USER GUIDE

RUCKUS Analytics User Guide, 3.4

Part Number: 800-73469-001 Rev A
Publication Date: 15 August 2023

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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see https://www.commscope.com/trademarks. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

Contact Information, Resources, and Conventions....9
Contacting RUCKUS Customer Services and Support....9
What Support Do I Need?....9
Open a Case....9
Self-Service Resources....10
Document Feedback....10
RUCKUS Product Documentation Resources....10
Online Training Resources....10
Document Conventions....11
Notes, Cautions, and Safety Warnings....11
Command Syntax Conventions....11

About This Guide....13
New in This Document....13

RUCKUS Analytics Overview....15
RUCKUS Analytics Introduction....15

Logging In to RUCKUS Analytics....17

Navigating the RUCKUS Analytics User Interface....19
Header Panel....19
Search Field....20
Using the Navigation Bar....21

Feature Support Matrix....23

Firewall Ports to Open for RUCKUS Analytics....25

RUCKUS Analytics Dashboard....27
Dashboard Overview....27
Melissa AI Assistant....28
Graphical Rendering of Data in Melissa....31
Melissa AI Assistant on Microsoft Teams....34
Activating Microsoft Teams with Melissa....34
Revoking Microsoft Teams Activation....37
Time Selection Field....38
Incident Severities....38
Scrolling Data Tile....38
Incident Categories....39
Listing Tile....40
Network History Tile....40
Interactive Network Hierarchy....40
Interactive Network Topology....41
Settings....42
Accounts....44

AI Analytics....47
AI Analytics Page....47
Network Filter Menu....48

Date and Time Filter.. 49
Network Node Details.. 50
Severity Filter.. 51
Incident Timeline.. 51
Incidents List Table.. 51
Incident Details Page.. 53
Network Impact Tile.. 55
Insights Tile.. 60
Incident Info Tile.. 61
Recommendations Page.. 62
Health Page.. 66
Unique Connected Clients Graph.. 68
Overview Tab.. 69
Connection Tab.. 71
Performance Tab.. 73
Infrastructure Tab.. 74
Configuration Change Page.. 75
Configuration Change Tile.. 76
Configuration Change Listing Tile.. 77
Health Tile.. 77
Client Troubleshoot Page.. 78
Packet Capture (PCAP).. 80
Occupancy Page.. 81
Utilization Tile.. 84
Total In-Site Visitors Tile.. 84
Avg. Dwell Time Tile.. 84
Sites Overview Chart.. 84
Sites Listing Table.. 85
Site Report.. 85
AI-Driven Cloud Radio Resource Management 89
AI-Driven Cloud RRM Overview.. 89
Benefits of AI-Driven Cloud RRM for an End User.. 89
Advantages of AI-Driven Cloud RRM for a Network Administrator.. 90
How AI-Driven Cloud RRM Works.. 90
AI-Driven Cloud RRM Considerations.. 92
AI-Driven Cloud RRM Behavior in 2.4 GHz.. 93
AI-Driven Cloud RRM with Dynamic Frequency Selection (DFS) Channels.. 93
AI-Driven Cloud RRM Operation at Zone and AP Level.. 93
AI-Driven Cloud RRM Interoperability in a Mixed AP Deployment.. 94
AI-Driven Cloud RRM AP Transmit Power.. 94
Network Health.. 97
Testing Client Services.. 97
Network Health Test Report.. 101
Overview Tab.. 101
Details Tab.. 102
Testing Video Call Quality.. 105
Video Call QoE Workflow.. 105
Creating a Test Call.. 108
Video Call Test Report.. 110

Participants Details Table........ 111
Zoom Call Statistics Tile........ 111

Report........ 115
Using the Overview Dashboard: Content Panel........ 115
Wireless Network Report........ 118
Overview Tile........ 118
Traffic Distribution Tile........ 119
Top APs by Traffic Tile........ 120
Top APs by Client Count Tile........ 121
Traffic Trend Graphs........ 122
Traffic Over Time Table........ 124
Wired Network Report........ 124
Overview Tile 125
Traffic Distribution by Switch Model and Port Speed Chart 126
Top Switches by Traffic Tile........ 127
Top Switches by PoE Usage Tile........ 128
Top Switches by Errors Tile........ 129
Traffic Trend Graph........ 129
Error Trend Graph........ 130
Inventory - APs Report........ 131
Overview Tile........ 132
Top APs by Offline Duration Tile........ 132
AP Count Trend Graph........ 133
AP Status Trends Tile........ 133
Top AP Models........ 134
Top AP Software Versions Tile........ 135
Top 10 AP Reboot Reasons Tile........ 136
Top APs by Reboot Count Tile........ 136
Top 10 AP Alarm Types Tile........ 137
APs Configured in Multiple Systems Tile........ 138
AP Details for Online/Offline Status Table........ 138
AP Details for Other Statuses Table........ 139
Inventory - Controllers Report........ 139
Overview Tile........ 140
Resource Utilization Table 141
License Utilization Table........ 141
KRACK Assessment Table........ 142
Inventory - Switches Report........ 142
Overview Tile 143
Switch Count Trend Graph........ 144
Top Switch Software Versions Tile........ 144
Top Switch Models Tile 145
Port Status Trends Tile........ 146
WLAN Report 147
Overview Tile........ 147
SSID Changes Over Time Tile........ 148
Top SSIDs by Traffic Table........ 148
Top SSIDs by Client Count Tile........ 149
Active SSIDs Trend Graphs........ 150
Clients Report........ 151

Overview Tile...... 152
Top 10 Unique Clients by Traffic Chart...... 153
Clients Details...... 153
Unique Clients Trend Over Time Graphs...... 154
Top 10 OS by Client Count Tile...... 155
Top 10 Manufacturers by Client Count Tile 156
Top 10 Authentication Methods by Client Count Tile...... 156
Client Health Dashboard...... 157
Client Health Report...... 157
Applications Report...... 160
Overview Tile...... 161
Top Applications by Traffic...... 162
Top Applications by Client Count Tile...... 162
Airtime Utilization Report...... 163
Overview Tile...... 164
Top 10 APs by Airtime Utilization Chart...... 165
Top APs by Airtime Utilization for 2.4 GHz Table...... 165
Top APs by Airtime Utilization for 5 GHz Table...... 166
Airtime Utilization Trend Graph...... 166
Airtime Utilization Over Time Table...... 167
AP Details Report...... 168
Summary Tile...... 169
Performance Tile 169
Details Tile...... 169
Stats Tile 170
Uptime History Graph...... 170
Traffic Trend Graphs...... 171
Unique Clients Trend Over Time Graphs 173
Top 10 Clients by Traffic Volume Tile 173
Top 10 Applications by Traffic Volume Tile...... 174
Top SSIDs by Traffic Table...... 174
Sessions Table 175
RSS Trend Graph...... 175
SNR Trend Graph...... 176
Airtime Utilization Trend Graphs...... 176
Clients Details Table 177
Alarms Table...... 177
Events Table...... 177
Anomalies Graph...... 178
Client Details Report...... 178
Summary Tile...... 179
Stats Tile...... 180
Client Details Stats...... 180
Traffic Trend Tile...... 181
RSS Trend Tile...... 182
SNR Trend Tile...... 182
Sessions tile...... 182
Switch Details Report Dashboard...... 183
Switch Details Report...... 183
Comparison Reports Dashboard...... 188

Compare Filters 188
PCI Profiles........ 192
Creating a PCI Profile........ 193
Opening and Downloading a PCI Profile........ 195
Editing or Deleting a PCI Profile........ 196

Data Studio........ 197
Data Studio........ 197
Home Tab........ 199
Charts Tab........ 200
Creating a Chart........ 200
Create a Report Schedule for the Chart........ 204
Dashboard Tab........ 207
Creating a Dashboard........ 207
Create a Report Schedule for the Dashboard........ 209
Export and Import Dashboard........ 210
Schedules Tab........ 211
Creating a Schedule........ 212
Dataset Filters........ 214
Columns Filter........ 215
Metrics Filter........ 227

Administration........ 233
Viewing Onboarded Systems........ 233
Onboarding the controller to RUCKUS Analytics........ 234
Managing Users........ 235
Adding a Brand........ 236
Managing Resource Groups........ 236
Labels........ 239
Creating Labels........ 239
Contacting Ruckus Support........ 241
Managing Licenses and Assigning APs........ 241
Viewing Schedules........ 245
Creating Webhooks........ 246
Integrating RUCKUS Analytics Incident Webhook with ServiceNow Application........ 247
Create a New Salesforce Case for RUCKUS Analytics Incident using Zapier Application........ 250
Updating an Existing Salesforce Case for RUCKUS Analytics Incident using Zapier Application........ 252

Brand 360........ 253
Brand 360 Overview........ 253
Brand Invitation........ 253
Accepting the Brand Invitation........ 255
Brand 360 Dashboard........ 256
Naming Convention........ 259
Data Studio 261
Labels........ 261

Appendix........ 263
AP - Client Connection Message Mapping........ 263

Contact Information, Resources, and Conventions

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

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.ruckusnetworks.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://community.ruckuswireless.com
- 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.

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.ruckusnetworks.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://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

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.
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.

About This Guide

- New in This Document....... 13

New in This Document

TABLE 2 Key Features and Enhancements in RUCKUS Analytics 3.4 (15 August 2023)

Feature	Description	Reference
AI-Driven Cloud RRM AP Transmit Power	**Updated**: This feature automatically identifies co-channel interference and recommends methods to reduce it in high-density deployment environments by adjusting AP transmit power. This optimization aims to create an ideal channel plan by eliminating interfering links and ensuring no coverage gaps. It enhances channel planning by eliminating disruptive links, preventing coverage gaps, and introduces 'Tx power control' alongside 'Channel plan' and 'Channel bandwidth' adjustments, optimizing customer networks and boosting throughput by minimizing interference.	AI-Driven Cloud RRM Overview on page 89
PCAP Report	**Updated**: Added packet capture feature information, which is a collection of packets generated for all failure events with respect to the specific client.	Client Troubleshoot Page on page 78
Minor editorial updates	**Updated**: Minor editorial updates were made throughout the Guide.	Throughout the guide.

RUCKUS Analytics Overview

- RUCKUS Analytics Introduction.. 15

RUCKUS Analytics Introduction

RUCKUS Analytics is a cloud service that delivers robust service assurance for IT and business intelligence to line-of-business stakeholders to help customers get the most from their enterprise network. Powered by artificial intelligence (AI) and machine learning (ML) algorithms, this cloud service simplifies operations by automatically classifying service incidents by severity-tracing root causes, and recommending steps for remediation. Artificial intelligence automatically recommends configurations that optimize the RF environment in the customers network. RUCKUS Analytics enables line-of-business stakeholders to define and monitor business key performance indicators (KPIs) for better business outcomes.

Smartzone controllers, access points, and switches serve as data sources, that measure and collect various key performance indicators (KPIs), connectivity status and flows, traffic, applications, and more. The data is packaged by the AP, switch, or controller as lightweight streaming telemetry and sent to the cloud through a secure transport. Once in the cloud, data is ingested into a scalable and efficient data warehouse, analyzed using machine learning and artificial intelligence 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.
- AI 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.
- Service Validation: Provides comprehensive end-to-end testing mechanism to validate LAN, WAN and connectivity to application servers.
- Reports: Leverages and displays pre-built reports and charts to understand network usage and inventory.
- Data Studio: Provides a fast and intuitive reporting tool that helps to create and edit charts and dashboards.
- Admin: Provide the list of SmartZone controllers that have onboarded to the system and additional information regrading their connection status, firmware versions, and so on.

Logging In to RUCKUS Analytics

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

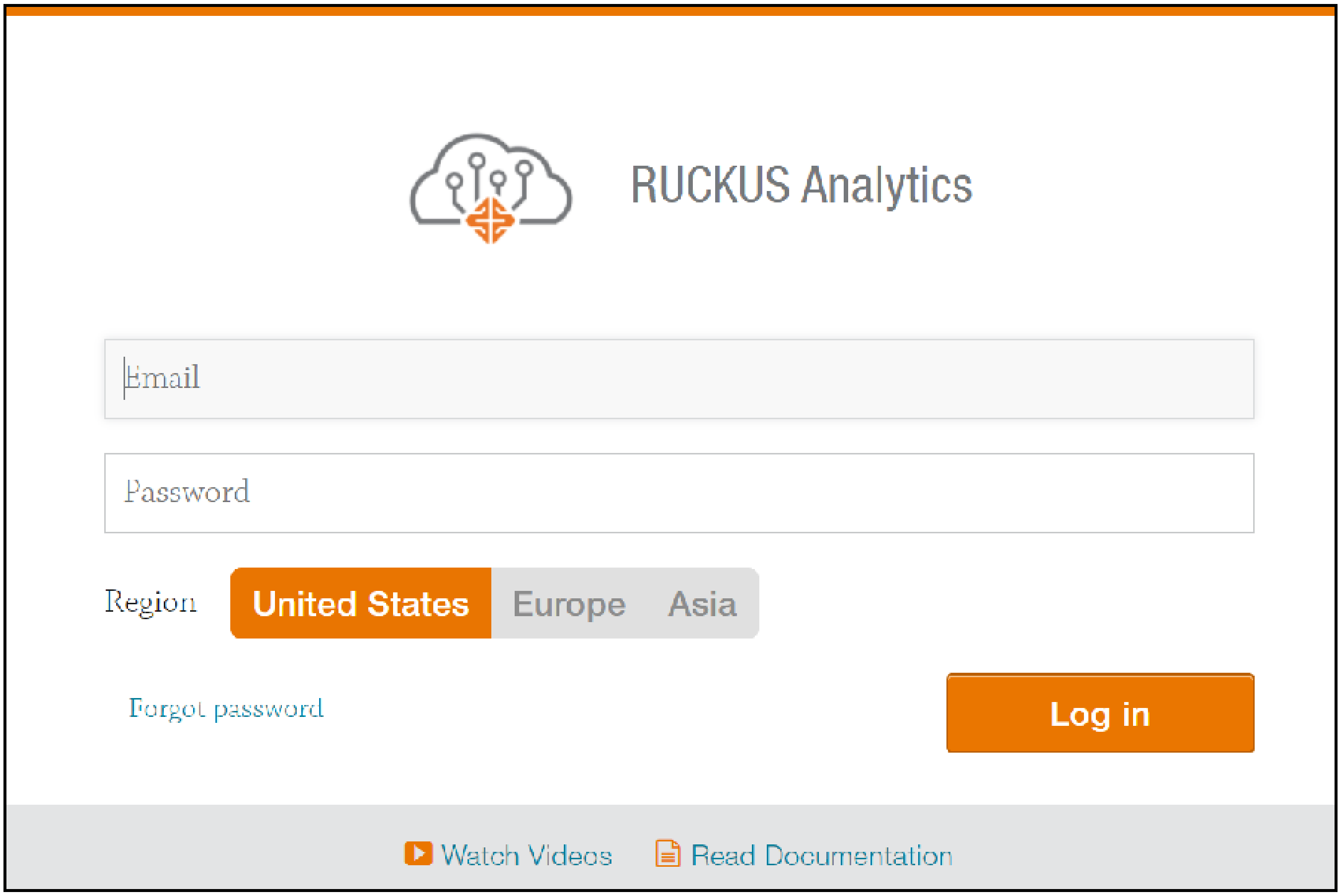
To access on-prem SmartZone RUCKUS Analytics and RUCKUS Analytics from RUCKUS Cloud, refer https://support.ruckuswireless.com/articles/000011818.

Complete the following steps to log in:

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

   The RUCKUS Analytics dashboard loads in your browser.

FIGURE 1 RUCKUS Analytics Login Page



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

Navigating the RUCKUS Analytics User Interface

- Header Panel.. 19
- Search Field 20
- Using the Navigation Bar.. 21

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

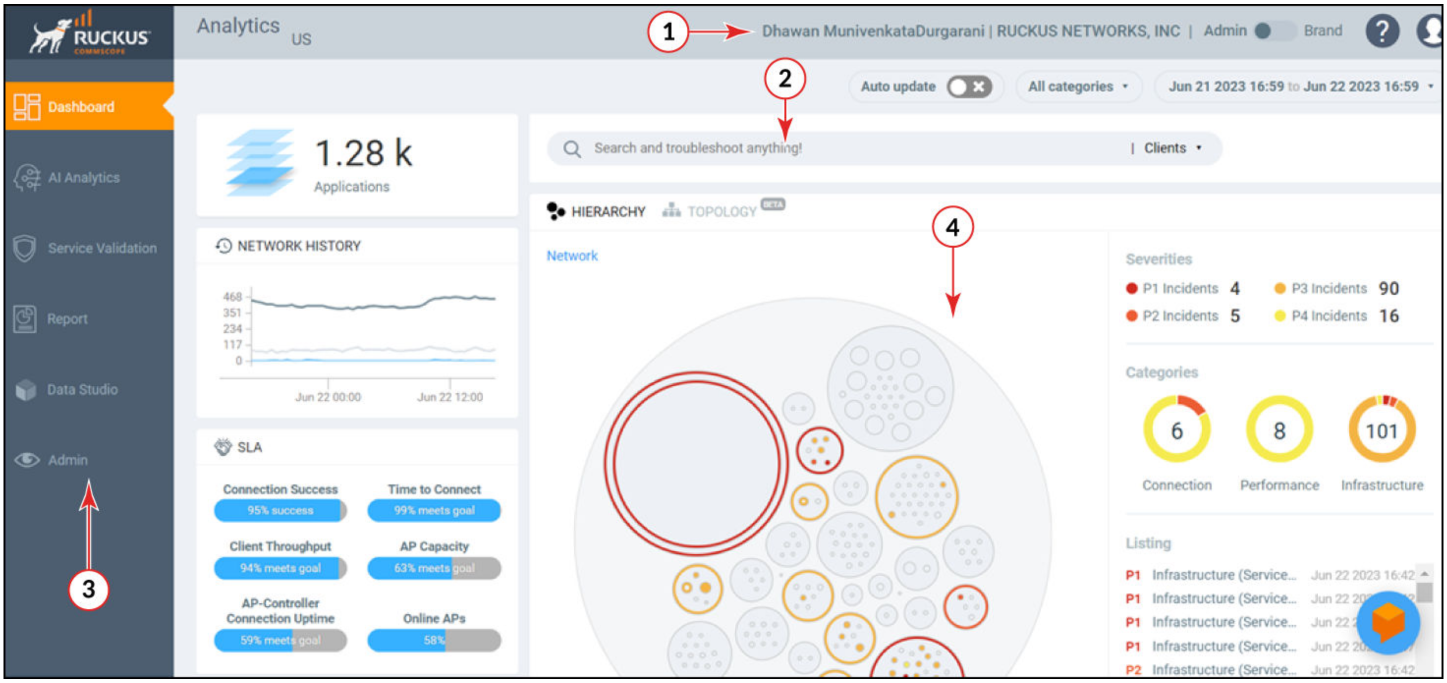


TABLE 3 Identifying RUCKUS Analytics Web Interface Components

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 Profile** : Allows you to 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, recommendations, and License expiry.
- **Accounts** : Displays the total number of user accounts, role associated with the user account, name of the inviter, and the status of the invitation.
- **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 4 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.

TABLE 4 Search Types (continued)

Search Type	Link Icon	Link Destination
	📈	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 27.
- AI Analytics: Allows exploration and drill-down on incidents, client impact areas, and network health requirements. For more information, refer to AI Analytics Page on page 47.
- Service Validation: Provides ability to create comprehensive end-to-end tests to validate LAN, WAN and connectivity to application servers. For more information, refer to Network Health on page 97
- Report: Provides pre-built reports and charts to understand network usage and inventory. For more information, refer to Report on page 115.
- Data Studio: Provides a fast and intuitive reporting tool that helps to create and edit charts and dashboards. For more information, refer to Data Studio on page 197.
- Admin: Provide the list of SmartZone controllers that have onboarded to the system and additional information regrading their connection status, firmware versions, and so on. For more information, refer to Administration on page 233.

Feature Support Matrix

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

TABLE 5 Feature-Software Compatibility Matrix

Feature	Supported SZ Release	Supported ICX FastIron Release
Switch Insights	5.2.1 and later	8.0.95 and later
Service Validation	5.2.1+KSP (MLISA_SERVICE_VALIDATION_5_2_1_811419.ksp) + AP patch (5.2.1.0.1038)	
CPU Insight	5.2.1 and later	
TTG Insight	5.2.1 and later	
All Released RUCKUS Analytics Features	5.1.2 and later	
AI Driven Cloud RRM	5.2.2 and later	
Dynamic PCAP	6.1.2 and later	

Firewall Ports to Open for RUCKUS Analytics

The following table lists the ports that must be opened in the network firewall to ensure that managed SmartZone (SZ) or Virtual SmartZone (vSZ) can communicate successfully with RUCKUS Analytics.

To allow RUCKUS Analytics to properly function, configure your firewall according to the following guidelines. These URLs and IPs must always be whitelisted & available.

Verify that your firewall allows outbound connectivity (port 443). You must allow the network traffic initiated from the SmartZone and vSZ to the above URLs & IPs.

US users:

- https://ruckus.cloud (34.102.183.44)
- https://messagehub.analytics.ruckus.cloud (34.69.139.151)
- https://serviceloc.ruckuswireless.com (23.236.63.97)

EU users:

- https://eu.ruckus.cloud (34.107.197.242)
- https://messagehub.analytics.eu.ruckus.cloud (34.89.193.24)
- https://serviceloc.ruckuswireless.com (23.236.63.97)

APAC users:

- https://asia.ruckus.cloud (35.190.34.117)
- https://messagehub.analytics.asia.ruckus.cloud (34.96.208.196)
- https://serviceloc.ruckuswireless.com (23.236.63.97)

TABLE 6

Service Name	URL and Region	Purpose
RUCKUS Cloud	https://ruckus.cloud (US) https://eu.ruckus.cloud (EU) https://asia.ruckus.cloud (APAC)	Used for the administration portal of Ruckus Cloud. The IP for this service is anycast and globally load balanced for performance. Data processing and compute is done in US (US) / Germany (EU) / Hong Kong (APAC).
Message Hub	https://messagehub.analytics.ruckus.cloud (US) https://messagehub.analytics.eu.ruckus.cloud (EU) https://messagehub.analytics.asia.ruckus.cloud (APAC)	Used by the SZ to send analytics data to the cloud. This is hosted in US (US) / Germany (EU) / Hong Kong (APAC).
Service Location	https://serviceloc.ruckuswireless.com	Used by the SZ to determine the correct endpoints to connect to. This is hosted in the United States. No analytical data will flow to this endpoint but connectivity is required for service discovery.

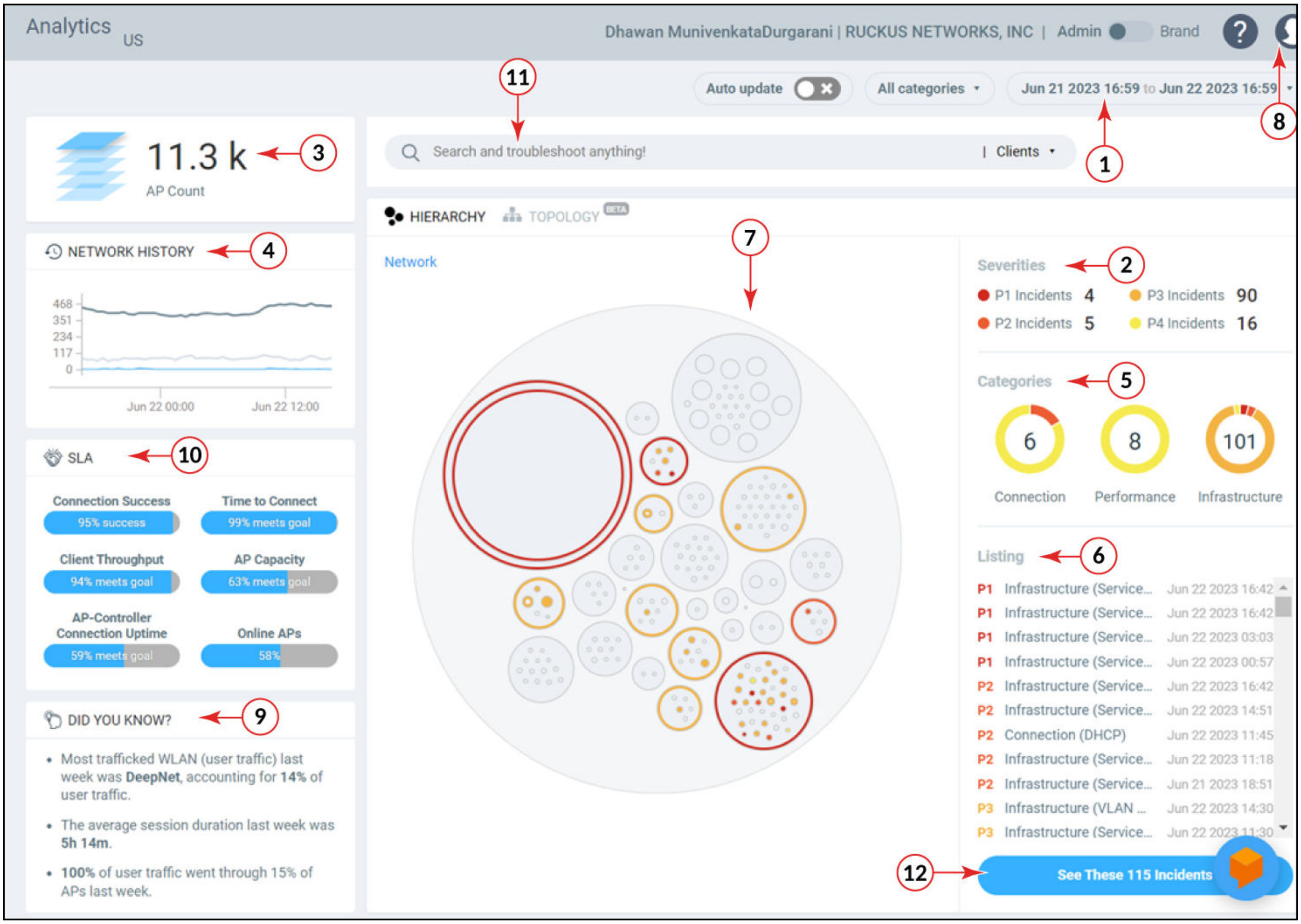
RUCKUS Analytics Dashboard

- Dashboard Overview... 27

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 19 more information.

FIGURE 3 RUCKUS Analytics Dashboard



- Most trafficked WLAN (user traffic) last week was **DeepNet**, accounting for **14%** of user traffic.
- The average session duration last week was **5h 14m**.
- **100%** of user traffic went through 15% of APs last week.

P1 Infrastructure (Service... Jun 22 2023 16:42
P1 Infrastructure (Service... Jun 22 2023 16:42
P1 Infrastructure (Service... Jun 22 2023 03:03
P1 Infrastructure (Service... Jun 22 2023 00:57
P2 Infrastructure (Service... Jun 22 2023 16:42
P2 Infrastructure (Service... Jun 22 2023 14:51
P2 Connection (DHCP) Jun 22 2023 11:45
P2 Infrastructure (Service... Jun 22 2023 11:18
P2 Infrastructure (Service... Jun 21 2023 18:51
P3 Infrastructure (VLAN ... Jun 22 2023 14:30
P3 Infrastructure (Service... Jun 22 2023 11:30

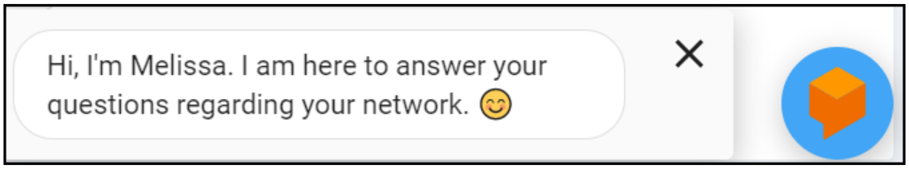
The dashboard comprises a number of components that provide a summary of network health:

TABLE 7 Dashboard Elements

Callout Number	Dashboard Elements
1	Time Selection field
2	Incident Severities
3	Scrolling Data tile
4	Network History tile
5	Incident Categories
6	Listing tile
7	Interactive Network Hierarchy
8	Settings
9	Did you know?
10	SLA
11	Search field
12	AI Assistant

Melissa AI Assistant

FIGURE 4 Melissa AI Assistant



Hi, I'm Melissa. I am here to answer your questions regarding your network. 😊

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

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

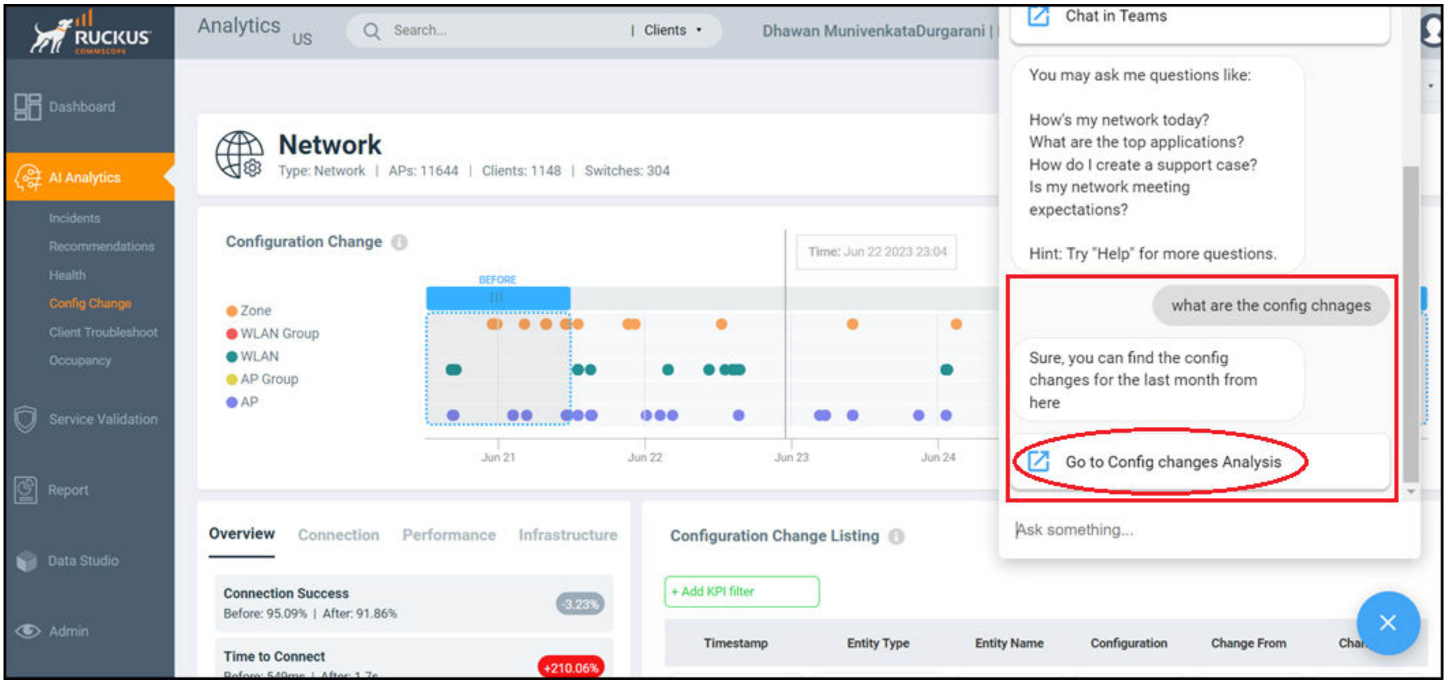
Using key identification words like **client**, **zone**, **system**, etc. before the name will ensure a faster response from Melissa as names are often non-unique strings. Full names are not necessary as Melissa has the capabilities for partial search. You could also indicate the time periods by using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

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

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

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

FIGURE 5 Example: Viewing Config Changes for the Last Month



You may ask me questions like:

How's my network today?
What are the top applications?
How do I create a support case?
Is my network meeting expectations?

Hint: Try "Help" for more questions.

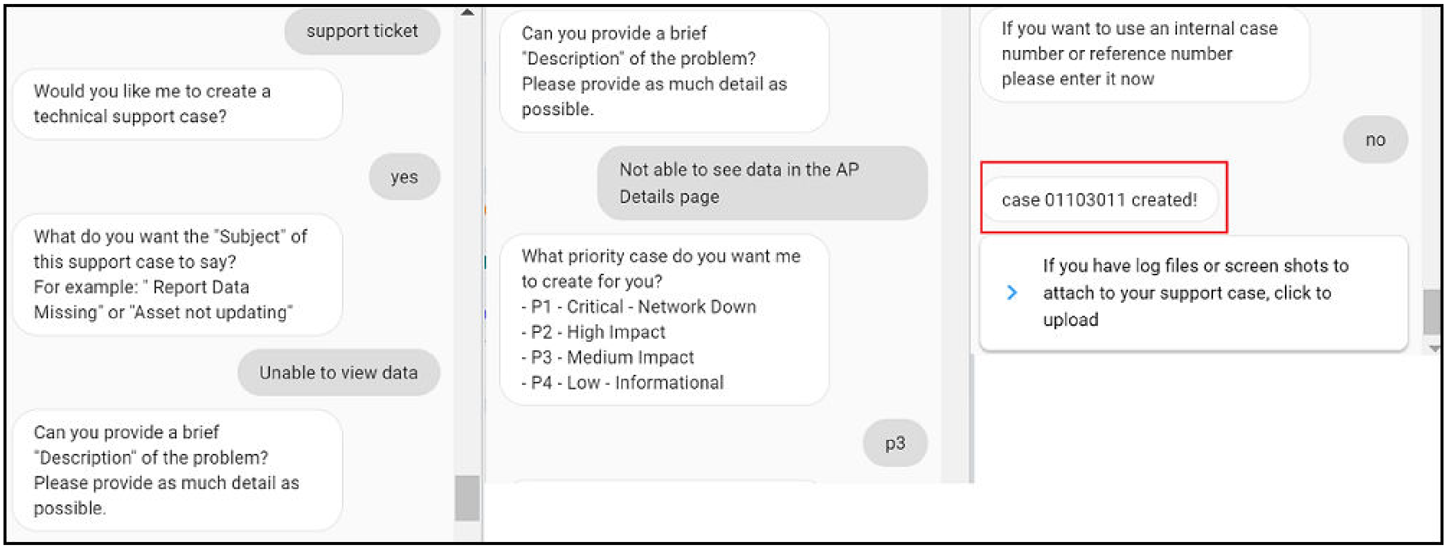
what are the config chnages

Sure, you can find the config changes for the last month from here

Go to Config changes Analysis

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

FIGURE 6 Creating a Support Case Using the Assistant



support ticket

Would you like me to create a technical support case?

yes

What do you want the "Subject" of this support case to say?
For example: " Report Data Missing" or "Asset not updating"

Unable to view data

Can you provide a brief "Description" of the problem? Please provide as much detail as possible.

Can you provide a brief "Description" of the problem? Please provide as much detail as possible.

Not able to see data in the AP Details page

What priority case do you want me to create for you?
- P1 - Critical - Network Down
- P2 - High Impact
- P3 - Medium Impact
- P4 - Low - Informational

p3

If you want to use an internal case number or reference number please enter it now

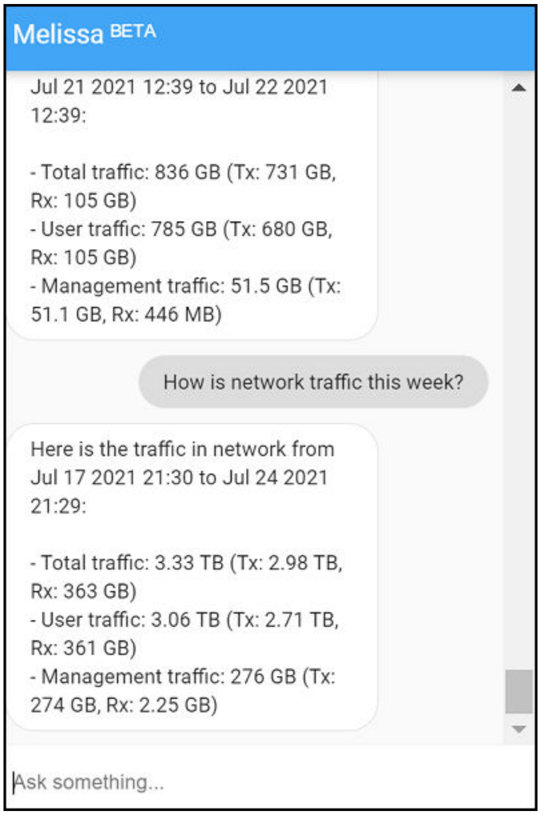
no

case 01103011 created!

If you have log files or screen shots to attach to your support case, click to upload

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

FIGURE 7 Traffic Trend for the Specified Week



Melissa BETA

Jul 21 2021 12:39 to Jul 22 2021 12:39:

- Total traffic: 836 GB (Tx: 731 GB, Rx: 105 GB)
- User traffic: 785 GB (Tx: 680 GB, Rx: 105 GB)
- Management traffic: 51.5 GB (Tx: 51.1 GB, Rx: 446 MB)

How is network traffic this week?

Here is the traffic in network from Jul 17 2021 21:30 to Jul 24 2021 21:29:

- Total traffic: 3.33 TB (Tx: 2.98 TB, Rx: 363 GB)
- User traffic: 3.06 TB (Tx: 2.71 TB, Rx: 361 GB)
- Management traffic: 276 GB (Tx: 274 GB, Rx: 2.25 GB)

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

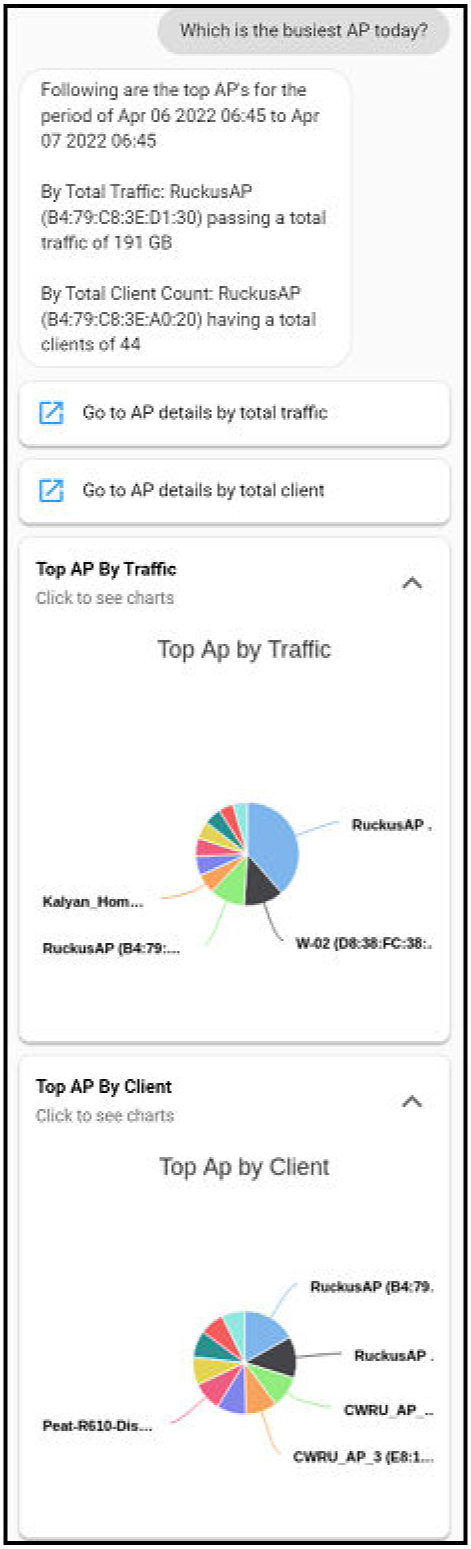
Graphical Rendering of Data in Melissa

For a select few user intents, Melissa provides graphical rendering of data in the form of pie charts. The advanced combination of textual display and graphical representation of data helps you to do easy and enhanced analysis of some of the important statistics of the network. Melissa supports rendering of charts for user intents with respect to top applications, node status, top zones, bad APs, top SSID, and top APs. Following are some questions (not limited to) that you can use to converse with Melissa to get the required data in a pie chart.

- What are the top applications? - Displays chart for top applications by traffic and client
- How's my network today? - Displays the chart with details of Node status by incidents
- What are the APs with problem in last week? - Displays the chart for bad APs

Here is an example in which Melissa displays top APs by traffic and top APs by client in pie charts .

FIGURE 8 Example - Pie Charts of Top APs



Which is the busiest AP today?

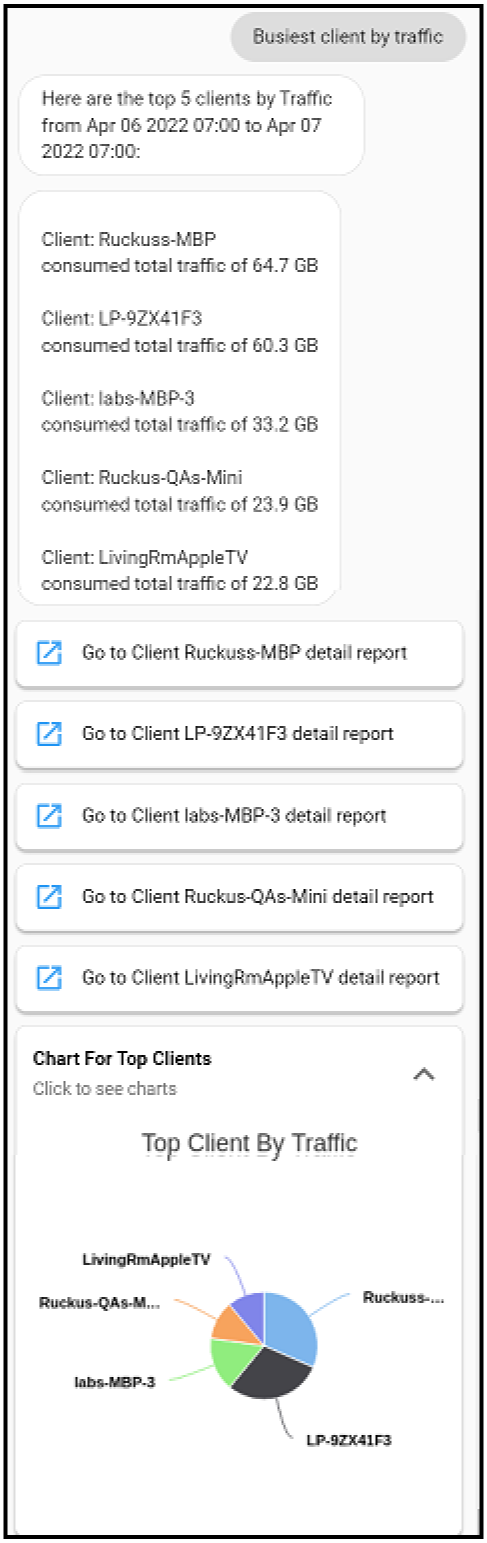
Following are the top AP's for the period of Apr 06 2022 06:45 to Apr 07 2022 06:45

By Total Traffic: RuckusAP (B4:79:C8:3E:D1:30) passing a total traffic of 191 GB

By Total Client Count: RuckusAP (B4:79:C8:3E:A0:20) having a total clients of 44

Here is an example in which Melissa displays pie chart of top Clients.

FIGURE 9 Example - Pie Chart of Top Client



Busiest client by traffic

Here are the top 5 clients by Traffic from Apr 06 2022 07:00 to Apr 07 2022 07:00:

Client: Ruckuss-MBP
consumed total traffic of 64.7 GB

Client: LP-9ZX41F3
consumed total traffic of 60.3 GB

Client: labs-MBP-3
consumed total traffic of 33.2 GB

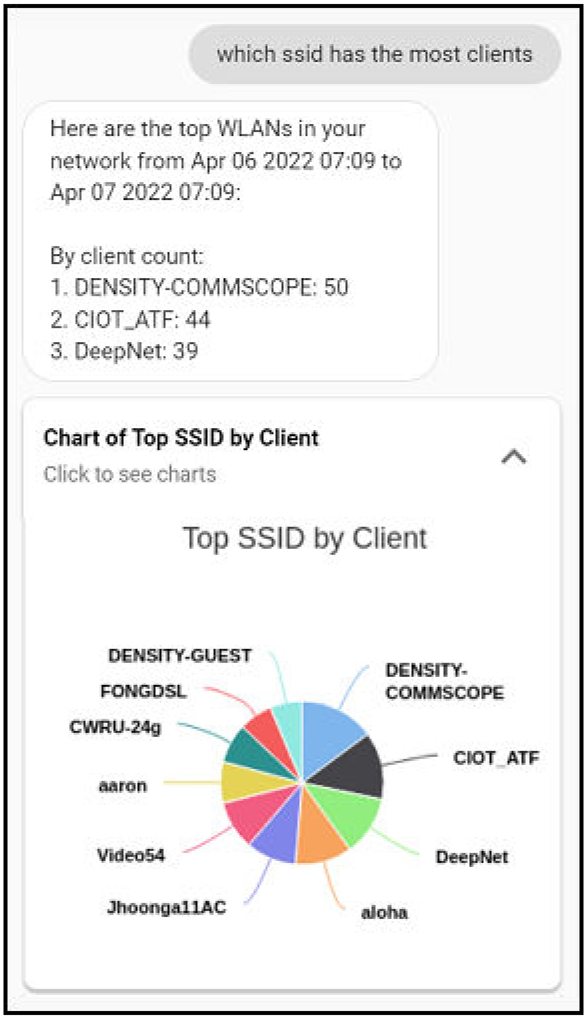
Client: Ruckus-QAs-Mini
consumed total traffic of 23.9 GB

Client: LivingRmAppleTV
consumed total traffic of 22.8 GB

Go to Client Ruckuss-MBP detail report
Go to Client LP-9ZX41F3 detail report
Go to Client labs-MBP-3 detail report
Go to Client Ruckus-QAs-Mini detail report
Go to Client LivingRmAppleTV detail report
Chart For Top Clients
Click to see charts
Top Client By Traffic
LivingRmAppleTV
Ruckuss-...
Ruckus-QAs-M...
labs-MBP-3
LP-9ZX41F3

Here is an example in which Melissa displays pie chart of top SSID by Client.

FIGURE 10 Example - Pie Chart of Top SSID by Client



which ssid has the most clients

Here are the top WLANs in your network from Apr 06 2022 07:09 to Apr 07 2022 07:09:

By client count:
1. DENSITY-COMMSCOPE: 50
2. CIOT_ATF: 44
3. DeepNet: 39

Chart of Top SSID by Client
Click to see charts

Melissa AI Assistant on Microsoft Teams

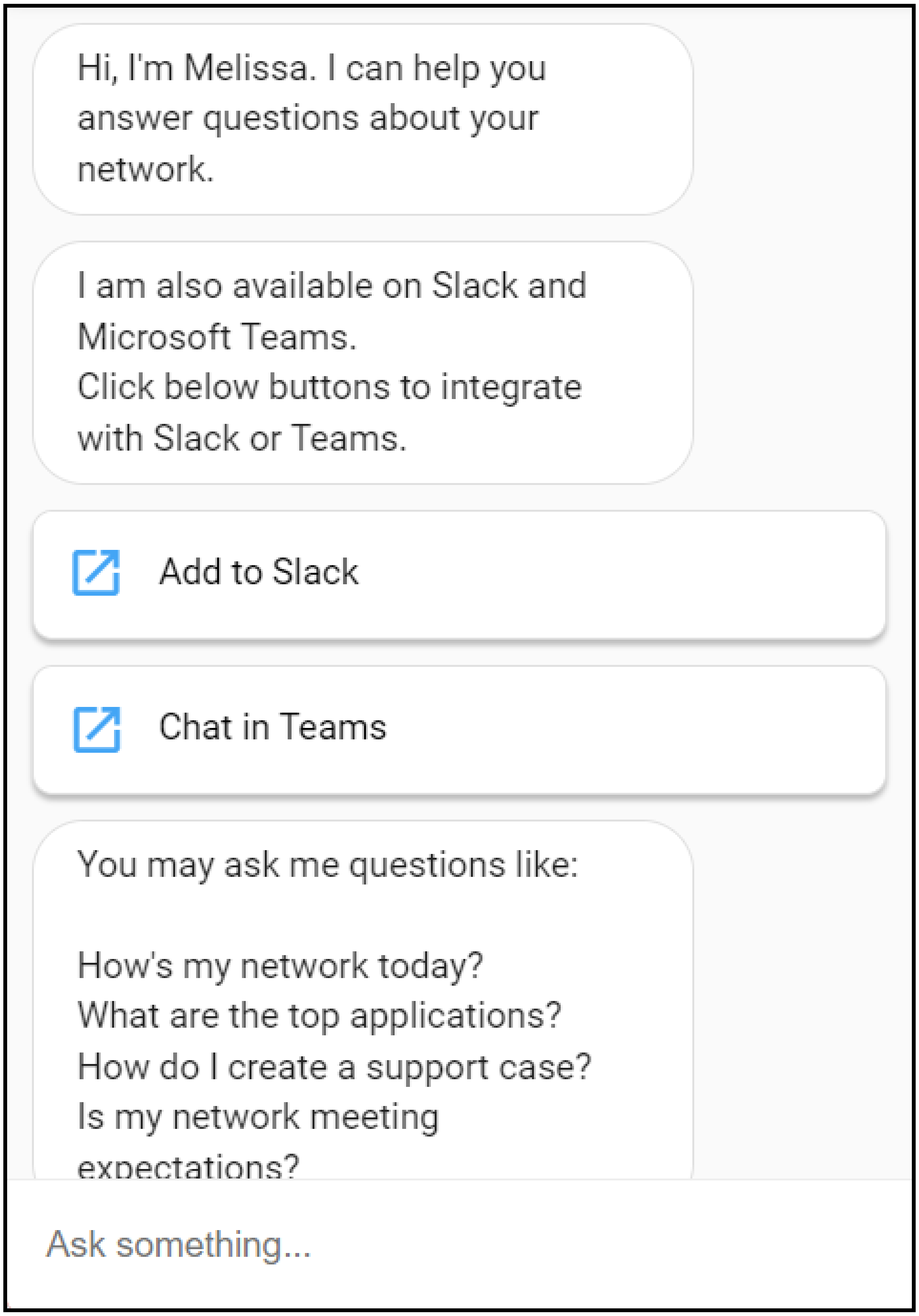
Melissa AI Assistant is now available on Microsoft Teams, thus extending Melissa's rich user experience to other collaboration platforms. Because Melissa provides interactive support to a variety of queries on Microsoft Teams' native chat canvas, you neither have to keep logged in to RUCKUS Analytics nor switch between applications to get information about your network. You can now monitor the health of your network, get status, and identify problem areas right from the Microsoft Teams chat window.

Activating Microsoft Teams with Melissa

To activate Microsoft Teams with Melissa, complete the following steps:

1. In the Melissa AI interface, click **Chat in Teams**. You will be prompted to launch Microsoft Teams.

FIGURE 11 Melissa Chat in Teams



Hi, I'm Melissa. I can help you answer questions about your network.

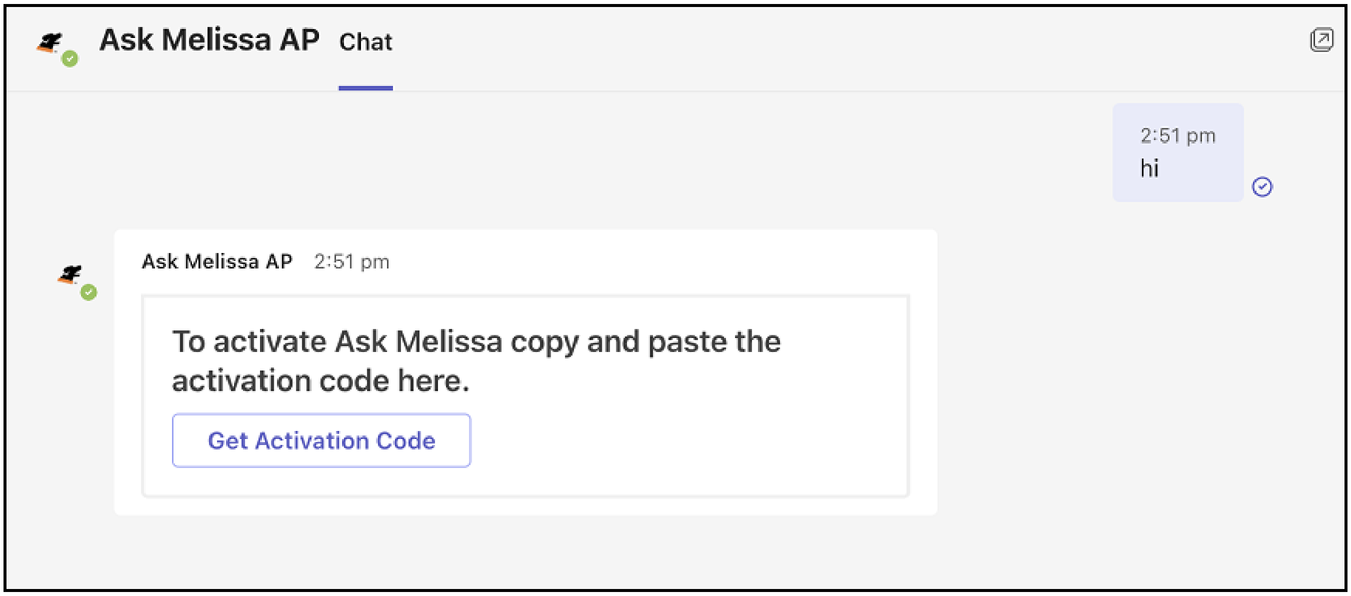
I am also available on Slack and Microsoft Teams.
Click below buttons to integrate with Slack or Teams.

You may ask me questions like:

How's my network today?
What are the top applications?
How do I create a support case?
Is my network meeting expectations?

2. Click **Open Microsoft Teams** in the launcher prompt. The Microsoft Teams is launched with Melissa AI Assistant.
3. Initiate a conversation with Melissa by entering a random word. Melissa responds with a card, prompting you to get the Activation Code to activate Microsoft Teams with Melissa.

FIGURE 12 Get Activation Code Card



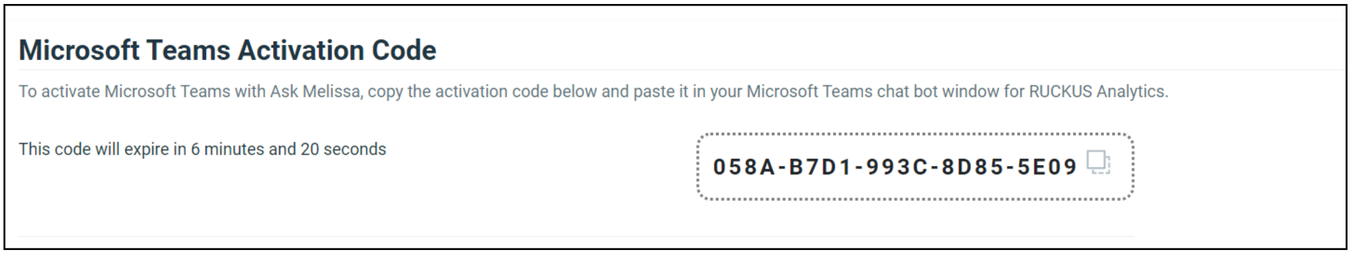
2:51 pm
hi

Ask Melissa AP 2:51 pm

To activate Ask Melissa copy and paste the activation code here.

4. Click **Get Activation Code**. You will be redirected to the **My Profiles Settings** page in RUCKUS Analytics where Microsoft Teams Activation Code is displayed.

FIGURE 13 Microsoft Teams Activation Code



Microsoft Teams Activation Code

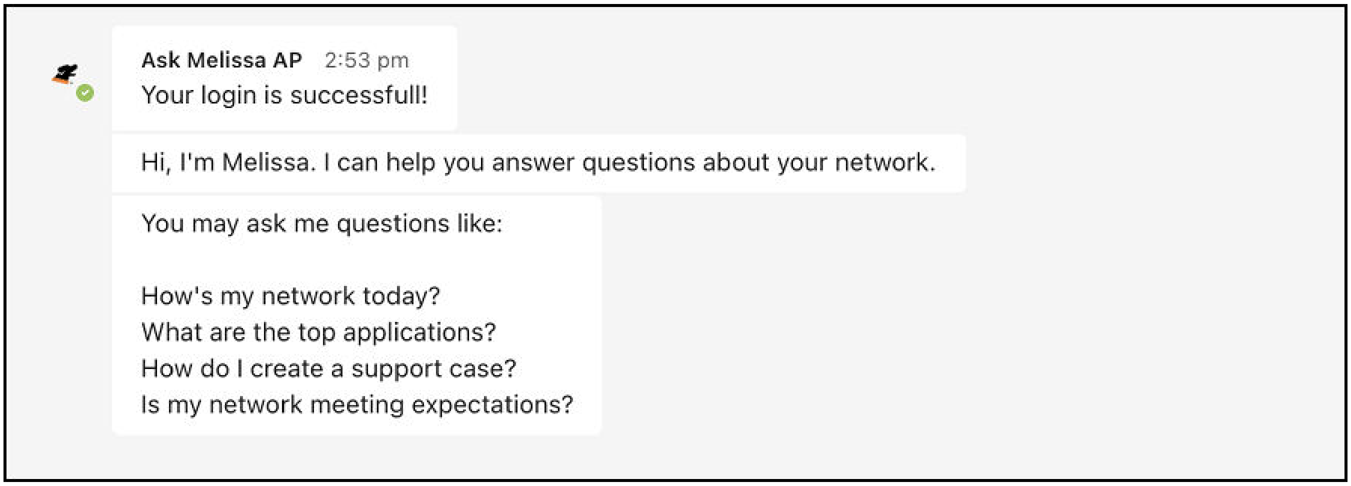
To activate Microsoft Teams with Ask Melissa, copy the activation code below and paste it in your Microsoft Teams chat bot window for RUCKUS Analytics.

This code will expire in 6 minutes and 20 seconds

058A-B7D1-993C-8D85-5E09

5. Copy the Microsoft Teams Activation Code and paste it in the Melissa chat window on Microsoft Teams. A Login success message is displayed indicating that Microsoft Teams is now activated with your Melissa account.

FIGURE 14 Teams Activation and Login Success Message



Ask Melissa AP 2:53 pm

Your login is successfull!

Hi, I'm Melissa. I can help you answer questions about your network.

You may ask me questions like:

How's my network today?
What are the top applications?
How do I create a support case?
Is my network meeting expectations?

Continue to interact with Melissa from Microsoft Teams as you interact in the RUCKUS Analytics application.

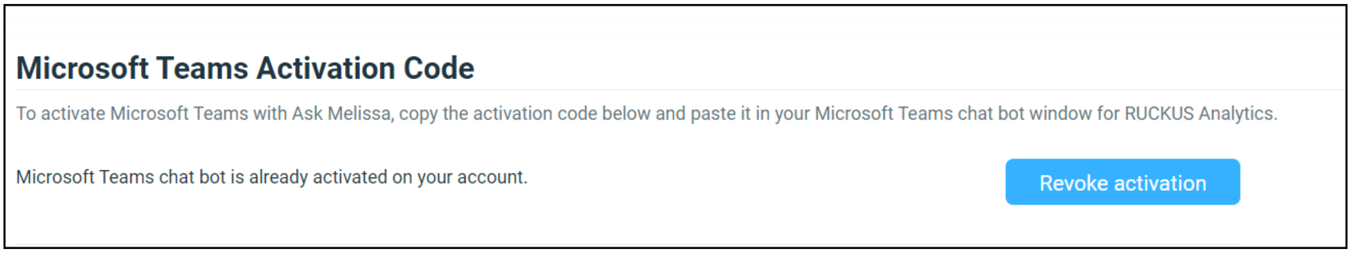
Revoking Microsoft Teams Activation

You can deactivate Ask Melissa from Microsoft Teams by revoking the Microsoft Teams activation.

To revoke Microsoft Teams activation, complete the following steps:

1. In the header panel, select **Settings** from the user profile. The **My Profiles Settings** page is displayed.

   FIGURE 15 Revoke Teams Activation

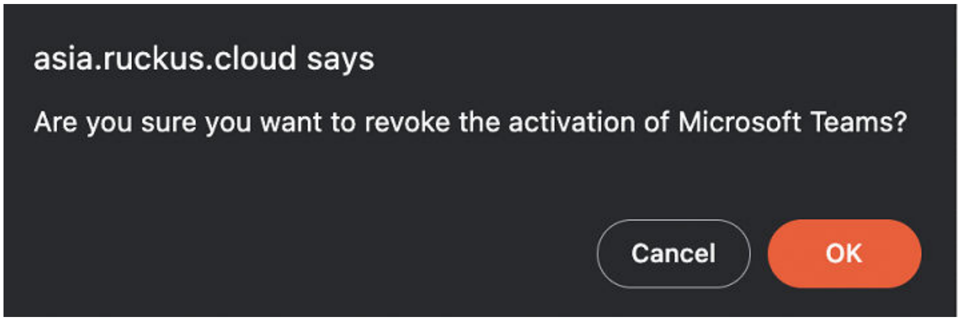
   Microsoft Teams Activation Code

   To activate Microsoft Teams with Ask Melissa, copy the activation code below and paste it in your Microsoft Teams chat bot window for RUCKUS Analytics.

   Microsoft Teams chat bot is already activated on your account.

2. In the **Microsoft Teams Activation Code** panel, click **Revoke activation**. A confirmation dialog box is displayed.

FIGURE 16 Revoke Activation Confirmation message



asia.ruckus.cloud says

Are you sure you want to revoke the activation of Microsoft Teams?

3. Click **Ok** to revoke Microsoft Teams Activation.

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 Severities

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.

It 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.

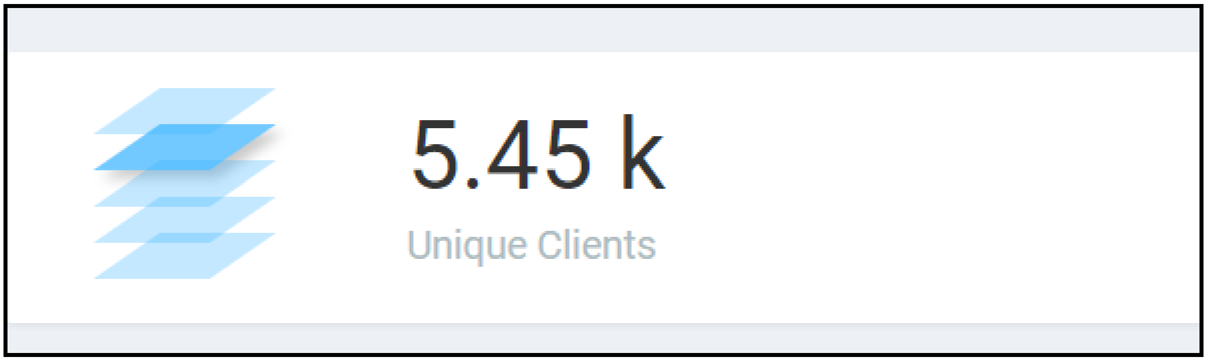
TABLE 8 Severity Levels of an Incident

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

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 17 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.

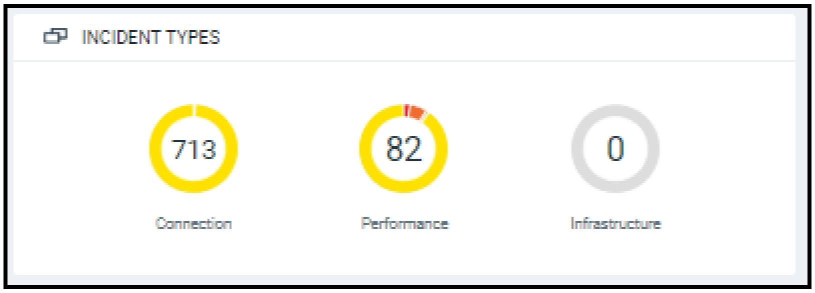
TABLE 9 Layers of Scrolling Data Tile

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 Categories

The incident categories 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 18 Incident Categories

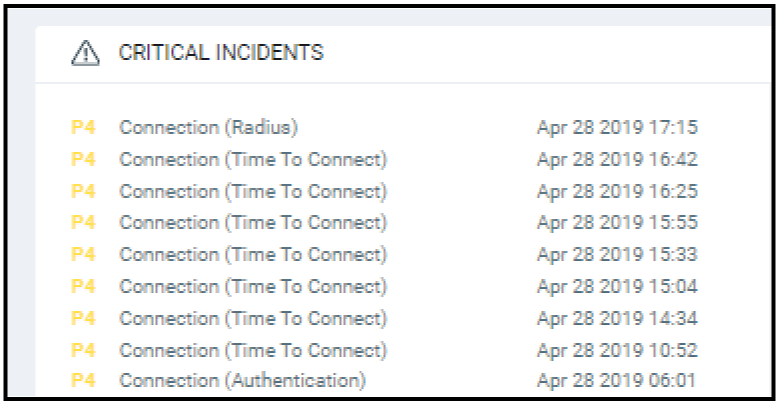


Listing Tile

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 19 Listing Tile



CRITICAL INCIDENTS

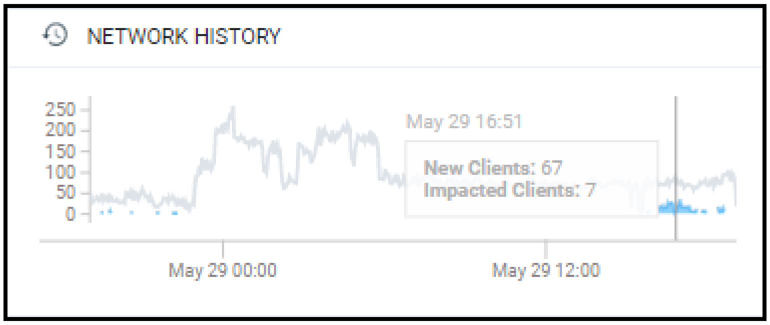
P4	Connection (Radius)	Apr 28 2019 17:15
P4	Connection (Time To Connect)	Apr 28 2019 16:42
P4	Connection (Time To Connect)	Apr 28 2019 16:25
P4	Connection (Time To Connect)	Apr 28 2019 15:55
P4	Connection (Time To Connect)	Apr 28 2019 15:33
P4	Connection (Time To Connect)	Apr 28 2019 15:04
P4	Connection (Time To Connect)	Apr 28 2019 14:34
P4	Connection (Time To Connect)	Apr 28 2019 10:52
P4	Connection (Authentication)	Apr 28 2019 06:01

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 20 Network History Tile

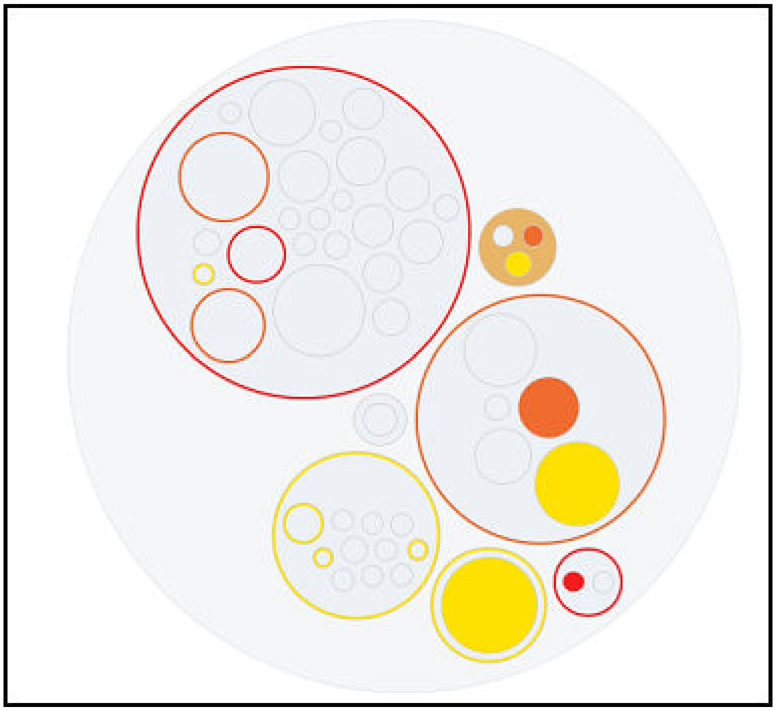


Interactive Network Hierarchy

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.

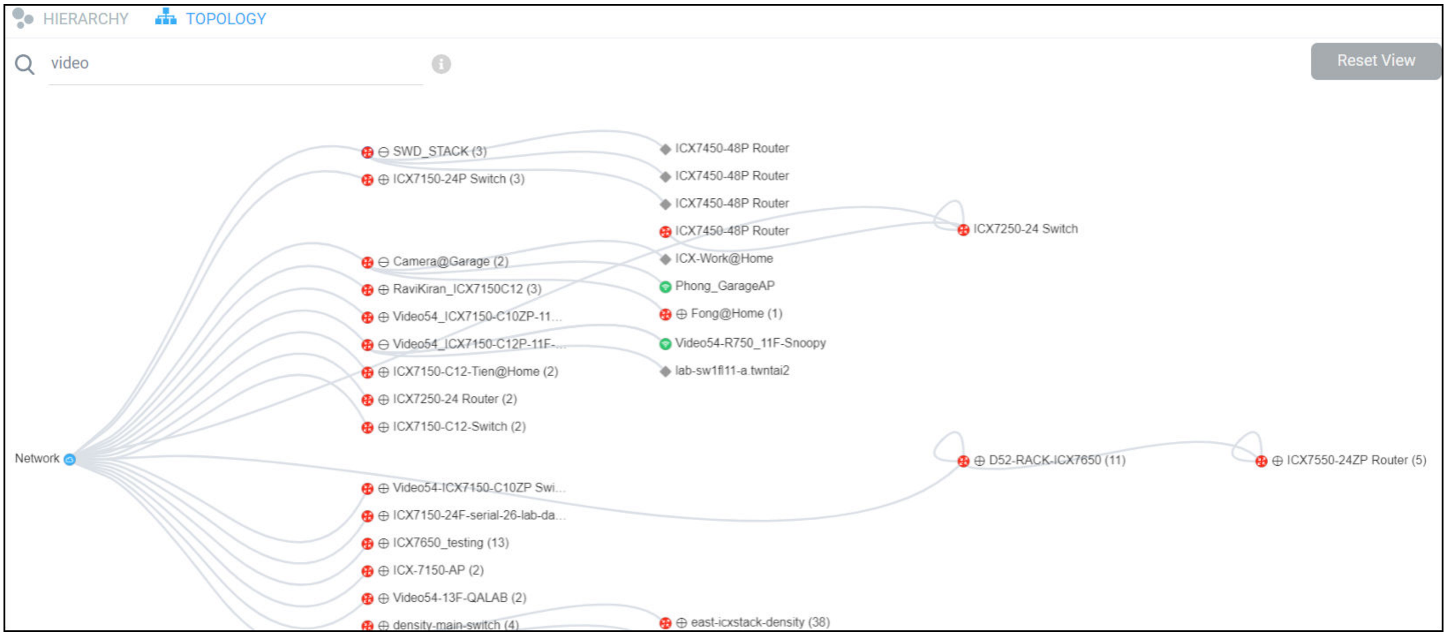
FIGURE 21 Circle Packing Example



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 22 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.

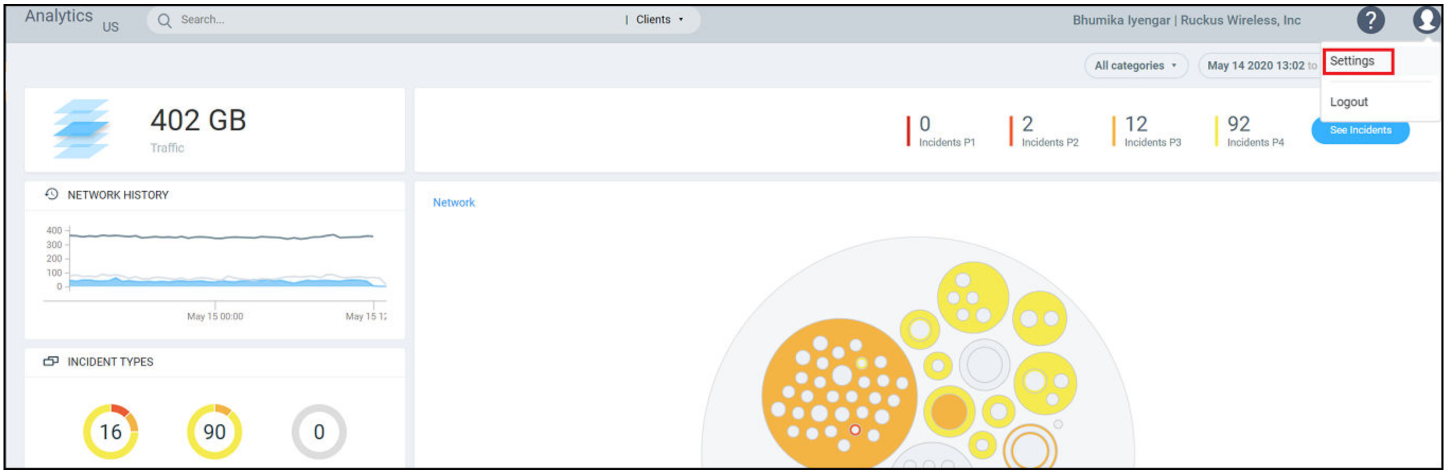
You can zoom-in or zoom-out the **Topology** page and also click on the page to move it.

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

Settings

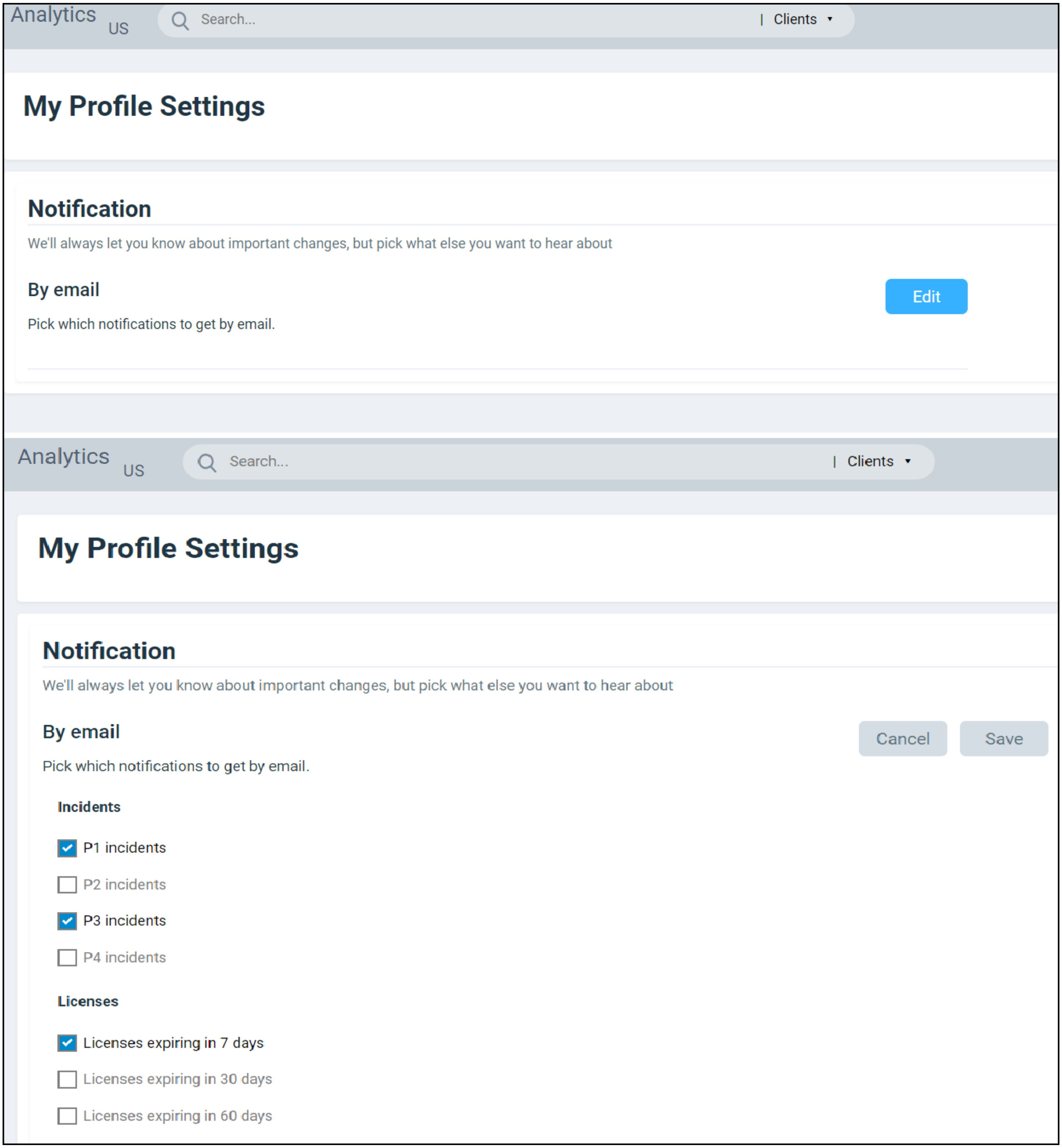
You can modify the user profile from the **My Profile Settings** page and enable the option to receive notification email alerts for incidents of varying severity ranging from P1 to P4.

FIGURE 23 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 24 Enabling Email Notifications



My Profile Settings

Notification

We'll always let you know about important changes, but pick what else you want to hear about

By email

Pick which notifications to get by email.

My Profile Settings

Notification

We'll always let you know about important changes, but pick what else you want to hear about

By email

Pick which notifications to get by email.

Incidents

☑ P1 incidents

□ P2 incidents

☑ P3 incidents

□ P4 incidents

Licenses

☑ Licenses expiring in 7 days

□ Licenses expiring in 30 days

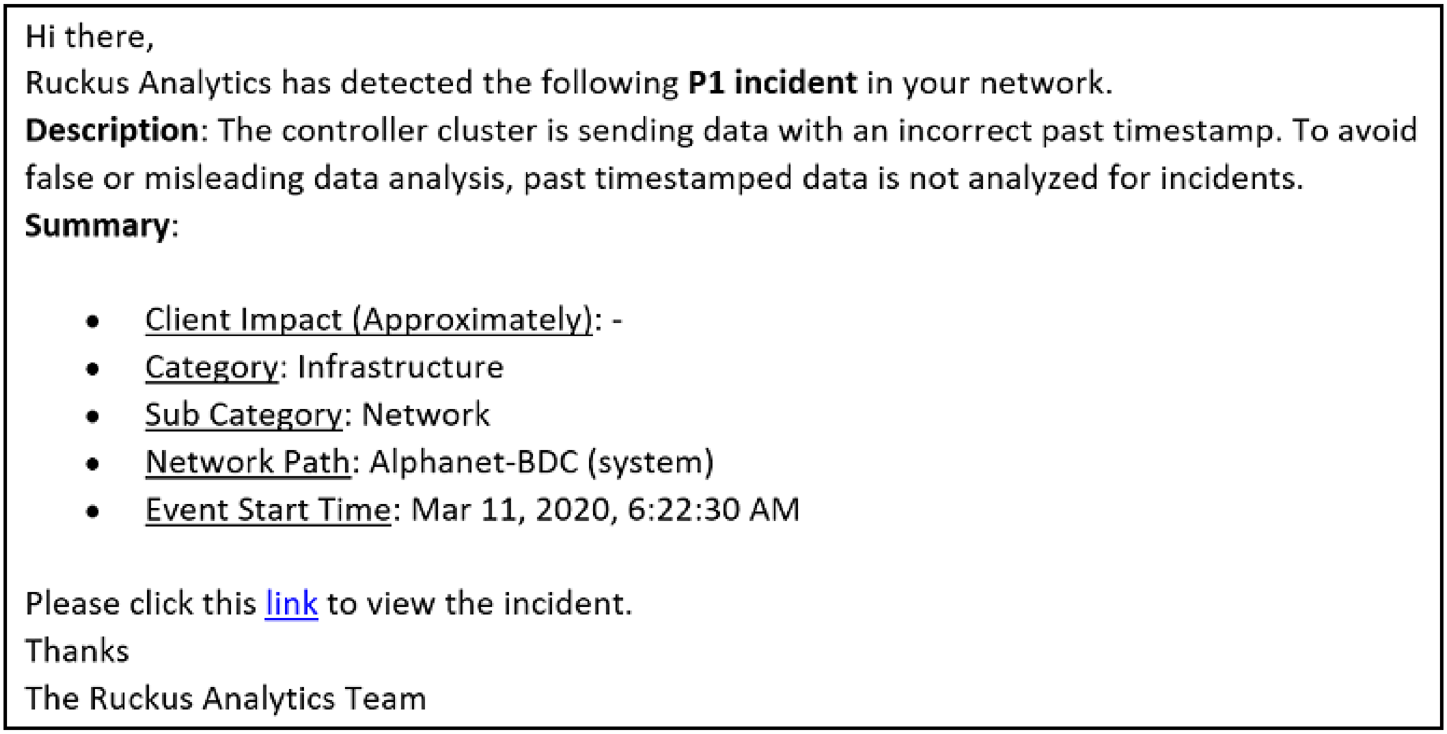
□ Licenses expiring in 60 days

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 AI Analytics Page on page 47.
- 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 25 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

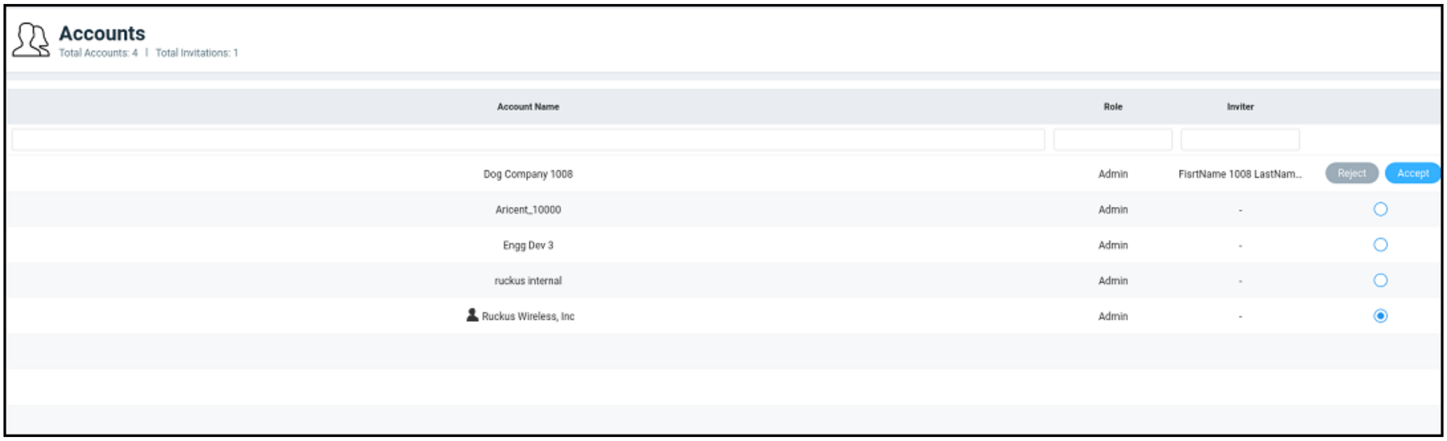
In the Brand view mode, the user is provided with options to customize the UI display names by setting the naming convention to use standard vocabulary that aligns with the company's common business glossary. The Brand administrator can configure the naming conventions related to SSIDs and set the regular expression to validate brand SSID compliance. For more information, refer to Naming Convention on page 259.

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.

The account name with the 👤 user icon is identified as the user's organisation service account.

FIGURE 26 Accounts Page



Accounts

Total Accounts: 4 | Total Invitations: 1

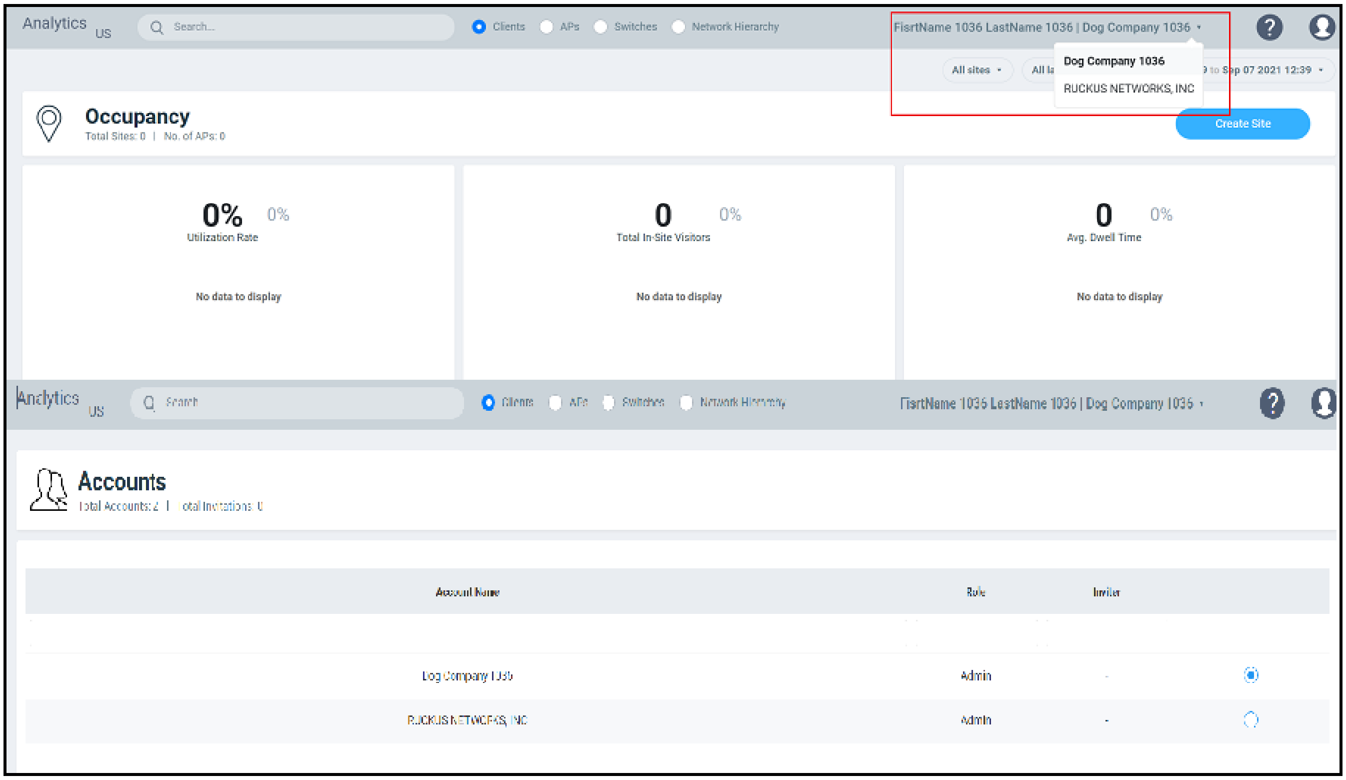
Account Name	Role	Inviter	
Dog Company 1008	Admin	FisrtName 1008 LastNam...	Reject Accept
Aricent_10000	Admin	-	○
Engg Dev 3	Admin	-	○
ruckus internal	Admin	-	○
Ruckus Wireless, Inc	Admin	-	●

NOTE

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

Partners can also view the list of their customer accounts which are displayed in the **Accounts** page. Different accounts can be selected from the drop-down menu near the top-right corner of the web interface, and analytics data can be viewed for that particular customer account.

FIGURE 27 Partner Accounts



Account Name	Role	Invites	
Dog Company 1036	Admin	-	●
RUCKUS NETWORKS, INC	Admin	-	○

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.

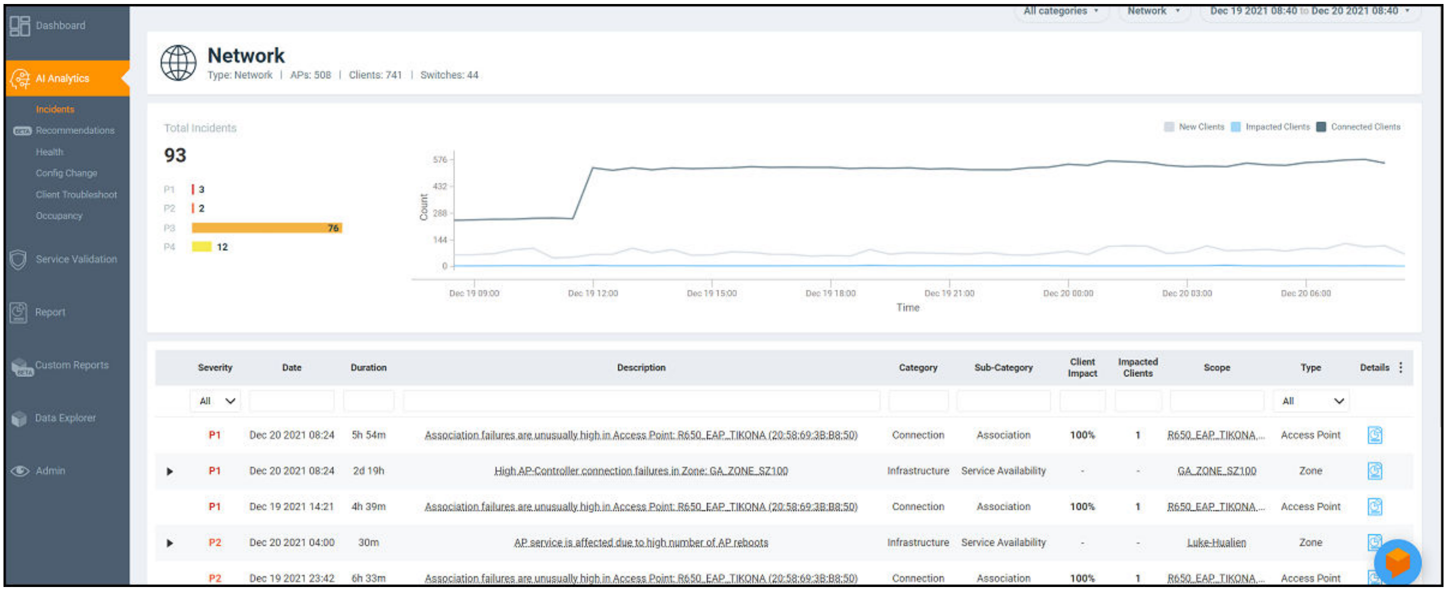
AI Analytics

- AI Analytics Page.. 47
- Recommendations Page.. 62
- Health Page.. 66
- Configuration Change Page... 75
- Client Troubleshoot Page...78
- Occupancy Page... 81

AI Analytics Page

The **AI 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 28 AI Analytics Page



	Severity	Date	Duration	Description	Category	Sub-Category	Client Impact	Impacted Clients	Scope	Type	Details ⋮
	All									All	
	P1	Dec 20 2021 08:24	5h 54m	Association failures are unusually high in Access Point: R650_EAP_TIKONA (20:58:69:3B:B8:50)	Connection	Association	100%	1	R650_EAP_TIKONA...	Access Point	
▶	P1	Dec 20 2021 08:24	2d 19h	High AP-Controller connection failures in Zone: GA_ZONE_SZ100	Infrastructure	Service Availability	-	-	GA_ZONE_SZ100	Zone	
	P1	Dec 19 2021 14:21	4h 39m	Association failures are unusually high in Access Point: R650_EAP_TIKONA (20:58:69:3B:B8:50)	Connection	Association	100%	1	R650_EAP_TIKONA...	Access Point	
▶	P2	Dec 20 2021 04:00	30m	AP service is affected due to high number of AP reboots	Infrastructure	Service Availability	-	-	Luke-Hualien	Zone	
	P2	Dec 19 2021 23:42	6h 33m	Association failures are unusually high in Access Point: R650_EAP_TIKONA (20:58:69:3B:B8:50)	Connection	Association	100%	1	R650_EAP_TIKONA...	Access Point	

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

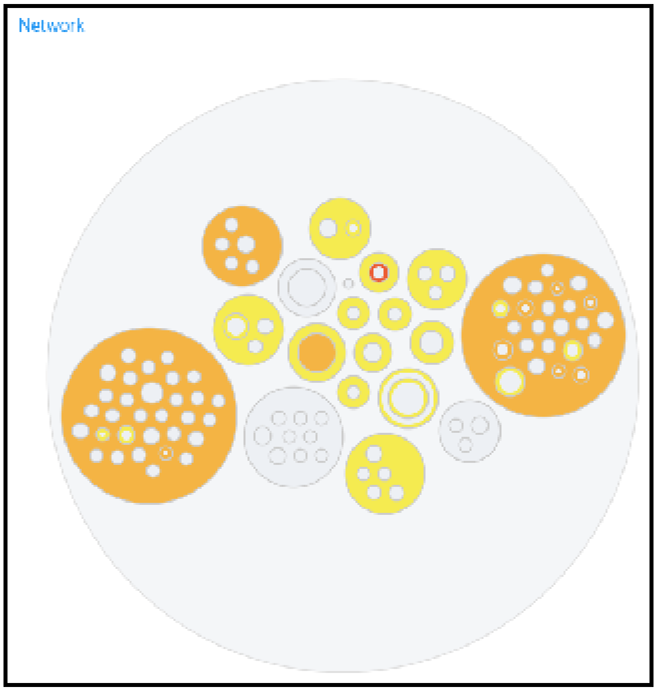
The AI Analytics page contains a number of components:

- 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.

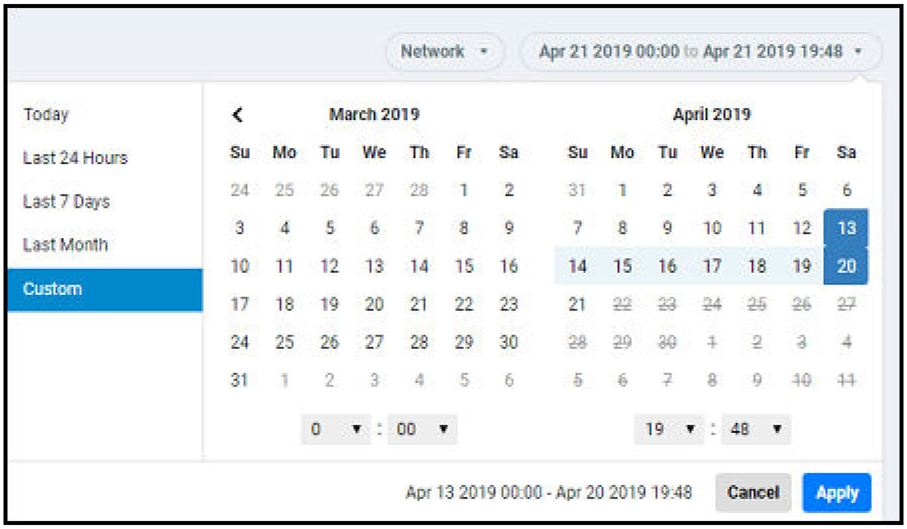
FIGURE 29 Nodes on the Network



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 30 Custom Mode



Apr 13 2019 00:00 - Apr 20 2019 19:48

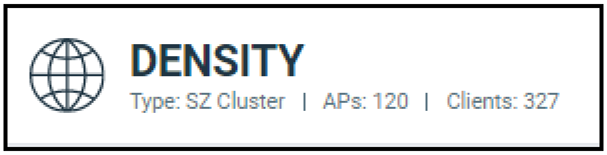
Click **Apply** to save the specified date and time filters and update the AI Analytics page.

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 31 Density Network Node



DENSITY

Type: SZ Cluster | APs: 120 | Clients: 327

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

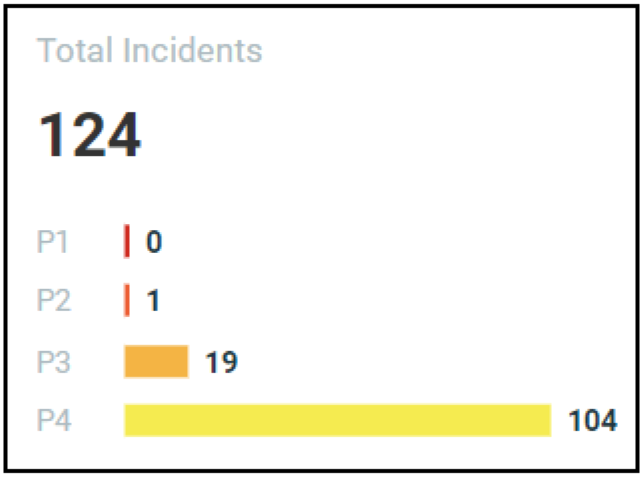
TABLE 10 Network Nodes and Attributes

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.

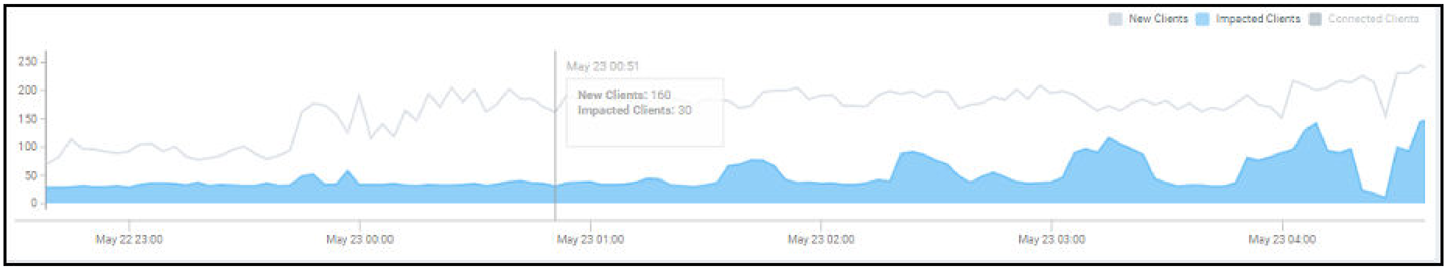
FIGURE 32 Severity Filter



Incident Timeline

The Incident Timeline 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 33 Incident Timeline



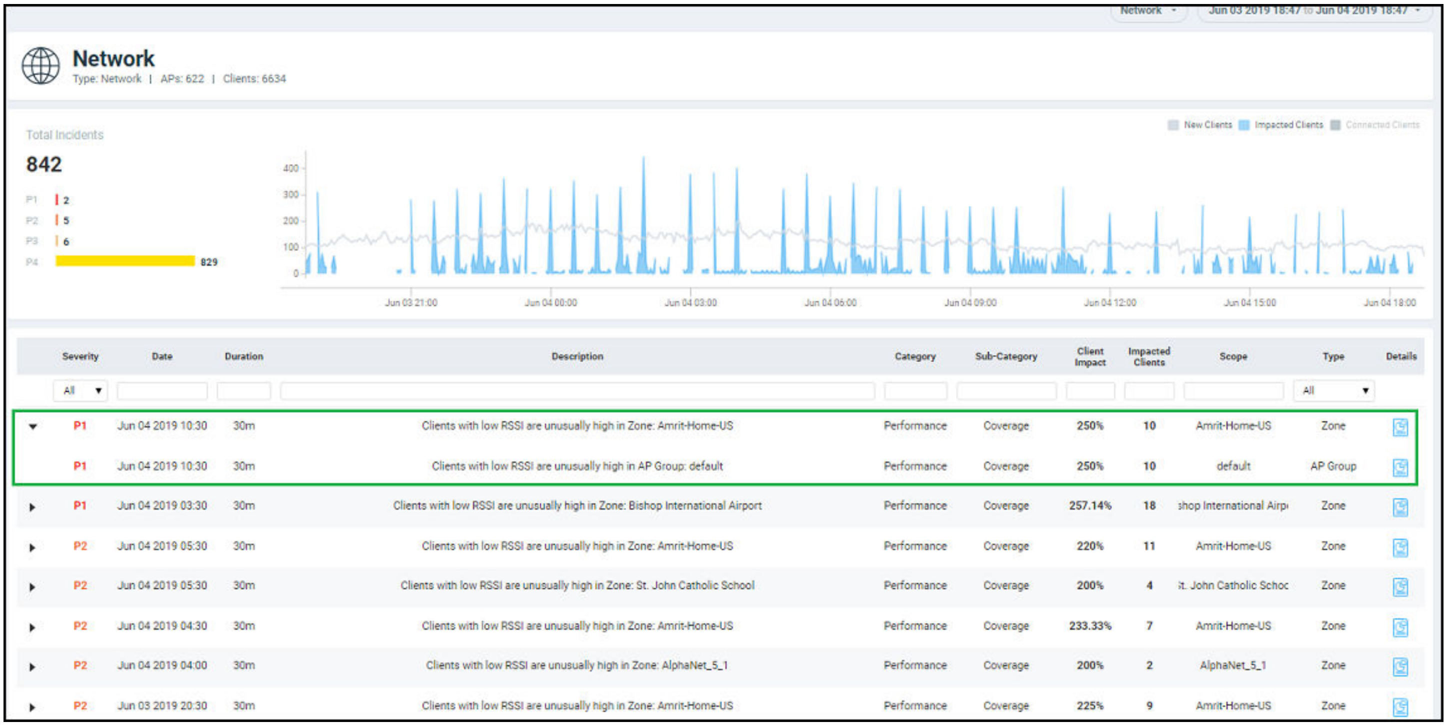
Pausing the pointer at any instance on the timeline displays an information box that shows the number of new clients, impacted clients, and connected clients. You can modify the information displayed in the information box by selecting the **New Clients**, **Impacted Clients**, and **Connected Clients** 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 34 Incidents List Table



Network
Type: Network | APs: 622 | Clients: 6634

	Severity	Date	Duration	Description	Category	Sub-Category	Client Impact	Impacted Clients	Scope	Type	Details
	All ▾									All ▾	
▾	P1	Jun 04 2019 10:30	30m	Clients with low RSSI are unusually high in Zone: Amrit-Home-US	Performance	Coverage	250%	10	Amrit-Home-US	Zone	
	P1	Jun 04 2019 10:30	30m	Clients with low RSSI are unusually high in AP Group: default	Performance	Coverage	250%	10	default	AP Group	
▸	P1	Jun 04 2019 03:30	30m	Clients with low RSSI are unusually high in Zone: Bishop International Airport	Performance	Coverage	257.14%	18	shop International Airp	Zone	
▸	P2	Jun 04 2019 05:30	30m	Clients with low RSSI are unusually high in Zone: Amrit-Home-US	Performance	Coverage	220%	11	Amrit-Home-US	Zone	
▸	P2	Jun 04 2019 05:30	30m	Clients with low RSSI are unusually high in Zone: St. John Catholic School	Performance	Coverage	200%	4	t. John Catholic Schoc	Zone	
▸	P2	Jun 04 2019 04:30	30m	Clients with low RSSI are unusually high in Zone: Amrit-Home-US	Performance	Coverage	233.33%	7	Amrit-Home-US	Zone	
▸	P2	Jun 04 2019 04:00	30m	Clients with low RSSI are unusually high in Zone: AlphaNet_5_1	Performance	Coverage	200%	2	AlphaNet_5_1	Zone	
▸	P2	Jun 03 2019 20:30	30m	Clients with low RSSI are unusually high in Zone: Amrit-Home-US	Performance	Coverage	225%	9	Amrit-Home-US	Zone	

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 11 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.

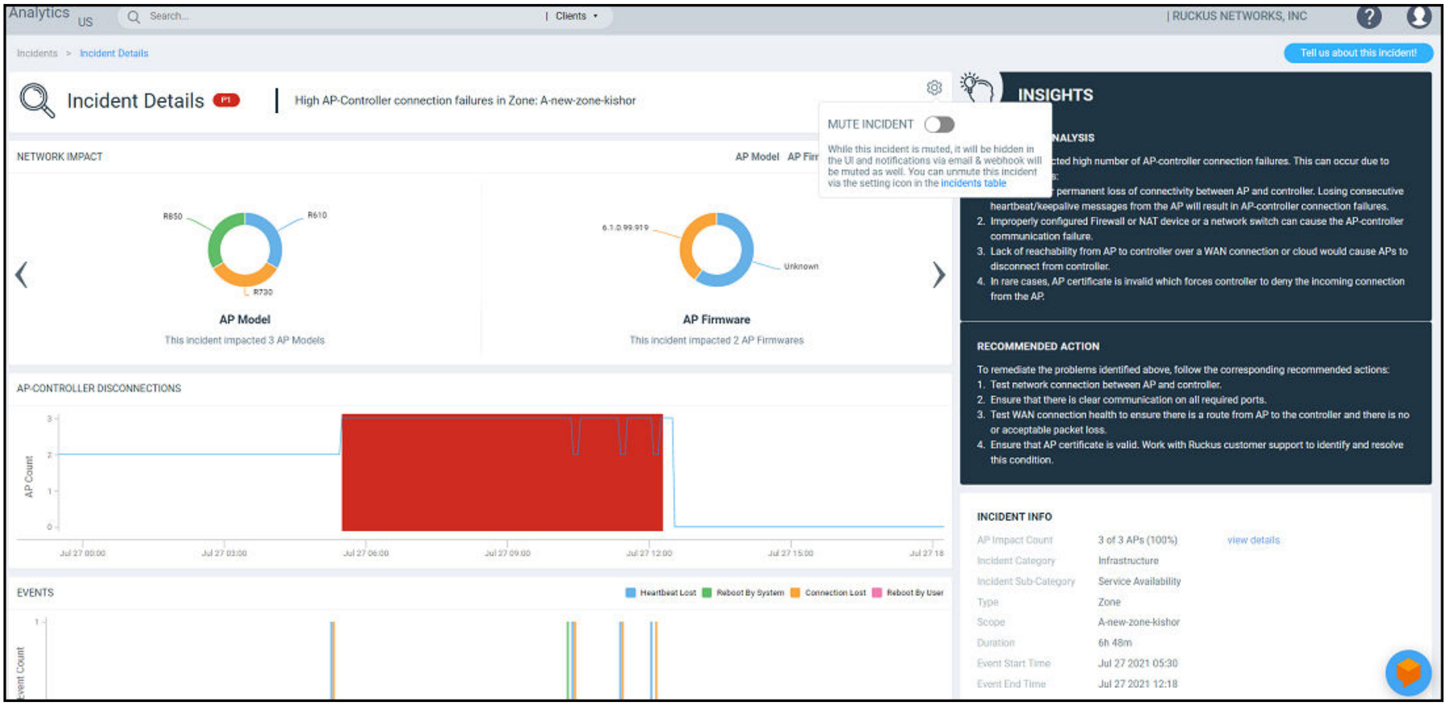
TABLE 11 Attributes of the Incidents List Table (continued)

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 ● Network
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 35 Incident Details Page



High AP-Controller connection failures in Zone: A-new-zone-kishor

This incident impacted 3 AP Models

This incident impacted 2 AP Firmwares

While this incident is muted, it will be hidden in the UI and notifications via email & webhook will be muted as well. You can unmute this incident via the setting icon in the incidents table

INSIGHTS

NALYSIS

cted high number of AP-controller connection failures. This can occur due to

s:

permanent loss of connectivity between AP and controller. Losing consecutive heartbeat/keepalive messages from the AP will result in AP-controller connection failures.
2. Improperly configured Firewall or NAT device or a network switch can cause the AP-controller communication failure.
3. Lack of reachability from AP to controller over a WAN connection or cloud would cause APs to disconnect from controller.
4. In rare cases, AP certificate is invalid which forces controller to deny the incoming connection from the AP.

RECOMMENDED ACTION

To remediate the problems identified above, follow the corresponding recommended actions:

1. Test network connection between AP and controller.
2. Ensure that there is clear communication on all required ports.
3. Test WAN connection health to ensure there is a route from AP to the controller and there is no or acceptable packet loss.
4. Ensure that AP certificate is valid. Work with Ruckus customer support to identify and resolve this condition.

INCIDENT INFO

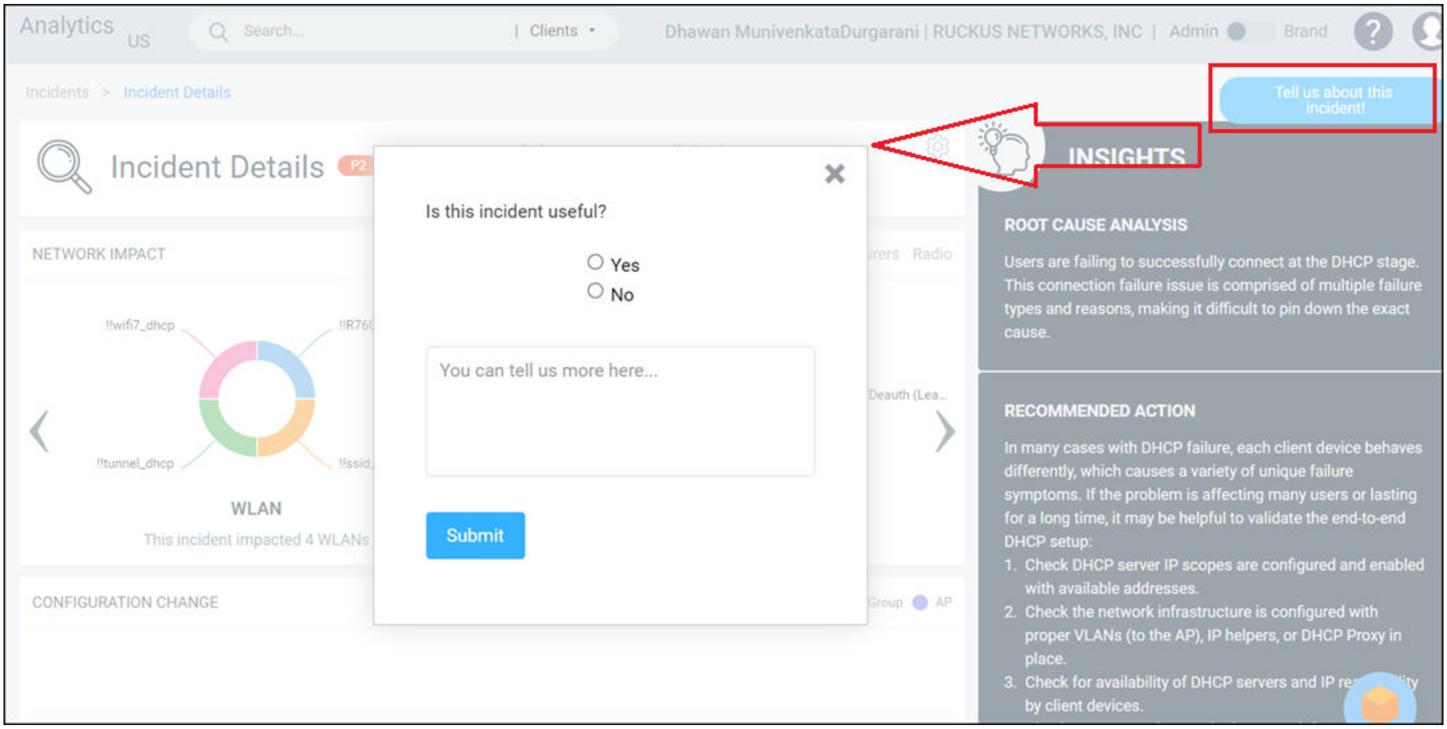
AP Impact Count	3 of 3 APs (100%)
Incident Category	Infrastructure
Incident Sub-Category	Service Availability
Type	Zone
Scope	A-new-zone-kishor
Duration	6h 48m
Event Start Time	Jul 27 2021 05:30
Event End Time	Jul 27 2021 12:18

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

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

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

FIGURE 36 Incident Feedback Option



Is this incident useful?

○ Yes
○ No

You can tell us more here...

Submit

ROOT CAUSE ANALYSIS

Users are failing to successfully connect at the DHCP stage. This connection failure issue is comprised of multiple failure types and reasons, making it difficult to pin down the exact cause.

RECOMMENDED ACTION

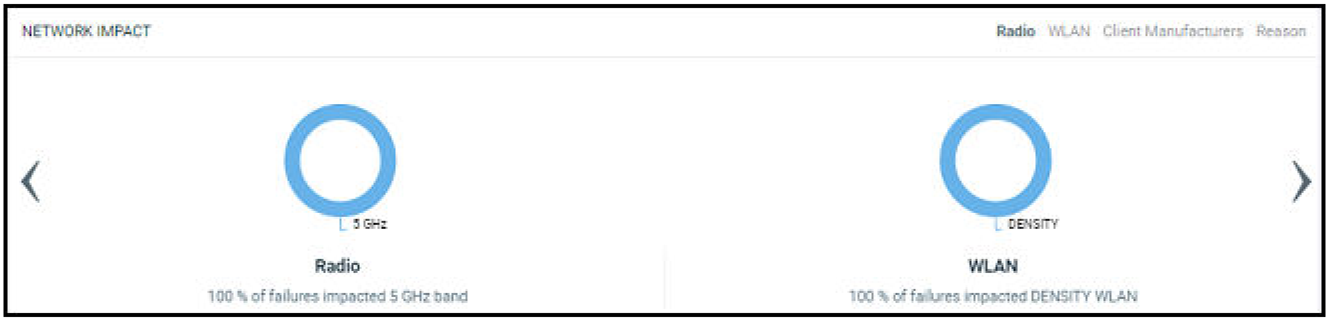
In many cases with DHCP failure, each client device behaves differently, which causes a variety of unique failure symptoms. If the problem is affecting many users or lasting for a long time, it may be helpful to validate the end-to-end DHCP setup:

1. Check DHCP server IP scopes are configured and enabled with available addresses.
2. Check the network infrastructure is configured with proper VLANs (to the AP), IP helpers, or DHCP Proxy in place.
3. Check for availability of DHCP servers and IP re... ...ity by client devices.

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 37 Network Impact Tile



Radio

100 % of failures impacted 5 GHz band

WLAN

100 % of failures impacted DENSITY WLAN

TABLE 12 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.
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.	● Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident. ● 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.

TABLE 12 Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
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.	• Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident. • 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.	• Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident. • 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 12 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.	● Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident. ● 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.	● Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident. ● 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 12 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. • Configuration Change: chart with drop-down table displaying configuration changes that are relevant to the specific incident. • 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.

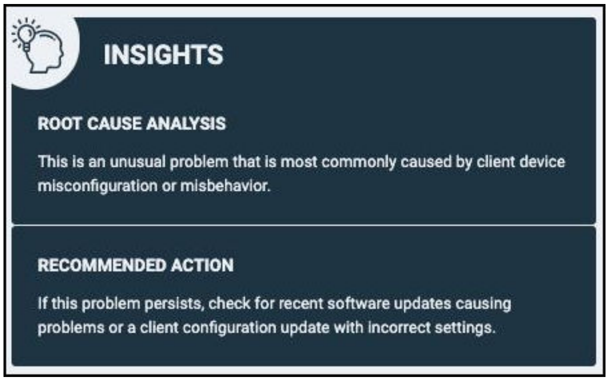
TABLE 12 Attributes of Network Impact Table (continued)

Incident Type	Donut Charts	Chart Elements
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.
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.
AP PoE Underpowered	• AP Model: displays the percentage of failure due to insufficient PoE power that impacted an AP model • AP Firmware: displays the percentage of failure due to insufficient PoE power that impacted an AP firmware version	• AP POE impact: displays the number of APs impacted at a time, due to insufficient power available on the PoE port • Impacted AP: displays the list of APs impacted by failure due to insufficient PoE power within the network
AP Ethernet Auto-negotiation	• AP Model: displays the percentage of failure due to Ethernet WAN link mismatch that impacted an AP model • AP Firmware: displays the percentage of failure due to Ethernet WAN link mismatch that impacted an AP firmware version	• APs WAN Throughput Impact: displays the number of APs impacted at a time, due to Ethernet WAN link mismatch • Impacted AP: displays the list of APs impacted by failure due to Ethernet WAN link mismatch within the network
SZ Cluster		Time Incidents: a time series chart that shows when the controller cluster sends data with an incorrect timestamp.

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 38 Insights Tile



INSIGHTS

ROOT CAUSE ANALYSIS

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

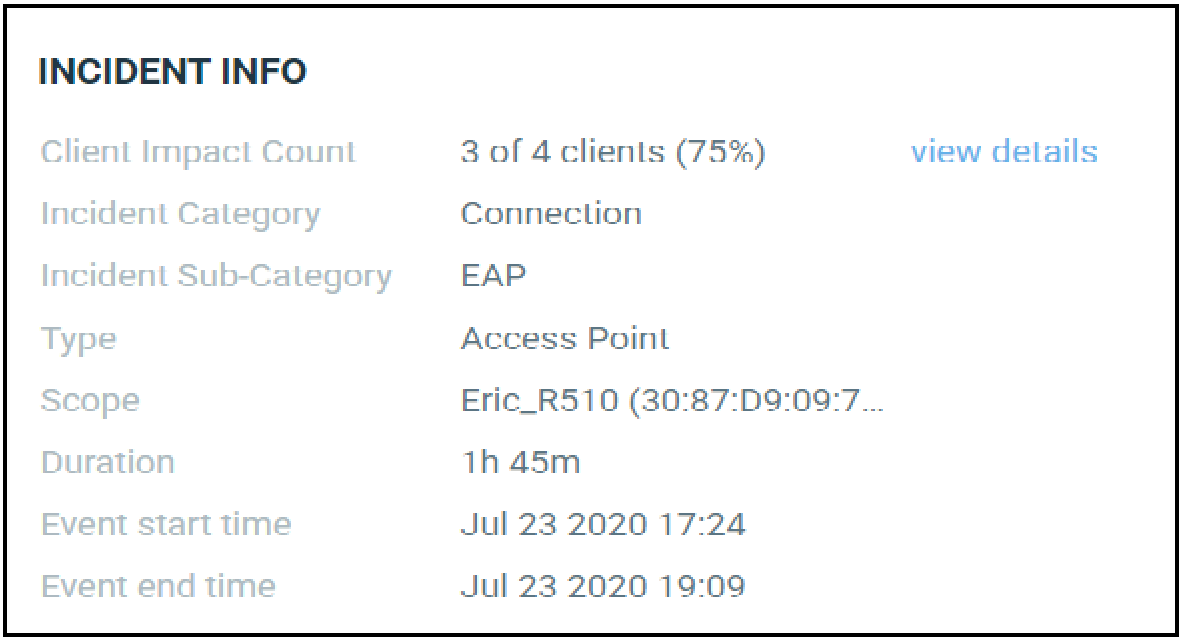
RECOMMENDED ACTION

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

Incident Info Tile

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

FIGURE 39 Incident Info Tile

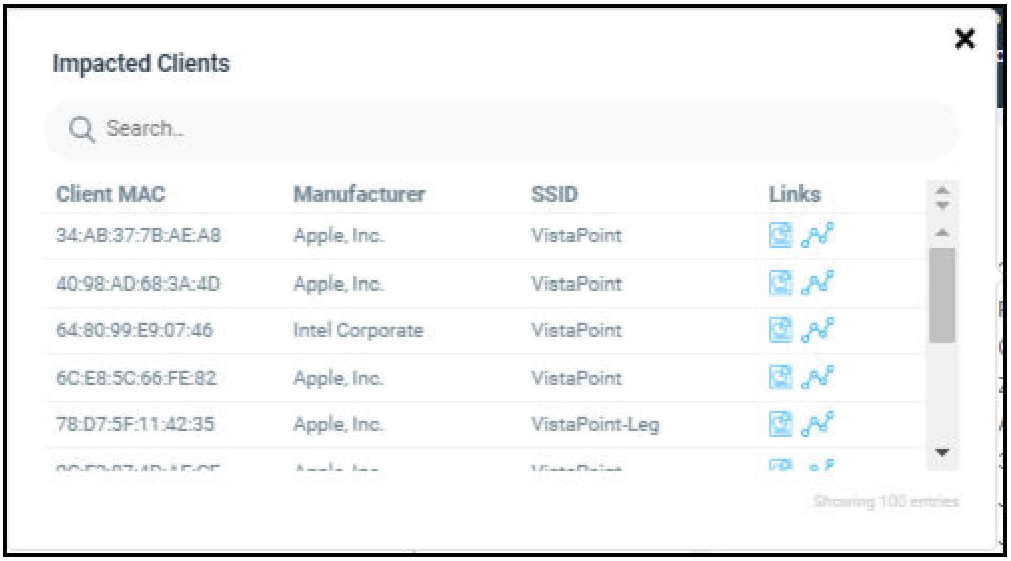


INCIDENT INFO

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

Click **view details** for more information about the impacted clients. The **Impacted Clients** page displays the user name, host name, client MAC address, SSID, and manufacturer of the client. To troubleshoot the client, click the Client Troubleshooting icon ( ) to generate the client details report, click the Client Details icon ( ) on the **Impacted Clients** page. You can search for impacted clients by the client MAC address and manufacturer.

FIGURE 40 Clients page



Impacted Clients

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

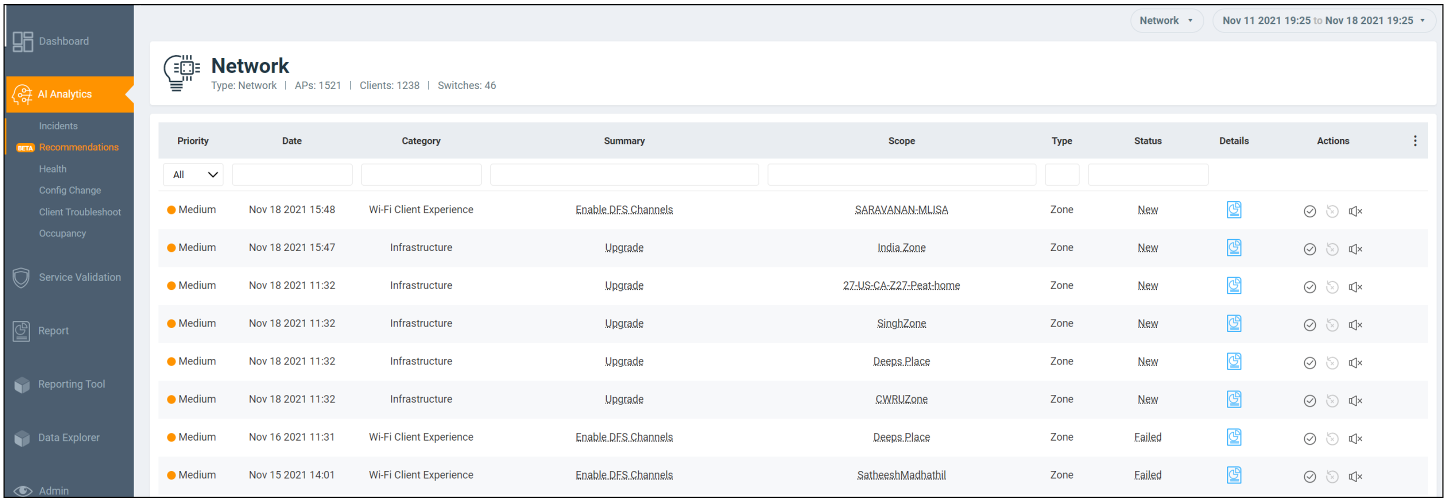
Showing 100 entries

Recommendations Page

RUCKUS Analytics creates recommendations after constantly monitoring the software configuration and analyzing network data. Changes in the expected behavior of a network or its performance are commonly detected and corrected by making physical changes to the network environment or by making configuration changes to the networking software. The network system configuration must be constantly monitored and regulated to achieve optimum performance. In the **Recommendations** page, RUCKUS Analytics provides recommendations by monitoring dynamic factors influencing network performance and also seeks to tune static factors with an objective to improve performance metrics, key performance indicators (KPIs), and the user experience. You can view the recommendations on this page and apply them to see how network performance can be improved. This page also provides insights into network performance before and after a recommendation is applied. A recommendation is a change suggested to the software configuration, and it is applied to the SmartZone controller.

NOTE
Only SmartZone controllers running SmartZone 5.2.2 or SmartZone 6.0 and later can make use of the **Recommendations** page in RUCKUS Analytics

FIGURE 41 Recommendations Page



Network
Type: Network | APs: 1521 | Clients: 1238 | Switches: 46

Priority	Date	Category	Summary	Scope	Type	Status	Details	Actions
● Medium	Nov 18 2021 15:48	Wi-Fi Client Experience	Enable DFS Channels	SARAVANAN-MLISA	Zone	New		
● Medium	Nov 18 2021 15:47	Infrastructure	Upgrade	India Zone	Zone	New		
● Medium	Nov 18 2021 11:32	Infrastructure	Upgrade	27-US-CA-Z27-Peat-home	Zone	New		
● Medium	Nov 18 2021 11:32	Infrastructure	Upgrade	SinghZone	Zone	New		
● Medium	Nov 18 2021 11:32	Infrastructure	Upgrade	Deeps Place	Zone	New		
● Medium	Nov 18 2021 11:32	Infrastructure	Upgrade	CWRUZone	Zone	New		
● Medium	Nov 16 2021 11:31	Wi-Fi Client Experience	Enable DFS Channels	Deeps Place	Zone	Failed		
● Medium	Nov 15 2021 14:01	Wi-Fi Client Experience	Enable DFS Channels	SatheeshMadhathil	Zone	Failed		

The **Recommendations** page table displays the following information:

- Priority: Displays the severity of the recommendation as **Low**, **Medium**, or **High**
- Date: Displays the date the recommendation was created.
- Category: Displays the type of recommendation, such as **Infrastructure** and **Wi-Fi Client Experience.**
- Summary: Displays a short description about the suggested recommendation, for example, "Firmware Upgrade", "Enable DFS Channel", and so on.
- Scope: Displays the cluster, domain, and zone levels at which the recommendation can be applied.
- Type: Displays the level at which the recommendation is applied. Currently, it can be applied only at the zone level.
- Status: Displays the status of the recommendation. The status is **New** when the recommendation is available but not applied. The status changes to **Scheduled** after you have scheduled to apply the recommendation. It changes to **Applied** after the scheduled recommendation has applied the change. If applying the recommendation fails, the status changes to **Failed**. Every state change triggers an email message to the network administrator providing information about the status. For more information, refer the following table.

TABLE 13 Recommendation States

State Name	Description	Possible Actions
New	Recommendation is available. Schedule a day and time to apply the recommendation.	Apply or Mute
Scheduled	Recommendation has been scheduled.	Edit Schedule or Cancel
Applied	Recommendation has been successfully applied and RUCKUS Analytics will monitor this configuration change for the next seven days.	Revert or Mute
Failed	An error was encountered when the recommended configuration change was applied and no configuration change was made.	Apply or Mute
Interrupted (Recommendation is not applied)	RUCKUS Analytics has detected a manual configuration change in the SmartZone controller that may interfere with this recommendation. The scheduled recommendation is canceled. Manually check if the recommendation is valid.	Apply or Mute
Interrupted (Recommendation is applied)	RUCKUS Analytics has detected a manual configuration change in the SmartZone controller that may interfere with this recommendation. Results from the monitoring of this configuration change may not be relevant. Manually check if the recommendation is valid.	Revert or Mute

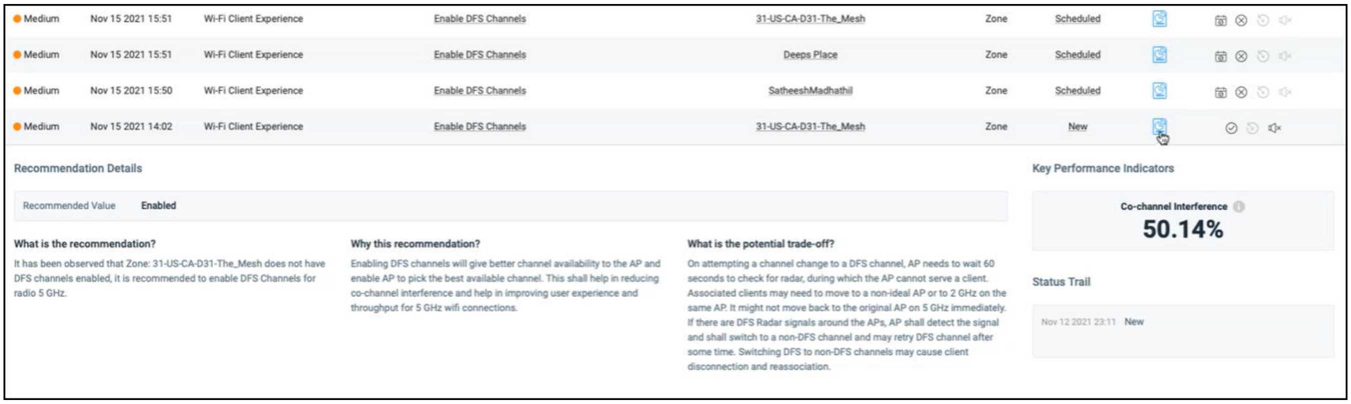
TABLE 13 Recommendation States (continued)

State Name	Description	Possible Actions
Revert	RUCKUS Analytics has detected a degradation in network performance after the application of the recommended configuration. Recommended to immediately revert to previous configuration settings.	Revert or Mute
Revert Scheduled	A reversion to undo the configuration change has been scheduled.	Scheduled
Revert Failed	An error was encountered when the reversion was applied. No reversion was made. Revert the configuration manually from the controller.	Revert or Mute
Reverted	A reversion has been successfully applied.	Mute

- Details: Click the 🗎 icon to view more information, such as the description of the recommendation, the reason why it is encouraged to apply the recommendation and the tradeoff in the network performance if it is not applied,the KPI that is impacted due to the current configuration, and the status trail tracking how the recommendation has changed states.

  In the following example, the recommendation suggest that the DFS channel be enabled for 5 GHz so that channel availability improves, thereby reducing co-channel interference (currently as high as 50.14 percent and impacting performance). If the recommendation is not applied, the potential tradeoffs are listed, such as AP unavailability, possible AP switch to non-DFS channels, disconnections, and so on. name a few.

FIGURE 42 Recommendation Details Example



● Medium	Nov 15 2021 15:51	Wi-Fi Client Experience	Enable DFS Channels	31-US-CA-D31-The_Mesh	Zone	Scheduled	🗎	📅 ⊗ ↺ 🔇
● Medium	Nov 15 2021 15:51	Wi-Fi Client Experience	Enable DFS Channels	Deeps Place	Zone	Scheduled	🗎	📅 ⊗ ↺ 🔇
● Medium	Nov 15 2021 15:50	Wi-Fi Client Experience	Enable DFS Channels	SatheeshMadhathil	Zone	Scheduled	🗎	📅 ⊗ ↺ 🔇
● Medium	Nov 15 2021 14:02	Wi-Fi Client Experience	Enable DFS Channels	31-US-CA-D31-The_Mesh	Zone	New	🗎	✓ ↺ 🔇

Recommendation Details

Recommended Value Enabled

What is the recommendation?

It has been observed that Zone: 31-US-CA-D31-The_Mesh does not have DFS channels enabled, it is recommended to enable DFS Channels for radio 5 GHz.

Why this recommendation?

Enabling DFS channels will give better channel availability to the AP and enable AP to pick the best available channel. This shall help in reducing co-channel interference and help in improving user experience and throughput for 5 GHz wifi connections.

What is the potential trade-off?

On attempting a channel change to a DFS channel, AP needs to wait 60 seconds to check for radar, during which the AP cannot serve a client. Associated clients may need to move to a non-ideal AP or to 2 GHz on the same AP. It might not move back to the original AP on 5 GHz immediately. If there are DFS Radar signals around the APs, AP shall detect the signal and shall switch to a non-DFS channel and may retry DFS channel after some time. Switching DFS to non-DFS channels may cause client disconnection and reassociation.

Key Performance Indicators

Co-channel Interference
50.14%

Status Trail

Nov 12 2021 23:11 New

- Actions: Displays all the actions you can perform, as described in the following table.

TABLE 14 Actions Descriptions

Icon	Action
📅	Edit the schedule for the recommendation.
⊗	Cancel applying the recommendation.
✓	Apply the recommendation. It takes an hour to apply the configuration change to the controller.
🔇	Mute the recommendation. Muting recommendations removes them from the list. You can view all muted recommendations or by clicking **Show muted recommendation** by clicking the ⋮ icon. Click the 🔊 icon to unmute a recommendation. Unmuted recommendations are displayed again in the list of recommendations.
↺	Revert the recommendation. The system reverts to the previous configuration settings.

NOTE

Recommendations are only available for a period of 90 days, after which they are removed. RUCKUS Analytics runs a daily check of the recommendations created to see if they are still relevant and applicable. Recommendations that are no longer relevant or valid are automatically removed from the list.

Recommendations that are applied successfully are also reflected in the **Config Change** page.

Following are the key AI Recommendations provided by RUCKUS Analytics to improve network performance, key performance indicators (KPIs), performance metrics, and the user experience.

TABLE 15 Recommendations

Category	Summary	Why is the Recommendation?
Wi-Fi Client Experience	Auto channel selection mode and background scan on 2.4 GHz radio	Auto Channel Selection feature works well only when RUCKUS APs can perform background scan of the available channels in the network. This helps in building the RF neighborhood. APs can then select an optimum channel for their operation. Hence, it is recommended to enable the Background Scan feature.
Wi-Fi Client Experience	Auto channel selection mode and background scan on 5 GHz radio	Auto Channel Selection feature works well only when RUCKUS APs can perform background scan of the available channels in the network. This helps in building the RF neighborhood. APs can then select an optimum channel for their operation. Hence, it is recommended to enable the Background Scan feature.
Wi-Fi Client Experience	Background scan timer on 2.4 GHz radio	An optimized scan timer for background feature enables RUCKUS APs to scan the channels for an appropriate time interval. Time interval that is too long would result in longer time for radio channel selection.
Wi-Fi Client Experience	Background scan timer on 5 GHz radio	An optimized scan timer for background feature enables RUCKUS APs to scan the channels for an appropriate time interval. Time interval that is too long would result in longer time for radio channel selection.
Wi-Fi Client Experience	Enable DFS channels	Enabling the DFS channels give more available channel options for the AP and enable the AP radio to pick the best available channel. This will help to reduce co-channel interference, enhance user experience and improve throughput for 5 GHz Wi-Fi connections.
Wi-Fi Client Experience	Disable DFS channels	If AP is placed in an area where there are genuine and consistent DFS Radar signals, then the AP should not select DFS channel to ensure uninterrupted operations.
Wi-Fi Client Experience	Enable band balancing	Band Balancing feature intelligently distributes WLAN clients on 2.4 GHz and 5 GHz channels to balance the client load. Band Balancing results in better radio utilization and gives better Wi-Fi experience to the user.
Wi-Fi Client Experience	Change band balancing mode	Band Balancing (BB) feature intelligently distributes the WLAN clients on the 2.4G and the 5G channels to balance the client load. The "PROACTIVE" mode has high efficiency in steering clients from one band to another and thus, balance the load on the AP resulting in better Wi-Fi experience to the user.

TABLE 15 Recommendations (continued)

Category	Summary	Why is the Recommendation?
Wi-Fi Client Experience	Enable load balancing based on client count	Client Load Balancing allows equal distribution of Clients by allowing heavily loaded APs to move clients to less loaded neighboring APs. This ensures better radio utilization and provides better Wi-Fi experience to the user.
Wi-Fi Client Experience	Tx power setting for 2.4 GHz and 5 GHz radio	Encourages client association to 5 GHz and reduces co-channel interference on 2.4 GHz
Infrastructure	Zone firmware upgrade	The latest AP Firmware version in the zone ensures all the APs in the Zone to have the best available firmware with appropriate security or bug fixes and new features.
AI-Driven Cloud Radio Resource Management (RRM)	AI-Driven Cloud RRM	Based on the AI Analytics, enabling the AI-Driven Cloud RRM will constantly monitor the network, and adjust the channel plan, bandwidth, and AP transmit power when necessary to decrease the number of interfering links to zero. For more information, refer to AI-Driven Cloud Radio Resource Management on page 89.

Health Page

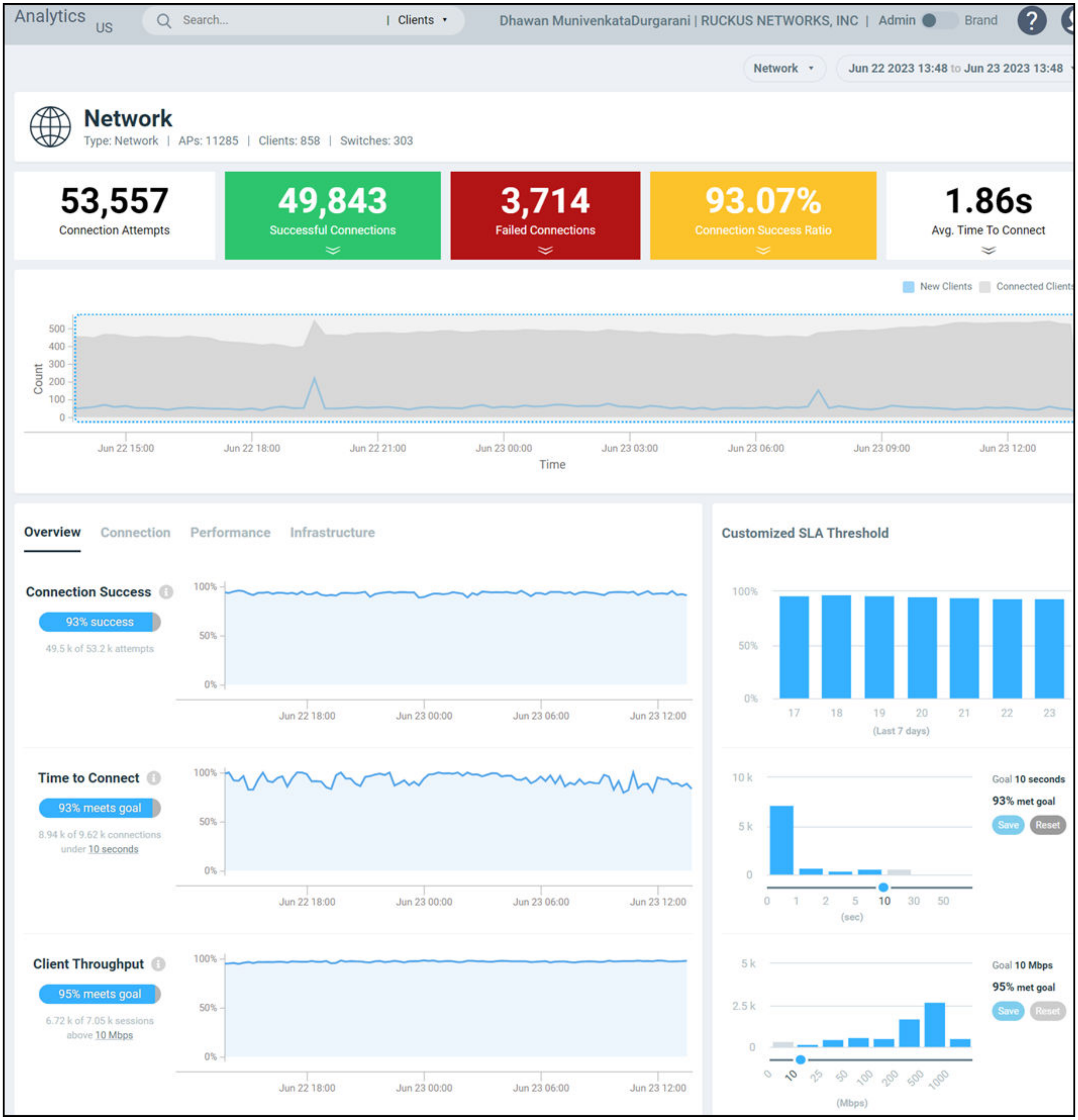
The **Health** page provides information about network health by giving insights about key performance indicators (KPIs) of the network. The information provided by the **Health** page allows you to analyze the network health and behavior in real time.

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 235 and Managing Resource Groups on page 236.

FIGURE 43 Health Page



Analytics US | Search... | Clients ▾ | Dhawan MunivenkataDurgarani | RUCKUS NETWORKS, INC | Admin | Brand

Network ▾ | Jun 22 2023 13:48 to Jun 23 2023 13:48

Network

Type: Network | APs: 11285 | Clients: 858 | Switches: 303

53,557 Connection Attempts

49,843 Successful Connections

3,714 Failed Connections

93.07% Connection Success Ratio

1.86s Avg. Time To Connect

Overview | Connection | Performance | Infrastructure

Connection Success: 93% success — 49.5 k of 53.2 k attempts

Time to Connect: 93% meets goal — 8.94 k of 9.62 k connections under 10 seconds

Client Throughput: 95% meets goal — 6.72 k of 7.05 k sessions above 10 Mbps

Customized SLA Threshold

Goal 10 seconds — 93% met goal — Save | Reset

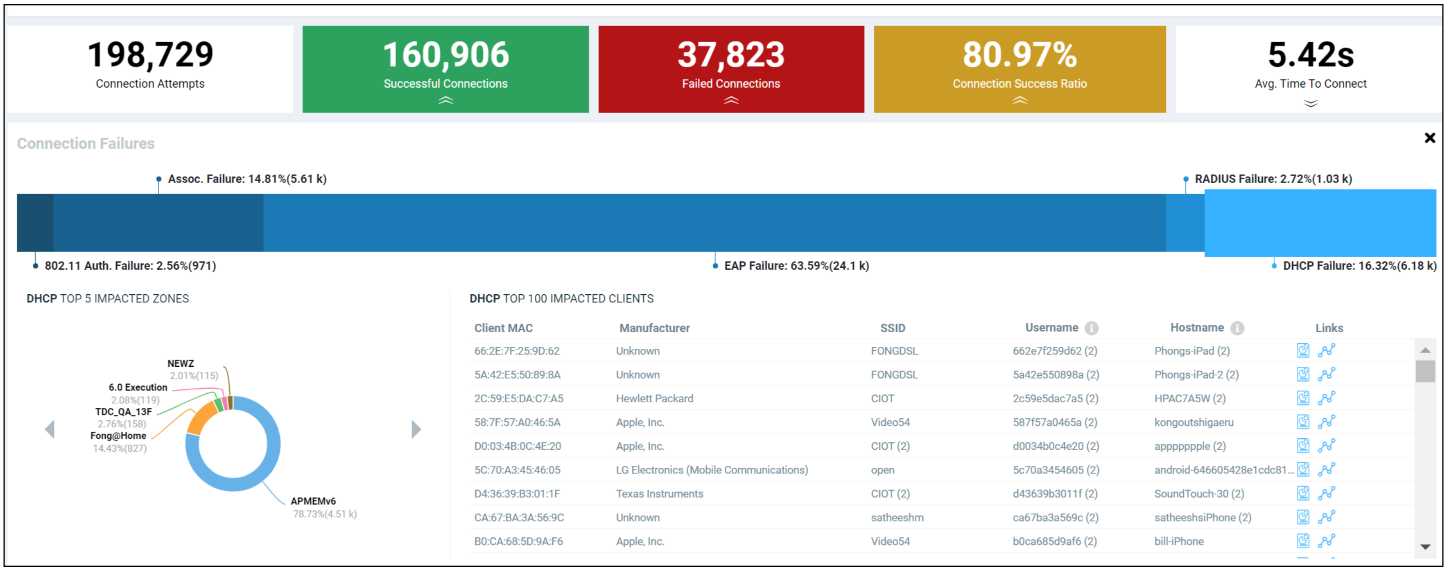
Goal 10 Mbps — 95% met goal — Save | Reset

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 gray 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 colored 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 44 Connection Failures Tile

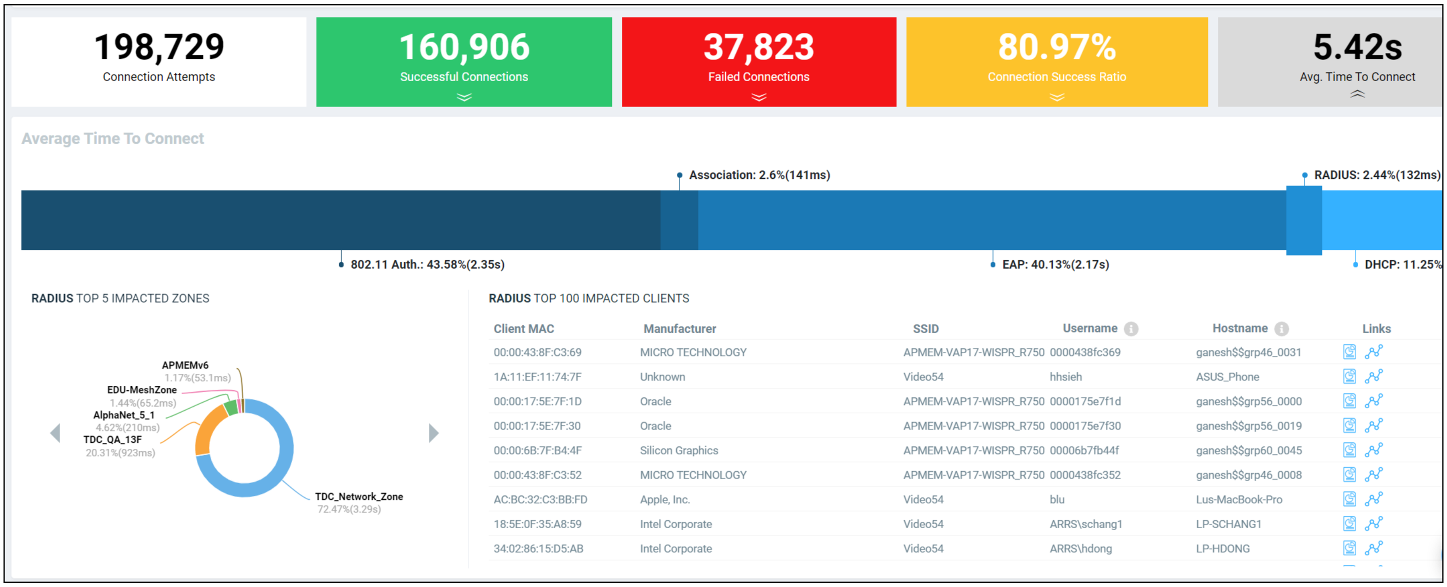


DHCP TOP 100 IMPACTED CLIENTS

Client MAC	Manufacturer	SSID	Username	Hostname	Links
66:2E:7F:25:9D:62	Unknown	FONGDSL	662e7f259d62 (2)	Phongs-iPad (2)	
5A:42:E5:50:89:8A	Unknown	FONGDSL	5a42e550898a (2)	Phongs-iPad-2 (2)	
2C:59:E5:DA:C7:A5	Hewlett Packard	CIOT	2c59e5dac7a5 (2)	HPAC7A5W (2)	
58:7F:57:A0:46:5A	Apple, Inc.	Video54	587f57a0465a (2)	kongoutshigaeru	
D0:03:4B:0C:4E:20	Apple, Inc.	CIOT (2)	d0034b0c4e20 (2)	apppppple (2)	
5C:70:A3:45:46:05	LG Electronics (Mobile Communications)	open	5c70a3454605 (2)	android-646605428e1cdc81...	
D4:36:39:B3:01:1F	Texas Instruments	CIOT (2)	d43639b3011f (2)	SoundTouch-30 (2)	
CA:67:BA:3A:56:9C	Unknown	satheeshm	ca67ba3a569c (2)	satheeshsiPhone (2)	
B0:CA:68:5D:9A:F6	Apple, Inc.	Video54	b0ca685d9af6 (2)	bill-iPhone	

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 authentication, 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 45 Average Time To Connect Tile



RADIUS TOP 100 IMPACTED CLIENTS

Client MAC	Manufacturer	SSID	Username	Hostname	Links
00:00:43:8F:C3:69	MICRO TECHNOLOGY	APMEM-VAP17-WISPR_R750	0000438fc369	ganesh$$grp46_0031	
1A:11:EF:11:74:7F	Unknown	Video54	hhsieh	ASUS_Phone	
00:00:17:5E:7F:1D	Oracle	APMEM-VAP17-WISPR_R750	0000175e7f1d	ganesh$$grp56_0000	
00:00:17:5E:7F:30	Oracle	APMEM-VAP17-WISPR_R750	0000175e7f30	ganesh$$grp56_0019	
00:00:6B:7F:B4:4F	Silicon Graphics	APMEM-VAP17-WISPR_R750	00006b7fb44f	ganesh$$grp60_0045	
00:00:43:8F:C3:52	MICRO TECHNOLOGY	APMEM-VAP17-WISPR_R750	0000438fc352	ganesh$$grp46_0008	
AC:BC:32:C3:BB:FD	Apple, Inc.	Video54	blu	Lus-MacBook-Pro	
18:5E:0F:35:A8:59	Intel Corporate	Video54	ARRS\schang1	LP-SCHANG1	
34:02:86:15:D5:AB	Intel Corporate	Video54	ARRS\hdong	LP-HDONG	

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. A connection is deemed successful when a Wi-Fi client is able to complete the 802.11 authentication, association, L2 authentication, and receives an IP address from the DHCP. If any of these stages fail, it is considered as a failed connection. For L3 authentication such as WISPr and captive portal authentication, since the WiFi client receives an IP address before the L3 authentication, the client connection is deemed successful before the L3 authentication completes.

  The time-series graph on the left displays the percentage of successful connections across time, and the bar chart on the right captures the daily percentage over the last seven days of the selected time range. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

- Time to Connect (TTC): Measures the total time taken for a WiFi client to successfully go through all the required stages in order to establish an IP connection, namely 802.11 authentication, association, L2 authentication, and receiving an IP address from the DHCP. For L3 authentication, such as WISPr and captive portal authentication, since the WiFi client will receive an IP address before the L3 authentication, the time to connect does not include the time taken for L3 authentication.

  The time-series graph on the left displays the percentage of successful connections across time, that meet the configured TTC SLA. Bar chart on the right displays the distribution of TTC. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

- Client Throughput: Measures the down link throughput estimate of the client, taking into consideration RF channel conditions, interference, channel contention, and client capabilities.

  The time-series graph on the left displays the percentage of WiFi sessions across time that have a client throughput that meets the configured SLA. The bar chart on the right displays the distribution of the client throughput. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.
- AP Capacity: Measures the downlink saturated throughput estimate of the AP radios, taking into consideration the RF channel conditions, interference, channel contention and client capabilities.

  The time-series graph on the left displays the percentage of AP capacity samples across time that meets the configured SLA. The bar chart on the right displays the distribution of AP capacity across the number of APs. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.
- AP-Controller Connection Uptime: Measures the percentage of time the AP radios are fully available for client service. the percentage of time the radios of an AP are fully available for client service.

  The time-series graph on the left displays the percentage of AP-Controller connection uptime samples across time that meets the configured SLA. The bar chart on the right displays the distribution of AP service uptime across the number of APs. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.
- Online APs: Measures the percentage of APs which are online and connected to Smart Zone.

  The time-series graph on the left displays the Online AP percentage across time. The bar chart on the right captures the daily Online AP percentage over the last seven days of the selected time range. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

TABLE 16 KPIs Snapshot: Overview Tab

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

TABLE 16 KPIs Snapshot: Overview Tab (continued)

KPI	Pill-Shaped Box	Time Series Graph	Histogram
AP-Controller Connection 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. A connection is deemed successful when a WiFi client is able to complete the 802.11 authentication, association, L2 authentication, and receives an IP address from the DHCP. If any of these stages fail, it is considered as a failed connection. For L3 authentication such as WISPr and captive portal authentication, since the WiFi client receives an IP address before the L3 authentication, the client connection is deemed successful before the L3 authentication completes.

  The time-series graph on the left displays the percentage of successful connections across time, and the bar chart on the right captures the daily percentage over the last seven days of the selected time range. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

- Time to Connect (TTC): Measures the total time taken for a WiFi client to successfully go through all the required stages in order to establish an IP connection, namely 802.11 authentication, association, L2 authentication, and receiving an IP address from the DHCP. For L3 authentication, such as WISPr and captive portal authentication, since the WiFi client will receive an IP address before the L3 authentication, the time to connect does not include the time taken for L3 authentication.

  The time-series graph on the left displays the percentage of successful connections across time, that meet the configured TTC SLA. Bar chart on the right displays the distribution of TTC. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

- 802.11 Authentication: The time-series graph on the left displays the percentage of 802.11 authentication attempts that has completed successfully. 802.11 authentication is the first step in establishing a WiFi connection, and it requires a WiFi client to establish its identity as a valid 802.11 device with an AP. No data encryption or security is available at this stage, and it is not to be confused with WPA or 802.1X authentication.

  The bar chart on the right captures the daily percentage over the past seven days. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the histogram remains fixed based on the date range selected at the top of the page.

- Association: Measures the percentage of association attempts that have completed successfully. An association attempt is deemed successful when the WiFi client receives an Association ID from the AP. It is normal for a single WiFi client to have more than one association attempts. The bar chart on the right captures the daily percentage over the last seven days of the selected time range. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

- EAP: The time-series graph on the left displays the percentage of EAP attempts (consisting the 4-way handshake between client and AP) that have completed successfully. An EAP attempt is deemed successful when all the necessary handshakes are completed. It is possible for a single WiFi client to have multiple EAP attempts. The bar chart on the right captures the daily percentage over the last seven days of the selected time range. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.
- RADIUS: The time-series graph on the left displays the percentage of RADIUS authentication attempts that have completed successfully. A RADIUS authentication attempt is deemed successful when all the necessary handshakes in the RADIUS protocol are completed, and the client is either allowed or denied access. It is possible for a single WiFi client to have multiple authentication attempts. The bar chart on the right captures the daily percentage over the last seven days of the selected time range. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.
- DHCP: The time-series graph on the left displays the percentage of DHCP connection attempts that have completed successfully. A DHCP connection attempt is deemed successful when the WiFi client has received an IP address from the DHCP server. It is possible for a single WiFi client to have multiple DHCP connection attempts. The bar chart on the right captures the daily percentage over the last seven days of the selected time range. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.
- Roaming Success: Measures the percentage of roaming attempts that have completed successfully. A roaming attempt is deemed successful when the WiFi client has its session transferred from one AP to the next. It is possible for a single WiFi client to have multiple roaming attempts. The bar chart on the right captures the daily percentage over the last seven days of the selected time range. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

TABLE 17 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
EAP	Displays the percentage of EAP attempts (consisting the 4-way handshake between client and AP) that have completed successfully.	Displays the percentage of EAP 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 EAP 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

TABLE 17 KPIs Snapshot: Connection Tab (continued)

KPI	Pill-Shaped Box	Time Series Graph	Histogram
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 down link throughput estimate of the client, taking into consideration RF channel conditions, interference, channel contention, and client capabilities.

  The time-series graph on the left displays the percentage of WiFi sessions across time that have a client throughput that meets the configured SLA. The bar chart on the right displays the distribution of the client throughput. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

- AP Capacity: Measures the downlink saturated throughput estimate of the AP radios, taking into consideration the RF channel conditions, interference, channel contention and client capabilities.

  The time-series graph on the left displays the percentage of AP capacity samples across time that meets the configured SLA. The bar chart on the right displays the distribution of AP capacity across the number of APs. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

- Client RSSI: The time-series graph on the left displays the percentage of client sessions with average RSS that met the configured SLA. The bar chart on the right captures the distribution of the RSS. Do note that the numbers related to the time-series graph will change as you zoom in/out of a time range, whereas the bar chart will stay fixed based on the selected time range at the top of the page.

TABLE 18 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-Controller Connection Uptime: Measures the percentage of time the AP radios are fully available for client service. the percentage of time the radios of an AP are fully available for client service.

  The time-series graph on the left displays the percentage of AP-Controller connection uptime samples across time that meets the configured SLA. The bar chart on the right displays the distribution of AP service uptime across the number of APs. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.
- AP-to-SZ-Latency: The time-series graph on the left displays the percentage of APs that have AP-to-SZ control plane latency which meets the configured SLA. The bar chart on the right captures the distribution of the latency across the number of APs. Note that the numbers related to the time-series graph will change as you zoom in/out of a time range, whereas the bar chart remains fixed based on the selected time range at the top of the page.
- Cluster Latency: The time-series graph on the left displays the percentage of samples that have intra-SZ cluster latency (which is the latency between each node within a SZ cluster) which meets the configured SLA. The bar chart on the right captures the distribution of the latency across the number of clusters. Note that the numbers related to the time-series graph will change as you zoom in/out of a time range, whereas the bar chart remains fixed based on the selected time range at the top of the page.

- PoE Utilization: Measures the percentage of PoE utilization by the switches in the network. The time-series graph on the left displays the percentage of switches across time that meet the configured SLA. The bar chart on the right captures the distribution of PoE utilization across the number of switches. Note that the numbers related to the time-series graph will change as you zoom in/out of a time range, whereas the bar chart remains fixed based on the selected time range at the top of the page.
- Online APs: Measures the percentage of APs which are online and connected to Smart Zone.

  The time-series graph on the left displays the Online AP percentage across time. The bar chart on the right captures the daily Online AP percentage over the last seven days of the selected time range. Note that the numbers related to the time-series will change as you zoom-in or zoom-out of a time range, whereas the bar chart remains fixed based on the time range selected at the top of the page.

TABLE 19 KPI Snapshot: Infrastructure Tab

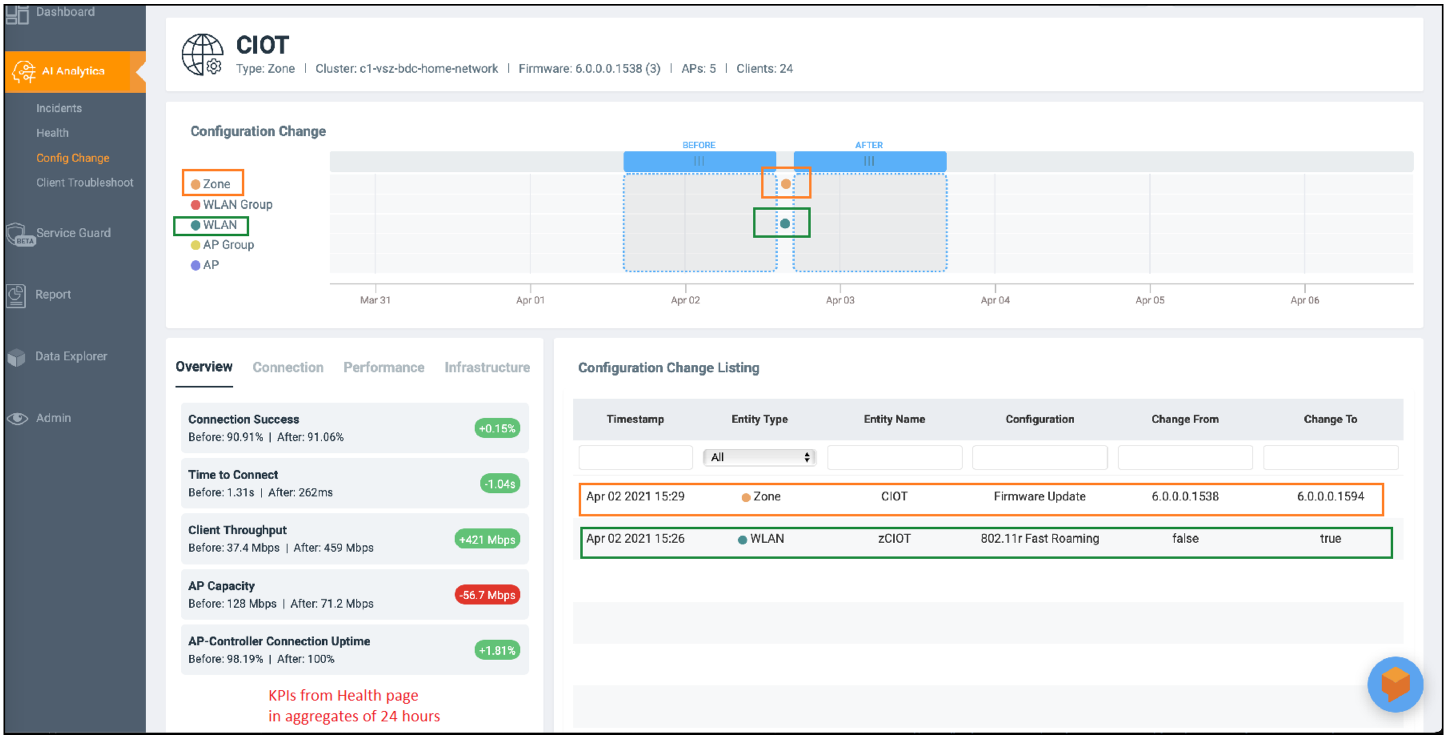
KPI	Pill-Shaped Box	Time Series Graph	Histogram
AP-to-SZ-Latency	Displays the percentage of APs with the AP-to-SZ latency that met the SLA (for the selected time range)	Displays the percentage of APs with the AP-to-SZ latency that met the SLA over time	Displays a bar chart of average latency percentage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

Configuration Change Page

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

NOTE
Configuration change analysis is only available for SmartZone controllers.

FIGURE 46 Configuration Change Page



CIOT

Type: Zone | Cluster: c1-vsz-bdc-home-network | Firmware: 6.0.0.0.1538 (3) | APs: 5 | Clients: 24

Configuration Change

Connection Success +0.15%
Before: 90.91% | After: 91.06%

Time to Connect -1.04s
Before: 1.31s | After: 262ms

Client Throughput +421 Mbps
Before: 37.4 Mbps | After: 459 Mbps

AP Capacity -56.7 Mbps
Before: 128 Mbps | After: 71.2 Mbps

AP-Controller Connection Uptime +1.81%
Before: 98.19% | After: 100%

KPIs from Health page
in aggregates of 24 hours

Configuration Change Listing

Timestamp	Entity Type	Entity Name	Configuration	Change From	Change To
	All				
Apr 02 2021 15:29	● Zone	CIOT	Firmware Update	6.0.0.0.1538	6.0.0.0.1594
Apr 02 2021 15:26	● WLAN	zCIOT	802.11r Fast Roaming	false	true

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

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

Configuration Change Tile

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

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

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

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

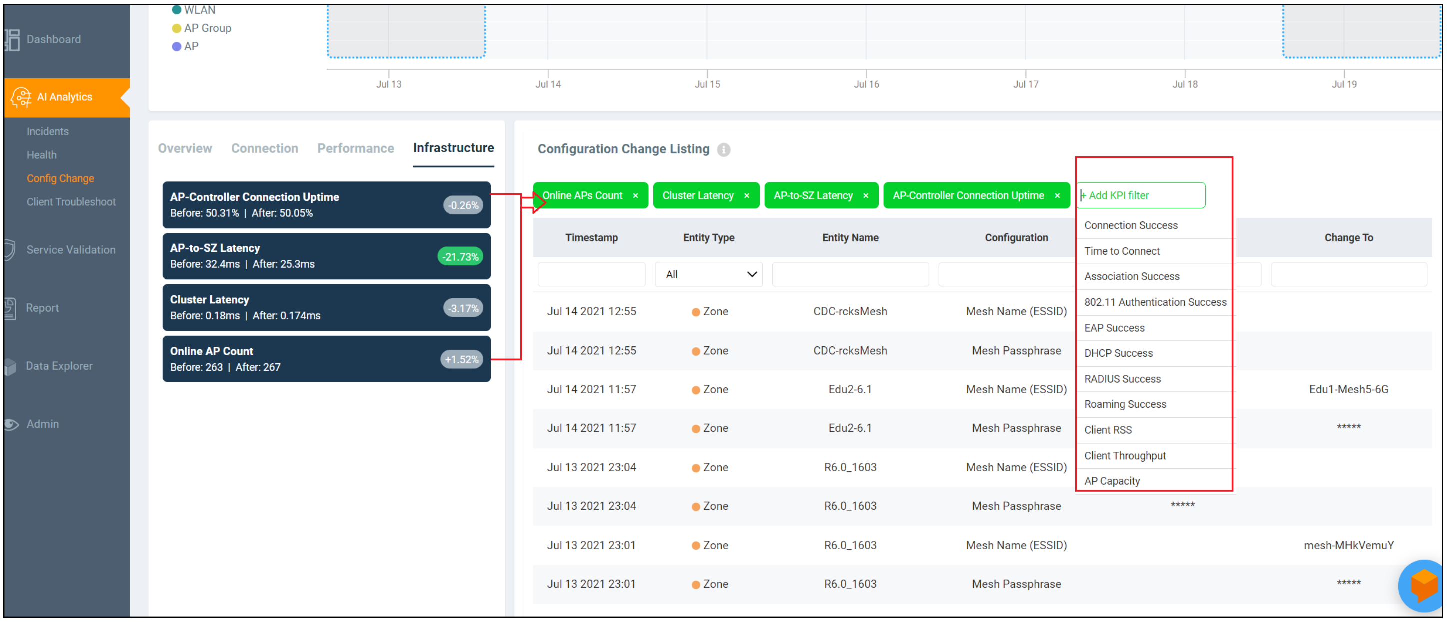
Configuration Change Listing Tile

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

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

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

FIGURE 47 Configuration Change Listing Tile: Adding Health KPIs



AP-Controller Connection Uptime -0.26%
Before: 50.31% | After: 50.05%

AP-to-SZ Latency -21.73%
Before: 32.4ms | After: 25.3ms

Cluster Latency -3.17%
Before: 0.18ms | After: 0.174ms

Online AP Count +1.52%
Before: 263 | After: 267

Configuration Change Listing

Timestamp	Entity Type	Entity Name	Configuration		Change To
	All				
Jul 14 2021 12:55	● Zone	CDC-rcksMesh	Mesh Name (ESSID)		
Jul 14 2021 12:55	● Zone	CDC-rcksMesh	Mesh Passphrase		
Jul 14 2021 11:57	● Zone	Edu2-6.1	Mesh Name (ESSID)		Edu1-Mesh5-6G
Jul 14 2021 11:57	● Zone	Edu2-6.1	Mesh Passphrase		*****
Jul 13 2021 23:04	● Zone	R6.0_1603	Mesh Name (ESSID)		
Jul 13 2021 23:04	● Zone	R6.0_1603	Mesh Passphrase	*****	
Jul 13 2021 23:01	● Zone	R6.0_1603	Mesh Name (ESSID)		mesh-MHkVemuY
Jul 13 2021 23:01	● Zone	R6.0_1603	Mesh Passphrase		*****

NOTE
When a configuration is disabled, the value of the configuration change appears as 0.

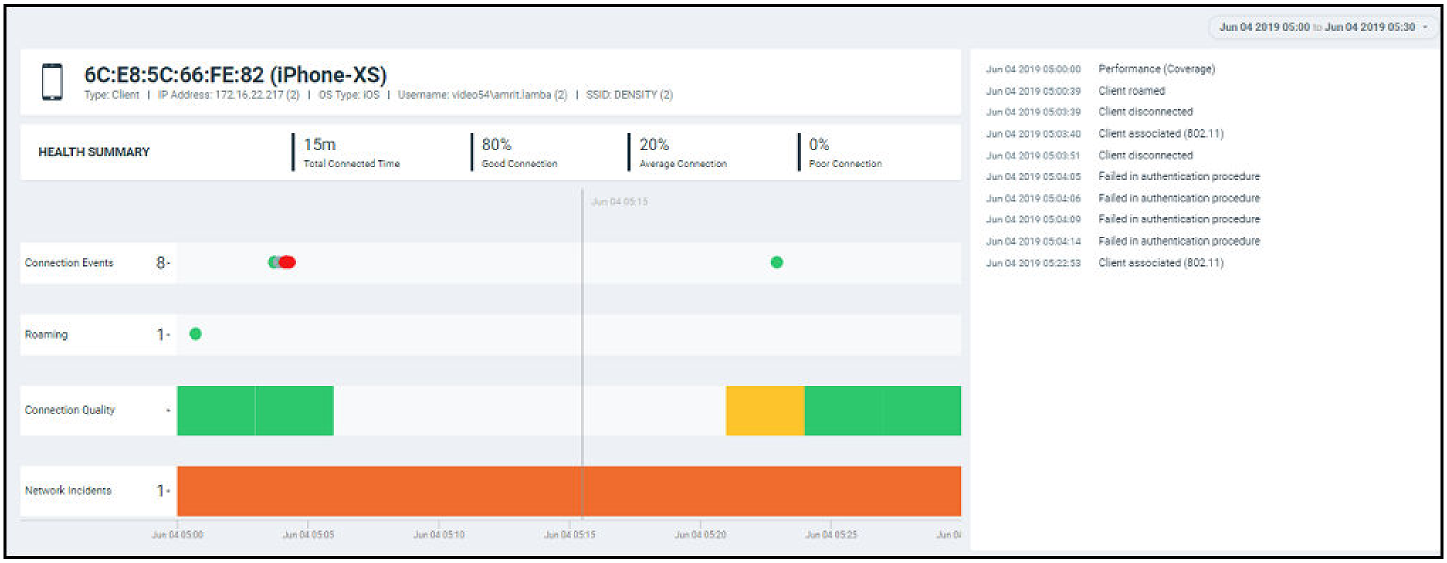
Health Tile

The **Health** tile displays the same KPIs that are available on the **Health** page, the difference being the **Health** tile displays KPI data aggregated over 24 hours, which is more granular than the Health page with respect to time. For more information, refer to Health Page on page 66. In the **Health** tile, you can view the before and after values of each KPI impacted by the configuration change. The overall impact of the change is displayed within a red, gray or green capsule based on the percentage change. The capsule appears green if the configuration change positively impacted the KPI or improved the performance by more than 5 percent. It appears red if the change negatively impacted the KPI value and diminished the performance by less than 5 percent. It appears gray if the KPI value is strictly + or - 5%. These granular details enable an administrator to monitor network health continuously and ensure the network performs to its highest capabilities.

Client Troubleshoot Page

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

FIGURE 48 Client Troubleshoot Page



Jun 04 2019 05:00 to Jun 04 2019 05:30

6C:E8:5C:66:FE:82 (iPhone-XS)

Type: Client | IP Address: 172.16.22.217 (2) | OS Type: iOS | Username: video54\amrit.lamba (2) | SSID: DENSITY (2)

HEALTH SUMMARY

15m Total Connected Time | 80% Good Connection | 20% Average Connection | 0% Poor Connection

```
Jun 04 2019 05:00:00   Performance (Coverage)
Jun 04 2019 05:00:39   Client roamed
Jun 04 2019 05:03:39   Client disconnected
Jun 04 2019 05:03:40   Client associated (802.11)
Jun 04 2019 05:03:51   Client disconnected
Jun 04 2019 05:04:05   Failed in authentication procedure
Jun 04 2019 05:04:06   Failed in authentication procedure
Jun 04 2019 05:04:09   Failed in authentication procedure
Jun 04 2019 05:04:14   Failed in authentication procedure
Jun 04 2019 05:22:53   Client associated (802.11)
```

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
- IP address
- OS type
- Username
- SSID

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

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

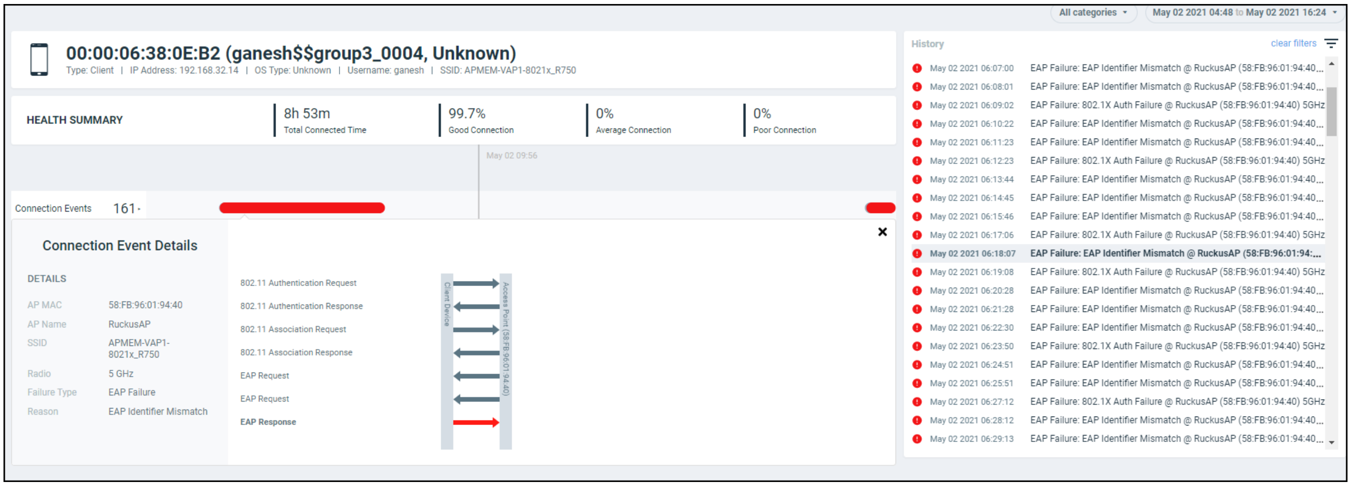
- Total Connected Time
- Percentage of Good Connection
- Percentage of Average Connection
- Percentage of Poor Connection

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

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

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

FIGURE 49 Failure Due to EAP Identifier Mismatch



00:00:06:38:0E:B2 (ganesh$$group3_0004, Unknown)
Type: Client | IP Address: 192.168.32.14 | OS Type: Unknown | Username: ganesh | SSID: APMEM-VAP1-8021x_R750

HEALTH SUMMARY
8h 53m Total Connected Time
99.7% Good Connection
0% Average Connection
0% Poor Connection

May 02 09:56

Connection Events 161

Connection Event Details

DETAILS

AP MAC	58:FB:96:01:94:40
AP Name	RuckusAP
SSID	APMEM-VAP1-8021x_R750
Radio	5 GHz
Failure Type	EAP Failure
Reason	EAP Identifier Mismatch

802.11 Authentication Request
802.11 Authentication Response
802.11 Association Request
802.11 Association Response
EAP Request
EAP Request
EAP Response

Client Device
Access Point (58:FB:96:01:94:40)
×
All categories
May 02 2021 04:48 to May 02 2021 16:24
History
clear filters

```
May 02 2021 06:07:00   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:08:01   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:09:02   EAP Failure: 802.1X Auth Failure @ RuckusAP (58:FB:96:01:94:40) 5GHz
May 02 2021 06:10:22   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:11:23   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:12:23   EAP Failure: 802.1X Auth Failure @ RuckusAP (58:FB:96:01:94:40) 5GHz
May 02 2021 06:13:44   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:14:45   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:15:46   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:17:06   EAP Failure: 802.1X Auth Failure @ RuckusAP (58:FB:96:01:94:40) 5GHz
May 02 2021 06:18:07   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:...
May 02 2021 06:19:08   EAP Failure: 802.1X Auth Failure @ RuckusAP (58:FB:96:01:94:40) 5GHz
May 02 2021 06:20:28   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:21:28   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:22:30   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:23:50   EAP Failure: 802.1X Auth Failure @ RuckusAP (58:FB:96:01:94:40) 5GHz
May 02 2021 06:24:51   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:25:51   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:27:12   EAP Failure: 802.1X Auth Failure @ RuckusAP (58:FB:96:01:94:40) 5GHz
May 02 2021 06:28:12   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
May 02 2021 06:29:13   EAP Failure: EAP Identifier Mismatch @ RuckusAP (58:FB:96:01:94:40...
```

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

Roaming shows the connection events and detailed metrics of the client when it roams between multiple APs. You can select the menu to view the roaming AP details. You can also pause the pointer over the graph to view more information such as radio mode, spatial stream, bandwidth and so on. These details help in troubleshooting issues that arise when clients roam from one AP to another. 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.

Packet Capture (PCAP)

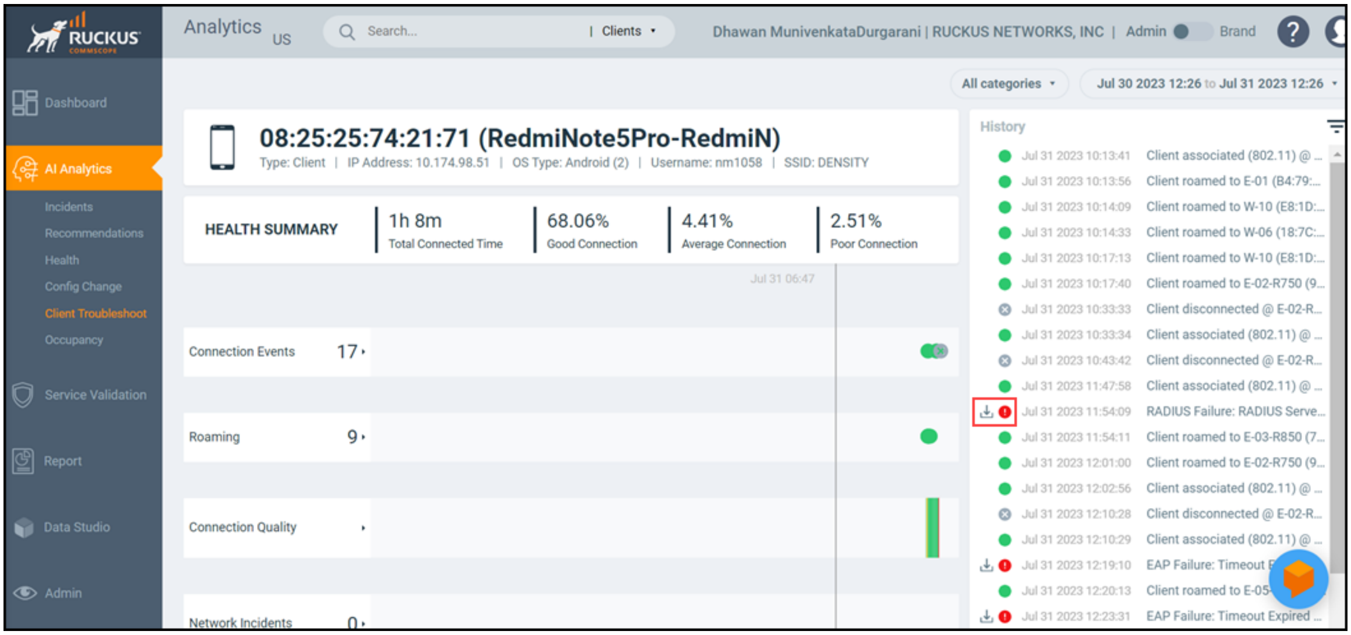
NOTE
PCAPs will be available in RUCKUS Analytics for associated Smartzone release 6.1.2 and later.

This is a collection of packets generated for all failure events with respect to the specific client. This allows the clients admins to inspect network packets and troubleshoot the issues. All PCAP reports will be stored for three months before they are deleted.

Complete the following steps to download the PCAP packets:

1. Search for the clients name in the **Client Troubleshoot** page **Search** field.

FIGURE 50 Client Troubleshoot - PCAP



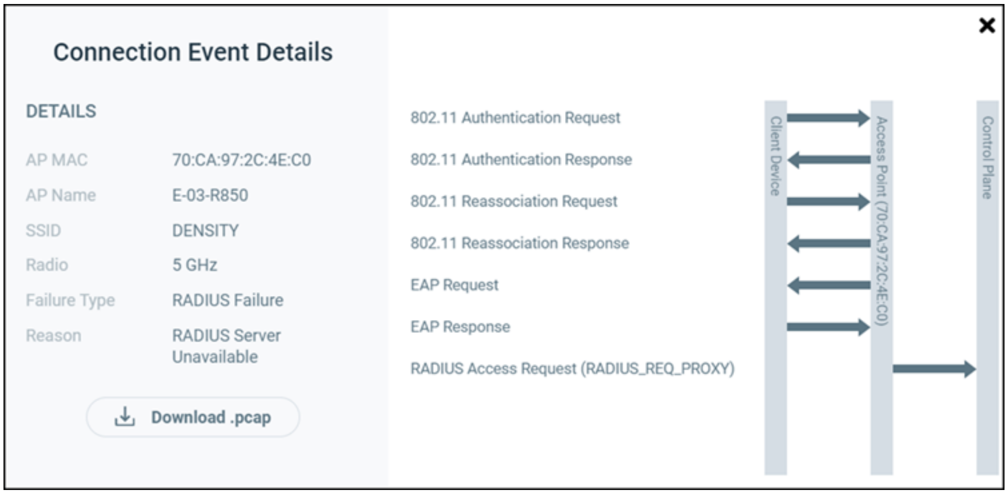
08:25:25:74:21:71 (RedmiNote5Pro-RedmiN)
Type: Client | IP Address: 10.174.98.51 | OS Type: Android (2) | Username: nm1058 | SSID: DENSITY

HEALTH SUMMARY | 1h 8m Total Connected Time | 68.06% Good Connection | 4.41% Average Connection | 2.51% Poor Connection

```
Jul 31 2023 10:13:41   Client associated (802.11) @ ...
Jul 31 2023 10:13:56   Client roamed to E-01 (B4:79:...
Jul 31 2023 10:14:09   Client roamed to W-10 (E8:1D:...
Jul 31 2023 10:14:33   Client roamed to W-06 (18:7C:...
Jul 31 2023 10:17:13   Client roamed to W-10 (E8:1D:...
Jul 31 2023 10:17:40   Client roamed to E-02-R750 (9...
Jul 31 2023 10:33:33   Client disconnected @ E-02-R...
Jul 31 2023 10:33:34   Client associated (802.11) @ ...
Jul 31 2023 10:43:42   Client disconnected @ E-02-R...
Jul 31 2023 11:47:58   Client associated (802.11) @ ...
Jul 31 2023 11:54:09   RADIUS Failure: RADIUS Serve...
Jul 31 2023 11:54:11   Client roamed to E-03-R850 (7...
Jul 31 2023 12:01:00   Client roamed to E-02-R750 (9...
Jul 31 2023 12:02:56   Client associated (802.11) @ ...
Jul 31 2023 12:10:28   Client disconnected @ E-02-R...
Jul 31 2023 12:10:29   Client associated (802.11) @ ...
Jul 31 2023 12:19:10   EAP Failure: Timeout E
Jul 31 2023 12:20:13   Client roamed to E-05
Jul 31 2023 12:23:31   EAP Failure: Timeout Expired ...
```

2. In the **History** tab, click failure events. The **Connection Event Details** dialog box is displayed.

FIGURE 51 Connection Event Details Dialog Box



Connection Event Details

DETAILS

AP MAC	70:CA:97:2C:4E:C0
AP Name	E-03-R850
SSID	DENSITY
Radio	5 GHz
Failure Type	RADIUS Failure
Reason	RADIUS Server Unavailable

Download .pcap

802.11 Authentication Request
802.11 Authentication Response
802.11 Reassociation Request
802.11 Reassociation Response
EAP Request
EAP Response
RADIUS Access Request (RADIUS_REQ_PROXY)

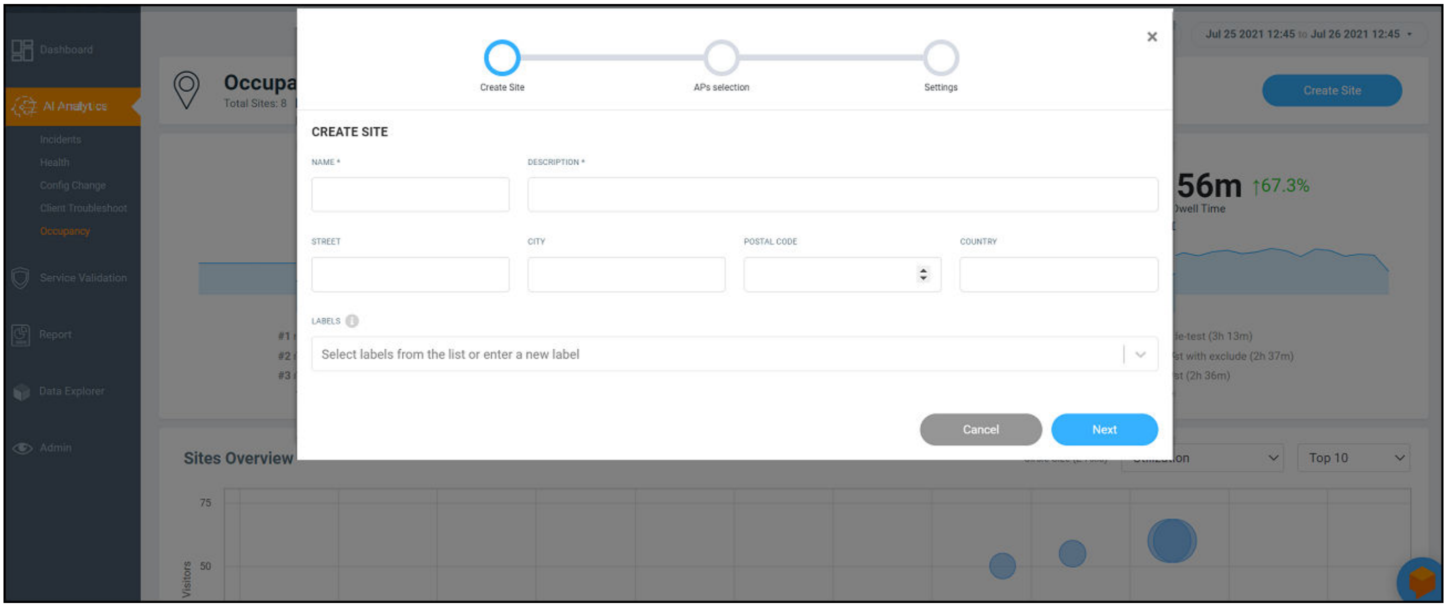
3. Click **Download .pcap** icon to download the zip file.

Occupancy Page

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

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

FIGURE 52 Creating a Site



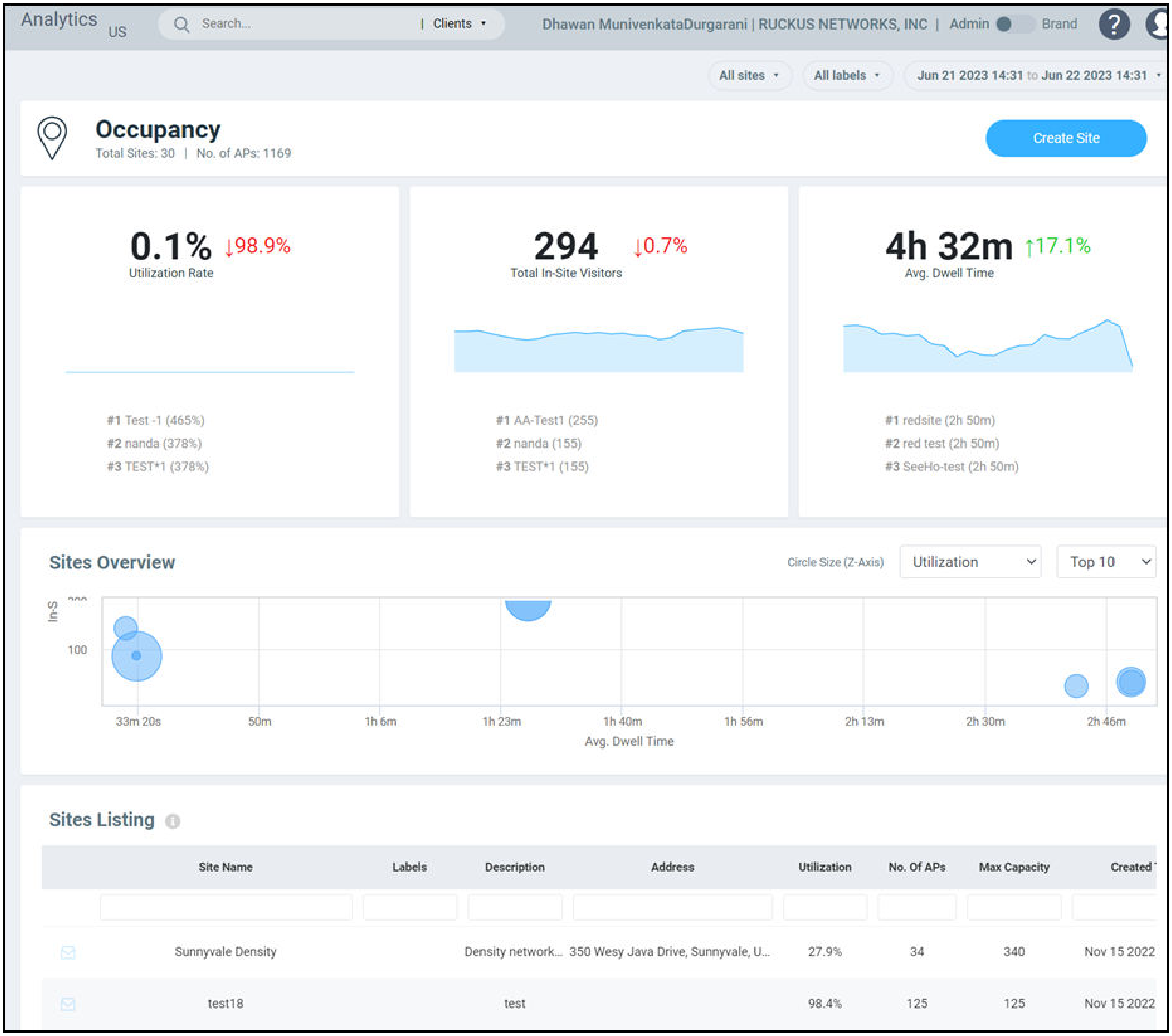
1. From the **Occupancy** page, click **Create Site**.
2. Enter the name of the site, a description (an area of the facility for which your are creating the site, for example, the gym, the lobby, the third floor, or a similar area), and the street, city, postal code, and country of the site. Also, select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

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

3. Click **Next**.
4. Select the APs you want to group within this site.
5. Click **Next**.
6. In the **Settings** page, set the maximum capacity per AP. Occupancy Analytics engine is always active and powers the email notification feature. Email notifications are designed to alert site owners when the occupancy reaches or exceeds 100% of maximum site capacity. Configuration for this feature is available in the **Settings** page. Based on the APs you selected, the number of APs are populated and the maximum capacity of the site is calculated and displayed. The site utilization is computed every 15min based on the maximum capacity set for the site. When the site utilization percentage reaches 100%, an email notification is sent to the address configured in the **Settings** page. You can include one or more e-mail addresses for communication to notify when the site utilization percentage reaches 100%.
7. Click **Create**. The site is created and displayed in the **Sites Listing** table.

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

FIGURE 53 Occupancy Page



Occupancy

Total Sites: 30 | No. of APs: 1169

0.1% ↓98.9%
Utilization Rate

#1 Test -1 (465%)
#2 nanda (378%)
#3 TEST*1 (378%)

294 ↓0.7%
Total In-Site Visitors

#1 AA-Test1 (255)
#2 nanda (155)
#3 TEST*1 (155)

4h 32m ↑17.1%
Avg. Dwell Time

#1 redsite (2h 50m)
#2 red test (2h 50m)
#3 SeeHo-test (2h 50m)

Sites Listing

	Site Name	Labels	Description	Address	Utilization	No. Of APs	Max Capacity	Created
	Sunnyvale Density		Density network...	350 Wesy Java Drive, Sunnyvale, U...	27.9%	34	340	Nov 15 2022
	test18		test		98.4%	125	125	Nov 15 2022

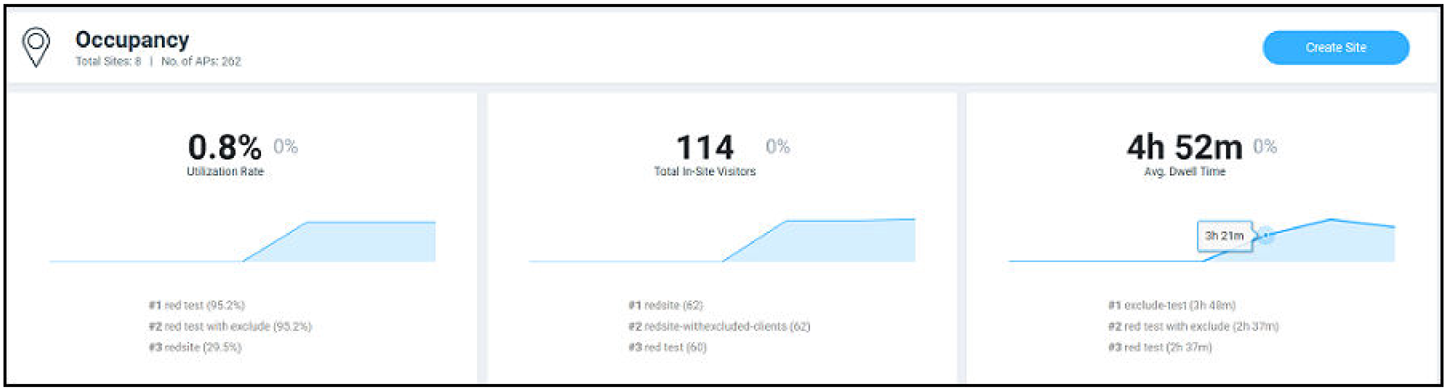
The **Occupancy** page contains a number of components:

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

Utilization Tile

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

FIGURE 54 Utilization, Total In-site Visitors, and Avg Dwell Time Tiles



#1 red test (95.2%)
#2 red test with exclude (95.2%)
#3 redsite (29.5%)

#1 redsite (62)
#2 redsite-withexcluded-clients (62)
#3 red test (60)

#1 exclude-test (3h 48m)
#2 red test with exclude (2h 37m)
#3 red test (2h 37m)

Total In-Site Visitors Tile

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

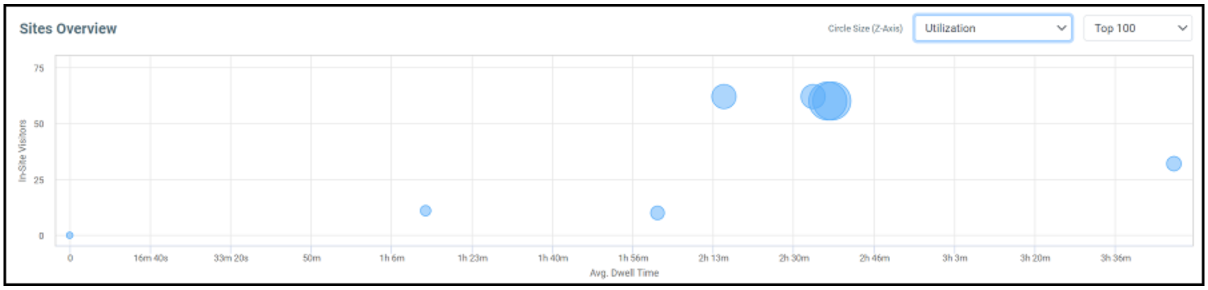
Avg. Dwell Time Tile

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

Sites Overview Chart

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

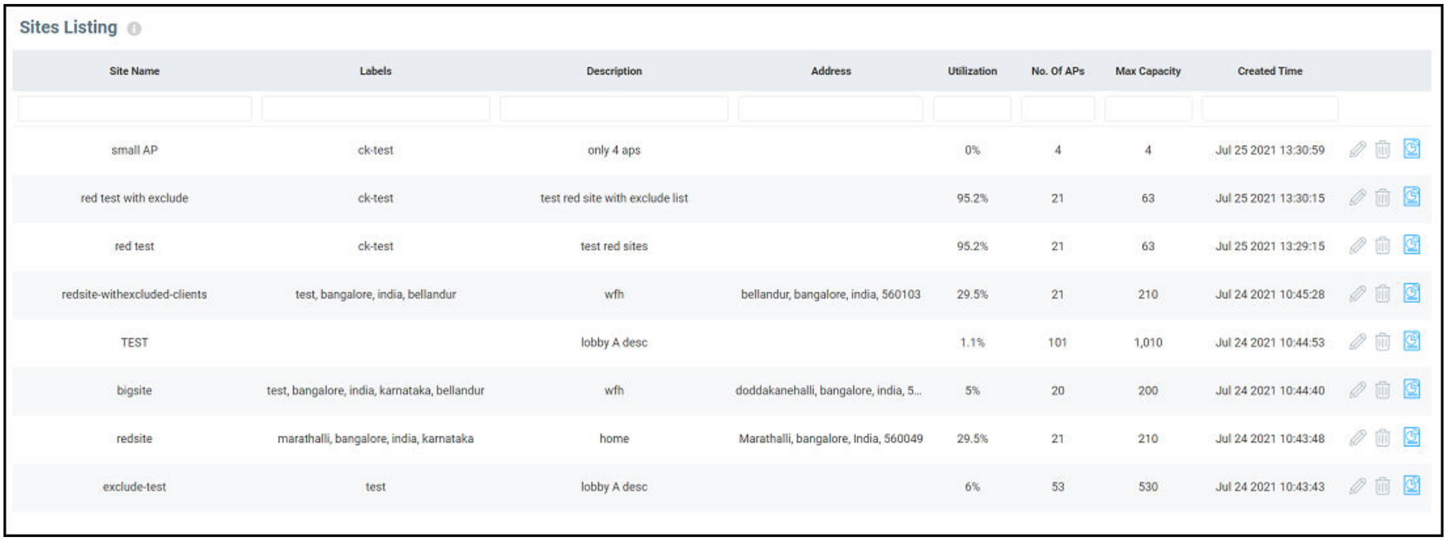
FIGURE 55 Sites Overview Chart



Sites Listing Table

The **Sites Listing** table displays information such as the site name, labels, description, city, country, AP count, and time of site creation. The properties of each site can be edited using the Edit icon(). Click the Report icon () to view the Site Report on page 85.

FIGURE 56 Sites Listing Table



Sites Listing

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

Site Report

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

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

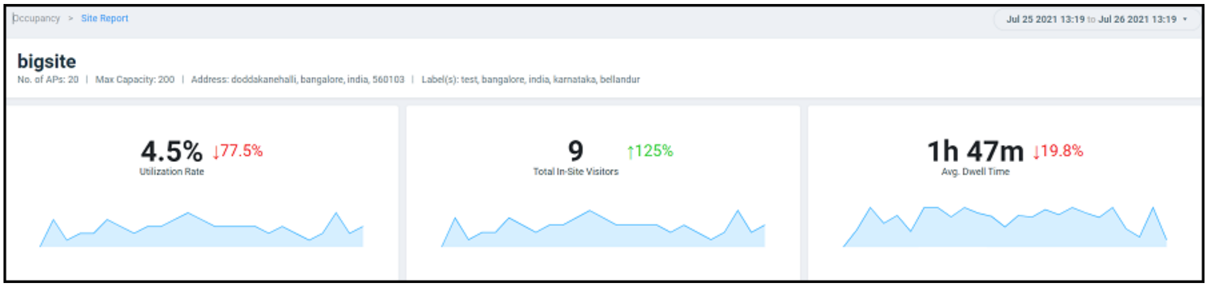
The **Site Report** consists of the following components:

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

- Dwell Time tile
- Clients table

Utilization Tile

FIGURE 57 Utilization, Total In-Site Visitors, and Avg. Dwell Time for a Selected Site



bigsite
No. of APs: 20 | Max Capacity: 200 | Address: doddakanehalli, bangalore, india, 560103 | Label(s): test, bangalore, india, karnataka, bellandur

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

Total In-Site Visitors Tile

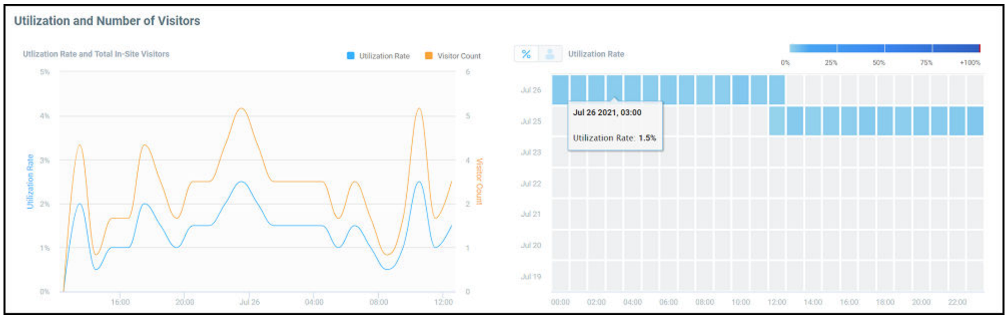
The **Total In-Site Visitors** tile displays the number of visitors visiting the selected site and the increase or decrease in the number of in-site visitors from the previous time. An increase in in-site visitors is displayed as a green number while a decrease is displayed as a red number. A "visitor"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

Avg. Dwell Time Tile

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

Utilization and Number of Users Tile

FIGURE 58 Utilization and Number of Users Tile

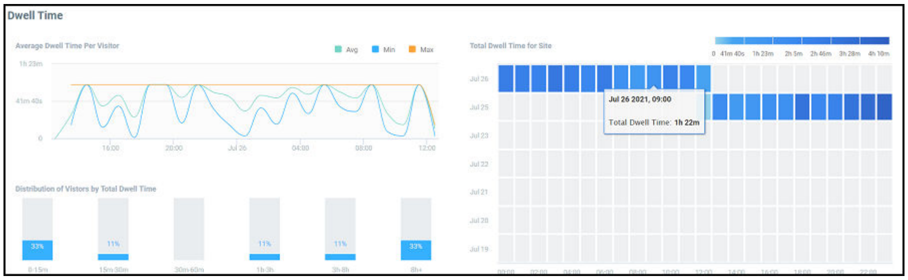


The **Utilization and Number of Users** tile displays the site utilization and number of users in a time series graph and a heat map. In the time series graph, the utilization rate is displayed as a percentage and the number of users at a time is also displayed. Pause the pointer over the graph for more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

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

Dwell Time Tile

FIGURE 59 Dwell Time Tile



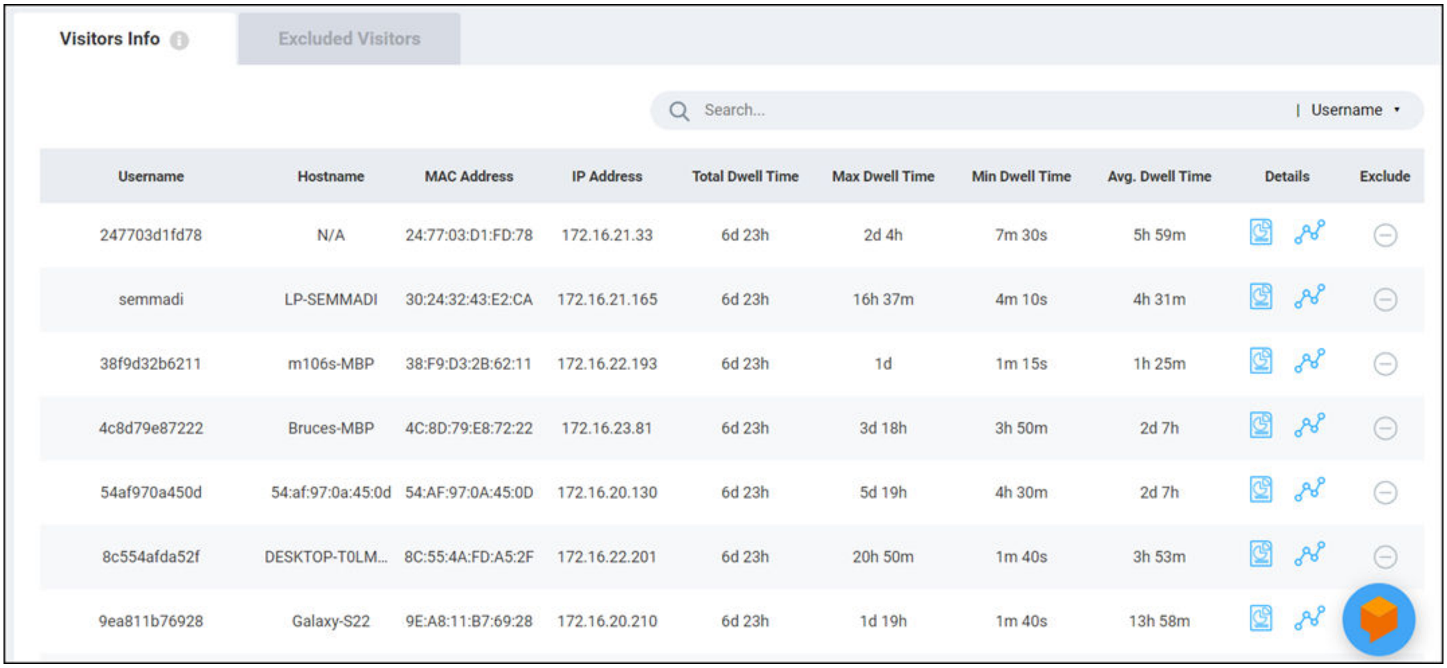
The **Dwell Time** tile displays the dwell time of a client or device for the selected time period as a time series graph,bar graph, and heat map. The time series graph displays the average, maximum, and minimum dwell time information. Pause the pointer over the graph for more information. You can choose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

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

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

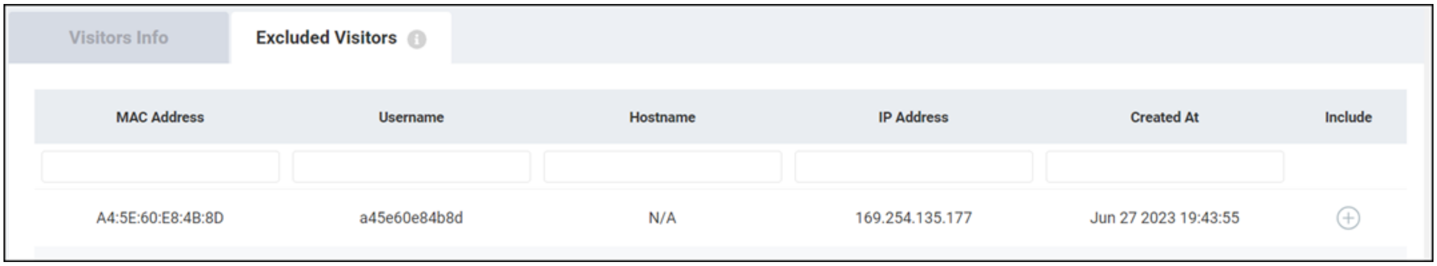
Clients Table

FIGURE 60 Clients Table - Visitors Info



Username	Hostname	MAC Address	IP Address	Total Dwell Time	Max Dwell Time	Min Dwell Time	Avg. Dwell Time	Details	Exclude
247703d1fd78	N/A	24:77:03:D1:FD:78	172.16.21.33	6d 23h	2d 4h	7m 30s	5h 59m		⊖
semmadi	LP-SEMMADI	30:24:32:43:E2:CA	172.16.21.165	6d 23h	16h 37m	4m 10s	4h 31m		⊖
38f9d32b6211	m106s-MBP	38:F9:D3:2B:62:11	172.16.22.193	6d 23h	1d	1m 15s	1h 25m		⊖
4c8d79e87222	Bruces-MBP	4C:8D:79:E8:72:22	172.16.23.81	6d 23h	3d 18h	3h 50m	2d 7h		⊖
54af970a450d	54:af:97:0a:45:0d	54:AF:97:0A:45:0D	172.16.20.130	6d 23h	5d 19h	4h 30m	2d 7h		⊖
8c554afda52f	DESKTOP-TOLM...	8C:55:4A:FD:A5:2F	172.16.22.201	6d 23h	20h 50m	1m 40s	3h 53m		⊖
9ea811b76928	Galaxy-S22	9E:A8:11:B7:69:28	172.16.20.210	6d 23h	1d 19h	1m 40s	13h 58m		

FIGURE 61 Clients Table - Excluded Visitors



MAC Address	Username	Hostname	IP Address	Created At	Include
A4:5E:60:E8:4B:8D	a45e60e84b8d	N/A	169.254.135.177	Jun 27 2023 19:43:55	⊕

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

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

AI-Driven Cloud Radio Resource Management

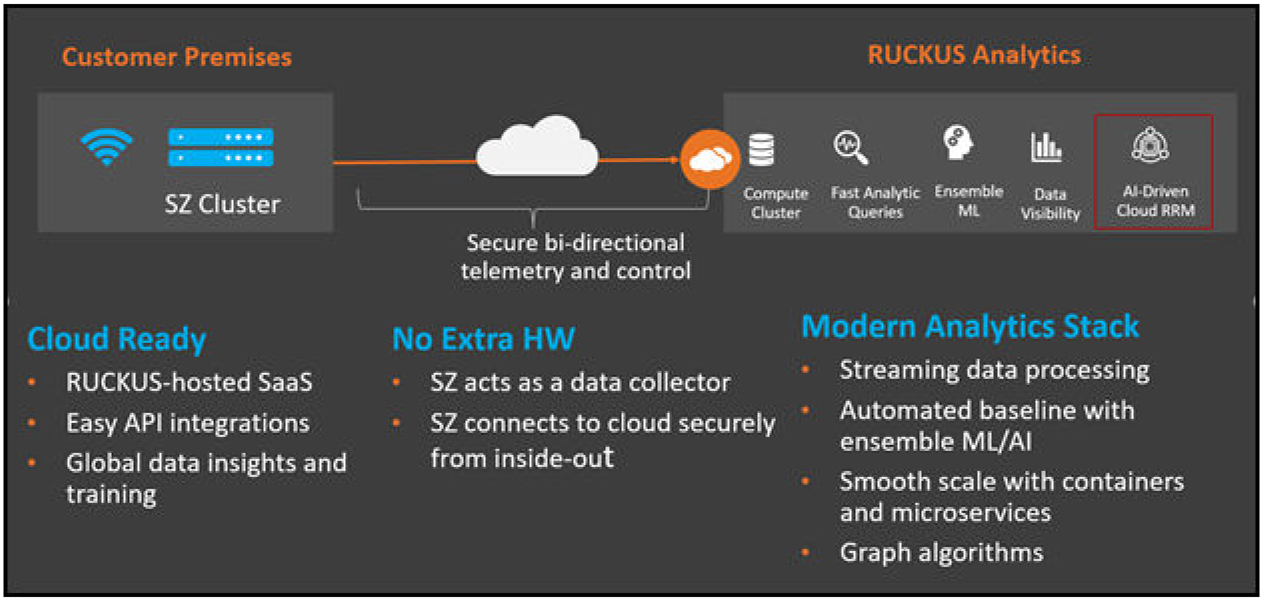
- AI-Driven Cloud RRM Overview....89

AI-Driven Cloud RRM Overview

AI-Driven Cloud Radio Resource Management (RRM) is a centralized algorithm that runs in the RUCKUS Analytics cloud and guarantees zero interfering links for the access points (APs) managed by SmartZone controllers, whenever theoretically achievable thus minimizing co-channel interference to the lowest level possible. This is accomplished by continuously gathering RF data from all the access points, holistically analyzing the RF environment and usage patterns, and jointly making optimal choices for channel re-use, channel bandwidth, and AP transmit power selection to maximize the network throughput. This new technology relies on sophisticated techniques of machine learning, artificial intelligence, graph algorithms, and cloud scale computation to jointly optimize channel, channel width, and AP transmit power. This method goes beyond adjusting the channel width because it optimizes across all combinations of channel, channel width, and AP transmit power to search for the optimal values across the network.

NOTE
When there are more than one node in a SZ cluster, AI Driven Cloud RRM needs SZ firmware 6.1.1 and later for it to work.

FIGURE 62 AI-Driven Cloud RRM in RUCKUS Analytics Cloud


Customer Premises
SZ Cluster
Secure bi-directional telemetry and control
RUCKUS Analytics
Compute Cluster
Fast Analytic Queries
Ensemble ML
Data Visibility
AI-Driven Cloud RRM
Cloud Ready
RUCKUS-hosted SaaS
Easy API integrations
Global data insights and training
No Extra HW
SZ acts as a data collector
SZ connects to cloud securely from inside-out
Modern Analytics Stack
Streaming data processing
Automated baseline with ensemble ML/AI
Smooth scale with containers and microservices
Graph algorithms

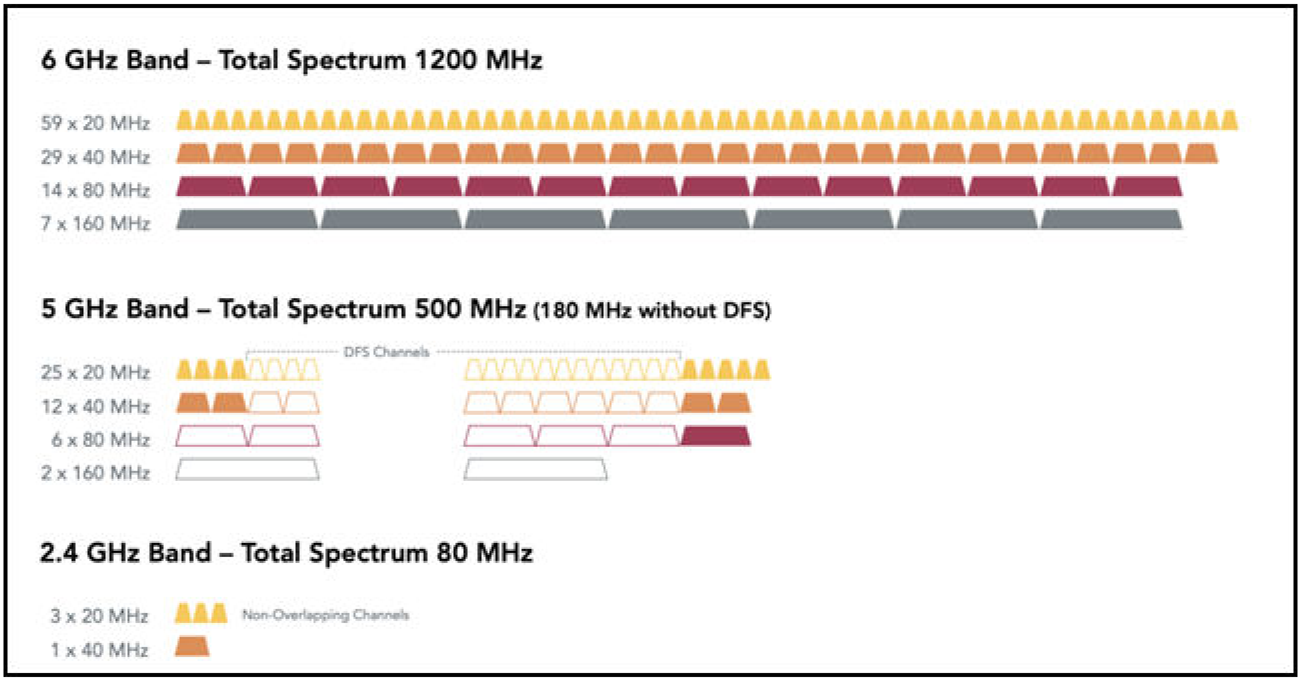
Benefits of AI-Driven Cloud RRM for an End User

With the introduction of AI-Driven Cloud RRM, customer Wi-Fi client devices can expect to operate in interference-free RF conditions, when possible, and experience higher throughput and higher reliability with fewer retries and errors. This results in higher user satisfaction when connecting wirelessly to the network. Maximizing the channel bandwidth allocation in the interference-free environment also ensures optimal performance to support high-throughput and low latency applications.

Advantages of AI-Driven Cloud RRM for a Network Administrator

While professional wireless engineers routinely optimize their network performance by selecting channel and power settings in addition to tuning other available configuration knobs, this task is getting more difficult with the advent of 6 GHz spectrum. A glance at the newly introduced spectrum and the available channel and channel width options make it tedious to manually optimize channel and channel width parameters required for a properly tuned Wi-Fi network. Not all enterprises have the wireless RF professionals available to tune these settings across the network. For a busy network administrator, sub-optimal conditions often go undiscovered until an end-user escalation.

FIGURE 63 Comparitive Channel Schema



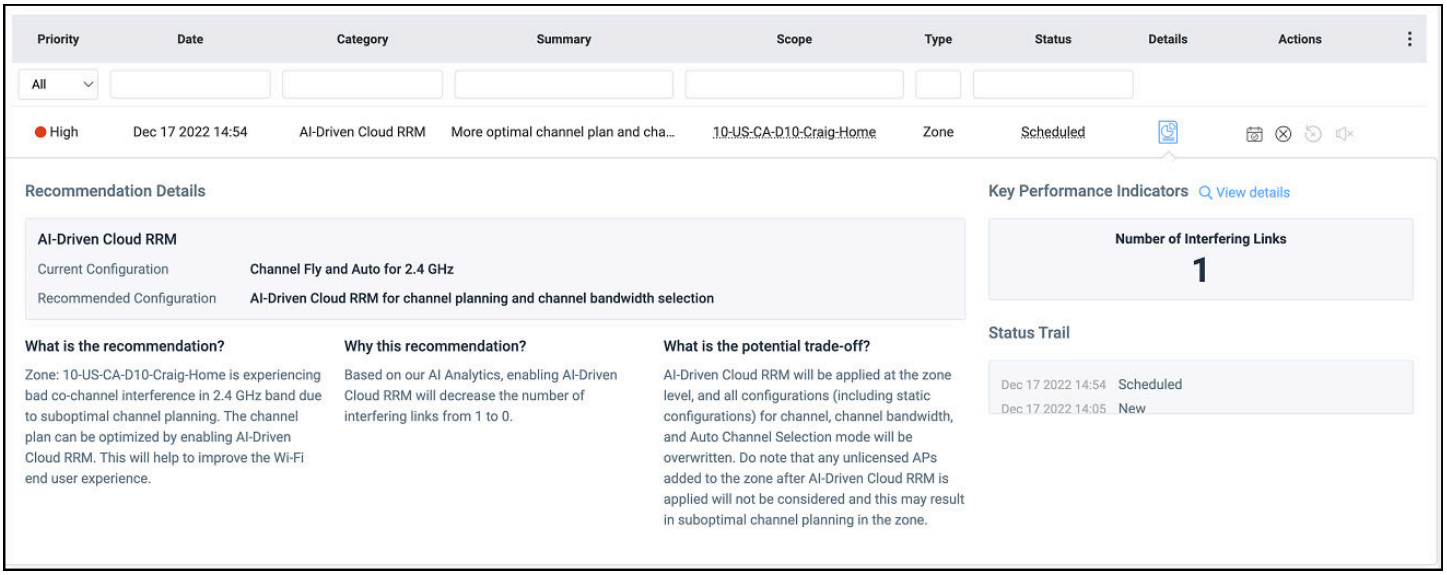
With AI-Driven Cloud RRM, network conditions are continuously monitored. When there is an opportunity to improve upon a sub-optimal configuration, the network administrator is presented with an optimized choice of channel and channel width in the form of an AI recommendation. With a single click, the network administrator can make changes to the network and apply the most optimal parameters to all the APs in a zone.

How AI-Driven Cloud RRM Works

AI-Driven Cloud RRM analyzes interference information received from every AP in the network, the user configuration hierarchy, access point capability, historical data about access point radio activity, rogue access points, and traffic patterns to jointly optimize channel, channel width, and AP transmit power.

Like other AI recommendations, the AI-Driven Cloud RRM recommendations include information such as *priority*, *date*, *category*, *summary*, *scope*, *type*, *status*, *details*, and *actions*. Recommendation details highlight the current configuration and the number of interfering links discovered in a zone. Clicking the 🗎 (Recommendation Details) icon displays the explainable AI recommendation, where the network administrator can find more information: what is this recommendation, why is it being made, and what are some of the potential trade-offs. Available actions include Apply, Revert, and Mute.

FIGURE 64 AI-Driven Cloud RRM Recommendation



Priority	Date	Category	Summary	Scope	Type	Status	Details	Actions
All								
● High	Dec 17 2022 14:54	AI-Driven Cloud RRM	More optimal channel plan and cha...	10-US-CA-D10-Craig-Home	Zone	Scheduled		

Recommendation Details

AI-Driven Cloud RRM

Current Configuration	Channel Fly and Auto for 2.4 GHz
Recommended Configuration	AI-Driven Cloud RRM for channel planning and channel bandwidth selection

What is the recommendation?

Zone: 10-US-CA-D10-Craig-Home is experiencing bad co-channel interference in 2.4 GHz band due to suboptimal channel planning. The channel plan can be optimized by enabling AI-Driven Cloud RRM. This will help to improve the Wi-Fi end user experience.

Why this recommendation?

Based on our AI Analytics, enabling AI-Driven Cloud RRM will decrease the number of interfering links from 1 to 0.

What is the potential trade-off?

AI-Driven Cloud RRM will be applied at the zone level, and all configurations (including static configurations) for channel, channel bandwidth, and Auto Channel Selection mode will be overwritten. Do note that any unlicensed APs added to the zone after AI-Driven Cloud RRM is applied will not be considered and this may result in suboptimal channel planning in the zone.

Key Performance Indicators View details

Number of Interfering Links
1

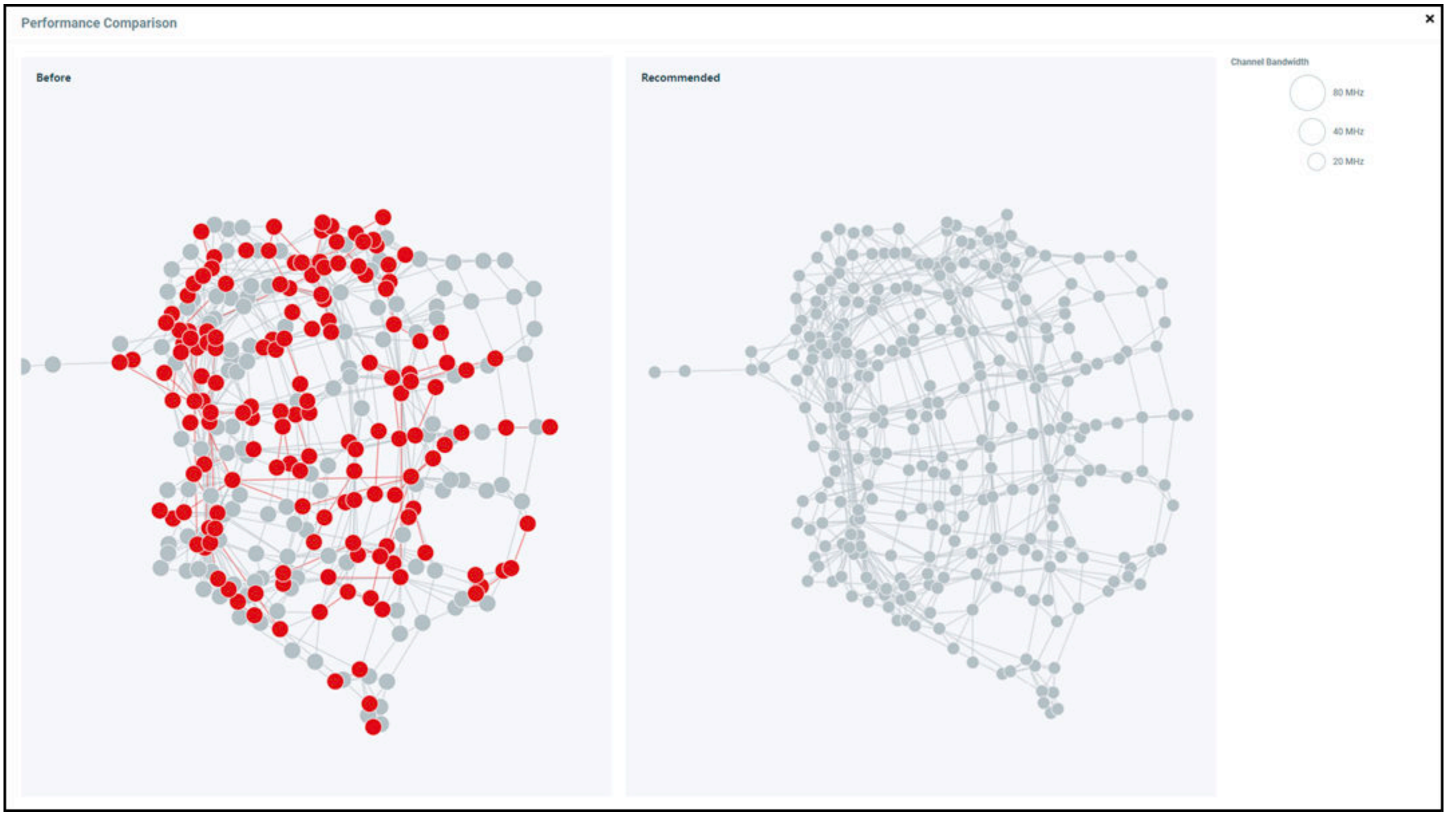
Status Trail

Dec 17 2022 14:54	Scheduled
Dec 17 2022 14:05	New

When a network administrator clicks the ✓ (Apply) icon available in the **Actions** column against each recommendation, a scheduling calender is displayed to select a date and time for the channel and channel width changes to be applied. This gives control to the network administrator to pick off-peak hours when the network is less busy to make the change. Changes are applied at the chosen time using SmartZone API calls to the controller from RUCKUS Analytics, and the scheduled time is stored in the system and used for future changes to channel and channel width if required.

The **View Details** option displays performance comparison between the current configuration including the number of interfering links discovered in a zone and the expected value (when the recommended AI-Driven Cloud RRM is applied) in a graph data structure. The below illustration displays 117 intefering links, that are reduced to zero after the RRM feature is applied.

FIGURE 65 Performance comaparison - Graph Data Structure



After the AI-Driven Cloud RRM recommendation is applied, it is pinned in the list of recommendations. If the network administrator reverts the recommendation, the original configuration is restored. Once the recommendation is applied, the KPI panel moves into the monitoring state for 24 hours where AI-Driven Cloud RRM starts gathering feedback about the change that was recently applied. The AI-Driven Cloud RRM is always active and any subsequent changes to the RF network, if required, are made at the selected time.

AI-Driven Cloud RRM Considerations

- When an AI-Driven Cloud RRM recommendation is applied, changes are made to RF parameters that overwrite previous configurations. If a ChannelFly configuration was previously selected for channel selection at the zone, the configuration moves under the control of AI-Driven Cloud RRM, and ChannelFly is disabled.
- The background scanning configuration and scanning interval is not changed, but continues to operate collecting data to discover the RF neighborhood that is used for seamless roaming, rogue AP detection, and AI-Driven Cloud RRM algorithms.
- AI-Driven Cloud RRM will overwrite existing static manual configurations except *ApRadioDeploy* and *ChannelRange*. If a static manual configuration is detected, RUCKUS Analytics flags this in the recommendation itself with corresponding warnings. This allows the network administrator to decide whether to override the static manual configuration by activating AI-Driven Cloud RRM.
- AI-Driven Cloud RRM does not co-exist with manual override or intervention after the AI-Driven Cloud RRM recommendation is applied. Network administrator must disable AI-Driven Cloud RRM completely to have manual override for a subset of APs in a zone.
- AI-Driven Cloud RRM enables rogue detection at the zone level. This is done to gather a complete RF picture of the environment before optimization decisions are made.
- AI-Driven Cloud RRM recommendations are triggered only for zones with 100 percent licensed APs. Any unlicensed APs added to the zone after AI-Driven Cloud RRM is applied are not considered, which may result in sub-optimal channel planning in the zone.

- In this release, AI-Driven Cloud RRM does not operate when zones have mesh configuration enabled.
- AI-Driven Cloud RRM requires SmartZone controller release 5.2.2 and later. All access points supported on this release are compatible.
- SmartZone controllers that are already onboarded to RUCKUS Analytics can immediately begin using AI-Driven Cloud RRM. For systems that are newly onboarded, AI-Driven Cloud RRM can be used immediately; however, the system improves in performance as historical information accumulates.
- AI-Driven Cloud RRM recommends channel and channel width configuration items at the zone level. Network Administrator is required to pick a date and time to apply the configuration. This is the local time for the zone for which recommendation is made. It is a best practice to include access points in the same time zone in a SZ zone because off-peak hours might differ across time zones.

NOTE
If the RUCKUS Analytics license is removed or expired, the last run AI-Driven Cloud RRM configuration will be used, and the channel plan will be set to static and not ChannelFly or Background Scanning.

NOTE
If a user reverts RUCKUS Analytics AI-Driven Cloud RRM recommendation, the original channel selection method is restored, and the recommendation will not resurface for 90 days.

AI-Driven Cloud RRM Behavior in 2.4 GHz

It is generally accepted and understood that 2.4 GHz is a crowded spectrum with only 3 non-overlapping channels. However, it is important because several clients still only support 2.4 GHz band. RF propagation characteristics unique to 2.4 GHz make it a useful choice due to its increased range.

Since 2.4 GHz band has only 3 non-overlapping channels - 1, 6, and 11 - it is likely that APs in this band will hear other APs and zero interfering links solution does not exist in dense AP deployments in 2.4 GHz. In this scenario, AI-Driven Cloud RRM will still guarantee lowest possible co-channel interference. It does not take action to turn off AP radios in 2.4 GHz band.

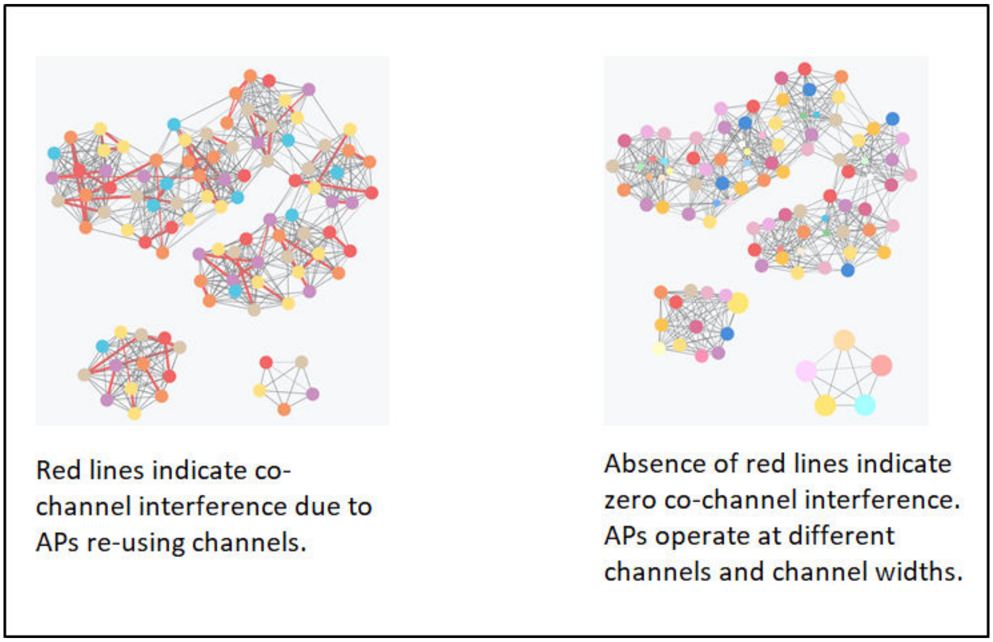
AI-Driven Cloud RRM with Dynamic Frequency Selection (DFS) Channels

AI-Driven Cloud RRM is aware of the constraints that DFS channels pose in 5 GHz spectrum usage. While the actual decision to operate in DFS channel is still done at an AP radio level after radar detection measures have been applied, AI-Driven Cloud RRM keeps track of radar activity on different DFS channels and intelligently crowd source this information across multiple APs within the same physical proximity. Based on this crowd sourced information, AI-Driven Cloud RRM may restrict the use of some of these DFS channels to avoid disruptions to end users. Of course, optimality in terms of zero interfering links and channel bandwidth selection will still be maintained.

AI-Driven Cloud RRM Operation at Zone and AP Level

The key insight fundamental to arriving at zero interfering links solution when possible is to jointly optimize channels and channel widths. Computationally, this is a NP-hard problem which can be solved using patented graph algorithms of RUCKUS.

FIGURE 66 Performance comaparison - Graph Data Structure



Red lines indicate co-channel interference due to APs re-using channels.

Absence of red lines indicate zero co-channel interference. APs operate at different channels and channel widths.

AI-Driven Cloud RRM Interoperability in a Mixed AP Deployment

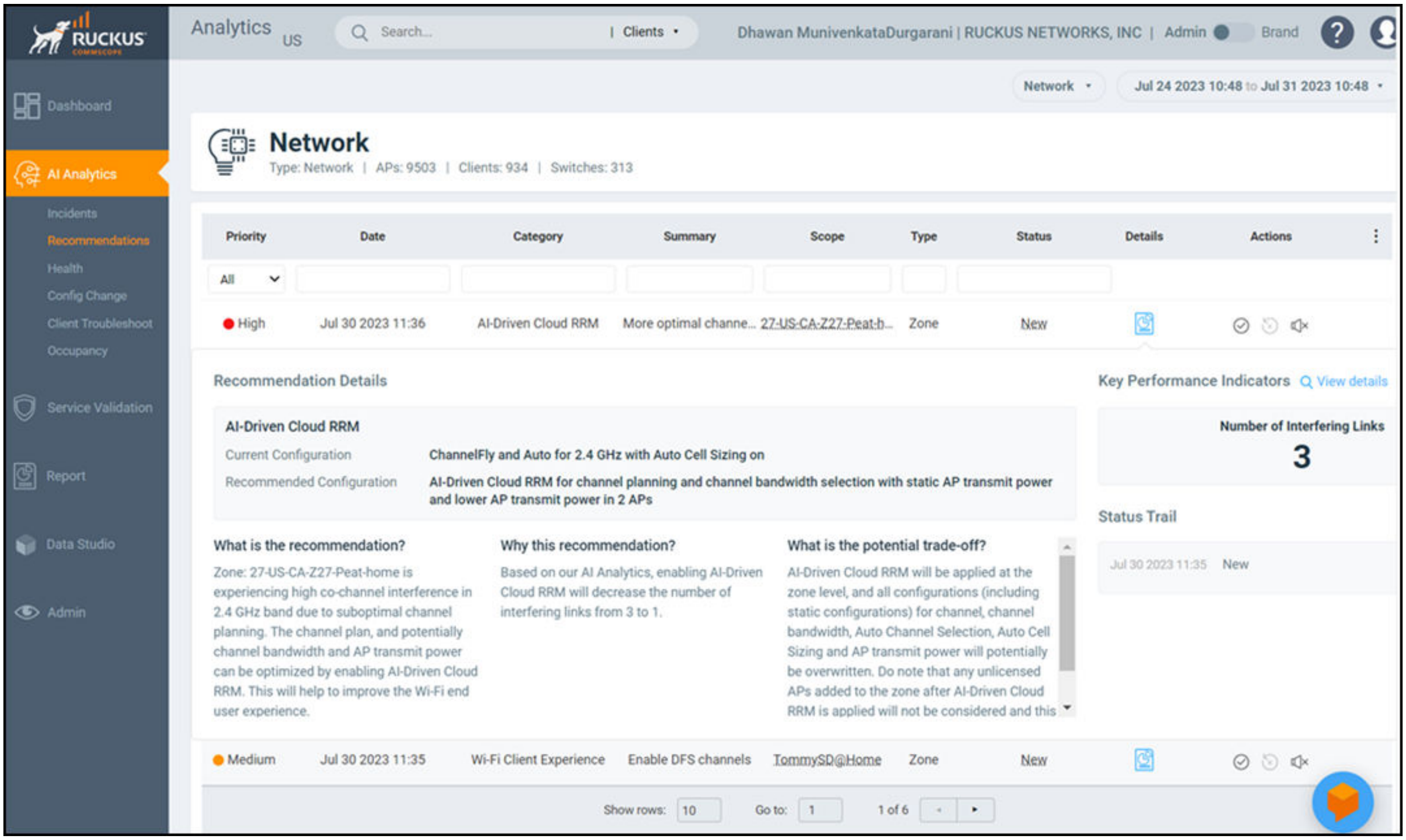
The AI-Driven Cloud RRM algorithm works on the information it receives from RUCKUS access points. Any third-party access point is treated as a rogue AP. These data points are fed into the computation to search for the best option for channel and channel width. These changes are recommended to the network administrator using the AI recommendation mechanism. There is no deauthentication action taken against rogue APs because the algorithms have built-in rogue AP avoidance. Even in presence of rogue access points or third-party access points, AI-Driven Cloud RRM delivers the most optimum solution for interfering AP links and co-channel interference possible.

AI-Driven Cloud RRM AP Transmit Power

In high-density deployment scenarios, an ideal channel plan with no interfering links may not be achievable. To address this, the AI-driven Cloud RRM automatically detects the residual co-channel interference and provides recommendations for further reducing the interference by reducing the AP transmit power, while at the same time, ensuring that no coverage holes will be created. This reduces the possibility of neighboring APs interfering with each other's signals, resulting in an enhanced Wi-Fi end-user experience.

The image below displays an example of Cloud RRM AP Transmit Power Recommendation to reduce the AP transmit power in two APs to reduce the interfering links from three to one.

FIGURE 67 CRRM Tx Power Recommendations Page



Network

Type: Network | APs: 9503 | Clients: 934 | Switches: 313

Priority	Date	Category	Summary	Scope	Type	Status	Details	Actions
● High	Jul 30 2023 11:36	AI-Driven Cloud RRM	More optimal channe...	27-US-CA-Z27-Peat-h...	Zone	New		
● Medium	Jul 30 2023 11:35	Wi-Fi Client Experience	Enable DFS channels	TommySD@Home	Zone	New		

Recommendation Details

AI-Driven Cloud RRM

Current Configuration	ChannelFly and Auto for 2.4 GHz with Auto Cell Sizing on
Recommended Configuration	AI-Driven Cloud RRM for channel planning and channel bandwidth selection with static AP transmit power and lower AP transmit power in 2 APs

What is the recommendation?

Zone: 27-US-CA-Z27-Peat-home is experiencing high co-channel interference in 2.4 GHz band due to suboptimal channel planning. The channel plan, and potentially channel bandwidth and AP transmit power can be optimized by enabling AI-Driven Cloud RRM. This will help to improve the Wi-Fi end user experience.

Why this recommendation?

Based on our AI Analytics, enabling AI-Driven Cloud RRM will decrease the number of interfering links from 3 to 1.

What is the potential trade-off?

AI-Driven Cloud RRM will be applied at the zone level, and all configurations (including static configurations) for channel, channel bandwidth, Auto Channel Selection, Auto Cell Sizing and AP transmit power will potentially be overwritten. Do note that any unlicensed APs added to the zone after AI-Driven Cloud RRM is applied will not be considered and this

Key Performance Indicators View details

Number of Interfering Links
3

Status Trail

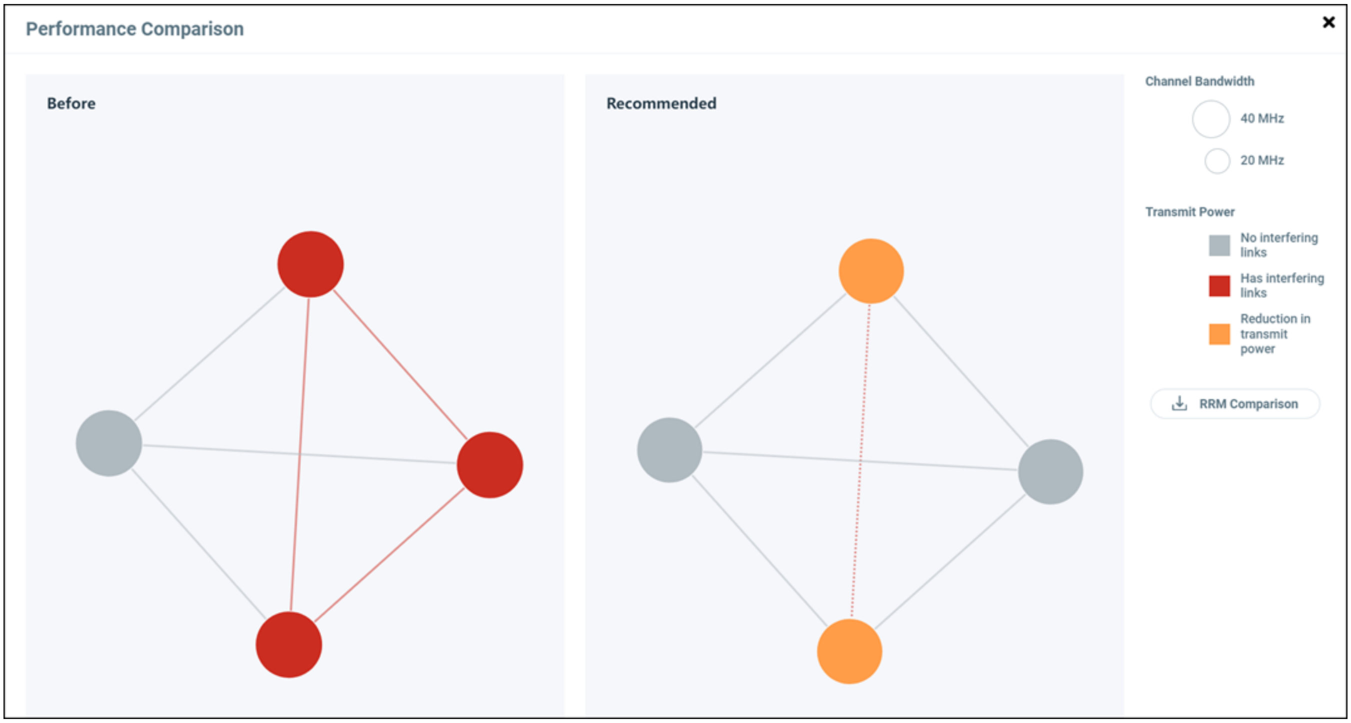
Jul 30 2023 11:35 New

Show rows: 10 Go to: 1 1 of 6

Complete the following steps to download the Cloud RRM recommendation report:

1. Click the **View details** icon to display the **Performance Comparison** page, which shows the image of interfering links before and after the recommendation.

FIGURE 68 CRRM Tx Power Comparison Page



2. Click **RRM Comparison** icon to download the Cloud RRM recommendation report in CSV format.

There are two types of recommendations that offer Tx power guidance to the user. The Wi-Fi client experience category of recommendations guides a user to adjust the Tx power setting for 2.4 and 5 GHz radios, mainly to encourage clients to move to a 5 GHz radio instead of a 2.4 GHz radio. This recommendation is also useful when APs have mesh networking enabled. While both recommendations may offer guidance about Tx Power, AI-Driven Cloud RRM recommends channel, channel width, and transmit power of radios to holistically reduce co-channel interference and maximize network throughput.

Network Health

- Testing Client Services.. 97
- Network Health Test Report.. 101

Testing Client Services

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

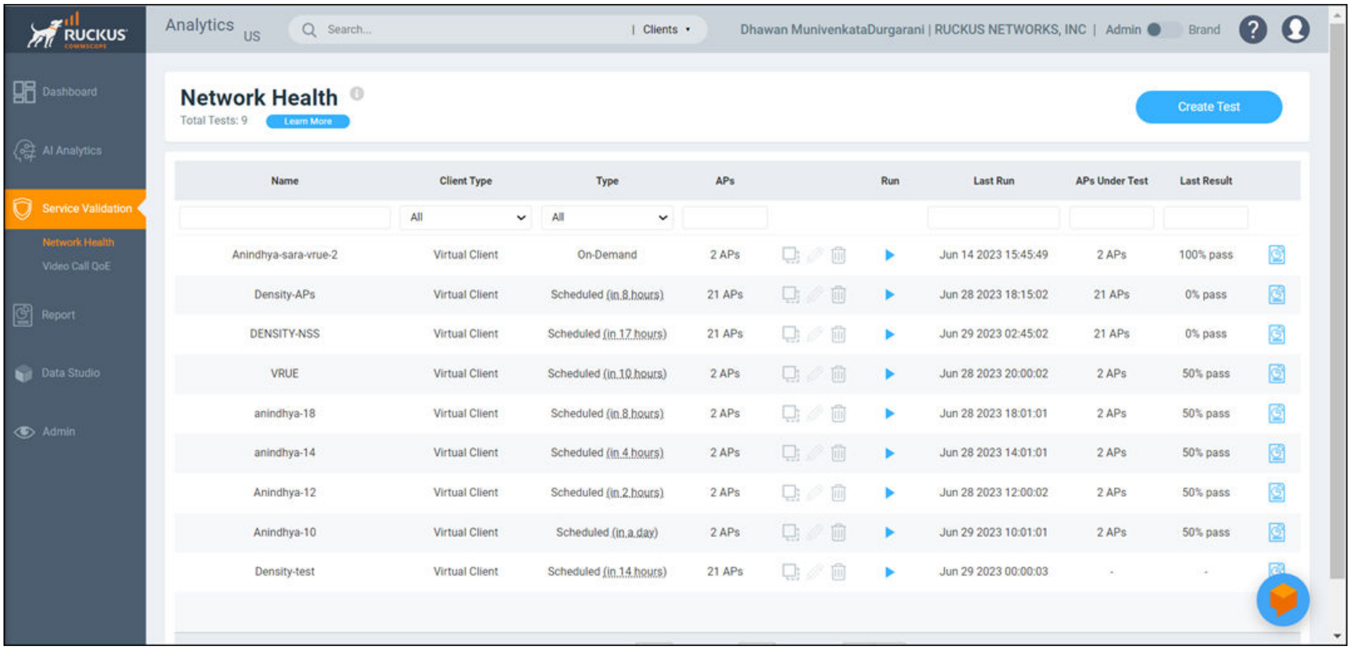
APs will emulate as virtual clients and perform the end-to-end connectivity tests (such as EAP, RADIUS, DHCP, DNS, ping, and traceroute) thereby connecting to a Wi-Fi network and the internet thereafter. It also performs speed tests to determine the quality of the connection. This feature therefore offers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

Follow these steps to create a test:

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

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

   FIGURE 69 Network Health Page



Network Health

Total Tests: 9

Name	Client Type	Type	APs	Run	Last Run	APs Under Test	Last Result
	All	All					
Anindhya-sara-vrue-2	Virtual Client	On-Demand	2 APs	▶	Jun 14 2023 15:45:49	2 APs	100% pass
Density-APs	Virtual Client	Scheduled (in 8 hours)	21 APs	▶	Jun 28 2023 18:15:02	21 APs	0% pass
DENSITY-NSS	Virtual Client	Scheduled (in 17 hours)	21 APs	▶	Jun 29 2023 02:45:02	21 APs	0% pass
VRUE	Virtual Client	Scheduled (in 10 hours)	2 APs	▶	Jun 28 2023 20:00:02	2 APs	50% pass
anindhya-18	Virtual Client	Scheduled (in 8 hours)	2 APs	▶	Jun 28 2023 18:01:01	2 APs	50% pass
anindhya-14	Virtual Client	Scheduled (in 4 hours)	2 APs	▶	Jun 28 2023 14:01:01	2 APs	50% pass
Anindhya-12	Virtual Client	Scheduled (in 2 hours)	2 APs	▶	Jun 28 2023 12:00:02	2 APs	50% pass
Anindhya-10	Virtual Client	Scheduled (in a day)	2 APs	▶	Jun 29 2023 10:01:01	2 APs	50% pass
Density-test	Virtual Client	Scheduled (in 14 hours)	21 APs	▶	Jun 29 2023 00:00:03	-	-

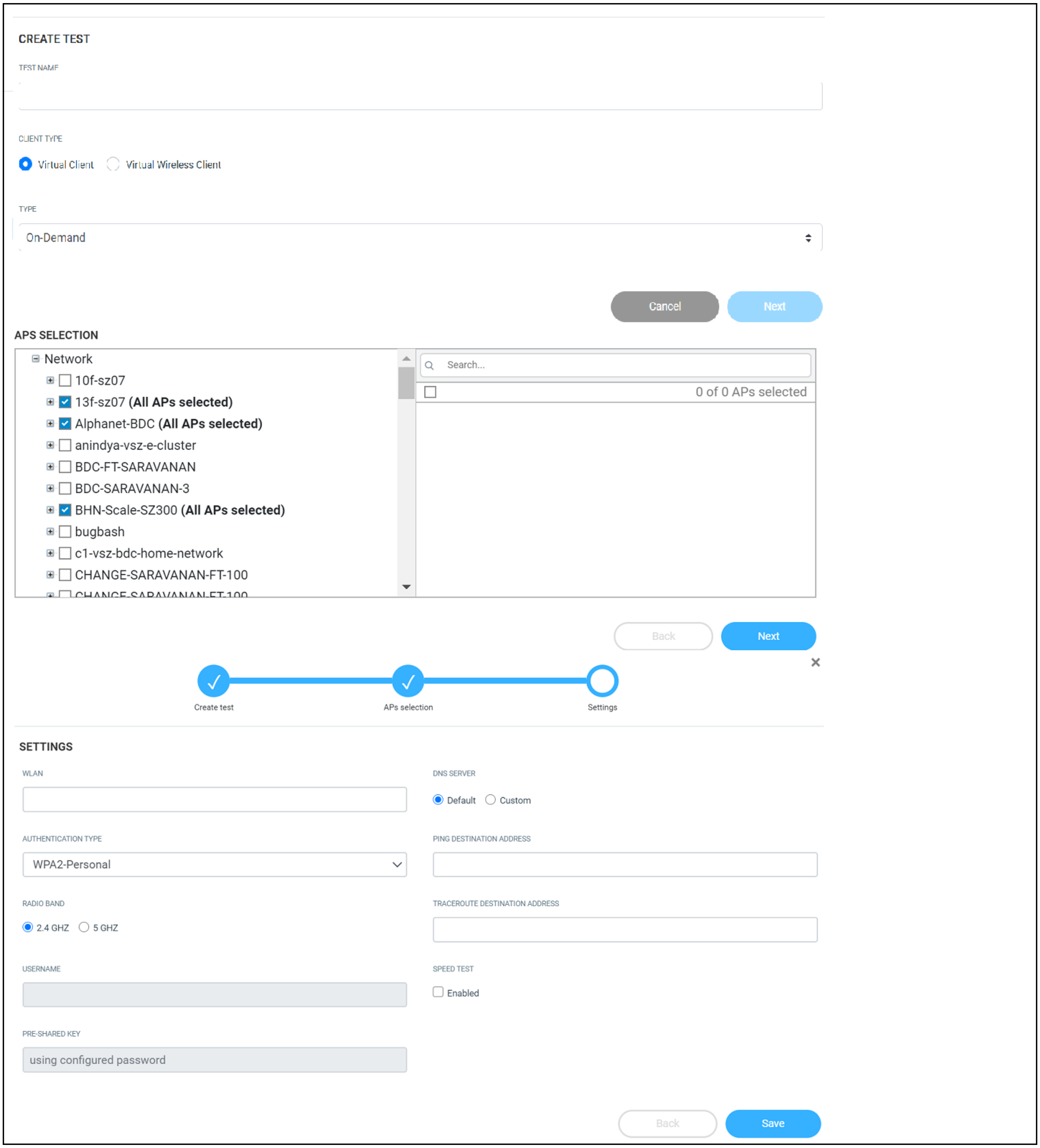
- Name: Displays the name of the test
- Type: Select from options such as On-Demand, Daily, Weekly, Monthly. Selecting Daily presents an option to choose the time of the day to run the test. Selecting Weekly presents options to select the day of the week and time for the test while selecting Monthly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

Click to view the test results.

2. Click **Create Test**.

   The **Create Test** page is displayed.

FIGURE 70 Creating a Test



CREATE TEST

TEST NAME

CLIENT TYPE

● Virtual Client ○ Virtual Wireless Client

TYPE

On-Demand

APS SELECTION

- ⊟ Network
  - ⊞ □ 10f-sz07
  - ⊞ ☑ 13f-sz07 **(All APs selected)**
  - ⊞ ☑ Alphanet-BDC **(All APs selected)**
  - ⊞ □ anindya-vsz-e-cluster
  - ⊞ □ BDC-FT-SARAVANAN
  - ⊞ □ BDC-SARAVANAN-3
  - ⊞ ☑ BHN-Scale-SZ300 **(All APs selected)**
  - ⊞ □ bugbash
  - ⊞ □ c1-vsz-bdc-home-network
  - ⊞ □ CHANGE-SARAVANAN-FT-100
  - ⊞ □ CHANGE-SARAVANAN-FT-100

Search...

□ 0 of 0 APs selected

SETTINGS

WLAN

DNS SERVER

● Default ○ Custom

AUTHENTICATION TYPE

WPA2-Personal

PING DESTINATION ADDRESS

RADIO BAND

● 2.4 GHZ ○ 5 GHZ

TRACEROUTE DESTINATION ADDRESS

USERNAME

SPEED TEST

□ Enabled

PRE-SHARED KEY

using configured password

3. Enter a name for the test
4. Select the Client Type - options include Virtual Client and Virtual Wireless Client.

   Service Validation now supports 2 options - **Virtual Client** and **Virtual Wireless Client**. For the Virtual Client option, the target AP to be tested will itself emulate as a Wi-Fi client and test the connection stages, without any actual RF transmission over the air. The benefit of this option is that Service Validation tests for the non-wireless portion of the network (e.g. DHCP, RADIUS, DNS, etc.) and can be simultaneously tested quickly over a large number of APs with no impact on existing Wi-Fi services.

   For the Virtual Wireless Client option, there will be actual RF transmissions over the air. For every target AP to be tested, a corresponding "station AP" is selected. The station AP is a neighboring AP with the best signal strength, and during the test, this station AP will behave as a station (i.e. a Wi-Fi client) and wirelessly connect to the target AP, just like a regular Wi-Fi client, for the test. The benefit of this option is that the Service Validation test will comprehensively cover both wireless and wired portions of the network. However, during this test, the station AP may need to switch its operating channel to be the same as the target AP. This change in channel may cause some disruptions to the end user Wi-Fi experience (e.g. during video calls). Thus, when Virtual Wireless Client is selected, the test procedure will be done one AP at a time to minimize disruption to the network, resulting in a longer test duration compared to the Virtual Client option.

   > **NOTE**
   > For Service Validation with virtual wireless client, only a neighbor on the same radio band can be used as the station AP. For example, if AP-1 has its 2.4 GHz radio turned off, it will not be used as the station AP for AP-2 even if AP-1 is the closest to AP-2 when the test is run on 2.4 GHz.

   After you choose one of the options, the Service Validation test cannot be modified. You can however create another test or clone this test to change the client type.
5. Click **Next**. The AP selection page is displayed.
6. Select the APs you want to include to the test from the network.
7. Click **Next**. The **Settings** page is displayed.

   Configure the following options:

   - WLAN: Select the WLAN
   - Authentication Type: after the WLAN is created, RUCKUS Analytics automatically selects the authentication method. However, you can still manually select the method as necessary.
   - Radio Band: Select the radio frequency that you want to test the APs at - options include 2.4 GHz, 5GHz, and 6 GHz.
   - 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
8. Click **Save** to save the test configuration.

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

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

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

Network Health Test Report

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

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

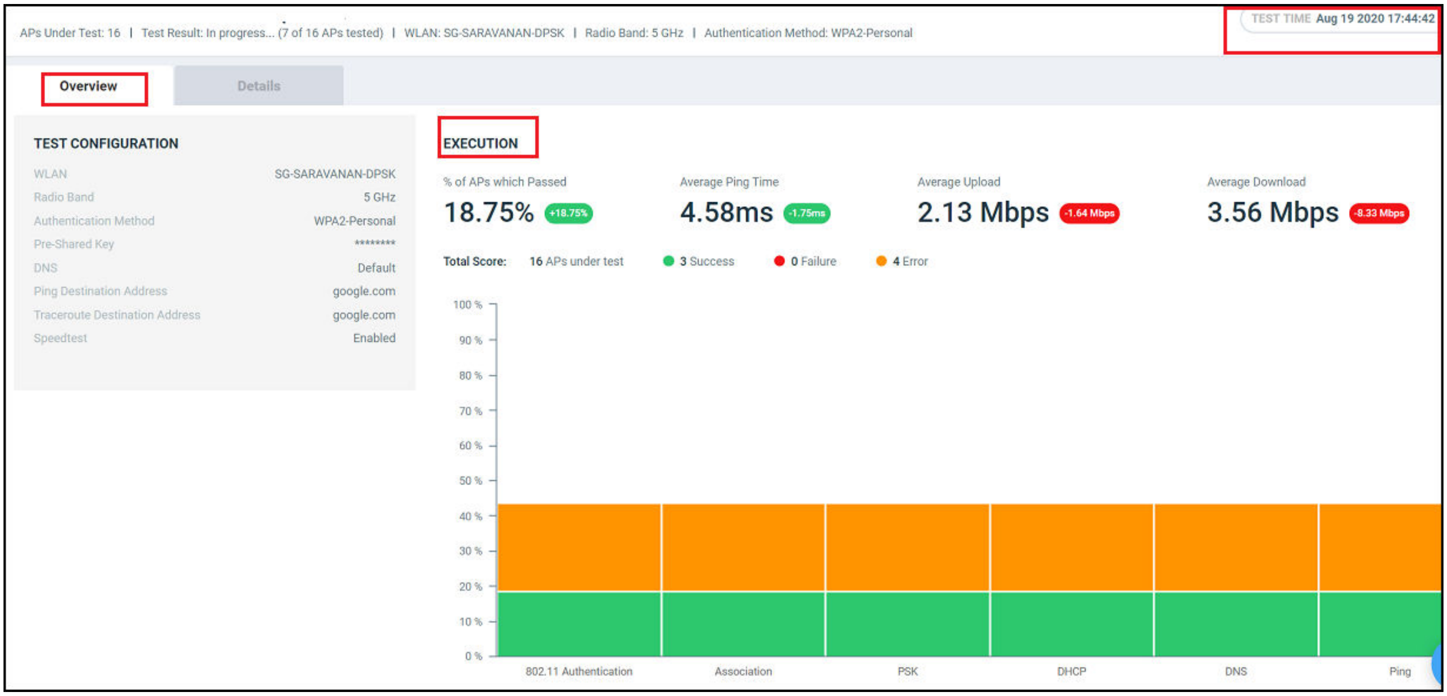
- Overview tab
- Details tab

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

Overview Tab

The **Overview tab** of the **Network Health** Report displays information about the test configuration that was used while creating the test. The Execution section displays information about the average ping time in ms, upload and download speeds in Mbps, and percentage of APs within that zone that passed the test criteria. In this report, only 3 out of the 16 APs passed the test, therefore the **% of APs which Passed** is displayed as 18.75%. Additionally, a small capsule is displayed next to these values which displays the values derived by comparing current values with the results from the previous test. If the values improved compared to previous test results, the capsule is displayed green and colored red if current values were lower than the previous one. For example, in this report, we can interpret that the average ping time has reduced by 1.75ms when compared to the previous result. Therefore, the capsule is colored green.

FIGURE 71 Network Health Report: Overview Tab



APs Under Test: 16 | Test Result: In progress... (7 of 16 APs tested) | WLAN: SG-SARAVANAN-DPSK | Radio Band: 5 GHz | Authentication Method: WPA2-Personal

TEST TIME Aug 19 2020 17:44:42

TEST CONFIGURATION

WLAN	SG-SARAVANAN-DPSK
Radio Band	5 GHz
Authentication Method	WPA2-Personal
Pre-Shared Key	********
DNS	Default
Ping Destination Address	google.com
Traceroute Destination Address	google.com
Speedtest	Enabled

EXECUTION

% of APs which Passed	Average Ping Time	Average Upload	Average Download
18.75% +18.75%	4.58ms -1.75ms	2.13 Mbps -1.64 Mbps	3.56 Mbps -8.33 Mbps

Total Score: 16 APs under test ● 3 Success ● 0 Failure ● 4 Error

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

- Success (green)

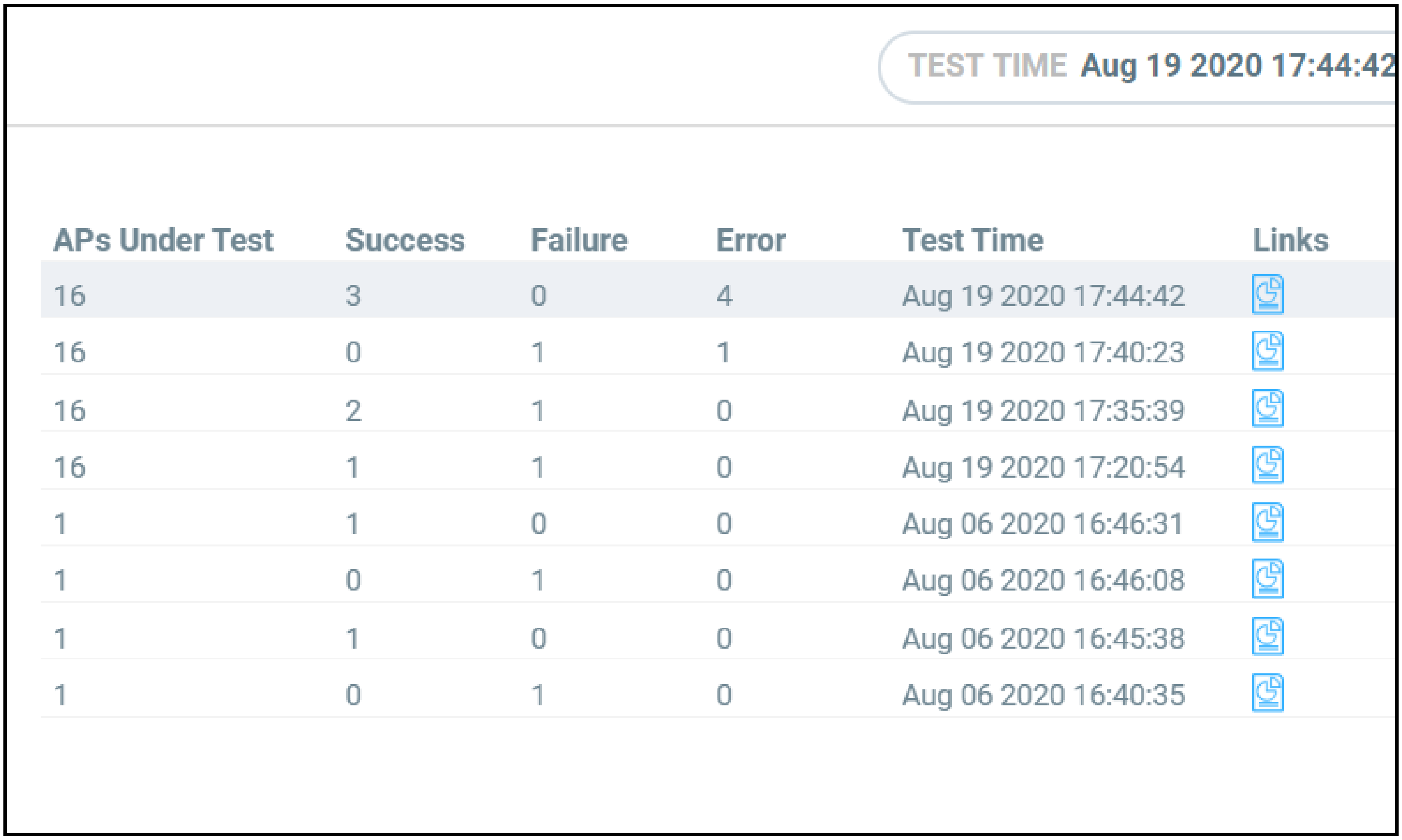
- Failure (red)
- Error (orange)

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 72 Test Time Log

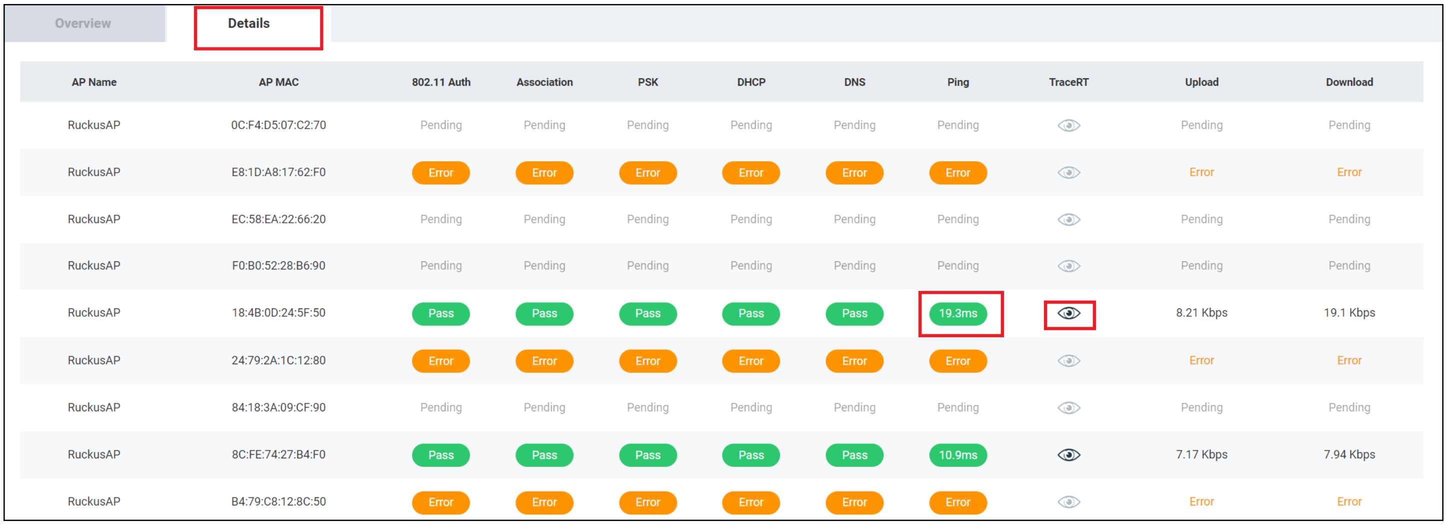


APs Under Test	Success	Failure	Error	Test Time	Links
16	3	0	4	Aug 19 2020 17:44:42	
16	0	1	1	Aug 19 2020 17:40:23	
16	2	1	0	Aug 19 2020 17:35:39	
16	1	1	0	Aug 19 2020 17:20:54	
1	1	0	0	Aug 06 2020 16:46:31	
1	0	1	0	Aug 06 2020 16:46:08	
1	1	0	0	Aug 06 2020 16:45:38	
1	0	1	0	Aug 06 2020 16:40:35	

Details Tab

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

FIGURE 73 Network Health 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 **Network Health** Report displays the following:

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

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

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

  Pause the pointer over the tarceroute icon (👁) for more information. It is enabled only when all authentication stages are passed successfully.
- Upload: Displays the upload speed of the network. **Timeout** is displayed if the speed test times out for some reason.
- Download: Displays the download speed of the network. **Timeout** is displayed if the speed test times out for some reason.

Testing Video Call Quality

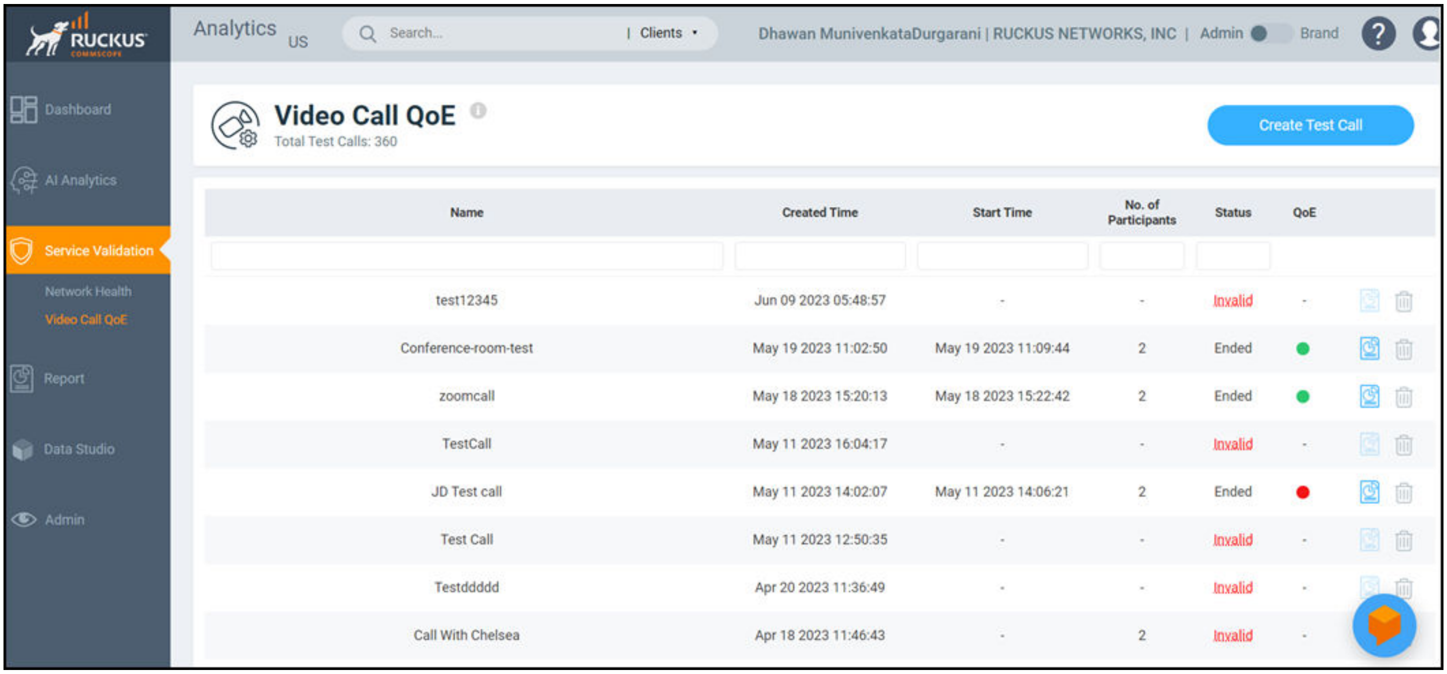
- Video Call QoE Workflow.. 105
- Creating a Test Call.. 108
- Video Call Test Report.. 110

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

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

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

FIGURE 74 Video Call QoE Page



Video Call QoE

Total Test Calls: 360

Name	Created Time	Start Time	No. of Participants	Status	QoE
test12345	Jun 09 2023 05:48:57	-	-	Invalid	-
Conference-room-test	May 19 2023 11:02:50	May 19 2023 11:09:44	2	Ended	●
zoomcall	May 18 2023 15:20:13	May 18 2023 15:22:42	2	Ended	●
TestCall	May 11 2023 16:04:17	-	-	Invalid	-
JD Test call	May 11 2023 14:02:07	May 11 2023 14:06:21	2	Ended	●
Test Call	May 11 2023 12:50:35	-	-	Invalid	-
Testddddd	Apr 20 2023 11:36:49	-	-	Invalid	-
Call With Chelsea	Apr 18 2023 11:46:43	-	2	Invalid	-

Video Call QoE Workflow

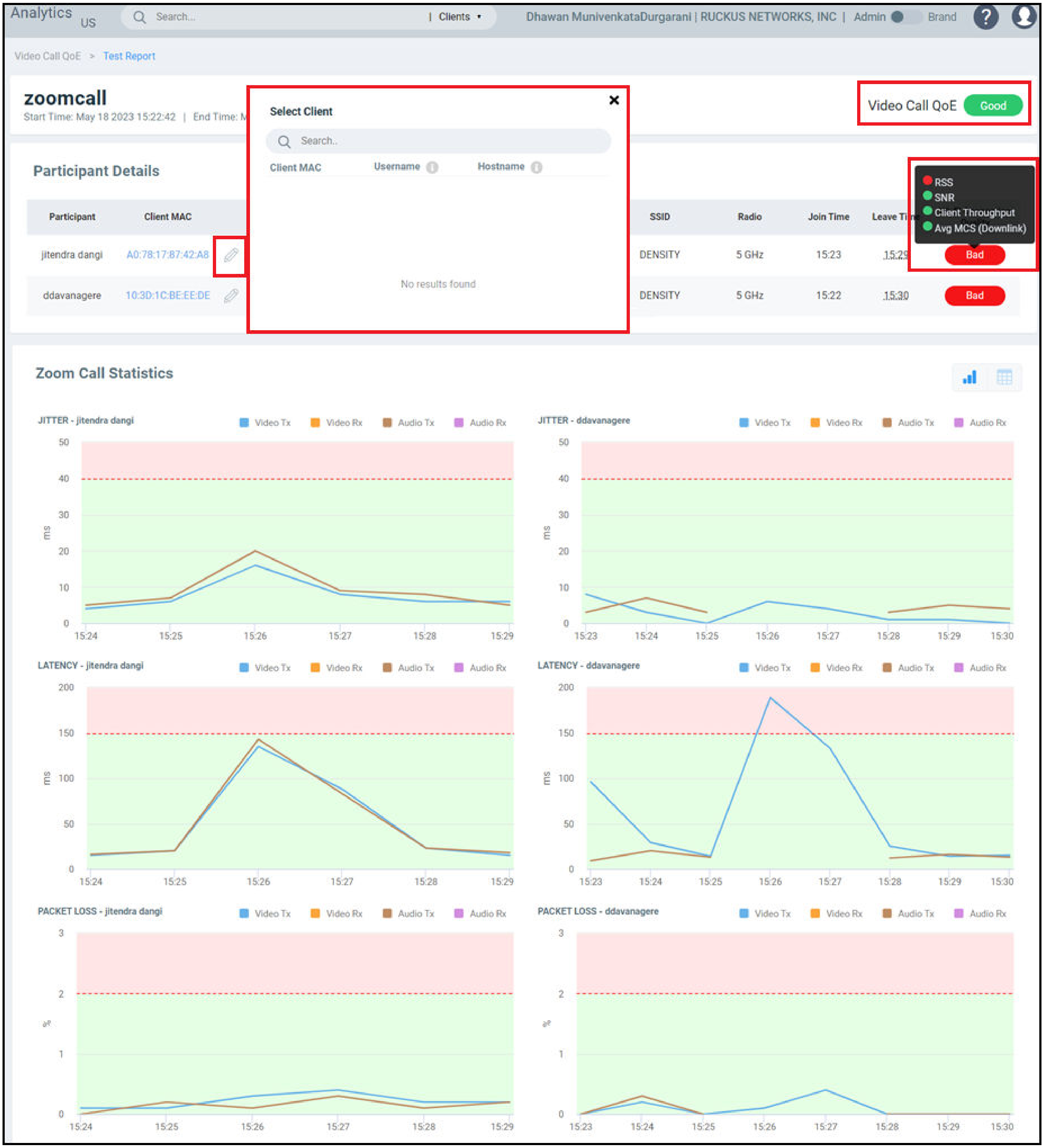
You can run a video call QoE test by following the steps listed in Creating a Test Call

After the test call is completed, a test call report is generated after approximately 8 to 10 minutes. For more information, refer to Video Call Test Report on page 110. You can click the 📄 Test Call Report icon to view the report.

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

Selecting the client MAC address displays the Client Troubleshoot Page on page 78 and clicking the AP MAC address displays the AP Details Report on page 168.

FIGURE 75 Selecting the Client MAC Address and Viewing Video Call QoE


Analytics US
Search...
Clients
Dhawan MunivenkataDurgarani | RUCKUS NETWORKS, INC | Admin
Brand
Video Call QoE > Test Report

zoomcall

Start Time: May 18 2023 15:22:42 | End Time: M

Video Call QoE Good

Participant Details

Participant	Client MAC		SSID	Radio	Join Time	Leave Ti	
jitendra dangi	A0:78:17:87:42:A8		DENSITY	5 GHz	15:23	15:29	Bad
ddavanagere	10:3D:1C:BE:EE:DE		DENSITY	5 GHz	15:22	15:30	Bad

Select Client

Search..

Client MAC	Username	Hostname

No results found

Zoom Call Statistics

Creating a Test Call

Complete the following steps to create a test call.

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

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

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

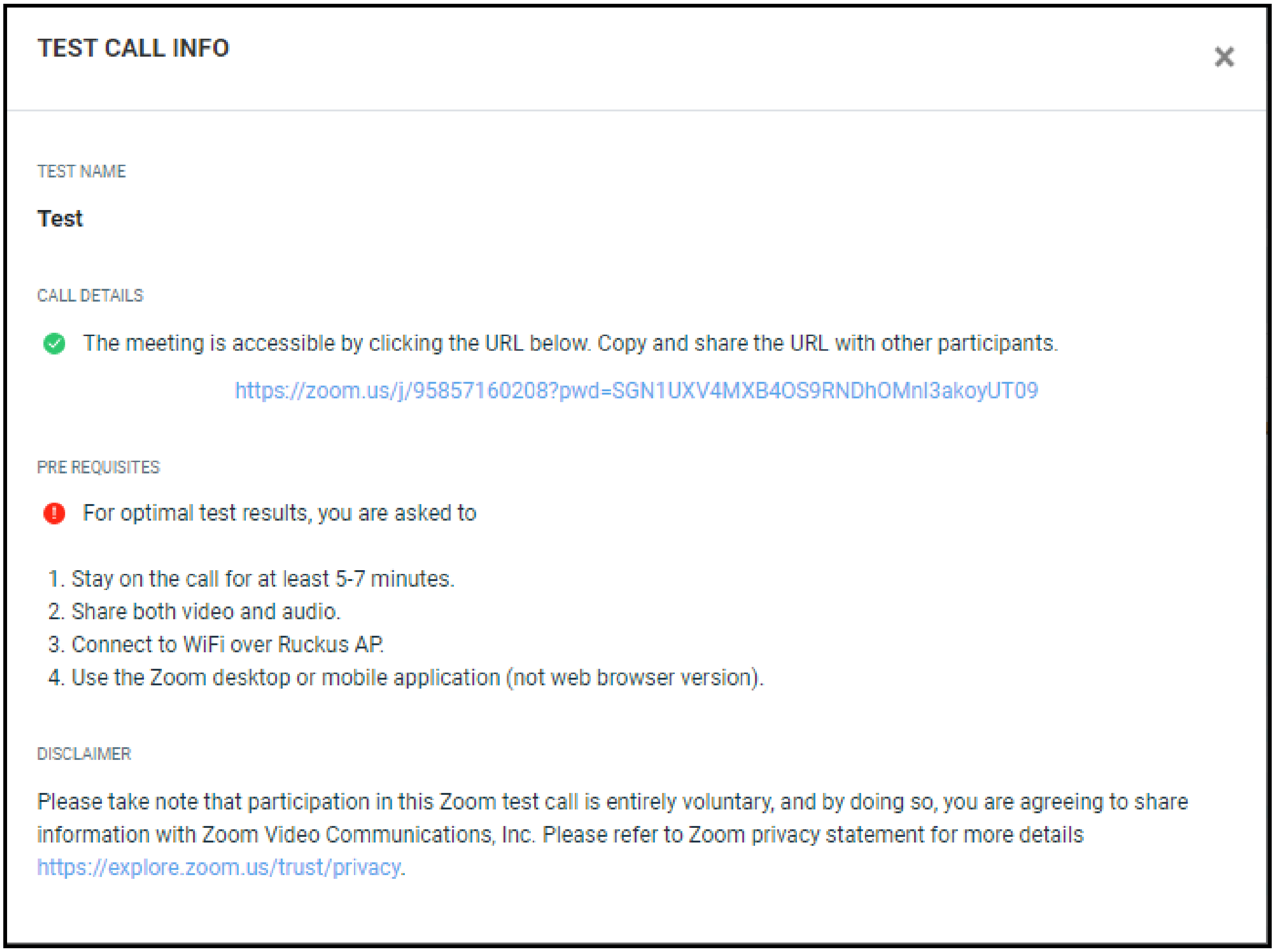
4. Click **Create**.

   A **Test Call Info** page is displayed containing information about the test name, a link to make the Zoom call, and prerequisites. Clicking the link takes you to the Zoom Meeting web user interface. You must use the Zoom desktop or mobile application (not the web browser version) for the test call. As with any Zoom meeting, you can edit the audio and video settings, chat with participants (only two in this case), record the meeting, use the reactions icons, share the screen, and so on.

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

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

FIGURE 76 Sample Test Call Info Page



TEST CALL INFO

×

TEST NAME

Test

CALL DETAILS

✓ The meeting is accessible by clicking the URL below. Copy and share the URL with other participants.

https://zoom.us/j/95857160208?pwd=SGN1UXV4MXB4OS9RNDhOMnl3akoyUT09

PRE REQUISITES

! For optimal test results, you are asked to

1. Stay on the call for at least 5-7 minutes.
2. Share both video and audio.
3. Connect to WiFi over Ruckus AP.
4. Use the Zoom desktop or mobile application (not web browser version).

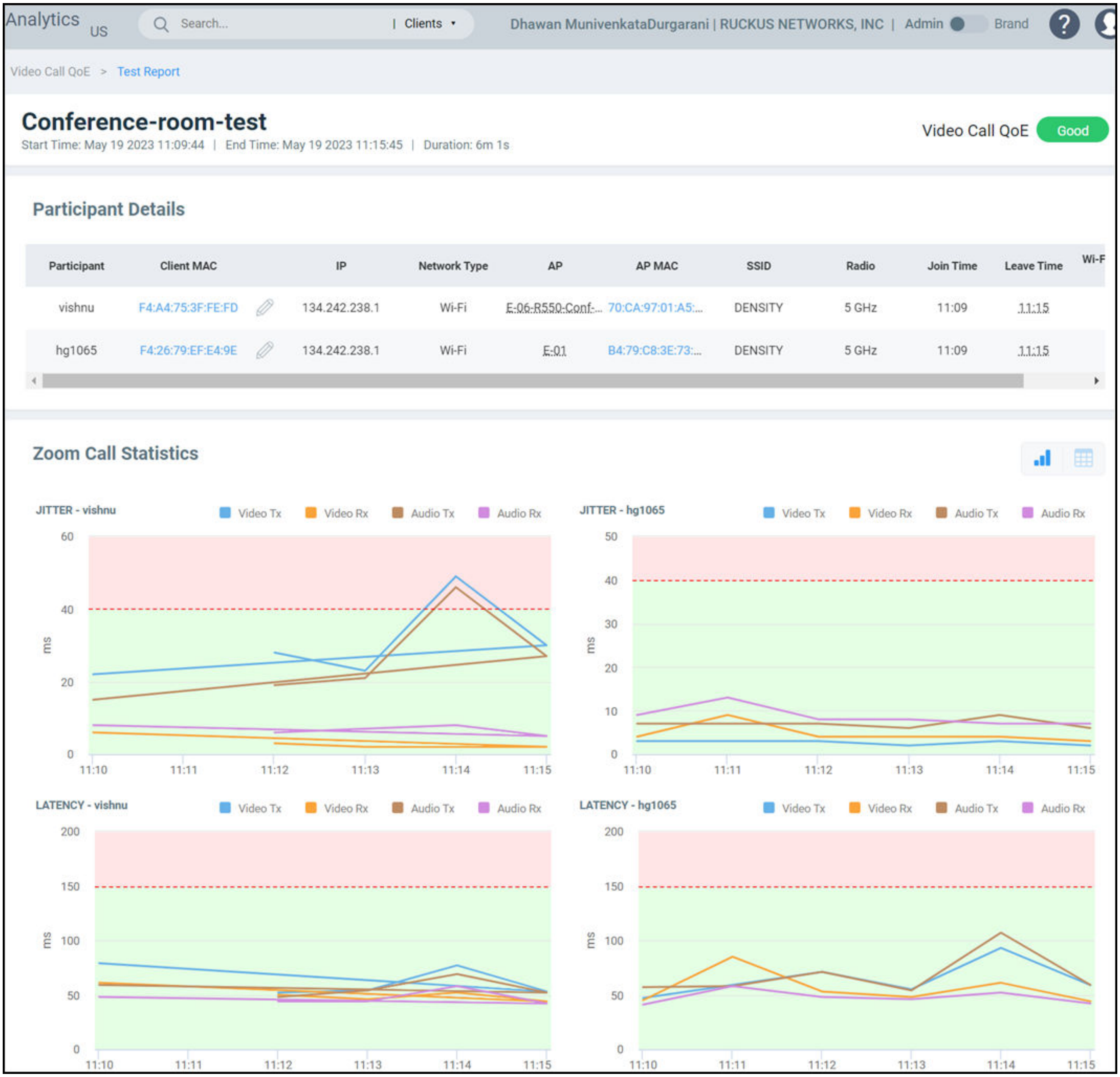
DISCLAIMER

Please take note that participation in this Zoom test call is entirely voluntary, and by doing so, you are agreeing to share information with Zoom Video Communications, Inc. Please refer to Zoom privacy statement for more details https://explore.zoom.us/trust/privacy.

Video Call Test Report

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

FIGURE 77 Video Call Report


Analytics US
Search...
Clients ▾
Dhawan MunivenkataDurgarani | RUCKUS NETWORKS, INC | Admin
Brand
?
Video Call QoE > Test Report

Conference-room-test

Start Time: May 19 2023 11:09:44 | End Time: May 19 2023 11:15:45 | Duration: 6m 1s

Video Call QoE Good

Participant Details

Participant	Client MAC	IP	Network Type	AP	AP MAC	SSID	Radio	Join Time	Leave Time	Wi-F
vishnu	F4:A4:75:3F:FE:FD	134.242.238.1	Wi-Fi	E-06-R550-Conf-...	70:CA:97:01:A5:...	DENSITY	5 GHz	11:09	11:15	
hg1065	F4:26:79:EF:E4:9E	134.242.238.1	Wi-Fi	E-01	B4:79:C8:3E:73:...	DENSITY	5 GHz	11:09	11:15	

Zoom Call Statistics

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

- Participants Details table
- Zoom Call Statistics tile

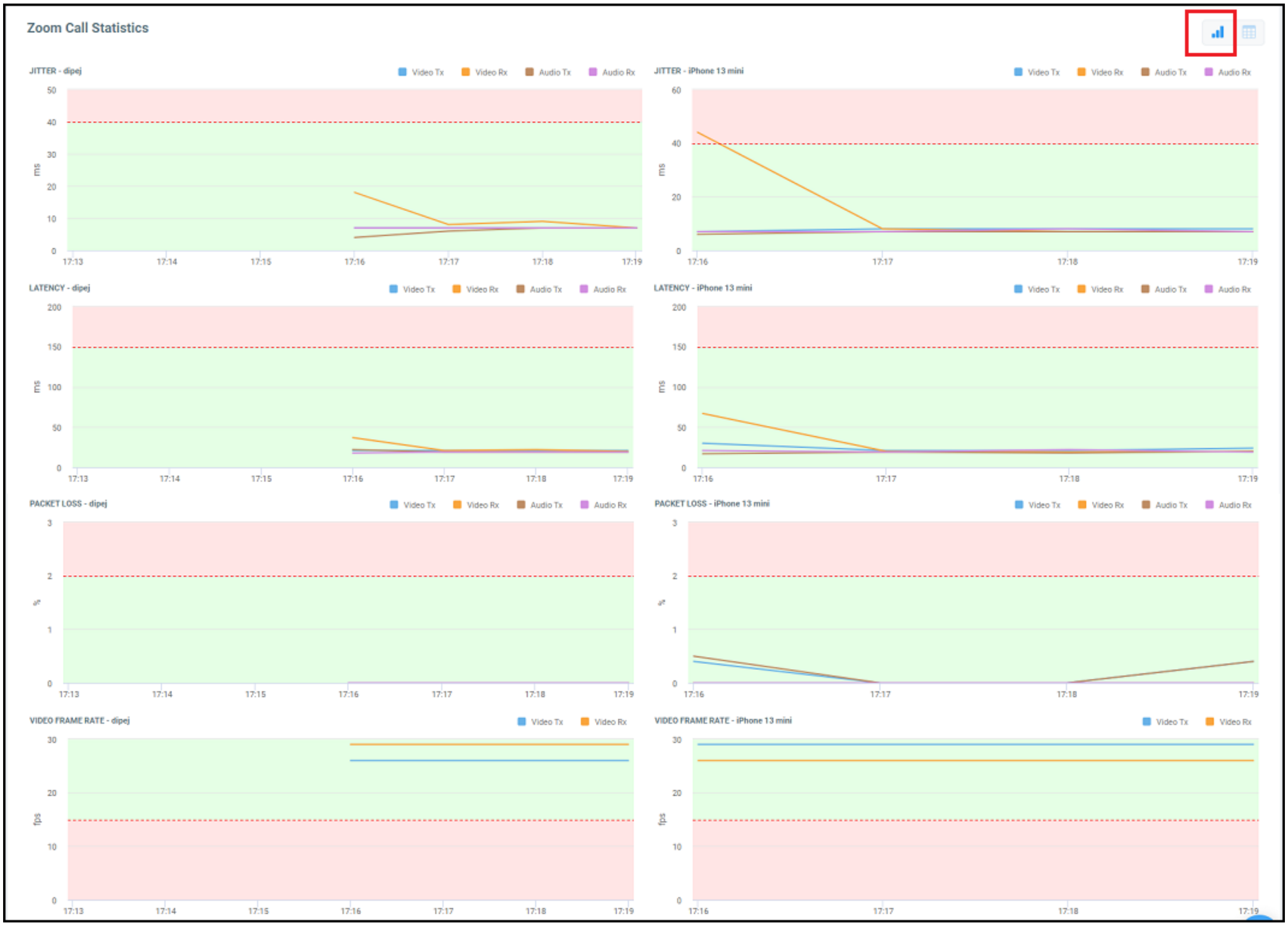
Participants Details Table

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

Zoom Call Statistics Tile

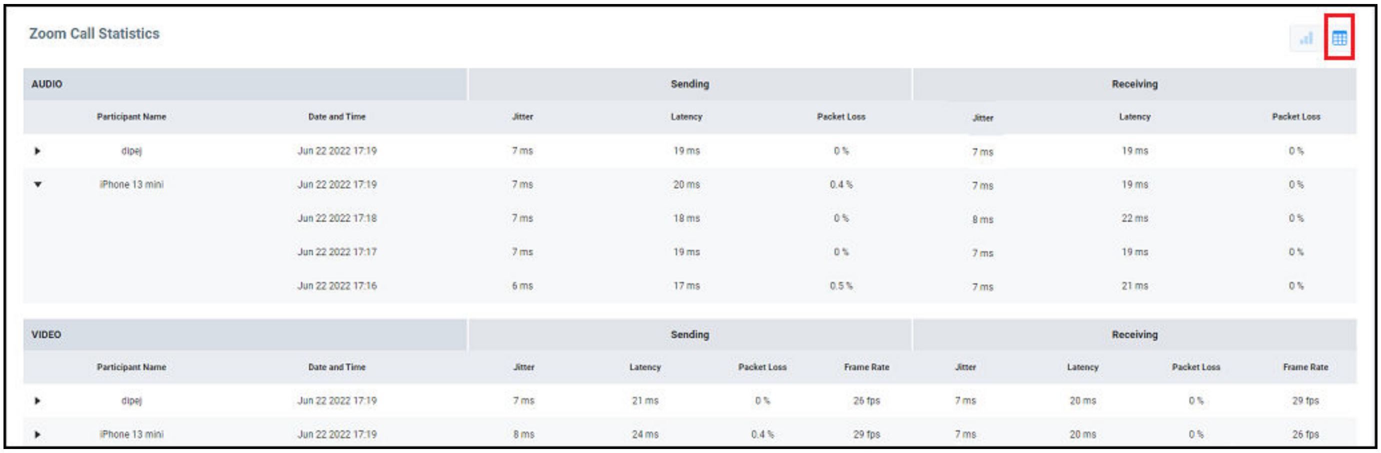
The **Zoom Call Statistics** tile provides time-series graph and table representation of jitters, latency, packet loss, and video frame rate experience in the call. Pausing the pointer over the time-series graph at a particular point displays the details of the respective quality metric at that time during the call. You can include or exclude the Tx and Rx values of both audio and video for each quality metric in the call statistics by selecting or deselecting the respective traffic type.

FIGURE 78 Zoom Call Statistics: Time-series Graph



- Jitter: Displays jitters produced during the call in milliseconds (ms) for both participants for the duration of the call. The participant with lower jitter values experienced better call quality.
- Latency: Displays latency (delay) produced during the call in milliseconds (ms) for both participants for the duration of the call. The participant with lower latency values experienced better call quality because there was minimum or no delay in audio and video transmission.
- Packet Loss: Displays the percentage of data packets lost during video and audio transmission for both participants. The participant with lower values experienced better call quality because there was minimum or no data loss during audio and video transmission.
- Video Frame Rate: Displays the number of video frames transmitted and received between both participants during the call. If the video call was successful for both participants, these values will be the same. The participant with lower frames per second experiences poor video quality.

FIGURE 79 Zoom Call Statistics: Table View



Zoom Call Statistics

AUDIO			Sending			Receiving		
	Participant Name	Date and Time	Jitter	Latency	Packet Loss	Jitter	Latency	Packet Loss
▸	dipej	Jun 22 2022 17:19	7 ms	19 ms	0 %	7 ms	19 ms	0 %
▾	iPhone 13 mini	Jun 22 2022 17:19	7 ms	20 ms	0.4 %	7 ms	19 ms	0 %
		Jun 22 2022 17:18	7 ms	18 ms	0 %	8 ms	22 ms	0 %
		Jun 22 2022 17:17	7 ms	19 ms	0 %	7 ms	19 ms	0 %
		Jun 22 2022 17:16	6 ms	17 ms	0.5 %	7 ms	21 ms	0 %

VIDEO			Sending				Receiving			
	Participant Name	Date and Time	Jitter	Latency	Packet Loss	Frame Rate	Jitter	Latency	Packet Loss	Frame Rate
▸	dipej	Jun 22 2022 17:19	7 ms	21 ms	0 %	26 fps	7 ms	20 ms	0 %	29 fps
▸	iPhone 13 mini	Jun 22 2022 17:19	8 ms	24 ms	0.4 %	29 fps	7 ms	20 ms	0 %	26 fps

The **Zoom Call Statistics** tile also provides table representation of jitters, latency, packet loss, and video frame rate experience in the call. Click the expand option next to the participant name to view the values of each quality metric at every minute of the call.

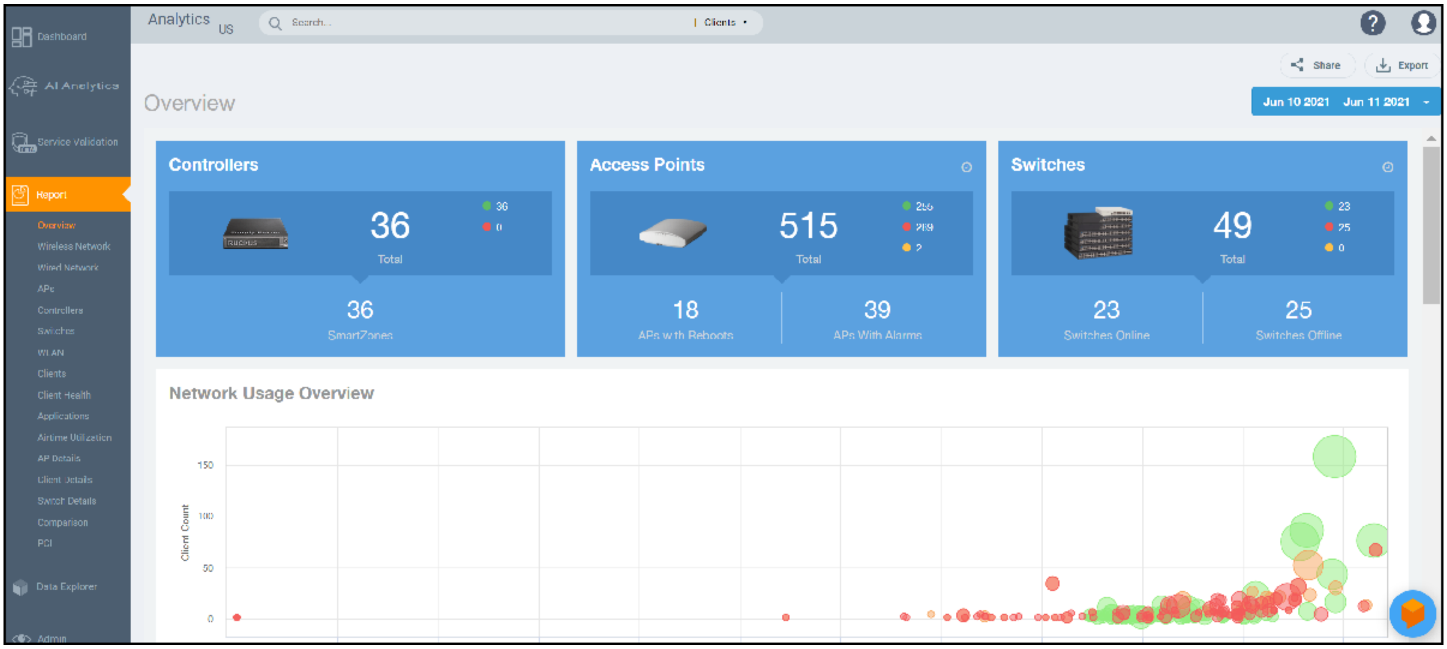
Report

- Using the Overview Dashboard: Content Panel 115
- Wireless Network Report 118
- Wired Network Report 124
- Inventory - APs Report 131
- Inventory - Controllers Report 139
- Inventory - Switches Report 142
- WLAN Report 147
- Clients Report 151
- Client Health Dashboard 157
- Applications Report 160
- Airtime Utilization Report 163
- AP Details Report 168
- Client Details Report 178
- Switch Details Report Dashboard 183
- Comparison Reports Dashboard 188
- PCI Profiles 192

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 80 Overview Dashboard : Top Portion

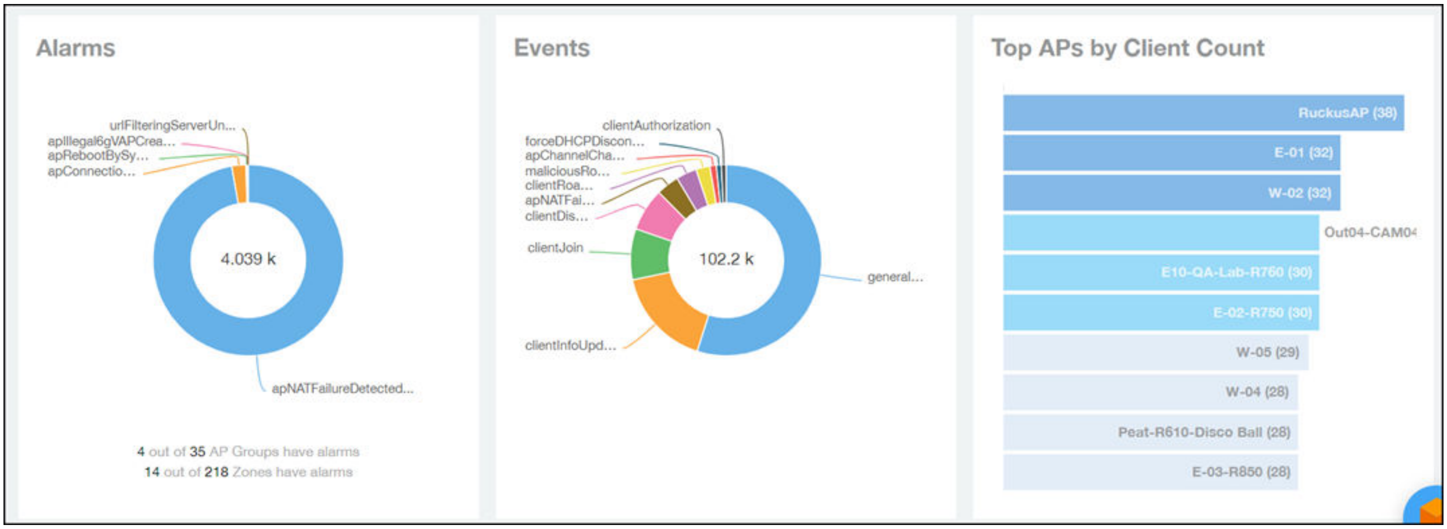


The top right corner of the Reports pages display options to share and export reports in PDF and CSV formats. You can also share them with recipients over e-mails on-demand or periodically by configuring a schedule (daily, weekly and monthly).

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).

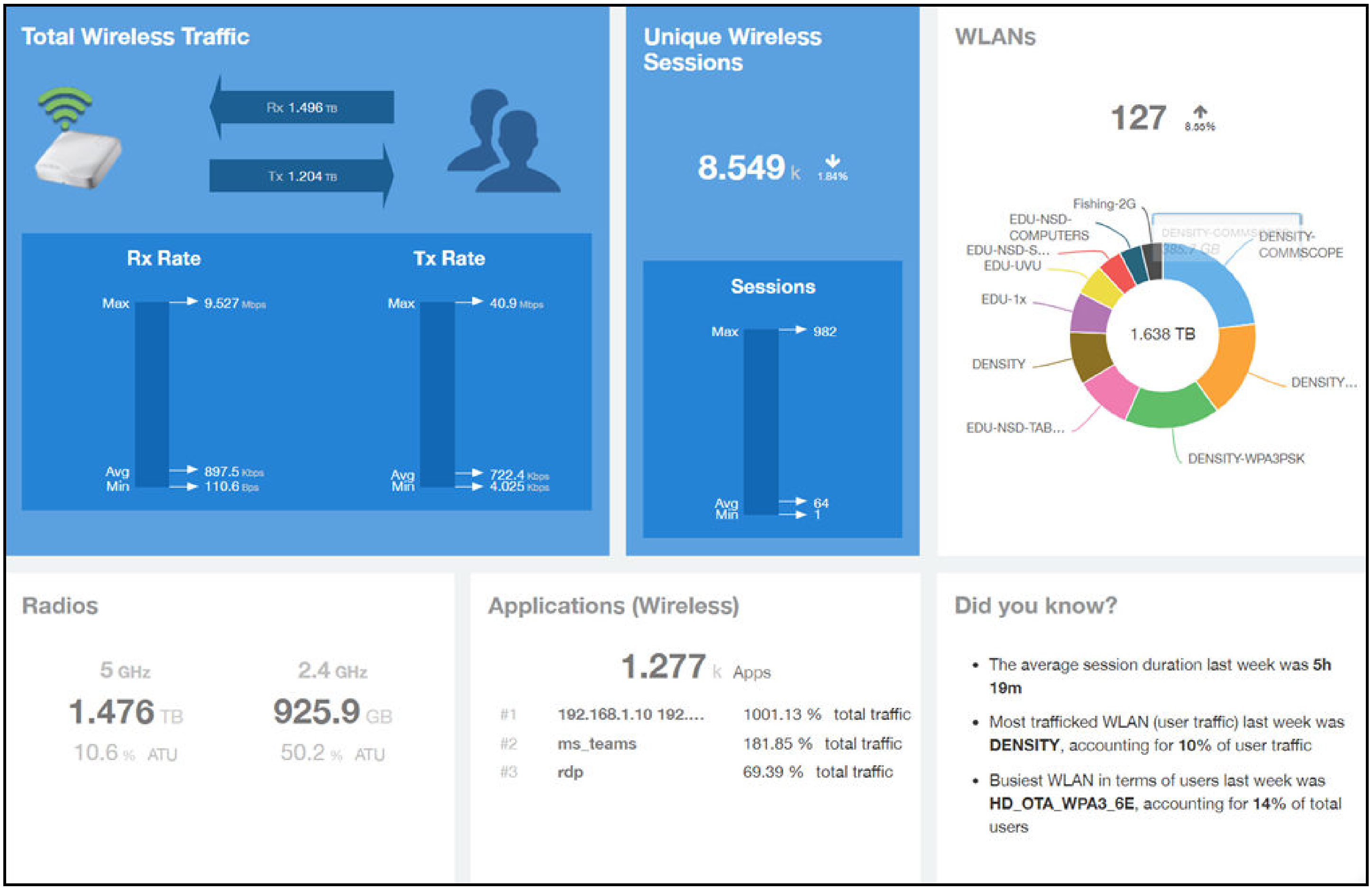
FIGURE 81 Overview Dashboard: Middle Portion



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.
- 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.
- 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 82 Overview Dashboard: Lower Portion



- The average session duration last week was **5h 19m**
- Most trafficked WLAN (user traffic) last week was **DENSITY**, accounting for **10%** of user traffic
- Busiest WLAN in terms of users last week was **HD_OTA_WPA3_6E**, accounting for **14%** of total users

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.
- 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**.

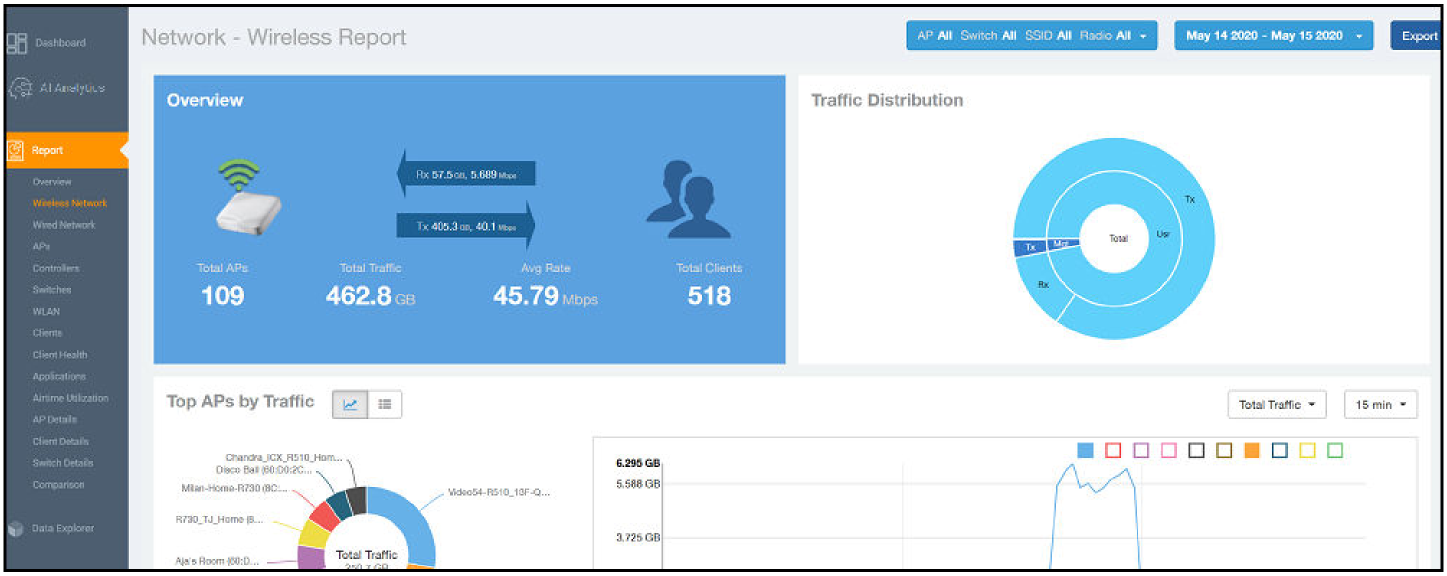
Wireless Network Report

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 83 Wireless Network Report (Upper Portion Only)



Network - Wireless Report

AP **All** Switch **All** SSID **All** Radio **All**

May 14 2020 - May 15 2020

Overview

Rx 57.5 GB, 5.689 Mbps

Tx 405.3 GB, 40.1 Mbps

Total APs 109

Total Traffic 462.8 GB

Avg Rate 45.79 Mbps

Total Clients 518

Total Traffic ▾

15 min ▾

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

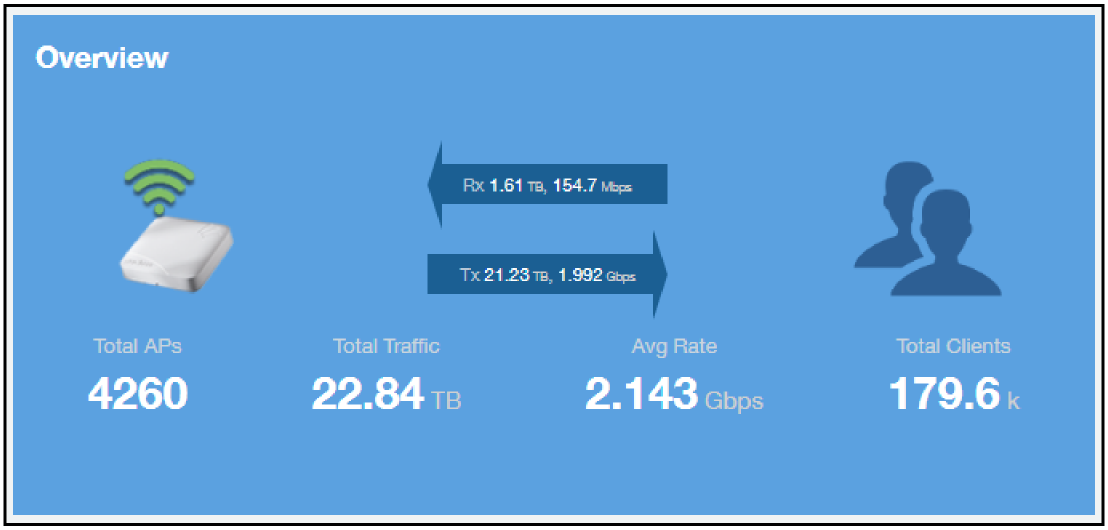
- Overview tile
- Traffic Distribution chart
- Top APs by Traffic tile
- Top APs by Client Count graph
- Traffic Trend graphs
- Traffic Over Time graph

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 84 Wireless Network Report: Overview Tile

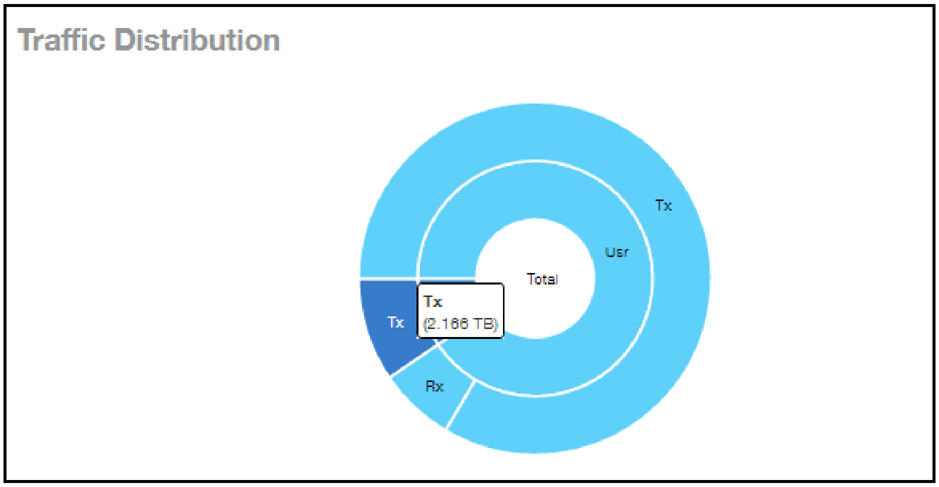


Traffic Distribution Tile

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 85 Wireless Network Report: Traffic Distribution Tile



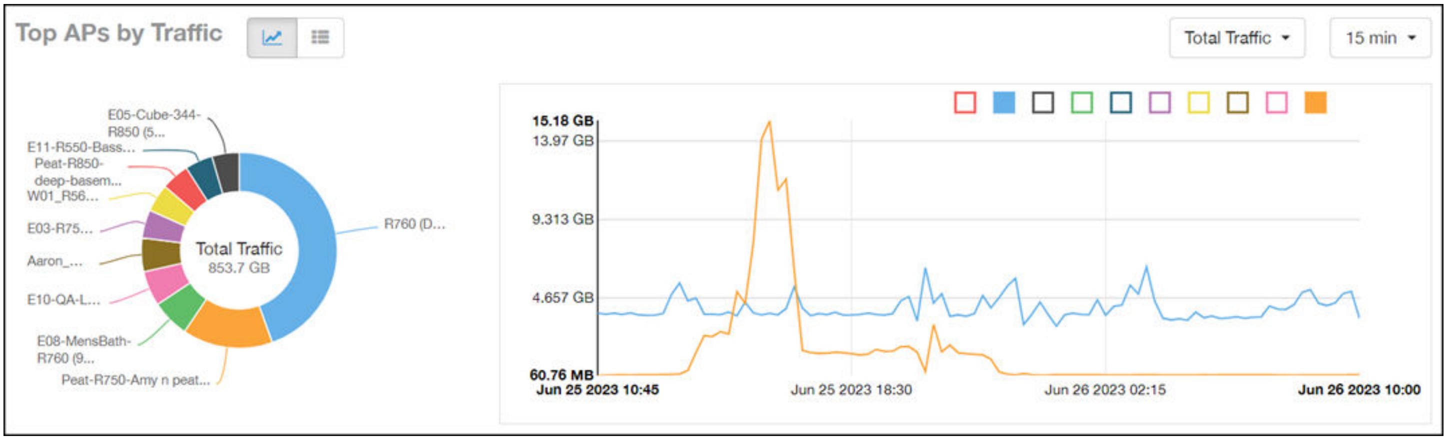
Top APs by Traffic Tile

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

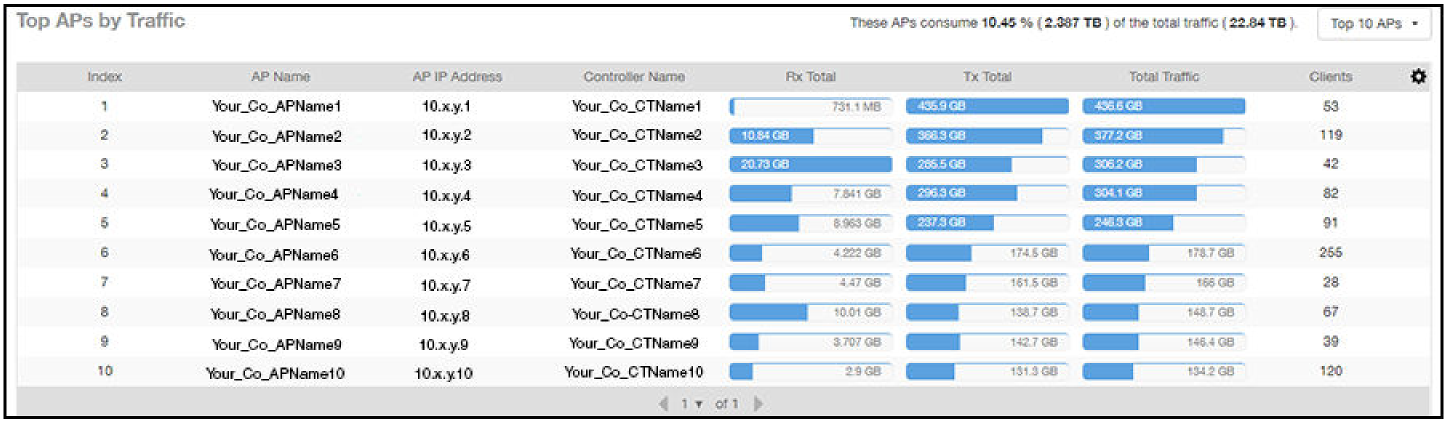


> **NOTE**
> If you pause the pointer over the line graph, an information box is displayed containing the selected AP details.

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



Top APs by Traffic

These APs consume **10.45** % (**2.387 TB**) of the total traffic (**22.84 TB**).

Top 10 APs

Index	AP Name	AP IP Address	Controller Name	Rx Total	Tx Total	Total Traffic	Clients
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	731.1 MB	435.9 GB	436.6 GB	53
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName2	10.84 GB	366.3 GB	377.2 GB	119
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName3	20.73 GB	265.5 GB	306.2 GB	42
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName4	7.841 GB	296.3 GB	304.1 GB	82
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName5	8.963 GB	237.3 GB	246.3 GB	91
6	Your_Co_APName6	10.x.y.6	Your_Co_CTName6	4.222 GB	174.5 GB	178.7 GB	255
7	Your_Co_APName7	10.x.y.7	Your_Co_CTName7	4.47 GB	161.5 GB	166 GB	28
8	Your_Co_APName8	10.x.y.8	Your_Co-CTName8	10.01 GB	138.7 GB	148.7 GB	67
9	Your_Co_APName9	10.x.y.9	Your_Co_CTName9	3.707 GB	142.7 GB	146.4 GB	39
10	Your_Co_APName10	10.x.y.10	Your_Co_CTName10	2.9 GB	131.3 GB	134.2 GB	120

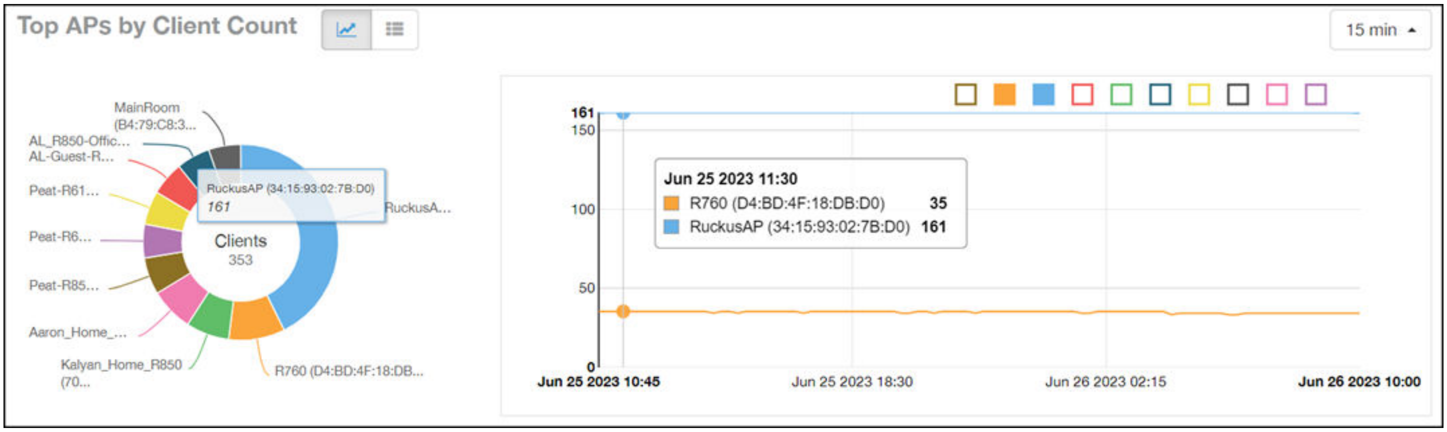
1 ▾ of 1

Top APs by Client Count Tile

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

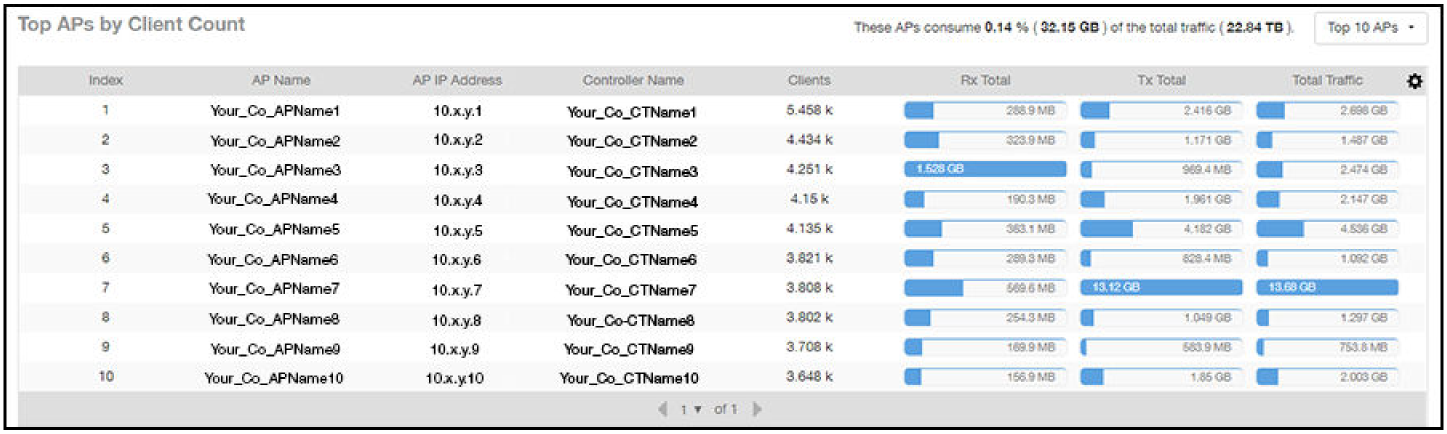
In the tile, use the menu to specify the time period of 15 minutes, 1 hour, or 1 day. If you pause the pointer over the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected AP details in the line graph.

FIGURE 88 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 89 Wireless Network Report : Top APs by Client Count (Table)



Top APs by Client Count

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

Top 10 APs ▾

Index	AP Name	AP IP Address	Controller Name	Clients	Rx Total	Tx Total	Total Traffic
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	5.458 k	288.9 MB	2.416 GB	2.698 GB
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName2	4.434 k	323.9 MB	1.171 GB	1.487 GB
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName3	4.251 k	1.528 GB	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	1.65 GB	2.003 GB

◀ 1 ▾ of 1 ▶

Traffic Trend Graphs

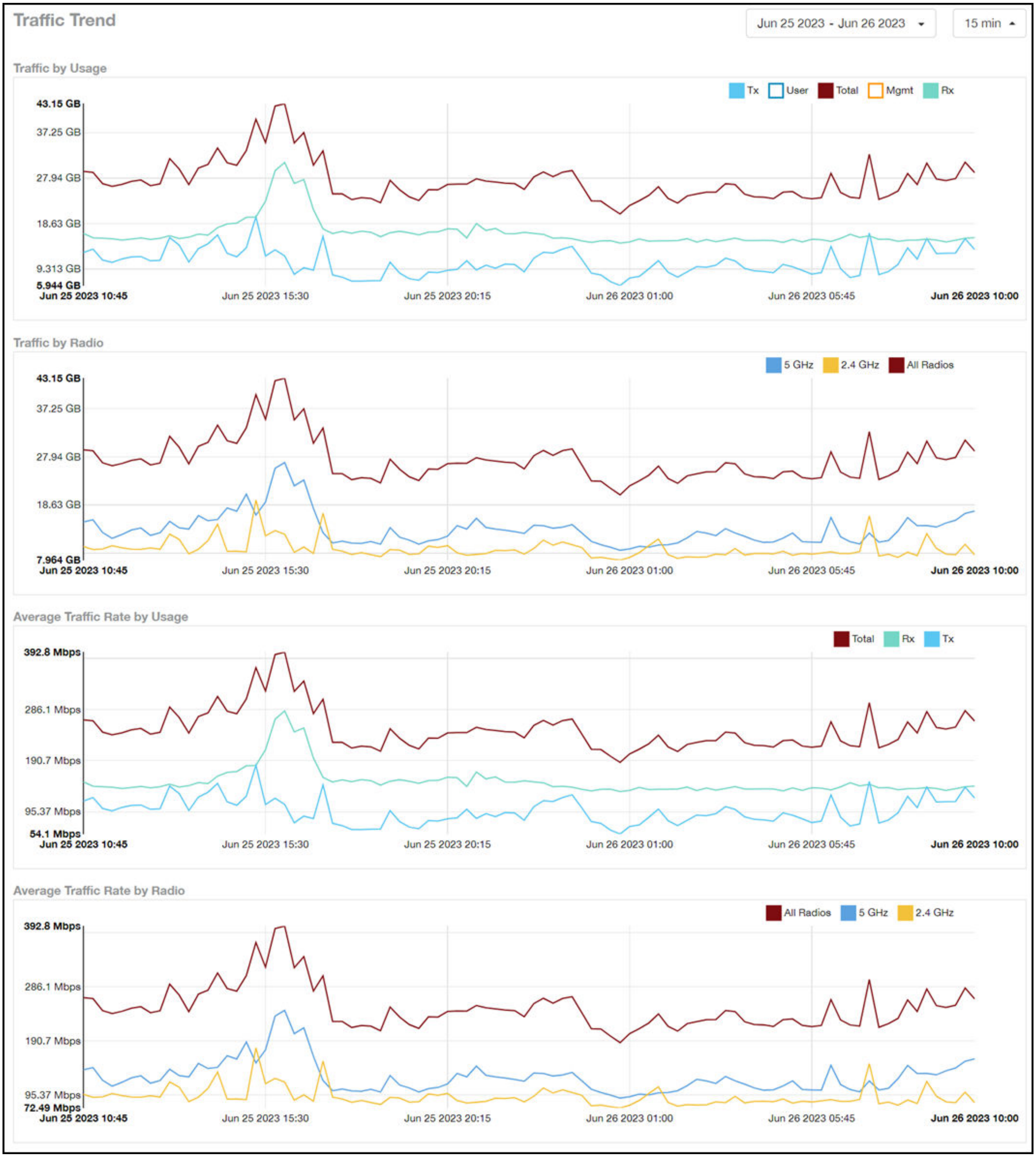
The **Traffic Trend** graphs of the **Wireless Network Report** display the traffic by usage and radio over time.

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 90 Wireless Network Report: Traffic Trend Graphs

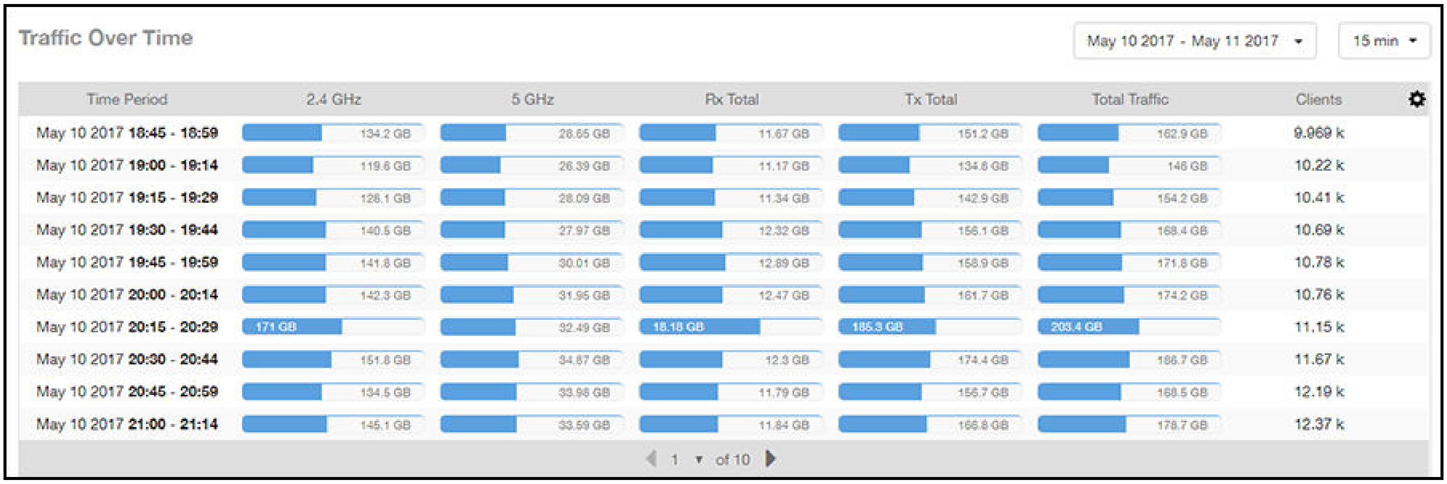


Traffic Over Time Table

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 91 Wireless Network Report: Traffic Over Time Table



Traffic Over Time

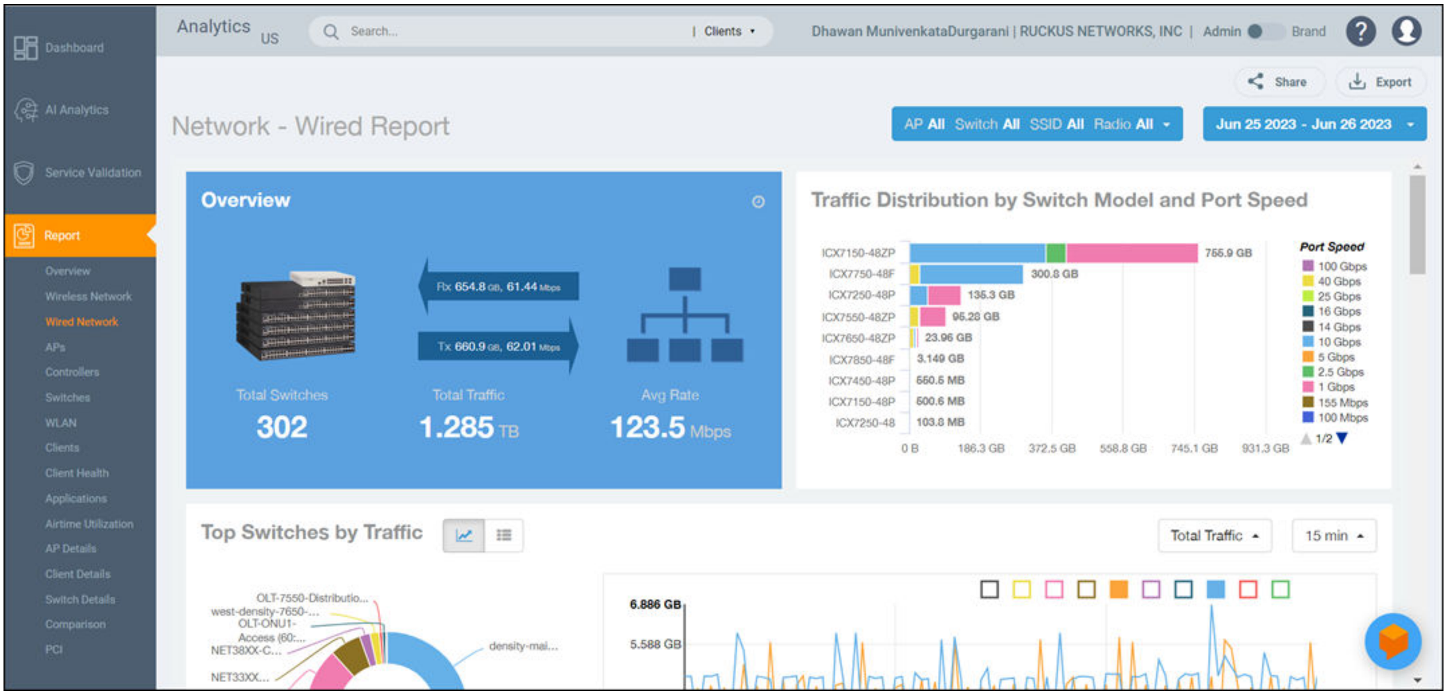
Time Period	2.4 GHz	5 GHz	Rx Total	Tx Total	Total Traffic	Clients
May 10 2017 **18:45 - 18:59**	134.2 GB	26.65 GB	11.67 GB	151.2 GB	162.9 GB	9.969 k
May 10 2017 **19:00 - 19:14**	119.6 GB	26.39 GB	11.17 GB	134.8 GB	146 GB	10.22 k
May 10 2017 **19:15 - 19:29**	126.1 GB	28.09 GB	11.34 GB	142.9 GB	154.2 GB	10.41 k
May 10 2017 **19:30 - 19:44**	140.5 GB	27.97 GB	12.32 GB	156.1 GB	168.4 GB	10.69 k
May 10 2017 **19:45 - 19:59**	141.8 GB	30.01 GB	12.89 GB	158.9 GB	171.8 GB	10.78 k
May 10 2017 **20:00 - 20:14**	142.3 GB	31.95 GB	12.47 GB	161.7 GB	174.2 GB	10.76 k
May 10 2017 **20:15 - 20:29**	171 GB	32.49 GB	18.18 GB	185.3 GB	203.4 GB	11.15 k
May 10 2017 **20:30 - 20:44**	151.8 GB	34.87 GB	12.3 GB	174.4 GB	186.7 GB	11.67 k
May 10 2017 **20:45 - 20:59**	134.5 GB	33.96 GB	11.79 GB	156.7 GB	168.5 GB	12.19 k
May 10 2017 **21:00 - 21:14**	145.1 GB	33.59 GB	11.84 GB	166.8 GB	178.7 GB	12.37 k

Wired Network Report

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

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

FIGURE 92 Wired Network Report (Upper Portion Only)



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

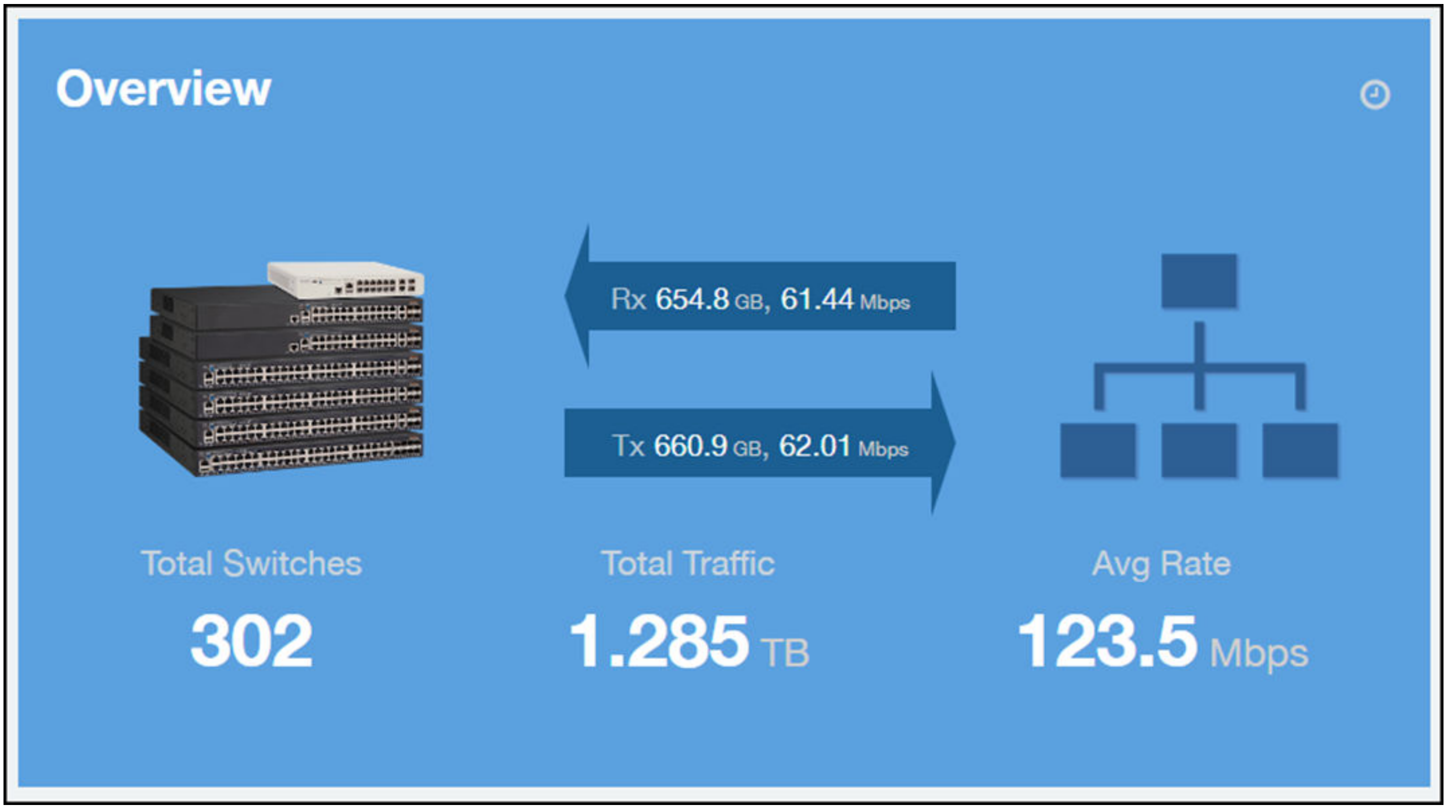
- Overview tile
- Traffic Distribution by Switch Model and Port Speed tile
- Top Switches by Traffic tile
- Top Switches by PoE Usage tile
- Top Switches by Errors tile
- Traffic Trend tile
- Error Trend tile

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 93 Wired Network Report: Overview Tile

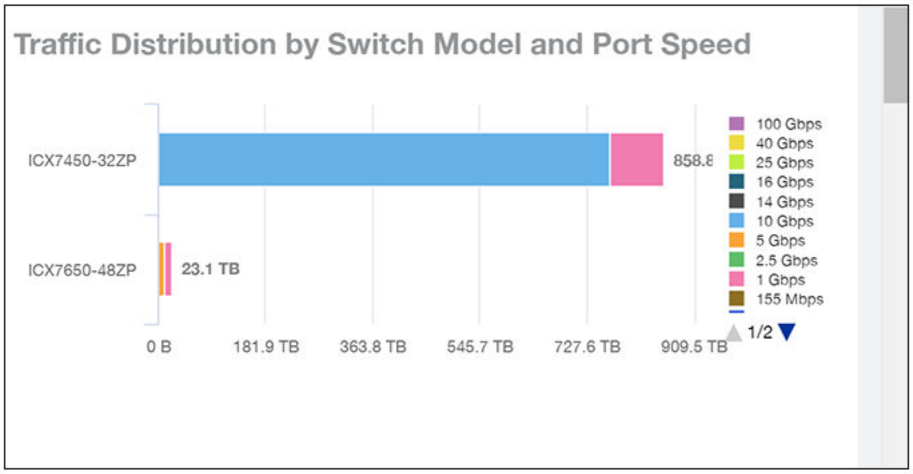


Traffic Distribution by Switch Model and Port Speed Chart

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

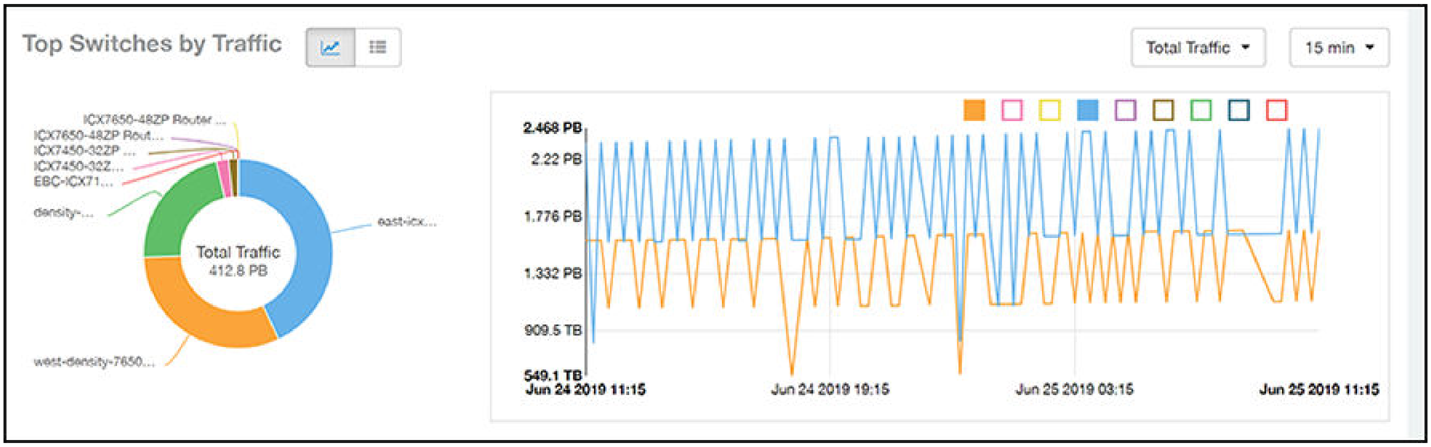


Top Switches by Traffic Tile

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.

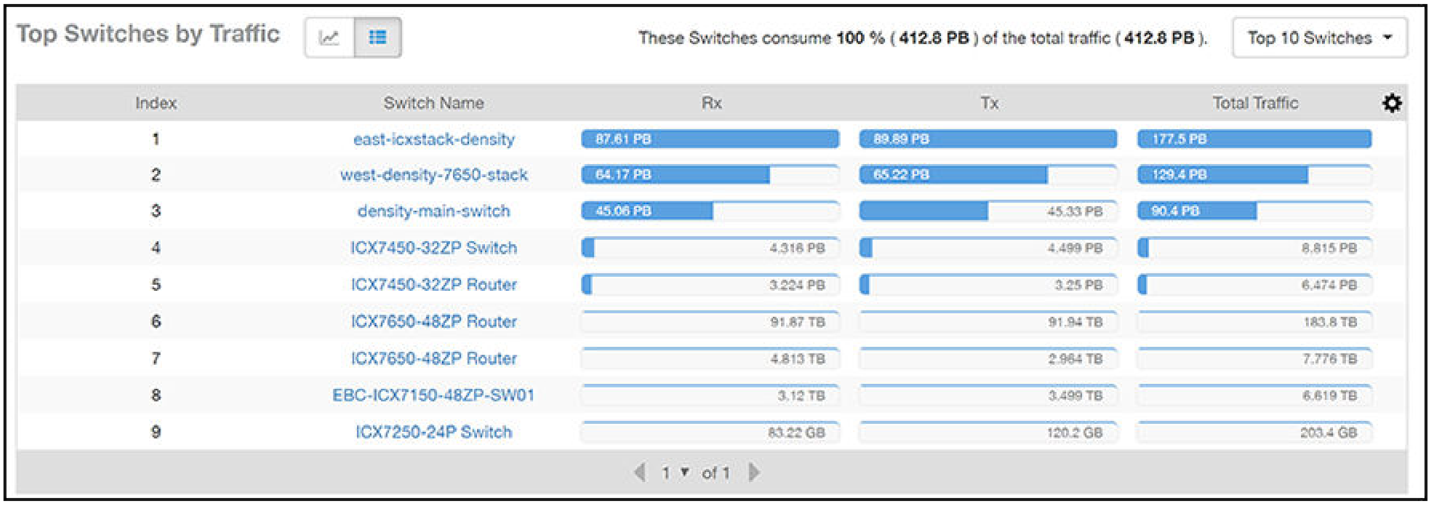
If you pause the pointer over the donut chart or the line graph, an information box is displayed containing the details on the selected data points. You can click one of the areas of the donut chart to go to the Switch Details dashboard for the corresponding switch. Click any of the colored squares to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

FIGURE 95 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 96 Wired Network Report Top Switches by Traffic Table


Top Switches by Traffic

These Switches consume **100 %** (**412.8 PB**) of the total traffic (**412.8 PB**).

Top 10 Switches

Index	Switch Name	Rx	Tx	Total Traffic
1	east-icxstack-density	87.61 PB	89.89 PB	177.5 PB
2	west-density-7650-stack	64.17 PB	65.22 PB	129.4 PB
3	density-main-switch	45.06 PB	45.33 PB	90.4 PB
4	ICX7450-32ZP Switch	4.316 PB	4.499 PB	8.815 PB
5	ICX7450-32ZP Router	3.224 PB	3.25 PB	6.474 PB
6	ICX7650-48ZP Router	91.87 TB	91.94 TB	183.8 TB
7	ICX7650-48ZP Router	4.813 TB	2.964 TB	7.776 TB
8	EBC-ICX7150-48ZP-SW01	3.12 TB	3.499 TB	6.619 TB
9	ICX7250-24P Switch	83.22 GB	120.2 GB	203.4 GB

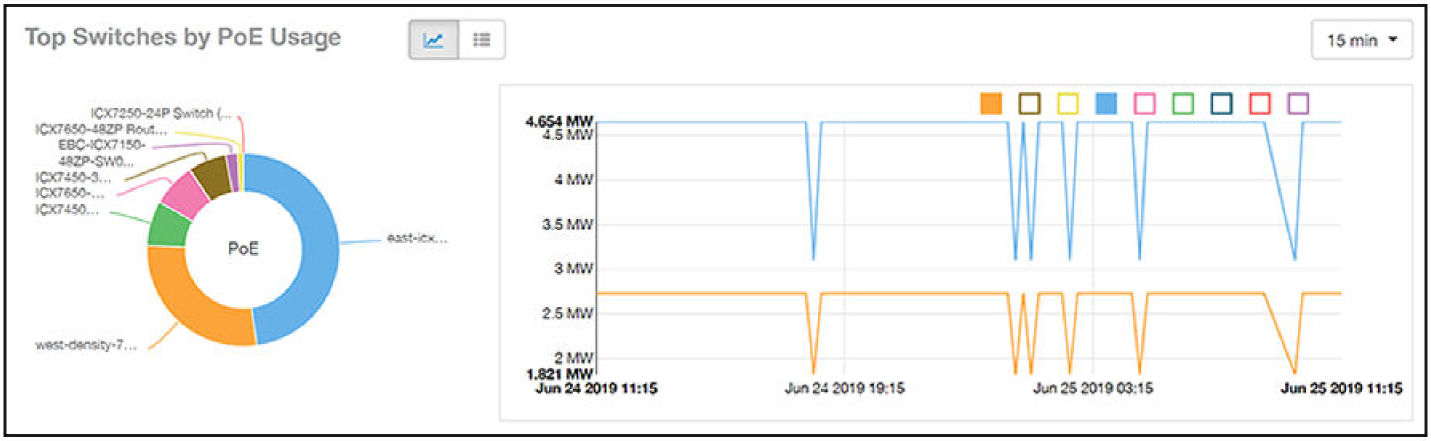
1 ▾ of 1

Top Switches by PoE Usage Tile

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

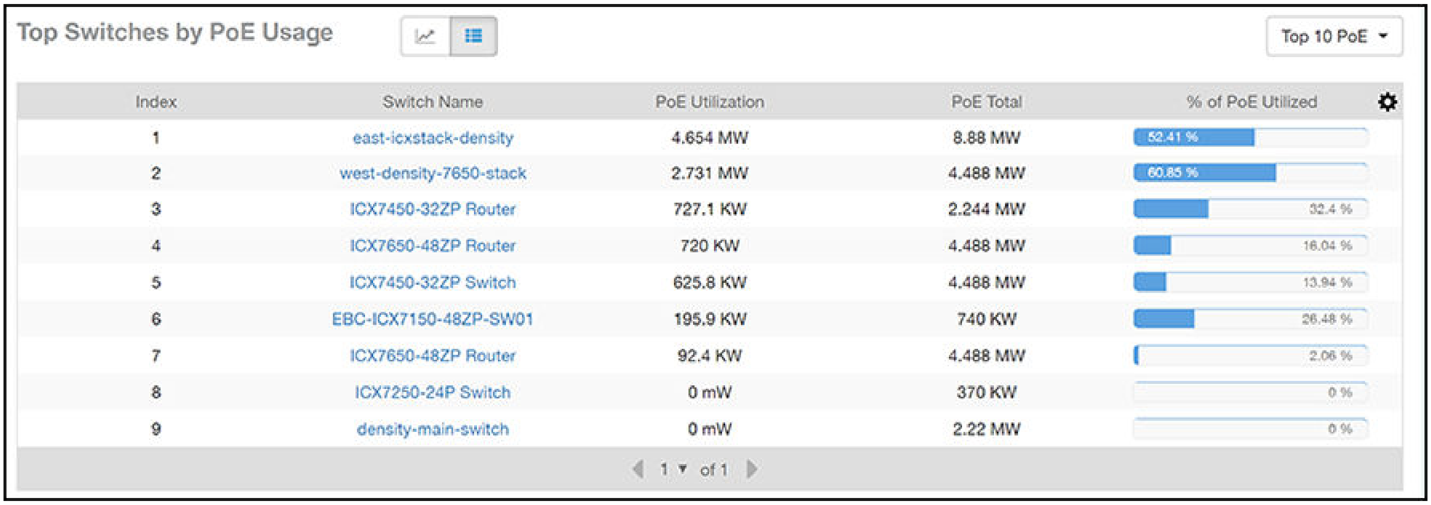
If you pause the pointer over the donut chart or the line graph, an information box is displayed containing the details on the selected data points. You can click one of the areas of the donut chart to go to the **Switch Details** dashboard for the corresponding switch. Click any of the colored squares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

FIGURE 97 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 98 Wired Network Report: Top Switches by PoE Usage Table


Top Switches by PoE Usage

Top 10 PoE

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

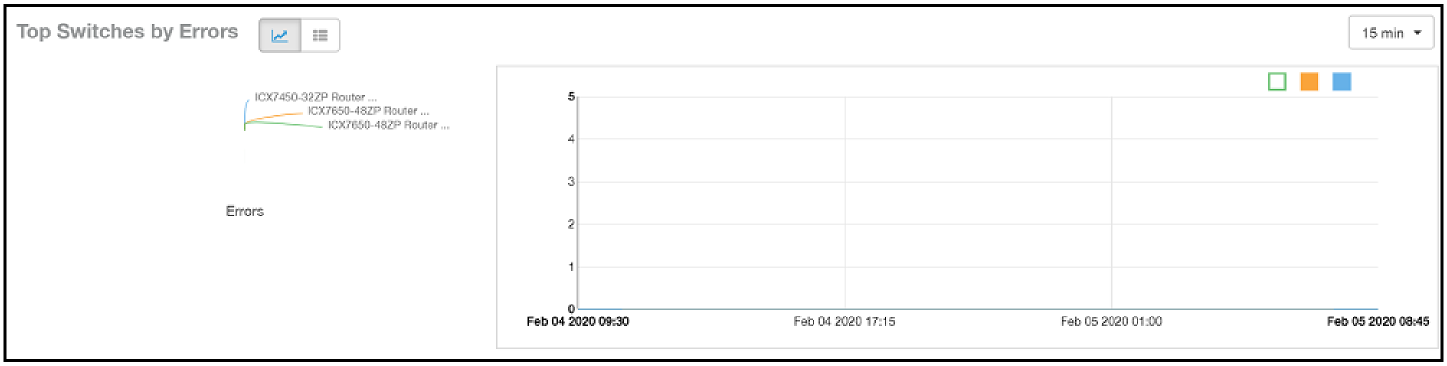
1 ▾ of 1

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.

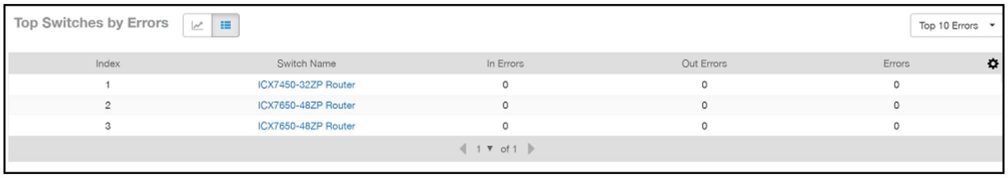
If you pause the pointer over the donut chart or the line graph, an information box is displayed containing the details on the selected data points. You can click one of the areas of the donut chart to go to the **Switch Details** dashboard for the corresponding switch. Click any of the colored squares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

FIGURE 99 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 100 Wired Network Report: Top Switches by Error Table



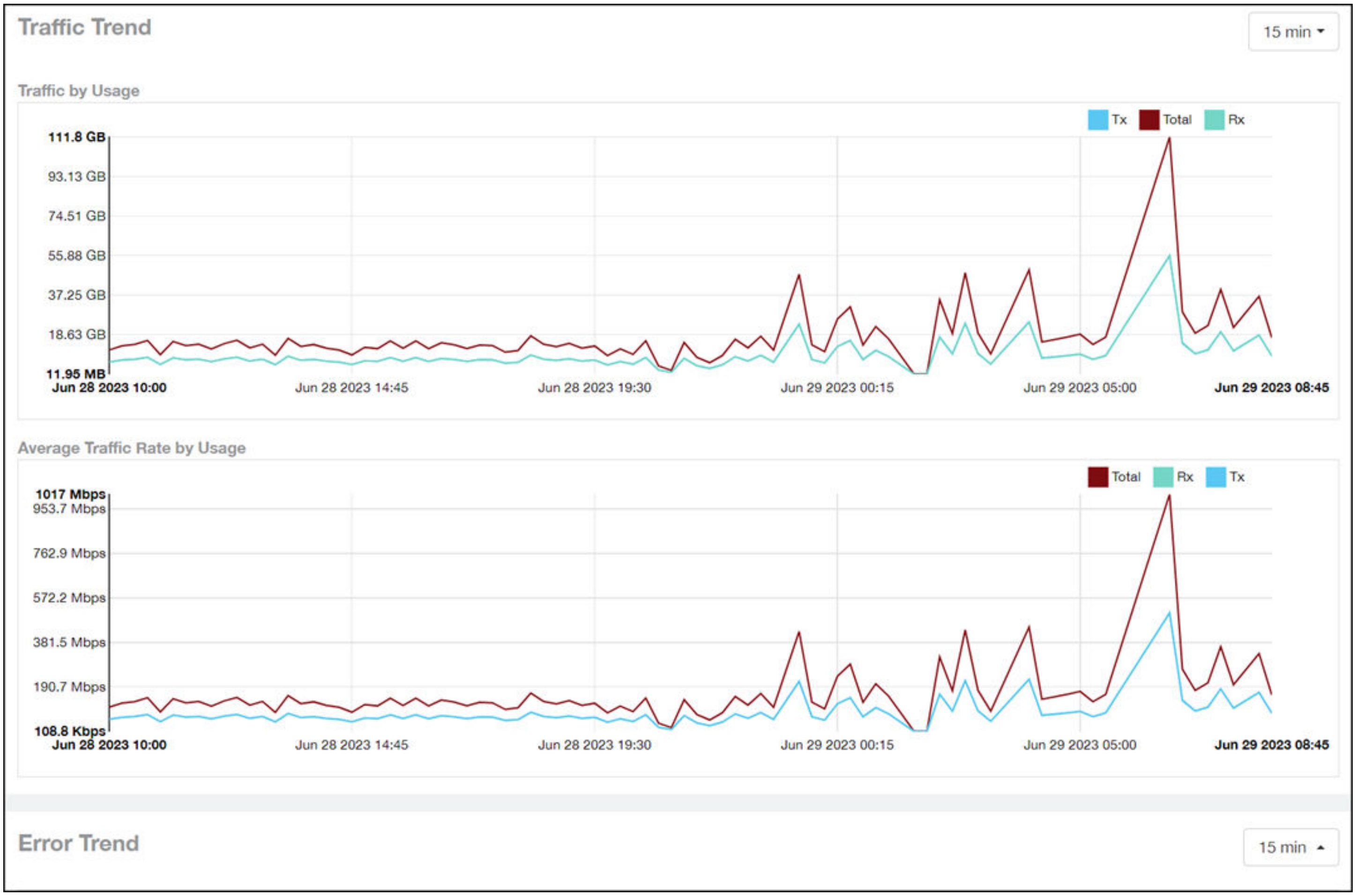
Index	Switch Name	In Errors	Out Errors	Errors
1	ICX7450-32ZP Router	0	0	0
2	ICX7650-48ZP Router	0	0	0
3	ICX7650-48ZP Router	0	0	0

Traffic Trend Graph

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

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

FIGURE 101 Wired Network Report: Traffic Trend Graph

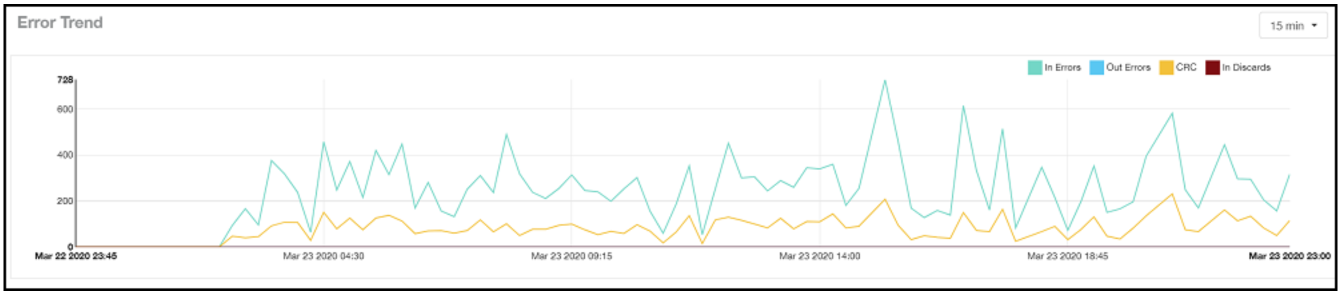


Error Trend Graph

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 102 Wired Network: Error Trend Graph

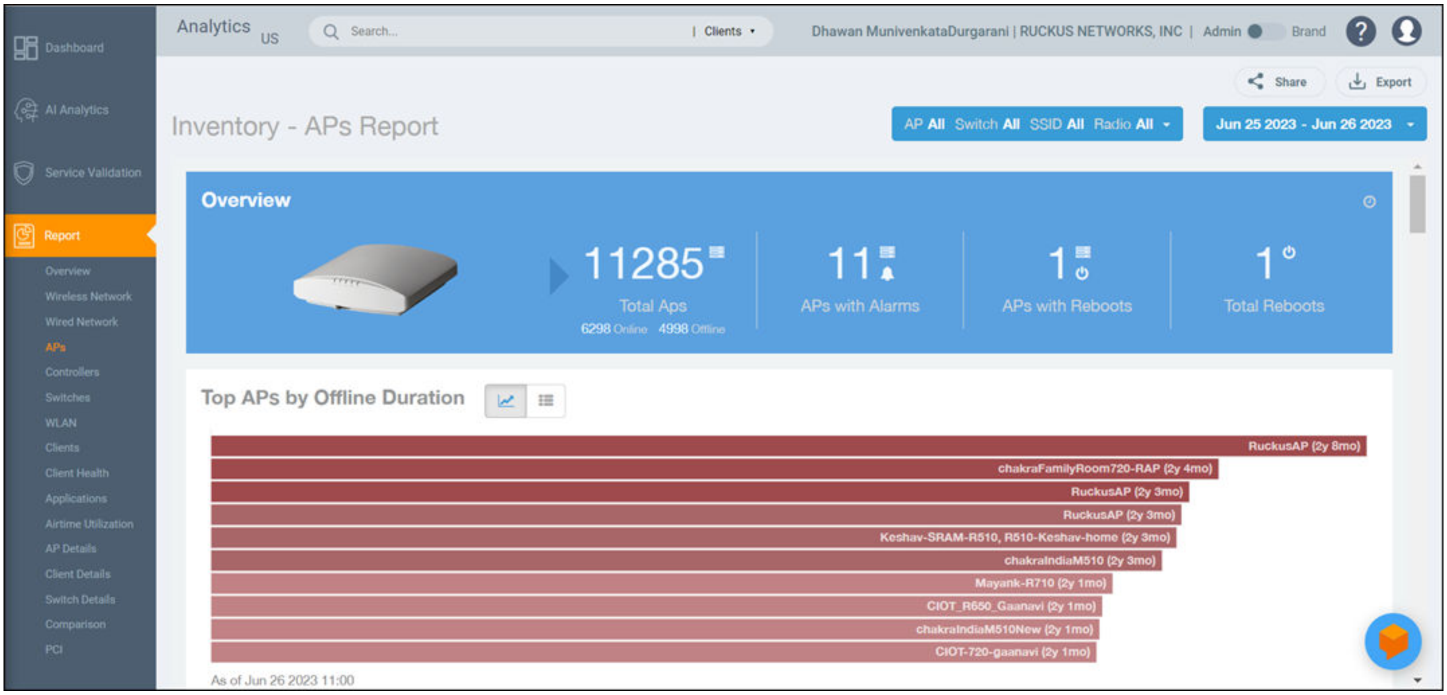


Inventory - APs Report

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 103 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.

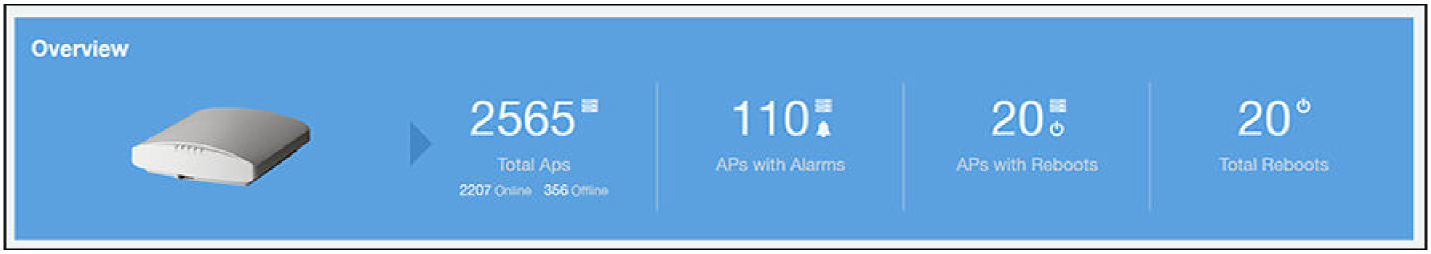
Overview Tile

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 104 Inventory - APs Report: Overview Tile

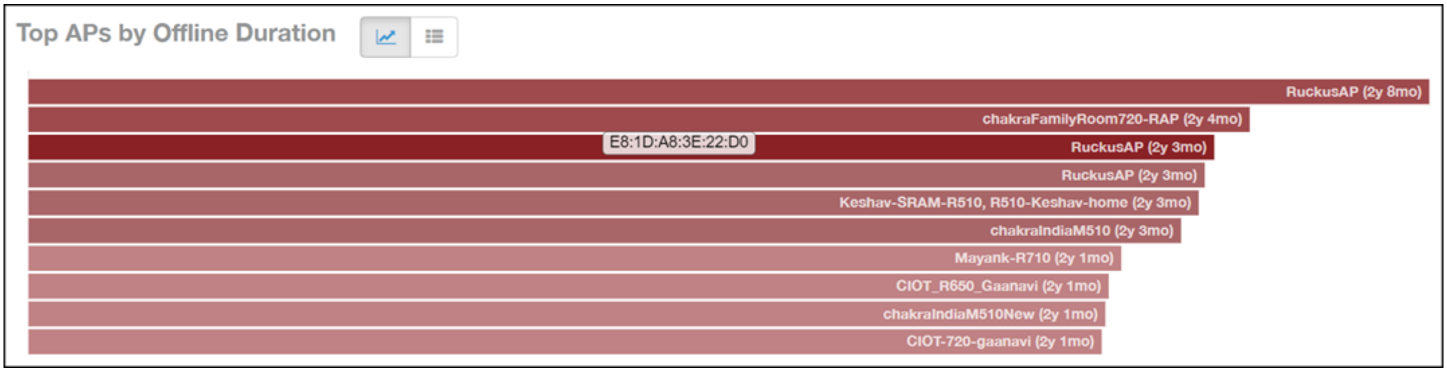


Top APs by Offline Duration Tile

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

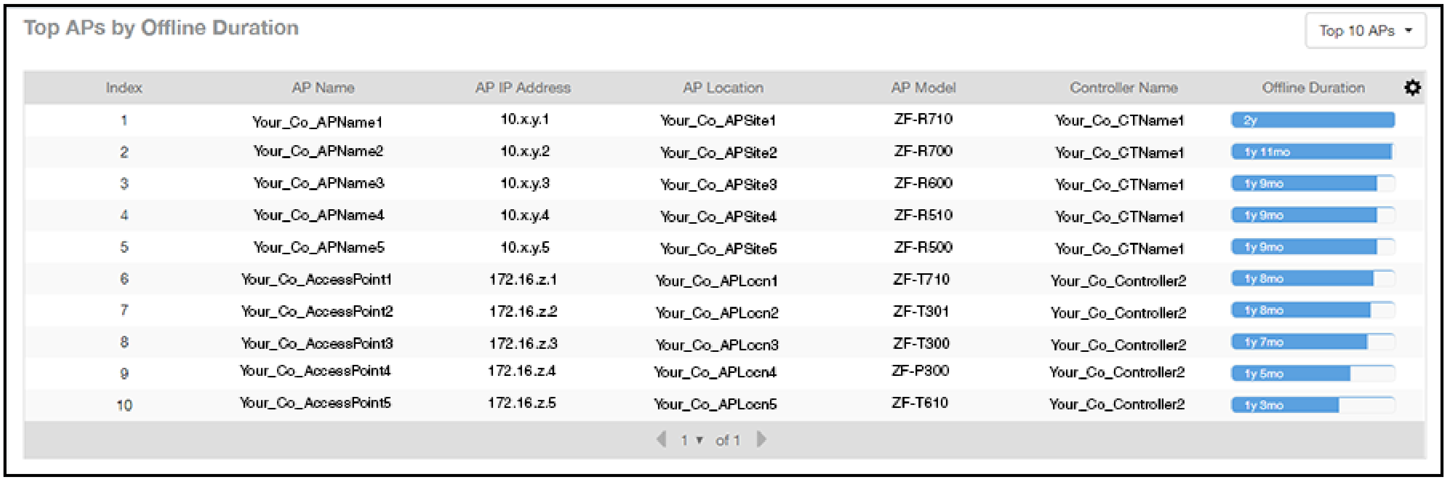

Top APs by Offline Duration
RuckusAP (2y 8mo)
chakraFamilyRoom720-RAP (2y 4mo)
E8:1D:A8:3E:22:D0
RuckusAP (2y 3mo)
RuckusAP (2y 3mo)
Keshav-SRAM-R510, R510-Keshav-home (2y 3mo)
chakraIndiaM510 (2y 3mo)
Mayank-R710 (2y 1mo)
CIOT_R650_Gaanavi (2y 1mo)
chakraIndiaM510New (2y 1mo)
CIOT-720-gaanavi (2y 1mo)

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



Top APs by Offline Duration

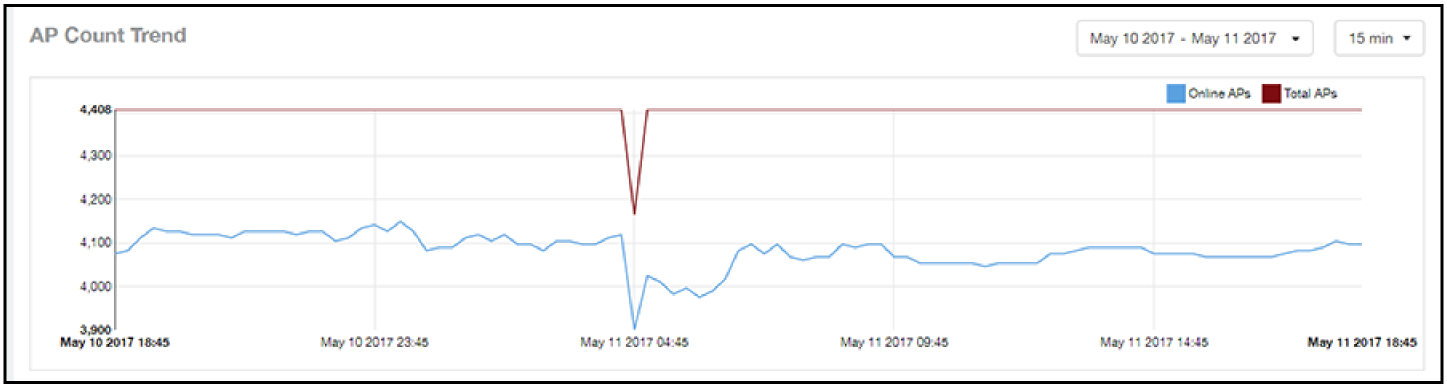
Index	AP Name	AP IP Address	AP Location	AP Model	Controller Name	Offline Duration
1	Your_Co_APName1	10.x.y.1	Your_Co_APSite1	ZF-R710	Your_Co_CTName1	2y
2	Your_Co_APName2	10.x.y.2	Your_Co_APSite2	ZF-R700	Your_Co_CTName1	1y 11mo
3	Your_Co_APName3	10.x.y.3	Your_Co_APSite3	ZF-R600	Your_Co_CTName1	1y 9mo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

AP Count Trend Graph

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

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

FIGURE 107 Inventory - APs Report: AP Count Trend Graph

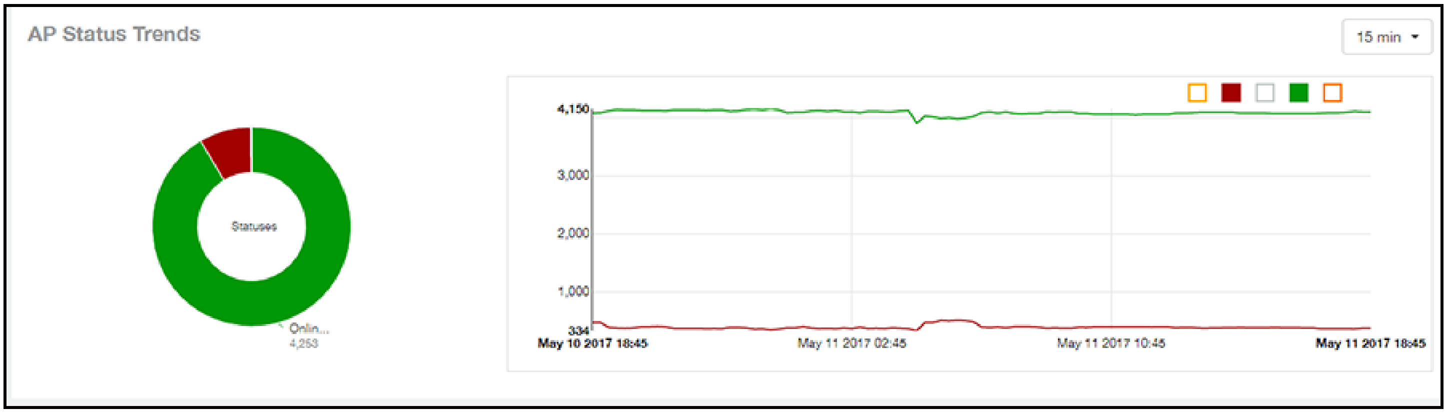


AP Status Trends Tile

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 108 Inventory - APs Report: AP Status Trends Tile

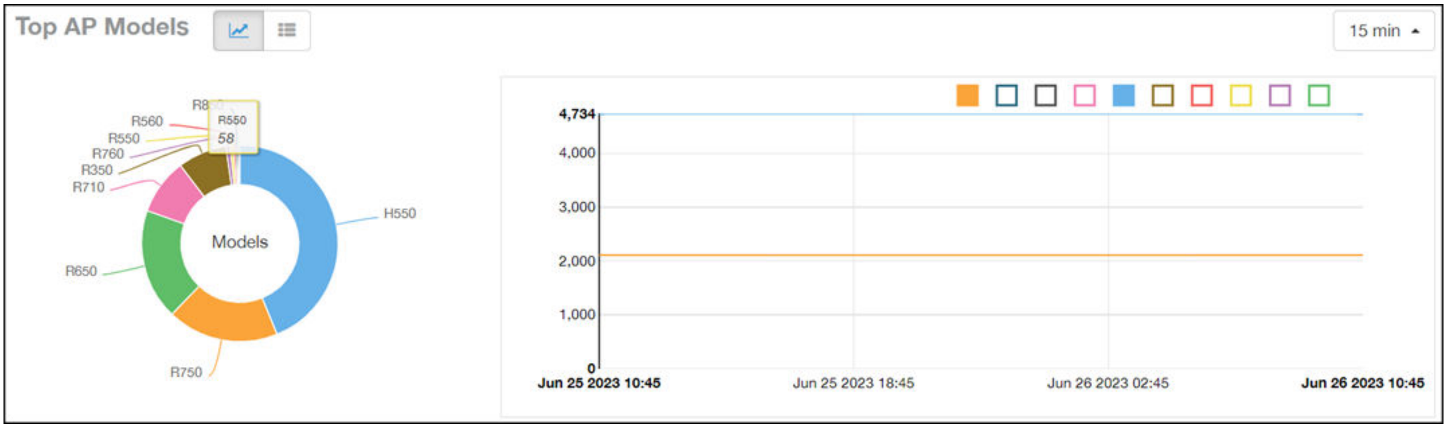


Top AP Models

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.

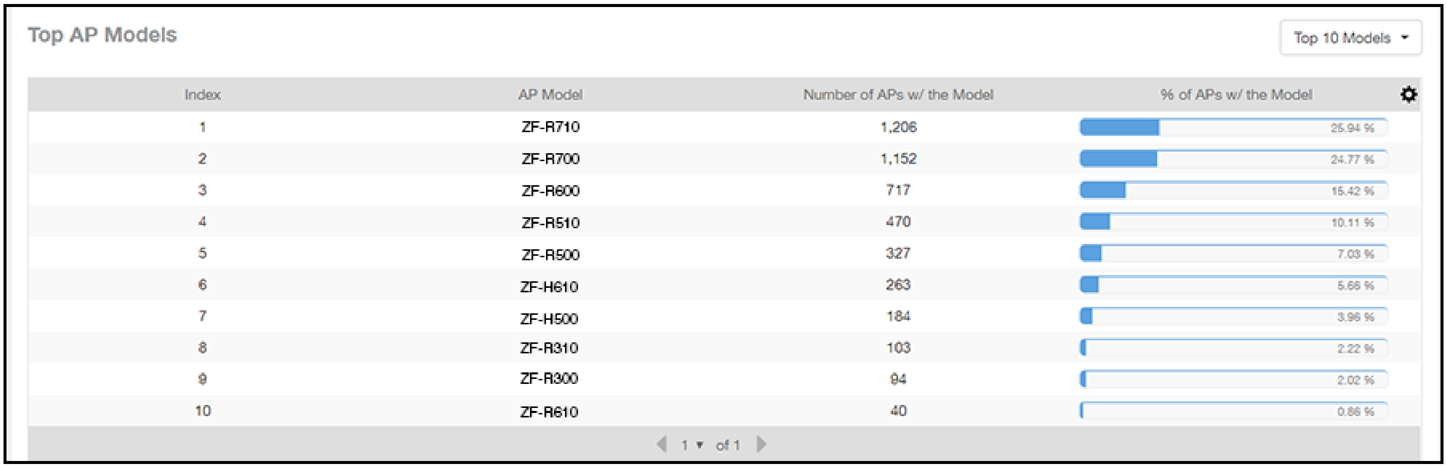
FIGURE 109 Inventory - APs Report: Top AP Models (Chart and Graph)



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



Top AP Models

Top 10 Models ▾

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

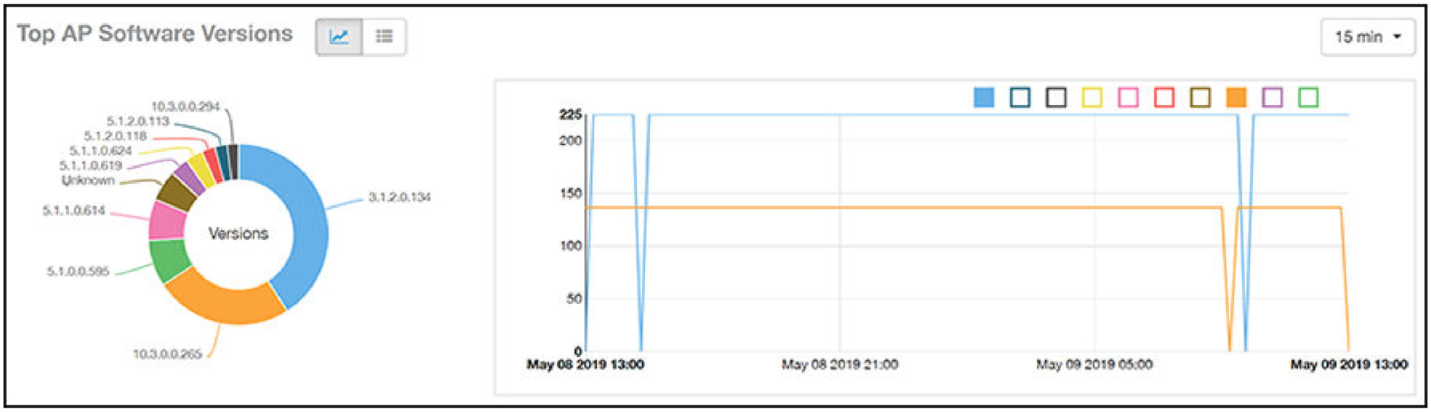
1 ▾ of 1

Top AP Software Versions 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.

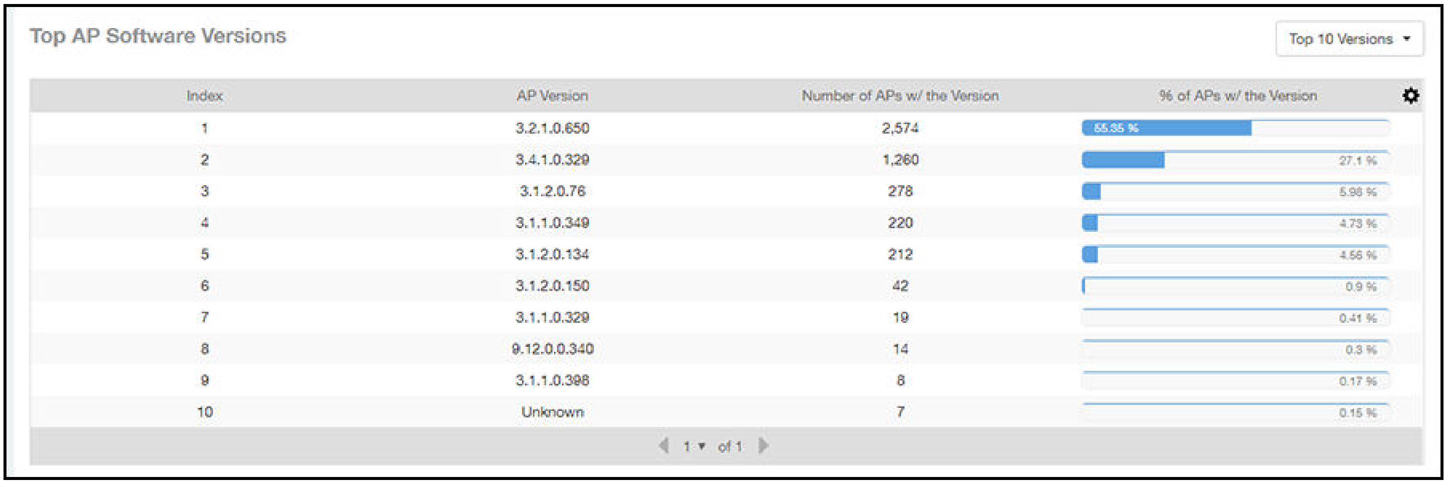
FIGURE 111 Inventory - APs Report: Top AP Software Versions (Graph and Chart)



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



Top AP Software Versions

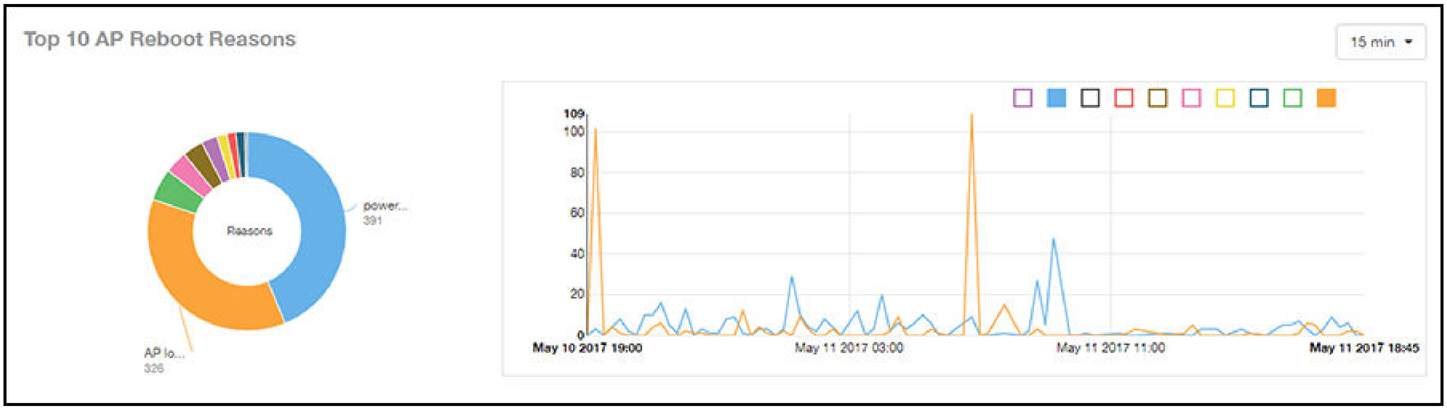
Index	AP Version	Number of APs w/ the Version	% of APs w/ the Version
1	3.2.1.0.650	2,574	55.35 %
2	3.4.1.0.329	1,260	27.1 %
3	3.1.2.0.76	278	5.98 %
4	3.1.1.0.349	220	4.73 %
5	3.1.2.0.134	212	4.56 %
6	3.1.2.0.150	42	0.9 %
7	3.1.1.0.329	19	0.41 %
8	9.12.0.0.340	14	0.3 %
9	3.1.1.0.398	8	0.17 %
10	Unknown	7	0.15 %

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

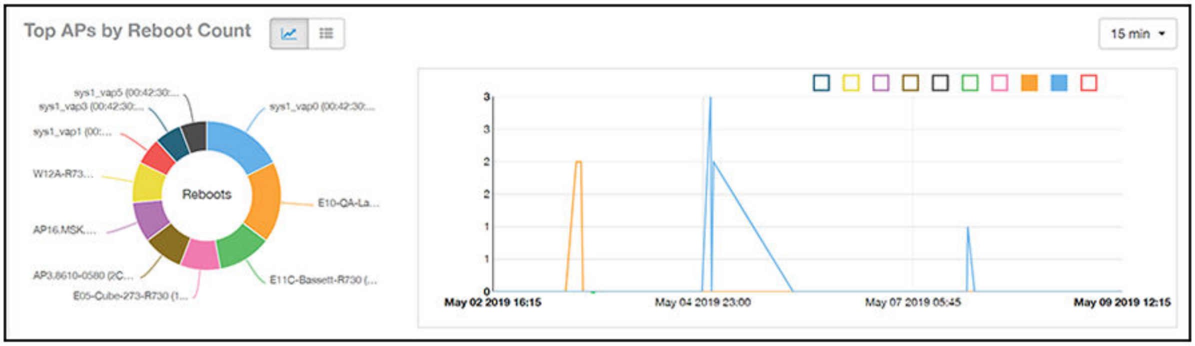


Top APs by Reboot Count Tile

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.

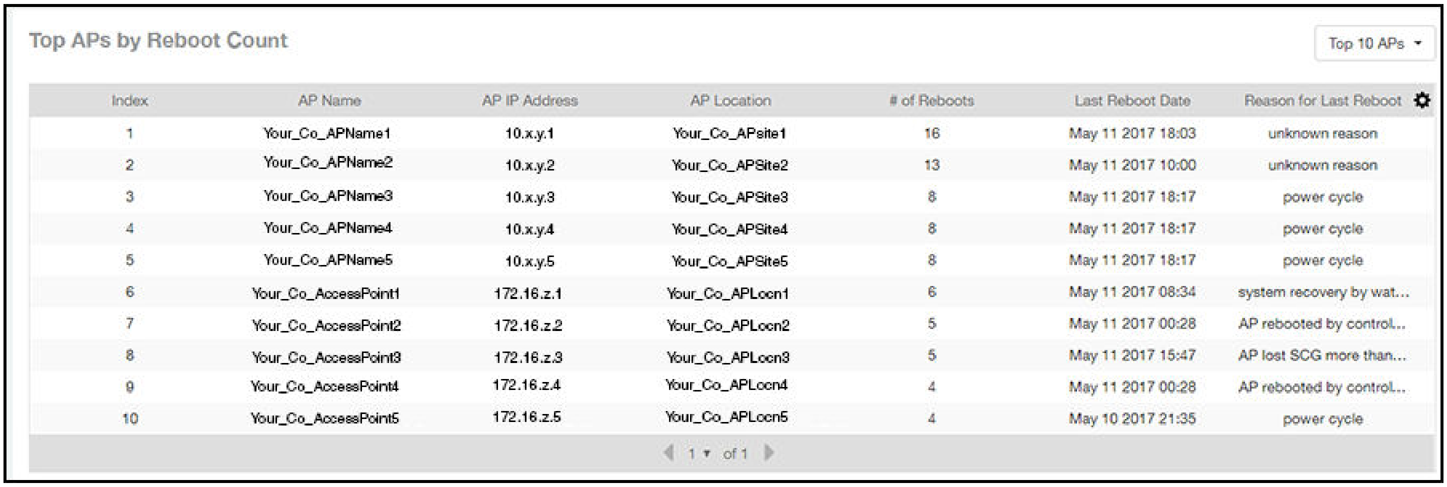
FIGURE 114 Inventory - APs Report: Top APs by Reboot Count (Chart and Graph)



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



Top APs by Reboot Count

Top 10 APs

Index	AP Name	AP IP Address	AP Location	# of Reboots	Last Reboot Date	Reason for Last Reboot ⚙
1	Your_Co_APName1	10.x.y.1	Your_Co_APsite1	16	May 11 2017 18:03	unknown reason
2	Your_Co_APName2	10.x.y.2	Your_Co_APSite2	13	May 11 2017 10:00	unknown reason
3	Your_Co_APName3	10.x.y.3	Your_Co_APSite3	8	May 11 2017 18:17	power cycle
4	Your_Co_APName4	10.x.y.4	Your_Co_APSite4	8	May 11 2017 18:17	power cycle
5	Your_Co_APName5	10.x.y.5	Your_Co_APSite5	8	May 11 2017 18:17	power cycle
6	Your_Co_AccessPoint1	172.16.z.1	Your_Co_APLocn1	6	May 11 2017 08:34	system recovery by wat...
7	Your_Co_AccessPoint2	172.16.z.2	Your_Co_APLocn2	5	May 11 2017 00:28	AP rebooted by control...
8	Your_Co_AccessPoint3	172.16.z.3	Your_Co_APLocn3	5	May 11 2017 15:47	AP lost SCG more than...
9	Your_Co_AccessPoint4	172.16.z.4	Your_Co_APLocn4	4	May 11 2017 00:28	AP rebooted by control...
10	Your_Co_AccessPoint5	172.16.z.5	Your_Co_APLocn5	4	May 10 2017 21:35	power cycle

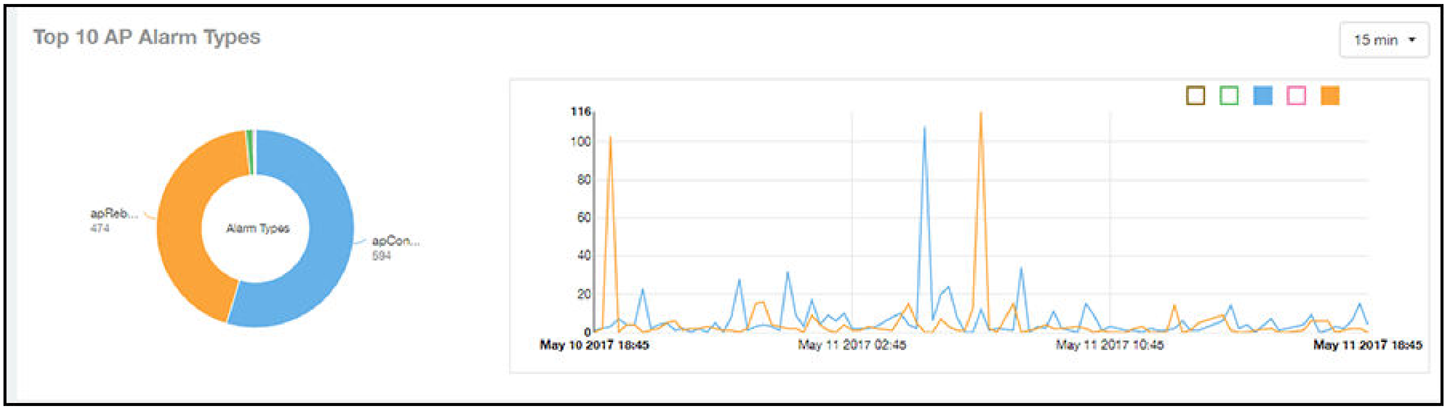
1 ▾ of 1

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 116 Inventory - APs Report: Top 10 AP Alarm Types Tile



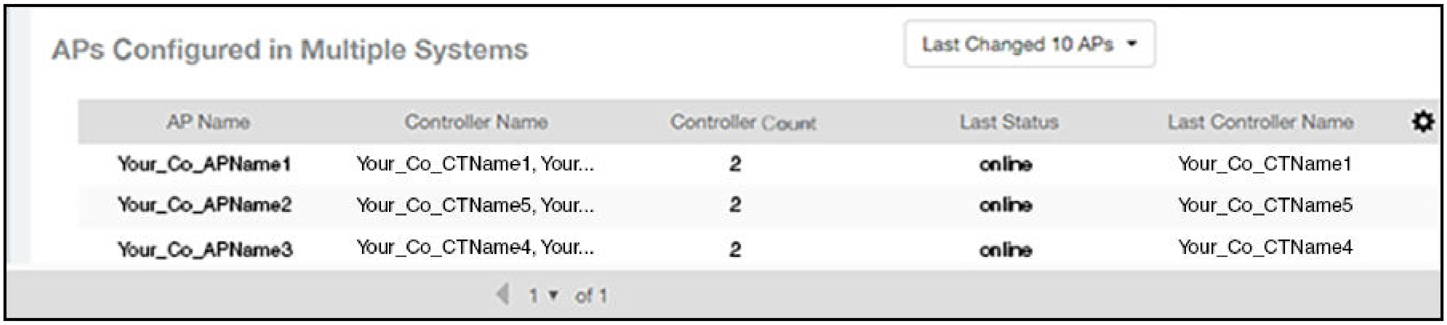
APs Configured in Multiple Systems Tile

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 117 Inventory - APs Report: APs Configured in Multiple Systems Table



APs Configured in Multiple Systems

Last Changed 10 APs ▾

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

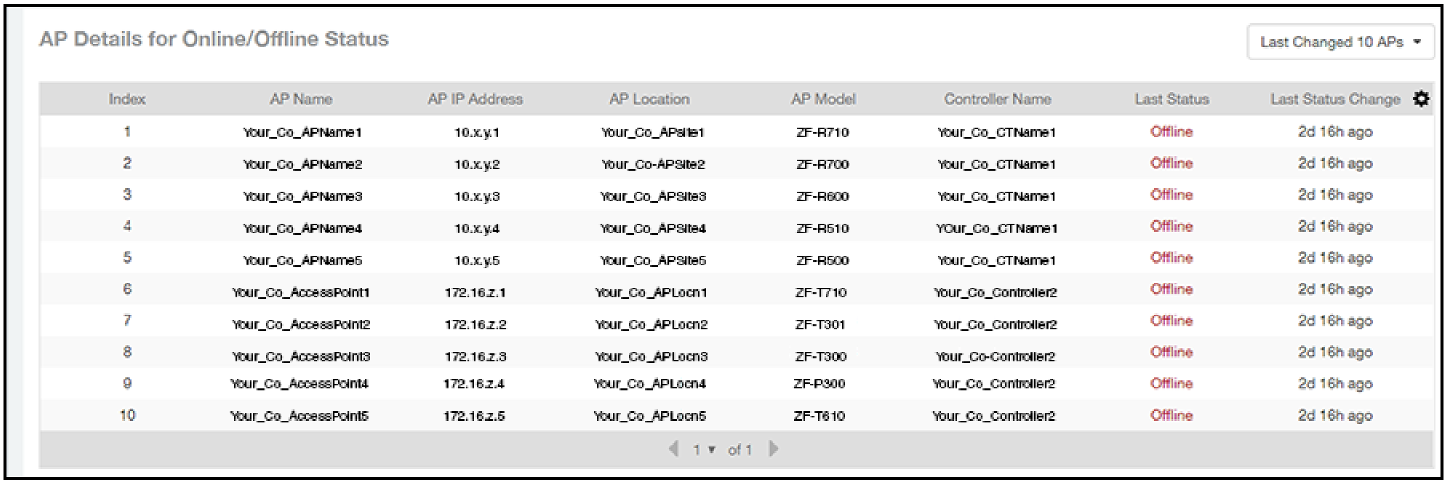
1 ▾ of 1

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



AP Details for Online/Offline Status

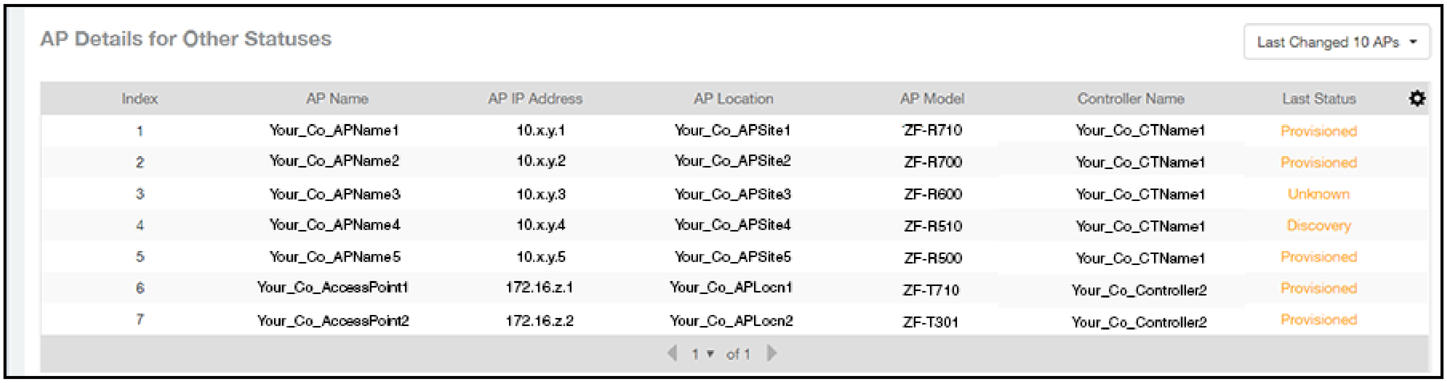
Index	AP Name	AP IP Address	AP Location	AP Model	Controller Name	Last Status	Last Status Change
1	Your_Co_APName1	10.x.y.1	Your_Co_APSite1	ZF-R710	Your_Co_CTName1	Offline	2d 16h ago
2	Your_Co_APName2	10.x.y.2	Your_Co-APSite2	ZF-R700	Your_Co_CTName1	Offline	2d 16h ago
3	Your_Co_APName3	10.x.y.3	Your_Co_APSite3	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

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



AP Details for Other Statuses

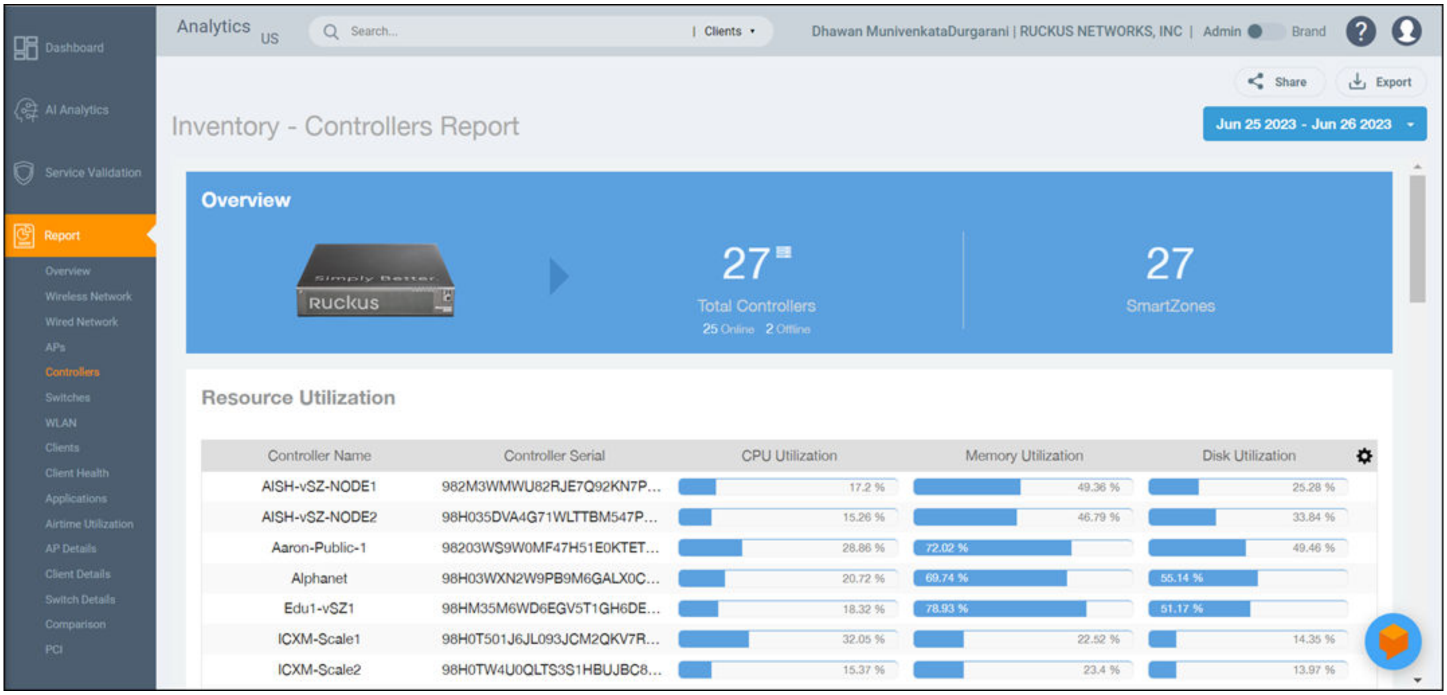
Index	AP Name	AP IP Address	AP Location	AP Model	Controller Name	Last Status
1	Your_Co_APName1	10.x.y.1	Your_Co_APSite1	ZF-R710	Your_Co_CTName1	Provisioned
2	Your_Co_APName2	10.x.y.2	Your_Co_APSite2	ZF-R700	Your_Co_CTName1	Provisioned
3	Your_Co_APName3	10.x.y.3	Your_Co_APSite3	ZF-R600	Your_Co_CTName1	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

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 120 Inventory - Controllers Dashboard (Upper Portion Only)



Inventory - Controllers Report

Overview

27 Total Controllers
25 Online 2 Offline

27 SmartZones

Resource Utilization

Controller Name	Controller Serial	CPU Utilization	Memory Utilization	Disk Utilization
AISH-vSZ-NODE1	982M3WMWU82RJE7Q92KN7P...	17.2 %	49.36 %	25.28 %
AISH-vSZ-NODE2	98H035DVA4G71WLTTBM547P...	15.26 %	46.79 %	33.84 %
Aaron-Public-1	98203WS9W0MF47H51E0KTET...	28.86 %	72.02 %	49.46 %
Alphanet	98H03WXN2W9PB9M6GALX0C...	20.72 %	69.74 %	55.14 %
Edu1-vSZ1	98HM35M6WD6EGV5T1GH6DE...	18.32 %	78.93 %	51.17 %
ICXM-Scale1	98H0T501J6JL093JCM2QKV7R...	32.05 %	22.52 %	14.35 %
ICXM-Scale2	98H0TW4U0QLTS3S1HBUJBC8...	15.37 %	23.4 %	13.97 %

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

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

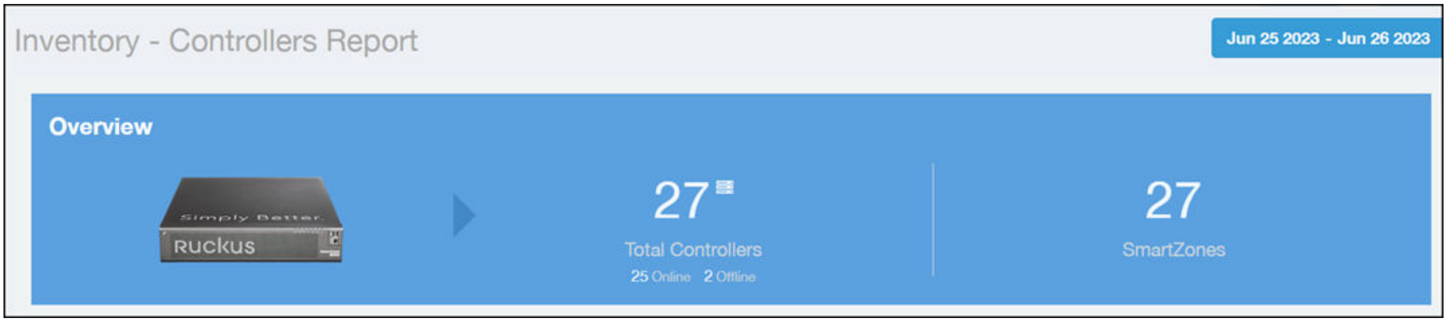
> **NOTE**
> All counts in the **Inventory - Controllers Report** are exact counts.

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 121 Inventory - Controllers Report: Overview Tile



Inventory - Controllers Report

Jun 25 2023 - Jun 26 2023

Overview

27 Total Controllers
25 Online 2 Offline

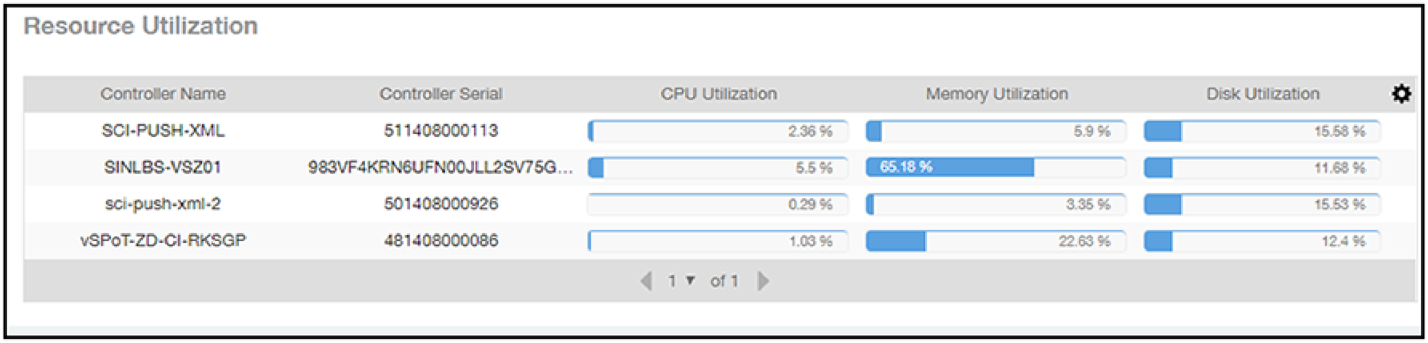
27 SmartZones

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 122 Inventory - Controllers Report: Resource Utilization Table



Resource Utilization

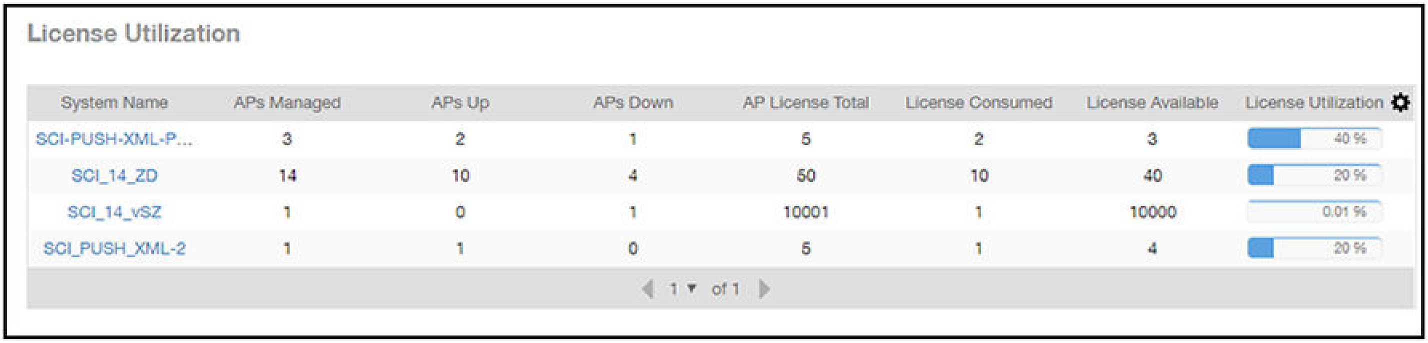
Controller Name	Controller Serial	CPU Utilization	Memory Utilization	Disk Utilization
SCI-PUSH-XML	511408000113	2.36 %	5.9 %	15.58 %
SINLBS-VSZ01	983VF4KRN6UFN00JLL2SV75G...	5.5 %	65.18 %	11.68 %
sci-push-xml-2	501408000926	0.29 %	3.35 %	15.53 %
vSPoT-ZD-CI-RKSGP	481408000086	1.03 %	22.63 %	12.4 %

License Utilization Table

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

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

FIGURE 123 Inventory - Controllers Report: License Utilization Table



License Utilization

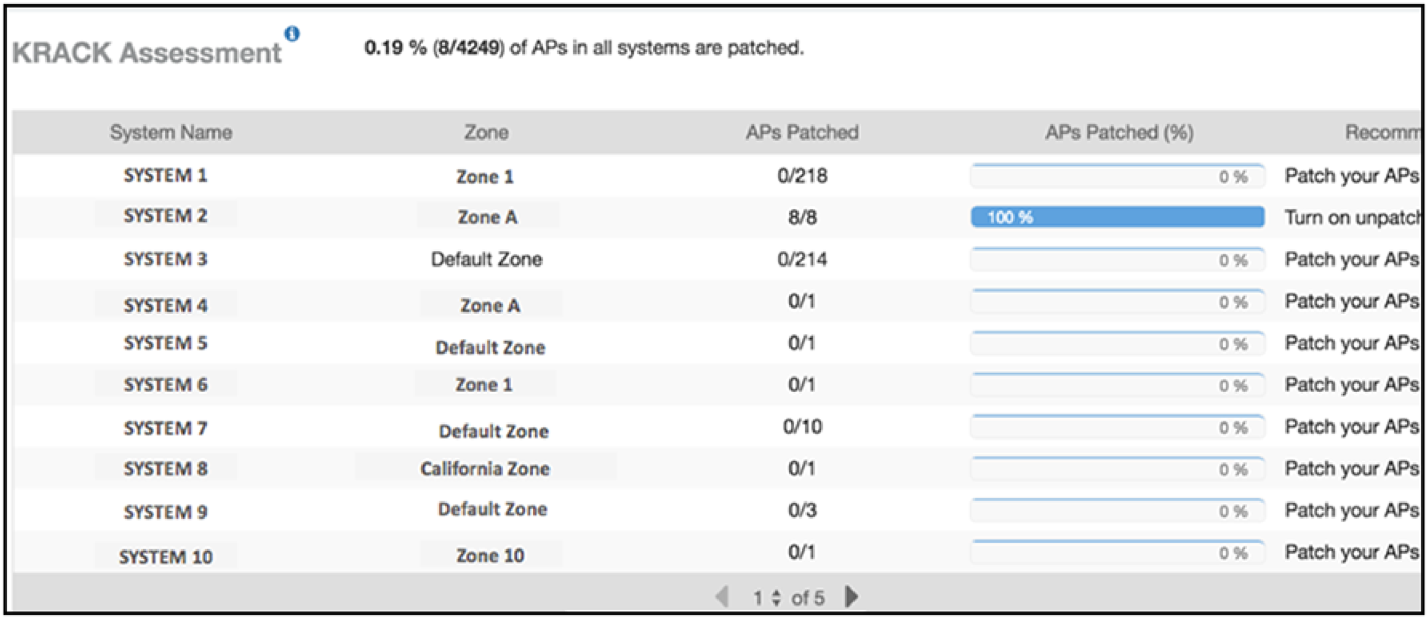
System Name	APs Managed	APs Up	APs Down	AP License Total	License Consumed	License Available	License Utilization
SCI-PUSH-XML-P...	3	2	1	5	2	3	40 %
SCI_14_ZD	14	10	4	50	10	40	20 %
SCI_14_vSZ	1	0	1	10001	1	10000	0.01 %
SCI_PUSH_XML-2	1	1	0	5	1	4	20 %

1 ▾ of 1

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 124 Inventory - Controllers Report: KRACK Assessment Table



KRACK Assessment

0.19 % (8/4249) of APs in all systems are patched.

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

1 ⇕ of 5

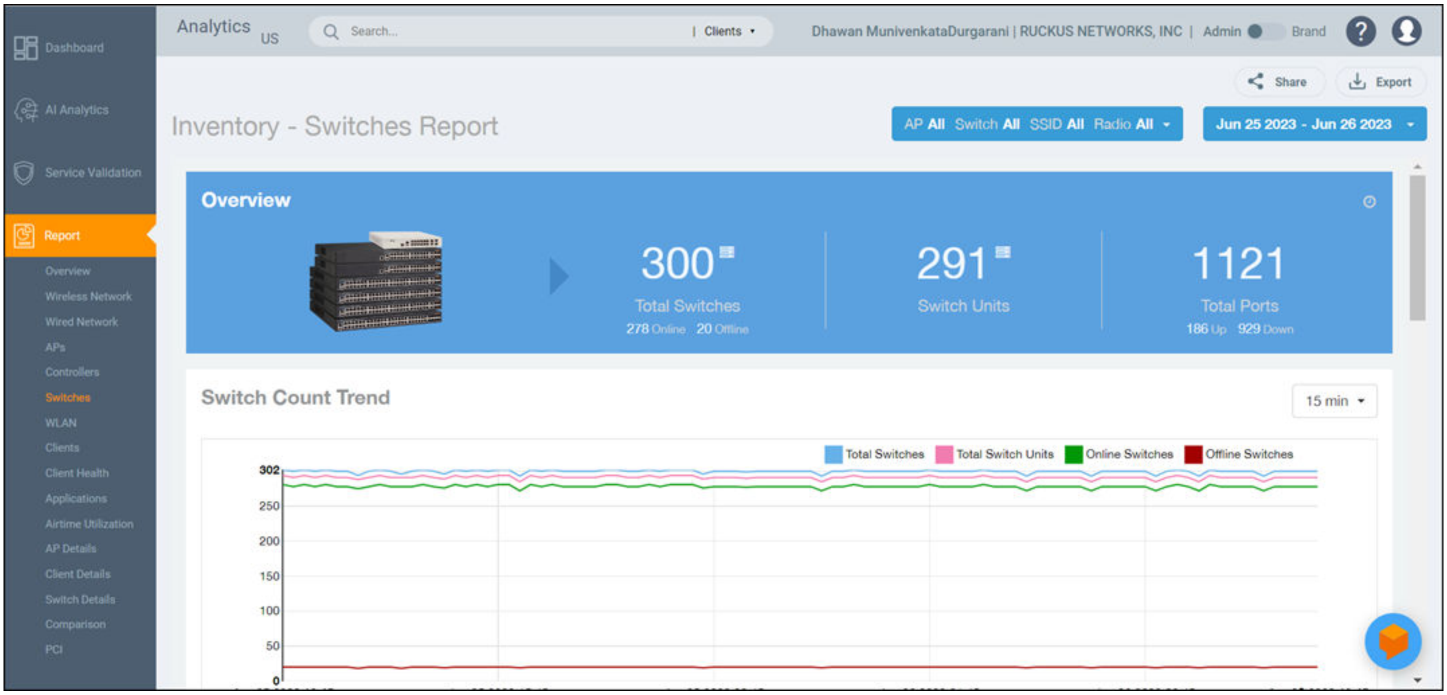
You can follow the recommendations displayed to patch your APs. For information and instructions, refer to: https://support.ruckuswireless.com/krack-ruckus-wireless-support-resource-center.

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 125 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

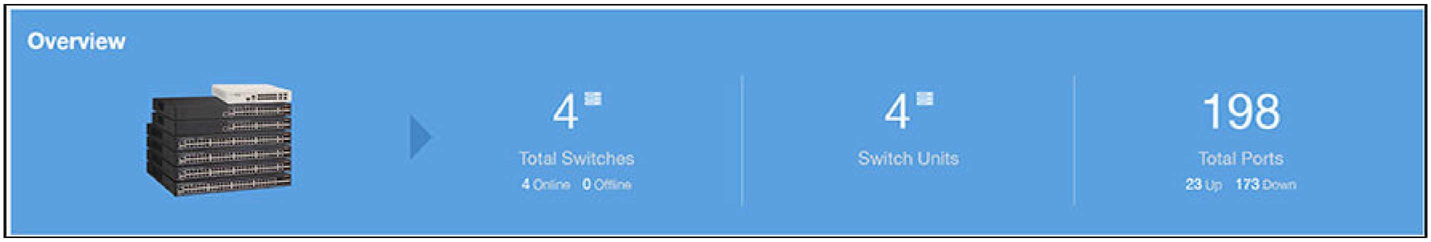
NOTE
All counts in the line graphs, donut charts, and tables of the **Inventory - Switches Report** are exact counts. The counts in trend graphs are approximate.

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 126 Inventory - Switches Report: Overview Tile



Overview

4 Total Switches
4 Online 0 Offline

4 Switch Units

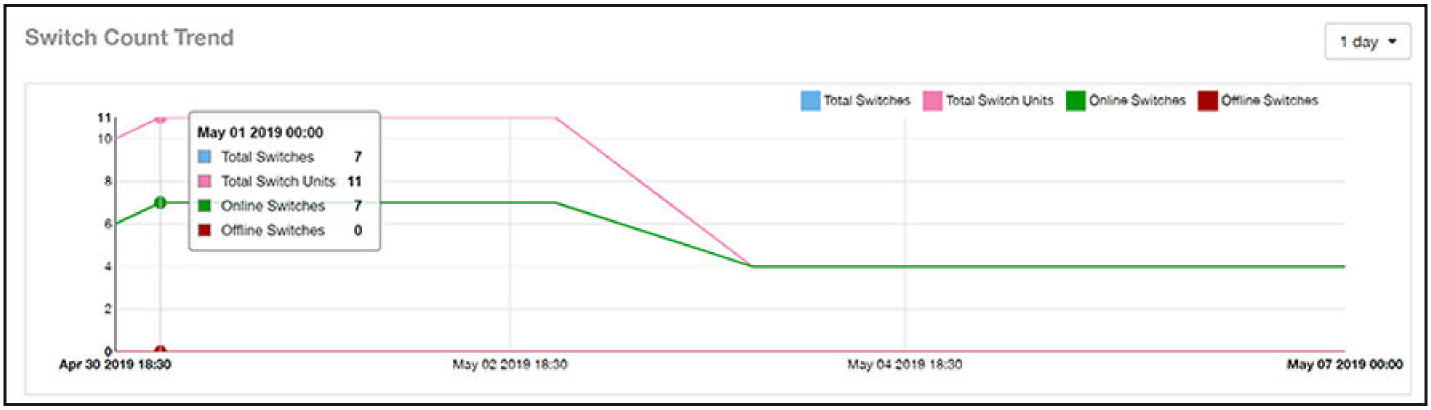
198 Total Ports
23 Up 173 Down

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 127 Inventory - Switches Report: Switch Count Trend Graph



Switch Count Trend

May 01 2019 00:00

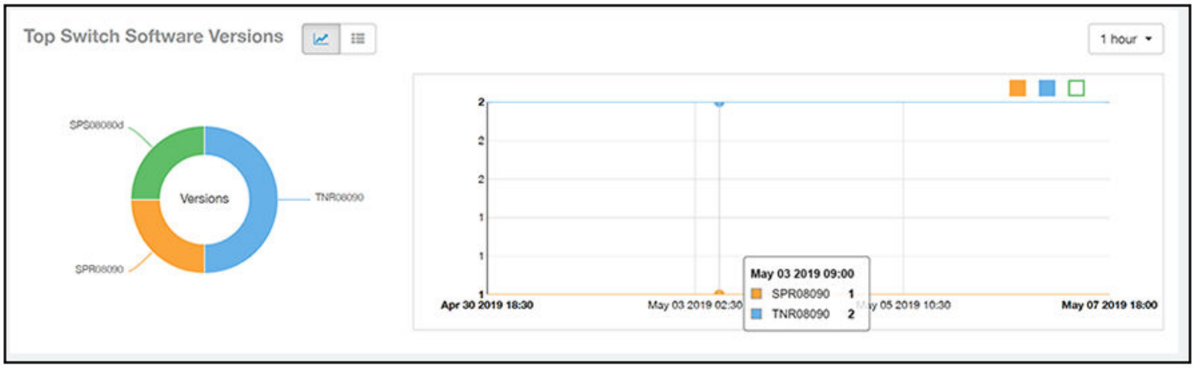
Total Switches	7
Total Switch Units	11
Online Switches	7
Offline Switches	0

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.

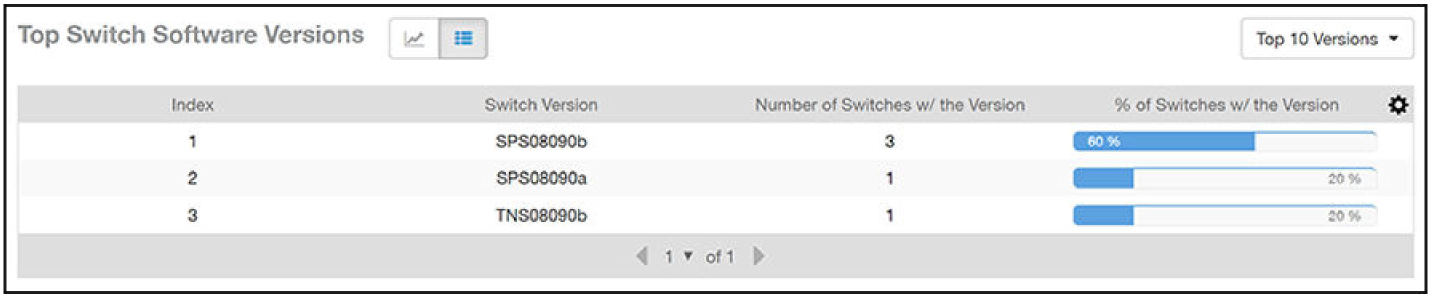
Use the menu to specify the time granularity. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected switch details in the line graph.

FIGURE 128 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 129 Inventory - Switches Report: Top Switch Software Versions Table



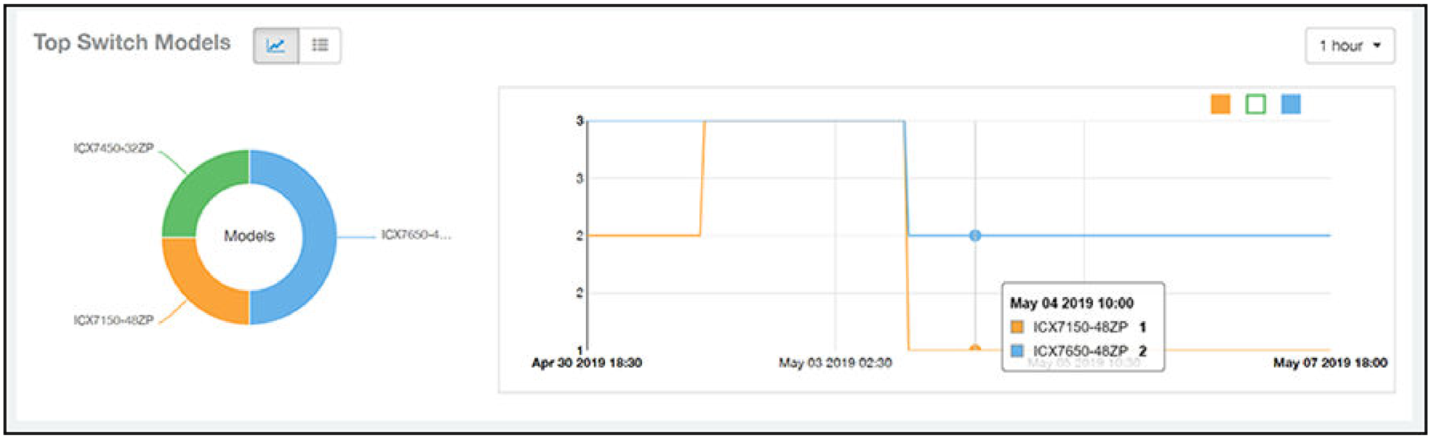
Index	Switch Version	Number of Switches w/ the Version	% of Switches w/ the Version
1	SPS08090b	3	60 %
2	SPS08090a	1	20 %
3	TNS08090b	1	20 %

Top Switch Models Tile

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

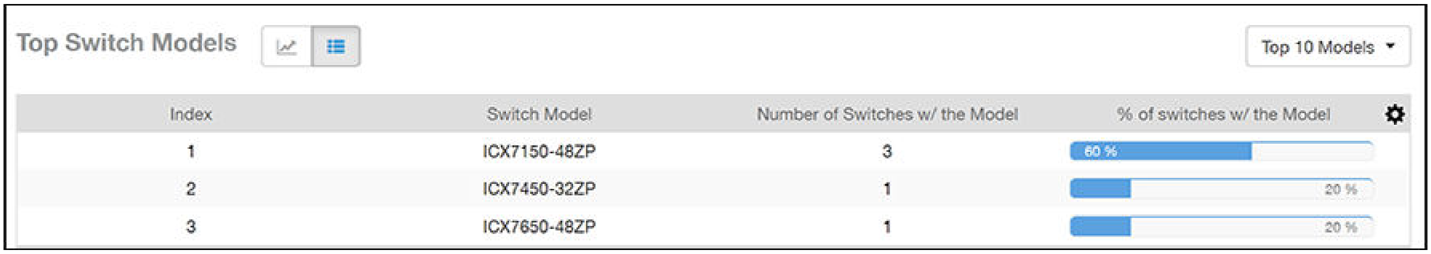
Use the menu to specify the time granularity. If you pause the pointer over the donut chart and the line graph, an information box is displayed containing the details on the selected data points. Click any of the colored squares to display the selected switch details in the line graph.

FIGURE 130 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 131 Inventory - Switches Report: Top Switch Models Table

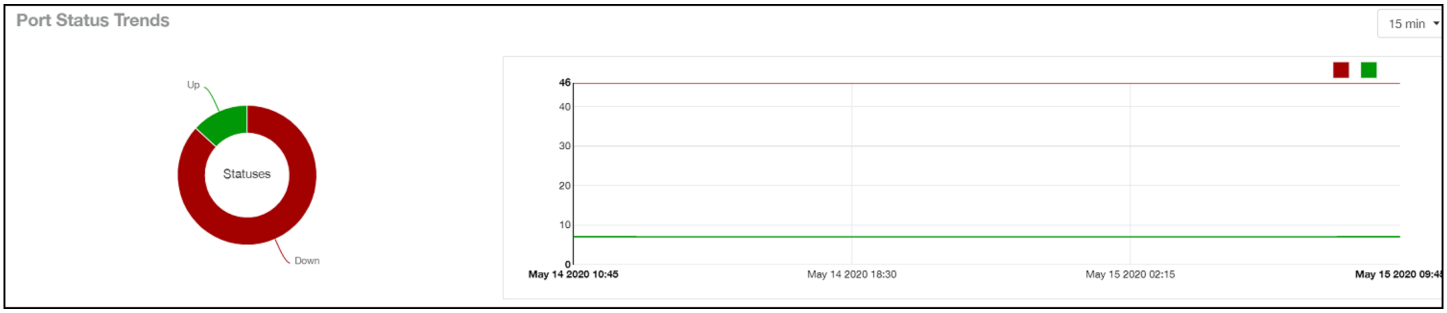


Index	Switch Model	Number of Switches w/ the Model	% of switches w/ the Model
1	ICX7150-48ZP	3	60 %
2	ICX7450-32ZP	1	20 %
3	ICX7650-48ZP	1	20 %

Port Status Trends Tile

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

FIGURE 132 Inventory - Switches Report: Port Status Trends Tile



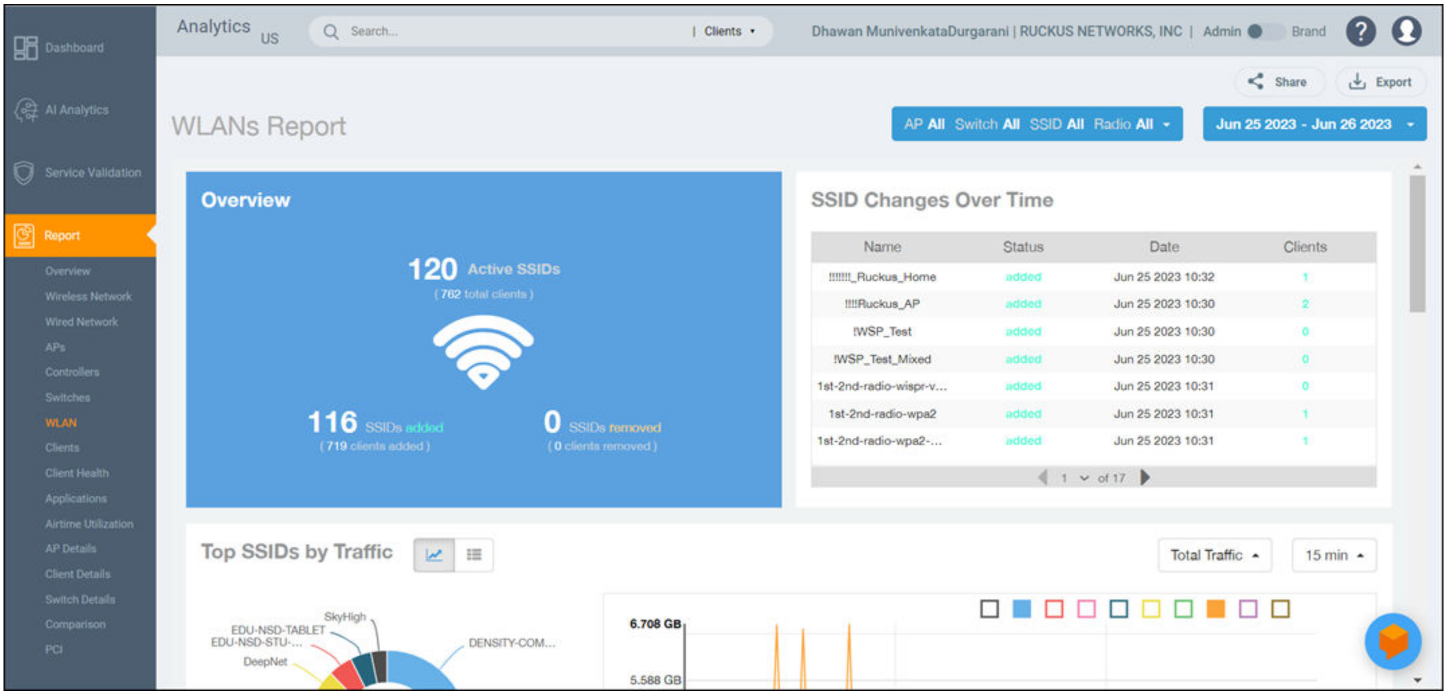
WLAN Report

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 133 WLAN Report (Upper Portion Only)



Name	Status	Date	Clients
!!!!!!_Ruckus_Home	added	Jun 25 2023 10:32	1
!!!!Ruckus_AP	added	Jun 25 2023 10:30	2
!WSP_Test	added	Jun 25 2023 10:30	0
!WSP_Test_Mixed	added	Jun 25 2023 10:30	0
1st-2nd-radio-wispr-v...	added	Jun 25 2023 10:31	0
1st-2nd-radio-wpa2	added	Jun 25 2023 10:31	1
1st-2nd-radio-wpa2-...	added	Jun 25 2023 10:31	1

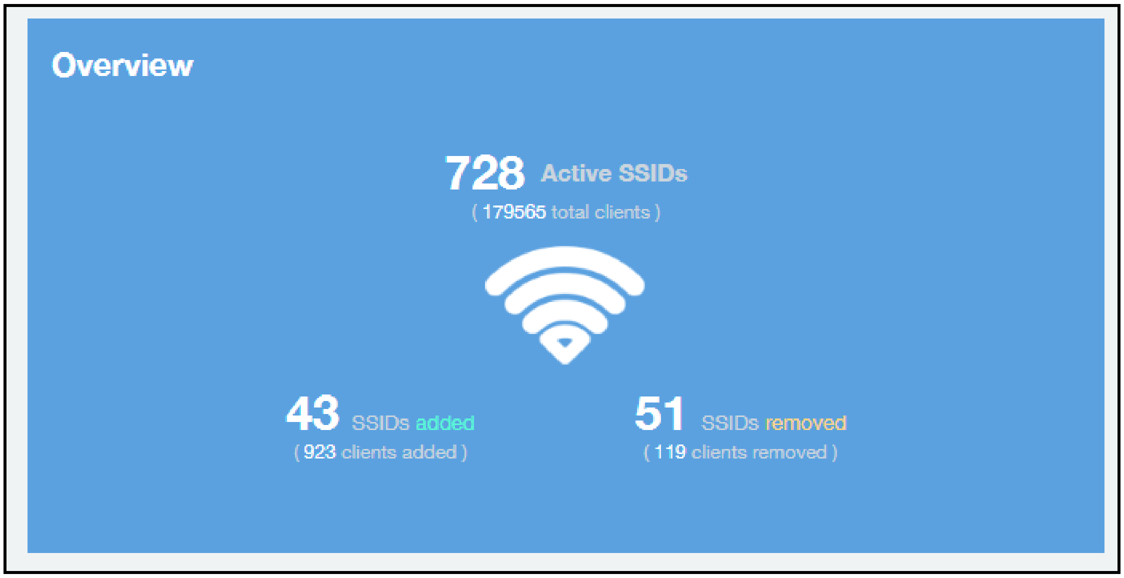
The WLANs Report consists of the following components:

- 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 134 WLAN: Overview Tile



Overview

728 Active SSIDs
(179565 total clients)

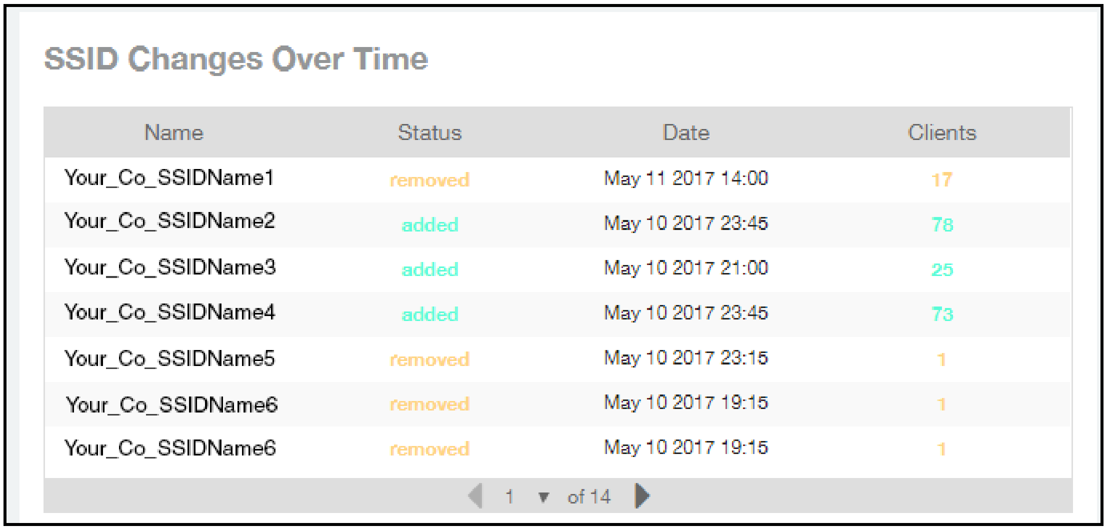
43 SSIDs added
(923 clients added)

51 SSIDs removed
(119 clients removed)

SSID Changes Over Time Tile

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

FIGURE 135 WLAN: SSID Changes Over Time Table



SSID Changes Over Time

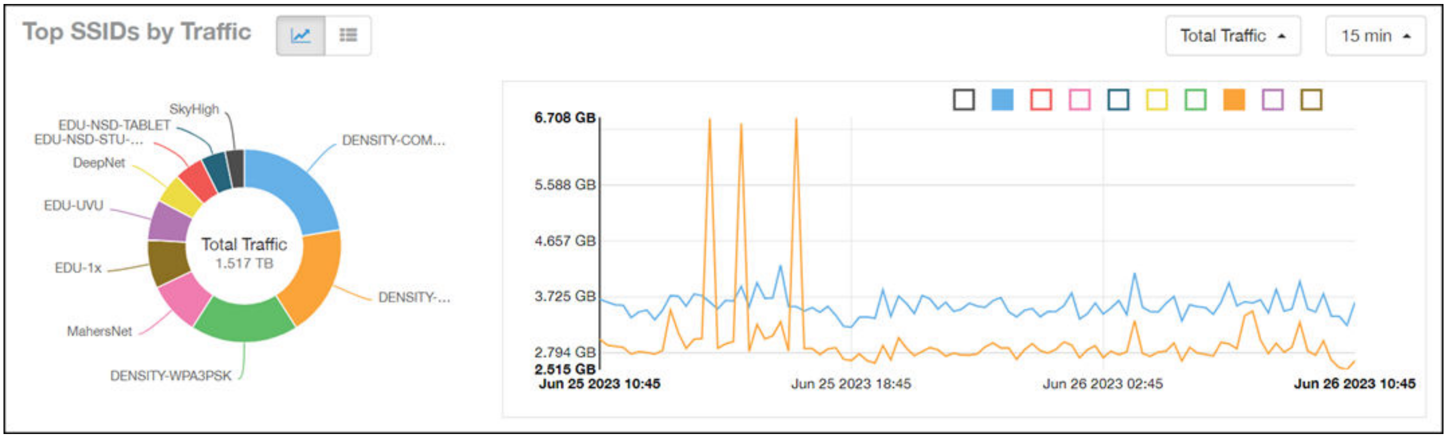
Name	Status	Date	Clients
Your_Co_SSIDName1	removed	May 11 2017 14:00	17
Your_Co_SSIDName2	added	May 10 2017 23:45	78
Your_Co_SSIDName3	added	May 10 2017 21:00	25
Your_Co_SSIDName4	added	May 10 2017 23:45	73
Your_Co_SSIDName5	removed	May 10 2017 23:15	1
Your_Co_SSIDName6	removed	May 10 2017 19:15	1
Your_Co_SSIDName6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

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 136 WLAN: Top SSIDs by Traffic Tile

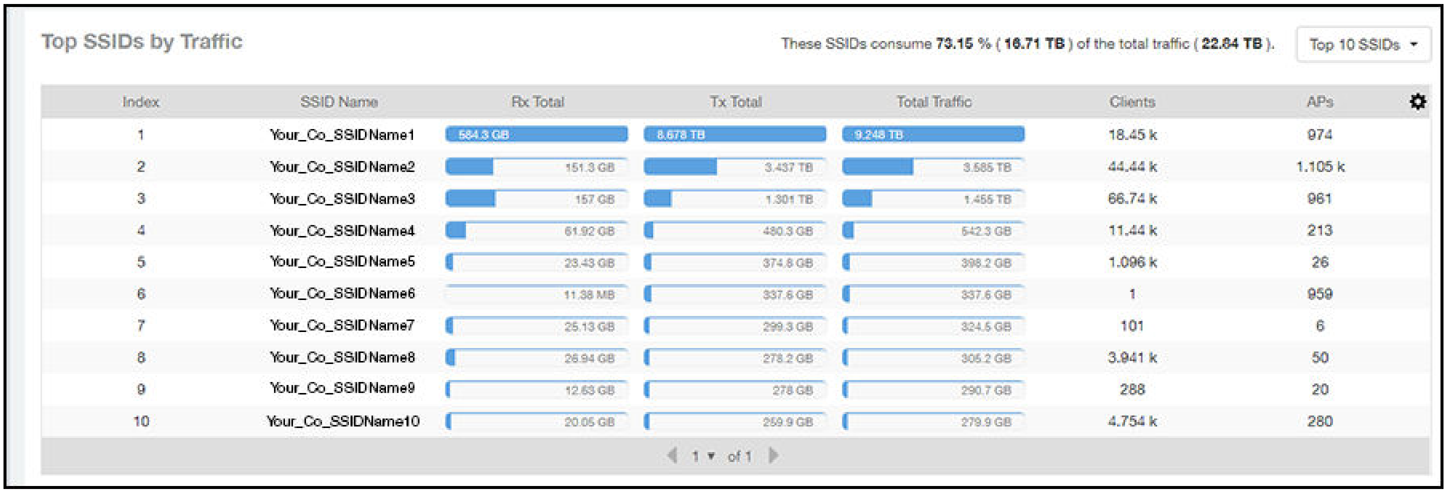


Use the chart and table icons ( ) to toggle between the chart and table views.

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 137 WLAN: Top SSIDs by Traffic (Table)



Top SSIDs by Traffic

These SSIDs consume **73.15 %** (**16.71 TB**) of the total traffic (**22.84 TB**).

Top 10 SSIDs

Index	SSID Name	Rx Total	Tx Total	Total Traffic	Clients	APs
1	Your_Co_SSIDName1	584.3 GB	8.678 TB	9.248 TB	18.45 k	974
2	Your_Co_SSIDName2	151.3 GB	3.437 TB	3.585 TB	44.44 k	1.105 k
3	Your_Co_SSIDName3	157 GB	1.301 TB	1.455 TB	66.74 k	961
4	Your_Co_SSIDName4	61.92 GB	480.3 GB	542.3 GB	11.44 k	213
5	Your_Co_SSIDName5	23.43 GB	374.8 GB	398.2 GB	1.096 k	26
6	Your_Co_SSIDName6	11.38 MB	337.6 GB	337.6 GB	1	959
7	Your_Co_SSIDName7	25.13 GB	299.3 GB	324.5 GB	101	6
8	Your_Co_SSIDName8	26.94 GB	278.2 GB	305.2 GB	3.941 k	50
9	Your_Co_SSIDName9	12.63 GB	278 GB	290.7 GB	288	20
10	Your_Co_SSIDName10	20.05 GB	259.9 GB	279.9 GB	4.754 k	280

1 ▾ of 1

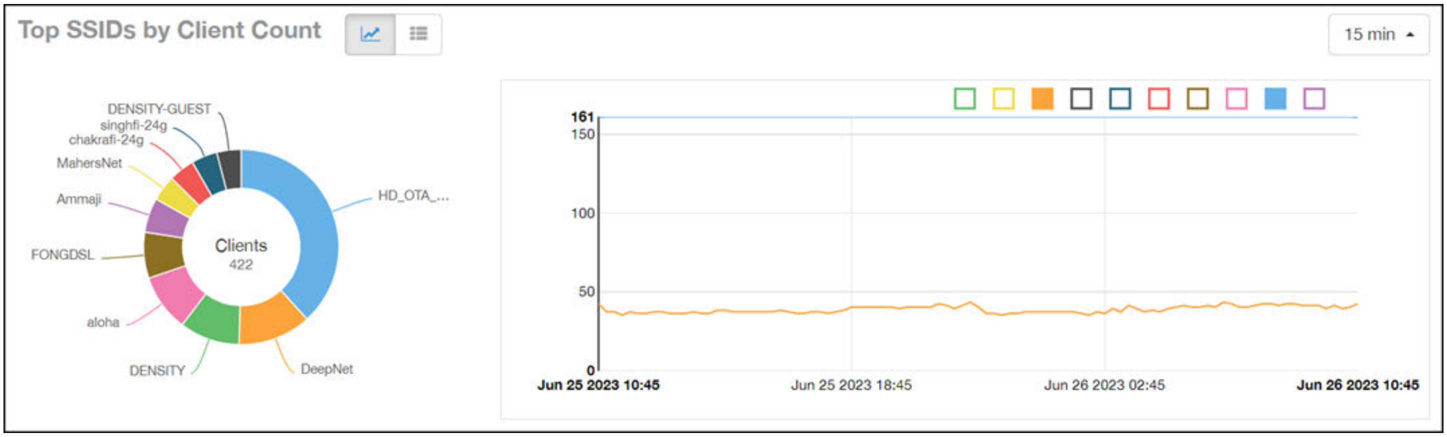
Top SSIDs by Client Count Tile

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 138 WLAN: Top SSIDs by Client Count Tile

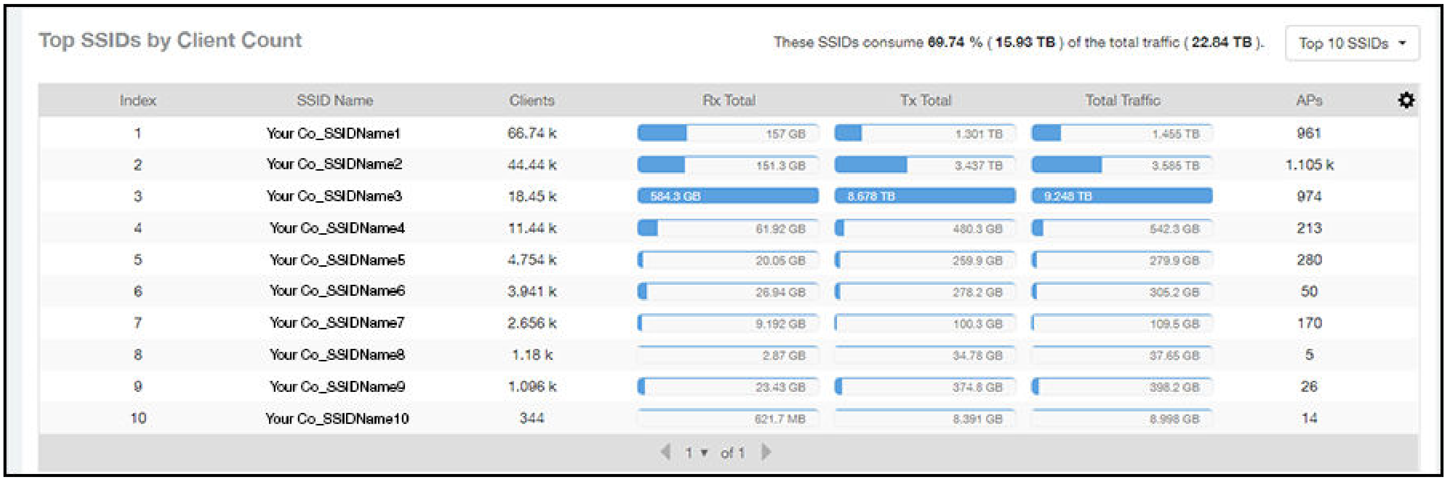


Use the chart and table icons (📈 ☰) to toggle between the chart and table views.

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 139 WLAN: Top SSIDs by Client Count (Table)



Top SSIDs by Client Count

These SSIDs consume **69.74** % (**15.93 TB**) of the total traffic (**22.84 TB**).

Top 10 SSIDs ▾

Index	SSID Name	Clients	Rx Total	Tx Total	Total Traffic	APs
1	Your Co_SSIDName1	66.74 k	157 GB	1.301 TB	1.455 TB	961
2	Your Co_SSIDName2	44.44 k	151.3 GB	3.437 TB	3.585 TB	1.105 k
3	Your Co_SSIDName3	18.45 k	584.3 GB	8.678 TB	9.248 TB	974
4	Your Co_SSIDName4	11.44 k	61.92 GB	480.3 GB	542.3 GB	213
5	Your Co_SSIDName5	4.754 k	20.05 GB	259.9 GB	279.9 GB	280
6	Your Co_SSIDName6	3.941 k	26.94 GB	278.2 GB	305.2 GB	50
7	Your Co_SSIDName7	2.656 k	9.192 GB	100.3 GB	109.5 GB	170
8	Your Co_SSIDName8	1.18 k	2.87 GB	34.78 GB	37.65 GB	5
9	Your Co_SSIDName9	1.096 k	23.43 GB	374.8 GB	398.2 GB	26
10	Your Co_SSIDName10	344	621.7 MB	8.391 GB	8.998 GB	14

1 ▾ of 1

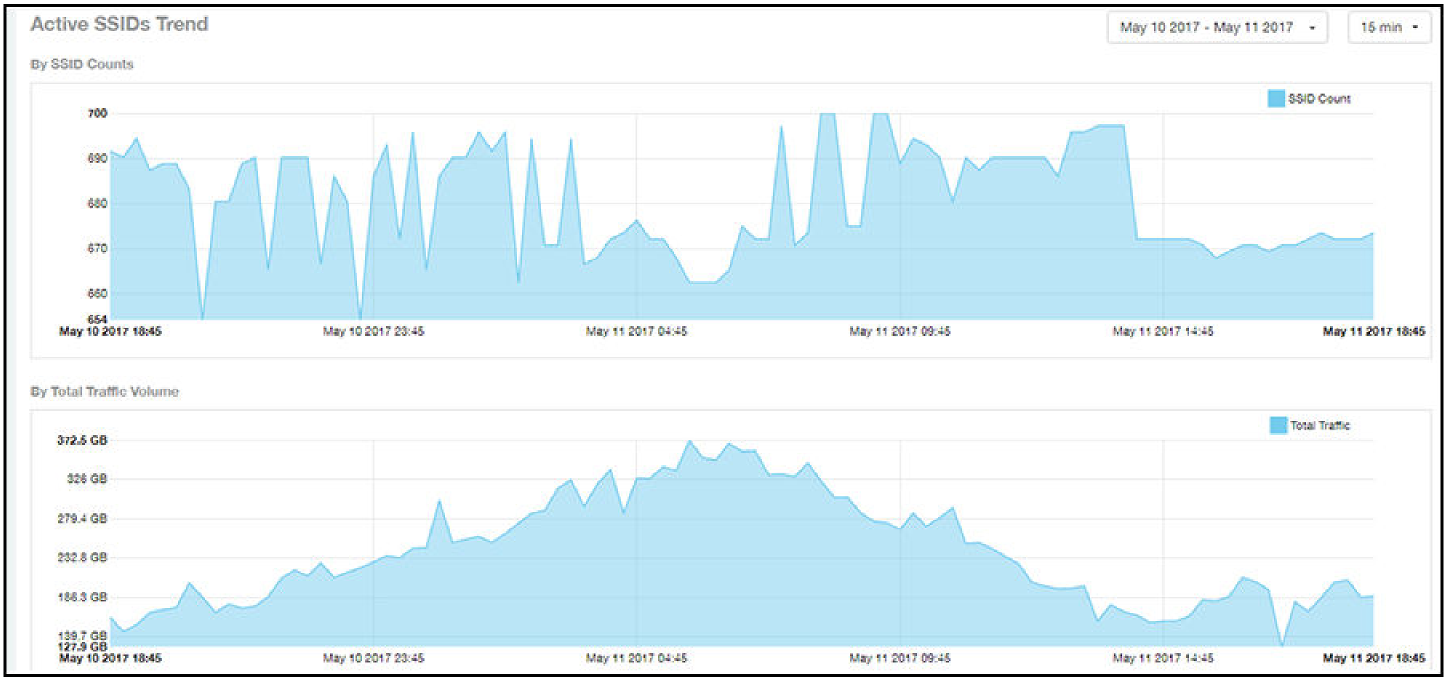
Active SSIDs Trend Graphs

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 140 WLAN: Active SSIDs Trend Graphs



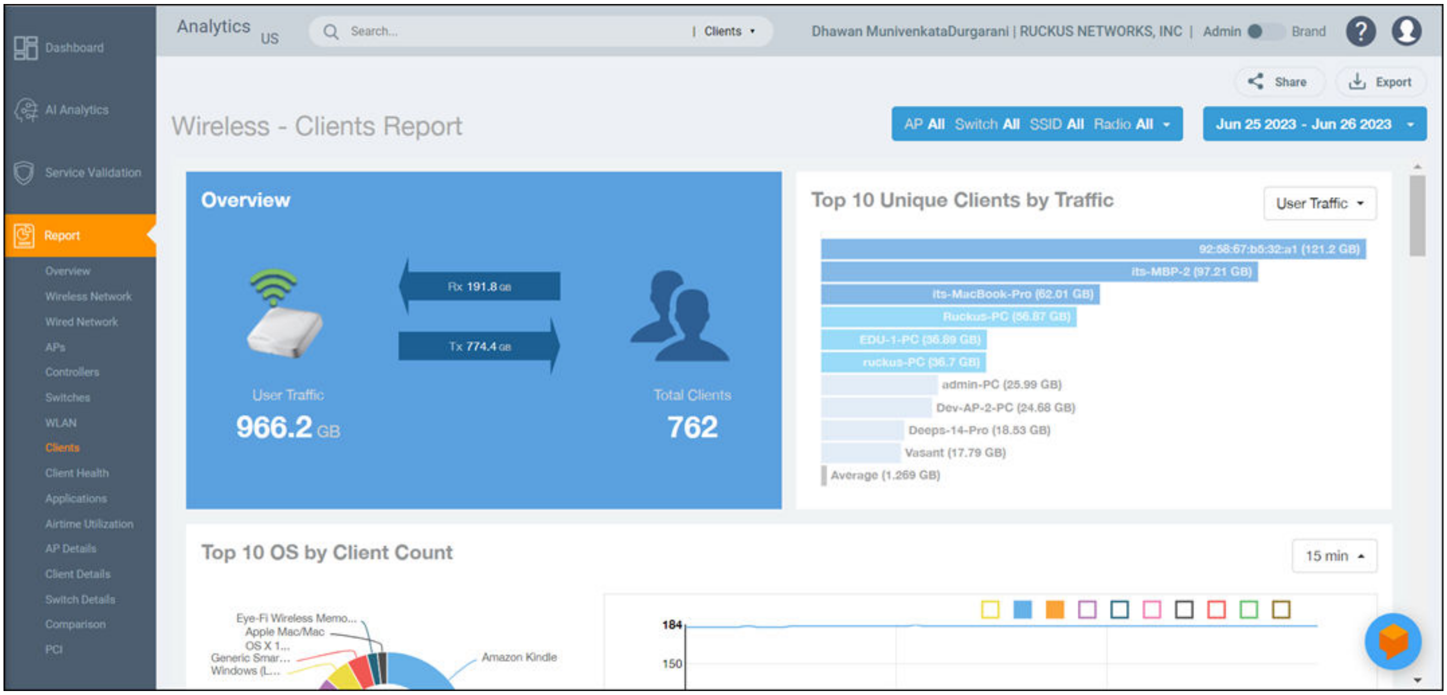
Clients Report

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 141 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

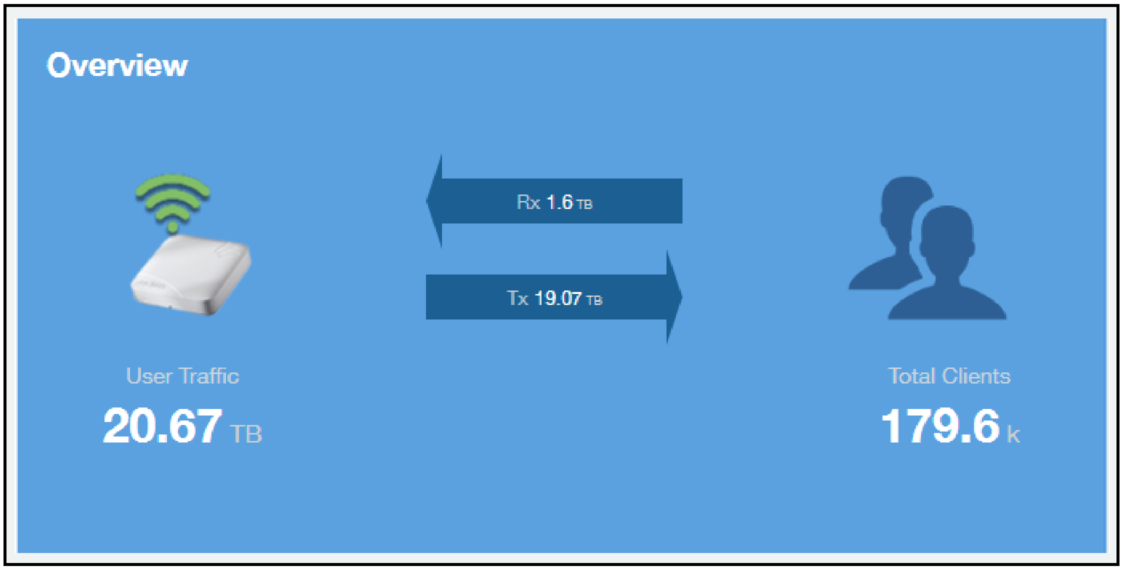
Overview Tile

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

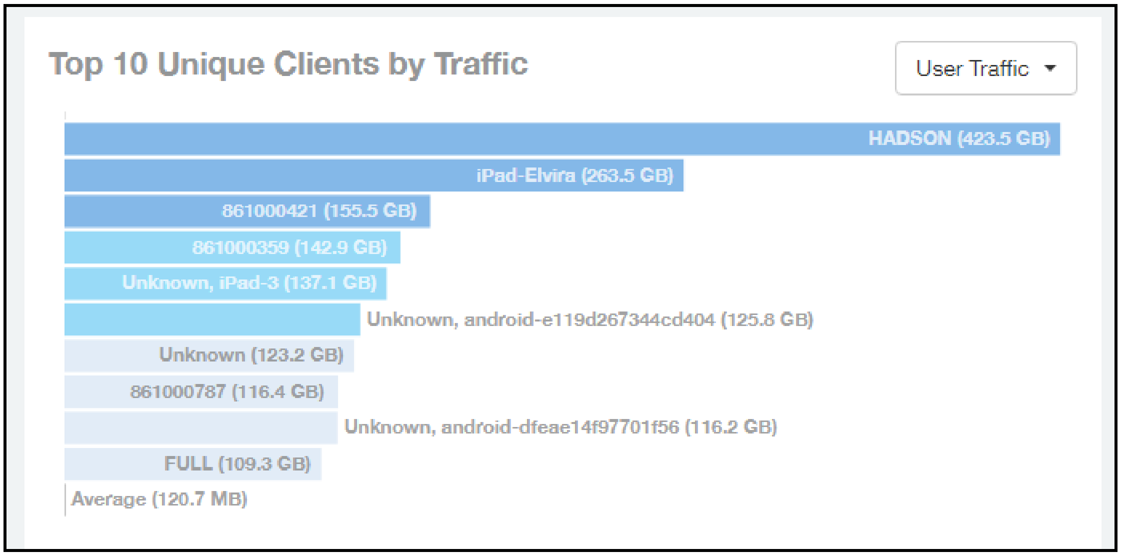
FIGURE 142 Clients: Overview Tile



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 143 Clients: Top 10 Unique Clients by Traffic

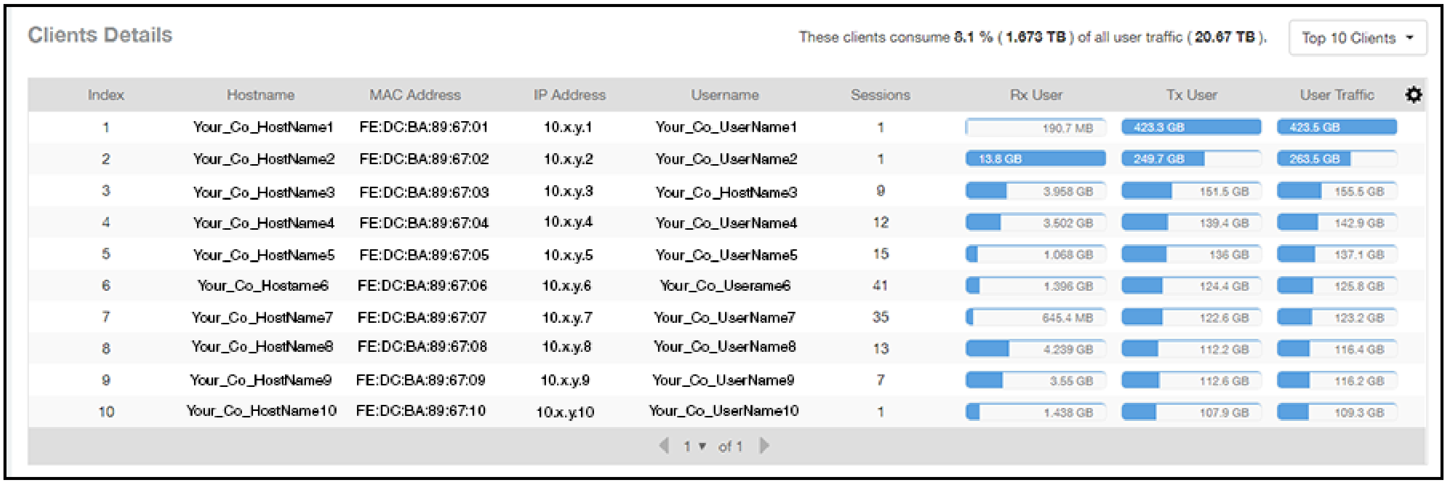


Clients Details

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 144 Clients: Clients Details Table



Clients Details

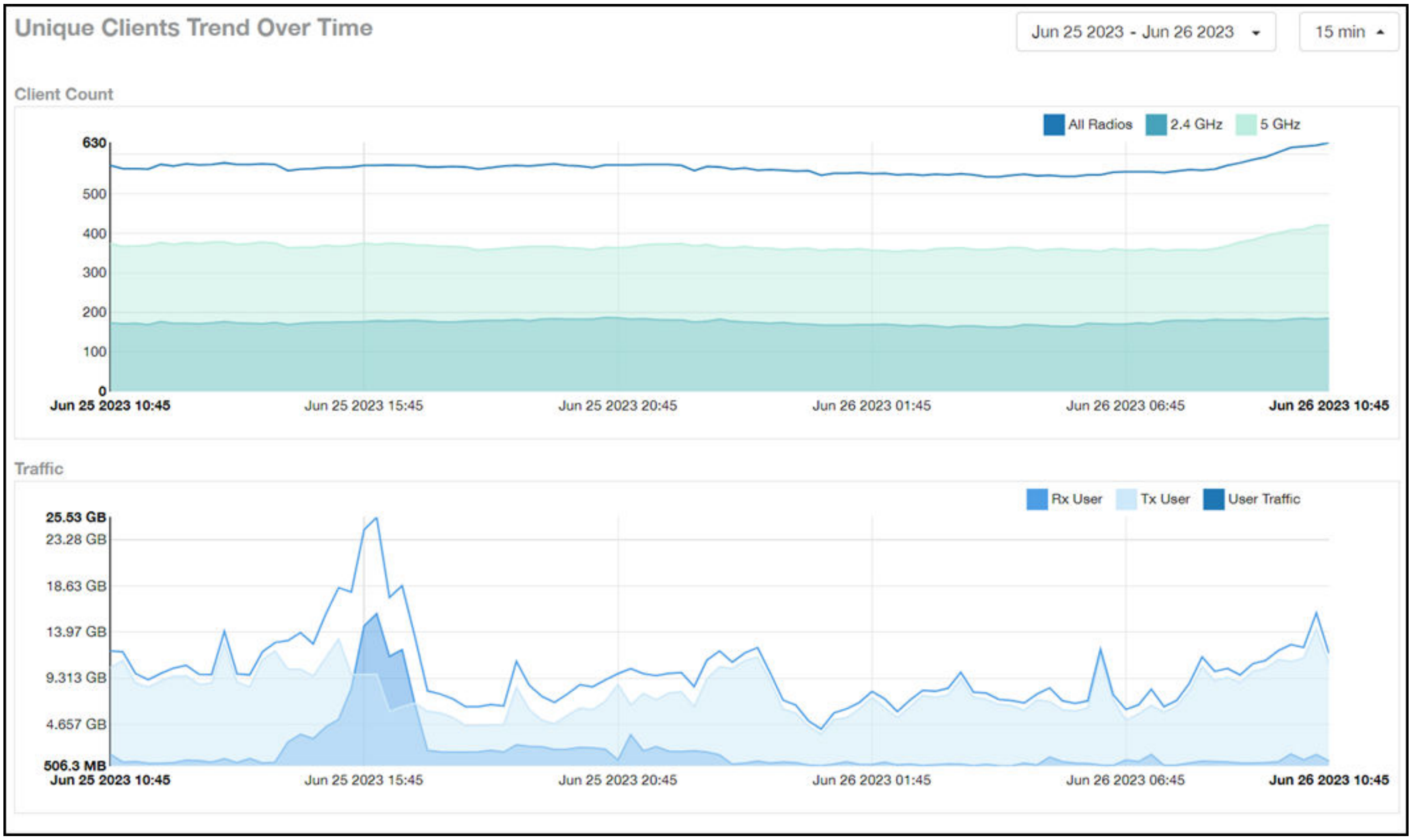
These clients consume **8.1 %** (**1.673 TB**) of all user traffic (**20.67 TB**).

Index	Hostname	MAC Address	IP Address	Username	Sessions	Rx User	Tx User	User Traffic
1	Your_Co_HostName1	FE:DC:BA:89:67:01	10.x.y.1	Your_Co_UserName1	1	190.7 MB	423.3 GB	423.5 GB
2	Your_Co_HostName2	FE:DC:BA:89:67:02	10.x.y.2	Your_Co_UserName2	1	13.8 GB	249.7 GB	263.5 GB
3	Your_Co_HostName3	FE:DC:BA:89:67:03	10.x.y.3	Your_Co_HostName3	9	3.958 GB	151.5 GB	155.5 GB
4	Your_Co_HostName4	FE:DC:BA:89:67:04	10.x.y.4	Your_Co_UserName4	12	3.502 GB	139.4 GB	142.9 GB
5	Your_Co_HostName5	FE:DC:BA:89:67:05	10.x.y.5	Your_Co_UserName5	15	1.068 GB	136 GB	137.1 GB
6	Your_Co_Hostame6	FE:DC:BA:89:67:06	10.x.y.6	Your_Co_Userame6	41	1.396 GB	124.4 GB	125.8 GB
7	Your_Co_HostName7	FE:DC:BA:89:67:07	10.x.y.7	Your_Co_UserName7	35	645.4 MB	122.6 GB	123.2 GB
8	Your_Co_HostName8	FE:DC:BA:89:67:08	10.x.y.8	Your_Co_UserName8	13	4.239 GB	112.2 GB	116.4 GB
9	Your_Co_HostName9	FE:DC:BA:89:67:09	10.x.y.9	Your_Co_UserName9	7	3.55 GB	112.6 GB	116.2 GB
10	Your_Co_HostName10	FE:DC:BA:89:67:10	10.x.y.10	Your_Co_UserName10	1	1.438 GB	107.9 GB	109.3 GB

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.

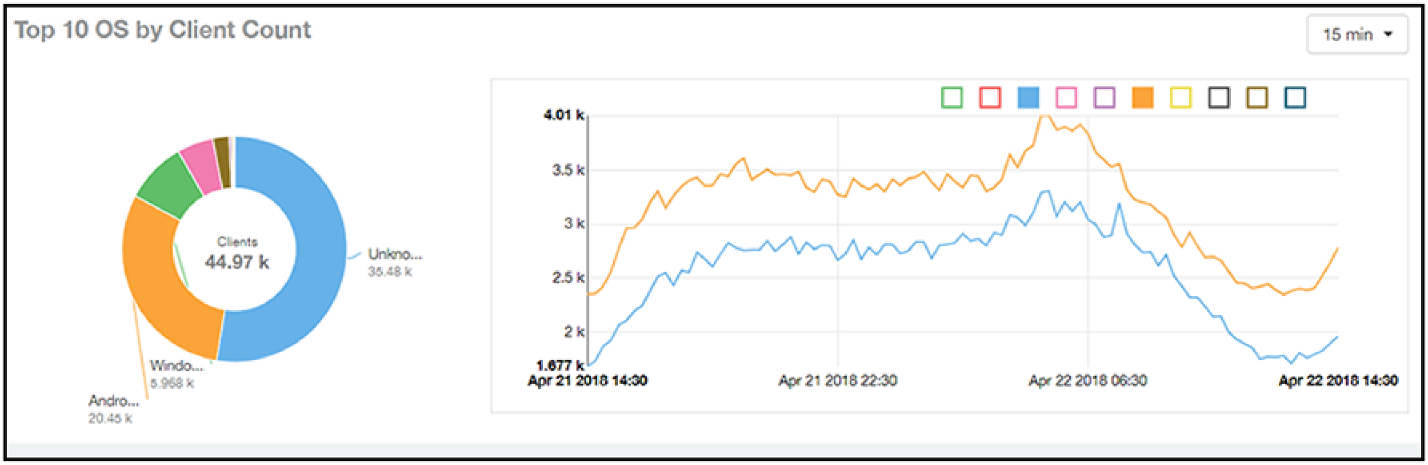
FIGURE 145 Clients: Unique Clients Trend Over Time Graph



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.

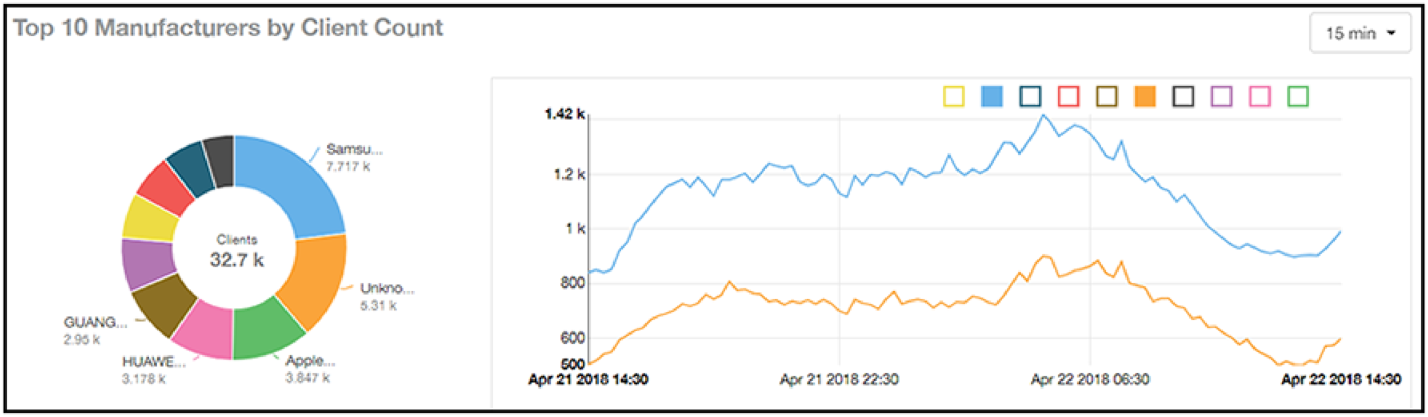
FIGURE 146 Clients: Top 10 OS by Client Count Tile



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.

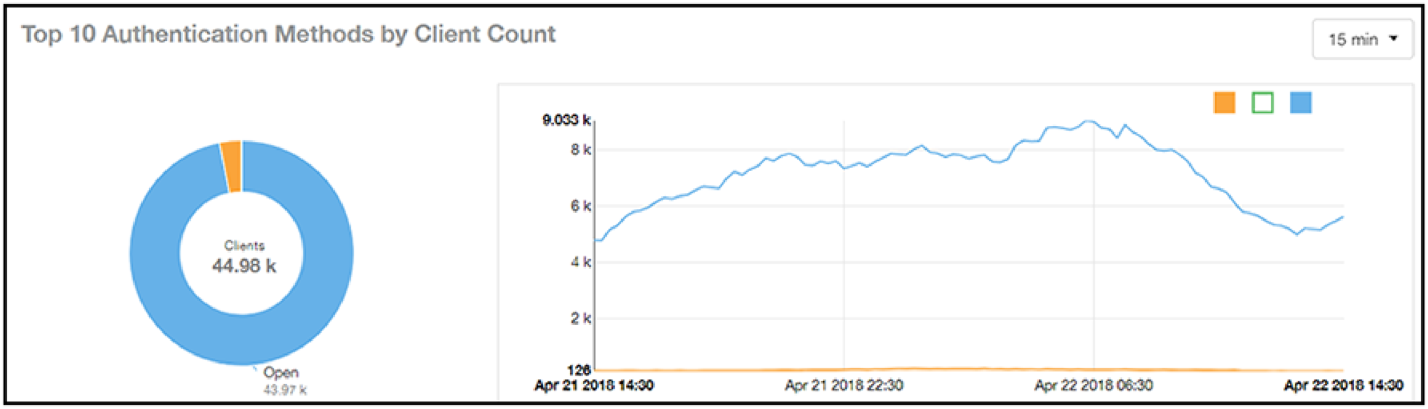
FIGURE 147 Clients: Top 10 Manufacturers by Client Count Tile



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 148 Clients - Top 10 Authentication Methods by Client Count Tile



Client Health Dashboard

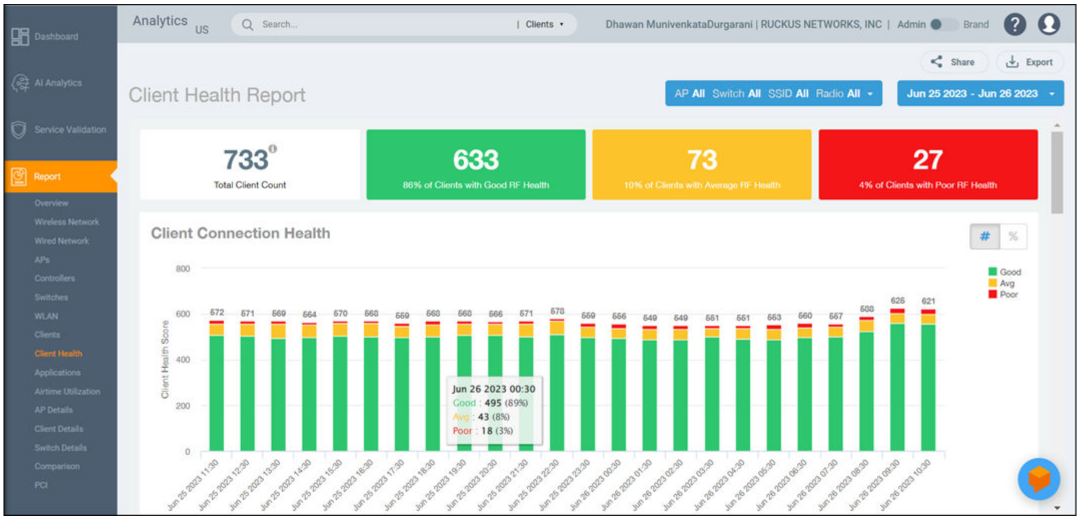
Client Health Report

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 149 Client Health Report (Upper Portion Only)



Client Health Report

733 Total Client Count

633 86% of Clients with Good RF Health

73 10% of Clients with Average RF Health

27 4% of Clients with Poor RF Health

Client Connection Health

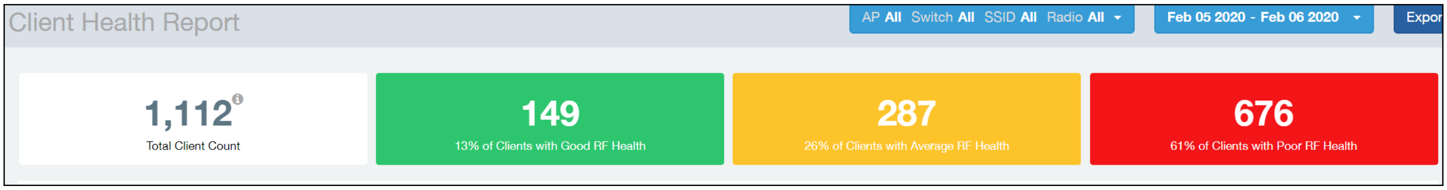
Jun 26 2023 00:30
Good : 495 (89%)
Avg : 43 (8%)
Poor : 18 (3%)

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.



Client Health Report

AP **All** Switch **All** SSID **All** Radio **All**

Feb 05 2020 - Feb 06 2020

Expor

1,112
Total Client Count

149
13% of Clients with Good RF Health

287
26% of Clients with Average RF Health

676
61% of Clients with Poor RF Health

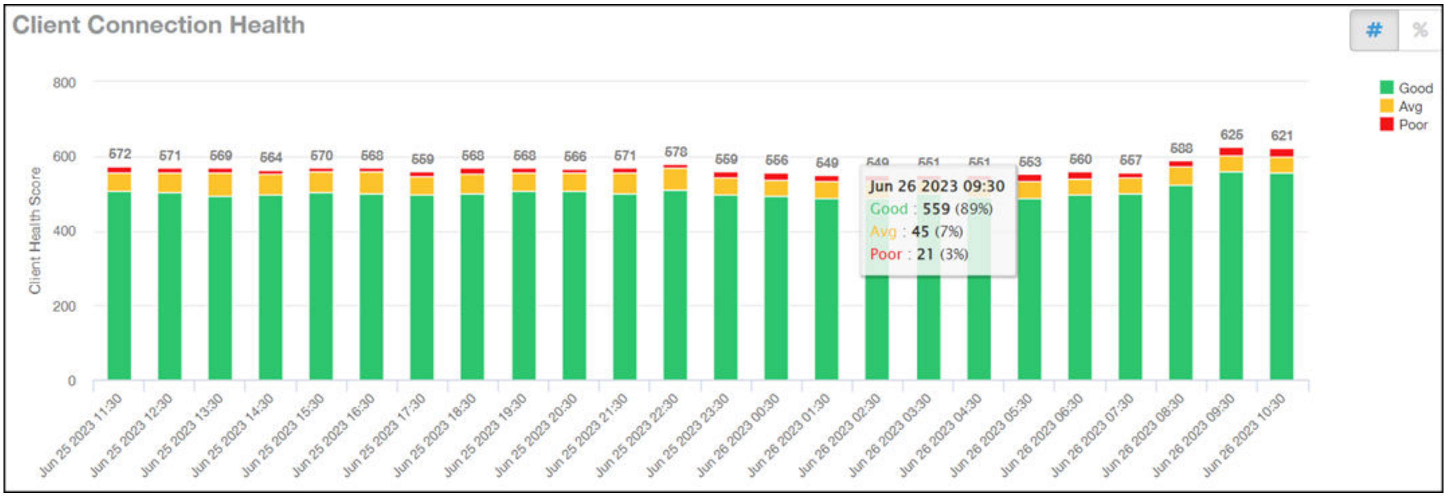
The green box shows the number of clients with good RF health. The yellow box shows the number fo clients with average RF health and the red box displays the number of clients with poor RF heath. The numbers are determined by the threshold that you set as per your expectations of client health in the 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 150 Client Health Score: Client Connection Health

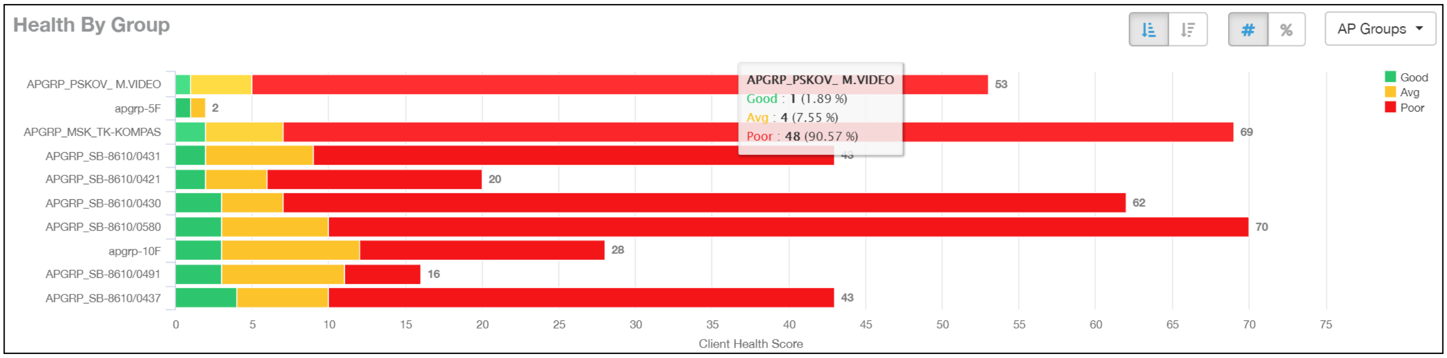


You can toggle the boxes on and off to display or not display clients classified by their score. For example, to only view the clients with a good score, you can disable the yellow and red boxes; you will only see the clients with a good RF health in the graph.

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 151 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.

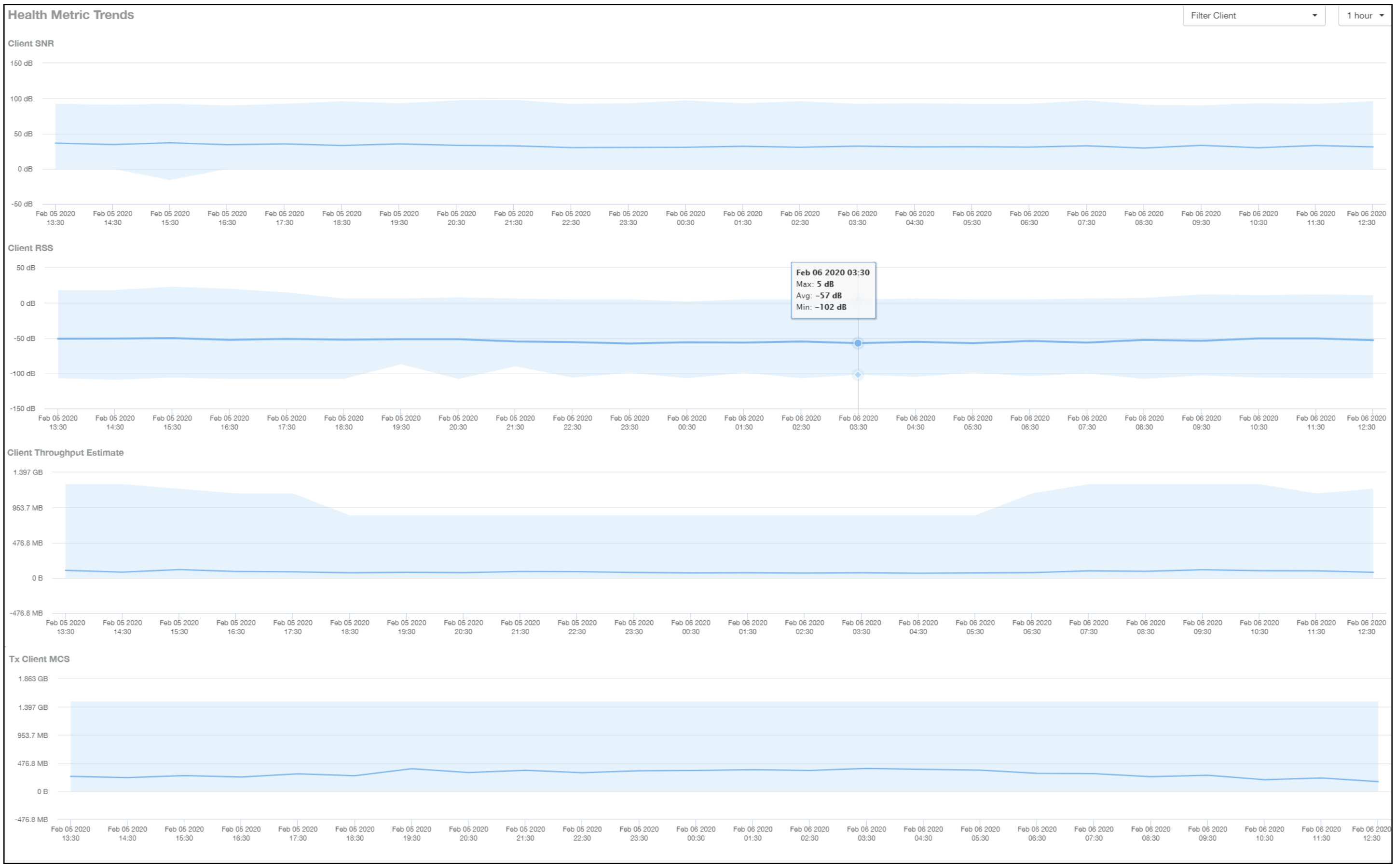
The ascending and descending order icons sort the groups as groups with highest percentage or count of good clients, and highest percentage or count of poor clients, respectively.

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 152 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.

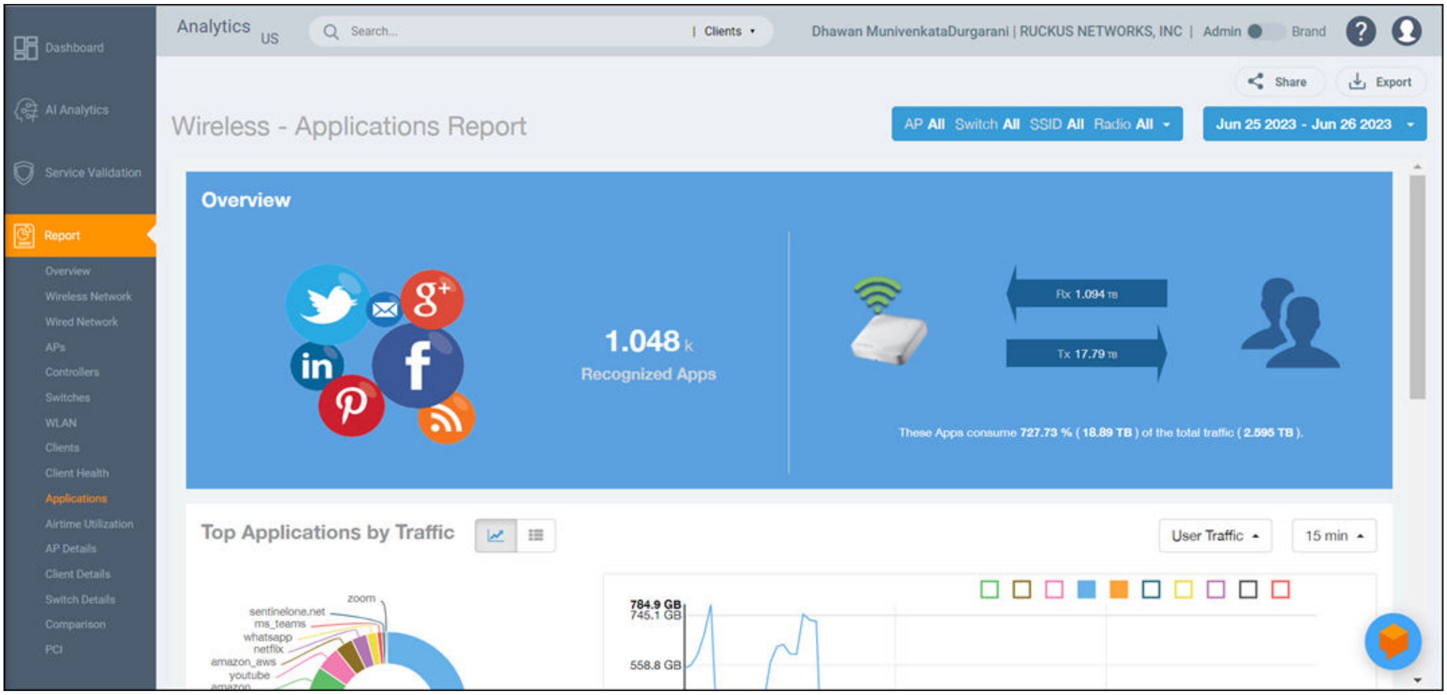
Applications Report

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 153 Applications Dashboard (Upper Portion Only)



Wireless - Applications Report

AP All Switch All SSID All Radio All

Jun 25 2023 - Jun 26 2023

1.048 k Recognized Apps

These Apps consume 727.73 % (18.89 TB) of the total traffic (2.595 TB).

User Traffic

15 min

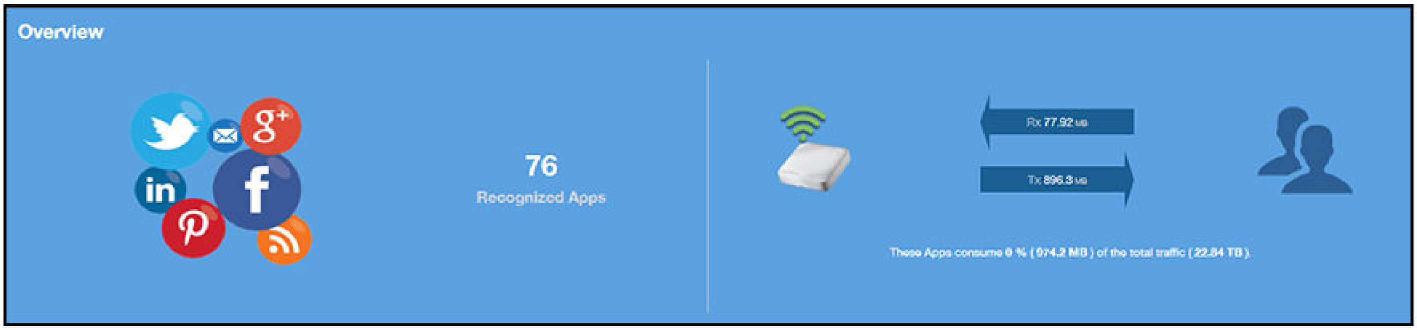
Overview Tile

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 154 Applications: Overview Tile



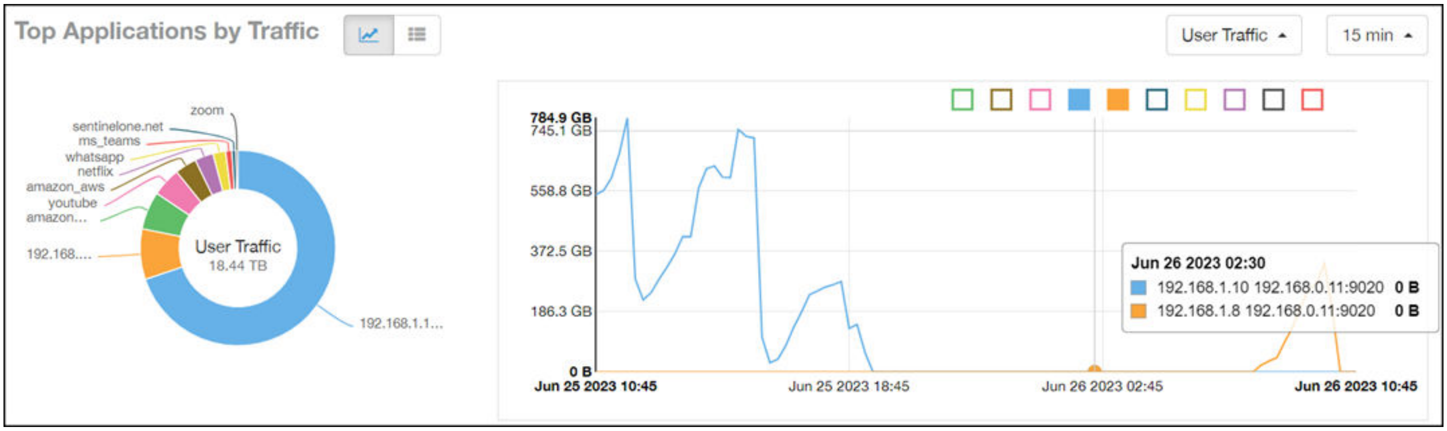
76 Recognized Apps

These Apps consume 0 % (974.2 MB) of the total traffic (22.84 TB).

Top Applications by Traffic

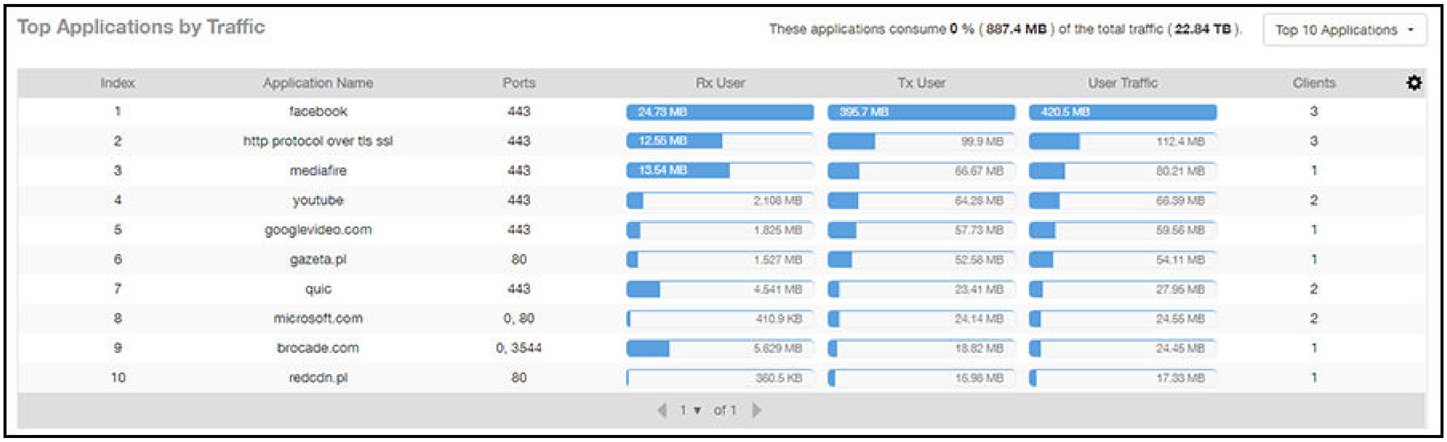
The **Top Applications by Traffic** donut chart and graph of the **Applications Report** display the top applications with the largest traffic in the network, along with the received and transmitted traffic.

FIGURE 155 Applications: Top Applications by Traffic Tile



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

FIGURE 156 Applications: Top Applications by Traffic Table



Top Applications by Traffic

These applications consume **0** % (**887.4 MB**) of the total traffic (**22.84 TB**).

Top 10 Applications

Index	Application Name	Ports	Rx User	Tx User	User Traffic	Clients
1	facebook	443	24.73 MB	395.7 MB	420.5 MB	3
2	http protocol over tls ssl	443	12.55 MB	99.9 MB	112.4 MB	3
3	mediafire	443	13.54 MB	66.67 MB	80.21 MB	1
4	youtube	443	2.108 MB	64.28 MB	66.39 MB	2
5	googlevideo.com	443	1.825 MB	57.73 MB	59.56 MB	1
6	gazeta.pl	80	1.527 MB	52.58 MB	54.11 MB	1
7	quic	443	4.541 MB	23.41 MB	27.95 MB	2
8	microsoft.com	0, 80	410.9 KB	24.14 MB	24.55 MB	2
9	brocade.com	0, 3544	5.629 MB	18.82 MB	24.45 MB	1
10	redcdn.pl	80	360.5 KB	16.98 MB	17.33 MB	1

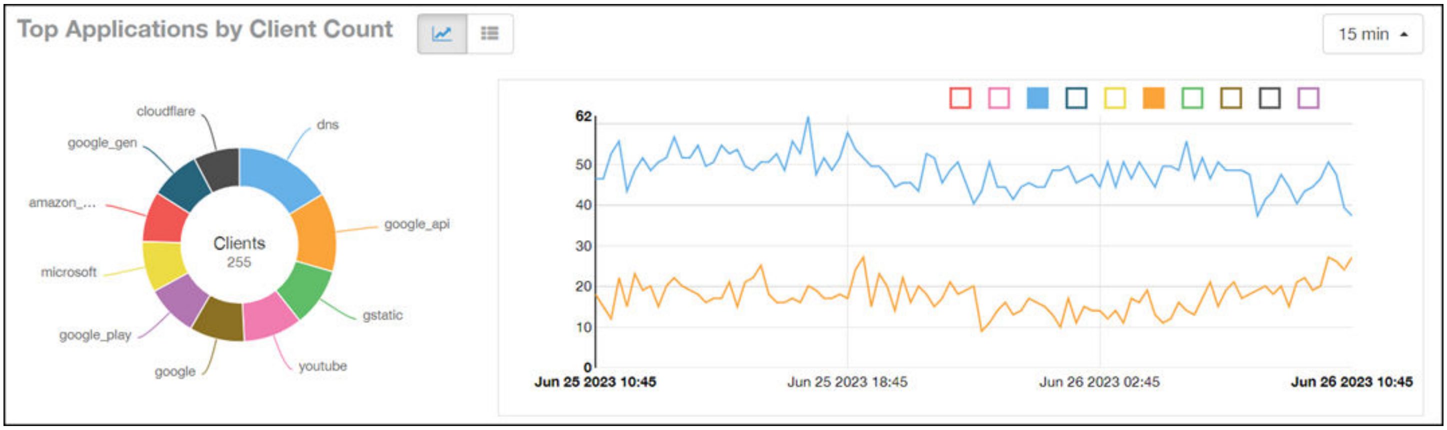
1 ▾ of 1

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 157 Applications - Top Applications by Client Count (chart)

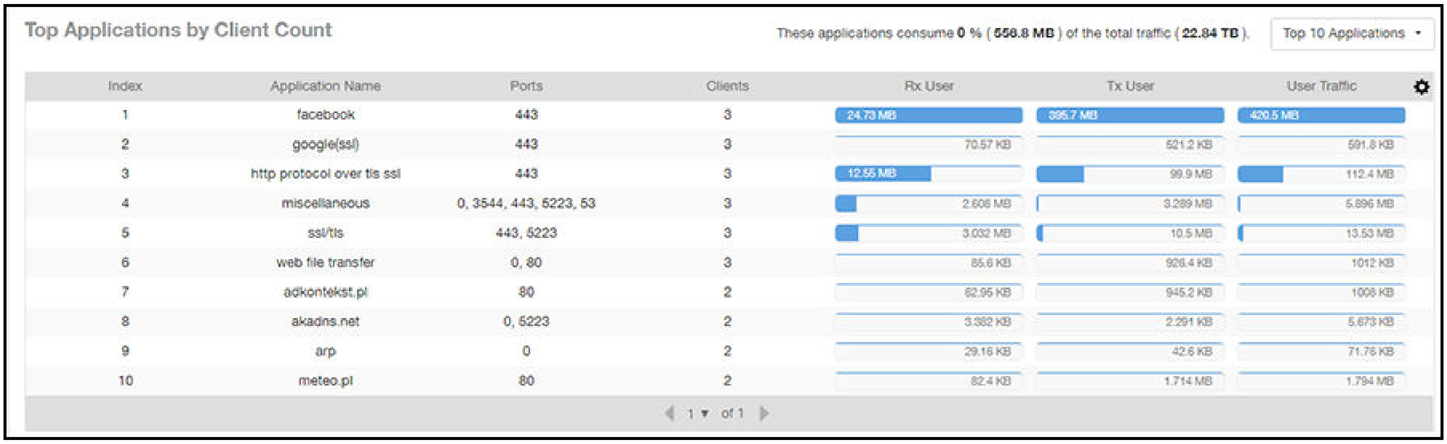


Use the chart and table icons (📈 ☰) to toggle between the chart and table views.

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 158 Applications: Top Applications by Client Count Table



Top Applications by Client Count

These applications consume **0** % (**556.8 MB**) of the total traffic (**22.84 TB**).

Top 10 Applications ▾

Index	Application Name	Ports	Clients	Rx User	Tx User	User Traffic
1	facebook	443	3	24.73 MB	395.7 MB	420.5 MB
2	google(ssl)	443	3	70.57 KB	521.2 KB	591.8 KB
3	http protocol over tls ssl	443	3	12.55 MB	99.9 MB	112.4 MB
4	miscellaneous	0, 3544, 443, 5223, 53	3	2.608 MB	3.289 MB	5.896 MB
5	ssl/tls	443, 5223	3	3.032 MB	10.5 MB	13.53 MB
6	web file transfer	0, 80	3	85.6 KB	926.4 KB	1012 KB
7	adkontekst.pl	80	2	62.95 KB	945.2 KB	1008 KB
8	akadns.net	0, 5223	2	3.382 KB	2.291 KB	5.673 KB
9	arp	0	2	29.16 KB	42.6 KB	71.76 KB
10	meteo.pl	80	2	82.4 KB	1.714 MB	1.794 MB

1 ▾ of 1

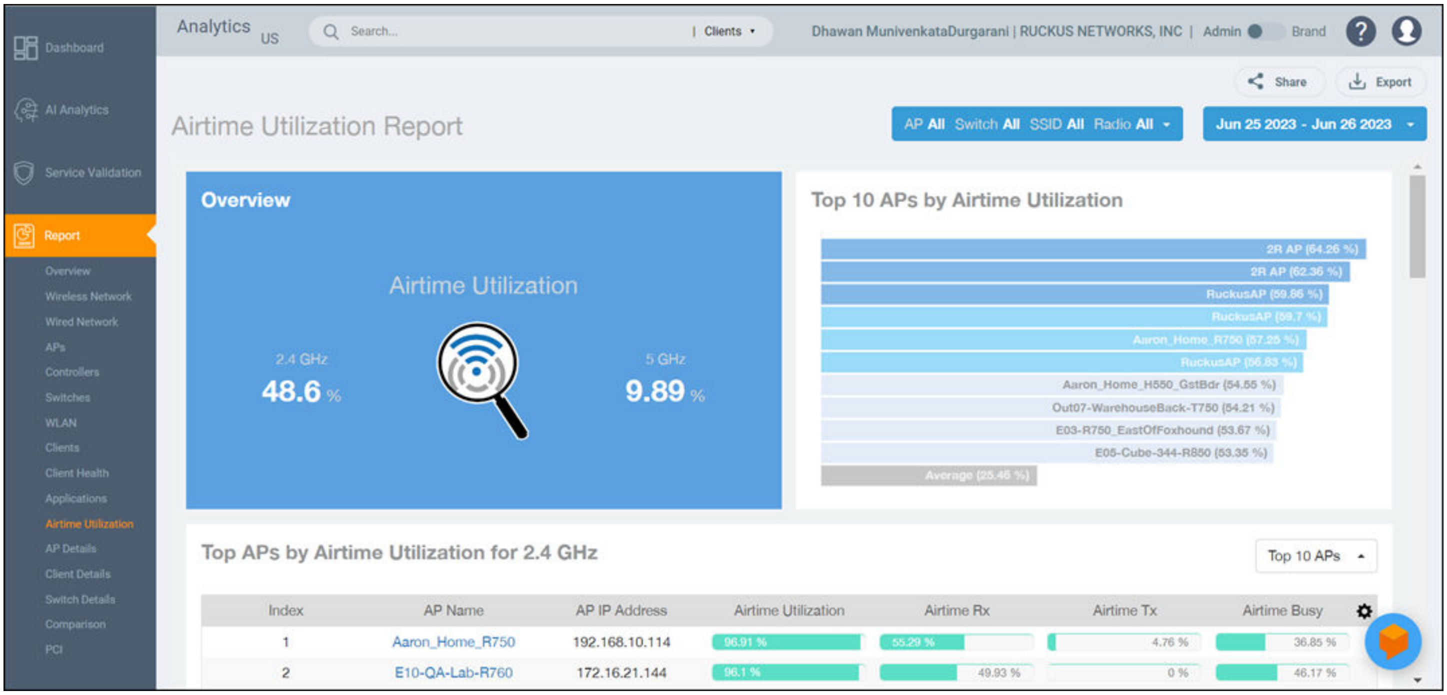
Airtime Utilization Report

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

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

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

FIGURE 159 Airtime Utilization Report (Upper Portion Only)



Index	AP Name	AP IP Address	Airtime Utilization	Airtime Rx	Airtime Tx	Airtime Busy
1	Aaron_Home_R750	192.168.10.114	96.91 %	55.29 %	4.76 %	36.85 %
2	E10-QA-Lab-R760	172.16.21.144	96.1 %	49.93 %	0 %	46.17 %

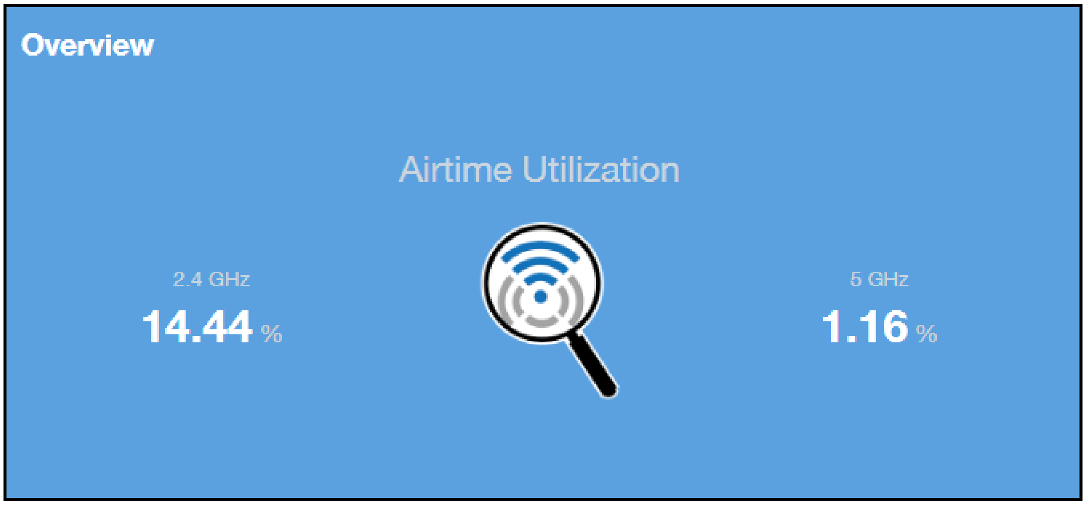
The Airtime Utilization Report consists of the following components:

- 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.

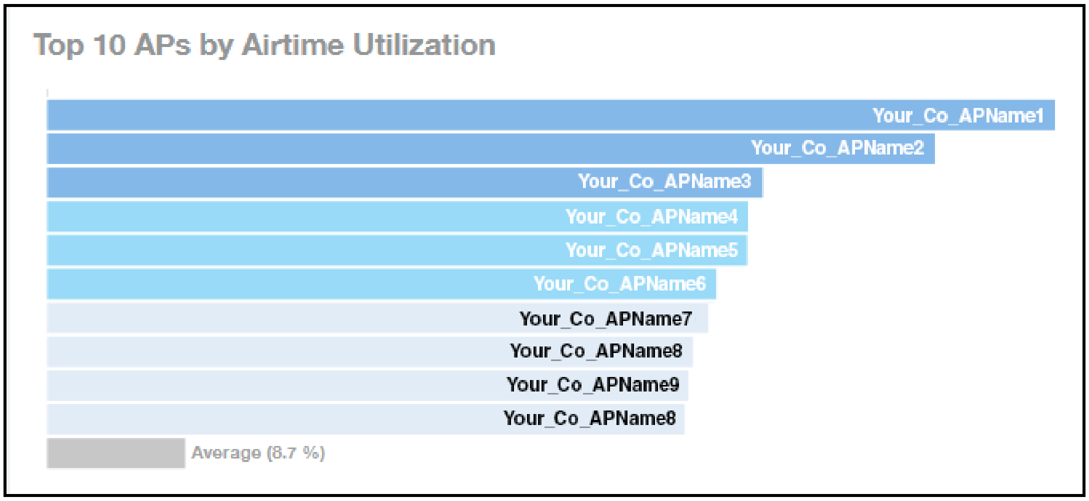
FIGURE 160 Airtime Utilization: Overview Tile



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 161 Top 10 APs by Airtime Utilization Chart



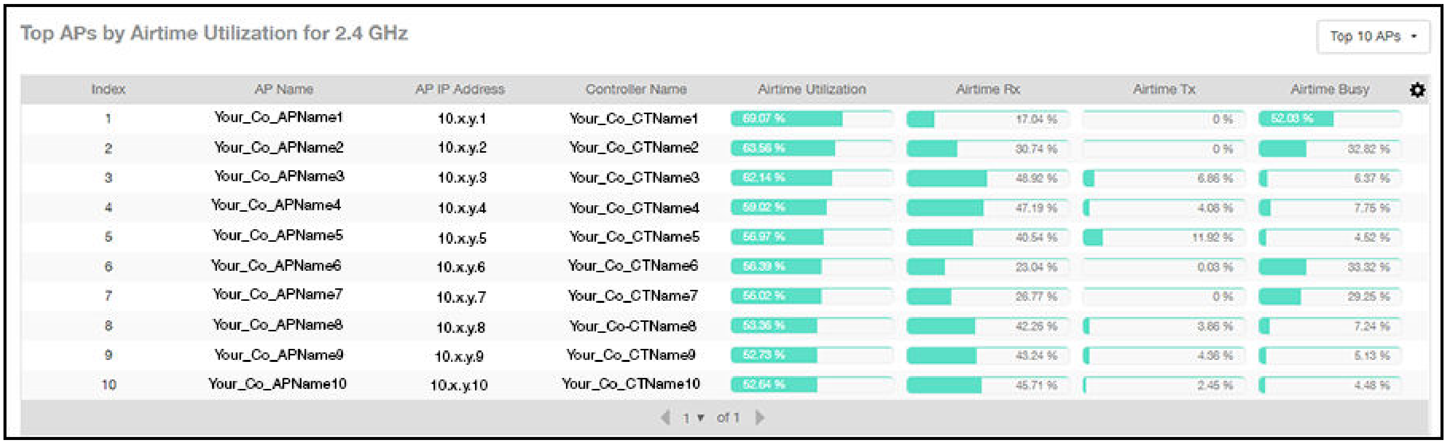
Top APs by Airtime Utilization for 2.4 GHz Table

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 162 Top APs by Airtime Utilization for 2.4 GHz Table



Top APs by Airtime Utilization for 2.4 GHz

Index	AP Name	AP IP Address	Controller Name	Airtime Utilization	Airtime Rx	Airtime Tx	Airtime Busy
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	69.07 %	17.04 %	0 %	52.03 %
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName2	63.56 %	30.74 %	0 %	32.82 %
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName3	62.14 %	48.92 %	6.86 %	6.37 %
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName4	59.02 %	47.19 %	4.08 %	7.75 %
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName5	56.97 %	40.54 %	11.92 %	4.52 %
6	Your_Co_APName6	10.x.y.6	Your_Co_CTName6	56.39 %	23.04 %	0.03 %	33.32 %
7	Your_Co_APName7	10.x.y.7	Your_Co_CTName7	56.02 %	26.77 %	0 %	29.25 %
8	Your_Co_APName8	10.x.y.8	Your_Co-CTName8	53.36 %	42.26 %	3.86 %	7.24 %
9	Your_Co_APName9	10.x.y.9	Your_Co_CTName9	52.73 %	43.24 %	4.36 %	5.13 %
10	Your_Co_APName10	10.x.y.10	Your_Co_CTName10	52.64 %	45.71 %	2.45 %	4.48 %

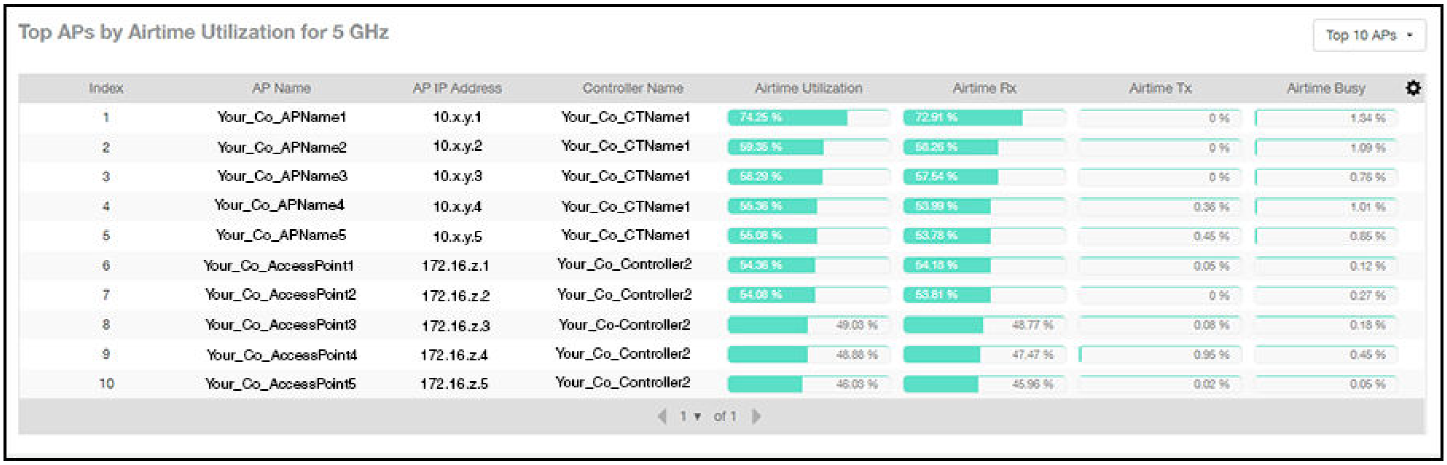
Top APs by Airtime Utilization for 5 GHz Table

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 163 Top APs by Airtime Utilization for 5 GHz Table



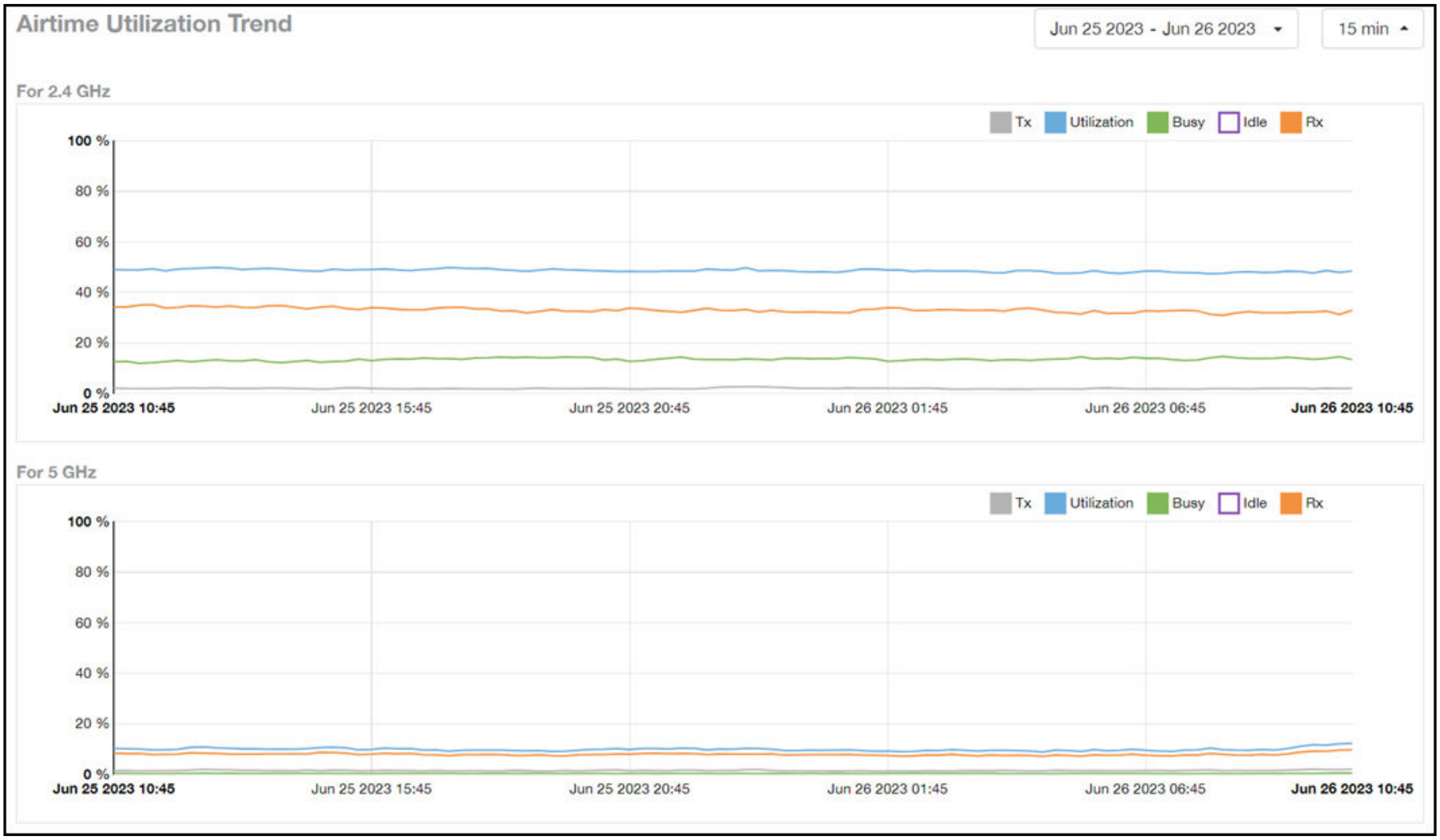
Top APs by Airtime Utilization for 5 GHz

Index	AP Name	AP IP Address	Controller Name	Airtime Utilization	Airtime Rx	Airtime Tx	Airtime Busy
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	74.25 %	72.91 %	0 %	1.34 %
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName1	59.35 %	58.26 %	0 %	1.09 %
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName1	58.29 %	57.54 %	0 %	0.76 %
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName1	55.36 %	53.99 %	0.36 %	1.01 %
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName1	55.08 %	53.78 %	0.45 %	0.85 %
6	Your_Co_AccessPoint1	172.16.z.1	Your_Co_Controller2	54.36 %	54.18 %	0.05 %	0.12 %
7	Your_Co_AccessPoint2	172.16.z.2	Your_Co_Controller2	54.08 %	53.81 %	0 %	0.27 %
8	Your_Co_AccessPoint3	172.16.z.3	Your_Co-Controller2	49.03 %	48.77 %	0.08 %	0.18 %
9	Your_Co_AccessPoint4	172.16.z.4	Your_Co_Controller2	48.88 %	47.47 %	0.95 %	0.45 %
10	Your_Co_AccessPoint5	172.16.z.5	Your_Co_Controller2	46.03 %	45.96 %	0.02 %	0.05 %

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.

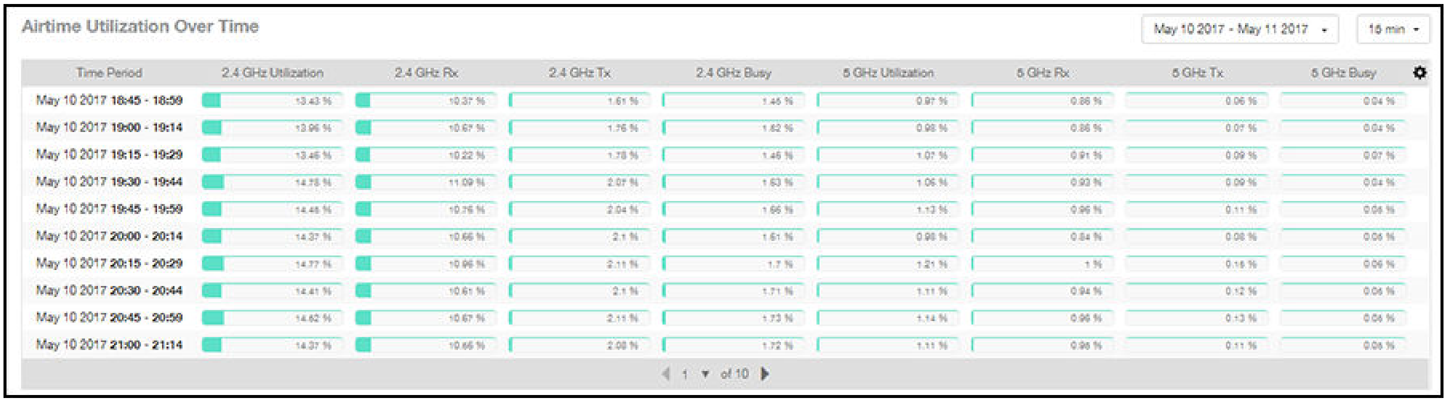
FIGURE 164 Airtime Utilization Trend Graph Trends



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 165 Airtime Utilization Over Time Table



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

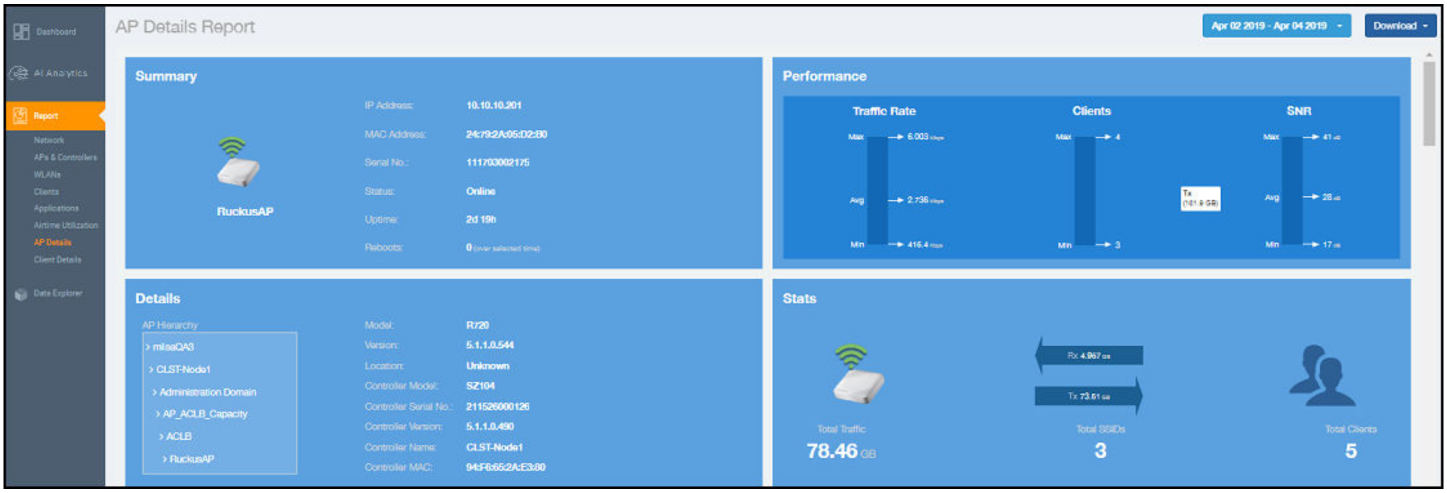
AP Details Report

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

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

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

FIGURE 166 AP Details Report (Upper Portion Only)



IP Address: 10.10.10.201
MAC Address: 24:79:2A:05:D2:B0
Serial No.: 111703002175
Status: Online
Uptime: 2d 19h
Reboots: 0 (over selected time)

Traffic Rate: Max 6.003, Avg 2.736, Min 416.4
Clients: Max 4, Min 3
SNR: Max 41, Avg 28, Min 17

AP Hierarchy
› milsaQA3
› CLST-Node1
› Administration Domain
› AP_ACLB_Capacity
› ACLB
› RuckusAP

Model: R720
Version: 5.1.1.0.544
Location: Unknown
Controller Model: SZ104
Controller Serial No.: 211526000126
Controller Version: 5.1.1.0.490
Controller Name: CLST-Node1
Controller MAC: 94:F6:65:2A:E3:80

Total Traffic 78.46 GB
Total SSIDs 3
Total Clients 5

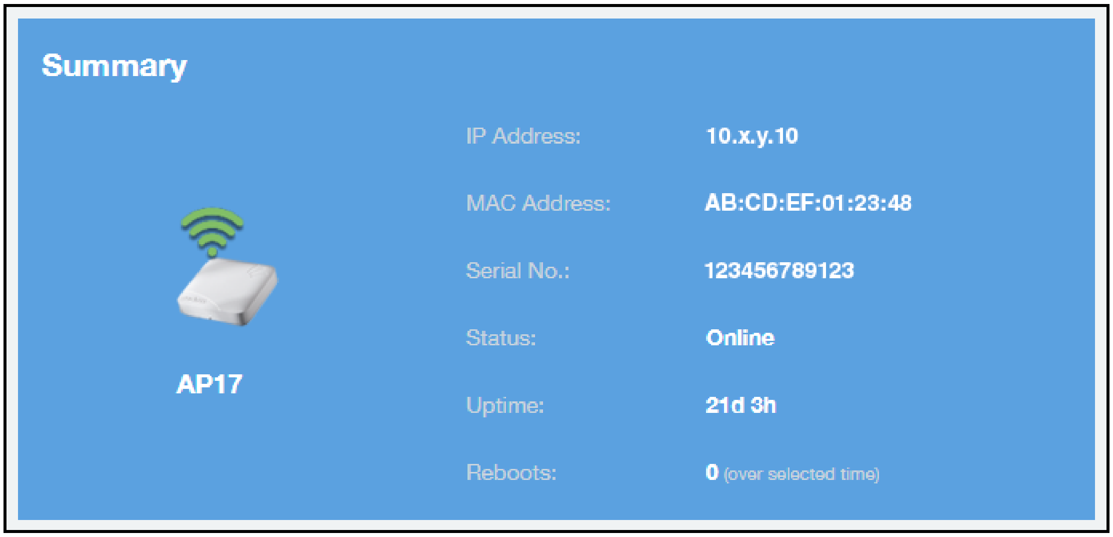
The **AP Details Report** consists of the following components:

- 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 167 AP Details: Summary Tile



Summary

AP17

IP Address: 10.x.y.10

MAC Address: AB:CD:EF:01:23:48

Serial No.: 123456789123

Status: Online

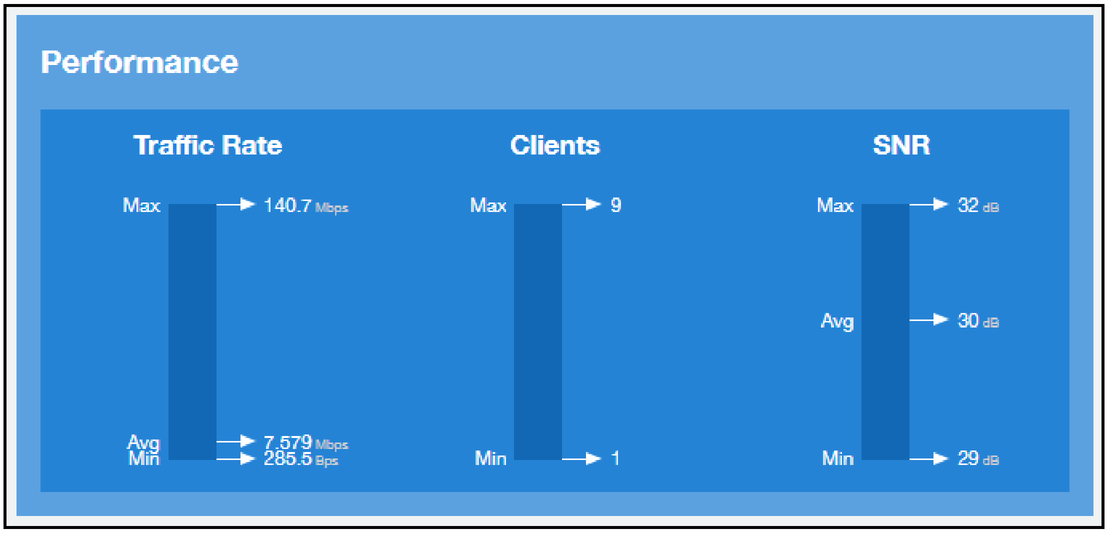
Uptime: 21d 3h

Reboots: 0 (over selected time)

Performance Tile

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

FIGURE 168 AP Details: Performance Tile

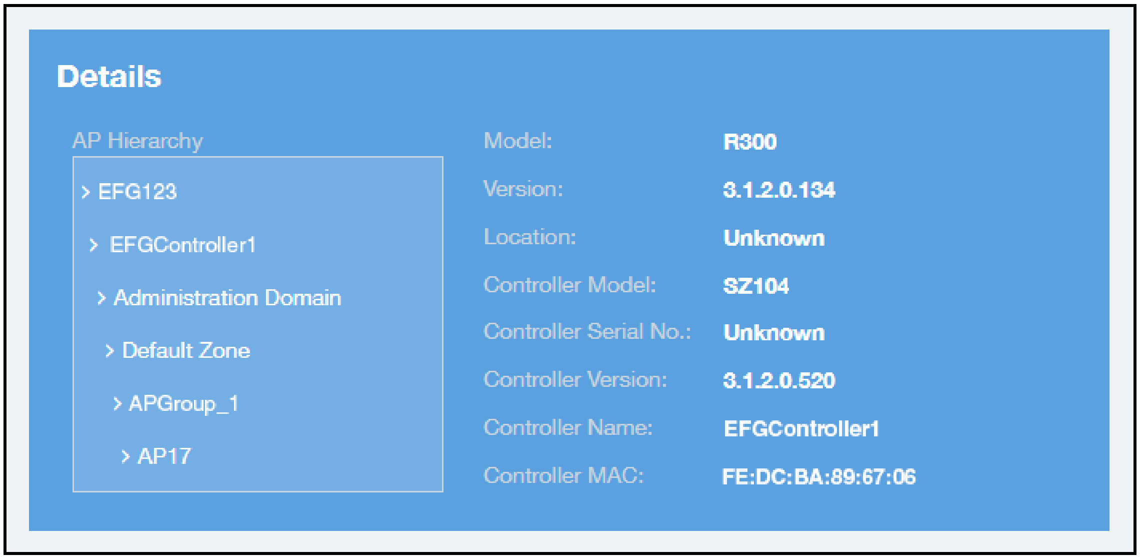


Details Tile

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 169 AP Details: Details Tile



Details

AP Hierarchy

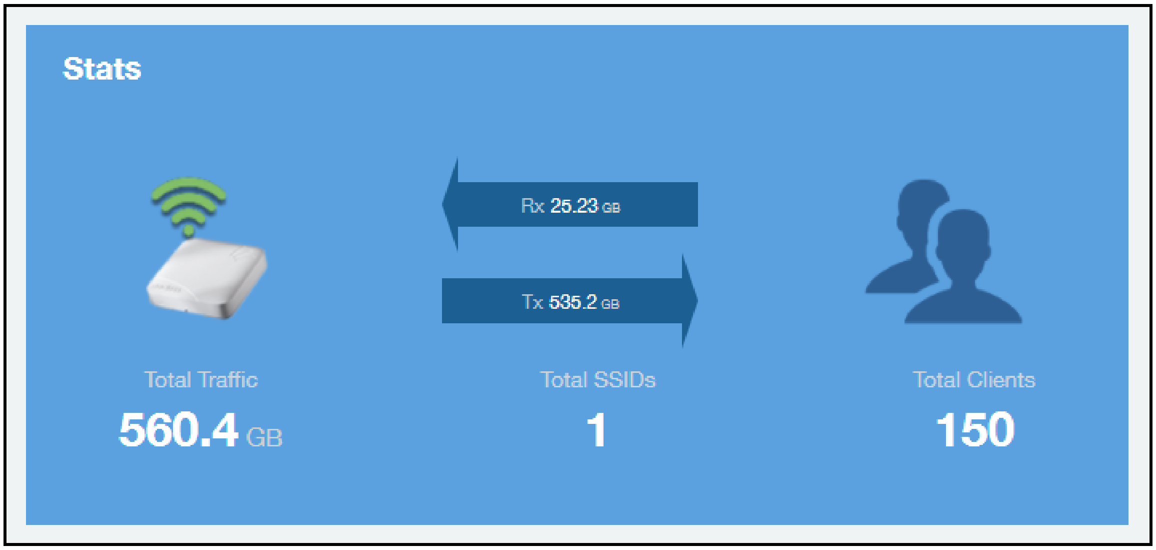
- › EFG123
- › EFGController1
- › Administration Domain
- › Default Zone
- › APGroup_1
- › AP17

Model:	R300
Version:	3.1.2.0.134
Location:	Unknown
Controller Model:	SZ104
Controller Serial No.:	Unknown
Controller Version:	3.1.2.0.520
Controller Name:	EFGController1
Controller MAC:	FE:DC:BA:89:67:06

Stats Tile

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

FIGURE 170 AP Details: Stats Tile



Stats

Rx 25.23 GB

Tx 535.2 GB

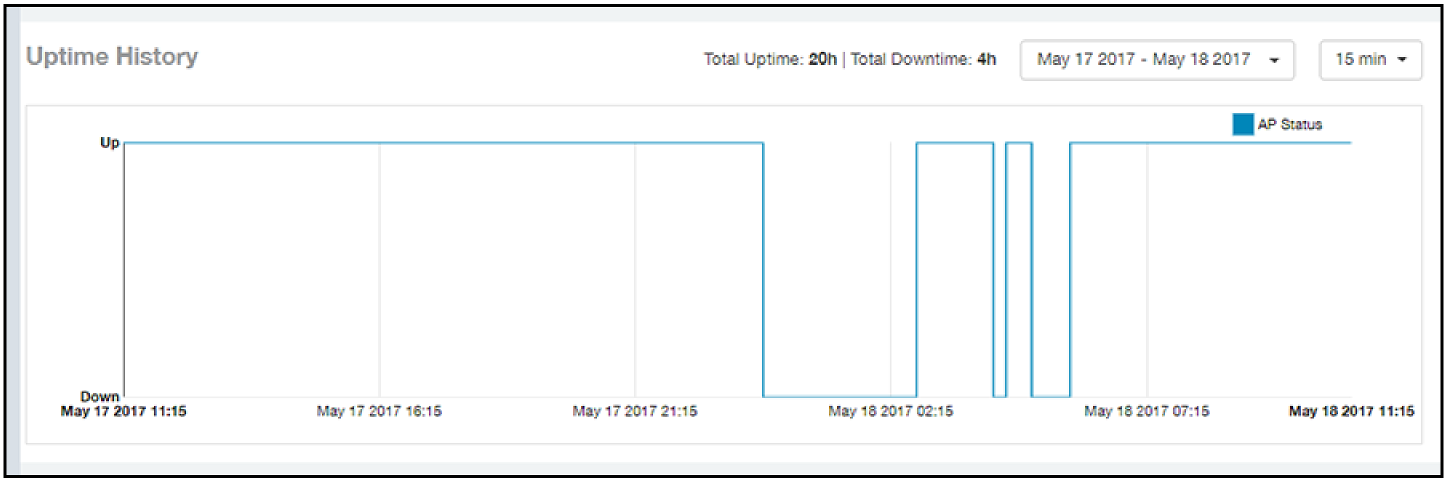
Total Traffic	Total SSIDs	Total Clients
560.4 GB	1	150

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 171 AP Details: Uptime History Graph

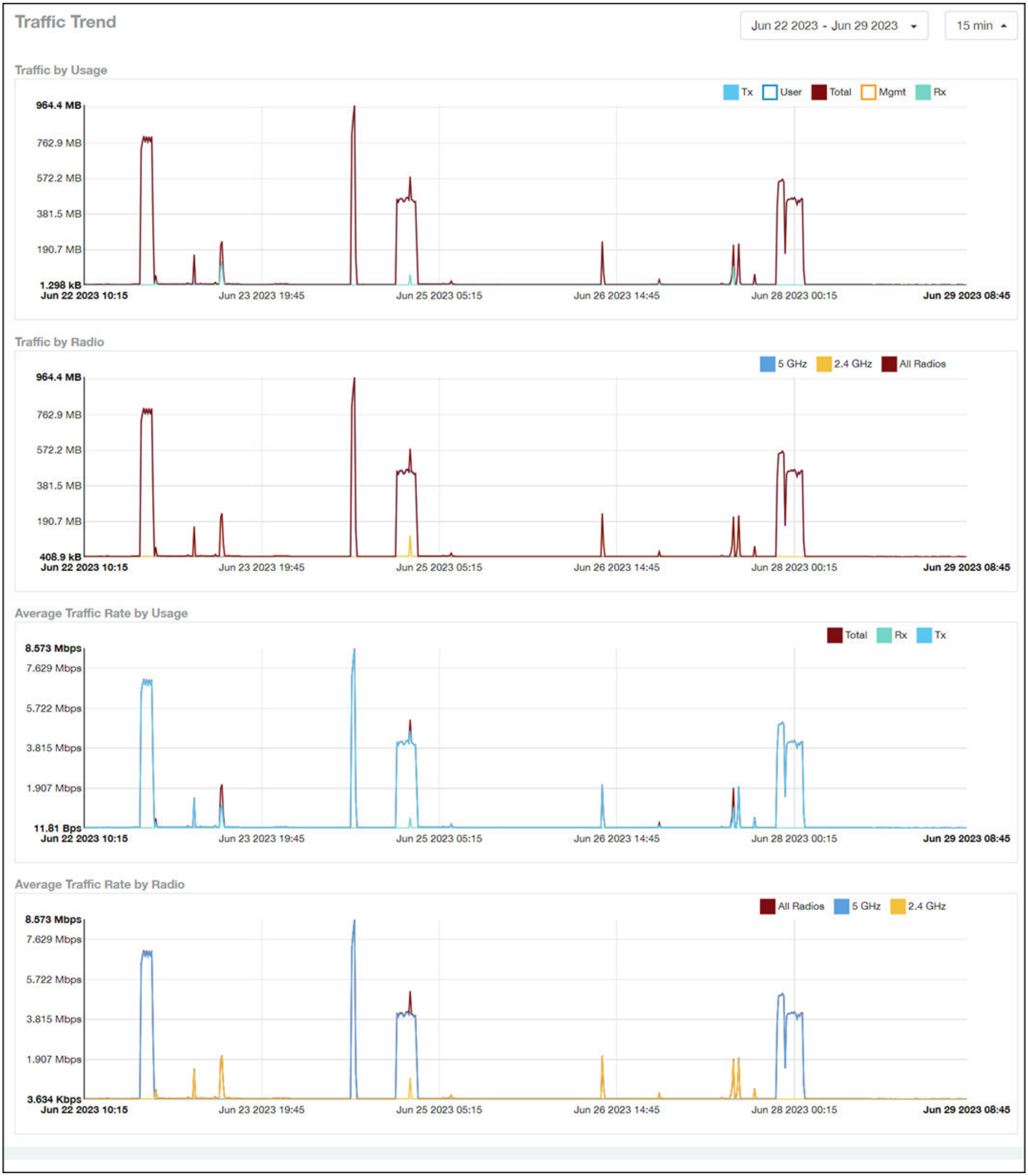


Traffic Trend Graphs

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 172 AP Details: Traffic Trend Graphs



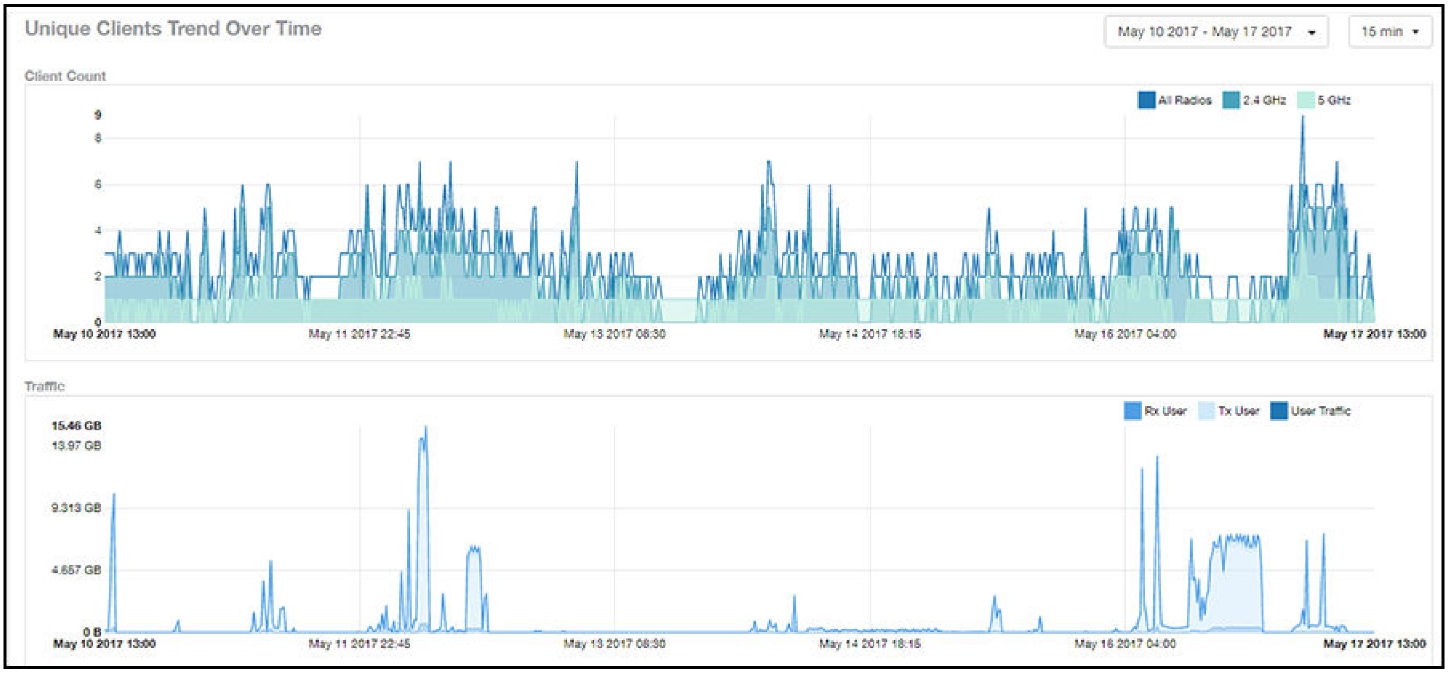
Unique Clients Trend Over Time Graphs

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 173 AP Details: Unique Clients Trend Over Time Graphs



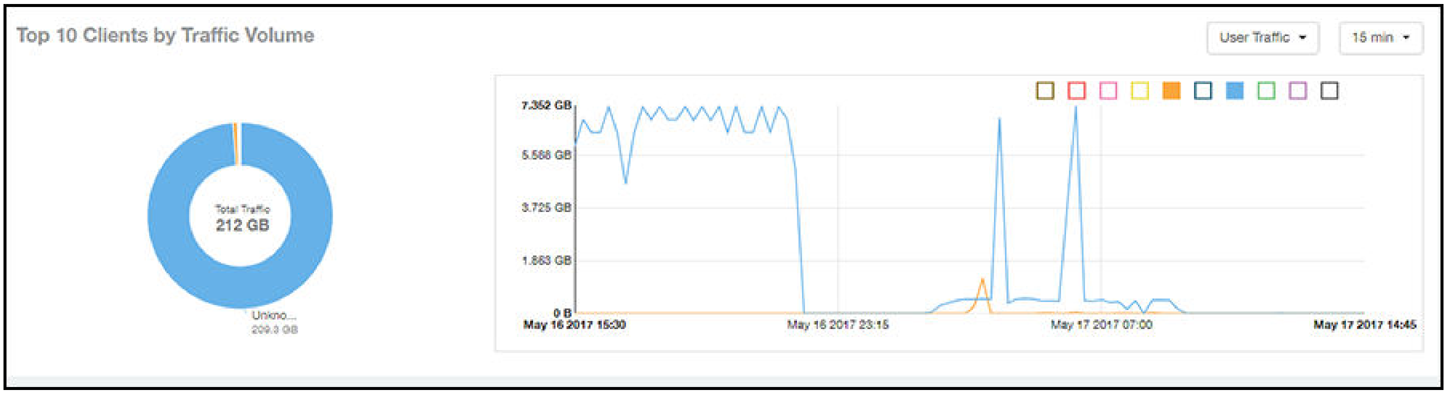
Top 10 Clients by Traffic Volume Tile

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 174 AP Details: Top 10 Clients by Traffic Volume Tile



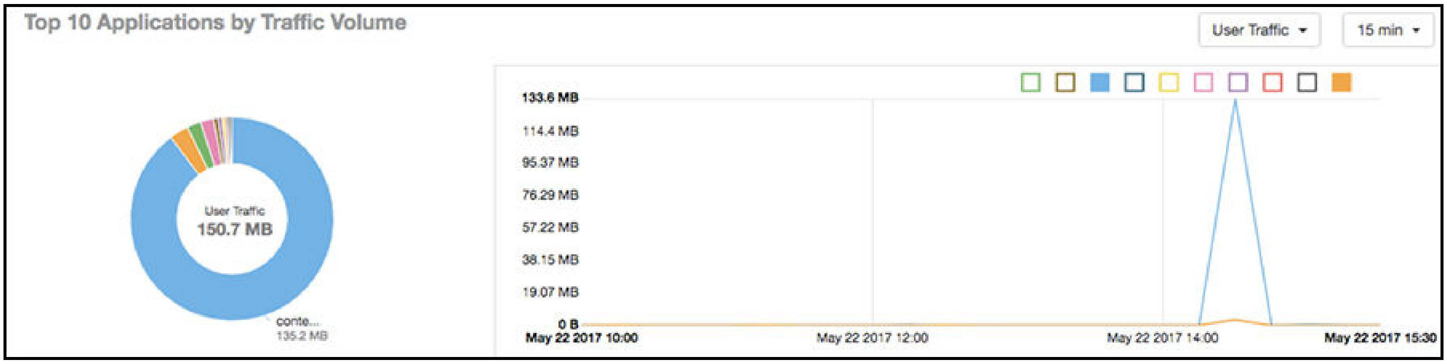
Top 10 Applications by Traffic Volume Tile

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 175 AP Details: Top 10 Applications by Traffic Volume Tile

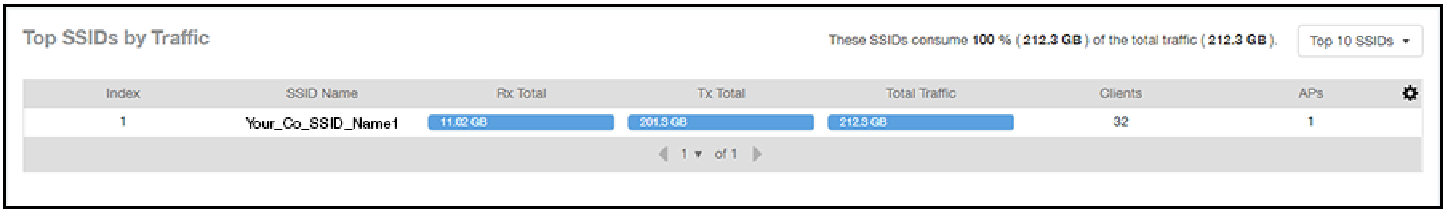


Top SSIDs by Traffic Table

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 176 AP Details: Top SSIDs by Traffic Table



Top SSIDs by Traffic

These SSIDs consume **100** % (**212.3 GB**) of the total traffic (**212.3 GB**).

Top 10 SSIDs ▾

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

◀ 1 ▾ of 1 ▶

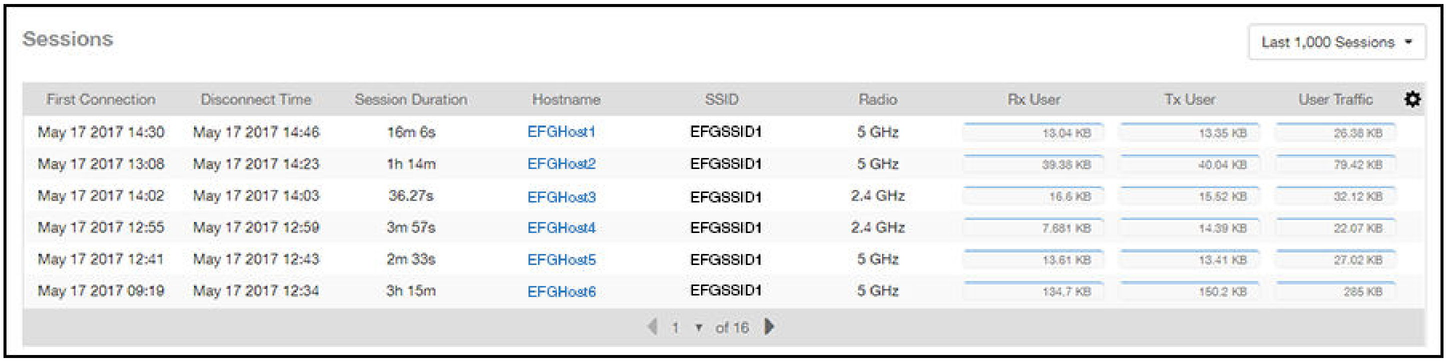
Sessions Table

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

Use the menu to specify how many sessions to display.

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

FIGURE 177 AP Details: Sessions Table



Sessions

Last 1,000 Sessions ▾

First Connection	Disconnect Time	Session Duration	Hostname	SSID	Radio	Rx User	Tx User	User Traffic
May 17 2017 14:30	May 17 2017 14:46	16m 6s	EFGHost1	EFGSSID1	5 GHz	13.04 KB	13.35 KB	26.38 KB
May 17 2017 13:08	May 17 2017 14:23	1h 14m	EFGHost2	EFGSSID1	5 GHz	39.38 KB	40.04 KB	79.42 KB
May 17 2017 14:02	May 17 2017 14:03	36.27s	EFGHost3	EFGSSID1	2.4 GHz	16.6 KB	15.52 KB	32.12 KB
May 17 2017 12:55	May 17 2017 12:59	3m 57s	EFGHost4	EFGSSID1	2.4 GHz	7.681 KB	14.39 KB	22.07 KB
May 17 2017 12:41	May 17 2017 12:43	2m 33s	EFGHost5	EFGSSID1	5 GHz	13.61 KB	13.41 KB	27.02 KB
May 17 2017 09:19	May 17 2017 12:34	3h 15m	EFGHost6	EFGSSID1	5 GHz	134.7 KB	150.2 KB	285 KB

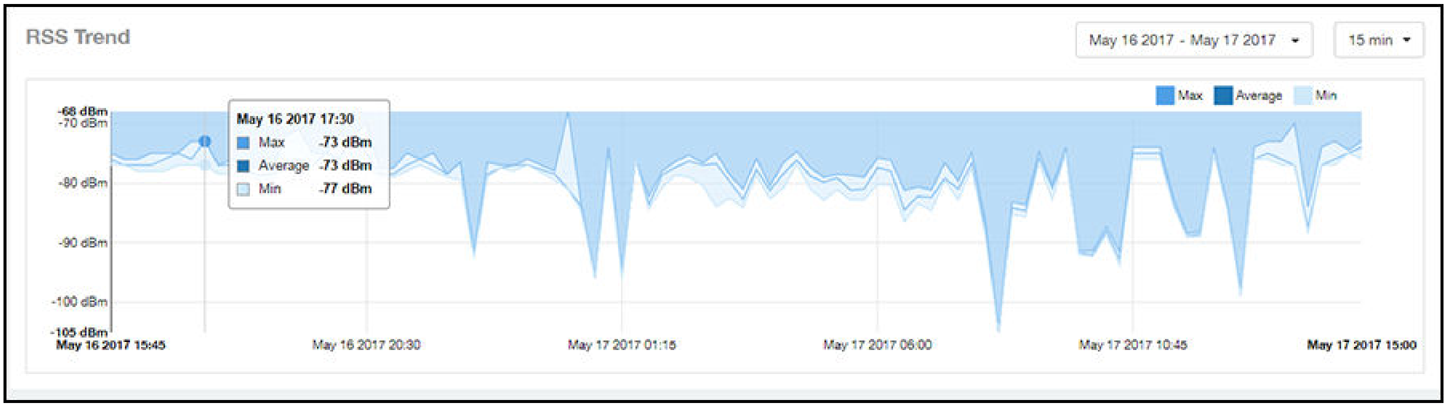
◀ 1 ▾ of 16 ▶

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 178 AP Details: RSS Trend Graph



RSS Trend

May 16 2017 - May 17 2017 ▾

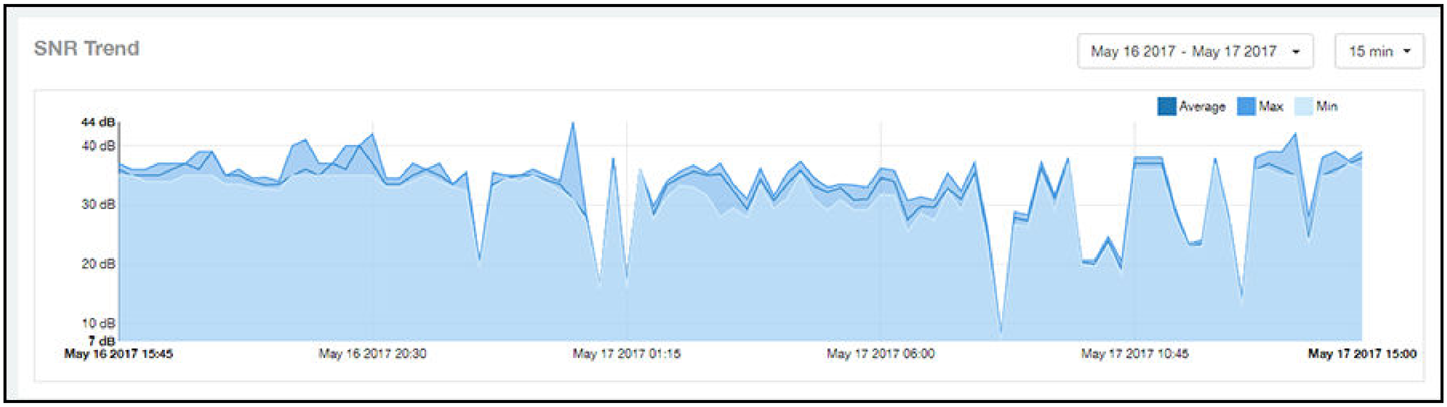
15 min ▾

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 179 AP Details: SNR Trend Graph

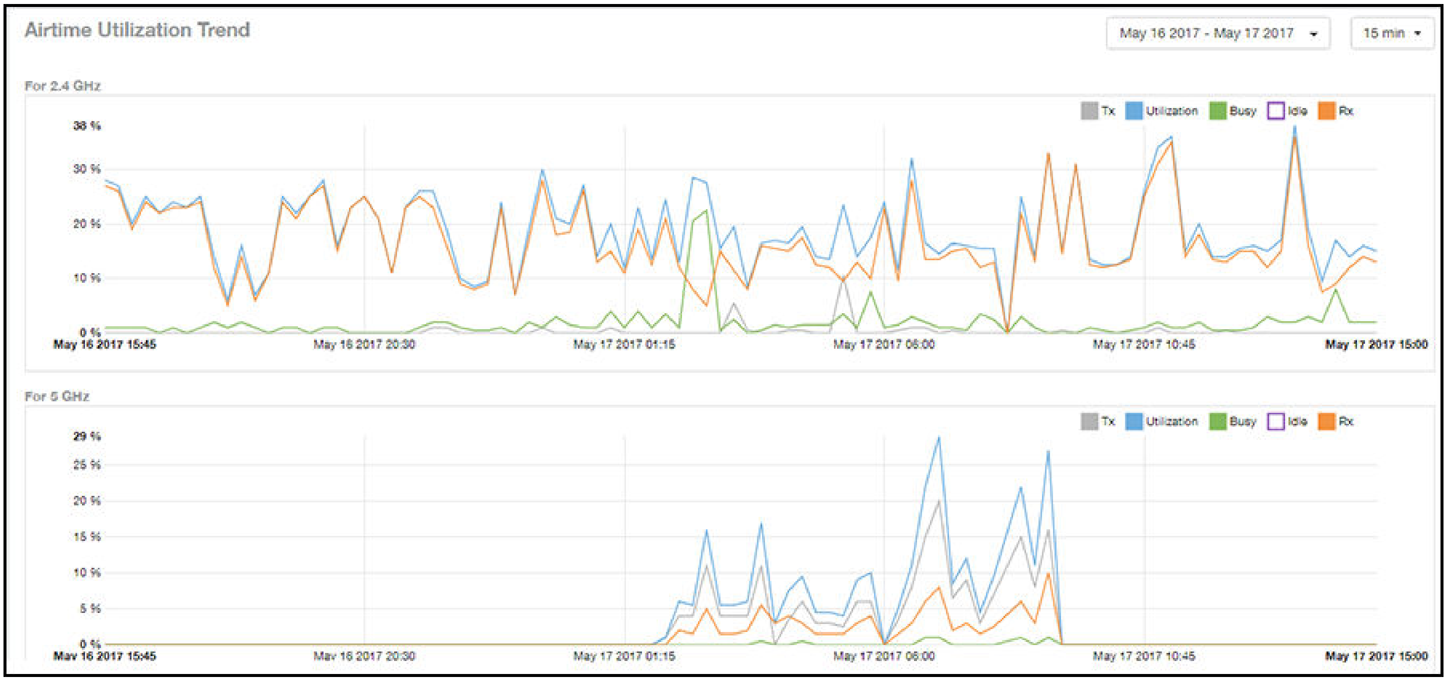


Airtime Utilization Trend Graphs

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 180 AP Details: Airtime Utilization Trend Graphs



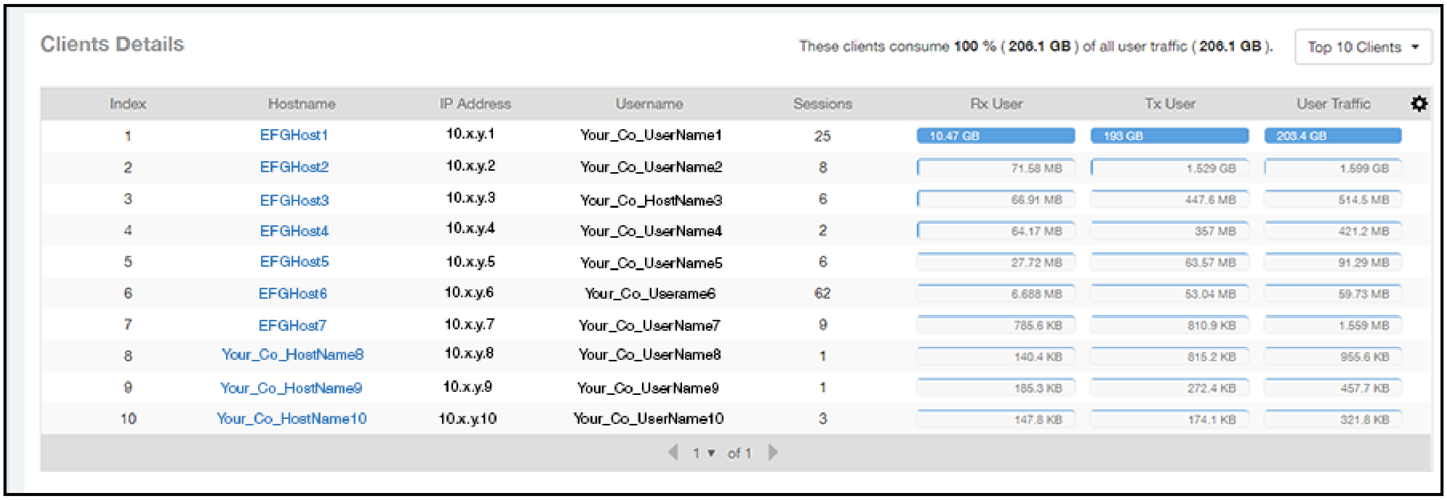
Clients Details Table

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 181 AP Details: Clients Details Table



Clients Details

These clients consume **100 %** (**206.1 GB**) of all user traffic (**206.1 GB**).

Index	Hostname	IP Address	Username	Sessions	Rx User	Tx User	User Traffic
1	EFGHost1	10.x.y.1	Your_Co_UserName1	25	10.47 GB	193 GB	203.4 GB
2	EFGHost2	10.x.y.2	Your_Co_UserName2	8	71.58 MB	1.529 GB	1.599 GB
3	EFGHost3	10.x.y.3	Your_Co_HostName3	6	66.91 MB	447.6 MB	514.5 MB
4	EFGHost4	10.x.y.4	Your_Co_UserName4	2	64.17 MB	357 MB	421.2 MB
5	EFGHost5	10.x.y.5	Your_Co_UserName5	6	27.72 MB	63.57 MB	91.29 MB
6	EFGHost6	10.x.y.6	Your_Co_Userame6	62	6.688 MB	53.04 MB	59.73 MB
7	EFGHost7	10.x.y.7	Your_Co_UserName7	9	785.6 KB	810.9 KB	1.559 MB
8	Your_Co_HostName8	10.x.y.8	Your_Co_UserName8	1	140.4 KB	815.2 KB	955.6 KB
9	Your_Co_HostName9	10.x.y.9	Your_Co_UserName9	1	185.3 KB	272.4 KB	457.7 KB
10	Your_Co_HostName10	10.x.y.10	Your_Co_UserName10	3	147.8 KB	174.1 KB	321.8 KB

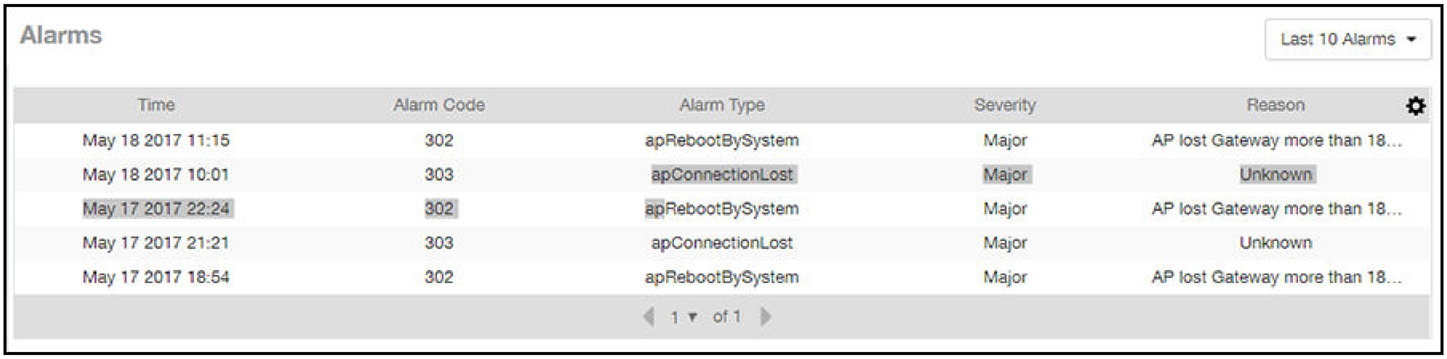
Alarms Table

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 182 AP Details: Alarms Table



Alarms

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

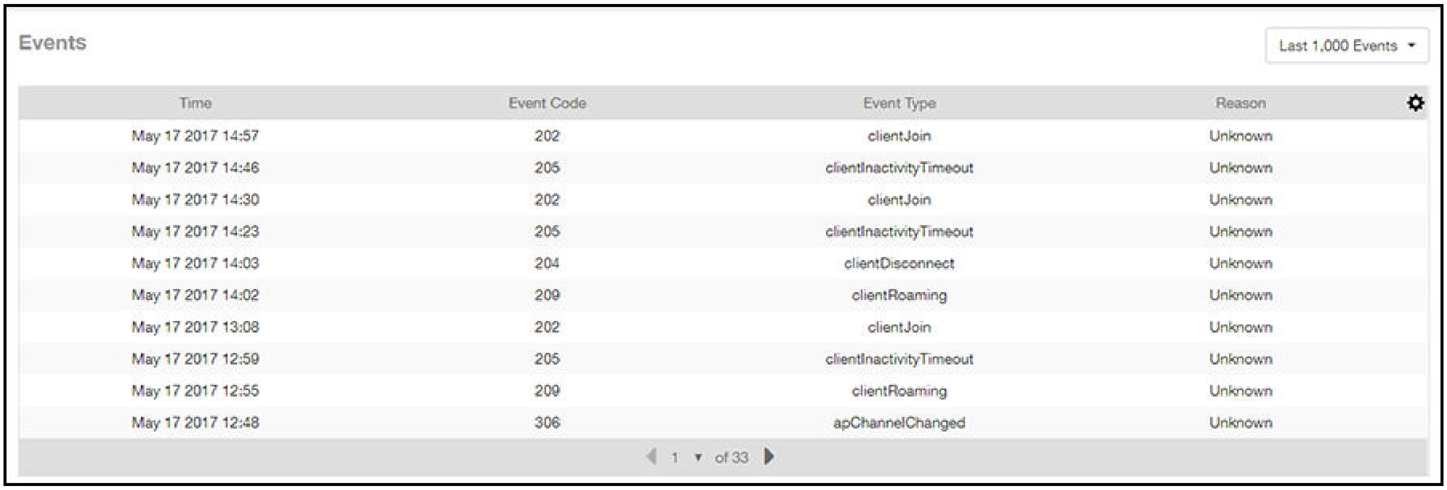
Events Table

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 183 AP Details: Events Table



Events

Last 1,000 Events ▾

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

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.

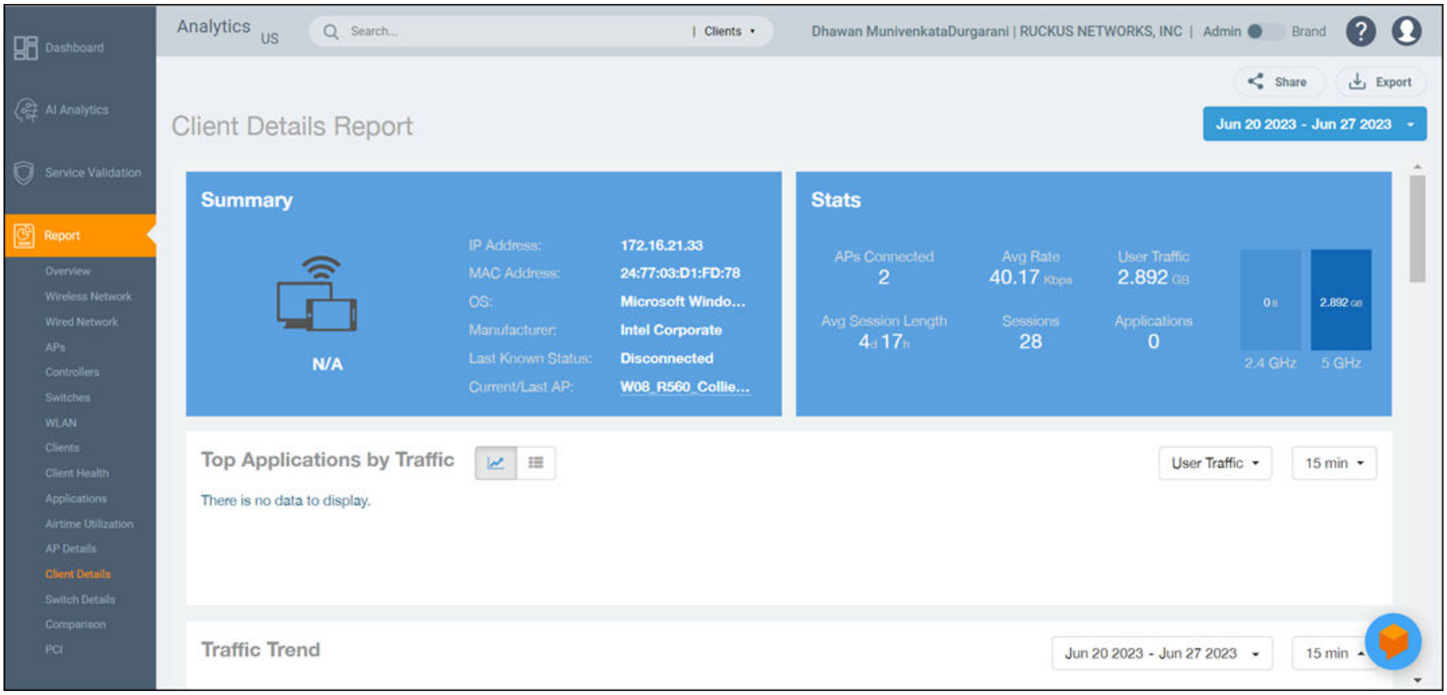
Client Details Report

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 184 Client Details Report (Upper Portion Only)



Client Details Report

Summary

IP Address: 172.16.21.33
MAC Address: 24:77:03:D1:FD:78
OS: Microsoft Windo...
Manufacturer: Intel Corporate
Last Known Status: Disconnected
Current/Last AP: W08_R560_Collie...

Stats

APs Connected 2
Avg Rate 40.17 Kbps
User Traffic 2.892 GB
Avg Session Length 4d 17h
Sessions 28
Applications 0

Top Applications by Traffic

There is no data to display.

Traffic Trend

The Wired Report consists of the following components:

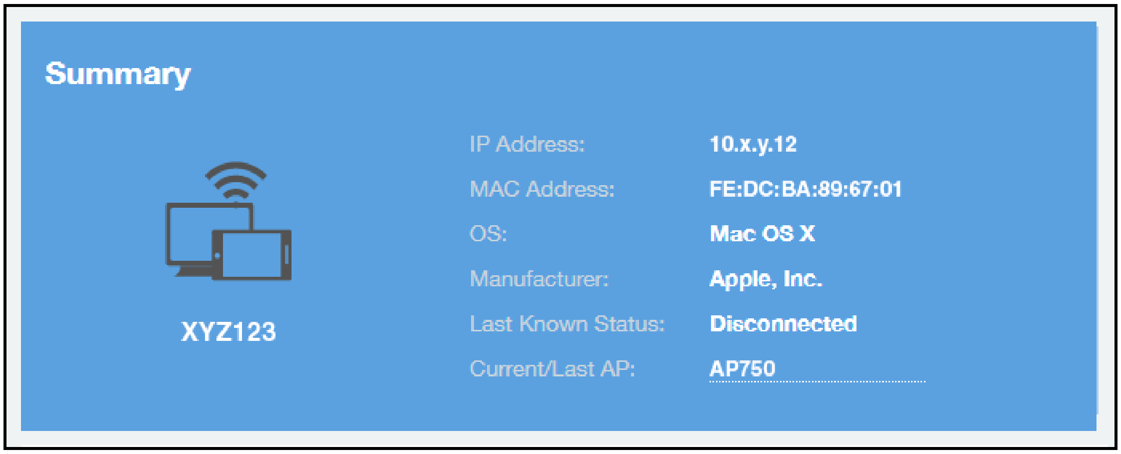
- Summary tile
- Stats tile
- Traffic Trend tile
- RSS Trend tile
- SNR Trend tile
- Sessions tile

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 185 Client Details - Summary



Summary

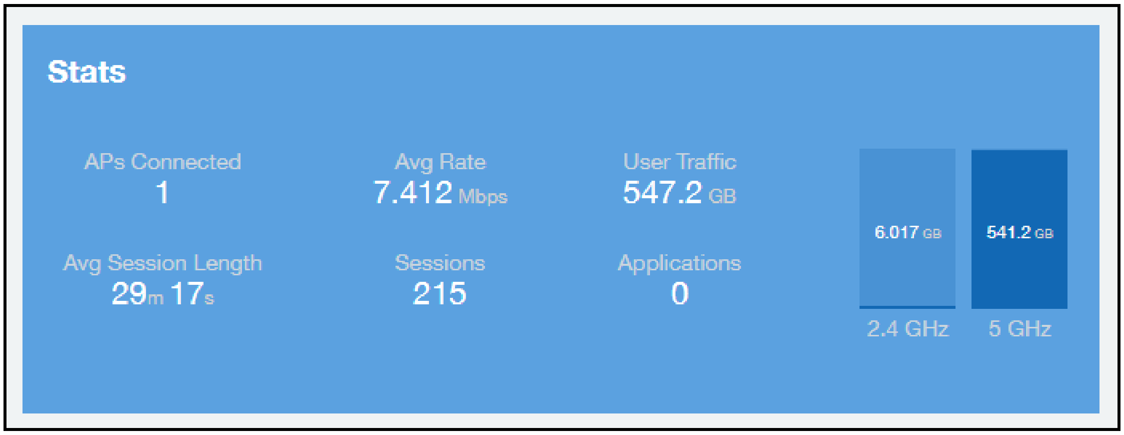
XYZ123

IP Address: 10.x.y.12
MAC Address: FE:DC:BA:89:67:01
OS: Mac OS X
Manufacturer: Apple, Inc.
Last Known Status: Disconnected
Current/Last AP: AP750

Stats Tile

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

FIGURE 186 Client Details - Stats



Stats

APs Connected 1
Avg Rate 7.412 Mbps
User Traffic 547.2 GB
Avg Session Length 29m 17s
Sessions 215
Applications 0

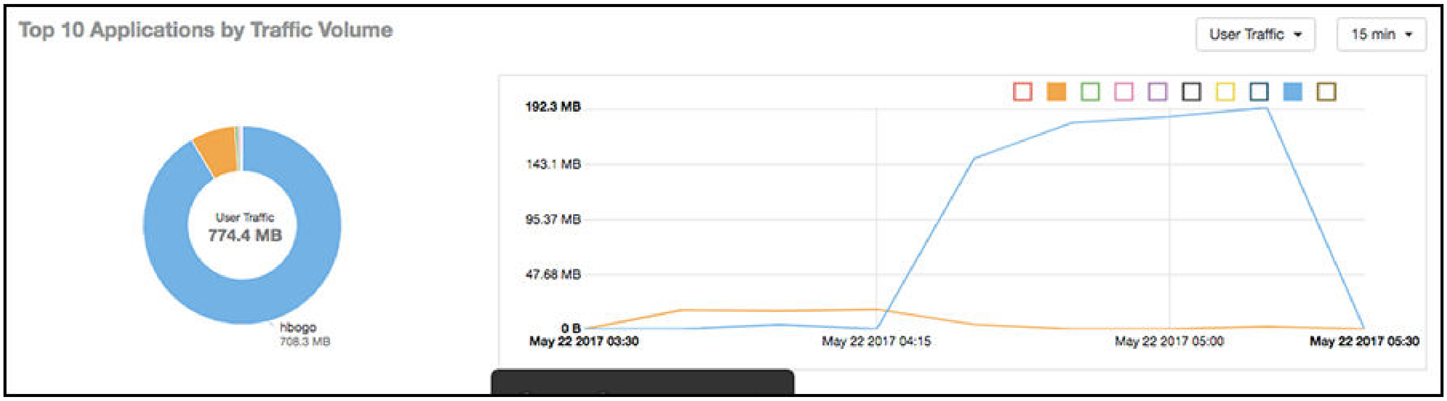
Client Details Stats

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 187 Client Details: Top 10 Applications by Traffic Volume Tile

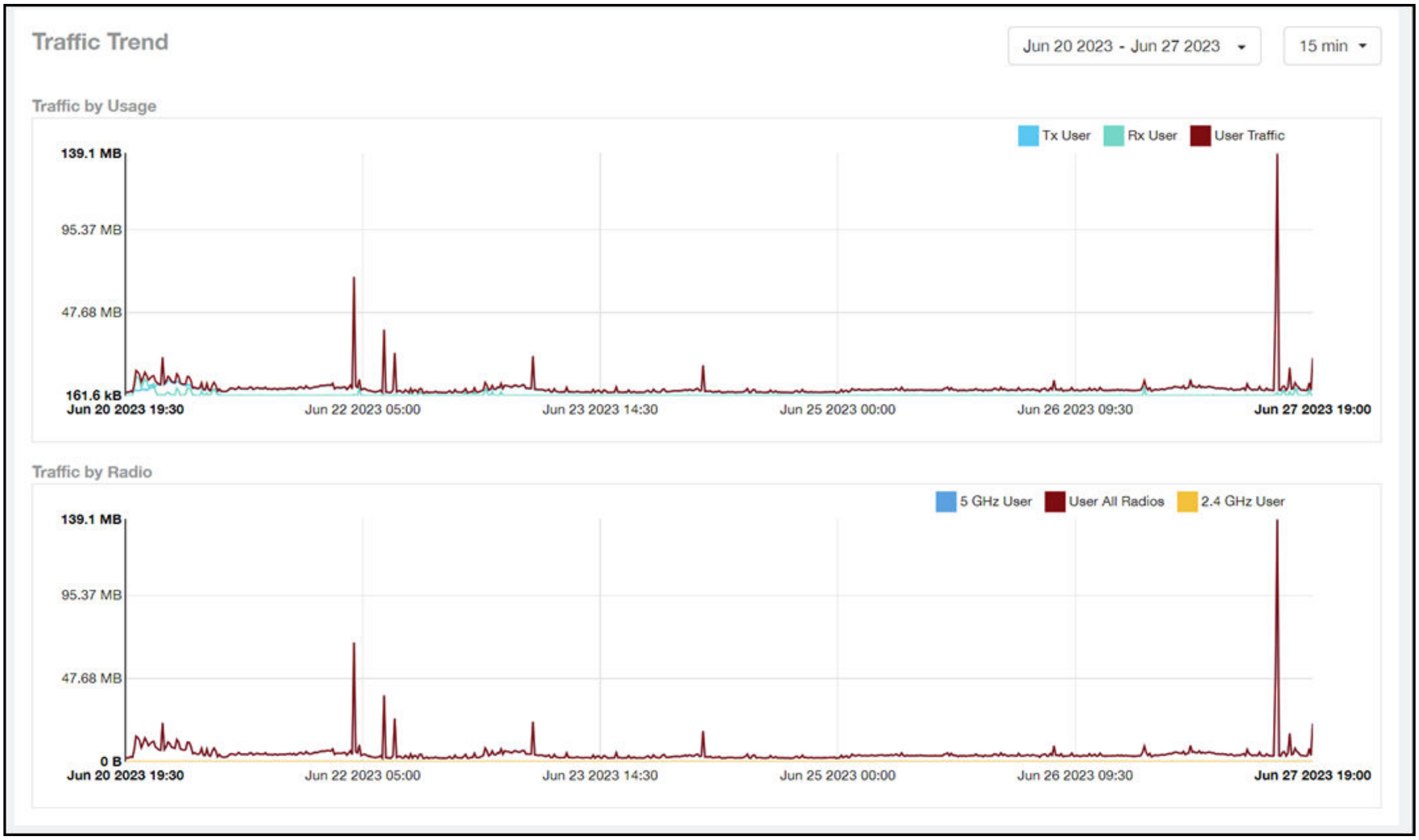


Traffic Trend Tile

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 188 Client Details - Traffic Trend Graphs

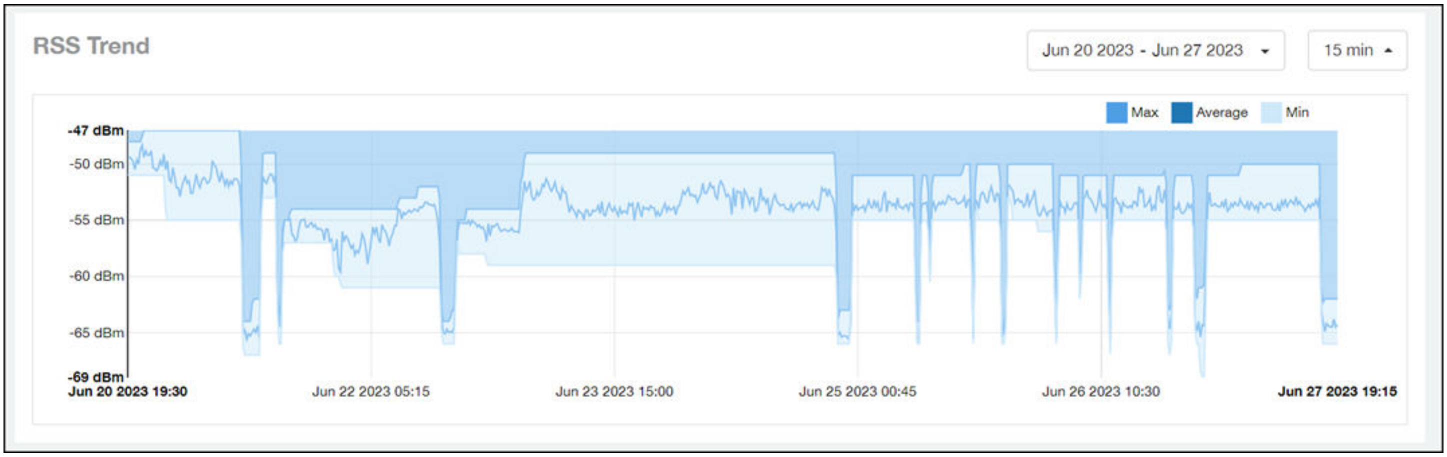


RSS Trend Tile

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 189 Client Details - RSS Trend Graph

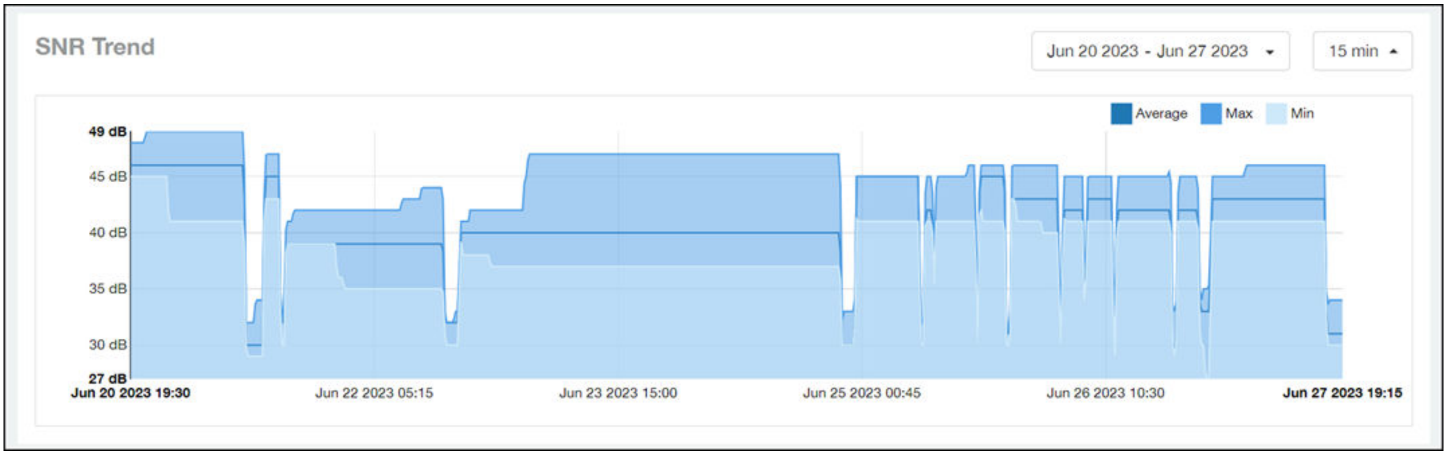


SNR Trend Tile

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 190 Client Details - SNR Trend Graph



Sessions tile

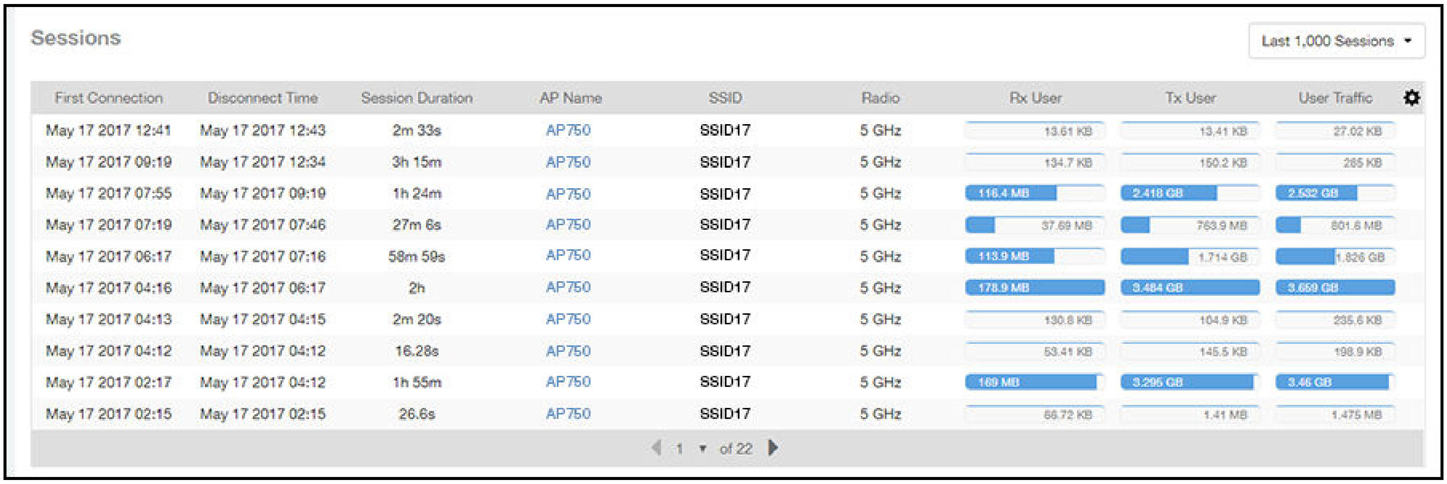
The Sessions table of the Client Details report provides details for sessions between this client and associated access points.

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 191 Client Details: Sessions Table



Sessions

Last 1,000 Sessions ▾

First Connection	Disconnect Time	Session Duration	AP Name	SSID	Radio	Rx User	Tx User	User Traffic
May 17 2017 12:41	May 17 2017 12:43	2m 33s	AP750	SSID17	5 GHz	13.61 KB	13.41 KB	27.02 KB
May 17 2017 09:19	May 17 2017 12:34	3h 15m	AP750	SSID17	5 GHz	134.7 KB	150.2 KB	285 KB
May 17 2017 07:55	May 17 2017 09:19	1h 24m	AP750	SSID17	5 GHz	116.4 MB	2.418 GB	2.532 GB
May 17 2017 07:19	May 17 2017 07:46	27m 6s	AP750	SSID17	5 GHz	37.69 MB	763.9 MB	801.6 MB
May 17 2017 06:17	May 17 2017 07:16	58m 59s	AP750	SSID17	5 GHz	113.9 MB	1.714 GB	1.826 GB
May 17 2017 04:16	May 17 2017 06:17	2h	AP750	SSID17	5 GHz	178.9 MB	3.484 GB	3.659 GB
May 17 2017 04:13	May 17 2017 04:15	2m 20s	AP750	SSID17	5 GHz	130.8 KB	104.9 KB	235.6 KB
May 17 2017 04:12	May 17 2017 04:12	16.28s	AP750	SSID17	5 GHz	53.41 KB	145.5 KB	198.9 KB
May 17 2017 02:17	May 17 2017 04:12	1h 55m	AP750	SSID17	5 GHz	169 MB	3.295 GB	3.46 GB
May 17 2017 02:15	May 17 2017 02:15	26.6s	AP750	SSID17	5 GHz	66.72 KB	1.41 MB	1.475 MB

Switch Details Report Dashboard

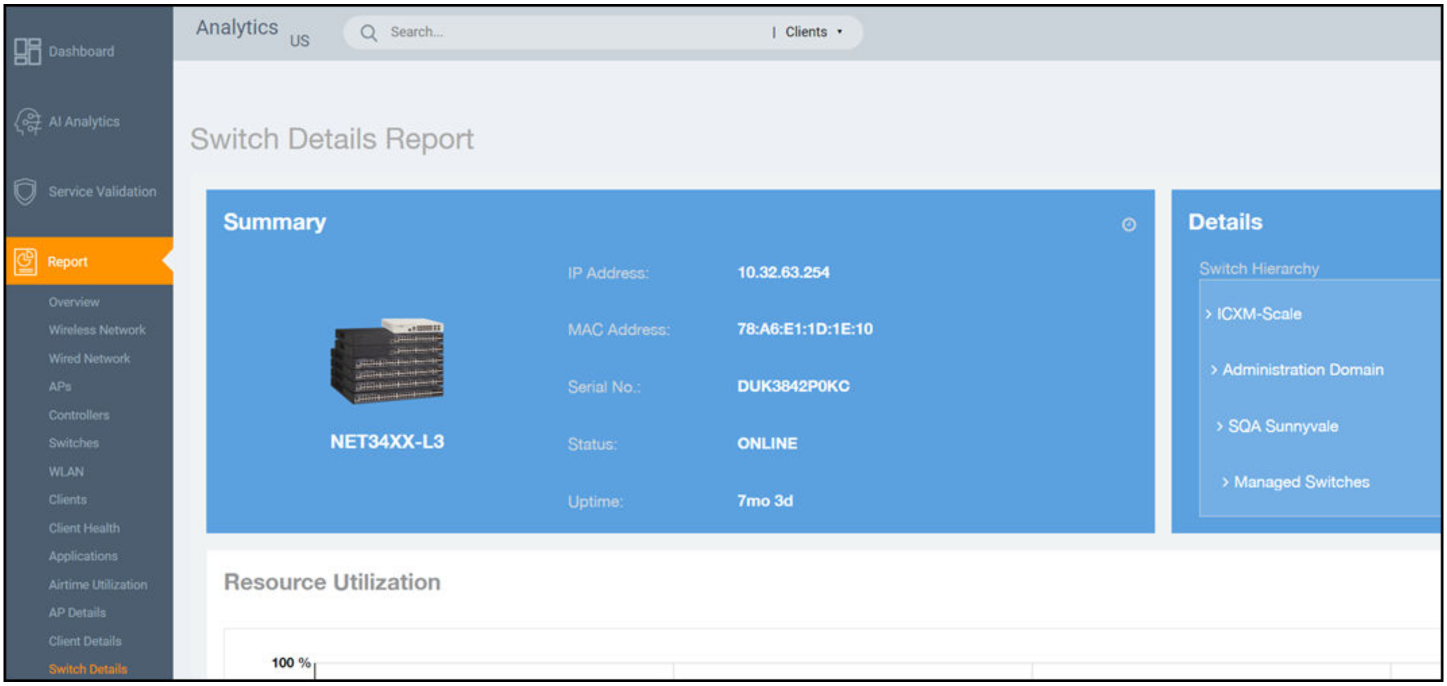
Switch Details Report

The Switch Details report provides details about one specific switch.

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

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

FIGURE 192 Switch Details Report (upper portion)



Switch Details Report

Summary

NET34XX-L3

IP Address: 10.32.63.254

MAC Address: 78:A6:E1:1D:1E:10

Serial No.: DUK3842P0KC

Status: ONLINE

Uptime: 7mo 3d

Details

Switch Hierarchy

› ICXM-Scale

› Administration Domain

› SQA Sunnyvale

› Managed Switches

Resource Utilization

The Switch Details Report consists of the following components:

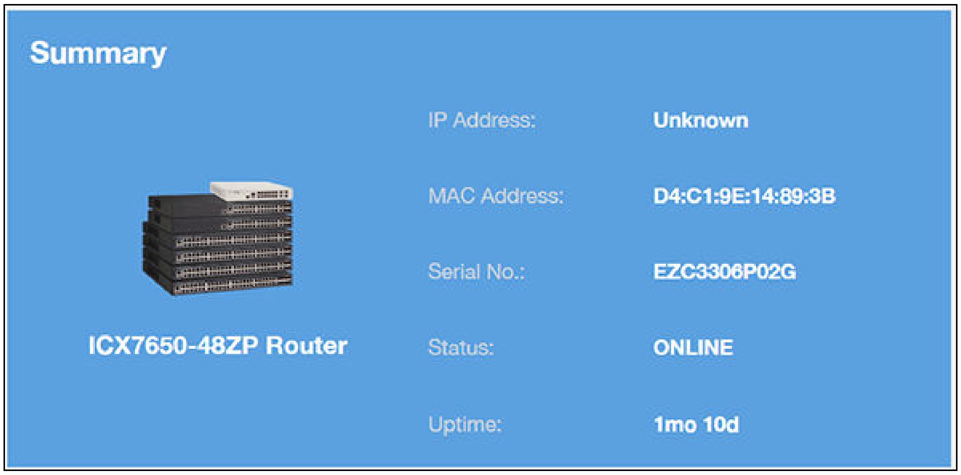
- Summary tile
- Details tile
- Resource Utilization tile
- Top Ports By Traffic tile
- Traffic Trend tile
- LLDP Neighbor List tile
- Uptime History tile

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 193 Switch Details - Summary



Summary

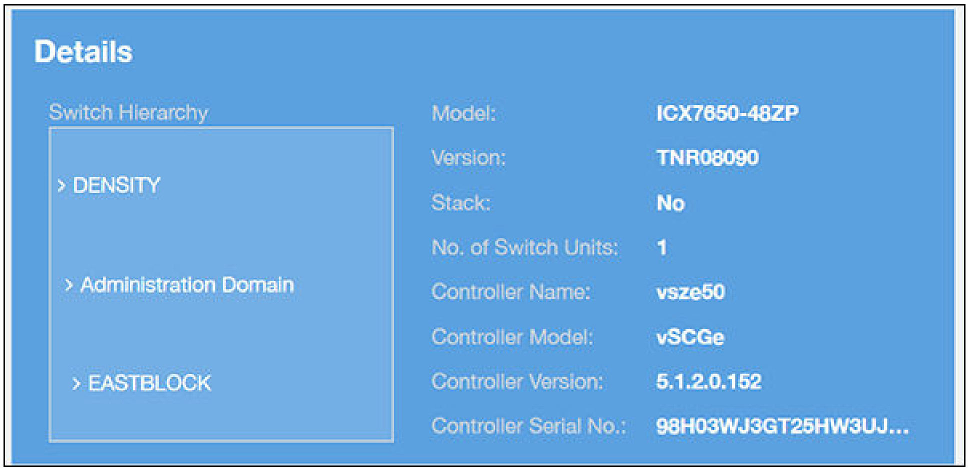
ICX7650-48ZP Router

IP Address:	Unknown
MAC Address:	D4:C1:9E:14:89:3B
Serial No.:	EZC3306P02G
Status:	ONLINE
Uptime:	1mo 10d

Details Tile

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

FIGURE 194 Switch Details - Details



Details

Switch Hierarchy

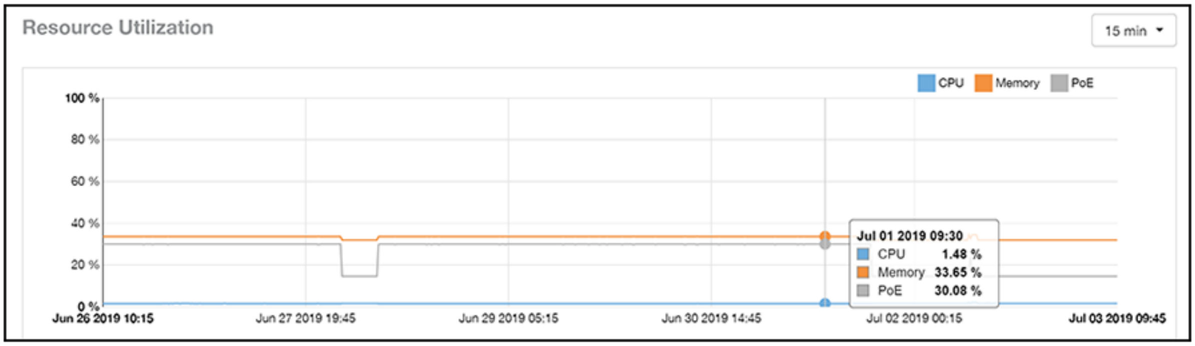
Model:	ICX7650-48ZP
Version:	TNR08090
Stack:	No
No. of Switch Units:	1
Controller Name:	vsze50
Controller Model:	vSCGe
Controller Version:	5.1.2.0.152
Controller Serial No.:	98H03WJ3GT25HW3UJ...

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 195 Switch Details - Resource Utilization

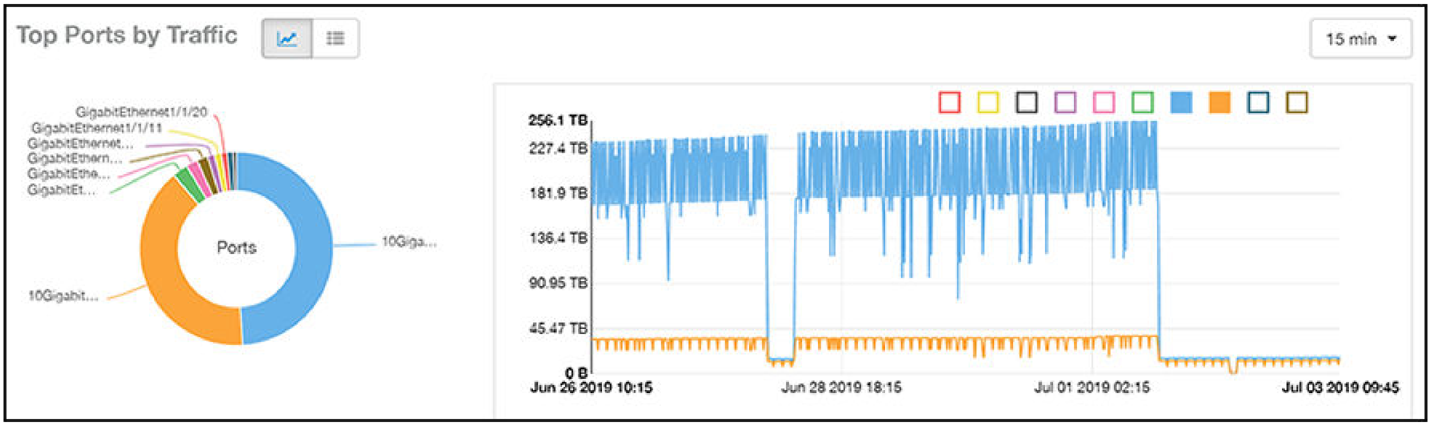


Top Ports By Traffic Tile

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 196 Switch Details - Top Ports By Traffic

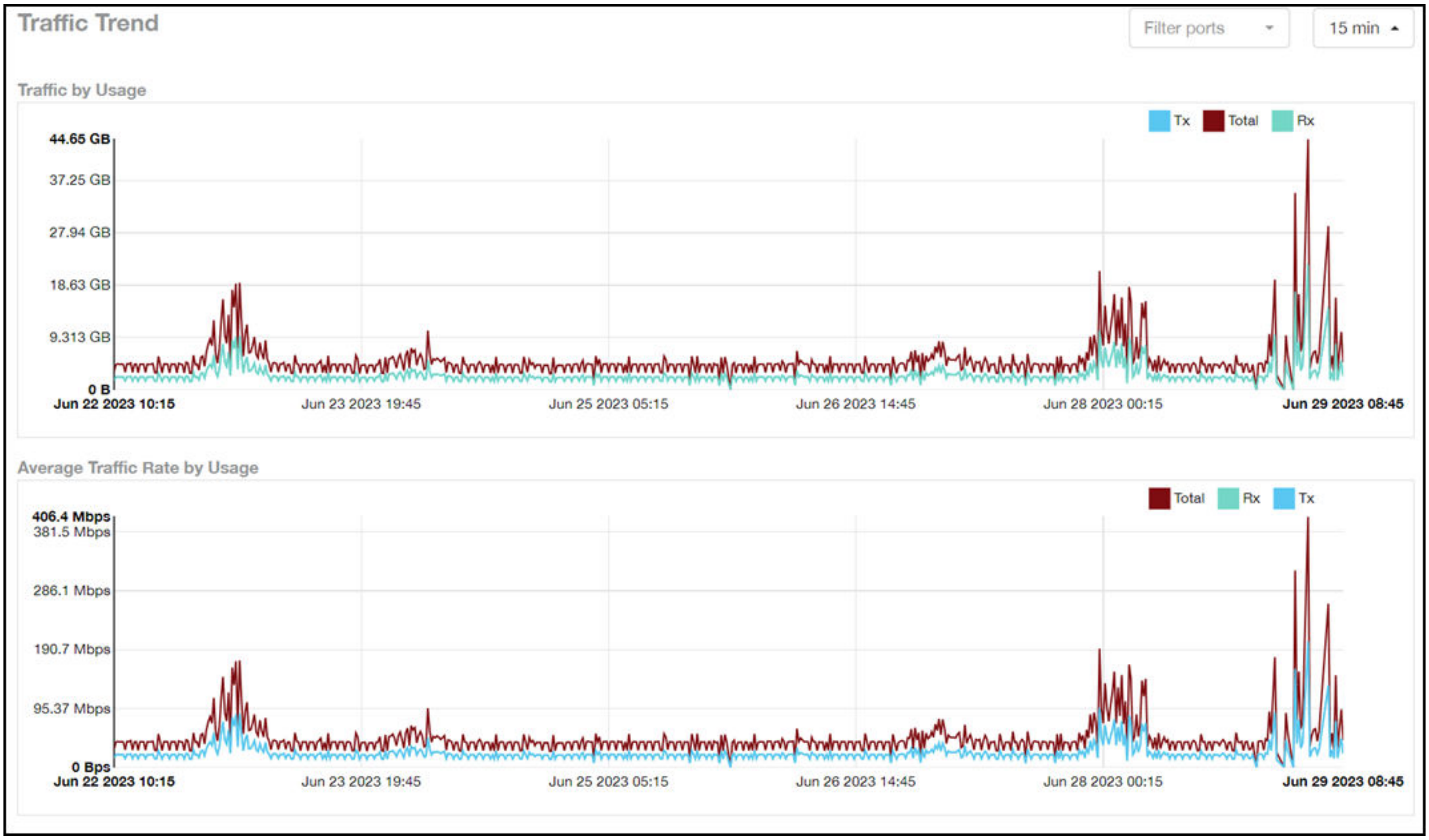


Traffic Trend Tile

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 197 Switch Details - Traffic Trend

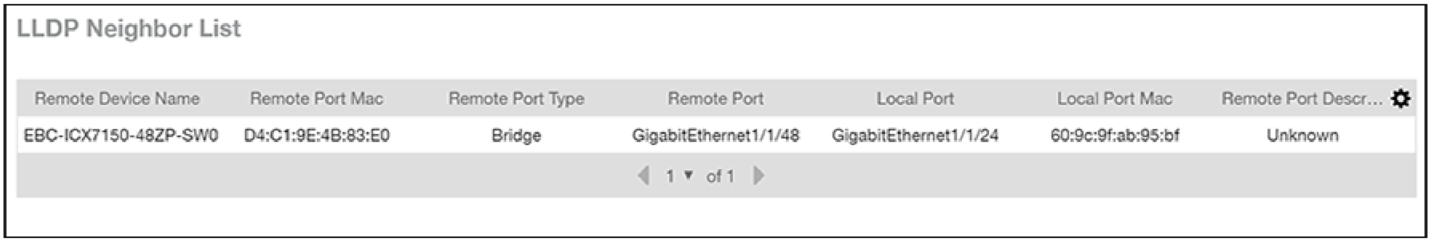


LLDP Neighbor List Tile

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 198 Switch Details - LLDP Neighbor List


LLDP Neighbor List

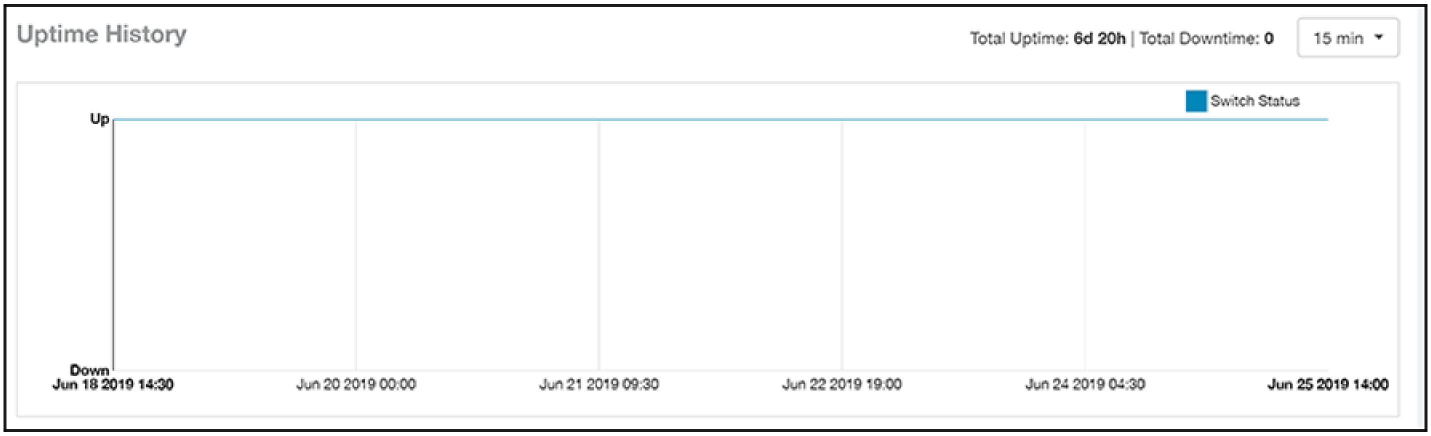
Remote Device Name	Remote Port Mac	Remote Port Type	Remote Port	Local Port	Local Port Mac	Remote Port Descr... ⚙
EBC-ICX7150-48ZP-SW0	D4:C1:9E:4B:83:E0	Bridge	GigabitEthernet1/1/48	GigabitEthernet1/1/24	60:9c:9f:ab:95:bf	Unknown

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 199 Switch Details - Uptime History



Comparison Reports Dashboard

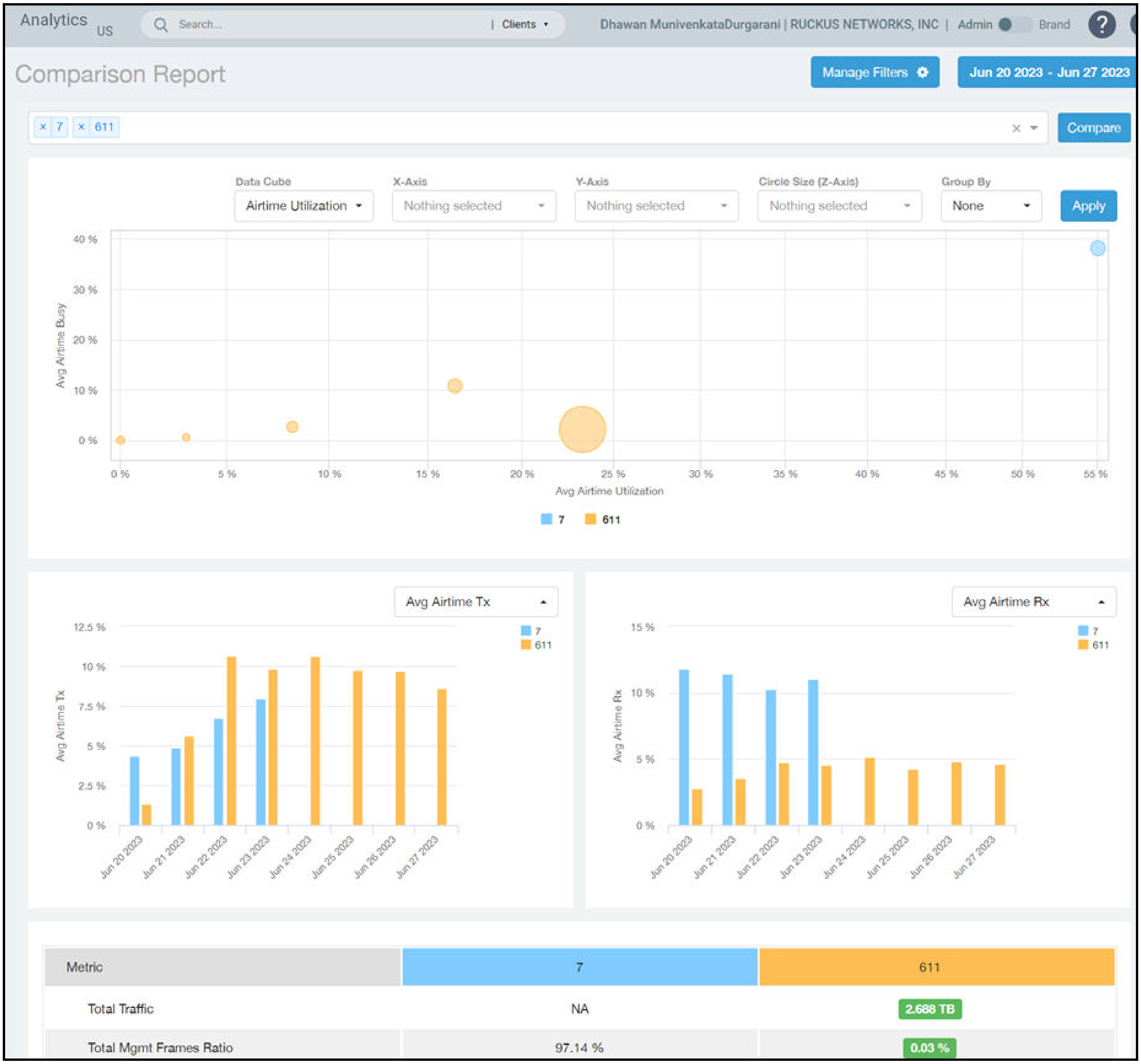
Compare Filters

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 200 Comparison Report



Data Cube: Airtime Utilization
X-Axis: Nothing selected
Y-Axis: Nothing selected
Circle Size (Z-Axis): Nothing selected
Group By: None

Metric	7	611
Total Traffic	NA	2.688 TB
Total Mgmt Frames Ratio	97.14 %	0.03 %

The Comparison Report consists of the following components:

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

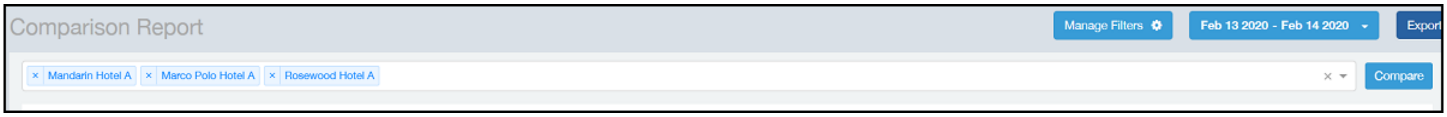
Compare Filters Tile

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.

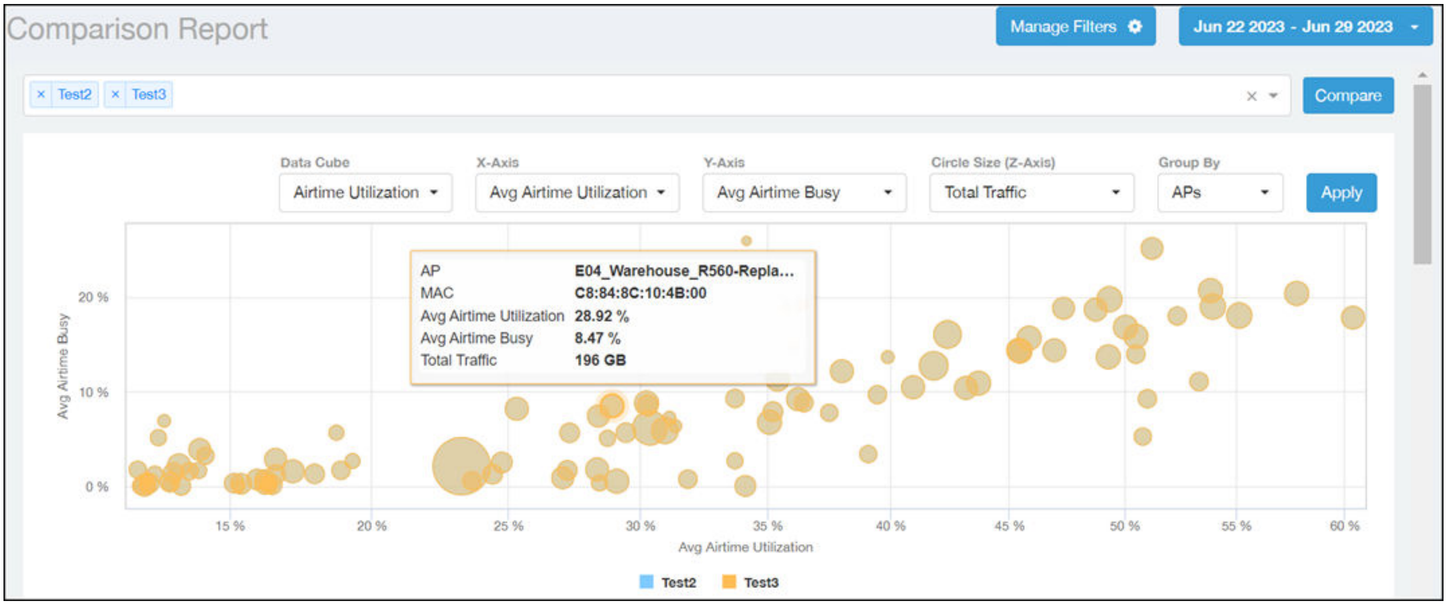
FIGURE 201 Comparison Reports - Compare Filters



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 202 Comparison Report - Overview scatter plot



Data Cube: Airtime Utilization
X-Axis: Avg Airtime Utilization
Y-Axis: Avg Airtime Busy
Circle Size (Z-Axis): Total Traffic
Group By: APs

AP: E04_Warehouse_R560-Repla...
MAC: C8:84:8C:10:4B:00
Avg Airtime Utilization: 28.92 %
Avg Airtime Busy: 8.47 %
Total Traffic: 196 GB

- Data Cube: 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 Dataset 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.

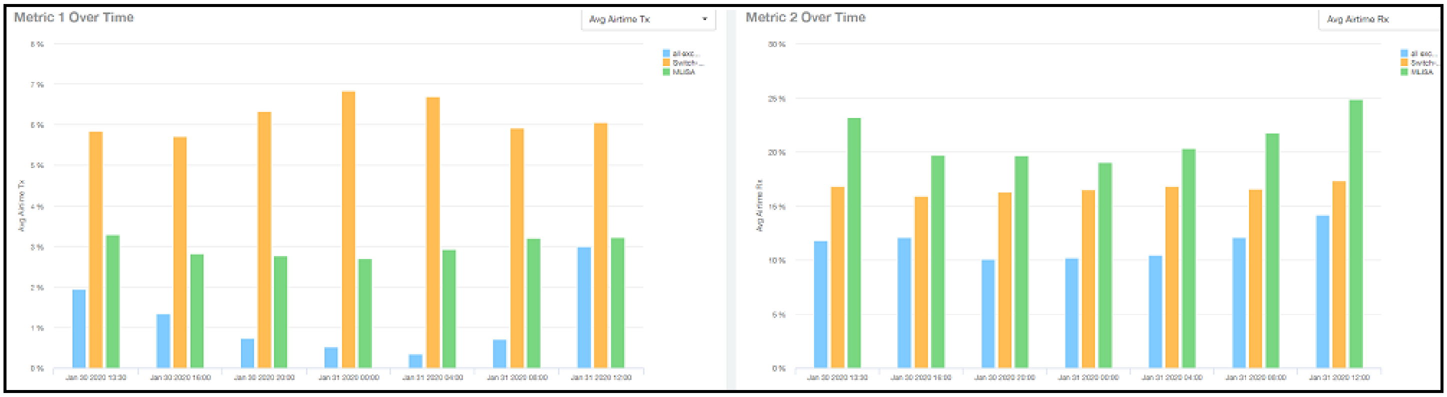
  You can toggle the circles below the chart (on and off) to display or not display the filters they represent.

  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.

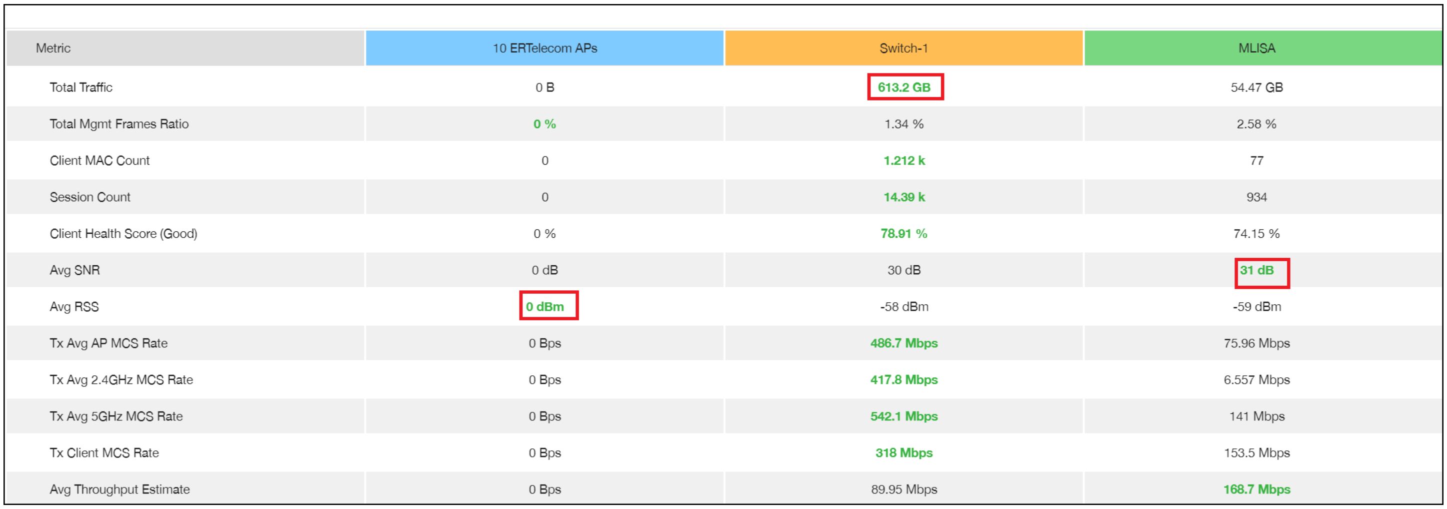
FIGURE 203 Comparison Report - Metric Over Time



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 204 Comparison Reports - Table



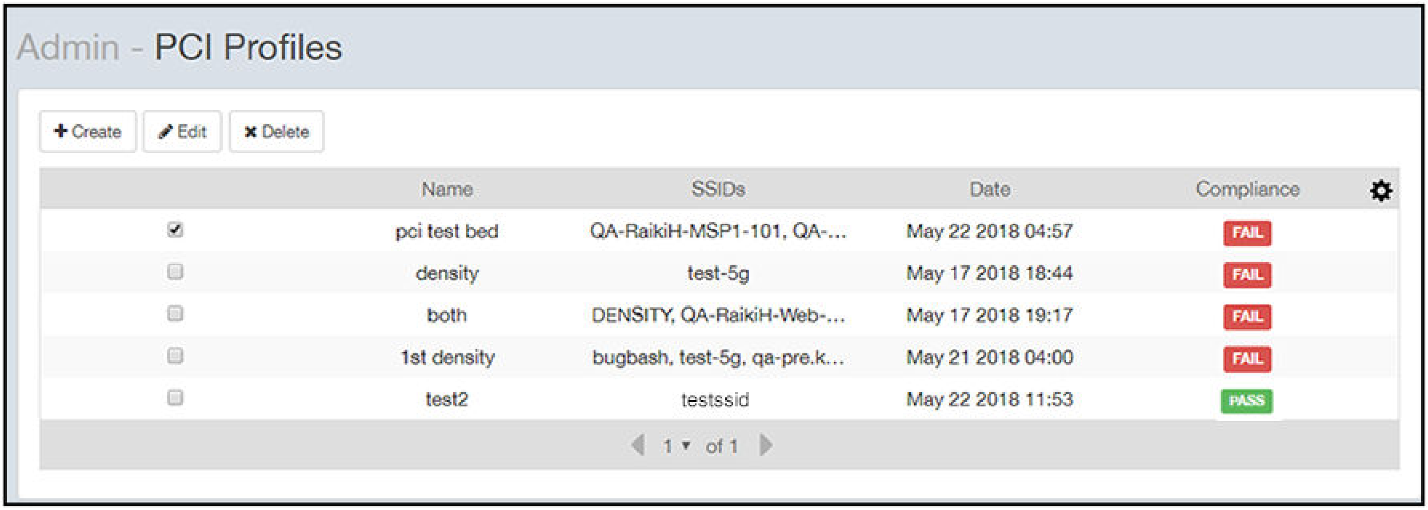
Metric	10 ERTelecom APs	Switch-1	MLISA
Total Traffic	0 B	613.2 GB	54.47 GB
Total Mgmt Frames Ratio	0 %	1.34 %	2.58 %
Client MAC Count	0	1.212 k	77
Session Count	0	14.39 k	934
Client Health Score (Good)	0 %	78.91 %	74.15 %
Avg SNR	0 dB	30 dB	31 dB
Avg RSS	0 dBm	-58 dBm	-59 dBm
Tx Avg AP MCS Rate	0 Bps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

PCI Profiles

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

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

FIGURE 205 PCI Profiles Screen



Admin - PCI Profiles

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

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

Creating a PCI Profile

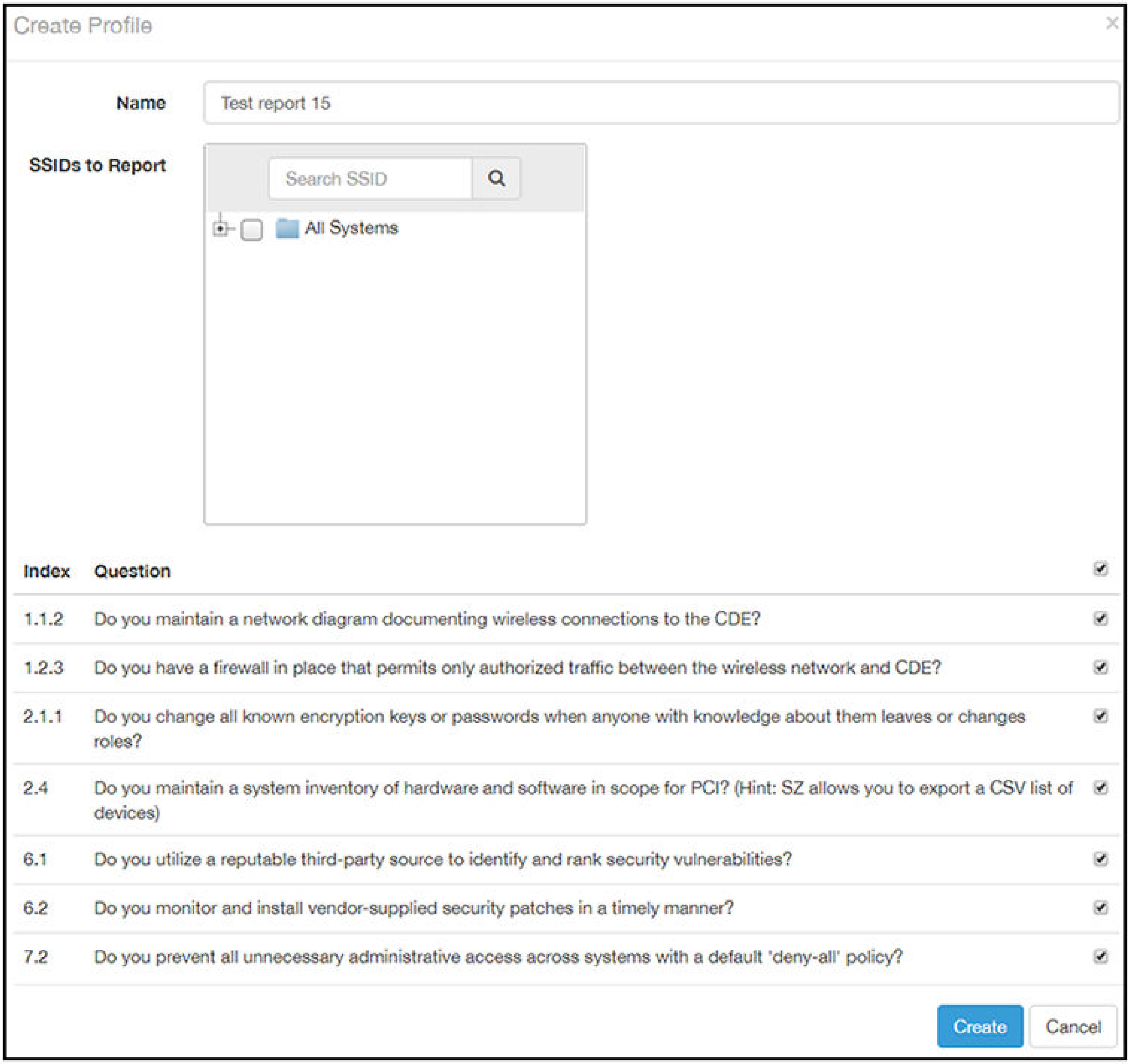
You can create a PCI profile to run a report that indicates if a WLAN is in compliance with the PCI Data Security Standard v3.2.

Follow the steps below to create a PCI profile:

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

   The **Create Profile** screen is displayed.

   FIGURE 206 Creating a PCI Profile



Create Profile

Name: Test report 15

SSIDs to Report: Search SSID

□ All Systems

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

2. Complete the screen configuration as follows:

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

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

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

     NOTE
     Not all questions are shown in the screen example above.

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

   The result of the profile (Pass or Fail) appears in the list of PCI profiles on the main PCI Profiles screen, an example of which is shown in Figure 205 on page 192.

Opening and Downloading a PCI Profile

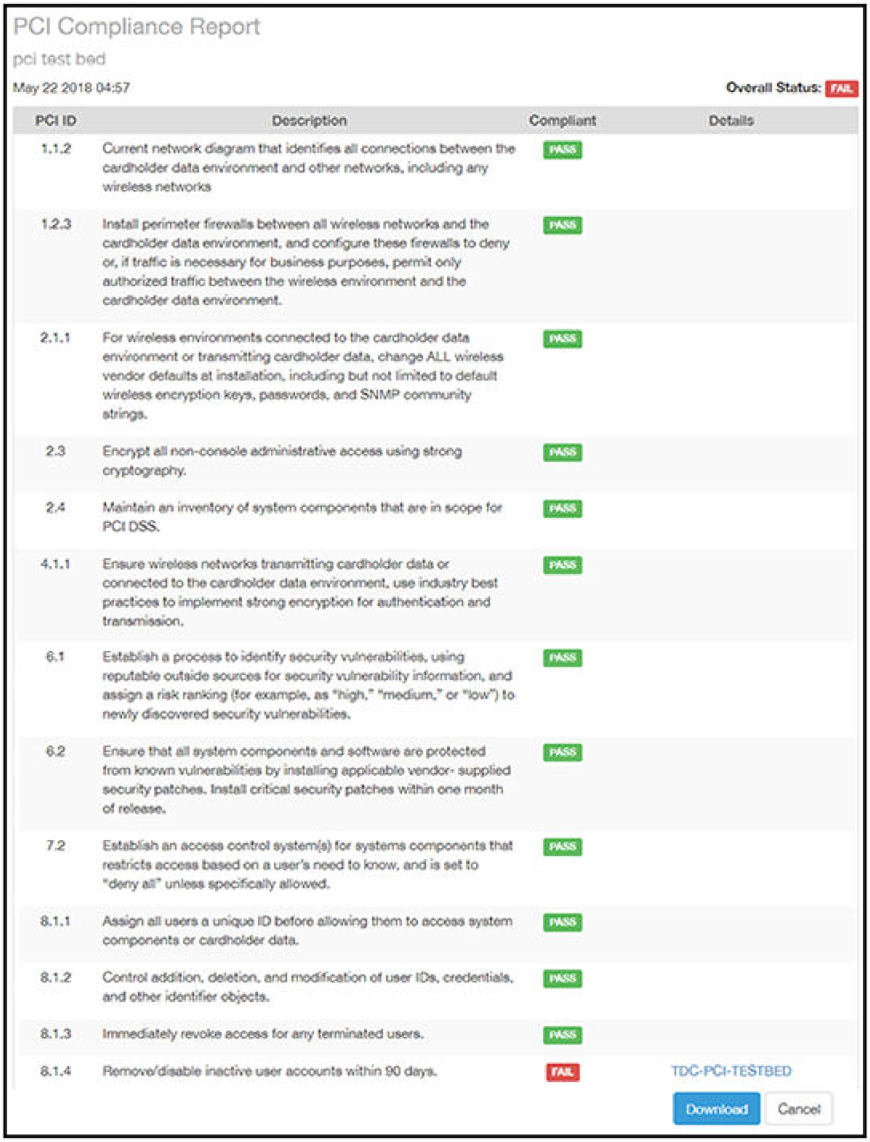
The PCI Profile gives you an overall status (Pass of Fail) as well as a breakdown of all categories you requested when you created the PCI profile.

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 205 on page 192, 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 207 PCI Report Example



PCI Compliance Report

pci test bed

May 22 2018 04:57

Overall Status: FAIL

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

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

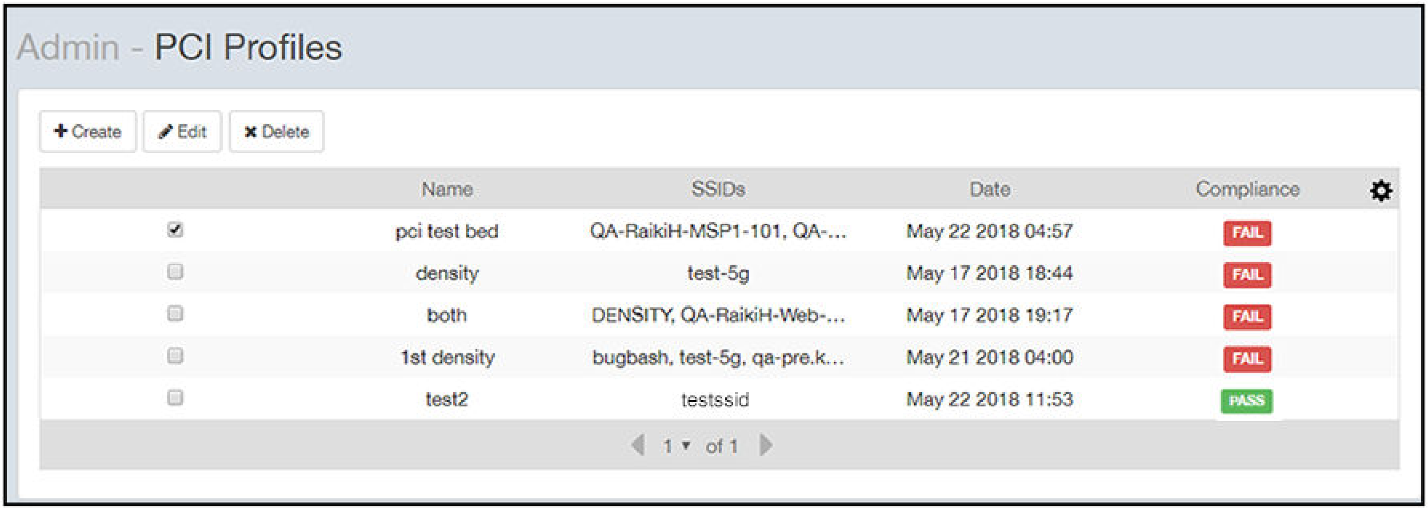
Editing or Deleting a PCI Profile

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 208 Edit or Delete PCI Profiles



Admin - PCI Profiles

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

Data Studio

- Data Studio........ 197
- Dataset Filters........ 214

Data Studio

Data Studio is a next-generation reporting tool that is fast and intuitive. It is easy to use and provides a rich user interface to create and edit charts and dashboards.

The Data Studio page displays the following tabs:

- Home tab
- Dashboard tab
- Charts tab
- Gallery tab
- Schedules tab

In the Brand mode, a brand can get an aggregate view of data of all the associated partners by creating dashboards, charts, and schedules. Note that, in the Brand mode, a brand can view dashboard templates created only by the users of the brand's RUCKUS Analytics service account. If a partner wants to share a dashboard template with the brand, the import and export dashboard option must be used.

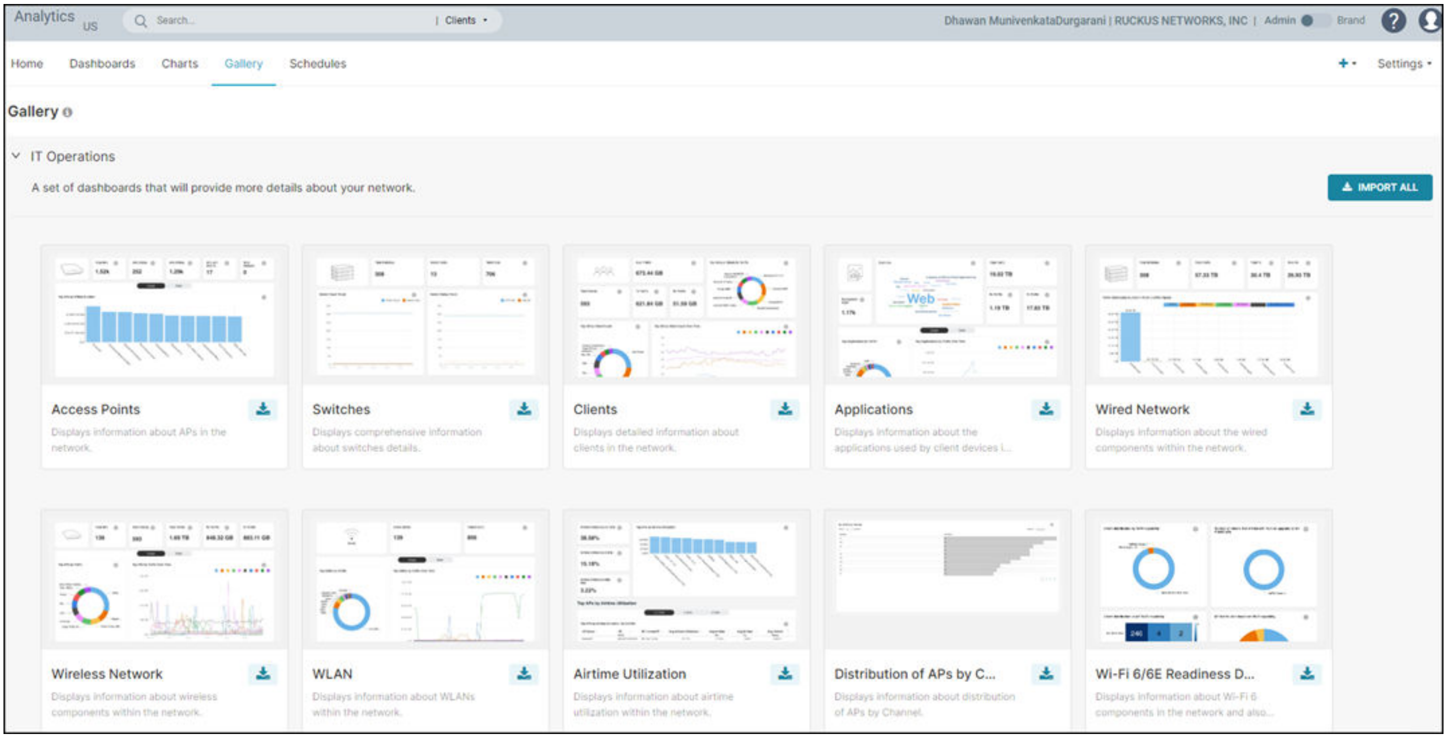
Gallery Tab

The **Gallery** tab displays a collection of pre-packaged dashboards. They are categorized as vertical-specific reports. The **Gallery** tab displays a preview into each of the dashboards listed on the page.

You can import all the dashboards in a category by clicking **Import all**, or view each dashboard and choose a specific dashboard to import by clicking the import icon next to it.

After importing the dashboard, it would appear in the **Dashboards** tab for review or analysis. The dashboards can be edited and deleted as required and are also customizable.

FIGURE 209 Gallery Tab - IT Operations



Gallery

IT Operations

A set of dashboards that will provide more details about your network.

Access Points
Displays information about APs in the network.

Switches
Displays comprehensive information about switches details.

Clients
Displays detailed information about clients in the network.

Applications
Displays information about the applications used by client devices i...

Wired Network
Displays information about the wired components within the network.

Wireless Network
Displays information about wireless components within the network.

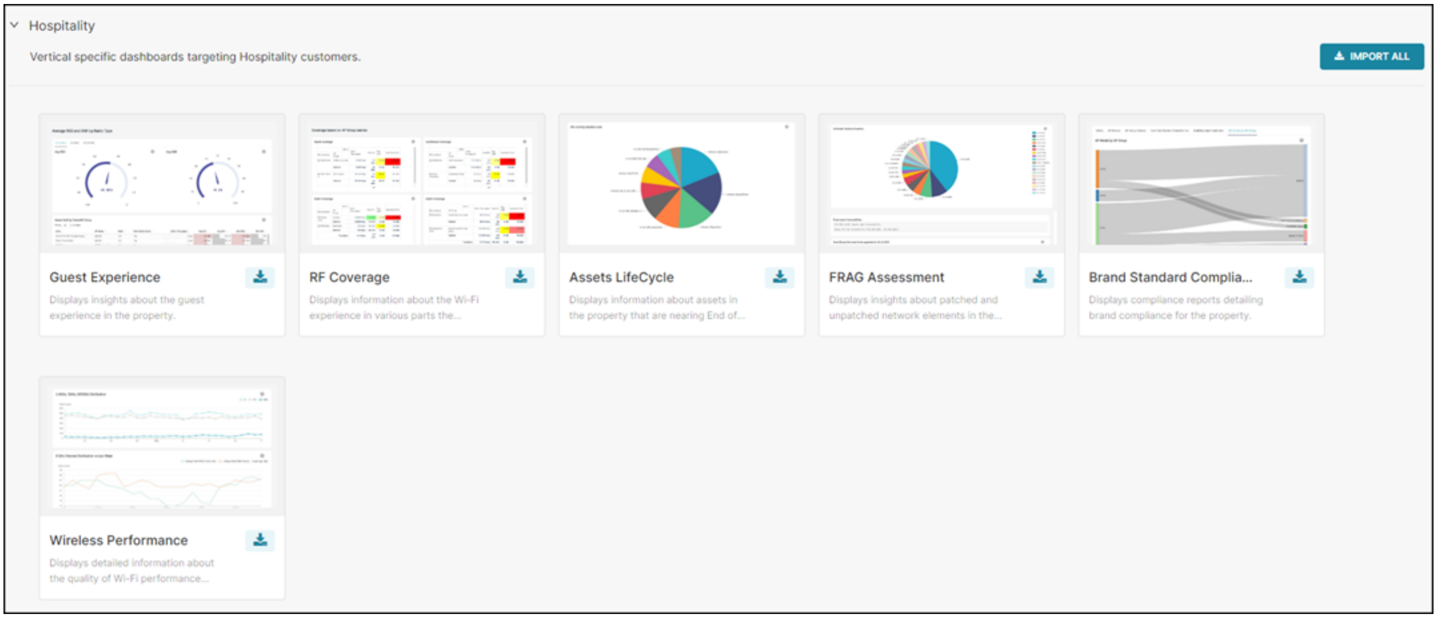
WLAN
Displays information about WLANs within the network.

Airtime Utilization
Displays information about airtime utilization within the network.

Distribution of APs by C...
Displays information about distribution of APs by Channel.

Wi-Fi 6/6E Readiness D...
Displays information about Wi-Fi 6 components in the network and also...

FIGURE 210 Gallery Tab - Hospatality



Hospitality

Vertical specific dashboards targeting Hospitality customers.

Guest Experience
Displays insights about the guest experience in the property.

RF Coverage
Displays information about the Wi-Fi experience in various parts the...

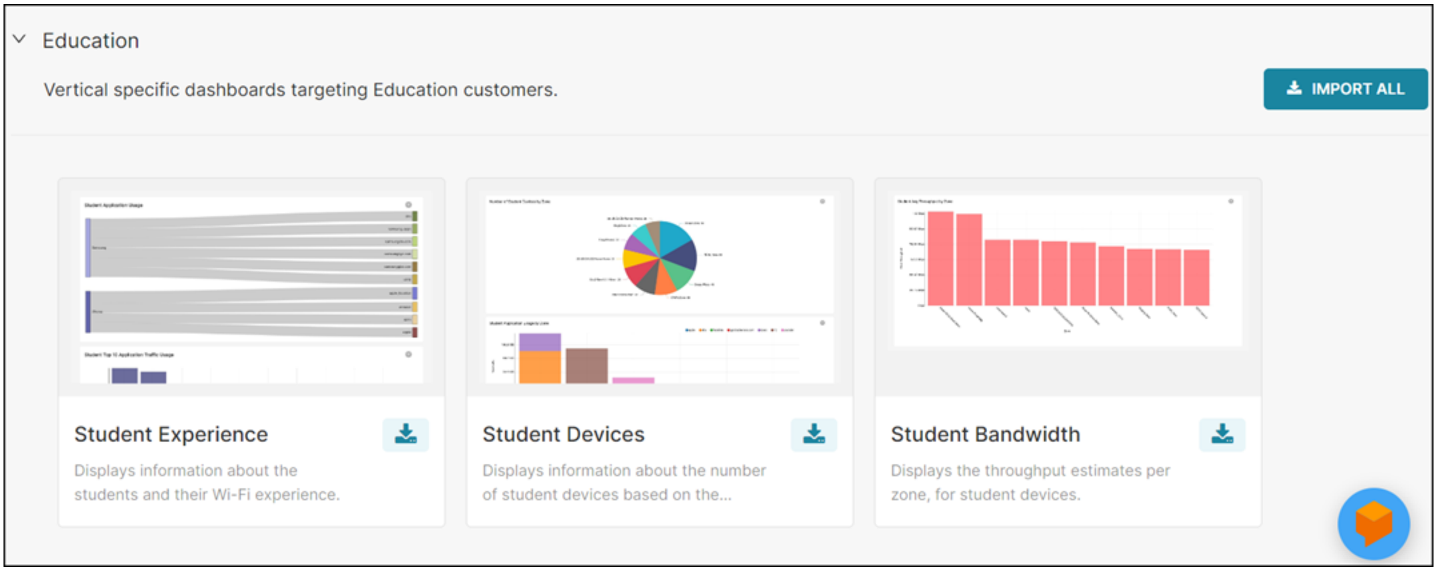
Assets LifeCycle
Displays information about assets in the property that are nearing End of...

FRAG Assessment
Displays insights about patched and unpatched network elements in the...

Brand Standard Complia...
Displays compliance reports detailing brand compliance for the property.

Wireless Performance
Displays detailed information about the quality of Wi-Fi performance...

FIGURE 211 Gallery Tab - Education



Education

Vertical specific dashboards targeting Education customers.

Student Experience

Displays information about the students and their Wi-Fi experience.

Student Devices

Displays information about the number of student devices based on the...

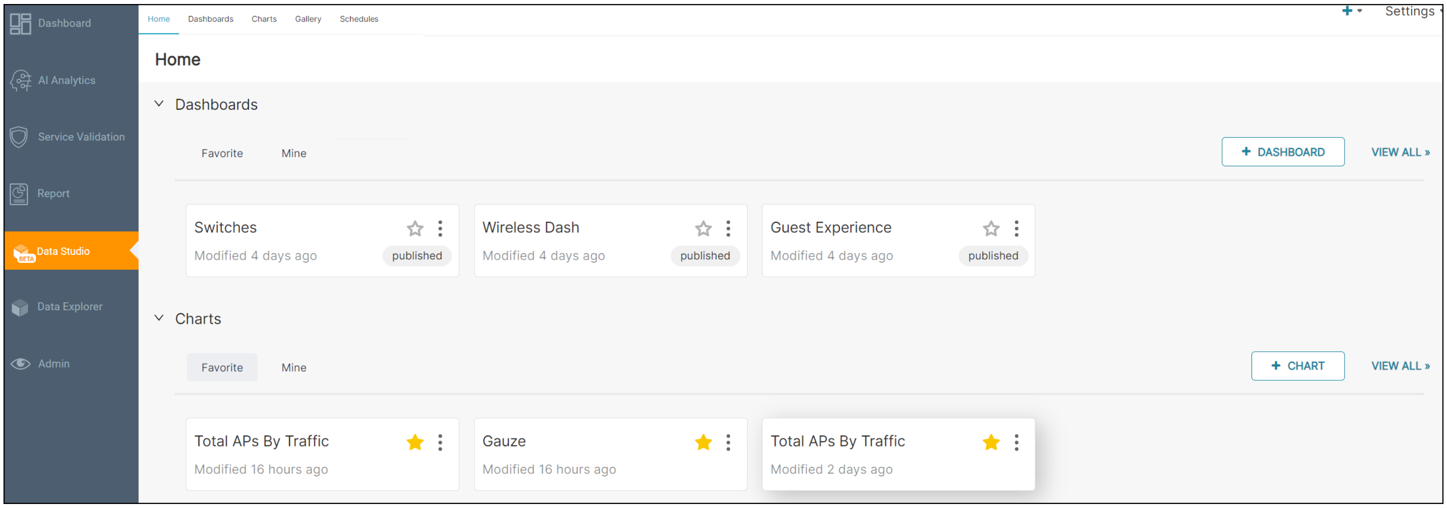
Student Bandwidth

Displays the throughput estimates per zone, for student devices.

Home Tab

The **Home** page displays dashboards and charts created within the system. You can click each dashboard or chart to view them individually and edit them.

FIGURE 212 Home Tab



Home

Dashboards

Switches
Modified 4 days ago
published

Wireless Dash
Modified 4 days ago
published

Guest Experience
Modified 4 days ago
published

Charts

Total APs By Traffic
Modified 16 hours ago

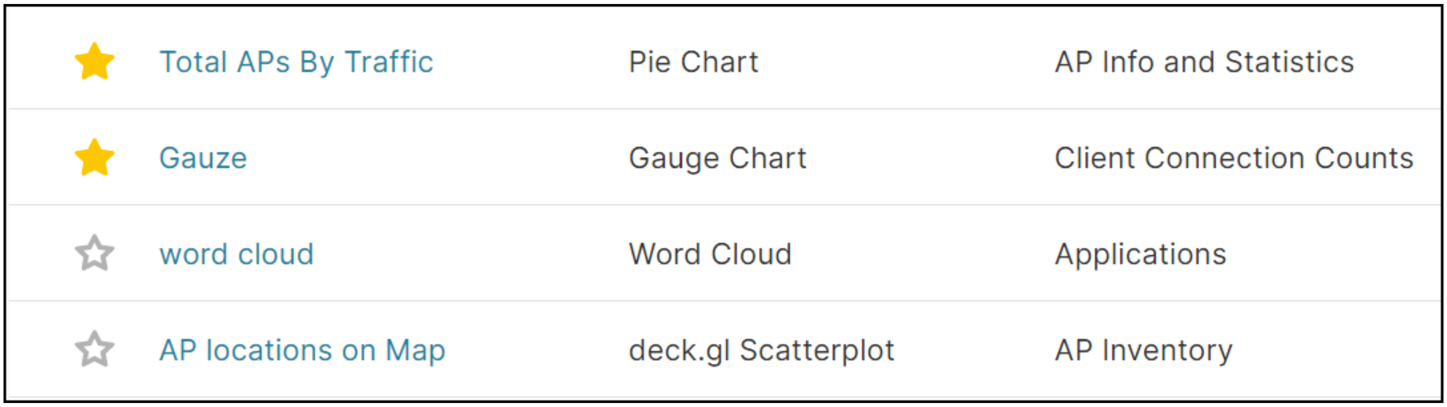
Gauze
Modified 16 hours ago

Total APs By Traffic
Modified 2 days ago

A dashboard can have a collection of one or more charts. Both dashboards and charts can be broadly customized into Favorite and Mine categories. You can click **View All** to see all the dashboards and charts within the network. Click the **+Dashboard** icon or **+Chart** icon to add dashboards and charts respectively.

Dashboards or charts that are viewed often can be marked as favorite by enabling the star icon as displayed in the image. Those marked appear within the **Favorite** tab.

FIGURE 213 Marking Favorites



★	Total APs By Traffic	Pie Chart	AP Info and Statistics
★	Gauze	Gauge Chart	Client Connection Counts
☆	word cloud	Word Cloud	Applications
☆	AP locations on Map	deck.gl Scatterplot	AP Inventory

You can create your own charts and dashboards and save them under the **Mine** tab.

Charts Tab

Charts aid in visualizing network data from as simple as a pie chart to complex network graphs. There are a variety of options to choose from, to visualize data.

The **Charts** tab displays all the charts created either as widgets or tables. It displays information about the owner of the chart, chart title, visualization type (such as bubble chart, pie chart, time-series chart, and so on), dataset type (such as AP inventory, applications, client info and statistics, and so on), favorites, and modification details. Every chart can be selected and deleted.

> **NOTE**
> Charts can be deleted or edited only by the owner. Other users can make a copy of the chart, by using the **Save As** option, and become an owner.

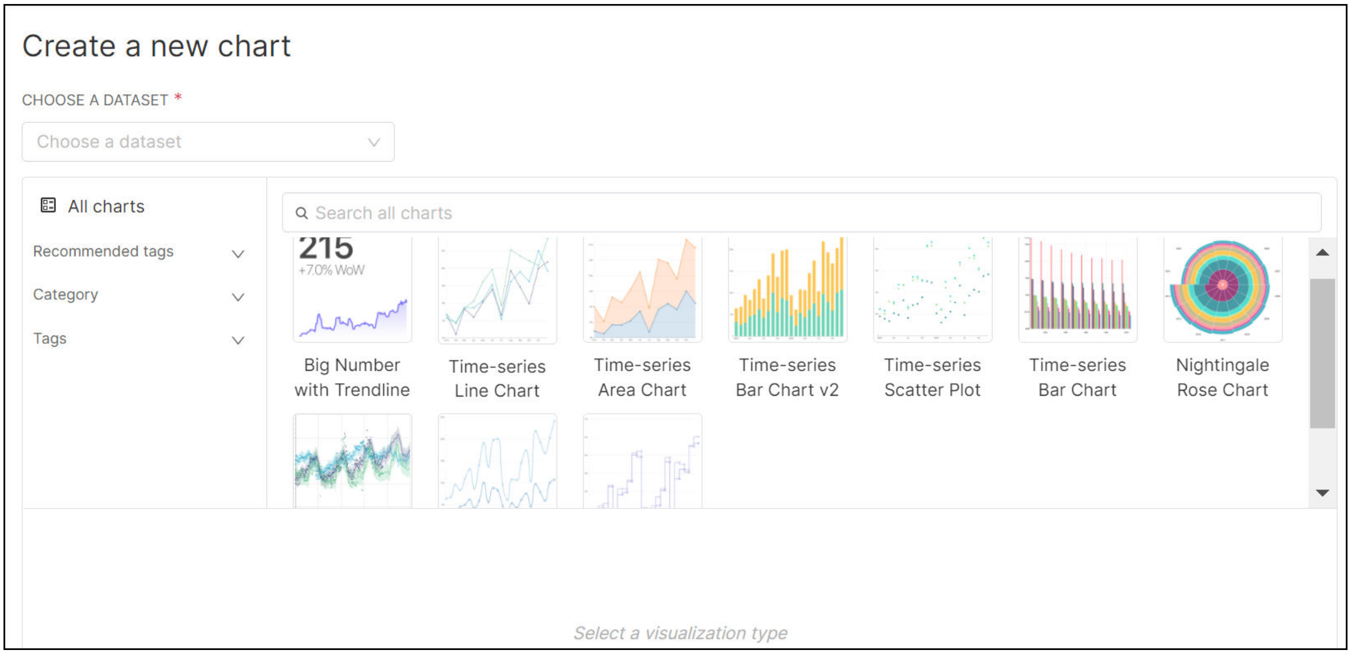
Click **Bulk Select** to select several charts at a time and delete them all at once. You can search for a particular chart in the search field, by title. The list of charts can also be sorted and viewed by the options recently modified, least recently modified, and in alphabetical order as well.

Creating a Chart

Complete the following steps to create a **Chart**.

1. Click **+Chart** icon. The **Create a new chart** page is displayed.

FIGURE 214 Creating a New Chart



Create a new chart

CHOOSE A DATASET *

2. In the **Choose a Dataset** field, select a **Dataset** from the list. Refer to Dataset Filters on page 214 **Columns** table, for more information on the **Dataset**.

3. In the **Choose a Chart Type** tab, select a chart type. You can choose a chart by filtering with following options:

   - **All charts**: This option displays the most used charts across organization.
   - **Recommended tags**: The option displays the most suitable charts based on the data being analyzed. This feature assists in optimal and meaningful data visualization. You can choose a chart from the following filter types:
     - **Popular**: This option displays the most popular charts that are used across organization.
     - **ECharts**: This option displays the **Funnel**, **Treemap**, **Gauge**, and various **Time-series** charts.
     - **Advanced-Analytics**: This option displays the **Big Number with Trendline** and various **Time-series** charts.
   - **Category**: The option displays the most used charts across organization based on the following catagories:
     - **Correlation**: This option displays the **Heatmap**, **Calendar Heatmap**, and **Bubble** charts.
     - **Distribution**: This option displays the **Histogram**, **Box Plot**, and **Horizon** charts.
     - **Evolution**: This option displays the various **Time-series** charts.
     - **Flow**: This option displays the **Sankey Diagram** and **Chord Diagram** charts
     - **KPI**: This option displays the **Big Number**, **Bullet**, **Funnel**, and **Gauge** charts.
     - **Map**: This option displays the **Deck.GL Scatterplot** chart.
     - **Parts of a Whole**: This option displays the **Pie**, **Treemap**, **Sunburts**, **Partitions**, and **Treemap** charts.
     - **Ranking**: This option displays the **Bar**, **Word**, **Nightingale**, and **Parallel** charts.
     - **Table**: This option displays the various **Tables** charts.
   - **Tags**: The option displays all available charts filtered by chart type.

   After you select the chart, a breif introduction and examples about the selected chart is displayed at the bottom.

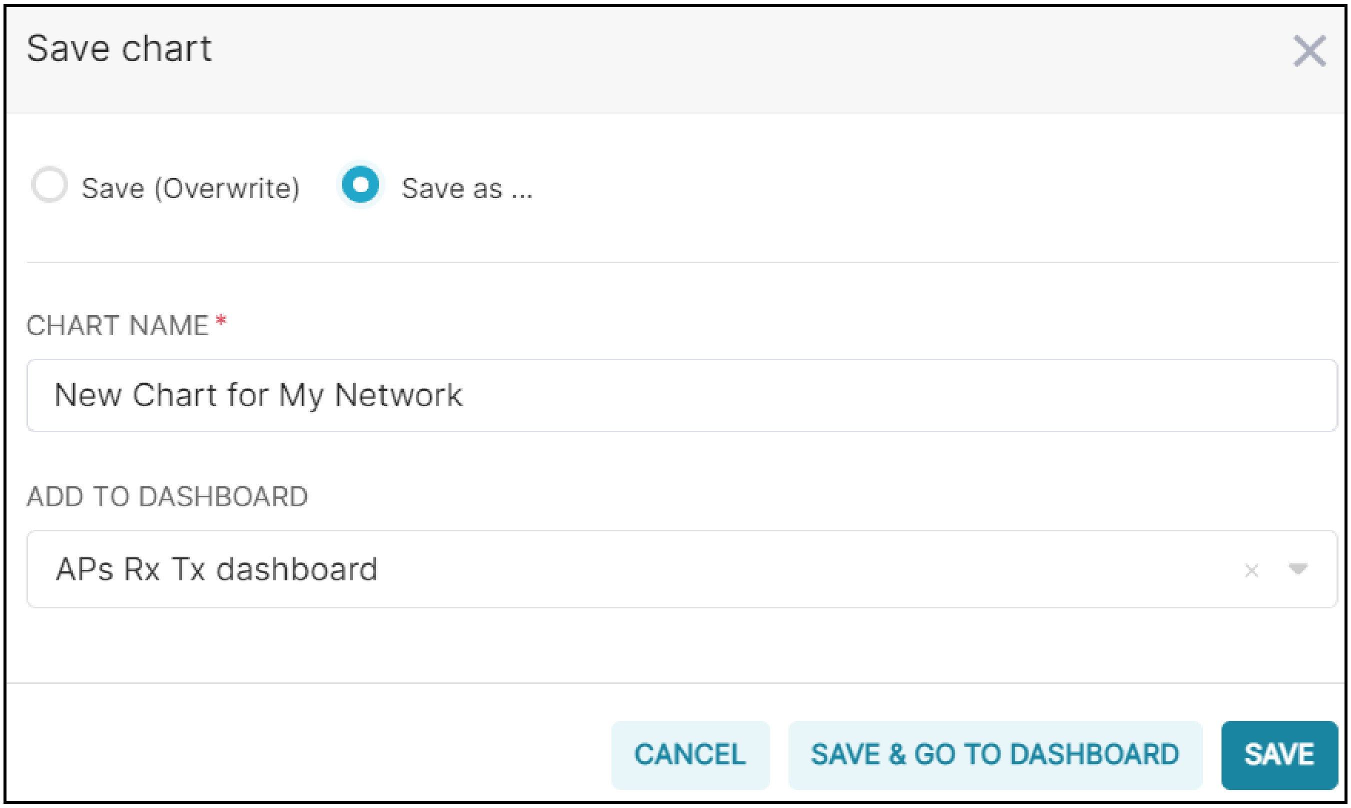
4. Click **Create New Chart**. A new page is displayed with two tabs **Data** and **Customize**.

From the **Data** tab, you can select the chart type, time, query, annotation and layers for the chart, and the analytics trends you wish to see. You can also open the left panel by clicking the table icon, which displays all the columns and calculated metrics of the dataset selected.

From the **Customize** tab you can select the color schemes for the chart, legend, X-axis and Y-axis parameters, and tool tip options.

5. Double click **Untitled** and enter a title for the chart.
6. Configure the **Data** tab. Refer to Dataset Filters on page 214 **Columns** and **Metrics** table, for more information on the columns and metrics.
7. If required, configure the **Customize** tab.
8. Click **Run** to view the chart that's created after processing the configuration settings.
9. Click **Save**. The **Save chart** dialog box is displayed, complete the following steps.

FIGURE 215 Save Chart Dialogue Box



Save chart

○ Save (Overwrite) ● Save as ...

CHART NAME *

New Chart for My Network

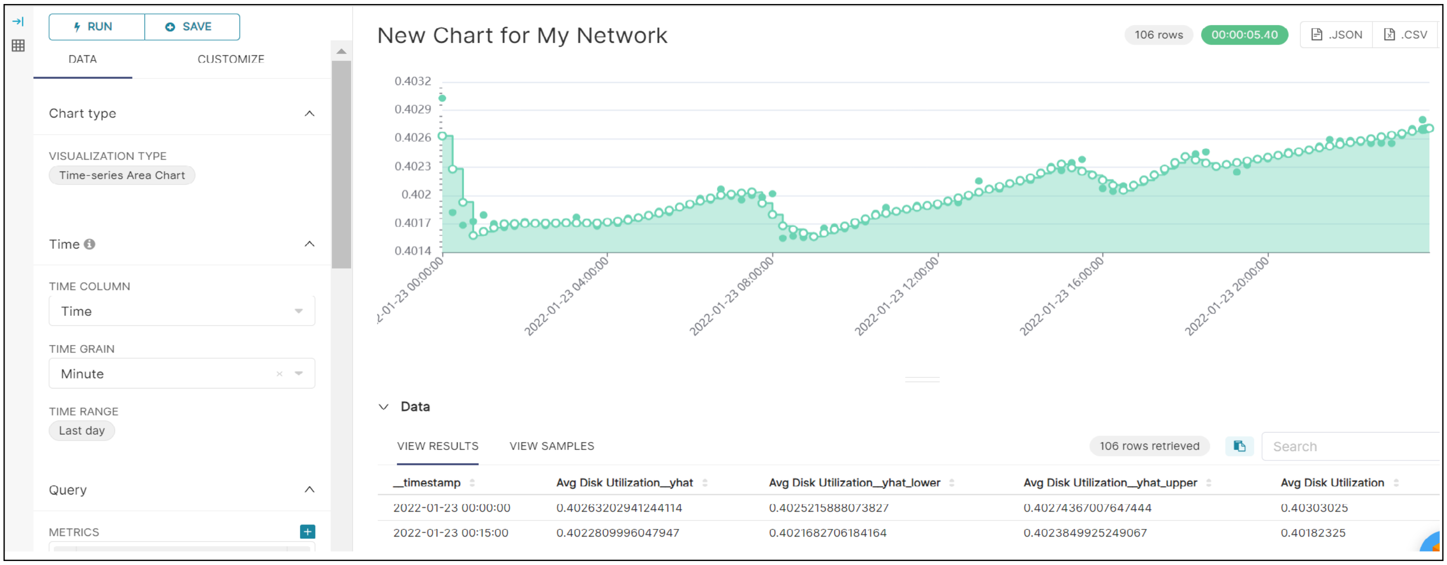
ADD TO DASHBOARD

APs Rx Tx dashboard

a. Complete the following fields:
   - **Chart Name**: Enter a name for the chart.
   - **Add to Dashboard**: Select a dashboard from the list. This option saves the chart to a **Dashboard** page.
b. Click **Save** to save the chart to the **Charts** page. If you have selected a dashboard, you can select **Save & Go To Dashboard** this will redirect you to the **Dashboard** page.

The following example is time series chart that displays the *average disk utilization* both as a time-series graph and as a table, in a green color scheme. The green dots represent the predictive analysis information calculated by the system against the green circles that are markers on the graph. You can export the chart into a `.json` or `.csv` file format, and also download it as a JPG file or image. Clicking **View Query** displays the script that is run to fetch data for a specific chart.

FIGURE 216 Sample Chart - "New Chart for My Network"



VISUALIZATION TYPE
Time-series Area Chart

TIME COLUMN
Time

TIME GRAIN
Minute

TIME RANGE
Last day

__timestamp	Avg Disk Utilization__yhat	Avg Disk Utilization__yhat_lower	Avg Disk Utilization__yhat_upper	Avg Disk Utilization
2022-01-23 00:00:00	0.40263202941244114	0.4025215888073827	0.40274367007647444	0.40303025
2022-01-23 00:15:00	0.4022809996047947	0.4021682706184164	0.4023849925249067	0.40182325

In the following example, the chart "New Chart for My Network" is added to the dashboard "APs Rx Tx dashboard".

FIGURE 217 Chart Named "New Chart for My Network" Added to Dashboard "APs Rx Tx dashboard"

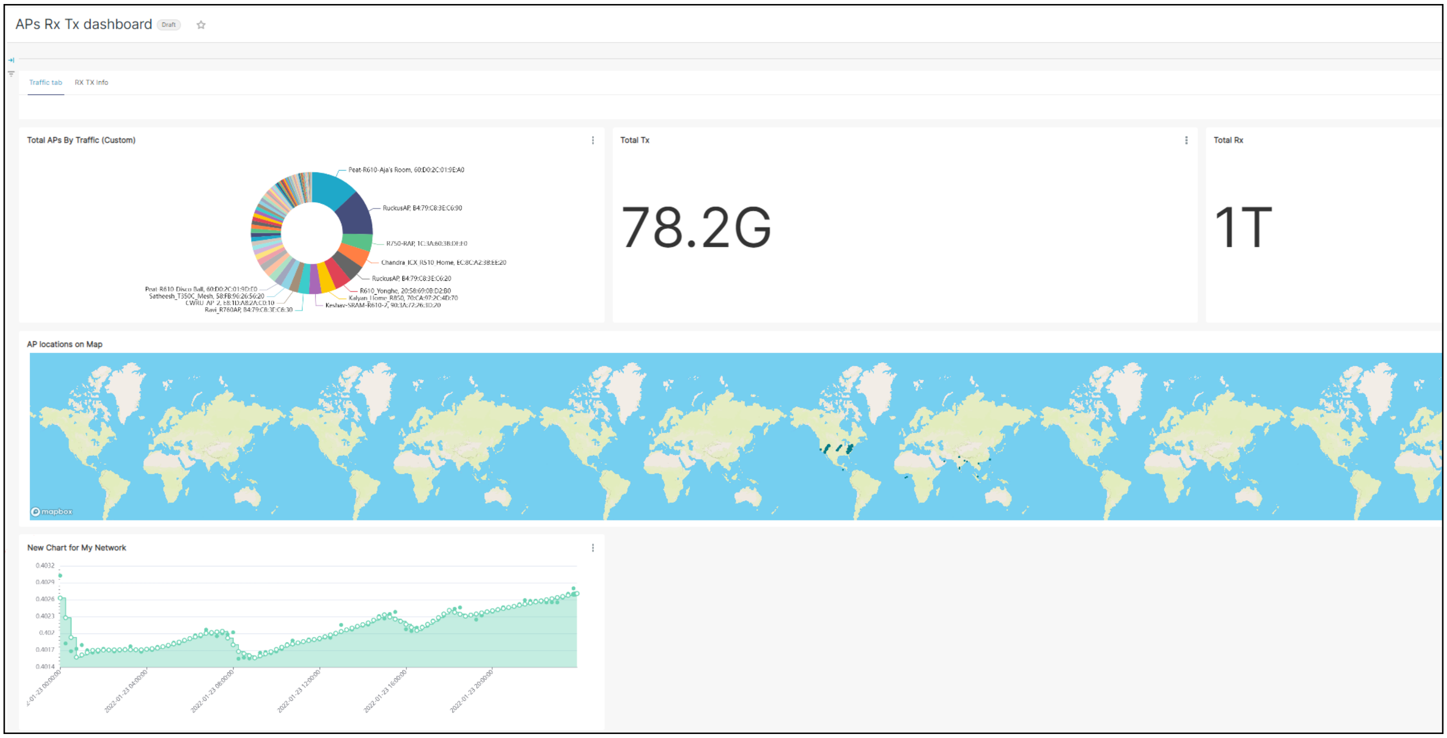

APs Rx Tx dashboard
Draft
Traffic tab
RX TX Info
Total APs By Traffic (Custom)
Peat-R610-Aja's Room, 60:D0:2C:01:9E:A0
RuckusAP, B4:79:C8:3E:C6:90
R750-RAP, 1C:3A:60:3B:DE:E0
Chandra_ICX_R510_Home, EC:8C:A2:3B:EE:20
RuckusAP, B4:79:C8:3E:C6:20
R610_Yonghe, 20:58:69:0B:D2:B0
Kalyan_Home_R850, 70:CA:97:2C:4D:70
Keshav-SRAM-R610-2, 90:3A:72:26:3D:20
Peat-R610-Disco Ball, 60:D0:2C:01:9D:E0
Satheesh_T350C_Mesh, 58:FB:96:26:56:20
CWRU_AP_2, E8:1D:A8:2A:C0:10
Ravi_R760AP, B4:79:C8:3E:C6:30
Total Tx
78.2G
Total Rx
1T
AP locations on Map
mapbox
New Chart for My Network
0.4032
0.4029
0.4026
0.4023
0.402
0.4017
0.4014

FIGURE 218 New Chart also Added to the Charts Tab

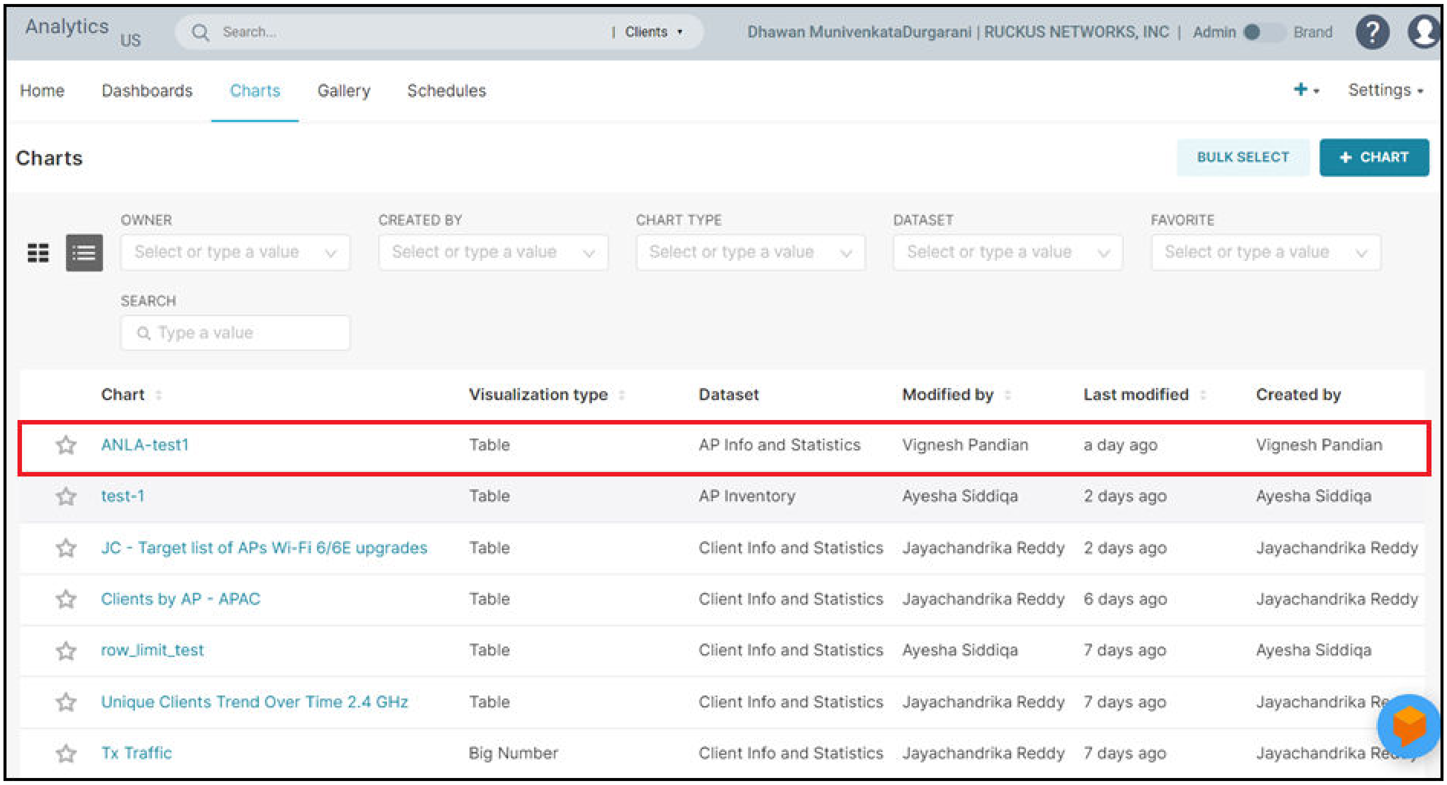


Chart	Visualization type	Dataset	Modified by	Last modified	Created by
☆ ANLA-test1	Table	AP Info and Statistics	Vignesh Pandian	a day ago	Vignesh Pandian
☆ test-1	Table	AP Inventory	Ayesha Siddiqa	2 days ago	Ayesha Siddiqa
☆ JC - Target list of APs Wi-Fi 6/6E upgrades	Table	Client Info and Statistics	Jayachandrika Reddy	2 days ago	Jayachandrika Reddy
☆ Clients by AP - APAC	Table	Client Info and Statistics	Jayachandrika Reddy	6 days ago	Jayachandrika Reddy
☆ row_limit_test	Table	Client Info and Statistics	Ayesha Siddiqa	7 days ago	Ayesha Siddiqa
☆ Unique Clients Trend Over Time 2.4 GHz	Table	Client Info and Statistics	Jayachandrika Reddy	7 days ago	Jayachandrika Re
☆ Tx Traffic	Big Number	Client Info and Statistics	Jayachandrika Reddy	7 days ago	Jayachandrika Re

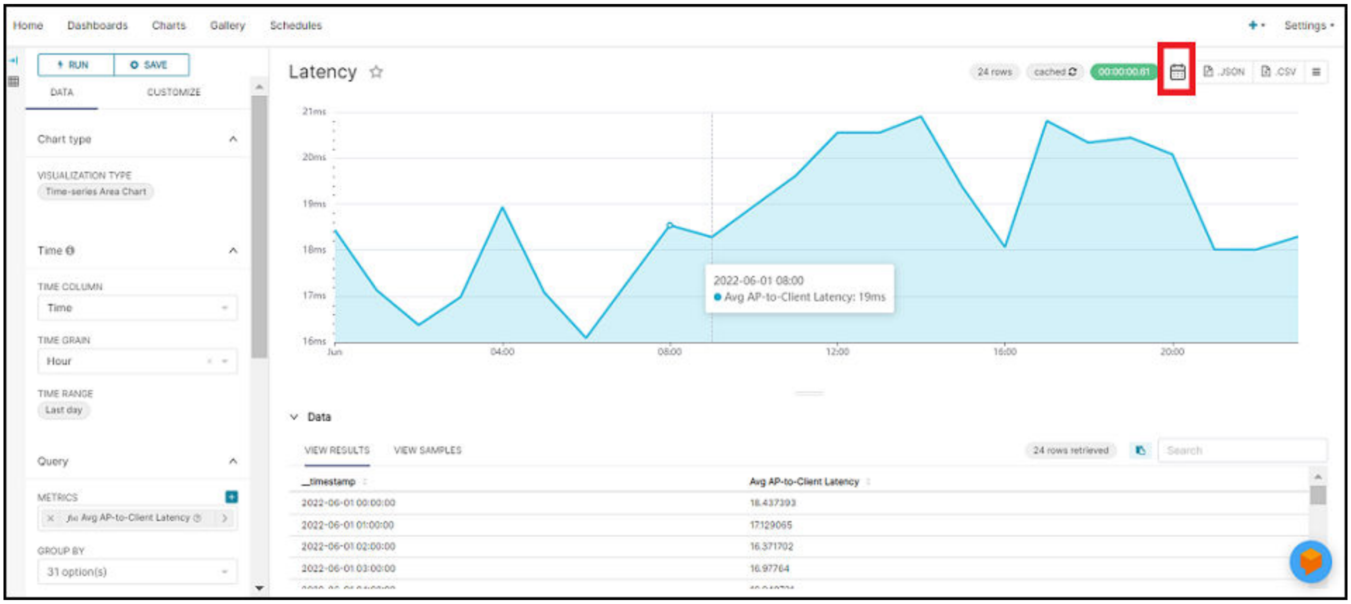
The owner of the chart is provided with an option to schedule an email report from the screen while viewing it. Click a chart to view the details.

Create a Report Schedule for the Chart

Complete the following steps to create an email schedules for the chart. The created schedule is displayed in the **Schedules** tab.

1. Click the 📅 icon at the top-right corner. The **New Email Schedule** dialog box is displayed.

FIGURE 219 Schedule Email from Chart Page



VISUALIZATION TYPE: Time-series Area Chart

TIME COLUMN: Time

TIME GRAIN: Hour

TIME RANGE: Last day

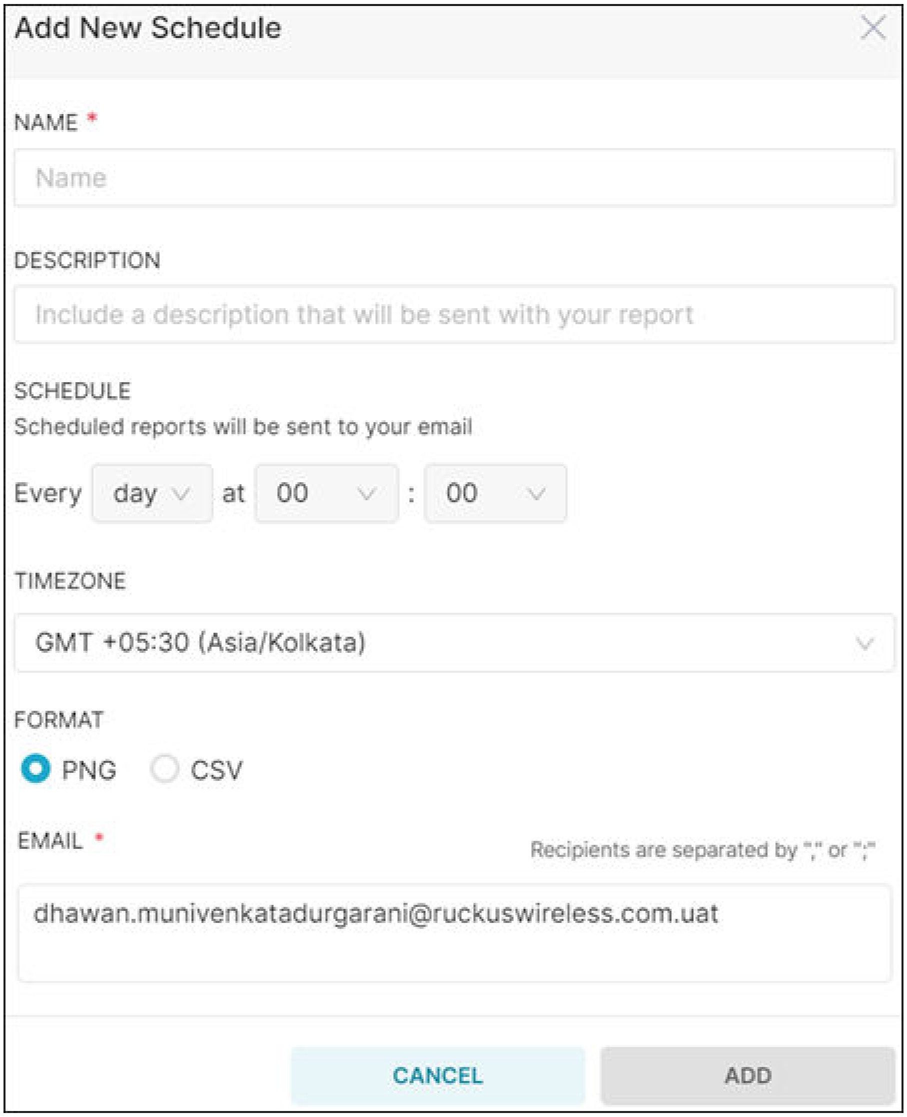
METRICS: Avg AP-to-Client Latency

GROUP BY: 31 option(s)

__timestamp	Avg AP-to-Client Latency
2022-06-01 00:00:00	18.437393
2022-06-01 01:00:00	17.129065
2022-06-01 02:00:00	16.371702
2022-06-01 03:00:00	16.97764

2. Complete the following fields:

FIGURE 220 New Email Schedule for Chart



Add New Schedule

NAME *

DESCRIPTION

SCHEDULE

Scheduled reports will be sent to your email

Every day at 00 : 00

TIMEZONE

GMT +05:30 (Asia/Kolkata)

FORMAT

● PNG ○ CSV

EMAIL * Recipients are separated by "," or ";"

dhawan.munivenkatadurgarani@ruckuswireless.com.uat

- **Name**: Add a name to the schedule.
- **Description**: If necessary, add a description of the schedule.
- **Schedule**: Select the scheduled interval **Day**, **Week**, or **Month**, and also the **Hours**, and **Minutes** at which the reports should be sent to your email.
- **Timezone**: Select a timezone from the list.
- **Format**: Select a report format **PNG**, or **CSV**.
- **Email**: Enter the email address to which the report will be sent.

3. Click **Add** to create a report schedule for the chart.

Dashboard Tab

Creating dashboards in the Data Studio page is simple and easy. The dashboards are a collection of charts which is highly customizable according to user needs.

The Dashboard tab displays all the dashboards created either as widgets or tables (contains one or many widgets, and or charts). It displays information about the owner of the dashboard, dashboard title, status (Published or Draft), modification details and so on. Individual dashboards can be selected and deleted, or they can be selected in bulk and deleted. Only dashboard owners can edit or delete them. You can search for a particular dashboard in the search field, by title. The dashboard information can also be sorted and viewed by the options recently modified, least recently modified, and in alphabetical order. You can also filter the dashboards by using created by or owner drop-downs.

Creating a Dashboard

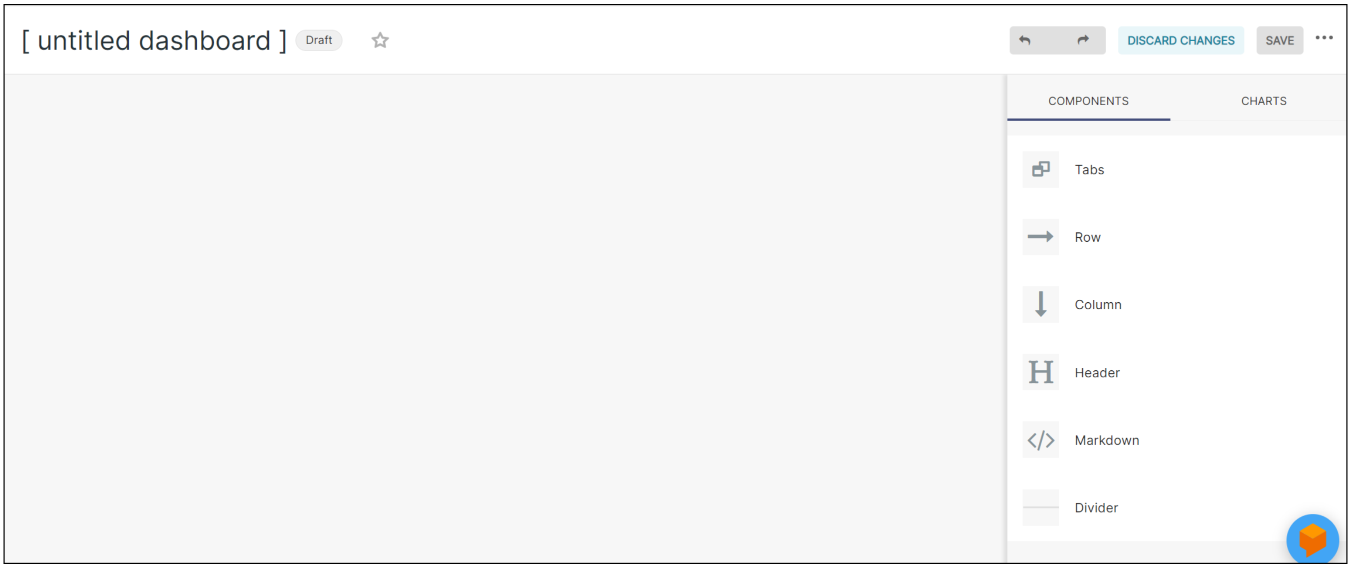
Complete the following steps to create a **Dashboard**.

1. Click **+Dashboard** icon. The **Untitled Dashboard** page is displayed with two tabs **Components** and **Charts**.

   From **Components**, you can add various components to customize the appearance of the dashboard, such as tabs, rows, columns, dividers, headers, and markdowns.

   From **Charts**, you can also choose the charts you want to add to the dashboard and view them based on their time of creation, dataset, visualization type, and name.

   FIGURE 221 Creating a New Dashboard



2. Double click **Untitled Dashboard** and enter a title for the dashboard.
3. If required, configure the **Components**.
4. Click **+Create a New Chart** to add a new chart, refer **Creating a Chart** section. To add an existing chart, select the **Charts** tab, then drag and drop the required charts from the list to the dashboard.

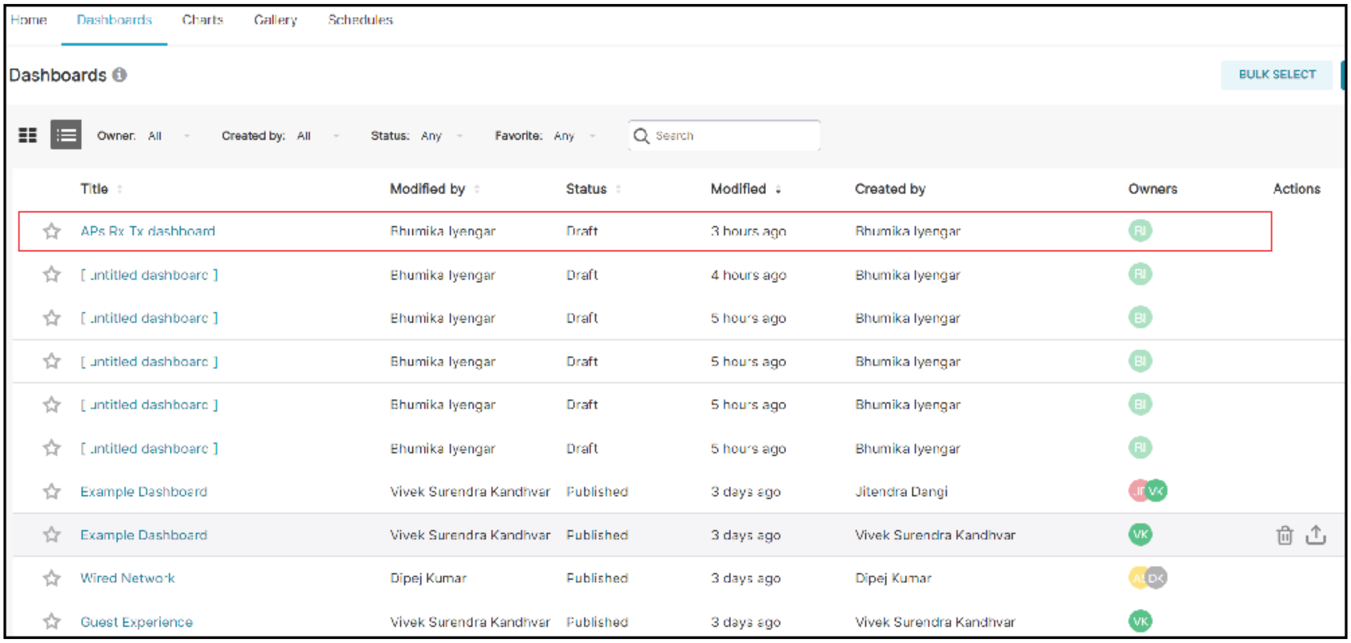
   Charts added to the dashboard appear as a widget or tile. You can click on the chart to modify the title and also expand or contract the chart to fit within the dashboard. You can also delete a chart within the dashboard by clicking the delete icon in the widget. For more information about the chart, you can click the data source link from where the chart is included.

5. Click **Save** to save the dashboard with the same name, or select **Options (three dots)** > **Save As** to overwrite the dashboard with the same name or save the dashboard with a new name, or select the option **also copy (duplicate) charts** to duplicate the dashboard and save it with a new name.

   The dashboard is saved by default as a **Draft**, and listed in the **Dashboard** tab.

   NOTE
   Click **Discard Changes** to removes changes done to the dashboard.

FIGURE 222 New Dashboard Added to the Dashboard Tab



Dashboards

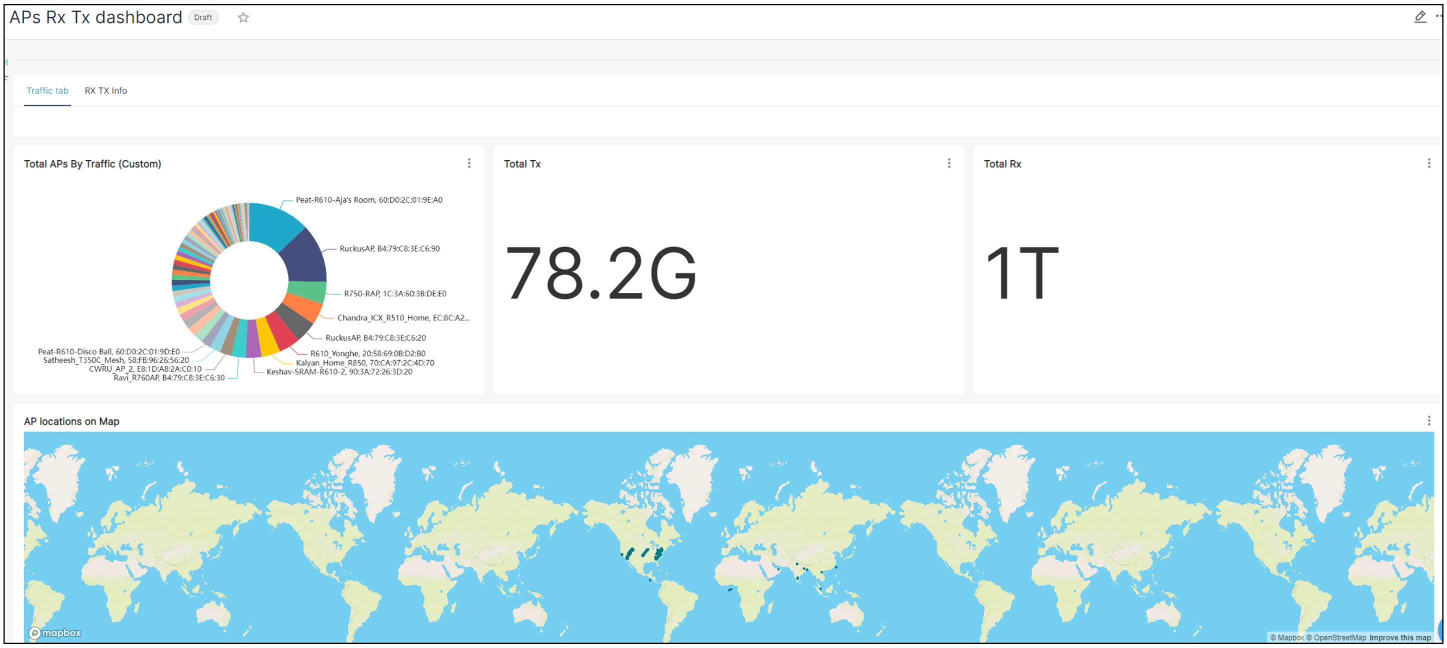
Owner: All   Created by: All   Status: Any   Favorite: Any

Title	Modified by	Status	Modified	Created by	Owners	Actions
☆ APs Rx Tx dashboard	Bhumika Iyengar	Draft	3 hours ago	Bhumika Iyengar	BI	
☆ [untitled dashboard]	Bhumika Iyengar	Draft	4 hours ago	Bhumika Iyengar	BI	
☆ [untitled dashboard]	Bhumika Iyengar	Draft	5 hours ago	Bhumika Iyengar	BI	
☆ [untitled dashboard]	Bhumika Iyengar	Draft	5 hours ago	Bhumika Iyengar	BI	
☆ [untitled dashboard]	Bhumika Iyengar	Draft	5 hours ago	Bhumika Iyengar	BI	
☆ [untitled dashboard]	Bhumika Iyengar	Draft	5 hours ago	Bhumika Iyengar	BI	
☆ Example Dashboard	Vivek Surendra Kandhvar	Published	3 days ago	Jitendra Dangi	JD VK	
☆ Example Dashboard	Vivek Surendra Kandhvar	Published	3 days ago	Vivek Surendra Kandhvar	VK	🗑 ⇪
☆ Wired Network	Dipej Kumar	Published	3 days ago	Dipej Kumar	AL DK	
☆ Guest Experience	Vivek Surendra Kandhvar	Published	3 days ago	Vivek Surendra Kandhvar	VK	

6. Select **Options (three dots)** > **Refresh Dashboard** to refresh the dashboard manually.
7. Complete the following steps to set up automatic dashboard refresh:
   a. Select **Options (three dots)** > **Set auto-refresh interval**. The **Refresh Interval** dialog box is displayed.
   b. Select the **Refresh Frequency** from the list and click **Save**.

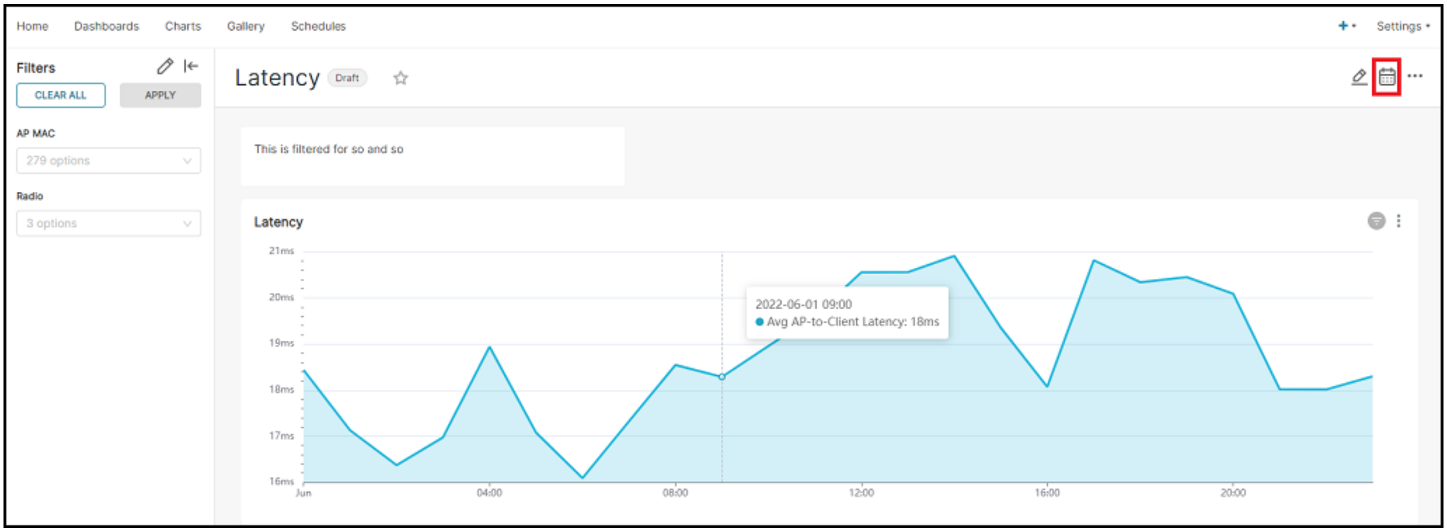
The following is a sample dashboard titled "APs Rx Tx dashboard", created with two tabs - one for network traffic and another for Rx and Tx values. It includes charts displaying values for Total Tx, Total Rx, a pie chart displaying the data distribution for totals APs by network traffic, and the location of APs within the globe.

FIGURE 223 Sample Dashboard - "APs Rx Tx dashboard"


APs Rx Tx dashboard
Draft
Traffic tab
RX TX Info
Total APs By Traffic (Custom)
Peat-R610-Aja's Room, 60:D0:2C:01:9E:A0
RuckusAP, B4:79:C8:3E:C6:90
R750-RAP, 1C:3A:60:3B:DE:E0
Chandra_ICX_R510_Home, EC:8C:A2...
RuckusAP, B4:79:C8:3E:C6:20
R610_Yonghe, 20:58:69:0B:D2:B0
Kalyan_Home_R850, 70:CA:97:2C:4D:70
Keshav-SRAM-R610-2, 90:3A:72:26:3D:20
Peat-R610-Disco Ball, 60:D0:2C:01:9D:E0
Satheesh_T350C_Mesh, 58:FB:96:26:56:20
CWRU_AP_2, E8:1D:A8:2A:C0:10
Ravi_R760AP, B4:79:C8:3E:C6:30
Total Tx
78.2G
Total Rx
1T
AP locations on Map
mapbox
© Mapbox © OpenStreetMap Improve this map

The owner of the dashboard is provided with an option to schedule an email report from the screen while viewing it. Click a dashboard to view the details.

FIGURE 224 Dashboard View - Schedule Icon



This is filtered for so and so

Create a Report Schedule for the Dashboard

Complete the following steps to create an email schedules for the dashboard. The created schedule is displayed in the **Schedules** tab.

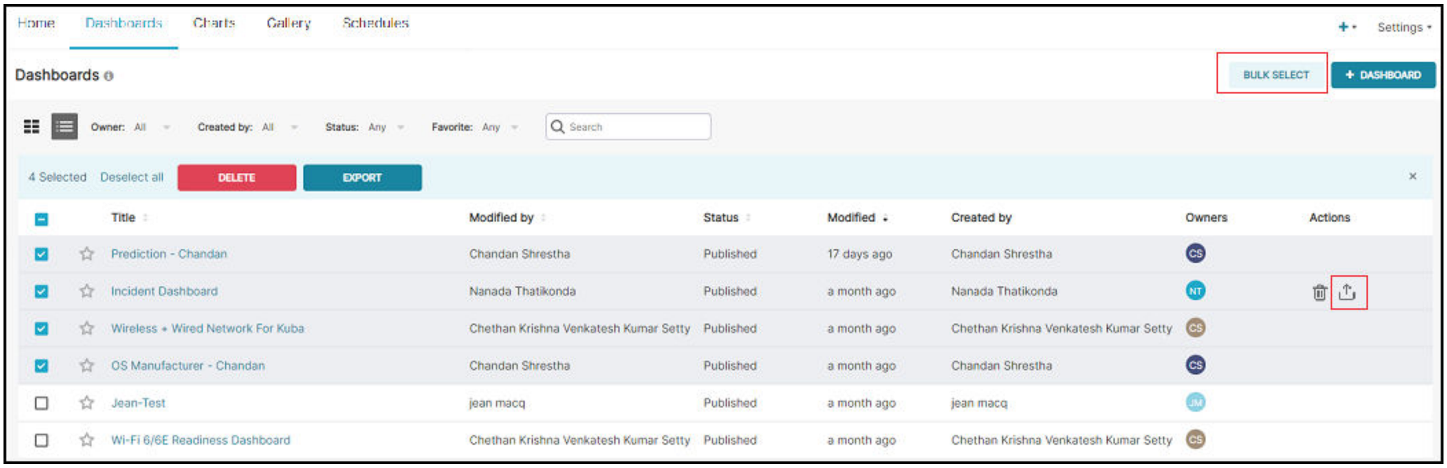
1. Click the 📅 icon at the top-right corner. The **New Email Schedule** dialog box is displayed.

2. Complete the following fields:
   - **Name**: Add a name to the schedule.
   - **Description**: If necessary, add a description of the schedule.
   - **Schedule**: Select the scheduled interval **Day**, **Week**, or **Month**, and also the **Hours**, and **Minutes** at which the reports should be sent to your email.
   - **Timezone**: Select a timezone from the list.
   - **Format**: Select a report format **PNG**, **CSV**, or **PDF**.
   - **Email**: Enter the email address to which the report will be sent.
3. Click **Add** to create a report schedule for the dashboard..

Export and Import Dashboard

Dashboards can be exported to make a copy or backup which can be imported at a later point of time. You can also share the exported file with other users who can import the dashboard into their account. From the **Dashboard** tab, you can export the dashboard details by clicking the ⇧ icon in the **Actions** column. You can also use the **BULK SELECT** option to select and export several dashboards at a time.

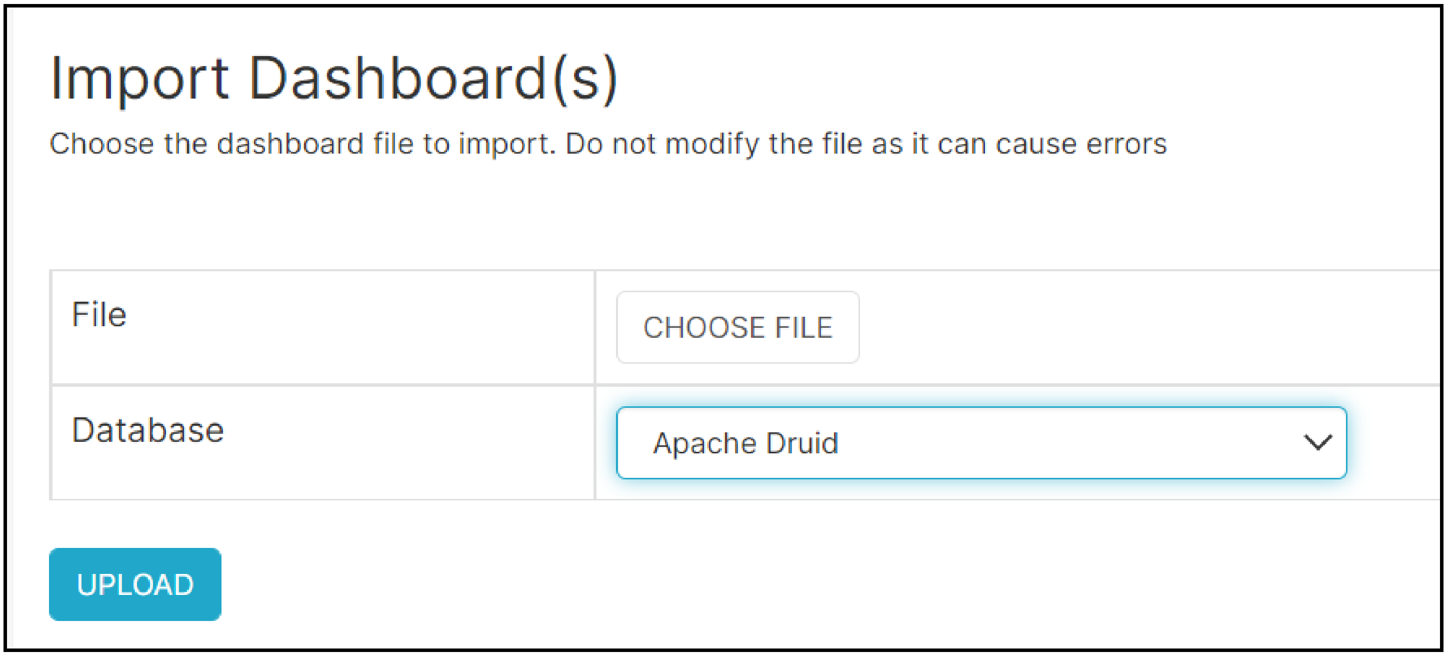
FIGURE 225 Dashboards - Export and Bulk Export



☐		Title	Modified by	Status	Modified	Created by	Owners	Actions
☑	☆	Prediction - Chandan	Chandan Shrestha	Published	17 days ago	Chandan Shrestha	CS	
☑	☆	Incident Dashboard	Nanada Thatikonda	Published	a month ago	Nanada Thatikonda	NT	🗑 ⇧
☑	☆	Wireless + Wired Network For Kuba	Chethan Krishna Venkatesh Kumar Setty	Published	a month ago	Chethan Krishna Venkatesh Kumar Setty	CS	
☑	☆	OS Manufacturer - Chandan	Chandan Shrestha	Published	a month ago	Chandan Shrestha	CS	
☐	☆	Jean-Test	jean macq	Published	a month ago	jean macq	JM	
☐	☆	Wi-Fi 6/6E Readiness Dashboard	Chethan Krishna Venkatesh Kumar Setty	Published	a month ago	Chethan Krishna Venkatesh Kumar Setty	CS	

To import the file, go to **Settings** > **Import Dashboard**.

FIGURE 226 Importing Dashboards



Import Dashboard(s)

Choose the dashboard file to import. Do not modify the file as it can cause errors

File	CHOOSE FILE
Database	Apache Druid

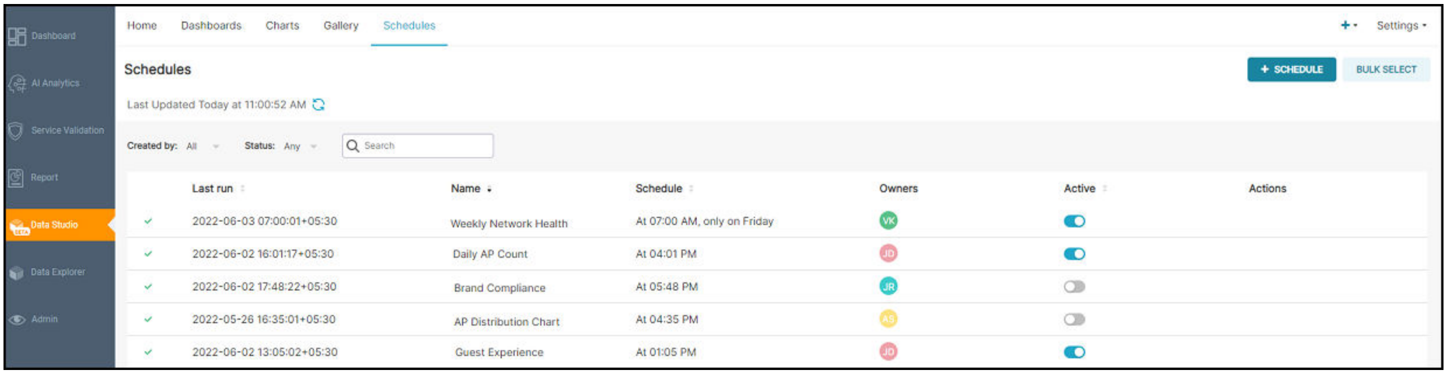
In the **Import Dashboard(s)** window, choose the exported dashboard file, select the database, and click **Upload** to import the dashboard file.

Note that the export and import is for the dashboard template only and the data is restricted based on the account and the resource group.

Schedules Tab

Reports presents a snapshots of the dashboards and charts. You can set up a schedule to send the reports by way of email to internal and external recipients at regular intervals (daily, weekly, or monthly). Only the owner of a dashboard or chart with Admin or Network Admin privileges can create a schedule of reports for the dashboard or chart. The schedules are visible to all users of the same tenant account with Admin or Network Admin privileges.

FIGURE 227 Schedules Tab



Schedules

Last Updated Today at 11:00:52 AM

Created by: All   Status: Any   Search

	Last run	Name	Schedule	Owners	Active	Actions
✓	2022-06-03 07:00:01+05:30	Weekly Network Health	At 07:00 AM, only on Friday	VK	●	
✓	2022-06-02 16:01:17+05:30	Daily AP Count	At 04:01 PM	JD	●	
✓	2022-06-02 17:48:22+05:30	Brand Compliance	At 05:48 PM	JR	○	
✓	2022-05-26 16:35:01+05:30	AP Distribution Chart	At 04:35 PM	AS	○	
✓	2022-06-02 13:05:02+05:30	Guest Experience	At 01:05 PM	JD	●	

The **Schedules** tab displays the following information:

- **Status**: Displays the status (successful or failed) of the scheduled report.

- **Last Run**: Displays the date and time (including time zone) at which the report was last run.
- **Name**: Displays the name of the report.
- **Schedule**: Displays the time at which the report is scheduled to run.
- **Owners**: Displays the name of the user who has created the scheduled report.
- **Active**: Indicates whether the schedule is enabled or disabled. Only the owner of the scheduled report and users with Admin privileges can enable or disable the schedule.
- **Actions**: Displays all the actions that you can perform on a configured schedule, as described in the following table.

TABLE 20 Actions Description

Action Icons	Description
🗒 (Execution Log)	View the execution log of the scheduled report.
✎ (Edit)	Edit the scheduled report. Only the user who created the schedule (the owner of the schedule) can edit the schedule.
🗑 (Delete)	Delete the scheduled report. Only the user who created the schedule (the owner of the schedule) can delete the schedule.

The owner of the schedule can also use the **Bulk Select** option to select several schedules and delete them all at once.

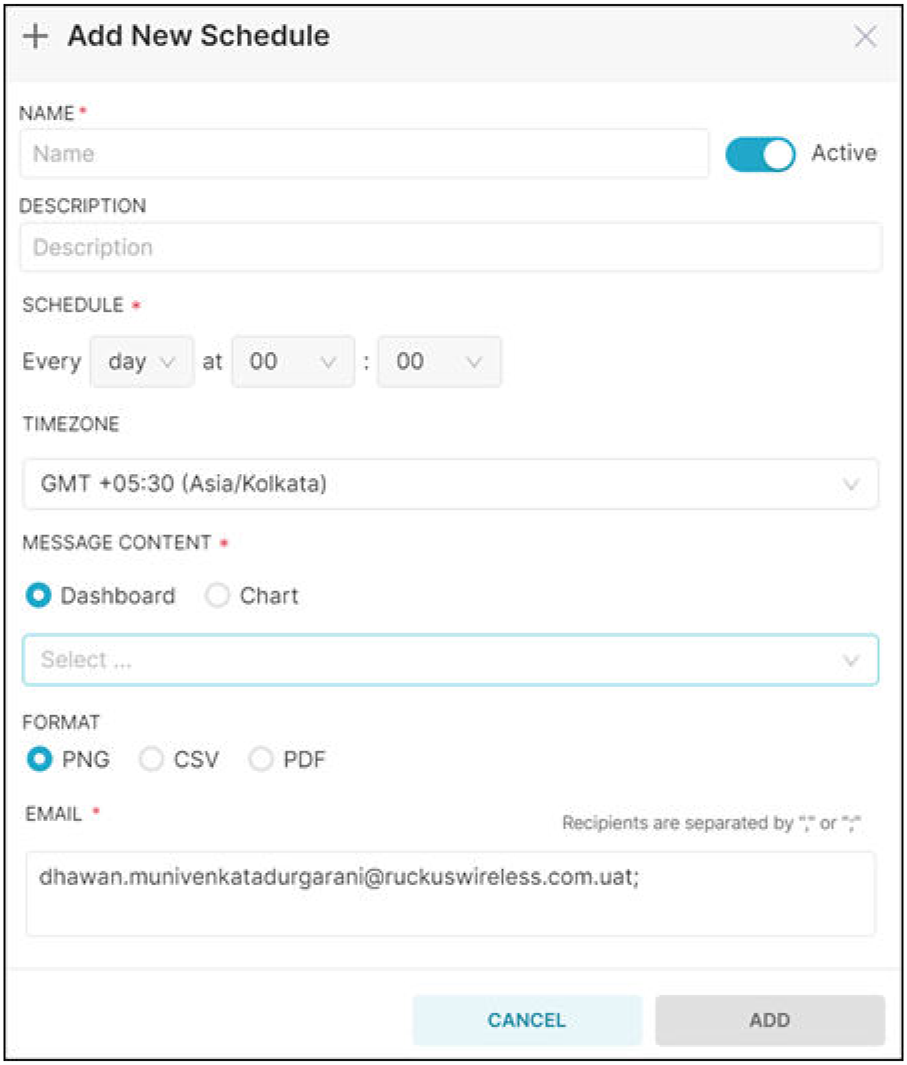
Creating a Schedule

Complete the following steps to create a schedule.

1. From the web interface, go to **Data Studio** and select **Schedules** tab.
2. Click **+ Schedule** to create a schedule.

   The **Add Schedule** dialog box is displayed.

FIGURE 228 Add Schedule Dialog Box



NAME *

Name

Active

DESCRIPTION

Description

SCHEDULE *

Every day at 00 : 00

TIMEZONE

GMT +05:30 (Asia/Kolkata)

MESSAGE CONTENT *

● Dashboard ○ Chart

Select ...

FORMAT

● PNG ○ CSV ○ PDF

EMAIL *

Recipients are separated by "," or ";"

dhawan.munivenkatadurgarani@ruckuswireless.com.uat;

3. Complete the following fields:

- **Name**: Enter a name for the report.
- **Description**: Enter a description of the report.
- **Active**: Use the slide button to enable or disable the schedule.

  If the schedule is enabled, the reports will be sent to the recipient according to the schedule. If the schedule is disabled, the schedule becomes inactive and the report does not run at the configured frequency.
- **Schedule**: Configure the schedule frequency to run the report (daily, weekly, or monthly).

  Selecting a daily schedule presents an option to choose the time of the day to send the report. Selecting a weekly schedule presents options to select the day of the week and time of day. Selecting a monthly schedule presents options to select the date of the month and time of day to run the schedule.
- **Timezone**: Select the time zone that must be considered for the schedule.

- **Message Content**: Select one of the following:
  - Dashboard: Specifies to create a schedule for a dashboard report. Select a dashboard from the list.
  - Chart: Specifies to create a schedule report for a chart report. Select a chart from the list.

    You can choose to send the chart report in the PNG, CSV, or PDF formats.
- **Email**: Specify the email address of the recipient to whom you want to send the report. You can enter email addresses of multiple recipients separated by commas or semicolons.

4. Click **Add** to create the schedule.

Dataset Filters

Datasets are collections of Columns and Metrics that are used to generate visualizations and queries that help in analyzing and monitoring the network performance. These Columns and Metrics are organized into separate groups to form multiple Datasets.

FIGURE 229 Dataset Filters

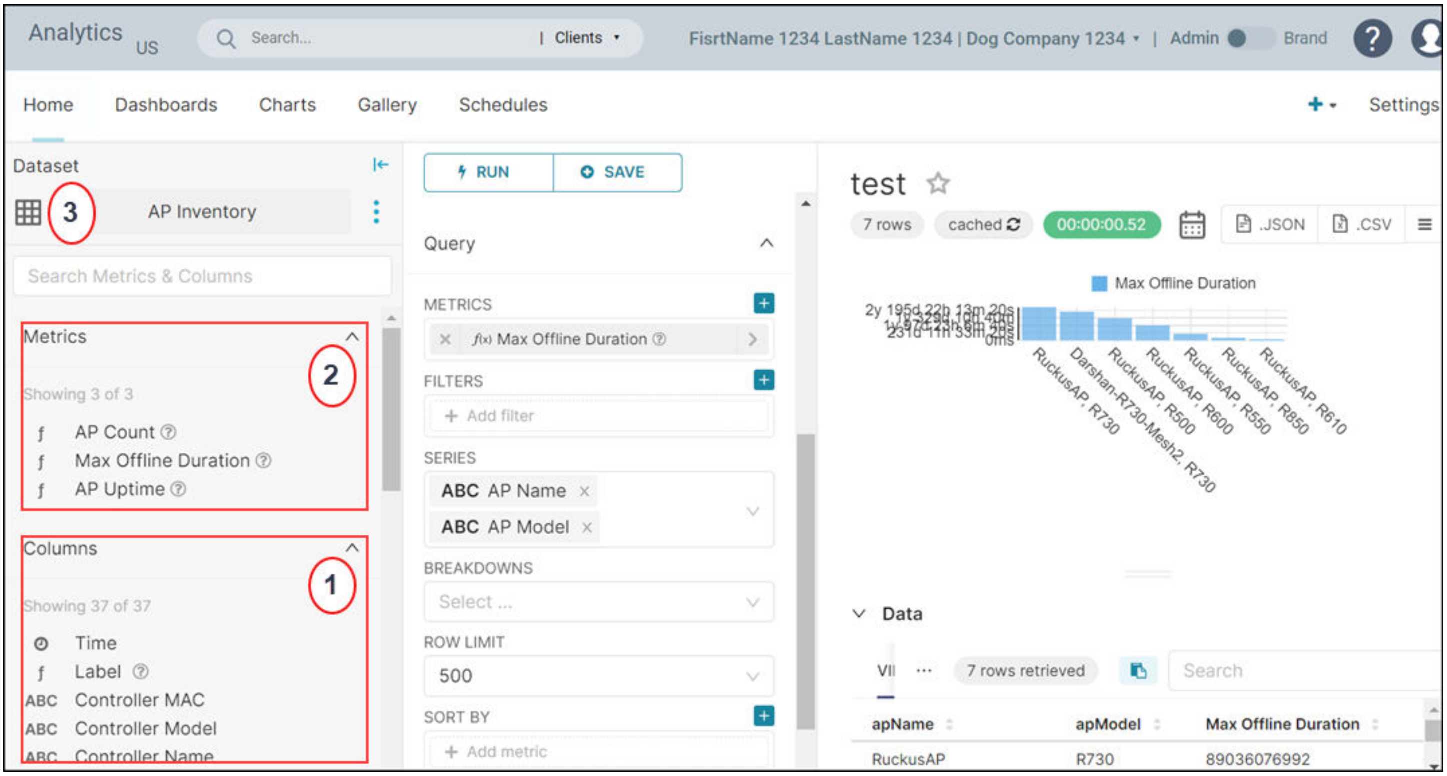


TABLE 21 Identifying Data Studio Interface Components

No	Name
1	Columns
2	Metrics
3	Table

Columns Filter

The **Columns filter** lists the following industry standard details.

- **AP**
- **Application**
- **Authentication**
- **Band**
- **BSSID**
- **Business Technology Management (BTM)**
- **Cable**
- **Channel**
- **Client**
- **Connection**
- **Controller**
- **Device**
- **Domain**
- **Event**
- **Lable**
- **LAN**
- **PoE**
- **Port**
- **Radio**
- **Rogue**
- **Session**
- **SSID**
- **Switch**
- **System**
- **Tenant**
- **Time**
- **Zone**

Click the **Table** icon to view the **Columns** tab. The applicable columns are grouped under their respective Datasets. After you select a Dataset, the columns grouped under that Dataset are displayed in the **Columns** tab.

The following table describes all the dimensions that are supported on one or more Dataset in RUCKUS Analytics.

TABLE 22 Columns

Column Name	Description	Supported Dataset
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 22 Columns (continued)

Column Name	Description	Supported Dataset
AP Description	Description string of the access point that is configured in the controller.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling
AP External IP	External IP address of the access point.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling
AP Group	AP Groups configured in the controller.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling
AP Group Location	AP group location.	• Client Info and Statistics • AP Inventory • AP Info and Statistics

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
AP Internal IP	Internal IP address of the access point.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling
AP Latitude	Latitude of GPS coordinates.	AP Inventory
AP Longitude	Longitude of GPS coordinates.	AP Inventory
AP Location	Location string of the access point that is configured in the controller.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling
AP MAC	Base MAC address of the access point.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
AP Model	Description of the access point model type.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling
AP Name	Name of the access point configured in the controller.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling
AP Serial	Serial number of the access point.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
AP Version	Firmware version number of the access point.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • AP WiFi Calling
AP WiFi Capability	Client WiFi6 Capability.	Client Info and Statistics
Application Category	Category of applications accessed by the Wi-Fi client.	Applications
Application Name	Name of the application accessed by the Wi-Fi client.	Applications
Authentication Method	The Wi-Fi encryption and authentication method adopted.	• Client Info and Statistics • Client Sessions
Band	Radio band used by the AP.	• Client Info and Statistics • AP Info and Statistics • AP Events
Band Capability	Band supported by the client.	• Client Info and Statistics • AP Info and Statistics
BSSID	Basic service set identifier.	AP Info and Statistics
BTM Capability	Client BTM capability.	Client Info and Statistics
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.	• AP Events • AP Alarms
Channel	The channel number used.	• AP Info and Statistics • Client Info and Statistics • Client Sessions • AP Events
Client IP	Internal IP address of the Wi-Fi client.	• Client Info and Statistics • Client Sessions • Applications
Client Capability	Indicates if client is WiFi6 or legacy client.	Client Info and Statistics
Client MAC	MAC address of the Wi-Fi client.	• Applications • Client Info and Statistics • Client Sessions • Client Connection Events
Client MAC Type	Indicates if clients MAC is OEM or a random MAC.	Client Info and Statistics

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
Client Radio Mode	Possible values are: ac, n, a, g, b, or "unknown" (if SmartZone version is prior to 3.6).	• Client Info and Statistics • Client Sessions
Client VLAN	VLAN ID used by the client.	Client Info and Statistics
Connection Stage	Indicates Client authentication type.	• Client Connection Counts • Client Connection Events
Connection Status	Connection status of the access point: Online, Offline, Discovery, Provisioned.	AP Inventory
Controller MAC	MAC address of the controller.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • Controller Inventory • AP Rogues • Client Connection Counts • Client Connection Events • Switch Inventory • Switch Network • AP WiFi Calling
Controller Model	Description of the model of the controller.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • Controller Inventory • AP Rogues • Client Connection Counts • Client Connection Events • Switch Inventory • Switch Network • AP WiFi Calling

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
Controller Name	Name of the configured controller.	- Applications - AP Info and Statistics - AP Airtime and Hardware - Client Info and Statistics - Client Sessions - AP Events - AP Inventory - AP Alarms - Controller Inventory - AP Rogues - Client Connection Counts - Client Connection Events - Switch Inventory - Switch Network - AP WiFi Calling
Controller Serial	Serial number of the controller.	- Applications - AP Info and Statistics - AP Airtime and Hardware - Client Info and Statistics - Client Sessions - AP Events - AP Inventory - AP Alarms - Controller Inventory - AP Rogues - Client Connection Counts - Client Connection Events - Switch Inventory - Switch Network - AP WiFi Calling
Controller Version	Firmware version number of the controller.	- Applications - AP Info and Statistics - AP Airtime and Hardware - Client Info and Statistics - Client Sessions - AP Events - AP Inventory - AP Alarms - Controller Inventory - AP Rogues - Client Connection Counts - Client Connection Events - Switch Inventory - Switch Network - AP WiFi Calling

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
Channel Bandwidth	Channel width used by the AP's radio.	• Client Info and Statistics • AP Info and Statistics
Device Type	Indicates device type of the client.	• Client Info and Statistics • Client Sessions
Disconnect Time	Disconnect time of a session.	Client Sessions
Domain	Domains configured in the controller.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • Switch Inventory • Switch Network • AP WiFi Calling
Event Code	Code number for access point and controller events.	AP Events
Event Description	Description of the event.	Client Connection Events
Event Type	Description for access point and controller events.	AP Events
Failed Message Info	Message ID to indicate what failures step in whole connection.	Client Connection Events
First Connection	First connection time of a session.	Client Sessions
FQDN of ePDG	FQDN of operator epdg gateway.	AP WiFi Calling
Hostname	Hostname of the client.	• Client Info and Statistics • Client Sessions • Applications
Is Stack		Switch Inventory

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
Label	User defined label / tag created by the MSP.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues • Client Connection Counts • Client Connection Events • Switch Inventory • Switch Network • AP WiFi Calling • Controller Inventory
LAG Name	LAG name.	Switch Network
LAN Ports WAN Connectivity	Description for this interface is WAN or LAN interface.	AP Inventory
LAN Ports Physical Link	Link attributes (up or down, speed, and duplex).	AP Inventory
LAN Ports Physical Capability	Description for this interface capability.	AP Inventory
LAN Ports	Port number for Ethernet interface.	AP Inventory
Last Status Change	Date and time of the last change in Connection Status of the access point.	AP Inventory
Manufacturer	Manufacturer of the client device.	• Client Info and Statistics • Client Sessions • Client Connection Events • OS Manufacturer
Message IDs	A sequence of message ID are recorded for this client session.	Client Connection Events
Number of Ports	Number of switch ports.	• Switch Inventory • Switch Network
Number of Switch Units	Number of units in the stack.	• Switch Inventory • Switch Network
Operators	Operator name.	AP WiFi Calling
Optics	Optics type of port.	Switch Network
OS Type	Operating System information for the Wi-Fi client.	• Client Info and Statistics • Applications
OS Vendor Type	Operating System vendor information for the Wi-Fi client.	• Client Info and Statistics • Client Sessions
Peer is Ruckus AP	RuckusAP support of remote device.	Switch Network
POE Mode Setting	8023af PoE mode.	AP Inventory
POE Under Powered	AP power level.	AP Inventory
POE Mode	8023af PoE power source.	AP Inventory
Port	Port of the application accessed by the Wi-Fi client.	Applications

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
Port Admin Status	Admin status of port.	Switch Network
Port Link Status	Link status of port.	Switch Network
Port MAC	MAC address of port.	Switch Network
Port Name	Name of port.	Switch Network
Port Number	Description of port.	Switch Network
Port Speed	Speed of port.	Switch Network
Port Status	Status of port, ex: CPU, Memory, Port Information (Network, PoE, Traffic, Packets In or Out).	Switch Network
Port Untagged VLAN	Untagged VLAN of port.	Switch Network
Port VLANs	Vlans of the port.	Switch Network
Radio	Indicates the radio frequency band: 2.4GHz or 5GHz.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • Client Connection Counts • Client Connection Events • AP WiFi Calling
Reason	Additional description for access point and controller alarms or events, if available.	• AP Events • AP Alarms
Roaming Flag	A flag to indicate this connection session is roaming or new join.	Client Connection Events
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.	• Client Info and Statistics • Client Sessions
Rogue AP MAC	MAC Address of the detected Rogue AP.	AP Rogues
Rogue Channel	The Wi-Fi channel that the Rogue APs was operating on.	AP Rogues
Rogue Encryption	The Wi-Fi encryption and authentication method adopted by the rogue AP.	AP Rogues
Rogue Radio	The radio band (2.4GHz or 5GHz) that the rogue AP was operating on.	AP Rogues
Rogue SSID	SSID of the detected Rogue AP.	AP Rogues
Rogue Type	Possible types are: ignore, known, rogue, and malicious.	Rogue AP
Router ID	Swtich Identifier.	Switch Network
Session ID	ID string assigned to a session.	• Client Info and Statistics • Client Sessions
Session Type	Indicates whether the session is authorized or unauthorized.	• Client Info and Statistics • Client Sessions
Severity	Severity level for access point and controller alarms or events.	• AP Events • AP Alarms

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
Spatial Stream Capability	Client STBC capability.	• Client Info and Statistics • AP Info and Statistics
SSID	Service set identifier (SSID) configured in the controller.	• Applications • AP Info and Statistics • Client Info and Statistics • Client Sessions • Client Connection Counts • Client Connection Events • AP WiFi Calling
Switch Firmware	Firmware version of switch.	• Switch Inventory • Switch Network
Switch Group Name	Switch group name.	• Switch Inventory • Switch Network
Switch IP	Switch IP.	• Switch Inventory
Switch MAC	Switch MAC.	• Switch Inventory • Switch Network
Switch Model	Model of switch.	• Switch Inventory • Switch Network
Switch Name	Hostname of switch.	• Switch Inventory • Switch Network
Switch Serial	Serial number of switch.	• Switch Inventory • Switch Network
Switch Status	Connection status of switch.	• Switch Inventory • Switch Network
Switch Subgroup Name	The list of switch groups.	• Switch Inventory • Switch Network
Switch Unit ID	Switch unit ID.	Switch Network
Switch Unit Status	Status of switch unit, ex: Switch Unit Information (ID, Uptime, Status, Serial Number).	Switch Network
Switch Uptime	Uptime of switch.	• Switch Inventory • Switch Network

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
System	System ID of the controller or the SmartZone Cluster.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • Controller Inventory • AP Rogues • Client Connection Counts • Client Connection Events • Switch Inventory • Switch Network • AP WiFi Calling
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 • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • Controller Inventory • AP Rogues • Client Connection Counts • Client Connection Events • Switch Inventory • Switch Network • AP WiFi Calling
Tenant		• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • Client Connection Counts • Client Connection Events • Switch Inventory • Switch Network • AP Events • AP Inventory • AP Alarms • Controller Inventory • AP WiFi Calling • AP Rogues

TABLE 22 Columns (continued)

Column Name	Description	Supported Dataset
Tx Power	Tx power of the WiFi interface.	• Client Info and Statistics • AP Info and Statistics
Username	Username of the user account associated with the Wi-Fi client.	• Client Info and Statistics • Client Sessions
Wired Device MAC	MAC address of the wired device.	Switch Network
Wired Device Name	Name of wired device.	Switch Network
Wired Device Port	Wired port interface.	Switch Network
Wired Device Port Description	Port description of the wired device.	Switch Network
Wired Device Port MAC	MAC address of wired port.	Switch Network
Wired Device Port Type	Type of wired port like Bridge, WLAN Access Point, Router, Station Only etc.	Switch Network
Zone	Zones configured in the controller.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP Events • AP Inventory • AP Alarms • AP Rogues
Zone Location	Zone location.	• Client Connection Counts • Client Connection Events • AP WiFi Calling • AP Inventory • AP Info and Statistics • Client Info and Statistics

Metrics Filter

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

Click the **Table** icon to view the **Metrics** tab. The applicable metrics are grouped under their respective Datasets. After you select a Dataset, the metrics grouped under that Dataset are displayed in the **Metrics** tab.

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

TABLE 23 Metrics

Metrics Name	Description	Supported Dataset
AP Count	Unique number of access points.	• Applications • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions • AP 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.	AP Info and Statistics
Attempt Count		Client Connection Counts
Avg Airtime Busy	Average of the airtime busy metric.	AP Airtime and Hardware
Avg Airtime Idle	Average of the airtime idle metric.	AP Airtime and Hardware
Avg Airtime Rx	Average of the airtime receive metric.	AP Airtime and Hardware
Avg Airtime Tx	Average of the airtime transmit metric.	AP Airtime and Hardware
Avg Airtime Utilization	Average of the total airtime utilization.	AP Airtime and Hardware
Avg CPU Utilization	Average CPU utilization for the controller.	• Controller Inventory • AP Airtime and Hardware
Avg Capacity Per AP	The saturated throughput estimate of a link.	AP Info and Statistics
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 • AP Airtime and Hardware
Avg 2.4 GHz Capacity	Average speed of the 2.4 GHz.	AP Info and Statistics
Avg 5 GHz Capacity	Average speed of the 5 GHz.	AP Info and Statistics
Avg 6(5) GHz Capacity	Average speed of the 6(5) GHz.	AP Info and Statistics
Avg AP-to-Client Latency	The time taken by a packet from AP to Client.	AP Info and Statistics
Avg Storage Utilization	The percentage of AP storage utilization.	AP Airtime and Hardware
Avg Noise Floor	Average noise floor power in dBm.	Client Info and Statistics
Avg RSS	Average received signal strength of the access point in dBm.	Client Info and Statistics
Avg Session Duration	Average time duration for a session.	Client Sessions
Avg SNR	Average signal to noise ratio at the access point in dB.	Client Info and Statistics
Avg Tx Rate	Average Tx rate.	AP Airtime and Hardware
Avg Rx Rate	Average Rx rate.	AP Airtime and Hardware
Avg Throughput Estimate	Average throughput estimate for the Wi-Fi client.	Client Info and Statistics
Call Duration	Duration of the WiFi call.	AP WiFi Calling
Client Hostname	Name of the client.	• Client Info and Statistics • Client Sessions

TABLE 23 Metrics (continued)

Metrics Name	Description	Supported Dataset
Client MAC Count	Unique number of Wi-Fi clients.	• Applications • Client Info and Statistics • Client Sessions • Client Connection Events
Client Throughput		Client Info and Statistics
Client Username	Name of the user.	• Client Info and Statistics • Client Sessions
Controller Count	Unique number of controllers.	Controller Inventory
Count	Client count.	• AP Events • AP Alarms • Client Connection Events
CPU (%)	CPU utilization of switch.	Switch Inventory
CRC	Crc Error.	Switch Network
Data Frames (Downlink)		AP Info and Statistics
Data Frames (Uplink)		AP Info and Statistics
Downlink Traffic	Bytes received by client.	AP WiFi Calling
Failed Associations	Number of failed associations.	AP Info and Statistics
Failed Authentications	Number of failed open authentications.	AP Info and Statistics
Failure Count		Client Connection Counts
Hostname Count	Number of hostnames.	• Client Sessions • Client Info and Statistics
In Discards	Input discards of port.	Switch Network
In Errors	Input Errors.	Switch 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.	• AP Info and Statistics • AP Airtime and Hardware
Mgmt Traffic (Downlink)		• AP Info and Statistics • AP Airtime and Hardware
Mgmt Traffic (Uplink)		• AP Info and Statistics • AP Airtime and Hardware
Mgmt Frames (Uplink)		AP Info and Statistics
Mgmt Frames (Downlink)		AP Info and Statistics
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.	AP Rogues
Max RSS	Maximum received signal strength of the access point in dBm.	Client Info and Statistics
Max SNR	Maximum signal to noise ratio at the access point in dB.	Client Info and Statistics
Memory (%)		Switch Inventory
Min RSS	Minimum received signal strength of the access point in dBm.	Client Info and Statistics

TABLE 23 Metrics (continued)

Metrics Name	Description	Supported Dataset
Min SNR	Minimum signal to noise ratio at the access point in dB.	Client Info and Statistics
Offline Duration		Switch Inventory
Out Errors	Output Errors.	Switch Network
PoE Free (mW)	PoE unallocated capacity of switch.	Switch Inventory
PoE Utilization (%)	Percentage of PoE allocated capacity of switch.	Switch Inventory
PoE Usage (mW)	PoE allocated capacity of switch.	Switch Inventory
PoE Total (mW)	Total PoE capacity of switch.	Switch Inventory
Port Count	Number of ports.	Switch Network
Port PoE Utilization (%)	Percentage of inline power consumed by the port.	Switch Network
Reboot Count	Number of times AP rebooted.	AP 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 Studio to obtain details about the APs.	• Client Info and Statistics • Client Sessions
Rogue AP Count	The number of rogue APs detected by all the APs in your network.	AP Rogues
Rx Avg 2.4GHz MCS Rate	2.4 GHz Radio median RX MCS rate in this bin.	AP Info and Statistics
Rx Avg 5GHz MCS Rate	5 GHz Radio median RX MCS rate in this bin.	AP Info and Statistics
Rx Avg 6(5)GHz MCS Rate	6(5) GHz Radio median RX MCS rate in this bin.	AP Info and Statistics
Rx Avg AP MCS Rate	Radio median RX MCS rate in this bin.	AP Info and Statistics
Rx Client MCS Rate	Client median RX MCS rate in this bin.	Client Info and Statistics
Rx Failures	Receive packets which failed to be processed due to insufficient buffer in AP.	AP Info and Statistics
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.	• AP Info and Statistics • AP Airtime and Hardware
Rx Total	Sum of the received user and management traffic.	• AP Info and Statistics • AP Airtime and Hardware
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 • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions
Session Count	Number of unique sessions.	• Client Info and Statistics • Client Sessions
Successful Associations	Number of successful associations.	AP Info and Statistics
Successful Authentications	Number of successful open authentications.	AP Info and Statistics
Successful Authentication Ratio	Ratio of number of successful open authentications over total number of open authentications.	AP Info and Statistics
Success Count		Client Connection Counts
Switch Count	Unique number of Switches.	Switch Inventory

TABLE 23 Metrics (continued)

Metrics Name	Description	Supported Dataset
Switch Unit Count	Unique number of Switch units.	Switch Network
System Count	Unique number of systems.	Controller Inventory
Total Data Frames Ratio	Percentage of all transmit and receive packets that are data.	AP Info and Statistics
Total Management Frames Ratio	Percentage of all transmit and receive packets that are management.	AP Info and Statistics
Total Session Duration		Client Sessions
Total Traffic	Total of sent and received bytes by client.	AP WiFi Calling
Traffic (Total)	Sum of the user and management traffic.	• AP Info and Statistics • AP Airtime and Hardware • Switch Network
Traffic (Downlink)	Bytes received.	• AP Airtime and Hardware • AP Info and Statistics • Switch Network
Traffic (Uplink)	Bytes sent.	• AP Airtime and Hardware • AP Info and Statistics • Switch Network
Tx Avg 2.4GHz MCS Rate	2.4 GHz Radio median Tx MCS rate.	AP Info and Statistics
Tx Avg 5GHz MCS Rate	5 GHz Radio median Tx MCS rate.	AP Info and Statistics
Tx Avg 6(5)GHz MCS Rate	6(5) GHz Radio median Tx MCS rate.	AP Info and Statistics
Tx Avg AP MCS Rate	Radio median Tx MCS rate.	AP Info and Statistics
TxBroadcastFrames	Number of broadcast packets transmitted by the network.	AP Info and Statistics
Tx Client MCS Rate	Client median TX MCS rate.	Client Info and Statistics
TxDropDataFrames	Transmit data frames that are dropped by the message queue.	AP Info and Statistics
Tx Failures	Transmit packets which failed to be processed due to insufficient buffer in AP.	AP Info and Statistics
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.	• AP Info and Statistics • AP Airtime and Hardware
TxMulticastFrames	Number of multicast packets transmitted by the network.	AP Info and Statistics
Tx PER	Radio Tx Packet Error Rate in this bin.	Client Info and Statistics
Tx Total	Sum of the transmit user and management traffic.	• AP Info and Statistics • AP Airtime and Hardware
TxUnicastFrames	The number of data packets transmitted by the network that are not broadcast or multicast packets.	AP Info and Statistics
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 • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions

TABLE 23 Metrics (continued)

Metrics Name	Description	Supported Dataset
Uplink Traffic	Bytes sent by client.	AP WiFi Calling
Username Count	Unique number of usernames.	• Client Sessions • Client Info and Statistics
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 • AP Info and Statistics • AP Airtime and Hardware • Client Info and Statistics • Client Sessions
User Traffic(Total)	Total of sent and received bytes by user.	• Client Sessions • Client Info and Statistics • AP Info and Statistics • AP Airtime and Hardware
User Traffic (Downlink)	Bytes received by the user.	• Client Sessions • Client Info and Statistics • AP Info and Statistics • AP Airtime and Hardware
User Traffic (Uplink)	Bytes sent by the user.	• Client Sessions • Client Info and Statistics • AP Info and Statistics • AP Airtime and Hardware

Administration

- Viewing Onboarded Systems......233
- Managing Users......235
- Managing Resource Groups......236
- Labels......239
- Contacting Ruckus Support......241
- Managing Licenses and Assigning APs......241
- Viewing Schedules......245
- Creating Webhooks......246

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 234.

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
- Accounts: displays the name of all the partner accounts
- Controller: displays the SmartZone controllers names associated with various accounts
- 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

In some partnerships where more than two organizations are involved, a primary account holder is defined as the one that owns the SmartZone controller and the secondary account holder is the one that has a RUCKUS Analytics license but does not own a controller. However, the primary account holder can onboard the controller to the secondary account. In this arrangement, networking data from the SmartZone network of the primary account holder can be streamed to the RUCKUS Analytics account of secondary account, and the secondary account holders can view data directly in their accounts even though they do not own the controller.

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.

> **NOTE**
> SmartZone must have fully paid RTU license and AP license to onboard to RUCKUS Analytics.

1. Login to the SmartZone controller web interface with your RUCKUS Support user credentials.
2. Enable SmartZone cloud software services and then connect SmartZone to your RUCKUS Analytics account by performing the following steps.

   The menu navigation has changed from SmartZone 6.0 and later releases.

   - In releases prior to SmartZone 6.0, complete the following steps:

   a) Go to **System** > **General Settings** > **Cloud Services**.

   b) Turn on **Cloud SZ Services** which displays the RUCKUS cloud single sign-on window that prompts you to log in with your RUCKUS Support credentials. After successful login, SmartZone is securely connected to your RUCKUS cloud account to use RUCKUS Analytics cloud services.

   c) Turn on **Ruckus Analytics**. This will connect SmartZone to your RUCKUS Analytics account and enable data streaming to the RUCKUS Analytics instance.

   - In SmartZone 6.0 and later releases, complete the following steps:

   a) Go to **Administration** > **External Services** > **Ruckus Services**, and select **Ruckus Cloud Services**.

   b) Turn on **Cloud Authentication** which displays the RUCKUS cloud single sign-on window that prompts you to log in with your RUCKUS Support credentials. After successful login, SmartZone is securely connected to your RUCKUS cloud account to use RUCKUS Analytics cloud services.

   c) Turn on **Ruckus Analytics**. This will connect SmartZone to your RUCKUS Analytics account and enable data streaming to the RUCKUS Analytics instance.

   > **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.

   When more than one organization is involved in the onboarding of a controller, a primary account holder is defined as the one that owns the SmartZone controller, and the secondary account holder is the one that possess RUCKUS Analytics license but does not own the controller. For example, in a typical channel partner model, where a partner and its end-customer are involved, the end-customer could be the primary account holder, and the channel partner is the secondary account holder. In this case, the secondary account holder can onboard the controller directly to the secondary account by using his Ruckus Support credentials. In this arrangement, networking data from the SmartZone network of the primary account holder will be streamed directly to the RUCKUS Analytics account of the secondary account, and the allocation (and thus consumption) of licenses happens in the secondary account. Do note that in this case, the primary account will have no access to the data in RUCKUS Analytics, unless the secondary account holder invites the primary account holder as a 3rd party user.

   Whenever a controller is onboarded to a secondary account, emails will be sent to the admins of the primary account to inform them of the event. Primary account holder will be able to cease this data streaming to the secondary account by logging into the SmartZone and offboard the SmartZone from RUCKUS Analytics.

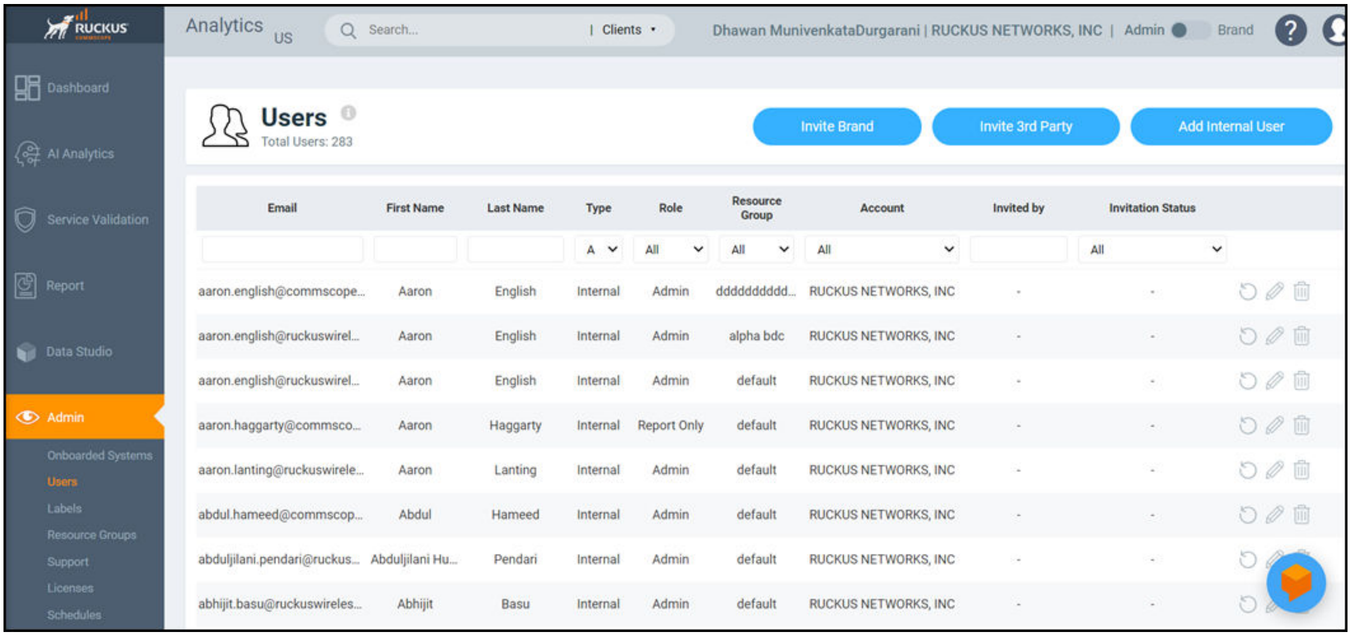
Managing Users

You can add registered users, assign roles to the 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** > **Users**.

   FIGURE 230 User Management

   Users
   Total Users: 283

Email	First Name	Last Name	Type	Role	Resource Group	Account	Invited by	Invitation Status
			A	All	All	All		All
aaron.english@commscope...	Aaron	English	Internal	Admin	dddddddddd...	RUCKUS NETWORKS, INC	-	-
aaron.english@ruckuswirel...	Aaron	English	Internal	Admin	alpha bdc	RUCKUS NETWORKS, INC	-	-
aaron.english@ruckuswirel...	Aaron	English	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-
aaron.haggarty@commsco...	Aaron	Haggarty	Internal	Report Only	default	RUCKUS NETWORKS, INC	-	-
aaron.lanting@ruckuswirele...	Aaron	Lanting	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-
abdul.hameed@commscop...	Abdul	Hameed	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-
abduljilani.pendari@ruckus...	Abduljilani Hu...	Pendari	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-
abhijit.basu@ruckuswireles...	Abhijit	Basu	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-

   The **Users** page displays the number of registered users and additional information such as the user email address, first and last names, role, associated resource group, and user account.

   If a user onboards the controller, that user can be added as a user to the account. However, the user has restricted administrator permissions. For example, the user can access account details but cannot delete other users from the account.

2. Click **Add Internal User**.

   The **Create User** page is displayed where you can select the registered users from **Email** 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**.

   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 3rd Party** 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 invitee is displayed in the **Users** page. The user can accept or reject the invitation; the status of which is also displayed on this page as **Accepted**, **Rejected** or **Pending**. The user must also have a registered RUCKUS Analytics account to accept the invitation. Additionally, only users having their own account with RUCKUS Analytics can accept invitations. Else, they will not be granted permission to access the application. If the user wants to use another account to accept invitations, then the new account has to be added and registered with RUCKUS Analytics before the user can accept invitation from that account.
4. 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.

Adding a Brand

A user can be invited to have the role of a Brand to access and monitor partner's network data. For more information, refer to Brand Invitation on page 253.

Managing Resource Groups

You can provide Role-Based Access Control (RBAC) to allow an administrator to manage APs and switches organized into resource groups.

A resource group is made up of your selection of APs and switches available in RUCKUS Analytics. There are many roles associated with resource groups with specific functional privileges. The roles available are Admin, Network Admin and Reporting. A resource group allows the Admin to confine access for a group of users to a restricted set of APs and switches. Therefore, a resource group is equivalent to a tenant.

RUCKUS Analytics contains a Default resource group. This group corresponds to the entire set of Wi-Fi assets. The Default resource group cannot be edited or deleted.

The following table lists the functional privileges of each role.

> **NOTE**
> Only users with Admin privileges can edit a resource group.

TABLE 24 Roles and their Privileges

Role	View Reports	UI View Mode	Save Filter	Scheduled Reports	Data Studio	Brand 360	Admin Control	Resource Group	License Management	Enable RUCKUS Support
Admin	Yes	Advanced	Yes	Yes	Create	No	Yes	Yes	Yes	Yes

TABLE 24 Roles and their Privileges (continued)

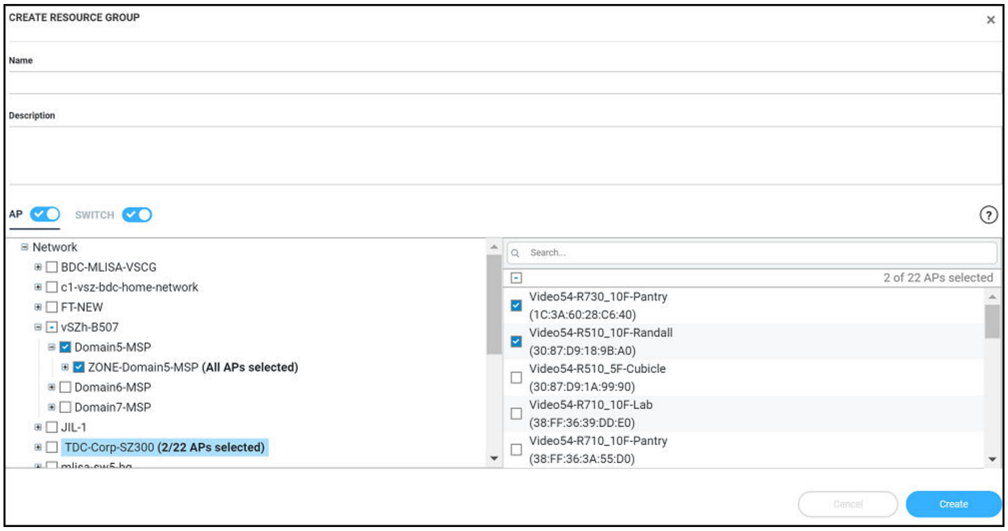
Role	View Reports	UI View Mode	Save Filter	Scheduled Reports	Data Studio	Brand 360	Admin Control	Resource Group	License Management	Enable RUCKUS Support
Network Admin	Yes	Advanced	Yes	Yes	Create	No	No	No	No	No
Reports	Yes	Report	Yes	Yes	View	No	No	No	No	No
Brand	No	No	No	No	Create	Yes	No	No	No	No

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 231 Creating a Resource Group



⊟ Network
- ⊞ □ BDC-MLISA-VSCG
- ⊞ □ c1-vsz-bdc-home-network
- ⊞ □ FT-NEW
- ⊟ ⊟ vSZh-B507
  - ⊟ ☑ Domain5-MSP
    - ⊞ ☑ ZONE-Domain5-MSP **(All APs selected)**
  - ⊞ □ Domain6-MSP
  - ⊞ □ Domain7-MSP
- ⊞ □ JIL-1
- ⊞ □ TDC-Corp-SZ300 **(2/22 APs selected)**
- ⊞ □ mlisa-sw5-hq

⊟ 2 of 22 APs selected

- ☑ Video54-R730_10F-Pantry (1C:3A:60:28:C6:40)
- ☑ Video54-R510_10F-Randall (30:87:D9:18:9B:A0)
- □ Video54-R510_5F-Cubicle (30:87:D9:1A:99:90)
- □ Video54-R710_10F-Lab (38:FF:36:39:DD:E0)
- □ Video54-R710_10F-Pantry (38:FF:36:3A:55:D0)

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.

Labels

Labels created in the organization network hierarchy can be used in Brand 360 dashboard to focus on dataset of interest. Labels can also be used with Data Studio reports to 'filter' the results to the narrow set required for analysis. Labels help the brand to organize and monitor properties. A brand can create and attach a color-coded label to the properties managed by the partners. Depending on the business requirement, multiple properties managed by different partners can be grouped under a single label. Multiple labels can be attached for the same set of properties. Both partners and brand have the ability to create labels. The labels created from the partner's account are also displayed on the brand 360 dashboard. The color-coded labels help the brand to identify the properties managed by different partners spreading across different locations, sites, geographical regions, or networks. Labels can be used as filters to aggregate data across multiple partners.

Creating Labels

Complete the following steps to create a label.

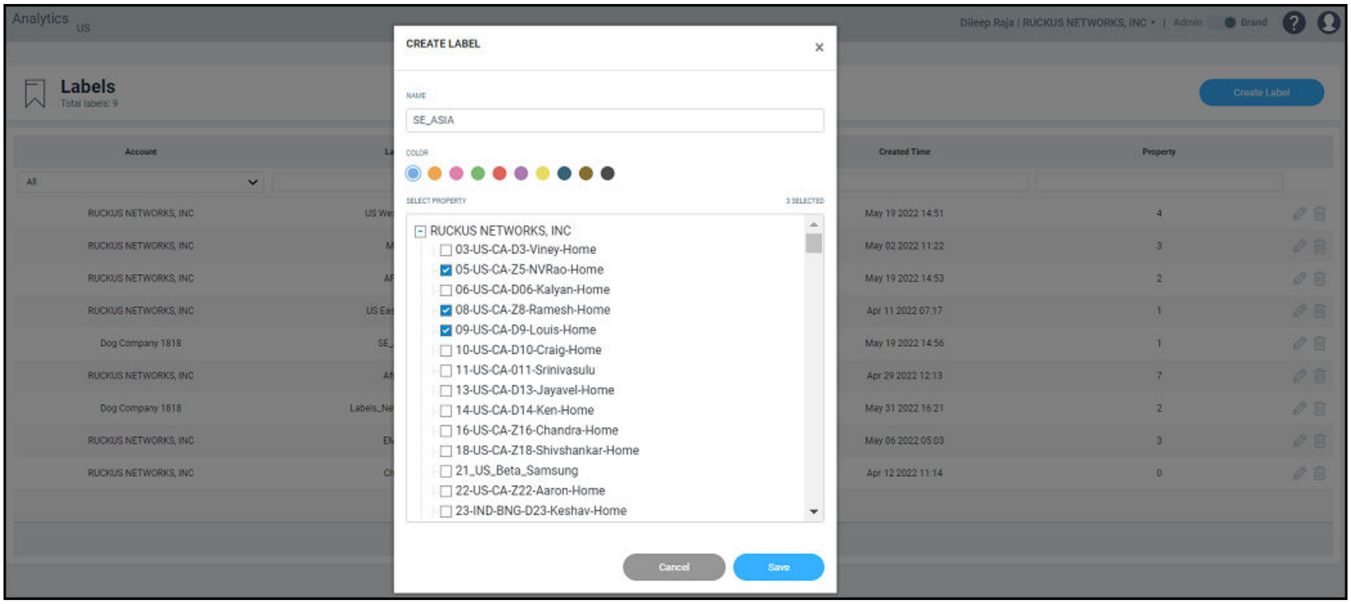
1. From the web interface, go to **Admin** > **Labels**.

   The **Labels** page is displayed.

2. Click **Create Label**.

   The **Create Label** dialog box is displayed.

   FIGURE 232 Creating Labels

   CREATE LABEL ×

   NAME

   SE_ASIA

   COLOR

   ● ● ● ● ● ● ● ● ● ●

   SELECT PROPERTY — 3 SELECTED

   - RUCKUS NETWORKS, INC
     - □ 03-US-CA-D3-Viney-Home
     - ☑ 05-US-CA-Z5-NVRao-Home
     - □ 06-US-CA-D06-Kalyan-Home
     - ☑ 08-US-CA-Z8-Ramesh-Home
     - ☑ 09-US-CA-D9-Louis-Home
     - □ 10-US-CA-D10-Craig-Home
     - □ 11-US-CA-011-Srinivasulu
     - □ 13-US-CA-D13-Jayavel-Home
     - □ 14-US-CA-D14-Ken-Home
     - □ 16-US-CA-Z16-Chandra-Home
     - □ 18-US-CA-Z18-Shivshankar-Home
     - □ 21_US_Beta_Samsung
     - □ 22-US-CA-Z22-Aaron-Home
     - □ 23-IND-BNG-D23-Keshav-Home

   Cancel Save

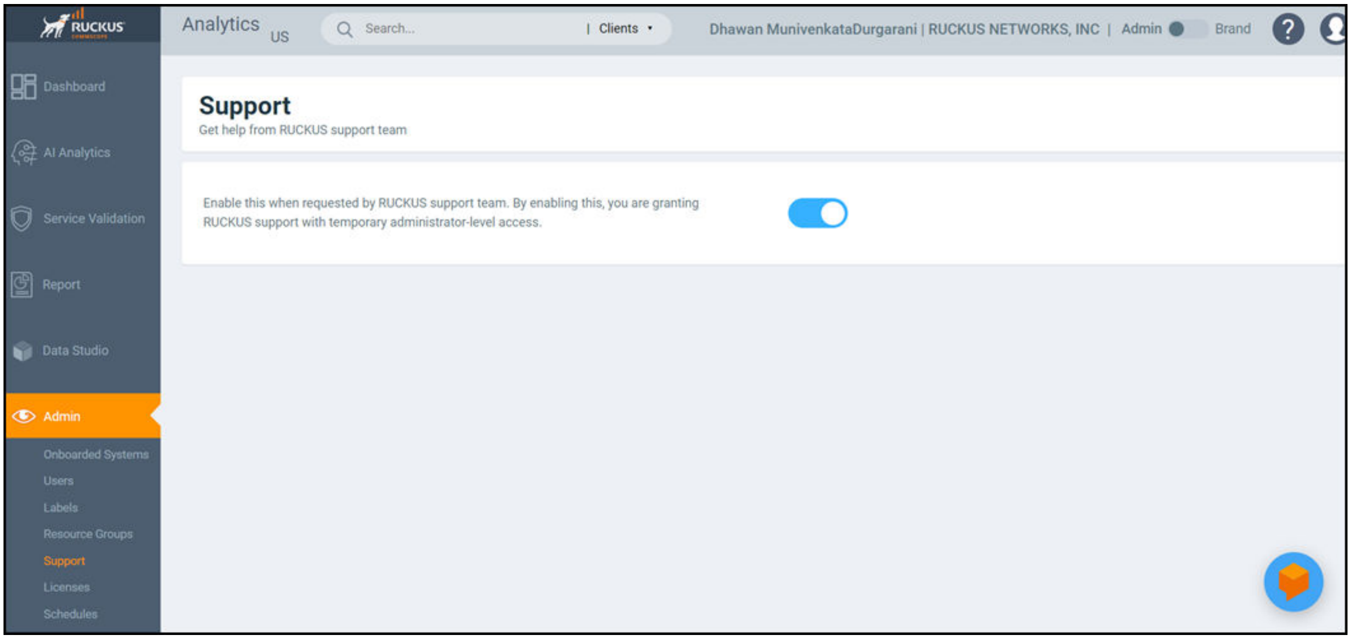
3. Complete the following details:
   - **Name**: Enter a name for the label.
   - **Color**: Pick a color for the label.
   - **Select Property**: Select the property that you want to attach to the labels.
4. Click **Save** to create the label.

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 233 Ruckus Support Page



Support

Get help from RUCKUS support team

Enable this when requested by RUCKUS support team. By enabling this, you are granting RUCKUS support with temporary administrator-level access.

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 25 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

TABLE 25 License Subscription Packages (continued)

License Type	Description
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:

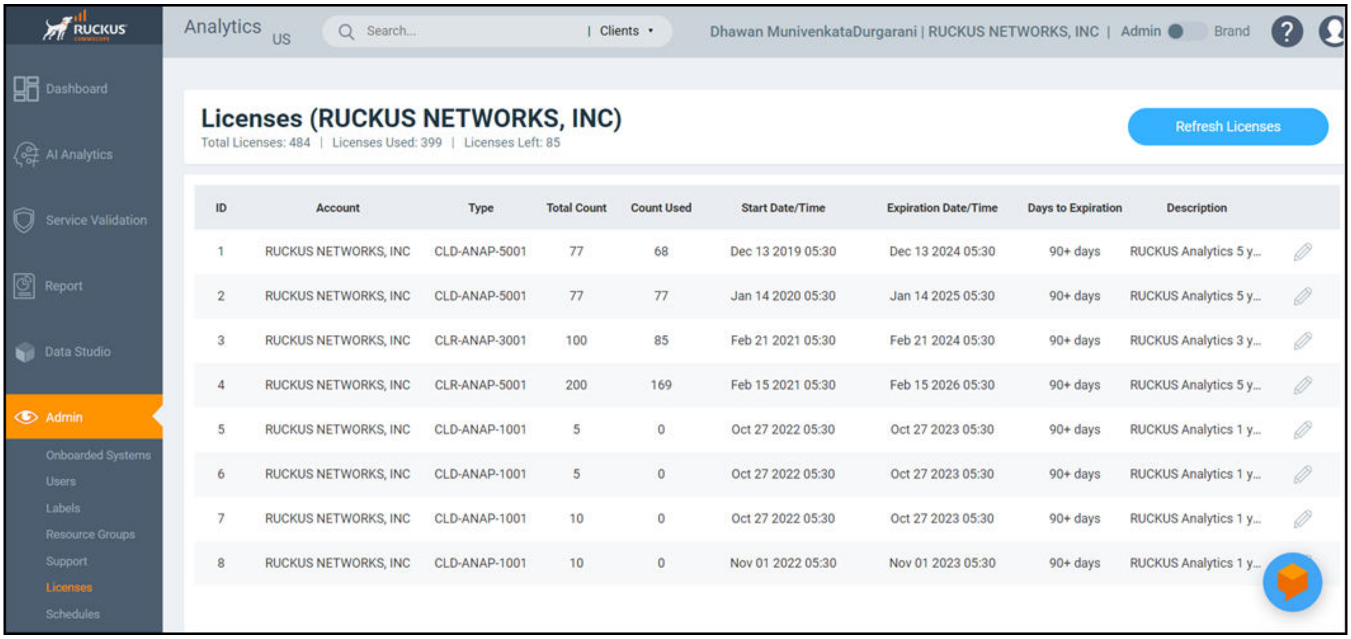
   - Type: Displays the type of license package as described in the preceding table
   - Total Count: Displays the total number of licenses assigned
   - Accounts: displays the licenses of all the partner accounts
   - Count Used: Displays the number of licenses used from the total number assigned
   - Start Date/Time: Displays the date and time when the license is activated
   - Expiration Date/Time: Displays the date and time when the license expires or deactivates
   - Days to Expiration: Displays the number of days available to use the license
   - Description: Displays a short description about the license type

   The **Refresh License** option refreshes this page to display the latest license information.

   The **Claim your free 90-day trial** option allows you to use the new built-in 90-day free trial license for 100 APs or ICX switches. Select this option to claim the license immediately. It can only be claimed once. The license is available to all accounts which do not have any paid licenses.

   Beneath the **Licenses** page title, **Total Count** displays the sum of all the license allotted, **Licenses Used** displays a sum of all the licenses used from the total number allotted, and **Licenses Left** displays the sum of all the licenses remaining from the total number allotted.

FIGURE 234 Licenses Page



Licenses (RUCKUS NETWORKS, INC)

Total Licenses: 484 | Licenses Used: 399 | Licenses Left: 85

ID	Account	Type	Total Count	Count Used	Start Date/Time	Expiration Date/Time	Days to Expiration	Description
1	RUCKUS NETWORKS, INC	CLD-ANAP-5001	77	68	Dec 13 2019 05:30	Dec 13 2024 05:30	90+ days	RUCKUS Analytics 5 y...
2	RUCKUS NETWORKS, INC	CLD-ANAP-5001	77	77	Jan 14 2020 05:30	Jan 14 2025 05:30	90+ days	RUCKUS Analytics 5 y...
3	RUCKUS NETWORKS, INC	CLR-ANAP-3001	100	85	Feb 21 2021 05:30	Feb 21 2024 05:30	90+ days	RUCKUS Analytics 3 y...
4	RUCKUS NETWORKS, INC	CLR-ANAP-5001	200	169	Feb 15 2021 05:30	Feb 15 2026 05:30	90+ days	RUCKUS Analytics 5 y...
5	RUCKUS NETWORKS, INC	CLD-ANAP-1001	5	0	Oct 27 2022 05:30	Oct 27 2023 05:30	90+ days	RUCKUS Analytics 1 y...
6	RUCKUS NETWORKS, INC	CLD-ANAP-1001	5	0	Oct 27 2022 05:30	Oct 27 2023 05:30	90+ days	RUCKUS Analytics 1 y...
7	RUCKUS NETWORKS, INC	CLD-ANAP-1001	10	0	Oct 27 2022 05:30	Oct 27 2023 05:30	90+ days	RUCKUS Analytics 1 y...
8	RUCKUS NETWORKS, INC	CLD-ANAP-1001	10	0	Nov 01 2022 05:30	Nov 01 2023 05:30	90+ days	RUCKUS Analytics 1 y...

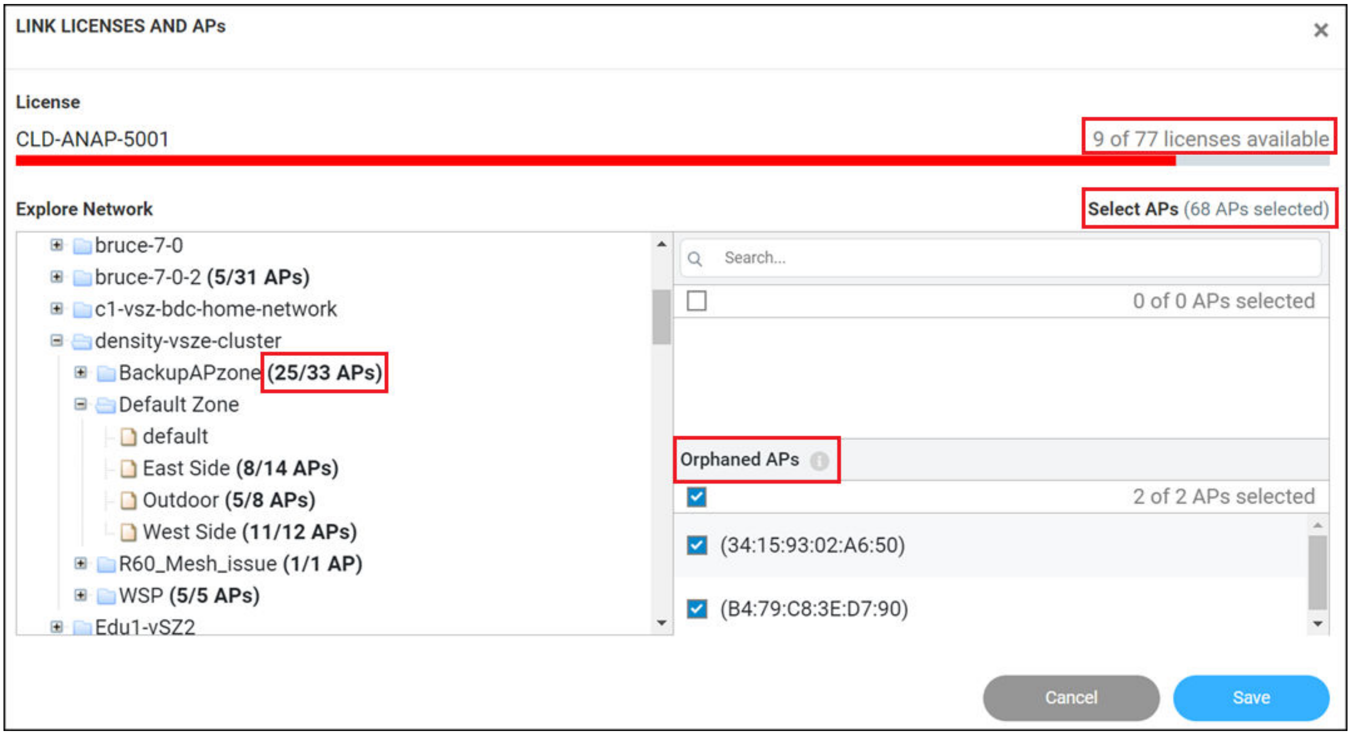
2. Click the edit icon to assign APs to the license selected.

   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 235 Link Licenses and APs Dialog Box



LINK LICENSES AND APs

License
CLD-ANAP-5001
9 of 77 licenses available

Explore Network
- bruce-7-0
- bruce-7-0-2 **(5/31 APs)**
- c1-vsz-bdc-home-network
- density-vsze-cluster
  - BackupAPzone **(25/33 APs)**
  - Default Zone
    - default
    - East Side **(8/14 APs)**
    - Outdoor **(5/8 APs)**
    - West Side **(11/12 APs)**
  - R60_Mesh_issue **(1/1 AP)**
  - WSP **(5/5 APs)**
- Edu1-vSZ2

Select APs (68 APs selected)

Search...

□ 0 of 0 APs selected

Orphaned APs

☑ 2 of 2 APs selected

☑ (34:15:93:02:A6:50)

☑ (B4:79:C8:3E:D7:90)

If an AP is already assigned a license, it will be unavailable and you will not be able to select it. A message is also displayed next to the AP stating the license to which it is assigned.

You can use the search bar to find an AP by the AP name or the AP MAC address. You can also see the number of APs matching the search string (name or MAC address) specified in the search bar.

The **Orphaned** APs column displays the APs that are no longer connected to the network. For example, the AP location may have changed or the AP may have lost network connectivity, and therefore there is no account for the AP in the network. You cannot find or search for an orphaned AP within the network. Pause the pointer over the Orphaned APs section for more information about scenarios in which an AP can become orphaned.

The MAC address of the orphaned AP is displayed. The license associated with the orphaned AP is no longer valid, so you can release the license to be assigned to another AP within the network.

A color bar is displayed on top of the columns representing the available licenses for the APs. The bar displays green when the number of licenses consumed is less than 50 percent of the available licenses. It displays yellow when more than 50 percent of the available licenses are consumed, and displays red when more than 75 percent of the available licenses are consumed.

3. Click **Save**.

Viewing Schedules

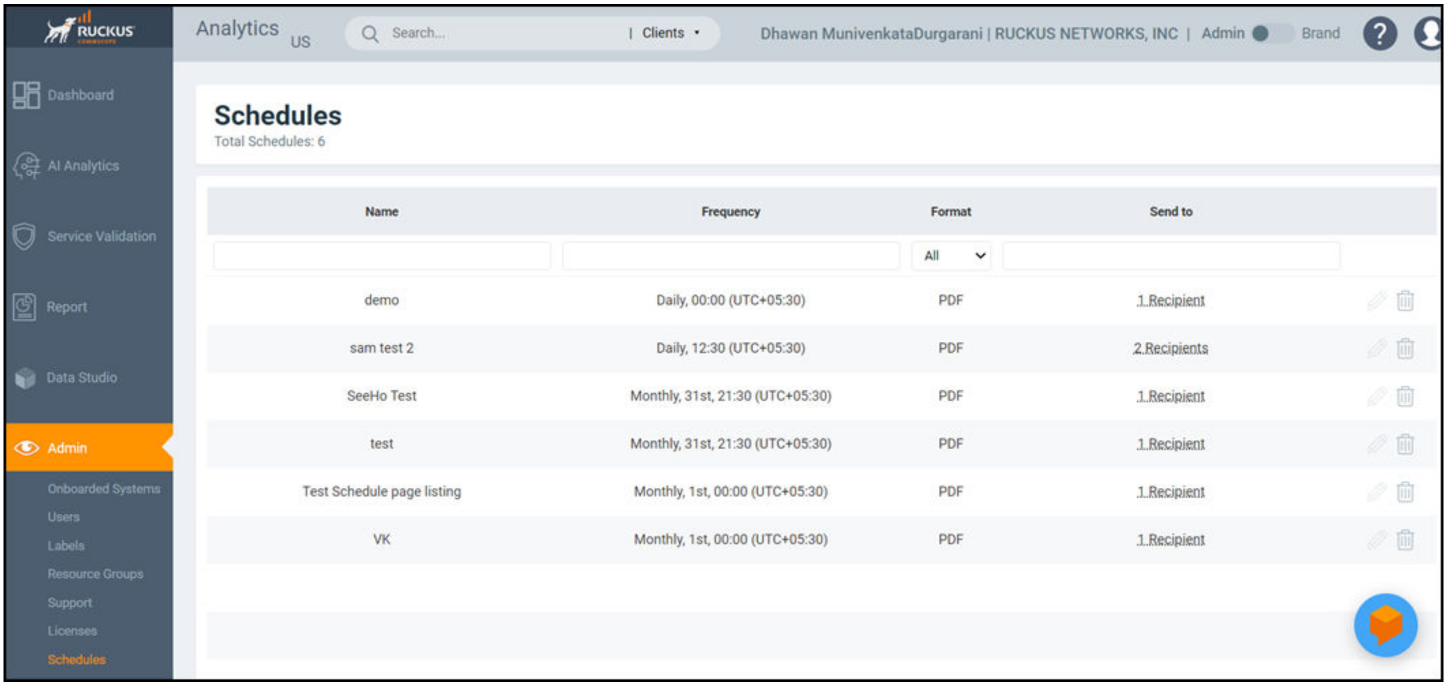
You can view all the schedules created for the reports and custom dashboards in **Schedules** window.

The schedule can only be edited by the user who created it, however, schedules can be deleted by any user.

From the web interface, go to **Admin** > **Schedules Systems**.

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

FIGURE 236 Schedules Page



Schedules
Total Schedules: 6

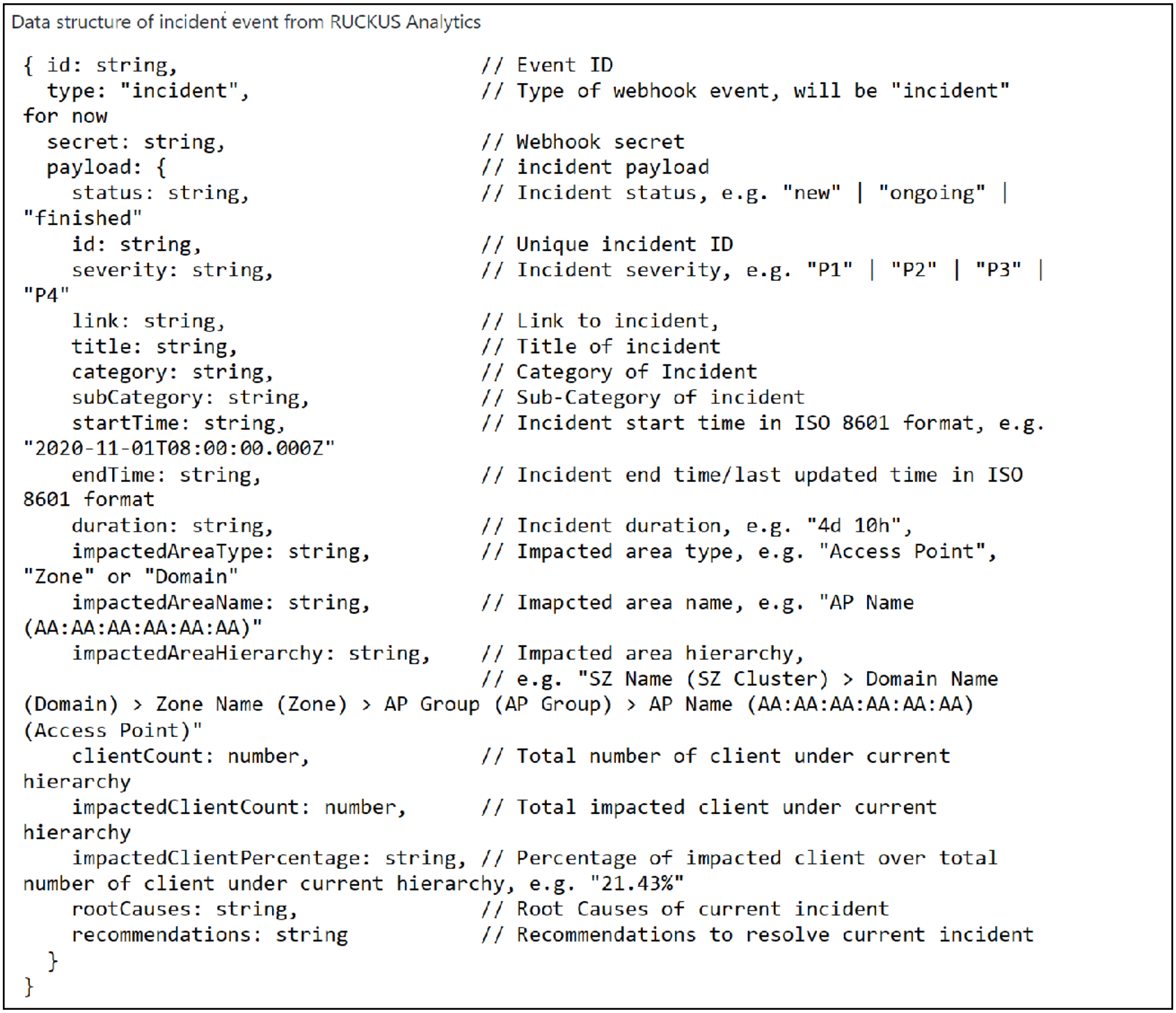
Name	Frequency	Format	Send to
		All	
demo	Daily, 00:00 (UTC+05:30)	PDF	1 Recipient
sam test 2	Daily, 12:30 (UTC+05:30)	PDF	2 Recipients
SeeHo Test	Monthly, 31st, 21:30 (UTC+05:30)	PDF	1 Recipient
test	Monthly, 31st, 21:30 (UTC+05:30)	PDF	1 Recipient
Test Schedule page listing	Monthly, 1st, 00:00 (UTC+05:30)	PDF	1 Recipient
VK	Monthly, 1st, 00:00 (UTC+05:30)	PDF	1 Recipient

- Name: displays the name of the schedule
- Frequency: displays the frequency to which the schedule is set - it can be daily, weekly, monthly, or on-demand
- Format: displays the format in which to save the schedule
- Sent to: displays the email ID of recipients who receive the schedule based on the frequency set

Creating Webhooks

RUCKUS Analytics allows you to configure Webhook URL addresses to receive real-time notifications when incidents are created or updated in the application – much like e-mail notifications. Webhooks help applications to communicate with each other in real-time and typically use a message or payload to communicate between each other. The message or payload contains real-time information about the incident.

FIGURE 237 Sample Webhook Message with Incident Details



Data structure of incident event from RUCKUS Analytics

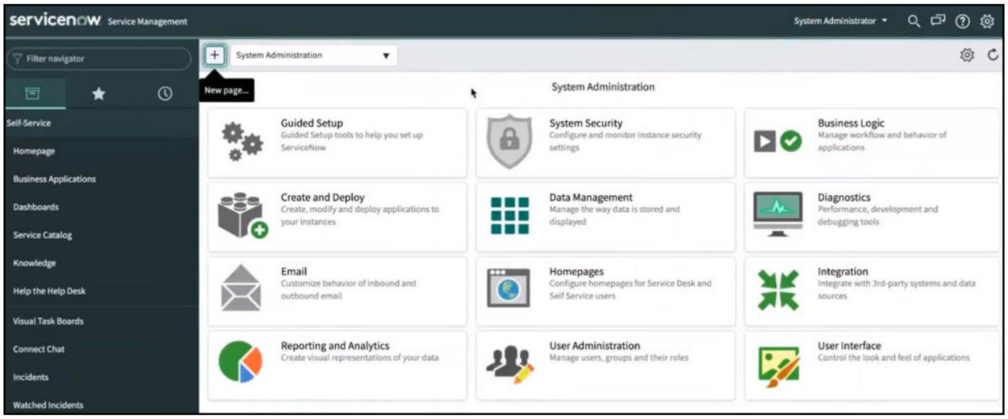
```
{ id: string,                         // Event ID
  type: "incident",                   // Type of webhook event, will be "incident"
for now
  secret: string,                     // Webhook secret
  payload: {                          // incident payload
    status: string,                   // Incident status, e.g. "new" | "ongoing" |
"finished"
    id: string,                       // Unique incident ID
    severity: string,                 // Incident severity, e.g. "P1" | "P2" | "P3" |
"P4"
    link: string,                     // Link to incident,
    title: string,                    // Title of incident
    category: string,                 // Category of Incident
    subCategory: string,              // Sub-Category of incident
    startTime: string,                // Incident start time in ISO 8601 format, e.g.
"2020-11-01T08:00:00.000Z"
    endTime: string,                  // Incident end time/last updated time in ISO
8601 format
    duration: string,                 // Incident duration, e.g. "4d 10h",
    impactedAreaType: string,         // Impacted area type, e.g. "Access Point",
"Zone" or "Domain"
    impactedAreaName: string,         // 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 Group (AP Group) > AP Name (AA:AA:AA:AA:AA:AA)
(Access Point)"
    clientCount: number,              // Total number of client under current
hierarchy
    impactedClientCount: number,      // Total impacted client under current
hierarchy
    impactedClientPercentage: string, // Percentage of impacted client over total
number of client under current hierarchy, e.g. "21.43%"
    rootCauses: string,               // Root Causes of current incident
    recommendations: string           // Recommendations to resolve current incident
  }
}
```

For example, RUCKUS Analytics communicates with ticketing applications in ServiceNow and Salesforce (SFDC) via webhooks. Through webhooks, the incidents generated in RUCKUS Analytics appear in the ServiceNow and Salesforce applications, in real-time. Following is a work-flow to configure Webhooks for ServiceNow and SFDC applications.

Integrating RUCKUS Analytics Incident Webhook with ServiceNow Application

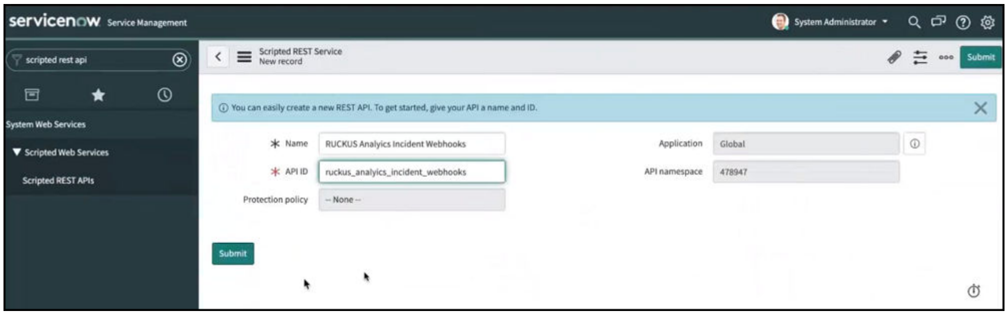
1. Login to the ServiceNow instance

   FIGURE 238 Logging into ServiceNow


servicenow Service Management
System Administrator
Filter navigator
System Administration
New page...
Self-Service
Homepage
Business Applications
Dashboards
Service Catalog
Knowledge
Help the Help Desk
Visual Task Boards
Connect Chat
Incidents
Watched Incidents
Guided Setup
Guided Setup tools to help you set up ServiceNow
System Security
Configure and monitor instance security settings
Business Logic
Manage workflow and behavior of applications
Create and Deploy
Create, modify and deploy applications to your instances
Data Management
Manage the way data is stored and displayed
Diagnostics
Performance, development and debugging tools
Email
Customize behavior of inbound and outbound email
Homepages
Configure homepages for Service Desk and Self Service users
Integration
Integrate with 3rd-party systems and data sources
Reporting and Analytics
Create visual representations of your data
User Administration
Manage users, groups and their roles
User Interface
Control the look and feel of applications

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

   FIGURE 239 Scripted Rest APIs Configuration



You can easily create a new REST API. To get started, give your API a name and ID.

Name: RUCKUS Analyics Incident Webhooks

API ID: ruckus_analyics_incident_webhooks

Protection policy: -- None --

Application: Global

API namespace: 478947

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.
    - Event Types: select the event types from severity P1 to P4.

13. Click **Create**. The new webhook is added to the **Webhook** page. This URL will establish communication between ServiceNow and RUCKUS Analytics and reflect incidents generated within resource groups, in real-time.

    You can edit the Webhook URL configuration by clicking the ✎ icon. Click **Update** to 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.

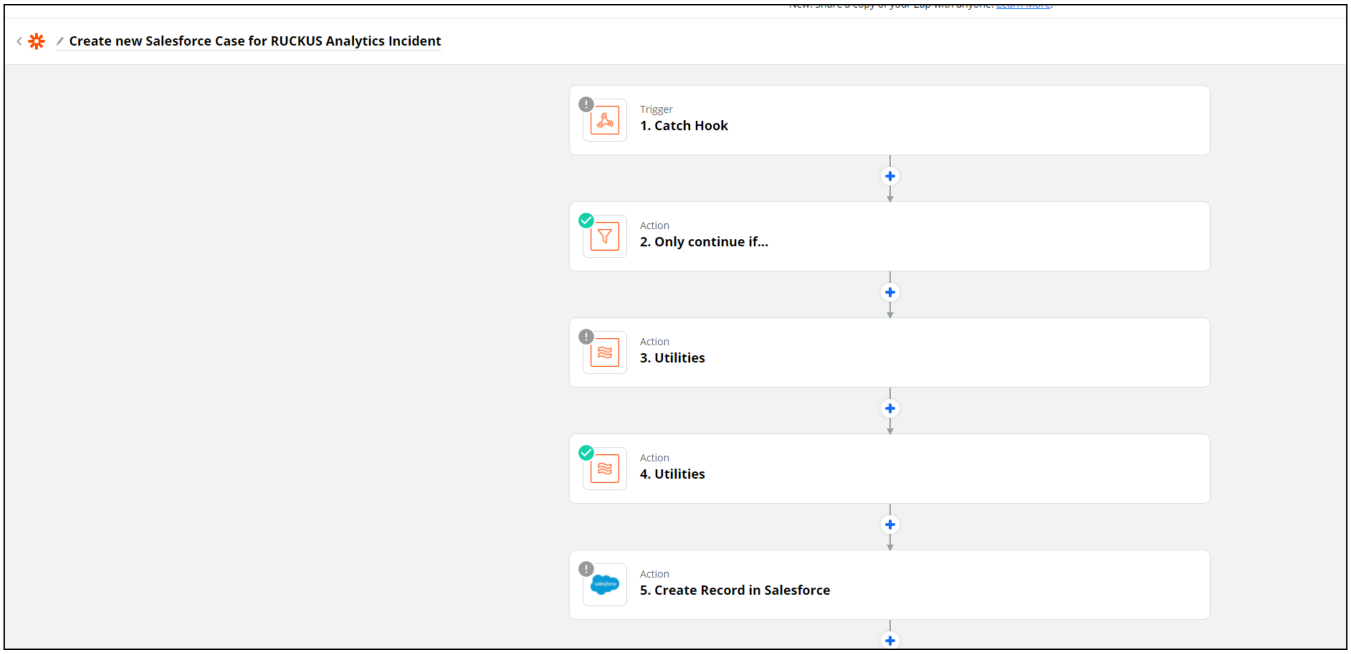
5. Click **Create** to save the configuration.

   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 240 Zapier Web Interface

   Create new Salesforce Case for RUCKUS Analytics Incident

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.

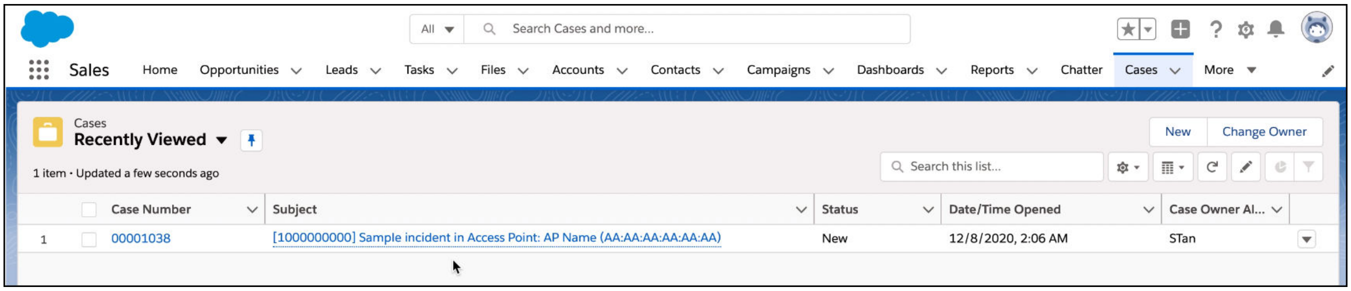
    NOTE
    Do not change the "Subject" as it is used when updating a case.

23. Click **Continue**.

    A Salesforce recorded is now created.

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

FIGURE 241 New Record in Salesforce



1 item • Updated a few seconds ago

	Case Number	Subject	Status	Date/Time Opened	Case Owner Al...
1	00001038	[1000000000] Sample incident in Access Point: AP Name (AA:AA:AA:AA:AA:AA)	New	12/8/2020, 2:06 AM	STan

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

Brand 360

- Brand 360 Overview.. 253

Brand 360 Overview

RUCKUS Analytics introduces a new data-sharing model that facilitates data analytics service for franchise business models related to hospitality sector. The key stakeholders in this model, brands and partners, are bound by a service-level agreement (SLA) that sets the benchmark for the service quality and operations management of the network that is expected to be delivered by the partners.

Brand 360 provides an isolated environment for the brands to view network data of multiple partners collected from network infrastructures deployed across different properties. Brand 360 enables the brands to set SLA thresholds for certain metrics and helps them gain quick insight into the network health and service quality of the properties managed by their partners.

RUCKUS Analytics provides several valuable resources for the brands:

- Dashboard: Provides exclusive access to partner network data that summarizes their SLA compliance level against key metrics.
- Data Studio: Extends intuitive reporting functionality support.
- Labels: Helps to organize and monitor partners and properties.

Brand Invitation

A user can be invited to have the role of a Brand to access and monitor partner's network data. The user who sends the brand invitation is considered the partner and the user who accepts the invitation is considered the brand. When the brand invitation is sent to a user who does not belong to the partner's organization, the partner is explicitly granting the Brand role access to its RUCKUS Analytics service account to the invitee. In addition, depending on the assigned role, the invitee gains access to the partner's account with Admin or Network Admin privileges. If the Admin role is granted, the brand will also be able to invite other users into the partner's account. If this is not desired, make sure to assign the Network Admin role.

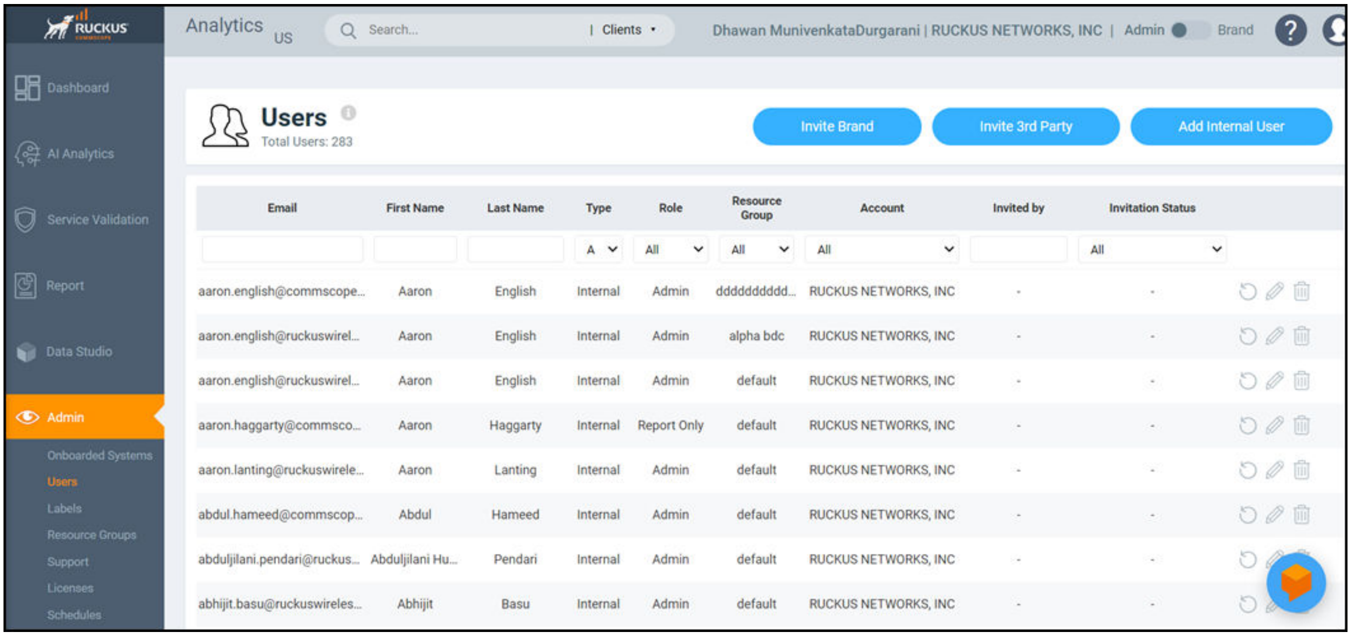
The following prerequisites apply to sending and accepting the brand invitation:

- Only the users who have Admin privileges can send a brand invitation.
- The invitees must have a valid email address registered with RUCKUS Support and have access to their own RUCKUS Analytics service account.
- The invitee cannot have preexisting access to the RUCKUS Analytics service account of the user sending the invitation. The invitee's user account must be removed before sending the brand invitation.

Complete the following steps to invite a user as a brand.

1. From the web interface, go to **Admin** > **Users**.

FIGURE 242 User Management



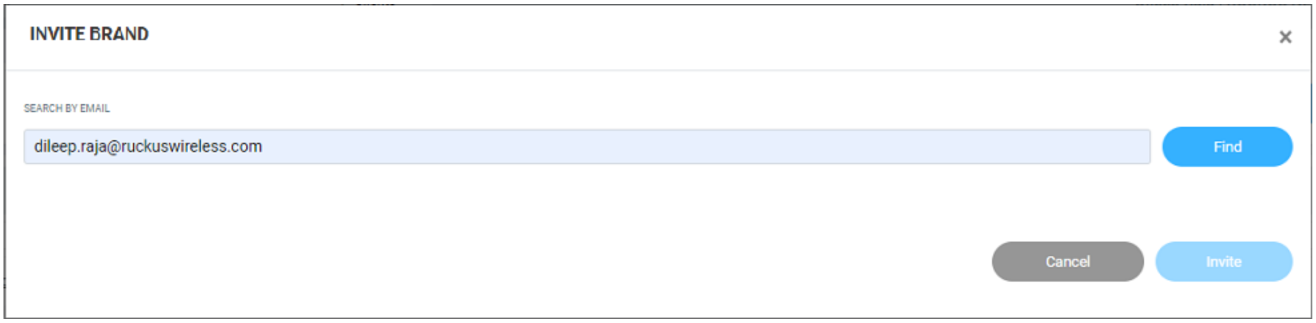
Users
Total Users: 283

Email	First Name	Last Name	Type	Role	Resource Group	Account	Invited by	Invitation Status
			A	All	All	All		All
aaron.english@commscope...	Aaron	English	Internal	Admin	dddddddddd...	RUCKUS NETWORKS, INC	-	-
aaron.english@ruckuswirel...	Aaron	English	Internal	Admin	alpha bdc	RUCKUS NETWORKS, INC	-	-
aaron.english@ruckuswirel...	Aaron	English	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-
aaron.haggarty@commsco...	Aaron	Haggarty	Internal	Report Only	default	RUCKUS NETWORKS, INC	-	-
aaron.lanting@ruckuswirele...	Aaron	Lanting	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-
abdul.hameed@commscop...	Abdul	Hameed	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-
abduljilani.pendari@ruckus...	Abduljilani Hu...	Pendari	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-
abhijit.basu@ruckuswireles...	Abhijit	Basu	Internal	Admin	default	RUCKUS NETWORKS, INC	-	-

2. Click **Invite Brand**.

   The **Invite Brand** dialog box is displayed.

FIGURE 243 Searching by Email ID

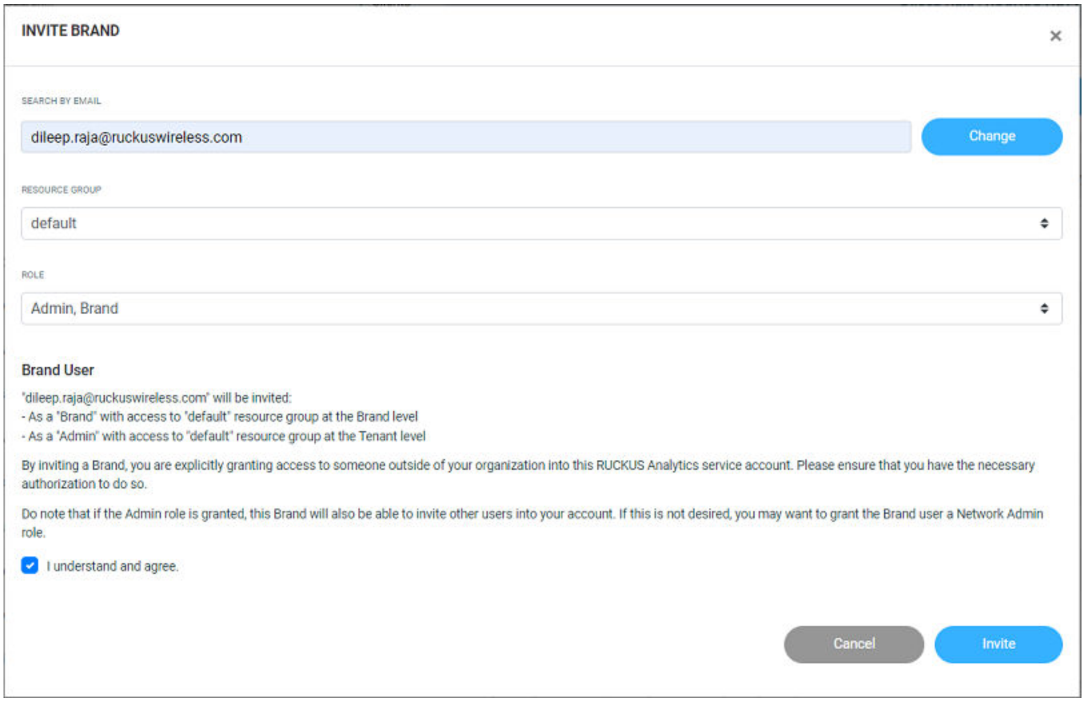


SEARCH BY EMAIL: dileep.raja@ruckuswireless.com

3. Enter the email address of the user and click **Find** to search for the user by email ID.

   The **Invite Brand** dialog box expands to display other required fields.

FIGURE 244 Invite Brand Dialog Box



INVITE BRAND ×

SEARCH BY EMAIL

dileep.raja@ruckuswireless.com

Change

RESOURCE GROUP

default

ROLE

Admin, Brand

Brand User

"dileep.raja@ruckuswireless.com" will be invited:
- As a "Brand" with access to "default" resource group at the Brand level
- As a "Admin" with access to "default" resource group at the Tenant level

By inviting a Brand, you are explicitly granting access to someone outside of your organization into this RUCKUS Analytics service account. Please ensure that you have the necessary authorization to do so.

Do note that if the Admin role is granted, this Brand will also be able to invite other users into your account. If this is not desired, you may want to grant the Brand user a Network Admin role.

☑ I understand and agree.

Cancel Invite

4. Select a resource group from the **Resource Group** list to assign a resource group to which the invitee will have access at the brand level. For more information, refer to Managing Resource Groups on page 236.

5. Select one of the following roles to assign to the user from the **Role** list:

   - **Admin, Brand**: The invitee will have the Brand role at the barnd level and the Admin role at the partner level.
   - **Network Admin, Brand**: The invitee will have the Brand role at the barnd level and the Network Admin role at the partner level.

6. Select the **I understand and agree** check box and click **Invite**.

   Information relevant to the invitee is displayed on the **Users** page. The invitee may accept or reject the invitation; the status of which is also displayed on this page as **Accepted**, **Rejected**, or **Pending**.

   An automated email notification with all the invitation details and an access link to RUCKUS Analytics is sent to the specified email address of the invitee. Simultaneously, the brand invitation details are displayed on the **Accounts** page of the invitee's RUCKUS Analytics service account.

Accepting the Brand Invitation

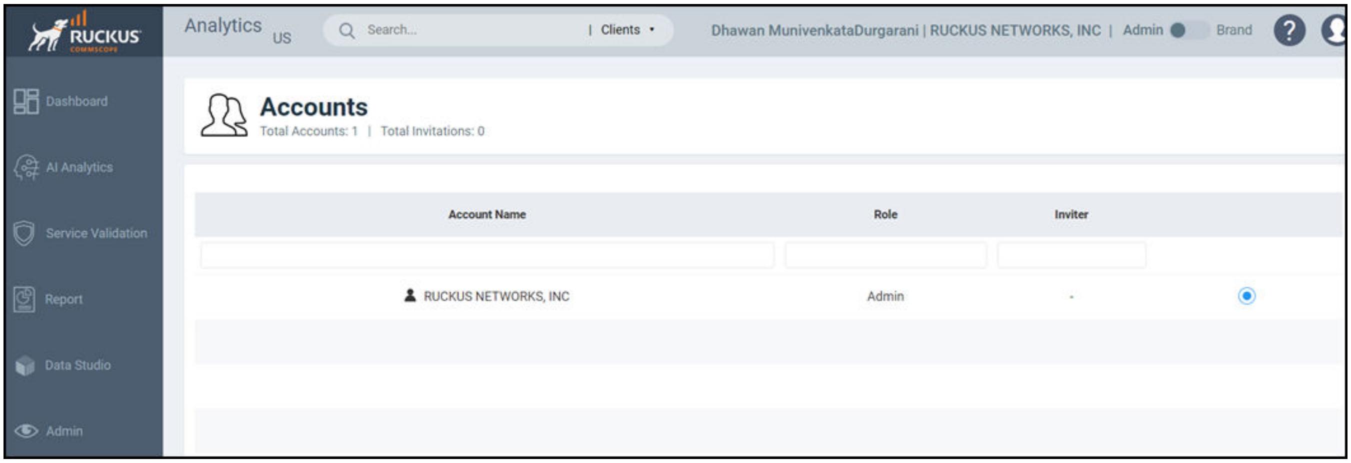
After receiving the brand invitation, the invitee must complete the following steps to accept the invitation.

1. Log in to the RUCKUS Analytics account.

2. Go to **Profile** > **Accounts**.

   The **Accounts** page displays the brand invitation details.

FIGURE 245 Accounts Page: Brand Invitation Notification Details



Accounts
Total Accounts: 1 | Total Invitations: 0

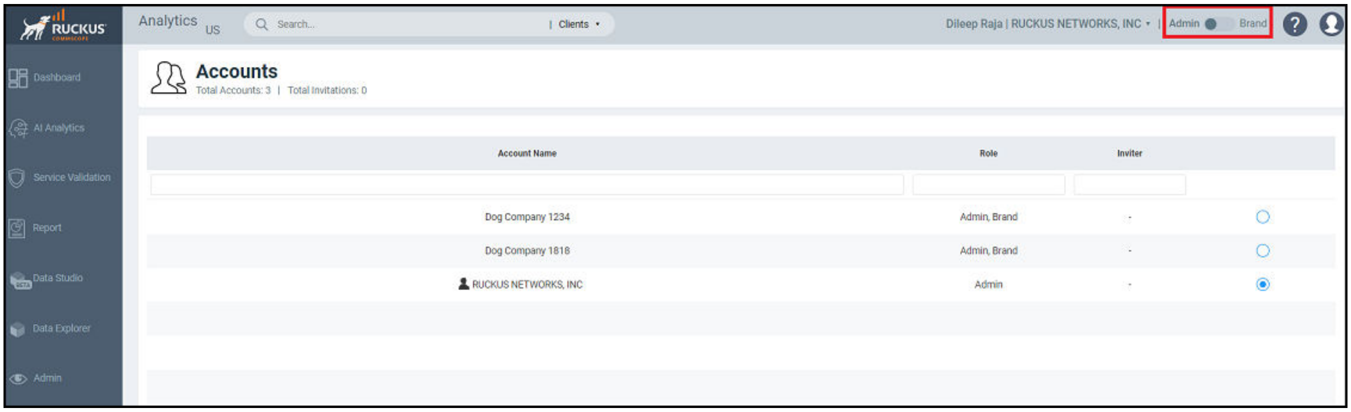
Account Name	Role	Inviter	
RUCKUS NETWORKS, INC	Admin	-	●

3. Click **Accept**.

   A rejected invitation is removed from the account immediately. After an invitation is accepted, a new toggle button is displayed which allows the invitee to switch between the Admin and Brand modes. For more information, refer to Brand 360 Dashboard.

   NOTE
   The toggle button is displayed only under the user's organization service account.

FIGURE 246 Admin and Brand Mode Toggle Button



Accounts
Total Accounts: 3 | Total Invitations: 0

Account Name	Role	Inviter	
Dog Company 1234	Admin, Brand	-	○
Dog Company 1818	Admin, Brand	-	○
RUCKUS NETWORKS, INC	Admin	-	●

Brand 360 Dashboard

The Brand 360 dashboard provides an overview of the associated partners and summarizes the data of the operations management and service quality of the property managed by the partners. The dashboard provides a centralized monitoring window exclusively for the brand to track the aggregate network data of the partners and assess their performance against some key metrics and compliance with service-level agreements (SLAs).

The brand can view the dashboard in two different modes:

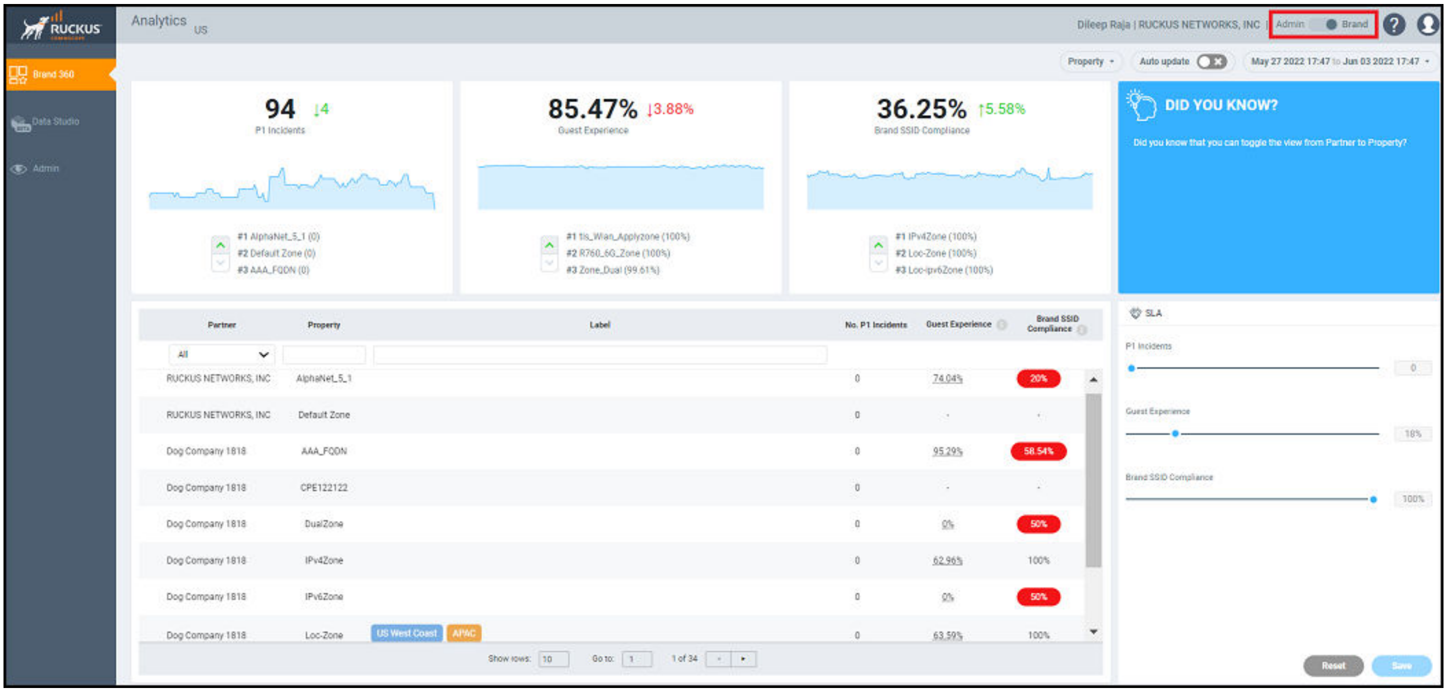
- Brand: Allows a view of the partner's network data for the predefined metrics.

- Admin: Allows a view of the brand's own RUCKUS Analytics service account.

> **NOTE**
> The terms *brand* and *partner* as used in this guide have different meanings in different contexts, and denote roles, modes, and view types at the User Admin level. The brand can customize the UI display names for these attributes in the **My Profile** settings page, where standard vocabulary that aligns with the company's common business glossary can be added. For more information, refer to Naming Convention.

The brand can switch between the Admin and Brand modes using the toggle button on the header panel. The brand can also access the RUCKUS Analytics service account of the partner by selecting the specific account from a list (which is available when the Admin mode is selected). At the partner level, the brand will have Admin or Network Admin privileges depending on the assigned role. For more information about roles and resource groups assigned to the brand, refer to Brand Invitation.

FIGURE 247 Brand 360 Dashboard



Did you know that you can toggle the view from Partner to Property?

Partner	Property	Label	No. P1 Incidents	Guest Experience	Brand SSID Compliance
All					
RUCKUS NETWORKS, INC	AlphaNet_5_1		0	74.04%	20%
RUCKUS NETWORKS, INC	Default Zone		0	-	-
Dog Company 1818	AAA_FQDN		0	95.29%	58.54%
Dog Company 1818	CPE122122		0	-	-
Dog Company 1818	DualZone		0	0%	50%
Dog Company 1818	IPv4Zone		0	62.96%	100%
Dog Company 1818	IPv6Zone		0	0%	50%
Dog Company 1818	Loc-Zone	US West Coast APAC	0	63.59%	100%

The dashboard displays analytics data for three key metrics: P1 Incidents, Guest Experience, and Brand SSID Compliance. These metrics measure the level of service that is expected to be delivered by the partner. The data on the dashboard is displayed based on the selection of date and time range filters. The top portion of the dashboard displays the following tiles:

- **P1 Incidents**: Displays the total number of high-severity incidents that have occurred in the network across all the partners.
- **Guest Experience**: Displays the average percentage of guest experience across all partners. The guest experience score is determined by calculating the average percentage of three metrics: Time to Connect, Connection Success, and Client Throughput.
- **Brand SSID Compliance**: Displays the percentage of the network properties that conforms to the SSID compliance rules set in the **My Profile** settings.

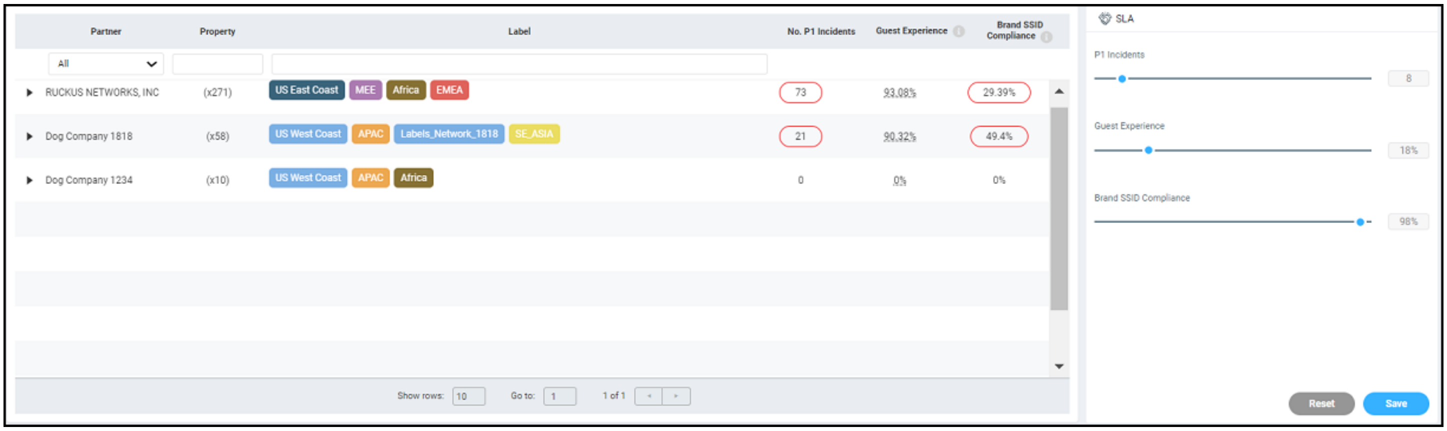
All of the three metrics have the following common elements in their respective tiles:

- Delta counter: Displays the difference in value compared to the previous time period indicating positive or negative change with respect to the metrics.

- Time series graph: Displays the value of respective metrics over time. Pausing the pointer over the time series graph at a particular point displays the value at that time and date.
- Selector arrow: The top three best performing and three underperforming partners or properties with respect to each metric are displayed. The selector arrow can be used to toggle the view to display the three best performers and the three underperformers. The selector arrow is available only if there are more than three partners or properties.

The lower portion of the dashboard displays the data of each partner and property in a table. The brand can customize the SLA threshold for the metrics according to requirements. Every time a new SLA threshold is set, the values displayed on the table change simultaneously as the metrics that meet the updated SLA are considered for analytics. To customize the SLA, in the **SLA** panel, move the slider to adjust the threshold value of each metric and click **Save**.

FIGURE 248 Setting the SLA Threshold



Partner	Property	Label	No. P1 Incidents	Guest Experience	Brand SSID Compliance
All					
RUCKUS NETWORKS, INC	(x271)	US East Coast MEE Africa EMEA	73	93.08%	29.39%
Dog Company 1818	(x58)	US West Coast APAC Labels_Network_1818 SE_ASIA	21	90.32%	49.4%
Dog Company 1234	(x10)	US West Coast APAC Africa	0	0%	0%

Show rows: 10 Go to: 1 1 of 1

SLA

P1 Incidents 8

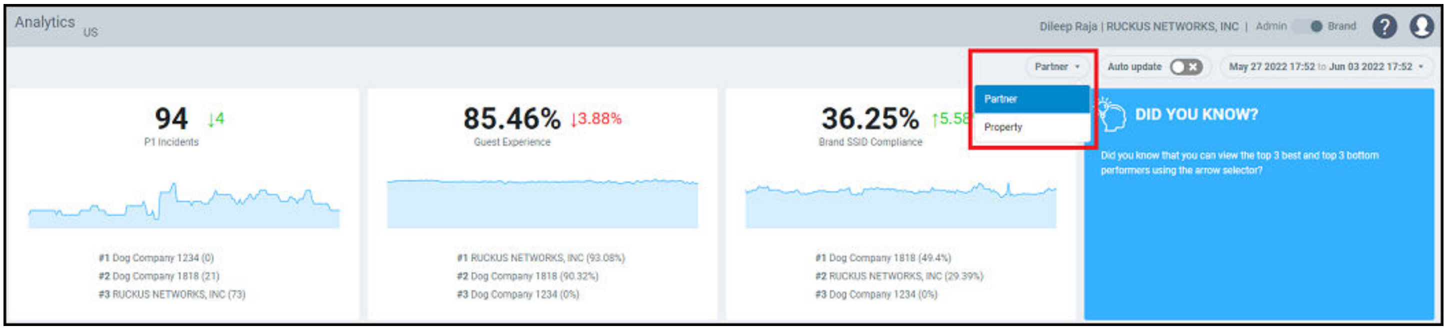
Guest Experience 18%

Brand SSID Compliance 98%

Depending on the selected view type, the format in which the data is populated in the table also changes. The brand can choose between the following view types from the menu:

- Partner: Displays the high-level data of each partner associated with the brand. You must expand each partner to view the details of each property.
- Property: Displays the data of each partner at a granular level showing the data of each property.

FIGURE 249 Brand 360 Dashboard View types



Analytics US

Dileep Raja | RUCKUS NETWORKS, INC | Admin Brand

Partner Auto update May 27 2022 17:52 to Jun 03 2022 17:52

94 ↓4
P1 Incidents

#1 Dog Company 1234 (0)
#2 Dog Company 1818 (21)
#3 RUCKUS NETWORKS, INC (73)

85.46% ↓3.88%
Guest Experience

#1 RUCKUS NETWORKS, INC (93.08%)
#2 Dog Company 1818 (90.32%)
#3 Dog Company 1234 (0%)

36.25% ↑5.58
Brand SSID Compliance

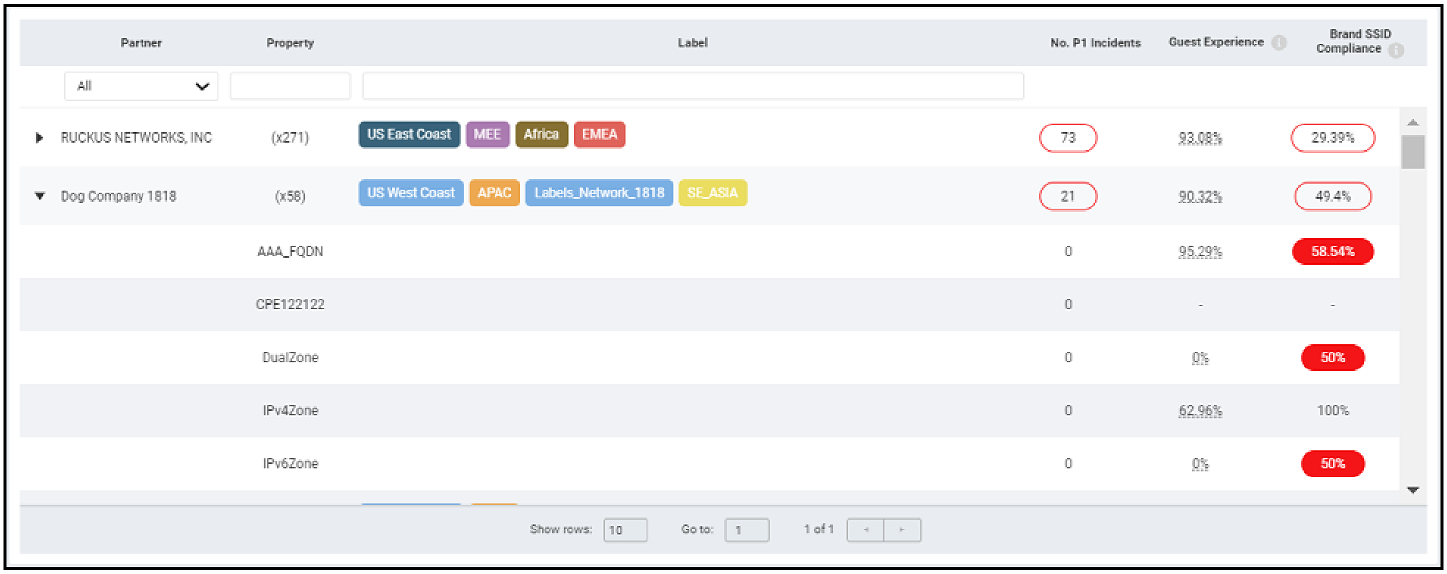
#1 Dog Company 1818 (49.4%)
#2 RUCKUS NETWORKS, INC (29.39%)
#3 Dog Company 1234 (0%)

DID YOU KNOW?

Did you know that you can view the top 3 best and top 3 bottom performers using the arrow selector?

The dashboard table at the bottom displays more information about each brand, partner, and property.

FIGURE 250 Brand 360 Dashboard Table



	Partner	Property	Label	No. P1 Incidents	Guest Experience	Brand SSID Compliance
	All					
▶	RUCKUS NETWORKS, INC	(x271)	US East Coast MEE Africa EMEA	73	93.08%	29.39%
▼	Dog Company 1818	(x58)	US West Coast APAC Labels_Network_1818 SE_ASIA	21	90.32%	49.4%
		AAA_FQDN		0	95.29%	58.54%
		CPE122122		0	-	-
		DualZone		0	0%	50%
		IPv4Zone		0	62.96%	100%
		IPv6Zone		0	0%	50%

Show rows: 10 Go to: 1 1 of 1

The search field under each column head allows you to filter the data and narrow down the search results. Data that matches the search input is rendered in the table. The search field is case-sensitive.

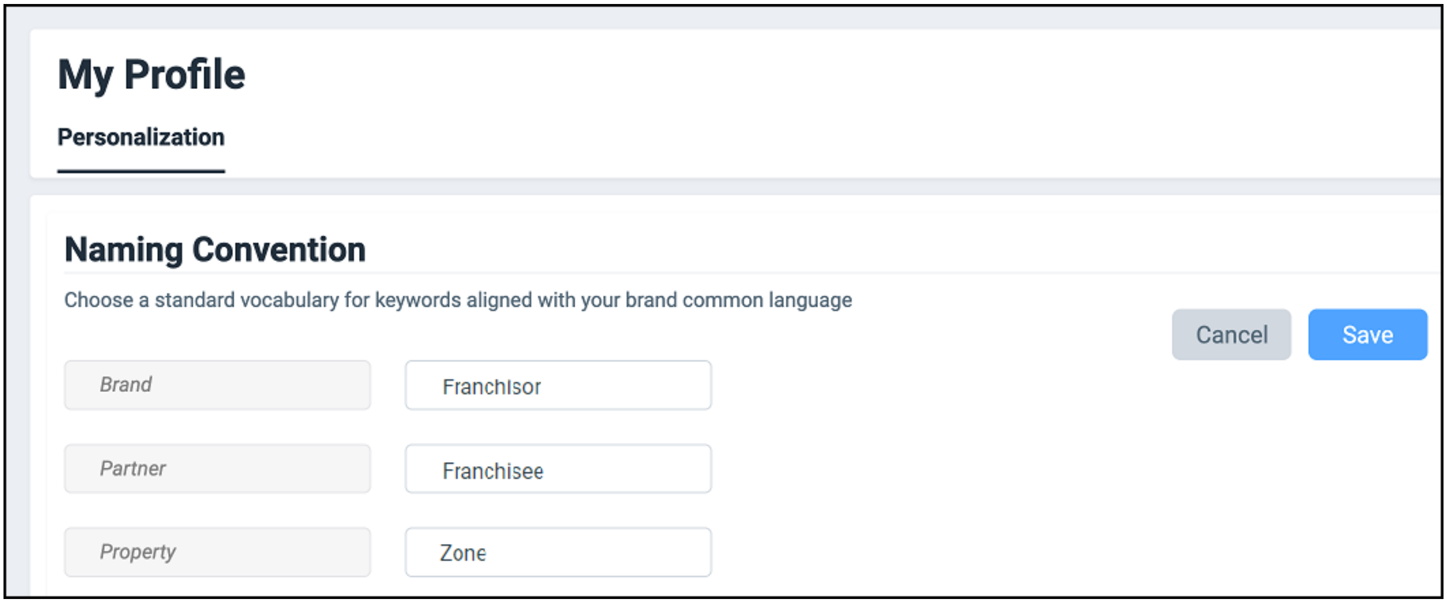
TABLE 26 Brand 360 Dashboard Table Information

Header Field	Description	Additional Information
Partner	Displays the name of the account that is associated with the brand account as a partner.	
Property	Displays the properties managed by the partners.	If the Partner view type is selected from the menu in the top-right of the dashboard, the total number of properties managed by each partner is displayed.
Label	Displays the color-coded labels attached to the partners and properties.	The color-coded labels help the brand to identify the properties managed by different partners spreading across different locations, sites, geographical regions, or networks. For more information, refer to Labels on page 261.
No. P1 Incidents	Displays the number of high-severity incidents that have occurred in the network.	The following design elements indicate SLA compliance status: • Value in a red outlined cell: Indicates that some of the properties managed by the partner do not meet the SLA defined for the respective metrics. This status indication is available only at the partner level. Expand the partner to view the properties that do not meet the SLA. • Value in a red filled cell: Indicates that the property does not meet the SLA defined for the respective metrics.
Guest Experience	Displays the average percentage of guest experience of each partner and property.	
Brand SSID Compliance	Displays the percentage of the network properties that conforms to the SSID compliance rules.	

Naming Convention

Company standards may specify certain naming conventions that must be followed to enable enterprise-wide views of the performance and metrics related to partners and properties. These naming conventions help to maintain consistency and conduct faster analysis of enterprise data. The brand can modify the **My Profile** settings page to change the default naming convention. Enter the standard vocabulary that aligns with the company's common business glossary and click **Save**.

FIGURE 251 My Profile Settings: Editing Naming Conventions



My Profile

Personalization

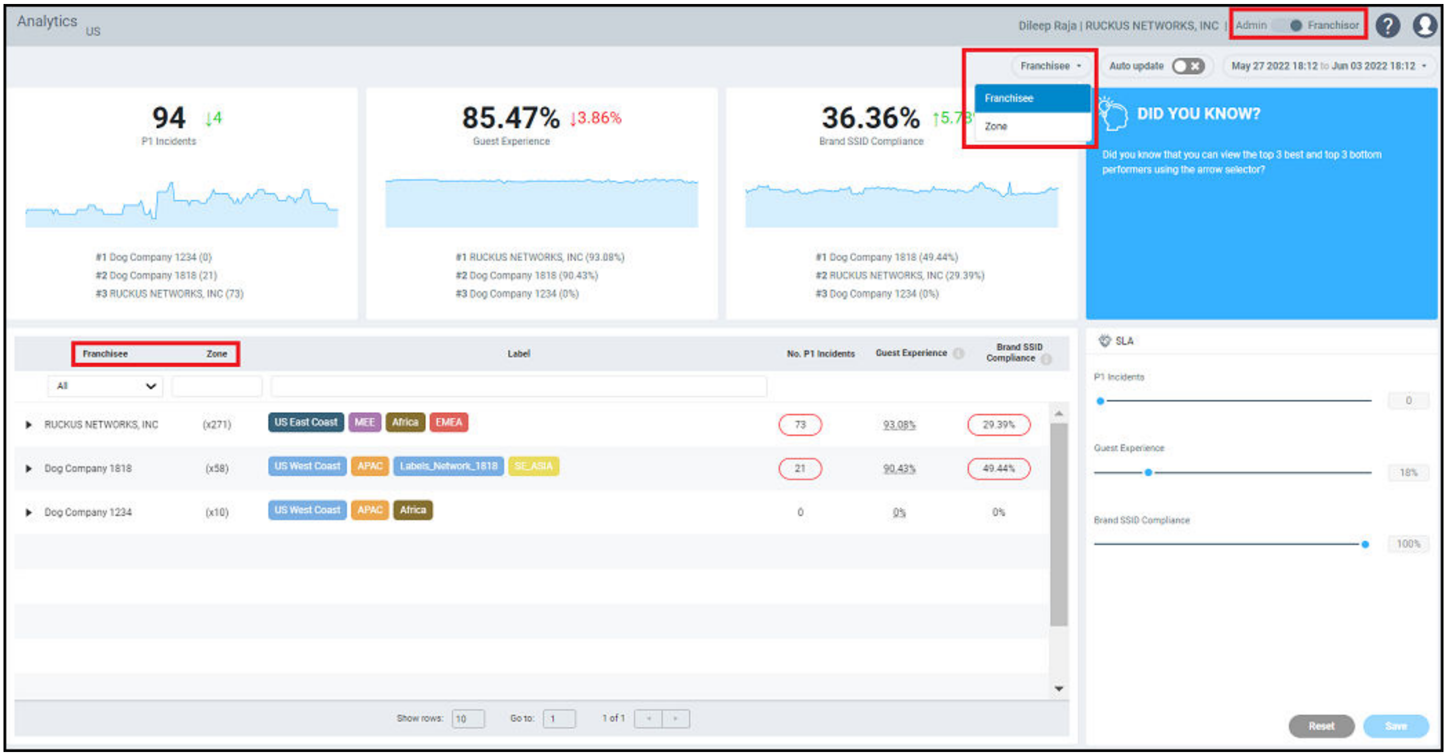
Naming Convention

Choose a standard vocabulary for keywords aligned with your brand common language

Brand	Franchisor
Partner	Franchisee
Property	Zone

The naming convention changes are reflected on the dashboard.

FIGURE 252 Customized Display Names



Analytics US
Dileep Raja | RUCKUS NETWORKS, INC | Admin Franchisor
Franchisee
Franchisee
Zone
Auto update
May 27 2022 18:12 to Jun 03 2022 18:12

94 ↓4
P1 Incidents

#1 Dog Company 1234 (0)
#2 Dog Company 1818 (21)
#3 RUCKUS NETWORKS, INC (73)

85.47% ↓3.86%
Guest Experience

#1 RUCKUS NETWORKS, INC (93.08%)
#2 Dog Company 1818 (90.43%)
#3 Dog Company 1234 (0%)

36.36% ↑5.73
Brand SSID Compliance

#1 Dog Company 1818 (49.44%)
#2 RUCKUS NETWORKS, INC (29.39%)
#3 Dog Company 1234 (0%)

DID YOU KNOW?

Did you know that you can view the top 3 best and top 3 bottom performers using the arrow selector?

Franchisee	Zone	Label	No. P1 Incidents	Guest Experience	Brand SSID Compliance
All					
▸ RUCKUS NETWORKS, INC	(x271)	US East Coast MEE Africa EMEA	73	93.08%	29.39%
▸ Dog Company 1818	(x58)	US West Coast APAC Labels_Network_1818 SE_ASIA	21	90.43%	49.44%
▸ Dog Company 1234	(x10)	US West Coast APAC Africa	0	0%	0%

Show rows: 10 Go to: 1 1 of 1

SLA

P1 Incidents 0

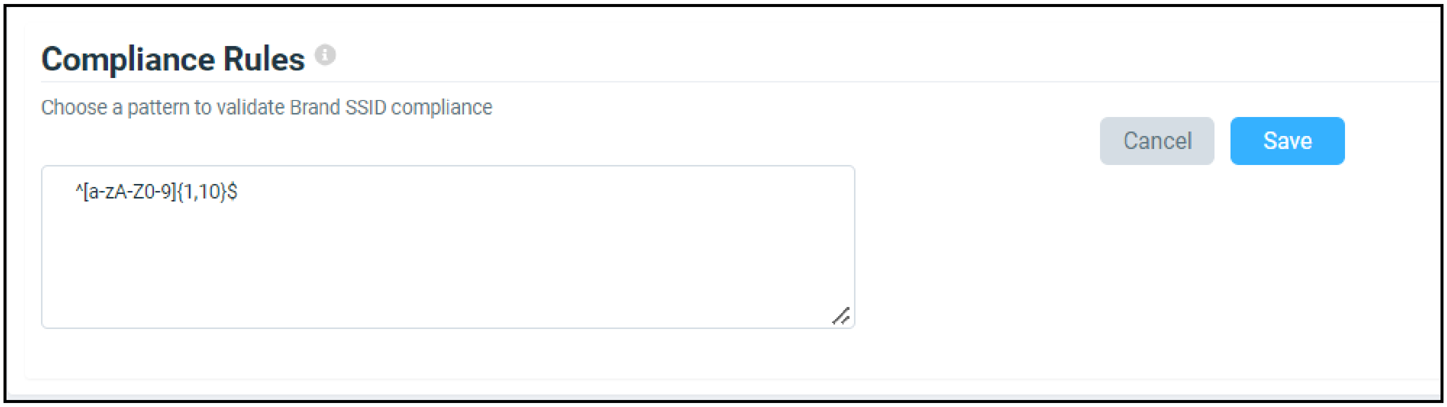
Guest Experience 18%

Brand SSID Compliance 100%

Company standards may require specific naming conventions related to SSIDs too. According to the specified standards, the brand can set the regular expression to validate brand SSID compliance in the **Compliance Rules** section of the **My Profile** settings page. Choose the pattern and click **Save**

NOTE
Regular expressions must be compatible with Java standards.

FIGURE 253 Setting Brand SSID Compliance Rules


Compliance Rules

Choose a pattern to validate Brand SSID compliance

```
^[a-zA-Z0-9]{1,10}$
```

Data Studio

Data Studio extends the intuitive reporting functionality support for the brand. In the Brand mode, a brand can get an aggregate view of data of all the associated partners by creating dashboards, charts, and schedules. Note that, in the Brand mode, a brand can view dashboard templates created only by the users of the brand's RUCKUS Analytics service account. If a partner wants to share a dashboard template with the brand, the import and export dashboard option must be used. For more information, refer to Data Studio on page 197.

Labels

A label is a component that helps the brand to organize and monitor properties. A brand can create and attach a color-coded label to the properties managed by the partners. Depending on the business requirement, multiple properties managed by different partners can be grouped under a single label. Multiple labels can be attached for the same set of properties. The labels attached to the properties are displayed on the dashboard. The labels created from the partner's account are also displayed on the Brand 360 dashboard. The color-coded labels help the brand to identify the properties managed by different partners spreading across different locations, sites, geographical regions, or networks. Labels can be used as filters to aggregate data across multiple partners. For more information, refer to Creating Labels on page 239.

Appendix

- AP - Client Connection Message Mapping... 263

AP - Client Connection Message Mapping

The client connection dataset in Data Studio helps you to visualize AP and client connectivity issues and status. The client and AP exchange a series of 802.11 management frames to get to an authenticated and associated state before establishing a connection. The message IDs in the visualized data represent WiFi messages exchanged between AP and Client or AP and RADIUS server during different stages of the AP-Client connection process. These messages help to determine the process stage at which the connection failed and the reasons for the failure.

TABLE 27 AP - Client Connection Message Mapping

Message ID	Message Category	Message	Source	Destination
1	Probe Request	Probe Request	STA	AP
2	802.11 Authentication	802.11 Authentication Request	STA	AP
3		802.11 Authentication Response	AP	STA
4	802.11 Association	802.11 Association Request	STA	AP
5		802.11 Association Response	AP	STA
6		802.11 Reassociation Request	STA	AP
7		802.11 Reassociation Response	AP	STA
8		802.11 Deauthentication	AP	STA
9		802.11 Disassociation	AP	STA
10		802.11 Deauthentication from STA	STA	AP
11		802.11 Disassociation from STA	STA	AP
21	EAP 4-Way Handshake	4-Way Handshake - Frame 1	AP	STA
22		4-Way Handshake - Frame 2	STA	AP
23		4-Way Handshake - Frame 3	AP	STA
24		4-Way Handshake - Frame 4	STA	AP
31	DHCP	DHCP Discover	STA	Broadcast
32		DHCP Offer	DHCP	STA
33		DHCP Request	STA	Broadcast
34		DHCP Ack	DHCP	STA
35		DHCP NAK	DHCP	STA
41	EAP	EAP Request	AP	STA
42		EAP Response	STA	AP
43		EAP Success	AP	STA
44		EAP Failure	AP	STA
51	RADIUS	RADIUS Access Request	AP	Control Plane
52		RADIUS Access Challenge	Control Plane	AP

TABLE 27 AP - Client Connection Message Mapping (continued)

Message ID	Message Category	Message	Source	Destination
53		RADIUS Access Accept	Control Plane	AP
54		RADIUS Access Reject	Control Plane	AP

350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com