Ruckus Wireless™ SmartCell Insight

Release 1.4 User Guide

Part Number 800-71041-001 Rev A
Published August 2015

www.ruckuswireless.com

Copyright Notice and Proprietary Information

Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

Limitation of Liability

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

Trademarks

Ruckus Wireless, Ruckus, the bark logo, ZoneFlex, FlexMaster, ZoneDirector, SmartMesh, Channelfly, Smartcell, Dynamic PSK, and Simply Better Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

Contents

Copyright Notice and Proprietary Information

About This Guide

Document Conventions . . . 10
Related Documentation . . . 11
Documentation Feedback . . . 11

1 Introducing SmartCell Insight

Introducing SmartCell Insight . . . 14
Overview . . . 14
Off-the-shelf value and easy to use . . . 14
Capabilities . . . 14
Greater Network Visibility . . . 14
Acronyms Used in This Document . . . 15

2 Installing the SmartCell Insight Application

Installation Overview . . . 20

3 Navigating the SmartCell Insight User Interface

Accessing the SCI User Interface . . . 22
Getting Familiar with the SCI User Interface. . . . 23
Interacting with Workspace Elements . . . 24
Viewing AP Details . . . 25
Scheduling Email Report Delivery for Custom Reports . . . 26

4 Using Dashboards and Built-In Reports

Using the Ruckus Dashboards . . . 30
Network Health Dashboard . . . 30
Client Health Dashboard . . . 33
Usage Distribution and Trends Dashboard . . . 34
Using the Ruckus Reports . . . 37
Client and Session Reports . . . 38
Inventory Reports . . . 47
Operational Reports . . . 51

Traffic Reports . . . 61

5 Configuring Custom Reports

Overview of Custom Report Creation . . . 68
Custom Report Schema Changes in SCI 1.3 . . . 69
Creating a New Report . . . 70
Choosing a Data Source . . . 70
The New Analyzer Report Page . . . 73
Adding Fields and Filters . . . 75
Switching to Chart Format . . . 77
Changing the Chart Type . . . 78
Applying Filters to Reports . . . 79
Adding a Description . . . 82
Saving the Report to a Shared Folder . . . 84
Creating Your Own Folder for Custom Reports . . . 85
Available Metrics . . . 88

6 Managing the SmartCell Insight System

Setting Administrator Preferences . . . 92
Accessing the Administration Interface . . . 92
Getting Familiar with the Administration Interface . . . 92
Monitor Page . . . 93
System Setup Page . . . 103
Sources Configuration . . . 103
AP Licensing . . . 107
System Configuration . . . 108
Diagnostics Page . . . 114
Changing the Administrator Password . . . 119
SCI Upgrade Procedure . . . 120
Hostname Verification . . . 120
SCI Uninstall Procedure . . . 121
SCI Backup and Restore . . . 121
SCI AP Grouping . . . 122
Uploading an SCI License . . . 123
System Timekeeping . . . 123
Using the Enterprise Console . . . 125
Creating Users and Roles . . . 125
Using the Scheduler to Define Public Schedules for Custom Reports . . . 129

7 Troubleshooting the SmartCell Insight Application

Before You Begin 138
Architecture Overview 138
Prerequisites 138
Using the SCI Admin Interface 140
The Monitoring Page 140
The Diagnostics Page 142
Job Performance 142
Capture Logs 143
Backup and Restore 144
Backup Server 144
Backup and Restore Process. 144
Uninstall Process 144
Troubleshooting the Vertica Database. 145
Using the Vertica Troubleshooting Admin Tools 145
Recovering the Database 145

8 Appendix

Appendix A: Station Session Statistics 148
Appendix B: Virtual AP Transmission and Reception Statistics 155
Appendix C: Aggregation of Measurements by ZoneDirector 159

Index

About This Guide

This *User Guide* provides information on installation, configuration and management of the Ruckus Wireless™ SmartCell Insight (SCI) application. Topics covered in this guide include SCI introduction, built-in report generation, custom report creation, application management and lists of metrics available for reporting.

This guide is intended for use by those responsible for managing Ruckus Wireless network equipment. Consequently, it assumes a basic working knowledge of local area networking, wireless networking, and wireless devices.

NOTE: If release notes are shipped with your product and the information there differs from the information in this guide, follow the instructions in the release notes.

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/documents.

Document Conventions

Table 1 and Table 2 list the text and notice conventions that are used throughout this guide.

Table 1. Text conventions

Convention	Description	Example
`monospace`	Represents information as it appears on screen	`[Device name]>`
`monospace bold`	Represents information that you enter	`[Device name]>` **`set ipaddr 10.0.0.12`**
default font bold	Keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Screen or page names	Click **Advanced Settings**. The *Advanced Settings* page appears.

Table 2. Notice conventions

Notice Type	Description
Note	Information that describes important features or instructions
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

In addition to this *User Guide*, each SmartCell Insight documentation set includes the following:

- *Installation Guide*: Provides detailed information on how to install SmartCell Insight. The Installation Guide is available for download on the Ruckus Wireless Support Web site at http://support.ruckuswireless.com.
- *SCI ISO Installation Guide*: Provides simplified instructions for installation using an ISO file that combines CentOS installation and SCI installation in an easier format, reducing the number of steps required for the OS installation.
- *Release Notes*: Provide information about the current software release, including new features, enhancements, and known issues.

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)

For example:

- SmartCell Insight User Guide Release 1.4
- Part number: 800-71041-001 Revision A
- Page 88

Introducing SmartCell Insight

1

In this chapter:

- Introducing SmartCell Insight
- Overview
- Off-the-shelf value and easy to use
- Capabilities
- Greater Network Visibility

Introducing SmartCell Insight

Overview

SmartCell Insight (SCI) is a massively scalable reporting and analytics engine, designed to collect data from Ruckus network equipment, analyze that data, and then present it using a wide variety of standard and custom reports.

Off-the-shelf value and easy to use

To facilitate immediate value, SmartCell Insight ships with pre-built reports that solve the most common use cases faced by Engineering, Operations, and Planning organizations. These reports cover themes such as traffic usage, client and session measurement, equipment uptime, network latency, etc. For example, some of the reports can highlight the most heavily utilized devices by both the number of subscribers as well as traffic load. If these reports are not sufficient or need to be tweaked, then additional reports can be generated on site.

Using any standard browser, network operators can create reports on the fly and get a deep insight into any Key Performance Indicator (KPI) that network equipment exposes to northbound systems. For example, compare subscriber equipment distribution (i.e., iPhone vs. Android vs. Windows Phone) market share growth today compared to last month or last year.

Capabilities

SmartCell Insight can collect data from the entire line of Ruckus Access Points (APs) along with the ZoneDirectors (ZDs), FlexMasters (FMs), or SmartZone (SZ) controllers. This data can be aggregated in an offline columnar database, which has been optimized for very high volume data retention and quick response time. Ruckus SmartCell Insight can provide a feed to upstream OSS/BSS applications using a wide variety of interfaces. This allows for further analysis of data collected in the WiFi RAN by upstream systems.

Greater Network Visibility

Getting the most from a carrier WiFi network, once deployed, requires clear visibility into its performance and user activity, both at a very granular level of detail as well as aggregated to measure global trends spanning many years.

Operators need this level of visibility to assess the network's achievement of their business objectives. These include user experience metrics, traffic load on the WiFi RAN, network uptime, etc.

SCI leverages two emerging trends: Firstly, Mobile Internet usage patterns, RAN strategies, and service models are all evolving rapidly, so the visibility required to address these questions must extend beyond typical short-horizon EMS/NMS health and statistics to enable long-term trend analysis that supports network and service evolution planning. With exploding volumes of users, devices, traffic, and radio nodes deployed, these two requirements spell a real scaling challenge for any network measurement and assessment tool.

Secondly, the emergence of Big Data brought to market by many popular applications that facilitate the collection, storage, and efficient retrieval and analysis of data. These technologies, in SCI, have been brought to the management of network equipment resulting in a comprehensive offering that can facilitate additional capabilities in future releases.

Ruckus' development of SmartCell Insight, similar to the development of SmartZone, takes whole new approach to measurement and assessment, designed specifically to provide the visibility, trend analysis, and raw scale required to manage a successful carrier WiFi network. The design of SmartCell Insight is informed by our experience powering the world's largest and most advanced WiFi networks.

Acronyms Used in This Document

Table 1lists the acronyms used in this document.

Table 1. Acronyms

Acronym	Description
A-MDPU	aggregated MPDU (feature of an HT AP or STA)
A-MSDU	aggregated MSDU (feature of an HT AP or STA)
AMRI	aggregate measurement reporting interval
AP	access point
BSS	basic service set
CCA	clear channel assessment [threshold] (when any received signal is above this threshold, the RF channel is considered "busy" by an 802.11-compliant transmitter).
CDF	cumulative distribution function

Table 1. Acronyms

Acronym	Description
CSV	comma separated values [file]
DA	destination [MAC] address
DHCP	dynamic host configuration protocol; DHCPv4 is DHCP for IPv4 and DHCPv6 is DHCP for IPv6.
DMS	directed multicast service (see [1])
DNS	domain name system
eMAP	mesh AP having another MAP plugged into its [local] Ethernet interface
ETL	extract, transform and load
FC	frame control (field in 802.11 MAC header, see [1])
FCS	frame check sequence
GCR	groupcast with retries (see [5])
HT	high throughput (aka 802.11n, see [1])
IE	information element
MAC	medium access control [layer]
MAP	mesh AP
mDNS	multicast DNS
MI	measurement interval
MMPDU	MAC management protocol data unit (see [1])
MPDU	MAC protocol data unit (the MAC header plus payload plus FCS, see Figure 8-1 in [1])
MSDU	MAC service data unit (the payload of the MPDU)
MTU	maximum transmission unit (longest frame/packet which can be transmitted on a link/path without fragmentation)
NTP	network time protocol
OS	operating system
PHY	physical [layer]
PLCP	physical layer convergence procedure (see [1])
QoS	quality of service
RAP	root AP (mesh AP connected to the wired infrastructure)

Table 1. Acronyms

Acronym	Description
RRM	radio resource measurement
SZ	SmartZone (AP controller)
SCI	smart cell insight (analytics appliance)
SIFS	short inter-frame space (see [1])
SINR	signal to interference plus noise ratio
SLAAC	[IPv6] stateless auto-configuration
SNR	signal to noise ratio
STA	IEEE 802.11 station
VAP	virtual AP (aka a BSS in IEEE 802.11 nomenclature)
ZD	ZoneDirector (AP controller)

References:

1 IEEE 802.11-2012, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

2 IEEE 802.2-1998, Part 2: Logical Link Control.

3 RFC-2865, Remote Authentication Dial In User Service (RADIUS), Rigney, Willens, Rubens and Simpson, June 2000.

Installing the SmartCell Insight Application

2

In this chapter:

- Installation Overview

Installation Overview

The standard SmartCell Insight package is distributed as a .tar compressed file designed to be installed on a CentOS or Red Hat Enterprise Linux (RHEL) server.

For complete installation instructions, see the *SmartCell Insight Installation Guide*, available from support.ruckuswireless.com.

Additionally, SCI is also distributed as an ISO image that contains the SCI application and the OS installation in one to provide a simpler system setup and installation process. The ISO installation method has some limitations however. Please refer to the *SmartCell Insight ISO Package Installation Guide* for more information.

The steps are outlined below for your reference.

NOTE: You must perform the installation as detailed in the *SCI Installation Guide* or the *SCI ISO Installation Guide*. This installation overview is for reference only.

1. Prepare the hardware for installation.
2. Install CentOS/Redhat Enterprise Linux exactly according to the instructions in the Installation Guide. Failure to do so will result in failure to install SCI properly.
3. Install SCI.
4. Install licenses.
5. Configure ZoneDirector, FlexMaster and/or SmartZone data sources.

Navigating the SmartCell Insight User Interface

3

In this chapter:

- Accessing the SCI User Interface
- Getting Familiar with the SCI User Interface
- Interacting with Workspace Elements
- Scheduling Email Report Delivery for Custom Reports

Accessing the SCI User Interface

After you have completed the installation procedures according to the instructions in either the *SCI Installation Guide* or the *SCI ISO Installation Guide*, and configured your SmartZone or ZoneDirector controller data sources (as described in Sources Configuration), you can begin using SCI to monitor your wireless networks after approximately 15 minutes. (The reporting interval for many of the data sets reported by ZoneDirector and SmartZone controllers is 15 minutes).

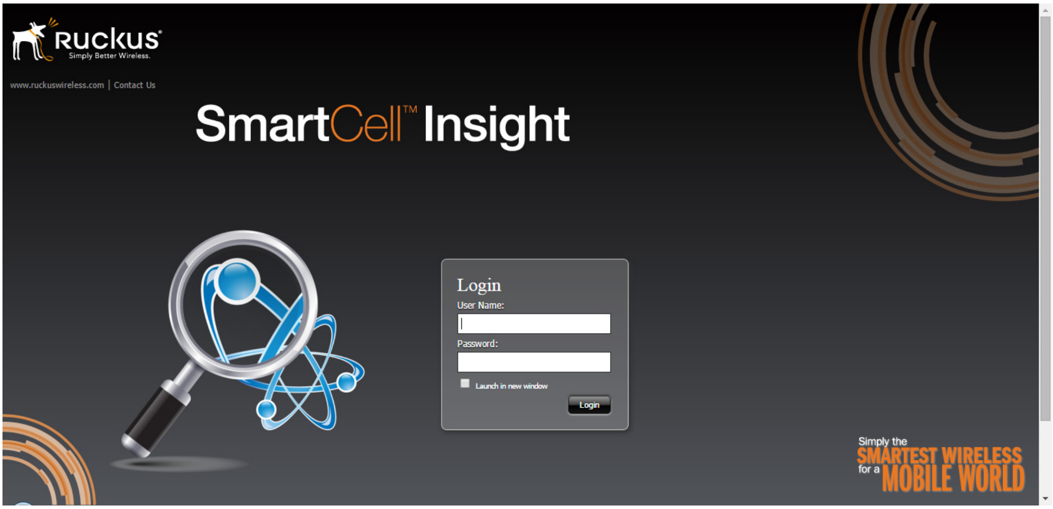
To begin using the SCI reporting interface:

1 Point your browser to: **https://[SCI-IP-Address]** and press **Enter**.

2 Enter your **User Name** and **Password**, and click **Login**.

NOTE: SCI supports Chrome and Firefox browsers. Internet Explorer is not recommended.

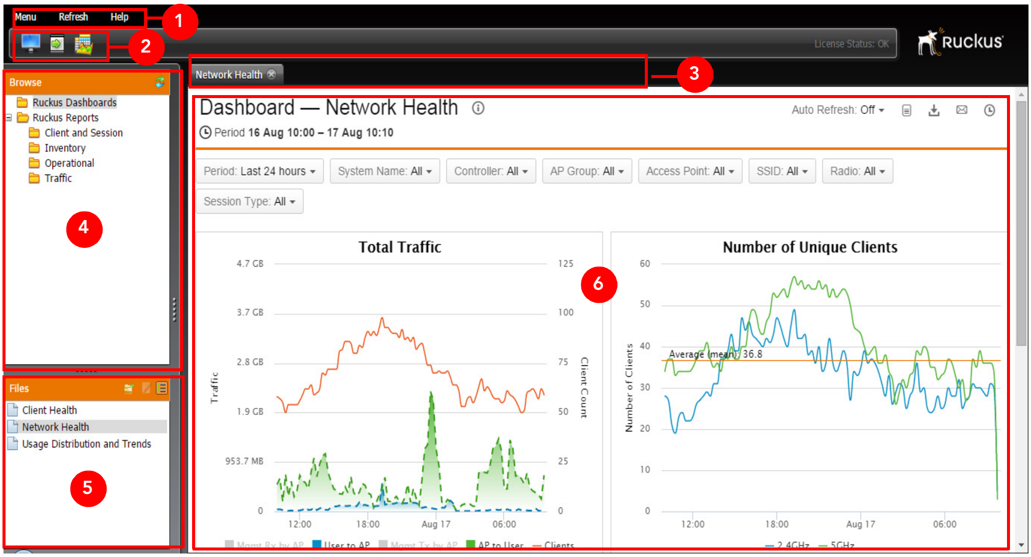
Figure 1. Log into the SCI reporting interface



Getting Familiar with the SCI User Interface

The SmartCell Insight User Console interface consists of 6 main elements, as shown in Figure 2. For a description of each UI element, see Table 2.

Figure 2. SmartCell Insight Web interface elements



Dashboard — Network Health

Period 16 Aug 10:00 – 17 Aug 10:10

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All | Session Type: All

Table 2. SCI User Console Web interface elements

Number	Description
1	**Menu**: Contains Logout, Refresh and Help menu items
2	**Action icons**: • **Workspace**: Open the *My Workspace* view, which shows reports that you have submitted to run in the background on the server. You can cancel reports that have not run yet or view or delete completed reports. • **Toggle Browser**: Toggle the Report and Files browser panels. • **New Analyzer Report**: Create a new analyzer report. Clicking this button launches the report creation view.
3	**Tabs**: Displays the windows that are currently open. Click the “x” icon next to a tab name to close the window.

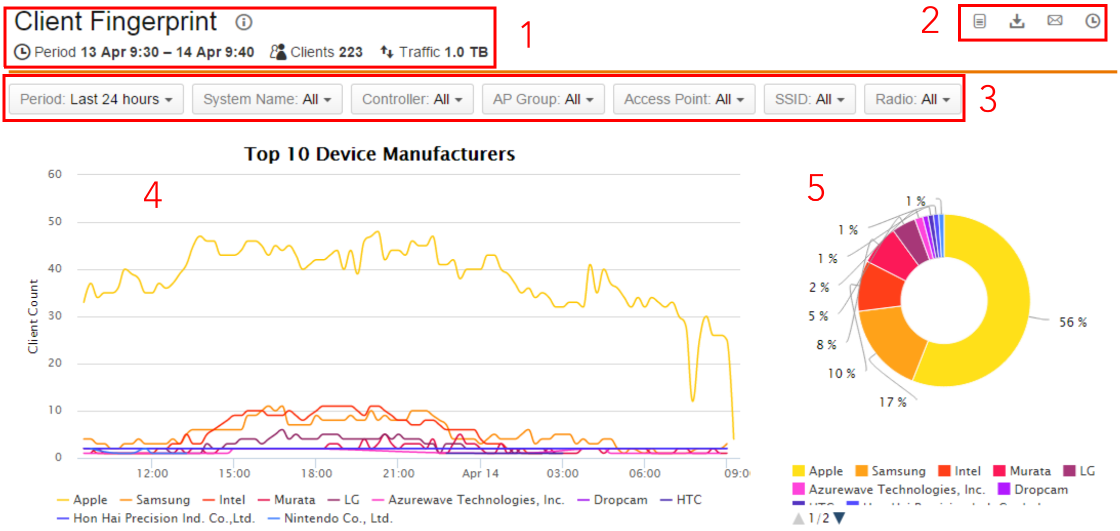
Table 2. SCI User Console Web interface elements

Number	Description
4	**Report browser panel**: Use this panel to select which category of report or dashboard to view.
5	**Files browser panel**: Use this panel to select the individual report/ dashboard to view in the workspace.
6	**Workspace**: This large area is used to display the report you are currently viewing, or to create and manage custom reports. See Using the Ruckus Dashboards and Using the Ruckus Reports for more information.

Interacting with Workspace Elements

The Workspace is used for viewing and manipulating reports. Table 3 lists the tools you can use to produce, deliver and interact with dashboards and other built-in reports displayed in the workspace.

Figure 3. Report workspace elements



Client Fingerprint

Period 13 Apr 9:30 – 14 Apr 9:40 Clients 223 Traffic 1.0 TB

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All

Table 3. Report workspace elements

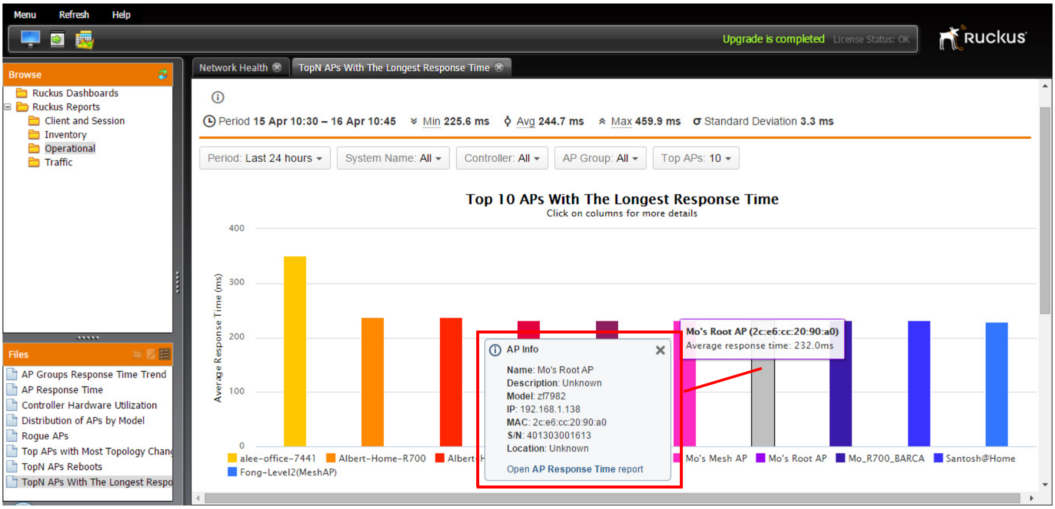
Number	Description
1	Report overview
2	Export this report: • Print this report. • Download as PDF file. • Send this report by email. • Schedule email delivery of this report (see Scheduling Email Report Delivery for Custom Reports for more information on custom report delivery).
3	Filters: Use the drop-down menus to filter the report contents by report-specific fields.
4	Graph: Select an area on the graph to zoom. Click Reset Zoom to reset.
5	Pie chart: Click a segment of the pie chart to view an exploded view with the selected segment detached.

Viewing AP Details

You can view specific details on an individual Access Point by clicking on its bar in bar chart type reports. The “AP Info” pop-up includes the AP name, description, IP address, MAC address and location coordinates.

Additionally, you can click the **Map** link to display the AP’s location on Google Maps. You can also click the **Open AP Response Time report** link to open a report on the individual AP’s response time.

Figure 4. Click an AP's bar to display details on the specific AP



Period **15 Apr 10:30 – 16 Apr 10:45** Min **225.6 ms** Avg **244.7 ms** Max **459.9 ms** σ Standard Deviation **3.3 ms**

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Top APs: 10

Mo's Root AP (2c:e6:cc:20:90:a0)
Average response time: 232.0ms

AP Info

Name: Mo's Root AP
Description: Unknown
Model: zf7982
IP: 192.168.1.138
MAC: 2c:e6:cc:20:90:a0
S/N: 401303001613
Location: Unknown

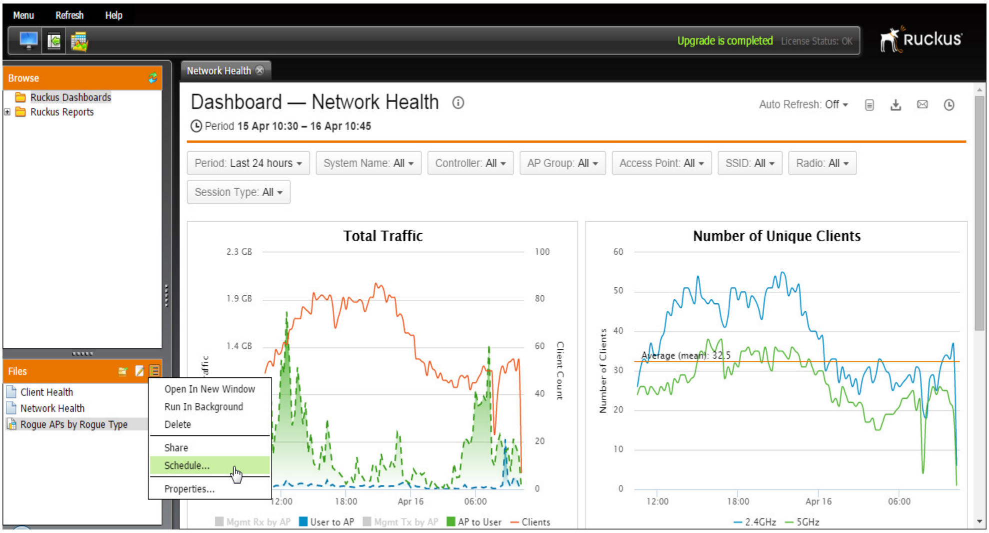
Scheduling Email Report Delivery for Custom Reports

For custom reports, you can schedule email report delivery using the Options pull-down menu from the Files browser panel.

To do so, use the following procedure:

1. Select the report for which you want to schedule email delivery from the **Files** browser panel.
2. Click the **Options** icon, and select **Schedule...**.
3. In the **New Report Schedule** dialog that appears, enter an email subject in the **Subscription/Subject** field, and enter comma separated destination addresses in the **Email To** field.
4. Select **Report Type** (PDF, XLS or CSV) and **Public Schedule**.
5. Click **Schedule** to confirm.

Figure 5. Scheduling email report delivery for custom reports

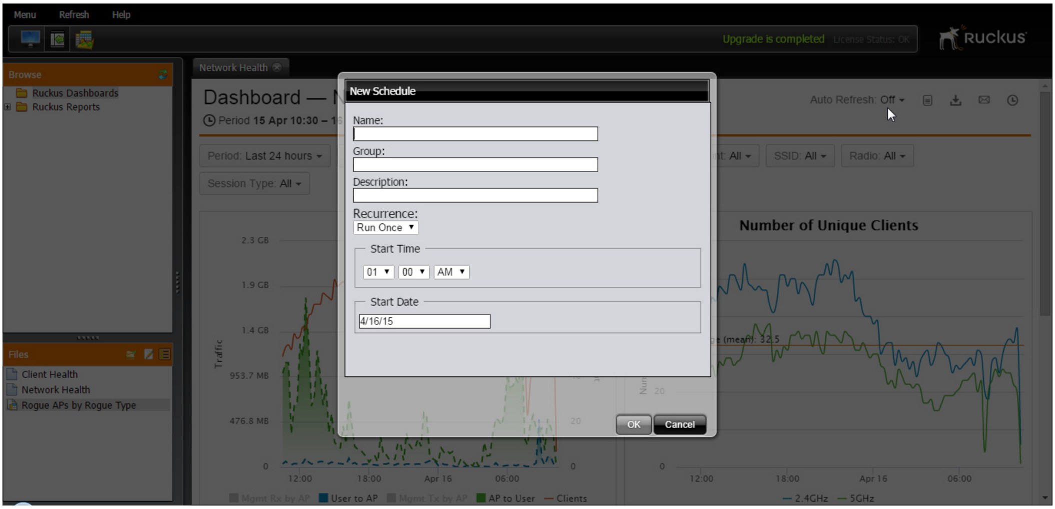


Period 15 Apr 10:30 – 16 Apr 10:45

Auto Refresh: Off

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All | Session Type: All

Figure 6. Scheduling email report delivery for custom reports (2)



Name:

Group:

Description:

Recurrence: Run Once

Start Time: 01 00 AM

Start Date: 4/16/15

Using Dashboards and Built-In Reports

4

In this chapter:

- Using the Ruckus Dashboards
- Using the Ruckus Reports
- Client and Session Reports
- Inventory Reports
- Operational Reports
- Traffic Reports

Using the Ruckus Dashboards

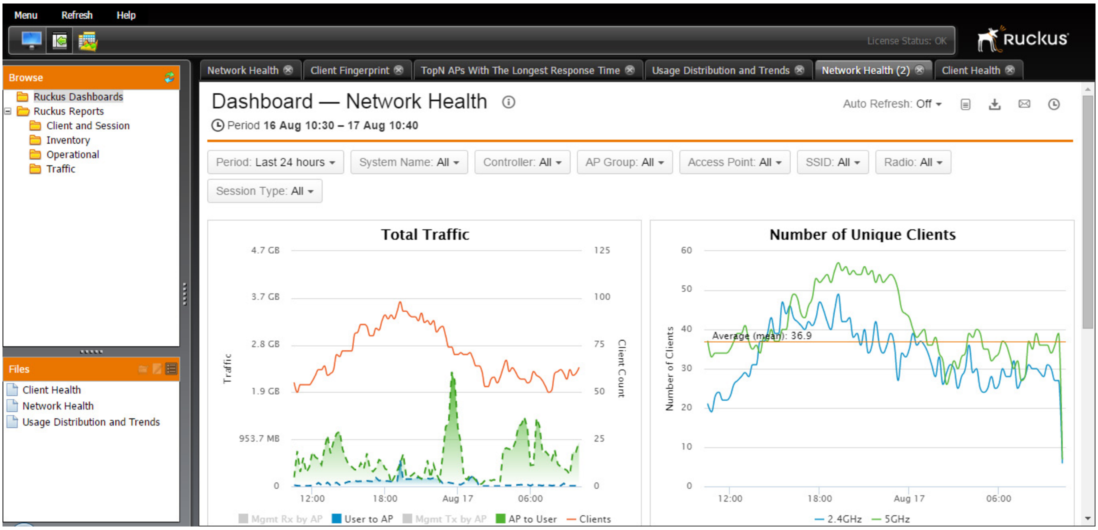
The Ruckus Dashboards (Network Health Dashboard, Client Health Dashboard and Usage Distribution and Trends Dashboard) provide a convenient at-a-glance overview of multiple sets of key network status information in a grid layout. Ruckus Dashboards contain general network and client statistics such as AP traffic volume, number of connected clients, session duration and client OS/manufacturer.

Network Health Dashboard

The Network Health Dashboard provides a general overview of the entire network using aggregated summary statistics collected by SCI, and consists of four components: AP Traffic, Number of Unique Clients, Sessions per Radio and Top 10 APs by Traffic Volume. Each of these reports can be filtered by date, system name, controller, AP group, AP, SSID, radio and session type (authorized vs. unauthorized).

The "Top 10 APs by Traffic Volume" displays your top 10 APs in a map view, allowing you to zoom in on an area of interest, locate specific APs and quickly find basic information about an AP such as its MAC address, IP address and serial number, along with a link to the AP's traffic report.

Figure 7. The Network Health Dashboard



Dashboard — Network Health

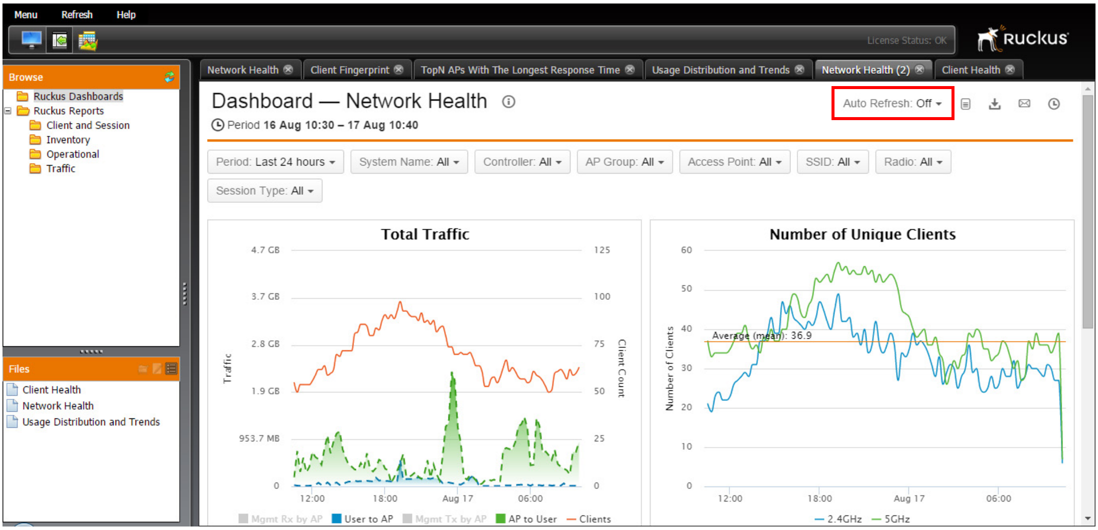
Period 16 Aug 10:30 – 17 Aug 10:40

Period: Last 24 hours
System Name: All
Controller: All
AP Group: All
Access Point: All
SSID: All
Radio: All
Session Type: All
Auto Refresh: Off

Starting and Stopping Auto-Refresh

The Auto Refresh button at the top right corner of the dashboard allows you to manually or automatically refresh the page. Auto-refresh is disabled by default. When enabled, the automatic refresh interval is 15 minutes.

Figure 8. Starting and stopping Auto-Refresh



Dashboard — Network Health

Period 16 Aug 10:30 – 17 Aug 10:40

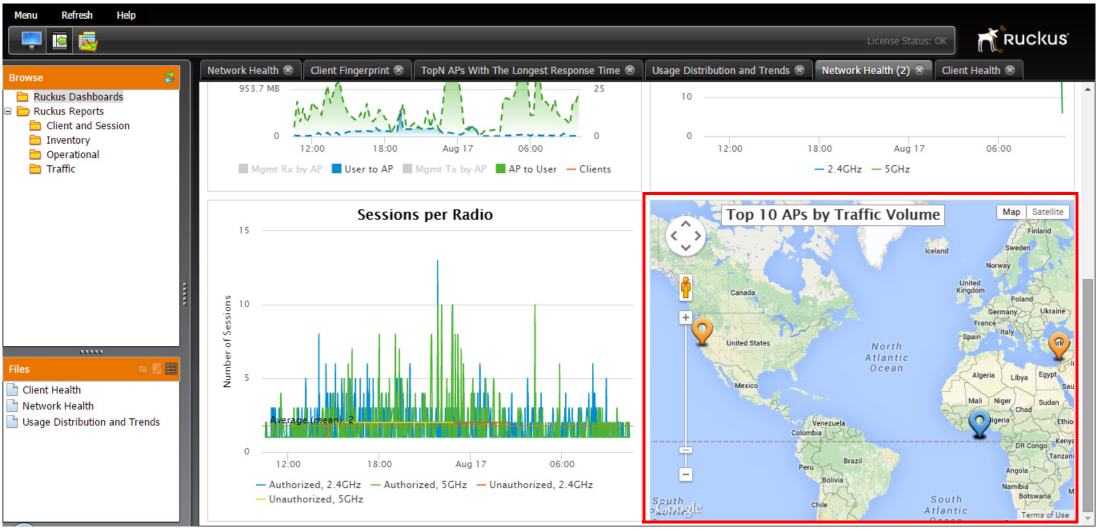
Auto Refresh: Off

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All | Session Type: All

Using the Map View

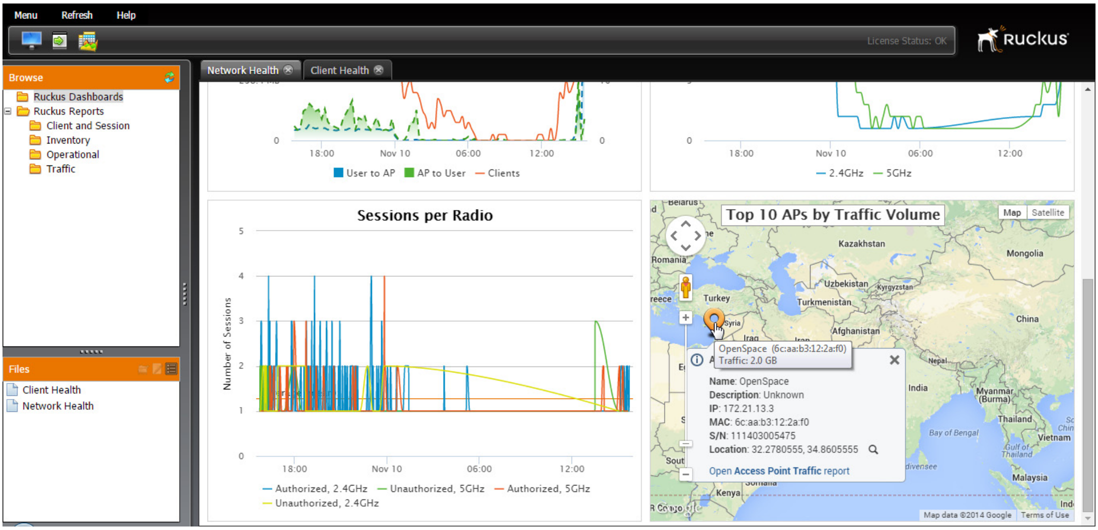
The map-based “Top 10 APs by Traffic Volume” dashboard report provides an overview of the top 10 APs by physical location, allowing you to quickly locate and troubleshoot a specific device.

Figure 9. Using the Map View



Hovering over an AP on the map displays its name, MAC address and traffic volume. Clicking the AP icon displays more information, including description, Serial Number, map coordinates and a link to the Individual AP Traffic Report.

Figure 10. Display more AP details



OpenSpace (6c:aa:b3:12:2a:f0)
Traffic: 2.0 GB

Name: OpenSpace
Description: Unknown
IP: 172.21.13.3
MAC: 6c:aa:b3:12:2a:f0
S/N: 111403005475
Location: 32.2780555, 34.8605555

Open **Access Point Traffic** report

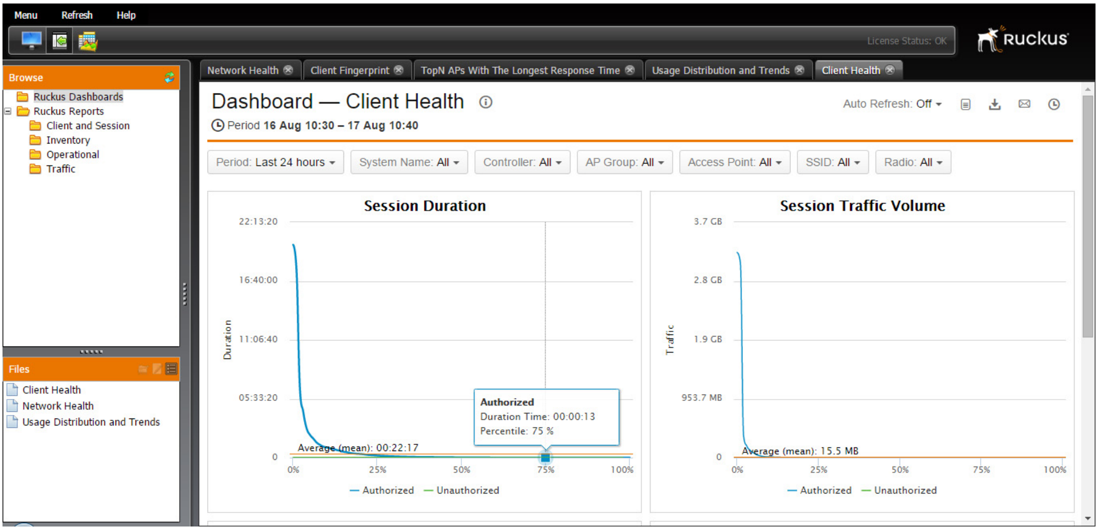
Examples of how the Network Health Dashboard could be used by network administrators:

- Used to quickly and easily compare traffic volume and connected clients over time.
- Used to compare numbers of clients connected on 2.4 or 5 GHz radios.
- Used to identify APs by geographic location.

Client Health Dashboard

The Client Health Dashboard displays an overview of client information such as session duration, traffic volume, throughput estimate and OS/manufacturer charts. It consists of four client-based reports: Session Duration, Session Traffic Volume, Throughput Estimate of Clients and Manufacturers/Operating Systems. Each of these reports can be filtered by date, system name, controller, AP group, AP, SSID, and radio.

Figure 11. Client Health Dashboard - top



Dashboard — Client Health

Period 16 Aug 10:30 – 17 Aug 10:40

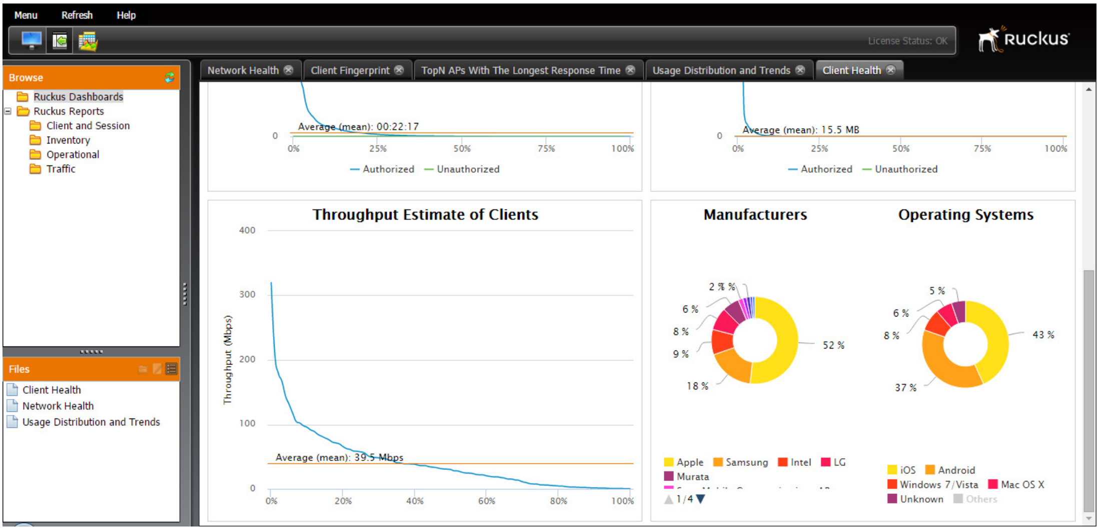
Auto Refresh: Off

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All

Authorized
Duration Time: 00:00:13
Percentile: 75 %

You can hover over a section of a pie chart in the client Manufacturers/Operating Systems report to view the actual client count and percentage of the total for each device manufacturer or OS.

Figure 12. Client Health Dashboard - bottom



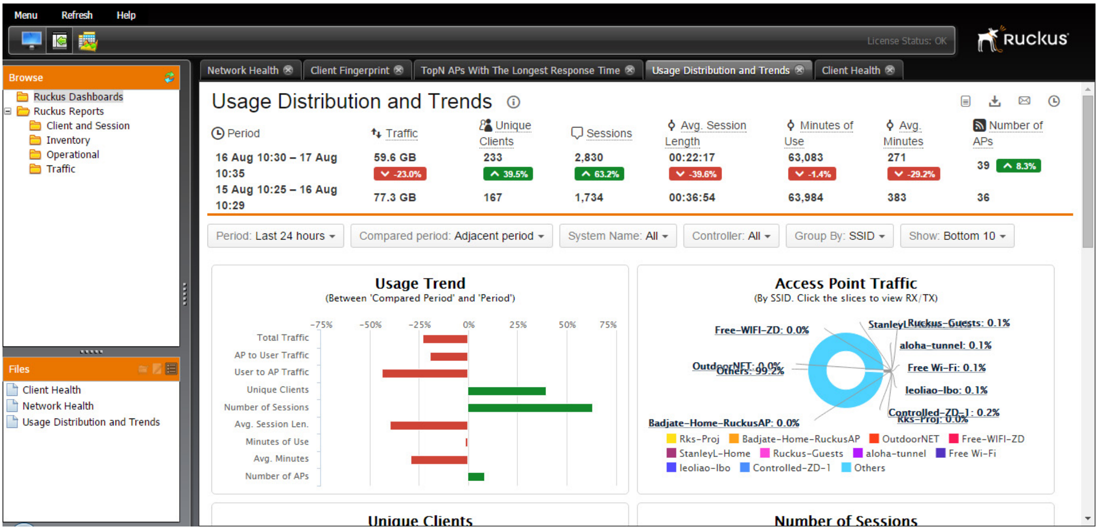
Examples of how the Client Health Dashboard could be used by network administrators:

- Used to identify the device types on the WiFi network over time.
- Used to identify average session durations, so that you can understand how much time users are spending connected your WiFi networks.
- Used to discover which APs and controllers are being used most often, what time of day or days of the week your networks are most congested, and the difference between number of authorized vs. unauthorized clients.
- Used to display the general performance experience connected clients are likely to have.

Usage Distribution and Trends Dashboard

The Usage Distribution and Trends Dashboard enables network administrators to view WiFi usage trends by comparing data between two equal-length time periods. These reports can be used to compare data such total traffic, unique clients, session length, AP traffic, minutes of use and number of APs grouped by location, SSID or AP group. The graphs can be further filtered to display statistics grouped by controller, and to display either the top 10 or bottom 10 sets of data for each graph.

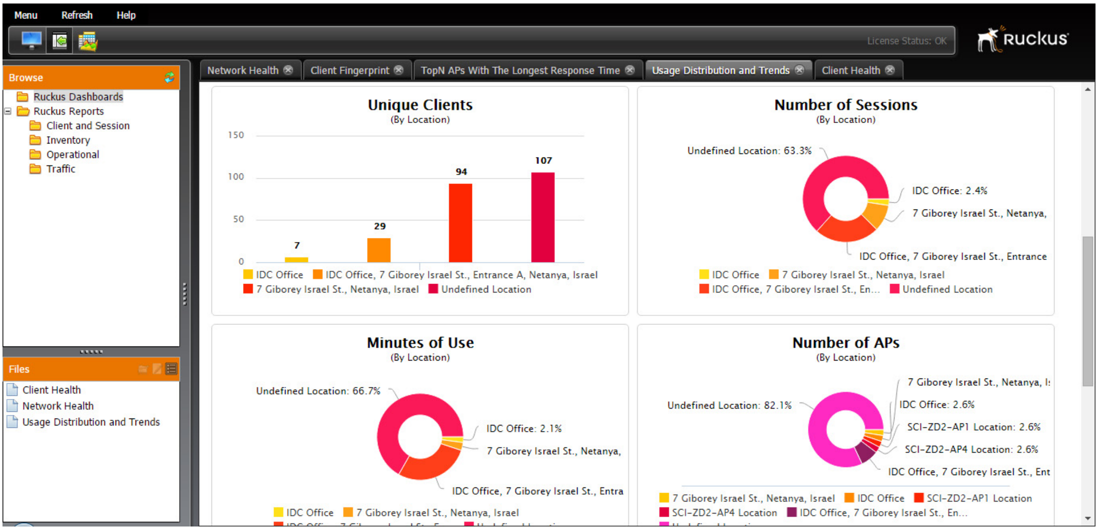
Figure 13. Usage Distribution and Trends Dashboard - top



Period	Traffic	Unique Clients	Sessions	Avg. Session Length	Minutes of Use	Avg. Minutes	Number of APs
16 Aug 10:30 – 17 Aug 10:35	59.6 GB ∨ -23.0%	233 ∧ 39.5%	2,830 ∧ 63.2%	00:22:17 ∨ -39.6%	63,083 ∨ -1.4%	271 ∨ -29.2%	39 ∧ 8.3%
15 Aug 10:25 – 16 Aug 10:29	77.3 GB	167	1,734	00:36:54	63,984	383	36

Period: Last 24 hours ▾ | Compared period: Adjacent period ▾ | System Name: All ▾ | Controller: All ▾ | Group By: SSID ▾ | Show: Bottom 10 ▾

Figure 14. Usage Distribution and Trends Dashboard - middle


Menu
Refresh
Help
License Status: OK
Ruckus
Network Health
Client Fingerprint
TopN APs With The Longest Response Time
Usage Distribution and Trends
Client Health
Browse
Ruckus Dashboards
Ruckus Reports
Client and Session
Inventory
Operational
Traffic
Files
Client Health
Network Health
Usage Distribution and Trends
Unique Clients
(By Location)
150
100
50
0
7
29
94
107
IDC Office
IDC Office, 7 Giborey Israel St., Entrance A, Netanya, Israel
7 Giborey Israel St., Netanya, Israel
Undefined Location
Number of Sessions
(By Location)
Undefined Location: 63.3%
IDC Office: 2.4%
7 Giborey Israel St., Netanya,
IDC Office, 7 Giborey Israel St., Entrance
IDC Office
7 Giborey Israel St., Netanya, Israel
IDC Office, 7 Giborey Israel St., En...
Undefined Location
Minutes of Use
(By Location)
Undefined Location: 66.7%
IDC Office: 2.1%
7 Giborey Israel St., Netanya,
IDC Office, 7 Giborey Israel St., Entra
IDC Office
7 Giborey Israel St., Netanya, Israel
Number of APs
(By Location)
Undefined Location: 82.1%
7 Giborey Israel St., Netanya, I:
IDC Office: 2.6%
SCI-ZD2-AP1 Location: 2.6%
SCI-ZD2-AP4 Location: 2.6%
IDC Office, 7 Giborey Israel St., Ent
7 Giborey Israel St., Netanya, Israel
IDC Office
SCI-ZD2-AP1 Location
SCI-ZD2-AP4 Location
IDC Office, 7 Giborey Israel St., En...

The dashboard also displays a table showing the following KPIs per each group (AP Group, AP Location, SSID), during the two periods, and the change, in percent, between the periods:

- AP -> User Traffic
- User -> AP Traffic
- Total Traffic (sum of two previous KPIs)
- Number of Unique Clients
- Number of Sessions
- Average Session Length
- Minutes of Use
- Average Minutes of Use Per Client
- Number of APs

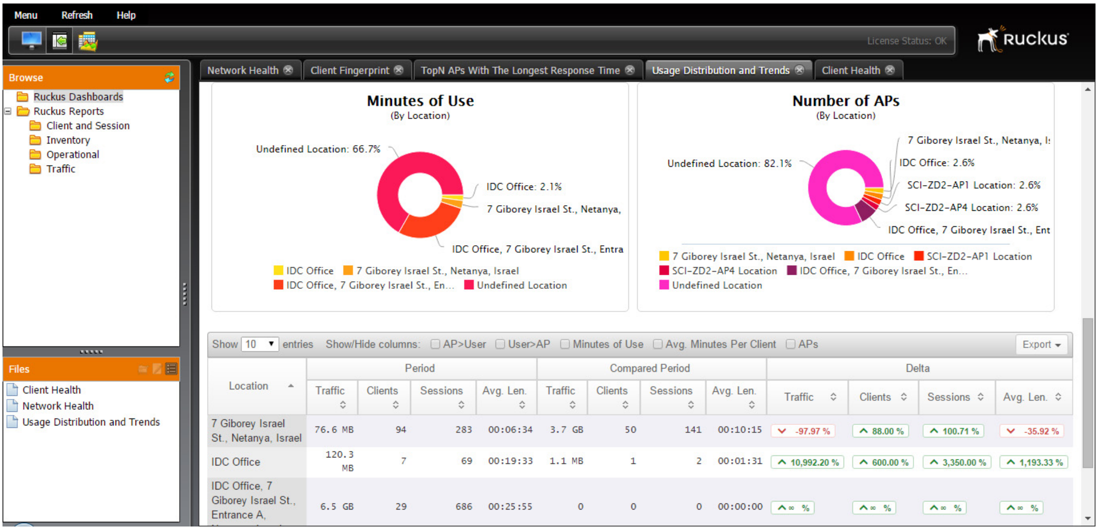
Some of these KPIs are hidden by default, in order to not clutter the screen. You may show/hide them by selecting the relevant check box at the table header.

You may sort each KPI or its delta by clicking on the column header of the KPI, and reverse the sort order by clicking again.

You may click-through some of the KPIs into other reports, filtered for the same group. When that is possible, the mouse cursor will change to a pointer when you hover over these KPIs.

You may click on the group name (left-most column) in order to drill down to per-AP views of all the above KPIs.

Figure 15. Usage Distribution and Trends Dashboard - bottom


Menu
Refresh
Help
License Status: OK
Ruckus
Browse
Ruckus Dashboards
Ruckus Reports
Client and Session
Inventory
Operational
Traffic
Files
Client Health
Network Health
Usage Distribution and Trends
Network Health
Client Fingerprint
TopN APs With The Longest Response Time
Usage Distribution and Trends
Client Health
Minutes of Use
(By Location)
Undefined Location: 66.7%
IDC Office: 2.1%
7 Giborey Israel St., Netanya,
IDC Office, 7 Giborey Israel St., Entra
IDC Office
7 Giborey Israel St., Netanya, Israel
IDC Office, 7 Giborey Israel St., En...
Undefined Location
Number of APs
(By Location)
Undefined Location: 82.1%
7 Giborey Israel St., Netanya, I:
IDC Office: 2.6%
SCI-ZD2-AP1 Location: 2.6%
SCI-ZD2-AP4 Location: 2.6%
IDC Office, 7 Giborey Israel St., Ent
7 Giborey Israel St., Netanya, Israel
IDC Office
SCI-ZD2-AP1 Location
SCI-ZD2-AP4 Location
IDC Office, 7 Giborey Israel St., En...
Undefined Location
Export

Show 10 entries Show/Hide columns: □ AP>User □ User>AP □ Minutes of Use □ Avg. Minutes Per Client □ APs

Location	Period				Compared Period				Delta			
	Traffic	Clients	Sessions	Avg. Len.	Traffic	Clients	Sessions	Avg. Len.	Traffic	Clients	Sessions	Avg. Len.
7 Giborey Israel St., Netanya, Israel	76.6 MB	94	283	00:06:34	3.7 GB	50	141	00:10:15	-97.97 %	88.00 %	100.71 %	-35.92 %
IDC Office	120.3 MB	7	69	00:19:33	1.1 MB	1	2	00:01:31	10,992.20 %	600.00 %	3,350.00 %	1,193.33 %
IDC Office, 7 Giborey Israel St., Entrance A,	6.5 GB	29	686	00:25:55	0	0	0	00:00:00	∞ %	∞ %	∞ %	∞ %

Using the Ruckus Reports

In addition to the Ruckus Dashboards, which contain combined views of several reports, SCI comes with a number of detailed reports to help you gain deeper insight into your network statistics using a wide variety of common use cases for analyzing network capacity, traffic trends, client statistics and device inventories.

In addition to the built-in reports, you can also create your own custom reports using any of the data provided by your data sources to SCI, as detailed in Configuring Custom Reports.

For detailed descriptions of the statistics used in calculating client session, AP transmission and aggregated statistics reports, see the relevant sections in the "Appendix" on page 147.

The following key assessments can be made using these built-in Ruckus Reports:

- Network capacity, carried traffic and utilization
- User experience (getting on the network, connection speed - simple high/low/average & CDF views)
- User activity (devices, applications, sessions, bandwidth)
- AP behavior (channel changes, meshing, band steering, load balancing)
- Network operating conditions (interference sources)
- Usual network mechanics (uptime, alarms, etc.)
- Capability to view stats at multiple layers (AP, radio, SSID) and session

Table 4 lists the built-in reports that SCI provides. The reports are organized according to the following categories:

- Client and Session Reports
- Inventory Reports
- Operational Reports
- Traffic Reports

Table 4. SCI Reports

Category	Reports
Client and Session Reports	Client Fingerprint First Experience of New Clients Number of Sessions Number of Unique Clients Session Bytes Transferred Session Duration Top Clients by Traffic Volume
Inventory Reports	AP Inventory Controller Inventory Session Inventory
Operational Reports	AP Groups Response Time Trend AP Response Time Controller Hardware Utilization Distribution of APs by Model Rogue APs Top APs with Most Topology Changes Top AP Reboots Top APs with the Longest Response Time
Traffic Reports	Access Point Traffic Client Potential Throughput Throughput Estimate of Clients Top APs by Traffic Volume

Client and Session Reports

Client and Session Reports include number of sessions, session duration, client device type and traffic volume of the most active clients.

- Client Fingerprint
- First Experience of New Clients
- Number of Sessions

- Number of Unique Clients
- Session Bytes Transferred
- Session Duration
- Top Clients by Traffic Volume

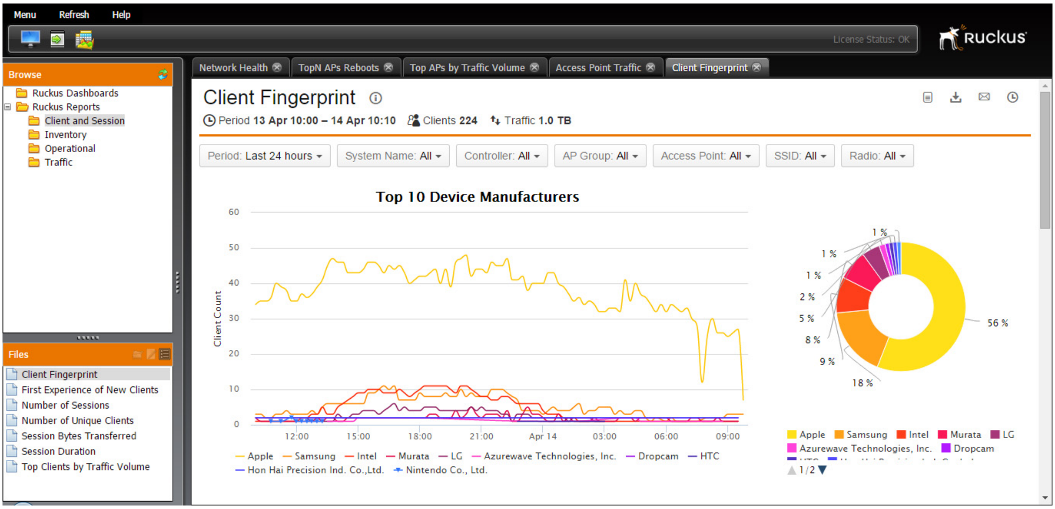
Client Fingerprint

This report provides a list of the manufacturers of the mobile devices on the WiFi network along with their OS type during a specific time interval.

Examples of how this report could be used by network administrators:

- Used to identify the device types on the WiFi network.

Figure 16. Client Fingerprint report



Client Fingerprint

Period 13 Apr 10:00 – 14 Apr 10:10 Clients 224 Traffic 1.0 TB

Period: Last 24 hours · System Name: All · Controller: All · AP Group: All · Access Point: All · SSID: All · Radio: All

First Experience of New Clients

This report displays statistics about the user experience of the first connection for new clients, including average session duration, noise floor, RSSI and potential throughput.

Examples of how this report could be used by network administrators:

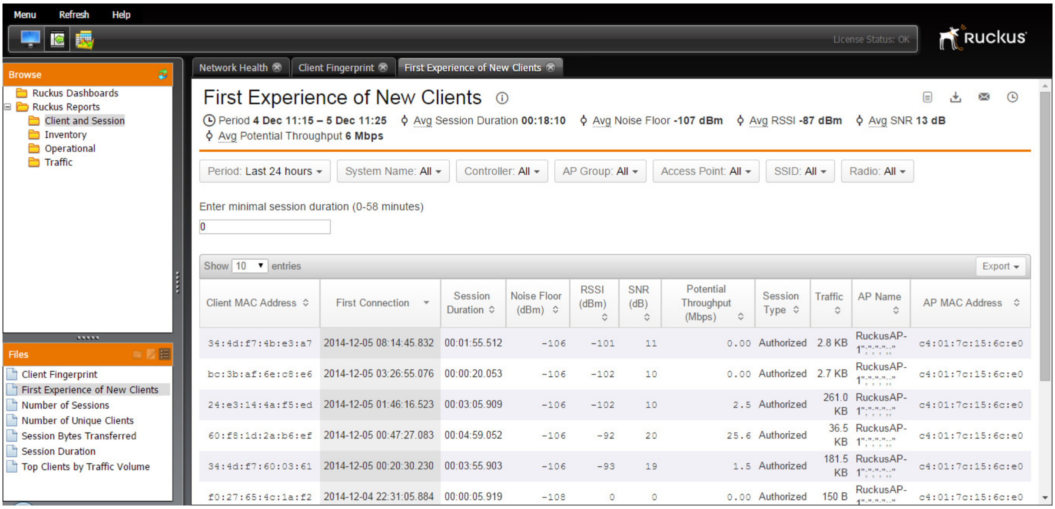
Some service providers have conducted studies which show that if the user's first experience is good, then the user tends to return and remain as a customer in the long run. Therefore, if metrics show a correlation between session duration and signal strength for new subscribers, then SCI can analytically predict where low RSSI will lead to customer satisfaction issues.

Notes:

- A new subscriber is one in which this report is for the first time they were observed associated to the WLAN. SCI keeps a database of MAC addresses and detects the existence of statistics for new mobile devices, not in the database. Mobile devices thus detected are then selected for inclusion into the CSV file based on being joined to a particular controller, AP, AP group, SSID or radio.
- Each record in the CSV file contains the mobile devices' MAC address, authentication time, association time, session end time, client throughput, SNR+RSSI statistics and serving AP.
- APs measure the SNR and noise floor on frames received from associated STAs. That is, uplink SNR is measured; downlink SNR is not reported by STAs nor is it estimated (in SCIv1.0) by APs. From these measurements RSSI is computed as RSSI (dBm) = SNR (dB) + NFE (dBm), where NFE = a noise floor estimate produced by the WiFi silicon. Note that while the SNR measurement is quite accurate, the NFE is an uncalibrated estimate. Therefore, the error in the RSSI value can be significant (several dB).
- Ruckus APs use BeamFlex technology. Indoor Ruckus APs employ omni-directional BeamFlex antennas (which can be controlled by BeamFlex algorithms to have omni-directional or directional patterns). Outdoor APs can have either omni-directional or directional antennas. The –N SKUs have two 30° beamwidth directional antennas and do not use BeamFlex technology; the gain of a single, 30° beamwidth antenna is ~11dB greater than an omni-directional antenna. The –S SKUs have two or three ~120° sector antennas and employ BeamFlex technology; each sector antenna has a gain ~5dB higher than the gain of an omni-directional antenna. Therefore for given set of link conditions, different SKUs will produce different RSSI values.
- BeamFlex algorithms cause each AP antenna to have an approximately omni-directional pattern when receiving WiFi signals. However, when transmitting WiFi signals, the BeamFlex algorithm will typically control the antennas to have a directional pattern, producing several dB of gain compared to an omni-direc-

tional pattern. Thus, the antenna gain in the downlink direction is typically different/higher than in the uplink direction. In addition, Ruckus APs usually have a higher transmitter power capability than STAs. The combination of higher transmitter power and higher antenna gain means that the received SNR at the STA (downlink direction) will typically be 3-6 dB higher than at the AP (uplink direction). This typically results in higher PHY rates in the downlink direction than in the uplink direction. In terms of user experience, higher downlink RSSI is better for the user because for many web services, the perceived quality is based on the time waiting for web pages to arrive.

Figure 17. First Experience of New Clients report



First Experience of New Clients

Period **4 Dec 11:15 – 5 Dec 11:25** Avg Session Duration **00:18:10** Avg Noise Floor **-107 dBm** Avg RSSI **-87 dBm** Avg SNR **13 dB** Avg Potential Throughput **6 Mbps**

Period: Last 24 hours · System Name: All · Controller: All · AP Group: All · Access Point: All · SSID: All · Radio: All

Enter minimal session duration (0-58 minutes)

0

Client MAC Address	First Connection	Session Duration	Noise Floor (dBm)	RSSI (dBm)	SNR (dB)	Potential Throughput (Mbps)	Session Type	Traffic	AP Name	AP MAC Address
34:4d:f7:4b:e3:a7	2014-12-05 08:14:45.832	00:01:55.512	-106	-101	11	0.00	Authorized	2.8 KB	RuckusAP-1":":":"::"	c4:01:7c:15:6c:e0
bc:3b:af:6e:c8:e6	2014-12-05 03:26:55.076	00:00:20.053	-106	-102	10	0.00	Authorized	2.7 KB	RuckusAP-1":":":"::"	c4:01:7c:15:6c:e0
24:e3:14:4a:f5:ed	2014-12-05 01:46:16.523	00:03:05.909	-106	-102	10	2.5	Authorized	261.0 KB	RuckusAP-1":":":"::"	c4:01:7c:15:6c:e0
60:f8:1d:2a:b6:ef	2014-12-05 00:47:27.083	00:04:59.052	-106	-92	20	25.6	Authorized	36.5 KB	RuckusAP-1":":":"::"	c4:01:7c:15:6c:e0
34:4d:f7:60:03:61	2014-12-05 00:20:30.230	00:03:55.903	-106	-93	19	1.5	Authorized	181.5 KB	RuckusAP-1":":":"::"	c4:01:7c:15:6c:e0
f0:27:65:4c:1a:f2	2014-12-04 22:31:05.884	00:00:05.919	-108	0	0	0.00	Authorized	150 B	RuckusAP-	c4:01:7c:15:6c:e0

Number of Sessions

The Number of Sessions report displays sessions per radio over time, authorized vs. unauthorized clients, and session distribution per radio (2.4 GHz vs. 5 GHz).

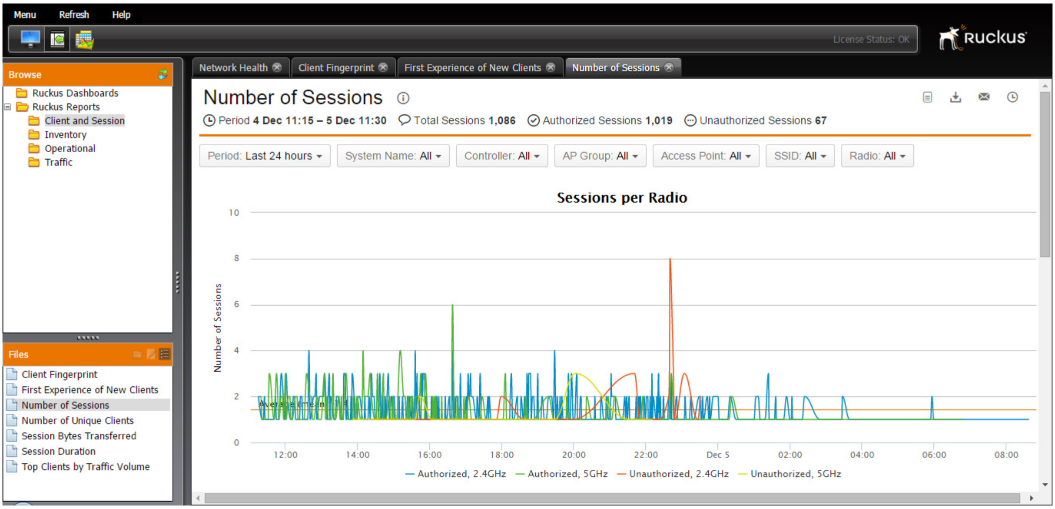
Examples of how this report could be used by network administrators:

- Used to analyze the number of devices on the network at any given time. Can be applied to network dimensioning, looking at possible revenue (e.g., from SPoT or advertising), etc.

Notes:

- A user may have multiple devices on the network, e.g., an iPhone and iPad. In this case, the number of sessions would be reported as 2 (devices), not 1 (user).
- A user may have one device on the network at two different times (e.g., from 1:03pm to 1:08pm and 2:25pm to 2:45pm). In this case, the number of sessions would be reported as 2 (sessions), not 1 (user).

Figure 18. Number of Sessions report



Number of Sessions

Period **4 Dec 11:15 – 5 Dec 11:30** Total Sessions **1,086** Authorized Sessions **1,019** Unauthorized Sessions **67**

Period: Last 24 hours ▾ System Name: All ▾ Controller: All ▾ AP Group: All ▾ Access Point: All ▾ SSID: All ▾ Radio: All ▾

Number of Unique Clients

This report displays the total number of unique subscriber devices during a specific time interval and which radio they are connected to.

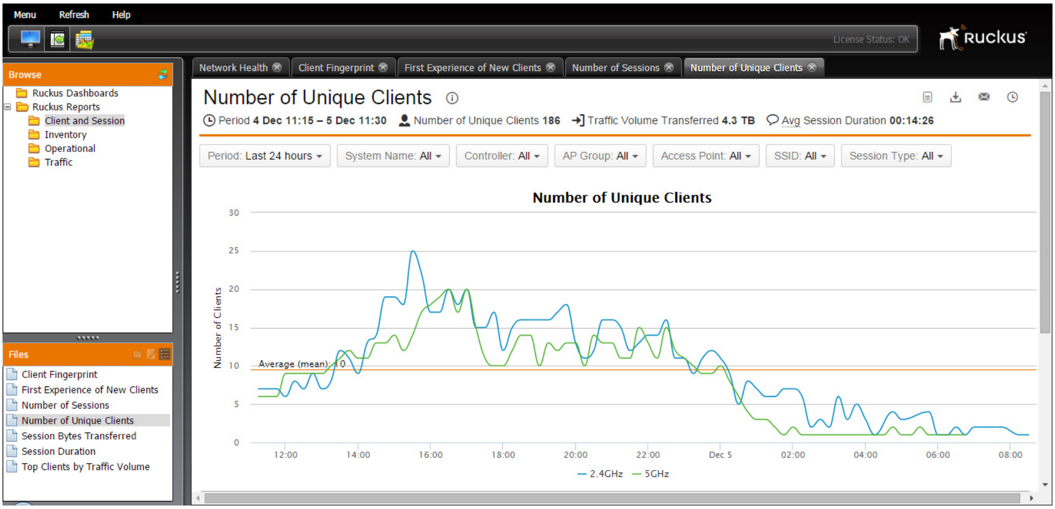
Examples of how this report could be used by network administrators:

- Used to analyze the number of unique subscriber devices using WiFi. Can also be used in conjunction with other reports to determine average number of devices/subscription.

Notes:

- A mobile device can associate to the WLAN during different time intervals and thus have multiple sessions. The device's MAC address is used to bind these multiple sessions together.

Figure 19. Number of Unique Clients report



Period 4 Dec 11:15 – 5 Dec 11:30 Number of Unique Clients 186 Traffic Volume Transferred 4.3 TB Avg Session Duration 00:14:26

Period: Last 24 hours System Name: All Controller: All AP Group: All Access Point: All SSID: All Session Type: All

Session Bytes Transferred

This report shows cumulative unicast traffic volume transmitted to or received by VAPs from STAs whose sessions begin and end during a specific time interval. In addition, the report shows a CDF of cumulative session traffic.

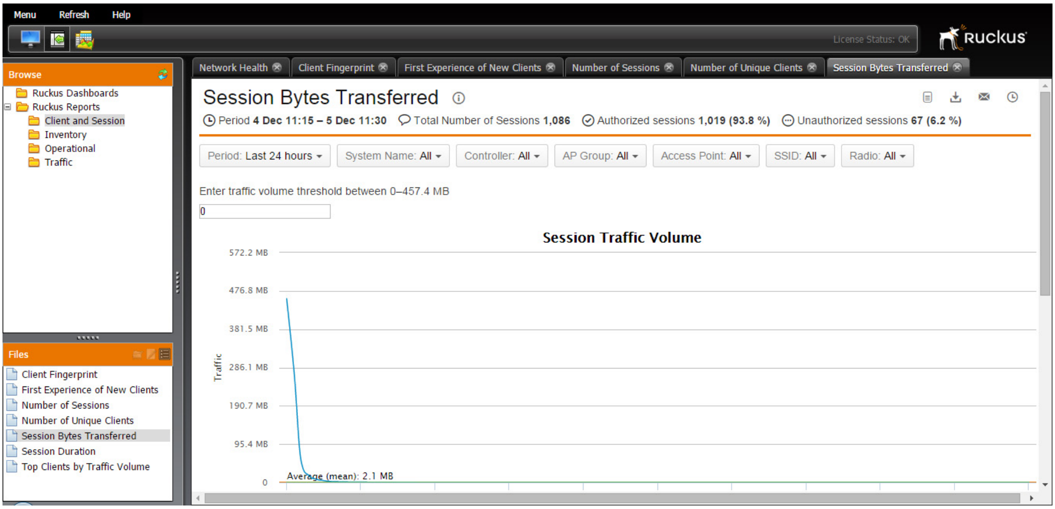
Examples of how this report could be used by network administrators:

- Track the session usage to determine how much traffic and where users are consuming data.

Notes:

- Included in session bytes are the number of bytes in successfully transmitted MSDUs.

Figure 20. Session Bytes Transferred report



Session Bytes Transferred

Period **4 Dec 11:15 – 5 Dec 11:30** Total Number of Sessions **1,086** Authorized sessions **1,019 (93.8 %)** Unauthorized sessions **67 (6.2 %)**

Period: Last 24 hours System Name: All Controller: All AP Group: All Access Point: All SSID: All Radio: All

Enter traffic volume threshold between 0–457.4 MB

0

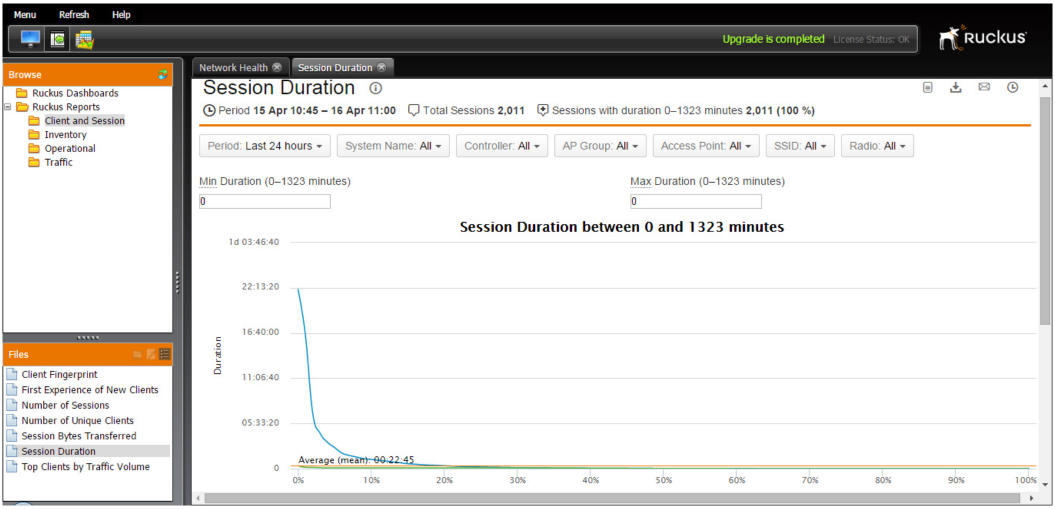
Session Duration

This report is a cumulative distribution function (CDF) of the mobile devices' session durations that exceed a user-specified duration which occurred during a given time interval. The session duration length is defined by the user.

Examples of how this report could be used by network administrators:

- Used to analyze how long users are on the network. Service delivery can then be optimized accordingly.

Figure 21. Session Duration report



Period 15 Apr 10:45 – 16 Apr 11:00 Total Sessions 2,011 Sessions with duration 0–1323 minutes 2,011 (100 %)

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All

Min Duration (0–1323 minutes): 0

Max Duration (0–1323 minutes): 0

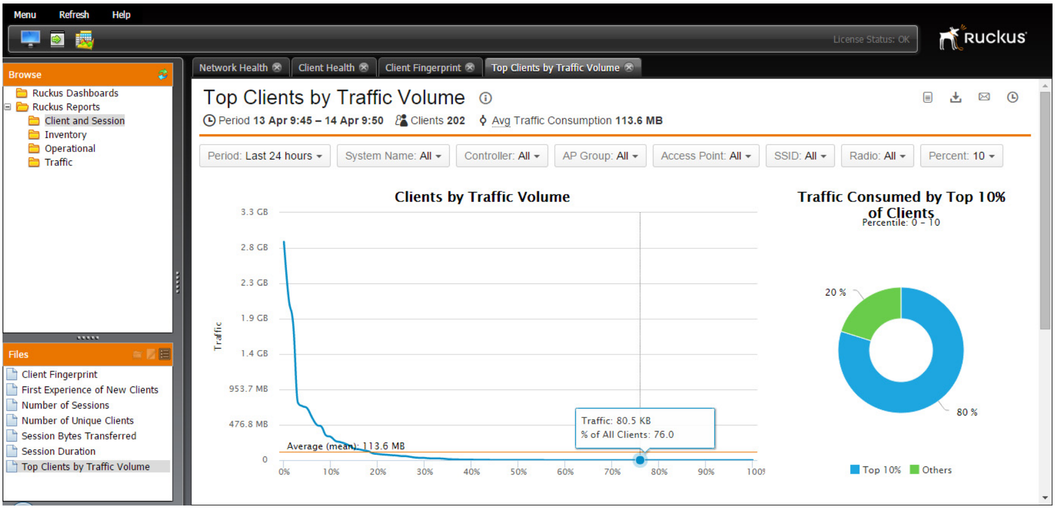
Top Clients by Traffic Volume

This report shows top N mobile devices having the greatest cumulative unicast traffic volume transmitted to or received from a VAP during a specific time interval. The data is represented as a Cumulative Distribution Function (CDF).

Examples of how this report could be used by network administrators:

- Track high-volume users, identify their subscriptions and potentially target for throttling or band steering.
- Discover natural “break points” in usage patterns. Make consequent future subscription price adjustments or set data caps.

Figure 22. Top Clients by Traffic Volume report



Top Clients by Traffic Volume

Period 13 Apr 9:45 – 14 Apr 9:50 Clients 202 Avg Traffic Consumption 113.6 MB

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All | Percent: 10

Traffic: 80.5 KB
% of All Clients: 76.0

Inventory Reports

Inventory reports consist of AP, Controller and Session inventories.

- AP Inventory
- Controller Inventory
- Session Inventory

AP Inventory

This report shows the list of all currently reachable APs in the WiFi network connected to a ZD or SmartZone controller during a given time interval.

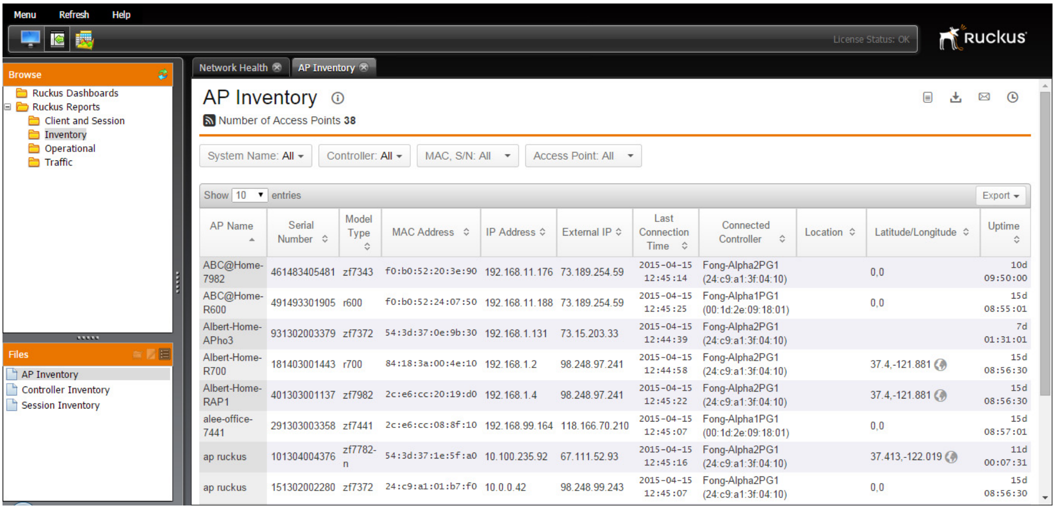
Examples of how this report could be used by network administrators:

- Used to ensure all the APs in the network are administratively and operationally online and enabled.

Notes:

- The following data is included in the report for each AP: name, serial number, model type (e.g., ZF-7982), MAC address, IP address, external IP address, last connection time, connected controller, location (string), latitude/longitude (if available) and uptime.
- The SZ version of this report will be provided in a future release.
- Click the “Globe” icon (🌐)to view the AP on Google Maps.

Figure 23. AP Inventory report



AP Inventory

Number of Access Points **38**

System Name: All | Controller: All | MAC, S/N: All | Access Point: All

Show 10 entries

AP Name	Serial Number	Model Type	MAC Address	IP Address	External IP	Last Connection Time	Connected Controller	Location	Latitude/Longitude	Uptime
ABC@Home-7982	461483405481	zf7343	f0:b0:52:20:3e:90	192.168.11.176	73.189.254.59	2015-04-15 12:45:14	Fong-Alpha2PG1 (24:c9:a1:3f:04:10)		0,0	10d 09:50:00
ABC@Home-R600	491493301905	r600	f0:b0:52:24:07:50	192.168.11.188	73.189.254.59	2015-04-15 12:45:25	Fong-Alpha1PG1 (00:1d:2e:09:18:01)		0,0	15d 08:55:01
Albert-Home-APho3	931302003379	zf7372	54:3d:37:0e:9b:30	192.168.1.131	73.15.203.33	2015-04-15 12:44:39	Fong-Alpha2PG1 (24:c9:a1:3f:04:10)			7d 01:31:01
Albert-Home-R700	181403001443	r700	84:18:3a:00:4e:10	192.168.1.2	98.248.97.241	2015-04-15 12:44:58	Fong-Alpha2PG1 (24:c9:a1:3f:04:10)		37.4,-121.881	15d 08:56:30
Albert-Home-RAP1	401303001137	zf7982	2c:e6:cc:20:19:d0	192.168.1.4	98.248.97.241	2015-04-15 12:45:22	Fong-Alpha2PG1 (24:c9:a1:3f:04:10)		37.4,-121.881	15d 08:56:30
alee-office-7441	291303003358	zf7441	2c:e6:cc:08:8f:10	192.168.99.164	118.166.70.210	2015-04-15 12:45:07	Fong-Alpha1PG1 (00:1d:2e:09:18:01)		0,0	15d 08:57:01
ap ruckus	101304004376	zf7782-n	54:3d:37:1e:5f:a0	10.100.235.92	67.111.52.93	2015-04-15 12:45:16	Fong-Alpha2PG1 (24:c9:a1:3f:04:10)		37.413,-122.019	11d 00:07:31
ap ruckus	151302002280	zf7372	24:c9:a1:01:b7:f0	10.0.0.42	98.248.99.243	2015-04-15 12:45:07	Fong-Alpha2PG1 (24:c9:a1:3f:04:10)		0,0	15d 08:56:30

Controller Inventory

The Controller Inventory report displays the currently reachable controllers in the WiFi network.

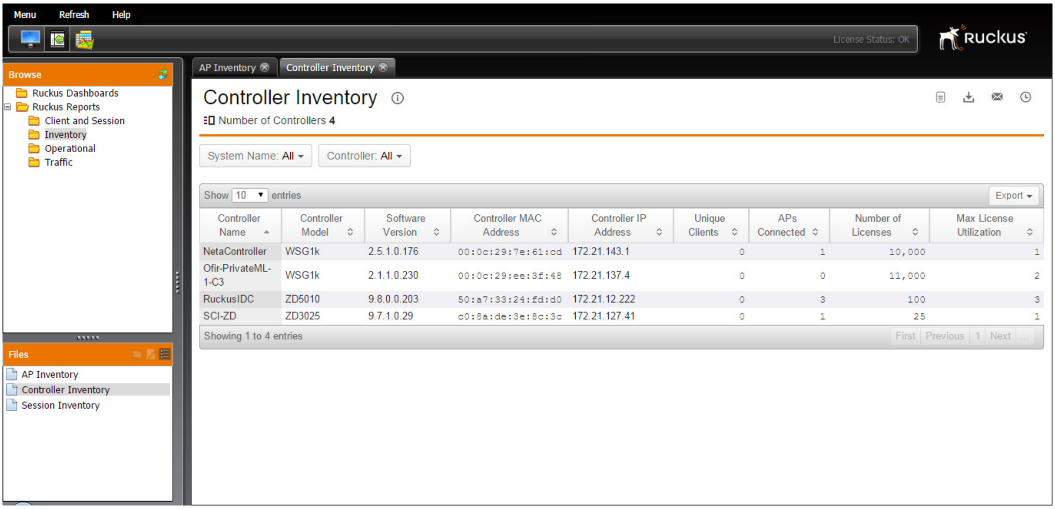
Examples of how this report could be used by network administrators:

- Used to ensure all the controllers in the network are administratively and operationally online and enabled.
- The following data is included in the report for each controller: name, SW version, MAC address, IP address, unique clients, connected APs, number of licenses and maximum license utilization.

Notes:

- The SZ version of this report will be provided in a future release.

Figure 24. Controller Inventory report



Controller Inventory

Number of Controllers **4**

System Name: All ▾ Controller: All ▾

Show 10 ▾ entries Export ▾

Controller Name	Controller Model	Software Version	Controller MAC Address	Controller IP Address	Unique Clients	APs Connected	Number of Licenses	Max License Utilization
NetaController	WSG1k	2.5.1.0.176	00:0c:29:7e:61:cd	172.21.143.1	0	1	10,000	1
Ofir-PrivateML-1-C3	WSG1k	2.1.1.0.230	00:0c:29:ee:3f:48	172.21.137.4	0	0	11,000	2
RuckusIDC	ZD5010	9.8.0.0.203	50:a7:33:24:fd:d0	172.21.12.222	0	3	100	3
SCI-ZD	ZD3025	9.7.1.0.29	c0:8a:de:3e:8c:3c	172.21.127.41	0	1	25	1

Showing 1 to 4 entries First Previous 1 Next ...

Session Inventory

This report is a CSV file which provides a session log for a set of mobile devices during a given time interval.

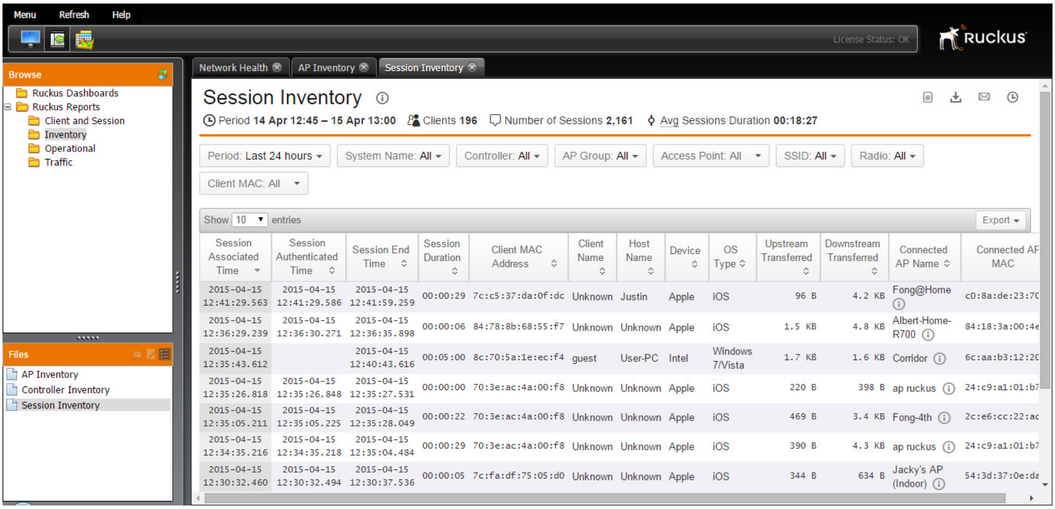
Examples of how this report could be used by network administrators:

- Used to analyze usage statistics using SP defined method; method takes CSV file as input.

Notes:

- Each record in the CSV file contains the mobile devices’ MAC address, device type, OS type, authentication time, association time, session end time, down-stream / upstream bytes transferred and serving AP.
- Mobile devices are selected based on being joined to a particular controller, AP, AP group, SSID or radio.

Figure 25. Session Inventory report



Session Inventory

Period **14 Apr 12:45 – 15 Apr 13:00** Clients **196** Number of Sessions **2,161** Avg Sessions Duration **00:18:27**

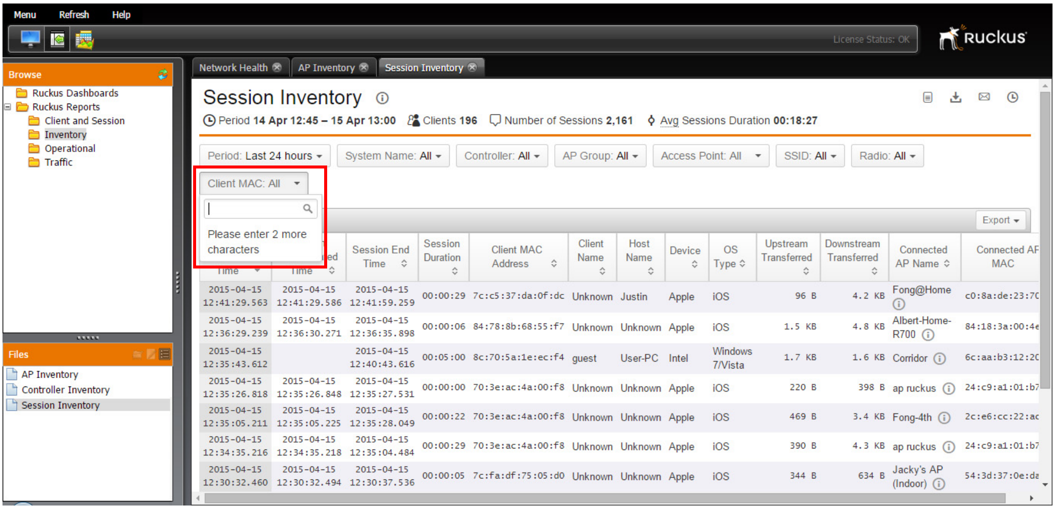
Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All | Client MAC: All

Show 10 entries | Export

Session Associated Time	Session Authenticated Time	Session End Time	Session Duration	Client MAC Address	Client Name	Host Name	Device	OS Type	Upstream Transferred	Downstream Transferred	Connected AP Name	Connected AF MAC
2015-04-15 12:41:29.563	2015-04-15 12:41:29.586	2015-04-15 12:41:59.259	00:00:29	7c:c5:37:da:0f:dc	Unknown	Justin	Apple	iOS	96 B	4.2 KB	Fong@Home	c0:8a:de:23:7c
2015-04-15 12:36:29.239	2015-04-15 12:36:30.271	2015-04-15 12:36:35.898	00:00:06	84:78:8b:68:55:f7	Unknown	Unknown	Apple	iOS	1.5 KB	4.8 KB	Albert-Home-R700	84:18:3a:00:4e
2015-04-15 12:35:43.612		2015-04-15 12:40:43.616	00:05:00	8c:70:5a:1e:ec:f4	guest	User-PC	Intel	Windows 7/Vista	1.7 KB	1.6 KB	Corridor	6c:aa:b3:12:2c
2015-04-15 12:35:26.818	2015-04-15 12:35:26.848	2015-04-15 12:35:27.531	00:00:00	70:3e:ac:4a:00:f8	Unknown	Unknown	Apple	iOS	220 B	398 B	ap ruckus	24:c9:a1:01:b7
2015-04-15 12:35:05.211	2015-04-15 12:35:05.225	2015-04-15 12:35:28.049	00:00:22	70:3e:ac:4a:00:f8	Unknown	Unknown	Apple	iOS	469 B	3.4 KB	Fong-4th	2c:e6:cc:22:ac
2015-04-15 12:34:35.216	2015-04-15 12:34:35.218	2015-04-15 12:35:04.484	00:00:29	70:3e:ac:4a:00:f8	Unknown	Unknown	Apple	iOS	390 B	4.3 KB	ap ruckus	24:c9:a1:01:b7
2015-04-15 12:30:32.460	2015-04-15 12:30:32.494	2015-04-15 12:30:37.536	00:00:05	7c:fa:df:75:05:d0	Unknown	Unknown	Apple	iOS	344 B	634 B	Jacky's AP (Indoor)	54:3d:37:0e:da

This table can be filtered using the search button and searching for clients by MAC address.

Figure 26. Filtering session inventory by client MAC address



Session Inventory

Period **14 Apr 12:45 – 15 Apr 13:00** Clients **196** Number of Sessions **2,161** Avg Sessions Duration **00:18:27**

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All | Client MAC: All

Please enter 2 more characters

Export

Session Associated Time	Session Authenticated Time	Session End Time	Session Duration	Client MAC Address	Client Name	Host Name	Device	OS Type	Upstream Transferred	Downstream Transferred	Connected AP Name	Connected AF MAC
2015-04-15 12:41:29.563	2015-04-15 12:41:29.586	2015-04-15 12:41:59.259	00:00:29	7c:c5:37:da:0f:dc	Unknown	Justin	Apple	iOS	96 B	4.2 KB	Fong@Home	c0:8a:de:23:7c
2015-04-15 12:36:29.239	2015-04-15 12:36:30.271	2015-04-15 12:36:35.898	00:00:06	84:78:8b:68:55:f7	Unknown	Unknown	Apple	iOS	1.5 KB	4.8 KB	Albert-Home-R700	84:18:3a:00:4e
2015-04-15 12:35:43.612		2015-04-15 12:40:43.616	00:05:00	8c:70:5a:1e:ec:f4	guest	User-PC	Intel	Windows 7/Vista	1.7 KB	1.6 KB	Corridor	6c:aa:b3:12:2c
2015-04-15 12:35:26.818	2015-04-15 12:35:26.848	2015-04-15 12:35:27.531	00:00:00	70:3e:ac:4a:00:f8	Unknown	Unknown	Apple	iOS	220 B	398 B	ap ruckus	24:c9:a1:01:b7
2015-04-15 12:35:05.211	2015-04-15 12:35:05.225	2015-04-15 12:35:28.049	00:00:22	70:3e:ac:4a:00:f8	Unknown	Unknown	Apple	iOS	469 B	3.4 KB	Fong-4th	2c:e6:cc:22:ac
2015-04-15 12:34:35.216	2015-04-15 12:34:35.218	2015-04-15 12:35:04.484	00:00:29	70:3e:ac:4a:00:f8	Unknown	Unknown	Apple	iOS	390 B	4.3 KB	ap ruckus	24:c9:a1:01:b7
2015-04-15 12:30:32.460	2015-04-15 12:30:32.494	2015-04-15 12:30:37.536	00:00:05	7c:fa:df:75:05:d0	Unknown	Unknown	Apple	iOS	344 B	634 B	Jacky's AP (Indoor)	54:3d:37:0e:da

Operational Reports

Operational Reports provide information on system operation statistics, such as AP response time, controller hardware resource utilization, and top 10 lists of AP reboots and topology changes.

- AP Groups Response Time Trend
- AP Response Time
- Controller Hardware Utilization
- Distribution of APs by Model
- Rogue APs
- Top APs with Most Topology Changes
- Top AP Reboots
- Top APs with the Longest Response Time

AP Groups Response Time Trend

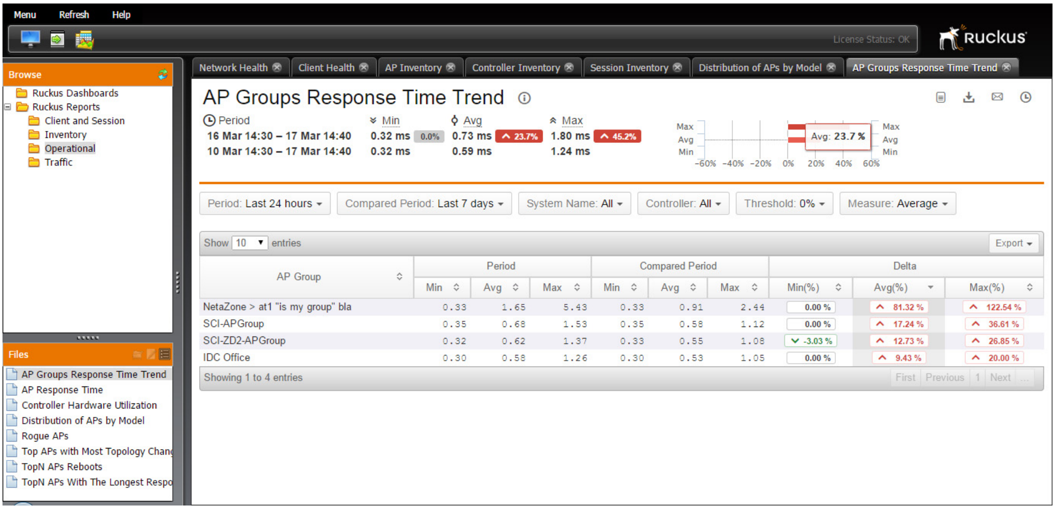
This report shows the Trend of Access Points Response Time (ping), averaged across each AP Group. It can be used to observe cases where the latency of a whole AP Group got worse (or later on, got better, if you took corrective measures) compared to another baseline period. The causes of increased latency could be due to network congestion, faulty hardware, software failure, misconfiguration, etc.

You can click on each AP Group in the table to drill down and see the change per AP within the AP Group.

Examples of how this report could be used by network administrators:

- AP group response times can be used to compare average ping times for an entire AP group over time, allowing the network administrator to see when changes to the network result in increased or decreased latency.

Figure 27. AP Groups Response Time Trend report



AP Groups Response Time Trend

Period	Min	Avg	Max
16 Mar 14:30 – 17 Mar 14:40	0.32 ms 0.0%	0.73 ms ^ 23.7%	1.80 ms ^ 45.2%
10 Mar 14:30 – 17 Mar 14:40	0.32 ms	0.59 ms	1.24 ms

Period: Last 24 hours
Compared Period: Last 7 days
System Name: All
Controller: All
Threshold: 0%
Measure: Average

Show 10 entries

AP Group	Period			Compared Period			Delta		
	Min	Avg	Max	Min	Avg	Max	Min(%)	Avg(%)	Max(%)
NetaZone > at1 "is my group" bla	0.33	1.65	5.43	0.33	0.91	2.44	0.00 %	^ 81.32 %	^ 122.54 %
SCI-APGroup	0.35	0.68	1.53	0.35	0.58	1.12	0.00 %	^ 17.24 %	^ 36.61 %
SCI-ZD2-APGroup	0.32	0.62	1.37	0.33	0.55	1.08	✓ -3.03 %	^ 12.73 %	^ 26.85 %
IDC Office	0.30	0.58	1.26	0.30	0.53	1.05	0.00 %	^ 9.43 %	^ 20.00 %

Showing 1 to 4 entries

AP Response Time

This report shows the ping latency between the SCI and an AP during a specific time interval.

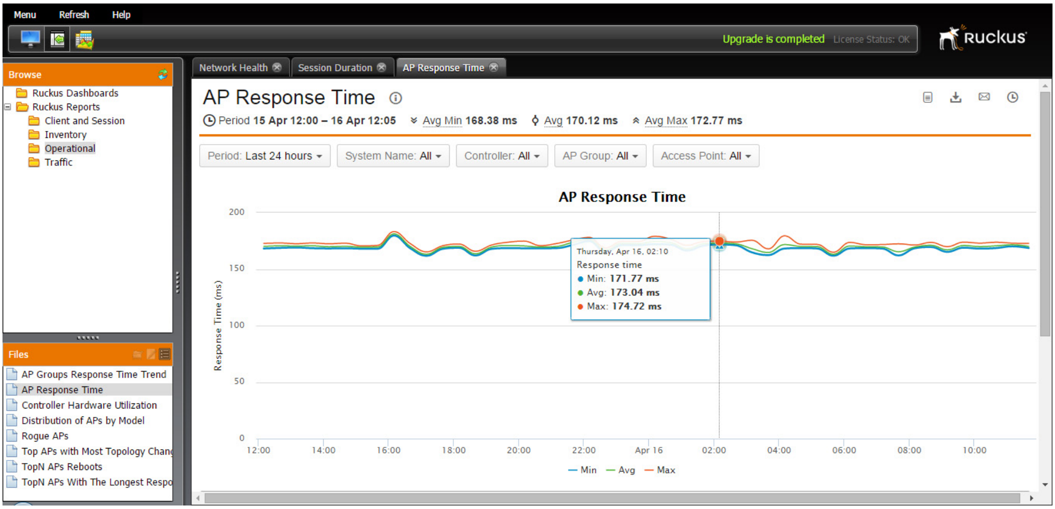
Examples of how this report could be used by network administrators:

- High latency and missing ping responses between the AP and SCI can be used to identify congested links or overloaded/mis-configured switches/routers.

Notes:

- Ping latency measured between AP and SCI was used due to the lack of a ping server on the SZ. Note: the SCI may not be on the "normal" data path taken by user traffic to/from a destination network. Therefore, this statistic's relevance may be limited for some deployments.

Figure 28. AP Response Time



AP Response Time

Period 15 Apr 12:00 – 16 Apr 12:05 Avg Min 168.38 ms Avg 170.12 ms Avg Max 172.77 ms

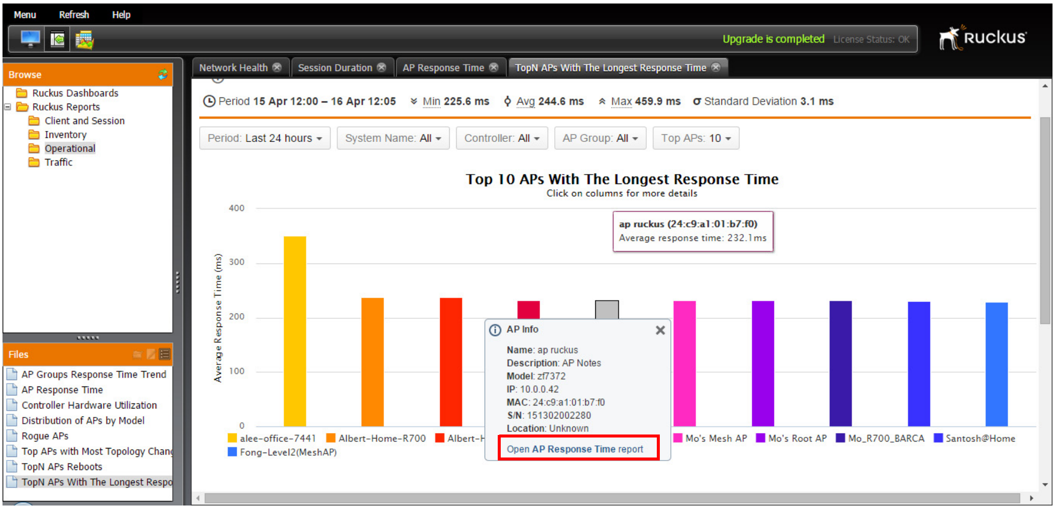
Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All

Thursday, Apr 16, 02:10
Response time
● Min: 171.77 ms
● Avg: 173.04 ms
● Max: 174.72 ms

Individual AP Response Time Report

To view a response time report for an individual AP, click on its bar in the chart, then click the **Open AP Response Time report** link.

Figure 29. Click the link to view an individual AP’s response time report



Period 15 Apr 12:00 – 16 Apr 12:05 Min 225.6 ms Avg 244.6 ms Max 459.9 ms σ Standard Deviation 3.1 ms

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Top APs: 10

ap ruckus (24:c9:a1:01:b7:f0)
Average response time: 232.1ms

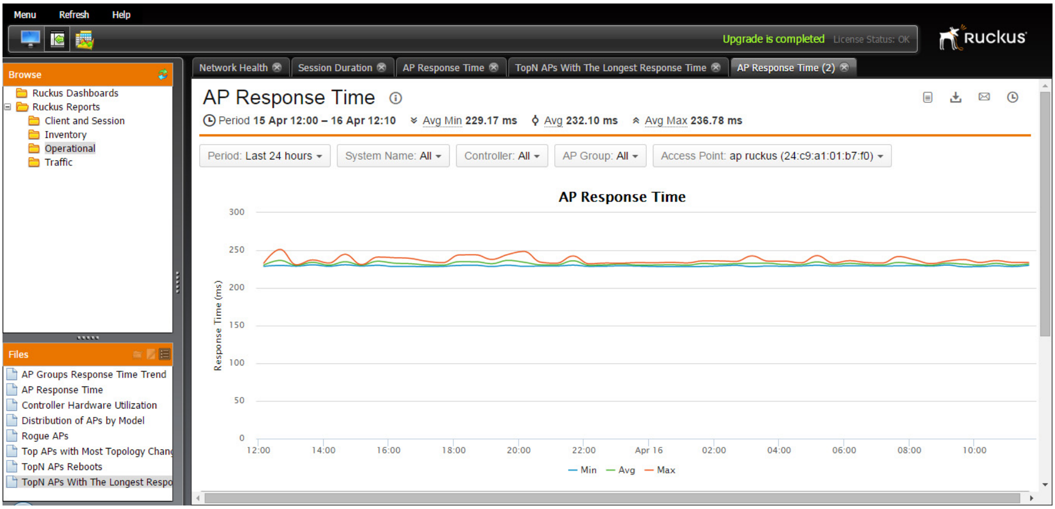
AP Info

Name: ap ruckus
Description: AP Notes
Model: zf7372
IP: 10.0.0.42
MAC: 24:c9:a1:01:b7:f0
S/N: 151302002280
Location: Unknown

Open AP Response Time report

The Response Time report for an individual AP provides the same filter options as the Top N APs With the Longest Response Time report, with the exception of the Access Point filter rather than the number of APs to display filter.

Figure 30. Viewing an individual AP’s response time report



AP Response Time

Period 15 Apr 12:00 – 16 Apr 12:10   Avg Min 229.17 ms   Avg 232.10 ms   Avg Max 236.78 ms

Period: Last 24 hours   System Name: All   Controller: All   AP Group: All   Access Point: ap ruckus (24:c9:a1:01:b7:f0)

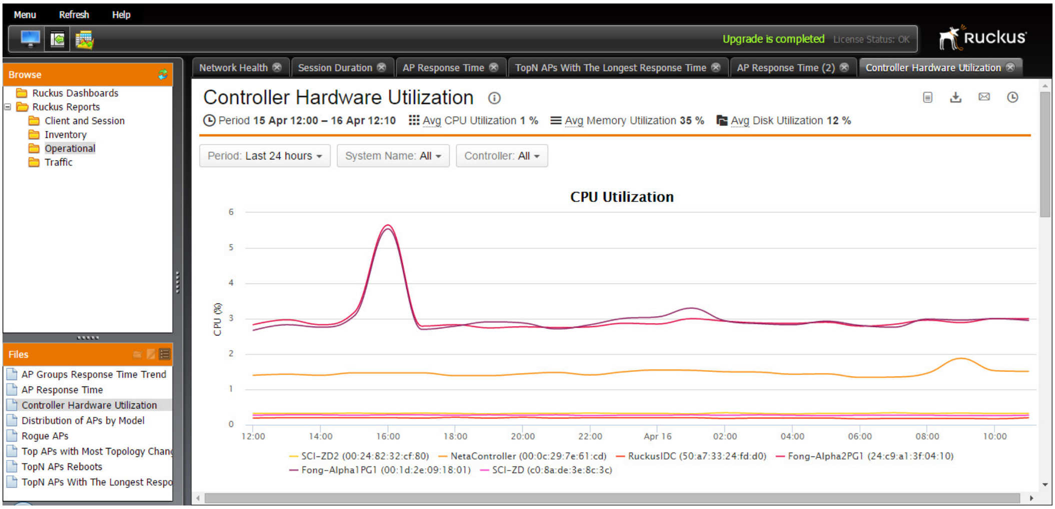
Controller Hardware Utilization

This report shows a ZD or SZ (see note) controller’s CPU, memory and disk utilization during a specific time interval.

Examples of how this report could be used by network administrators:

- Used to predict when a controller will no longer have sufficient processing resources to adequately handle all its joined AP and users.
- Used to identify a software bug (e.g., memory leak or bug causing high CPU utilization).

Figure 31. Controller Hardware Utilization report


Menu
Refresh
Help
Upgrade is completed
License Status: OK
Ruckus
Browse
Ruckus Dashboards
Ruckus Reports
Client and Session
Inventory
Operational
Traffic
Files
AP Groups Response Time Trend
AP Response Time
Controller Hardware Utilization
Distribution of APs by Model
Rogue APs
Top APs with Most Topology Chang
TopN APs Reboots
TopN APs With The Longest Respo
Network Health
Session Duration
AP Response Time
TopN APs With The Longest Response Time
AP Response Time (2)
Controller Hardware Utilization
CPU Utilization
CPU (%)
6
5
4
3
2
1
0
12:00
14:00
16:00
18:00
20:00
22:00
Apr 16
02:00
04:00
06:00
08:00
10:00
SCI-ZD2 (00:24:82:32:cf:80)
NetaController (00:0c:29:7e:61:cd)
RuckusIDC (50:a7:33:24:fd:d0)
Fong-Alpha2PG1 (24:c9:a1:3f:04:10)
Fong-Alpha1PG1 (00:1d:2e:09:18:01)
SCI-ZD (c0:8a:de:3e:8c:3c)

Controller Hardware Utilization

Period **15 Apr 12:00 – 16 Apr 12:10** Avg CPU Utilization **1 %** Avg Memory Utilization **35 %** Avg Disk Utilization **12 %**

Period: Last 24 hours System Name: All Controller: All

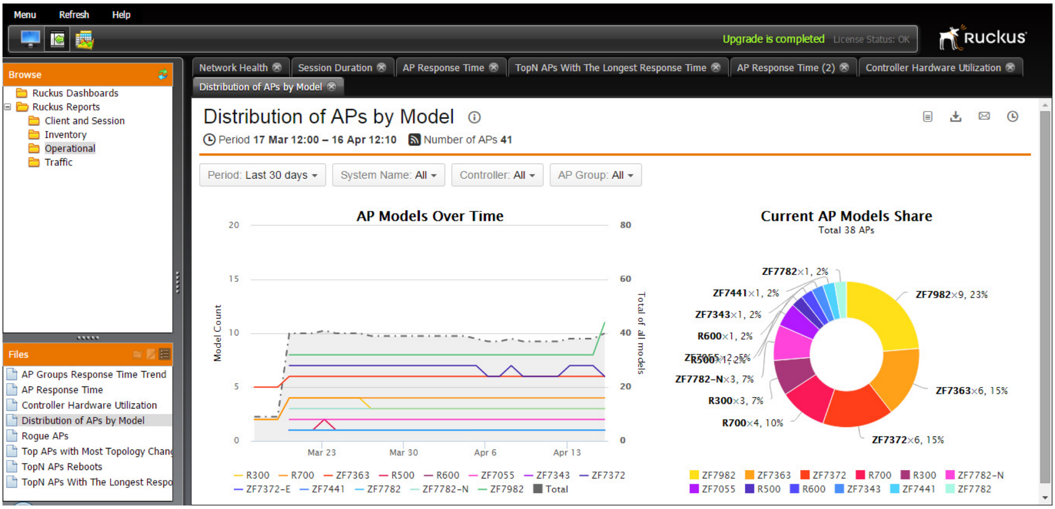
Distribution of APs by Model

This report displays the number of each AP model deployed over time. The AP Models over Time graph can be used to track a deployment as it grows, and see which AP models are increasing and decreasing over time. The pie chart provides a snapshot of the current deployment, displaying the model distribution.

Examples of how this report could be used by network administrators:

- Used by WiFi managers to show the rate of growth and to compare against Ruckus AP licenses. This report could be run monthly or quarterly by the admin to compare against the contracts that they've signed with Ruckus.
- When an issue arises with a particular model, the WiFi administrators will know how many APs of that model they have deployed.

Figure 32. Distribution of APs by Model



Rogue APs

This report can help admins locate and protect the network from malicious APs, maintain data on rogue devices over time, and satisfy legal requirements for wireless security practices. The report displays various types of rogue BSSIDs of rogue APs.

Tips

- Click on a bar chart to filter the table by rogue AP type.
- Click on a table row for details on the AP that is detecting the rogue device.
- Click on the Show AP Info icon at the Reporting AP MAC column of an AP for details on the AP that is reporting the rogue BSSID.

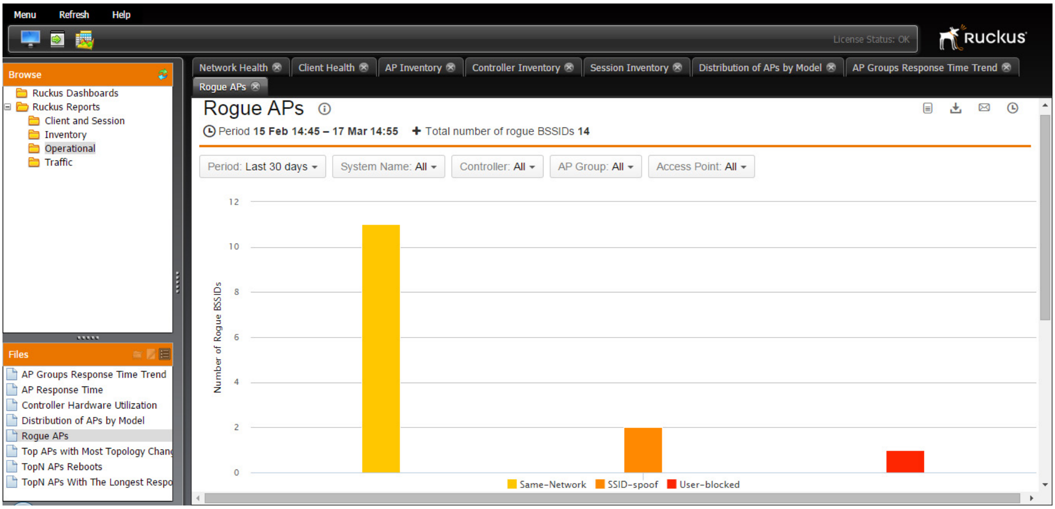
Notes

- Report shows data coming from ZoneDirector only.
- The AP Groups filter selects the AP Groups of the APs that reported the rogue BSSID".
- Chart shows distinct rogue BSSIDs.

Examples of how this report could be used by network administrators:

- An IT Administrator can run this report periodically and go out to locate and disconnect any offending rogue APs when found.
- This report can be run over a longer period to show all the events that occurred and demonstrate that the IT Administrator was diligent in finding and fixing the issues.

Figure 33. Rogue APs



Rogue APs

Period 15 Feb 14:45 – 17 Mar 14:55 ✚ Total number of rogue BSSIDs 14

Period: Last 30 days System Name: All Controller: All AP Group: All Access Point: All

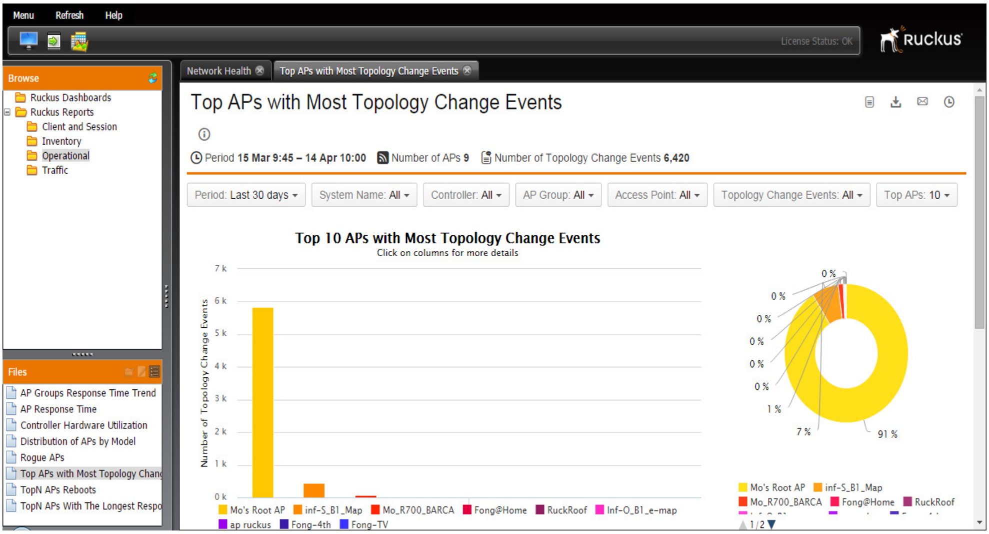
Top APs with Most Topology Changes

This report shows which mesh APs had the most topology change events during a given time interval.

Examples of how this report could be used by network administrators:

- Used to identify mesh APs having deployment issues needing remediation.

Figure 34. Top APs with Most Topology Changes



Menu
Refresh
Help
License Status: OK
Ruckus
Browse
Ruckus Dashboards
Ruckus Reports
Client and Session
Inventory
Operational
Traffic
Files
AP Groups Response Time Trend
AP Response Time
Controller Hardware Utilization
Distribution of APs by Model
Rogue APs
Top APs with Most Topology Chang
TopN APs Reboots
TopN APs With The Longest Respo
Network Health
Top APs with Most Topology Change Events

Top APs with Most Topology Change Events

Period **15 Mar 9:45 – 14 Apr 10:00** Number of APs **9** Number of Topology Change Events **6,420**

Period: Last 30 days | System Name: All | Controller: All | AP Group: All | Access Point: All | Topology Change Events: All | Top APs: 10

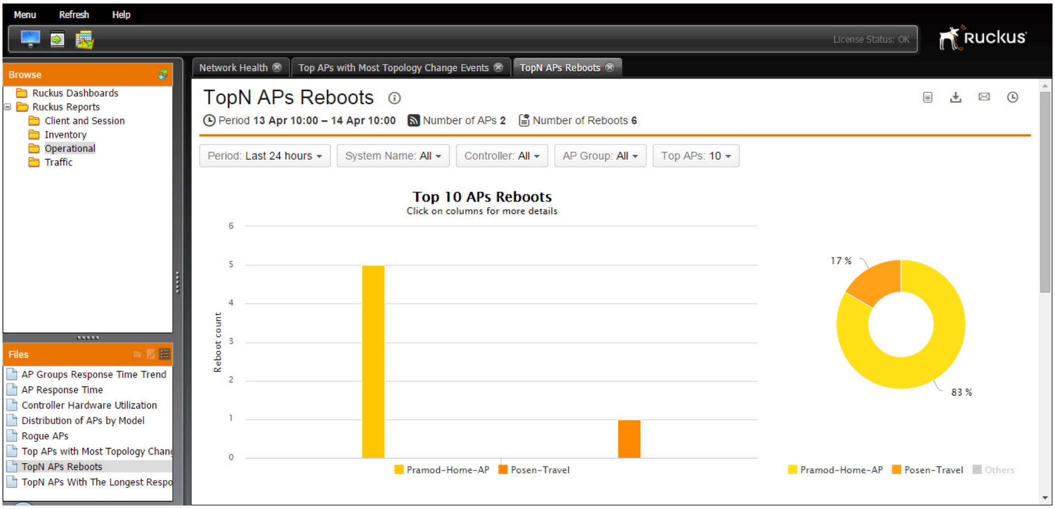
Top AP Reboots

This report shows which APs have been administratively or autonomously rebooted the most during a given time interval.

Examples of how this report could be used by network administrators:

- Used to identify APs having hardware or software defects.
- Used to identify APs succumbing to attackers.

Figure 35. Top 10 AP Reboots report



TopN APs Reboots

Period **13 Apr 10:00 – 14 Apr 10:00** Number of APs **2** Number of Reboots **6**

Period: Last 24 hours · System Name: All · Controller: All · AP Group: All · Top APs: 10

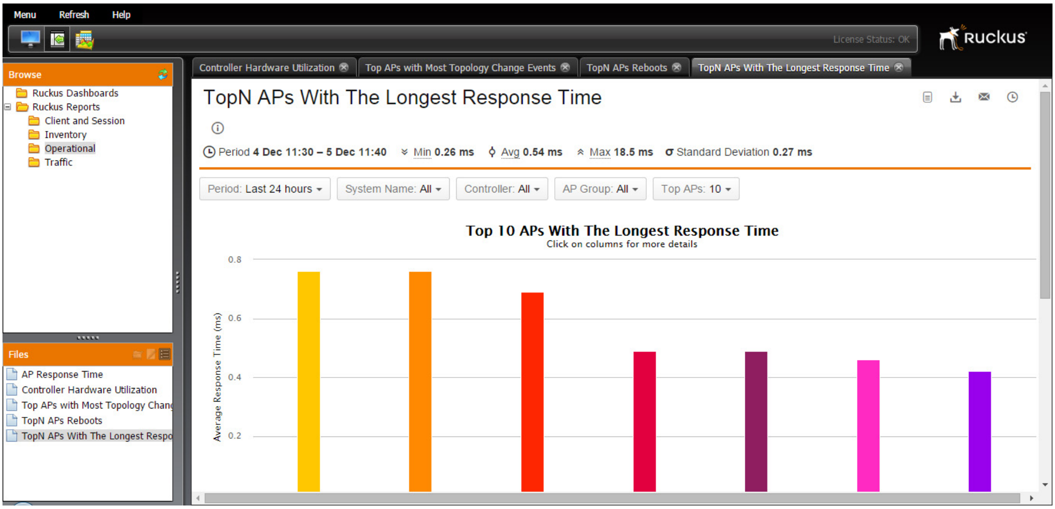
Top APs with the Longest Response Time

This report shows the APs having the greatest ping latency between themselves and the SCI during a specific time interval.

Examples of how this report could be used by network administrators:

- Identify paths in the wired/wireless network having performance problems.
- In mesh networks, identify mesh APs having excessive interference or supporting too many downlink mesh APs (e.g., poor mesh topology).

Figure 36. Top APs with the Longest Response Time report



Menu
Refresh
Help
License Status: OK
Ruckus
Browse
Ruckus Dashboards
Ruckus Reports
Client and Session
Inventory
Operational
Traffic
Files
AP Response Time
Controller Hardware Utilization
Top APs with Most Topology Chang
TopN APs Reboots
TopN APs With The Longest Respo
Controller Hardware Utilization
Top APs with Most Topology Change Events
TopN APs Reboots
TopN APs With The Longest Response Time
Top 10 APs With The Longest Response Time
Click on columns for more details
0.8
0.6
0.4
0.2
Average Response Time (ms)

TopN APs With The Longest Response Time

Period 4 Dec 11:30 – 5 Dec 11:40 Min 0.26 ms Avg 0.54 ms Max 18.5 ms σ Standard Deviation 0.27 ms

Period: Last 24 hours ▾ System Name: All ▾ Controller: All ▾ AP Group: All ▾ Top APs: 10 ▾

Traffic Reports

Traffic Reports consist of actual AP and client throughput reports as well as client throughput potential and top APs by traffic volume.

- Access Point Traffic
- Client Potential Throughput
- Throughput Estimate of Clients
- Top APs by Traffic Volume

Access Point Traffic

This report provides the cumulative volume of unicast traffic transmitted to or received from mobile devices associated to any WLAN on a physical AP for a specific time interval. Note that the reported traffic is actually traffic density (traffic/time); the value of the traffic reported is scaled to the time dimension on the x-axis of the graph (e.g., traffic/15-min, traffic/hour, traffic/day).

The graph displays user traffic only by default. Select **Mgmt Rx by AP** or **Mgmt Tx by AP** to display management receive/transmit traffic.

Examples of how this report could be used by network administrators:

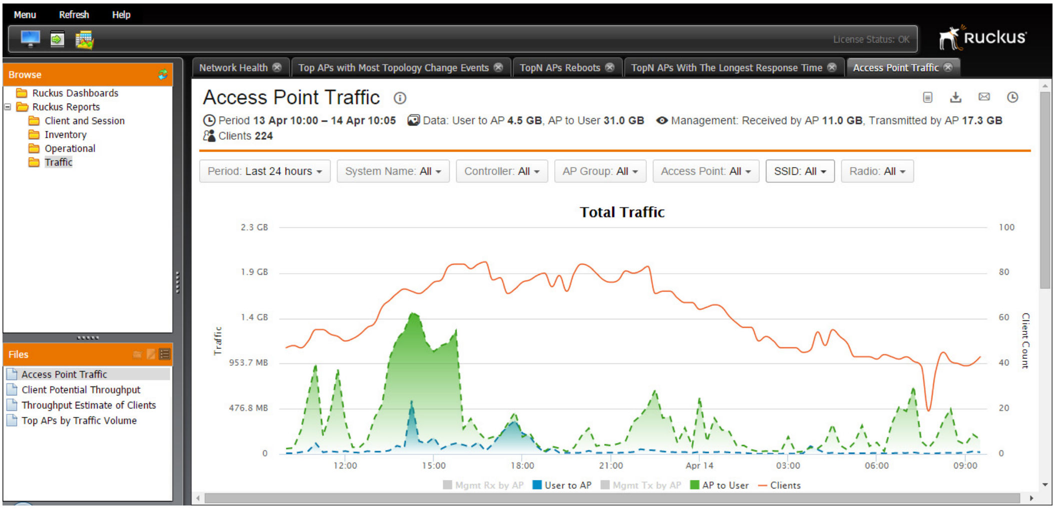
- How busy the AP is with traffic to/from users (includes unicast/multicast packets).
- How much traffic is uploaded vs. downloaded.
- Find network locations which are the busy areas.
- View the relative proportion of total traffic (user + management) to management traffic.

Notes:

- Data used to create the report includes STA session statistics from all VAPs configured on a [physical] AP.
- Includes both 2.4- and 5-GHz radios (if present) on an AP.
- Includes the following traffic:
  - IP datagrams carrying client traffic.
  - Non IP, layer-3 packets.
  - Network-layer management traffic a STA needs to access network resources
  - Data link layer traffic above the 802.11 MAC).

  - Mesh AP backhaul traffic.
- Includes 802.11 management frame traffic.

Figure 37. Access Point Traffic report



Access Point Traffic

Period **13 Apr 10:00 – 14 Apr 10:05** Data: User to AP **4.5 GB**, AP to User **31.0 GB** Management: Received by AP **11.0 GB**, Transmitted by AP **17.3 GB**
Clients **224**

Period: Last 24 hours · System Name: All · Controller: All · AP Group: All · Access Point: All · SSID: All · Radio: All

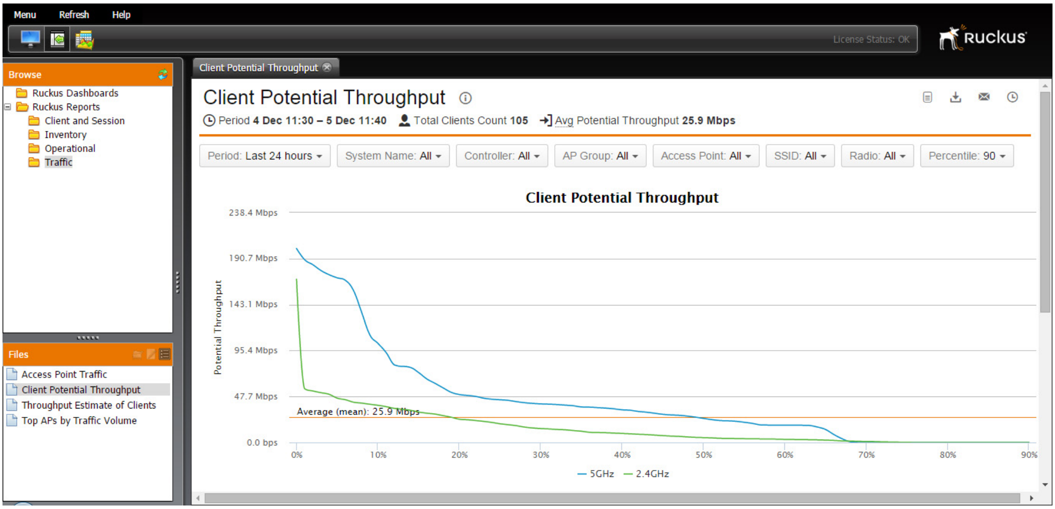
Client Potential Throughput

The Client Potential Throughput report displays the saturated RF channel capacity between an AP radio and given STA. The saturated throughput can be thought of as the throughput an AP would achieve if there were a continuous stream of data for only this STA given the achievable over-the-air PHY layer data-rate and the local interference environment on the RF channel.

Examples of how this report could be used by network administrators:

- The report can be used to determine how much capacity is available to subscribers at that location at that time of day. If throughputs are low in a given area, it can indicate there is foreign interference present or too much 802.11 interference. The 802.11 interference could come from surrounding ESSs (i.e., not the ESS being analyzed by SCI) or self interference.
- The report can be used to see if there is sufficient bandwidth available to subscribers and if the numbers are low, perhaps it's a candidate for adding additional APs or moving the location, etc.

Figure 38. Client Potential Throughput report



Period **4 Dec 11:30 – 5 Dec 11:40** Total Clients Count **105** Avg Potential Throughput **25.9 Mbps**

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All | Percentile: 90

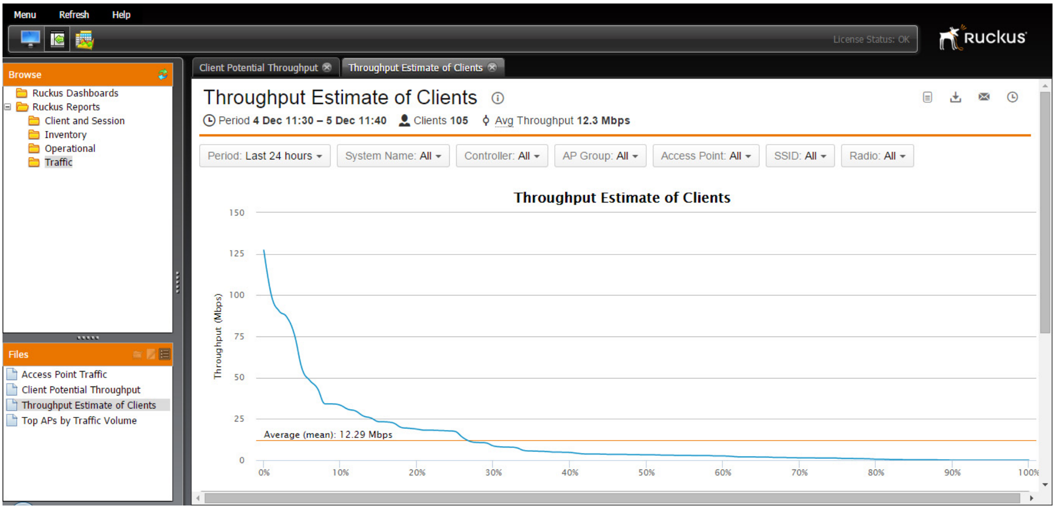
Throughput Estimate of Clients

The Throughput Estimate of Clients report displays the devices with the greatest cumulative unicast and multicast traffic volume transmitted to or received during a specific time interval. The data is represented as a Cumulative Distribution Function (CDF).

Examples of how this report could be used by network administrators:

- Provides a measure of network performance by identifying the top throughput speeds possible for users.
- Can be used in conjunction with Client Fingerprint report to determine the best performing mobile devices in the WLAN.

Figure 39. Throughput Estimate of Clients report



Throughput Estimate of Clients

Period 4 Dec 11:30 – 5 Dec 11:40 Clients 105 Avg Throughput 12.3 Mbps

Period: Last 24 hours · System Name: All · Controller: All · AP Group: All · Access Point: All · SSID: All · Radio: All

Average (mean): 12.29 Mbps

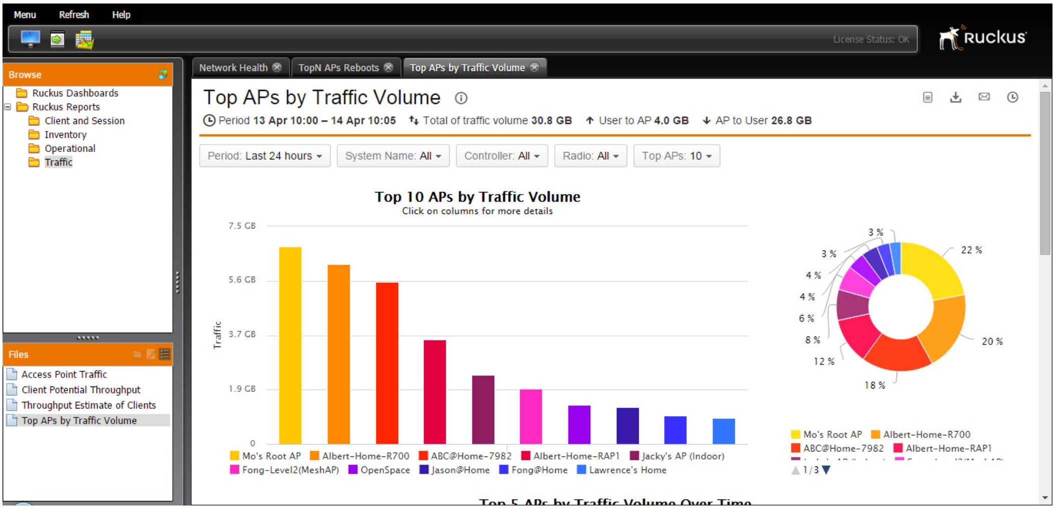
Top APs by Traffic Volume

This report shows the physical APs having the greatest cumulative volume of unicast and multicast traffic transmitted to or received from mobile devices associated to any of its WLANs during a specific time interval. The pie chart represents what percentage of the total traffic in the network is consumed by the N APs. The default value for N is 10.

Examples of how this report could be used by network administrators:

- Find the busiest APs and locations in the network.

Figure 40. Top APs by Traffic Volume report



Top APs by Traffic Volume

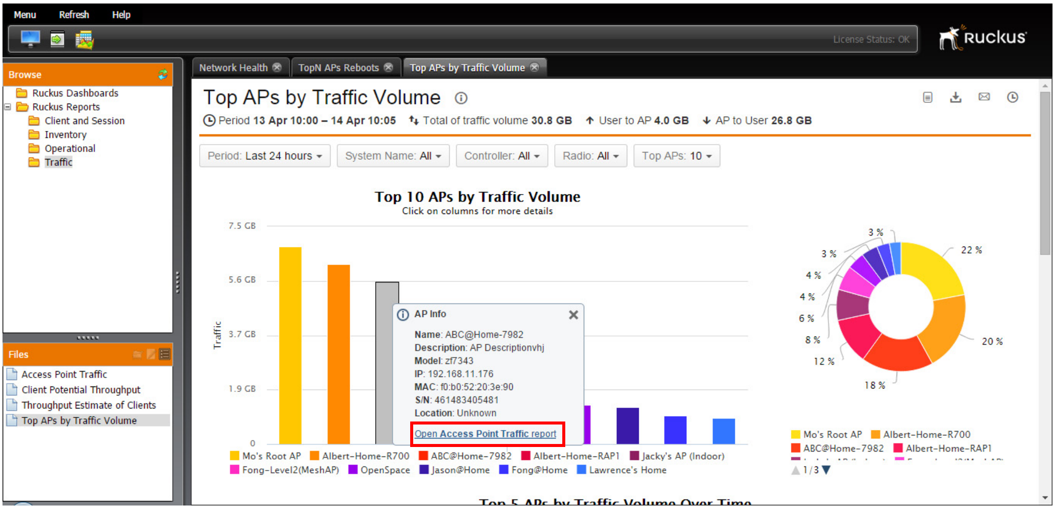
Period 13 Apr 10:00 – 14 Apr 10:05 Total of traffic volume 30.8 GB User to AP 4.0 GB AP to User 26.8 GB

Period: Last 24 hours System Name: All Controller: All Radio: All Top APs: 10

Individual AP Traffic Report

To view a traffic report for an individual AP, click on its bar in the chart, then click the **Open Access Point Traffic report** link.

Figure 41. Click the link to view an individual AP’s traffic report



Top APs by Traffic Volume

Period 13 Apr 10:00 – 14 Apr 10:05 Total of traffic volume 30.8 GB User to AP 4.0 GB AP to User 26.8 GB

Period: Last 24 hours System Name: All Controller: All Radio: All Top APs: 10

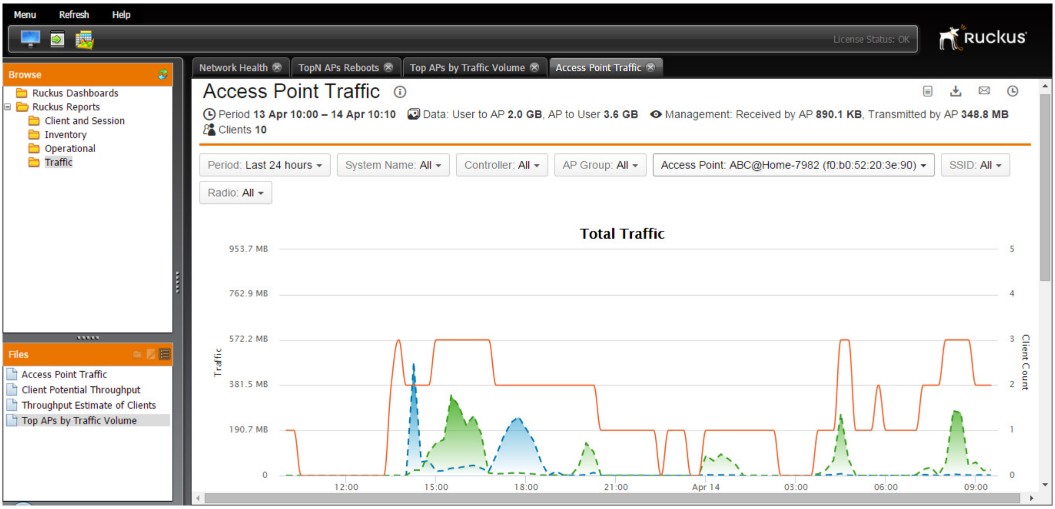
AP Info

Name: ABC@Home-7982
Description: AP Descriptionvhj
Model: zf7343
IP: 192.168.11.176
MAC: f0:b0:52:20:3e:90
S/N: 461483405481
Location: Unknown

Open Access Point Traffic report

The Access Point Traffic report for an individual AP provides the same filter options as the Top N AP traffic report, with the exception of the Access Point filter rather than the number of APs to display filter.

Figure 42. Viewing an individual AP's traffic report



Access Point Traffic

Period **13 Apr 10:00 – 14 Apr 10:10** Data: User to AP **2.0 GB**, AP to User **3.6 GB** Management: Received by AP **890.1 KB**, Transmitted by AP **348.8 MB**
Clients **10**

Period: Last 24 hours ▾ | System Name: All ▾ | Controller: All ▾ | AP Group: All ▾ | Access Point: ABC@Home-7982 (f0:b0:52:20:3e:90) ▾ | SSID: All ▾ | Radio: All ▾

Configuring Custom Reports

5

In this chapter:

- Overview of Custom Report Creation
- Creating a New Report
- Available Metrics

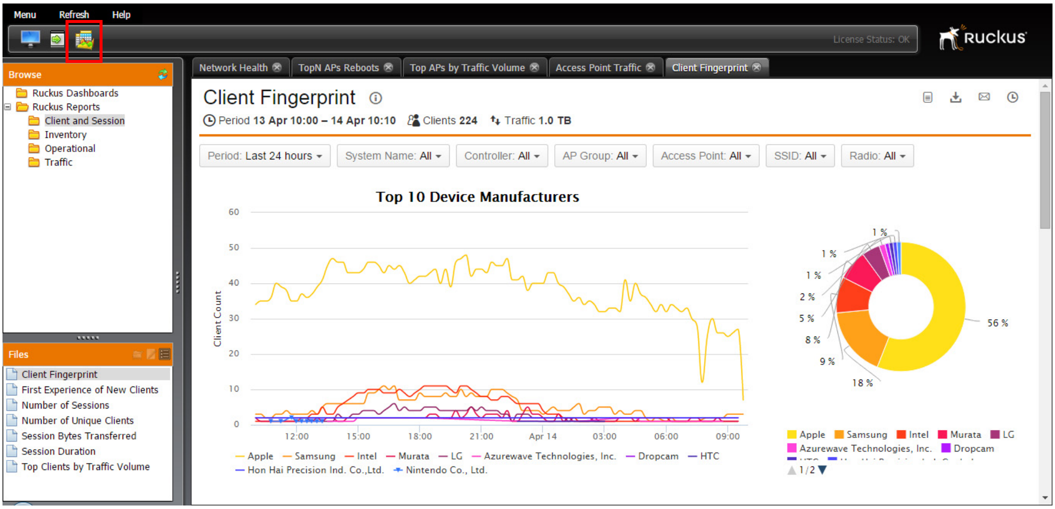
Overview of Custom Report Creation

This chapter describes the procedures for creating custom reports using the New Analyzer Report feature. This feature allows you to query the data in a database without having to understand how the database is structured. You can drill down into the data to discover details that may help you make important business decisions. The Analyzer presents data multi-dimensionally and lets you select which dimensions and measures you want to explore.

The Report Analyzer is an interactive data analysis tool that provides you with a rich drag-and-drop user interface that makes it easy for you to create reports quickly based on your exploration of your data. Once your new report is created, you can display reports in a dashboard to make them available for other users.

To enter the New Analyzer Report creation interface and begin creating a new report, simply click the New Analyzer Report icon on the dashboard.

Figure 43. New Analyzer Report icon



Client Fingerprint

Period 13 Apr 10:00 – 14 Apr 10:10 Clients 224 Traffic 1.0 TB

Period: Last 24 hours ▾ System Name: All ▾ Controller: All ▾ AP Group: All ▾ Access Point: All ▾ SSID: All ▾ Radio: All ▾

Custom Report Schema Changes in SCI 1.3

SCI 1.3 contains significant changes in the Access Point dimensions of Custom Reports schema. Previously created reports (SCI 1.0-1.2) are not silently upgradeable. Therefore, in order to continue using custom reports created in previous SCI versions, the procedure is as follows:

1. During the upgrade process, if no Custom Reports are found, the schema will be upgraded to 1.3 silently.
2. If any custom reports are found by the upgrade process, there are two possible upgrade paths:
   - **a** If the upgrade is performed from SCI 1.0, all reports will be upgraded to a newer Custom Report 1.1 schema. Both schema versions (CR 1.1 and 1.3) will be available in the system.
   - **b** If the upgrade is performed from SCI 1.1 or 1.2, all reports will remain as is. Both schema versions (CR 1.1 and CR 1.3) will be available in the system.
3. The user is required to port all reports from CR 1.1 to CR 1.3 version manually.
4. After the porting process is complete, it is possible to remove all legacy reports together with their CR 1.1 schema, using the /opt/ruckuswireless/sci/scripts/purge_old_schema_with_reports.sh script. This operation is irreversible, unless a previous backup is used to restore the system.
5. In a later SCI versions (post 1.3), no special treatment will be taken for 1.1-based legacy reports.

Creating a New Report

Creating a new report consists of the following steps:

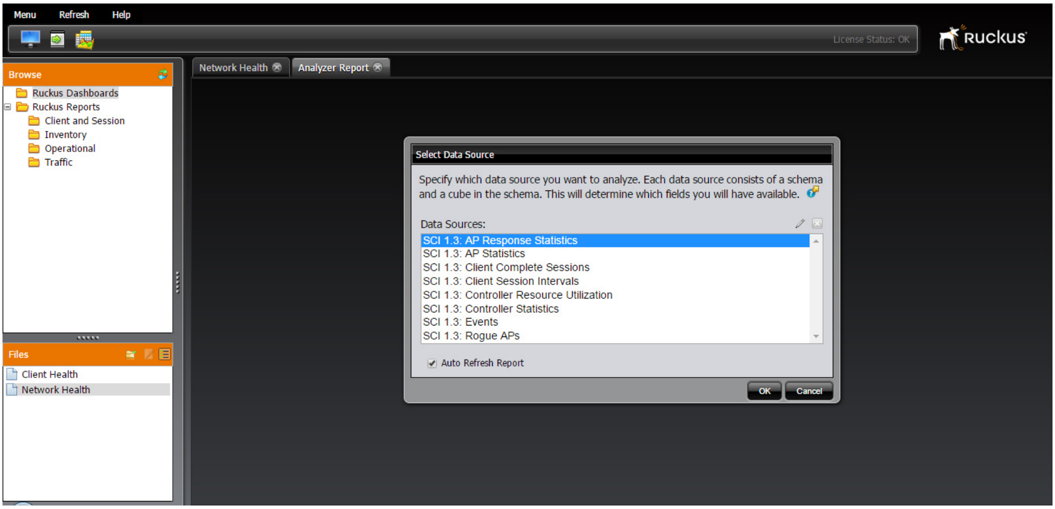
1. Choosing a Data Source
2. Adding Fields and Filters
3. Adding a Description
4. Changing the Chart Type
5. Adding a Description
6. Saving the Report to a Shared Folder
7. Creating Your Own Folder for Custom Reports

Choosing a Data Source

To create a new blank report from scratch, complete the following steps:

1. Click the **New Analyzer Report** icon (📊) to open the *Select Data Source* dialog box.
2. Choose a Data Source which consists of a schema and data set from the list box in the *Select Data Source* dialog box. This choice determines which fields will be available when you build your report. For example, if you selected a data source called “AP Statistics,” all AP-related fields (e.g. number of APs) would be available.
3. Click **OK** to continue.

Figure 44. Select a Data Source



Select Data Source

Specify which data source you want to analyze. Each data source consists of a schema and a cube in the schema. This will determine which fields you will have available.

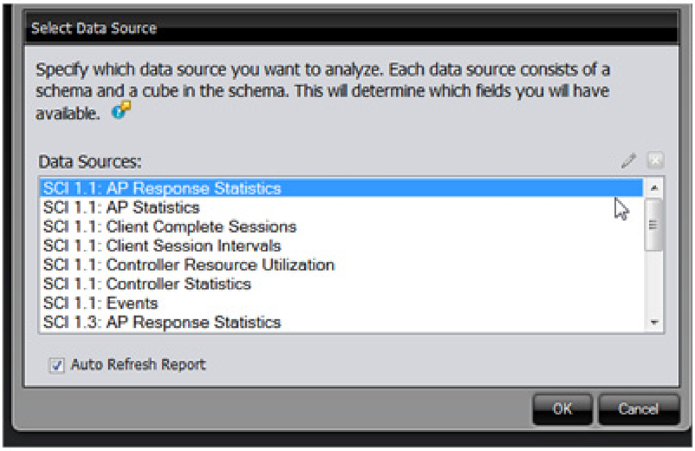
Data Sources:

- SCI 1.3: AP Response Statistics
- SCI 1.3: AP Statistics
- SCI 1.3: Client Complete Sessions
- SCI 1.3: Client Session Intervals
- SCI 1.3: Controller Resource Utilization
- SCI 1.3: Controller Statistics
- SCI 1.3: Events
- SCI 1.3: Rogue APs

☑ Auto Refresh Report

NOTE: If you are upgrading from a previous release with pre-1.3 custom reports created using pre-1.3 schema, the "Select Data Source" dialog will also include data sources that conform to the previous schema, as shown in Figure 45.

Figure 45. Select Data Source with pre-1.3 schema



Select Data Source

Specify which data source you want to analyze. Each data source consists of a schema and a cube in the schema. This will determine which fields you will have available.

Data Sources:

- SCI 1.1: AP Response Statistics
- SCI 1.1: AP Statistics
- SCI 1.1: Client Complete Sessions
- SCI 1.1: Client Session Intervals
- SCI 1.1: Controller Resource Utilization
- SCI 1.1: Controller Statistics
- SCI 1.1: Events
- SCI 1.3: AP Response Statistics

☑ Auto Refresh Report

About Data Sources

Each report must use a single Data Source. The following built-in data sources are available:

- **AP Response Statistics**: Includes measures such as packets transmitted, packets lost percentage, ping total time, minimum, maximum, average and deviance.
- **AP Statistics**: Includes measures such as number of APs, Tx data bytes and Rx data bytes.
- **Client Complete Sessions**: Includes measures such as number of sessions, number of unique clients, session length, Tx and Rx data bytes.
- **Client Session Intervals**: Includes measures such as estimated throughput, maximum/minimum signal strength and RSSI, number of sessions and number of intervals.
- **Controller Resource Utilization**: Includes measures such as CPU, memory and disk usage percentages.
- **Controller Statistics**: Includes measures such as client count, license count and license utilization.
- **Events**: Includes measures such as number of events.
- **Rogue APs**: Includes the Number of Rogue BSSIDs measure and levels such as Rogue AP BSSID & Rogue Type.

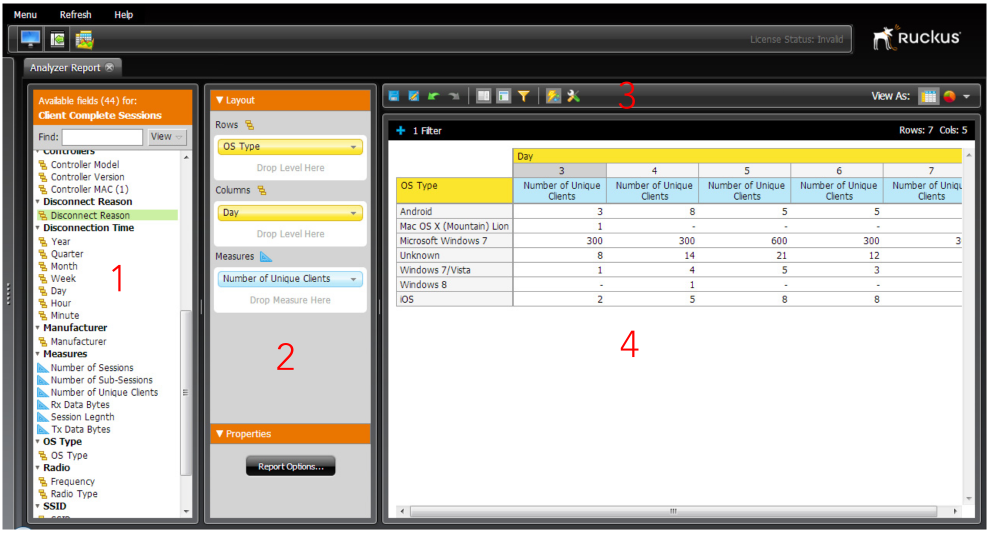
More about Data Sources:

- Each report is tied to one Data Source.
- You cannot change the Data Source for a report.
- Many Data Sources have overlapping fields. For example, the “AP Model” field exists in multiple Data Sources. Therefore, there could be more than one data source that would work for the report that you want to generate.
- The reason you are asked to choose a Data Source before you add fields is that certain fields don't work well together, and using them in the same report leads to incorrect or confusing results. Therefore, Data Sources bundle the appropriate fields together so that your report will make more sense.

The New Analyzer Report Page

Once you have chosen a Data Source, the New Analyzer Report page appears. Figure 46 identifies the main sections of the New Analyzer Report page, and each of these page elements is described in Table 5.

Figure 46. The New Analyzer Report page



	Day				
	3	4	5	6	7
OS Type	Number of Unique Clients	Number of Unique Clients	Number of Unique Clients	Number of Unique Clients	Number of Uniqu Clients
Android	3	8	5	5	
Mac OS X (Mountain) Lion	1	-	-	-	
Microsoft Windows 7	300	300	600	300	3
Unknown	8	14	21	12	
Windows 7/Vista	1	4	5	3	
Windows 8	-	1	-	-	
iOS	2	5	8	8	

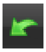
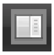
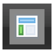
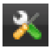
Table 5. New Analyzer Report page elements

Number	Description
1	Available Fields: Choose which fields to include in your report. You can drag fields to the Layout section, drag them directly onto the Report Preview.
2	Layout: Use this section to define the layout of your report.
3	Action Icons: See Table 6 for Action Icon descriptions.
4	Report Preview: Displays the actual report as it is currently defined.

Action Icons

Table 6 describes the Action Icons available from the New Analyzer Report page.

Table 6. Action Icons

Icon	Description
	Save icon
	Save as icon
	Undo icon
	Redo icon
	Hide/show Available Fields icon
	Hide/show Layout panel icon
	Hide/show Filters icon
	Disable/enable Auto refresh icon
	More Actions and Options icon

Adding Fields and Filters

Once you are on the Analyzer Report page, you are ready to add fields and filters. You can do this in any order, but here is a good way to get started:

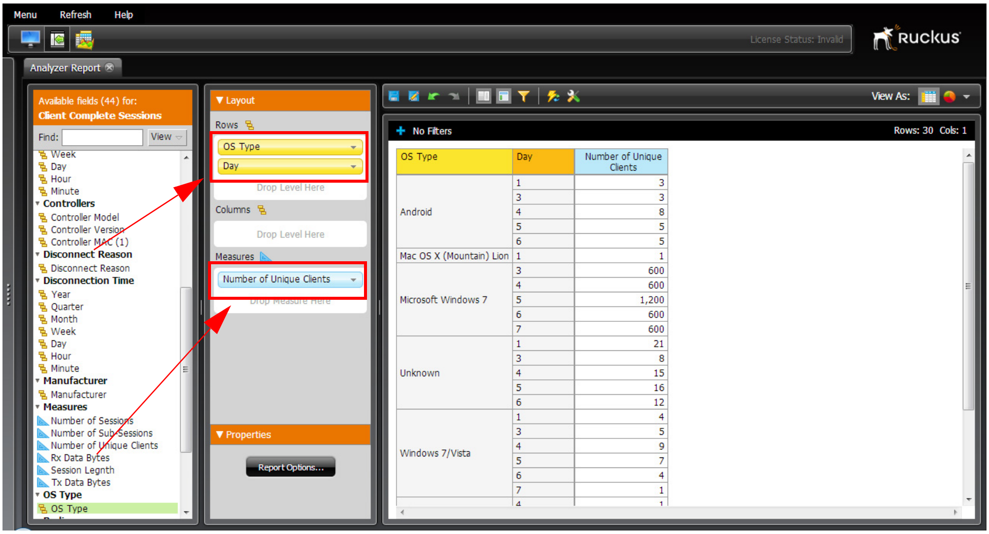
1. Drag a Time Period field (such as Year or Quarter) onto the report.
2. Add a Measure field (such as Number of Sessions, etc).
3. Click the Time Period field on the report, and select Filter from the menu. Choose the time periods you are interested in from the Filter dialog box.

NOTE: You can view the definition of a field by clicking on the field and selecting **Tell me About...** from the menu.

NOTE: Reports make the most sense when they display at least one measure field. (Measure fields are highlighted blue.)

NOTE: Add filters early on. To get the best response time and avoid too much data being displayed, add filters before you drag too many fields onto the report. For example, if you already have two or three fields in the report and you want to add another field that you suspect has hundreds or thousands of values, add a filter to this field before you add it to the report.

Figure 47. Adding fields and measures



OS Type	Day	Number of Unique Clients
Android	1	3
	3	3
	4	8
	5	5
	6	5
Mac OS X (Mountain) Lion	1	1
Microsoft Windows 7	3	600
	4	600
	5	1,200
	6	600
	7	600
Unknown	1	21
	3	8
	4	15
	5	16
	6	12
Windows 7/Vista	1	4
	3	5
	4	9
	5	7
	6	4
	7	1
	4	1

About Fields

Examples of Fields include "AP Model," "SSID," "OS Type," etc. Fields are what define the content of your report.

The following types of fields are available:

Level Fields (Names, Types, Categories, etc.): Level fields are usually text-based. “OS Type” is an example of a Level field. “Android” and “Windows 7/Vista” are examples of possible values for the OS Type field.

Time Period Fields: “Year” and “Month” are examples of Time Period fields. Possible values for these fields could be 2012 and Jan-2011, respectively.

Measure Fields: Measure fields are numeric and most often represent Access Point, client or controller metrics. “Number of Unique Clients” and “Tx Data Bytes” are examples of Measure fields.

Fields are color-coded by type in both the report and the Available Fields panes. The colors are assigned as follows:

- **Level Fields and Time Period Fields**: Orange
- **Measure Fields**: Blue

Viewing the Definition of a Field

Complete the following steps to view the definition of a field:

1. Right-click the field name (in the report or in the list of available fields).
2. Select **Tell me about...** from the menu to open the *About...* dialog box.

The About... dialog box provides the following information:

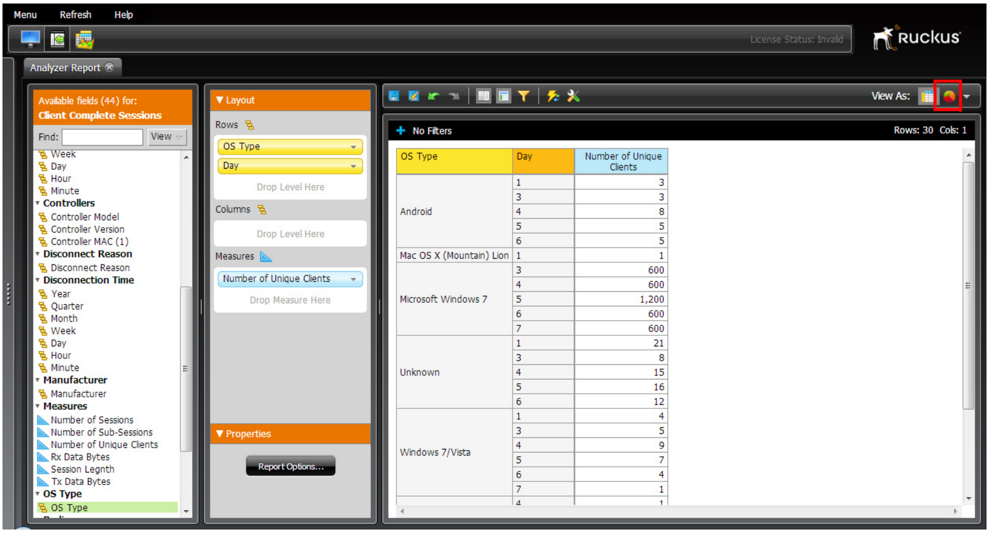
- **Name**: The name of the field as it appears in this report.
- **Type**: The type of field. For more about field types, see "About Fields" on page 76.
- **Description**: The description of the field.
- **MDX**: The data source definition. For example, for the Controller Model field, the MDX value is [Controllers].[Controller Model].
- **Member Properties***: Certain fields contain member properties that can be used to constrain membership to specific values based on these properties.

NOTE: If a field has a number in parenthesis next to its name the field list, this means it has member properties associated with it. You can constrain the data displayed according to one or more of these member properties by selecting **Show Properties** from the drop-down menu of a field after dragging it onto the Layout pane.

Switching to Chart Format

By default, new reports are displayed in table format according to the fields and layouts (rows and columns) that you selected. You can easily switch from table format to any of several chart formats by clicking the **Chart Format** icon.

Figure 48. The Chart Format icon

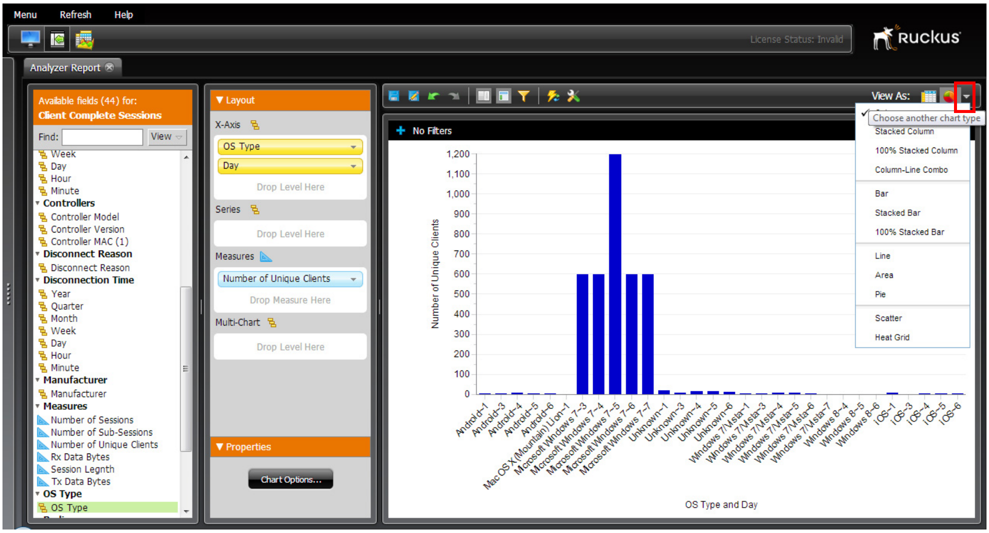


OS Type	Day	Number of Unique Clients
Android	1	3
	3	3
	4	8
	5	5
	6	5
Mac OS X (Mountain) Lion	1	1
Microsoft Windows 7	3	600
	4	600
	5	1,200
	6	600
	7	600
Unknown	1	21
	3	8
	4	15
	5	16
	6	12
Windows 7/Vista	1	4
	3	5
	4	9
	5	7
	6	4
	7	1
	4	1

Changing the Chart Type

Click the **Choose Another Chart Type** icon and select a chart type from the list.

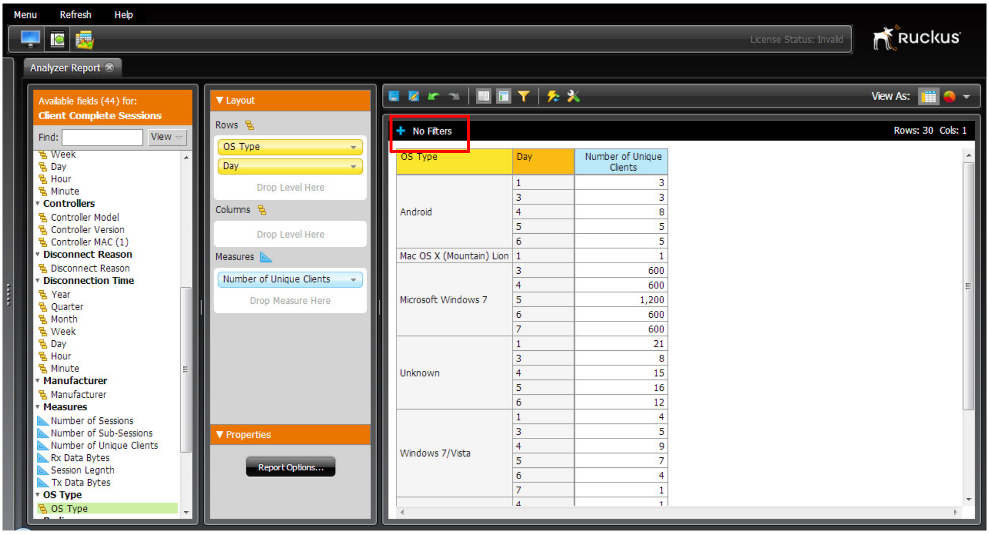
Figure 49. Choose another chart type



Applying Filters to Reports

If your report contains a large amount of data, it is a good idea to apply filters before you add too many additional fields and measures. Click the blue **+** icon (next to “No filters” if there are no filters applied so far).

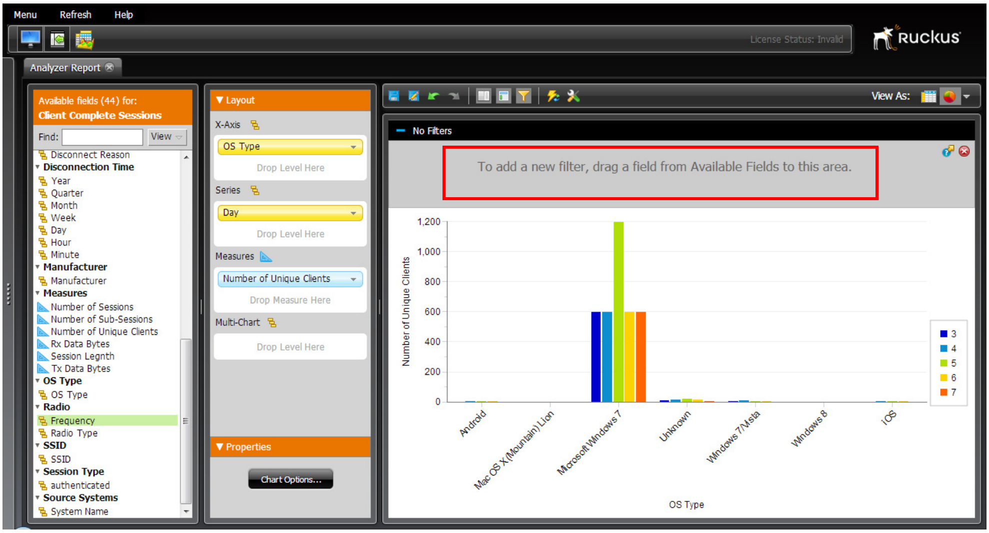
Figure 50. Click the + icon to add a new filter



OS Type	Day	Number of Unique Clients
Android	1	3
	3	3
	4	8
	5	5
	6	5
Mac OS X (Mountain) Lion	1	1
Microsoft Windows 7	3	600
	4	600
	5	1,200
	6	600
	7	600
Unknown	1	21
	3	8
	4	15
	5	16
	6	12
Windows 7/Vista	1	4
	3	5
	4	9
	5	7
	6	4
	7	1
	4	1

When you click the + icon to add a filter, the screen changes to display an area with the label “To add a new filter, drag a field from the Available Fields to this area.”

Figure 51. Drag a field to this area to add a new filter

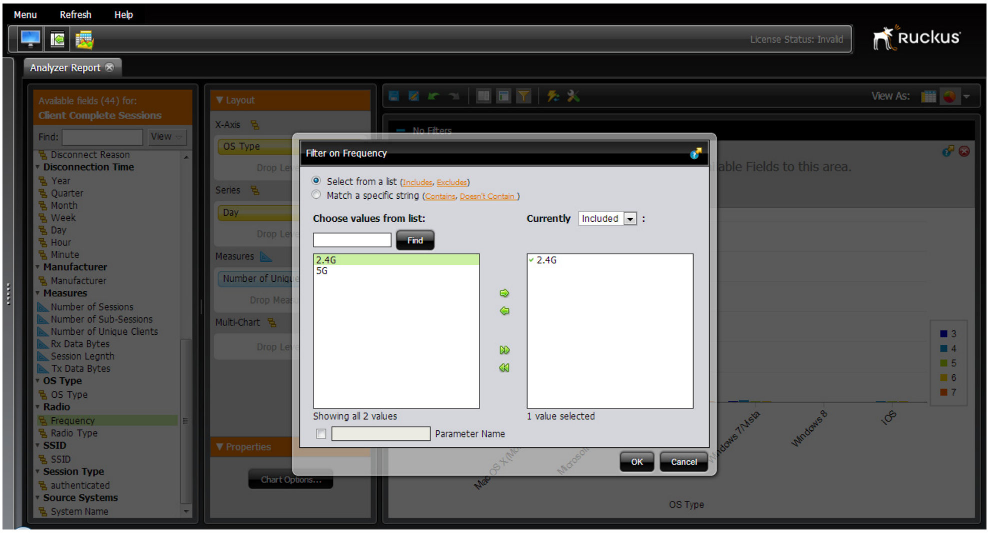


To add a new filter, drag a field from Available Fields to this area.

For example, if you want to filter for only 2.4 GHz clients, drag the **Frequency** field to the add filter section. A “Filter on Frequency” dialog appears, from which you can select which values you want to filter for.

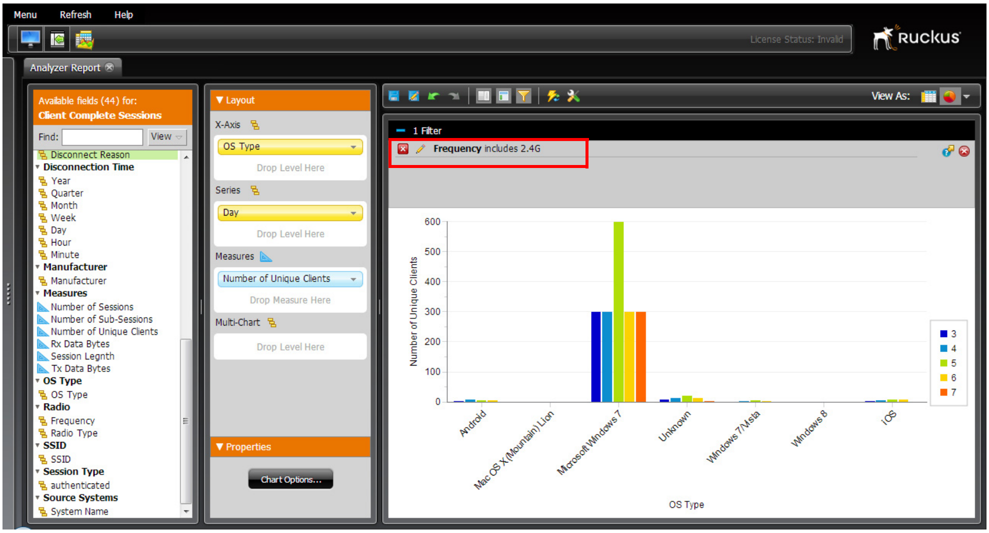
Select **2.4G** from the list, and click the right arrow icon to add it to the filter list. Then click **OK** to confirm.

Figure 52. Add the 2.4G value to filter results for only 2.4G clients



After the filter is applied, you can see which filters are applied in the updated chart view.

Figure 53. Frequency includes 2.4G



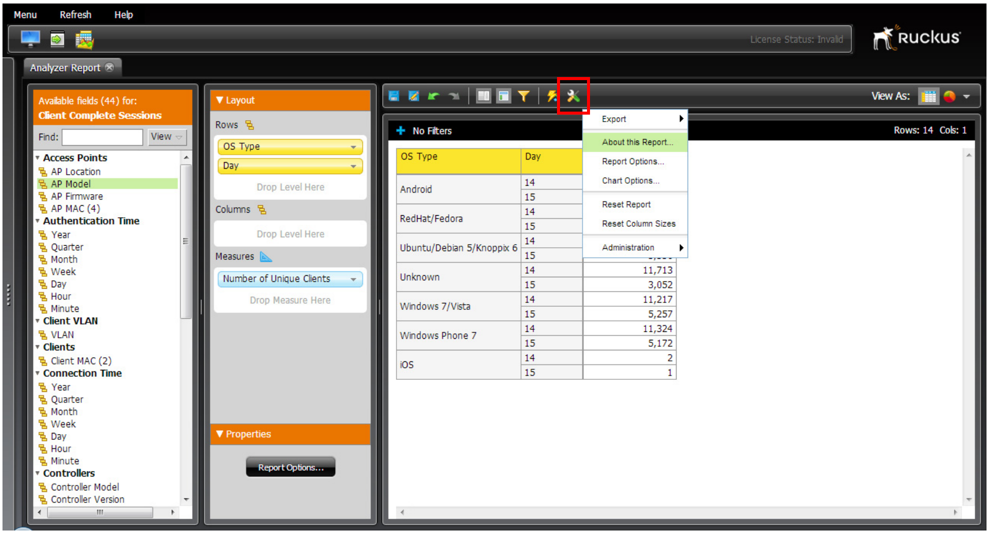
Adding a Description

A description of your report will help other users understand it. Complete the following steps to add, edit, or view a description of a report.

1. Open the report.
2. Click the **More actions and options** icon on the toolbar and select **About this Report…**
3. Use the Description field to add, edit, or view the report description.

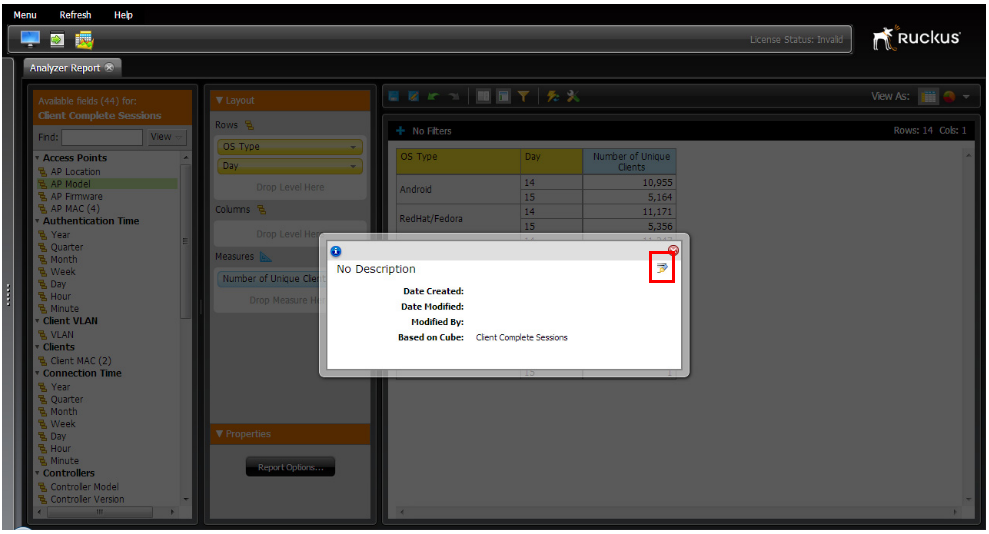
NOTE: You also can view the description on the Report Home page by clicking the Information symbol (i) next to the report.

Figure 54. Select About this Report… from the More Actions list



OS Type	Day	
Android	14	[illegible]
	15	[illegible]
RedHat/Fedora	14	[illegible]
	15	[illegible]
Ubuntu/Debian 5/Knoppix 6	14	[illegible]
	15	[illegible]
Unknown	14	11,713
	15	3,052
Windows 7/Vista	14	11,217
	15	5,257
Windows Phone 7	14	11,324
	15	5,172
iOS	14	2
	15	1

Figure 55. Click the Edit icon to edit the report description

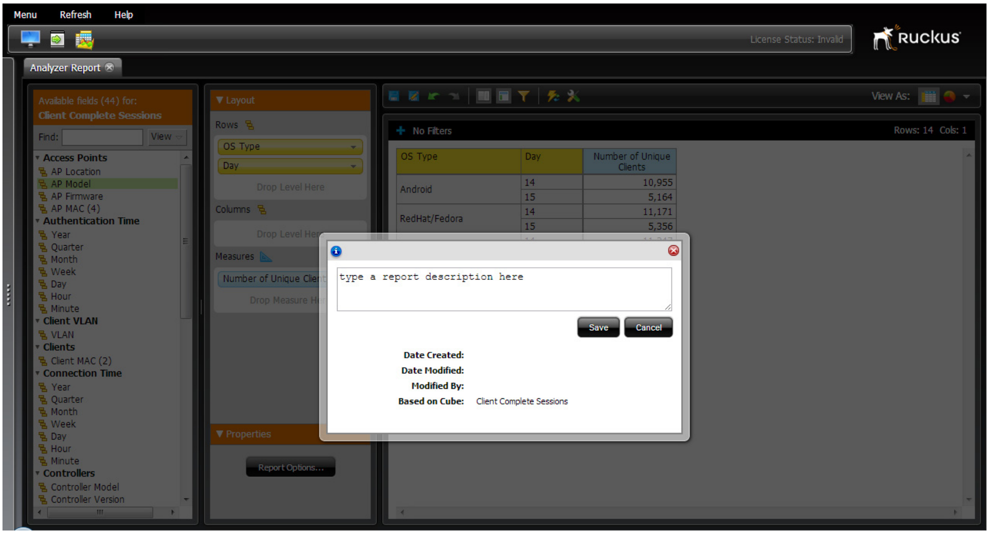


OS Type	Day	Number of Unique Clients
Android	14	10,955
	15	5,164
RedHat/Fedora	14	11,171
	15	5,356

No Description

Date Created:
Date Modified:
Modified By:
Based on Cube: Client Complete Sessions

Figure 56. Type your report description in the text box



OS Type	Day	Number of Unique Clients
Android	14	10,955
	15	5,164
RedHat/Fedora	14	11,171
	15	5,356

```
type a report description here
```

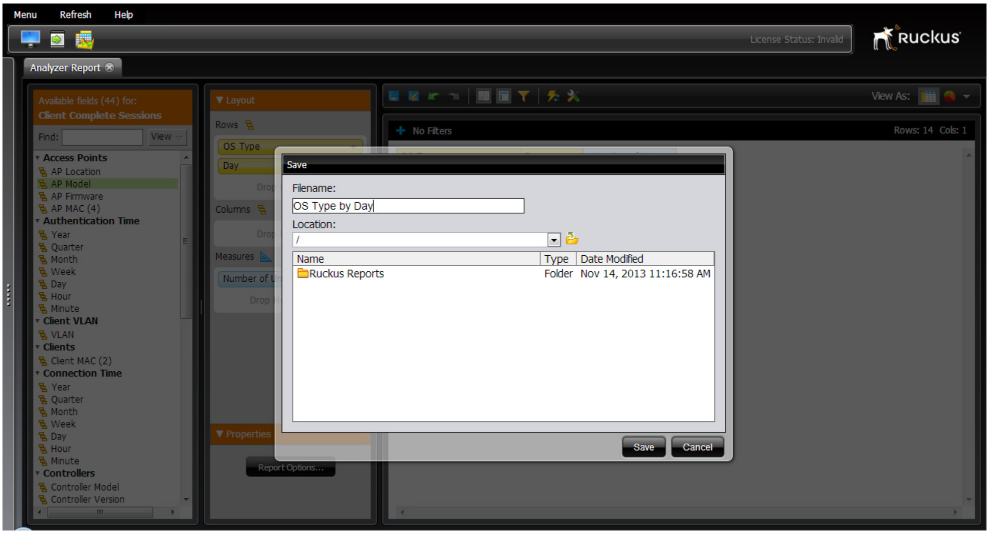
Date Created:
Date Modified:
Modified By:
Based on Cube: Client Complete Sessions

Saving the Report to a Shared Folder

To let other users access a report you create, save your report into a shared folder. In this example, we will save the new report to the existing "Ruckus Reports" folder.

1. Click the **Save Current Report** icon.
2. The **Save** dialog opens. Enter a recognizable name for this report. In this example, we created a report called "OS Type by Day."
3. Browse to your preferred destination directory. In this example, we saved the report in the existing */ruckus-reports/subscriber-and-session* folder.
4. Click **Save** to save your report.

Figure 57. Enter a filename for your report



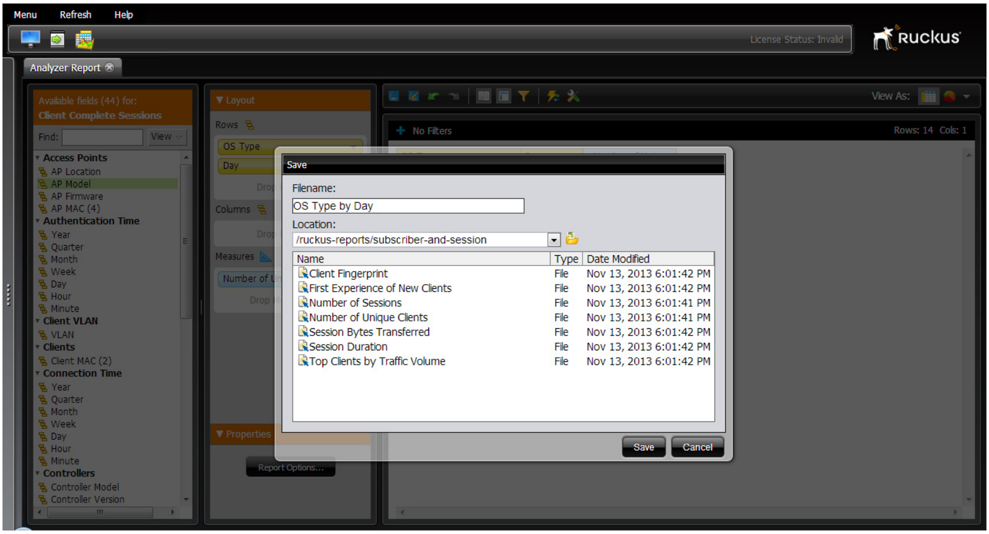
Save

Filename: OS Type by Day

Location: /

Name	Type	Date Modified
Ruckus Reports	Folder	Nov 14, 2013 11:16:58 AM

Figure 58. Save the report to the Subscriber and Session folder



Save

Filename: OS Type by Day

Location: /ruckus-reports/subscriber-and-session

Name	Type	Date Modified
Client Fingerprint	File	Nov 13, 2013 6:01:42 PM
First Experience of New Clients	File	Nov 13, 2013 6:01:42 PM
Number of Sessions	File	Nov 13, 2013 6:01:41 PM
Number of Unique Clients	File	Nov 13, 2013 6:01:41 PM
Session Bytes Transferred	File	Nov 13, 2013 6:01:42 PM
Session Duration	File	Nov 13, 2013 6:01:42 PM
Top Clients by Traffic Volume	File	Nov 13, 2013 6:01:42 PM

Creating Your Own Folder for Custom Reports

In general, Ruckus recommends creating a special folder for your reports under the “Ruckus Reports” folder. In this way, you can have full control over who has access to each of your custom reports.

To create a folder for all of your users:

1 Login as a user with an Admin role.

2 Right click **Ruckus Reports** and click **New Folder...**.

3 Enter a name for the folder, for example “Company Reports”. The new folder appears in the list under Ruckus Reports.

4 Right click your new folder and click **Properties**.

5 In the **Share** tab, click **Add...**.

6 Select user or role, for example, **Authenticated**, and click **OK**.

7 Check **All Permissions** in the *Permissions for Authenticated* section.

8 Click **OK** to apply your changes and close the dialog window.

Figure 59. Create new folder

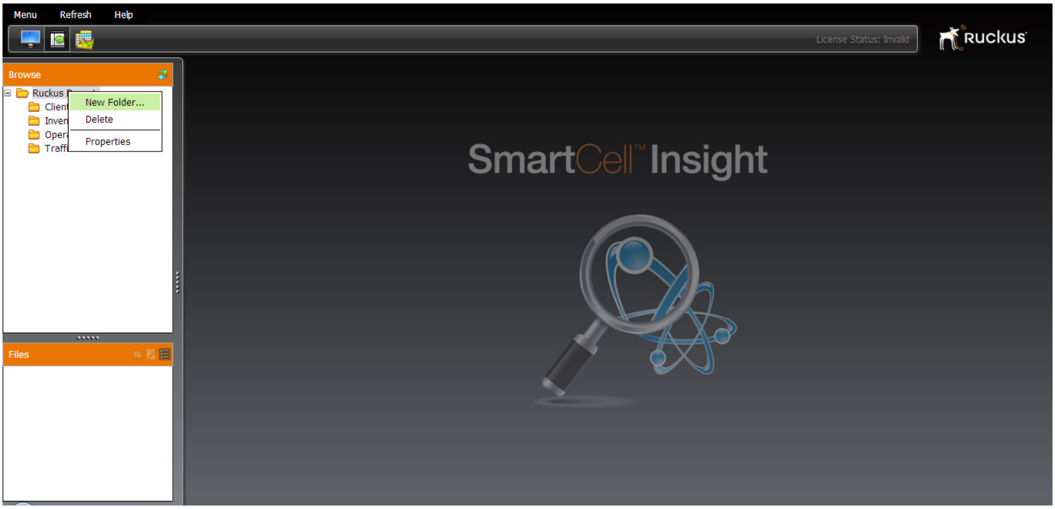
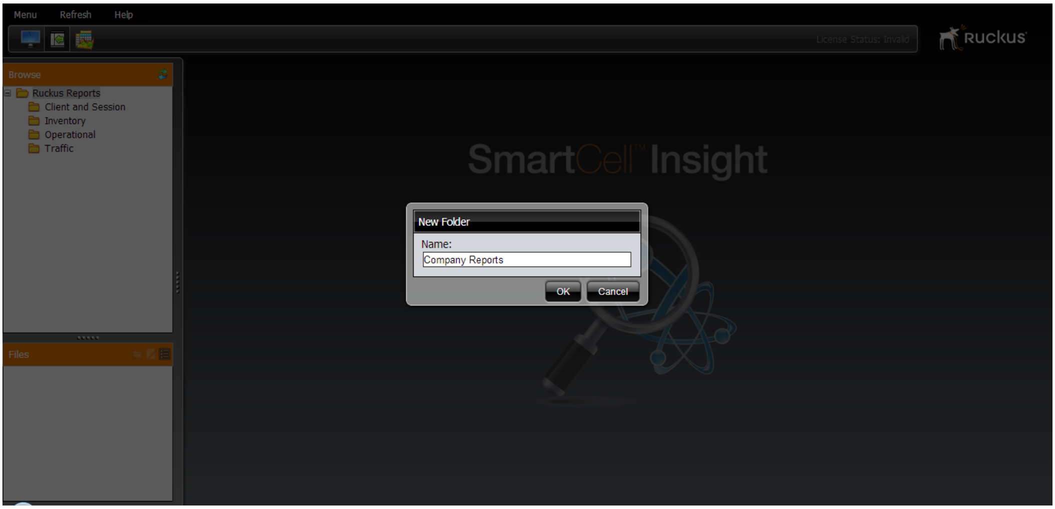
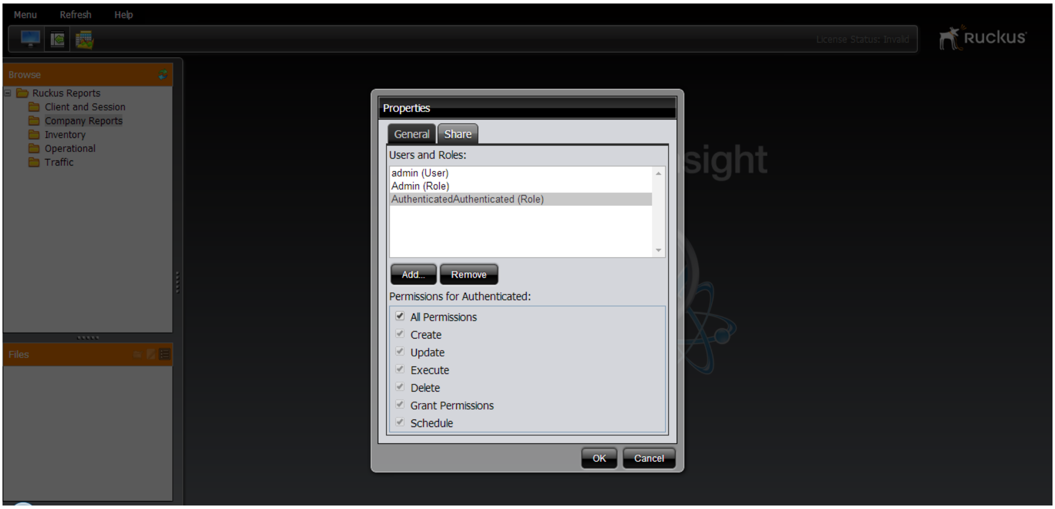


Figure 60. Enter a name for the new folder



Name: Company Reports

Figure 61. Give all permissions to users with the Authenticated role



Properties

General | Share

Users and Roles:

admin (User)
Admin (Role)
AuthenticatedAuthenticated (Role)

Add... | Remove

Permissions for Authenticated:

- ☑ All Permissions
- ☑ Create
- ☑ Update
- ☑ Execute
- ☑ Delete
- ☑ Grant Permissions
- ☑ Schedule

OK | Cancel

Now all users with the *Authenticated* role should have access to this folder and can open and save reports to it.

NOTE: It is best practice to allow only users with advanced permissions (such as *Admin* users) to create reports, while others (such as *Authenticated*) should have permission to execute reports but not to create or save them.

Available Metrics

The following table lists the metrics available for report creation. You can create reports for any combination of these metrics, and filter results by any of the values that exist within each metric for each available data source.

Table 7. Available metrics

Category	Metric
AP Stats	• AP Name, MAC, Description, Serial Number, GPS • Controller Name & MAC • # APs • Tx & Rx bytes
AP Response	• AP Name, MAC, Description, Serial #, GPS • Min, Max, Avg response time • Deviance • % Packets Lost • Tx & Rx Packets • Ping Total Response Time
Controller	• Controller Name & MAC • Client Count • License Count • License Utilization
Controller Resources	• CPU Util % • Disk Usage % • Mem Usage %
Client Sessions	• AP Name, MAC, Description, Serial #, GPS • Controller Name & MAC • Client Hostname & Username • # of sessions • # of subsessions • # of unique clients • Session Length • Tx & Rx bytes

Table 7. Available metrics

Category	Metric
Events	• AP Name, MAC, Description, Serial #, GPS • Controller Name & MAC • Number of Events
Client Session Intervals	• AP Name, MAC, Description, Serial #, GPS • Controller Name & MAC • Client Hostname & Username • Estimated Throughput • Min, Max RSSI • Max, Min Signal Strength • Noise Floor • Number of Intervals • Number of Sub-Sessions • Tx & Rx Bytes

Managing the SmartCell Insight System

6

In this chapter:

- Setting Administrator Preferences
- Getting Familiar with the Administration Interface
- Monitor Page
- System Setup Page
- Diagnostics Page
- Changing the Administrator Password
- SCI Upgrade Procedure
- SCI Uninstall Procedure
- SCI Backup and Restore
- SCI AP Grouping
- Uploading an SCI License
- System Timekeeping
- Using the Enterprise Console

Setting Administrator Preferences

This section describes the settings and procedures used to configure administrator preferences, such as setting the admin user name and password, configuring data sources, data purge settings and SMTP settings.

Accessing the Administration Interface

Many administration tasks can be performed through the administration interface (Admin Console). To access the administration interface, point your browser to: https://[SCI-IP-address]:8443, and enter your administrator user name and password.

NOTE: If you have not yet changed the default admin password, a warning message appears each time you access an admin interface page, prompting you to change the default password. See Changing the Administrator Password for instructions on changing the admin password.

Getting Familiar with the Administration Interface

The administration interface consists of the following three pages:

- Monitor Page
- System Setup Page
- Diagnostics Page

Use these pages to monitor and configure SCI data sources and to view ETL job status logs.

Monitor Page

The *Monitor* page displays currently configured SCI data sources, and provides options for deactivating/reactivating a data source, and enabling/disabling SCI > AP Response Time Tests. The *Monitor* page contains the following sections:

- **Sources**: Displays the data sources that have been configured on the *System Setup* page.
- **General Information**: Includes services status and system information including OS version, system resources and uptime.

SCI Data Sources

This section displays a list of the data sources configured from the System Setup page. It is divided into the following three sections (depending on which data sources have been configured):

- FlexMaster
- ZoneDirector Groups
- SmartZone

FlexMaster

Table 8 describes the information provided for each FlexMaster data source.

Table 8. SCI Data Source information items

Item	Description
SCI System Name	The Name of the FM or SZ data source.
FM DB Host	The IP address of the FM server.
FM DB Port	The Port number of the FM server.
FM DB User	The user name of the FM user account used to access the FM server.
FM DB Name	The name of the FM database.
ZoneDirectors List	Displays the IP/Port, Name and Status of configured ZoneDirectors. The Status indicator displays OK if the data source is currently reachable by SCI, or Disconnected if the data source is currently unreachable.

Table 8. SCI Data Source information items

Item	Description
Response Time Tests	Displays whether the AP Response Time Tests are enabled. This feature gathers data for a special SCI report (AP Response Time) that SCI measures by itself. This feature is only effective if the APs are reachable (i.e., they are not behind NAT, from the SCI's perspective in the network).
Status	Displays OK if the data source is currently reachable by SCI, or Error if an error is detected. The "?" icon contains more information on the error on mouse over.

ZoneDirector Groups

Table 9 describes the information provided for each ZoneDirector Group data source.

Table 9. ZD Data Source information items

Item	Description
SCI System Name	The Name of the FM or SZ data source.
ZD IP Address	The IP address of the ZoneDirector controller.
ZD Port Number	The Port number of the ZD.
ZD User Name	The user name of the ZD user account used to access the controller.
Response Time Tests	Displays whether the AP Response Time Tests are enabled. This feature gathers data for a special SCI report (AP Response Time) that SCI measures by itself. This feature is only effective if the APs are reachable (i.e., they are not behind NAT, from the SCI's perspective in the network).
Status	Displays OK if the data source is currently reachable by SCI, or Error if an error is detected. The "?" icon contains more information on the error on mouse over.

SmartZone

Table 10 describes the information provided for each SZ data source.

Table 10. SZ Data Source information items

Item	**Description**
SCI System Name	The Name of the FM or SZ data source.
SZ Control Plane Nodes MGMT IPs	The Management IP address of the SZ Control Plane.
SZ User	The SZ User name.
Response Time Tests	Displays whether the AP Response Time Tests are enabled. This feature gathers data for a special SCI report (AP Response Time) that SCI measures by itself. This feature is only effective if the APs are reachable (i.e., they are not behind NAT, from the SCI's perspective in the network).
Status	Displays OK if the data source is currently reachable by SCI, or Error if an error is detected. The "?" icon contains more information on the error on mouse over.

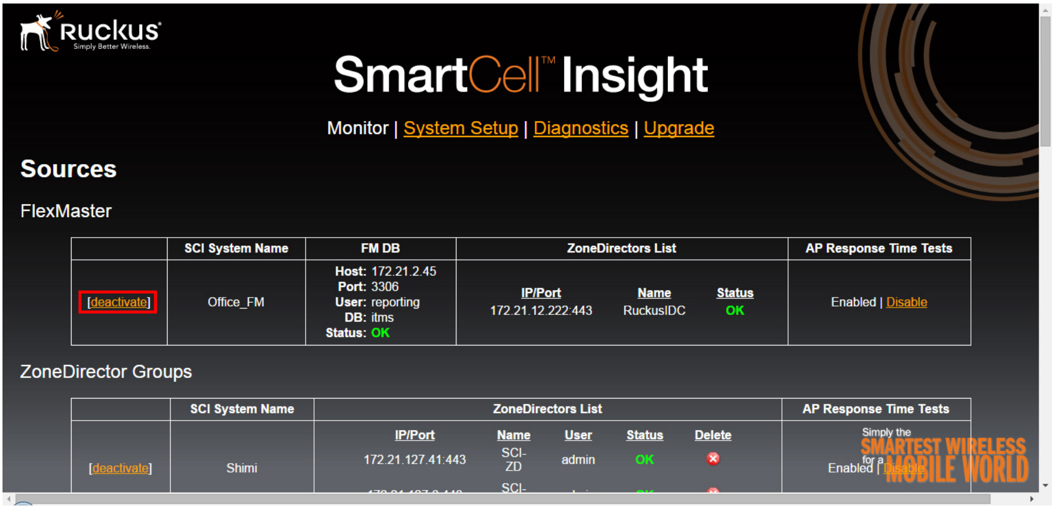
Deactivating a Data Source

To deactivate a data source, use the following procedure:

1. Locate the SCI System Name that you want to deactivate, and click the **deactivate** link on the same line.
2. The page refreshes and a confirmation message appears.

NOTE: Deactivating a system will not stop active data fetches, if there are any in progress; only future data fetches will be deactivated. SCI fetches data every 15 minutes from each data source.

Figure 62. Deactivate an SCI data source



SmartCell™ Insight

Monitor | System Setup | Diagnostics | Upgrade

Sources

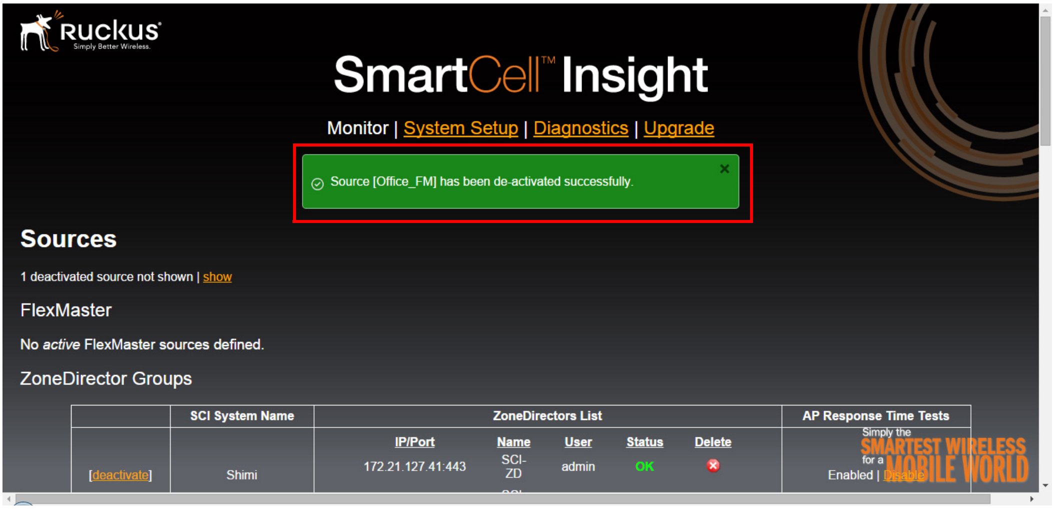
FlexMaster

	SCI System Name	FM DB	ZoneDirectors List			AP Response Time Tests
			IP/Port	Name	Status	
[deactivate]	Office_FM	**Host:** 172.21.2.45 **Port:** 3306 **User:** reporting **DB:** itms **Status:** OK	172.21.12.222:443	RuckusIDC	OK	Enabled | Disable

ZoneDirector Groups

	SCI System Name	ZoneDirectors List					AP Response Time Tests
		IP/Port	Name	User	Status	Delete	
[deactivate]	Shimi	172.21.127.41:443	SCI-ZD	admin	OK	✖	Enabled | Disable
			SCI-			✖	

Figure 63. Deactivation successful



SmartCell™ Insight

Monitor | System Setup | Diagnostics | Upgrade

Source [Office_FM] has been de-activated successfully. ✖

Sources

1 deactivated source not shown | show

FlexMaster

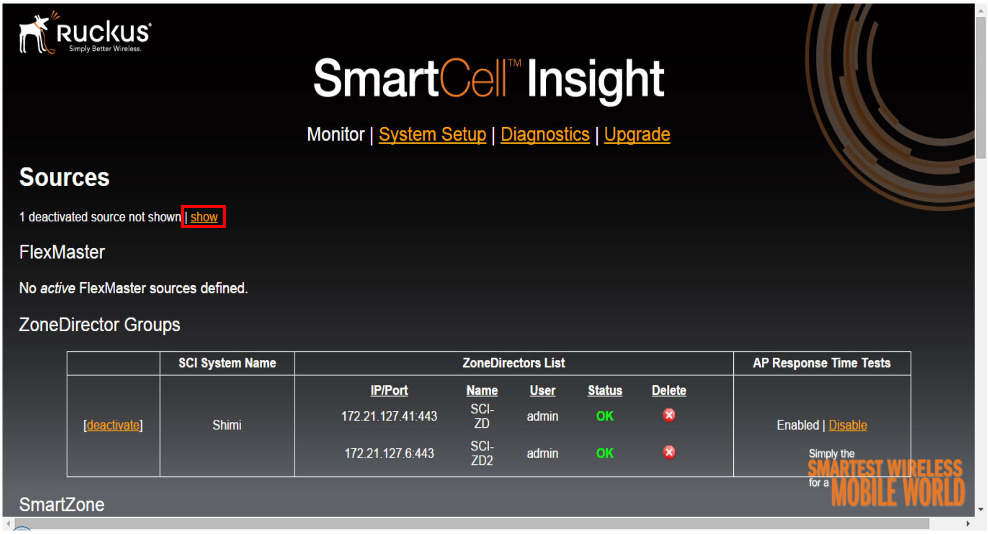
No *active* FlexMaster sources defined.

ZoneDirector Groups

	SCI System Name	ZoneDirectors List					AP Response Time Tests
		IP/Port	Name	User	Status	Delete	
[deactivate]	Shimi	172.21.127.41:443	SCI-ZD	admin	OK	✖	Enabled | Disable

The deactivated data source is now hidden from the list and a new line appears providing a link to display deactivated data sources. If you click the **Show** link, the list is refreshed to display both the active and deactivated data sources.

Figure 64. Show deactivated data sources



SmartCell™ Insight

Monitor | System Setup | Diagnostics | Upgrade

Sources

1 deactivated source not shown | show

FlexMaster

No *active* FlexMaster sources defined.

ZoneDirector Groups

	SCI System Name	ZoneDirectors List					AP Response Time Tests
		IP/Port	Name	User	Status	Delete	
[deactivate]	Shimi	172.21.127.41:443	SCI-ZD	admin	OK	☒	Enabled | Disable
		172.21.127.6:443	SCI-ZD2	admin	OK	☒	

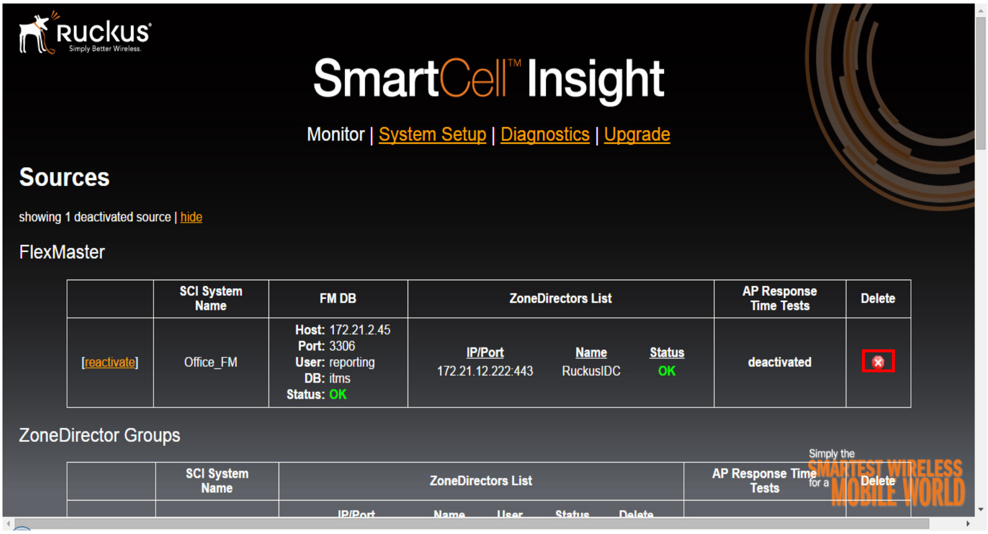
SmartZone

Permanently Deleting a Deactivated Data Source

To delete a data source permanently, you can now click the red “X” icon in the **Delete** column.

NOTE: Note that you can only delete a *Deactivated* data source, and once it is deleted, all data stored about this system is deleted forever.

Figure 65. Permanently delete a Deactivated data source



SmartCell™ Insight

Monitor | System Setup | Diagnostics | Upgrade

Sources

showing 1 deactivated source | hide

FlexMaster

	SCI System Name	FM DB	ZoneDirectors List			AP Response Time Tests	Delete
			IP/Port	Name	Status		
[reactivate]	Office_FM	**Host:** 172.21.2.45 **Port:** 3306 **User:** reporting **DB:** itms **Status:** OK	172.21.12.222:443	RuckusIDC	OK	deactivated	⊗

ZoneDirector Groups

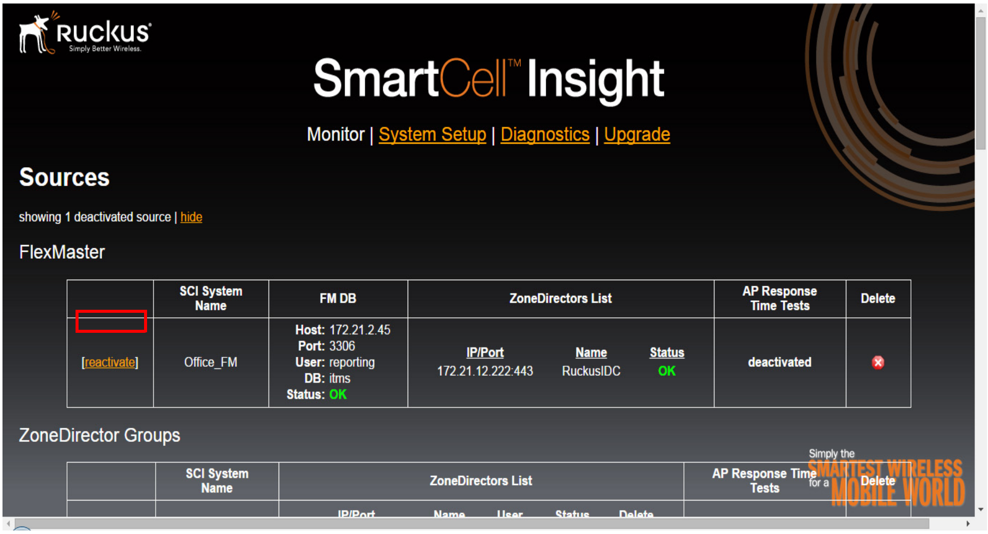
	SCI System Name	ZoneDirectors List					AP Response Time Tests	Delete
		IP/Port	Name	User	Status	Delete		

Reactivating a Deactivated Data Source

To reactivate a data source, use the following procedure:

1. Click the **Show** link to display deactivated data sources as well as active. The page refreshes to display deactivated and active data sources.
2. Click the **Reactivate** link for the data source you want to reactivate.

Figure 66. Reactivate a deactivated data source


Ruckus
Simply Better Wireless.
SmartCell™ Insight
Monitor | System Setup | Diagnostics | Upgrade
Simply the SMARTEST WIRELESS for a MOBILE WORLD

Sources

showing 1 deactivated source | hide

FlexMaster

	SCI System Name	FM DB	ZoneDirectors List	AP Response Time Tests	Delete
[reactivate]	Office_FM	**Host:** 172.21.2.45 **Port:** 3306 **User:** reporting **DB:** itms **Status:** OK	**IP/Port** **Name** **Status** 172.21.12.222:443 RuckusIDC OK	**deactivated**	✖

ZoneDirector Groups

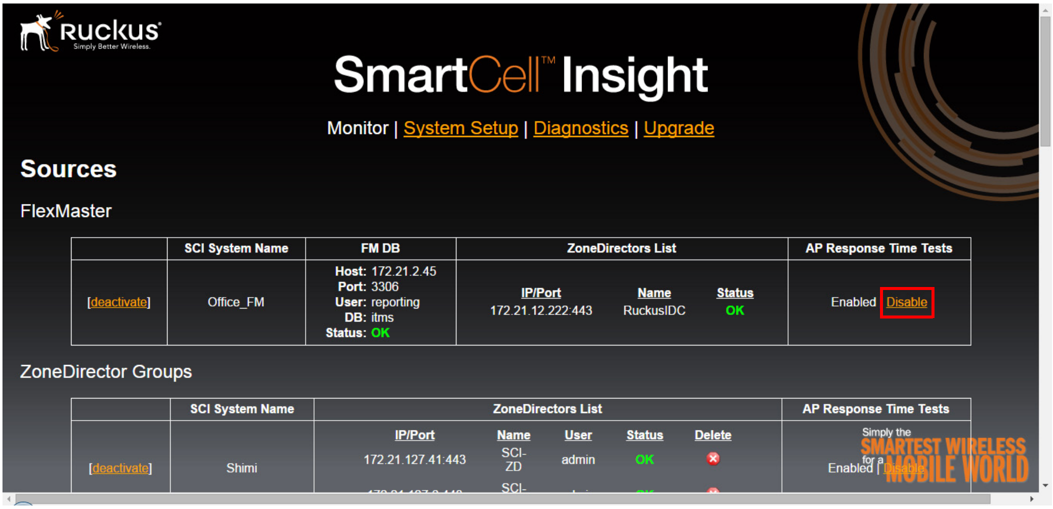
	SCI System Name	ZoneDirectors List	AP Response Time Tests	Delete
		IP/Port Name User Status Delete		

Enabling/Disabling SCI - AP Response Time Tests

To enable or disable SCI - AP response time tests, use the following procedure:

1. Click the **Enable** or **Disable** link for the relevant data source.
2. The page refreshes, and a “Success!” notification appears.

Figure 67. Enable or disable SCI > AP Response Time tests



Ruckus
Simply Better Wireless.
SmartCell™ Insight
Monitor | System Setup | Diagnostics | Upgrade
Simply the SMARTEST WIRELESS for a MOBILE WORLD

Sources

FlexMaster

	SCI System Name	FM DB	ZoneDirectors List	AP Response Time Tests
[deactivate]	Office_FM	**Host:** 172.21.2.45 **Port:** 3306 **User:** reporting **DB:** itms **Status:** OK	**IP/Port** 172.21.12.222:443 **Name** RuckusIDC **Status** OK	Enabled Disable

ZoneDirector Groups

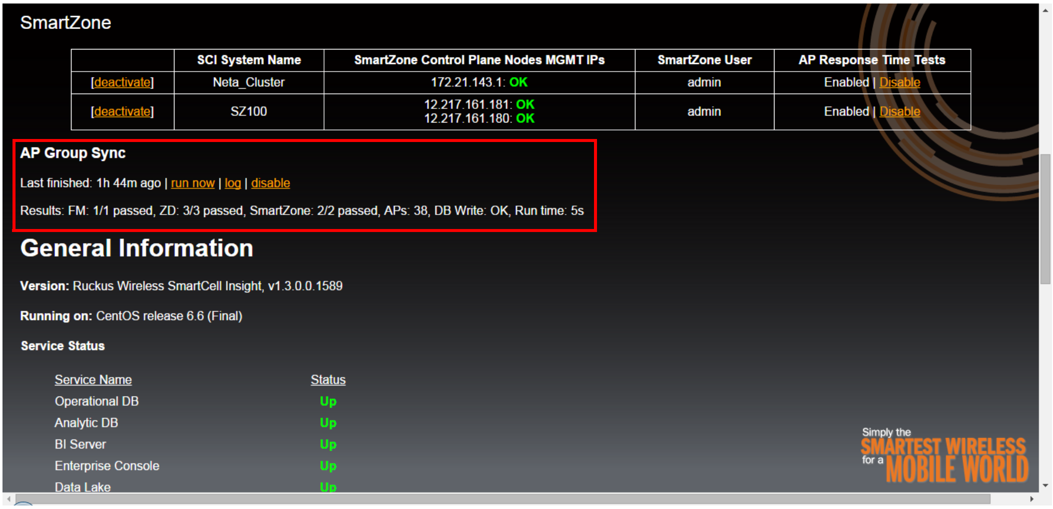
	SCI System Name	ZoneDirectors List					AP Response Time Tests
		IP/Port	**Name**	**User**	**Status**	**Delete**	
[deactivate]	Shimi	172.21.127.41:443	SCI-ZD	admin	OK	✖	Enabled | Disable

Performing AP Group Synchronization

The AP Group Sync section allows you to synchronize SCI's AP groups with ZoneDirector AP groups or SZ zones and AP groups. Click **run now** to run the sync operation now, or click **log** to display the log file.

Additionally, you can **disable** AP group synchronization if you do not want SCI to sync AP groups with those configured on the controller. This can be useful if you want to import your own custom AP groups, as described in SCI AP Grouping.

Figure 68. AP group sync



SmartZone

	SCI System Name	SmartZone Control Plane Nodes MGMT IPs	SmartZone User	AP Response Time Tests
[deactivate]	Neta_Cluster	172.21.143.1: OK	admin	Enabled | Disable
[deactivate]	SZ100	12.217.161.181: OK 12.217.161.180: OK	admin	Enabled | Disable

AP Group Sync

Last finished: 1h 44m ago | run now | log | disable

Results: FM: 1/1 passed, ZD: 3/3 passed, SmartZone: 2/2 passed, APs: 38, DB Write: OK, Run time: 5s

General Information

Version: Ruckus Wireless SmartCell Insight, v1.3.0.0.1589

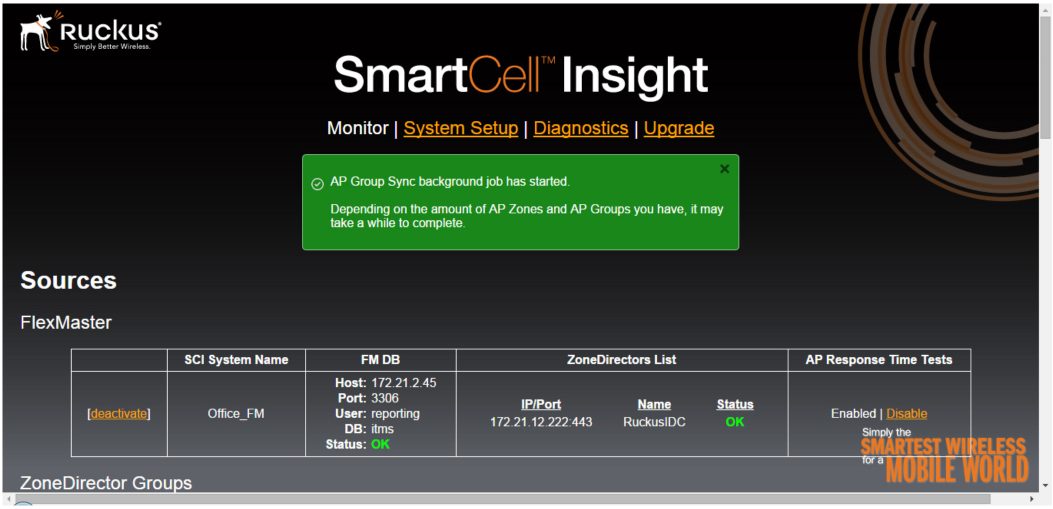
Running on: CentOS release 6.6 (Final)

Service Status

Service Name	Status
Operational DB	Up
Analytic DB	Up
BI Server	Up
Enterprise Console	Up
Data Lake	Up

Running the AP group sync task may take several minutes, depending on the number of AP zones and groups deployed.

Figure 69. AP Group Sync job started



Monitor | System Setup | Diagnostics | Upgrade

AP Group Sync background job has started.

Depending on the amount of AP Zones and AP Groups you have, it may take a while to complete.

Sources

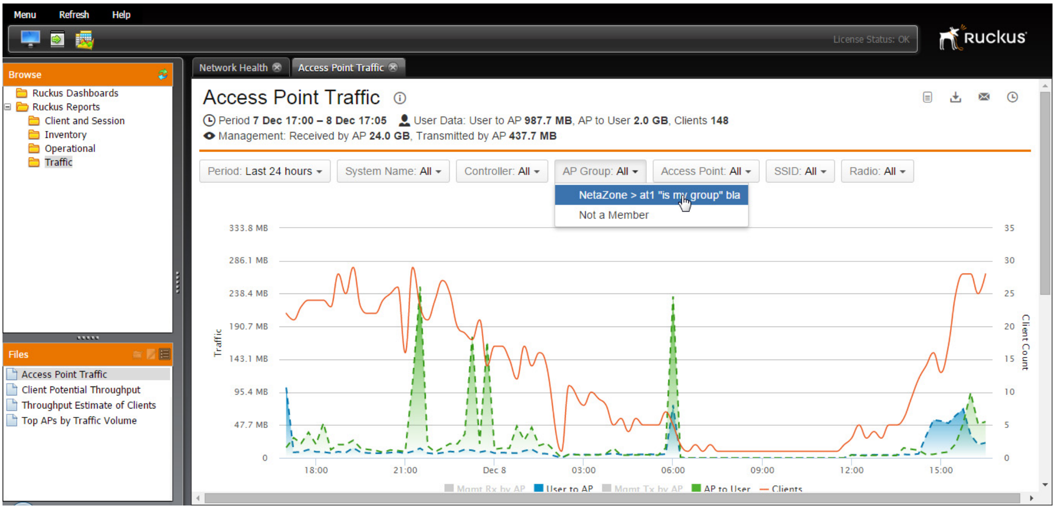
FlexMaster

	SCI System Name	FM DB	ZoneDirectors List			AP Response Time Tests
			IP/Port	Name	Status	
[deactivate]	Office_FM	**Host:** 172.21.2.45 **Port:** 3306 **User:** reporting **DB:** itms **Status:** OK	172.21.12.222:443	RuckusIDC	OK	Enabled | Disable

ZoneDirector Groups

Once complete, these AP groups can now be used to filter data displayed in reports such as the Access Point Traffic report for a specific AP group, as shown in Figure 70.

Figure 70. Filtering data by AP group



Access Point Traffic

Period **7 Dec 17:00 – 8 Dec 17:05** User Data: User to AP **987.7 MB**, AP to User **2.0 GB**, Clients **148**

Management: Received by AP **24.0 GB**, Transmitted by AP **437.7 MB**

Period: Last 24 hours | System Name: All | Controller: All | AP Group: All | Access Point: All | SSID: All | Radio: All

System Setup Page

The System Setup page provides options for configuring Data Sources, importing AP Licenses, and System Configuration settings, which including options for importing an SSL Certificate, configuring the Data Purge policy, and configuring SMTP settings and email recipients for alerts and scheduled report delivery.

Sources Configuration

SCI data sources refers to the systems from which SCI collects its data. Data can be collected from Ruckus Wireless ZoneDirector controllers, FlexMaster servers, and/or SmartZone controllers.

The following sections provide information on adding each of the data source types:

- FlexMaster
- ZoneDirectors Group
- Standalone ZoneDirector
- SmartZone (SCG/SZ/vSZ)

FlexMaster

To add a new FlexMaster data source, use the following procedure:

1 In the *FlexMaster* section, enter the following details for connecting to the FlexMaster server:

- **System Name**: Enter a recognizable name for the FM server.

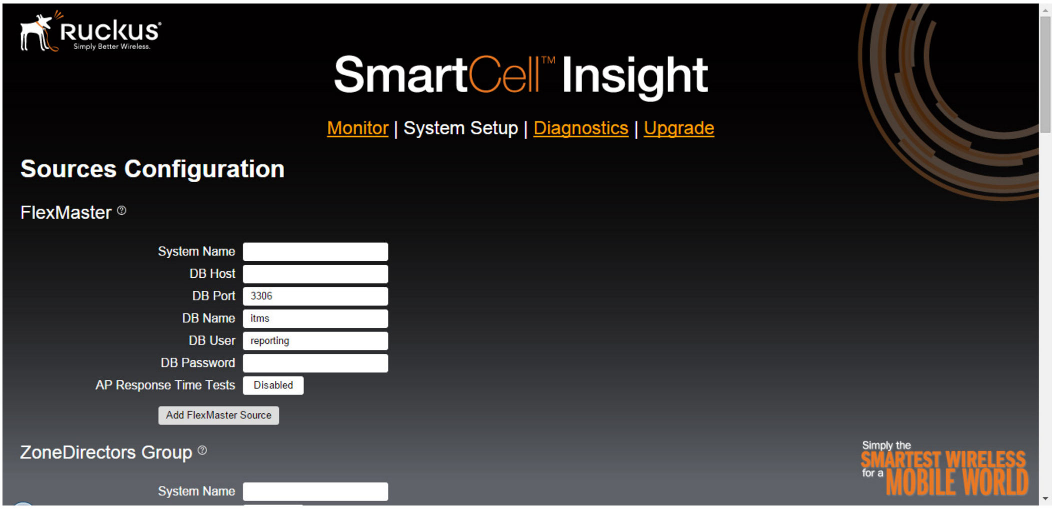
NOTE: This is the internal name that SCI uses to identify the FM server. Note that this name cannot be changed afterwards without removing all the data from this source, so choose carefully.

- **DB Host**: Enter the IP address of the FM server.
- **DB Port**: Enter the Port number for the FM server (default: 3306).
- **DB Name**: Enter “itms” as the name for the FM database. (This can only be “itms”.)
- **DB User**: Enter a user name for the FM database. This user name must be configured as a mySQL Reporting user for the FlexMaster database.
- **DB Password**: Enter the user password.

- **AP Response Time Tests**: Select Enabled or Disabled. This feature gathers data for the AP Response Time report that SCI measures by itself. This feature is only effective if the APs are reachable (i.e., they are not behind NAT, from the SCI's perspective in the network).

2 Click the **Add FlexMaster Source** button.

Figure 71. Add a FlexMaster data source



Ruckus
Simply Better Wireless.
SmartCell™ Insight
Monitor | System Setup | Diagnostics | Upgrade
Simply the SMARTEST WIRELESS for a MOBILE WORLD

Sources Configuration

FlexMaster

System Name	
DB Host	
DB Port	3306
DB Name	itms
DB User	reporting
DB Password	
AP Response Time Tests	Disabled

ZoneDirectors Group

System Name	

NOTE: FlexMaster requires that a read-only user on FlexMaster's MySQL database be created for SmartCell Insight.

ZoneDirectors Group

ZoneDirector Groups are filterable entities in SCI reports that contain multiple ZoneDirectors. In order to connect a ZoneDirector to SCI without a FlexMaster server controlling the ZD, you must assign the ZD to a ZoneDirectors Group.

To create a new ZoneDirector Group data source, use the following procedure:

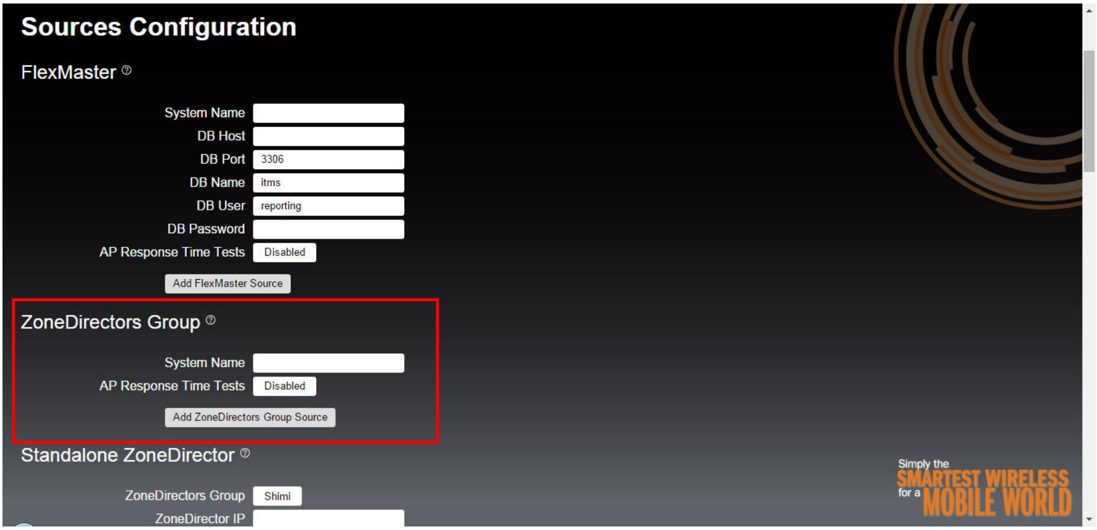
1 In the *ZoneDirectors Group* section, enter the following:

- **System Name**: Enter a name for the ZoneDirectors Group.

- **AP Response Time Tests**: Select Enabled or Disabled. This feature gathers data for the AP Response Time report that SCI measures by itself. This feature is only effective if the APs are reachable (i.e., they are not behind NAT, from the SCI's perspective in the network).

2 Click the **Add ZoneDirectors Group Source** button.

Figure 72. Add a ZoneDirector data source



Sources Configuration

FlexMaster

System Name
DB Host
DB Port: 3306
DB Name: itms
DB User: reporting
DB Password
AP Response Time Tests: Disabled

ZoneDirectors Group

System Name
AP Response Time Tests: Disabled

Standalone ZoneDirector

ZoneDirectors Group: Shimi
ZoneDirector IP

Add FlexMaster Source
Add ZoneDirectors Group Source
Simply the SMARTEST WIRELESS for a MOBILE WORLD

Standalone ZoneDirector

Use this section to add a standalone ZoneDirector to an SCI "ZoneDirectors Group" (for reporting to SCI without an FM server).

NOTE: The ZoneDirector clock must be synchronized with NTP, and show the same time as SCI.

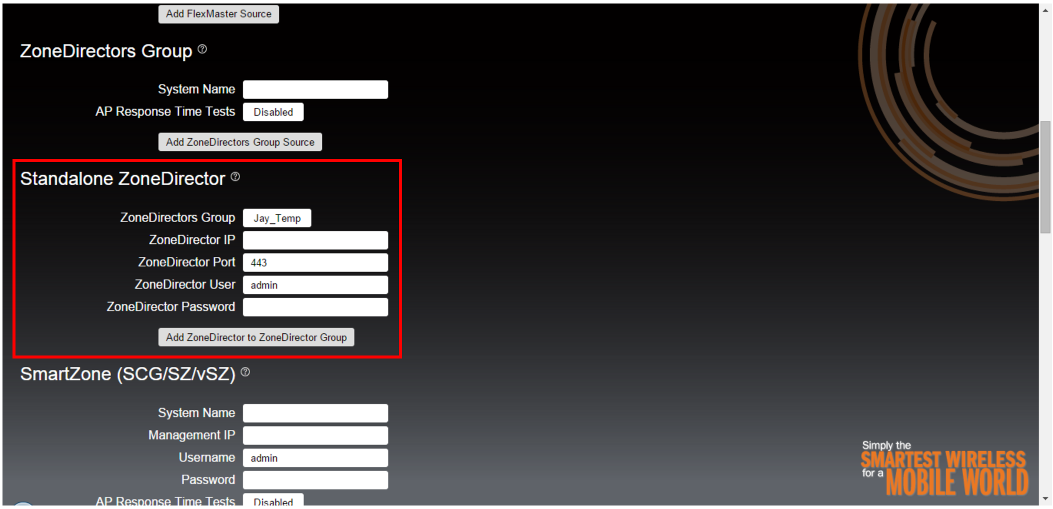
NOTE: The ZoneDirector must run an SCI-compatible firmware.

NOTE: Standalone ZoneDirectors do not send event data to SCI, so reports based on events (such as "AP Reboots") will show no data for these sources. For events, either an FM or SmartZone-based controller is required.

To add a standalone ZoneDirector to a ZoneDirectors Group, use the following procedure:

1. In the *Standalone ZoneDirector* section, enter the following:
   - **ZoneDirectors Group**: Select a ZD Group from the list of ZD groups you created above in ZoneDirectors Group.
   - **ZoneDirector IP**: Enter the IP address of the ZD to be added to the group.
   - **ZoneDirector Port**: Enter the TCP Port of the ZD to be added to the group.
   - **ZoneDirector User**: Enter the administrator User Name of the ZD to be added to the group.
   - **ZoneDirector Password**: Enter the password of the administrative user to be added to the group.
2. Click the **Add ZoneDirector to ZoneDirector Group** button.

Figure 73. Add a standalone ZD to a ZD group


Add FlexMaster Source
ZoneDirectors Group
Add ZoneDirectors Group Source
Standalone ZoneDirector
Add ZoneDirector to ZoneDirector Group
SmartZone (SCG/SZ/vSZ)
Simply the SMARTEST WIRELESS for a MOBILE WORLD

System Name
AP Response Time Tests: Disabled

ZoneDirectors Group: Jay_Temp
ZoneDirector IP
ZoneDirector Port: 443
ZoneDirector User: admin
ZoneDirector Password

System Name
Management IP
Username: admin
Password
AP Response Time Tests: Disabled

SmartZone (SCG/SZ/vSZ)

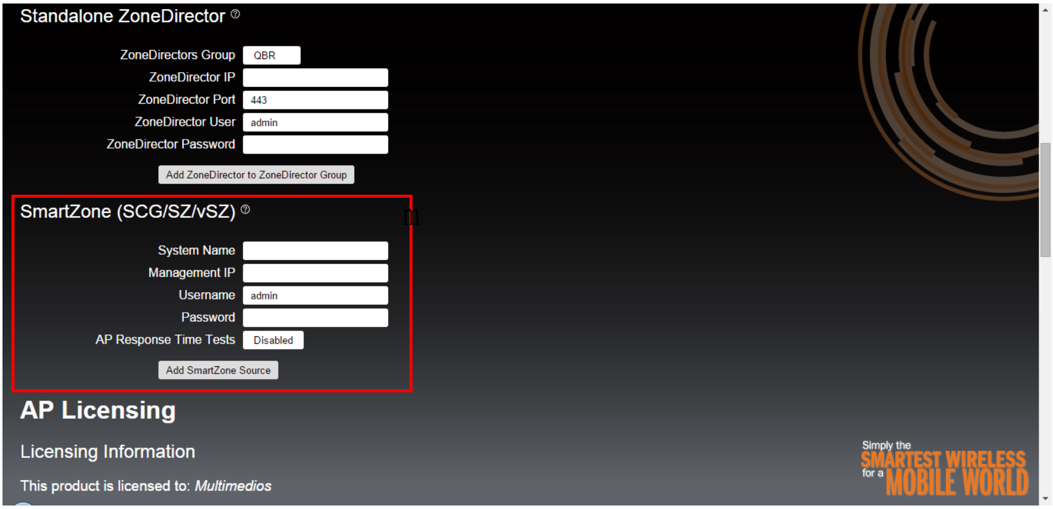
To add a SmartZone data source, use the following procedure:

1. In the *SmartZone* section, enter the following details for connecting to the SZ controller:
   - **System Name**: Enter a recognizable name for the SZ controller.
   - **Management IP**: Enter the IP address of the SZ management interface.

- **Username**: Enter a user name for the SZ user. This user name must be configured as a valid user with a ‘Super Admin’ role.
- **Password**: Enter the user password.
- **AP Response Time Tests**: Select Enabled or Disabled. This feature gathers data for the AP Response Time report that SCI measures by itself. This feature is only effective if the APs are reachable (i.e., they are not behind NAT, from the SCI’s perspective in the network).

2 Click the **Add SmartZone Source** button.

Figure 74. Add an SZ data source



Standalone ZoneDirector

ZoneDirectors Group: QBR
ZoneDirector IP:
ZoneDirector Port: 443
ZoneDirector User: admin
ZoneDirector Password:

SmartZone (SCG/SZ/vSZ)

System Name:
Management IP:
Username: admin
Password:
AP Response Time Tests: Disabled

AP Licensing

Licensing Information

This product is licensed to: *Multimedios*

Add ZoneDirector to ZoneDirector Group
Add SmartZone Source
Simply the SMARTEST WIRELESS for a MOBILE WORLD

NOTE: SZ requires that AP statistics delivery be enabled so that APs can send data directly to SCI. To enable AP statistics delivery, enter the command `ap-sci enable` from the SZ CLI config context (see SZ CLI documentation for instructions on using the SZ command line interface).

AP Licensing

The AP Licensing section allows you to import an SCI license file. SCI supports a maximum of 10 APs without a license for demo or testing purposes. The SCI license can be upgraded at any time to accommodate more APs as your SCI deployment grows. It includes the customer name and the number of licensed APs. If a license violation exists (more APs reporting stats than the license level), SCI will display a warning message directing you to either upgrade your license or reduce the number of APs reporting to SCI.

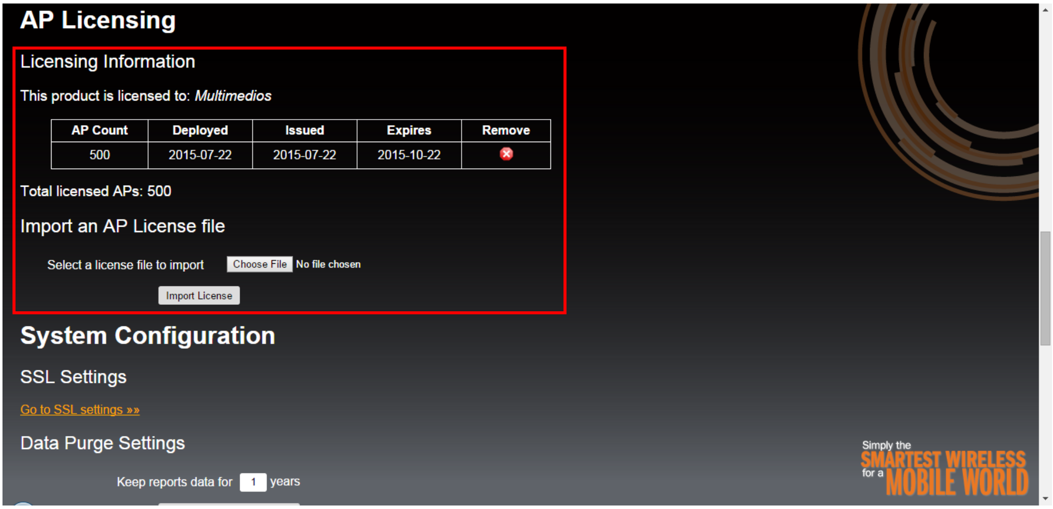
The SCI license can be upgraded at any time by completing the following procedure:

1 Go to the **System Setup** page.

2 In the *Import an AP License File* section, click **Choose File** to select a license file to import.

3 Select the file and click **Import License**.

Figure 75. Importing an SCI license file



AP Licensing

Licensing Information

This product is licensed to: *Multimedios*

AP Count	Deployed	Issued	Expires	Remove
500	2015-07-22	2015-07-22	2015-10-22	✖

Total licensed APs: 500

Import an AP License file

Select a license file to import [Choose File] No file chosen

[Import License]

System Configuration

SSL Settings

Go to SSL settings »»

Data Purge Settings

Keep reports data for 1 years

System Configuration

The System Configuration section provides options for configuring SSL certificate settings, data purge policy, SMTP settings for email report delivery, and Alert Settings for configuring email addresses of recipients for email alerts.

SSL Settings

During installation, SCI automatically creates a unique RSA 2048 key, Self-Signed Server Certificate and a unique 2048 bit Diffie-Helman Group for all access to SCI.

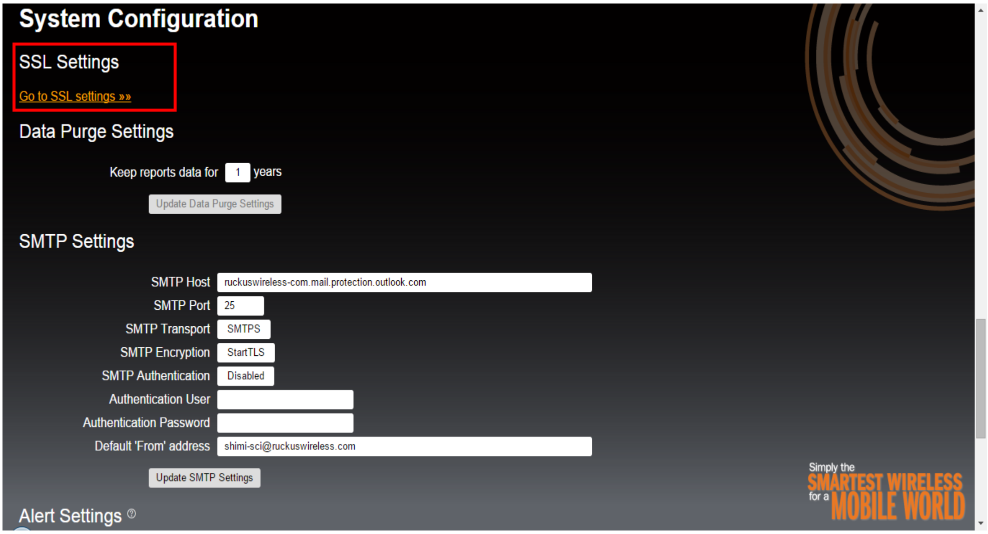
Self-Signed certificates will cause browsers to issue a warning that the authenticity of the site cannot be verified. This is normal and cannot be avoided if you use a self-signed certificate.

You may opt to use a Certificate Authority (CA)-provided certificate for a DNS name that you will assign to your SCI installation. SCI provides you with an SSL wizard to create your own Private Key and a Certificate Signing Request for that Private Key, to be used when requesting a certificate from a CA.

Alternatively, if you already have a Private Key (.pem) and a Server Certificate (.crt) from another server (e.g. if you have a wildcard certificate for your domain), you may directly import them into SCI. Further, if your CA requires it, you may import a CA-provided Intermediate Certificate Chain, to help browsers establish the trust chain between your Server Certificate and one of their Trusted Root CAs.

After you create/import a Private Key and a Server Certificate (and possibly an Intermediate Certificate Chain), click "Deploy SSL" to have SCI start using them.

Figure 76. SSL Settings



System Configuration

SSL Settings

Go to SSL settings »»

Data Purge Settings

Keep reports data for 1 years

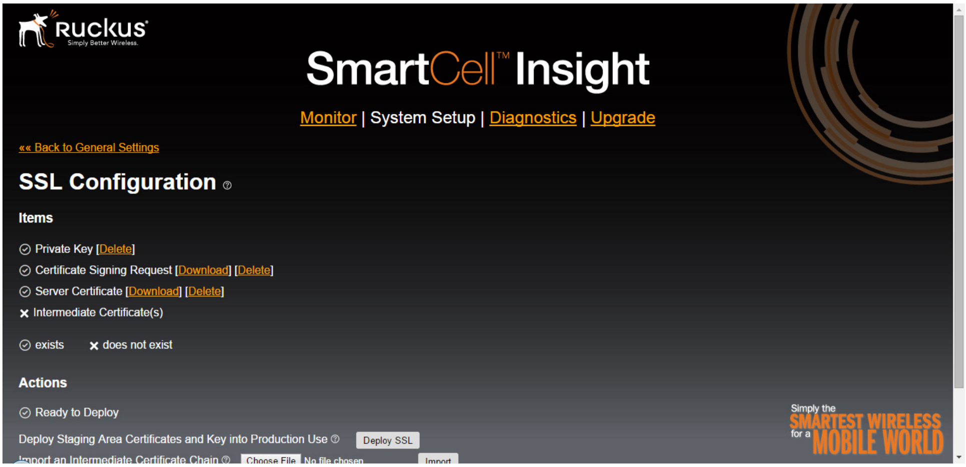
SMTP Settings

SMTP Host: ruckuswireless-com.mail.protection.outlook.com
SMTP Port: 25
SMTP Transport: SMTPS
SMTP Encryption: StartTLS
SMTP Authentication: Disabled
Authentication User:
Authentication Password:
Default 'From' address: shimi-sci@ruckuswireless.com

Alert Settings

Update Data Purge Settings
Update SMTP Settings
Simply the SMARTEST WIRELESS for a MOBILE WORLD

Figure 77. SSL Configuration wizard


Ruckus
Simply Better Wireless.
SmartCell™ Insight
Monitor | System Setup | Diagnostics | Upgrade
«« Back to General Settings
Simply the SMARTEST WIRELESS for a MOBILE WORLD
Deploy SSL
Choose File
No file chosen
Import

SSL Configuration

Items

✓ Private Key [Delete]
✓ Certificate Signing Request [Download] [Delete]
✓ Server Certificate [Download] [Delete]
✕ Intermediate Certificate(s)

✓ exists ✕ does not exist

Actions

✓ Ready to Deploy

Deploy Staging Area Certificates and Key into Production Use

Import an Intermediate Certificate Chain

Data Purge Settings

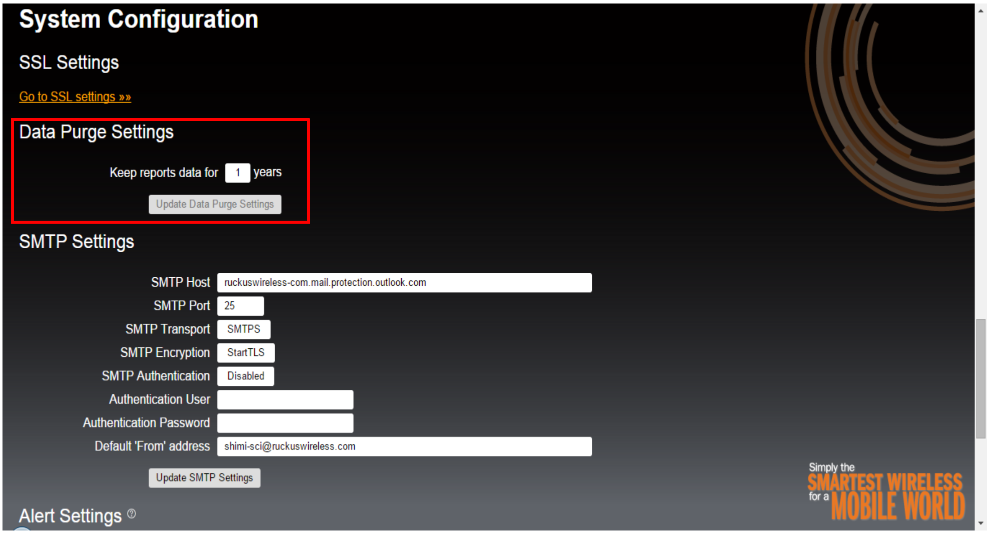
To configure the data purge policy, use the following procedure:

1 In **Keep reports data for __ years**, select the number of years for which SCI will maintain report data before purge.

2 Click **Update Data Purge Settings** to save your changes.

NOTE: When reducing the number of years to a number lower than the current setting, a warning will appear to alert you that you are about to remove old data if you continue. If you approve this operation, data older than the new purge setting will be removed, irrecoverably. By default, SCI keeps data for 1 year. When getting close to 1 year, you will need to monitor disk space usage and evaluate your network volume to determine if your current storage will suffice for storing more than 1 year's worth of data, and only if so, increase this number.

Figure 78. Data Purge Settings



System Configuration

SSL Settings

Go to SSL settings »»

Data Purge Settings

Keep reports data for 1 years

SMTP Settings

SMTP Host: ruckuswireless-com.mail.protection.outlook.com
SMTP Port: 25
SMTP Transport: SMTPS
SMTP Encryption: StartTLS
SMTP Authentication: Disabled
Authentication User:
Authentication Password:
Default 'From' address: shimi-sci@ruckuswireless.com

Alert Settings

SMTP Settings

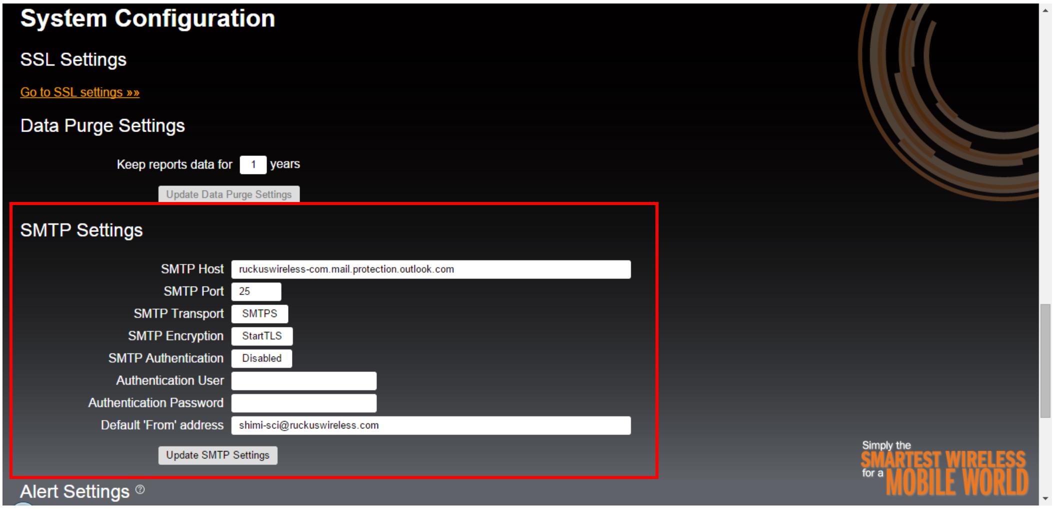
To configure SMTP settings, use the following procedure:

1 Enter the following SMTP settings for email delivery of SCI reports:

- **SMTP Host**: The outgoing mail server for your organization.
- **SMTP Port**: The SMTP port number (default: 25).
- **SMTP Transport**: Select normal SMTP or SMTP with transport layer security.
- **SMTP Encryption**: Select whether to use STARTTLS transport layer security or SSL encryption.
- **SMTP Authentication**: Select whether to use SMTP authentication.
- **Authentication User**: Enter user name if SMTP authentication is used.
- **Authentication Password**: Enter user password if SMTP authentication is used.
- **Default 'From:' address**: Enter the email address from which emails will be delivered.

2 Click **Update SMTP Settings** to save your changes.

Figure 79. SMTP Settings for Email Delivery



System Configuration

SSL Settings

Go to SSL settings »»

Data Purge Settings

Keep reports data for 1 years

SMTP Settings

SMTP Host: ruckuswireless-com.mail.protection.outlook.com
SMTP Port: 25
SMTP Transport: SMTPS
SMTP Encryption: StartTLS
SMTP Authentication: Disabled
Authentication User:
Authentication Password:
Default 'From' address: shimi-sci@ruckuswireless.com

Alert Settings

Use the Alert Settings to configure email addresses of recipients of email alerts. The SMTP settings are also used to configure the recipients for automated report delivery.

1 Enter a primary recipient's email address in **Alert To**.

2 Enter additional recipient email addresses in the **Alert CC**, **Alert BCC** and **Escalation CC** fields.

NOTE: The Escalation CC field can be used to notify a recipient when a problem occurs and has not been resolved. Escalation CC alerts will be sent after two cycles.

---

3 Enter an interval after which a repeat email will be sent in **First Repeat After__**. Subsequent repeat alerts will be sent at increasing time intervals, doubling each time. For example, if you enter 3600 seconds (1 hour), the 2nd alert will be sent after 1 hour, the 3rd alert after 2 hours, the 4th alert after 4 hours, etc.

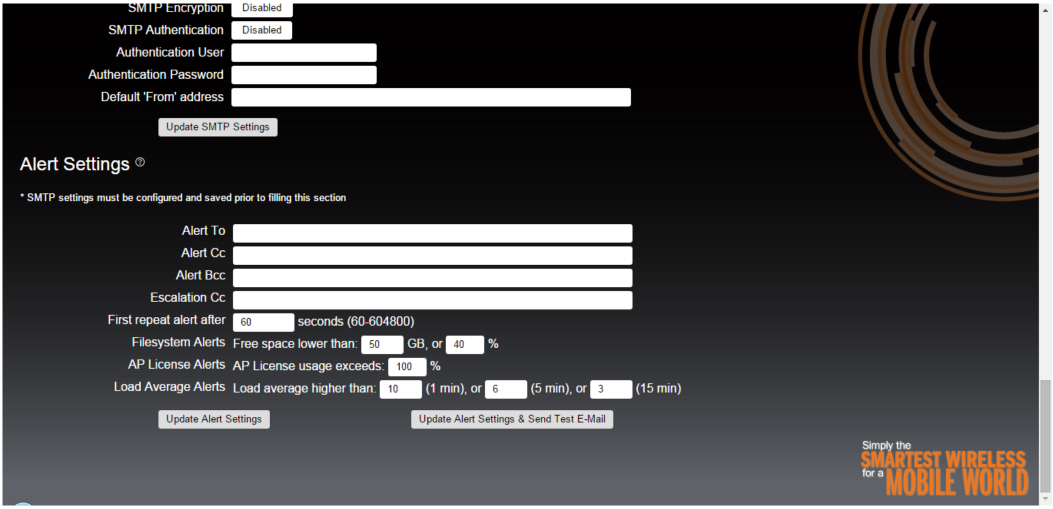
4 In **Filesystem Alerts**, enter a disk space (in GB) or disk space percentage threshold after which an alert will be sent when the disk space falls below this threshold.

5 In **AP License Alerts**, enter a percentage threshold to trigger an alert when the percentage of APs reporting to SCI of the Total Licensed APs exceeds this set threshold.

6 In **Load Average Alerts**, enter load average thresholds above which alerts will be sent. (To disable these alerts, enter the value 0 in the relevant field/fields.)

7 Click **Update Alert Settings** to save your changes, or click **Update Alert Settings & Send Test E-Mail** to save changes and test your settings.

Figure 80. Configure email alert settings



SMTP Encryption: Disabled
SMTP Authentication: Disabled
Authentication User:
Authentication Password:
Default 'From' address:

Alert Settings

* SMTP settings must be configured and saved prior to filling this section

Alert To:
Alert Cc:
Alert Bcc:
Escalation Cc:
First repeat alert after: 60 seconds (60-604800)
Filesystem Alerts: Free space lower than: 50 GB, or 40 %
AP License Alerts: AP License usage exceeds: 100 %
Load Average Alerts: Load average higher than: 10 (1 min), or 6 (5 min), or 3 (15 min)

Update SMTP Settings
Update Alert Settings
Update Alert Settings & Send Test E-Mail
Simply the SMARTEST WIRELESS for a MOBILE WORLD

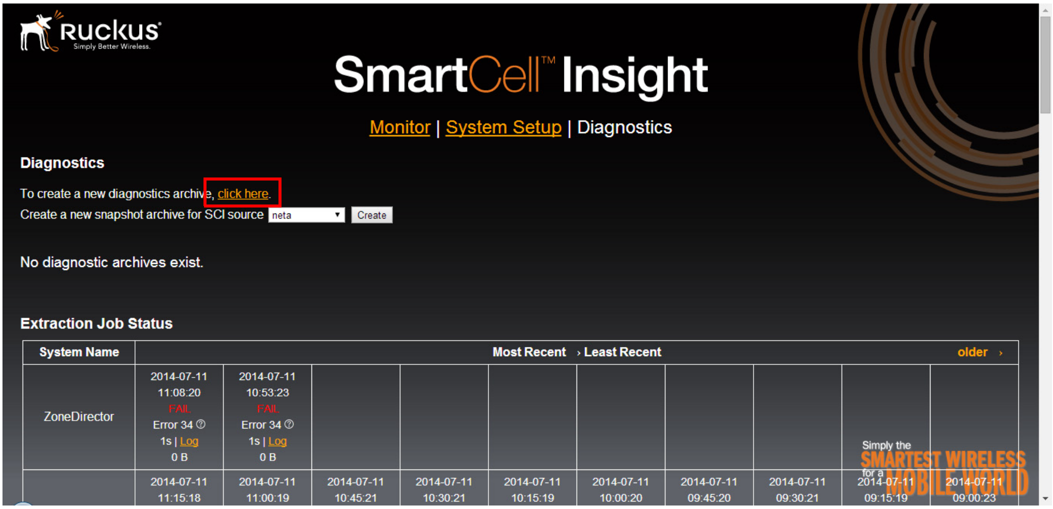
Diagnostics Page

The Diagnostics page provides tools for creating diagnostics log files and viewing previously created diagnostics archives.

Creating a New Diagnostics Archive

1 To create a new diagnostics archive, click the **click here** link. The page refreshes and a *Diagnostics collection in progress* dialog appears. The page will automatically refresh once the diagnostics archive creation is complete.

Figure 81. Create a new diagnostics archive



Diagnostics

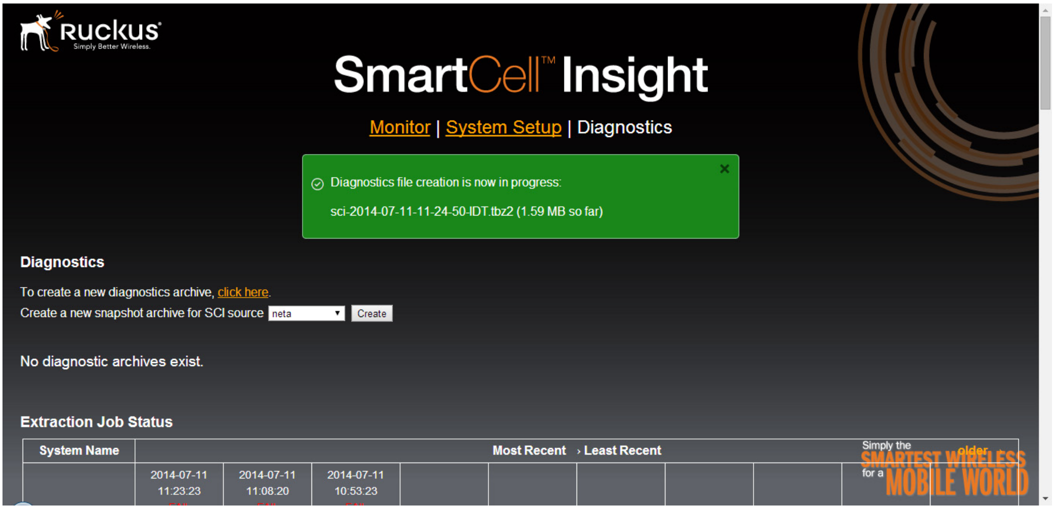
To create a new diagnostics archive, click here.
Create a new snapshot archive for SCI source neta

No diagnostic archives exist.

Extraction Job Status

System Name	Most Recent › Least Recent									older ›
ZoneDirector	2014-07-11 11:08:20 FAIL Error 34 ⓘ 1s | Log 0 B	2014-07-11 10:53:23 FAIL Error 34 ⓘ 1s | Log 0 B								
	2014-07-11 11:15:18	2014-07-11 11:00:19	2014-07-11 10:45:21	2014-07-11 10:30:21	2014-07-11 10:15:19	2014-07-11 10:00:20	2014-07-11 09:45:20	2014-07-11 09:30:21	2014-07-11 09:15:19	2014-07-11 09:00:23

Figure 82. Diagnostics collection in progress



Diagnostics file creation is now in progress:
sci-2014-07-11-11-24-50-IDT.tbz2 (1.59 MB so far)

Diagnostics

To create a new diagnostics archive, click here.
Create a new snapshot archive for SCI source neta ▾ Create

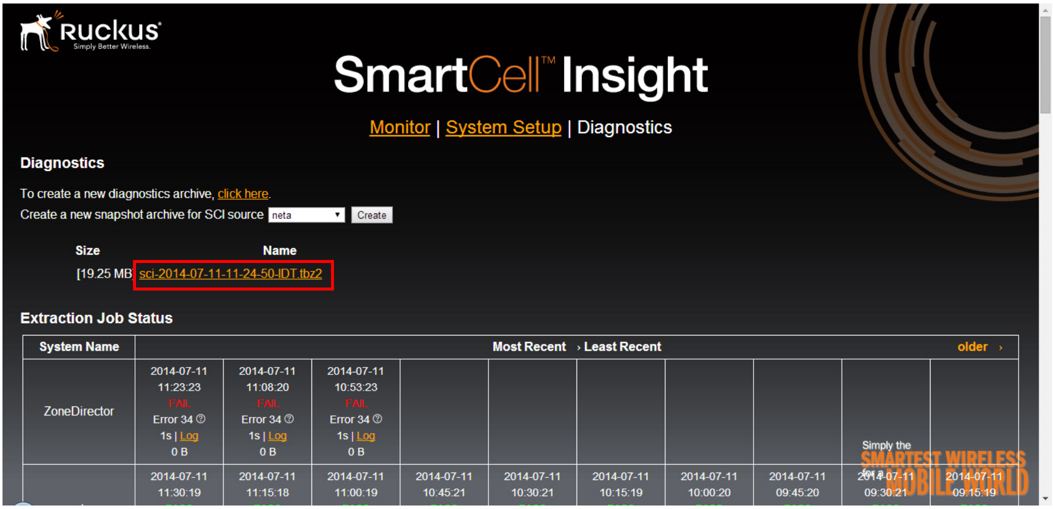
No diagnostic archives exist.

Extraction Job Status

System Name	Most Recent › Least Recent								older ›
	2014-07-11 11:23:23	2014-07-11 11:08:20	2014-07-11 10:53:23						

Once the process is complete (and the page refreshed), you can click the log file name to download the file to your local computer.

Figure 83. Download a diagnostics archive file



Diagnostics

To create a new diagnostics archive, click here.
Create a new snapshot archive for SCI source neta ▾ Create

Size	Name
[19.25 MB]	sci-2014-07-11-11-24-50-IDT.tbz2

Extraction Job Status

System Name	Most Recent › Least Recent									older ›
ZoneDirector	2014-07-11 11:23:23 FAIL Error 34 ⓘ 1s | Log 0 B	2014-07-11 11:08:20 FAIL Error 34 ⓘ 1s | Log 0 B	2014-07-11 10:53:23 FAIL Error 34 ⓘ 1s | Log 0 B							
	2014-07-11 11:30:19	2014-07-11 11:15:18	2014-07-11 11:00:19	2014-07-11 10:45:21	2014-07-11 10:30:21	2014-07-11 10:15:19	2014-07-11 10:00:20	2014-07-11 09:45:20	2014-07-11 09:30:21	2014-07-11 09:15:19

Creating a Snapshot Archive

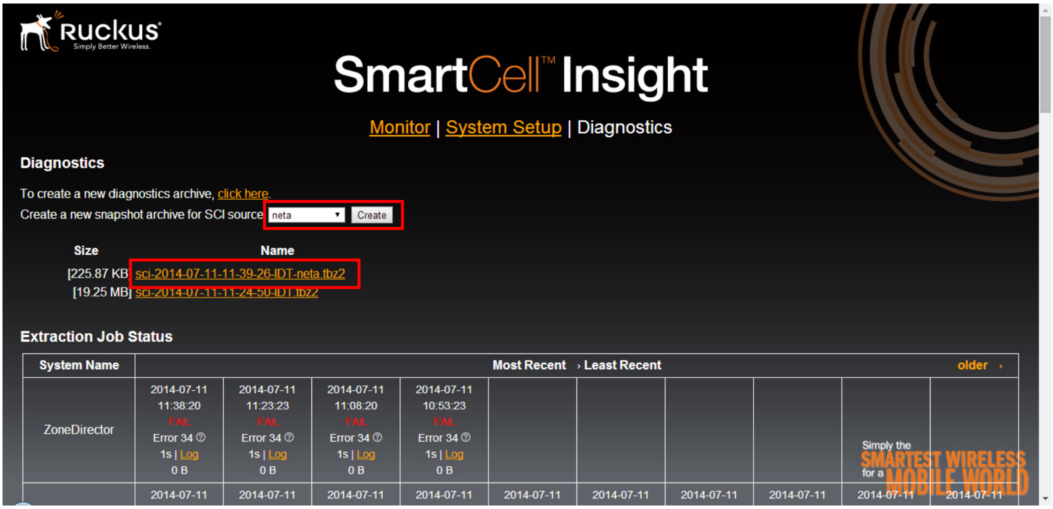
Creating a Snapshot Archive may be necessary for debugging purposes if you encounter an ETL error and need help from Ruckus support in identifying the issue. This procedure should only be performed if you are asked to create a snapshot by Ruckus support personnel. It should be used only in the case of ETL failures, and be run only on the specific source where ETL errors were spotted. It creates a compressed archive of all the raw data received from a data source for analysis.

1 If asked to do so by Ruckus customer support, select the data source from the list, and click **Create**.

2 A snapshot archive file is created for the data source and appears in the archive list for download.

3 Download the file and email it to Ruckus support for analysis.

Figure 84. Creating a snapshot archive



Diagnostics

To create a new diagnostics archive, click here.

Create a new snapshot archive for SCI source neta ▼ Create

Size	Name
[225.87 KB]	sci-2014-07-11-11-39-26-IDT-neta.tbz2
[19.25 MB]	sci-2014-07-11-11-24-50-IDT.tbz2

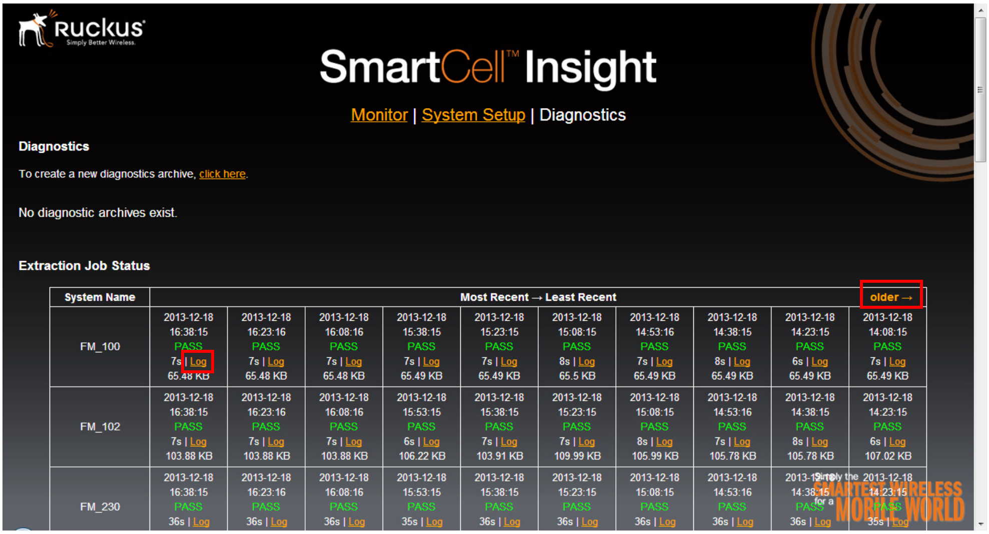
Extraction Job Status

System Name	Most Recent › Least Recent									older ›
ZoneDirector	2014-07-11 11:38:20 FAIL Error 34 ⓘ 1s | Log 0 B	2014-07-11 11:23:23 FAIL Error 34 ⓘ 1s | Log 0 B	2014-07-11 11:08:20 FAIL Error 34 ⓘ 1s | Log 0 B	2014-07-11 10:53:23 FAIL Error 34 ⓘ 1s | Log 0 B						
	2014-07-11	2014-07-11	2014-07-11	2014-07-11	2014-07-11	2014-07-11	2014-07-11	2014-07-11	2014-07-11	2014-07-11

ETL Log Results Display

ETL (Extraction, Transform and Load) is the method by which SCI gathers data from its data sources, transforms it to fit operational needs, and loads it into the target formats. The two tables titled *Extraction Job Status* and *Transform/Load Job Status* display the 10 most recent diagnostic log results, displayed from most recent to least recent from left to right. You can click the **older >** link to view older logs, after which you can browse by using the **< newer** and **older >** links. You can also click the **Log** link for any log entry to view the specific log files.

Figure 85. Extraction Job Status display



SmartCell™ Insight

Monitor | System Setup | Diagnostics

Diagnostics

To create a new diagnostics archive, click here.

No diagnostic archives exist.

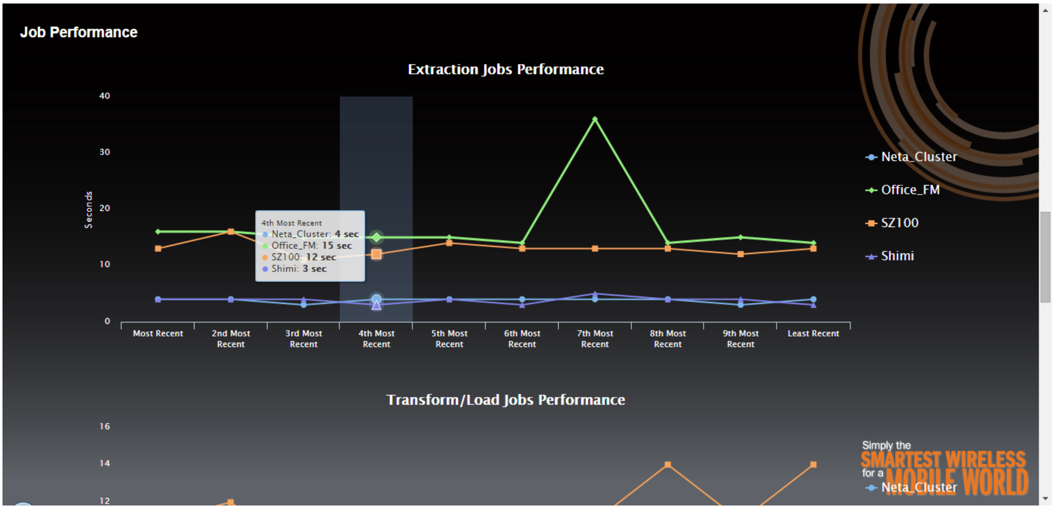
Extraction Job Status

System Name	Most Recent → Least Recent									older →
FM_100	2013-12-18 16:38:15 PASS 7s | Log 65.48 KB	2013-12-18 16:23:16 PASS 7s | Log 65.48 KB	2013-12-18 16:08:16 PASS 7s | Log 65.48 KB	2013-12-18 15:38:15 PASS 7s | Log 65.49 KB	2013-12-18 15:23:15 PASS 7s | Log 65.49 KB	2013-12-18 15:08:15 PASS 8s | Log 65.5 KB	2013-12-18 14:53:16 PASS 7s | Log 65.49 KB	2013-12-18 14:38:15 PASS 8s | Log 65.49 KB	2013-12-18 14:23:15 PASS 6s | Log 65.49 KB	2013-12-18 14:08:15 PASS 7s | Log 65.49 KB
FM_102	2013-12-18 16:38:15 PASS 7s | Log 103.88 KB	2013-12-18 16:23:16 PASS 7s | Log 103.88 KB	2013-12-18 16:08:16 PASS 7s | Log 103.88 KB	2013-12-18 15:53:15 PASS 6s | Log 106.22 KB	2013-12-18 15:38:15 PASS 7s | Log 103.91 KB	2013-12-18 15:23:15 PASS 7s | Log 109.99 KB	2013-12-18 15:08:15 PASS 8s | Log 105.99 KB	2013-12-18 14:53:16 PASS 7s | Log 105.78 KB	2013-12-18 14:38:15 PASS 8s | Log 105.78 KB	2013-12-18 14:23:15 PASS 6s | Log 107.02 KB
FM_230	2013-12-18 16:38:15 PASS 36s | Log	2013-12-18 16:23:16 PASS 36s | Log	2013-12-18 16:08:16 PASS 36s | Log	2013-12-18 15:53:15 PASS 35s | Log	2013-12-18 15:38:15 PASS 36s | Log	2013-12-18 15:23:15 PASS 36s | Log	2013-12-18 15:08:15 PASS 36s | Log	2013-12-18 14:53:16 PASS 36s | Log	2013-12-18 14:38:15 PASS 36s | Log	2013-12-18 14:23:15 PASS 35s | Log

Job Performance Graphs

The Job Performance section displays the amount of time required for ETL process completion per data source in a time graph format. In this way, you can easily see and compare how much time (in seconds) the Extract and Transform/Load processes took for each of the last 10 data queries.

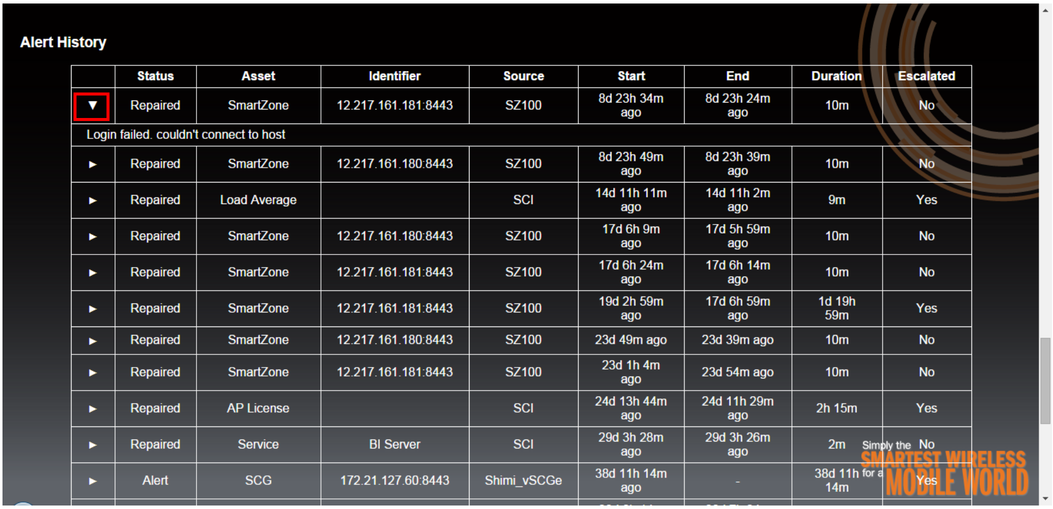
Figure 86. Job Performance graphs



Alert History

The Alert History table displays the most recent alert messages, their status, source, duration and Escalated status. Click the arrow next to an alert to see the exact alert message.

Figure 87. Alert history table



Alert History

	Status	Asset	Identifier	Source	Start	End	Duration	Escalated
▼	Repaired	SmartZone	12.217.161.181:8443	SZ100	8d 23h 34m ago	8d 23h 24m ago	10m	No
Login failed. couldn't connect to host								
►	Repaired	SmartZone	12.217.161.180:8443	SZ100	8d 23h 49m ago	8d 23h 39m ago	10m	No
►	Repaired	Load Average		SCI	14d 11h 11m ago	14d 11h 2m ago	9m	Yes
►	Repaired	SmartZone	12.217.161.180:8443	SZ100	17d 6h 9m ago	17d 5h 59m ago	10m	No
►	Repaired	SmartZone	12.217.161.181:8443	SZ100	17d 6h 24m ago	17d 6h 14m ago	10m	No
►	Repaired	SmartZone	12.217.161.181:8443	SZ100	19d 2h 59m ago	17d 6h 59m ago	1d 19h 59m	Yes
►	Repaired	SmartZone	12.217.161.180:8443	SZ100	23d 49m ago	23d 39m ago	10m	No
►	Repaired	SmartZone	12.217.161.181:8443	SZ100	23d 1h 4m ago	23d 54m ago	10m	No
►	Repaired	AP License		SCI	24d 13h 44m ago	24d 11h 29m ago	2h 15m	Yes
►	Repaired	Service	BI Server	SCI	29d 3h 28m ago	29d 3h 26m ago	2m	No
►	Alert	SCG	172.21.127.60:8443	Shimi_vSCGe	38d 11h 14m ago	-	38d 11h 14m	Yes

Changing the Administrator Password

To change the admin password, use the following procedure:

1 Open an SSH connection to the SCI server’s location and run the following commands to configure the password for the Root user:

```
$ ssh -l root 172.227.226
Password:
Last login: Wed Nov 6 15:32:37 2013 from 172.20.181
[root@sci-dev ~]# /opt/ruckuswireless/sci/scripts/sci_change_admin_password.php

 ####################################################
 # Ruckus Wireless SmartCell Insight v1.0.0.0.1407 #
 ####################################################

This utility changes the password for the 'admin' user on Administrative Web
Interface, User Console and Enterprise Console.

Please enter a new admin password (or hit Ctrl+C to abort)?
Please enter the new admin password again to verify (or hit Ctrl+C to abort)?

New password accepted. Updating new password across all systems...

Updating User Console... SUCCESS!
Updating AdminWeb/User Console... SUCCESS!

Restarting User Console...
Waiting 10 seconds for service to go down...

Utility finished.
[root@sci-dev ~]#
```

2 The next time you log in to the Administration Interface, User Console or Enterprise Console (as admin), use the new password to log in.

SCI Upgrade Procedure

Perform the following procedure to upgrade SCI:

1. Upload the TAR package file (sci-repo-[build number].tar) to the SCI host as the 'root' user, to the /root home directory.
2. SSH to the SCI host as the user 'root'. Remain in the home directory (don't 'cd' to another directory).
3. Perform a backup to avoid potential data loss in case upgrade fails (see SCI Backup and Restore).
4. Extract the TAR package using the following command:

   ```
   tar xf sci-repo-[build number].tar
   ```
5. Run the SCI installer using the following command:

   ```
   ./deploy-sci.sh
   ```
6. While the installer runs, it will ask you if you have backed up your data. If you don't answer 'y', upgrade will not continue. If you opt to not perform the backup and say 'y' anyway, you accept the potential loss of all your data.

After the upgrade process finishes, DO NOT reboot the system, it is not necessary.

NOTE: During the upgrade process, SCI performs a verification check to ensure that the hostname format meets SCI's requirements before installation or upgrade can continue. If upgrading from a previous release (which did not have this verification) using an invalid hostname, you will be required to change the hostname first before upgrading, or the upgrade will fail. See Hostname Verification for more information.

Hostname Verification

Valid hostnames can include lower-case letters, numbers and hyphens. All other characters are invalid. Hostname requirements:

- May not be 'localhost'.
- May contain only lower-case letters (a-z), numbers (0-9) and hyphen (-) signs.
- Must begin with a-z.
- May not end with a hyphen (-).

If you need to change your hostname to comply with the format requirements, use the following procedure prior to performing the upgrade:

1 Edit /etc/sysconfig/network and/or /etc/sysconfig/network-scripts/ifcfg-eth0 (wherever a HOSTNAME line appears with this hostname).

2 Add the new name without the dot to /etc/hosts on the 127.0.0.1 line as the first item after 127.0.0.1 (do NOT remove the old one, just prefix the new name before it, with a space between the names)

   Example before:

```
127.0.0.1   sci-node-1.state.gov localhost local-
host.localdomain localhost4 localhost4.localdomain4

::1        localhost localhost.localdomain localhost6
localhost6.localdomain6
```

   Example after:

```
127.0.0.1   sci-node-1 sci-node-1.state.gov localhost
localhost.localdomain localhost4 localhost4.localdo-
main4

::1        localhost localhost.localdomain localhost6
localhost6.localdomain6
```

3 Run the command: hostname <the new hostname>

   Example:

```
hostname sci-node-1
```

4 Continue with the SCI upgrade as normal.

SCI Uninstall Procedure

1 Uninstall licenses:

```
yum remove rks-sci-bi-server-license-*
```

2 Uninstall SCI:

```
/opt/ruckuswireless/sci/scripts/sci_uninstall.sh
```

3 Refresh repository:

```
yum clean all
```

SCI Backup and Restore

Do the following the first time you backup to the backup server:

1 Create a backup server on a different machine.

2 On the source server, execute:

```
/opt/ruckuswireless/sci/scripts/setup_backup_host.sh
```

You do not need to repeat these steps when backing up again to the same backup server.

Backup

From the second time you backup to the backup server:

1 Clean previous backups from the backup server (/opt & /tmp folders).

2 Execute:

```
/opt/ruckuswireless/sci/scripts/sci_backup.sh
```

Restore

1 Once your backup server is set up, execute:

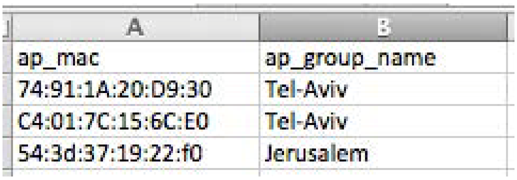
```
/opt/ruckuswireless/sci/scripts/sci_restore.sh
```

SCI AP Grouping

AP Grouping is strictly optional. You do not need to perform this procedure if you do not want to create SCI AP Groups.

1 Create a CSV file mapping MAC to AP group in the following format:

Figure 88. AP Group CSV file format



A	B
ap_mac	ap_group_name
74:91:1A:20:D9:30	Tel-Aviv
C4:01:7C:15:6C:E0	Tel-Aviv
54:3d:37:19:22:f0	Jerusalem

2 Save the file as /tmp/ap_group.csv

3 Login as rkssci user:

```
su -s /bin/sh rkssci
```

4 Switch to the following directory:

```
cd /opt/ruckuswireless/sci/pentaho/data-integration
```

5 Run the command:

```
sh kitchen.sh -level=Rowlevel -norep -file="/opt/ruckuswireless/sci/pentaho/
etl/external/loadApGroups.kjb" /tmp/ap_group.csv
```

CAUTION! If you do not disable AP Group Sync (from the Monitor page), the AP Groups you have imported will be overwritten when the automatic AP Group Sync function runs (once per day).

Uploading an SCI License

SCI requires two kinds of licenses – the Business Intelligence (BI) license and the Ruckus SCI license. The BI license only needs to be installed once (as described in the Installation section). The SCI license can be upgraded at any time to accommodate more APs as your SCI deployment grows. It includes the customer name and the number of licensed APs. If a license violation exists (more APs reporting stats than the license level), SCI will display a warning message informing you to either upgrade your license or reduce the number of APs reporting to SCI.

The SCI license can be upgraded at any time by completing the following procedure:

1. Go to the **System Setup** page.
2. In the *Licensing* section, click **Choose File** to select a license file to import.
3. Select the file and click **Import License**.

System Timekeeping

APs synchronize their time-of-day clock (aka wall clock) every 12 hours to network time using NTP. Each AP's wall clock is set to the GMT time zone. APs are not configured with their local time zone. Whenever APs reboot, they use NTP to re-initialize their wall clock; system time is not preserved across reboots. There are several important implications stemming from these facts:

- System Administrators must ensure that outgoing connections to NTP servers are not blocked on the corporate network or else provide a local NTP Server. Otherwise, APs will not be able to initialize their wall clocks.
- APs' timestamps on statistics will not be perfectly synchronized and AP-to-AP clocks (and therefore timestamps) will drift with respect to one another.
- When an AP reboots and doesn't have access to NTP Servers, it will not be able to properly initialize its wall clock. This could happen, for example, when a WAN connection is down; APs can locally switch traffic, but their timestamps will be incorrect because NTP Servers are unreachable.
  - APs connected to ZDs will always be able to synchronize their time stamps as they cannot operate without a connection to ZD.

- - APs connected to SZ, however, are capable of starting their WLAN service without first connecting to their SZ.
- SCI is aware of the time zone in which every AP is deployed and ensures that its reports time-zone align with the statistics reported from APs in different time zones.

Using the Enterprise Console

The Enterprise Console provides tools for managing users and roles, and for scheduling jobs for creation of user-defined reports.

CAUTION! The Enterprise Console should not be used for anything other than creating users and roles and scheduling jobs for creation of custom reports.

To access the Enterprise Console, enter the following URL in your browser:

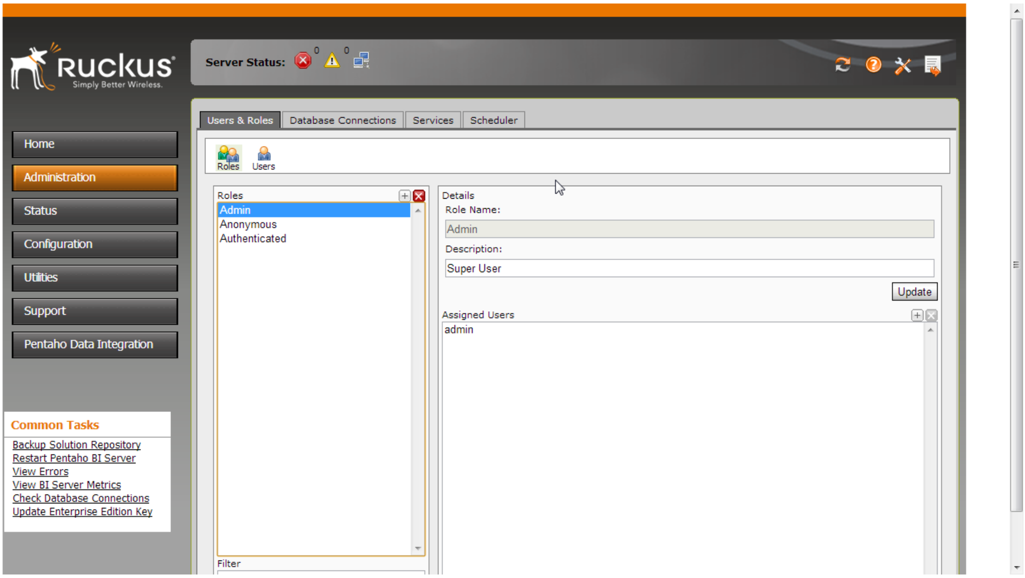
```
https://[SCI-IP-address]:9443
```

Creating Users and Roles

Three roles - Admin, Anonymous and Authenticated - are included by default. You can use the Users & Roles page to customize roles and create additional users.

CAUTION! The Enterprise Console allows you to change the password for the user **admin**. You must NOT do this, because the password change will not be synchronized to all places. You must use the script described in the section "Changing the Administrator Password" on page 119.

Figure 89. Administration - Users & Roles page



Role Name: Admin

Description: Super User

Assigned Users
admin

Adding Users

Follow the instructions below to add users to the SCI system:

1 In the Enterprise Console go to **Administration > Users & Roles**.

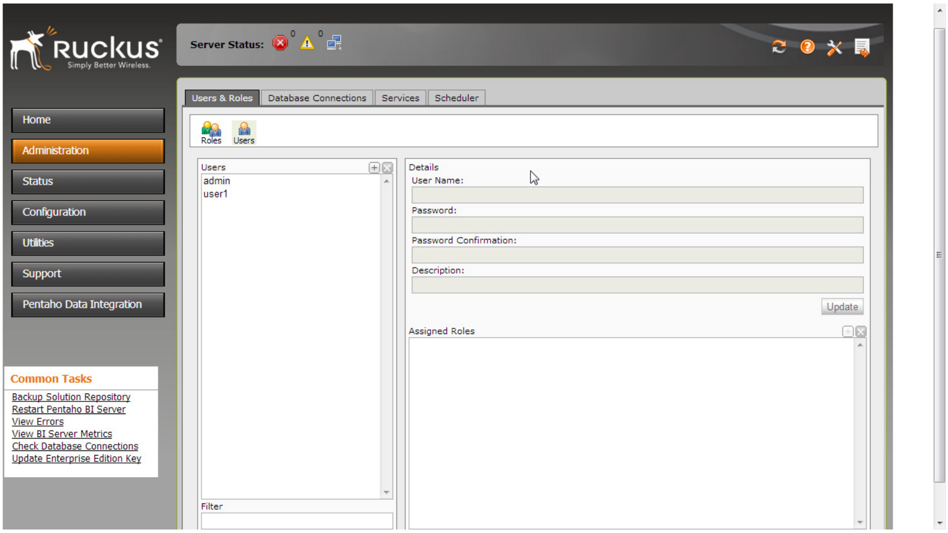
2 Click the **Users** icon if you are not in **Users** mode.

3 Click the plus sign (**+**) next to **Users**.

4 In the **Details** pane, enter the **User Name**, **Password**, **Password Confirmation**, and **Description**.

5 Click **OK**. The new user's name appears in the list of users.

Figure 90. Adding a user



Editing User Information

Follow the instructions below to edit user information:

1 In the Enterprise Console go to **Administration > Users & Roles**.

2 Select the user whose information you want to edit.

3 In the **Details** pane, edit the user details as needed.

4 Click **Update**.

Deleting Users

Follow the instructions below to delete a users from the SCI system:

1. In the Enterprise Console go to **Administration > Users & Roles**.
2. Select the user or users you want to delete from the **Users** list.
3. Click the Delete Users icon (**X**) next to **Users** to delete the users you selected. A confirmation dialog appears.
4. Click **OK** to refresh the user list.

Finding Users

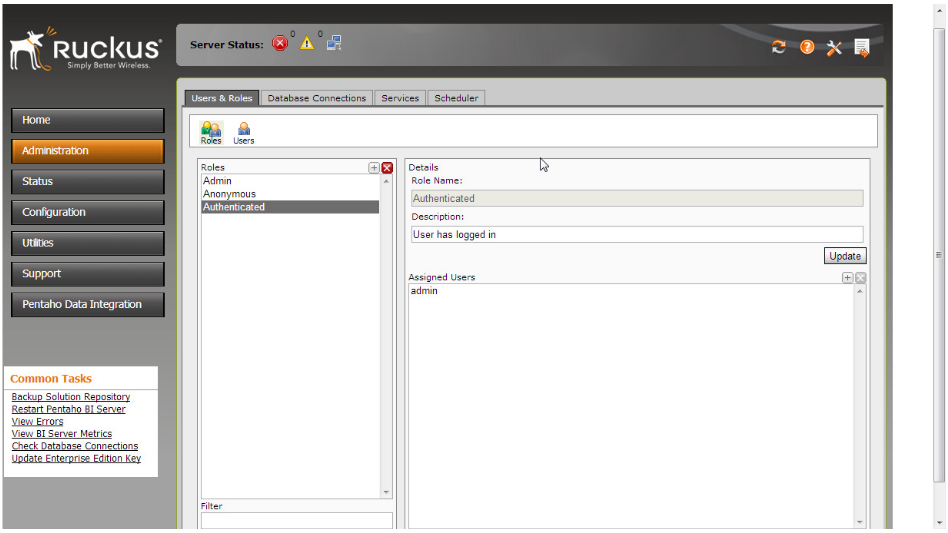
The User List Filter allows you to find specific users in the list of current users. To find a user, enter the first few letters of the user's name in the text box. A list of names matching your entry appears.

Managing Roles

Follow the instructions below to add roles to the BI Platform:

1. In the Enterprise Console go to **Administration > Users & Roles**.
2. Click the **Roles** icon if you are not in **Roles** mode.
3. Click the plus sign (**+**) next to **Roles**.
4. In the new window, type a new **Role Name** and **Description**.
5. Click **OK**. The new role appears in the list of roles.

Figure 91. Creating a new Role



Roles
Admin
Anonymous
Authenticated

Details
Role Name: Authenticated
Description: User has logged in

Assigned Users
admin

Editing Roles

Follow the instructions below to edit roles:

1 In the Enterprise Console go to **Administration > Users & Roles**.

2 Select the role you want to edit.

3 In the right pane, edit the details as needed.

4 Click **Update**.

Deleting Roles

Follow the instructions below to delete roles:

1 In the Enterprise Console go to **Administration > Users & Roles**.

2 Select role or roles you want to delete from the **Roles** list.

3 Click the Delete Roles icon (**X**) next to **Roles** to delete the roles you selected. A confirmation dialog appears.

4 Click **OK** to refresh the roles list.

Finding Roles

The Role List Filter allows you to find specific roles in the list of current roles. To find a role, enter the first few letters of the role name in the text box. A list of role names matching your entry appears.

Using the Scheduler to Define Public Schedules for Custom Reports

The Scheduler allows you to create, update, delete, run, suspend, and resume one or more schedules, (private and public), in the BI Platform. In addition, you can suspend and resume the Scheduler itself. In the context of the BI platform, a schedule is a time (or group of times) associated with an action sequence (or group of action sequences). In many cases, the output of an action sequence associated with a public schedule is a report; for example, a sales report to which a manager or salesperson can subscribe. As the administrator, the schedule (or schedules) you designate determines when the Scheduler allows the action sequence to run. Regular schedules are ad hoc, non-subscription schedules, which are associated with one action sequence only.

In addition to associating a time (or group of times in the case of a repeating schedule) with an action sequence (or group of action sequences), the public schedule is also associated with a user's My Workspace. When an action sequence runs on its defined schedule, the output of the action sequence (typically a report) is archived in the My Workspace of the user(s) who have subscribed to that action sequence. This allows the subscribers to view the output of the action sequence (the report) at any time following its execution.

Entering Schedules in the Schedule Creator Dialog Box

Enter schedules associated with your action sequences in the Schedule Creator dialog box. The Schedule Creator makes it easy for you to enter schedules without having to learn the arcane syntax of CRON expressions; however, it provides you with the option to enter CRON expressions if that is your preference.

Follow the instructions below to use the Schedule Creator:

1 In the main page of the Enterprise Console, click **Administration**.

2 Click the **Scheduler** tab.

3 In the **Scheduler**, click first icon on the left to open the **Scheduler Creator** dialog box.

4. Under **Schedule**, enter a **Name** for the schedule, for example, Monthly Sales.
5. Enter a **Group** associated with the schedule, for example, Sales Schedules.
6. Enter a short **Description** of the schedule. for example, "Schedule runs on the first of each month, schedule runs on Monday of each week."
7. Select a **Recurrence Type**. You can schedule the action sequence to run once at a particular date and time only, or have it recur in seconds, minutes, hours, daily, weekly, monthly, yearly, or recur based on a CRON string. The options in the Recurrence Editor change depending on the type of recurrence you select.
8. Click **OK**.

NOTE: Note: You can use the Schedule Creator to enter a CRON expression manually by selecting CRON from the Recurrence Type list. See "CRON Expressions in Detail" on page 131 to learn more about CRON expressions.

Adding the Action Sequences

After you add your schedules, you must associate them with action sequences. Follow the instructions below to enter the paths to the action sequences:

1. Under **Scheduled Action**, enter the path to each action sequence separated by commas.
2. Click **OK**.

Examining the List of Schedules

As you create new schedules, the schedules appear in a list box. By examining the list, you can identify the Name and Group associated with each schedule. You can also determine the status (State) of each schedule and read a brief description of the schedule. In addition, you can determine when the schedule was first run (Fire Time - Last/Next) and when it will run again. The controls on the top corners of the Scheduler page allow you to perform tasks such as:

Table 11. Schedule icons

Icon	Control Name	Function
🗋	Create Schedule	Allows you to create a new schedule
✎	Edit Schedule	Allows you to edit the details of a schedule

Table 11. Schedule icons

Icon	Control Name	Function
✕	Delete Schedule	Allows you to delete a specified schedule; however, if the schedule is currently executing in a scheduler thread it continues to execute but no new instances are run
⏸	Suspend Schedule	Allows you to pause a specified schedule. Once the job is paused the only way to start it again is with a Resume
➦	Resume selected Schedule(s)	Allows you to resume a previously suspended schedule. Once the schedule is resumed the Scheduler applies misfire rules if needed
▶	Run Now	Allows you to run a schedule immediately
⟳	Refresh	Allows you to refresh the list of schedules
Filter By: ⌄	Filter by	Allows you to search for a specific schedule by group name

CRON Expressions in Detail

NOTE: The following was copied from the CronTriggers Tutorial located on the Quartz website.

Introduction

CRON is a UNIX tool that has been around for a long time, so its scheduling capabilities are powerful and proven. The scheduler uses "CRON expressions", which are able to create firing schedules such as: "At 8:00am every Monday through Friday" or "At 1:30am every last Friday of the month".

Format

A CRON expression is a string comprised of 6 or 7 fields separated by white space. Fields can contain any of the allowed values, along with various combinations of the allowed special characters for that field. The fields are as follows:

Table 12. CRON expression formats

Field Name	Mandatory?	Allowed Values	Allowed Special Characters
Seconds	YES	0-59	, - * /
Minutes	YES	0-59	, - * /
Hours	YES	0-23	, - * /
Day of month	YES	1-31	, - * ? / L W C
Month	YES	1-12 or JAN-DEC	, - * /
Day of week	YES	1-7 or SUN-SAT	, - * ? / L C #
Year	NO	empty, 1970-2099	, - * /

So CRON expressions can be as simple as this: * * * * ? *

or more complex, like this: 0 0/5 14,18,3-39,52 ? JAN,MAR,SEP MON-FRI 2002-2010

Special characters

- # ** ("all values") - used to select all values within a field. For example, "" in the minute field means "every minute".
- ?* ("no specific value") - useful when you need to specify something in one of the two fields in which the character is allowed, but not the other. For example, if I want my trigger to fire on a particular day of the month (say, the 10th), but don't care what day of the week that happens to be, I would put "10" in the day-of-month field, and "?" in the day-of-week field. See the examples below for clarification.
- -* - used to specify ranges. For example, "10-12" in the hour field means "the hours 10, 11 and 12".
- ,* - used to specify additional values. For example, "MON,WED,FRI" in the day-of-week field means "the days Monday, Wednesday, and Friday".
- /* - used to specify increments. For example, "0/15" in the seconds field means "the seconds 0, 15, 30, and 45". And "5/15" in the seconds field means "the seconds 5, 20, 35, and 50". You can also specify '/' after the '' character - in this case '' is equivalent to having '0' before the '/'. '1/3' in the day-of-month field means "fire every 3 days starting on the first day of the month".

- L* ("last") - has different meaning in each of the two fields in which it is allowed. For example, the value "L" in the day-of-month field means "the last day of the month"- day 31 for January, day 28 for February on non-leap years. If used in the day-of-week field by itself, it simply means "7" or "SAT". But if used in the day-of-week field after another value, it means "the last xxx day of the month" - for example "6L" means "the last friday of the month". When using the 'L' option, it is important not to specify lists, or ranges of values, as you'll get confusing results.
- W ("weekday") - used to specify the weekday (Monday-Friday) nearest the given day. As an example, if you were to specify "15W" as the value for the day-of-month field, the meaning is: "the nearest weekday to the 15th of the month". So if the 15th is a Saturday, the trigger will fire on Friday the 14th. If the 15th is a Sunday, the trigger will fire on Monday the 16th. If the 15th is a Tuesday, then it will fire on Tuesday the 15th. However if you specify "1W" as the value for day-of-month, and the 1st is a Saturday, the trigger will fire on Monday the 3rd, as it will not 'jump' over the boundary of a month's days. The 'W' character can only be specified when the day-of-month is a single day, not a range or list of days.
  - The 'L' and 'W' characters can also be combined in the day-of-month field to yield 'LW', which translates to "last weekday of the month".
- #* - used to specify "the nth" XXX day of the month. For example, the value of "6#3" in the day-of-week field means "the third Friday of the month"(day 6 = Friday and "#3" = the 3rd one in the month). Other examples: "2#1" = the first Monday of the month and "4#5" = the fifth Wednesday of the month. Note that if you specify "#5" and there is not 5 of the given day-of-week in the month, then no firing will occur that month.
- C ("calendar") - this means values are calculated against the associated calendar, if any. If no calendar is associated, then it is equivalent to having an all-inclusive calendar. A value of "5C" in the day-of-month field means "the first day included by the calendar on or after the 5th". A value of "1C" in the day-of-week field means "the first day included by the calendar on or after Sunday".
  - The legal characters and the names of months and days of the week are not case sensitive. MON is the same as mon.

Examples

Here are some full examples:

Table 13. CRON expression examples

Expression	Meaning
0 0 12 * * ?	Fire at 12pm (noon) every day
0 15 10 ? * *	Fire at 10:15am every day
0 15 10 * * ?	Fire at 10:15am every day
0 15 10 * * ? *	Fire at 10:15am every day
0 15 10 * * ? 2005	Fire at 10:15am every day during the year 2005
0 * 14 * * ?	Fire every minute starting at 2pm and ending at 2:59pm, every day
0 0/5 14 * * ?	Fire every 5 minutes starting at 2pm and ending at 2:55pm, every day
0 0/5 14,18 * * ?	Fire every 5 minutes starting at 2pm and ending at 2:55pm, AND fire every 5 minutes starting at 6pm and ending at 6:55pm, every day
0 0-5 14 * * ?	Fire every minute starting at 2pm and ending at 2:05pm, every day
0 10,44 14 ? 3 WED	Fire at 2:10pm and at 2:44pm every Wednesday in the month of March.
0 15 10 ? * MON-FRI	Fire at 10:15am every Monday, Tuesday, Wednesday, Thursday and Friday
0 15 10 15 * ?	Fire at 10:15am on the 15th day of every month
0 15 10 L * ?	Fire at 10:15am on the last day of every month
0 15 10 ? * 6L	Fire at 10:15am on the last Friday of every month
0 15 10 ? * 6L	Fire at 10:15am on the last Friday of every month
0 15 10 ? * 6L 2002-2005	Fire at 10:15am on every last friday of every month during the years 2002, 2003, 2004 and 2005
0 15 10 ? * 6#3	Fire at 10:15am on the third Friday of every month
0 0 12 1/5 * ?	Fire at 12pm (noon) every 5 days every month, starting on the first day of the month.
0 11 11 11 11 ?	Fire every November 11th at 11:11am.

NOTE:

- Support for the features described for the 'C' character is not complete.
- Support for specifying both a day-of-week and a day-of-month value is not complete (you must currently use the '?' character in one of these fields).
- Be careful when setting fire times between mid-night and 1:00 AM - "daylight savings" can cause a skip or a repeat depending on whether the time moves back or jumps forward.

Troubleshooting the SmartCell Insight Application

7

In this chapter:

- Before You Begin
- Using the SCI Admin Interface
- Backup and Restore
- Uninstall Process
- Troubleshooting the Vertica Database

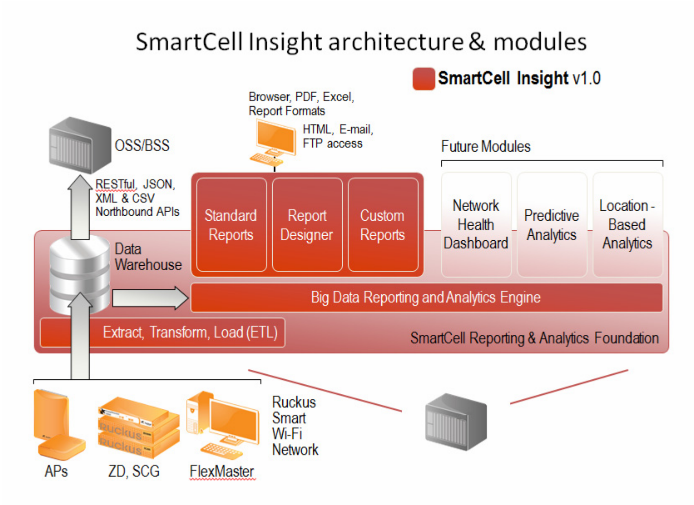
Before You Begin

SmartCell Insight is designed to be installed on a CentOS or RedHat Enterprise Linux server and is distributed as a .tar file for installation on CentOS/RHEL.

Architecture Overview

Figure 92 illustrates the data flow from data sources in structured or unstructured data formats to SCI for data integration and consolidation, transformation, query and reporting to various output formats.

Figure 92. SCI architecture overview


SmartCell Insight architecture & modules
SmartCell Insight v1.0
Browser, PDF, Excel, Report Formats
HTML, E-mail, FTP access
OSS/BSS
RESTful, JSON, XML & CSV Northbound APIs
Future Modules
Standard Reports
Report Designer
Custom Reports
Network Health Dashboard
Predictive Analytics
Location - Based Analytics
Data Warehouse
Big Data Reporting and Analytics Engine
Extract, Transform, Load (ETL)
SmartCell Reporting & Analytics Foundation
APs
ZD, SCG
FlexMaster
Ruckus Smart Wi-Fi Network

Prerequisites

The following prerequisites must be met for proper SCI operation:

Ensure NTP Server Is Reachable

The time on the machine must be correct with regards to the time zone displayed by the 'date' command. The clock must be synchronized at all times with all other Ruckus equipment by using public clock source such as an Internet NTP or a company’s internal NTP in case of no Internet access.

By default, SCI will enable NTP with the CentOS default servers, which are on the Internet.

Enable SCI-SZ Interaction

1. Login to the SZ CLI: **wsgcli**
2. Enter privileged mode: **enable**
3. Enter configuration mode: **config**
4. Enable SZ > SCI interaction: **ap-sci enable**
5. Confirm SCI interaction is enabled:
   - For SCG-200: **show running zone-global ap-sci**
   - For SZ-100 (as of 3.0): **show running common-settings ap-sci**

Enable SCI-FlexMaster Interaction

1. Log in to FlexMaster.
2. Enter the MySQL console by running the following command on the FlexMaster host:

   /opt/FlexMaster/3rdparty/mysql/mysql*/bin/mysql --socket /opt/FlexMaster/3rdparty/mysql/mysql*/mysql.sock -uroot –p
3. Enter the MySQL root user name that you used during the FM installation.
4. Run the following SQL queries:

   ```
   mysql> GRANT SELECT ON itms.* TO [reporting]@'%' IDENTIFIED BY [ruckus]
   mysql> FLUSH PRIVILEGES;
   ```

NOTE: Replace [reporting] and [ruckus] with the user name and password you would like to use for SCI.

Using the SCI Admin Interface

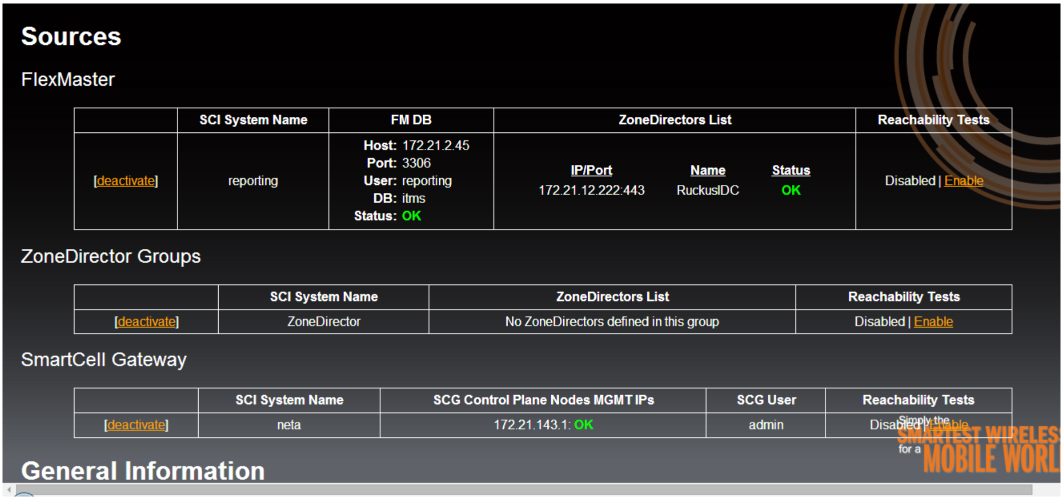
The following Web interface pages provide options for configuring and troubleshooting SCI and its connected data sources. To access the SCI Admin Console, use the following URL:

https://[SCI_IP_address]:8443

The Monitoring Page

The Monitoring page is the first place to check for information on how the system is doing. It provides a one-stop-shop for information on data source connection status, system processes, RAM distribution, HDD usage, NTP and other important OS information.

Figure 93. Data Sources



Sources

FlexMaster

	SCI System Name	FM DB	ZoneDirectors List	Reachability Tests
[deactivate]	reporting	**Host:** 172.21.2.45 **Port:** 3306 **User:** reporting **DB:** itms **Status:** OK	**IP/Port** **Name** **Status** 172.21.12.222:443 RuckusIDC OK	Disabled | Enable

ZoneDirector Groups

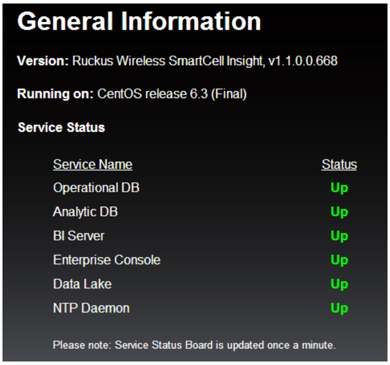
	SCI System Name	ZoneDirectors List	Reachability Tests
[deactivate]	ZoneDirector	No ZoneDirectors defined in this group	Disabled | Enable

SmartCell Gateway

	SCI System Name	SCG Control Plane Nodes MGMT IPs	SCG User	Reachability Tests
[deactivate]	neta	172.21.143.1: OK	admin	Disabled | Enable

General Information

Figure 94. Service Status



General Information

Version: Ruckus Wireless SmartCell Insight, v1.1.0.0.668

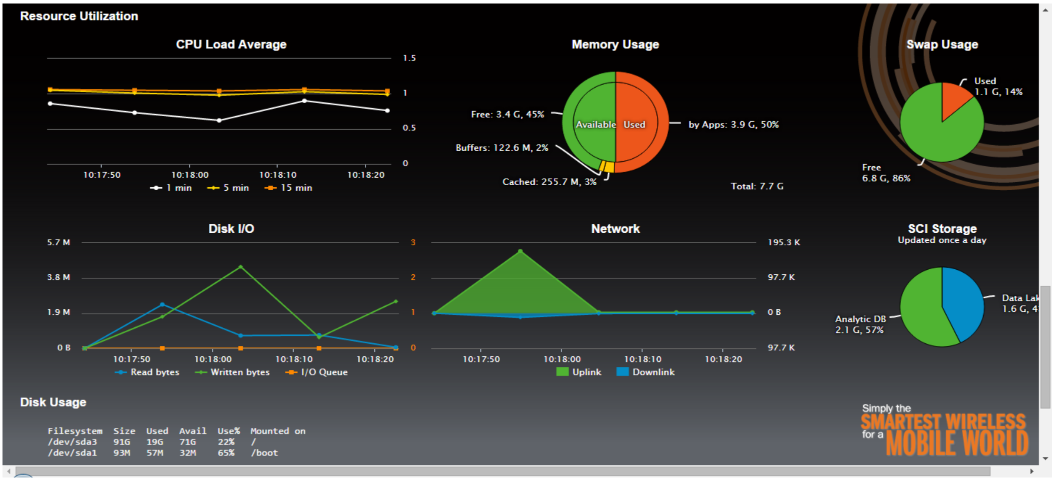
Running on: CentOS release 6.3 (Final)

Service Status

Service Name	Status
Operational DB	Up
Analytic DB	Up
BI Server	Up
Enterprise Console	Up
Data Lake	Up
NTP Daemon	Up

Please note: Service Status Board is updated once a minute.

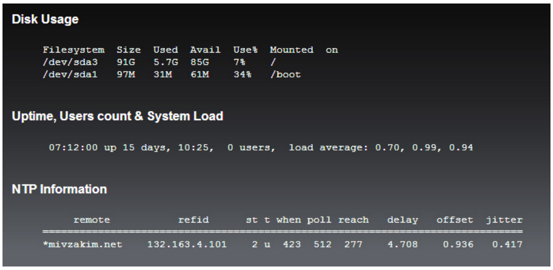
Figure 95. Resource Utilization



Disk Usage

```
Filesystem  Size  Used  Avail  Use%  Mounted on
/dev/sda3   91G   19G   71G    22%   /
/dev/sda1   93M   57M   32M    65%   /boot
```

Figure 96. Disk Usage, Uptime, NTP Information, etc.



Disk Usage

```
Filesystem  Size  Used  Avail  Use%  Mounted  on
/dev/sda3   91G   5.7G  85G    7%    /
/dev/sda1   97M   31M   61M    34%   /boot
```

Uptime, Users count & System Load

```
 07:12:00 up 15 days, 10:25,  0 users,  load average: 0.70, 0.99, 0.94
```

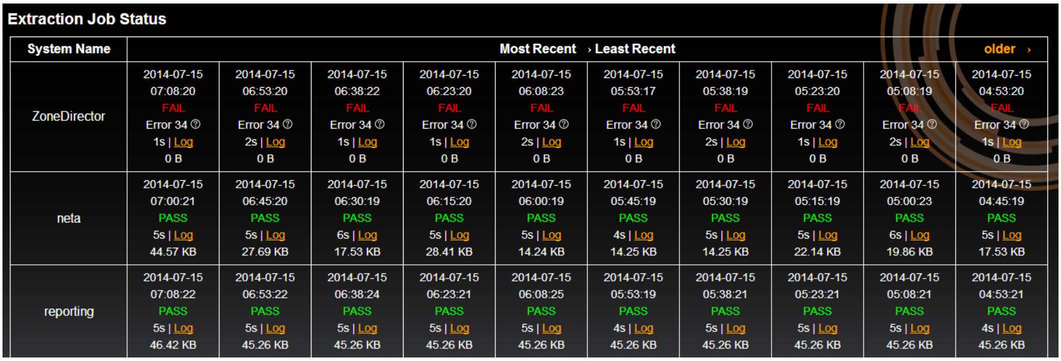
NTP Information

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*mivzakim.net    132.163.4.101    2 u  423  512  277    4.708    0.936   0.417
```

The Diagnostics Page

The Diagnostics page provides advanced debugging options for job execution and polling statistics. It shows relevant information for both Extraction and Transformation jobs including timestamp, runtime, status, link to logs and polled file size. Runtime trend graphs display overall status views. Logs are kept for 7 days and deactivated or removed sources info will be shown for another 7 days.

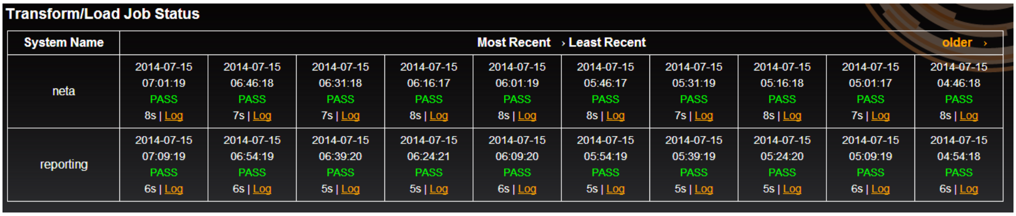
Figure 97. Extraction Job Status



Extraction Job Status

System Name	Most Recent › Least Recent									older ›
ZoneDirector	2014-07-15 07:08:20 FAIL Error 34 ? 1s | Log 0 B	2014-07-15 06:53:20 FAIL Error 34 ? 2s | Log 0 B	2014-07-15 06:38:22 FAIL Error 34 ? 1s | Log 0 B	2014-07-15 06:23:20 FAIL Error 34 ? 1s | Log 0 B	2014-07-15 06:08:23 FAIL Error 34 ? 2s | Log 0 B	2014-07-15 05:53:17 FAIL Error 34 ? 1s | Log 0 B	2014-07-15 05:38:19 FAIL Error 34 ? 2s | Log 0 B	2014-07-15 05:23:20 FAIL Error 34 ? 1s | Log 0 B	2014-07-15 05:08:19 FAIL Error 34 ? 2s | Log 0 B	2014-07-15 04:53:20 FAIL Error 34 ? 1s | Log 0 B
neta	2014-07-15 07:00:21 PASS 5s | Log 44.57 KB	2014-07-15 06:45:20 PASS 5s | Log 27.69 KB	2014-07-15 06:30:19 PASS 6s | Log 17.53 KB	2014-07-15 06:15:20 PASS 5s | Log 28.41 KB	2014-07-15 06:00:19 PASS 5s | Log 14.24 KB	2014-07-15 05:45:19 PASS 4s | Log 14.25 KB	2014-07-15 05:30:19 PASS 5s | Log 14.25 KB	2014-07-15 05:15:19 PASS 5s | Log 22.14 KB	2014-07-15 05:00:23 PASS 6s | Log 19.86 KB	2014-07-15 04:45:19 PASS 5s | Log 17.53 KB
reporting	2014-07-15 07:08:22 PASS 5s | Log 46.42 KB	2014-07-15 06:53:22 PASS 5s | Log 45.26 KB	2014-07-15 06:38:24 PASS 5s | Log 45.26 KB	2014-07-15 06:23:21 PASS 5s | Log 45.26 KB	2014-07-15 06:08:25 PASS 5s | Log 45.26 KB	2014-07-15 05:53:19 PASS 4s | Log 45.26 KB	2014-07-15 05:38:21 PASS 5s | Log 45.26 KB	2014-07-15 05:23:21 PASS 5s | Log 45.26 KB	2014-07-15 05:08:21 PASS 5s | Log 45.26 KB	2014-07-15 04:53:21 PASS 4s | Log 45.26 KB

Figure 98. Transform & Load Job Status



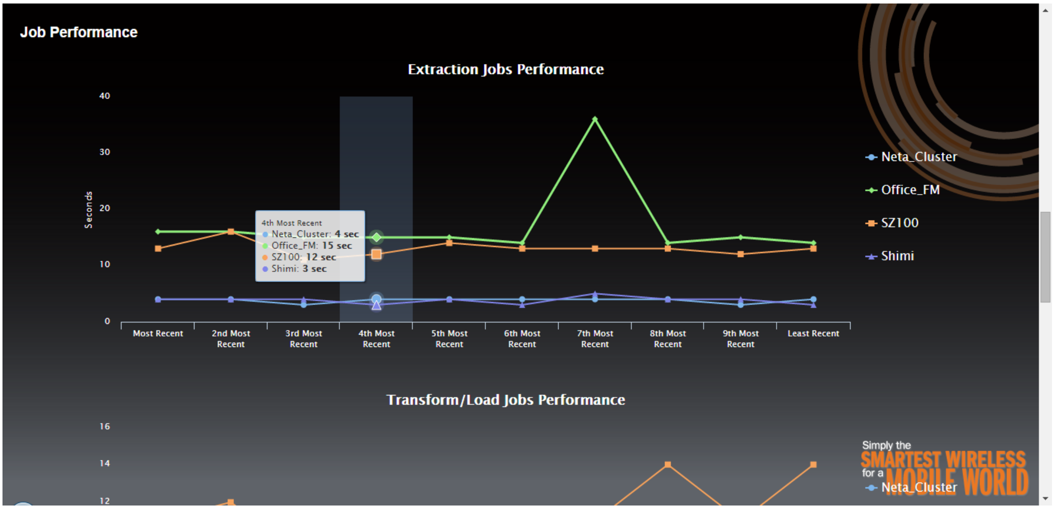
Transform/Load Job Status

System Name	Most Recent › Least Recent									older ›
neta	2014-07-15 07:01:19 PASS 8s | Log	2014-07-15 06:46:18 PASS 7s | Log	2014-07-15 06:31:18 PASS 7s | Log	2014-07-15 06:16:17 PASS 8s | Log	2014-07-15 06:01:19 PASS 8s | Log	2014-07-15 05:46:17 PASS 8s | Log	2014-07-15 05:31:19 PASS 7s | Log	2014-07-15 05:16:18 PASS 8s | Log	2014-07-15 05:01:17 PASS 7s | Log	2014-07-15 04:46:18 PASS 8s | Log
reporting	2014-07-15 07:09:19 PASS 6s | Log	2014-07-15 06:54:19 PASS 6s | Log	2014-07-15 06:39:20 PASS 5s | Log	2014-07-15 06:24:21 PASS 5s | Log	2014-07-15 06:09:20 PASS 6s | Log	2014-07-15 05:54:19 PASS 5s | Log	2014-07-15 05:39:19 PASS 5s | Log	2014-07-15 05:24:20 PASS 5s | Log	2014-07-15 05:09:19 PASS 6s | Log	2014-07-15 04:54:18 PASS 6s | Log

Job Performance

The Job Performance graphs display the performance of the most recent Extraction and Transform/Load jobs.

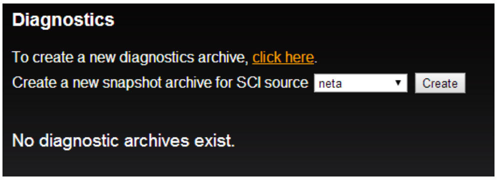
Figure 99. Job Performance



Capture Logs

From the Diagnostics page, click the **click here** link to generate a logs package. The logs will be available for download from the same location after a couple of minutes. This compressed archive contains all logs and relevant information needed for the engineering team to further debug the system. It is advisable to provide the information described in previous sections when a job is suspected to have caused the problem.

Figure 100. Create a new diagnostics archive



Diagnostics

To create a new diagnostics archive, click here.

Create a new snapshot archive for SCI source neta ▾ Create

No diagnostic archives exist.

Backup and Restore

Backup Server

The following procedure must be followed the first time you perform a backup to a backup server:

1. Create a backup server on a different machine.
2. On the backup server:
   a. Create dbadmin user.
   b. Turn off iptables.
   c. Turn off SELinux.
3. On the source server, execute the following command:

   /opt/ruckuswireless/sci/scripts/setup_backup_host.sh

You do not need to repeat these steps when backing up again to the same backup server.

Backup and Restore Process

Backup

From the second time you backup to the backup server:

1. Clean previous backups from the backup server (/opt & /tmp folders).
2. Run the following command:

   /opt/ruckuswireless/sci/scripts/sci_backup.sh

Restore

Once your backup server is set up, run the following command to restore from the backup server:

/opt/ruckuswireless/sci/scripts/sci_restore.sh

Uninstall Process

1. Uninstall SCI using the following command:

   /opt/ruckuswireless/sci/scripts/sci_uninstall
2. Refresh repository:

   yum clean all

Troubleshooting the Vertica Database

Vertica is very sensitive to abnormal system shutdown. It can recover from corrupted data due to abnormal system shutdown - however, this is NOT recommended as a practice. Some data which has not been fully committed will be lost, and this is not a guaranteed operation. It is advisable to maintain backups at intervals equal to the maximum acceptable amount of data loss in the event of a catastrophe.

NOTE: To prevent loss of data due to power outage, SCI should always be run on a redundant power supply such as a UPS system.

Using the Vertica Troubleshooting Admin Tools

1 Log into SCI via SSH as the root user.

2 Run the command:

su – dbadmin

3 Run the command:

adminTools

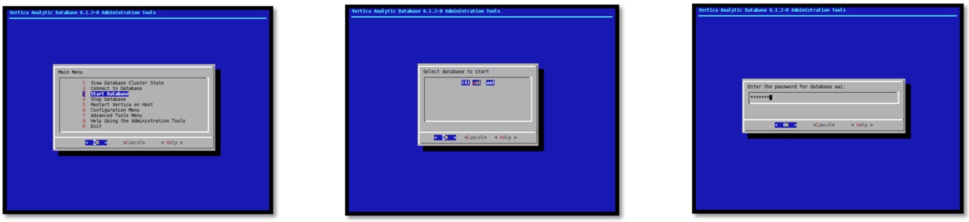
4 Type **3** and then **Enter** to run option 3 from the menu.

5 Click the **space** key to select *aa1 DB* (an X displays the selected option, as depicted).

6 Press the **Enter** key to confirm.

7 You will be asked for your password.

Figure 101. Vertica Analytic Database Administration Tools



Vertica Analytic Database 6.1.2-0 Administration Tools

Vertica Analytic Database 6.1.2-0 Administration Tools

Select database to start

(X) aa1 aa1

Vertica Analytic Database 6.1.2-0 Administration Tools

Enter the password for database aa1:

****

Recovering the Database

1 Type **dbadmin** and press the **Enter** key to confirm.

2 Since at first it will try a regular startup, it will fail.

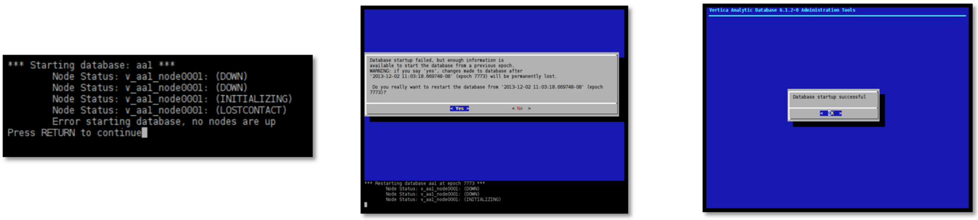
3 Press **Enter** to continue.

4 A notice asking you if you want to recover will appear. Click **Yes**.

5 It will restart from the last known good point in time and will tell you that the DB started successfully.

6 Press **Enter** to confirm, **E** to exit.

Figure 102. Vertica database startup



```
*** Starting database: aal ***
        Node Status: v_aal_node0001: (DOWN)
        Node Status: v_aal_node0001: (DOWN)
        Node Status: v_aal_node0001: (INITIALIZING)
        Node Status: v_aal_node0001: (LOSTCONTACT)
        Error starting database, no nodes are up
Press RETURN to continue
```

```
Database startup failed, but enough information is
available to start the database from a previous epoch.
WARNING: if you say 'yes', changes made to database after
'2013-12-02 11:03:18.669748-08' (epoch 7773) will be permanently lost.

 Do you really want to restart the database from '2013-12-02 11:03:18.669748-08' (epoch
7773)?
```

```
*** Restarting database aal at epoch 7773 ***
        Node Status: v_aal_node0001: (DOWN)
        Node Status: v_aal_node0001: (DOWN)
        Node Status: v_aal_node0001: (INITIALIZING)
```

```
Vertica Analytic Database 6.1.2-0 Administration Tools

Database startup successful
```

Appendix

8

In this chapter:

- Appendix A: Station Session Statistics
- Appendix B: Virtual AP Transmission and Reception Statistics
- Appendix C: Aggregation of Measurements by ZoneDirector

Appendix A: Station Session Statistics

Each virtual AP (VAP) keeps track of station session statistics and reports them to ZoneDirector or SZ. Session traffic is traffic for which a subscriber can be billed. If a station's session has not started, statistics on the 802.11 data and management frames exchanged between the station and the VAP is classified, accounted and reported as "Pre-Session" traffic and accumulated as part of VAP statistics. When a station's session has started, its statistics are accumulated as part of STA session statistics.

NOTE: In SCI v1.0, for both ZD and SZ, each WLAN has a configuration to "Ignore statistics from unauthorized clients". If this configuration is disabled and the WLAN is configured for Hotspot (WISPr) service, the client's session traffic statistics will erroneously include traffic while the client is in the un-authorized state (e.g., walled-garden traffic).

The following table lists the session statistics collected and descriptions of how SCI calculates and consolidates them for use in reports.

Table 14. Station session statistics

Name	Description
AP-ZD: client > interval-stats > tx-packets AP-SZ: ueSession > txFrames	The cumulative number of individually addressed (unicast) MSDUs encapsulated into 802.11 frames of type data and sub-type “Data” or “QoS-data” successfully transmitted by an AP to a particular STA during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. Does not include MSDUs from any frames unsuccessfully transmitted (i.e., frames for which AP did not receive an ACK control frame)—these frames will typically be retried at layer 2. However, this statistic does include re-transmitted MSDUs due to upper-layer retransmission mechanisms (e.g., TCP retries). 2. For HT frames (802.11n frames), each MSDU in the A-MSDU frame, A-MPDU frame or A-MPDU frame carrying an A-MSDU payload is decapsulated and counted as an individual packet. Only MSDUs which are successfully transmitted are counted. For example, if an AP transmits an A-MPDU frame containing 20 MSDUs and receives a Block-Ack indicating 18 MSDUs were successfully received, tx-packets would incremented by 18. 3. Frame subtypes of “Data” and “QoS-Data” are mutually exclusive, dependent on whether the STA associates as a QoS-capable STA (b13 set in FC) or a WMM STA. 4. If the frame subtype is “QoS-data”, then the user priority value in the 802.11 QoS header can have any value. 5. Frames of subtype “Null” and “QoS-Null” frames are not included in these counts. 6. Includes the following traffic: a. IP datagrams carrying application traffic. b. Non IP, layer-3 packets. c. Network-layer management traffic a STA needs to access network resources (e.g., DHCP, ARP, DNS, IGMP, SIP, etc.). d. Includes data link layer traffic above the 802.11 MAC (e.g., 802.1 frames such as LLDP (802.1ab)).
AP-ZD: client > interval-stats > tx-bytes AP-SZ: ueSession > txBytes	The cumulative number of bytes in all 802.11 MSDUs counted in tx-packets transmitted by an AP to a particular STA during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. Same notes as for tx-packets. 2. tx-bytes does not include the 8-octet LLC/SNAP header (see [2]) in an MSDU.

Name	Description
AP-ZD client > interval-stats > rx-packets AP-SZ: ueSession > rxFrames	The cumulative number of individually addressed (unicast) MSDUs decapsulated from 802.11 frames of type data and sub-type “Data” or “QoS-data” received by an AP from a particular STA during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. Same notes as for tx-packets. 2. MSDUs received from duplicate frames are excluded.
AP-ZD: client > interval-stats > rx-bytes AP-SZ: ueSession > rxBytes	The cumulative number of bytes in all 802.11 MSDUs counted in rx-packets received by an AP from a particular STA during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: same notes as for tx-bytes.
AP-ZD: client > interval-stats > throughput-est AP-SZ: ueSession > throughputEst	Estimated-throughput is the short-time averaged MSDU throughput the client is receiving when the AP is actually transmitting to that client. It is measured in bits/s and takes into account the PHY rate, error rate, and all contention due to 802.11 and non-802.11 transmitters. Because it takes into account every source of link impairment, Estimated-throughput is the best possible way of numerically characterizing client performance in a single number.
AP-ZD: session > session-sta > rssi AP-SZ: ueSession > rssi	An estimate of the received signal to noise ratio, reported in dB, at the AP for each received frame from a particular STA during a given MI. The SNR is rounded to the nearest dB. Type: 8-bit integerUnits: dB (a positive number, e.g., 19dB) Notes: 1. For SCIv1, only the last snr-uplink value in an MI is retained by the AP, regardless of the number of frames successfully received from the STA. 2. WiFi silicon produces SNR measurements for each BeamFlex antenna (individually) as well as for the combination of the two or three (depending on the AP model) antennas. The combined SNR measurement is reported to SCI. 3. Note that the combined antenna gain is determined by WiFi radio’s signal processing algorithms (maximal ratio combiner). This means that the on average, the upstream SNR reported is typically 3 to 5dB higher than the single antenna SNR.

Name	Description
AP-ZD: session > session-sta > received-signal-strength AP-SZ: ueSession > received-signal-strength	An estimate of the received signal power (aka received signal strength), reported in dBm, at the AP for each received frame from a particular STA during a given MI. The RSSI is rounded to the nearest dB. Type: 8-bit integerUnits: dBm (a negative number, e.g., -62dBm) Notes: 1. RSSI is computed from the WiFi silicon's measurement of SNR on frames received from associated STAs and a computed noise floor estimate . From these measurements, RSSI is computed as RSSI (dBm) = SNR (dB) + NFE (dBm), where NFE = a noise floor estimate computed by the WiFi silicon.
	2. Note that, the combined SNR, which is transformed to a combined RSSI, is reported to SCI. Radio engineers familiar with single-antenna RSSI should be careful to note this difference. 3. The user experience is actually determined by the STA's throughput, which in turn is governed by SNR / SINR, not the RSSI. The reason for this is because the local noise floor [physically / geographically] around the AP (or STA) can be higher than the thermal noise floor due to spurious transmitters in the environment (e.g., every electronic device transmits so-called unintentional interference, which is regulated by the FCC and other international regulatory agencies). Also, the local environment can have elevated levels of interference (e.g., caused by microwave ovens, cordless phones, distant WiFi transmitters, etc.). The result being that while the RSSI reports an absolute signal level, it does not provide information on the quality of the received signal (unlike SNR)—that is, the underlying amount of interference plus noise.

Name	Description
	4. WiFi silicon computes the NFE as follows: a) Noise floor calibration is scheduled periodically so as to have an updated NFE once per minute. b) When calibration commences, RF switches in the AP's radio "disconnect" the antennas from the receiver chain. "Disconnect" in the RF sense means the RF switches are placed in the "open" state, maximizing their isolation. This helps to make a more accurate measurement. However, strong signals incident on the antenna(s) can corrupt the measurement because the RF switches are only capable of providing a limited degree of isolation. c) When a NFE measurement is scheduled, the inter-frame gap is used (see SIFS in [1]) because for the AP making the measurement, no other STAs or APs should be transmitting at this time. Note that so-called "hidden stations" (see clause 3 in [1]) could be transmitting; interference could also be received from foreign transmitters. d) The NFE algorithm averages several of the lowest-valued NFE measurements to create the NFE. The concept of taking the minimum-valued measurements is that these are the least likely to have been corrupted by interference. e) Note: in deployments, NFE variations greater than 10dB have been observed, dependent on the environment.
	5. The RSSI together with SNR can be used to diagnose throughputs lower than expected in a given environment. For example, if the reported RSSI is high, but the SNR is low, local interference may be the cause. 6. For cost reasons, Ruckus' AP manufacturing test process does not calibrate the absolute gain of the WiFi radios' receivers. Therefore, the reported RSSI is an approximation (i.e., an uncalibrated measurement). 7. For SCIv1, only the last rssi [-uplink] value in an MI is retained by the AP, regardless of the number of frames successfully received from the STA.
AP-ZD: session > session-sta > noise-floor AP-SZ: ueSession > noiseFloor	An estimate of the radio's thermal noise floor, reported in dBm, at the AP during a given MI. The noise floor estimate is rounded to the nearest dB. Type: 8-bit integerUnits: dBm (a negative number, e.g., 102dBm) Notes: 1. The noise floor is computed by WiFi silicon in the AP. This measurement is made by the silicon during inter-packet gaps (e.g., see SIFS in [1]), when the AP is not otherwise using the airlink.

Name	Description
	2. Note that even when the AP is not using the airlink, other APs might be using the same RF channel causing low-level interference or there could be Foreign Interference, corrupting the thermal noise floor estimate. 3. Radio firmware on the AP produces one NFE estimate approximately every 60s, and only one values is used per statistics MI. The value reported to statistics is actually the median value of the last 5 NFEs produced by the WiFi silicon. Taking the median value produces a better estimate when interference is present in the environment. 4. The noise floor value will be the same for all VAPs configured on a radio.
AP-ZD: session > session-sta > associated-time AP-SZ: ueSession > firstConnection	The timestamp of the time at which the STA is successfully associated. This timestamp is used to compute the duration of time a STA must wait for authorization to access the WiFi network. Type: 64-bit signed integerUnits: Unix/Posix time ? 1000 (least significant bit has units of ms) Notes: 1. When the STA transitions from one AP to another in a given ESS, the first-assoc[-time] is not updated. The associated-time is used only on the initial association to the ESS. 2. The STA is associated when the AP successfully transmits an 802.11 Association Response frame to the STA.
AP-ZD: session > session-sta > authorized-time AP-SZ: ueSession > authorizedTime	The timestamp of the time at which a particular STA is authorized to access the WiFi network. Type: 64-bit signed integerUnits: Unix/Posix time ? 1000 (least significant bit has units of ms) Notes: 1. When the authentication method is WPA2-Enterprise, the timestamp is the time at which the 4-way handshake completes (i.e., the AP successfully receives Message 4, see clause 11.6.6.1 in [1]).
	2. When the authentication method is Open (i.e., 802.11 open system authentication without a captive portal), the timestamp is the time at which the AP successfully transmits the Association Response to the STA. 3. When the authentication method is Captive Portal (or WISPr), the timestamp is the time at which the AP receives from the Captive Portal a signal indicating the STA is authorized. Note for this authentication method, the time-to-authorized state for the STA includes the time for IP address allocation and the first DNS name resolution.

Name	Description
AP-ZD: session > session-sta > end-time AP-SZ: ueSession > disconnectTime	The timestamp of the time at which a particular STA's session ends. Note the events which cause the session to end are described in the introductory paragraphs of this section. Type: 64-bit signed integerUnits: Unix/Posix time ? 1000 (least significant bit has units of ms)
AP-ZD: session > session-sta > ap AP-SZ: apClient > ap	The base MAC address of the AP to which the STA is associated. Type: StringUnits: MAC address Notes: 1. The 4 least significant bits of the base MAC address are set to 0 (e.g., 01:23:45:2b:de:f0).
	2. The two most significant bits of the 7th most significant nibble (i.e., the "y" nibble in xx:xx:xx:yx:xx:x0) can take one of the following four values (in binary): 00xx, 01xx, 10x or 11xx. The base MAC address of the AP has the form 00xx for the "y" nibble. 3. Thus, there are a total of 64 MAC addresses assigned during the manufacturing process to each AP. Up to 32 MAC addresses can be used per radio. The AP's Ethernet MAC address is also drawn from this pool. 4. Each VAP configured on this AP is allocated a unique MAC address so constructed (e.g., 01:23:45:ab:de:f3).
AP-ZD: session > session-sta > ssid AP-SZ: apClient > ssid	The SSID value identifying the ESS to which the STA is associated. Type: StringUnits: -
AP-ZD: session > session-sta > vap-mac AP-SZ: apClient > vapMac	The MAC address of the VAP to which the STA is associated. Type: StringUnits: MAC address
AP-ZD: session > session-sta > radio-type AP-SZ: apClient > radio > mode	The radio type of the STA. Type: StringUnits: Enumeration ? {11b, 11g, 11bg, 11ng, 11a, 11na}
AP-ZD: session > session-sta > user AP-SZ: ueSession > user	The username of the username/password credential the STA used to authenticate to the WiFi network. Type: StringUnits: - Notes: 1. When EAP authentication is used, the user string is set to the value supplied by the STA in the EAP Identity Response frame
AP-ZD: session > session-sta > acct-session-id AP-SZ: ueSession > sessionID	The session ID is assigned by the WiFi network to the STA while it's associated to this particular AP. Type: StringUnits: -

Name	Description
AP-ZD: session > session-sta > acct-multi-session-id AP-SZ: ueSession > multiSessionID	The multi-session ID is assigned by the WiFi network to the STA while it's authorized on the ESS. This identifier binds together all the acct-session-ids so that statistics for a single STA, while associated to various APs in the ESS, can be properly combined. Type: StringUnits: -
AP-ZD: client > hostname AP-SZ: apClient > sta > hostname	The STA's hostname which the AP obtains by snooping on DHCP. Type: StringUnits: -
AP-ZD: session > session-sta > vlan AP-SZ: apClient > sta > vlan	The STA's VLAN ID is assigned by the WiFi network. Type: StringUnits: -
AP-ZD: session > session-sta > dvcinfo AP-SZ: apClient > sta > devInfo	Information on the STA including it's OS (operating system) type. Type: StringUnits: -
AP-ZD: session > session-sta > disconnect-reason AP-SZ: ueSession > disconnectReason	The reason the STA ended the session. Valid reasons are take from Table 8-36 inn [1]. Type: EnumerationUnits: - Notes: 1. Reason code value 64 means the user logged out using the Captive Portal and overrides the reason provided in Table 8-36 of [1].

Notes:

1 "subtype any" means the subtype value in the FC field (802.11 MAC header) can take on values of 0 to 15 inclusive.

Appendix B: Virtual AP Transmission and Reception Statistics

Each virtual AP keeps track of transmission and reception statistics which are not included in STA session statistics and reports them to ZD/SZ. These statistics are described in Table 15 below.

Table 15. AP Transmission and Reception Statistics

Name	Description
AP-ZD: vap > interval-stats > tx-packets AP-SZ: report > bin > radio > wlan > txDataFrames_r	The cumulative number of MSDUs encapsulated into 802.11 frames of type data and sub-type “Data” or “QoS-data” successfully transmitted by an AP to any STA during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. This counter includes both individually addressed (unicast) and group addressed (multicast and broadcast) frames.
	2. Does not include MSDUs from any frames unsuccessfully transmitted (i.e., frames for which AP did not receive an ACK control frame)—these frames will typically be retried at layer 2. However, this statistic does include re-transmitted MSDUs due to upper-layer retransmission mechanisms (e.g., TCP retries). 3. For HT frames (802.11n frames), each MSDU in the A-MSDU frame, A-MPDU frame or A-MPDU frame carrying an A-MSDU payload is decapsulated and counted as an individual packet. Only MSDUs which are successfully transmitted are counted. For example, if an AP transmits an A-MPDU frame containing 20 MSDUs and receives a Block-Ack indicating 18 MSDUs were successfully received, tx-packets would incremented by 18.
	4. Frame subtypes of “Data” and “QoS-Data” are mutually exclusive, dependent on whether the STA associates as a QoS-capable STA (b13 set in FC) or a WMM STA. 5. If the frame subtype is “QoS-data”, then the user priority value in the 802.11 QoS header can have any value. 6. Frames of subtype “Null” and “QoS-Null” frames are not included in these counts. 7. Includes the following traffic: a. IP datagrams carrying application traffic. b. Non IP, layer-3 packets. c. Network-layer management traffic a STA needs to access network resources (e.g., DHCP, ARP, DNS, IGMP, SIP, etc.). d. Includes data link layer traffic above the 802.11 MAC (e.g., 802.1 frames such as LLDP (802.1ab)).
AP-ZD: vap > interval-stats > tx-bytes AP-SZ: report > bin > radio > wlan > txDataBytes_r	The cumulative number of bytes in all 802.11 MSDUs counted in tx-packets transmitted by an AP to any STA during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. Same notes as for tx-bytes. 2. tx-bytes does not include the 8-octet LLC/SNAP header (see [2]) in an MSDU.

Name	Description
AP-ZD: vap > interval-stats > rx-packets AP-SZ: report > bin > radio > wlan > rxDataFrames_r	The cumulative number of MSDUs decapsulated from 802.11 frames of type data and sub-type “Data” or “QoS-data” received by an AP from any STA during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. This counter includes both individually addressed (unicast) and group addressed (multicast and broadcast) frames. 2. Same notes as for tx-packets. 3. MSDUs received from duplicate frames are excluded.
AP-ZD: vap > interval-stats > rx-bytes AP-SZ: report > bin > radio > wlan > rxDataBytes_r	The cumulative number of bytes in all 802.11 MSDUs counted in rx-packets received by an AP from a particular STA during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: same notes as for tx-bytes.
AP-ZD: vap > interval-stats > tx-mgmt-frames AP-SZ: report > bin > radio > wlan > txMgmtFrames_r	The cumulative number of 802.11 frames of type management and sub-type "any" successfully transmitted by an AP during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. This counter includes both individually addressed (unicast) and group addressed (multicast and broadcast) frames.
	2. Does not include any frames unsuccessfully transmitted (i.e., frames for which AP did not receive an ACK control frame)—these frames will typically be retried at layer 2. 3. Does not include any class-1 management frames transmitted to the STA before it associated to the VAP (see clause 10.3.2 and 10.3.3 in [1], e.g., Probe Response frames, Authentication frames and Public Action frames such as IEEE 802.11u GAS, etc.). 4. Includes all class-2 management frames (e.g., (Re)Association Response) and all class-3 management frames.
AP-ZD: vap > interval-stats > tx-mgmt-bytes AP-SZ: report > bin > radio > wlan > txMgmtBytes_r	The cumulative number of bytes in all 802.11 frames included in tx-mgmt-frames successfully transmitted by an AP during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. Includes all bytes in the MMDPU—includes the 802.11 MAC header, frame body and FCS (see Figure 8-1 in [1]). Does not include any bytes in the PHY header or PLCP header.

Name	Description
AP-ZD: vap > interval-stats > rx-mgmt-frames AP-SZ: report > bin > radio > wlan > rxMgmtFrames_r	The cumulative number of 802.11 frames of type management and sub-type "any" successfully received by an AP during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. This counter includes both individually addressed (unicast) and group addressed (multicast and broadcast) frames.
	2. For frame sub-types which require the AP to transmit an ACK control frame (e.g., Association Request frame), duplicate frames are excluded. Note if the AP receives Probe Request frames unicast transmitted to its BSSID, it will exclude duplicate (re-tried) Probe Request frames. 3. An AP receiving Probe Request frames transmitted to the broadcast MAC destination address having a matching SSID (either exact match or wildcard match) will count each successfully received Probe Request frame in this parameter.
AP-ZD: vap > interval-stats > rx-mgmt-bytes AP-SZ: report > bin > radio > wlan > rxMgmtBytes_r	The cumulative number of bytes in all 802.11 frames included in rx-mgmt-frames successfully received by an AP during a given MI. Type: 64-bit unsigned integerUnits: n/a Notes: 1. Same notes as for tx-mgmt-bytes. 2. Includes all bytes in the MMDPU—includes the 802.11 MAC header, frame body and FCS (see Figure 8-1 in [1]). Does not include any bytes in the PHY header or PLCP header.

Appendix C: Aggregation of Measurements by ZoneDirector

Table 16 explains the method used by ZDs to aggregate statistics reported by APs as well as the method APs used to aggregate data to report to SZ. Statistics for which no aggregation is performed are omitted from this table.

Table 16. Mapping of Aggregated Statistics to AP Statistics

No.	ZD & SZ Aggregated Statistic	Description of Aggregation Method
1	ZD: vap > interval-stats > tx-bytes AP > SZ: report > bin > radio > wlan > txDataBytes_r	$\sum_{i=0}^{9} tx\text{-}bytes(i)$ where, • tx-bytes(i) are the number of tx-bytes transmitted by the AP during the ith MI. Note: there are 10 90-s MIs in a 15-min AMRI.
2	ZD: vap > interval-stats > rx-bytes AP > SZ: report > bin > radio > wlan > rxDataBytes_r	$\sum_{i=0}^{9} rx\text{-}bytes(i)$ where, • rx-bytes(i) are the number of rx-bytes received by the AP during the ith MI. Note: in general, the number of STAs associated to the VAP will not remain constant over the duration of the AMRI. Note: there are 10 90-s MIs in a 15-min AMRI.
3	ZD: client > interval-stats > tx-bytes AP > SZ: ueSession > txBytes	$\sum_{i=0}^{9} tx\text{-}bytes(i)$ where, • tx-bytes(i) are the number of tx-bytes transmitted to the STA during the ith MI. Note: there are 10 90-s MIs in a 15-min AMRI.
4	ZD: client > interval-stats > rx-bytes AP > SZ: ueSession > rxBytes	$\sum_{i=0}^{9} rx\text{-}bytes(i)$ where, • rx-bytes(i) are the number of rx-bytes received from the STA during the ith MI. Note: there are 10 90-s MIs in a 15-min AMRI.

No.	ZD & SZ Aggregated Statistic	Description of Aggregation Method
5	ZD: client > interval-stats > throughput-est AP > SZ: ueSession > throughputEst	last(throughput-est(0), throughput-est(1), … throughput-est(9)) where, • throughput-est(i) is the saturated throughput of the VAP towards the STA during the ith MI. • last(•) is a function whose output equals the value of the last argument (i.e., the value of throughput-est on the final MI in the AMRI)
6	ZD: session > session-sta > rssi AP > SZ: ueSession > rssi	last(rssi(0), rssi(1), … rssi(9)) where, • rssi(i) is the uplink SNR in the ith MI during an AMRI
7	ZD: session > session-sta > max-rssi AP > SZ: ueSession > maxRssi	max(rssi(0), rssi(1), … rssi(9)) where, • max(•) is a function whose output equals the maximum value of all the arguments
8	ZD: session > session-sta > min-rssi AP > SZ: ueSession > minRssi	min(rssi(0), rssi(1), … rssi(9)) where, • min(•) is a function whose output equals the minimum value of all the arguments
9	ZD: session > session-sta > first-rssi AP > SZ: ueSession > firstRssi	first(rssi(0), rssi(1), … rssi(9)) where, • first(•) is a function whose output equals the value of the first argument
10	ZD: session > session-sta > received-signal-strength AP > SZ: ueSession > received-signal-strength	last(received-signal-strength(0), received-signal-strength(1), … received-signal-strength(9)) where, • received-signal-strength(i) is the uplink received signal power during the ith MI during an AMRI.
11	ZD: session > session-sta > max-received-signal-strength AP > SZ: ueSession > max-received-signal-strength	max(received-signal-strength(0), received-signal-strength(1), … received-signal-strength(9))

No.	ZD & SZ Aggregated Statistic	Description of Aggregation Method
12	ZD: session > session-sta > min-received-signal-strength AP > SZ: ueSession > min-received-signal-strength	min(received-signal-strength(0), received-signal-strength(1), … received-signal-strength(9))
13	ZD: session > session-sta > first-received-signal-strength AP > SZ: ueSession > first-received-signal-strength	first(received-signal-strength(0), received-signal-strength(1), … received-signal-strength(9))
14	ZD: session > session-sta > noise-floor AP > SZ: ueSession > noisefloor	last(noise-floor(0), noise-floor(1), … noise-floor(9)) where, • nfe(i) is the noise floor estimate of the VAP during the ith MI.

Index

A

Access Point Traffic Report 61
Action Icons 74
Adding a FlexMaster Data Source 103
Adding a Report Description 82
Adding Fields and Filters 75
Adding Users 126
Admin Console 92
Admin Interface
  Diagnostics Page 114
  Monitor Page 93
  System Setup Page 103
Administration Interface 92
Administrator Login 119
Alert History 118
Alert Settings 112
AP Groups Response Time Trend Report 51
AP Inventory Report 47
AP Licensing 107
AP Model Distribution 55
AP Reboots Report 58
AP Response Statistics 72
AP Response Time Report 52
AP Statistics 72
AP Traffic Volume Report 64
APs by Model 55
Auto-Refresh 31
Available Metrics 88

B

Backup 144

C

Changing the Admin Password 119
Chart Format 77
Chart Type 78
Client Complete Sessions 72
Client Fingerprint Report 39
Client Health Dashboard 33
Client Potential Throughput Report 62
Client Session Intervals 72
Client Throughput Estimate Report 63
Configuring a FlexMaster Data Source 103
Configuring Data Purge Policy 110
Configuring Data Sources 103
Configuring SmartZone Data Sources 106
Configuring SMPT Settings 111
Controller Hardware Utilization Report 54
Controller Inventory Report 48
Controller Resource Utilization 72
Controller Statistics 72
Creating Users and Roles 125
CRON 131
Custom Report Scheduling 129
Custom Reports 68

D

Dashboards 30
Data Purge Policy 110
Data Purge Settings 110
Data Source Configuration 103
Data Sources 93, 103
Deactivated Data Source
  Reactivating 98
Deactivating a Data Source 95
Deleting a Deactivated Data Source 97
Deleting Roles 128
Deleting Users 127
Description 82
Diagnostics Archive 114
Diagnostics Page 114, 142
Displaying ETL Log Files 116
Distribution of APs by Model 55

E

Editing Roles 128
Editing User Information 126
Email Alerts 112
Email Settings 111
Enterprise Console 125
ETL Log Results Display 116
Events 72

Extraction Job Status 116

F

Field Definition 77
Fields and Filters 75
Filters 79
Finding Roles 129
Finding Users 127
First Experience of New Clients Report 39
FlexMaster Data Source Configuration 103

I

Importing a License File 107
Importing a SmartZone Data Source 106
Individual AP Response Time Report 53
Individual AP Traffic Report 65
Installation Overview 20
Interface settings 23
Introducing SmartCell Insight 14
Inventory Reports 47

J

Job Performance 117

L

Level Fields 76
Licensing 107
Log Files 116
Longest Response Time Report 59

M

Managing Roles 127
Map View 31
Measure Fields 76
Metrics 88
Monitor Page 93
Monitoring Page 140

N

Network Health Dashboard 30
New Analyzer Report 68, 70
New Analyzer Report Page 73
NTP 123, 138
Number of Sessions Report 41
Number of Unique Clients Report 42

O

Operational Reports 51

P

Performance Graphs 117
Potential Throughput Report 62
Pre-installation Procedures 20, 138
Purge Policy 110

R

Reactivating a Deactivated Data Source 98
Report Description 82
Report Workspace Elements 24
Response Time Report 59
Response Time Tests 94, 95, 99
Restore 144
Rogue APs 72
Rogue APs Report 56
Ruckus Dashboards 30
Ruckus Reports 37

S

Schedling Custom Reports 129
SCI - AP Response Time Tests 99
SCI > AP Response Time Tests 94, 95
SCI Sources Configuration 103
Session Bytes Transferred report 43
Session Duration Report 44
Session Inventory Report 49
SmartZone Data Source 106
SMTP Settings 111
Snapshot Archive 116
SSL Settings 108
System Configuration 108
System Setup Page 103
System Timekeeping 123

T

Throughput Estimate of Clients Report 63
Throughput Estimate Report 63
Time Period Fields 76
Top AP Reboots Report 58
Top APs by Traffic Volume Report 64

Top APs with Most Topology Changes Report 57
Top Clients by Traffic Volume Report 45
TopN APs with the Longest Response Time Report 59
Topology Change Report 57
Traffic Report 61
Traffic Reports 61
Transform/Load Job Status 116
Troubleshooting
  Vertica 145

U

Uninstall 144
Upgrading the SCI License 107
Usage Distribution and Trends Dashboard 34
User interface 23
Users and Roles 125
Using the Enterprise Console 125
Using the Map View 31
Using the Scheduler 129

V

Vertica 145

W

Workspace 24

Z

ZoneDirector Groups 104

Ruckus®

Simply Better Wireless.

350 West Java Dr. Sunnyvale, CA 94089. USA
www.ruckuswireless.com