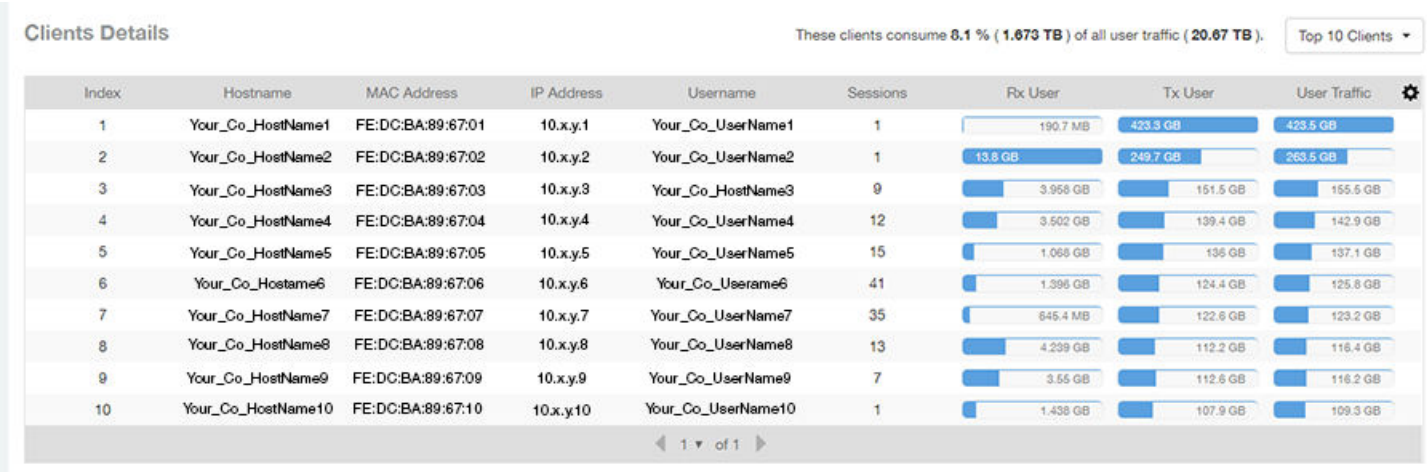


Clients Details

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.

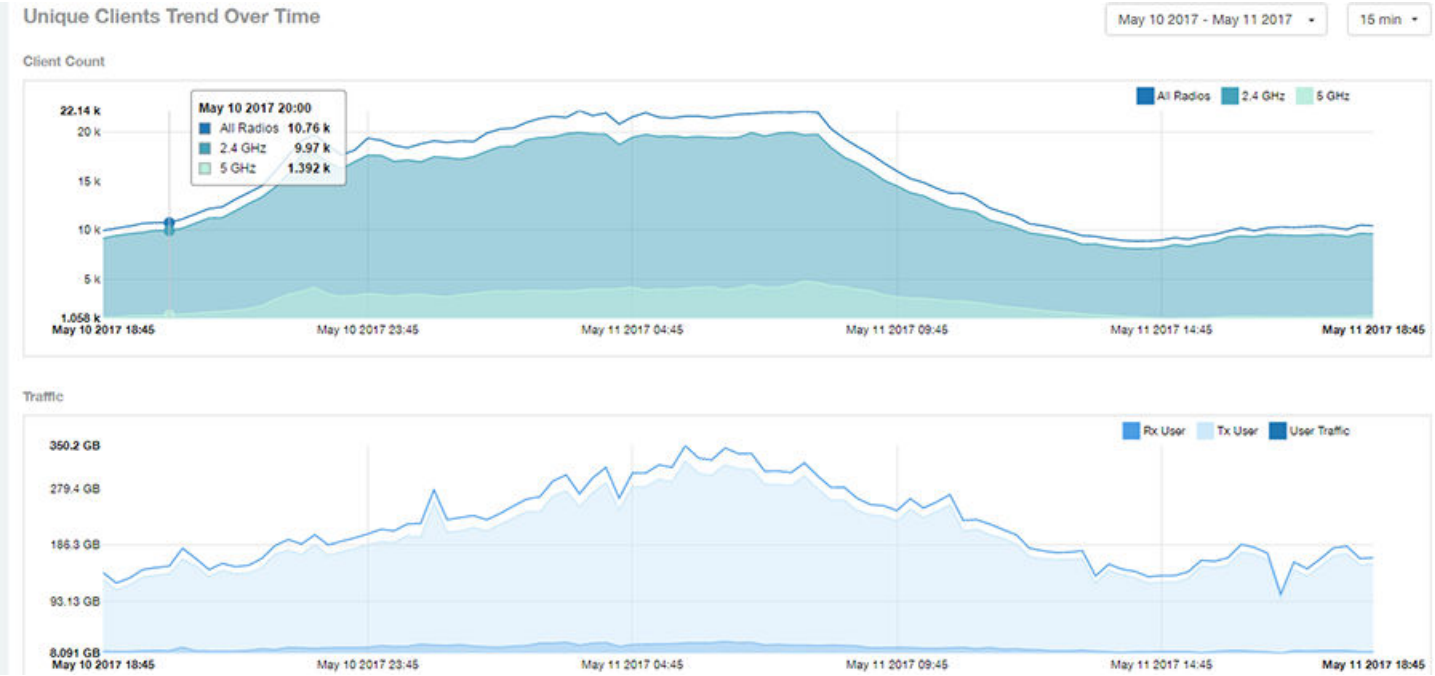
FIGURE 102 Clients: Clients Details Table



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.

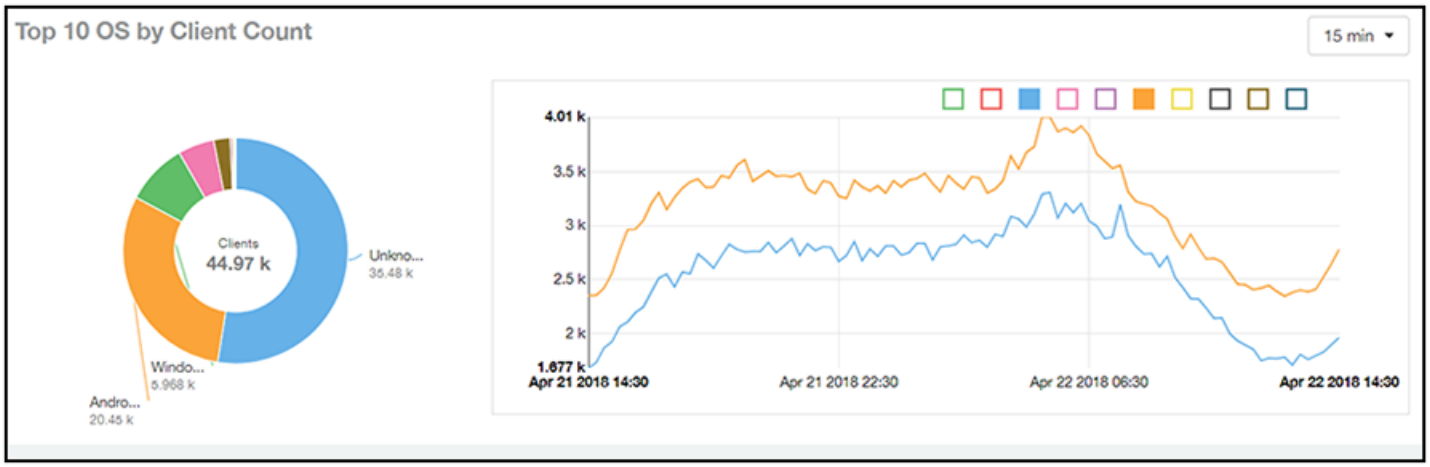
FIGURE 103 Clients: Unique Clients Trend Over Time Graph



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.

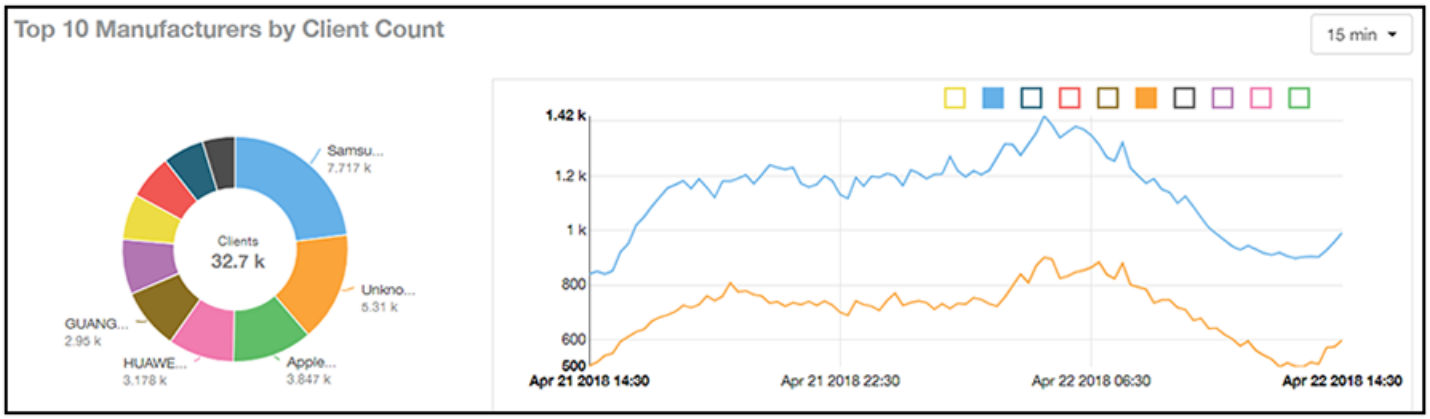
FIGURE 104 Clients: Top 10 OS by Client Count Tile



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.

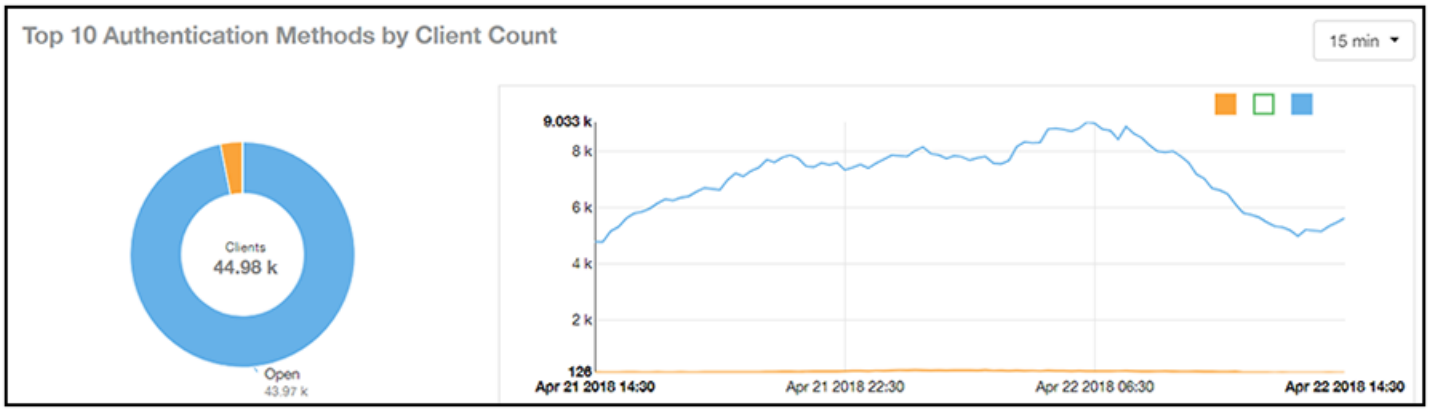
FIGURE 105 Clients: Top 10 Manufacturers by Client Count Tile



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 106 Clients - Top 10 Authentication Methods by Client Count Tile



Client Health Dashboard

Client Health Report

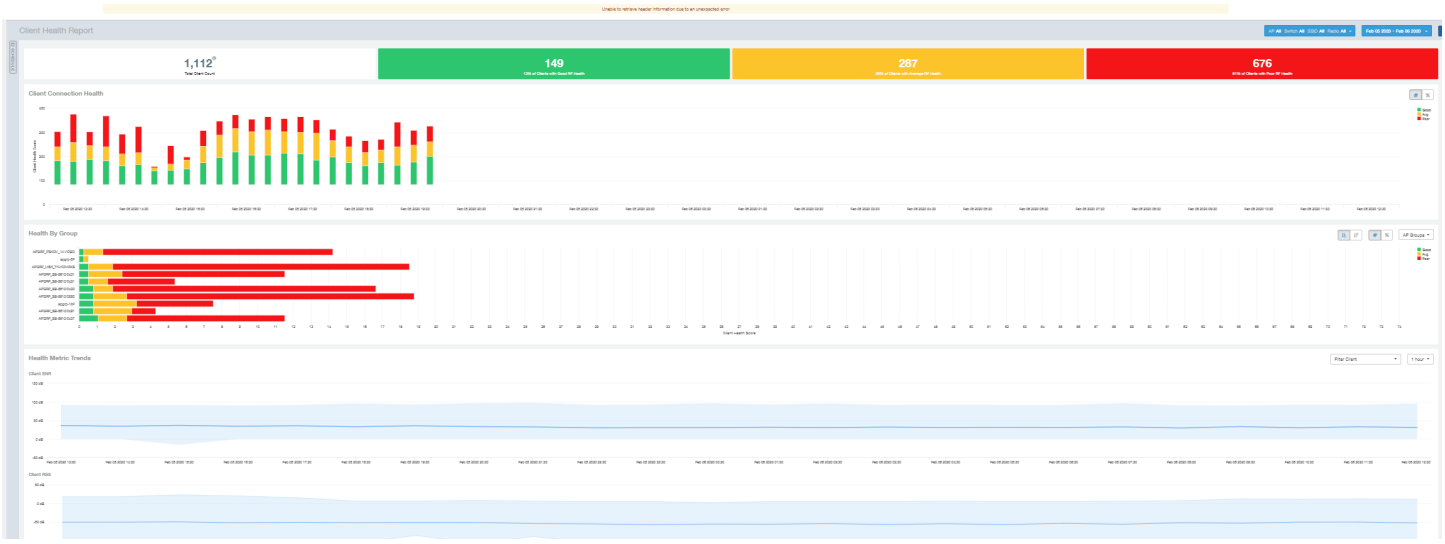
The Client Health Report page calculates and displays a client health score to quickly assess the health of client connections.

The score is determined by the following metrics:

- RSSI
- SNR
- Throughput

- MCS (for transmission)

FIGURE 107 Client Health Report (Upper Portion Only)

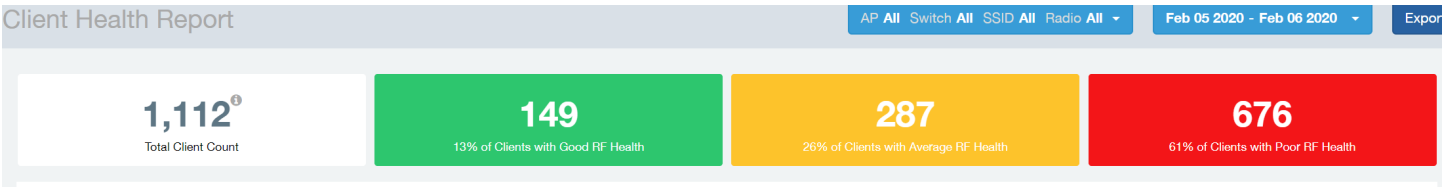


The Client Health Report consists of the following components:

- 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.



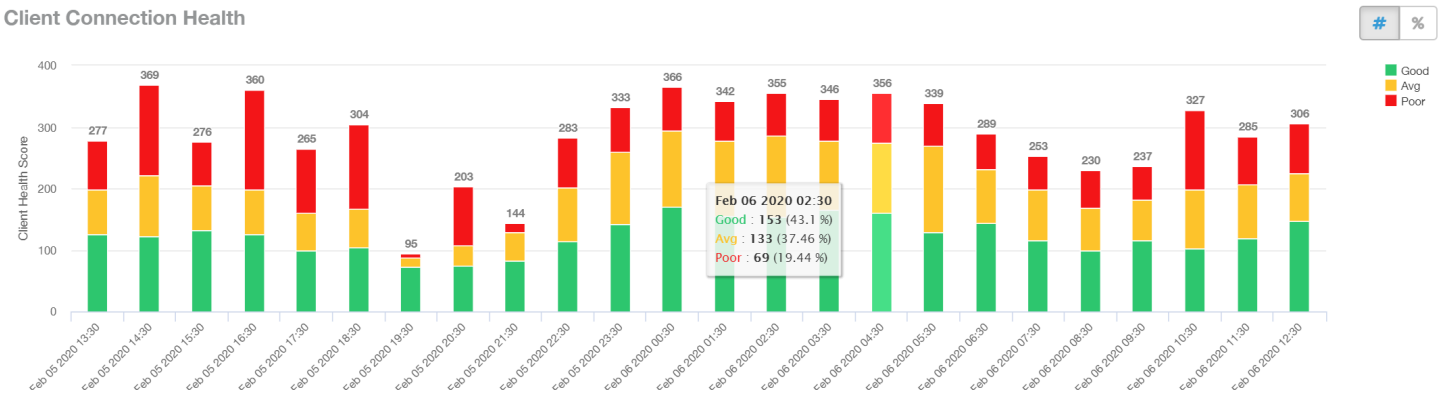
The green box shows the number of clients with good RF health. The yellow box shows the number fo clients with average RF health and the red box displays the number of clients with poor RF heath. The numbers are determined by the threshold that you set as per your expectations of client health in the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

For example, here, out fo 1112 clients in total, 149 have good RF heath, 287 have average RF health, and 676 clients ahve 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 108 Client Health Score: Client Connection Health

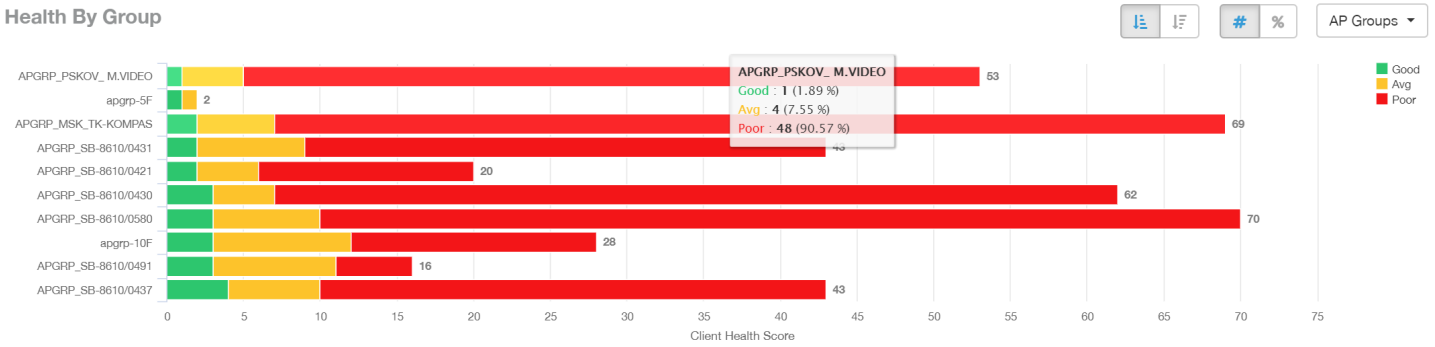


You can toggle the boxes on and off to display or not display clients classified by their score. For example, to only view the clients with a good score, you can disable the yellow and red boxes; you will only see the clients with a good RF health in the graph.

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 drop-down, stacked color bars are displayed depicting the client score for the group selected.

FIGURE 109 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.

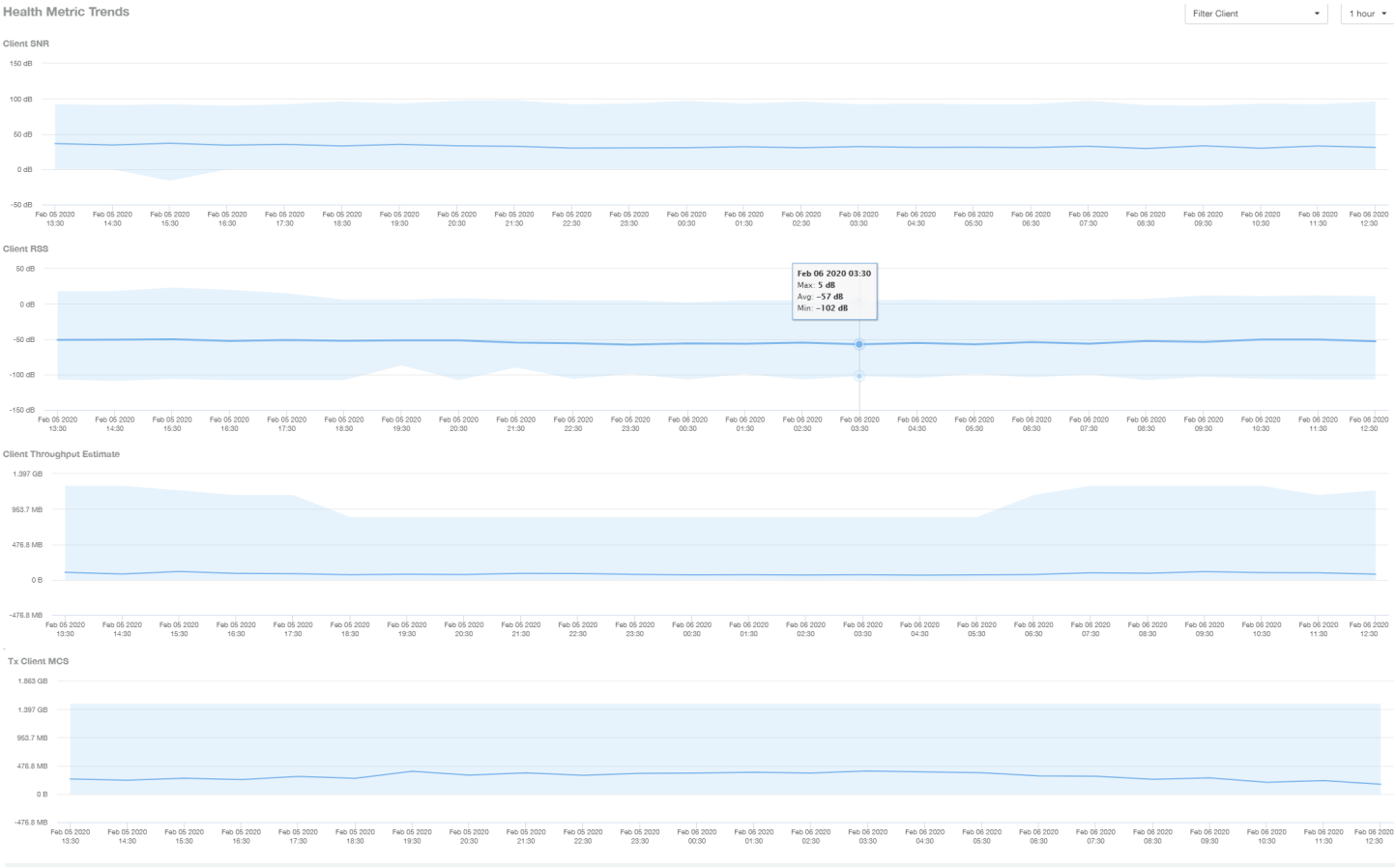
The ascending and descending order icons sort the groups as groups with highest percentage or count of good clients, and highest percentage or count of poor clients, respectively.

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 graphgs 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 110 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.

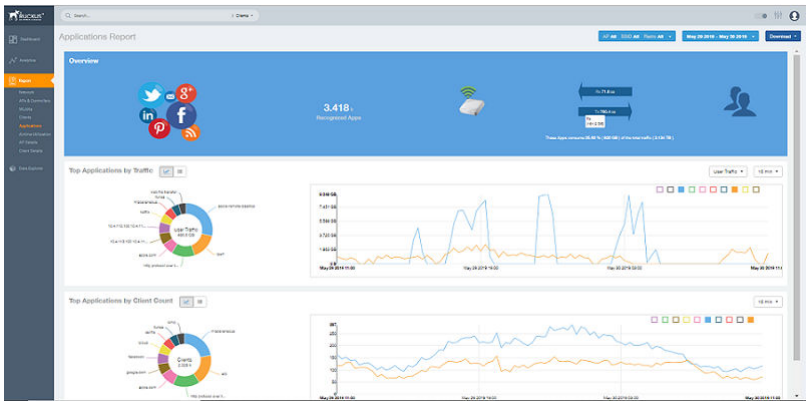
Applications Report

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 111 Applications Dashboard (Upper Portion Only)



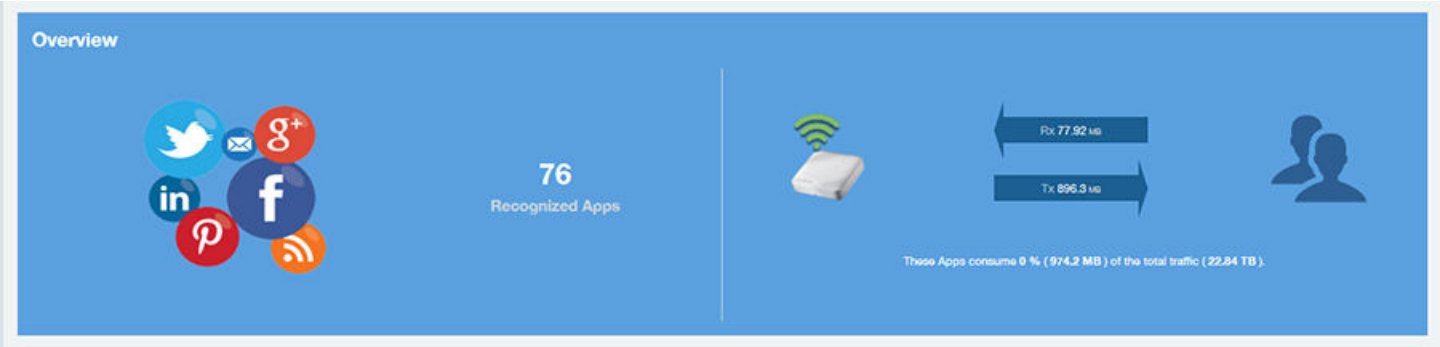
Overview Tile

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

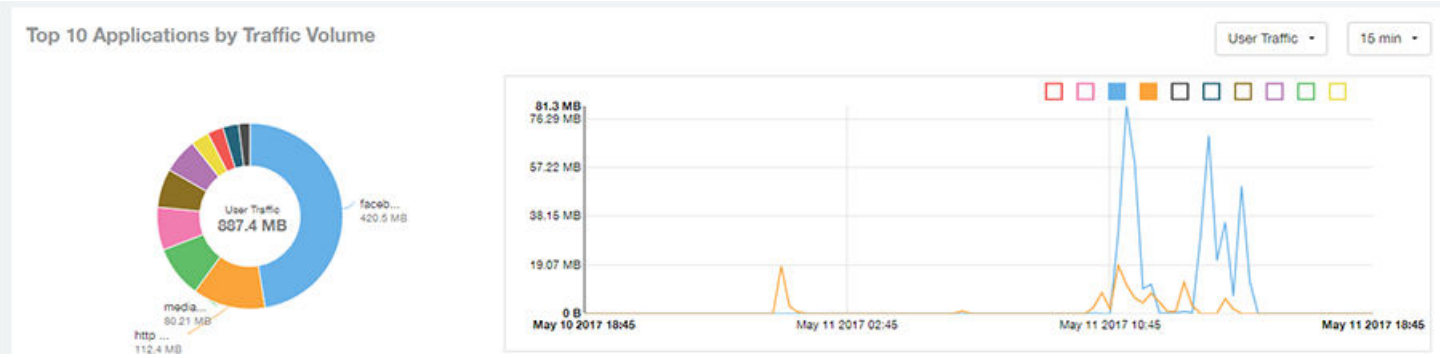
FIGURE 112 Applications: Overview Tile



Top Applications by Traffic

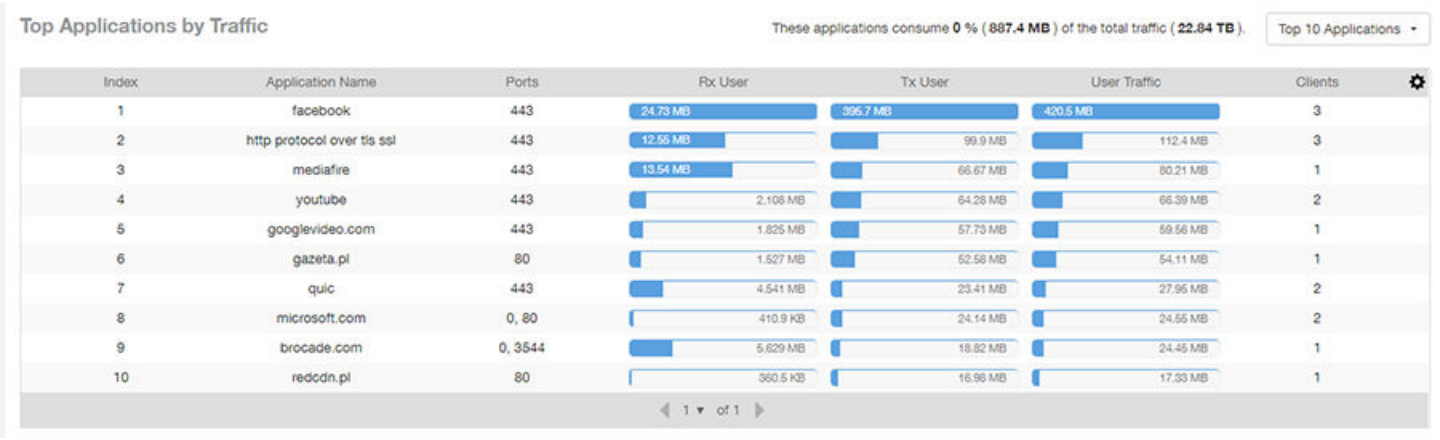
The **Top Applications by Traffic** donut chart and graph of the **Applications Report** display the top applications with the largest traffic in the network, along with the received and transmitted traffic.

FIGURE 113 Applications: Top Applications by Traffic Tile



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

FIGURE 114 Applications: Top Applications by Traffic Table

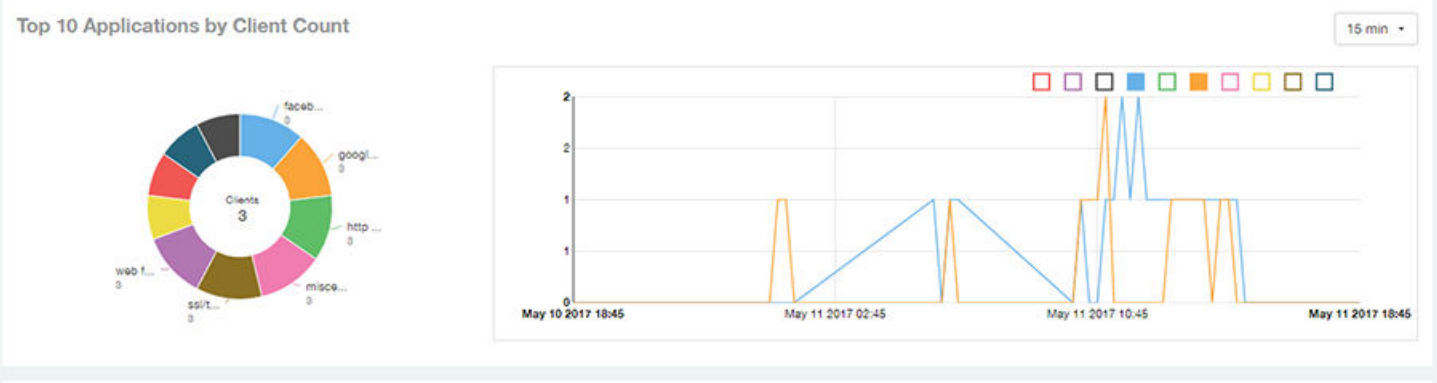


You can view the received and transmitted traffic volumes based on the Rx and Tx filter. In the graph, click any of the colored squares to display the corresponding application details in the line graph. If you pause the pointer over the line graph, an information box is displayed containing the selected 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 115 Applications - Top Applications by Client Count (chart)

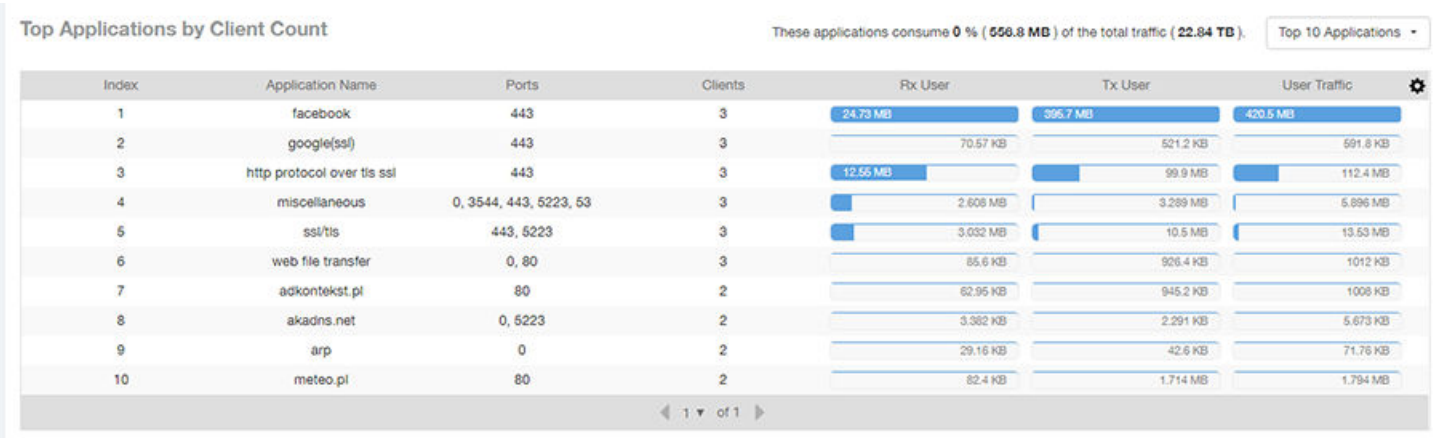


Use the chart and table icons ( ) to toggle between the chart and table views.

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 116 Applications: Top Applications by Client Count Table



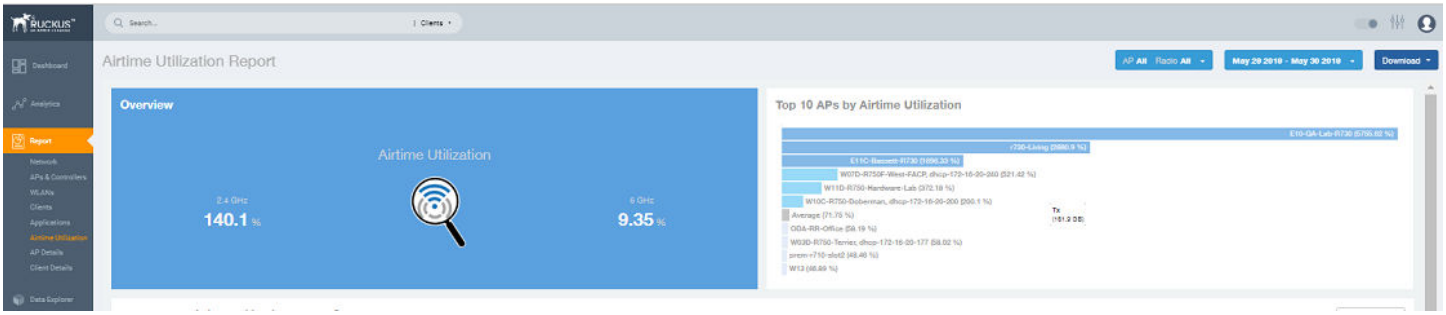
Airtime Utilization Report

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.

FIGURE 117 Airtime Utilization Report (Upper Portion Only)



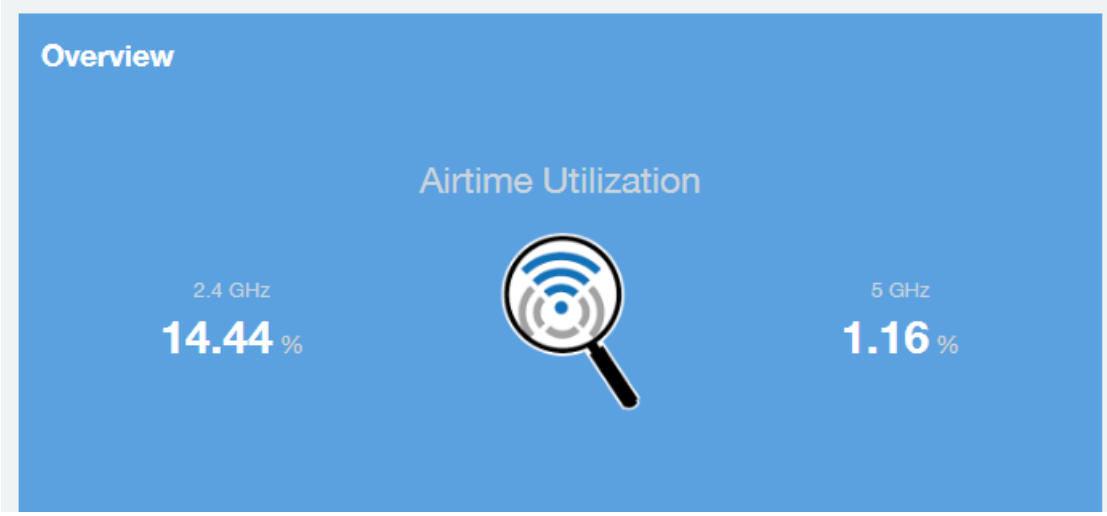
The Airtime Utilization Report consists of the following components:

- 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.

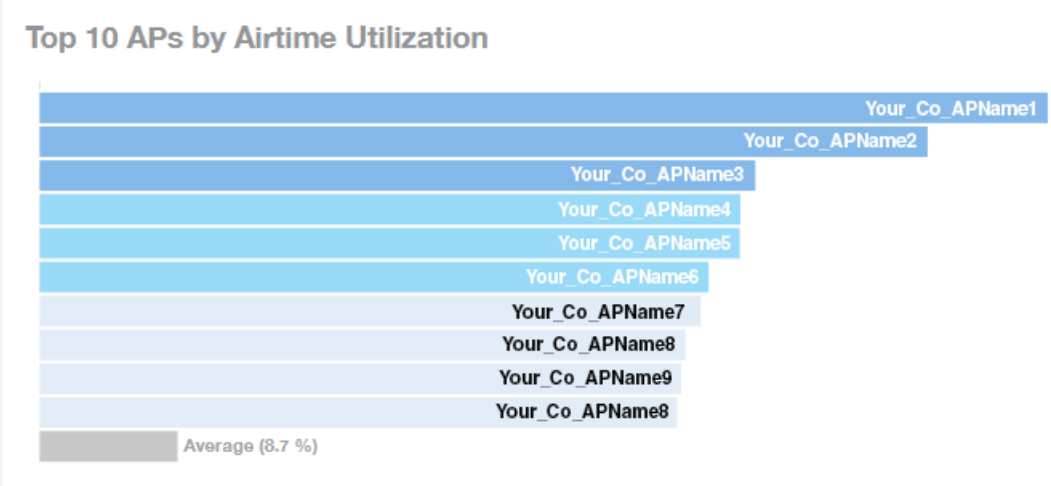
FIGURE 118 Airtime Utilization: Overview Tile



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 119 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 120 Top APs by Airtime Utilization for 2.4 GHz Table

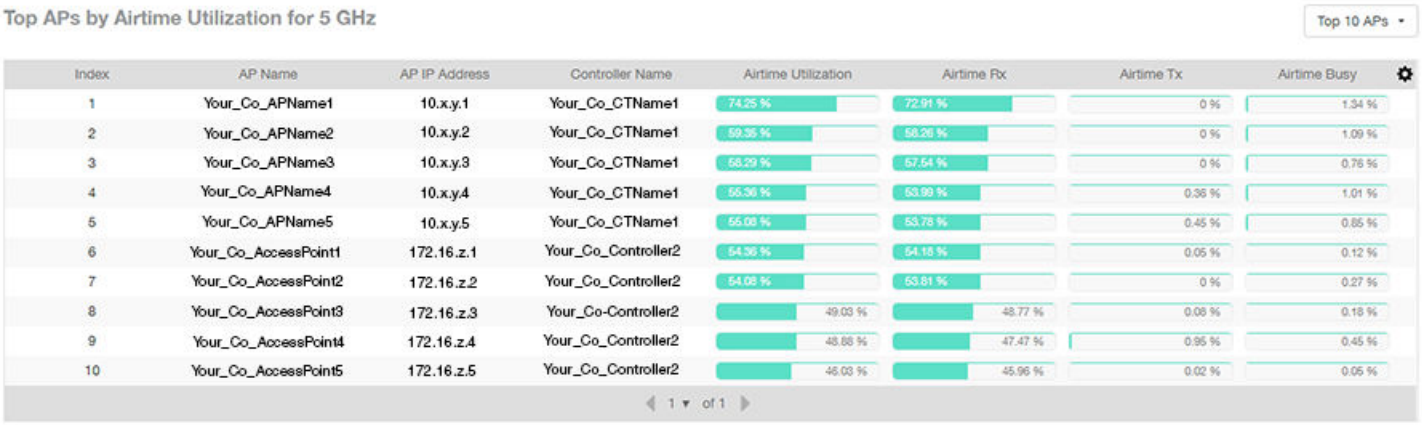
Top APs by Airtime Utilization for 5 GHz Table

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.

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.

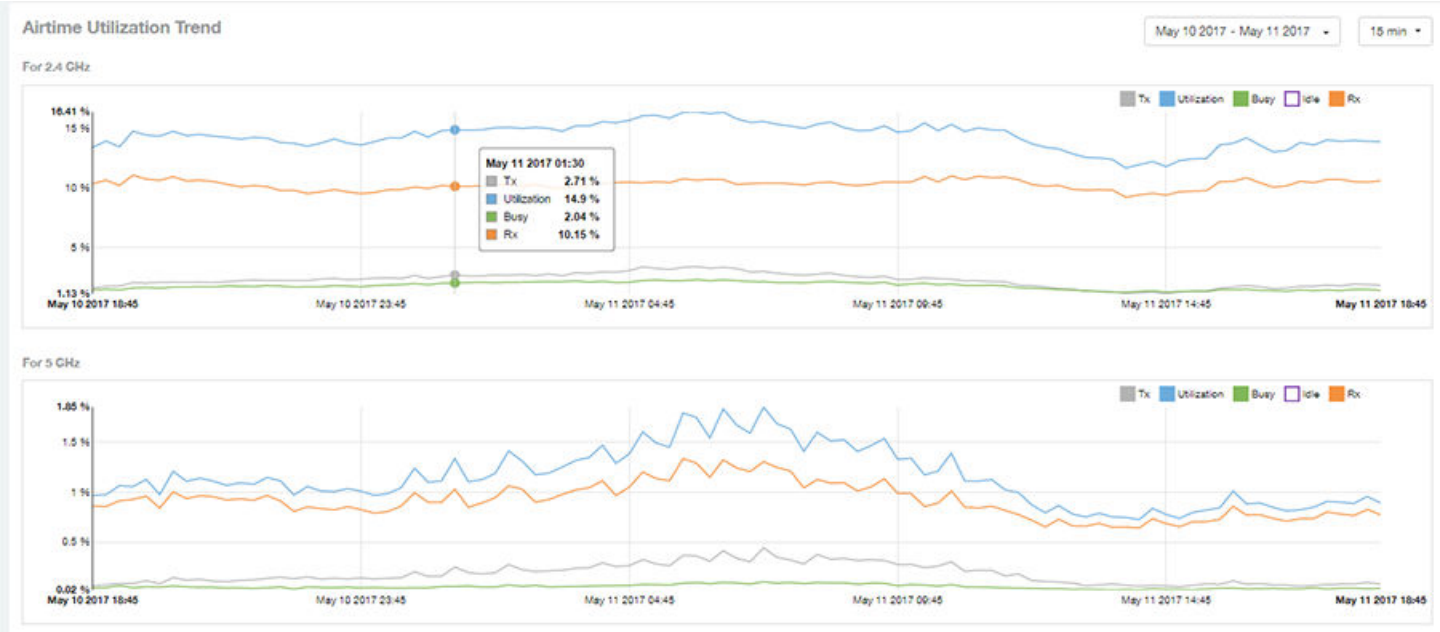
FIGURE 121 Top APs by Airtime Utilization for 5 GHz Table



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.

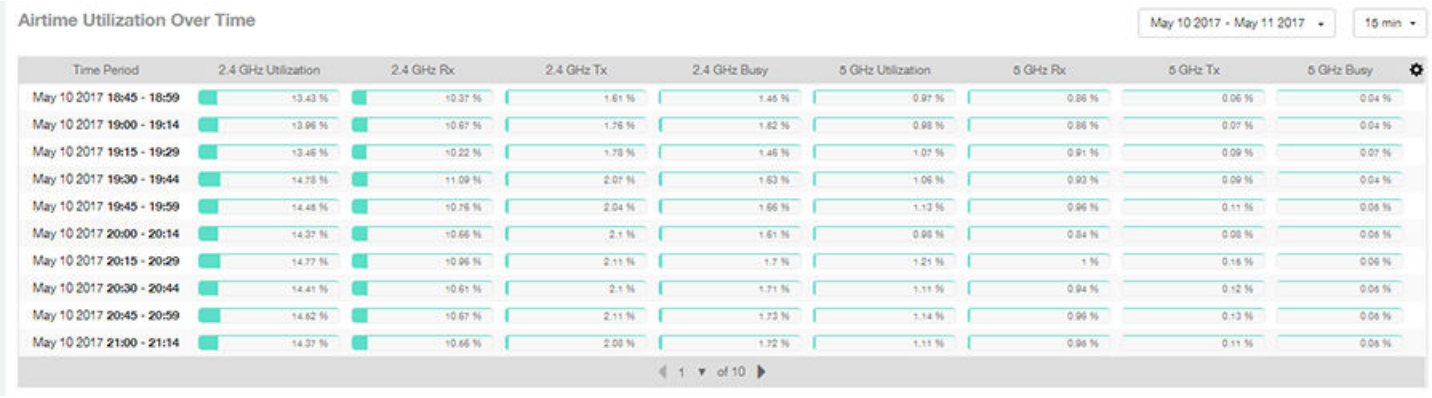
FIGURE 122 Airtime Utilization Trend Graph Trends



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 123 Airtime Utilization Over Time Table



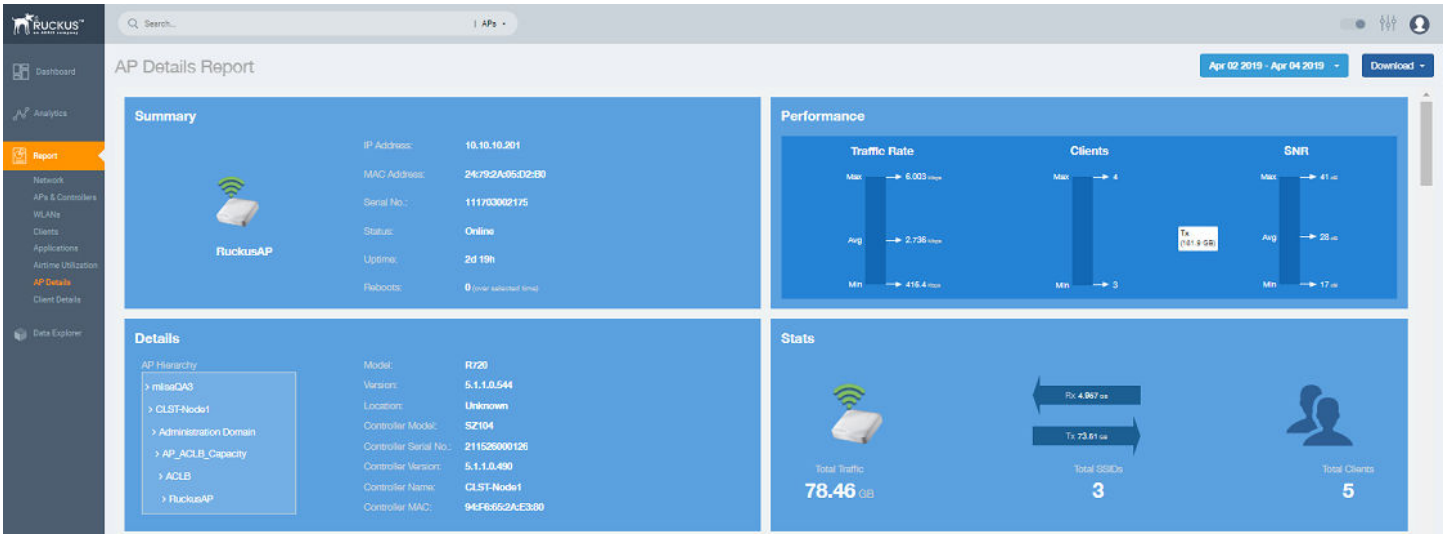
AP Details Report

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 124 AP Details Report (Upper Portion Only)



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

- Summary tile

- 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 125 AP Details: Summary Tile

Performance Tile

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

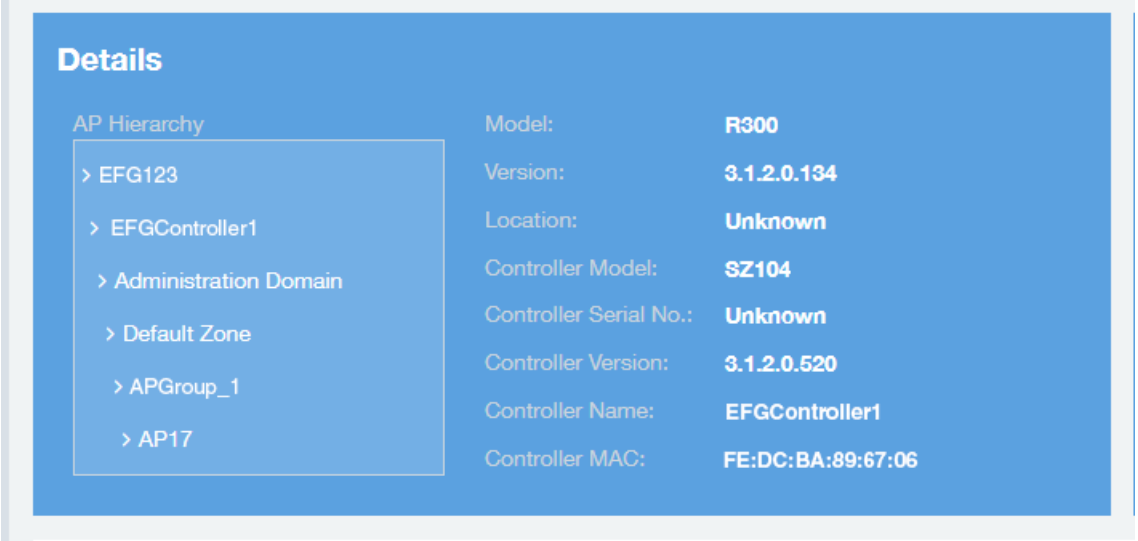
FIGURE 126 AP Details: Performance Tile

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 127 AP Details: Details Tile



Stats Tile

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

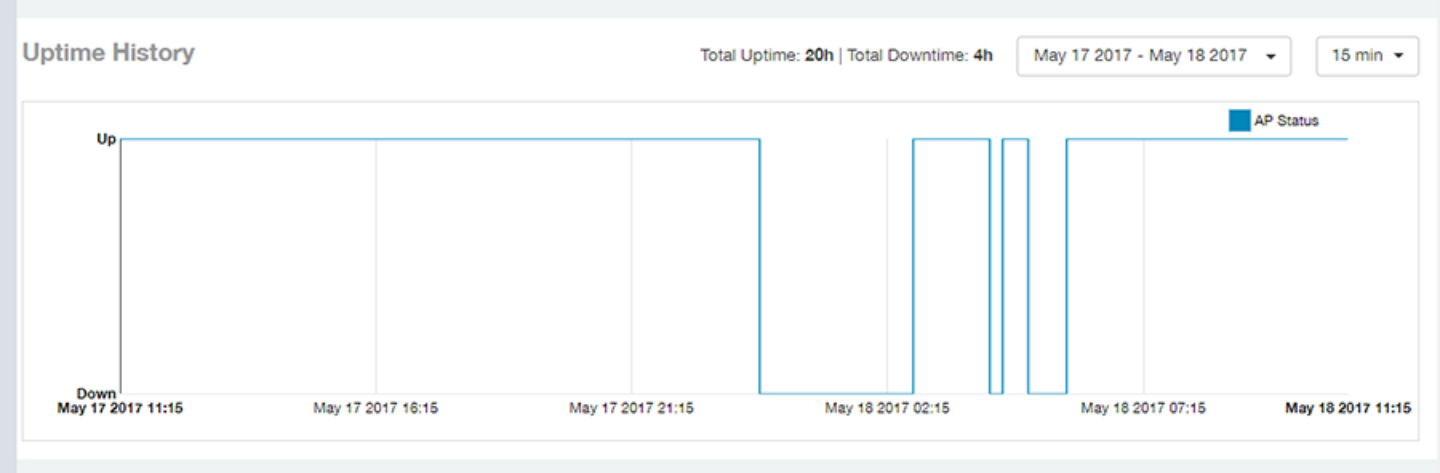
FIGURE 128 AP Details: Stats Tile

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 129 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 130 AP Details: Traffic Trend Graphs

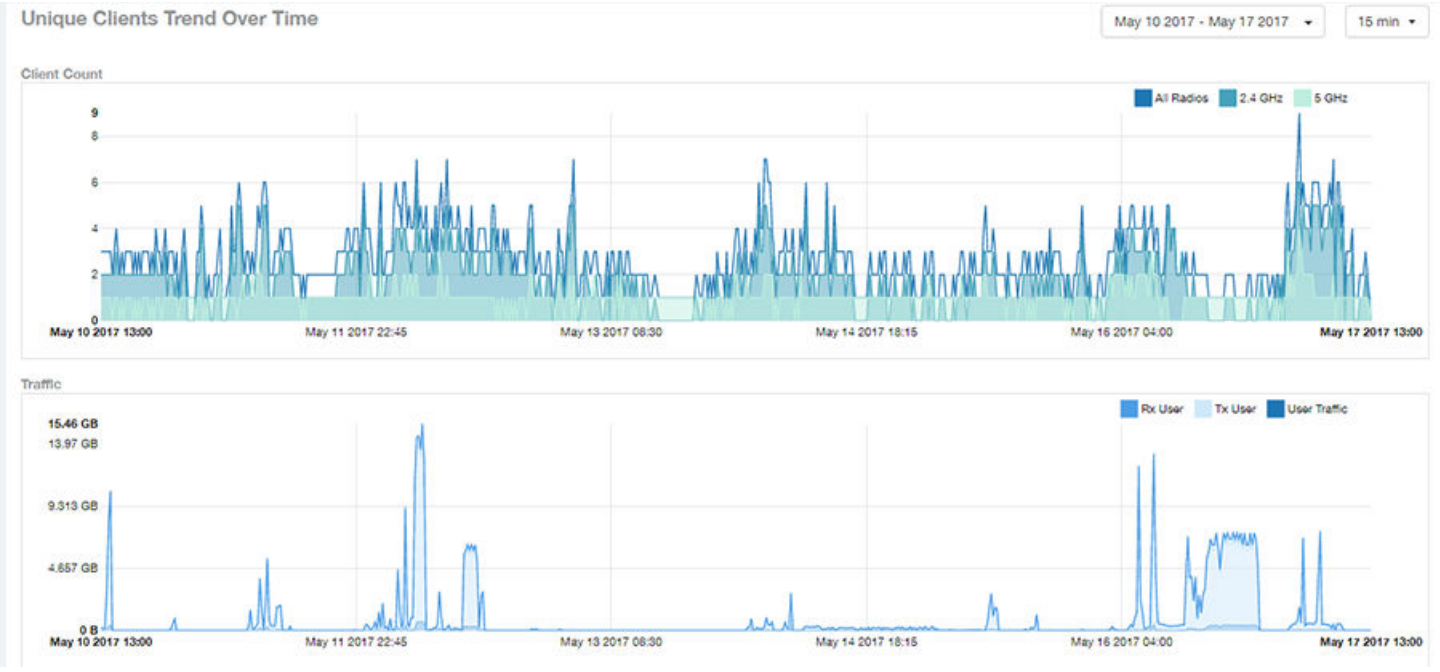
Unique Clients Trend Over Time Graphs

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 131 AP Details: Unique Clients Trend Over Time Graphs



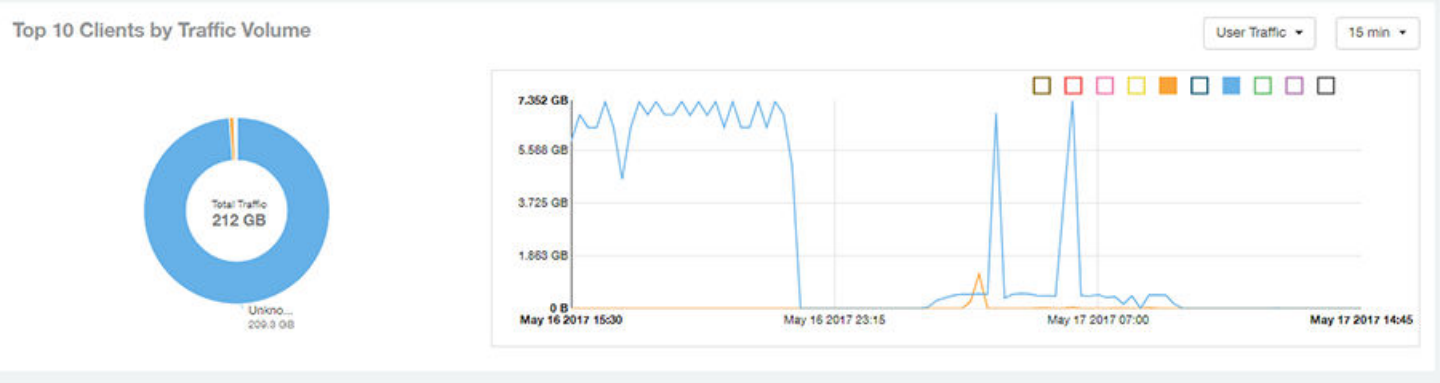
Top 10 Clients by Traffic Volume Tile

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 132 AP Details: Top 10 Clients by Traffic Volume Tile



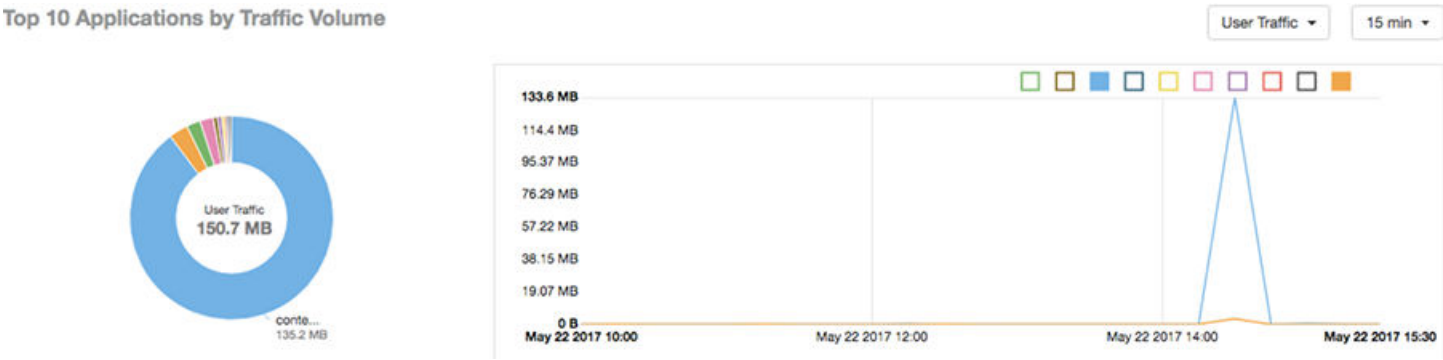
Top 10 Applications by Traffic Volume Tile

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 133 AP Details: Top 10 Applications by Traffic Volume Tile

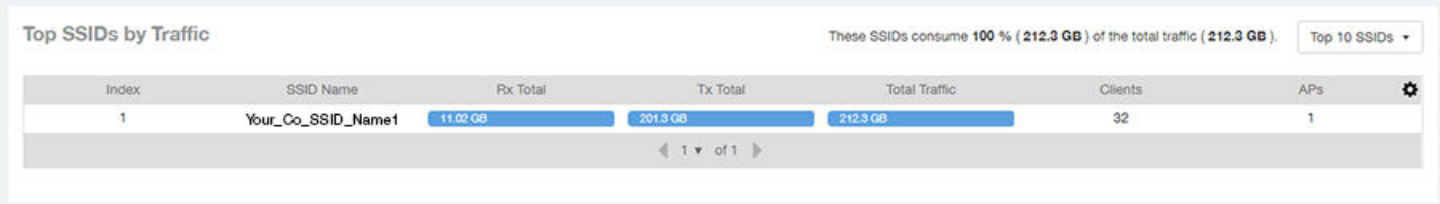


Top SSIDs by Traffic Table

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 134 AP Details: Top SSIDs by Traffic Table



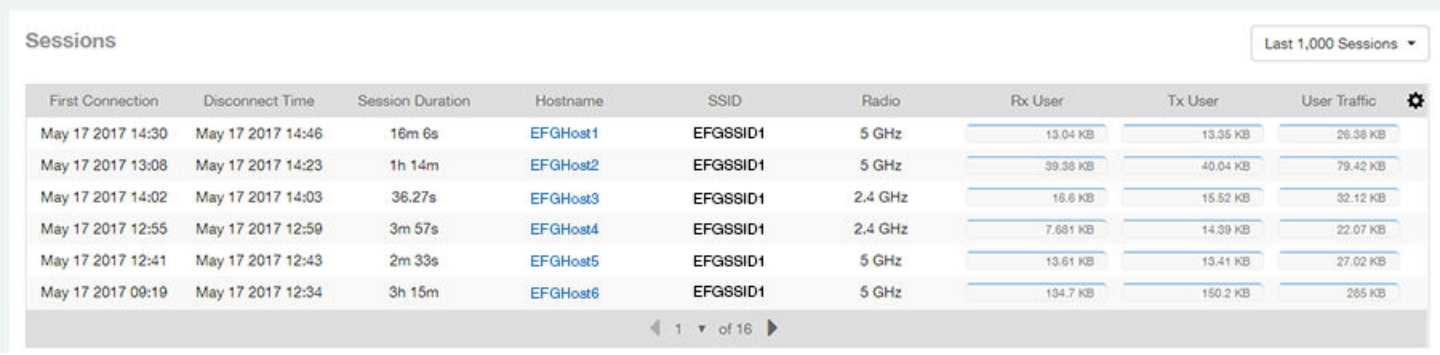
Sessions Table

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 135 AP Details: Sessions Table



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 136 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.

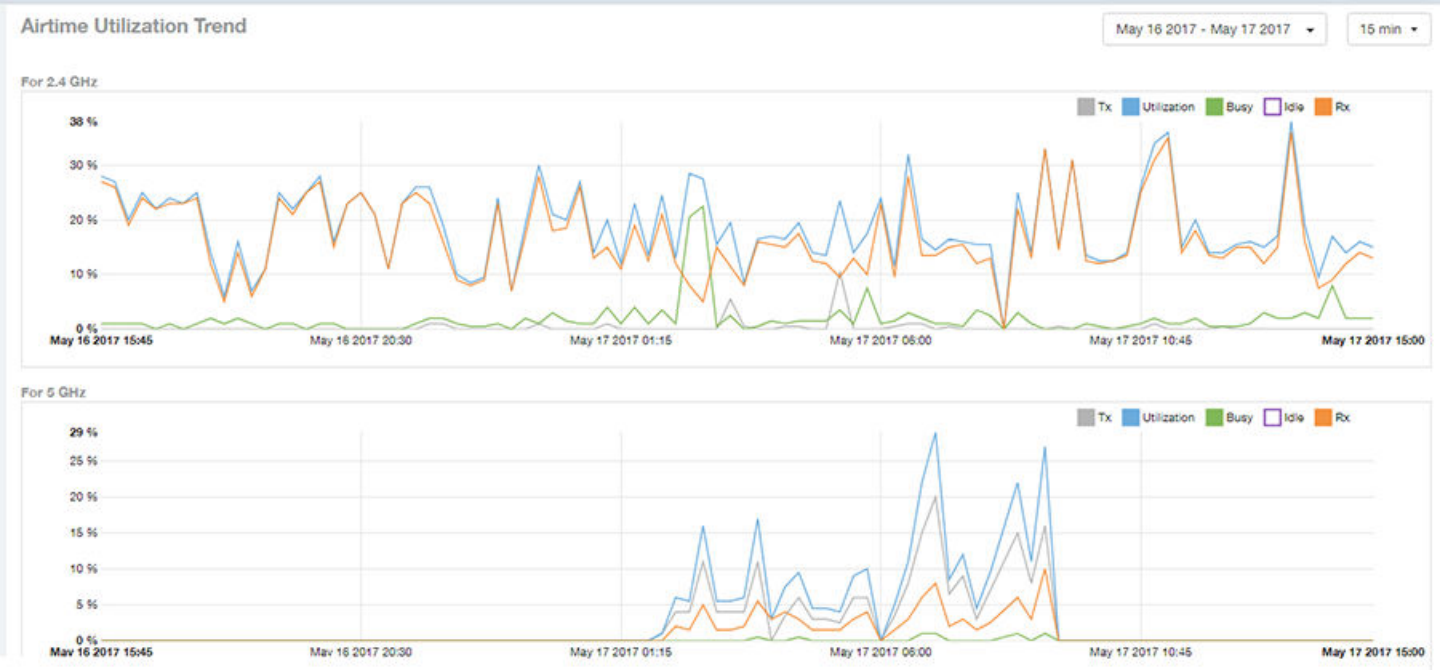
FIGURE 137 AP Details: SNR Trend Graph

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 138 AP Details: Airtime Utilization Trend Graphs



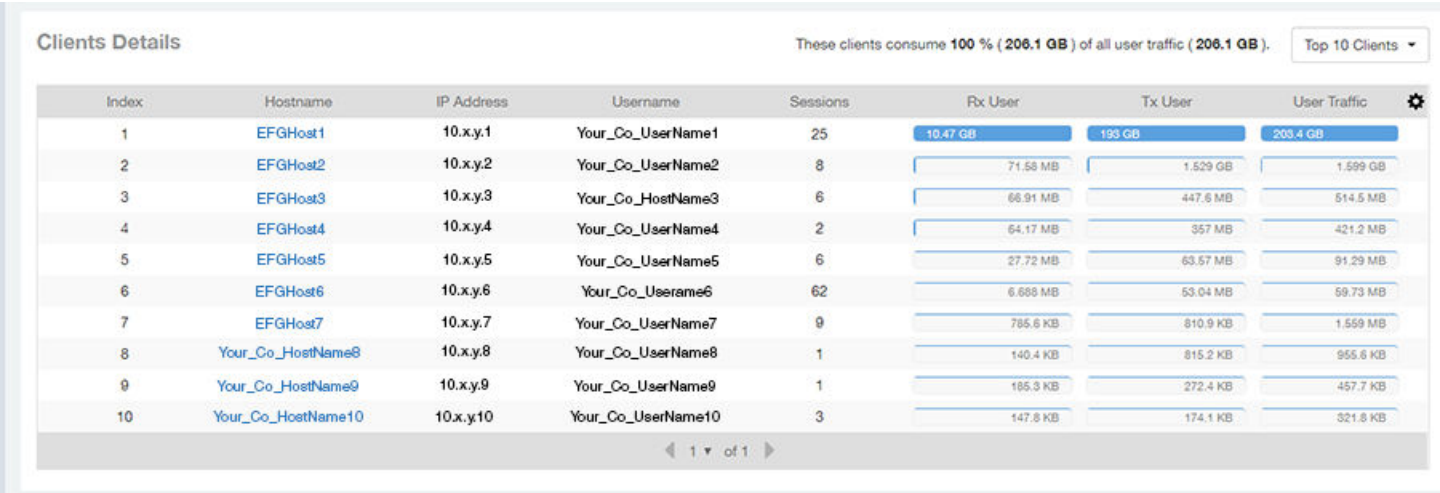
Clients Details Table

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 139 AP Details: Clients Details Table



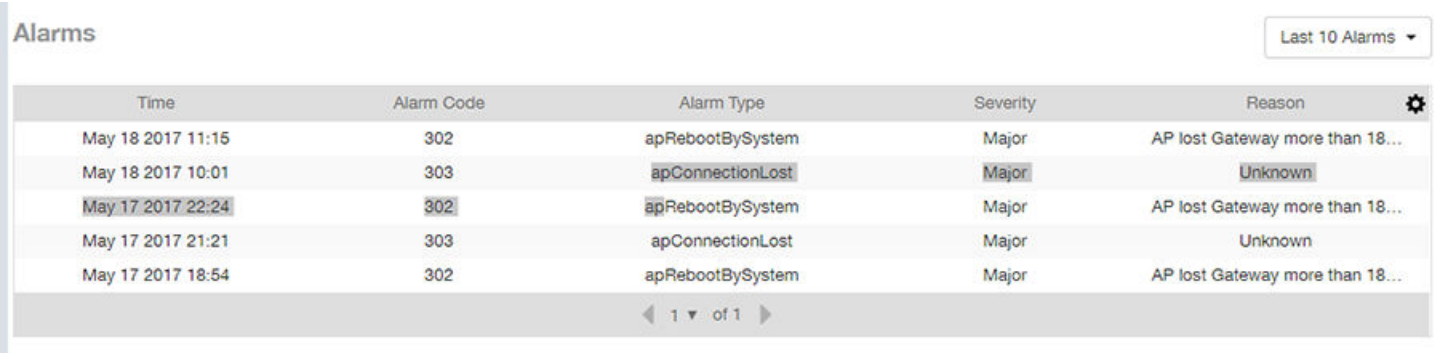
Alarms Table

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 140 AP Details: Alarms Table



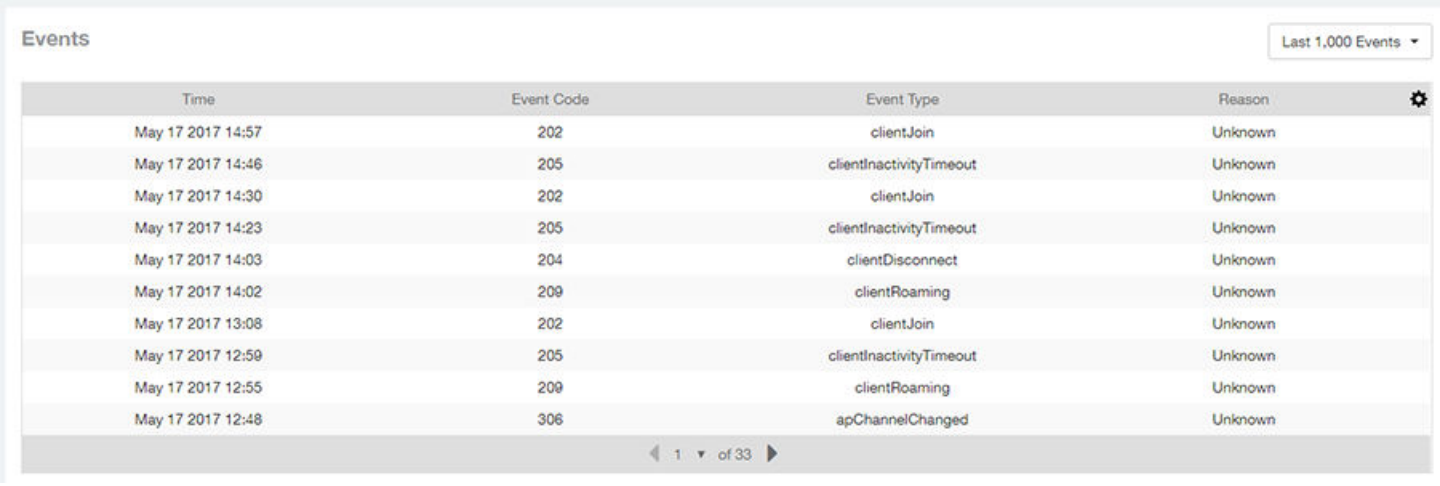
Events Table

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 141 AP Details: Events Table



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.

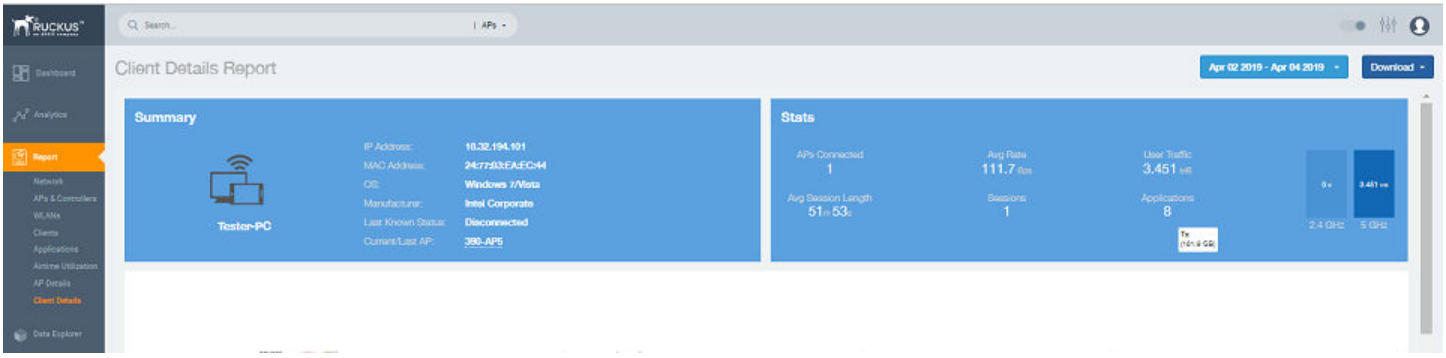
Client Details Report

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 142 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.

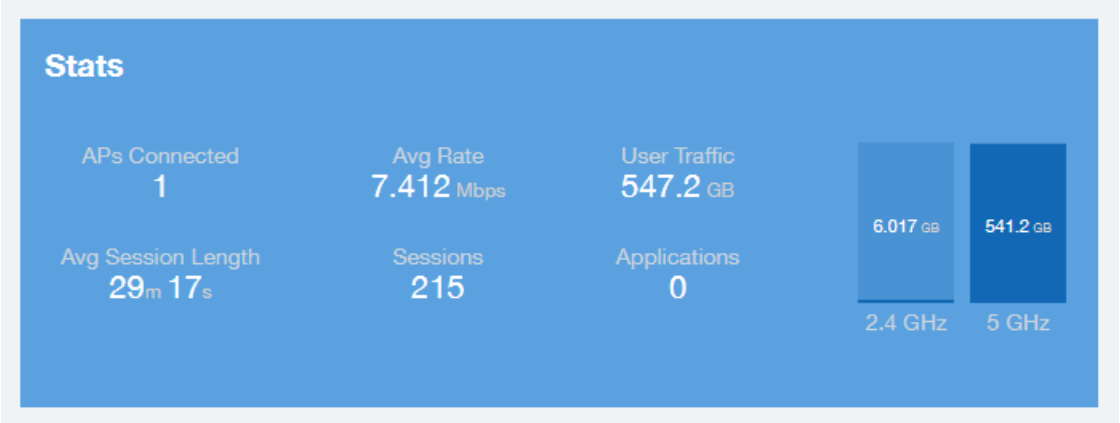
The hostname for the client shown in this example is XYZ123.

FIGURE 143 Client Details - Summary

Stats Tile

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

FIGURE 144 Client Details - Stats



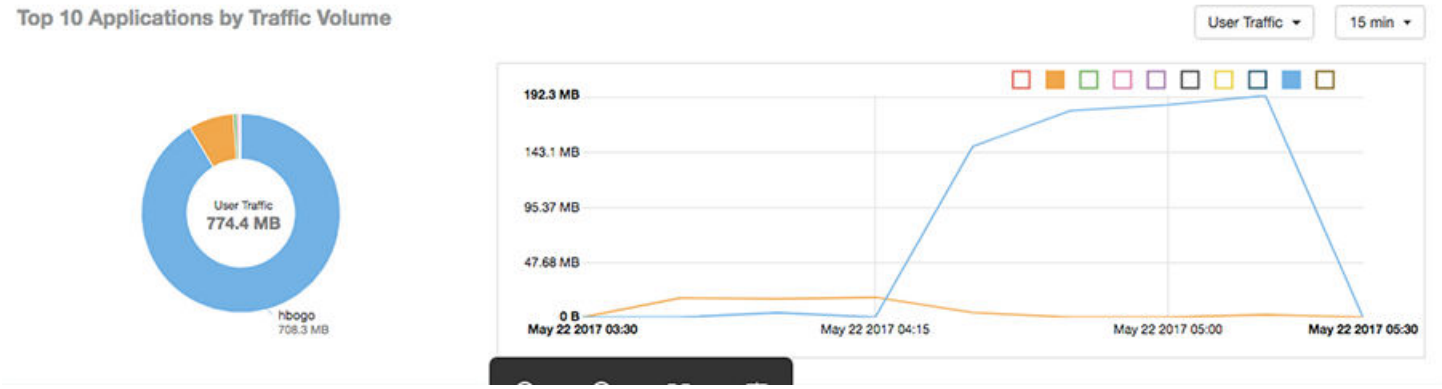
Client Details Stats

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 145 Client Details: Top 10 Applications by Traffic Volume Tile

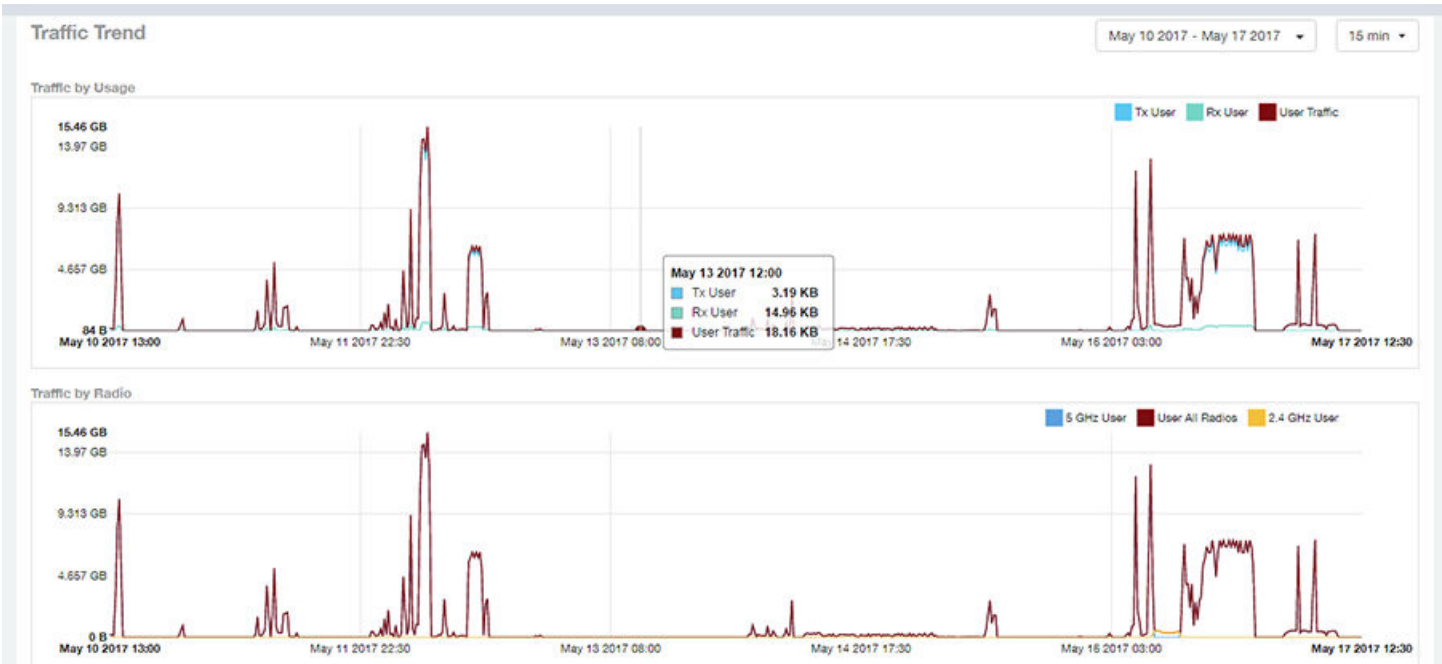


Traffic Trend Tile

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 146 Client Details - Traffic Trend Graphs

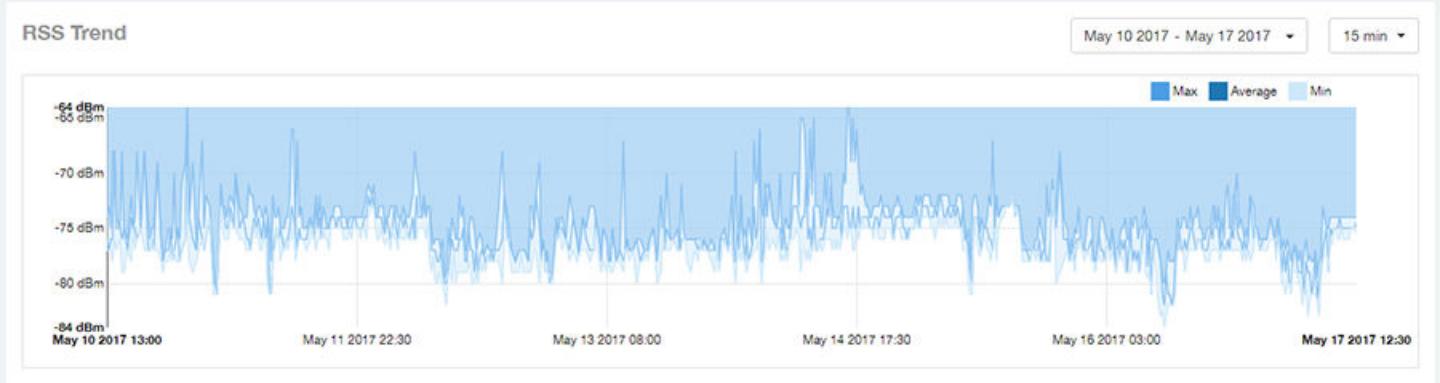


RSS Trend Tile

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 147 Client Details - RSS Trend Graph

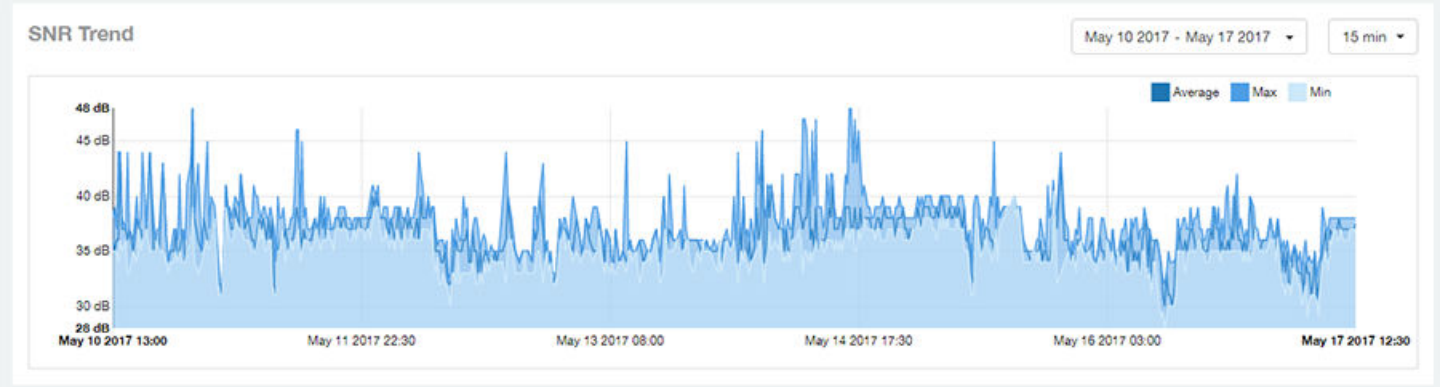


SNR Trend Tile

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 148 Client Details - SNR Trend Graph



Sessions tile

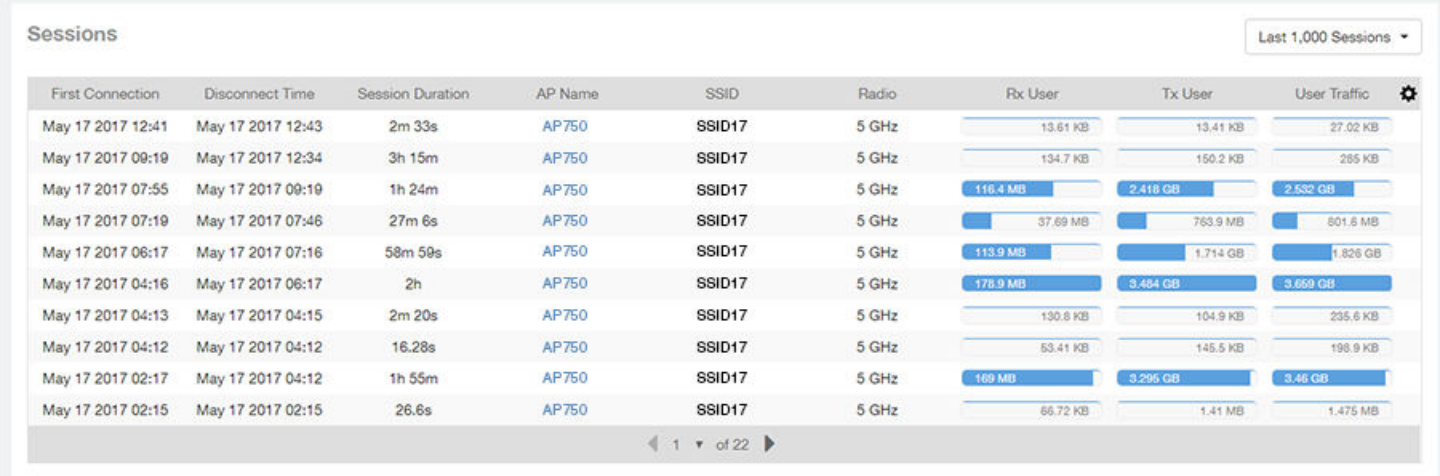
The Sessions table of the Client Details report provides details for sessions between this client and associated access points.

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 149 Client Details: Sessions Table



Switch Details Report Dashboard

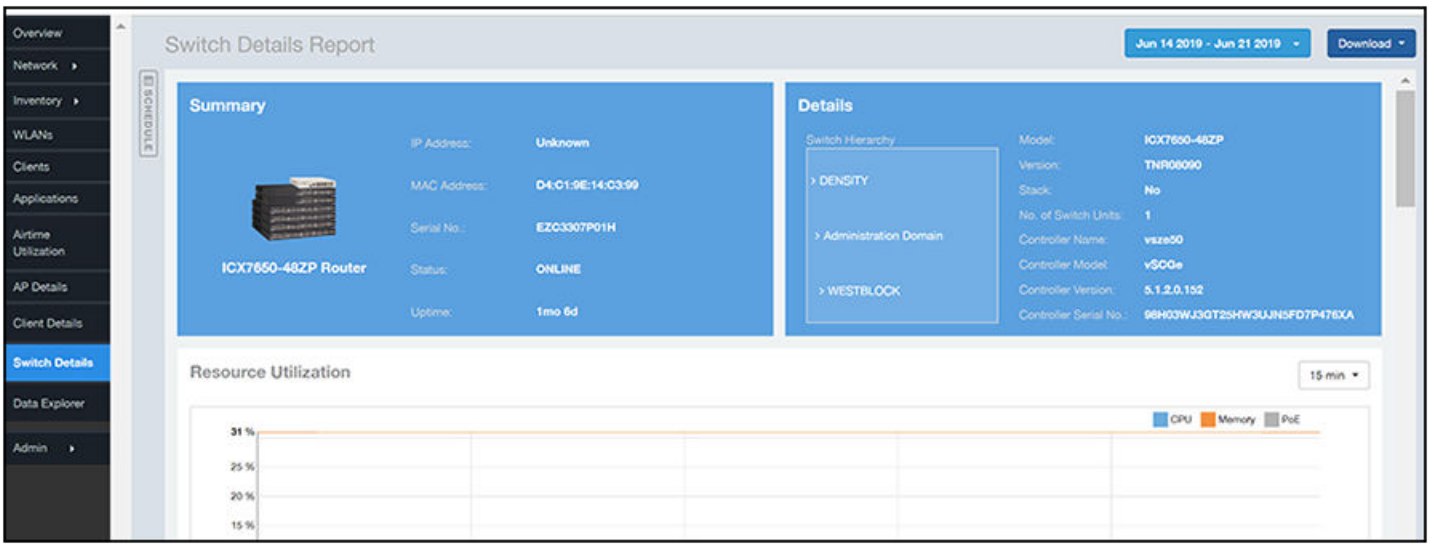
Switch Details Report

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 150 Switch Details Report (upper portion)



The Switch Details Report consists of the following components:

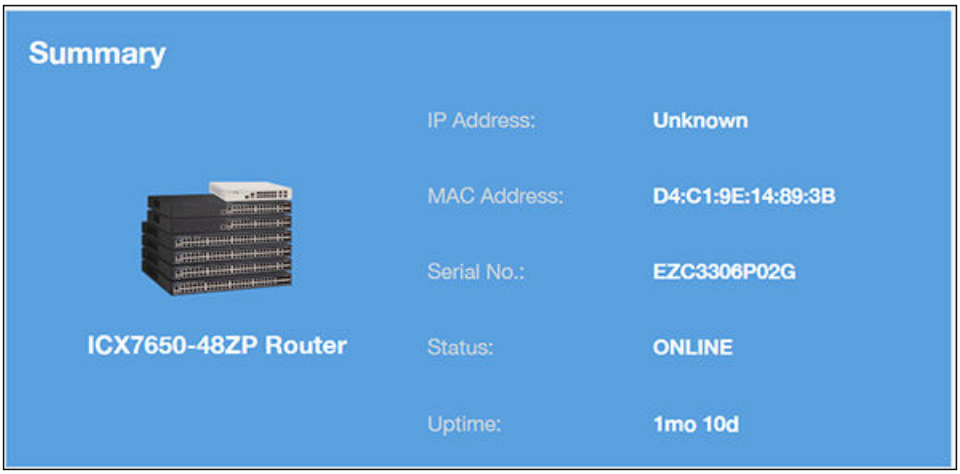
- Summary tile
- Details tile
- Resource Utilization tile
- Top Ports By Traffic tile
- Traffic Trend tile
- LLDP Neighbor List tile
- Uptime History tile

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.

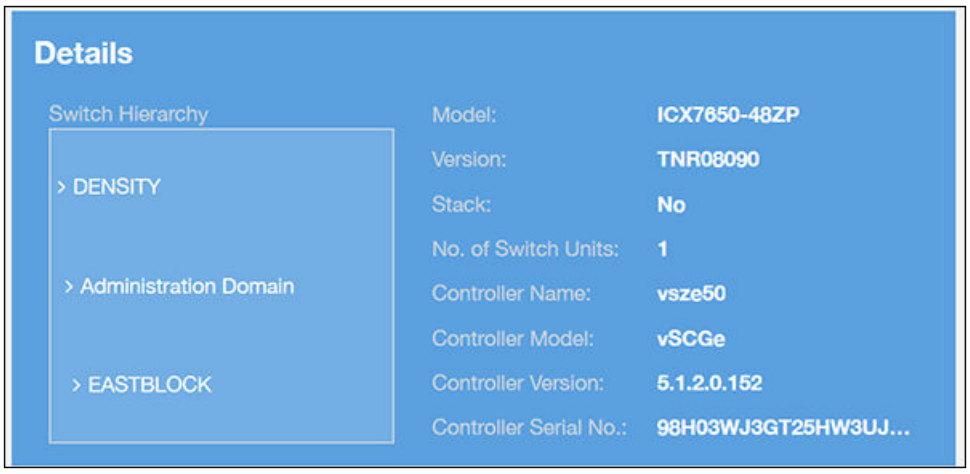
FIGURE 151 Switch Details - Summary



Details Tile

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

FIGURE 152 Switch Details - Details

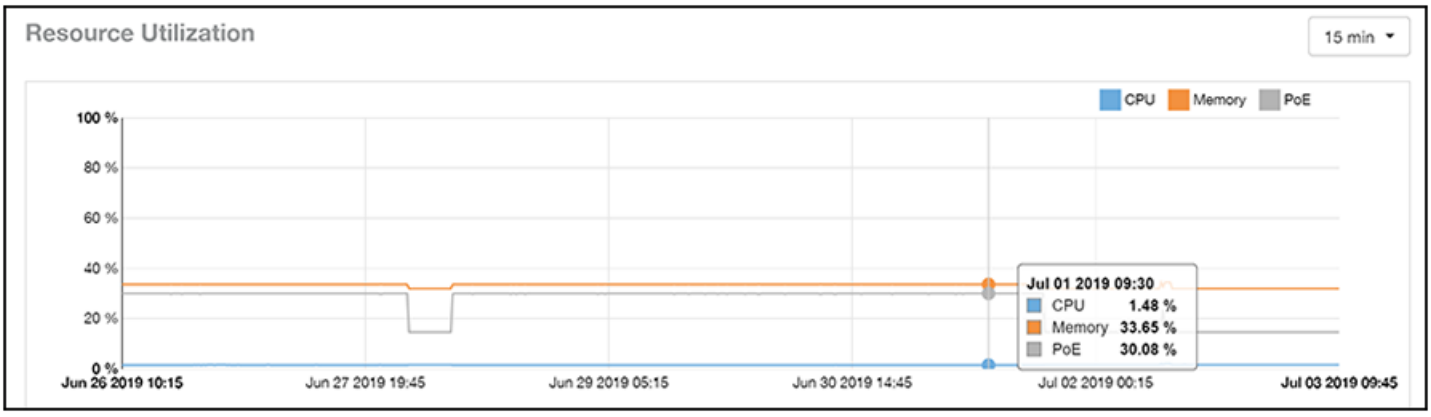


Resource Utilization Tile

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 153 Switch Details - Resource Utilization

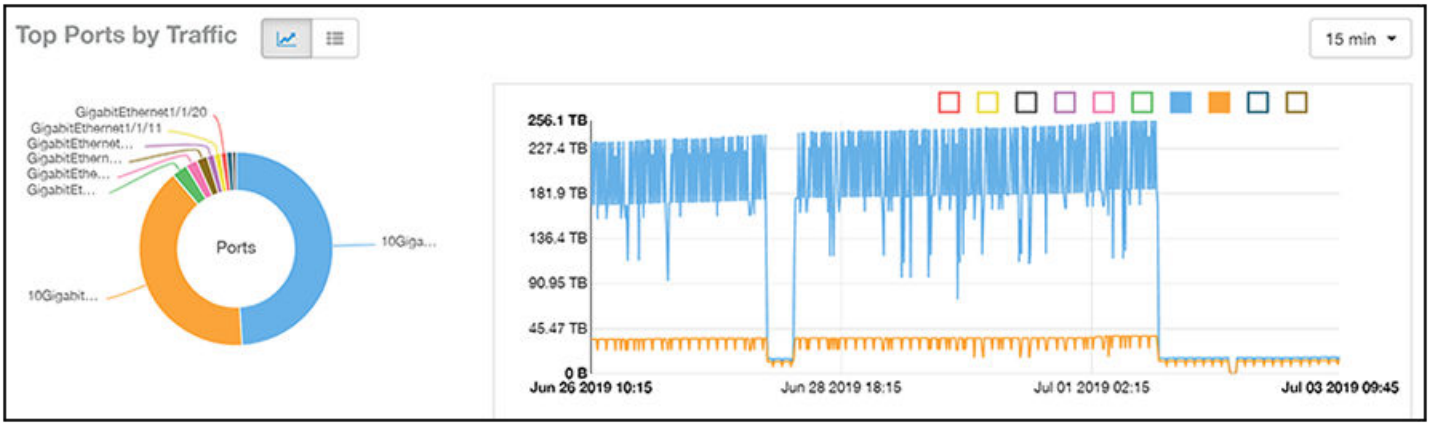


Top Ports By Traffic Tile

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.

FIGURE 154 Switch Details - Top Ports By Traffic

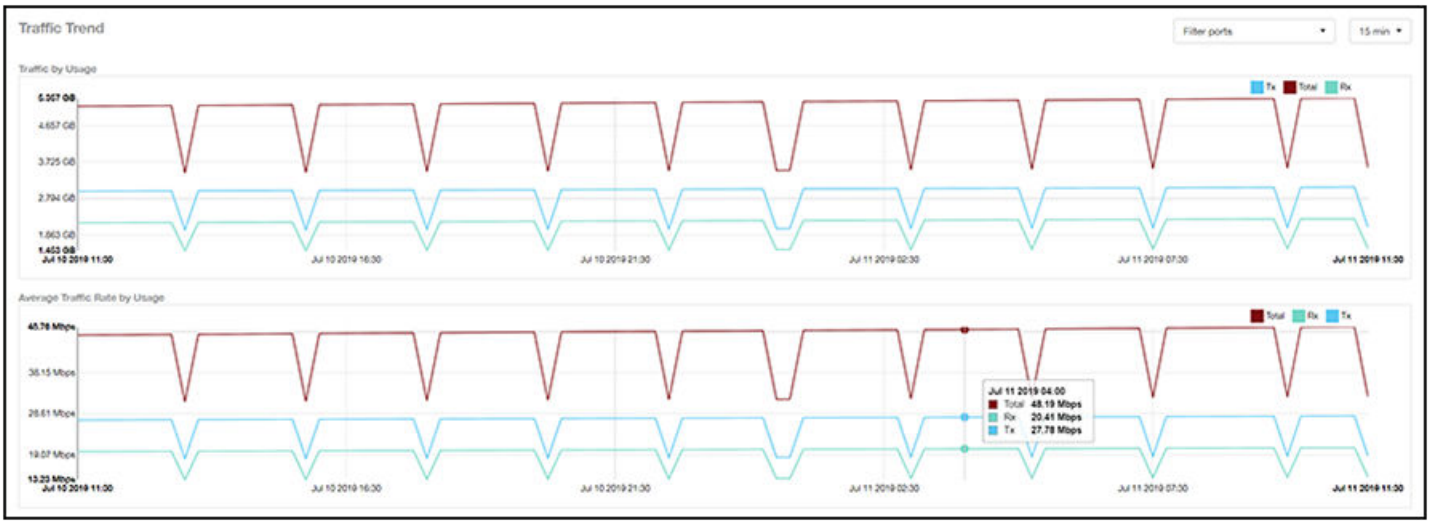


Traffic Trend Tile

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 155 Switch Details - Traffic Trend

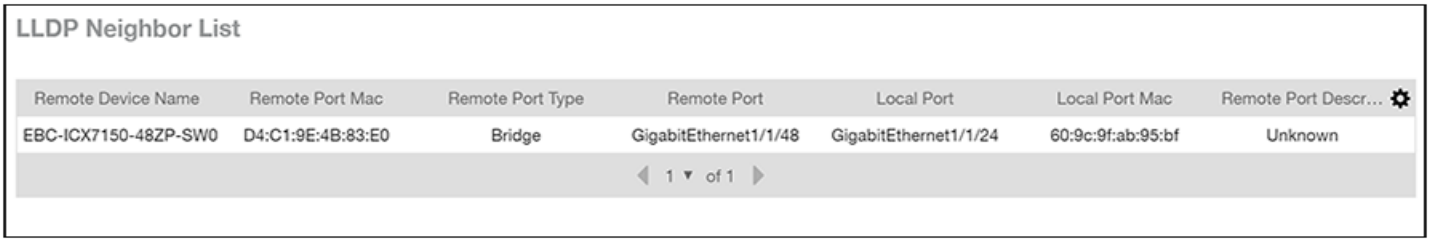


LLDP Neighbor List Tile

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 156 Switch Details - LLDP Neighbor List

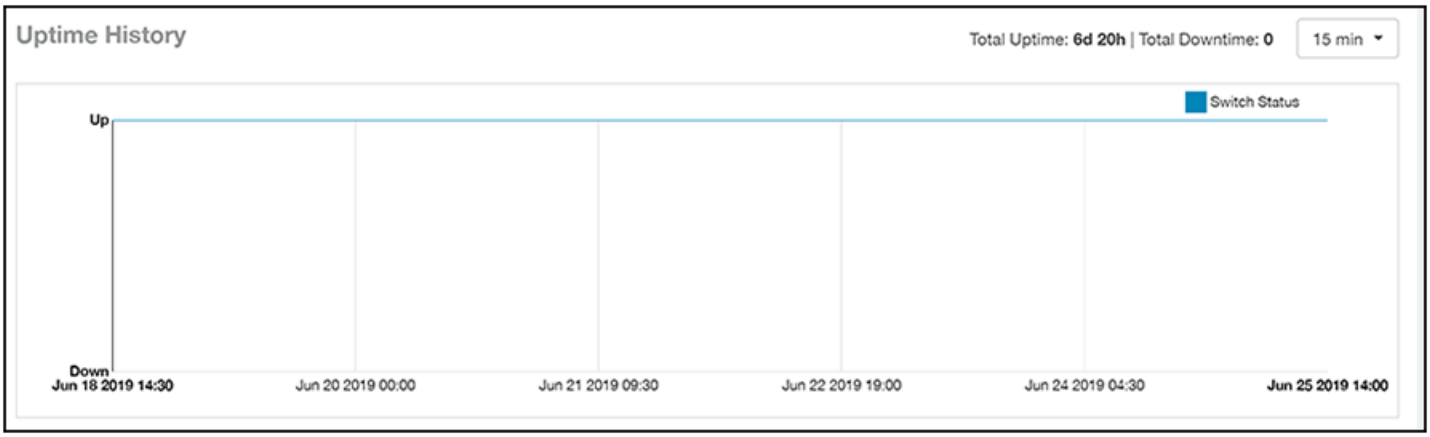


Uptime History Tile

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 157 Switch Details - Uptime History



Comparison Reports Dashboard

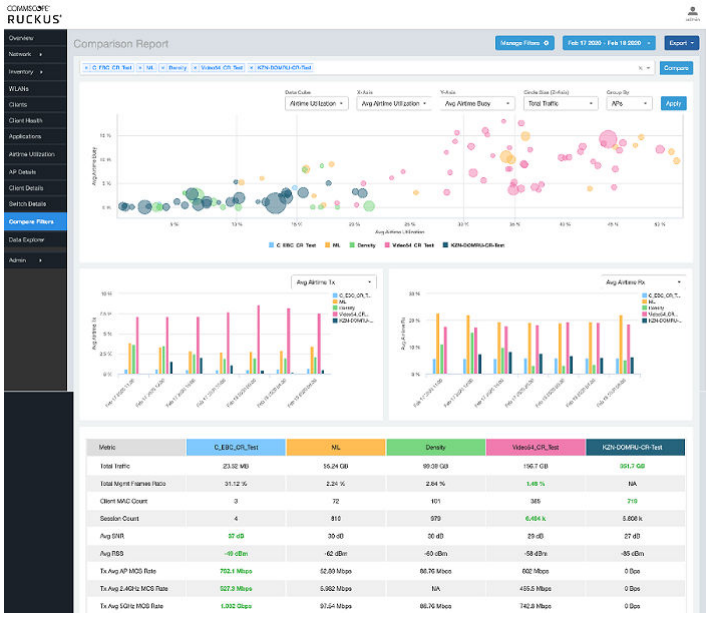
Compare Filters

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 158 Comparison Report



The Comparison Report consists of the following components:

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

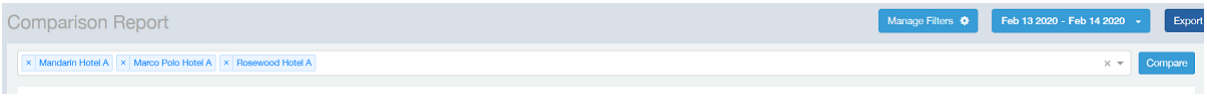
Compare Filters Tile

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.

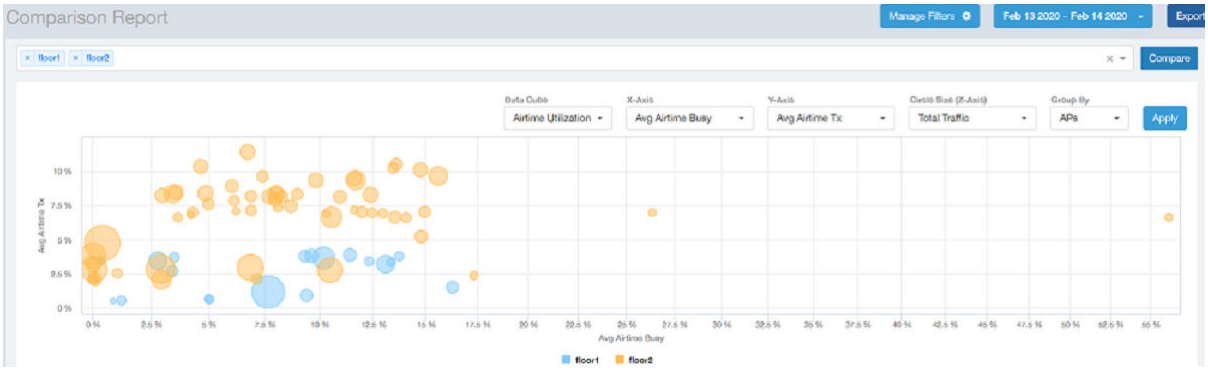
FIGURE 159 Comparison Reports - Compare Filters



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 160 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.

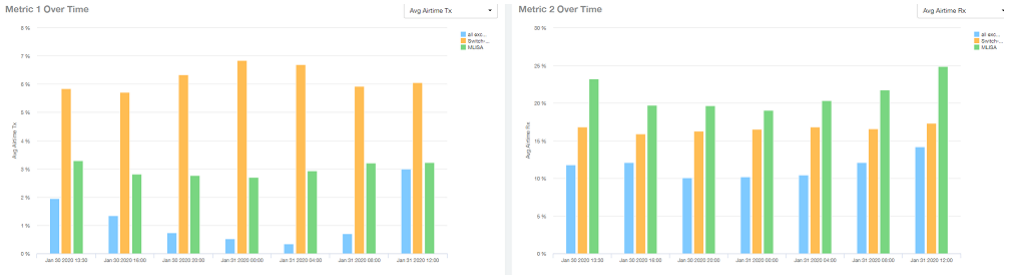
  You can toggle the circles below the chart (on and off) to display or not display the filters they represent.

  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 161 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 displays 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 162 Comparison Reports - Table

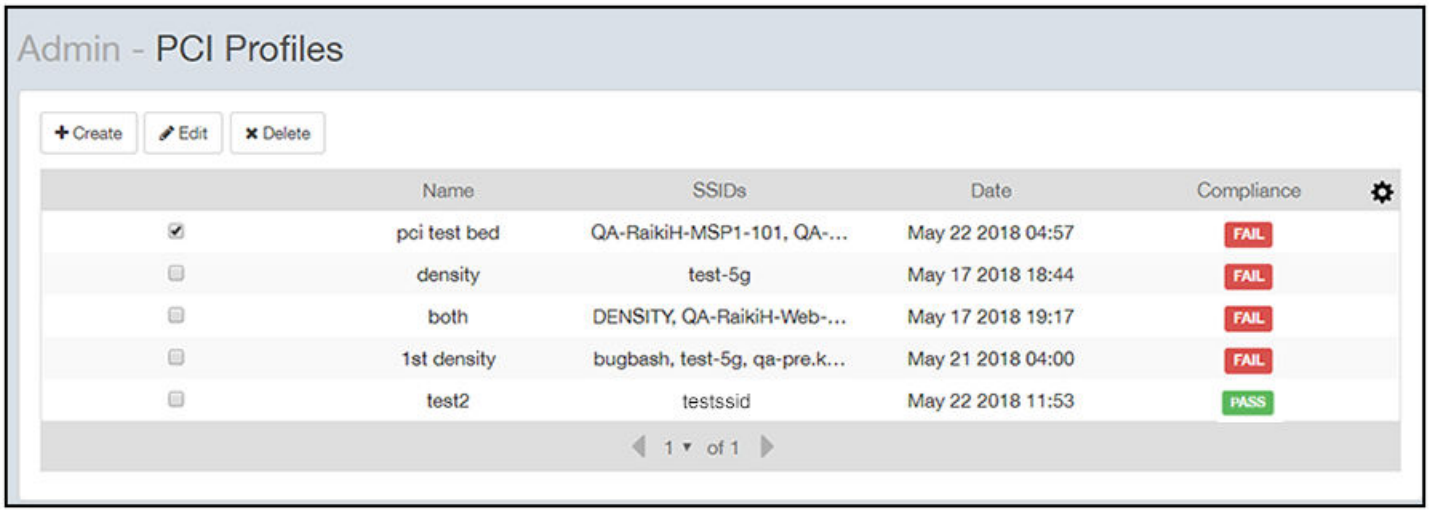
Metric	10 ERTelecom APs	Switch-1	MLISA
Total Traffic	0 B	613.2 GB	54.47 GB
Total Mgmt Frames Ratio	0 %	1.34 %	2.58 %
Client MAC Count	0	1.212 k	77
Session Count	0	14.39 k	934
Client Health Score (Good)	0 %	78.91 %	74.15 %
Avg SNR	0 dB	30 dB	31 dB
Avg RSS	0 dBm	-58 dBm	-59 dBm
Tx Avg AP MCS Rate	0 Bps	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 SCI to determine if your WLANs are compliant with the Payment Card Industry (PCI) Data Security Standard v3.2.

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

FIGURE 163 PCI Profiles Screen



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

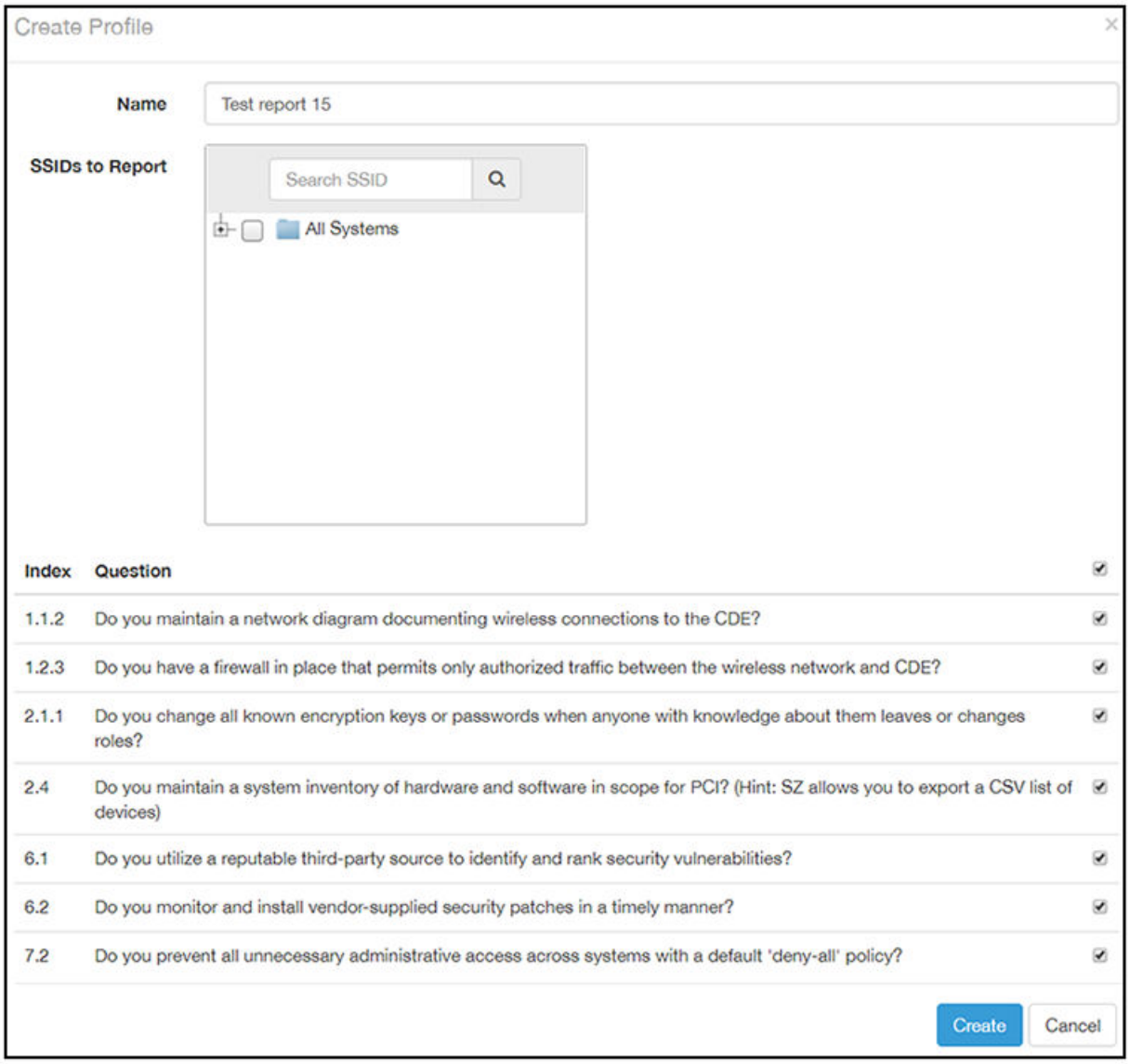
You can create a PCI profile to run a report that indicates if a WLAN is in compliance with the PCI Data Security Standard v3.2.

Follow the steps below to create a PCI profile:

1. From **Admin > PCI** in the SCI user interface, click the **Create** button in the upper left of the screen.

   The **Create Profile** screen is displayed.

   FIGURE 164 Creating a PCI Profile



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. SCI 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 163 on page 132.

Opening and Downloading a PCI Profile

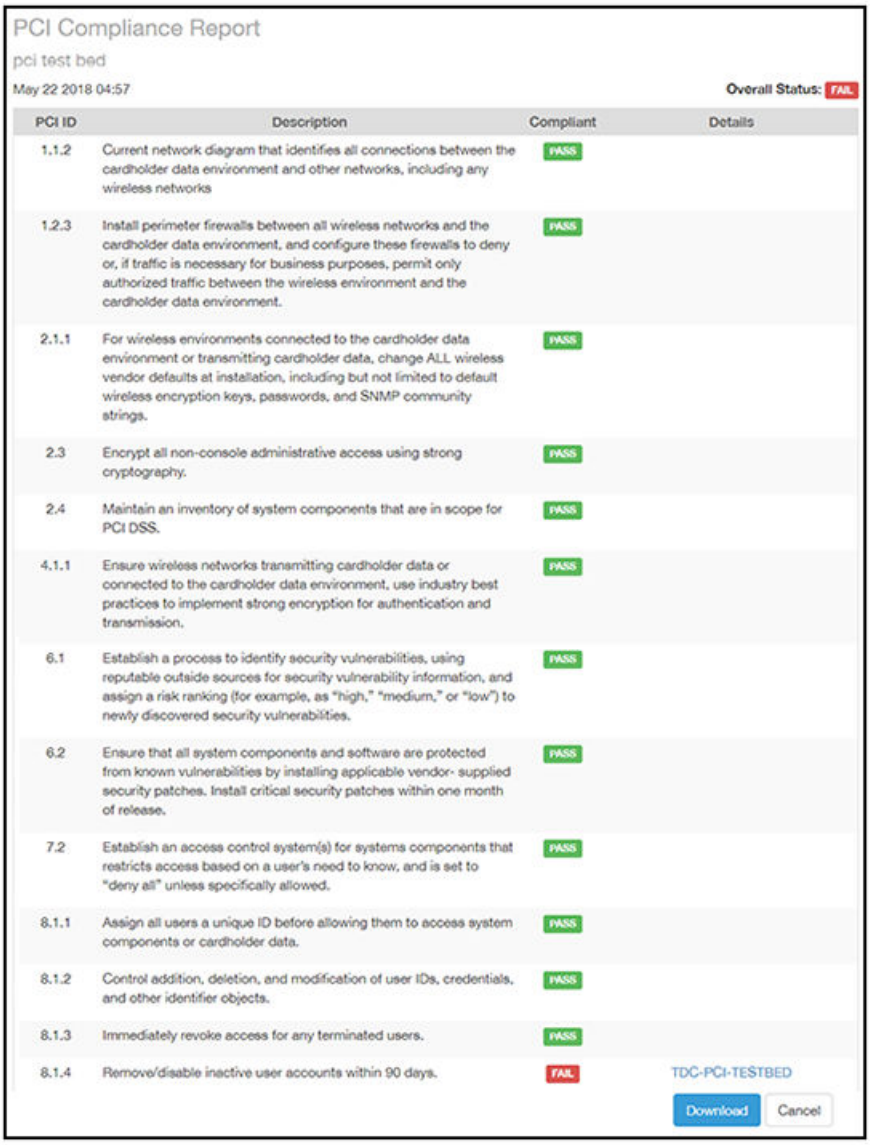
The PCI Profile gives you an overall status (Pass of Fail) as well as a breakdown of all categories you requested when you created the PCI profile.

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 163 on page 132, 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 165 PCI Report Example



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

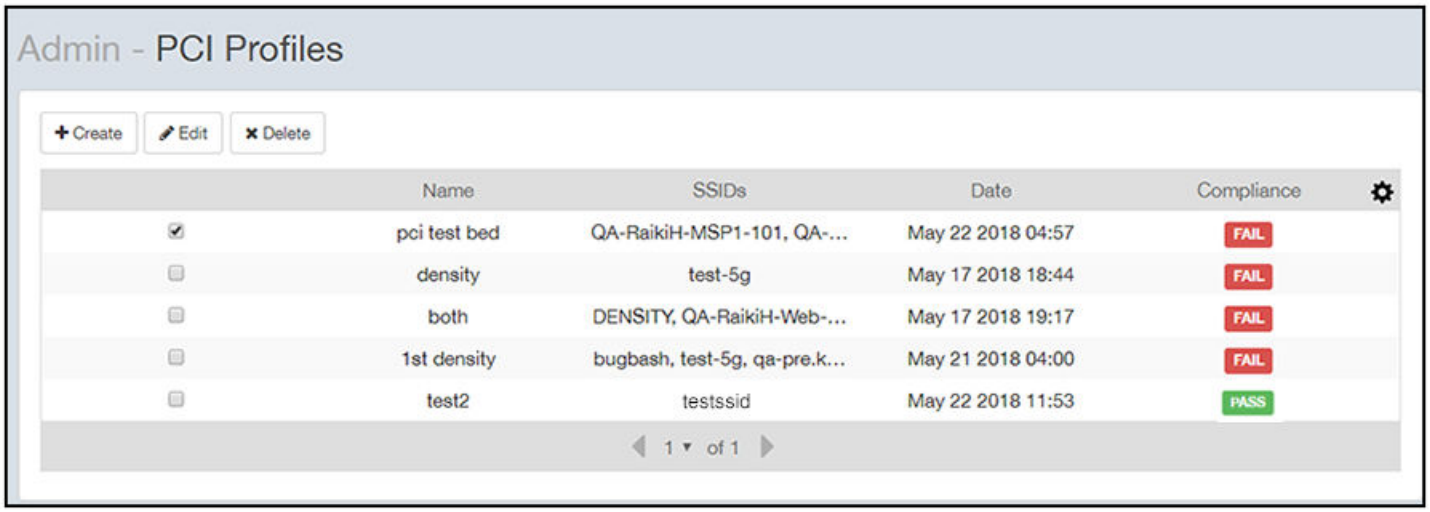
Editing or Deleting a PCI Profile

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 166 Edit or Delete PCI Profiles



Data Explorer

- Data Explorer and Data Cubes....137
- Data Cube Filters....149
- Creating a Data Explorer Dashboard....172
- Actions You Can Perform on an Existing Dashboard....177

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.

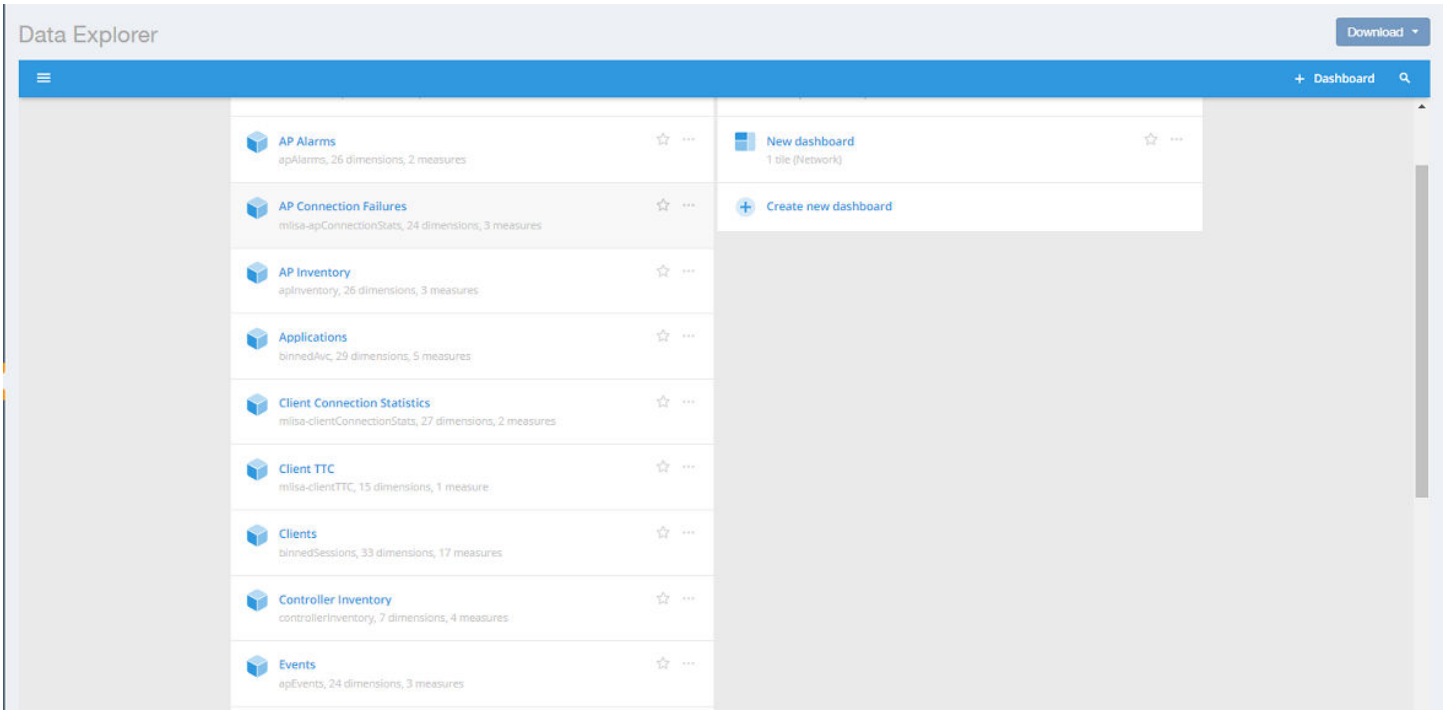
Consider your data to be a three-dimensional cube that you would like to explore, both inside out and outside in, so that you can glean more insights from your data. Of course, most real world data sets will have more than three dimensions, but the concepts from a 3D cube can be directly extended to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

FIGURE 167 Data Explorer and Data Cubes



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

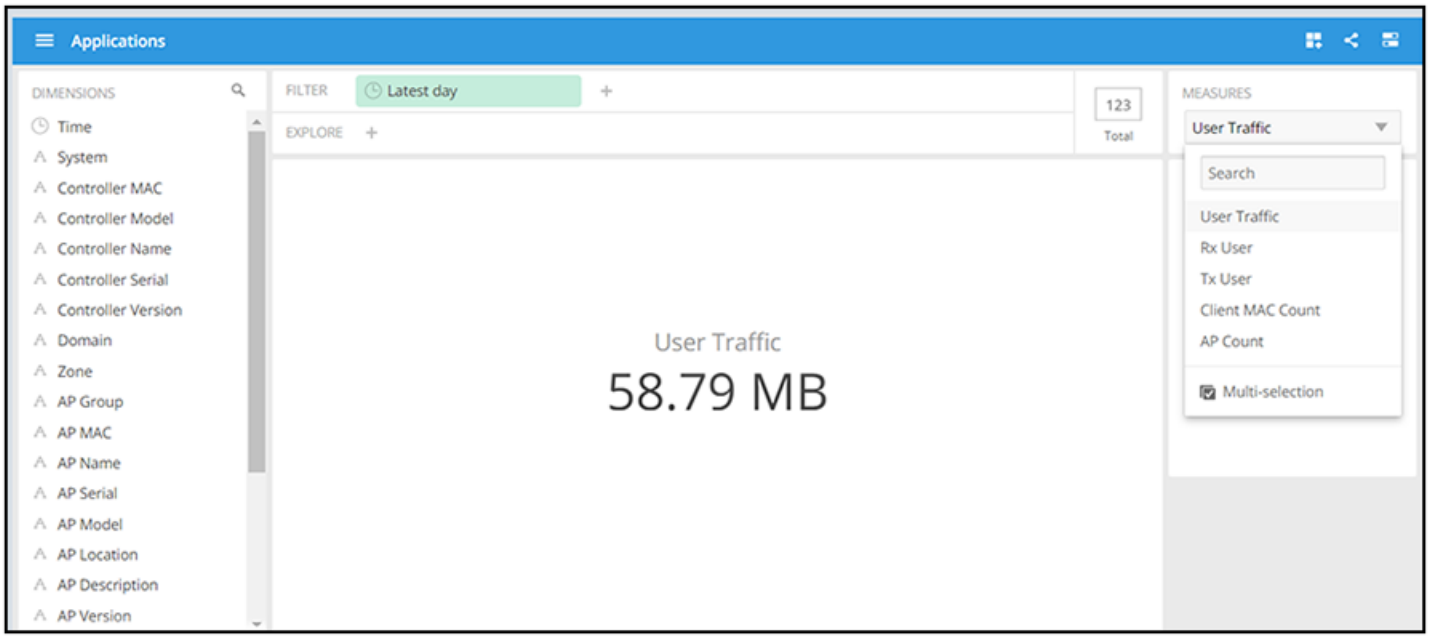
NOTE
The **Schedule** tab is for use only with dashboards you create, not with data cubes themselves.

For information on how to use data cube filters, which are common to all the data cubes, refer to Data Cube Filters on page 149. 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 172 and Actions You Can Perform on an Existing Dashboard on page 177 for more information.

Applications

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

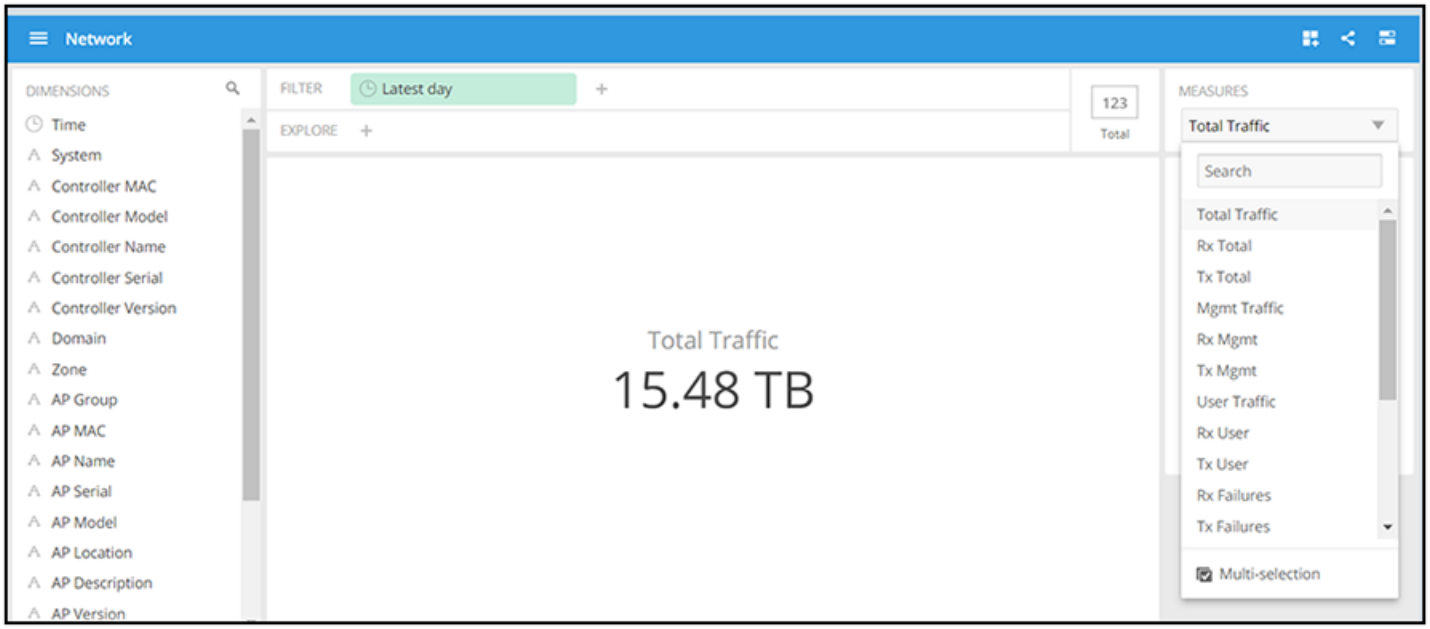
FIGURE 168 Data Explorer: Applications



Network

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

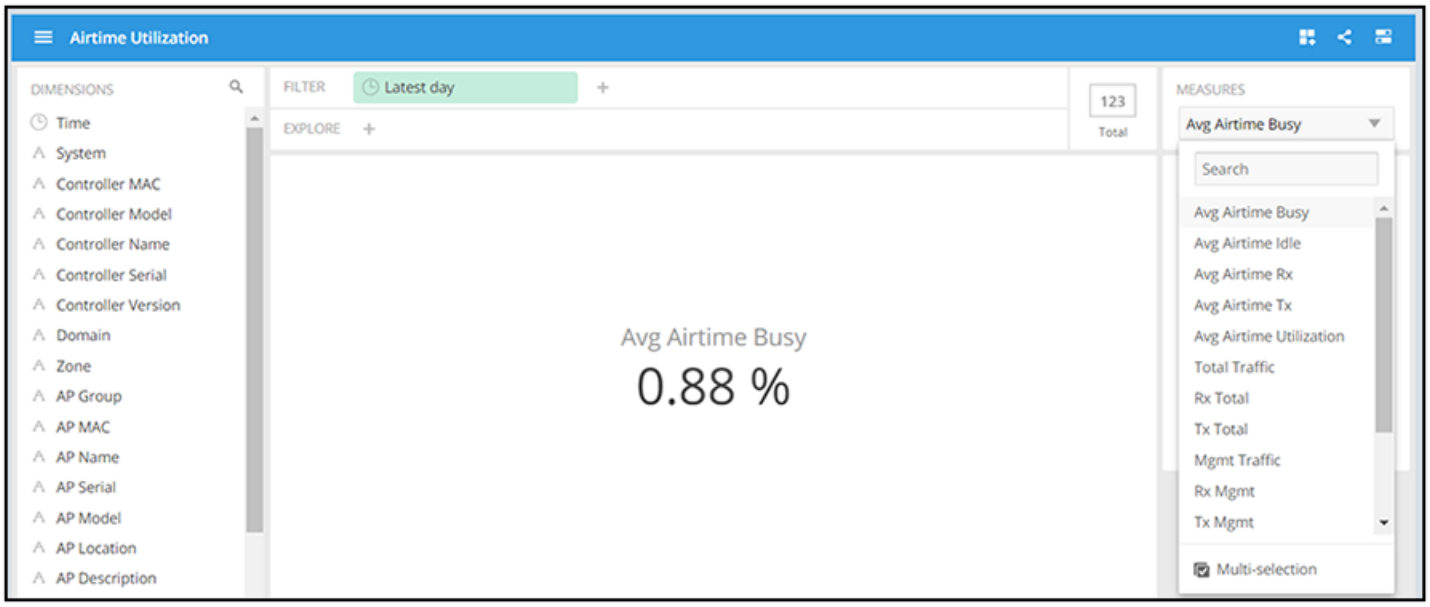
FIGURE 169 Data Explorer: Network



Airtime Utilization

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

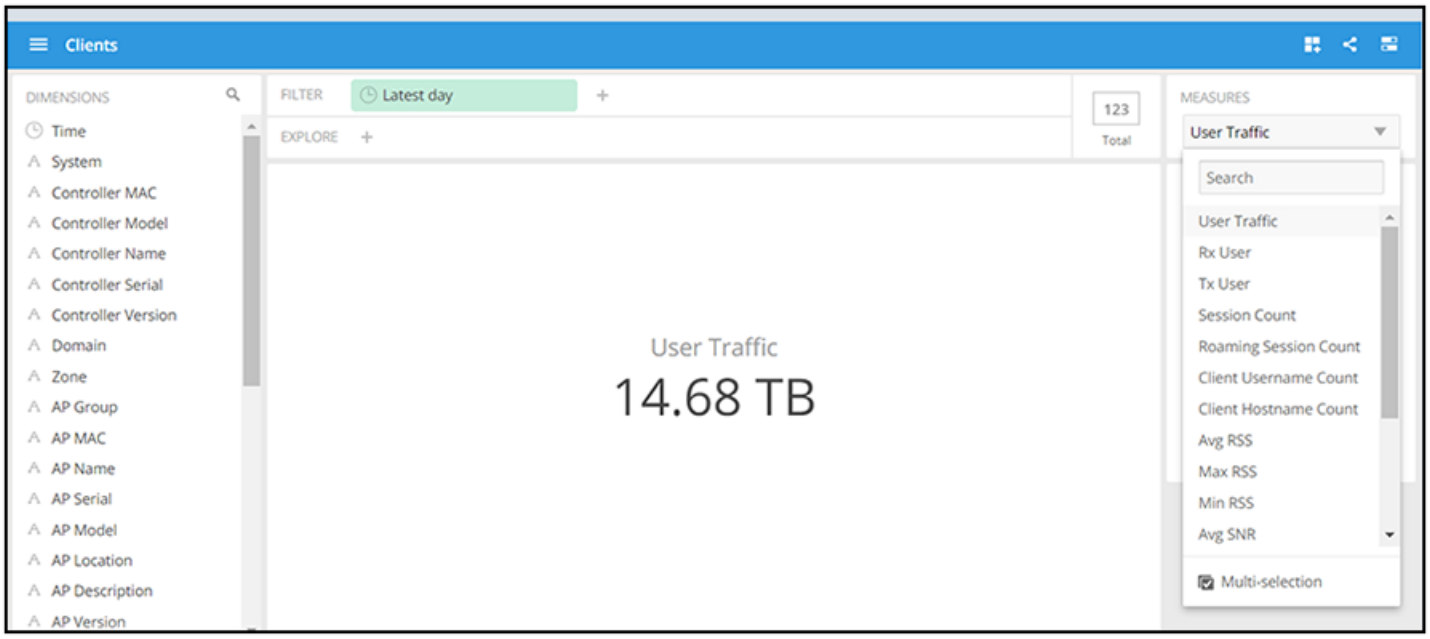
FIGURE 170 Data Explorer: Airtime Utilization



Clients

The **Clients** cube allows you to explore client data for your system.

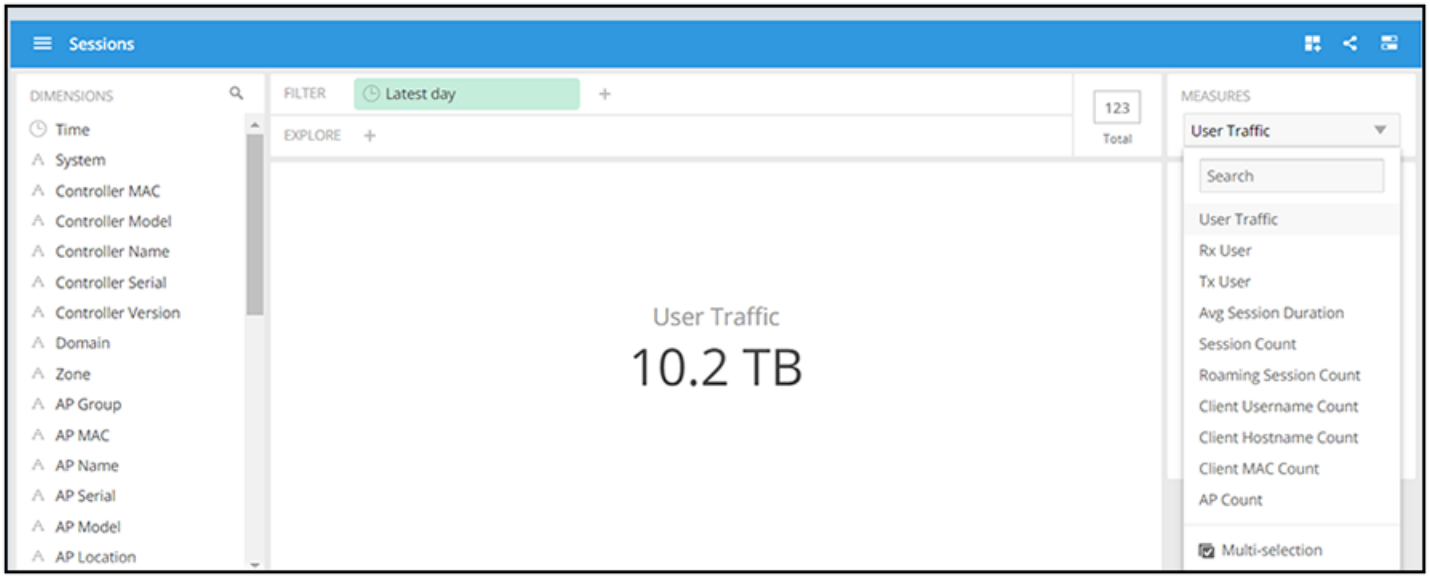
FIGURE 171 Data Explorer: Clients



Sessions

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

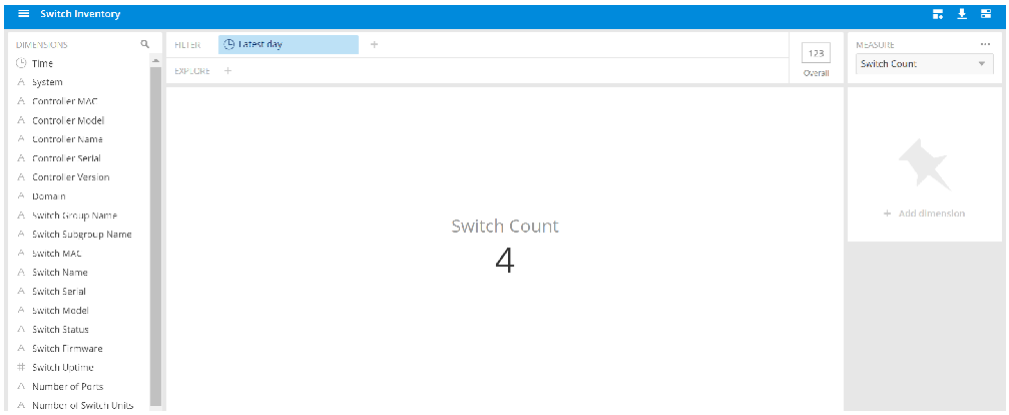
FIGURE 172 Data Explorer: Sessions



Switch Inventory

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

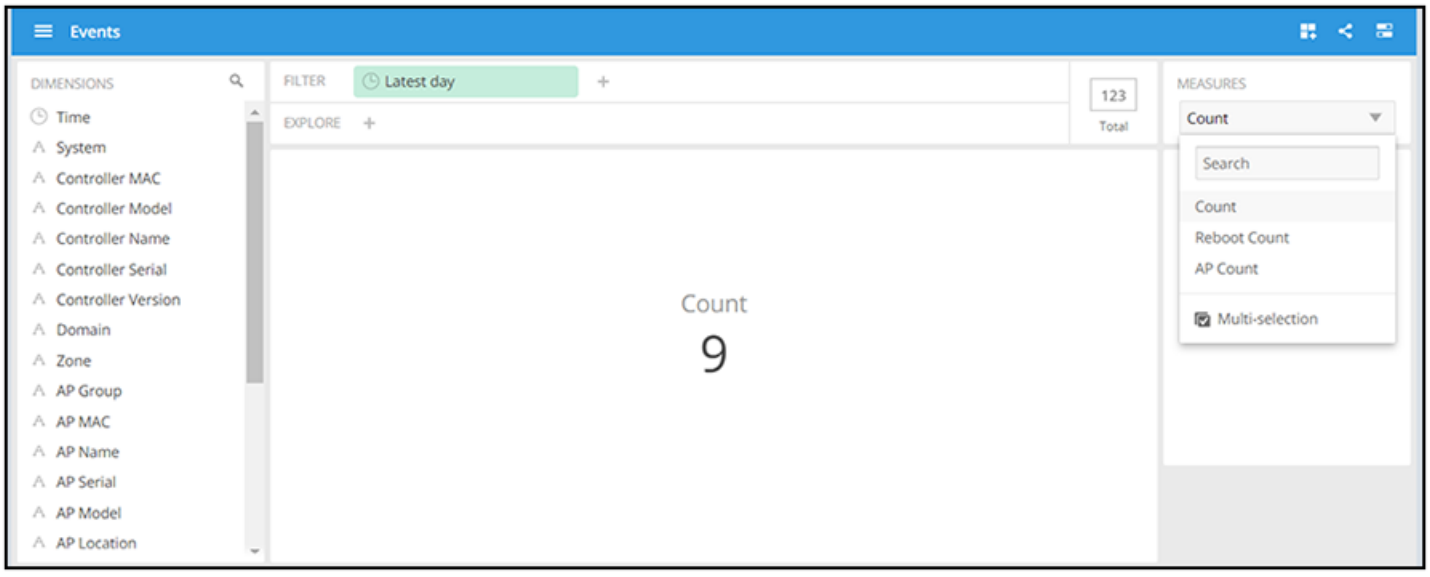
FIGURE 173 Data Explorer: Switch Inventory



Events

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

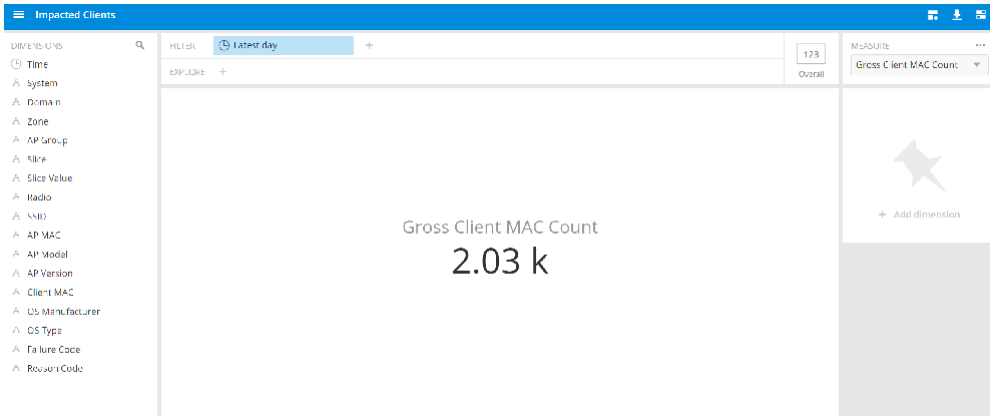
FIGURE 174 Data Explorer: Events



Impacted Clients

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

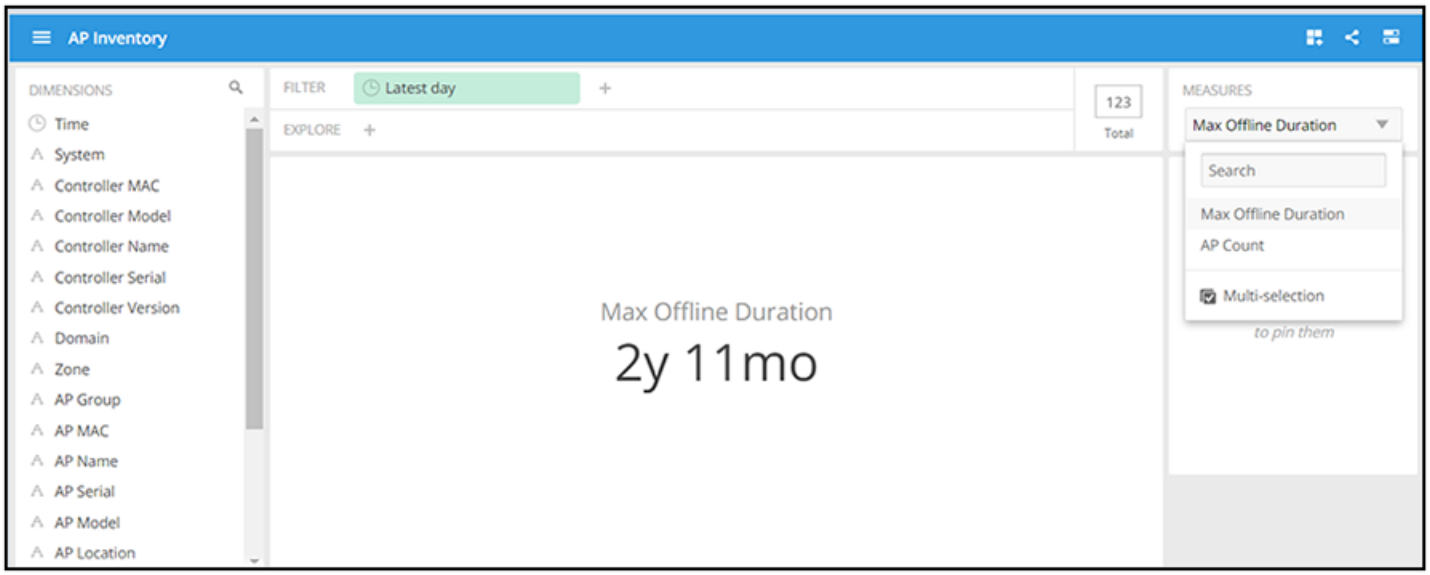
FIGURE 175 Data Explorer: Impacted Clients



AP Inventory

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

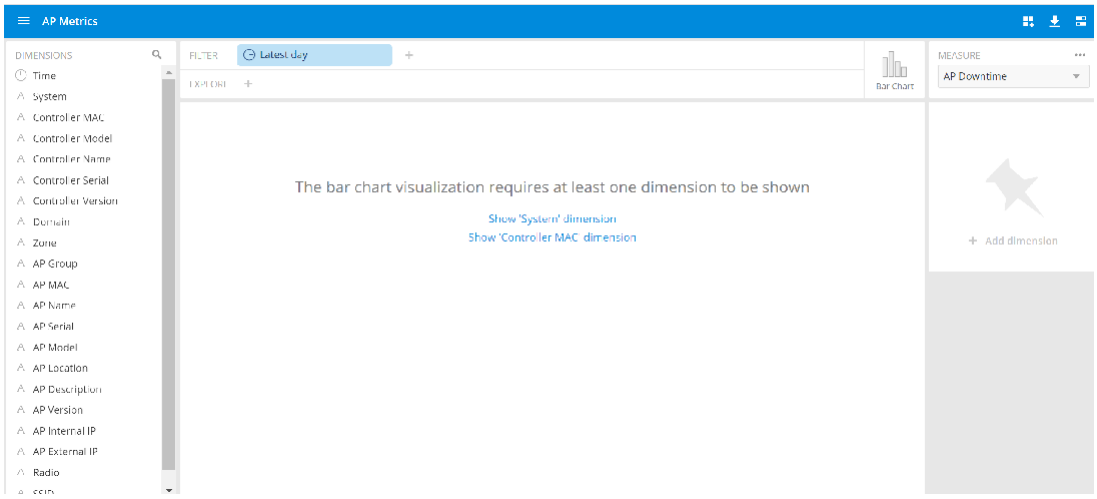
FIGURE 176 Data Explorer: AP Inventory



AP Metrics

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

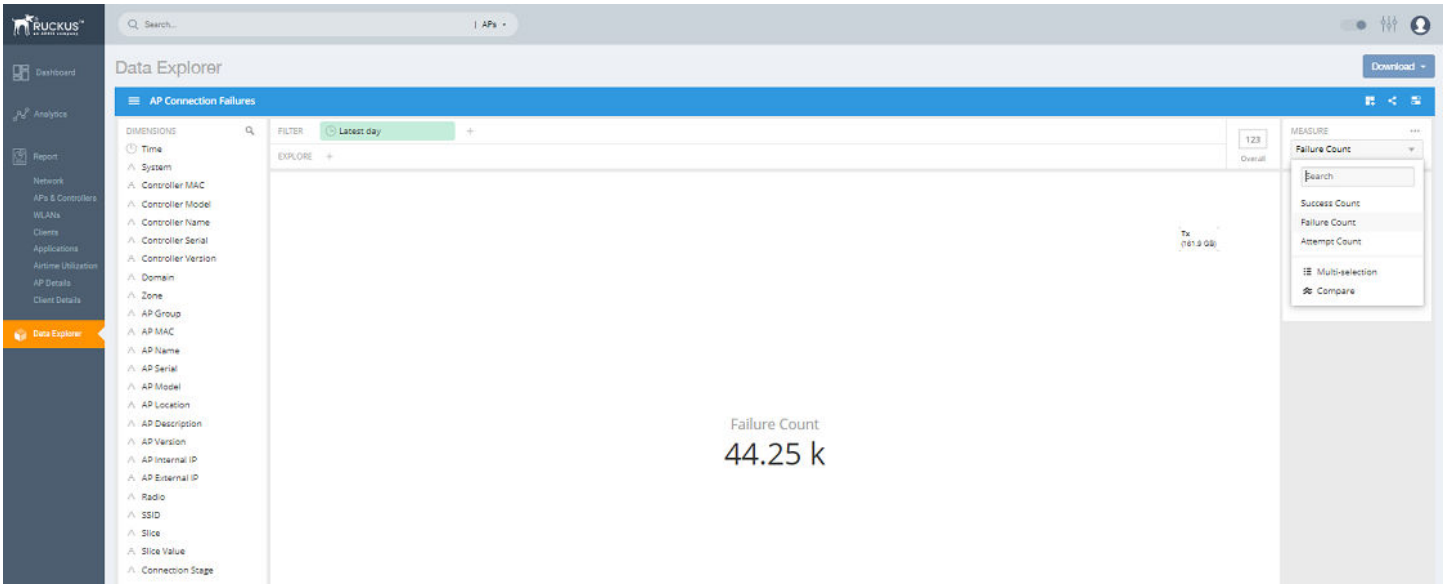
FIGURE 177 Data Explorer: AP Metrics



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.

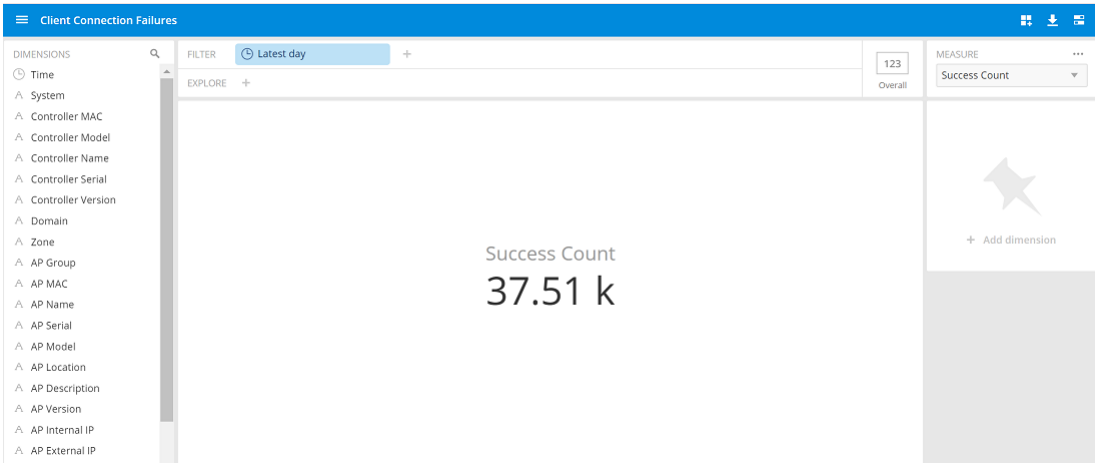
FIGURE 178 Data Explorer: AP Connection Failures



Client Connection Failures

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

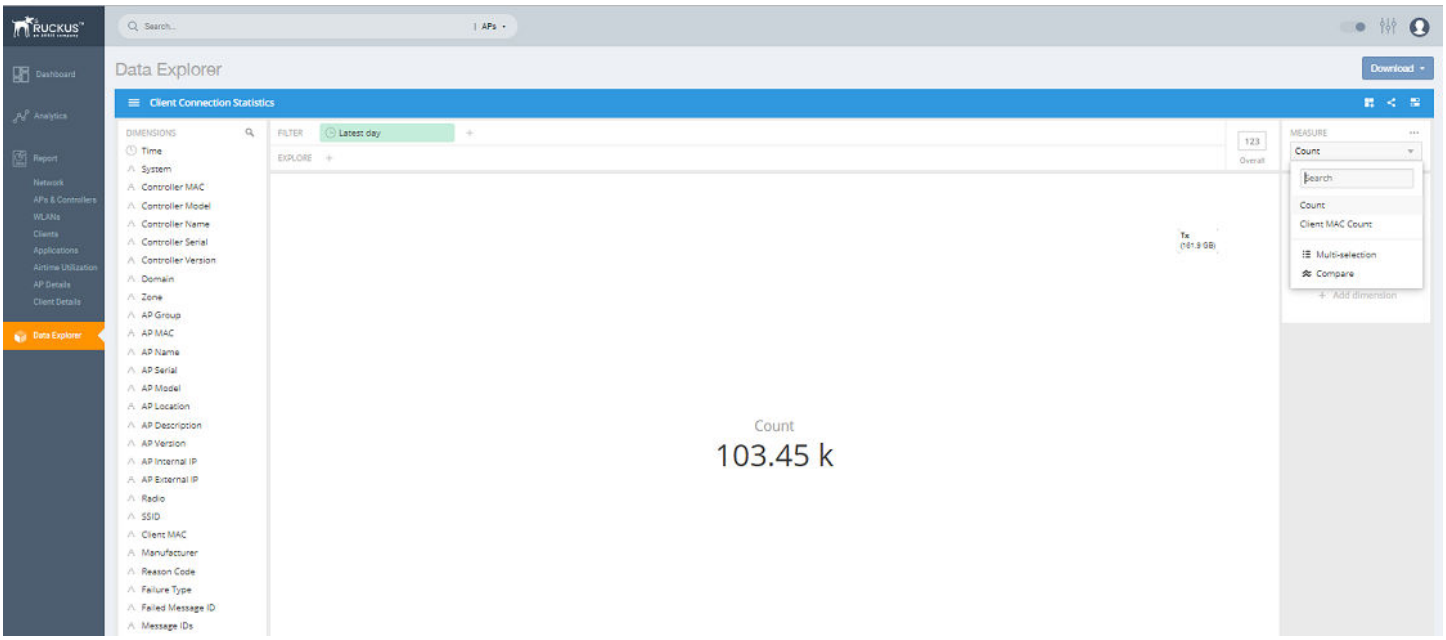
FIGURE 179 Data Explorer: Client Connection Failures



Client Connection Statistics

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

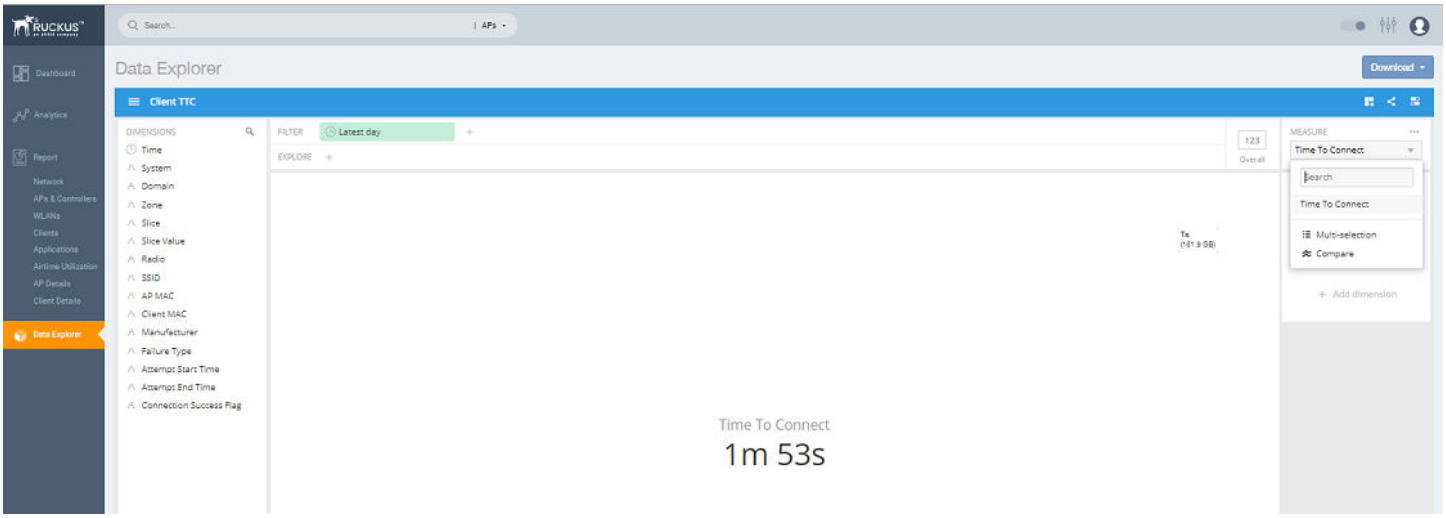
FIGURE 180 Data Explorer: Client Connection Statistics



Client TTC

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

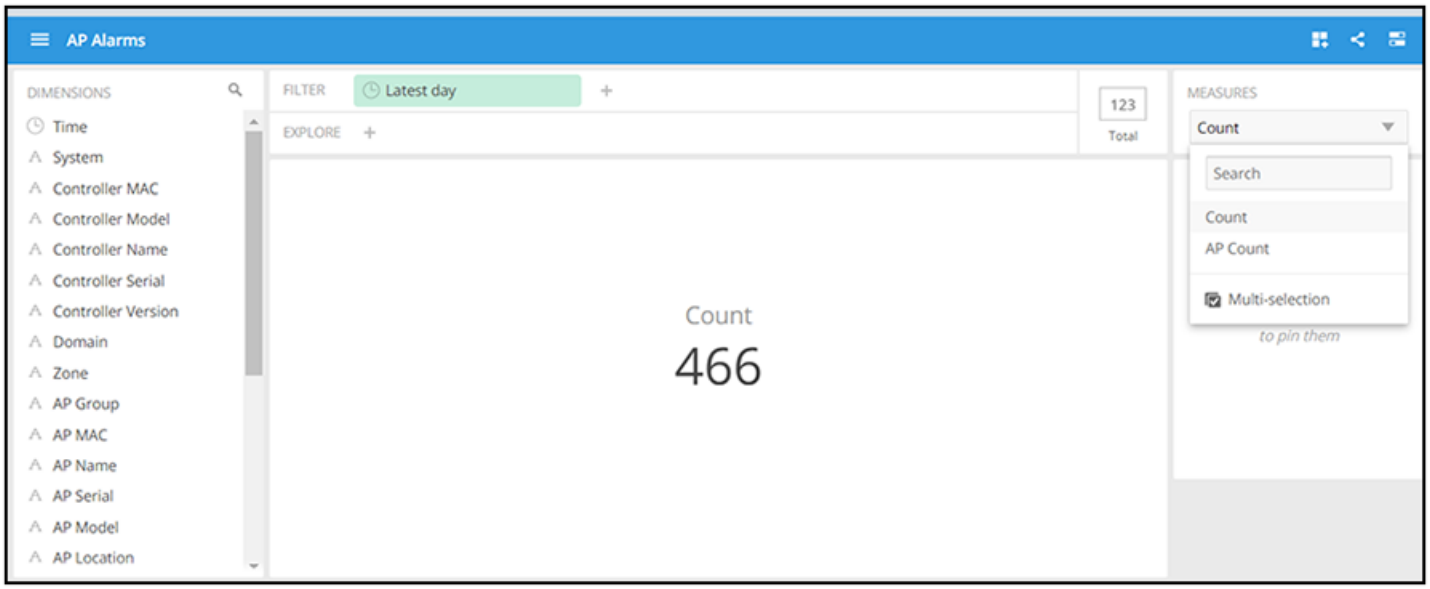
FIGURE 181 Data Explorer: Client TTC



AP Alarms

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

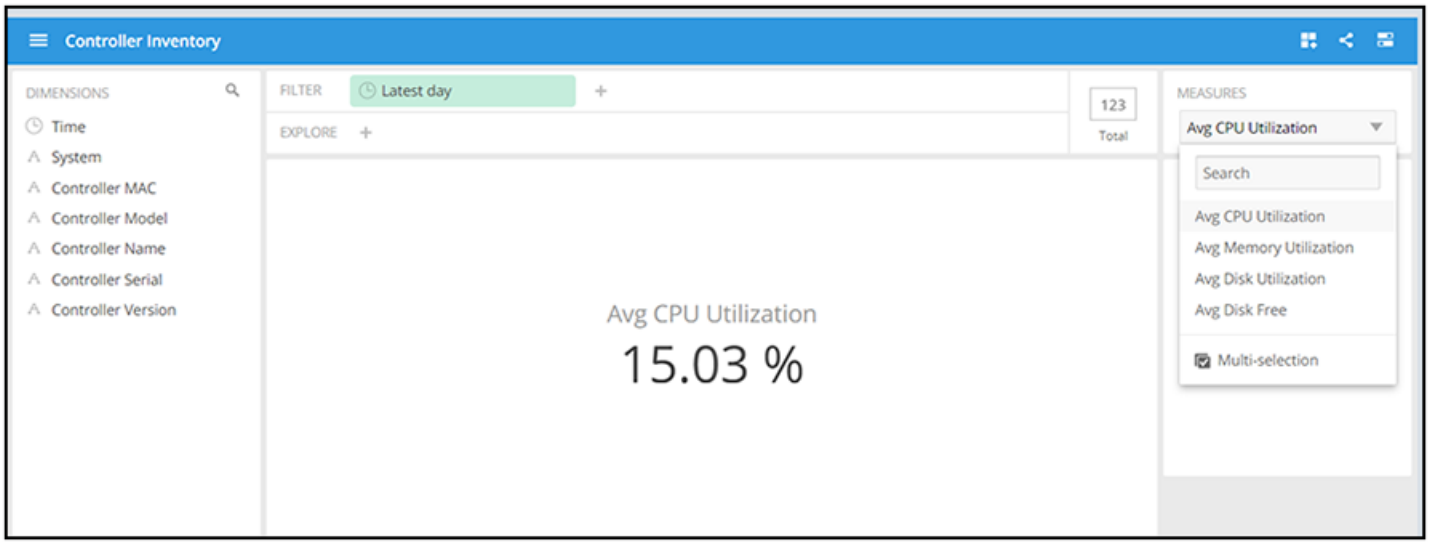
FIGURE 182 Data Explorer: AP Alarms



Controller Inventory

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

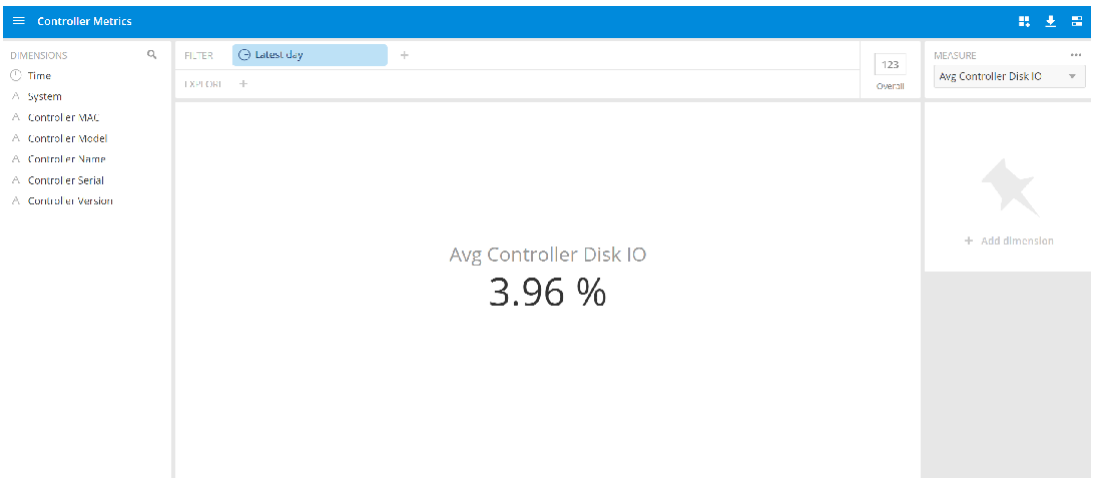
FIGURE 183 Data Explorer: Controller Inventory



Controller Metrics

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

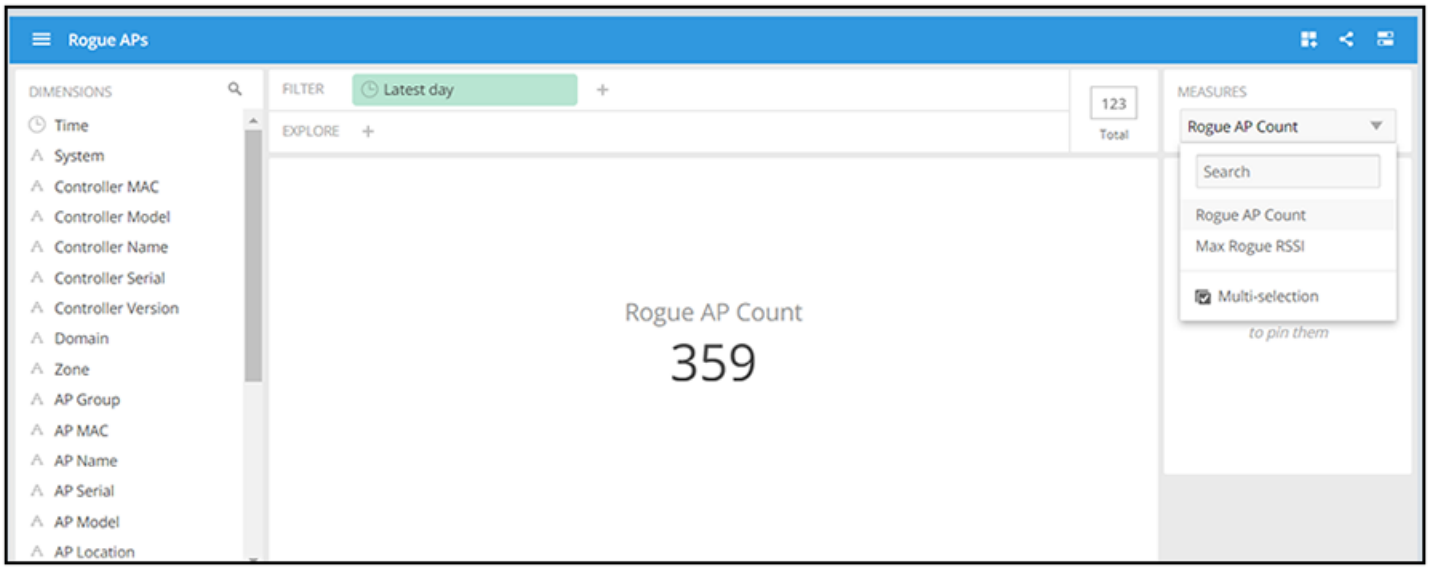
FIGURE 184 Data Explorer: Controller Metrics



Rogue APs

The **Rogue APs** 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.

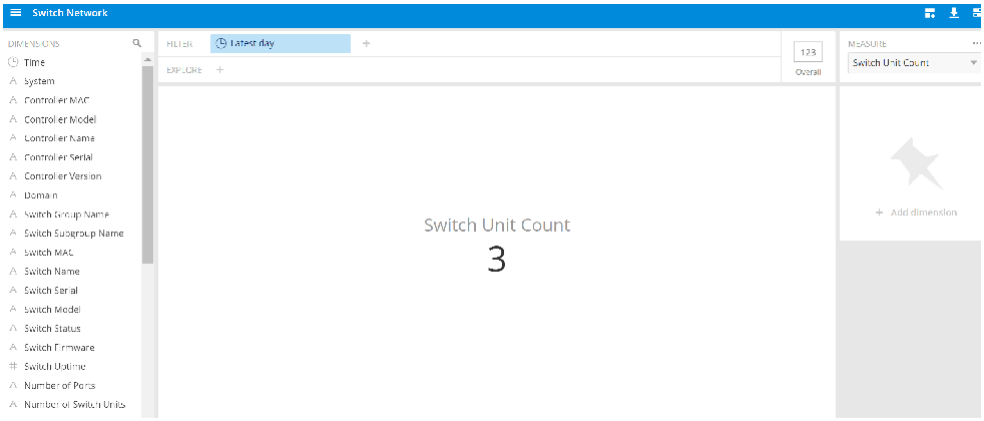
FIGURE 185 Data Explorer: Rogue APs



Switch Network

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

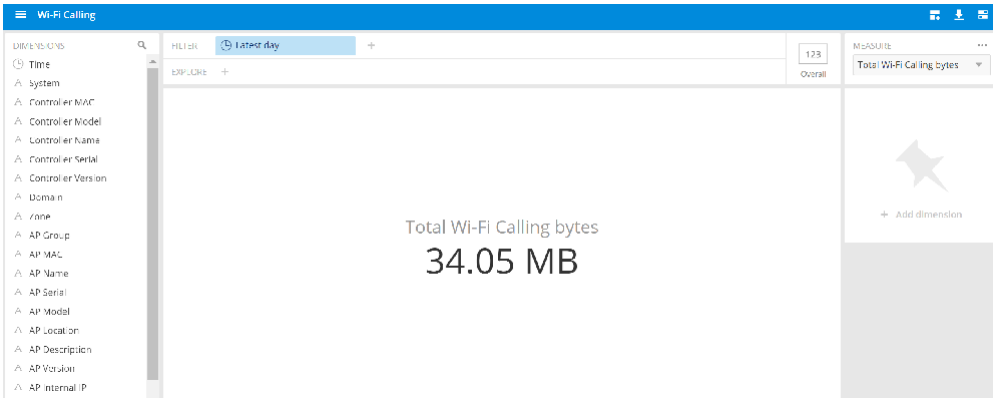
FIGURE 186 Data Explorer: Switch Network



Wi-Fi Calling

The **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 187 Data Explorer: 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 188 Data Cube Filters

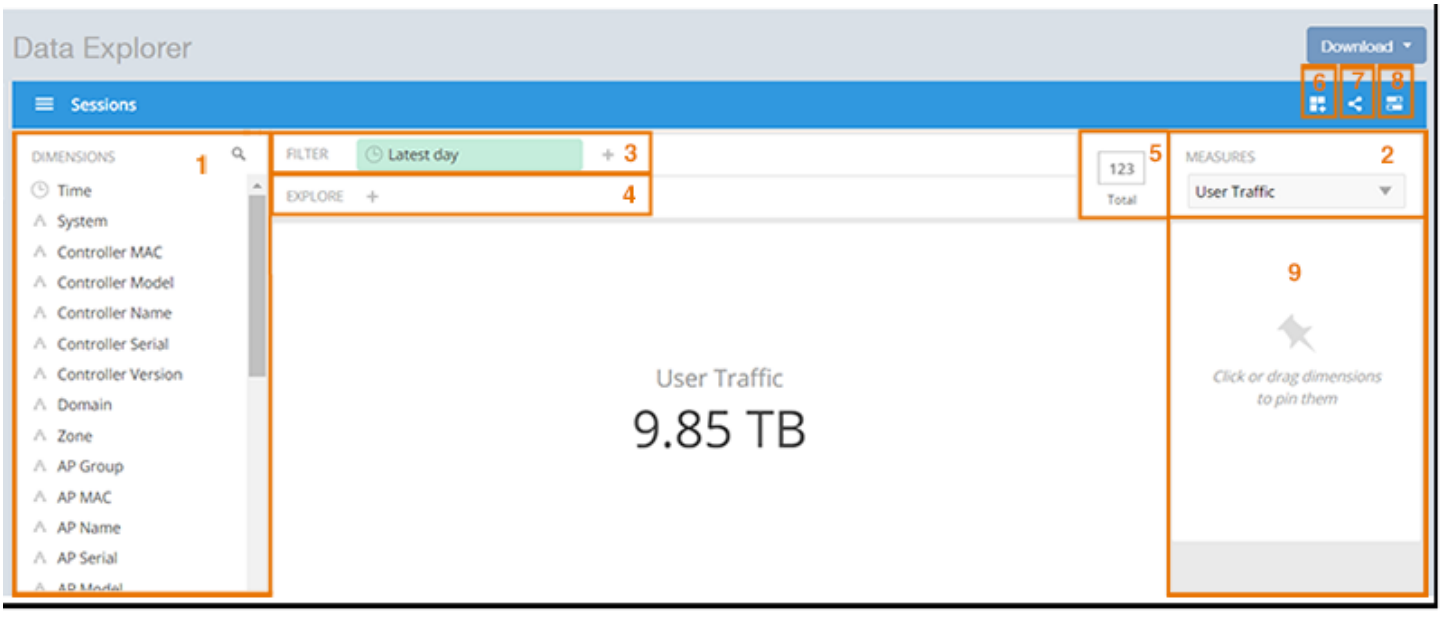


TABLE 14 Identifying Data Explorer Interface Components

No	Name
1	Dimensions
2	Measures
3	Filter
4	Explore
5	View Outputs

TABLE 14 Identifying Data Explorer Interface Components (continued)

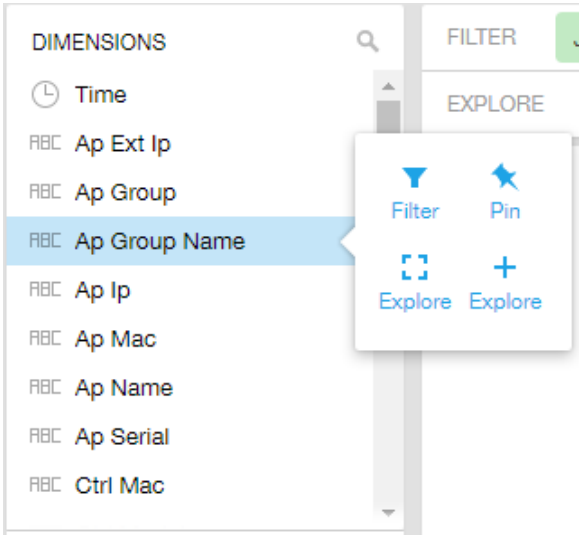
No	Name
6	Add to Dashboard
7	Share Link
8	Options
9	Pinboard

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 189 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 15 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

TABLE 15 Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
AP Description	Description string of the access point that is configured in the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
AP External IP	External IP address of the access point.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
AP Group	AP Groups configured in the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
AP Internal IP	Internal IP address of the access point.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
AP Latitude	Latitude of GPS coordinates.	AP Inventory
AP Longitude	Longitude of GPS coordinates.	AP Inventory

TABLE 15 Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
AP Location	Location string of the access point that is configured in the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
AP MAC	Base MAC address of the access point.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
AP Model	Description of the access point model type.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
AP Name	Name of the access point configured in the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
AP Serial	Serial number of the access point.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs

TABLE 15 Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
AP Version	Firmware version number of the access point.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
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.	• Clients • Sessions
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
Category	Category for access point and controller alarms or events.	• Events • AP Alarms
Channel	The Wi-Fi channel number used.	• Network • Clients • Sessions
Client IP	Internal IP address of the Wi-Fi client.	• Clients • Sessions
Client MAC	MAC address of the Wi-Fi client.	• Applications • Clients • Sessions
Client Radio Mode	Possible values are: ac, n, a, g, b, or "unknown" (if SmartZone version is prior to 3.6).	• Clients • Sessions
Connection Status	Connection status of the access point: Online, Offline, Discovery, Provisioned.	• AP Inventory
Controller MAC	MAC address of the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Controller Inventory • Rogue APs

TABLE 15 Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
Controller Model	Description of the model of the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Controller Inventory • Rogue APs
Controller Name	Name of the configured controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Controller Inventory • Rogue APs
Controller Serial	Serial number of the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Controller Inventory • Rogue APs
Controller Version	Firmware version number of the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Controller Inventory • Rogue APs
Disconnect Time	Disconnect time of a session.	Sessions

TABLE 15 Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
Domain	Domains configured in the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs
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.	• Clients • Sessions
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.	• Clients • Sessions
OS Type	Operating System information for the Wi-Fi client.	• Clients • Sessions
Port	Port of the application accessed by the Wi-Fi client.	Applications
Radio	Indicates the radio frequency band: 2.4GHz or 5GHz.	• Applications • Network • Airtime Utilization • Clients • Sessions
Reason	Additional description for access point and controller alarms or events, if available.	• Events • AP Alarms
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.	• Clients • Sessions
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.	• Clients • Sessions

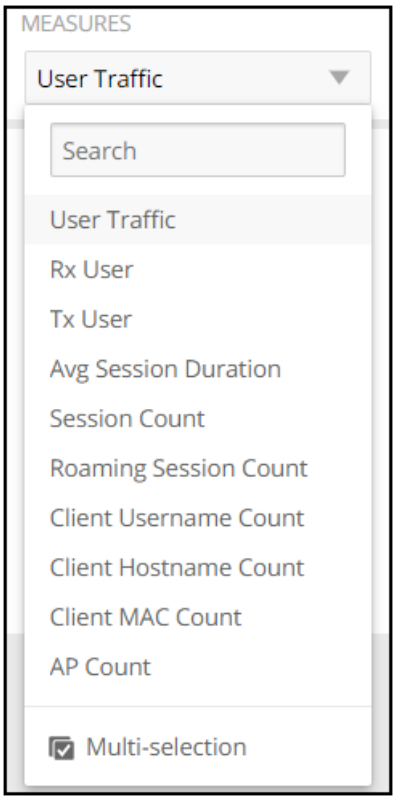
TABLE 15 Dimensions (continued)

Dimension Name	Description	Supported Data Cubes
Session Type	Indicates whether the session is authorized or unauthorized.	• Clients • Sessions
Severity	Severity level for access point and controller alarms or events.	• Events • AP Alarms
SSID	Service set identifier (SSID) configured in the controller.	• Applications • Network • Clients • Sessions
System	System ID of the controller or the SmartZone Cluster.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Controller Inventory • Rogue APs
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.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Controller Inventory • Rogue APs
Username	Username of the user account associated with the Wi-Fi client.	• Clients • Sessions
Zone	Zones configured in the controller.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms • Rogue APs

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 190 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 16 Measures

Measure Name	Description	Supported Data Cubes
AP Count	Unique number of access points.	• Applications • Network • Airtime Utilization • Clients • Sessions • Events • AP Inventory • AP Alarms
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 16 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	• Clients • Sessions
Client MAC Count	Unique number of Wi-Fi clients.	• Applications • Clients • Sessions
Client Username	Name of the user	• Clients • Sessions
Count	Client count	• Events • AP Alarms
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.	• Network • Airtime Utilization
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.	• Clients • Sessions

TABLE 16 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.	• Network • Airtime Utilization
Rx Total	Sum of the received user and management traffic.	• Network • Airtime Utilization
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.	• Applications • Network • Airtime Utilization • Clients • Sessions
Session Count	Number of unique sessions.	• Clients • Sessions
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.	• Network • Airtime Utilization
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.	• Network • Airtime Utilization
TxMulticastFrames	Number of multicast packets transmitted by the network.	Network
Tx Total	Sum of the transmit user and management traffic.	• Network • Airtime Utilization
TxUnicastFrames	The number of data packets transmitted by the network that are not broadcast or multicast packets.	Network

TABLE 16 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.	• Applications • Network • Airtime Utilization • Clients • Sessions
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	• Applications • Network • Airtime Utilization • Clients • Sessions

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 191 Filter

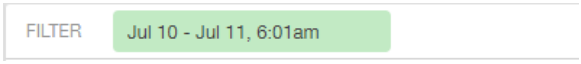
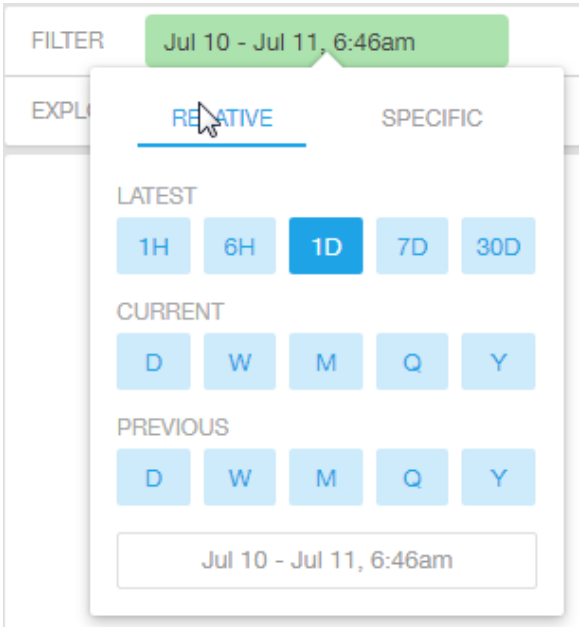


FIGURE 192 Relative Time Settings

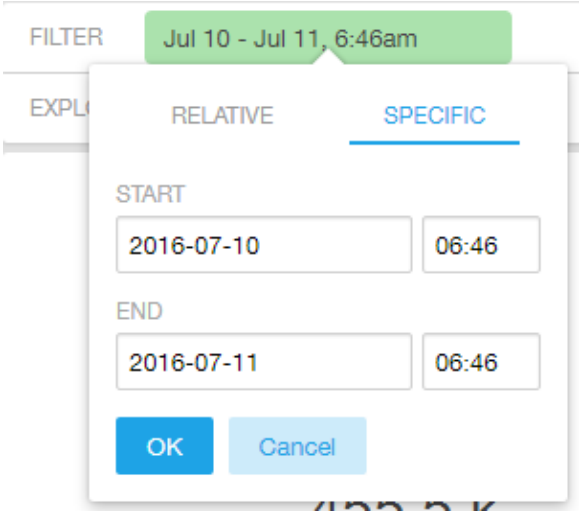


You can specify the following relative time settings:

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

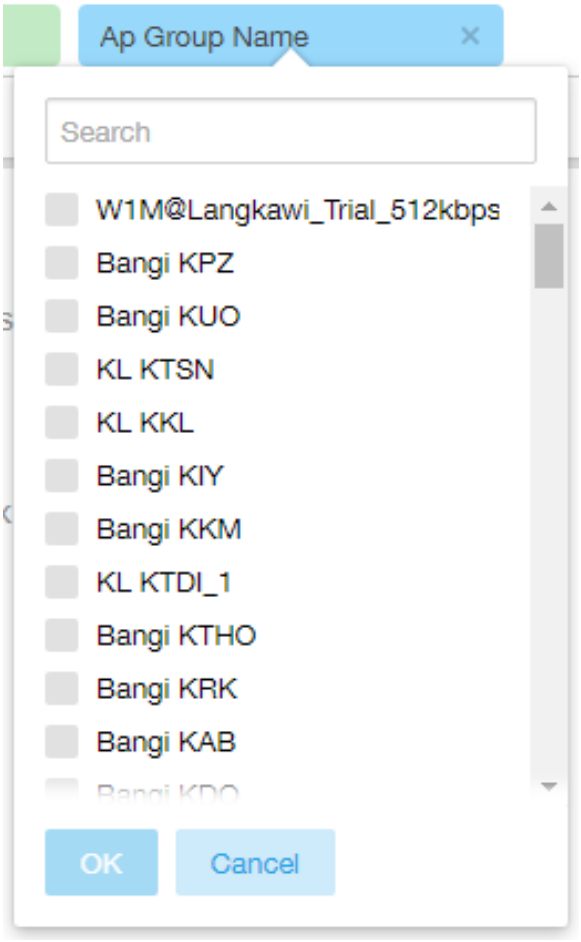
- Current time of day, week, month, quarter, or year
- Previous time of day, week, month, quarter, or year

FIGURE 193 Specific Time Settings



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

FIGURE 194 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.

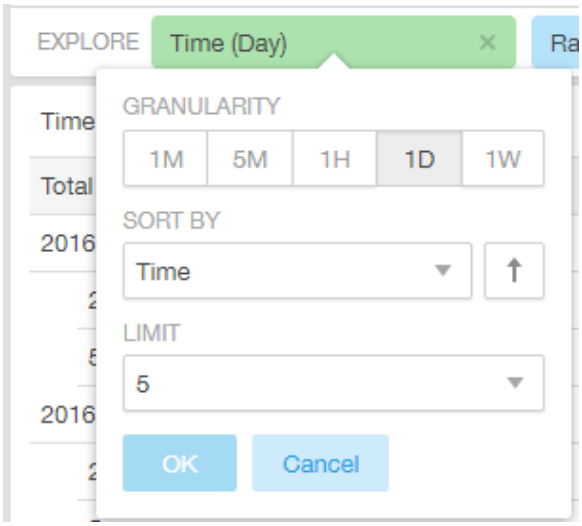
Explore Filter

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

FIGURE 195 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.

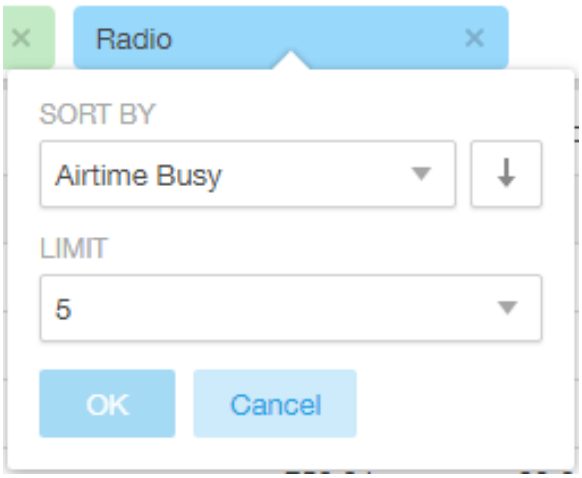
FIGURE 196 Explore Time



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 197 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.

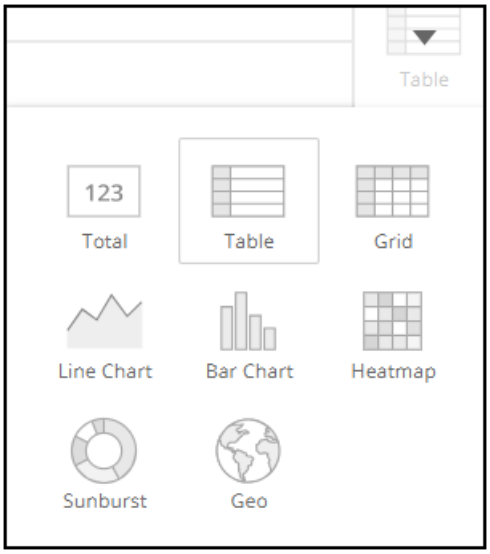
View Outputs Filter

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 198 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 199 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 200 Share Link

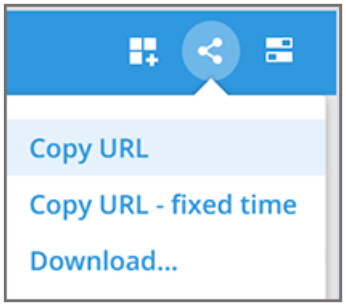
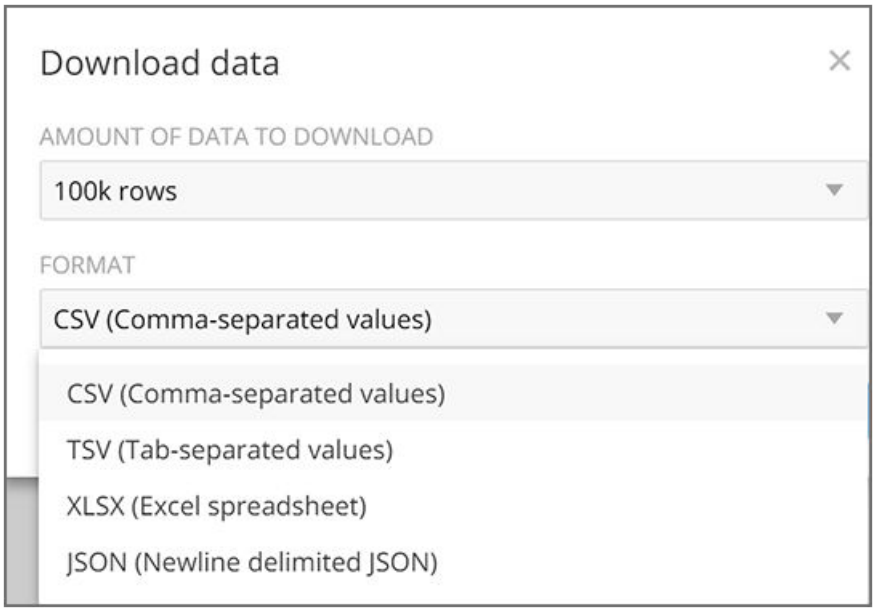


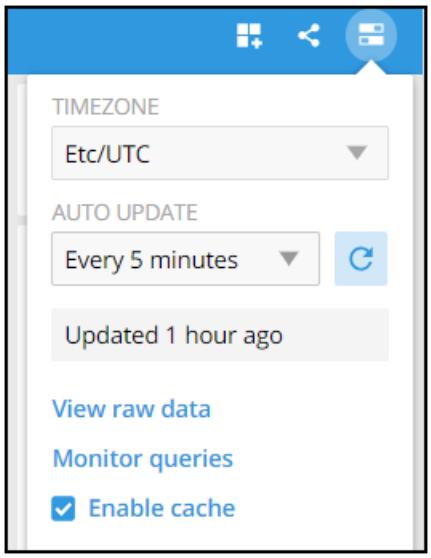
FIGURE 201 Selecting the Amount of Data to Download and the Desired Format



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 202 Options



Pinboard Pane

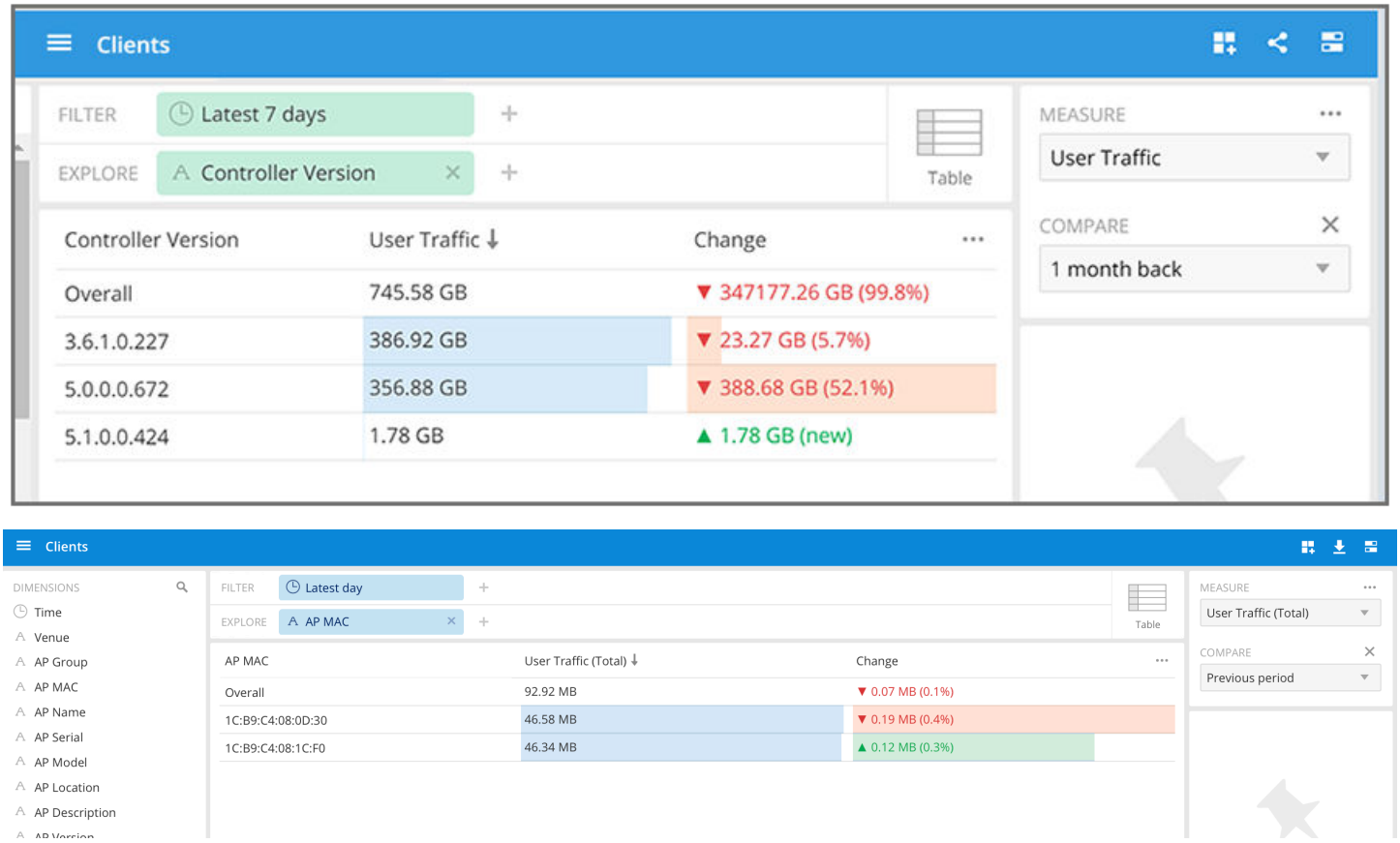
You can click or drag dimensions and pin them on the pinboard. Retain the dimensions for ready reference during visualization.

FIGURE 203 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 204 Comparison Over Time

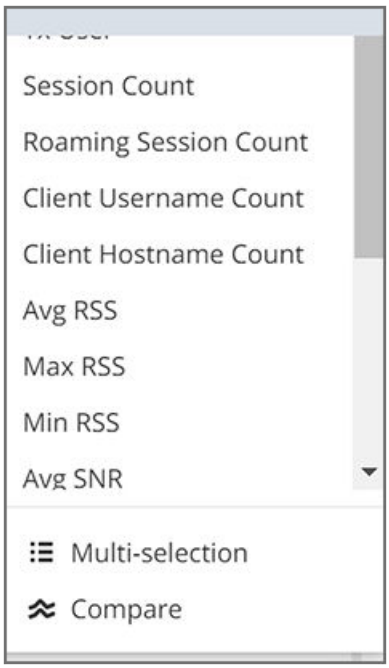


Creating a Data Comparison

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

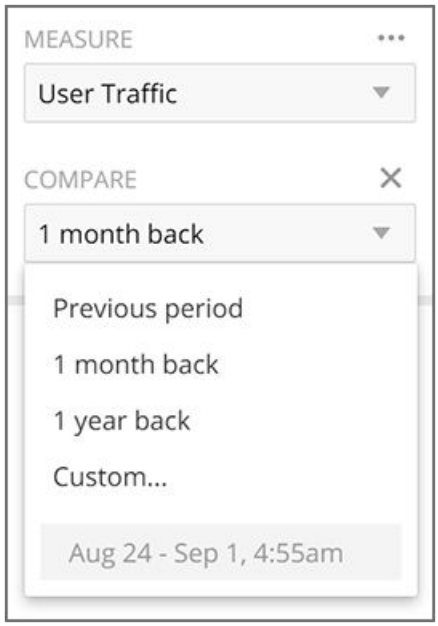
1. From **Data Explorer**, select one of the data cubes.
2. Drag one or more dimensions into the center pane, for example, Controller Version.
3. From the **Measure** list, select one or more measures (use **Multi-Selection** for more than one).
4. From the **Measure** list, select **Compare**.

FIGURE 205 Selecting Compare from the Measure List



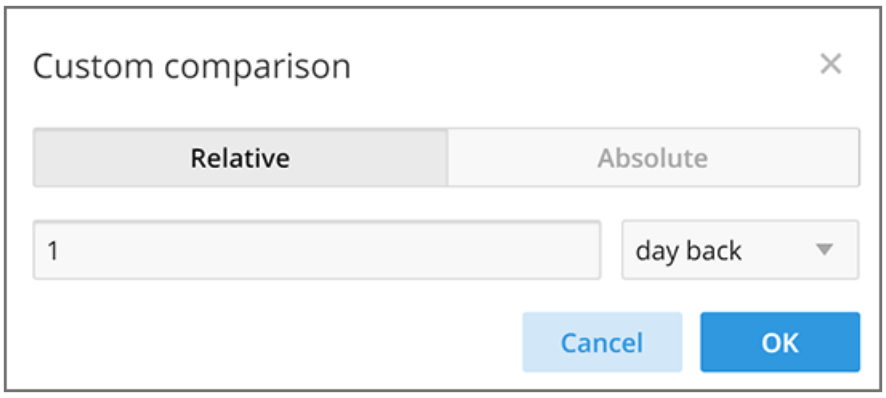
5. If you have already invoked **Compare**, the previous time period you selected is automatically used, and a display such as the one in Figure 204 is displayed. However, if you have not yet used Compare, or if you want to change the current time-period, invoke the **Compare** list:

FIGURE 206 Using the Compare List



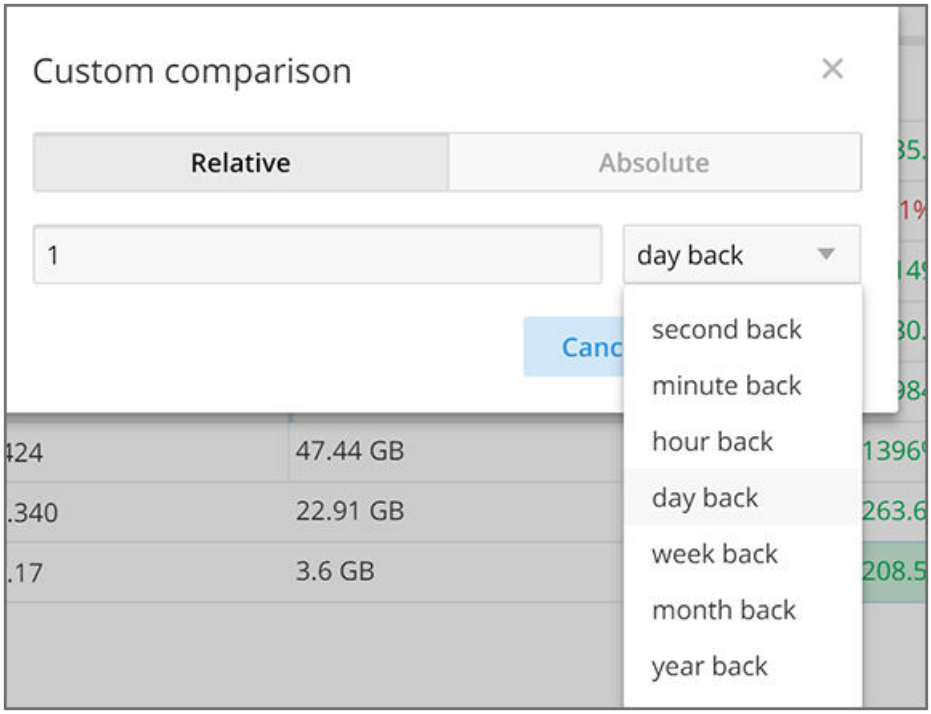
6. (Optional) To customize your choice, click **Custom**. **Custom comparison** dialog box is displayed.

FIGURE 207 Custom Comparison Dialog Box



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

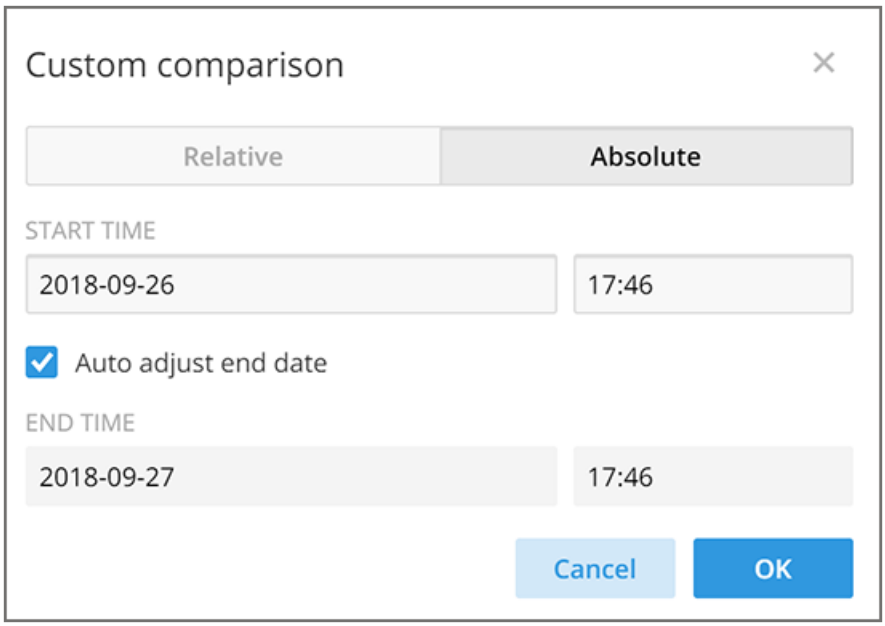
  FIGURE 208 List of Choices from the Relative Measure List



  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 209 Custom Comparison: Absolute Tab

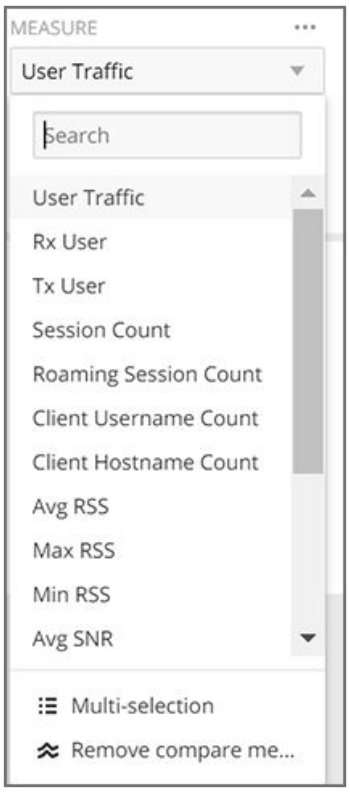


You can change the times as desired, and to have the end date automatically adjusted. Click **OK** to set the custom time period.

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 210 Removing the Compare Measure



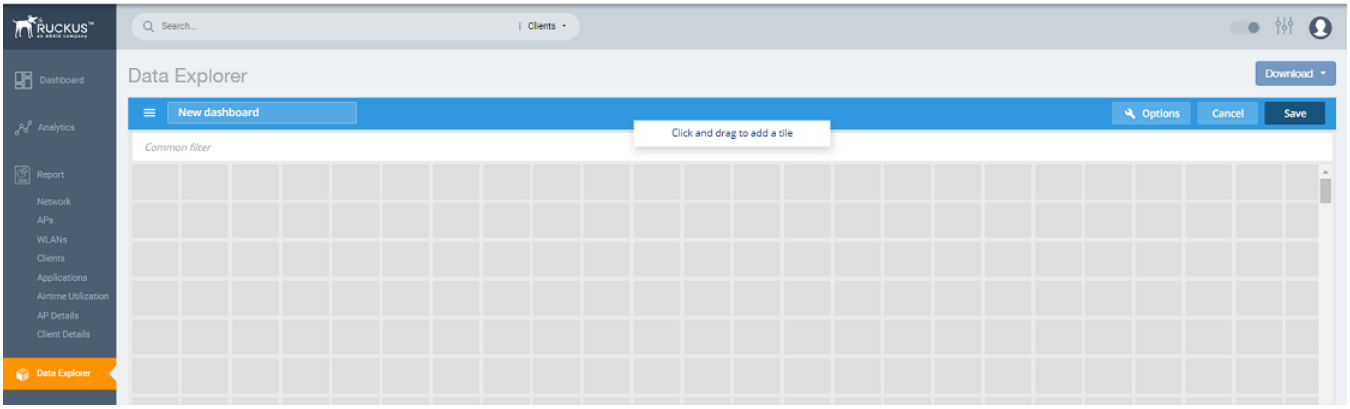
Creating a Data Explorer Dashboard

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**.

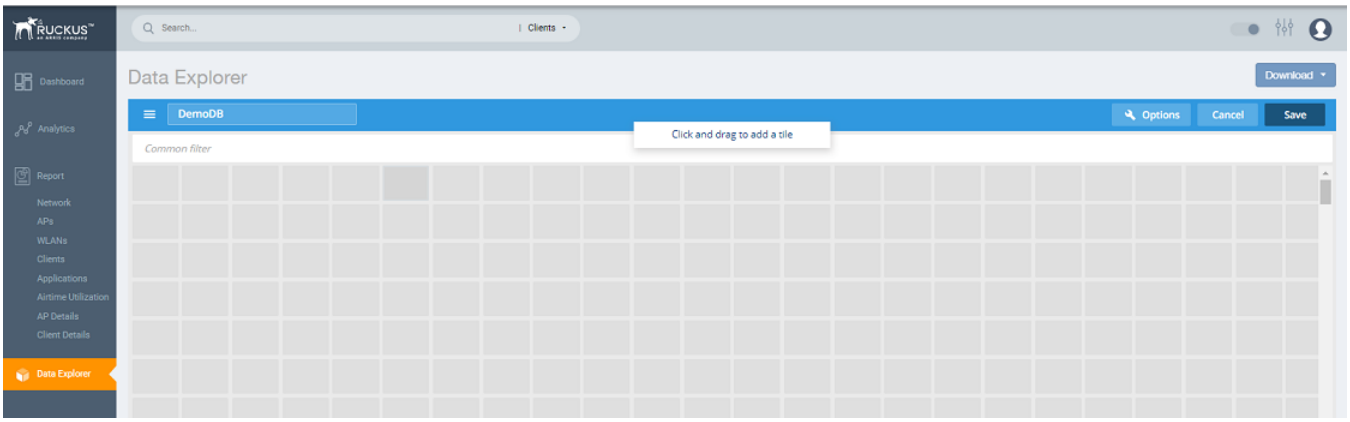
   The **New dashboard** screen is displayed.

   FIGURE 211 New Dashboard Screen



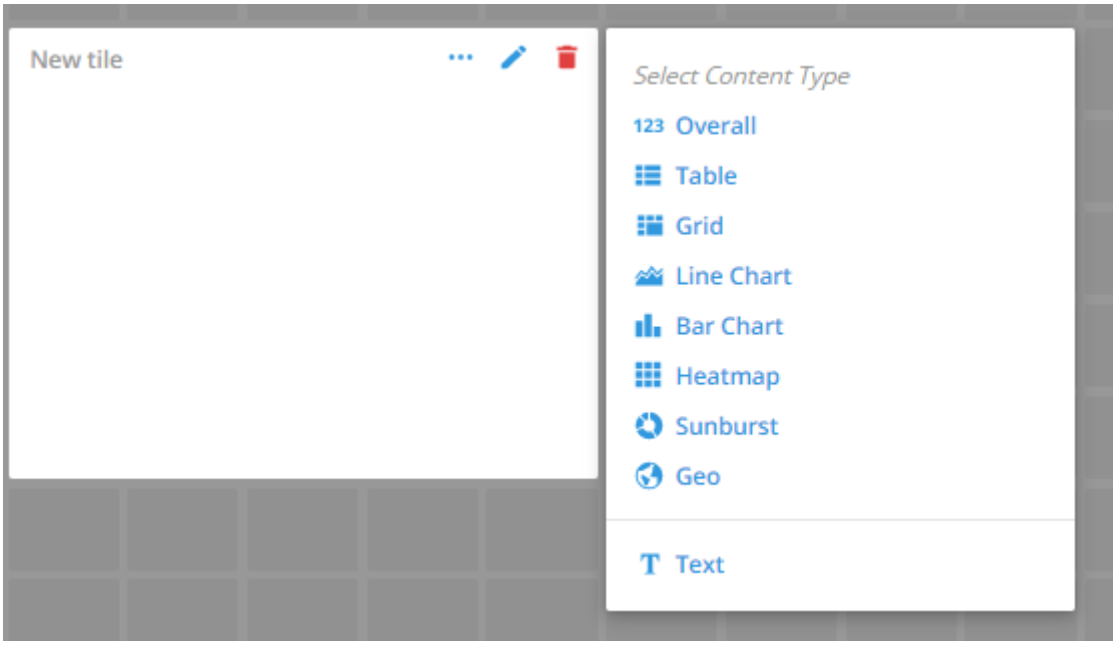
2. Highlight **New dashboard** and enter a name for the dashboard (for example, DemoDB, as shown in the following figure).

   FIGURE 212 Naming the New Dashboard



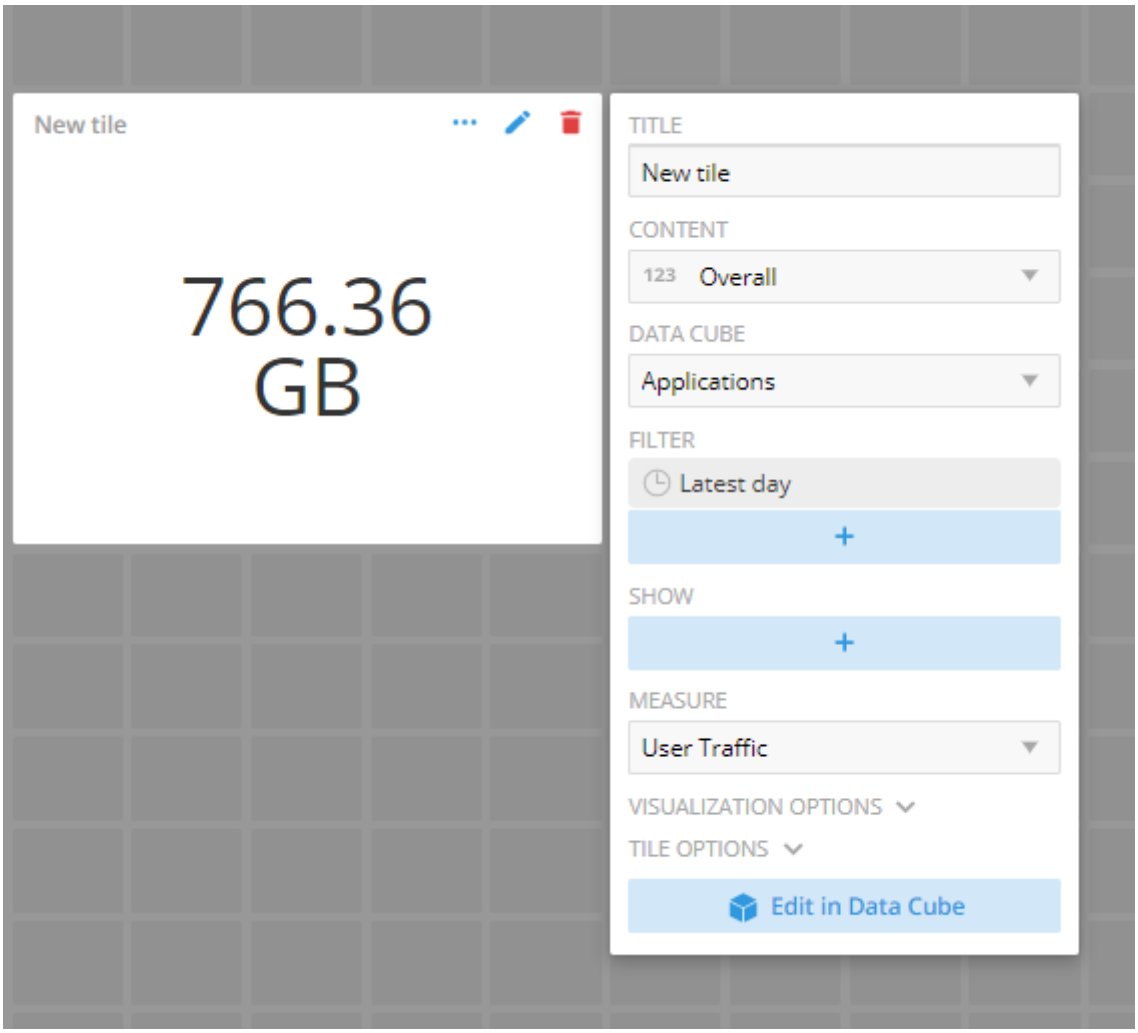
3. Highlight any number of small boxes in the grid on the screen to add a tile to your dashboard. The **Select Content Type** pane is displayed along with the new tile.

FIGURE 213 Adding a Tile to Your Dashboard



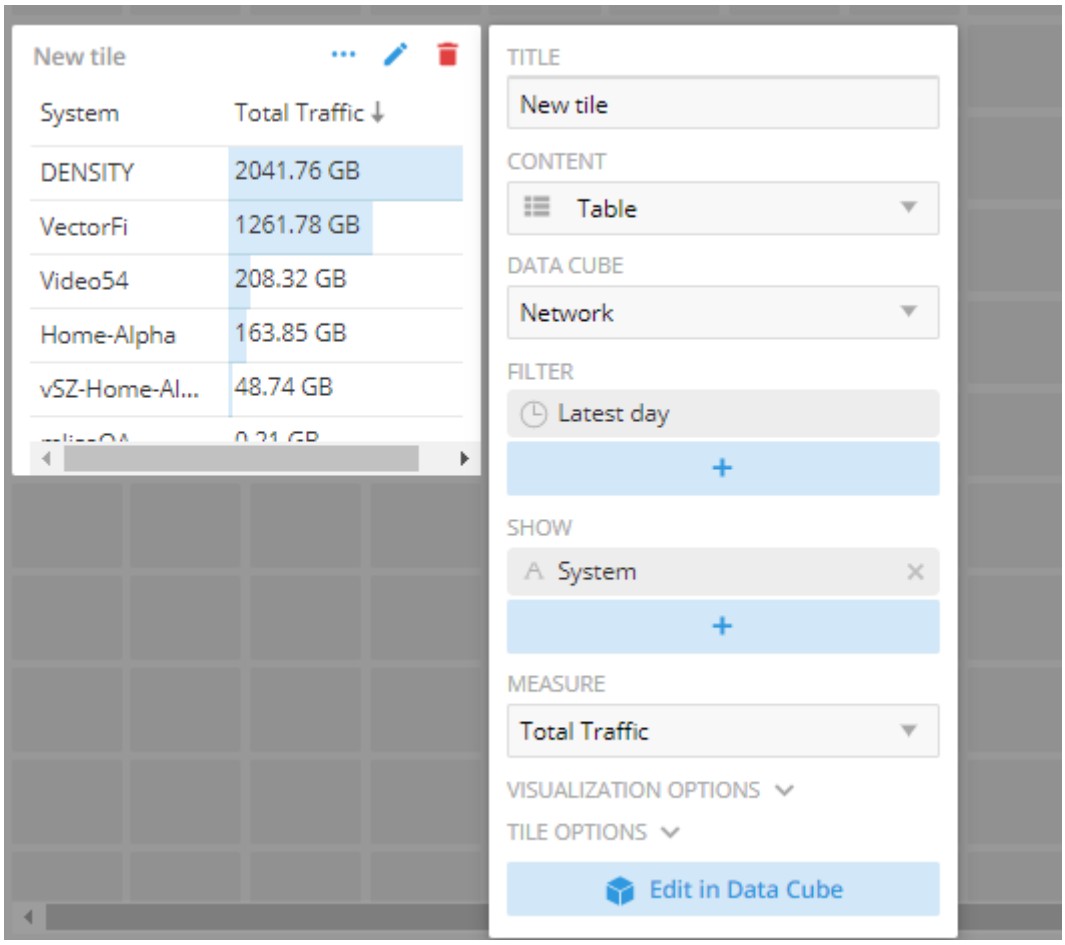
4. Select a content type, for example, 123 Overall, as shown in the following figure

FIGURE 214 New Tile Options for 123 Overall Content Type



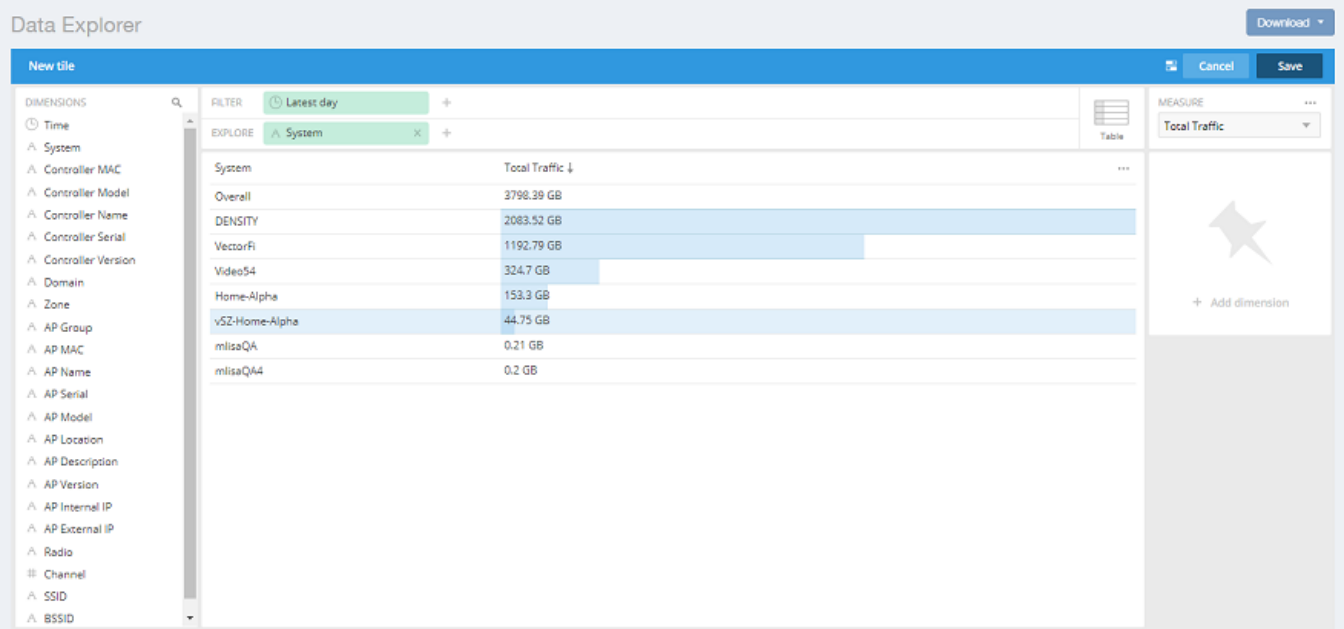
5. Select options to customize the new tile.

FIGURE 215 Selecting Options for New Tile



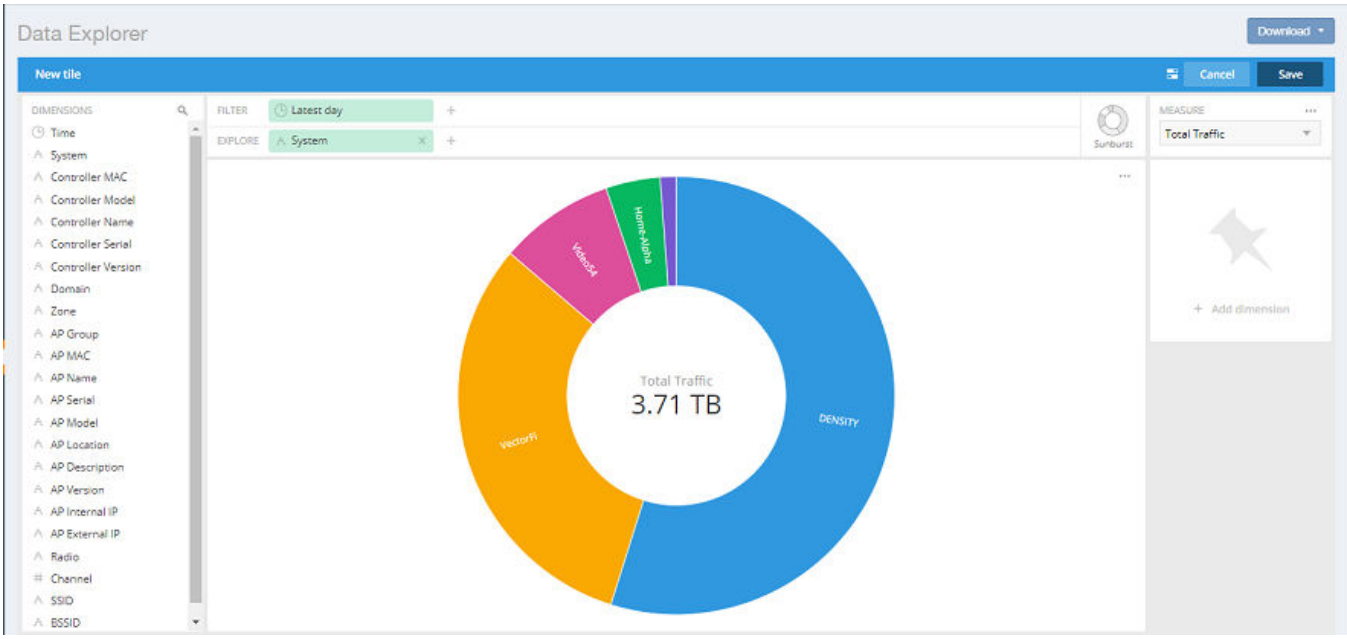
6. Click **Edit in Data Cube** to make changes to the new tile in the data cube.

FIGURE 216 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 217 Sunburst Representation of Tile in Data Cube



8. 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

Actions You Can Perform on an Existing Dashboard

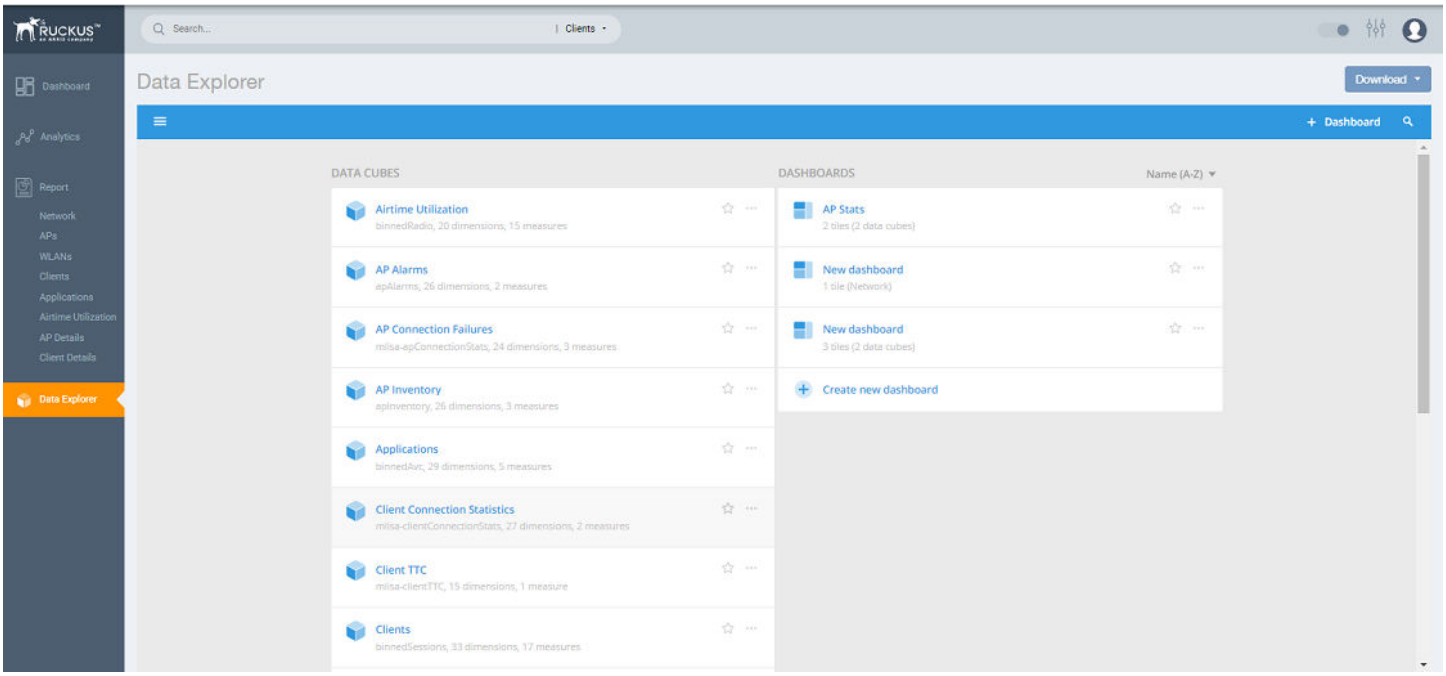
You can perform many actions on an existing dashboard, such as adding or removing tiles, editing existing tiles, deleting tiles and deleting the entire dashboard.

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.

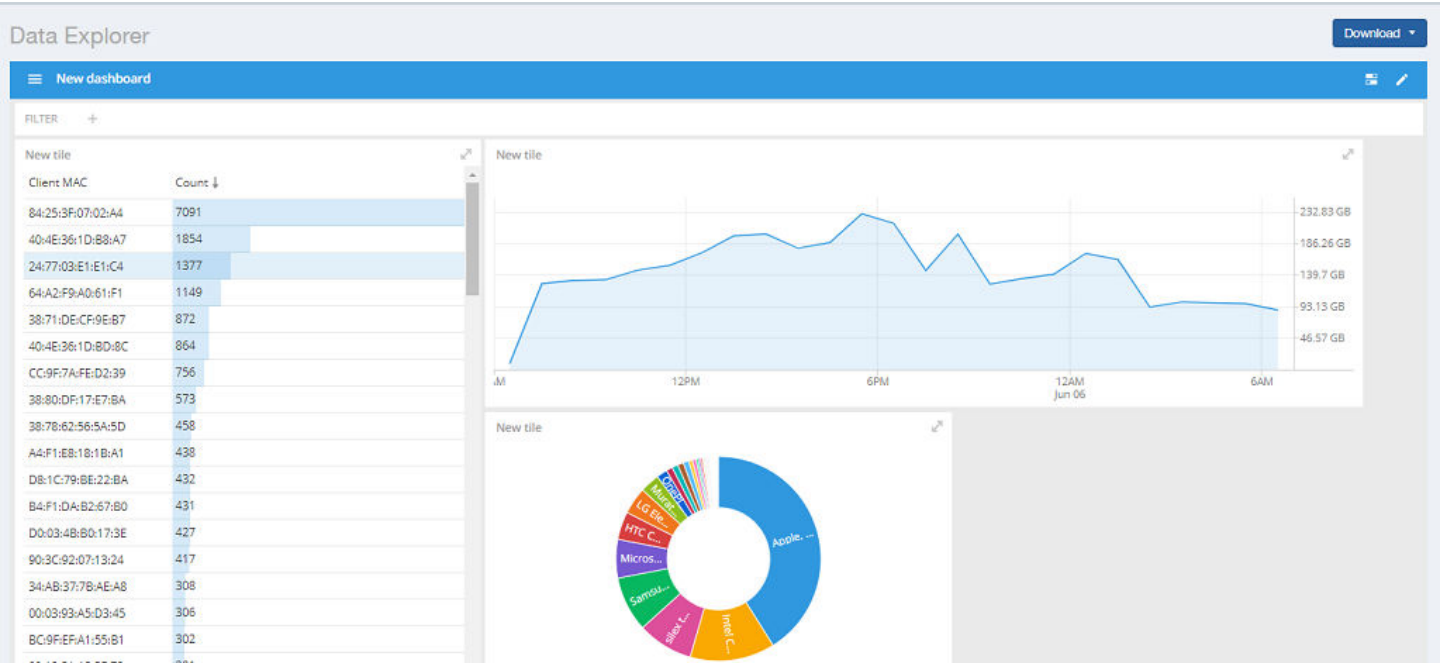
FIGURE 218 Data Cubes and Dashboards in Data Explorer



Editing a Dashboard

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

FIGURE 219 Dashboard Example with Three Tiles



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

FIGURE 220 Dashboard-Editing Icons

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

TABLE 17 Icons for Editing a Dashboard

Icon	Name of Icon	Actions
	Dashboard options	You can change the following settings: • Time zone • Auto-update interval • Enabling or disabling cache

TABLE 17 Icons for Editing a Dashboard (continued)

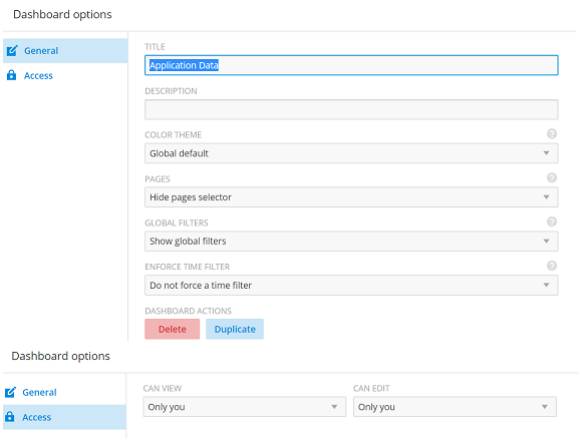
Icon	Name of Icon	Actions
	Edit this dashboard	You can perform the following actions: • Rearrange or resize the tiles. • Make changes to specific tiles within the dashboard by using the icons are displayed for each tile: – Click the three dots icon to duplicate the tile. – Click the pencil icon to add or remove dimensions and measures for the tile, and to change the representation of the data for the tile. – Click the garbage can icon to delete the tile from the dashboard.

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 221 General and Access Options to Edit Dashboards



Administration

- Viewing Onboarded Systems....181
- Managing Users....182
- Managing Resource Groups....183
- Contacting Ruckus Support....186
- Managing Licenses and Assigning APs....187
- Creating Webhooks....190

Viewing Onboarded Systems

You can view the list of your SmartZone controllers that have onboarded to the system and also view additional information regrading 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 181.

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.

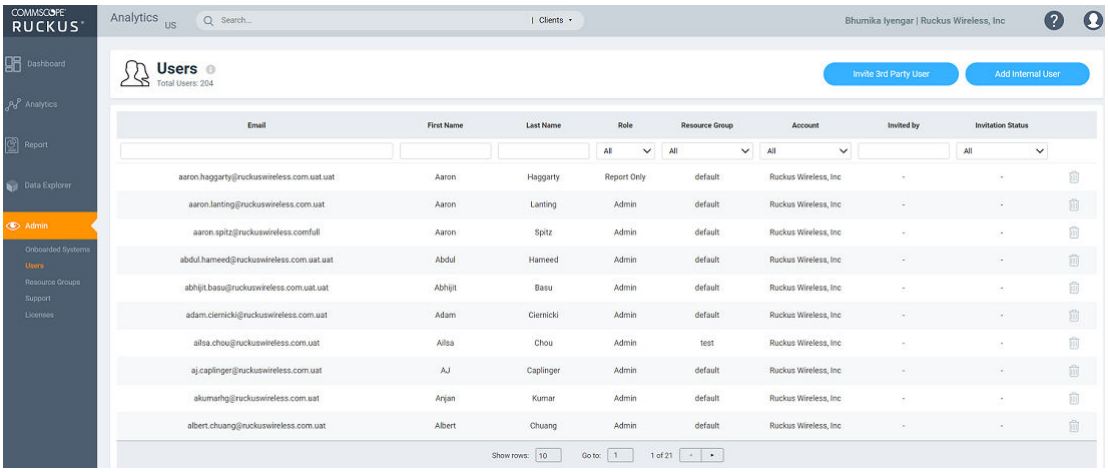
Managing Users

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 222 User Management



   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 acess 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 wifi 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 18 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	Yes	Yes	Yes	No

TABLE 18 Roles and their Privileges (continued)

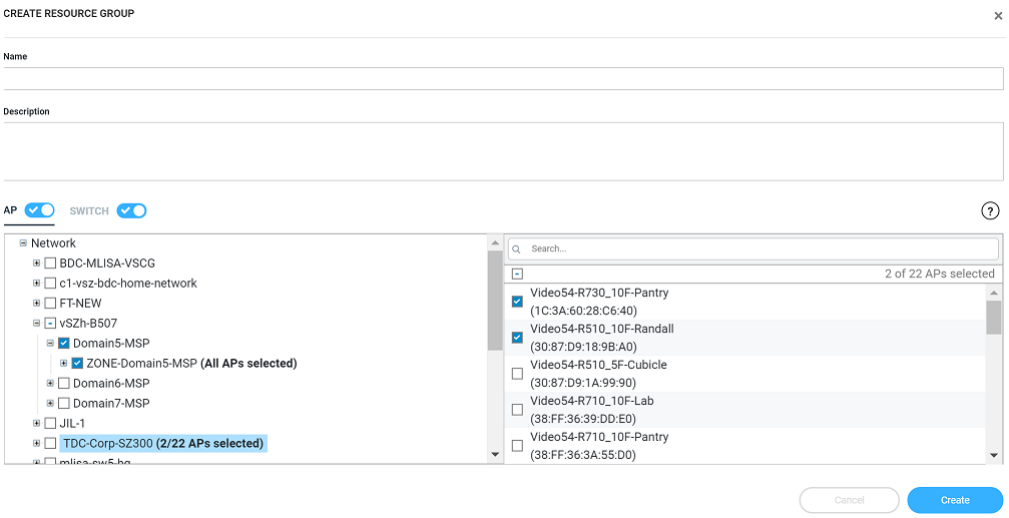
Role	View Reports	UI View Mode	Save Filter	Scheduled Reports	Data Explorer	Admin Control	Resource Group	License Management	Enable RUCKUS Support
Reports	Yes	SCI and Data Explorer	Yes	Yes	Create	No	No	No	No

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 223 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

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**.

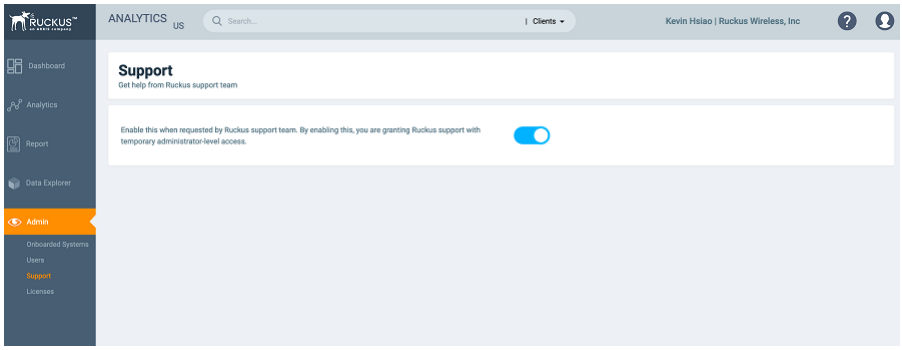
NOTE
Currently, the entire network cannot be selected and included in a resource group.

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 224 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 19 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

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**.

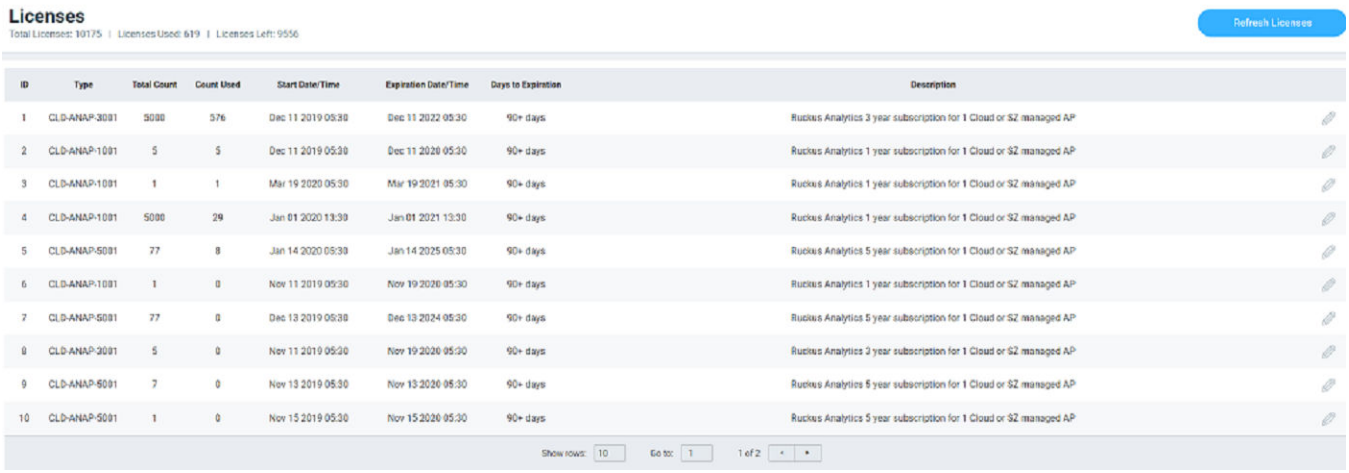
   The **Licenses** page displays the following information:

   - 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.

   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 225 Licenses Page



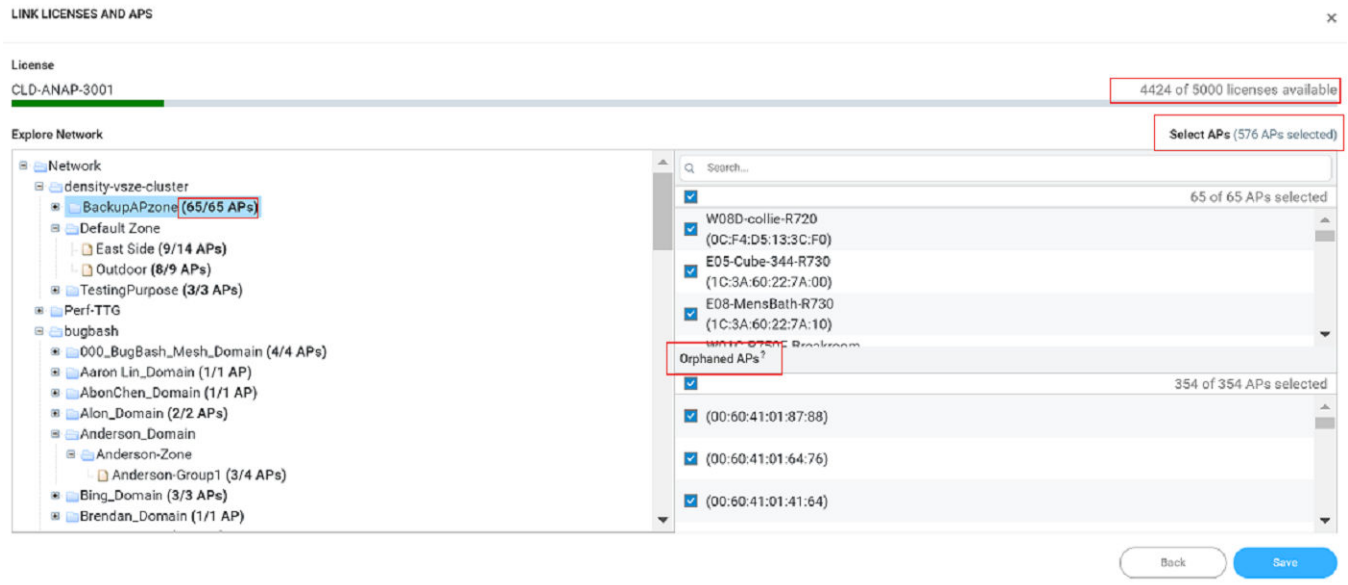
2. Click the edit icon to assign APs to the license selected.

   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 226 Link Licenses and APs 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**.

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 227 Sample Webhook Message with Incident Details

Data structure of incident event from RUCKUS Analytics

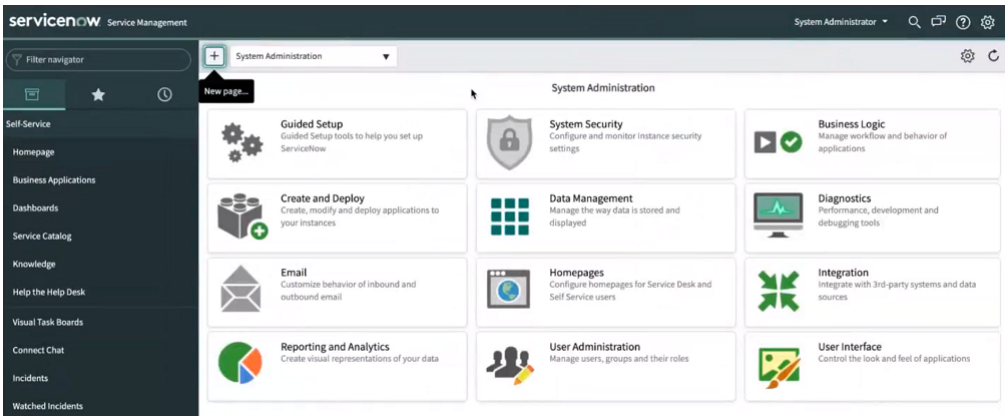
```
{ id: string,                          // Event ID
  type: "incident",                    // Type of webhook event, will be "incident" for now
  secret: string,                      // Webhook secret
  payload: {                           // incident payload
    status: string,                    // Incident status, e.g. "new" | "ongoing" | "finished"
    id: number,                        // 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,          // Imapcted 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 Gro
    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 hiera
    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

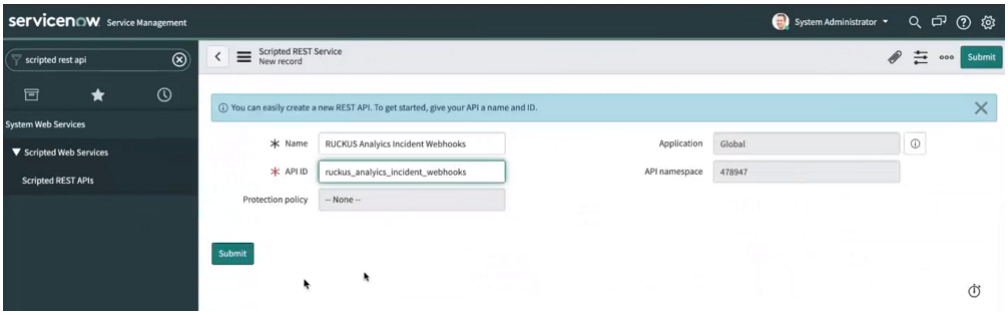
1. Login to the ServiceNow instance

   FIGURE 228 Logging into ServiceNow



2. Under **System Web Services**, select **Scripted Rest APIs**

   FIGURE 229 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);
    }
```

```
    // 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)
    - 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.

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 saved 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.

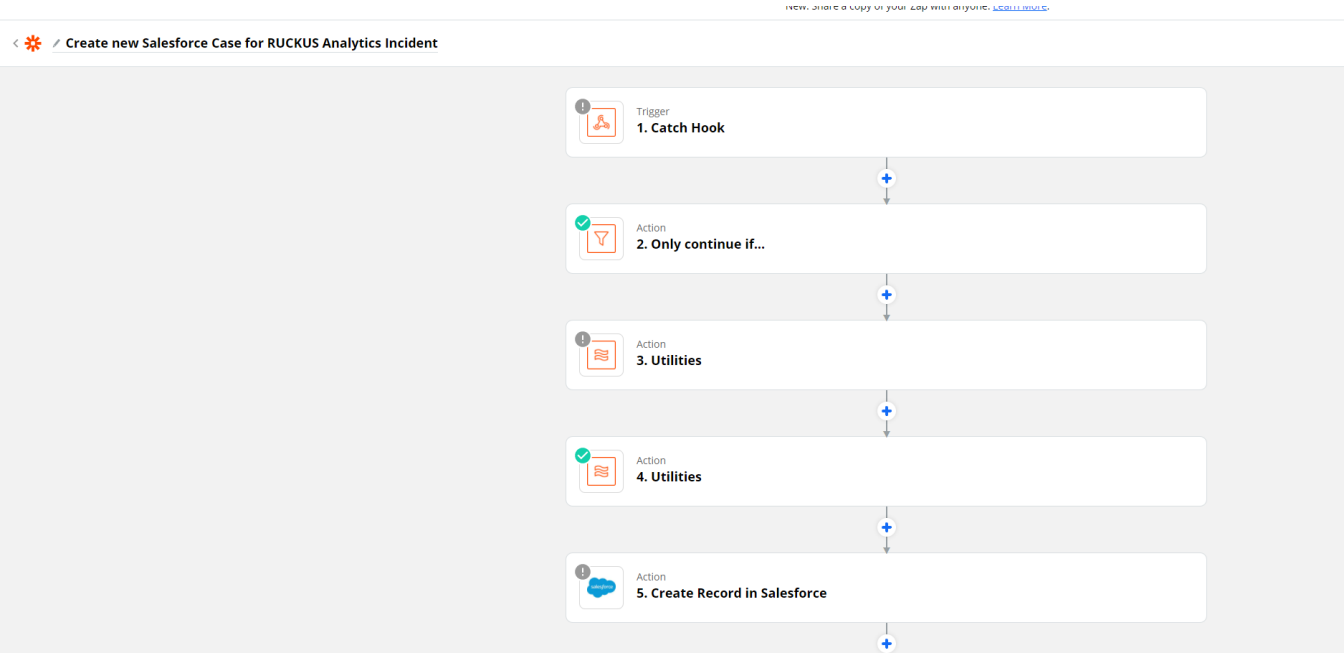
5. Click **Create** to save the configuration.

   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 230 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**

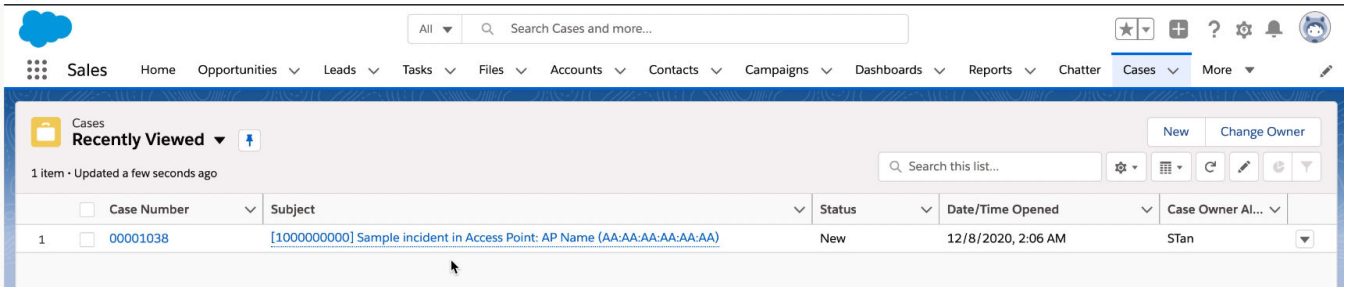
21. In **Create Record in Salesforce**, go to **Choose account** and select your Salesforce account.
22. Under **Setup Action**, select Case as the Salesforce object. Set the other fields as necessary. Modify the fields as required, such as changing the description or assigning the Salesforce case to a particular person or group.

    NOTE
    Do not change the "Subject" as it is used when updating a case.

23. Click **Continue**.

    A Salesforce recorded is now created.
24. Login to Salesforce Web interface. A new case is created as shown.

    FIGURE 231 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

COMMSCOPE®
RUCKUS®

© 2021 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com