USER GUIDE



Ruckus SmartCell Insight[™] User Guide

Supporting SmartCell Insight[™] 5.2.1

Part Number: 800-72154-001 Rev A Publication Date: 11 February 2019

Copyright, Trademark and Proprietary Rights Information

© 2019 ARRIS Enterprises LLC. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS 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. ARRIS 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. ARRIS 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 ARRIS 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 ARRIS, ARRIS 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 ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup[™], Wi-Fi Multimedia[™], and WPA2[™] are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

About this Document	
Overview	
Document Conventions	7
Related Documentation	8
Documentation Feedback	8
SmartCell Insight Overview	9
SmartCell Insight Introduction	9
Definition of Terms	9
Navigating the SCI User Interface	.10
Header Panel	.11
Using the Navigation Bar	13
Using the Scheduler	14
Overview Dashboard	.17
Using the Overview Dashboard - Content Panel	
Using Ruckus Smart Analytics	19
Actions You Can Perform on the Smart Analytics Display	20
How to View Details from the Ruckus Smart Analytics Display	21
Filters	25
Working With Filters	
AP, SSID and Radio filter	
Date Filter	
Download	
Rx+Tx Filter	
Time Filter	
AP Filters	
SSID Filter	
Client Filter	
Application Filter	
Alarms Filter	
Events Filter	
Sessions Filter	
Using Saved Filters	
Actions You Can Take on a Saved Filter	
Network Report Dashboard	37
Network Report	
Network - Overview	
Network - Traffic Distribution	
Network - Top 10 APs by Traffic Volume	
Network - Top 10 APs by Client Count	
Network - Top APs by Traffic Volume (Table)	
Network - Top APs by Client Count (table)	
Network - Traffic Trend	
Network - Traffic Over Time	
APs & Controllers Report Dashboard	

	APs & Controllers Report	43
	APs & Controllers - Overview	45
	APs & Controllers - Top 10 APs by Offline Duration	
	APs & Controllers - Count Trend	46
	APs & Controllers - Status Trends	47
	APs & Controllers - Top 10 AP Models	47
	APs & Controllers - Top 10 AP Software Versions	48
	APs & Controllers - Top 10 AP Reboot Reasons	
	APs & Controllers - Top 10 APs by Reboot Counts	49
	APs & Controllers - Top 10 AP Alarm Types	49
	APs & Controllers - Top AP Models (table)	50
	APs & Controllers - Top AP Software Versions (table)	
	APs & Controllers - Top APs by Offline Duration (table)	
	APs & Controllers - Top APs by Reboot Count	52
	APs & Controllers - APs Configured in Multiple Systems	53
	APs & Controllers - AP Details for Online/Offline Status	53
	APs & Controllers - AP Details for Other Statuses	54
	APs & Controllers - Resource Utilization	55
	APs & Controllers - License Utilization	55
	KRACK Assessment	56
WL	ANs Report Dashboard	57
	WLANs Report	57
	WLANs - Overview	58
	WLANs - SSID Changes Over Time	59
	WLANs -Top Ten SSIDs by Traffic	59
	WLANs -Top Ten SSIDs by Client Count	60
	WLANs -Active SSIDs Trend	60
	WLANs -Top SSIDs by Traffic (table)	61
	WLANs -Top SSIDs by Client Count (table)	62
Clie	ents Report Dashboard	63
	Clients Report	63
	Clients - Overview	64
	Clients - Top 10 Unique Clients by Traffic	65
	Clients - Clients Details	
	Clients - Unique Clients Trends Over Time (graph)	
	Clients - Unique Clients Trend Over Time (Table)	67
	Clients - Top 10 OS by Client Count	67
	Clients - Top 10 Manufacturers by Client Count	68
	Clients - Top 10 Authentication Methods by Client Count	68
App	blications Report Dashboard	69
• •	Applications Report	
	Applications - Overview	
	Applications - Top 10 by Traffic Volume	
	Applications - Top 10 by Client Count	
	Applications - Top Applications by Traffic (table)	
	Applications - Top Applications by Client Count (table)	
∆ir	time Utilization Report Dashboard	72
	Airtime Utilization Report Dashboard	
	······································	

Airtime Utilization - Overview	
Top 10 APs By Airtime Utilization	
Top APs by Airtime Utilization for 2.4 Ghz	75
Airtime Utilization - Top APs by Airtime Utilization for 5 GHz	
Airtime Utilization Trend	
Airtime Utilization - Over Time	77
AP Details Report Dashboard	
AP Details Report	79
AP Details - Summary	81
AP Details - Performance	
AP Details - Details	
AP Details - Stats	
AP Details - Uptime History	
AP Details - Traffic Trend	
AP Details - Unique Clients Trend Over Time	
AP Details - Top 10 Clients by Traffic Volume	85
AP Details - Top 10 Applications by Traffic Volume	
AP Details - Top SSIDs by Traffic	86
AP Details - Sessions	
AP Details - RSS Trend	
AP Details - SNR Trend	
AP Details - Airtime Utilization Trend	
AP Details - Clients Details	
AP Details - Alarms	
AP Details - Events	
AP Details - Anomalies	
Client Details Report Dashboard	
Client Details Report	
Client Details - Summary	
Client Details - Stats	
Client Details - Top 10 Applications by Traffic Volume	
Client Details - Traffic Trend	
Client Details - RSS Trend	
Client Details - SNR Trend	
Client Details - Sessions	
Data Explorer Dashboard	97
Data Explorer and Data Cubes	
Data Exploration	
Using Filters	
Dashboards	
Applications	
Network	
Airtime Utilization	101
Clients	
Sessions	
Events	
AP Inventory	
AP Alarms	
Controller Inventory	

Rogue APs	
Data Cube Filters	
Dimensions	
Measures	115
Filter	
Explore	
View Outputs	
Add to Dashboard	
Share Link	
Options	
Pinboard	
Time Compares	
Creating a Data Explorer Dashboard	
Actions You Can Perform on an Existing Dashboard	
Opening a Dashboard	
Editing a Dashboard	
Exporting Raw Data Using the SCI Virtual Machine Command Line Interface	
Template File for Exporting Raw Data	
Raw Data Output for Dimensions and Measures	
PII Hashing	151
Hashing Data-Source Attributes	
Template File for PII Hashing	
Admin Dashboard	
Admin Console	
Status and Update	
Nodes	
Notifications	
Update	
Diagnostics	
Settings	
Controller Settings SMTP Settings	
Data Retention	
Instantly Pruning Old Data	
Authentication Tab on the SCI UI	
License	
PCI Profiles	
Creating a PCI Profile	
Opening and Downloading a PCI Profile Report	
Editing or Deleting a PCI Profile	
Users and Roles	
Resource Groups	
Users and Their Roles	
Creating Resource Groups	
Creating Users and Roles	
Creating Users and Roles	

About this Document

•	Overview	.7
•	Document Conventions	
•	Related Documentation	
•	Documentation Feedback	

Overview

This *SmartCell Insight User Guide* provides instructions about how the Ruckus Wireless[™] SmartCell Insight (SCI) application works, the reports that it generates, and how to use these reports.

This guide is written for service operators and system administrators who are responsible for managing, configuring, and troubleshooting Wi-Fi networks. This guide assumes basic working knowledge of local area networks, wireless networking, and wireless devices.

NOTE

Refer to the release notes shipped with your product to be aware of certain challenges when upgrading to this release.

Most user guides and release notes are available in Adobe Acrobat Reader Portable Document Format (PDF) or HTML on the Ruckus Wireless Support Web site at https://support.ruckuswireless.com/contact-us.

Document Conventions

The following two tables list the text and notice conventions that are used throughout this guide.

Convention	Description	Example
monospace	Represents information as it appears on screen	[Device name]>
monospace bold	Represents information that you enter	<pre>[Device name]> set ipaddr 10.0.0.12 ruckus# show running-configap-heartbeat</pre>
default font bold	UI components such as screen or page names, keyboard keys, software buttons, and field names CLI command names and keywords	On the Start menu, click All Programs . ruckus# show running-config ap-heartbeat
italics	Publication titles CLI command modifiers and variables.	Refer to the SmartZone TM (SZ) 100 and Virtual SmartZone Essentials (vSZ- E) Command Reference for more information ap- mac

TABLE 2 Notice conventions

Notice Type	Description
NOTE	Information that describes important features or instructions

TABLE 2 Notice conventions (continued)

Notice Type	Description
CAUTION	Information that alerts you to potential loss of data or potential damage to an application, system, or device
WARNING	Information that alerts you to potential personal injury

Related Documentation

For a complete list of documents that accompany this release, refer to the Release Notes.

Documentation Feedback

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

You can email your comments to Ruckus Wireless at: docs@ruckuswireless.com

When contacting us, please include the following information:

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

SmartCell Insight Overview

•	SmartCell Insight Introduction	9
	Definition of Terms	
•	Navigating the SCI User Interface	
•	Header Panel	
	Using the Navigation Bar	
	Using the Scheduler	

SmartCell Insight Introduction

SmartCell Insight (SCI) is a big data analytics and reporting platform that enables efficient management of wireless networks. SCI provides visibility into network performance, operation, and planning of Ruckus wireless networks.

SCI also provides predictive analytics through automated machine learning, without requiring manual configuration.

SCI uses scale-out architecture with support for clustering. A single instance of SCI can collect, process, correlate and aggregate data from more than 100,000 access points.

SCI helps manage and optimize a wireless network by providing analytics, reporting, and key performance indicators (KPIs) about devices, users, applications, access points, controllers, and more. SCI has several pre-built dashboards/reports, in addition to the ability to slice-and-dice data in Data Explorer to create custom reports.

SCI supports Ruckus SmartZone and Ruckus ZoneDirector controllers.

NOTE

All values in the reports, except AP counts, are approximate values unless otherwise stated.

Definition of Terms

The following are terms used in SCI.

TABLE 3 Definition of Terms

Term	Definition
User Traffic	
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
Rx User	Traffic volume, which is received by AP (Access Point) in IEEE 802.11 MAC Service Data Unit (MSDU) data frames. This includes all unicast, multicast and broadcast traffic.
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
Management Traffic	
Management Traffic	Traffic volume, which is transmitted and received in IEEE 802.11 control and management frames. This includes all unicast, multicast and broadcast traffic. Abbreviations <i>Mgmt</i> or <i>Mgt</i> are frequently used in the user interface. Mgmt Traffic = Rx Mgmt + Tx Mgmt
Rx Mgmt	Traffic volume, which is received by AP (Access Point) in IEEE 802.11 control and management frames. This includes al unicast, multicast and broadcast traffic.

TABLE 3 Definition of Terms (continued)

Term	Definition
Tx Mgmt	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
Total Traffic	
Total Traffic	Is the sum of the user traffic and management traffic.
Rx Total	Is the sum of the Rx user traffic and management traffic.
Tx Total	Is the sum of the Tx user traffic and management traffic.
Relationship betwee	n various traffic metrics
• Total Traffic =	- User Traffic + Management Traffic = Rx Total + Tx Total
• Rx Total = Rx	User + Rx Managemet
• Tx Total = Tx	User + Tx Managemet
User Traffic =	Rx User + Tx User
 Managemet[*] 	Traffic = Rx Managemet + Tx Managemet
Average Traffic Rate	Traffic volume divided by the selected time period, displayed in bits per second. For example, if the traffic volume for a 15 minutes period is 100GB, the average traffic rate is 889Mbps.
Unique Client	A Wi-Fi client, uniquely identified by its MAC address.
	NOTE <i>All Radios</i> unique count will not be larger than the sum of the <i>2.4GHz</i> and <i>5GHz</i> radios. This is because a Wi- Fi client could connect to both radios within the selected time granularity, and <i>All Radios</i> unique count will consider this client as a single count.
Session	In SCI, session refers to IEEE 802.11 session. This is an OSI Layer 2 session that is established when a Wi-Fi client associates to an access point and it ends when the client disassociates from the access point.
	This is NOT the same as OSI Layer 7 application layer sessions, like a HTTP session, telnet session, etc. More often than not, a single IEEE 802.11 session cannot support multiple application layer sessions, and the creation and termination of IEEE 802 sessions are often transparent to the user at the application layer.

Navigating the SCI User Interface

The SCI user interface consists of four major sections: a header panel at the top, a navigation bar to the left of the screen, an expandable Schedules panel, and the main content panel.

Use the navigation bar on the left side of the screen to access any of the built-in reports, customize the way you view your data using the Data Explorer, or configure administrator settings.

The following image illustrates the four main sections of the SCI user interface. Refer to the table below for descriptions of each web interface element.

FIGURE 1 SCI web interface elements

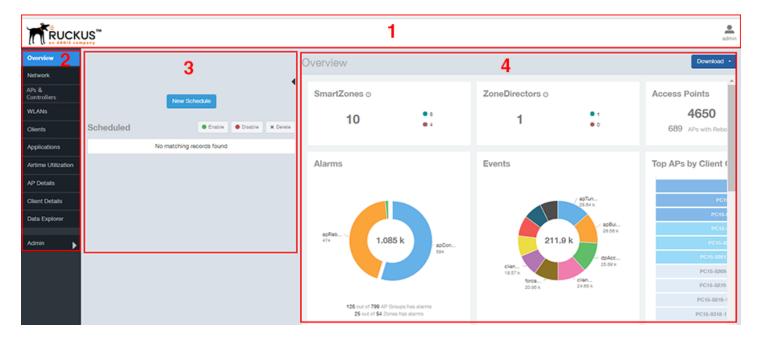


TABLE 4 SCI web interface elements

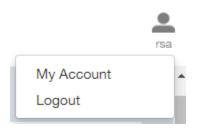
No.	Name	Description
1	Header Panel	Displays the currently logged in user profile. Click the user icon 🔎 to update the profile or change the password as required.
2	Navigation Bar	Contains links that take you to the various dashboards and the Data Explorer cubes and Admin console.
3	Schedules Panel	Allows you to create schedules for generating and delivering reports.
4	Content Panel	This large section contains the content of the page you are currently viewing.

Header Panel

The header panel contains information about the user.

When you click the user icon \blacksquare a pop-up appears with two options.

FIGURE 2 User Information pop-up



Click the:

- **My Account** link to launch the My Account screen and enter user information.
- **Logout** link to log out of SCI.

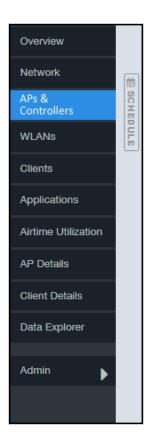
FIGURE 3 My Account

My Account	
Profile	
Email:*	ops@ruckuslbs.com
	This email will receive alerts regarding the system
Username:*	admin
First Name:*	First
Last Name:*	Last
	Update Profile
Password	
Current Password:	
New Password:	Minimum 8 characters
Confirm Password:	Minimum 8 characters
	Change Password

You can add profile information such as email ID for the user, and click the **Update Profile** button to save the change. You can also enter, change and confirm your password, and click the **Change Password** button to save the changes.

Using the Navigation Bar

Use the navigation bar to access all dashboards of the SCI, as shown in the following figure.



The main actions you can take from the navigation bar include:

- Using the **Admin** console. The Admin console is where you add controllers to your network. The admin console also shows the health of the system and checks for updates. Links to view the status of external sources that SCI uses, such as Hadoop, Spark and Druid, are also provided.
- Using **Data Explorer**. Data Explorer is a custom reporting tool that allows you to manipulate an OLAP (Online Analytical Processing) cube to address the needs of a wide variety of users. Refer to Data Explorer and Data Cubes on page 97 for details.
- Generating reports. The remaining dashboards in SCI can be used to generate reports.
 - To filter the content displayed, click either the **AP SSID Radio** filter or the **Time Period** filter. For more information about using filters to generate specific reports, refer to the Working With Filters on page 25
 - To download a copy of the content currently displayed on the screen, click **Download**, and select **CSV** or **PDF** as the file type.

Using the Scheduler

The Scheduler allows you to create schedules to generate reports to be sent out to recipients.

To invoke the Scheduler, click the thin "Schedule" frame just to the right of the navigation bar in any of the report dashboards. The example below is from the Overview dashboard.

FIGURE 4 Schedule frame to click to invoke Scheduler

SmartCell Insi	gnt				
Overview	(Overview			
Network					
APs & Controllers	SCHEDULE	SmartZones @		ZoneDirectors o	
WLANs	ULE	11	• 6	1	• 1
Clients			● 5		• 0
Applications					

The Scheduler allows you to create reports at set dates and times. The area numbered 1 in the figure below contains the Schedules frame. The black arrow head at the top right hand corner of the Schedules frame works like a toggle switch, and allows you to expand or collapse the frame. Select the **New Schedule** button on the top of the Scheduler to create a new schedule. The **Create Schedule** screen appears, as shown in the area numbered 2 in the figure below.

FIGURE 5 Scheduler on the Overview Dashboard

		-		Overview			2		Download •
		New Sch	•0.60	Schedule Name		Format	Select one	Repeat Select one •	
Sched	uled		Enable Enable X Delete	Recipient(s)	Email addresses separate	i by comma ()			
0	Jason Test PDF	•	May 19 2017 13:00 +08:00	For quarterly and yearly sele 23:59	ction, the date range is fixed	i.e. 1st Jan 00:00 - 31 Mar	r 23:59 and 1st Jan 00:00 - 31 Dec	Save	Cancel
. 0	Jason Test CSV	•	May 19 2017 13:00 +08:00						1
				SmartZones ⊘ 11	• 0 • 0	ZoneDirecto	ors () • 1 • 0	Access Points 4731 465 APs with Reboots	• 43 • 40 • 4

- **Name**: Enter the name of the schedule.
- Format: Select the format of the report from the drop down list, either PDF or CSV.
- **Repeat**: Select a time frame for the schedule, whether Daily, Weekly, Monthly, Quarterly, or Yearly. If you select Daily, you also need to set the hour from the Hour drop down list. If you select Weekly, you also need to set the Day of Week and Hour. If you select Monthly, you also need to set the Day of Month and Hour. If you set Quarterly or Yearly, the date range is fixed before hand.
- **Recipient(s)**: Enter the email addresses of one or more recipients. If you have more than one email address to enter, separate the email addresses with a comma.

Click **Save** to save the schedule details. A new schedule is created and listed in the Schedule frame numbered 1 in the figure above.

NOTE

The Scheduler creates reports one hour after the specified time regardless of whether data exists.

The Schedule frame contains the list of created schedules, and above this list of schedules, the **Enable**, **Disable**, and **Delete** buttons. Select the schedule from the list and click the:

- **Enable** button to activate the schedule.
- **Disable** button to deactivate the schedule.
- **Delete** button to remove the schedule.

The schedule frame is integrated into all the report dashboards. All the filters and functionality of the dashboards can be used to create reports to be sent at specific dates and times to recipients. A sample Network dashboard is shown in the figure below. Refer to the specific dashboard for the description of how the dashboard and filters work.

FIGURE 6 Network Dashboard Containing Schedules



Overview Dashboard

•	Using the Overview Dashboard - Content Panel	.17
•	Using Ruckus Smart Analytics	19

Using the Overview Dashboard - Content Panel

The Overview dashboard is the main dashboard that is displayed when you log in to SCI. It provides an overview of some important statistics of your WiFi network, shown in the figures below.

The purpose of this section is to describe the areas of the content panel of the Overview dashboard.

FIGURE 7 Overview Dashboard - Top Portion

hetriew letwork	Over	view						I	Jan 11 2018 - Jan 12 2018 -	Download
Pa & Controllers VLANs	Sm	nartZones o	•		oneDirectors o	••	Acce	ss Points 3002	• 2000	
lients polications		11	• 5		4	•1		278 APs with Reboot	• 992 5 • • 4	
utime Utilization	Ru	ckus SmartAnalyt	cs							
P Details					Found 51	APs for review ^{385ers mix?}				
Nent Details		User Traffic (10	Client Count 12	Se	ssion Count 🔟	Short Session	Ratio 🚺	Reboot Count 🔘	
ata Explorer		AP Name	Anomalies (Yesterday)	Anomalies (30 Day	vs) User Traffic So	core Client Count So	core Session Count	Score Short Session	Ratio Reboot Count 8	s 🌣
dmin 🕨		AP1	3	0	7.4	7.1	7.3			
		AP2	2	20	8.5	-	-	8.1		
		AP3	2	1		6.5	7.9			
		AP4	2	0		8.6	8.7			
		AP5	2	0		6.0	7.0			
		AP6	2	1		7.0	7.1			
		AP7	2	11		7.7	7.8			
		AP8	2	7		82	7.4			
		AP9	2	0		7.4	7.4			
		AP10	1	0			6.9			
						1 ¢ of 6 🕨				

The areas shown in this portion of the Overview Dashboard are:

- SmartZones Displays the number of SmartZone controllers being used in your WiFi network. The green and red dots depict how many of these controllers are active and inactive. For more information on the controllers that you have registered, go to the Admin Console > Settings portion of SCI.
- ZoneDirectors Displays the number of ZoneDirector controllers being used in your WiFi network. The green and red dots depict how many of these controllers are active and inactive. For more information on the controllers that you have registered, go to the Admin Console > Settings portion of SCI.
- Access Points Shows the number of APs in the network. Green and red status indicates if they are up or down, and yellow indicates other statuses, such as "Provisioned," "Discovery," and " Rebooting."

Overview Dashboard

Using the Overview Dashboard - Content Panel

• Ruckus SmartAnalytics - For information about how to use Smart Analytics, refer to Using Ruckus Smart Analytics on page 19.

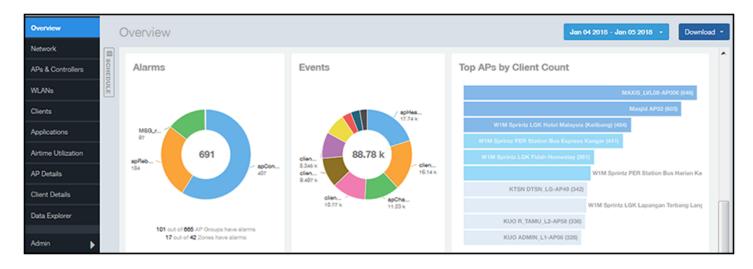


FIGURE 8 Overview Dashboard - Middle Portion

The areas shown in this portion of the Overview Dashboard are:

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



FIGURE 9 Overview Dashboard - Lower Portion

The areas shown in this portion of the Overview Dashboard are:

- Total Traffic Shows statistics about traffic received and transmitted by the access points, including the maximum and minimum rates of traffic. Go to the Network dashboard for more information about traffic.
- Total Unique Sessions Shows the number of IEEE 802.11 sessions between all clients and APs on the network. Go to the Data Explorer dashboard for more information about sessions.
- WLANs Displays the top SSIDs by traffic, which is also shown in the WLANs dashboard. Hover over a portion of the pie 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 dashboard.
- Applications Shows the applications being used more frequently by the clients in the network. For more information about applications usage, go to the Applications dashboard.
- "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.

Using Ruckus Smart Analytics

Ruckus Smart Analytics uses advanced analytics techniques to identify APs that are exhibiting different-from-normal behavior, and flags them for review.

If an AP is flagged for review, it does not necessarily mean that there is a problem with the AP. It just means that Ruckus Smart Analytics detected outside-of-normal behavior for that AP. An AP is flagged for review under the following conditions:

- User Traffic: An AP is flagged for review when the User Traffic is unusually high or low compared to the expected trends
- Client Count: An AP is flagged for review when the Client Count is unusually high or low compared to the expected trends
- Session Count: An AP is flagged for review when the Session Count is unusually high or low compared to the expected trends
- Short Session Ratio: An AP is flagged for review when the ratio of short sessions per total sessions becomes unusually high.
- Reboot Count: An AP is flagged for review when the number of times the AP has been rebooted is unusually high.

The following figure shows an example of Ruckus Smart Analytics output, which appears only on the Overview dashboard:

FIGURE 10 Default Display Example of Ruckus SmartAnalytics

			Found 51 APs f	or review What's this?			
User Traff	ic 10	Client Count 12	Session	Count 10	Short Session Ratio	Rel	poot Count 📵
AP Name	Anomalies (Yesterday)	Anomalies (30 Days)	User Traffic Score	Client Count Score	Session Count Score	Short Session Ratio	Reboot Count S
AP1	3	0	7.4	7.1	7.3		-
AP2	2	20	8.5	-		8.1	-
AP3	2	1	-	6.8	7.9		
AP4	2	0	-	8.6	8.7		
AP5	2	0	-	6.8	7.0		-
AP6	2	1	-	7.0	7.1		-
AP7	2	11		7.7	7.8		
AP8	2	7	-	8.2	7.4		-
AP9	2	0	-	7.4	7.4		
AP10	1	0	-		6.9		-

After the first few days, the system begins showing results, but the accuracy of the results improves over time, as the system learns more about the AP user traffic, client and session patterns. The results are usually accurate after one month, when the system completes learning and understands the short-term, medium-term and long-term trends for each of these metrics for each AP. The list of APs for review is refreshed every 24 hours.

NOTE

At the top of the SmartAnalytics display, shown above, each anomaly type (User Traffic, Client Count, Session Count, Short Session Ratio, and Reboot Count) has a number in grey. These numbers indicate the total number of access points flagged for possible problems for the corresponding anomaly type.

Actions You Can Perform on the Smart Analytics Display

The default display of the Ruckus SmartAnalytics information shows all possible anomalies for all access points that you have currently selected. You can do the following:

- To interpret the color coding and associated scores, note that the closest the score is to 10, the more likely there is to be an issue with the AP for the corresponding anomaly type:
 - Deep red = a score in the range of 9 to 10
 - Orange red = a score in the range of 8 to 9
 - Amber = a score in the range of 7 to 8
 - Deep yellow = a score in the range of 6 to 7
 - Bright yellow = a score in the range of 5 to 6
- Click on any AP to go to the AP Details dashboard for that AP, where you can then view anomaly charts for details, as shown in How to View Details from the Ruckus Smart Analytics Display.
- Use the gear icon on the upper right of the SmartAnalytics display to customize the output.
- Click on any of the Anomaly tabs to display the output for only the tabs you select. For example, if you want to view only the access points that have a possible anomaly with reboot count, highlight the Reboot Count tab only. The following

figure shows a sample display for this scenario (note that the Reboot Count tab has been selected and appears in gray below):

			Found 51 APs f	or review What's this?			
User Traff	ic 16	Client Count 12	Session (Count 10	Short Session Ratio	14 Re	boot Count 🕐
AP Name	Anomalies (Yesterday)	Anomalies (30 Days)	User Traffic Score	Client Count Score	Session Count Score	Short Session Ratio	Reboot Count S
AP11	1	30	-	-	-		8.6
AP12	1	0	-				7.1
AP13	1	3	-	-	-	-	6.6
AP14	1	2	-	-			6.6
AP15	1	2	-	-	-	-	6.4
AP16	1	2	-				6.4
AP17	1	0	-	-		-	6.4
AP18	1	4	-	-	-	-	6.2
AP19	1	2					6.2

FIGURE 11 Ruckus SmartAnalytics Output When Filtering on Reboot Count Only

• To sort anomalies by one of the scores, click on the desired column, then use the arrow that appears. The screen below shows sorting on Client Score Count, with the highest score on top.

ickus Smarl	Analytics						
			Found 51 APs	for review What's this?			
User Traff	ic 16	Client Count 12	Session	Count 10	Short Session Ratio	14 Ret	boot Count 💿
AP Name	Anomalies (Yesterday)	Anomalies (30 Days)	User Traffic Score	Client Count Score V	Session Count Score	Short Session Ratio	Reboot Count S
AP1	2	0	-	8.6	8.7	-	-
AP2	2	7	-	8.2	7.4	-	-
AP3	2	11	-	7.7	7.8	-	-
AP4	1	4		7.6			-
AP5	2	0	-	7.4	7.4	-	-
AP6	3	0	7.4	7.1	7.3	-	-
AP7	2	1	-	7.0	7.1	-	-
AP8	1	0	-	6.9	-	-	-
AP9	2	1	-	6.8	7.9	-	-
AP10	2	0	-	6.8	7.0		-
			-1¢	of 6 🕨			

How to View Details from the Ruckus Smart Analytics Display

From the Ruckus Smart Analytics output, you can click on an AP/MAC Address link, which takes you to the AP Details Dashboard, where graphical representations of each anomaly type for that AP are shown (see the illustrations below for examples).

The following figures show examples of each anomaly type, with extra detail provided when you place your cursor over a portion of the chart.

FIGURE 12 Client Count



FIGURE 13 User Traffic

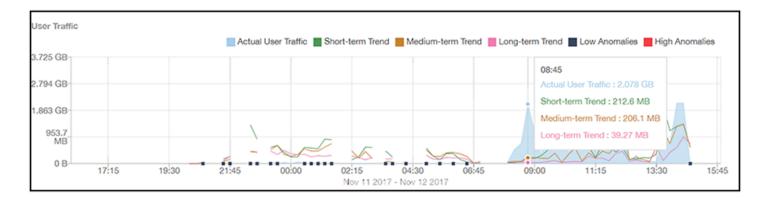


FIGURE 14 Session Count

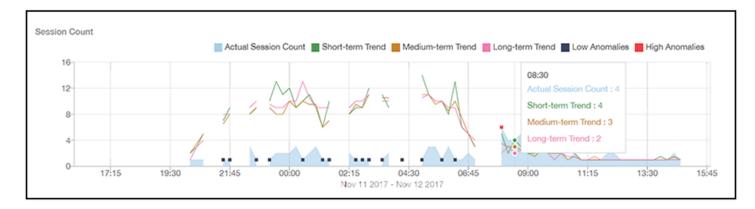


FIGURE 15 Short Session Ratio

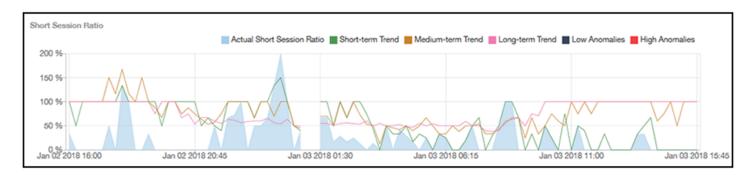
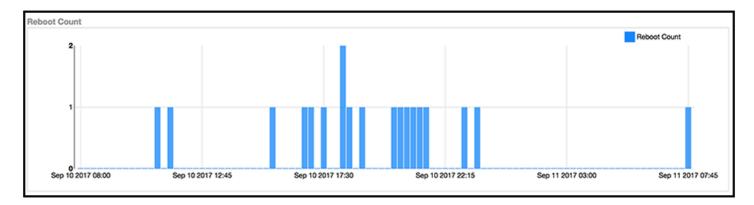


FIGURE 16 Reboot Count



Filters

•	Working With Filters	25
•	AP, SSID and Radio filter	25
•	Date Filter	
•	Download	27
•	Rx+Tx Filter	
•	Time Filter	28
•	AP Filters	29
•	SSID Filter	29
•	Client Filter	30
•	Application Filter	30
•	Alarms Filter	30
•	Events Filter	31
•	Sessions Filter	31
•	Using Saved Filters	31

Working With Filters

Filters are built into the report dashboards so that you can segregate and drill down into the data.

By selecting APs and setting a date range, you can examine specific subsets of data for any AP or group of APs for any time period in any of your wireless networks. For example, if you want to see just the total traffic and client counts for a certain AP on a certain day, you could use the Network Overview report, and simply select that AP and date only.

The same filters are available on most dashboards:

- AP/Radio Filter (on some screens, AP/SSID/Radio filter)
- Date Filter
- Saved Filters. For information on how to use Saved Filters, refer to Using Saved Filters on page 31.

Once you have filtered the data, you can use the **Download** button to download the current dashboard reports in CSV or PDF format.

FIGURE 17 AP/Radio Filter, Date Filter, Saved Filters, and Download button



AP, SSID and Radio filter

Use these filters to generate SCI dashboards.

Custom AP, SSID and Radio Filter: The user can select APs, SSID and Radio (numbered **1** in the figure below) to view and analyze data.

FIGURE 18 Custom AP and Radio Filter

		AP All SSID All Radio 5 GHz 👻
APs		1
Search group Q	A	Search AP Q
占 📄 🚞 All Systems	- 11	170 of 170 APs checked
		AP1 FE:DC:BA:89:67:01
uter → → → → → → → → → → → → → → → → → → →		AP2 FE:DC:BA:89:67:02
t		AP3 FE:DC:BA:89:67:03
€-	+	AP4 FE:DC:BA:89:67:04
4	•	AP5 -
SSID	•	
Radio 5 GHz 2.4 GHz		
		Reset Filter Save Cancel

- The APs area contains a nested list of APs, You need to click on one of the system names and continue to expand the list to drill down to the APs. The hierarchy of the list is: System > Controller > Domain > Zone > AP group > AP. You can select the AP, or/and controller, or/and zone as per your requirement. If you select a particular zone or AP group, the total number of APs is displayed. You can search the APs by AP name, and AP MAC. You can also search by controller, zone, AP group, and even a partial string.
- The SSID dropdown lists contains a nested list of SSID. You can select the SSID and by default all SSID is selected. You can select or deselect all SSID or a particular SSID.

NOTE

SSID option is seen on the nework, WLAN, client and application dashboards.

• Radio select 5 or 2.4 or both GHz.

Follow these steps to:

- 1. Choose the AP, SSID and Radio filters
- 2. Click the Save button to save your selections
- 3. Use the **Reset Filter** button to clear the previous selections.

Date Filter

FIGURE 19 Custom Date Filter

0	7/07/	2016					iii 0	7/08	/2016					Today		
<		Ji	ul 201	16					Au	ıg 20	16			Last 24	Hours	
Мо	Ти	We	Th	Fr	Sa	Su	Мо	Ти	We	Th	Fr	Sa	Su	Last 7 D	ays	2
27	28	29	30	1	2	3	25	26	27	28	20	30	31	Custom	Range	
4	5	6	7	8	9	10	4	2	3	4	5	6	7	Apply	Cancel	
11	12	13	44	15	16	17	8	9	10	44	12	13	44			
18	10	20	21	22	23	2 4	15	16	47	18	10	20	21			
25	26	2 7	28	20	30	31	22	23	2 4	25	26	27	28			
4	2	З	4	5	6	7	20	30	31	4	2	З	4			

Custom Date Select a date range to update the dashboard. You can plot time for a certain period which could be today, last 24 hours, last 7 days, or a custom range (default value). This filter is numbered as **2** in the figure above.

Click on **Apply** to save the specified filters and to update the dashboard.

Download

Use the download option to export the report in either CSV or PDF format.

FIGURE 20 Download option



This filter (numbered **3** in the figure above) is available on most dashboards.

Click on the format required. The report is downloaded, which needs to be opened and saved to the selected drive.

Filters Rx+Tx Filter

Rx+Tx Filter

Use Rx+Tx filters to choose operating ranges in various dashboards.

FIGURE 21 Rx+Tx filter

Rx + Tx ▼
Rx + Tx
Rx
Tx

Select the Rx+Tx (default value), Rx, or Tx operating ranges. This filter can be used in the Network, WLAN and Application dashboards.

Time Filter

Time filter for various dashboards allows you to specify the level of granularity.

The smaller the amount of time you specify, the more detail will appear in the corresponding dashboard.

FIGURE 22 Time filter

15 min 🔻
1 min
15 min
1 hour
1 day

Specify the time frame of 1 minute, 15 minutes (default value), 1 hour or 1 day for applicable dashboards.

AP Filters

AP filters for various dashboards.

FIGURE 23 Top 100 APs

Top 10 APs 🔻
All
Top 10 APs
Top 20 APs
Top 50 APs
Top 100 APs

Specify the APs filter of top 10 (default value), 20, 50, or 100 for applicable dashboards.

FIGURE 24 Last Changed 10 APs

Last Changed 10 APs 🔻
All
Last Changed 10 APs
Last Changed 20 APs
Last Changed 50 APs
Last Changed 100 APs

Specify the changed APs to display; the default is 10.

SSID Filter

SSID filter for WLAN dashboard.

FIGURE 25 SSID filter

Top 10 SSIDs 🔻
All
Top 10 SSIDs
Top 20 SSIDs
Top 50 SSIDs
Top 100 SSIDs

Specify the SSID filter of top 10 (default value), 20, 50, or 100 SSIDs for WLAN traffic and client sections.

Filters Client Filter

Client Filter

Use the Client filter for determining client usage.

FIGURE 26 Client filter



Specify the client filter of top 10 (default value), 20, 50, or 100 for client and trends section in the Client dashboard.

Application Filter

Application filter for the Applications dashboard:

FIGURE 27 Application filter



Specify the application filter of top 10 (default value), 20, 50, or 100 for the Applications dashboard sections of traffic and client reports.

Alarms Filter

Specify the last 10 (default value), 20, 50, or 100 alarms to display on applicable dashboards.

FIGURE 28 Alarms Filter

Last 10 Alarms 💌
All
Last 10 Alarms
Last 20 Alarms
Last 50 Alarms
Last 100 Alarms

Events Filter

Specify the last 1,000 (default value), 2000, or 5,000 events to display on applicable dashboards.

FIGURE 29 Events Filter

Last 1,000 Events 💌
All
Last 1,000 Events
Last 2,000 Events
Last 5,000 Events

Sessions Filter

Specify the last 1,000 (default value), 2000, or 5,000 sessions in applicable dashboards.

FIGURE 30 Sessions Filter

Last 1,000 Sessions 💌
All
Last 1,000 Sessions
Last 2,000 Sessions
Last 5,000 Sessions

Using Saved Filters

SCI allows you to create custom filters and then save them for future use on a per-report basis.

For all dashboards that support filters, you can create any number of customized filters from which to run reports. This can be useful if you want to use a specific filter repeatedly for a specific set of APs, for example.

The bar at the top of a dashboard that support filters is shown below:

FIGURE 31 Radio, Date and Saved Filters and Download bar



The following steps show an example of how to create and save a new filter:

1. Open a dashboard for which you want to create a filter. For example, if you want to create a saved filter for the Network dashboard, the upper portion of that dashboard is shown below.



FIGURE 32 Network Dashboard Example of Creating a Saved Filter - Before Changes

2. Make the desired selections to any filter. In the example figure below, no changes are made to the Radio or Date filters, but in the Top 10 APs by Traffic Volume filters, the Traffic and time-increment drop-downs have been changed to Rx Total and 1 day, respectively.

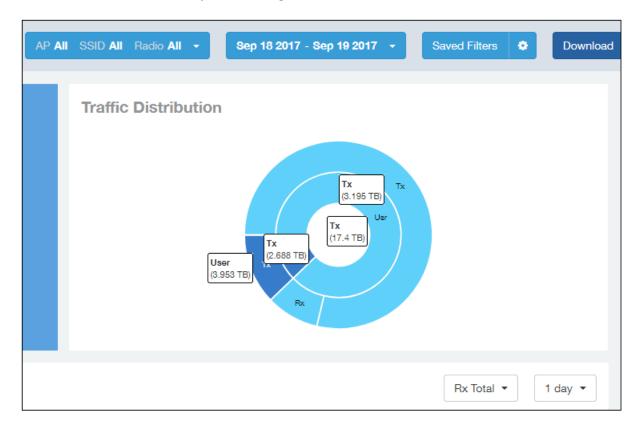
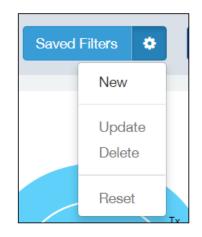


FIGURE 33 Network Dashboard Example of Creating a Saved Filter - After Desired Filter Selections

3. To save these settings so that they can be used again at a later time, click the wheel icon as shown below, and you are presented with a popup.

FIGURE 34 Popup Window to Take Actions on Filters



4. Select New. A popup appears. Enter a name for the filter, as shown in the example below, and click **Create**.

FIGURE 35 Entering a Name for the New Saved Filter

Create Saved Filte	r	×
Name:	Traffic_filter1	
		Create

5. Check that the newly created saved filter is now in effect on this dashboard. For the example shown, the Network Dashboard should now appear as follows, with the selections of Rx Total and 1 day in effect, and the name of the saved filter shown next to the wheel icon:

FIGURE 36 Network Dashboard Example of Creating a Saved Filter - After Saving the Filter



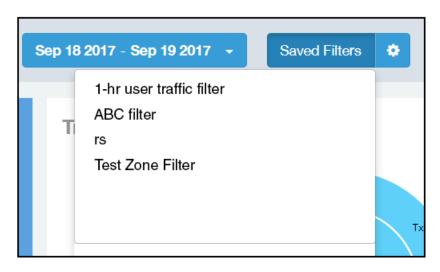
NOTE

A saved filters apply only to the dashboard on which it was created. You cannot import a saved filter on another dashboard.

Actions You Can Take on a Saved Filter

Whenever you go to a dashboard that supports filters, you can click on **Saved Filters** in the Radio, Date and Saved Filters and Download bar. If there are any saved filters, they will display, as shown in the following example figure:

FIGURE 37 Example List of Saved Filters



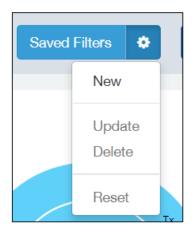
You can click on any of the saved filters and generate a report.

NOTE

The "Saved Filters" text will be replaced by the name of any filter that you open. But you can still click in the same area, and the list of saved filters is displayed.

If you click on the wheel icon, the following possible actions are allowed on a filter:

FIGURE 38 Actions You can Take on Filters



Descriptions of each action are:

• New: Allows you to create a new saved filter, as shown in the example earlier in this section.

- Update: Allows you to make changes to an existing saved filter, including changing the filter name if desired. Make any changes you wish to the filter selections, then select Update. A popup appears next, where you click **Update** again to save your changes.
- Delete: Deletes an existing saved filter.
- Reset: Displays default settings for all filters. To return to a saved filter, simply click on **Saved Filters** again in the Radio, Date and Saved Filters and Download bar.

Network Report Dashboard

•	Network Report	37
•	Network - Overview	38
	Network - Traffic Distribution	
•	Network - Top 10 APs by Traffic Volume	
•	Network - Top 10 APs by Client Count	
•	Network - Top APs by Traffic Volume (Table)	
•	Network - Top APs by Client Count (table)	
•	Network - Traffic Trend	
	Network - Traffic Over Time	

Network Report

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

The following figure shows only the upper portion of the Network report that appears when you click **Network** on the navigation bar.

FIGURE 39 Network Report (upper portion)



The Network report consists of eight sections, and they are described in the table below. Figures showing each of these sections appear later.

1	Overview	Contains the total traffic and the total clients on the network. It also contains the received and transmitted traffic between them.
2	Traffic Distribution	Contains the distribution of traffic in terms of size.

3	Top 10 APs by Traffic Volume	A pie chart and graph contain the top APs with the largest traffic volume in the network, along with the received and transmitted traffic volumes.
4	Top 10 APs by Client Count	A pie chart and graph contain the top APs by client count in the network, along with the received and transmitted traffic volumes.
5	Top APs by Traffic	A table contains the top APs with the largest traffic volume in the network.
6	Top APs by Client	A table contains the top APs by client count in the network.
7	Traffic Trend	A graph displays the traffic by usage and radio, and also the corresponding average traffic rate.
8	Traffic Over Time	A table tracks the traffic on the network based on time and other components.

Network - Overview

The Network Overview section of the Network report provides a general overview of the entire network.

The Network Overview section displays the following, based on your selection of AP, SSID and Radio and Date Range filters:

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

FIGURE 40 Network - Overview

Overview			
2		тв, 154.7 Маря Тв, 1.992 Glaps	5
Total APs		Avg Rate	Total Clients
4260	22.84 тв	2.143 Gbps	179.6 k

Network - Traffic Distribution

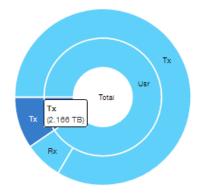
The Traffic Distribution pie chart of the Network report displays the distribution of traffic types.

Use this chart to display management traffic vs. 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 41 Network - Traffic Distribution

Traffic Distribution



Network - Top 10 APs by Traffic Volume

The Top 10 APs by Traffic Volume chart and graph of the Network report display the highest-traffic APs.

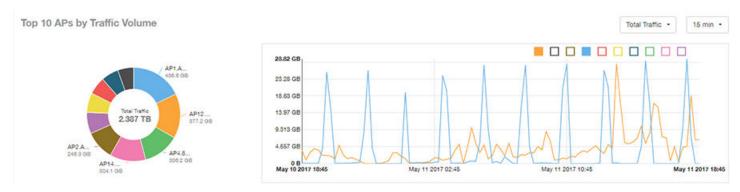
Use the drop-down menus to specify the traffic type (Tx, Rx, or Tx+Rx) and the time granularity. Click any of the colored squares to toggle display of the AP in the line graph.

NOTE

The **Rx+Tx** drop-down menu applies to both the pie chart and the line graph, but the time granularity applies to the line graph only. This applies to all sections in all reports that appear in this format (pie chart + line graph with Rx/Tx + time granularity menus).

rection rop for a by chemic counc

FIGURE 42 Network - Top 10 APs by Traffic Volume



NOTE

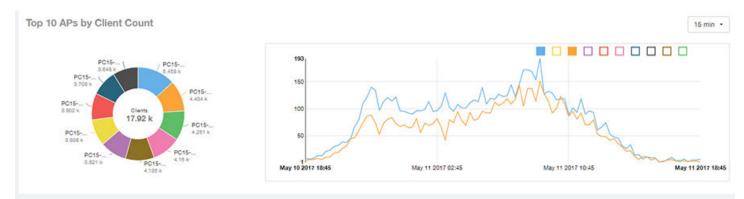
If you hover over the line graph, a pop-up appears containing the selected AP details.

Network - Top 10 APs by Client Count

The Top 10 APs by Client Count pie chart and graph display the APs with the most clients on your network.

Use the drop-down menu to specify the time granularity of 15 minutes, 1 hour or 1 day. If you hover over the line graph a pop-up appears containing the details on the selected data points. Click any of the colored squares to toggle display of the AP in the line graph.

FIGURE 43 Network - Top 10 APs by Client Count



Network - Top APs by Traffic Volume (Table)

The Top APs by Traffic table lists the APs with the highest traffic volume in the network.

Use this table to view a list the top APs with the highest traffic volume, sorted according to the selected columns. Click the gear

icon 🔯 to select which columns to display, or click any column heading to sort by that column.

You can also select whether to display the top 10, 20, 50, or 100 APs by traffic volume from the Top APs filter. The number of rows per page can be defined using the **Rows per page** option in the table settings drop down list.

FIGURE 44 Network - Top APs by Traffic

Index	AP Name	AP IP Address	Controller Name	Fix Total		Tx Total	Total	Traffic	Clients	ł
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	731.1 M	B 435.9 G	8	436.6 GB		53	
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName2	10.84 G8	366.3 (8	377.2 GB		119	
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName3	20.73 G8	285.5 0	8	306.2 GB		42	
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName4	7.841 0	8 296.5 0	8	304.1 GB		82	
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName5	8.963 0	8 237.3 0	8	246.3 GB		91	
6	Your_Co_APName6	10.x.y.6	Your_Co_CTName6	4.222 (8	174,5 GB		178.7 GB	255	
7	Your_Co_APName7	10.x.y.7	Your_Co_CTName7	4.47 (8	161.5 GB		168 GB	28	
8	Your_Co_APName8	10.x.y.8	Your_Co-CTName8	10.01 0	8	138.7 G8		148.7 GB	67	
9	Your_Co_APName9	10.x.y.9	Your_Co_CTName9	3.707 (8	142.7 08		146.4 GB	39	
10	Your_Co_APName10	10.x.y.10	Your_Co_CTName10	2.90	8	131.3 GB		134.2 GB	120	

Network - Top APs by Client Count (table)

The Top APs by Client Count table of the Network report displays the APs with the most clients in the network.

Click the gear icon to view the list of table columns, or click any column heading to sort by that column. You can also select the top 10, 20, 50, or 100 APs by client count. The number of rows in a page is defined by the Rows per Page list in the table settings drop-down list.

FIGURE 45 Network - Top APs by Client

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 G
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName2	4.434 k	323.9 MB	1.171 GB	1,487 G
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName3	4.251 k	1.528 GB	969.4 MB	2.474 G
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName4	4.15 k	190.3 MB	1.961 GB	2.147 G
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName5	4,135 k	363.1 MB	4,182 GB	4.536 G
6	Your_Co_APName6	10.x.y.6	Your_Co_CTName6	3.821 k	289,3 MB	828.4 MB	1.092 G
7	Your_Co_APName7	10.x.y.7	Your_Co_CTName7	3.808 k	569.6 MB	13.12 G8	13.68 G8
8	Your_Co_APName8	10.x.y.8	Your_Co-CTName8	3.802 k	254.3 MB	1.049 GB	1.297 G
9	Your_Co_APName9	10.x.y.9	Your_Co_CTName9	3.708 k	169.9 MB	583.9 MB	753.8 M
10	Your_Co_APName10	10.x.y.10	Your_Co_CTName10	3.648 k	156.9 MB	1.85 G8	2.003 G

Network - Traffic Trend

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

If you hover over the line graph, a pop-up appears 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, - namely by user, total received traffic, total transmitted traffic, the total received and transmitted traffic, and the management traffic. You can also select a date range to view this date on the line graph. You can also specify the time granularity increment.

Network Report Dashboard Network - Traffic Over Time

Traffic by Radio: You can select the traffic by radio details from the check boxes listed in the legend on top of the graph - namely by 5GHz, 2.4GHz, or/and view the total traffic by radio details. You can also select a date range to view this date on the line graph. This also applies to the corresponding average traffic rate graphs.

FIGURE 46 Network - Traffic Trend



Network - Traffic Over Time

The Traffic Over Time table of the Network report allows you to compare traffic over multiple time periods. Click the gear icon to select/deselect columns to display, or click any column heading to sort by that column.

Traffic Over Time May 10 2017 - May 11 2017 -15 min • 2.4 GHz 5 GHz Time Period Rx Total Tx Total Total Traffic Clients ¢ May 10 2017 18:45 - 18:59 28.65 GB 11.67 GB 151.2 GB 162.9 GB 9.969 k 134.2 GB May 10 2017 19:00 - 19:14 146 GB 10.22 k 119.6 GB 26.39 GB 11 17 GB 134 8 GB May 10 2017 19:15 - 19:29 154.2 GB 10.41 k 126.1 GB 28.09 GB 142.9 GB May 10 2017 19:30 - 19:44 140.5 GB 27.97 GB 155.1 GB 168.4 GB 10.69 k May 10 2017 19:45 - 19:59 171.8 GB 10.78 k 141.8 GB 30.01 GB 12.89 GB 158.9 GB May 10 2017 20:00 - 20:14 10.76 k 142.3 GB 31.95 GB 161.7 GB 174.2 GB May 10 2017 20:15 - 20:29 11.15 k May 10 2017 20:30 - 20:44 11.67 k 34.87 GB 12.3 GB 174.4 GB 186.7 GB 151.8 GB May 10 2017 20:45 - 20:59 134.5 GB 33.98 GB 168.5 GB 12.19 k 156.7 GB 12.37 k May 10 2017 21:00 - 21:14 145.1 GB 33.59 GB 11.84 GB 166.8 GB 178.7 GB 🔹 1 🔻 of 10 🕨

FIGURE 47 Network - Traffic Over Time

APs & Controllers Report Dashboard

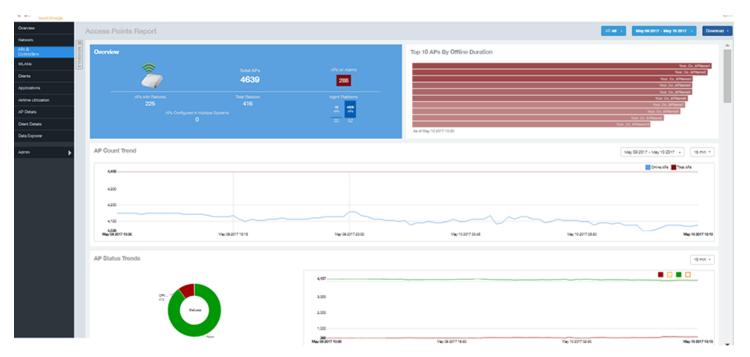
•	APs & Controllers Report	43
•	APs & Controllers Report APs & Controllers - Overview	45
•	APs & Controllers - Top 10 APs by Offline Duration	46
•	APs & Controllers - Count Trend	46
•	APs & Controllers - Status Trends	47
•	APs & Controllers - Top 10 AP Models	47
•	APs & Controllers - Top 10 AP Software Versions	
•	APs & Controllers - Top 10 AP Reboot Reasons	
•	APs & Controllers - Top 10 APs by Reboot Counts	49
•	APs & Controllers - Top 10 AP Alarm Types	49
•	APs & Controllers - Top AP Models (table)	50
•	APs & Controllers - Top AP Software Versions (table)	51
•	APs & Controllers - Top APs by Offline Duration (table)	51
•	APs & Controllers - Top APs by Reboot Count	52
•	APs & Controllers - APs Configured in Multiple Systems	
•	APs & Controllers - AP Details for Online/Offline Status	53
•	APs & Controllers - AP Details for Other Statuses	54
•	APs & Controllers - Resource Utilization	55
•	APs & Controllers - License Utilization	55
•	KRACK Assessment	56

APs & Controllers Report

The APs & Controllers report provides details on AP inventory, AP reboots, AP software version, AP models and AP Alarms.

The following figure shows only the upper portion of the Access Points dashboard that appears when you click **APs & Controllers** on the navigation bar.





The APs & Controllers report consists of 18 sections, which are listed in the table below. Figures showing each of these sections appear later.

NOTE

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

1	Overview	Contains an overview of the AP inventory – how many APs are connected, how many reboots, and so on.
2	Top 10 APs By Offline Duration (graph)	Contains the APs that have been disconnected over a specified duration. The APs are ordered from longest offline duration to shortest offline duration.
3	AP Count Trend	A pie chart and graph show the number of available APs on the network based on the total number of APs and its online status.
4	AP Status Trends	A line chart shows the trend of various AP statuses such as online, offline, provisioned, discovery and so on.
5	Top 10 AP Models	A pie chart and graph contain the top APs models by count in the network, along with the trend of APs models over a specified time frame.
6	Top 10 AP Software Versions	A pie chart and graph contain the top APs software versions by AP count in the network, along with the trend of APs software versions over a specified time frame.
7	Top 10 AP Reboot Reasons	A pie chart and graph list the most common reasons why the APs in your network have restarted over a specified time frame.
8	Top 10 APs by Reboot Counts	A pie chart and graph contain the top APs that restarted, along with the APs based on the number of restart over a specified time frame.
9	Top 10 AP Alarm Types	A pie chart and graph contain the Top 10 Alarm types that have been generated, along with number of occurrences generated over a specified time frame.
10	Top AP Models	A table lists the distribution of AP models in the network.
11	Top AP Software Versions	A table lists the top AP software versions.
12	Top APs by Offline Duration (table)	A table lists the APs that are offline over a specified duration. The APs are ordered from longest offline duration to shortest offline duration.

APs & Controllers - Overview

13	Top APs by Reboot Count	A table lists the APs that have restarted over a specified time.
14	APs Configured in Multiple Systems	A table lists APs that have been associated with multiple controllers.
15	AP Details for Online/Offline Status	A table lists the APs on the network based on its online or offline status with AP name, IP address, location, model, controller and status.
16	AP Details for Other Statuses	A table lists the APs on the network based on AP name, IP address, location, model, controller and status
17	Resource Utilization	A table shows the CPU, memory and disk utilization percentages for each controller in your system.
18	License Utilization	A table shows the licenses available and consumed for the APs for each system.
19	KRACK Assessment	A table shows the KRACK vulnerability status of all Access Points that are filtered to be displayed.

APs & Controllers - Overview

The APs & Controllers overview section provides a general overview of the APs on the network.

This overview section displays the following, based on your selection of AP, Radio and Date Range filters:

- Total APs
- APs with alarms
- APs with reboots
- Total reboots
- Management Platforms
- APs configured in multiple controllers

FIGURE 49 APs & Controllers - Overview

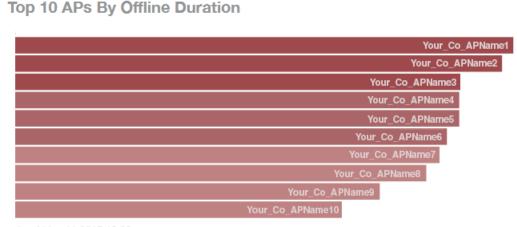


APs & Controllers - Top 10 APs by Offline Duration

The Top 10 APs by Offline Duration chart of the APs & Controllers report displays the top 10 APs in the network that have been disconnected for the longest duration.

Use the drop-down menu to specify the time granularity. If you hover over the line graph, a pop-up appears containing the details on the selected data points.

FIGURE 50 APs & Controllers - Top 10 APs by Offline Duration



As of May 11 2017 19:00

APs & Controllers - Count Trend

The Count Trend graph of the APs & Controllers report depicts how many access points in your network are being utilized over time.

To show access points being used over certain time periods, use the drop-down menu to specify the time granularity. If you hover over the line graph and pie chart, a pop-up appears containing the details on the selected data points. Click any of the colored squares to toggle the display of the AP in the line graph.

FIGURE 51 APs & Controllers - Count Trend

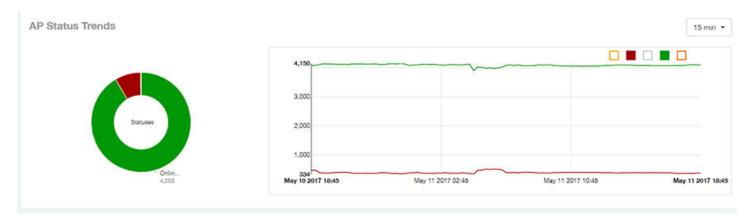


APs & Controllers - Status Trends

The Status Trends pie chart and graph of the APs & Controllers report 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 hover over the line graph and pie chart, a pop-up appears containing the details on the selected data points. Click any of the colored squares to toggle display of the AP in the line graph.

FIGURE 52 APs & Controllers - Status Trends



APs & Controllers - Top 10 AP Models

The Top 10 AP Models pie chart and line graph of the APs & Controllers report display the model type that is most often used in your network.

Use the drop-down menu to specify the time granularity. If you hover over the line graph and pie chart, a pop-up appears containing the details on the selected data points. Click any of the colored squares to toggle display of the AP in the line graph.

FIGURE 53 APs & Controllers - Top 10 AP Models



APs & Controllers - Top 10 AP Software Versions

The Top 10 AP Software Versions pie chart and graph of the APs & Controllers report display the top 10 APs based on which software versions are most frequently used in your network.

Use the drop-down menu to specify the time granularity. If you hover over the line graph or the pie chart, a pop-up appears containing the details on the selected data points. Click any of the colored squares to toggle display of the AP in the line graph.

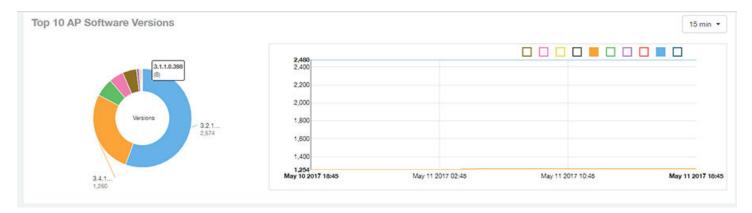


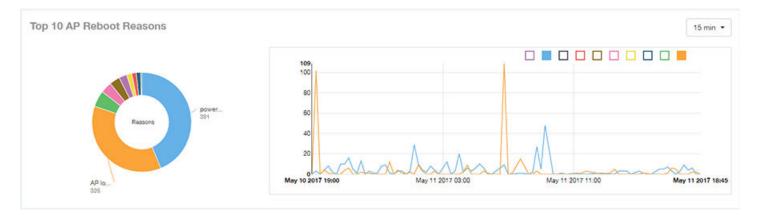
FIGURE 54 APs & Controllers - Top 10 AP Software Versions

APs & Controllers - Top 10 AP Reboot Reasons

The Top 10 AP Reboot Reasons pie chart and graph of the APs & Controllers report display the 10 most common reasons why APs in your network have rebooted.

Use the drop-down menu to specify the time granularity. If you hover over the line graph and pie chart, a pop-up appears containing the details on the selected data points. Click any of the colored squares to toggle display of the AP in the line graph.

FIGURE 55 APs & Controllers - Top 10 AP Reboot Reasons

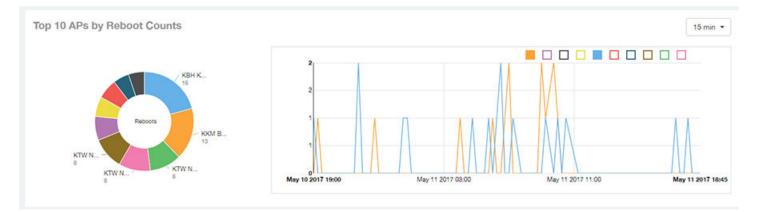


APs & Controllers - Top 10 APs by Reboot Counts

The Top 10 APs by Reboot Counts pie chart and line graph of the APs & Controllers report display the top 10 APs in your network that have rebooted most frequently.

Use the drop-down menu to specify the time granularity. If you hover over the line and pie graph, a pop-up appears containing the details on the selected data points. Click any of the colored squares to toggle display of the AP in the line graph.

FIGURE 56 APs & Controllers - Top 10 APs by Reboot Counts

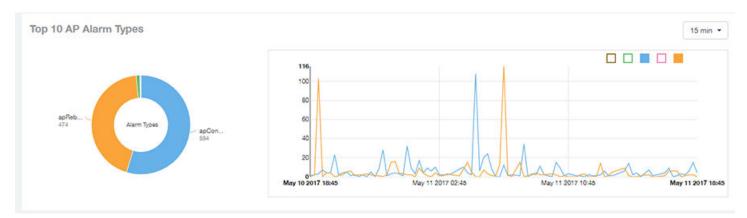


APs & Controllers - Top 10 AP Alarm Types

The Top 10 AP Alarm Types pie chart and line graph of the APs & Controllers report display the 10 alarm types most that have most frequently occurred to access points in your network.

Use the drop-down menu to specify the time granularity. If you hover over the line graph, a pop-up appears containing the details on the selected data points. Click any of the colored squares to toggle display of the AP in the line graph.

FIGURE 57 APs & Controllers - Top 10 AP Alarm Types



APs & Controllers - Top AP Models (table)

The Top AP Models table of the APs & Controllers report displays the model type being used most often by the APs in your network.

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

FIGURE 58 APs & Controllers - Top AP Models	
•	

op 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 %
		r of 1 🕨	

APs & Controllers - Top AP Software Versions (table)

The Top AP Software Versions table of the APs & Controllers report displays the AP software versions most frequently used in your network and the number of APs using each version.

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

AP Software Versions			Тор	10 Versio
Index	AP Version	Number of APs w/ the Version	96 of APs w/ the Version	
1	3.2.1.0.650	2,574	65.35 %	
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	8	0.3 W
9	3.1.1.0.398	8		0.17 9
10	Unknown	7		0.15 %

FIGURE 59 APs & Controllers - Top AP Software Versions

APs & Controllers - Top APs by Offline Duration (table)

The Top APs by Offline Duration table of the APs & Controllers report displays the top APs based on which ones have been offline for the longest duration, with details of AP name, IP address, location, model, controllers and duration in a tabular format.

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

FIGURE 60 APs & Controllers - Top APs by Offline Duration

APs by Offlin	o porotron					Top 10 A
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	ty 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_APLoon3	ZF-T300	Your_Co_Controller2	1y 7mo
9	Your_Co_AccessPoint4	172.16.z.4	Your_Co_APLocn4	ZF-P300	Your_Co_Controller2	ty 5mo
10	Your_Co_AccessPoint5	172.16.z.5	Your_Co_APLocn5	ZF-T610	Your_Co_Controller2	1y 3mo

APs & Controllers - Top APs by Reboot Count

The Top AP by Reboot Count table of the APs & Controllers report displays the APs that have rebooted the most times, and includes AP name, IP address, location, number of reboots, last reboot date and reason.

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

FIGURE 61 APs & Controllers - Top AP by Reboot Count

APs by Rebo	ot 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

APs & Controllers - APs Configured in Multiple Systems

The APs Configured in Multiple Systems table of the APs & Controllers report shows you information about APs that have been associated with more than one controller.

In the Controller Name field, 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 list of columns to display. Click any column heading to sort by that value. You can also select the top 10 (default value), 20, 50, or 100 APs to display, or display all APs. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 62 APs & Controllers - APs Configured in Multiple Systems

onfigured in M	ultiple Systems		Last Changed 10 APs ·		
AP Name	Controller Name	Controller Count	Last Status	Last Controller Name	¢
our_Co_APName1	Your_Co_CTName1, Your	2	online	Your_Co_CTName1	
our_Co_APName2	Your_Co_CTName5, Your	2	online	Your_Co_CTName5	
our_Co_APName3	Your_Co_CTName4, Your	2	online	Your_Co_CTName4	

APs & Controllers - AP Details for Online/Offline Status

The AP Details for Online/Offline Status table of the APs & Controllers 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 list of columns to display. The table is sorted on the top AP model by default. Click any column heading to sort by that value. You can also select the top 10 (default value), 20, 50, or 100 clients to display, or display all AP models. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.

FIGURE 63 APs & Controllers - AP Details for Online/Offline Status

Details for C	Inline/Offline Status						Last Changed 10 APs
Index	AP Name	AP IP Address	AP Location	AP Model	Controller Name	Last Status	Last Status Change
1	Your_Co_APName1	10.x.y.1	Your_Co_APsile1	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

APs & Controllers - AP Details for Other Statuses

The AP Details for Other Statuses table of the APs & Controllers report displays the details for APs that are currently in a status other than online or offline.

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

FIGURE 64 APs & Controllers - AP Details for Other Statuses

letails for Oti	her Statuses					Last Changed 1
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	2F-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

APs & Controllers - Resource Utilization

The Resource Utilization table of the APs & Controllers report displays the CPU, memory and disk utilization percentages for each controller in your system.

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

FIGURE 65 APs & Controllers - 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 %

APs & Controllers - License Utilization

The License Utilization table of the APs & Controllers report displays the number of available and consumed licenses for the APs for each system.

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

FIGURE 66 APs & Controllers - License Utilization

System Name	APs Managed	APs Up	APs Down	AP License Total	License Consumed	License Available	License Utilization
CI-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 %
CI_PUSH_XML-2	1	1	0	5	1	4	20 %

KRACK Assessment

The KRACK Assessment table of the APs & Controllers report shows the KRACK vulnerability status of all Access Points that are filtered to be displayed.

The following is an example of the Krack Assessment section of the Access Points dashboard.

FIGURE 67 KRACK Assessment Example section

KRACK Assessment	0.19 % (8/4249) of APs in all systematics	erns 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 Access points. Refer to the following site for information and instructions: https://support.ruckuswireless.com/krack-ruckus-wireless-support-resource-center

WLANs Report Dashboard

•	WLANs Report	57
	WLANs - Overview	
•	WLANs - SSID Changes Over Time	59
	WLANs -Top Ten SSIDs by Traffic	
	WLANs -Top Ten SSIDs by Client Count	
	WLANs -Active SSIDs Trend	
	WLANs -Top SSIDs by Traffic (table)	
•	WLANs -Top SSIDs by Client Count (table)	

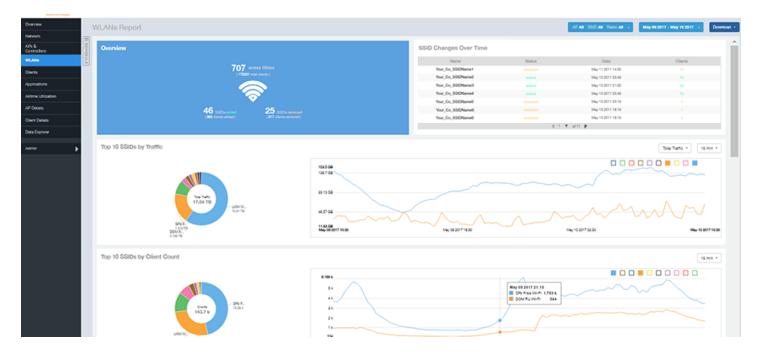
WLANs Report

The Wireless LANs report contains information about the SSIDs added as well as which are active or have been removed.

The report also includes details about SSID changes over time, SSIDs by received and transmitted traffic, client count over a time range and trend of the SSIDs based on traffic count and volume. The WLANs report allows you to filter the information based on APs, SSID and Radio, day and date and Rx+Tx filters. You can also customize the table reports be selecting the list of available components for each category.

The following figure shows only the upper portion of the WLANs dashboard that appears when you click **WLANs** on the navigation bar.

FIGURE 68 WLANs Report (upper portion)



The WLANs report consists of seven sections, which are listed in the table below. Figures showing each of these sections appear later.

1	Overview	This report section contains the total number of active SSIDs, added and removed.
2	SSID Changes Over Time	A chart contains the SSID status, its last modified date and the number of clients associated to the SSID.
3	Top 10 SSIDs by Traffic	A pie chart and graph contain the top 10 SSIDs by traffic volume for received and transmitted traffic.
4	Top 10 SSID by Client Count	A pie chart and graph contain the top 10 SSIDs to show the most congested networks in terms of client count.
5	Active SSIDs Trends	The active SSID trend displays the traffic by SSID count and traffic volume.
6	Top SSIDs by Traffic (table)	This tabular report contains the top SSIDs with the largest traffic volume in the network as per the selected components.
7	Top SSIDs by Client (table)	The tabular report contains the top SSIDs by client count in the network as per the selected components.

WLANs - Overview

Thie Overview section of the WLANs report shows the total number of active SSIDs, and the number of added and removed SSIDs over the selected period.

FIGURE 69 WLANs - Overview



WLANs - SSID Changes Over Time

The SSID Changes Over Time display of the WLANs report shows the most recent SSID changes.

FIGURE 70 WLANs - SSID Changes Over Time

SSID Changes Ove	r 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
	1	🔻 of 14 🕨	

WLANs -Top Ten SSIDs by Traffic

Use the Top 10 SSIDs by Traffic 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.

Click any of the colored squares to toggle display of the corresponding SSID. You can use the Total Traffic drop-down menu to choose whether to display transmitted data only, received data only, or total traffic.



FIGURE 71 WLANs - Top Ten SSIDs by Traffic

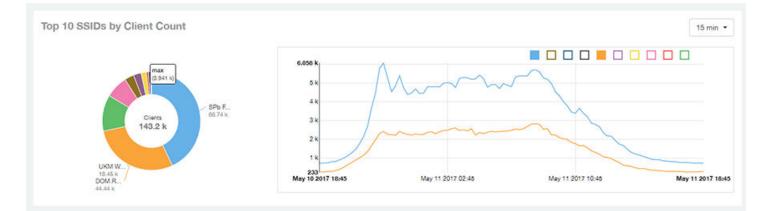
WLANs -Top Ten SSIDs by Client Count

Use the Top 10 SSIDs by Client Count pie chart and graph of the WLANs report to view which wireless networks are most congested in terms of client count, and to compare client counts over different time periods.

Click any of the colored squares to toggle the display of the corresponding SSID.

If you hover over the line graph a pop-up appears containing the selected SSID names and client counts at the chosen data point.

FIGURE 72 WLANs - Top Ten SSIDs by Client Count



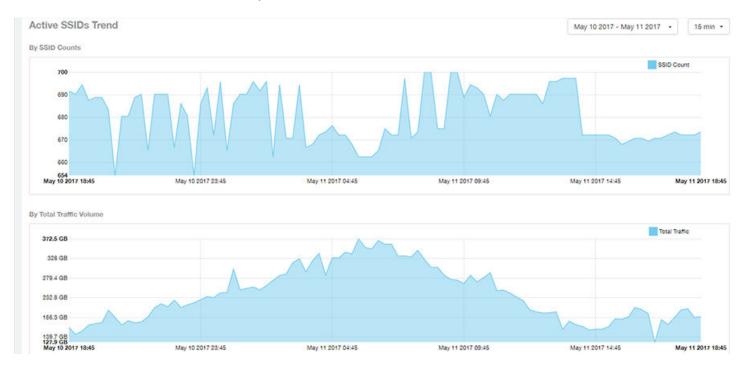
WLANs -Active SSIDs Trend

The Active SSIDs Trend graphs of the WLANs report contains two graphs: total number of SSIDs over time, and total traffic volume over time.

These graphs allow you to quickly view how many WLANs are active and what the total traffic volume is over time.

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

FIGURE 73 WLANs - Active SSIDs Trend Graphs



WLANs -Top SSIDs by Traffic (table)

The Top SSIDs by Traffic table of the WLANs report lists the top 10, 20, 50 or 100 SSIDs in the network by traffic volume.

You can sort the table by Total Traffic, Clients, AP count, or alphabetically by SSID name. Additionally, you can customize the table

by clicking the gear icon **P** and selecting from the list of columns. You can configure the number of rows per a page using the **Rows per Page** option in the table settings drop down menu.

You can also select whether to display only the top 10 (default value), 20, 50, or 100 SSIDs by traffic volume, or list all SSIDs.

FIGURE 74 WLANs - Top SSIDs by Traffic

SSIDs by Traff	nc			These	SSIDs consi	ume 73.15 % (16.71 Ti	B) of the total traffic (22.84 TB).	Top 10 SS	SIDs
Index	SSID Name	Rx Total		Tx Total	Te	otal Traffic	Clients	APs	
1	Your_Co_SSIDName1	584.3 GB	8.678 TE		9.248 TB	3	18.45 k	974	
2	Your_Co_SSIDName2	151.3	GB C	3.437 TB	(3.585 TB	44,44 k	1.105 k	
3	Your_Co_SSIDName3	157	GB C	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	1	337.6 GB	1	959	
7	Your_Co_SSIDName7	25.13	G8	299.3 GB	-	324.6 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	

WLANs -Top SSIDs by Client Count (table)

The Top SSIDs by Client Count table of the WLANs report lists the top SSIDs by client count.

You can sort the table by Total Traffic, Clients, AP count, or alphabetically by SSID name. Additionally, you can customize the table

by clicking the gear icon and selecting from the list of columns. You can configure the number of rows per a page using the **Rows per Page** option in the table settings drop down menu.

You can also select whether to display only the top 10 (default value), 20, 50, or 100 SSIDs by client count, or list all SSIDs.

FIGURE 75 WLANs - Top SSIDs by Client Count

SSIDs by Clie	ent Count		Th	ese SSIDs con	isume 69.74 % (15.	93 TB) of the to	otal traffic (22.84 TB).	Top 10 SS	Ds •
Index	SSID Name	Clients	Rx Total		Tx Total	Total	Traffic	APs	4
1	Your Co_SSIDName1	66.74 k	157	в с	1.301 TB		1.455 TB	961	
2	Your Co_SSIDName2	44.44 k	151.3	18	3.437 TB	(3.585 TB	1.105 k	
3	Your Co_SSIDName3	18.45 k	584.3 GB	8.678 T	в	9.248 TB	3	974	
4	Your Co_SSIDName4	11.44 k	61.92	8	480.3 GB		542.3 GB	213	
5	Your Co_SSIDName5	4.754 k	20.05	в	259.9 GB	(279.9 GB	280	
6	Your Co_SSIDName6	3.941 k	26.94	8	278.2 GB		305.2 GB	50	
7	Your Co_SSIDName7	2.656 k	9.192	18	100.3 GB	ſ.	109.5 GB	170	
8	Your Co_SSIDName8	1.18 k	2.87	B	34.78 GB	1	37.65 GB	5	
9	Your Co_SSIDName9	1.096 k	23.43	8	374.6 GB		398.2 GB	26	
10	Your Co_SSIDName10	344	621.71	IB	8.391 GB	-	8.998 GB	14	

Clients Report Dashboard

•	Clients Report	63
•	Clients - Overview	64
	Clients - Top 10 Unique Clients by Traffic	65
	Clients - Clients Details	
	Clients - Unique Clients Trends Over Time (graph)	
	Clients - Unique Clients Trend Over Time (Table)	
	Clients - Top 10 OS by Client Count	
	Clients - Top 10 Manufacturers by Client Count	
	Clients - Top 10 Authentication Methods by Client Count	

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.

The following figure shows only the upper portion of the Clients report that appears when you click **Clients** on the navigation bar.

FIGURE 76 Clients Report (upper portion)

Overview	(Clients Report	AP AR 500 AR Flads AR - May 992917 - May 992917 - Download -
Network			
APs & Controlls is	S-C×LO	Overview	Top 10 Unique Clients by Traffic
VILANE	Ē.		WADBON DOLS GR
Climits		States Contraction of the second seco	Uniterant, PaulPathold 91 (55.3-56) android disart 69270166 (55.7-56)
Appleations			Binkerwen, android Se [*] auccid00c0002 (1931.8 600) Name got (103.7 600)
Artime Utilization			Coloradore, and out-27 1164/21 0/218 (2013) 648 Web-06/202200 (87.36.68)
AP Details		uw late to the Days 179.3 k	Underwark, Windows Phone (8) 38 GB 1-Metrola-draub (80.27 GB) - 444 W
Orient Details			Unner-(85.86.68) Average (927.8 Mil)
Data Explorer			- and the same
Aanan 🕨			These clients consume 6.56 % (1.65 TB) of all user traffic (21.57 TB).

The Clients report consists of eight sections, which are listed in the table below. Figures showing each of these sections appear later.

1	Overview	Contains the total traffic and the total clients on the network. It also contains the received and transmitted traffic between them.
2	Top 10 Unique Clients by traffic	Contains the list of top 10 clients in terms of size of traffic.
3	Top 10 OS by Client Count	Contains information about the 10 operating systems being used the most by the clients in your network.
4	Top 10 Manufacturers by Client Count	Contains information about the 10 manufacturers of wireless equipment most represented in your network.

5	Top 10 Authentication Methods by Client Count	Contains information about the top 10 methods most commonly used in your system to authenticate users.
6	Client details	Contains the client information and display the quantity of traffic consumed by the listed clients.
7	Unique Clients Trend over time (graph)	Displays the unique clients trend over time for client count and for traffic.
8	Unique Clients Trend over time (table)	Lists the unique clients trend over time.

Clients - Overview

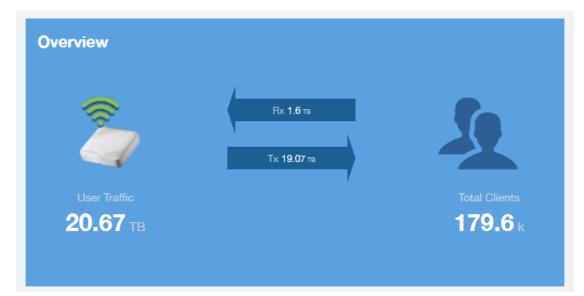
The Overview section of the Clients report provides information about the total traffic, both received and transmitted, and the total number of clients over the selected time period.

The Overview section contains the following:

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

This is based on your selection of AP/Radio and Date Range filters.

FIGURE 77 Overview



Clients - Top 10 Unique Clients by Traffic

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

FIGURE 78 Clients - Top 10 Unique Clients by Traffic

	er Traffic 🔻
iPad-Elvira (263.5 GB) 861000421 (155.5 GB) 861000359 (142.9 GB) Unknown, iPad-3 (137.1 GB) Unknown, android-e119d267344cd404 (125.8 GB)	N (423.5 GB)
861000421 (155.5 CB) 861000359 (142.9 CB) Unknown, iPad-3 (137.1 CB) Unknown, android-e119d267344cd404 (125.8 CB)	
861000359 (142.9 GB) Unknown, iPad-3 (137.1 GB) Unknown, android-e119d267344cd404 (125.8 GB)	
Unknown, iPad-3 (137.1 GB) Unknown, android-e119d267344cd404 (125.8 GB)	
Unknown, android-e119d267344cd404 (125.8 CB)	
Unknown (123.2 GB)	
861000787 (116.4 GB)	
Unknown, android-dfeae14f97701f56 (116.2 GB)	
FULL (109.3 GB)	
Average (120.7 MB)	

Clients - 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 list of components from the table. By default, the table is sorted by total traffic (Rx + Tx). Click on a column heading to sort by that value. You can also 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 79 Clients - Clients details

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 G	
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 GE	8
3	Your_Co_HostName3	FE:DC:BA:89:67:03	10.x.y.3	Your_Co_HostName3	9		3.958 GB		151.5 GB		155.6 GB
4	Your_Co_HostName4	FE:DC:BA:89:67:04	10.x.y.4	Your_Co_UserName4	12		3.502 G/B	-	139.4 GB		142.9 GE
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 GE
6	Your_Co_Hostame6	FE:DC:BA:89:67:06	10.x.y.6	Your_Co_Userame6	41		1.395 GB		124.4 GB		125.8 GE
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 G8
8	Your_Co_HostName8	FE:DC:BA:89:67:08	10.x.y.8	Your_Co_UserName8	13	6	4.239 GB		112.2 GB		116.4 GE
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 GE
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 GE

Clients - Unique Clients Trends Over Time (graph)

Use the Unique Clients Trend graphs of the Clients report to view a breakdown of unique clients by radio type over time.

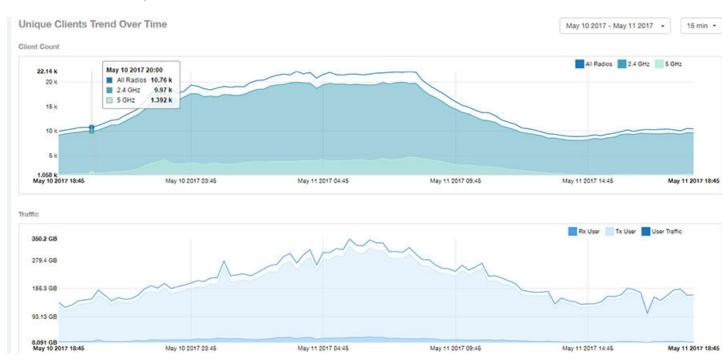


FIGURE 80 Clients - Unique Clients Trend Over Time Chart

Clients - Unique Clients Trend Over Time (Table)

The Unique Clients Trend Over Time table of the Clients report displays the total numbers of unique clients over the specified time intervals, as well as unique client count per radio, and client traffic (Tx, Rx, total) for a given time period.

The unique clients trend can be used to identify which time periods have the highest number of new clients connecting to the

networks, or to compare transmit/receive traffic over different time periods throughout the day. Click the gear icon to select the list of columns to display. The table is sorted on the total traffic by default. Click any column heading to sort by that value. You can also select the top 10 (default value), 20, 50, or 100 clients to display, or display all clients. The number of rows per page is defined by the **Rows per Page** option in the table settings menu.



FIGURE 81 Clients - Unique Clients Trend Over Time Table

Clients - Top 10 OS by Client Count

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

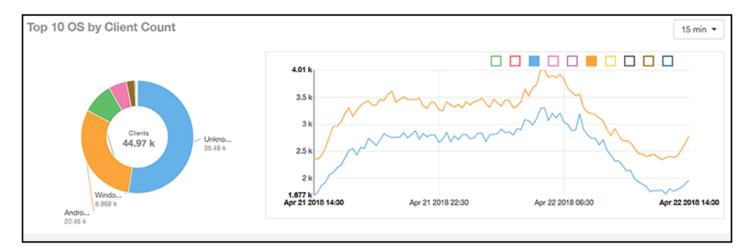
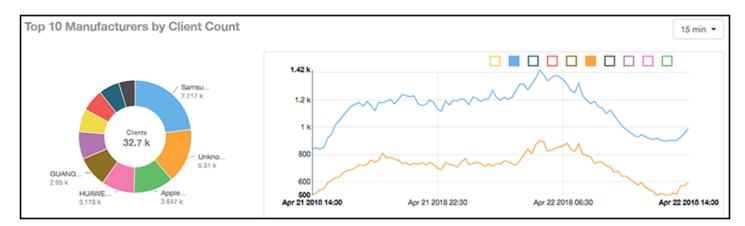


FIGURE 82 Clients - Top 10 OS by Client Count

Clients - Top 10 Manufacturers by Client Count

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

FIGURE 83 Clients - Top 10 Manufacturers by Client Count



Clients - Top 10 Authentication Methods by Client Count

The Top 10 Authentication Methods chart and graph of the Clients report provides you with information about the top 10 methods most commonly used in your system to authenticate users.

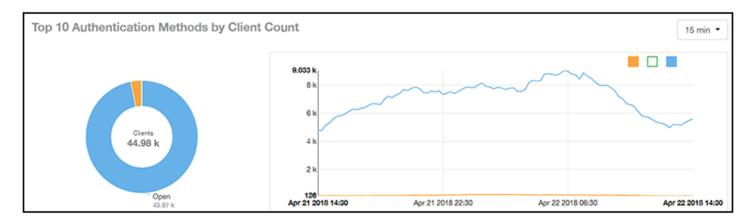


FIGURE 84 Clients - Top 10 Authentication Methods

Applications Report Dashboard

•	Applications Report	69
•	Applications - Overview	
•	Applications - Top 10 by Traffic Volume	
•	Applications - Top 10 by Client Count	
•	Applications - Top Applications by Traffic (table)	
•	Applications - Top Applications by Client Count (table)	

Applications Report

The Applications report provides the details of the applications accessed by the user.

The Applications report contains the details of the applications accessed by the user and predefined by SCI. The overview contains the list of recognized applications. The rest of the report contains the top 10 applications by traffic volume received and transmitted over time, client count, traffic, and clients.

The following figure shows only the upper portion of the Applications dashboard that appears when you click **Applications** on the navigation bar.

FIGURE 85 Applications Dashboard (upper portion)

Overview	Applications Report			AP AN SSID AN PART AN -	May 09 2017 - May 19 2017 - Download -
Network					
AFe & Controllers	Overview				
WLANE .					
Clients	∞₀8		<u>@</u>	1×20.02 m	1
Applications		52			
Artime Utilization	(in) (in) (in) (in) (in) (in) (in) (in)			To 200.5 vie	
AP Details	2 N			These Apps consume 0 % (405.7 MB) of 1 (10.8 TB).	
Crient Details				(Break)	
Data Explorer			1. And the second s		
Aaman 🕨	Top 10 Applications by Traffic Volume				UserTato + Samo +
	Min (1973) Min (1913) Min (1913) Min (1913)	102.2 MB 102.110 853210 47.8410 47.8410 86 May 69.867 10.45	Nay (9 2011 W-4)	Ner top7 tited	May 10 2017 10 300
	Top 10 Applications by Client Count	* * *			

The Applications report consists of five sections, which are listed in the table below. Figures showing each of these sections appear later.

1	Overview	Contains the list of applications that SCI recognizes, and displays the percentage of
		traffic consumed by these applications

2	Top 10 Applications by Traffic Volume	Contains the list of top 10 applications in terms of volume of traffic.
3	Top 10 Applications by Client Count	Contains the application information and displays the quantity of traffic consumed by the listed applications.
4	Top Applications by Traffic	Displays the top applications by traffic and the percentage consumed of the total traffic.
5	Top Applications by Client Count	Displays the top applications by clients and the percentage consumed of the total traffic by the applications.

Applications - Overview

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

This Overview report contains the following:

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

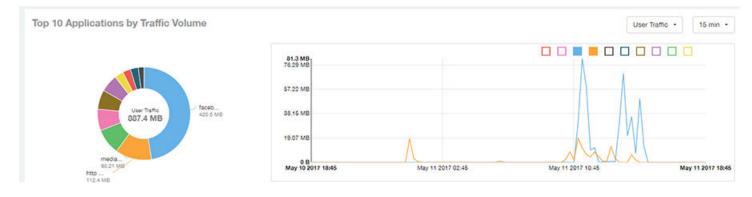
FIGURE 86 Applications - Overview

Overview	
T6 Recognized Apr	ps

Applications - Top 10 by Traffic Volume

The Top 10 Applications by Traffic Volume pie chart and graph of the Applications report display the top applications with the largest traffic volume in the network, along with the received and transmitted traffic volumes.

FIGURE 87 Applications - Top 10 Applications by Traffic Volume



The pie chart and graph contain the top applications with the largest traffic volume in the network, along with the received and transmitted traffic volumes. You can view the received and transmitted traffic volumes based on the Rx+Tx Filter on page 28. To view the top 10 applications, choose from the legend available on the top of the graph. Each applications will appear as a separate graph line. If you hover over the line graph a pop-up appears containing the selected details.

Applications - Top 10 by Client Count

The Top 10 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.



Applications - Top Applications by Traffic (table)

The Top Applications by Traffic table of the Applications report displays the top (10, 20 or 50) applications by the amount of traffic generated over the time period selected.

FIGURE 88 Applications - Top Applications by Traffic

Index	Application Name	Ports	Rx	User	Tx	User	User	fraffic	Clients	ł
1	facebook	443	24.73 MB		395.7 MB		420.5 MB		3	
2	http protocol over tis ssl	443	12.55 MB		C	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		69.56 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	0	24.45 MB	1	
10	redcdn.pl	80	0	360.5 KB	(16.96 MB		17.33 MB	1	

Applications - Top Applications by Client Count (table)

Use the Top Applications by Client Count table of the Applications report to view which applications are being used by the most clients on the network.

You can sort the table by any column by clicking on the column heading. Additionally, you can customize the table by clicking the

gear icon 🐼 and selecting from the list of columns to display.

You can also select whether to display only the top 10 (default value), 20, 50, or 100 applications, or list all applications. Configure the number of rows per a page using the **Rows per Page** list in the table settings drop down menu.

FIGURE 89 Applications - Top Applications by Client Count

	y Client Count			These applications consume 0 % (558.8		 Top 10 Application 	
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 K3	
3	http protocol over tis ssl	443	3	12.55 MB	99.9 MB	112.4 M	
4	miscellaneous	0, 3544, 443, 5223, 53	3	2.608 MB	3.289 MB	5.896 M8	
5	ssi/tis	443, 5223	з	3.032 MB	10.5 MB	13.53 ME	
6	web file transfer	0, 80	3	85.6 KB	926.4 KB	1012 K	
7	adkontekst.pl	80	2	62.95 KB	945.2 KB	1008.00	
8	akadns.net	0, 5223	2	3.382 KB	2.291 KB	5.673 K	
9	arp	0	2	29.16 KB	42.6 KB	71.76 K	
10	meteo.pl	80	2	82.4 KB	1.714 MB	1.794 M	

Airtime Utilization Report Dashboard

•	Airtime Utilization Report	73
	Airtime Utilization - Overview	
	Top 10 APs By Airtime Utilization	. 74
	Top APs by Airtime Utilization for 2.4 Ghz	
	Airtime Utilization - Top APs by Airtime Utilization for 5 GHz	
	Airtime Utilization Trend.	
	Airtime Utilization - Over Time	77

Airtime Utilization Report

The Airtime Utilization report provides an overview of airtime utilization.

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

The following figure shows the upper portion of the Airtime Utilization dashboard that appears when you click **Airtime Utilization** on the navigation bar.

FIGURE 90 Airtime Utilization Dashboard (upper portion)

Overview	1	Airtime Utilization Report			- XP AB - Radio AB May 99 2017 - May 19	Download +
Network	e i					
APs & Controllers	SCH10	Overview			Top 10 APs by Airtime Utilization	Î
WUANS	10				SC WCenter AHD Cafe	
Cients					EC WConter APRI C EC Media Conter	
Appleations					KDO KQE, LI 40 APH (D. 56 No.	
Airtime Utilization		2.4 OHs	(<u>@</u>)		ADVE TAPAR 13 201 3000 (0.5 %) KTHO KULLS PEAPE (MARE NA	
AP Details		15.03 s	\sim	1.52 s	107 (2, 4, 5, 4, 5, 4, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7, 7,	
Cient Details			•		10 T 1 (1 (1 (1 (1 (1 (1 (1 (1 (1	
Data Explorer					Arrespt (\$2.5)	

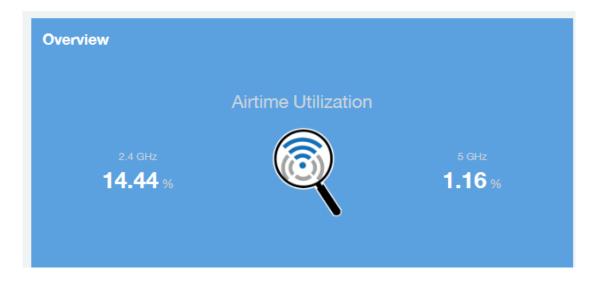
The Airtime Utilization report consists of the six sections listed in the table below.

1	Overview	The overview report section contains the total number of APs based on the radio category.
2	Top 10 APs by Airtime Utilization	This tabular report pertains to top ten APs airtime utilization, represented as percentage. This is based on your selection of APs, Radio and Date Range filters.
3	Top APs by Airtime Utilization for 2.4 GHz	This tabular report pertains to top APs airtime utilization based on the radio category of 2.4 GHz.
4	Top APs by Airtime Utilization for 5 GHz	This tabular report pertains to top APs airtime utilization based on the radio category of 5 GHz.
5	Airtime Utilization Trend	This graph pertains to the utilization trend of APs based on the radio category of 2.4 and 5 GHz.
6	Airtime Utilization Over Time	The tabular report contains the utilization trend of APs as per the selected components.

Airtime Utilization - Overview

The Overview section of the Airtime Utilization report displays the aggregate utilization rates for all of the 2.4 and 5 GHz radios on all APs for the selected time period.

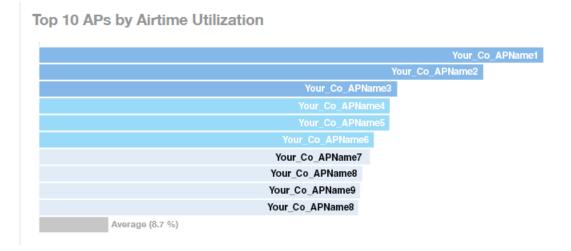
FIGURE 91 Airtime Utilization - Overview



Top 10 APs By Airtime Utilization

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

FIGURE 92 Top 10 APs by Airtime Utilization



Top APs by Airtime Utilization for 2.4 Ghz

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

Use this report to view a list the top APs with the highest airtime utilization sorted according to the selected columns. Click the

gear icon 🐼 to select which columns to display, or click any column heading to sort by that column.

You can also select whether to display the top 10, 20, 50, or 100 APs by airtime utilization from the Top APs filter. The number of rows per page can be defined using the **Rows per page** option in the table settings drop down list.

FIGURE 93 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 %	62.03.96
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName2	63.56 %	30.74 %	0.96	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	69.02 %	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	56.00 %	23.04 %	0.03 %	33.52 %
7	Your_Co_APName7	10.x.y.7	Your_Co_CTName7	56.02 %	26.77 %	0.96	29.25 %
8	Your_Co_APName8	10.x.y.8	Your_Co-CTName8	55.36.%	42.26 %	3.86 %	7.24 %
9	Your_Co_APName9	10.x.y.9	Your_Co_CTName9	62.73 %	43.24 %	4.38.%	5.13.96
10	Your_Co_APName10	10.x.y.10	Your_Co_CTName10	52.64 %	45.71 %	2.45 %	4.48 %

Airtime Utilization - Top APs by Airtime Utilization for 5 GHz

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 report to view a list the top APs with the highest airtime utilization sorted by the selected columns. Click the gear icon so select which columns to display, or click any column heading to sort by that column.

You can also select whether to display the top 10, 20, 50, or 100 APs by airtime utlization from the Top APs filter. The number of rows per page can be defined using the **Rows per page** option in the table settings drop down list.

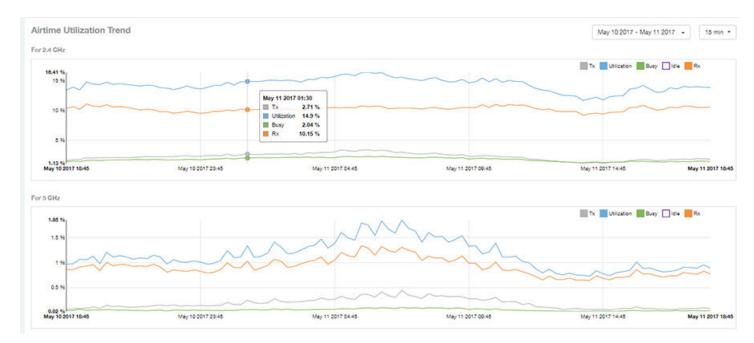
FIGURE 94 Airtime Utilization - Top APs by Airtime Utilization for 5 GHz

Index	AP Name	AP IP Address	Controller Name	Airtime	Utilization	Airtii	me Rx	Airtime Tx		Airtime Busy	1
1	Your_Co_APName1	10.x.y.1	Your_Co_CTName1	74.25 %		72.91 %		0 %	I.	1.34 %	1
2	Your_Co_APName2	10.x.y.2	Your_Co_CTName1	59.35 %		58.26 W		0 %	F	1.09 %	1
3	Your_Co_APName3	10.x.y.3	Your_Co_CTName1	58.29 %		57.54 %		0.96	C	0.76 %	1
4	Your_Co_APName4	10.x.y.4	Your_Co_CTName1	55.36 N		53.99 N		0.36 %	C	1.01 %	
5	Your_Co_APName5	10.x.y.5	Your_Co_CTName1	55.08 %		53,78 %		0.45 %	1	0.85 %	
6	Your_Co_AccessPoint1	172.16.z.1	Your_Co_Controller2	5436%		54.18 %		0.05 %		0.12 %	1
7	Your_Co_AccessPoint2	172.16.z.2	Your_Co_Controller2	54.08 %		53.81 %		0.96		0.27 %	
8	Your_Co_AccessPoint3	172.16.z.3	Your_Co-Controller2		49.03 %	6	48.77 %	0.08 %	E	0.18 %	1
9	Your_Co_AccessPoint4	172.16.z.4	Your_Co_Controller2	(48.88 %	6	47.47 %	0.95 %		0.45 %	1
10	Your_Co_AccessPoint5	172.16.z.5	Your_Co_Controller2		46.03 %		45.96 %	0.02 %	-	0.05 %	

Airtime Utilization Trend

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

FIGURE 95 Airtime Utilization Trend



Airtime Utilization - Over Time

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

FIGURE 96 Airtime Utilization Over Time

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
Aay 10 2017 18:45 - 18:59	13.43 %	10.37 %	1.61.16	1.45 %	0.97 %	0.86 %	0.06 %	0.04 %
Aay 10 2017 19:00 - 19:14	12.96 %	10.67.%	1.76.%	1.82 %	0.98 %	0.86 %	0.07 %	0.04 %
Aay 10 2017 19:15 - 19:29	13.46 %	10.22 %	1.78 %	1.46 %	1.07 %	0.91 %	0.09.95	0.07 %
Aay 10 2017 19:30 - 19:44	14.78 %	11.09.94	2.07 %	1.63 %	1.05.%	0.93 %	0.09.%	0.04 %
Aay 10 2017 19:45 - 19:59	14.45 %	10.76 %	2.04 %	1.66.%	1.13.96	0.96 %	0.11.96	0.06 %
Aay 10 2017 20:00 - 20:14	14.37 %	10.66 %	2.1 %	1.61 %	0.90 %	0.84 %	0.08 %	0.06 %
Aay 10 2017 20:15 - 20:29	14.77.%	10.06.%	2.11 %	17.5	1.21 %	1 %	0.16.96	0.06 %
Aay 10 2017 20:30 - 20:44	12,41 %	10.61 %	2.1 %	1.71.56	131%	0.94 %	0.12.96	0.06.96
Aay 10 2017 20:45 - 20:59	14.62 %	10.67.96	2.11.%	1.73.%	1.14.%	0.96 %	0.+3 %	0.06 %
Aay 10 2017 21:00 - 21:14	14.37 %	10.66 %	2.00 N	1.72 %	1.33 %	0.95 %	0.11.96	0.06 %

AP Details Report Dashboard

•	AP Details Report	79
•	AP Details Report AP Details - Summary	81
•	AP Details - Performance	
•	AP Details - Details	
•	AP Details - Stats	
•	AP Details - Uptime History	83
•	AP Details - Traffic Trend.	
•	AP Details - Unique Clients Trend Over Time	84
•	AP Details - Top 10 Clients by Traffic Volume	
•	AP Details - Top 10 Applications by Traffic Volume	
•	AP Details - Top SSIDs by Traffic	
•	AP Details - Sessions	86
	AP Details - RSS Trend	87
	AP Details - SNR Trend	87
	AP Details - Airtime Utilization Trend	
	AP Details - Clients Details	
•	AP Details - Alarms	
	AP Details - Events	
•	AP Details - Anomalies	

AP Details Report

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

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

The following figure shows only the upper portion of the AP Details Report screen:

FIGURE 97 AP Details Report (upper portion)



The AP Details report consists of 17 sections and are described in the following table. Figures showing each of these sections appear later.

1	Summary	Contains basic information about the AP. The AP in this example figure above is AP17.
2	Performance	Contains performance data about the access point named AP17 in the example figure above.
3	Details	Contains some details about the example AP17 access point, including showing the nested hierarchy of how the administrator has set up the APs in the network.
4	Stats	Contains statistics specific to the example AP 17 access point.
5	Uptime History	A line graph shows when this AP has been up or down over different time periods.
6	Traffic Trend	Two type of line graphs depict traffic by usage, and two line graphs depict traffic by radio type for this AP.
7	Unique Clients Trend Over Time	Two line graphs depict unique clients associated with this AP. One graph shows the number of unique clients and the other shows the traffic generated by unique clients - both over specified time periods.
8	Top 10 Clients by Traffic Volume	A pie chart and line graph depict the clients that have generated the largest volume of traffic over this AP over a specified period of time.
9	Top 10 Applications by Traffic Volume	A pie chart and line graph depict the applications that have generated the largest volume of traffic over this AP over a specified time period.
10	Top SSIDs by Traffic	A table lists the SSIDs that have generated the most traffic associated with this AP over a specified time period. An SSID is a logical group of APs. An AP can belong to multiple SSIDs.
11	Sessions	A table provides details for whatever number of client sessions that you specify for this AP.
12	RSS Trend	A line graph depicts the received signal strength trends over time for this AP.
13	SNR Trend	A line graph depicts the signal-to-noise ratio trends over time for this AP.

14	Airtime Utilization Trend	Two line graphs depict the airtime utilization for this AP, by radio type, over a specified time period.
15	Clients Details	A table provides details for however many top clients for this AP that you specify.
16	Alarms	A table lists the alarms that have been generated for this AP for the time period that you specify.
17	Events	A table lists the events that have been generated for this AP for the time period that you specify.

AP Details - Summary

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

The AP shown in this example is named AP17.

FIGURE 98 AP Details - Summary

Summary		
	IP Address:	10.x.y.10
~	MAC Address:	AB:CD:EF:01:23:48
- Ž		123456789123
		Online
AP17	Uptime:	21d 3h
	Reboots:	0 (over selected time)

AP Details - Performance

The Performance section of the AP Details report displays data about the specified AP.

FIGURE 99 AP Details - Performance



AP Details - Details

The Details section 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 the administrator has named APGroup_1. EFGController1 in this example is one of the controllers being used on a wireless network named EFG123.

FIGURE 100 AP Details - Details

P Hierarchy	Model:	R300
FG123	Version:	3.1.2.0.134
> EFGController1	Location:	Unknown
> Administration Domain	Controller Model:	SZ104
> Default Zone	Controller Serial No.:	Unknown
> APGroup_1	Controller Version:	3.1.2.0.520
	Controller Name:	EFGController1
> AP17	Controller MAC:	FE:DC:BA:89:67:06

AP Details - Stats

The Stats section of the AP Details report displays some traffic statistics about the specified AP.

FIGURE 101 AP Details - Summary



AP Details - Uptime History

The Uptime History line 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 drop-down menus to specify the timeframe and the granularity of the graph.

FIGURE 102 AP Details - Uptime History

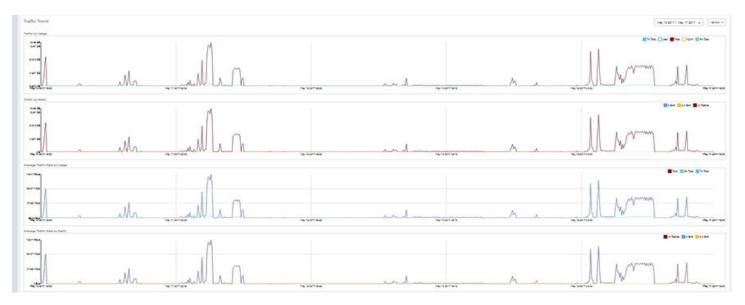


AP Details - Traffic Trend

The Traffic Trend section of the AP Details report contains 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 drop-down menus to specify the timeframe and the granularity of the graphs.

FIGURE 103 AP Details - Traffic Trend



AP Details - Unique Clients Trend Over Time

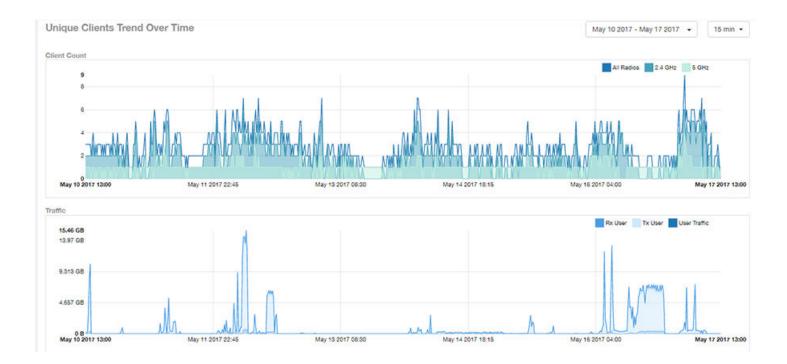
The Unique Clients Trend Over Time section of the AP Details report contains two line graphs that provide information about unique clients associated with the specified AP over a certain time period.

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

Use the drop-down menus to specify the timeframe and the granularity of the graphs.

AP Details Report Dashboard

AP Details - Top 10 Clients by Traffic Volume



AP Details - Top 10 Clients by Traffic Volume

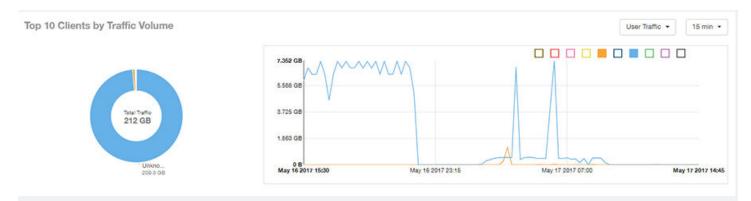
The Top 10 Clients by Traffic Volume pie chart and line graph of the AP Details report depict the clients that have generated the largest volume of traffic over this AP for a specified period of time.

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

NOTE

If you click on one of the clients listed in the pie chart, you will be taken to the Client Details dashboard for that client.

FIGURE 104 AP Details - Top 10 Clients by Traffic Volume

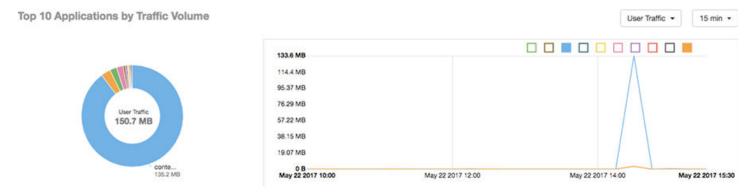


AP Details - Top 10 Applications by Traffic Volume

The Top 10 Applications by Traffic Volume pie 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 drop-down menus to specify the traffic type and the granularity of the graph. Click any of the colored squares to toggle display of the corresponding applications.

FIGURE 105 AP Details - Top 10 Applications by Traffic Volume



AP Details - Top SSIDs by Traffic

The Top SSIDs by Traffic table of the AP Details report lists the SSIDs that have generated the most traffic associated with this AP. An SSID is a logical group of APs. An AP can belong to multiple SSIDs. Use the drop-down menu to specify the number of SSIDs to display.

FIGURE 106 AP Details - Top SSIDs by Traffic

Index	SSID Name	Rx Total	Tx Total	Total Traffic	Clients	APs	<
1	Your_Co_SSID_Name1	11.02 G8	201.3 G8	212.3 GB	32	1	

AP Details - Sessions

The Sessions table of the AP Details report provides details for however many client sessions that you specify for this AP.

Use the drop-down menu to specify how many sessions to display.

If you click on one of the client **hostname** links, you will be taken to the Client Details report for that client.

FIGURE 107 AP Details - Sessions

essions							L	ast 1,000 Session
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

AP Details - RSS Trend

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

Use the drop-down menus to specify the timeframe and the granularity of the graph.

FIGURE 108 AP Details - RSS Trend



AP Details - SNR Trend

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

You can use the drop-down arrows to select the time frame and granularity for this graph.

FIGURE 109 AP Details - SNR Trend



AP Details - Airtime Utilization Trend

The Airtime Utilization Trend line graphs of the AP Details report depict the airtime utilization for this AP, by radio type, over a specified time period.

You can use the drop-down arrows to select the time frame and granularity for this graph.

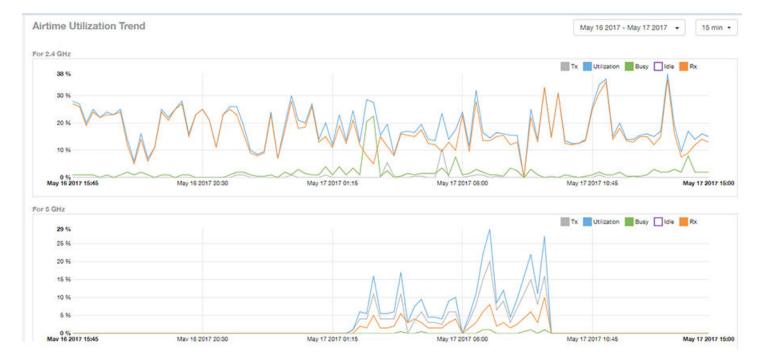


FIGURE 110 AP Details - Airtime Utilization Trend

AP Details - Clients Details

The Clients Details table of the AP Details report provides details for however many top clients that you specify for this AP.

Use the drop-down menu to specify how many top clients to display.

If you click on one of the client **hostname** links, you will be taken to the Client Details report for that client.

FIGURE 111 AP Details - Clients Details

ents Details				These clients	consume 100 % (206.1 GB)) of all user traffic (206.1 GB)	Top 10 Client
Index	Hostname	IP Address	Username	Sessions	Rx User	Tx User	User Traffic
1	EFGHost1	10.x.y.1	Your_Co_UserName1	25	10.47 68	195 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

AP Details - Alarms

The Alarms table of the AP Details report lists the alarms generated for this AP for the time period that you specify. Use the drop-down menu to specify how many alarms to display.

You can use the gear icon 🍄 to choose what columns of information you wish to display.

FIGURE 112 AP Details - Alarms

arms				Last 10 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
		🚽 1 🔻 of 1 🐌		

AP Details - Events

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

Use the drop-down menu to specify how many events to display.

You can use the gear icon 🍄 to choose what columns of information you wish to display.

FIGURE 113 AP Details - Events

rents			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

AP Details - Anomalies

The anomalies charts provide information about any behavior that might 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.

For more information about anomalies, as well as screen shots of each type, refer to the Using Ruckus Smart Analytics on page 19.

Client Details Report Dashboard

	Client Details Report	91
	Client Details - Summary	
•	Client Details - Stats	. 92
•	Client Details - Top 10 Applications by Traffic Volume	.93
•	Client Details - Traffic Trend	. 93
•	Client Details - RSS Trend	. 94
•	Client Details - SNR Trend	94
•	Client Details - Sessions	.95

Client Details Report

The Client Details report provides details about one specific client.

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

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

FIGURE 114 Client Details Report (upper portion)

Overview	(Clients Report			AP AN GOD AN FROM AN .	May 09 2017 - May 19 2	017 - Down	end -
Network								
APs & Controlle s	B-CHEO	Overview	Тор	10 Unique Clients by Traffic			UserTraffo +	1
WLANE	ŝ.						RADSON (2013) 680	
Clients		Sector States			Unknown, PadPolscietter (25 17.7.68)	8.3-640		
Appleations				University, and real-da-Nacot2005-00027 (1931.8-603) Nation-pre (1932.7-603)				
Artime Utilization				Unknown, andreid 7115405747807300 (1023 G8) W8-067827501 (9735 G8)				
AP Details		Luer Tarte Exter Charms 21.87 m 179.3 s		Unknown, Windows-Phone (85.86.68) 1-Netbuk-dna2 (89.77.68)	74 (*2+44 *9)			
Client Details				User- (65.90 G8) rispe (157.8 M8)	(10.04)			
Outa Explorer				raga cur a ma				
Aaman 🕨					These clients consume 6.66 % (1.436 TB) of all use	r taño (21.87 TB).	Top 10 Crients +	

The Client Details report consists of seven sections and are described in the following table. Figures showing each of these sections appear later.

1	Summary	Contains basic information about the client. The hostname in this example figure above is XYZ123.
2	Stats	Contains basic statistics specific to this client.
3	Top 10 Applications by Traffic Volume	A pie chart and line graph contain the applications run by this client that have the largest traffic volume.
4	Traffic Trend	Two line graphs depict traffic by usage and traffic by radio type for this client.
5	RSS Trend	A line graph depicts the received signal strength trends over time for this client.
6	SNR Trend	A line graph depicts the signal-to-noise ratio trends over time for this client.
7	Sessions	A table provides details for sessions between this client and associated access points.

Client Details - Summary

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 115 Client Details - Summary

Summary		
	IP Address:	10.x.y.12
<u> </u>	MAC Address:	FE:DC:BA:89:67:01
	OS:	Mac OS X
	Manufacturer:	Apple, Inc.
XYZ123	Last Known Status:	Disconnected
	Current/Last AP:	AP750

Client Details - Stats

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

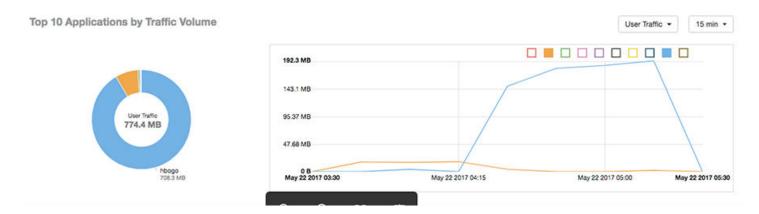
FIGURE 116 Client Details Stats

Stats					
APs Connected 1	Avg Rate 7.412 Mbps	User Traffic 547.2 gB			
Avg Session Length 29m 17s	Sessions 215	Applications 0	6.017 GB	541.2 gb	
			2.4 GHz	5 GHz	

Client Details - Top 10 Applications by Traffic Volume

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 drop-down menus to specify the traffic type and the granularity of the graph. Click any of the colored squares to toggle display of the corresponding applications.

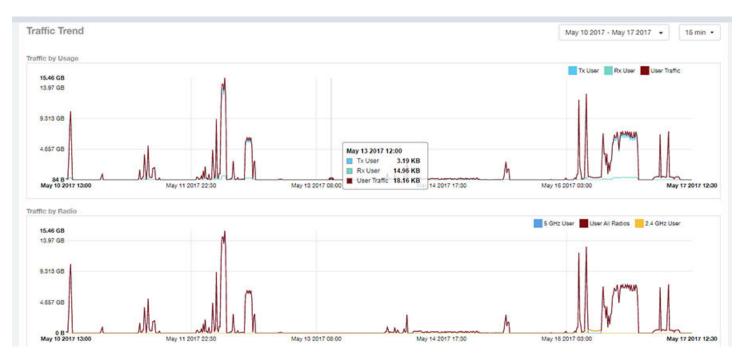


Client Details - Traffic Trend

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

You can use the drop-down arrows to select the time frame and granularity for the graphs.

FIGURE 117 Client Details - Traffic Trend



Client Details - RSS Trend

The RSS Trend graph of the Client Details report depicts the received signal strength trends over time for this client. Use the drop-down menus to specify the timeframe and the granularity of the graph.

FIGURE 118 Client Details - RSS Trend

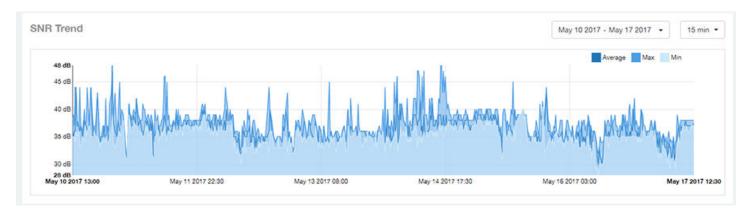


Client Details - SNR Trend

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

You can use the drop-down arrows to select the time frame and granularity for this graph.

FIGURE 119 Client Details - SNR Trend



Client Details - Sessions

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

You can use the drop-down arrows to select the number of sessions you want to display.

You can use the gear icon 🕸 to choose what columns of information you wish to display.

NOTE

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

FIGURE 120 Client Details Sessions

essions								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 G8
lay 17 2017 07:19	May 17 2017 07:46	27m 6s	AP750	SSID17	5 GHz	37,69 MB	763.9 MB	801.6 MB
lay 17 2017 06:17	May 17 2017 07:16	58m 59s	AP750	SSID17	5 GHz	113.9 MB	1.714 GB	1.826 GB
lay 17 2017 04:16	May 17 2017 06:17	2h	AP750	SSID17	5 GHz	178.9 MB	3.484 GB	3.659 GB
lay 17 2017 04:13	May 17 2017 04:15	2m 20s	AP750	SSID17	5 GHz	130.8 KB	104.9 KB	235.6 KB
lay 17 2017 04:12	May 17 2017 04:12	16.28s	AP750	SSID17	5 GHz	53.41 KB	145.5 KB	198.9 KB
lay 17 2017 02:17	May 17 2017 04:12	1h 55m	AP750	SSID17	5 GHz	169 MD	3.295 GB	3.46 GB
tay 17 2017 02:15	May 17 2017 02:15	26.6s	AP750	SSID17	5 GHz	66.72 KB	1.41 MB	1.475 MB

Data Explorer Dashboard

•	Data Explorer and Data Cubes	
•	Applications	
•	Applications Network	
•	Airtime Utilization	101
•	Clients	
•	Sessions	
•	Events	103
•	AP Inventory	104
•	AP Alarms	
•	Controller Inventory	
•	Rogue APs	
•	Data Cube Filters	
•	Creating a Data Explorer Dashboard	
•	Actions You Can Perform on an Existing Dashboard	
•	Exporting Raw Data Using the SCI Virtual Machine Command Line Interface	

Data Explorer and Data Cubes

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

Data Exploration

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

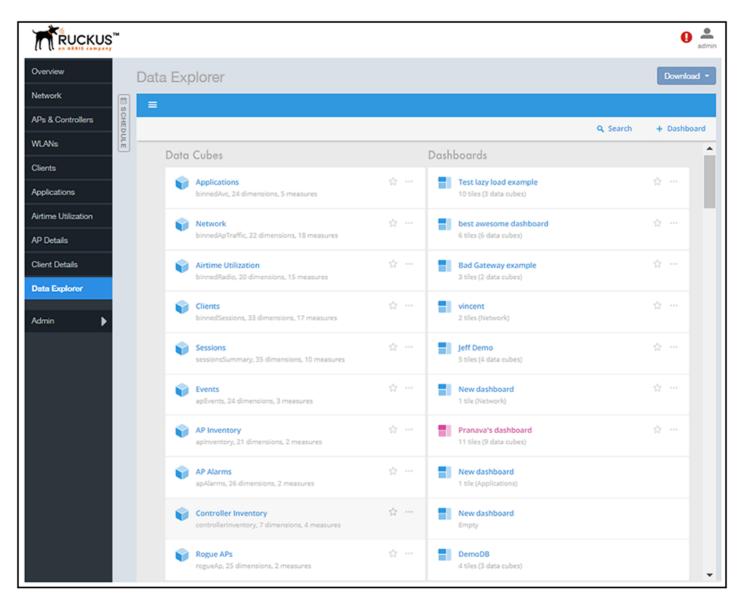
Consider your data to be a three-dimensional cube which you would like to explore, both inside out and outside in, so that you could glean more insights from your data. Of course, most real world data sets will have more than three dimensions, but the concepts from a 3D cube can be directly extended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

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

- 1. **Slice:** Think of slicing a piece of cheese you make a single cut to the cheese to expose the insides. A typical slice operation is the time slice. Instead of looking at all the data from Day 1, you slice the data to just the last 30 days.
- 2. **Dice:** Think of dicing a piece of cheese you make multiple cuts and mash the cheese into much smaller pieces. A typical dice operation is after slicing the cube to just the last 30 days, you "cut" it further by filtering by the controller name and AP group. After the above slice and dice is a smaller piece of the original OLAP cube.
- 3. **Drill Up/Down:** In order to delve into the details, you drill down into a specific AP in the above AP Group, and further drilling down to a specific client hostname. Conversely, you could also search for client MAC in the beginning and drill up to see which AP and controller it belongs to.
- 4. **Roll Up:** This operation typically involves certain numbers, also known as measures which will be explained in detail below. In short, after doing your slice, dice and drill down, you would like to "roll up" the numbers to find out the total transmit traffic for the selected APs.
- 5. **Pivot:** Pivot is simply an operation that allows you to view the data from a different perspective. For example, you have a table showing a list of controllers and the APs belonging to each controller. You may pivot the table to show a list of APs and the controllers they belong to. Think of pivoting as changing the hierarchy between the dimensions.

Thus, as you use the custom reporting, refer to these five operations.

FIGURE 121 Data Explorer and Data Cubes



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

- Applications on page 99
- Network on page 100
- Airtime Utilization on page 101
- Clients on page 102
- Sessions on page 103
- Events on page 103
- AP Inventory on page 104
- AP Alarms on page 105

- Controller Inventory on page 106
- Rogue APs on page 106

NOTE

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

Using Filters

For information on how use data cube filters, which are common to all the data cubes, refer to Data Cube Filters on page 107

Dashboards

You can create and save dashboards, which allow you to customize reports by using data from any or all of the nine data cubes. Refer to the following sections for information on these dashboards:

- Creating a Data Explorer Dashboard on page 130
- Actions You Can Perform on an Existing Dashboard on page 135

Applications

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

FIGURE 122 Data Explorer - Applications

		# < #
DIMENSIONS	FILTER CLatest day + EXPLORE +	123 Total User Traffic V
System Controller MAC Controller Model Controller Name Controller Serial		Search User Traffic Rx User Tx User
A Controller Version Domain Zone AP Group AP MAC	User Traffic 58.79 MB	Client MAC Count AP Count Multi-selection
AP Name AP Serial AP Model AP Location AP Description AP Version		

Data Explorer Dashboard Network

Network

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

FIGURE 123 Data Explorer - Network

■ Network							: < =
DIMENSIONS	٩	FILTER	() Latest day	+	123	MEASURES	
() Time	^	EXPLORE	+		Total	Total Traffic	v
A System	- 1					Search	
A Controller MAC	- 1					Scorer	
A Controller Model	- 1					Total Traffic	<u>^</u>
A Controller Name	- 1					Rx Total	
A Controller Serial	- 1					Tx Total	
A Controller Version	- 1					Mgmt Traffic	
A Domain	- 1			Total Traffic		Rx Mgmt	
∧ Zone	- 1					Tx Mgmt	
A AP Group	- 1			15.48 TB		User Traffic	
A AP MAC	- 1					Rx User	
AP Name	- 1					Tx User	
A AP Serial						Rx Failures	
A AP Model						Tx Failures	-
A AP Location							
A AP Description						Multi-selectio	n
A AP Version					_		

Airtime Utilization

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

FIGURE 124 Data Explorer - Airtime Utilization

■ Airtime Utilization						# < #
DIMENSIONS	٩	FILTER	🕒 Latest day	+	123	MEASURES
() Time	Â	EXPLORE	+		Total	Avg Airtime Busy 🔍
A System	- 1					Search
△ Controller MAC	- 1					Avg Airtime Busy
A Controller Model	- 1					Avg Airtime Idle
A Controller Serial	- 1					Avg Airtime Rx
A Controller Version	- 1					Avg Airtime Tx
A Domain	- 1			Avg Airtime Busy		Avg Airtime Utilization
A Zone	- 1					Total Traffic
A AP Group	- 1			0.88 %		Rx Total
A AP MAC	- 1					Tx Total
A AP Name	- 1					Mgmt Traffic
A AP Serial	- 1					Rx Mgmt
A AP Model	1.1					Tx Mgmt 👻
 △ AP Location △ AP Description 					_	Multi-selection

Data Explorer Dashboard Clients

Clients

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

FIGURE 125 Data Explorer - Clients

≡ Clients						n < a
DIMENSIONS	٩	FILTER	() Latest day	+	123	MEASURES
() Time	^	EXPLORE	+		Total	User Traffic 🛛 🔍
A System	- 1					Search
A Controller MAC	- 1					
A Controller Model	- 1					User Traffic
A Controller Name	- 1					Rx User
A Controller Serial	- 1					Tx User
A Controller Version	- 1					Session Count
A Domain	- 1			User Traffic		Roaming Session Count
A Zone						Client Username Count
A AP Group				14.68 TB		Client Hostname Count
A AP MAC						Avg RSS
A AP Name						Max RSS
A AP Serial						Min RSS
A AP Model						Avg SNR 👻
A AP Location						
A AP Description						Multi-selection
A AP Version		_			_	

Sessions

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

FIGURE 126 Data Explorer - Sessions

≡ Sessions						n < a
DIMENSIONS	٩	FILTER	🕒 Latest day	+	123	MEASURES
() Time	Â	EXPLORE	+		Total	User Traffic 🛛 🔍
A System						Search
A Controller MAC	- 1					
A Controller Model						User Traffic
A Controller Name	- 1					Rx User
A Controller Serial	- 1					Tx User
A Controller Version				User Traffic		Avg Session Duration
A Domain				40.0 70		Session Count
A Zone				10.2 TB		Roaming Session Count
A AP Group						Client Username Count
A AP MAC						Client Hostname Count
A AP Name						Client MAC Count
A AP Serial						AP Count
A AP Model						
A AP Location	÷					Multi-selection

Events

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

FIGURE 127 Data Explorer - Events

≡ Events				≡ < ≈
DIMENSIONS	Q,	RLTER C Latest day +	123	MEASURES
 Time A System 	- 11	EPLORE +	Total	Count V
A Controller MAC	- 1			Search
A Controller Model	- 1			Count
A Controller Name	- 1			Reboot Count
△ Controller Serial	- 1			AP Count
△ Controller Version	- 1	Count		Multi-selection
A Domain	- 1	9		Mon-seccion
A Zone	- 11	9		
A AP Group A AP MAC				
A AP Name				
A AP Serial				
A AP Model				
A AP Location	÷			

NOTE

Refer to the SmartZone *Alarm and Event Reference Guide* based on the controller platform (SCG200/SZ300 and vSZ-H) or (SZ100 and vSZ-E) for details on alarms and events.

NOTE

Also, refer to the ZoneDirector Syslog Events Reference Guide.

AP Inventory

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

FIGURE 128 AP Inventory

■ AP Inventory						≈ < ≈
DIMENSIONS	ď,	FILTER	() Latest day	+	123	MEASURES
A System		EXPLORE	+		Total	Search
A Controller MAC						Max Offline Duration
A Controller Name						AP Count
A Controller Version A Domain				Max Offline Duration		to pin them
A Zone A AP Group				2y 11mo		
A AP MAC A AP Name						
A AP Serial A AP Model						
A AP Location	÷					

AP Alarms

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

FIGURE 129 AP Alarms

■ AP Alarms						# < #
DIMENSIONS	۹.	FILTER	 Latest day + 	+	123 Total	MEASURES
System Controller MAC Controller Model Controller Name						Search Count AP Count
 Controller Serial Controller Version Domain Zone AP Group AP MAC 				Count 466		Multi-selection
AP Name AP Serial AP Model AP Location	Ţ					

NOTE

Refer to the SmartZone *Alarm and Event Reference Guide* based on the controller platform (SCG200/SZ300 and vSZ-H) or (SZ100 and vSZ-E) for details on alarms and events.

Controller Inventory

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

FIGURE 130 Controller Inventory

Controller Inventory	/					a < a
DIMENSIONS ③ Time A System	٩	FILTER	() Latest day	+	123 Total	MEASURES
Controller MAC Controller Model Controller Name Controller Serial						Search Avg CPU Utilization Avg Memory Utilization Avg Disk Utilization
A Controller Version				Avg CPU Utilization 15.03 %		Avg Disk Free

Rogue APs

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

FIGURE 131 Rogue APs

■ Rogue APs						11 × 12
DIMENSIONS	٩	FILTER	🕒 Latest day	+	123	MEASURES
() Time	<u></u>	EXPLORE	+		Total	Rogue AP Count 🛛 🔍
A System						Search
A Controller MAC	- 11					Search
A Controller Model	- 11					Rogue AP Count
A Controller Name	- 11					Max Rogue RSSI
A Controller Serial	- 11					
A Controller Version	- 11			Rogue AP Count		Multi-selection
A Domain	- 11					to pin them
A Zone	- 11			359		
A AP Group						
A AP MAC						
A AP Name						
A AP Serial						
A AP Model						
A AP Location						

Data Cube Filters

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

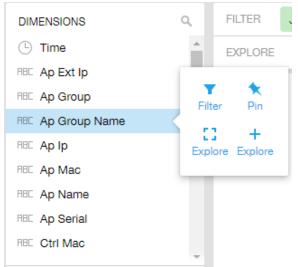
FIGURE 132 Data Cube Filters

RUCK	JSĨ	0 admin
Overview	Data Explorer	Download •
Network	≡ Sessions	678
APs & Controllers	123	MEASURES 2 User Traffic V
WLANs Clients	System Controller MAC Controller Model	9
Applications Airtime	Controller Model Controller Serial	*
Utilization AP Details		Click or drag dimensions to pin them
Client	A Zone 9.00 ID A AP Group A AP MAC	
Data Explorer	A AP Name A AP Serial	
Explorer	A ad Maxial	

The data cube filters are explained in detail in the sections below.

Dimensions

FIGURE 133 Dimensions



Number 1 in Data Cube Filters. Lists industry standard details for Radio such as Time, AP name, System, and Zone name. You can use one or more dimensions to:

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

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

TABLE 5 Dimensions

Dimension name	Description	Supported Data Cubes
Alarm Code	Unique string assigned by the controller to an alarm.	AP Alarms
Alarm State	Indicates if the alarm is outstanding.	AP Alarms
Alarm Type	Description for access point and controller alarms.	AP Alarms
Alarm UUID	Unique string assigned by the controller to an alarm.	AP Alarms
AP Description	Description string of the access point that is configured in the controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP

Dimension name	Description	Supported Data Cubes
AP External IP	External IP address of the access point.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP
AP Group	AP Groups configured in the controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP
AP Internal IP	Internal IP address of the access point.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP
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 Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP

Dimension name	Description	Supported Data Cubes
AP MAC	Base MAC address of the access point.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP
AP Model	Description of the access point model type.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP
AP Name	Name of the access point configured in the controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP
AP Serial	Serial number of the access point.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP
AP Version	Firmware version number of the access point.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP

Dimension name	Description	Supported Data Cubes
Application Category	Amount of user traffic by category	Applications
Application Name	Name of the application accessed by the WiFi client.	Applications
Authentication Method	The WiFi encryption and authentication method adopted.	ClientsSessions
BSSID	Basic service set identifier	Network
Cable modem firmware	Firmware version of the cable modem.	AP Inventory
Cable modem IP	IP address of the cable modem.	AP Inventory
Cable modem MAC	MAC address of the cable modem.	AP Inventory
Category	Category for access point and controller alarms or events.	Events AP Alarms
Channel	The WiFi channel number used.	NetworkClientsSessions
Client IP	Internal IP address of the WiFi client.	ClientsSessions
Client MAC	MAC address of the WiFi client.	 Applications Clients Sessions
Client Radio Mode	Possible values are: ac, n, a, g, b, or "unknown" (if SmartZone version is prior to 3.6).	ClientsSessions
Connection Status	Connection status of the access point: Online, Offline, Discovery, Provisioned.	AP Inventory
Controller MAC	MAC address of the controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Controller Inventory Rogue AP
Controller Model	Description of the model of the controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Controller Inventory Rogue AP

Dimension name	Description	Supported Data Cubes
Controller Name	Name of the configured controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Controller Inventory Rogue AP
Controller Serial	Serial number of the controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Controller Inventory Rogue AP
Controller Version	Firmware version number of the controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Controller Inventory Rogue AP
Disconnect Time	Disconnect time of a session.	Sessions
Domain	Domains configured in the controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP
Event Code	Code number for access point and controller events.	Events
Event Type	Description for access point and controller events.	Events
First Connection	First connection time of a session.	Sessions

Dimension name	Description	Supported Data Cubes
Hostname	Hostname configured in the WiFi client.	ClientsSessions
Last Status Change	Date and time of the last change in Connection Status of the access point.	AP Inventory
Manufacturer	Manufacturer information for the WiFi client.	Clients Sessions
OS Type	OS information for the WiFi client.	Clients Sessions
Port	Port of the application accessed by the WiFi client.	Applications
Radio	Indicates the radio frequency band: 2.4GHz or 5GHz.	 Applications Network Airtime Utilization Clients Sessions
Reason	Additional description for access point and controller alarms or events, if available.	Events AP Alarms
Roaming Session ID	A unique session ID that is created when a client roams to multiple APs within a short- enough time span that the client is connected to these APs simultaneously.	ClientsSessions
Rogue AP MAC	MAC Address of the detected Rogue AP.	Rogue AP
Rogue Channel	The WiFi channel that the rogue AP was operating on.	Rogue AP
Rogue Encryption	The WiFi encryption and authentication method adopted by the rogue AP.	Rogue AP
Rogue Radio	The radio band (2.4GHz or 5GHz) that the rogue AP was operating on.	Rogue AP
Rogue SSID	SSID of the detected Rogue AP.	Rogue AP
Rogue Type	Possible types are: ignore, known, rogue, and malicious	Rogue AP
Session ID	ID string assigned to a session.	Clients Sessions
Session Type	Indicates whether the session is authorized or unauthorized.	Clients Sessions
Severity	Severity level for access point and controller alarms or events.	Events AP Alarms
SSID	Service set identifier (SSID) configured in the controller.	 Applications Network Clients Sessions

Dimension name	Description	Supported Data Cubes
System	System ID of the controller or the SmartZone Cluster.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Controller Inventory Rogue AP
Time	Allows the data to be viewed in terms of data points with timestamps. Time granularity of 1 minute, 15 minutes, 1 hour, 1 day and 1 week can be chosen.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Controller Inventory Rogue AP
Username	Username of the user account associated with the WiFi client.	Clients Sessions
Zone	Zones configured in the controller.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms Rogue AP

Measures

FIGURE 134 Measures

MEASURES
User Traffic 🔹 💌
Search
User Traffic
Rx User
Tx User
Avg Session Duration
Session Count
Roaming Session Count
Client Username Count
Client Hostname Count
Client MAC Count
AP Count
Multi-selection

Number 2 in Data Cube Filters with the drop-down list shown. Select one or more measures by which you want to sort the selected dimension.

Based on the selected cube, measures can vary.

You can use the drop-down lists on the screen for each data cube to view the supported measures for that cube. The following table lists and describes all the measures that are supported on one or more data cubes in SCI:

NOTE

For more information about traffic-related terms, refer to the Definition of Terms on page 9 section.

TABLE 6 Measures

Measure name	Description	Supported Data Cubes
AP Count	Unique number of access points.	 Applications Network Airtime Utilization Clients Sessions Events AP Inventory AP Alarms

TABLE 6 Measures (continued)

Measure name	Description	Supported Data Cubes
AP Uptime	Uptime percentage for an access point.	AP Inventory
AP-to-SZ Ping Latency	Average time, in milliseconds, for the AP to transmit a packet to the SZ controller, and receive the packet back.	Network
Avg Airtime Busy	Average of the airtime busy metric.	Airtime Utilization
Avg Airtime Idle	Average of the airtime idle metric.	Airtime Utilization
Avg Airtime Rx	Average of the airtime receive metric.	Airtime Utilization
Avg Airtime Tx	Average of the airtime transmit metric.	Airtime Utilization
Avg Airtime Utilization	Average of the total airtime utilization.	Airtime Utilization
Avg CPU Utilization	Average CPU utilization for the controller.	Controller Inventory
Avg Disk Free	Average free disk space for the controller.	Controller Inventory
Avg Disk Utilization	Average disk utilization for the controller.	Controller Inventory
Avg Memory Utilization	Average memory utilization for the controller.	Controller Inventory
Avg Noise Floor	Average noise floor power in dBm.	Clients
Avg RSS	Average received signal strength of the access point in dBm.	Clients
Avg Session Duration	Average time duration for a session.	Sessions
Avg SNR	Average signal to noise ratio at the access point in dB.	Clients
Avg Throughput Estimate	Average throughput estimate for the WiFi client.	• Clients
Client Hostname		Clients Sessions
Client MAC Count	Unique number of WiFi clients.	 Applications Clients Sessions
Client Username		ClientsSessions
Count		EventsAP Alarms
Failed Associations	Number of failed associations.	Network
Failed Authentications	Number of failed open authentications	Network
Mgmt Traffic	Traffic volume, which is transmitted and received in IEEE 802.11 control and management frames. This includes all unicast, multicast and broadcast traffic.	NetworkAirtime Utilization
Max Offline Duration	The maximum offline duration within the selected time range.	AP Inventory
Max Rogue SNR	The maximum detected SNR of the rogue AP.	Rogue AP
Max RSS	Maximum received signal strength of the access point in dBm.	Clients
Max SNR	Maximum signal to noise ratio at the access point in dB.	Clients
Min RSS	Minimum received signal strength of the access point in dBm.	Clients

TABLE 6 Measures (continued)

Measure name	Description	Supported Data Cubes
Min SNR	Minimum signal to noise ratio at the access point in dB.	Clients
Reboot Count		Events
Roaming Session Count	The number of roaming sessions for a specific client. A roaming session occurs when a client roams quickly enough to remain connected to multiple APs simultaneously. If you find a client that has a large number of roaming sessions, you can use various dimensions in Data Explorer to obtain details about the APs.	ClientsSessions
Rogue AP Count	The number of Rogue APs detected by all the APs in your network.	Rogue AP
Rx Failures	Receive packets which failed to be processed due to insufficient buffer in AP.	Network
Rx Management	Traffic volume, which is received by AP (Access Point) in IEEE 802.11 control and management frames. This includes all unicast, multicast and broadcast traffic.	NetworkAirtime Utilization
Rx Total	Sum of the Rx user and management traffic.	NetworkAirtime Utilization
Rx User	Traffic volume, which is received by AP (Access Point) in IEEE 802.11 MAC Service Data Unit (MSDU) data frames. This includes all unicast, multicast and broadcast traffic.	 Applications Network Airtime Utilization Clients Sessions
Session Count	Number of unique sessions.	ClientsSessions
Successful Associations	Number of successful associations.	Network
Successful Authentications	Number of successful open authentications	Network
Successful Authentication Ratio	Ratio of number of successful open authentications over total number of open authentications.	Network
Total Data Frames Ratio	Percentage of all Tx and Rx packets that are data.	Network
Total Management Frames Ratio	Percentage of all Tx and Rx packets that are management.	Network
Total Traffic	Sum of the user and management traffic.	NetworkAirtime Utilization
TxBroadcastFrames	Number of broadcast packets transmitted by the network.	Network
TxDropDataFrames	Tx data frames that are dropped by the message queue.	Network
Tx Failures	Transmit packets which failed to be processed due to insufficient buffer in AP.	Network
Tx Management	Traffic volume, which is transmitted by AP (Access Point) in IEEE 802.11 control and management frames. This includes all unicast, multicast and broadcast traffic.	NetworkAirtime Utilization

TABLE 6 Measures (continued)

Measure name	Description	Supported Data Cubes
TxMulticastFrames	Number of multicast packets transmitted by the network.	Network
Tx Total	Sum of the Tx user and management traffic.	NetworkAirtime Utilization
TxUnicastFrames	The number of data packets transmitted by the network that are not broadcast or multicast packets.	Network
Tx User	Traffic volume, which is transmitted by AP (Access Point) in IEEE 802.11 MAC Service Data Unit (MSDU) data frames. This includes all unicast, multicast and broadcast traffic.	 Applications Network Airtime Utilization Clients Sessions
User Traffic	Traffic volume, which is transmitted and received in IEEE 802.11 MAC Service Data Unit (MSDU) data frames. This includes all unicast, multicast and broadcast traffic. User Traffic = Rx User + Tx User	 Applications Network Airtime Utilization Clients Sessions

Filter

FIGURE 135 Filter

FILTER	Jul 10 - Jul 11, 6:01am	
--------	-------------------------	--

Number 3 in Data Cube Filters. Segregates the data by dimensions such as Time Range, and other dimensions. You can filter on one or more dimensions, and change the sorting hierarchy as required. You can also define the dimensions based on specific properties of the dimension, for example, Time has relative and specific settings. The default dimension is Time, as the databases are very large and can crash the system without this filter.

FIGURE 136 Time - Relative Settings

FILTER	Jul	10 - Jul	11, 6:4	6am	
EXPL	RE	REATIVE		SPECIF	FIC
	LATEST				
	1H	6H	1D	7D	30D
	CURREI	T			
	D	w	м	Q	Y
	PREVIO	US			
	D	W	М	Q	Y
Jul 10 - Jul 11, 6:46am					

You can specify the following:

- Latest time of 1 hour, 6 hours, 1 day, 7 days, or 30 days.
- Current time of day, week, month, quarter, or year.
- Previous time of day, week, month, quarter, or year.

FILTER	Jul 10 - Jul 11, 6:	46am
EXPL	RELATIVE	SPECIFIC
S	TART	
	2016-07-10	06:46
E	ND	
	2016-07-11	06:46
	OK Cancel	
_	/1*	

FIGURE 137 Time - Specific Settings

You can specify the start and end dates and times and click **OK** to save the details.

FIGURE 138 Dimension Options

Ap Gi	oup Name	×
Search		
W1M	@Langkawi_Trial_8	512kbps
Bangi	KPZ	
Bangi	KUO	
KL KT	SN	
KL Kł	(L	
Bangi	KIY	
Bangi	ККМ	
KL KT	DI_1	
Bangi	KTHO	
Bangi	KRK	
Bangi	KAB	
Bangi	KDO	
ОК	Cancel	

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

Explore

FIGURE 139 Explore



Number 4 in Data Cube Filters. Enables visualization based on dimensions and time (data granularity).

FIGURE 140 Explore Time

EXPLO	RE	Tim	ne (Day)		\times	Ra
Time	GR	ANU	LARITY	(
Total	1	1M	5M	1H	1D	1W	
2016	so	RT B	Y				
2010	Ti	ime				1	
-	LIN	/IT					
2016	5						
2010		ОК		Cancel			
2				0.00			- 1

Use this filter to:

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

FIGURE 141 Sort Dimension by Measure

×	Radio			×
S	ORT BY			
4	Airtime Bu	sy	•	Ŧ
LI	MIT			
ŧ	5			~
	ОК	Cancel		

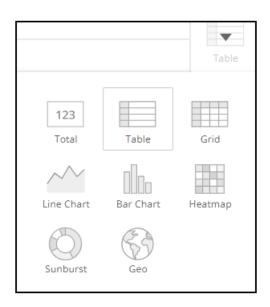
Use this filter to:

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

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

View Outputs

FIGURE 142 View Outputs



Number 5 in Data Cube Filters. Create outputs from visualization in the forms shown above. The default view is Totals.

Add to Dashboard

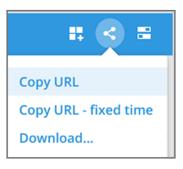
FIGURE 143 Add to Dashboard



Number 6 in Data Cube Filters. Allows you to add a tile you are currently developing to an existing dashboard or to a dashboard that you want to create.

Share Link

FIGURE 144 Share Link



Number 7 in Data Cube Filters. You can share the URL, Export to various formats, View raw data, or download the information. The following figure shows the various formats you can choose for downloading data. You can also select the number of rows to download:

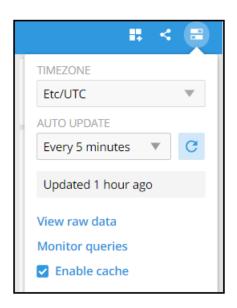
FIGURE 145 Selecting the Amount of Data to Download and the Desired Format

Download data	×
AMOUNT OF DATA TO DOWNLOAD	
100k rows	v
FORMAT	
CSV (Comma-separated values)	v
CSV (Comma-separated values)	
TSV (Tab-separated values)	
XLSX (Excel spreadsheet)	
JSON (Newline delimited JSON)	

Data Explorer Dashboard Data Cube Filters

Options

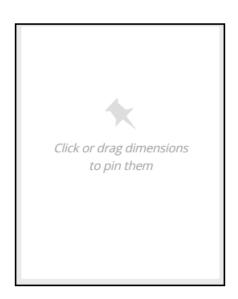
FIGURE 146 Options



Number 8 in Data Cube Filters. Allows you to set the time zone as well as to perform the other functions shown.

Pinboard

FIGURE 147 Pinboard



Number 9 in Data Cube Filters. Click or drag dimensions and pin them on the pinboard. Retain the dimensions for ready reference during visualization.

Time Compares

The Time Compares feature allows you to compare the current data of specified dimensions and measures to the same dimensions and measures during previous time periods. An example is shown in the following figure, where the Controller Version dimension has been chosen along with the User Traffic measure. The Change column indicates how much user traffic has gone up or down for the corresponding controller version over the specified period of time. The method of specifying time periods is described later.

FIGURE 148 Time Compares

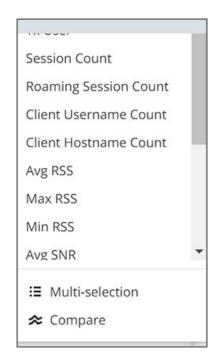
≡ Clients				< =
FILTER 🕒 Latest 7 da	ys +		MEASURE	
EXPLORE A Controller	Version × +	Table	User Traffic	Y
Controller Version	User Traffic 🕹	Change	COMPARE	×
Overall	745.58 GB	▼ 347177.26 GB (99.8%)	1 month back	Ψ.
3.6.1.0.227	386.92 GB	▼ 23.27 GB (5.7%)		
5.0.0.0.672	356.88 GB	▼ 388.68 GB (52.1%)		
5.1.0.0.424	1.78 GB	▲ 1.78 GB (new)		

Creating a Data Comparison

The following procedure demonstrates how you can create a data comparison from scratch, using the figure above as an example:

- 1. From Data Explorer, select one of the data cubes. (In the figure above, the Clients data cube is being used.)
- 2. Drag one or more dimensions into the center pane. In the above example, Controller Version is the only dimension.
- 3. From the Measure drop-down list, you can select one or more measure (use Multi-Selection for more than one). By default, User Traffic is already selected in this example.
- 4. From the Measure drop-down list, select Compare:

FIGURE 149 Selecting Compare from the Measure Drop-Down List



5. If you have already invoked the Compare feature, the previous time period you selected is automatically used, and a display such as the one in Figure 148 appears. However, if you have not yet used Compare, or if you want to change the current time-period, invoke the **Compare** drop-down list:

FIGURE 150 Using the Compare Drop-Down

MEASURE	***
User Traffic	
COMPARE	×
1 month back	W
Previous period	
1 month back	
1 year back	
Custom	
Aug 24 - Sep 1, 4:5!	5am

- 6. You can select one of the listed time periods or you can customize your choice.
- 7. (Optional) To customize your choice, click **Custom**. The following pop-up appears:

FIGURE 151 Custom Comparison Pop-Up Window

Custom comparison	×
Relative	Absolute
1	day back 🔍
	Cancel OK

• If you want to use one of the selections from the **Relative** tab, click the drop-down arrow to view the following possibilities:

Custom c	omparison			×	
	Relative	Ab	solute		35.
1			day back	•	19 49
		Canc	second back minute back		30. 984
124	47.44 GB		hour back		1396
.340	22.91 GB		day back		263.6
.17	3.6 GB		week back month back year back		208.5

FIGURE 152 List of Choices from the Relative Drop-Down List

You can also change the Number 1 to a different number to correspond to your choice in the drop-down list. Click **OK** to have this selection take effect.

• If you want to create a custom time-period, click the **Absolute** Tab:

FIGURE 153 Custom Comparison - Absolute Tab

Custom comparison	×
Relative	Absolute
START TIME	
2018-09-26	17:46
🗹 Auto adjust end date	
END TIME	
2018-09-27	17:46
	Cancel OK

You can change the times as desired, as well as to have the end date automatically adjusted, then click **OK** for your choices to take effect.

Removing the Compare Feature

If you want to remove the Compare feature from the data display, go back to the Measure drop-down list, and select Remove Compare Measure, as shown in the following figure:

FIGURE 154 Removing the Compare Measure

IEASURE	
User Traffic	
Şearch	
User Traffic	
Rx User	
Tx User	
Session Count	
Roaming Session Count	
Client Username Count	
Client Hostname Count	
Avg RSS	
Max RSS	
Min RSS	
Avg SNR	-
∷ Multi-selection	
🗢 Remove compare n	ne

Creating a Data Explorer Dashboard

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

The steps below guide you through an example of creating a dashboard in Data Explorer.

1. Click + **Dashboard** in the upper-right portion of the Data Explorer page in SCI.

The New dashboard screen is displayed:

FIGURE 155 New dashboard screen

12	Data Explorer		Download *
SCHEDULE	New dashboard		Cancel Save
	Click and drag to add a tile		
m			

2. Highlight the "New dashboard" text and give the dashboard a name (DemoDB in this example):

FIGURE 156 Naming the New Dashboard

_	

3. Drag your cursor to highlight any number of small boxes on this screen. A popup configuration window appears, as shown in the following figure:

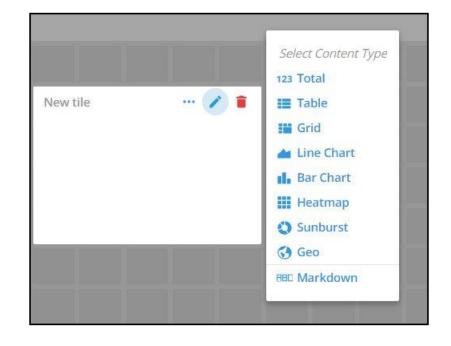


FIGURE 157 Adding a Tile to Your Dashboard by Using the Popup

4. Using the popup and the icons, continue to build your tile. For example, you could select the following the Content Type **123 Total**.

The following popup appears:

FIGURE 158 New-Tile Popup After Selecting Content Type of 123 Total

	TITLE	
	New tile	
lew tile 🧪 💼	CONTENT	
ewale	123 Total	W
	DATA CUBE	
	Applications	
3.7 MB	FILTER	
J./ IVID	🕒 Latest day	
	+	
	SHOW	
	+	
	MEASURES	
	User Traffic	V .
	VISUALIZATION OPTIONS >	
	TILE OPTIONS >	
	📦 Edit in Data Cube	

5. Next, you can customize this tile by making the selections you want, as shown in the following example:

FIGURE 159 New-Tile Popup After Doing Some Customization

		TITLE	
		Network tile	
		CONTENT	
		Table	$\overline{\mathbf{v}}$
Vetwork tile		DATA CUBE	
AP Version	Total Traffic	Network	V
		FILTER	
3.2.1.0.650	8277.2 GB	🕒 Latest day	
3.1.2.0.76	95.15 GB	A AP Description (2)	×
3.1.2.0.134	5.42 GB	+	
10.0.1.0.17	1.4 GB	SHOW	
		A AP Version	×
		+	
•		MEASURES	
		Total Traffic	W
		VISUALIZATION OPTIONS >	
		TILE OPTIONS >	
		😭 Edit in Data Cul	be

6. You could then click the option to Edit in Data Cube, which brings you to the following mode:

Network tile					Cancel	Save
DIMENSIONS	Q	FILTER 🕓 Latest day	∧ AP Description (2) × +		MEASURES	
) Time	-	EXPLORE A AP Version	× +	Table	Total Traffic	
A System	- 8					
A Controller MAC	- 11	AP Version	Total Traffic	***		
A Controller Model	- 1	Total	8281.41 GB			
A Controller Name	- 11	3.2.1.0.650	8180.24 GB			
A Controller Serial	- 1	3.1.2.0.76	94.31 GB	0	X	
A Controller Version	- 11	3.1.2.0.134	5.41 GB		Click or drag d	
A Domain	- 11	10.0.1.0.17	1.45 GB		to pin th	12177
A Zone	- 11	100010017	1170 500			
A AP Group	- 11					
A AP MAC	- 11					
△ AP Name	- 11					
A AP Serial	- 11					
AP Model						
A AP Location						
A AP Description						
A ADManian	_					

FIGURE 160 Editing New Tile in the Data Cube

7. You can continue to make edits to the tile. For example, you can hover over the Table icon and change the way the data is represented. The example below shows this data in a sunburst representation.

FIGURE 161 Sunburst Representation of Tile in Data Cube



- 8. When you are done with your selections for the first tile you are adding to your dashboard, click **Save** in the upper-right portion of the screen.
- 9. Using the steps demonstrated above, you can continue to add as many tiles as you want to your dashboard.

Actions You Can Perform on an Existing Dashboard

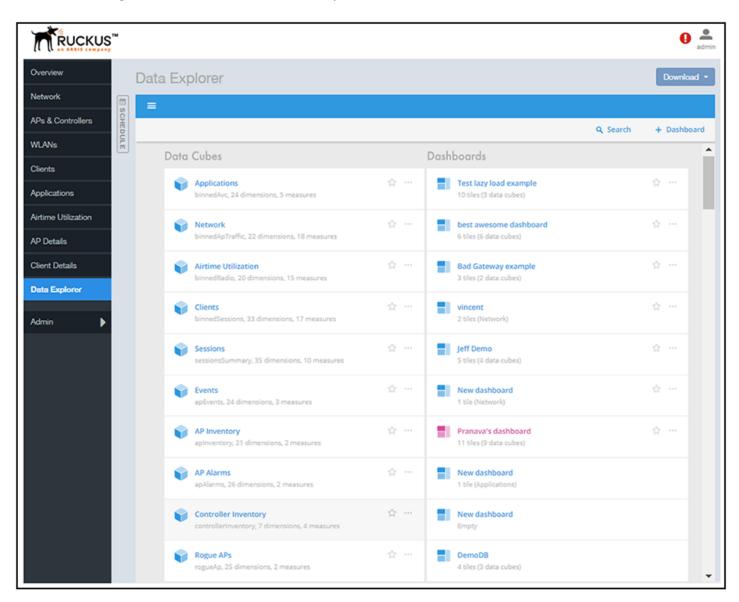
You can perform many actions on an existing dashboard, such as adding or removing tiles, editing existing tiles, deleting tiles and deleting the entire dashboard.

Opening a Dashboard

When you click the Data Explorer tab in SCI, you get a display of all the data cubes on the left side of the window, and a list of existing dashboard on the right side. To open a dashboard, do one of the following:

- Locate the dashboard you are interested in from the list on the right side of the screen, and click on it.
- Click the Options menu (the three horizontal-lines "hamburger" bar near the upper-left portion of the screen), then either use the Search area or locate the desired dashboard to open it.

FIGURE 162 Existing Dashboards Listed on Main Data Explorer Window



Editing a Dashboard

To perform various editing functions on a dashboard, first open the dashboard you want, as in the example below:

FIGURE 163 Dashboard example with three tiles

Data Explorer							Download •
DemoDB							s /
PLTER +							
AP Location, AP Version by Total Traffic	Jane - Constant - Cons	 wⁿ -1927.35 M8 -1420.51 M8 -953.67 M8 476.84 M8 Max Offline Duration ↓ 0 0 0 	Controller Version, Time by Ses	Sion Count GAM AP Count 1 1	1294	6 ^{pm}	

In the upper-right portion of the screen, the following icons are displayed:

FIGURE 164 Dashboard-Editing buttons



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

TABLE 7 Icons for Editing a Dashboard

lcon	Name of Icon	Actions You Can Perform
=	Dashboard options	Clicking this icon allows you to change the following settings: Time zone Auto-update interval Enabling/disabling cache

Data Explorer Dashboard

Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

TABLE 7 Icons for Editing a Dashboard (continued)

Icon	Name of Icon	Actions You Can Perform
	Edit this dashboard	 Clicking this icon allows you to do the following: Rearrange or resize the tiles by using your cursor. Make changes to specific tiles within the dashboard by using the icons that appear for each tile: Use the three dots to duplicate the tile. Use the three dots to duplicate the tile. Use the Pencil icon to add or remove dimensions and measures for the tile as well as to change the representation of the data for the tile. Use the garbage-can icon to delete the tile from the dashboard. Click on the Options tab in the upper-right portion of the screen: This invokes another screen containing general information about the dashboard. From there, there are two tabs - one called "General" and one called "Sharing." In the General tab, you can do the following: Rename the dashboard Change the color theme Decide whether to enforce the time filter Delete the dashboard. In the upper dashboard.

Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

You can use the SCI VM command line interface to export larger amounts of raw data than can be obtained with the user interface. This data can come from any data cubes, dimensions, filters, etc. that you want.

Follow these steps to export the raw data you are interested in.

NOTE

It is recommended to never run more than one export command at a time because data could accidentally be overwritten.

- 1. Log in to your SCI VM.
- 2. Navigate to the following directory:

/storage/ rsa-api/ export /configs

- 3. Locate the file called config-template.yml
- 4. Open the file using a text editor.

The file contains instructions on what to do. You will need to either comment out certain lines or un-comment certain lines in the file, as directed, and will need to fill in the desired values of data cubes, dimensions, and other items as directed.

5. Once you have made the changes in the config-template.yml file, be sure to save it under a different name that is meaningful to you, while leaving the original config-template.yml file in tact for future use.

NOTE

If you are using SFTP, place the key file in the following directory:

/storage/rsa-api/ export /keys

6. Run the following command to export the raw data:

```
sudo docker exec -it rsa-api yarn export-raw <config-file-name>
```

where <config-file-name> is the name of your customized .yml file.

The raw data should be returned to the command line interface. Refer to the following topics for more information:

- Template File for Exporting Raw Data on page 139
- Raw Data Output for Dimensions and Measures on page 141

Template File for Exporting Raw Data

This is the example config-template.yml that you can copy and edit according to the desired output.

```
#
# This is an example configuration file in YAML format. Lines starting with '#' are comments.
# Refer to http://www.yaml.org for detailed specification. Please change values accordingly.
# All attributes are required unless specified as 'Optional'.
#
# Version: 1.0
# Date: 17 Oct 2017
#
source:
# The data source name (case-sensitive). Refer to detailed API reference guide regarding how to
# retrieve the actual value of data source name. Alternatively you may get it from URL
# while accessing a particular Data cube via Data Explorer.
#
# Example: access Data cube 'Clients' by accessing URL (replace {HOST} with your SCI master node
# IP address, authentication may be required):
#
# https://{HOST}/report/dataExplorer#/d/binnedSessions/Clients
#
# The 'dataSource' of 'Clients' is 'binnedSessions' in this example
dataSource: 'foo'
```

Data Explorer Dashboard

Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

ISO 8601 timestamp (e.g, yyyy-MM-ddTHH:mmZ) # Examples: (1) '1970-01-01T00:00Z' for UTC # (2) '2017-01-01T00:00+0300' for UTC +3 # (3) '2017-01-01T00:00-0800' for UTC -8 # (4) '2017-01-01T00:00+0530' for UTC +5:30 # Make sure that 'startTime' is before 'endTime'. startTime: '2017-01-01T00:00:00Z' endTime: '2017-02-01T00:00:00Z' # Optional (comment out if it does not apply) # In the format of '<key>': [a list of values], e.g., 'system': ['foo', 'bar'] # The key name refers to the actual case-sensitive value (not display name) of a particular # dimension of a data cube. Refer to detailed API reference guide regarding how to retrieve the values of # dimensions. Alternatively, you may export a few rows (i.e., 1 minute) without filter and check # out the title of the CSV file for all filter dimension names # For a particular filter, results match any of the values specified in the list for that specific # key would be returned. If multiple filters specified, only results match all of them would be # returned. # Example: # (1) Get all rows for 'system' equals to 'foo' or 'bar' # filters: 'system': ['foo', 'bar'] # # (2) Get all rows for 'system' equals to 'foo', AND 'ctrlMac' equals '99:F6:66:2A:B2:80' # # filters: 'system': ['foo'] 'ctrlMac': ['99:F6:66:2A:B2:80'] # Uncomment and change the following lines to apply filters # filters: # '<key1>': ['value1', 'value2']
'<key2>': ['value1', 'value2'] destination: # 'ftp' or 'sftp' only (case-sensitive) protocol: 'ftp' # The hostname or IP address of the FTP server host: 'localhost' # FTP login username # For 'sftp', it refers to the SSH login username user: 'ftp-username' # Required by 'ftp' protocol only
FTP server login password password: 'ftp-password' # Required by 'sftp' protocol only # File name only of the SSH public key. The file must exist in directory # '/storage/rsa-api/export/keys' on 'SCI' master host # privateKey: 'changeme.pem' # Apply to 'sftp' protocol only # Appry co step proceed only
Passphrase for 'privateKey' if any, leave it with empty value '' or remove it otherwise # passphrase: 'changeme' # The prefix for exported file names. If it contains path of sub-directories (e.g., # 'path/to/dir/example'), those directories (i.e., 'path/to/dir') must exist on FTP server

```
# beforehand
prefix: 'example'
```

Raw Data Output for Dimensions and Measures

The output you generate from raw data contains dimensions and measurements for the various data cubes.

Refer to the following tables:

- Table 8
- Table 9

The following table lists and describes all the dimensions that can be displayed in the raw-data output you generate.

TABLE 8 Dimensions

Dimension name	Description	Supported Data Sources
alarmCode	Unique string assigned by the controller to an alarm.	AP Alarms
alarmState	Indicates if the alarm is outstanding.	AP Alarms
alarmType	Description for access point and controller alarms.	AP Alarms
alarmUUID	Unique string assigned by the controller to an alarm.	AP Alarms
apDescription	Description string of the access point that is configured in the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms
apExtIp	External IP address of the access point.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms
apFwVersion	Firmware version number of the access point.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms

Data Explorer Dashboard

Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

Dimension name	Description	Supported Data Sources
apGroupName	AP Groups configured in the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms
aplp	Internal IP address of the access point.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms
apLocation	Location string of the access point that is configured in the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms
арМас	Base MAC address of the access point.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms
apModel	Description of the access point model type.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms

Data Explorer Dashboard Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

Dimension name	Description	Supported Data Sources
apName	Name of the access point configured in the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms
арр	Name of the application accessed by the WiFi client.	Applications
apSerial	Serial number of the access point.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms
AuthMethod	The WiFi encryption and authentication method adopted.	ClientsSessions
category	Category for access point and controller alarms or events.	AP EventsAP Alarms
channel	The WiFi channel number used.	NetworkClientsSessions
clientlp	Internal IP address of the WiFi client.	Clients Sessions
clientMac	MAC address of the WiFi client.	 Applications Clients Sessions
connectionStatus	Connection status of the access point: Online, Offline, Discovery, Provisioned.	AP Inventory
ctrlFwVersion	Firmware version number of the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms Controller Inventory

Data Explorer Dashboard

Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

Dimension name	Description	Supported Data Sources
ctrlMac	MAC address of the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms Controller Inventory
ctrlModel	Description of the model of the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms Controller Inventory
ctrlName	Name of the configured controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms Controller Inventory
ctrlSerial	Serial number of the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms Controller Inventory
disconnectTime	Disconnect time of a session.	Sessions
domains	Domains configured in the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms

Data Explorer Dashboard Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

TABLE 8 Dimensions (continued)

Dimension name	Description	Supported Data Sources
eventCode	Code number for access point and controller events.	AP Events
eventType	Description for access point and controller events.	AP Events
firstConnection	First connection time of a session.	Sessions
hostname	Hostname configured in the WiFi client.	Clients Sessions
lastStatusChangeTime	Date and time of the last change in Connection Status of the access point.	AP Inventory
manufacturer	Manufacturer information for the WiFi client.	ClientsSessions
memoryUtilization	Percentage of memory being used by the controller.	Controller Inventory
osType	OS information for the WiFi client.	ClientsSessions
port	Port of the application accessed by the WiFi client.	Applications
radio	Indicates the radio frequency band: 2.4GHz or 5GHz.	 Applications Network traffic Airtime Utilization Clients Sessions
radioMode	Possible values are: ac, n, a, g, b, or "unknown" (if SmartZone version is prior to 3.6).	ClientsSessions
reason	Additional description for access point and controller alarms or events, if available.	AP Events AP Alarms
roamingSessionId	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.	ClientsSessions
sessionId	ID string assigned to a session.	Clients Sessions
sessionType	Indicates whether the session is authorized or unauthorized.	Clients Sessions
severity	Severity level for access point and controller alarms or events.	AP Events AP Alarms
ssid	Service set identifier (SSID) configured in the controller.	 Applications Network traffic Clients Sessions

Data Explorer Dashboard

Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

TABLE 8 Dimensions (continued)

Dimension name	Description	Supported Data Sources
system	System ID of the controller or the SmartZone Cluster.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms Controller Inventory
timestamp	Timestamps are represented in UTC timezone format.	 Airtime Utilization Network traffic Applications AP Events AP Alarms AP Inventory Clients Controller Inventory Sessions
username	Username of the user account associated with the WiFi client.	ClientsSessions
zoneName	Zones configured in the controller.	 Applications Network traffic Airtime Utilization Clients Sessions AP Events AP Inventory AP Alarms

The following table lists and describes all the measures that can be displayed in the raw-data output you generate.

TABLE 9 Measures

Measure name	Description	Supported Data Sources
airtimeBusy	Average of the airtime busy metric in percentage form.	Airtime Utilization
airtimeldle	Average of the airtime idle metric in percentage form.	Airtime Utilization
airtimeRx	Average of the airtime receive metric in percentage form.	Airtime Utilization
airtimeTx	Average of the airtime transmit metric in percentage form.	Airtime Utilization
airtimeUtilization	Average of the total airtime utilization in percentage form.	Airtime Utilization
count	A count for each event and alarm type.	AP Events
		AP Alarms

Data Explorer Dashboard Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

TABLE 9 Measures (continued)

Measure name	Description	Supported Data Sources
cpuUtilization	Average CPU utilization for the controller in percentage form.	Controller Inventory
disconnectDuration	Indicated how many milliseconds an AP has been disconnected.	AP Inventory
diskFree	Average free disk space, in bytes, for the controller.	Controller Inventory
diskUtilization	Average disk utilization, in percentage, for the controller.	Controller Inventory
failedAssoc	Number of failed associations.	Network
diskTotal	Total amount of disk space, in bytes, on the controller.	Controller Inventory
firstRss	First received signal strength of the access point in dBm.	• Clients
firstSnr	First signal to noise ratio at the access point in dB.	• Clients
lastRss	Last received signal strength of the access point in dBm.	• Clients
lastSnr	Last signal to noise ratio at the access point in dB.	• Clients
licenseCount	Total number of licenses available on the controller?	Controller Inventory
licenseUtilization	Percentage of available licenses currently being used on the controller.	Controller Inventory
maxRss	Maximum received signal strength of the access point in dBm.	• Clients
maxSnr	Maximum signal to noise ratio at the access point in dB.	• Clients
memoryUtilization	Average memory utilization for the controller, given in percentage form.	Controller Inventory
mgmtRxBytes	Traffic volume, which is received from AP (Access Point) in IEEE 802.11 control and management frames. This includes all unicast, multicast and broadcast traffic.	Network trafficAirtime Utilization
mgmtTraffic	Traffic volume, which is transmitted and received in IEEE 802.11 control and management frames. This includes all unicast, multicast and broadcast traffic.	Network trafficAirtime Utilization
mgmtTxBytes	Traffic volume, which is transmitted by AP (Access Point) in IEEE 802.11 control and management frames. This includes all unicast, multicast and broadcast traffic.	Network trafficAirtime Utilization
minRss	Minimum received signal strength of the access point in dBm.	• Clients
minSnr	Minimum signal to noise ratio at the access point in dB.	• Clients
noiseFloor	Average noise floor power in dBm.	Clients
newAssoc	Number of successful associations.	Network
rxFail_r	Receive packets which failed to be processed due to insufficient buffer in AP.	Network

Data Explorer Dashboard

Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

TABLE 9 Measures (continued)

Measure name	Description	Supported Data Sources
rxBytes	Sum of userRxBytes and mgmtRxBytes.	 Network traffic Airtime Utilization Applications Clients Sessions
Session Count	Number of unique sessions.	ClientsSessions
sessionDuration	The length of a session, given in milliseconds.	Sessions
throughputEstimate	Average throughput estimate for the WiFi client.	• Clients
traffic	Sum of the user and management traffic.	 Network traffic Airtime Utilization Applications Clients Session
txBcastFrames_r	Number of broadcast packets transmitted by the network.	Network
txDropDataFrames_r	Tx data frames that are dropped by the message queue.	Network
txFail_r	Transmit packets which failed to be processed due to insufficient buffer in AP.	Network
txBytes	Sum of userTxBytes and mgmtTxBytes.	 Network traffic Airtime Utilization Applications Clients Sessions
txMcastFrames_r	Number of multicast packets transmitted by the network.	Network
txUcastFrames_r	The number of data packets transmitted by the network that are not broadcast or multicast packets.	Network
userRxBytes	Traffic volume, which is received by AP (Access Point) in IEEE 802.11 MAC Service Data Unit (MSDU) data frames. This includes all unicast, multicast and broadcast traffic.	 Applications Network traffic Airtime Utilization Clients Sessions
userTraffic	Traffic volume, which is transmitted and received in IEEE 802.11 MAC Service Data Unit (MSDU) data frames. This includes all unicast, multicast and broadcast traffic. User Traffic = Rx User + Tx User	 Applications Network traffic Airtime Utilization Clients Sessions

Data Explorer Dashboard Exporting Raw Data Using the SCI Virtual Machine Command Line Interface

TABLE 9 Measures (continued)

Measure name	Description	Supported Data Sources
userTxBytes	Traffic volume, which is transmitted by AP (Access Point) in IEEE 802.11 MAC Service Data Unit (MSDU) data frames. This includes all unicast, multicast and broadcast traffic.	 Applications Network traffic Airtime Utilization Clients Sessions

PII Hashing

•	Hashing Data-Source Attributes	.1	51
•	Template File for PII Hashing	. 1	51

Hashing Data-Source Attributes

You can use the SCI VM command line interface to hash various data-source attributes.

Follow these steps to hash the attributes you are interested in.

- 1. Log in to your SCI VM.
- Navigate to the following directory: 2.

/storage/rsa-api/hashing/configs

- 3. Locate the file called config.template.yml
- Open the file using a text editor. 4.

The file contains instructions on what to do. You will need to either comment out certain lines or un-comment certain lines in the file, as directed, and specify the desired data-source attributes that you want hashed.

- 5. Once you have made the changes in the config.template.yml file, be sure to save it under a different name that is meaningful to you, while leaving the original config.template.yml file in tact for future use.
- Run the following command to perform hashing on the desired attributes: 6.

sudo docker exec -it rsa-api yarn configure-hashing <config-file-name>

where <config-file-name> is the name of your customized .yml file.

Template File for PII Hashing

Use the example config.template.yml file to copy and edit according to the desired attributes to hash.

```
# This is an example configuration file for PII data hashing in YAML format.
# Lines starting with '#' are comments. Refer to http://www.yaml.org for detailed specification.
# Please change values accordingly. It expects content in the following format:
# <datasource>: [<attribute>]
# where <datasource> refers to the data source name and <attribute> refers to the field to be hashed.
# Multiple attributes are separated by comma. Note that only data sources with `clientMac` dimension
# are hashable.
# !!! WARNING !!!
# Values of attributes given in this configuration file will be hashed to meaningless strings and
# they are NOT reversible. Resetting hash for those attributes only affect future values.
# Version: 1.0
          18 Jan 2018
# Date:
# Example:
example: ['attr1', 'attr2', 'attr3']
# Hash `clientMac`, `hostname`, `username` and `clientIp` for data source `binnedSessions`
```

#

#

#

Uncomment to apply changes. You may add or remove one or more attributes. #binnedSessions: ['clientMac', 'hostname', 'username', 'clientIp'] # Hash `clientMac` for data source `binnedAvc` # Uncomment to apply changes. You may add or remove one or more attributes. #binnedAvc: ['clientMac']

Hash `clientMac`, `hostname`, `username` and `clientIp` for data source `sessionsSummary` # Uncomment to apply changes. You may add or remove one or more attributes. #sessionsSummary: ['clientMac', 'hostname', 'username', 'clientIp']

Admin Dashboard

•	Admin Console	153
	Status and Update	
	Diagnostics	
	Settings	
	License	
	PCI Profiles	
	Users and Roles	

Admin Console

The Admin pages provide options for configuring SCI's administrative settings, performing diagnostics and system updates, and defining user roles and creating resource groups.

The Admin section is divided into the following pages:

- Status and Updates
- Diagnostics
- Settings
- License
- PCI
- Users & Roles

NOTE

For information on SCI installation, refer to the SCI Installation Guide, available from support.ruckuswireless.com

Status and Update

The Status & Update page lists the active SCI nodes, alerts you to any important notifications, and displays the current firmware version.

Nodes

The following illustration shows an example of the Status and Update screen when the **Node** tab is selected.

FIGURE 165 Status and Update Screen with Node Tab selected

- Status	& Update				
Nodes	Notifications	Update			
10	>	Node IP	Node Token	Node Type	Node State
data-3b	62d48d	10.0.0.168	6805196779	data	•
data-96	a3c9fc	10.0.240	4499070968	data	•
master-ei	7d3ce7a	10.0.2.162	3843798771	master	•

The Nodes section lists the active SCI nodes, and includes the following information on each node:

- Node ID: The ID number of the node
- **Node IP:** The IP address of the node
- **Node Token:** The Token number or SSH password of the node. This token number is required for a node to connect to another node. The number is available on the UI so that it is a ready reference to the user who wants to connect to a specific node.
- **Node Type:** The type of node. There are two types of nodes, namely master and data nodes. One or more data nodes are required as the system scales and grows larger.
- **Node State:** The node state is green when in use and red when disconnected and not in use.

Notifications

The following illustration shows an example of the Status and Update screen when the **Notifications** tab is selected.

FIGURE 166 Status and Update Screen with Notifications Tab selected

dmin -	Status	& Update	Э			
Nod	les	Notifica	tions	Update		
Level	Source	Туре		Mess	ago	Details
Critical	Node	Disk Usage	Y	our data node (IP: 10.0.0.168)	has reached 82% disk usage	Please refer to the Notifications Section in the User guide
Critical	Node	Disk Usage	Yo	ur master node (IP: 10.0.2.162) has reached 85% disk usage	Please refer to the Notifications Section in the User guide



If any notifications are present in this section of the SCI UI, a red notifications icon disappears in the upper-right portion of the SCI user interface next to the admin icon. (This icon disappears once the issue has been handled.)

NOTE

The only current "level" of notification at this time is *critical*, as shown in the screen above.

In addition, an email notification is sent out every 15 minutes to the email address provided in the My Account screen > Profile section of the SCI UI, which you open by clicking on the admin icon in the upper right of the SCI user interface, as shown in the following figure.

FIGURE 167 Email Address to Receive Notifications

			0 🚊
My Account			My Account Logout
Profile			
	Username:	admin	
	Email:	user1@ruckuslbs.com	
		This email will receive alerts regarding the system	
		Update Profile	

To receive notifications, you must also be sure that you have configured the outgoing mail server (SMTP) in the Admin dashboard > Settings section.

The following table lists examples of the two types of notifications that you could receive, along with possible solutions.

Notification Description Action(s) to Try Your master node (IP: 10.x.y.1) has reached 83 This notification appears whenever one of the Reduce the data retention period by percent disk usage. SCI nodes has a disk usage of 80% or more. going to the **Admin > Settings** This notification indicates that you could screen, "Data Retention" section. potentially run out of disk space on SCI. For more information, refer to the Settings on page 158 section, "Data Retention" portion. Copy your data to a new SCI with more disk space. If you need assistance, contact Ruckus support. Add new data nodes. Because the Hadoop Distributed File System (HDFS) replication factor is two, you need at least two data nodes in your SCI cluster. Go to Admin > Diagnostics > Spark Master. Your Spark cluster (Spark master IP: 10.x.y.2) This notification appears when an ETL Spark was unable to accept a job submission. job is taking a long time, and SCI is unable to Search for "Running Applications." If this submit the next job. This could mean that SCI section shows more than one job running, is unable to ingest data from the controllers check again in a half hour. If there is still more and that SCI is unable to continue to collect than one job shown running in the "Running Application" section, contact Ruckus customer data. support to ensure that you are not losing data.

TABLE 10 Notifications and Possible Corrective Actions

Update

The following illustration shows an example of the Status and Update screen when the **Update** tab is selected.

FIGURE 168 Status and Update Screen with Update Tab selected

Admin - Status & Update			
Node	18	Notifications	Update
c	urrent Versior	v5.0.0-rc.2	
, i	Latest Version	v5.0.0-rc.2	
		Check for Updates	

The Update section contains the details of the current version of SCI that you are running and the latest version of SCI that is available (if any).

Diagnostics

The Diagnostics admin page provides links to external tools that can be used to troubleshoot issues in database storage and data transformation.

The following links to diagnostic tools are provided:

• **Data ingestion and ETL jobs:**The Spark Master UI provides details of workers, running applications, running drivers, completed applications and completed drivers.

For more details, see http://spark.apache.org/docs/latest/spark-standalone.html

• **Data lake and raw data storage:**The HDFS or Hadoop system provides details of datanodes, datanode volume failures, snapshot summaries, startup progress, and utilities such as logs and browsing the file system.

For more details, see https://en.wikipedia.org/wiki/Apache_Hadoop

• **Data warehouse:**The Druid Coordinator or Console provides details of the data sources, cluster and indexing services.

For more details, see http://druid.io/docs/latest/design/coordinator.html

FIGURE 169 Diagnostics

Diagnostics

Data ingestion and ETL jobs Spark Master UI

Data lake and raw data storage HDFS

Data warehouse Druid Coordinator Druid Overlord Admin Dashboard Settings

Settings

The Settings area of the Admin Console is the location to store and update settings required for various features of SCI.

Controller Settings

FIGURE 170 Controller Settings

ystems	5				× Delete + Ac
0	System ID	Туре	URL	User	Last Seen
	SystemID1	SmartZone (SCG/SZ/vSZ < 3.5)	149pe-180.115-80.177.8x40	admin	2 minutes ago
	SystemID2	SmartZone (SCG/SZ/vSZ >= 3.5)	100pt-100.000.110.111.011.010	admin	
	SystemID3	SmartZone (SCG/SZ/vSZ >= 3.5)	19px/98.70.27.10.8443	admin	3 months ago
8	SystemID4	SmartZone (SCG/SZ/vSZ < 3.5)	100pe-1108-104-105-110440	sci_mon	2 minutes ago
a)	SystemID5	SmartZone (SCG/SZ/vSZ < 3.5)	Manufacture straights (which show one water	ruckus.sci	2 minutes ago
3	SystemID6	SmartZone (SCG/SZ/vSZ < 3.5)	1993au 1180-001 1780-001 001 001	rsa-agent	2 minutes ago
9	SystemID7	SmartZone (SCG/SZ/vSZ < 3.5)	145pan-152, 11, 116, 252, 2821	admin	2 minutes ago
3	SystemID8	ZoneDirector (Poll, all ZD versions)	100pm/52.11.116.202.0000	admin	3 minutes ago
0	SystemID9	ZoneDirector (Poll, all ZD versions)	14(par./52.11.198.000)	admin	3 minutes ago
9	SystemID10	SmartZone (SCG/SZ/vSZ >= 3.5)	August (12), 11, 116, 202, 5052	admin	4 minutes ago
9	SystemID11	SmartZone (SCG/SZ/vSZ < 3.5)	Magaza (1988, 1987, 112, 128-128-12	admin	20 days ago
	SystemID12	SmartZone (SCG/SZ/vSZ < 3.5)	100pper/102.001.000.1000.00000	admin	5 months ago

To add a controller, click the **Add** button in the upper right of the Settings screen; a drop-down menu appears for you to select the controller type, as shown in the figure below.

FIGURE 171 Adding a New Controller Popup

New System	×
System ID:	
Туре:	SmartZone (SCG/SZ/vSZ < 3.5)
URL:	ZoneDirector (Poll, all ZD versions) ZoneDirector (Push, ZD >= 9.13)
Backup URL:	SmartZone (SCG/SZ/vSZ < 3.5) SmartZone (SCG/SZ/vSZ >= 3.5)
Username:	
Password:	
	Create

NOTE

For instructions on adding the different types of controllers as well as instructions on deleting or editing controllers, refer to the *SmartCell Insight Installation Guide*, "Configuring SCI" chapter, "Adding and Managing Controllers" section.

SMTP Settings

SCI requires certain settings to enable different areas of the functionality. These settings are listed in this section.

FIGURE 172 SMTP Settings

Outgoing Mail Server (SM	TP)
Host:	email-smtp.us-west-2.amazonaws.com
Port:	587
Username:	User123
Password:	Leave blank to remain unchanged
Encryption:	STARTTLS
From Email:	rsa@ruckuslbs.com
	Update Send Test Email

You can configure the SMTP mail server to send or receive e-mail messages to or from SCI. The SMTP settings section contains the configuration details:

- **Host**: Enter the name of the host. The system now checks the SMTP connectivity and displays an error if the authentication is not successful.
- **Port**: Enter the port number.
- **Username**: Enter the user name required to access the SMTP mail server.
- **Password**: Enter the password required to access the SMTP mail server.
- **Encryption**: Select the encryption method from the drop down list. You can also disable the encryption by selecting **Disabled** from the drop down list.
- From email: Enter the email ID that the messages are sent from.

To save your changes, click **Update**.

You can test your settings by sending a test email. Follow these steps:

1. After you have configured SMTP and saved your changes, click **Send Test Email**. The following popup should appear:

FIGURE 173 Send Test Email Popup

Send Test Email	×
Email:	ops@ruckuslbs.com
	Send Cancel

2. Click Send.

3. Check that you receive an email to confirm that SMTP is working properly. The subject of the email that you receive should be: "Test email from your Ruckus SmartCell Insight." The body of the email should be: " Hi there, this is a test email."

NOTE

You should receive the email almost instantly. The email will be sent to the email address that is configured in the My Account screen > Profile section, which you open by clicking on the admin icon in the upper right of the SCI user interface, as shown in the following figure:

FIGURE 174 Email Address to Receive SMTP Test Email Reply from Ruckus

My Account	
Profile	
Email:*	user1@ruckuslbs.com
	This email will receive alerts regarding the system
Username:*	admin
First Name:*	First
Last Name:*	Last
	Update Profile

Data Retention

You can configure the time, in months, that you want SCI to retain all your raw and indexed data.

By default, this setting is 12 months, as shown in the screen below:

FIGURE 175 Data Retention section of Admin Dashboard

Data Retention		
Period (months):	t 12 Update	

This means that SCI will delete any data older than 12 months. This action takes place on the 1st of each month.

If you want to change the data-retention time, follow example the steps below:

1. Slide the bar to the desired time in months (from 1 to 60) for which you want to retain data. For example, if you want to retain data for 22 months, slide the bar as follows:

FIGURE 176 Retaining Data for 22 Months

Data Retention			
Period (months):	0	22	
	Update		

2. Click **Update**. A confirmation popup appears:

FIGURE 177 Data Retention Confirmation Popup window

Update Data Retention Period	×
A scheduled task will run on the 1st of each month to prune data older than the retention period. Are you sure you want to update the data retention period to 2	
Confirm	Cancel

3. Click **Confirm**. SCI will now flush data every 22 months, starting on the first of the upcoming month.

NOTE

Once data is deleted from SCI, the data cannot be recovered.

Instantly Pruning Old Data

If you need to purge data immediately instead of waiting until the first of the month, run the following script as root user: **sudo /root/cronscripts/prune-data.sh**

The length of time that the script runs depends of the amount of data to remove. Any data older than the data-retention period specified in **Admin > Settings** of the SCI user interface is immediately purged.

Authentication Tab on the SCI UI

The Authentication tab of the **Admin > Settings** screen lets you set whether you want local SCI users or external AAA server users to authenticate to SCI. You can also add new external servers from the Authentication tab. The following figure shows this tab if there are already some configured external servers (the IP addresses are just example values):

FIGURE 178 Authentication Tab Main Page Example

Systems	Outgoing Mail	Server Da	ata Retention	Authentication					
hentication Type	e: Local	T							
-									
pdate									
pdate									
	r Configurations								
ernal Server	r Configurations								
ernal Server		Config Type	Auth Type	Primary Server	Primary Port	Secondary Server	Secondary Port	Status	
ternal Server	× Delete	Config Type RADIUS	Auth Type PAP	Primary Server 35.193.55.1	Primary Port 1812	Secondary Server	Secondary Port	Status	

By default, only users local to the SCI are authenticated.

Before you add external servers, there are certain steps you need to perform on the external server. Depending on whether the external server is RADIUS, TACACS+, or Cisco ACS, see the subsections below for how to add users, roles, and resource groups.

NOTE

If you add users and roles via external server configuration, this is indicated in the Figure 209 on page 191.

Configuration to Perform on External AAA RADIUS Server:

- 1. Add the SCI server as a RADIUS client, specifying the AAA client name, IP address, shared secret, and other parameters.
- 2. If you are using the Ruckus dictionary file for vendor-specific attributes, install a new Ruckus dictionary file (or update the existing file) with the following attributes:
 - ATTRIBUTE, Ruckus-SCI-Role, 200, string
 - ATTRIBUTE, Ruckus-SCI-Resource-Group, 201, string
- 3. Configure an authentication policy with the following objectives:
 - Allow authentication from the SCI server.
 - Define the valid users and user groups.
 - Configure vendor-specific return attributes for the Ruckus-SCI-Role and Ruckus-SCI-Resource-Group, which maps the RADIUS user into SCI privilege sets.

NOTE

As with SCI, one user is associated with one resource group and one role only. There are three roles.

Sample Configuration Using FreeRADIUS for External AAA RADIUS Authentication:

- 1. Using SSH, log in to the FreeRADIUS server.
- 2. Enter CLI mode.
- 3. AAA admin should add two new attributes to dictionary.ruckus as shown below:

vi /usr/share/freeradius/dictionary.ruckus

ATTRIBUTE	Ruckus-SCI-Role	200	string
ATTRIBUTE	Ruckus-SCI-Resource-Group	201	string

4. Add all users, their roles and their resource groups:

```
vi /etc/freeradius/3.0/users
aaaadmin Cleartext-Password := "admin123"
    Reply-Message = "Hello Admin",
    Ruckus-SCI-Role = admin,
    Ruckus-SCI-Resource-Group = Default
aaagroupadmin Cleartext-Password := "admin123"
    Reply-Message = "Hello Group Admin",
    Ruckus-SCI-Role = groupadmin,
    Ruckus-SCI-Role = groupadmin,
    Ruckus-SCI-Resource-Group = AAA_MLISA
aaaview Cleartext-Password := "admin123"
    Reply-Message = "Hello User",
    Ruckus-SCI-Role = view-only,
    Ruckus-SCI-Resource-Group = AAA_VIDE054
```

5. Configure the SCI server IP that you wish to authenticate with the FreeRADIUS server:

```
vi /etc/freeradius/3.0/clients.conf
client all {
    ipaddr = 0.0.0.0/0
    secret = testing123
}
```

6. After adding the above configuration, restart FreeRADIUS by running the following command:

service freeradius restart

Configuration to Perform on External AAA TACACS+ Server:

- 1. Identify the TACACS administrators who need SCI administration privileges, and then create an admin group (or reuse an existing group).
- 2. Assign the SCI administrators to the SCI admin group on the TACACS server.
- 3. Within the TACACS SCI admin group, configure the SCI service (service = sci-resource-group) and map the Ruckus RBAC attributes (e.g. Ruckus-SCI-Role = admin; Ruckus-SCI-Resource-Group = Default).

Sample Configuration For External AAA TACACS+ Authentication:

- 1. Using SSH, log in to the TACACS+ server.
- 2. Enter CLI mode.

```
3. Open vi and type:
```

```
/etc/tacacs+/tac_plus.conf
```

4. Create a group:

```
group = admins {
}
```

5. Add a service, role, and mgmt-devicegroups to the group you created above, as follows:

- 6. If needed, create additional groups and add a service, role, and mgmt-devicegroups to the group, as you did previously.
- 7. Create a user, associate the user with the correct group, and create a user password, as shown below:

```
user = aaaadmin {
    member = admins
    global = cleartext admin123
}
```

8. The final configuration should now appear as follows:

```
vi /etc/tacacs+/tac plus.conf
group = admins {
        service = sci-resource-group {
            Ruckus-SCI-Role = admin
            Ruckus-SCI-Resource-Group = Default
        }
}
user = aaaadmin {
      member = admins
       global = cleartext admin123
}
group = groupadmins {
        service = sci-resource-group {
            Ruckus-SCI-Role = groupadmin
            Ruckus-SCI-Resource-Group = AAA MLISA
        }
}
user = aaagroupadmin {
       member = groupadmins
       global = cleartext admin123
}
group = view-only {
        service = sci-resource-group {
            Ruckus-SCI-Role = view-only
          Ruckus-SCI-Resource-Group = AAA VIDE054
        }
}
user = aaaview {
   member = view-only
    global = cleartext admin123
}
```

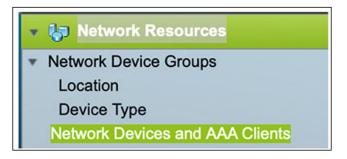
9. Restart the TACACS+ server by running the command:

service tacacs+ restart

Configuration to Perform on Cisco ACS Server:

1. To configure ACS to accept connections from SCI, click **Network Devices and AAA Clients** on the Cisco ACS configuration screen shown below:

FIGURE 179 Invoking Network Devices and AAA Clients Configuration



- 2. In the Network Devices and Clients screen (shown below):
 - a. Enter the name.
 - b. Enter the IP address of the SCI.
 - c. Select either RADIUS or TACACS+ from the drop-down list.
 - d. Click Submit.

Name: CIS	CO ACS Firewall			
Description:				
Network Device Gro	oups			
Location	All Locations	Select		
Device Type	All Device Types	Select		
IP Address		Authentication Options		
 Single IP Add 	Iress IP Subnets IP Range(s)	Shared Secret:	TACACS+	
o IP: 10.137.11.4	E	testing123		
·		Hide		
		Single Connect Device		
		Legacy TACACS+ Single Connect Support		
		TACACS+ Draft Compliant Single Connect Support		
		-	RADIUS 🗹	
		Shared Secret:		
		o testing123		
		Hide		
		CoA port: 1700		
		Enable KeyWrap		
		Key Encryption Key:		
		Message Authenticator Code Key:		
		Key Input Format ASCII		

FIGURE 180 Network Devices and Clients Configuration Screen

- 3. To create AAA users, click **Users** in the left pane of the Create Users screen (shown below), and do the following:
 - a. Enter the Name.
 - b. Enter the password.
 - c. Confirm the password.
 - d. Click Submit.
 - e. Repeat the preceding steps to add more users.

FIGURE 181 Creating Users Configuration Screen

t i	Users and Identity Stores > 1	indical reprinty order	es - opers - oreere			
6-	General					
S Users and Identity Stores	O Name: 88	admin	Status: Enal	bled 🖸 \Theta		
lentity Groups	Description:					
ternal Identity Stores	o Identity Group: All	Crewes		Select		
User: Hosts	Email	Groups		Select		
ternal Identity Stores	Address:					
DAP						
Active Directory	Account Disable					
RSA SecurID Token Servers RADIUS Identity Servers	Disable Account if	Date Exceeds: 20)19-Apr-02 🔛 (yyy)	-Mmm-dd)		
ertificate Authorities			and an deside of a strength			
ertificate Authentication Profile	Disable account af	er 3 succes	ssive failed attempts			
lentity Store Sequences						
	Password Hash					
	Enable Password H	lash	Applicable only for Authentication type	Internal Users to store pas s CHAP/MSCHAP will not	sword as hash. work if this option is enabled.	
					rd is reconfigured using change password option.	
	Password Lifetime					
	Password Never E	xpired/Disabled:	Overwrites user a	ccount blocking in case pa	ssword expired/disabled	
	Password Informatio	n			Enable Password Information	
	Password must:				Password must:	
	 Contain 4 - 32 	characters			 Contain 4 - 128 characters 	
	Password Type:	Internal Users		Select	Enable Password:	
	o Password:				Confirm	
		-	T~		Password:	
	 Confirm Password: 		T~			
	Change passw	ord on next login				
	User Information					
		onal identity attribut	tes defined for user			

- 4. Install a new Ruckus dictionary file or update an existing dictionary with the following attributes to create the Ruckus-SCI-Role (see figure below):
 - a. Attribute: Ruckus-SCI-Role
 - b. Vendor Attribute ID: 25053
 - c. Attribute Type: String
 - d. Click OK.

FIGURE 182 Creating the Ruckus-SCI-Role

> 🖏 🛛	System Administration > Cor	nfiguration > Dictionaries > Protocols > RADIUS > RADIUS VSA > Ruckus > Create
- La	General	
. 🎬	Attribute: Rucku	s-SCI-Role
2		
1	Description:	
	RADIUS Configuratio	n
System Administration	Vendor Attribute ID:	25053
 Dictionaries 	Direction:	вотн
* Protocols	Multiple Allowed:	False
 RADIUS RADIUS IETF 		
* RADIUS VSA	Include attribute log	In
Ascend		
Cisco	Attribute Type Attribute	
Cisco Airespace	Type: Str	ing 😌
Cisco Aironet Cisco BBSM		
Cisco VPN 3000/ASA/PIX 7.)		
Cisco VPN 5000	Attribute Configuration	
Juniper	Policy Condition Di	
Microsoft Nortel (Bay)		
RedCreek	e = Required fields	
Ruckus		
US Robotics		
TACACS+		

- 5. Install a new Ruckus dictionary file or update an existing dictionary with the following attributes to create the Ruckus-SCI-Resource-Group (see figure below):
 - a. Attribute: Ruckus-SCI-Resource-Group
 - b. Vendor Attribute ID: 25053
 - c. Attribute Type: String
 - d. Click OK.

FIGURE 183 Creating the Ruckus-SCI-Resource-Group

> đi	System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA > Ruckus > Creat
> 🕼 > 🎉 > 🎭	General Attribute: Ruckus-SCI-Resource-Group
> 🎭 > 💼	RADIUS Configuration
System Administration Dictionaries Protocols RADIUS RADIUS IETF RADIUS VSA Ascend Cisco Cisco Airespace Cisco Aironet Cisco BBSM	 Vendor Attribute ID: 25053 Direction: BOTH © Multiple Allowed: False © Include attribute in log Attribute Type Attribute Type: String ©
Cisco VPN 3000/ASA/PI Cisco VPN 5000 Juniper Microsoft Nortel (Bay) RedCreek Ruckus	Attribute Configuration Add Policy Condition Policy Condition Display Name: C = Required fields

6. Go to the Create RADIUS Authorization Profiles screen (shown below).

FIGURE 184 Create RADIUS Authorization Profiles Screen

	General	Common Tasks	RADIUS Attributes	
Users and Identity Stores	• Name:	RadiusAdmin		
Policy Elements				
Session Conditions	Descrip	tion:		
Date and Time	🗢 = Require	ed fields		
Custom				
 Network Conditions 				
Authorization and Permissions				
 Network Access 				
Authorization Profiles				
 Device Administration Shell Profiles 				
Command Sets				
Continuity Cotto				
Named Permission Objects				
Named Permission Objects				
Access Policies	-			

- a. Enter **RadiusAdmin** in the Name field.
- b. In the RADIUS Attributes tab, select RADIUS-RUCKUS from the Dictionary Type drop-down list, then, for the RADIUS Attribute, select Ruckus-SCI-Role (see screen below), and enter **admin** for the Attribute Value.

A My Workspace	Policy Elements > Authorizati	on and Permissions > Netw	ork Access > Authorization	19 😐 😐	0			Cisco Secure ACS			
Network Resources	General Common T	sks RADIUS Attribute		① A https://10.137.11.44/acsadmin/VendorSpecificAttributeLPInputAction.do							
Users and Identity Stores	Common Tasks Attribu			RADI	US Dictionary					Showing 1-41 of 41	
Sy Policy Elements	Attribute		Val	10	and the second	Danas					
Session Conditions				Filter	91	Match if:		🖸 Go 🕶			
Date and Time Custom				0	Attribute Nuckus-CDH-I YM	٤.	1D +	Type Unsigned Integer 32	Direction BUTH	Multiple / true	
Network Conditions				0	Ruckus-Session-T	ype	125	Enumeration	BOTH	true	
Authorization and Permissions • Network Access				0	Ruckus-Accounting	g-Status	126	Enumeration	BOTH	true	
Authorization Profiles				- 0	Ruckus-Zone-Id		127	String	BOTH	true	
Device Administration	Manually Entered Attribute		lype Val	0	Ruckus-Auth-Serv	er-ld	128	String	BOTH	true	
Shell Profiles Command Sets	Addiouve		ype va		Ruckus-Utp-Id		129	String	BOTH	true	
 Named Permission Objects 					Ruckus-Wispr-Rec	Sirect-Policy	132	String	BOTH	true	
🔂 Access Policies				0	Ruckus-Eth-Profile	⊳ld	133	Unsigned Integer 32	BOTH	true	
Monitoring and Reports					Ruckus-Zone-Nam	10	134	String	BOTH	true	
System Administration				0	Ruckus-Wlan-Nam	10	135	String	BOTH	true	
	Add A Edit V	Replace A Dele	ste	0	Ruckus-Admin-Ro	le .	136	String	BOTH	true	
	Dictionary Type:	RADIUS-Ruckus	O	0	Ruckus-Resource-	Group	137	String	BOTH	true	
	o RADIUS Attribute:		Select		Ruckus-SCI-Role	7	200	String	BOTH	true	
	Attribute Type:			0	Ruckus-SCI-Reso	urce-Group	201	String	BOTH	true	
	Attribute Value:	Static	0							10 30	
	0			OK	Cancel						
	e = Required fields										

FIGURE 185 Selecting Ruckus-SCI-Role

c. Still in the RADIUS Attributes tab, for the RADIUS Attribute, select Ruckus-SCI-Resource-Group (see screen below), and enter **Default** for the Attribute Value.

B Network Resources					-			VICTOR OF THE OWNER OF	Cisco Secur	A CONTRACTOR OF THE OWNER OF	-	
	General Common Ta	sks RADIUS Attrit	outes	1	I 🖗	https://10.137.1	1.44/acsadmin		cificAttributeLP			
Stores and Identity Stores	Common Tasks Attribut	05			RADI	IS Dictionary					St	nowing 1-41 of 4
Policy Elements	Attribute		Туре	Value	Filter:	(Match if:		Go			
Session Conditions Date and Time						Attribute Ruckus-CDR-TYP		1D -	Type Unsigned in	Direc	tion	Multiple A
Custom Network Conditions					0	Ruckus-Session-		125	Enumeration		отн	true
Authorization and Permissions					0	Ruckus-Accountin		126	Enumeration		отн	true
Network Access Authorization Profiles					0	Ruckus-Zone-Id		127	String		отн	true
Device Administration	Manually Entered Attribute		Туре	Value	Ó	Ruckus-Auth-Ser	ver-ld	128	String	B	отн	true
Shell Profiles Command Sets			1990	1000	0	Ruckus-Utp-Id		129	String	B	отн	true
 Named Permission Objects 					0	Ruckus-Wispr-Re	direct-Policy	132	String	B	отн	true
Access Policies					0	Ruckus-Eth-Profil	le-ld	133	Unsigned In	teger 32 BC	отн	true
Monitoring and Reports					0	Ruckus-Zone-Na	me	134	String	B	отн	true
System Administration					0	Ruckus-Wlan-Nar	me	135	String	B	отн	true
	Add A Edit V	Replace / 0	Delete		0	Ruckus-Admin-R	ole	136	String	B	отн	true
	Dictionary Type:	RADIUS-Ruckus		•	0	Ruckus-Resource	p-Group	137	String	84	отн	true
	o RADIUS Attribute:			Select	0	Ruckus-SCI-Role		200	String	B	отн	true
	Attribute Type:				•	Ruckus-SCI-Reso	urca-Group	201	String	B	отн	true
	Attribute Value:	Static		0								141 040
	•				OK	Cancel						
	o = Required fields											

FIGURE 186 Selecting Ruckus-SCI-Resource-Group

d. Check that the Create RADIUS Authorization Profiles screen now shows the added attributes:

	General Common Tasks RADIU Common Tasks Attributes Attribute	JS Attributes Type	Value	
Policy Elements Session Conditions Date and Time	Common Tasks Attributes		Value	
Session Conditions Date and Time		Туре	Value	
Date and Time				
Network Conditions Authorization and Permissions Network Access				
Authorization Profiles	Manually Entered			
Shell Profiles	Attribute	Туре	Value	
Command Sets Named Permission Objects	Ruckus-SCI-Role Ruckus-SCI-Resource-Group	String String	admin Default	
Access Policies				
Monitoring and Reports				
System Administration				
	Add A Edit V Replac	e A Delete		
	Dictionary Type: RADIUS-Ru	uckus	0	
	o RADIUS Attribute:		Select	
	Attribute Type:			
	Attribute Value: Static		O	
	o			
	e = Required fields			

FIGURE 187 Added Attributes Now Appearing on Authorization Profiles Screen

- e. Click Submit.
- f. Repeat the steps you followed when you created the RadiusAdmin authorization profile to create profiles for RadiusGroupAdmin and RadiusView, listed on the screen below:

FIGURE 188 RadiusGroupAdmin and RadiusView Profiles Must Also Be Created

► 🖓 My Workspace	Policy Element	ts > Authorizatio	n and Per	missions > Ne	twork Acces	s > Auth	orization Profiles
Network Resources	Authorizat	ion Profiles					
Users and Identity Stores	Filter:		Match if:	0		Go	~
🔹 🎭 Policy Elements				2 			
 Session Conditions Date and Time Custom Network Conditions Authorization and Permissions Network Access Authorization Profiles Device Administration Shell Profiles Command Sets Named Permission Objects Monitoring and Reports System Administration 		ne mit Access liusAdmin liusGroupAdmi liusView		cription			

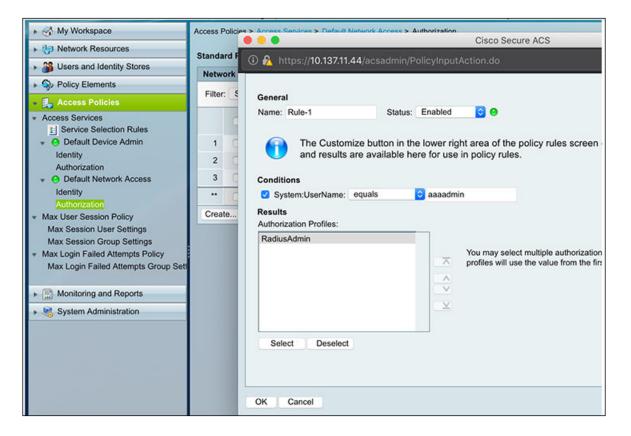
- 7. Create access policies for RADIUS:
 - a. Go to **Authorization**, click the Customize button on the far right, then select **System:Username**, and click **OK**:

FIGURE 189 Selecting System:Username Customization

Hy Workspace Hy Network Resources	Access Po	licies > A	ccess Services > Default Network Acce	ss > Authorization				
	Standard	Policy	Exception Policy					
 Stores 	Networ	k Acci		Mozilla Firefox		12		
Policy Elements	Filter:	Ctatur	0.0					
Access Policies	rindr.	Otatio	① A https://10.137.11.44/act	admin/PolicyInputAction.do	⊠ ☆ ≡			
Access Services Service Selection Rules		•	Customize Conditions Available:	Selected:		Profiles	Hit Count	
+ O Default Device Admin	1		ACS Host Name	System:UserName			0	
Identity	2		AD1:ExternalGroups Authentication Method	>	~	Admin	0	
Authorization	3		Authentication Status	<	A		0	
Identity			Compound Condition Device Filter				20	
Muthorization Max User Session Policy	Create	-1-	Device IP Address Device Port Filter	>>>>		2		Customize
Max Session User Settings Max Session Group Settings			Eap Authentication Method Eap Tunnel Building Method		×			
Max Login Failed Attempts Policy								
Max Login Failed Attempts Group Set								
Monitoring and Reports								
System Administration			OK Cancel					

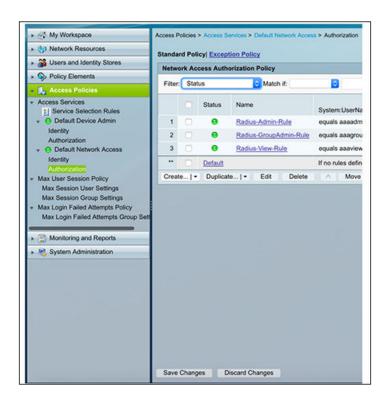
b. Click the **Create** button (just to the left of the popup shown below), then configure the popup with the values shown ("Name" can be anything you want), then click **OK**:

FIGURE 190 Configuring a Rule



c. Repeat the steps that you followed for creating **aaaadmin** to create policies for **aaagroupadmin** and **aaaview**, which are listed on the screen below:

FIGURE 191 Authorization Policy Screen



- 8. Create TACACS+ shell profiles:
 - a. Go to Shell Profiles (shown below):

FIGURE 192 Creating Shell Profiles

My Workspace	Policy Elements > A	uthorization and	Permissions	Device Adn	ninistration > Shell Profile	s > Create
Network Resources	Common Task	o Allebudoo				
Big Users and Identity Stores	Attribute	is Attributes	Requiremen	ıt	Value	
Solicy Elements						
Session Conditions Date and Time Custom Network Conditions Authorization and Permissions Network Access						
Authorization Profiles	Manually Ente	red				
Device Administration Shell Profiles Command Sets Named Permission Objects	Attribute		Requiremen	ıt	Value	
Access Policies						
Monitoring and Reports						
System Administration	Add A	Edit V	Replace /	Delete	Bulk Edit	
	Attribute:	Ruckus-SCI-F	Role			
	Requirement:	Mandatory	0			
	Attribute Value:	Static C				
	G = Required f	admin				Æ

- b. In the Attribute field, enter **Ruckus-SCI-Role**.
- c. For the Attribute value, enter **admin**.
- d. Click **Add**.
- e. In the Attribute field, enter **Ruckus-SCI-Resource-Group**.
- f. For the Attribute value, enter **Default**.
- g. Click Add.
- h. Check that both shell profiles have been added to the Shell Profile Create screen, shown below, then click **Submit**.

FIGURE 193 Shell Profile Create Screen

Network Resources	Common Tasks Attrib	dea.	
Stores	Attribute	Requirement	Value
Policy Elements			
Session Conditions Date and Time Custom Network Conditions Authorization and Permissions			
 Network Access 	Manually Entered		
Authorization Profiles	Attribute	Requirement	Value
Device Administration Shell Profiles Command Sets Named Permission Objects	Ruckus-SCI-Role Ruckus-SCI-Resource	Mandatory	admin Default
Access Policies			
Monitoring and Reports			
System Administration	Add A Edit Attribute: Requirement: Mand Attribute Static Value:	atory 🔁	Bulk Edit
	• = Required fields		

- 9. Configure access policies to enable TACACS+:
 - a. Go to **Default Device Admin > Authorization** (see the highlighted areas on the left pane of the screen below):

FIGURE 194 Configuring Access Policies

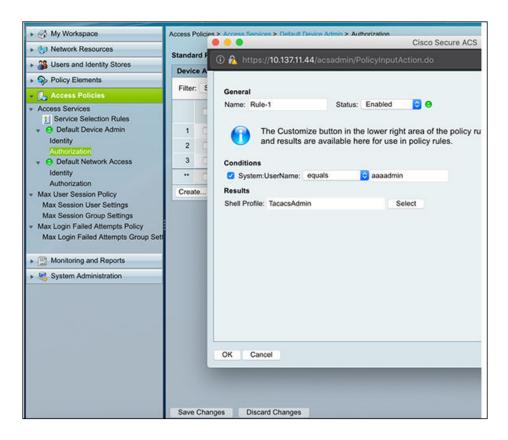
• 🚭 My Workspace	Access P	olicies	> Access 5	ervices > Delt	• • • •		illa Firefox		
the second	Standar	rd Poli	icyl Excep	tion Policy	Customize Conditions	paor nary -			
	Devic	e Adm	inistration	Authorizati	Available:	2	Selected:		
Policy Elements Access Policies	Filter	Stat	us	🖸 Ma	ACS Host Name AD1 ExternalGroups Authentication Method	->	System UserName	× 1	
Access Services			Status	Name	Authentication Status Compound Condition Device Filter	<		-	
O Default Device Admin	1			Bule-1	Device IP Address	>>		~	
Identity Autocation	2		•	Bule-2	Device Port Filter Eap Authentication Method	-		× .	
 Default Network Access Identity 	3	0	•	Bule:3	Eap Turnel Building Method Customize Results				
Authorization			Default		Available:		Selected:		
Max User Session Policy Max Session User Settings Max Session Group Settings Max Login Failed Attempts Policy Max Login Failed Attempts Group Set	Creat	e[*	Duplica	10_ * E	Command Sets		Shell Profile	*	Custon
Monitoring and Reports						44		×	
System Administration									
					OK Cancel				

b. Click the **Customize** button in the lower right of the screen to invoke the popup that is shown above, then select **System:Username**, then click **OK**.

10. Create an authorization rule:

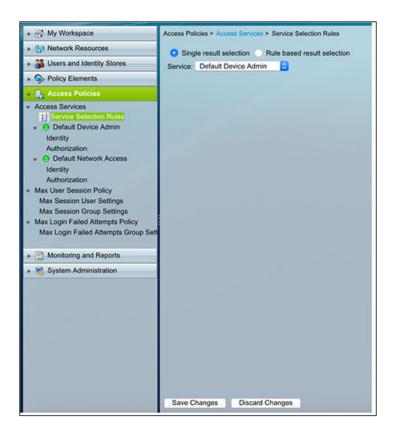
a. Still in the Authorization area, click **Create** to invoke the popup shown below:

FIGURE 195 Creating an Authorization Rule



- b. Enter a descriptive name of your choice in the Name field, and configure the settings with the values shown above to create a rule for **aaaadmin**.
- c. Click **OK**.
- d. Create rules for **aaagroupadmin** and **aaaview** by repeating the steps you just performed for **aaaadmin**.
- 11. Enable the AAA server by performing the steps listed below the figure:

FIGURE 196 Enabling the AAA Server



- a. Click Service Selection Rules (highlighted above in the left pane).
- b. For Service, select either:
 - "Default Device Admin" to enable TACACS+
 - "Default Network Access" to enable RADIUS
- c. Click Save Changes.

Adding an External Server:

1. To add an external AAA server for user authentication, navigate to **Admin > Settings** in the SCI UI, and click the Authentication tab:

FIGURE 197 Authentication Tab

Systems	Outgoing Mail	Server Data	a Retention	Authentication					
uthentication Type	Local	•							
Update									
Update									
	Configurations								
	Configurations								
xternal Server		Config Type	Auth Type	Primary Server	Primary Port	Secondary Server	Secondary Port	Status	
xternal Server	× Delete	Config Type RADIUS	Auth Type PAP	Primary Server 35.193.55.1	Primary Port 1812	Secondary Server	Secondary Port	Status	

NOTE

Config Name (in the figure above) is not used by SCI, but is a descriptive name that the administrator of the external server configured to help identify the server.

- 2. Click Create.
- 3. Configure the external server information, an example of which is shown below:

FIGURE 198 Creating an External Server

Name:*	us-server1			
Type:*	TACACS	\$ Protocol:*	ASCII	4
Primary Serv	rer			
Server:*	35.193.55.1			
Port:*	49	Secret:*		
Secondary S	Gerver 🛛			
Server:*				
Port:*	49	Secret:*		
Test Connec	tion			
Username:*	Testuser1	Password:*		
		O Primary	y 🧿 Secondary	Test

- Name: The name of the external AAA server that you can choose to activate.
- Type: RADIUS or TACACS+. Select the proper value for the external server.
- Protocol: For a RADIUS server, this value can be either PAP or CHAP. For a TACACS+ server, the only choice for protocol is ASCII. Make sure the value matches that of the external server.

NOTE

The protocol must be the same for the secondary server as for the primary server.

- Server: The IP address of the external server.
- Port: Must match the port being used for authentication on the external server. Default is 1812 for RADIUS and 49 for TACACS+.
- Secret: The secret key that has been configured on the server to allow communication between the server and SCI; *must match exactly* the secret that has been configured on the external server.

Test AAA Server Connection:

To test the AAA configuration, perform the following steps:

- a. Enter the username and password (used only for test-connection purpose) that are configured on the AAA server (RADIUS or TACACS+).
- b. Select "Primary" for validating the connection with primary-server details, then click Test.
- c. If secondary server details are provided, then select "Secondary" for validating the connection with secondaryserver details, then click **Test**.

NOTE

The secondary server is an optional standby server, which is tried only when the primary server is not reachable after 3 retries.

Selecting an External Server for User Authentication:

To select one specific external AAA server for SCI user authentication, follow these steps:

1. From the Authentication Type drop-down list, select External:

FIGURE 199 Selecting the External Authentication Type

Systems	Outgoing Mail	l Server Da	ta Retention	Authentication					
thentication Type:	External	•	External S	erver(s): Tacacs	*				
Jpdate									
dernal Server (Configurations								
	Configurations × Delete								
		Config Type	Auth Type	Primary Server	Primary Port	Secondary Server	Secondary Port	Status	
	× Delete	Config Type RADIUS	Auth Type PAP	Primary Server 35.193.55.1	Primary Port 1812	Secondary Server	Secondary Port	Status	
Create	× Delete Config Name					Secondary Server	Secondary Port	Status	

2. Click the External Server(s) drop-down list to view all configured external servers. The figure below shows such an example:

FIGURE 200 Configured External Servers in the Drop-Down List

Systems	Outgoing Mail	Server	Data Retention	Authen	tication					
thentication Type:	External	•	External	Server(s):	Tacacs	•				
					1.000					
Jpdate					Select					
Jpdate					Select Radius					
opdate sternal Server C	Configurations									
ternal Server C	Configurations				Radius					
ternal Server C		Config Type	Auth Type	Primar	Radius	Primary Port	Secondary Server	Secondary Port	Status	
ternal Server C	× Delete	Config Type RADIUS	Auth Type PAP		Radius Tacacs	Primary Port 1812	Secondary Server	Secondary Port	Status	

3. From this drop-down list, select the external server from which users must be authenticated. You can select only one such server. If a user is not associated with that server, that user cannot be authenticated and will not be able to log in to SCI.

Systems	Outgoing Mail	Server	Data Retention	Auther	ntication					
thentication Type:	External	•	External	Server(s):	Radius	۲				
Update										
	Configurations									
xternal Server C										
tternal Server C	Configurations									
tternal Server C		Config Typ	pe Auth Type	Primar	ry Server	Primary Port	Secondary Server	Secondary Port	Status	
kternal Server C	× Delete	Config Typ RADIUS			ry Server 93.55.1	Primary Port 1812	Secondary Server	Secondary Port	Status	

FIGURE 201 Selecting the External Server from the Drop-Down List

4. Once you have selected the desired external server ("Radius" in the example above), click **Update**. You will need to confirm a pop-up message that you wish to continue because all active sessions will be invalidated. At next login, the status "ACTIVE" appears for the corresponding external server, as shown below:

FIGURE 202 "ACTIVE" Appears in Status Column for Selected External Server

Systems	Outgoing Mai	l Server D	ata Retention	Authentication					
Authentication Type:	External	¥	External Se	erver(s): Radius	×				
Update									
Update									
Update External Server (Configurations								
External Server (Configurations * Delete								
External Server (Config Type	Auth Type	Primary Server	Primary Port	Secondary Server	Secondary Port	Status	,
External Server (× Delete	Config Type TACACS	Auth Type ASCII	Primary Server 35.193.55.1	Primary Port 49	Secondary Server	Secondary Port	Status	

5. (Optional) To edit or delete an external server, check the box for the server, then use the **Edit** or **Delete** buttons as desired.

NOTE

If you want to revert to only local SCI users being authenticated, select "Local" from the Authentication Type drop-down list, then click **Update**. You will need to confirm a pop-up message that you wish to continue because all active sessions will be invalidated.

Notes about the "admin" user:

The "admin" user is always authenticated locally and is a fallback user if the external server is not reachable for the admin to log in and make changes. The "admin" user cannot be deleted or renamed.

License

SCI supports a trial license that you can use to try out the product before you purchase it. SCI also supports a permanent SCI license.

SCI has a built in trial license that is valid for three months. You must update this license to the permanent license before the trial license expires to prevent you from being locked out of SCI.

NOTE

When your license has expired, you cannot log in to SCI. Instead, you receive a message that your trial license has expired, along with a link to the License page to upload your permanent license.

Follow these steps to upgrade to the permanent license:

- 1. In the SCI web UI, click **Admin > License**.
- 2. Generate a serial number for the SCI product.
- 3. Use the serial number to purchase and activate a license from the Ruckus support website. The Ruckus website provides a license file that you can download.
- 4. Upload this file to SCI on the License page. The following illustration is example of how the License Page appears, providing status of your licenses:

FIGURE 203 Page to Upload Your License and Obtain Status of Licenses

License				
Feature	Start	Expiration	Count	Notice
INSTANCE-SCI	Aug 16 2016 10:53	Perpetual License	1	SCI - Application Perpetual License
CAPACITY-SCI	Aug 16 2016 10:53	Perpetual License	1073741824	SCI WiFi analytics-1 AP lic. perpetual
SUP-SCI-EU	Aug 16 2016 10:53	Perpetual License	1	End User WatchDog Support for SCI, 1-year
Upload License				
Serial Number	XXXXXXXXXX			
File	Click here to select a file			
	Upload			

PCI Profiles

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

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

FIGURE 204 PCI Profiles Screen

+ Create & Edit X Delete					
	Name	SSIDs	Date	Compliance	ł
2	pci test bed	QA-RaikiH-MSP1-101, QA	May 22 2018 04:57	FAIL	
0	density	test-5g	May 17 2018 18:44	FAIL	
	both	DENSITY, QA-RaikiH-Web	May 17 2018 19:17	FAIL	
0	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 reports that have been run, the SSIDs on which each report has been run, the date of each report, and whether the overall report passed or failed the PCI compliance test. You can click on the red "Fail" or green "Pass" to observe the detailed report.

Creating a PCI Profile

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

Follow the steps below to create a PCI profile:

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

The **Create Profile** screen is displayed.

FIGURE 205 Creating a PCI Profile

	Name	Test report 15	
SSIDs	to Report	Search SSID Q	
Index	Question		
1.1.2	1949 1949	tain a network diagram documenting wireless connections to the CDE?	
.1.2	Do you main	tain a network diagram documenting wireless connections to the CDE?	
	Do you main Do you have		
.2.3	Do you main Do you have Do you chan roles?	a firewall in place that permits only authorized traffic between the wireless network and CDE?	f
2.3	Do you main Do you have Do you chan roles? Do you main devices)	a firewall in place that permits only authorized traffic between the wireless network and CDE?	f
.2.3 .1.1 .4	Do you main Do you have Do you chan roles? Do you main devices) Do you utiliz	a firewall in place that permits only authorized traffic between the wireless network and CDE? Ige all known encryption keys or passwords when anyone with knowledge about them leaves or changes tain a system inventory of hardware and software in scope for PCI? (Hint: SZ allows you to export a CSV list o	f

- 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 report, then click the box next to each desired SSID.

NOTE

When an SSID is selected for the PCI report, 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 report.

• Index/Question: Checkmark the compliance questions that you want included in your report. SCI will pull data directly from the controller to check the compliance of each question against the PCI Data Security Standard.

NOTE

Not all questions are shown in the screen example above.

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

The result of the report (Pass or Fail) appears in the list of PCI profiles on the main PCI Profiles screen, an example of which is shown in Figure 204 on page 186.

Opening and Downloading a PCI Profile Report

The PCI Profile report 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 report.

1. From the main PCI Profile screen, an example of which is shown in Figure 204 on page 186, click on either the green "Pass" or red "Fail" button, depending on the report you wish to view.

The report 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 206 PCI Report Example

pci test b	mpliance Report		
May 22 201			Overall Status: TAL
PCIID	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 frewalls 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.	MASS	
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.	MSS	
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(a) 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.	MASS	
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	INSS	
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 report.

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 207 Edit or Delete PCI Profiles

+ Create Sedit X Delete					
	Name	SSIDs	Date	Compliance	ł
2	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	
0	1st density	bugbash, test-5g, qa-pre.k	May 21 2018 04:00	FAIL	
	test2	testssid	May 22 2018 11:53	PASS	

Users and Roles

The Users and Roles page of the Admin dashboard allows you to define who can control the various wifi resources in your system.

At its most basic level, you perform the following steps to define who has control over these resources:

- 1. Create resource groups. For each group that you create, you select the Access Points, SSIDs, and other assets that you want to belong to that group. This procedure is described in Creating Resource Groups on page 192.
- 2. Create users, then give the user a role, then assign the user to an resource group. The Super Admin role automatically is assigned to all resource groups. This procedure is described in Creating Users and Roles on page 194.

Resource Groups

The following screen shows an example of several configured resource groups:

FIGURE 208 Resource Groups Screen

Group Name	Providence			
Group Name	Base of all the			
	Description	Associated Users	Created By	Last Edit Time
Default	Full access to all resource groups	2		Mar 09 2018 10:59
Dev Group	For RSC dev team	1		
Group 1		2	admin	Mar 09 2018 11:44
Group 2		2	admin	Mar 08 2018 09:29
Controller 1		2	admin	Mar 08 2018 09:33
Domain 1	Filter by domain	1	admin	Mar 08 2018 09:43
Zone 2		1	admin	Mar 08 2018 15:49
All Zones		3	admin	Mar 08 2018 09:48
Controller 2		1	admin	Mar 08 2018 10:08
Controller 3		2	admin	Mar 09 2018 10:54
	Group 1 Group 2 Controller 1 Domain 1 Zone 2 All Zones Controller 2	Group 1 Group 2 Controller 1 Domain 1 Filter by domain Zone 2 All Zones Controller 2	Group 1 2 Group 2 2 Controller 1 2 Domain 1 Filter by domain 1 Zone 2 1 All Zones 3 Controller 2 1	Group 1 2 admin Group 2 2 admin Controller 1 2 admin Domain 1 Filter by domain 1 admin Zone 2 1 admin All Zones 3 admin

A resource group is made up of your selection of a subset of the wifi assets available in SCI. The filters provided during resourcegroup selection allow you to select any systems, controllers, domains, zones, AP groups, SSIDs, or individual APs. A resource group allows the Super Admin to confine access for a group of users to a restricted set of wifi assets. Therefore, a resource group is equivalent to a tenant.

SCI contains a **Default** resource group. This group corresponds to the entire set of wifi assets. The **Default** resource group cannot be edited or deleted.

NOTE

SCI can support up to 2,000 resource groups.

Users and Their Roles

The following screen shows an example of several configured users and their roles, including those belonging to external AAA authentication servers:

FIGURE 209 Users and Roles Screen

Users	Resourc	e Groups							
Create 🖉	Edit X Delete								
	Email	Username	First Name	Last Name	Role	Resource Group	Created By	User Type	Last Login Ti 🕻
	nodata@test.com	nodata	no	data	View Only	dummy	admin	Local	Jan 11 2019
	scilocaladmin@	scilocaladmin	SCI	Local Admin	Super Admin	Default		Local	Jan 19 2019
	aaaadmin@exa	aaaadmin	FIRST	LAST	Super Admin	Default		External	Jan 18 2019
8	aaaview@exam	aaaview	FIRST	LAST	View Only	AAA_VIDEO54		External	Jan 14 2019
	aaagroupadmin	aaagroupadmin	FIRST	LAST	Admin	AAA_MLISA		External	Jan 14 2019

Users are uniquely defined by their email address and their username. and each user must be assigned to only one of three possible roles: Super Admin, Admin, and View Only. The following figure shows the access rights of each role.

FIGURE 210 Access Rights for Each User Role

	View Data	Manage Saved Filters	Manage Schedules	Manage Users	Manage Resource Groups	Manage Cluster
Super Admin	~	~	~	~	~	~
Admin	~	~	~	~	×	ж
View Only	~	ж	ж	×	×	×

Note the following information about the Super Admin and Admin roles:

- Super Admin: This role can be assigned *only* to the **Default** resource group. The Super Admin has full access rights to all functionality in SCI. The Super Admin is the only role that can exist within the default resource group.
- Admin: This role exists within a resource group. However, a resource group *can* exist without anyone assigned to the role of Admin.

Creating Resource Groups

You can create resource groups and then assign user roles who can manage various wifi resources in your system.

It is recommended that you first create a resource group, and then create users and roles to assign to the resource group. The reason is that, during user creation, you are required to assign a user to a resource group.

Creating a New Resource Group

Follow these steps to create a new resource group:

1. In SCI, navigate to Admin > Users & Roles.

2. On the Users & Roles screen, click the Resource Groups tab.

A screen such as the following appears, assuming that some resource groups have already been configured.

FIGURE 211 Resource Groups Screen Examp

Users Resource Groups						
+ Create 🖌 Edit 🛛 🗴 Delete						
	Group Name	Description	Associated Users	Created By	Last Edit Time	٥
	Default	Full access to all resource groups	2		Mar 09 2018 10:59	
0	Dev Group	For RSC dev team	1			
0	Group 1		2	admin	Mar 09 2018 11:44	
0	Group 2		2	admin	Mar 08 2018 09:29	
0	Controller 1		2	admin	Mar 08 2018 09:33	
0	Domain 1	Filter by domain	1	admin	Mar 08 2018 09:43	
0	Zone 2		1	admin	Mar 08 2018 15:49	
0	All Zones		3	admin	Mar 08 2018 09:48	
0	Controller 2		1	admin	Mar 08 2018 10:08	
0	Controller 3		2	admin	Mar 09 2018 10:54	
		- 1 0 of 2 🕽	•			

3. Click Create.

A popup appears, such as in the example below:

FIGURE 212 Create Resource Group Popup

Name:*		
Description:		
s Search group Q	Search AP	Q
All Systems All System 1 System 2 System 3 System 4 System 5 System 6		0 of 0 APs checke

- 4. In the **Create Resource Group** popup, do the following:
 - a) In the **Name** field, enter a universally unique name for the resource group.
 - b) In the **Description** field, enter a useful description of the group for your own information.
 - c) In the **APs** section, use the filters to select the desired wifi assets.
 - d) Once you select one or more APs, the SSID dropdown is activated, and you can select desired SSIDs.
 - e) To complete the configuration of the new resource group, click **Create**.

The newly configured resource group should now appear in the list of resource groups on the **Users & Roles** screen under the **Resource Groups** tab.

Editing a Resource Group

To edit a resource group, do the following:

- 1. Click the box to the left of the group you want to edit.
- 2. Click Edit.
- 3. In the popup, make the desired changes, then click **Update**.

Deleting One or More Resource Groups

To delete resource groups, do the following:

- 1. Click the box to the left of the group for each group that you want to delete.
- 2. Click Delete.

NOTE

All users associated with these groups are also deleted.

Creating Users and Roles

Once you create resource groups, you can create users, assign roles to these users, and assign users to manage one or all resource groups.

It is recommended that you first create a resource group, and then create users and roles to assign to the resource group. The reason is that, during user creation, you are required to assign a user to a resource group.

Creating a New User

Follow these steps to create a new user:

1. In SCI, navigate to Admin > Users & Roles.

2. On the **Users & Roles** screen, click the **Users** tab.

A screen such as the following appears, assuming there are already configured users and resource groups:

FIGURE 213 Users Screen Example

Users	Resource Groups							
Preate / Edit	× Delete							
	Email	Username	First Name	Last Name	Role	Resource Group	Created By	Last Login Time
0	aaa@abc.com	admin	Alison	Knight	Super Admin	Default		Mar 16 2018 10:18
0	jd@abc.com	iamvo	John	Doe	View Only	Domain1		Mar 08 2018 10:11
0	bbb@abc.com	bbb	Bobb	8urnett	View Only	All Zones		Feb 27 2018 16:25
0	jd1@abc.com	iamvo2	Jeff	Doe	View Only	Controller1		Mar 08 2018 15:49
0	ccc@abc.com	carol	Carol	Conway	Super Admin	Default		Mar 08 2018 10:32
0	johnadmin@abc.com	iamadmin	Jon	Doe	Admin	Controller1		Mar 14 2018 15:37
0	eee@abc.com	erika	Erika	Eshethe	View Only	Default		Feb 27 2018 11:47
0	alicevo@ruckus.com	alicevo	Alice	White	View Only	Default		Mar 09 2018 09:56
0	ggg@abc.com	gary	Gary	Goodman	Admin	All Zones		Feb 27 2018 11:47
0	hhh@abc.com	henry	Henry	Henman	View Only	Zone 2		Feb 27 2018 13:53
				-1 0 of 2 🕨				

3. Click **Create**.

The Create Users popup appears:

FIGURE 214 Create User Popup

Create User		×
Email:*]
Username:*]
Password:*	Minimum 8 characters]
Confirm Password:*	Minimum 8 characters]
First Name:*]
Last Name:*]
Role:*	Super Admin	0
Resource Group:*	(Full access to all resource groups)]
	Create	Cancel

- 4. In the **Create Users** popup, fill out all the information, taking into account the following:
 - All fields are mandatory.
 - Users are uniquely defined by their email address and their username. Therefore, no two users can share the same email address and/or username.
 - The Role field has three possible roles: Super Admin, Admin, and View Only. If you select Super Admin, then this user automatically has full access to all resource groups, as shown in the popup above. Therefore, a Super Admin is assigned to the Default resource group because that group contains the entire set of wifi assets in the system. However, if you select either the Admin or View Only role for the user, you then need to select only one group from the Resource Group dropdown.
- 5. Click Create.

The newly configured user should now appear in the list of users on the **Users & Roles** screen under the **Users** tab.

Editing a User

To edit a user, do the following:

- 1. Click the box to the left of the user whose configuration you wish to edit.
- 2. Click Edit.
- 3. In the popup, make the desired changes, then click **Update**.

Deleting One or More Users

To delete users, do the following:

- 1. Click the box to the left of the user for all users that you want to delete.
- 2. Click **Delete**.

NOTE

Only a Super Admin can delete another Super Admin. However, a Super Admin cannot be demoted to Admin or View Only roles. The only way to demote a Super Admin is to delete the Super Admin user, then recreate the user with the desired role.



© 2019 ARRIS Enterprises LLC. All rights reserved. Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc. 350 West Java Dr., Sunnyvale, CA 94089 USA www.ruckuswireless.com