

# Ruckus SmartZone 100 and Virtual SmartZone-Essentials Administrator Guide, 5.1

Supporting SmartZone 5.1

# Copyright, Trademark and Proprietary Rights Information

© 2019 CommScope, Inc. All rights reserved.

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

## Export Restrictions

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

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

## Disclaimer

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

## Limitation of Liability

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

## Trademarks

ARRIS, the ARRIS logo, CommScope, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, Edgelron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, and ZoneFlex are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

# Contents

---

<b>Preface.....</b>	<b>11</b>
Document Conventions.....	11
Notes, Cautions, and Warnings.....	11
Command Syntax Conventions.....	12
Document Feedback.....	12
Ruckus Product Documentation Resources.....	12
Online Training Resources.....	13
Contacting Ruckus Customer Services and Support.....	13
What Support Do I Need?.....	13
Open a Case.....	13
Self-Service Resources.....	13
<b>Navigating the Dashboard.....</b>	<b>15</b>
Setting Up the Controller for the First Time.....	15
Logging On to the Web Interface.....	15
Web Interface Features.....	16
Changing the Administrator Password.....	18
Setting User Preferences.....	18
Logging Off the Controller.....	19
Configuring Global Filters.....	20
Warnings and Notifications.....	21
Warnings.....	21
Setting Global Notifications.....	22
Health and Maps.....	22
Understanding Cluster and AP Health Icons.....	23
Customizing Health Status Thresholds.....	23
Using the Health Dashboard Map.....	25
Viewing Switches on the Dashboard.....	33
Traffic Analysis.....	34
Customizing Traffic Analysis.....	35
Configuring Traffic Analysis Display for APs.....	35
Configuring Traffic Analysis Display for WLANs.....	37
Configuring Traffic Analysis Display for Top Clients.....	37
SmartCell Insight Report on Actual Traffic Rate for APs and Client.....	38
<b>Configuring General Settings.....</b>	<b>41</b>
Viewing System Settings.....	41
Configuring System Time.....	43
Configuring the Remote Syslog Server.....	43
Configuring Northbound Data Streaming Settings.....	45
Setting the Northbound Portal Password.....	46
Enabling Global SNMP Notifications.....	46
Configuring SNMP v2 Agent.....	46
Configuring SNMP v3 Agent.....	47
Configuring SMTP Server Settings.....	48
Configuring FTP Server Settings.....	49
Configuring the SMS Gateway Server.....	50

Location Service.....	50
Working with Maps.....	52
Importing a Floorplan Map.....	52
Viewing RF Signal Strength.....	55
Monitoring APs Using the Map View.....	55
<b>Configuring AP Settings.....</b>	<b>57</b>
Approving APs.....	57
Working with AP Registration Rules.....	57
Creating an AP Registration Rule.....	57
Configuring Registration Rule Priorities.....	58
Tagging Critical APs.....	59
Configuring the Tunnel UDP Port.....	60
Setting the Country Code.....	60
<b>Working With Access Points.....</b>	<b>61</b>
Understanding WLAN Services.....	61
Hierarchy Overview.....	61
Working with AP Zones.....	62
Working with AP Groups.....	71
Monitoring Domains, Zones, and AP Groups.....	80
Viewing Modes.....	82
AP Status.....	83
Configuring Access Points.....	83
Configuring the M510 AP.....	88
Managing Access Points.....	93
Overview of Access Point Configuration.....	93
Viewing Managed Access Points.....	93
Downloading the Support Log from an Access Point.....	94
Provisioning and Swapping Access Points.....	94
Editing Swap Configuration.....	96
Approving Mesh APs.....	96
Moving a Single Access Point to a Different AP Zone.....	97
Monitoring Access Points.....	97
Multi-Tunnel Support for Access Points.....	102
Configuring Multiple Tunnels for Zone Templates.....	103
Configuring Multiple Tunnels for Zone.....	104
Configuring Multiple Tunnels in WLANs.....	106
<b>Viewing the System Cluster Overview.....</b>	<b>107</b>
Control Planes and Data Planes.....	107
Interface and Routing.....	108
Displaying the Chassis View of Cluster Nodes.....	109
Configuring the Control Plane.....	110
Rebalancing APs.....	113
Monitoring Cluster Settings.....	114
Clearing or Acknowledging Alarms.....	115
Filtering Events.....	115
Creating DP Zone Affinity Profile.....	115
Verifying DP and Profile Version Match.....	116
Verifying Zone and Profile Version Match.....	116
Enabling Flexi VPN.....	116



Enabling L3 Roaming Criteria for DP.....	117
<b>Certificates.....</b>	<b>119</b>
Importing New Certificates.....	119
Assigning Certificates to Services.....	120
Generating Certificate Signing Request (CSR).....	120
Managing AP Certificates.....	121
Importing Trusted CA Certificates.....	123
<b>Configuring Templates.....</b>	<b>125</b>
Working with Zone Templates.....	125
Creating Zone Templates.....	125
Applying Zone Templates.....	130
Exporting Zone Templates.....	130
Importing Zone Templates.....	131
Working with WLAN Templates.....	131
Creating WLAN Templates.....	131
Applying a WLAN Template.....	131
<b>Managing ICX Switches.....</b>	<b>133</b>
Overview of ICX Switch Management.....	133
Preparing ICX Devices to be Managed by SmartZone.....	133
<b>ICX Switch Configuration and Behavior.....</b>	<b>135</b>
ICX Switch Behavior with SmartZone.....	135
Enabling an ICX Device to be Managed by SmartZone.....	135
Manually Configuring the SmartZone IP Address on an ICX Switch.....	135
Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch.....	136
Displaying the SmartZone Connection Status.....	136
Disconnecting the Switch Connection with SmartZone.....	137
Disabling SmartZone Management on the ICX Switch.....	137
<b>SmartZone Switch Management.....</b>	<b>139</b>
Using SmartZone Settings to Manage ICX Switch Groups.....	139
Creating ICX Switch Groups.....	139
Creating Switch Registration Rules.....	140
Approving ICX Switches.....	141
Moving the Switches between Groups.....	142
Deleting Switches.....	143
Backing up and Restoring ICX Switch Configuration.....	143
Scheduling a Firmware Upgrade.....	144
Viewing Switch Information.....	146
Viewing Switch Configuration Information.....	148
Viewing Port Details.....	149
Viewing Switch Health.....	153
Viewing Alarms.....	156
Viewing Events.....	158
Viewing LLDP Neighbor Information.....	159
Viewing Traffic Trends in the Switch.....	159
Viewing Firmware History of the Switch.....	161
<b>Troubleshooting Switch Issues.....</b>	<b>163</b>
Troubleshooting Using Custom Events.....	164

Troubleshooting Using Remote Operations.....	164
<b>Viewing Switches on the Dashboard.....</b>	<b>167</b>
<b>Working with WLANs and WLAN Groups.....</b>	<b>169</b>
Zones, AP Groups, and WLANs.....	169
Viewing Modes.....	169
WLAN Groups.....	170
Creating a WLAN Group.....	170
Creating a WLAN Configuration.....	171
802.11 Fast BSS Transition.....	184
802.11w MFP.....	184
Airtime Decongestion.....	184
Band Balancing.....	184
Bypassing Apple CNA.....	184
Client Admission Control.....	185
Client Load Balancing.....	185
Mobility Domain ID.....	186
Portal-based WLANs.....	186
Rate Limiting Ranges for Policies.....	187
Transient Client Management.....	188
Optimized Connectivity Experience.....	188
Working with WLAN Schedule Profiles.....	188
Managing WLANs.....	189
Extracting a WLAN Template.....	189
Applying a WLAN Template.....	190
How Dynamic VLAN Works.....	190
<b>Managing Clients.....</b>	<b>193</b>
Working with Wireless Clients.....	193
Viewing a Summary of Wireless Clients.....	193
Viewing Information about a Wireless Client.....	194
Deauthorizing a Wireless Client.....	195
Blocking a Wireless Client.....	195
Unblocking a Wireless Client.....	195
Disconnecting a Wireless Client.....	196
Working with Wired Clients.....	196
Viewing a Summary of Wired Clients.....	196
Viewing Information about a Wired Client.....	197
Deauthorizing a Wired Client.....	197
Working with Users and Roles.....	197
Creating a User Role.....	198
Creating a User Role with Active Directory Authentication.....	207
Creating a User Role with 802.1x Authentication.....	207
Limitations Applying Role Policies to Users.....	208
Creating a Local User.....	208
Creating a Subscription Package.....	210
Working with Guest Passes.....	211
Generating Guest Passes.....	212
Creating a Guest Pass Template.....	216
Creating a Guest Instruction SMS Template.....	217
Exporting the Guest Pass to CSV.....	219

Generating Guest Passes from an Imported CSV.....	219
Printing the Guest Pass.....	222
Sending the Guest Pass via Email.....	222
Sending the Guest Pass via SMS.....	223
Working with Dynamic PSKs.....	224
Viewing Dynamic PSKs.....	225
Generating Dynamic PSKs.....	226
Importing Dynamic PSKs.....	227
Creating an External DPSK Over RADIUS WLAN.....	228
<b>Application Recognition and Control.....</b>	<b>231</b>
Monitoring Applications.....	231
<b>Services and Profiles.....</b>	<b>235</b>
Working with Hotspots and Portals.....	235
Creating a Guest Access Portal.....	235
Working with Hotspot (WISPr) Services.....	237
Creating a Web Authentication Portal.....	240
Creating a WeChat Portal.....	242
Working with Hotspot 2.0 Services.....	244
Creating a UA Blacklist Profile.....	250
Creating a Portal Detection and Suppression Profile.....	252
Configuring Access Control.....	254
Creating a User Traffic Profile.....	254
Creating OS Policy Service.....	259
VLAN Pooling.....	260
Create Precedence Profile.....	262
Creating an L2 Access Control Service.....	264
Creating Blocked Clients.....	265
Creating a Client Isolation Whitelist.....	266
Creating Time Schedules.....	267
Creating a DNS Server Profile.....	267
Creating a Traffic Class Profile .....	268
Configuring Application Controls.....	271
Creating an Application Control Policy.....	271
Implementing an Application Control Policy.....	274
Creating a User Defined Application.....	276
Working with Application Signature Package.....	278
URL Filtering.....	279
Viewing a Summary of URL Filters.....	280
Creating a URL Filtering Policy.....	280
Enabling URL Filtering on the Controller.....	283
Enabling URL Filtering in the User Traffic Profile.....	284
Managing URL Filtering Licenses.....	285
Understanding WiFi Calling.....	286
Creating a WiFi Calling Profile.....	286
Configuring WiFi Calling in WLAN.....	287
Analyzing WiFi Calling Statistics.....	288
Authentication.....	289
Creating Non-Proxy Authentication AAA Servers for Standby Cluster.....	289
Creating Proxy AAA Servers for Standby Cluster.....	291

Authentication Support Matrix.....	297
Accounting.....	301
Creating Non-Proxy Accounting AAA Servers for Standby Cluster.....	301
Creating Proxy Accounting AAA Servers for Standby Cluster.....	303
Classifying Rogue Policy.....	305
Bonjour.....	306
Bonjour Gateway.....	306
Bonjour Fencing.....	308
Working with Tunnels and Ports.....	312
Creating a Ruckus GRE Profile.....	312
Creating a Soft GRE Profile.....	313
Creating an IPsec Profile.....	314
Creating an Ethernet Port Profile.....	317
Creating a Tunnel DiffServ Profile.....	321
Split Tunnel Profile.....	322
Enabling Tunnel Encryption.....	323
Forwarding Multicast Packets.....	324
DHCP/NAT.....	325
AP-based DHCP/NAT.....	325
Profile-based DHCP.....	325
Profile-based NAT.....	325
Network Topology.....	326
Hierarchical Network Topology.....	328
Configuring AP-based DHCP Service Settings.....	328
Creating an AP DHCP Pool.....	334
Creating Profile-based DHCP.....	336
Creating Profile-based NAT.....	338
Configuring DHCP/NAT with Mesh Options.....	339
3rd Party Service.....	340
Enabling Ekahau and Aeroscout/Stanley RTLS Tags.....	340
<b>Working with Reports.....</b>	<b>343</b>
Types of Reports.....	343
Client Number Report.....	343
Client Number vs Airtime Report.....	343
Continuously Disconnected APs Report.....	343
Failed Client Associations Report.....	343
New Client Associations Report.....	343
System Resource Utilization Report.....	344
TX/RX Bytes Report.....	344
Managing Report Generation.....	344
Creating Reports.....	344
Generating Reports.....	346
Rogue Access Points.....	346
Viewing Rogue Access Points.....	346
Marking Rogue Access Points.....	347
Locating a Rogue Access Point.....	347
Historical Client Stats.....	348
Viewing AP Client Statistics.....	348
Ruckus AP Tunnel Stats.....	349
Viewing Statistics for Ruckus GRE Tunnels.....	349

Viewing Statistics for SoftGRE Tunnels.....	350
Viewing Statistics for SoftGRE IPsec Tunnels.....	351
<b>Troubleshooting.....</b>	<b>353</b>
Troubleshooting Client Connections.....	353
Troubleshooting through Spectrum Analysis.....	355
<b>Managing Events and Alarms.....</b>	<b>357</b>
Viewing Events.....	357
Sending SNMP Traps and Email Notifications for Events.....	357
Configuring Event Threshold.....	358
Creating Custom Events for ICX Switches.....	359
Configuring Alarms.....	361
Clearing Alarms.....	361
Acknowledging Alarms.....	362
Applying Filters.....	362
<b>Administering the Controller.....</b>	<b>363</b>
Managing Administrator and Roles.....	363
Creating User Groups.....	363
Creating Administrator Accounts.....	366
Configuring Administrator Accounts.....	368
Working with AAA Servers.....	370
Enabling the Access Control List.....	376
Creating Account Security.....	377
Backing Up and Restoring Clusters.....	381
Creating a Cluster Backup.....	381
Backing Up and Restoring the Controller's Network Configuration from an FTP Server.....	382
Backing up Cluster Configuration.....	389
Upgrading the Controller.....	391
Performing the Upgrade.....	391
Uploading an AP Patch File.....	392
Verifying the Upgrade.....	393
Rolling Back to a Previous Software Version.....	393
Upgrading the Data Plane.....	393
Uploading the Switch Firmware to the Controller.....	396
Managing Licenses.....	396
Viewing Installed Licenses.....	397
Configuring the License Server.....	399
Configuring License Bandwidth.....	400
Configuring the DHCP/NAT License Assignment.....	401
Configuring URL Filtering Licenses.....	402
ZoneDirector to SmartZone Migration.....	403
Monitoring Administrator Activities.....	403
<b>Diagnostics.....</b>	<b>405</b>
Applying Scripts.....	405
Uploading AP CLI Scripts.....	405
Executing AP CLI Scripts.....	406
Scheduling AP CLI Scripts.....	407
Viewing Scripts.....	408
Viewing Script Execution Summary.....	409

Viewing and Downloading Logs.....	410
Available System Logs for platforms.....	411
RADIUS.....	411
Viewing RADIUS Proxy Settings.....	411
<b>Ports to Open for AP-Controller Communication.....</b>	<b>413</b>
<b>Web Server Support.....</b>	<b>417</b>
<b>Appendix.....</b>	<b>419</b>
Copyright.....	419

# Preface

- Document Conventions..... 11
- Command Syntax Conventions..... 12
- Document Feedback..... 12
- Ruckus Product Documentation Resources..... 12
- Online Training Resources..... 13
- Contacting Ruckus Customer Services and Support..... 13

## Document Conventions

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

**TABLE 1** Text Conventions

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

## Notes, Cautions, and Warnings

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

### NOTE

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

### ATTENTION

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



### CAUTION

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



### DANGER

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

# Command Syntax Conventions

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

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

## Document Feedback

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

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

When contacting us, include the following information:

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

For example:

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

## Ruckus Product Documentation Resources

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

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

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



## Online Training Resources

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

## Contacting Ruckus Customer Services and Support

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

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

### What Support Do I Need?

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

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

### Open a Case

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

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

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

### Self-Service Resources

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

- Technical Documentation—<https://support.ruckuswireless.com/documents>

## Preface

### Contacting Ruckus Customer Services and Support

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

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

# Navigating the Dashboard

---

• Setting Up the Controller for the First Time.....	15
• Logging On to the Web Interface.....	15
• Web Interface Features.....	16
• Changing the Administrator Password.....	18
• Setting User Preferences.....	18
• Logging Off the Controller.....	19
• Configuring Global Filters.....	20
• Warnings and Notifications.....	21
• Health and Maps.....	22
• Traffic Analysis.....	34

## Setting Up the Controller for the First Time

The controller must first be set up on the network.

### NOTE

Setting up the controller is described in the *Getting Started Guide* or *Quick Setup Guide* for your controller platform.

For information on how to set up the controller for the first time, including instructions for running and completing the controller's *Setup Wizard*, see the *Getting Started Guide* or *Quick Setup Guide* for your controller platform.

### NOTE

While deploying vSZ, iSCSI must be used for block storage and make the hosts see everything as Direct-attached storage (DAS) for real-time database access/synchronisation as it requires lower latency and a high number of r/w transactions. Due to higher r/w latency, SAN and NAS might not be suitable for vSZ deployment.

You can deploy vSZ and vSZ-D via vCenter 6.7 on ESXi. Some of the new features (for example, location based services, rogue AP detection, force DHCP, and others) that this guide describes may not be visible on the controller web interface if the AP firmware deployed to the zone you are configuring is earlier than this release. To ensure that you can view and configure all new features that are available in this release, Ruckus recommends upgrading the AP firmware to the latest version.

## Logging On to the Web Interface

Before you can log on to the controller web interface, you must have the IP address that you assigned to the Management (Web) interface when you set up the controller on the network using the Setup Wizard.

Once you have this IP address, you can access the web interface on any computer that can reach the Management (Web) interface on the IP network.

Follow these steps to log on to the controller web interface.

1. On a computer that is on the same subnet as the Management (Web) interface, start a web browser.

Supported web browsers include:

- Google Chrome 47 and later (recommended)
- Safari 7 and later (Mac OS)

- Mozilla Firefox 44 and later
  - Internet Explorer 11 and later
  - Microsoft Edge
2. In the address bar, type the IP address that you assigned to the Management (Web) interface, and then append a colon and **8443** (the controller's management port number) at the end of the address.

For example, if the IP address that you assigned to the Management (Web) interface is **10.10.101.1**, then you should enter: **https://10.10.101.1:8443**

**NOTE**

The controller web interface requires an **HTTPS** connection. You must append https (not **http**) to the Management interface IP address to connect to the web interface. If a browser security warning appears, this is because the default SSL certificate (or security certificate) that the controller is using for HTTPS communication is signed by Ruckus and is not recognized by most web browsers.

The controller web interface logon page appears.

3. Log on to the controller web interface using the following logon details:
  - **User Name:** admin
  - **Password:** {the password that you set when you ran the Setup Wizard}
4. Click **Log On**.

The web interface refreshes, and then displays the **Dashboard**, which indicates that you have logged on successfully.

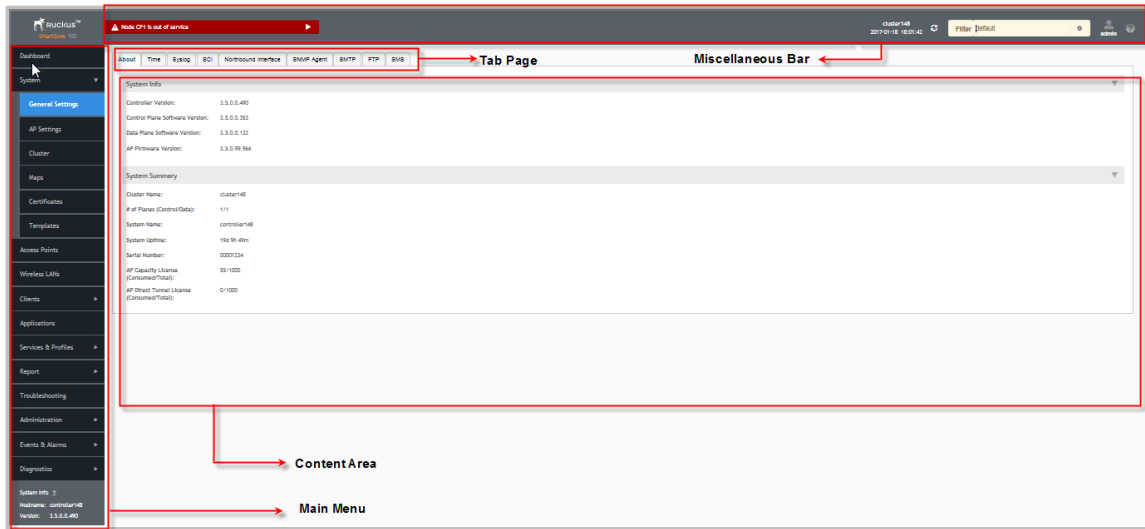
## Web Interface Features

The web interface is the primary graphical front end for the controller and is the primary interface

You can use it to:

- Manage access points and WLANs
- Create and manage users and roles
- Monitor wireless clients, managed devices, and rogue access points
- View alarms, events, and administrator activity
- Generate reports
- Perform administrative tasks, including backing up and restoring system configuration, upgrading the cluster, downloading support , performing system diagnostic tests, viewing the status of controller processes, and uploading additional licenses (among others)


**FIGURE 1** Controller Web Interface Features



The following table describes the web interface features.

**TABLE 2** Controller Web Interface Features

Feature	Description	Action
Main Menu	Lists the menus for administrative task.	Select the required menu and sub-menu.
Tab Page	Displays the options specific to the selected menu.	Select the required tab page.
Content Area	Displays tables, forms, and information specific to the selected menu and tab page.	View the tables, forms and information specific to the selected menu, sub-menu and tab page. Double-click an object or profile in a table, for example: a WLAN, to edit the settings.
Header Bar	Displays information specific to the web interface.	Select the required option (from left to right): <ul style="list-style-type: none"> <li>Warning—Lists the critical issues to be resolved.</li> <li>System Date and time—Displays the current system date and time.</li> <li>Refresh—Refreshes the web page.</li> <li>Global filter—Allows you to set the preferred system filter.</li> <li>My Account link—Allows you to:               <ul style="list-style-type: none"> <li>Change password</li> <li>Set session preference</li> <li>Log off</li> </ul> </li> <li>Online Help—Allows access to web help.</li> </ul>

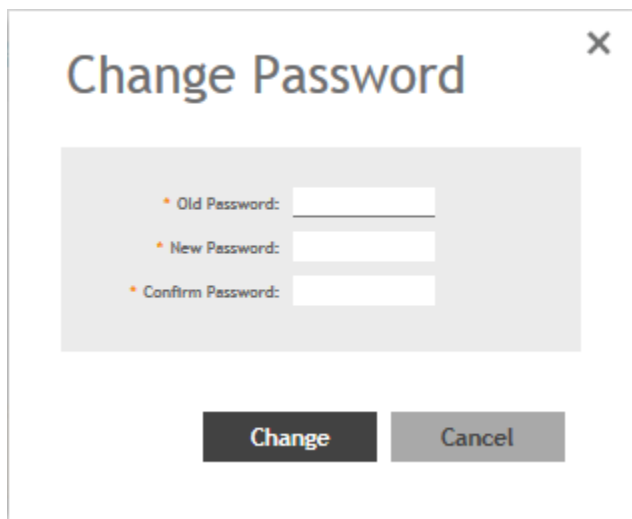
You can also use the  icon to expand and shrink the main menu. Shrinking the main menu increases the size of the content area for better readability and viewing.

## Changing the Administrator Password

Follow these steps to change the administrator password.

1. From the **Header** bar, click **admin** and select **Change Password**. The following window appears.

**FIGURE 2** Change Password Form

A screenshot of a web browser window titled "Change Password" with a close button (X) in the top right corner. The form contains three input fields, each preceded by an asterisk: "Old Password:", "New Password:", and "Confirm Password:". Below the input fields are two buttons: "Change" (dark grey) and "Cancel" (light grey).

2. Enter:
  - **Old Password**—Your current password.
  - **New Password**—Your new password.
  - **Confirm Password**—Your new password.
3. Click **Change**, your new password is updated.

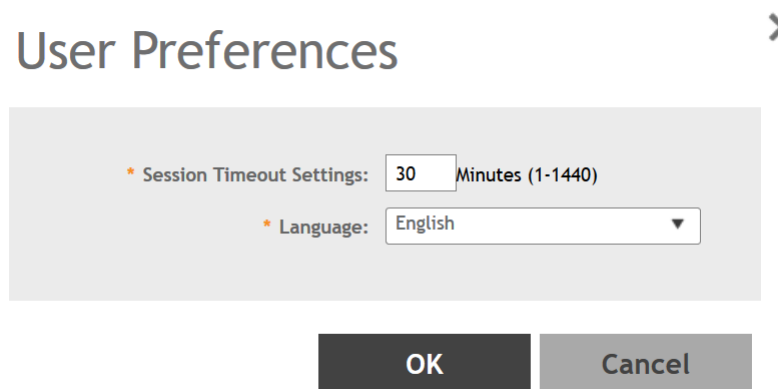
## Setting User Preferences

You can configure the language in which the user interface must appear, and also customize the session tie for the interface.

1. From the **Header** bar, click **admin**.
2. Select **Preferences** from the drop-down menu.  
The **User Preferences** page appears.
3. In Session Timeout Setting, enter the duration the web interface session must last for, in minutes.

4. In Language, select the language that you want to view the web interface in. The following languages are supported:
  - Spanish
  - Brazilian Portugese
  - French
  - German
  - Italian
  - Russian
  - Simplified Chinese
  - Traditional Chinese
  - Korean
  - Japanese

**FIGURE 3** User Preferences

A screenshot of the 'User Preferences' dialog box. The title 'User Preferences' is at the top right with a close button. The dialog contains two settings: '\* Session Timeout Settings:' with a text input '30' and 'Minutes (1-1440)', and '\* Language:' with a dropdown menu showing 'English'. At the bottom are 'OK' and 'Cancel' buttons.

User Preferences

\* Session Timeout Settings: 30 Minutes (1-1440)

\* Language: English ▼

OK Cancel

## Logging Off the Controller

You must be aware of how to log off the controller using the web interface and the CLI.

1. From the **Header** bar, click **admin** and select **Log off**.

The following message appears: Are you sure you want to log off?

2. Click **Yes**.

The controller logs you off the web interface and the logon page appears.

You have completed logging off the web interface.

You can also use CLI commands to shutdown the controller.

To shutdown the controller gracefully, use the following command: **shutdown** and specify the number of seconds before controller shutdowns.

To shutdown the controller immediately, use the following command: **shutdown now**. The controller will shutdown in 30 seconds.

## Configuring Global Filters

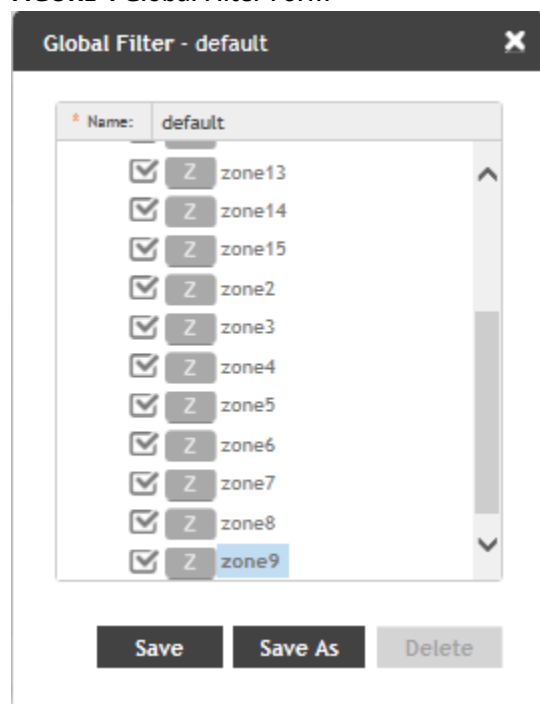
The Global filter setting allows you to set your preferred system filter.

Global filters allow the administrator to define a system scope or system context that applies to all pages of the system as they navigate to different menus. For example, if your system includes 5 zones, but you want to view Zone1 and Zone2 only, you can create and apply such a filter. As you navigate throughout the system, the view will be restricted to show only the data, objects, and profiles contained within Zones 1 and 2.

To set the global filter:

1. From the **Header** bar, click **Filter** setting . The below figure appears.

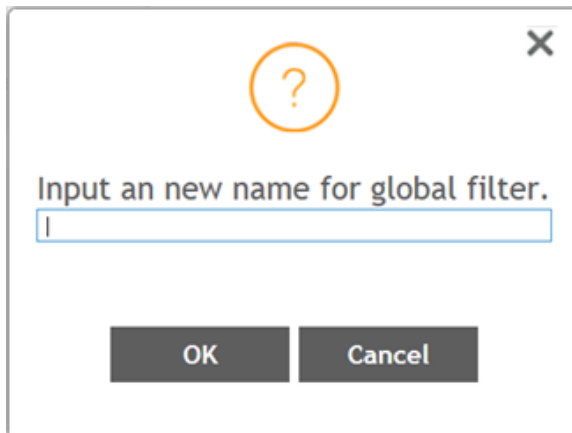
**FIGURE 4** Global Filter Form

A screenshot of the 'Global Filter - default' form. The form has a title bar with 'Global Filter - default' and a close button. Below the title bar, there is a field labeled '\* Name:' with the value 'default'. Below this is a list of zones, each with a checkbox and a 'Z' icon. The zones are: zone13, zone14, zone15, zone2, zone3, zone4, zone5, zone6, zone7, zone8, and zone9. All checkboxes are checked. At the bottom of the form are three buttons: 'Save', 'Save As', and 'Delete'.

2. Select or clear the required system filters and click
  - **Save**—To save the filter settings with the default group.
  - **Save As**—To save the filter settings as a new group. The below figure appears. Enter a new name for the group and click **OK**.



**FIGURE 5** New Name Form

A dialog box titled "New Name Form" with a close button (X) in the top right corner. Inside the dialog, there is a large orange circle with a question mark. Below this, the text "Input an new name for global filter." is displayed. Underneath the text is a text input field with a blue border and a cursor. At the bottom of the dialog are two buttons: "OK" and "Cancel".

**NOTE**

You can delete the filter setting. To do so, click the Filter  setting button. The Global Filter form appears, click **Delete**.

## Warnings and Notifications

This section explains about warnings and notifications.

### Warnings

Warnings are displayed in the Miscellaneous bar. They are issues which are critical in nature. Warnings cannot be removed or acknowledged unless the critical issue is resolved.

**FIGURE 6** Sample Warning Message



A list of warning messages that appear are as follows:

- Default 90-day support expiring soon
- System support expiring soon
- System support has expired
- Default 90-day AP license expiring soon
- Default AP license has expired
- Default 90-day RTU license expiring soon
- RTU has expired
- AP Certificate Expiration
- Node Out of Service
- Cluster Out of Service
- VM Resource Mismatch

- Suggested AP Limit Exceeded
- AP/DP version mismatch
- HDD Health Degradation

## Setting Global Notifications

Notifications are integrated with existing alarms and they are displayed only when a notification alarm exists and is not acknowledged by the administrator. Notifications can be viewed from the **Content** area. Administrators can acknowledge the notification by either:


- Clearing the alarm
- Acknowledging the Alarm

For more information, refer to the “Managing Alarms and Events” chapter.

Alarm severity are of three types:

- Minor
- Major
- Critical

The administrator can change the alarm severity shown on the dashboard. To do so:

1. From the Notifications area, Click the Setting  button. The Settings - Global Notification form appears.
2. From the **Lowest alarm severity** drop-down, select the required severity level.
3. Click **OK**. Notifications corresponding to the selected alarm severity and severity above it are displayed in the Notification area of the Dashboard.

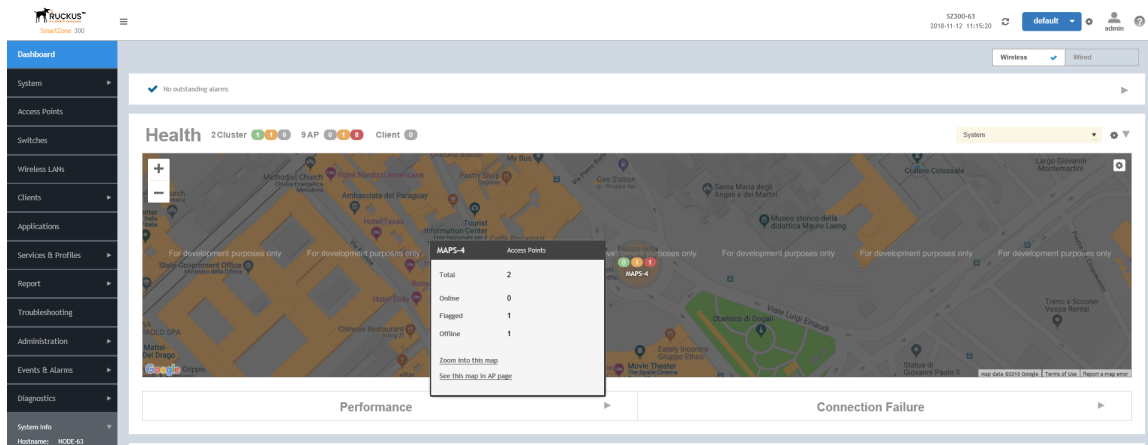
## Health and Maps

The Health dashboard gives you a very high-level overview of wireless devices such as cluster, AP and clients, and wired devices such as ICX switches. For wireless devices, it displays a world map view using Google Maps, which provides a global view of your SmartZone-controlled wireless network deployments.

You must click **Wireless** or **Wired** in the dashboard to view the respective devices.

The status bar at the top of the Health dashboard contains an iconic representation of the total Cluster, AP and Client counts for the entire system. This information can be filtered to display a single zone, AP group, or venue using the drop-down filter menu. You can also customize the dashboard layout and threshold settings using the Settings (gear) icon.

**FIGURE 7** Health Workspace area



The Wired devices section provides information about the health of the switch and the traffic it handles.

For more information on customizing the information displayed on the Health dashboard, see the “Customizing Health Status Thresholds” section.

## Understanding Cluster and AP Health Icons

The Health dashboard status bar displays the following Cluster and AP information using three colored icons to denote the number of APs/clusters currently in that state.

The icons for both Cluster and AP status overviews are represented by the following color coding scheme:

- 1 (Green): Online
- 3 (Orange): Flagged
- 3 (Red): Offline

Online and Offline status are self-explanatory. "Flagged" status is user-defined. You can customize the thresholds at which an AP or cluster enters "flagged" state using the **Settings** (gear) icon in the status bar. For more information, see [Customizing Health Status Thresholds](#) on page 23.

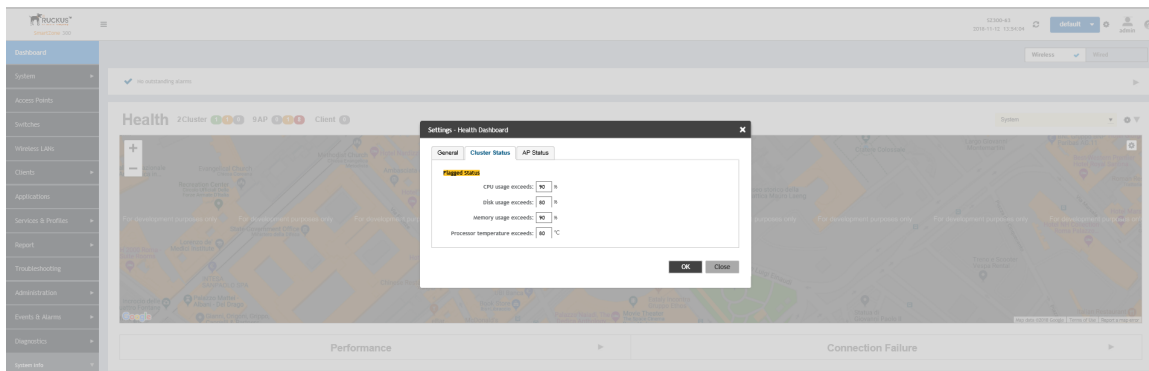
## Customizing Health Status Thresholds

You can customize the way SmartZone categorizes and displays clusters and APs shown in “Flagged Status” in the status bar.

To customize the Health dashboard, click the **Settings** (gear) icon. In the **Settings - Health Dashboard** form, click the **Cluster Status** or **AP Status** tab, and configure the following:

- Cluster Status:** Configure CPU, hard disk and memory usage percentages above which the cluster will be marked as flagged status.
- AP Status:** Configure the criteria upon which APs will be flagged. For more information, see the “Customizing AP Flagged Status Thresholds” section.

**FIGURE 8** Setting Cluster Health Status Thresholds



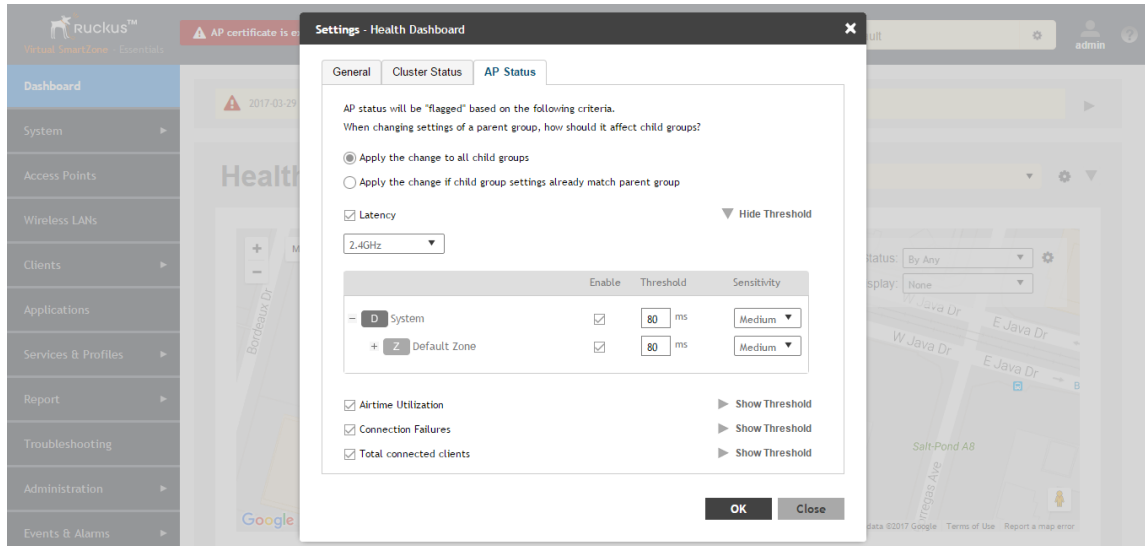
### Customizing AP Flagged Status Thresholds

Use the following procedure to customize when APs will be marked as "flagged" on the Health dashboard status bar.

1. Click the **Gear** icon on the **Health** dashboard.
2. The **Settings - Health Dashboard** form appears. Click the **AP Status** tab.
3. Select the behavior of flagging policies when applying changes to parent or child groups:
  - Apply the change to all child groups
  - Apply the change if child group settings already match the parent group
4. Configure thresholds above which APs will be marked as "flagged" for the following criteria:
  - Latency
  - Airtime Utilization
  - Connection Failures
  - Total connected clients
5. Configure the radio (2.4 / 5 GHz) from the drop-down menu and select the level (system, zone, AP group) at which you want to apply the policy, and configure the **Sensitivity** control for the threshold (Low, Medium, High). Setting the Sensitivity level to Low means that an AP must remain above the threshold for a longer period of time before it will appear in the flagged category, while a High sensitivity means that APs will more quickly alternate between flagged and non-flagged status.

- Click **OK** to save your changes.

**FIGURE 9** Configuring AP flagged status thresholds



## SCI Thresholds for each AP

The following are the thresholds from SCI for each AP.

The below thresholds provided is based on per AP model.

**TABLE 3** SCI Thresholds

Resource	Low Threshold	Normal Threshold Range	High Threshold Range
CPU	Less than 25%	Between 25% to 75%	Greater than 75%
Memory	Less than 2GB	Between 2GB to 8GB	Higher than 8GB
Hard Disk	Less than 50GB	Between 50GB to 100GB	Higher than 100GB

## Using the Health Dashboard Map

Use the Google Maps view just as you would normally use Google Maps - including zoom, satellite view, rotate and even street view icons. You can customize the AP icon information displayed on the map using the tools in the upper-right hand corner.

Use the **AP Status** pull-down menu to configure which AP health parameters will be displayed on the AP icons on the map. Use the Display menu to display the client count or radio channel in use.

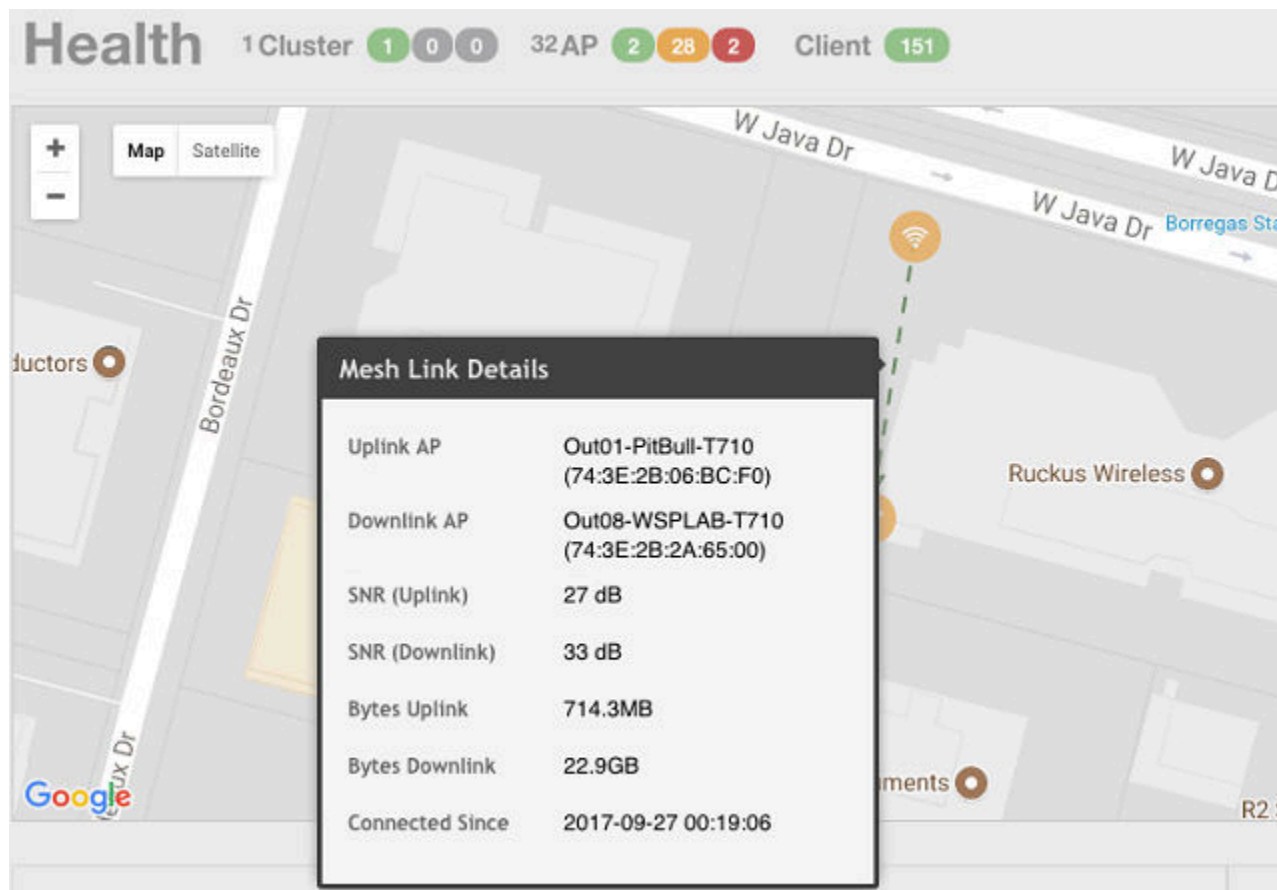
Use the **Settings** (gear) icon to configure the information displayed in tooltips when hovering over an AP on the map. You can also change the view mode altogether, from map view to Groups, Control Planes or Data Planes view mode using the settings menu. Additionally, you can also select the check-box to show mesh links. These links appear as dotted lines. If you hover over the mesh link on the map, a pop-up appears displaying more information such as the following:

- Uplink AP: displays the IP address of the uplink AP to which the wireless client sends data
- Downlink AP: displays the IP address of the downlink AP from which data is sent back to the wireless client
- SNR (Uplink): displays the signal-to-noise ratio in the uplink path
- SNR (Downlink): displays the signal-to-noise ratio in the downlink path

- Bytes (Uplink): displays the bytes of data transferred from the client to the uplink AP
- Bytes (Downlink): displays the bytes of data transferred from the downlink AP to the client
- Connected Since: displays the date and time when the mesh connection was established

*Bytes (Uplink)* and *Bytes (Downlink)* are aggregate counters for the mesh connection since the start of that mesh connection. If the mesh link is broken and restarts, the counter restarts. If the mesh AP connects to a different mesh root or uplink, the counter restarts.

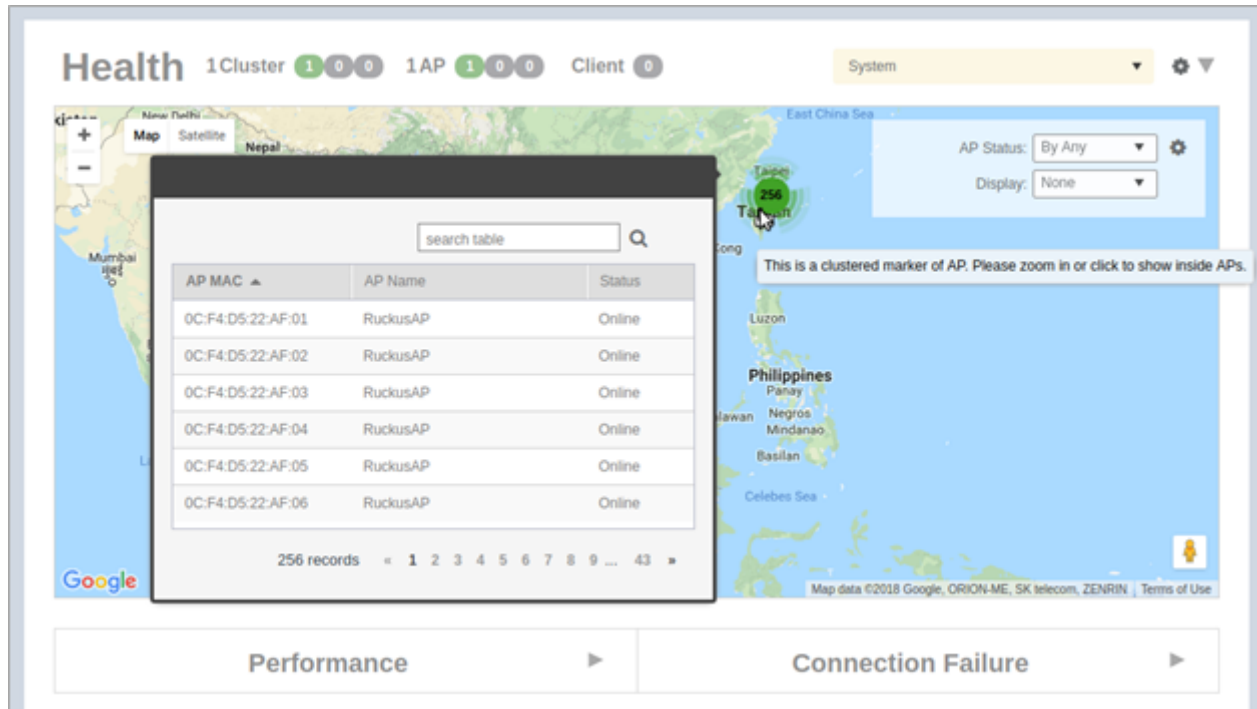
**FIGURE 10** Mesh Link Details



You can view and identify APs with the same GPS. If you hover over and click the clustered marker of AP on the map, a pop-up appears displaying more information such as the following:

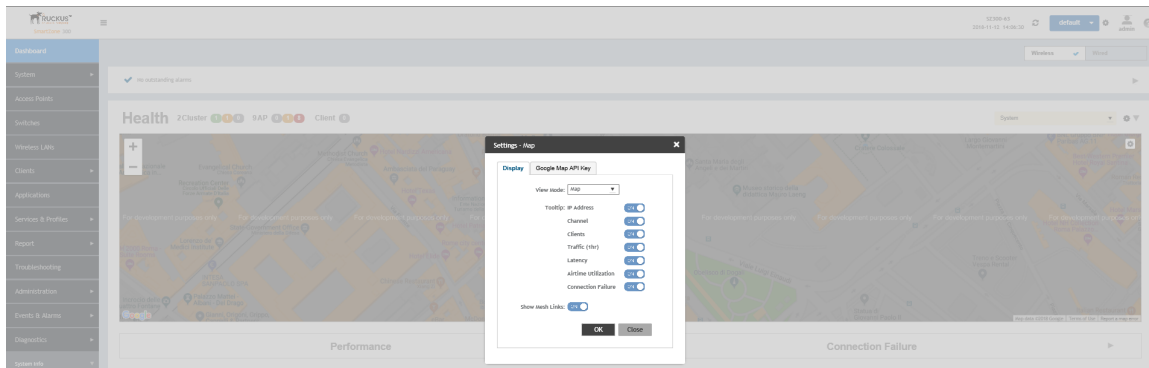
- AP MAC: Displays the MAC address of the AP
- AP Name: Displays the name assigned to the access point
- Status: Displays the status of the AP such as Online or Offline

**FIGURE 11** AP Details



You can also select the Google Map API key to use the Maps service with the application.

**FIGURE 12** Configuring map settings



## NOTE

In order for your venues to appear on the world map, you must first import a map of your site floorplan.

## Configuring the Google Map API Key Behavior

The Google Maps feature in the controller application works based on API interaction between the application and the Maps service hosted by Google. By default, these APIs are commonly available without the need for an API key but sometimes, you might have to generate a key.

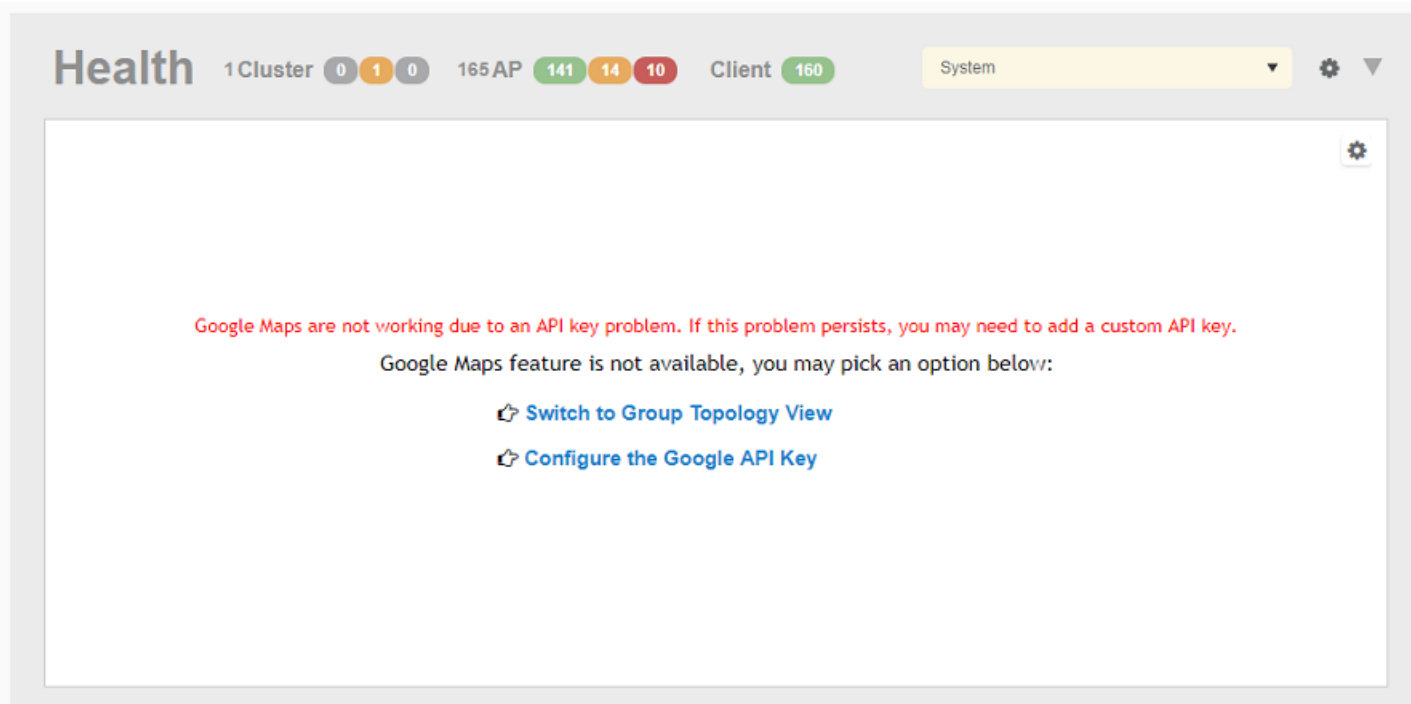
If Google Maps do not display properly in the absence of an API key, or when the API usage exceeds the daily limit, then an API key needs to be generated to ensure the map displays all the elements properly.

You would also have to generate an API key if you encounter errors such as

`MissingKeyMapError`  
or

`NoApiKeys`  
.

**FIGURE 13** Health dashboard view when API key is not available



Clicking **Configure the Google API Key** directs you to the **Google Map API Key** tab, where you can manage the Google Map API Key behavior.

All administrators of the system can use the same API key, or apply a unique API key per administrator. Allowing an API key per administrator enables more flexibility when API usage is high, or in circumstances when each tenant must use their own API key.

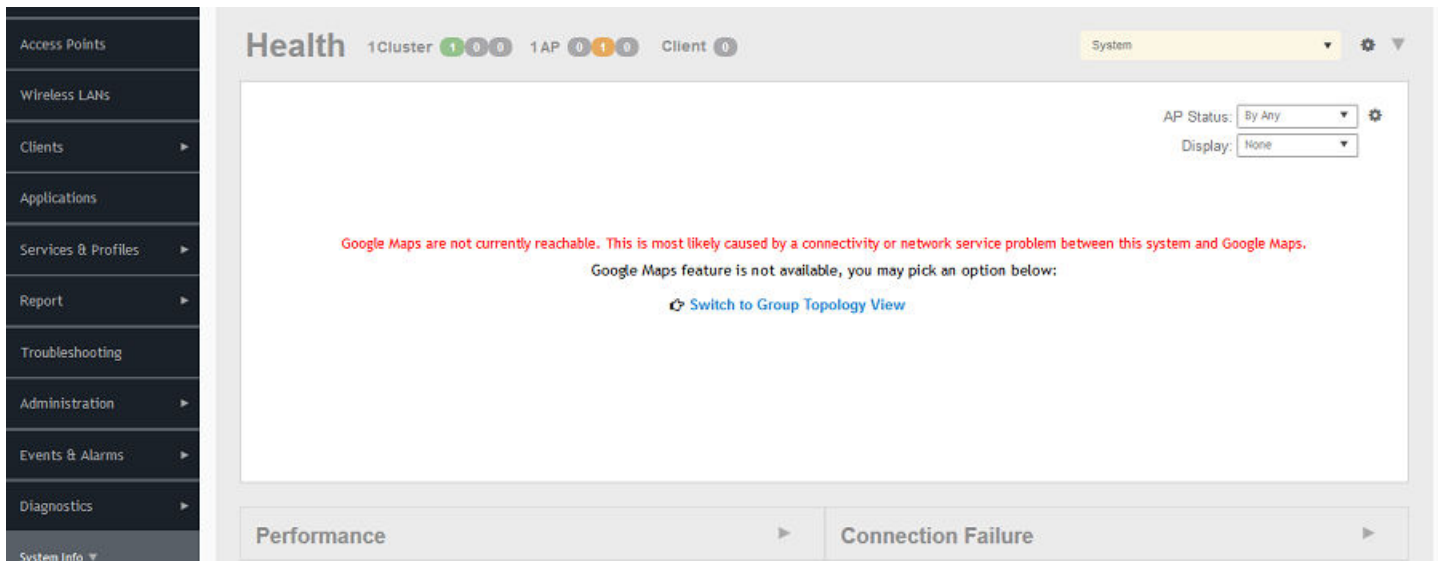
Follow these steps to configure the Google Map API Key behavior.

Launching the application displays the **Dashboard** menu, by default.

In **Health**, the map view appears if you are connected to a network. If you are not, then you might see the following screen and would have to view your network deployment as a topology diagram.

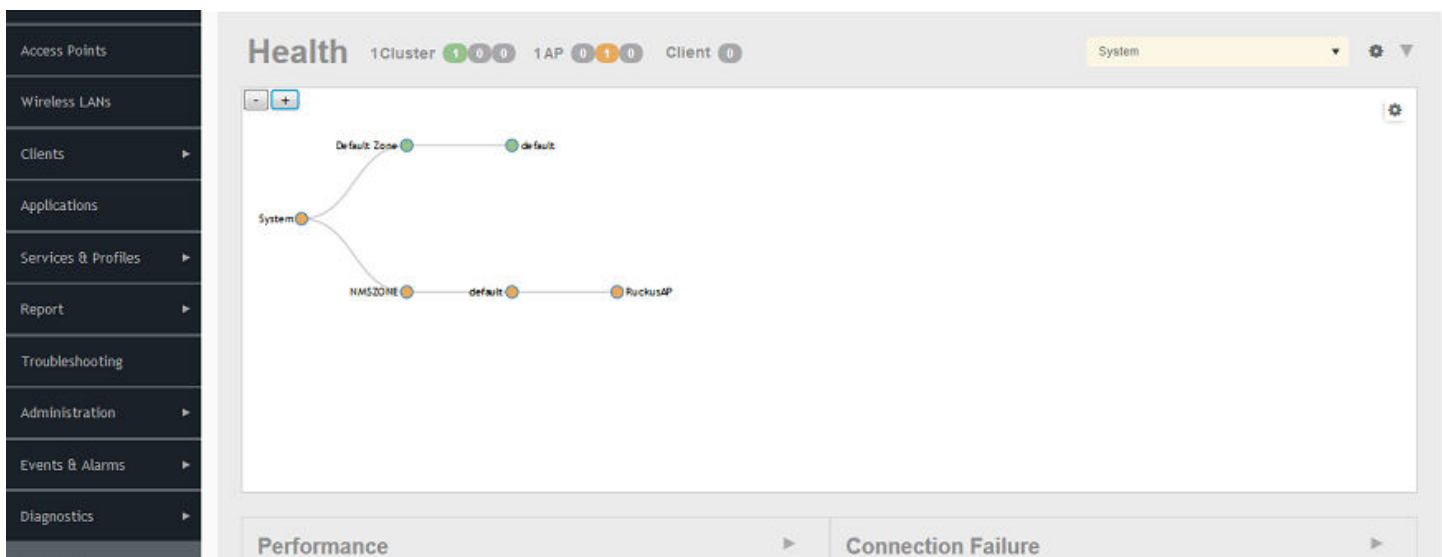


**FIGURE 14** No Map View



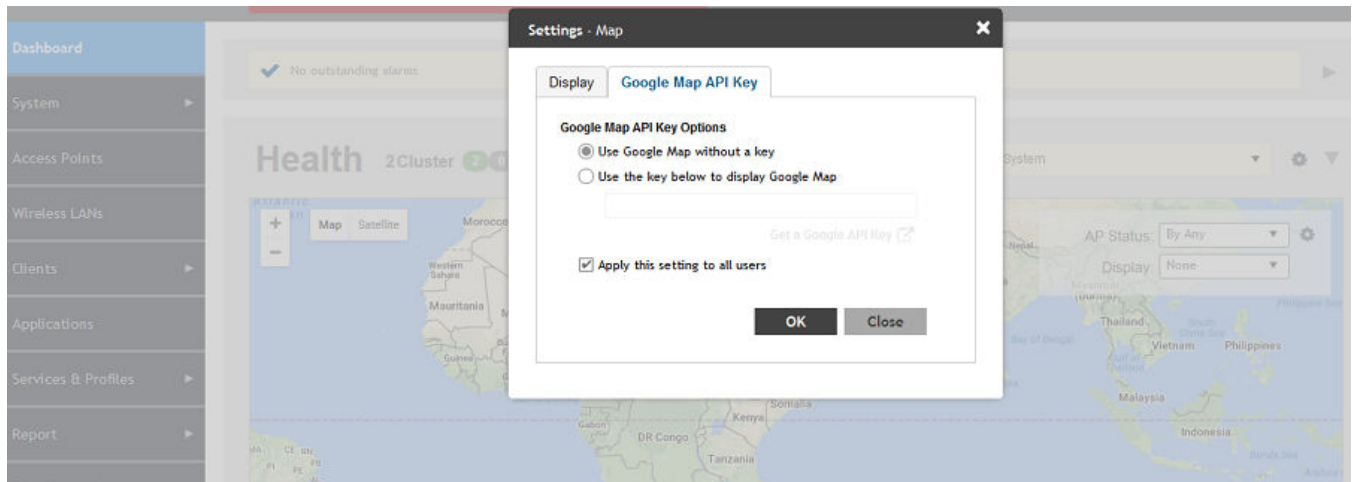
If you click the **Switch to Group Topology View**, a topology diagram similar to the following figure is displayed.

**FIGURE 15** Topology View



1. From the map view in **Health**, click the **Settings** (gear-shaped) icon.  
The **Settings-Map** page appears.

**FIGURE 16** Google Map API Key Options



From the **Display** tab, you can choose the mode in which you want to view your network deployment.

2. Click the **Google Map API Key** tab.
3. From the **Google Map API Key Options**, select one of the following:

Option	Description
Use Google Map without a key	Allows you to use the Google map feature without an API key.
Use the key below to display Google Map	Allows you to enter an API key which you already have to use the Google map feature. If you do not have a pre-existing API key, you can generate one by following the instructions in the <b>Get a Google API Key</b> link.

**NOTE**

The Google API Console is a platform on which you can build, test, and deploy applications. To use Google Maps API, you must register your application on the Google API Console and generate a Google API key which you can add to the application. For more information, see <https://developers.google.com/maps/documentation/javascript/tutorial>

If you already have a Google API Map Key, type the key to establish a connection with Google Maps.

4. Select **Apply this setting to all users** to apply the configuration settings to all users in the network deployment.
5. Click **OK**.

You have successfully configured the Google Map API Key options for your network deployment.

## Viewing AP Performance

Click the Performance tab to analyze the following parameters:

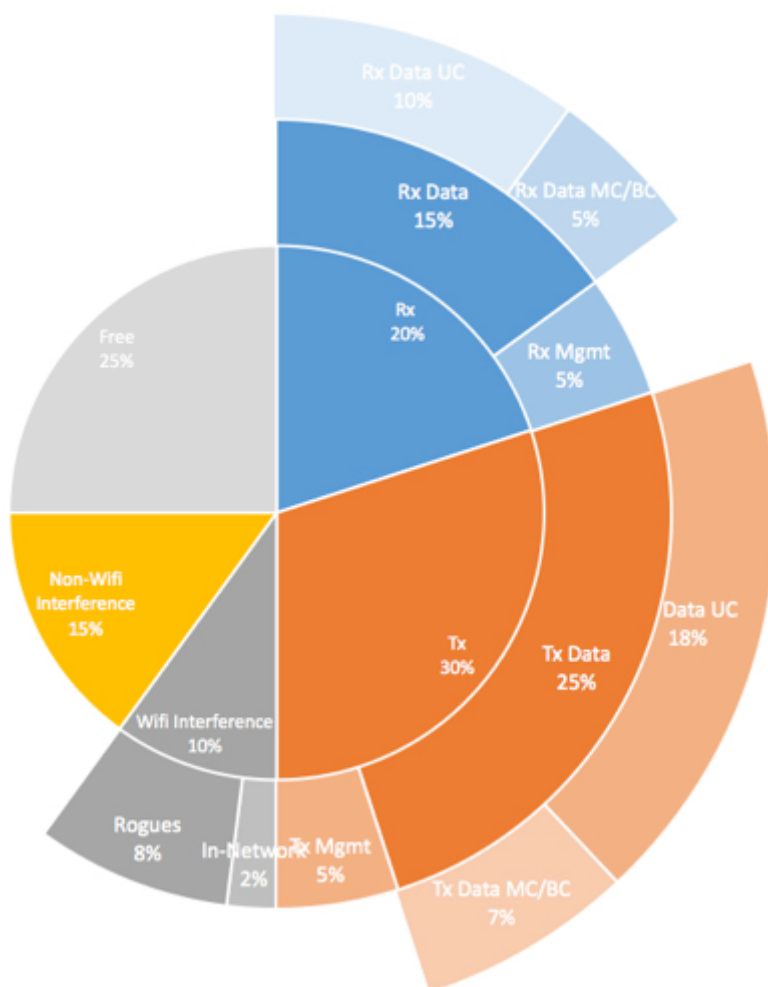
- Latency - Average time delay between an AP and connected clients.

- Airtime Utilization - Percent of airtime utilized, by radio. Clicking **Airtime Detail** displays a pie chart that depicts a detailed breakup of the reception and transmission percentages (Rx and Tx) against parameters such as Data, Management, Unicast, Multicast, Interference and Network Load. Following are the statistics that are evaluated:

**TABLE 4** Airtime Utilization Statistics

Total	Total Airtime under observation
RxLoad	Airtime spent in receiving frames destined to AP in Micro seconds
RxInt	Airtime spent in receiving frames NOT destined to AP in Micro seconds
TxSuccess	Airtime spent in transmitting frames successfully in Micro seconds
TxFailed	Airtime spent in transmit failed in Micro seconds
NonWifi	Airtime where CCA is busy in Micro seconds
RxTotal	Same as RxLoad or sum of Rx (Mgmt Unicast + Mgmt Bcast + Data Unicast + Data Bcast)
RxMgmtU	Airtime spent in receiving Management Unicast frames in Micro seconds
RxMgmtB	Airtime spent in receiving Management Broadcast frames in Micro seconds
RxDataU	Airtime spent in receiving Data Unicast frames in Micro seconds
RxDataB	Airtime spent in receiving Data Broadcast frames in Micro seconds
TxTotal	Same as TxSuccess or sum of Tx (Mgmt Unicast + Mgmt Bcast + Data Unicast + Data Bcast)
TxMgmtU	Airtime spent in transmitting Management Unicast frames in Micro seconds
TxMgmtB	Airtime spent in transmitting Management Broadcast frames in Micro seconds

**FIGURE 17** Sample Airtime Utilization Pie Chart



- Capacity - Measurement of potential data throughput based on the recent air-time efficiency and the performance potential of the AP and its currently connected clients.

You can view the parameters based on specific:

- Duration: 1 hour, 24 hours, 7 days, and 14 days
- Radio: 2.4 GHz, 5GHz

The parameters are displayed as Graphs and Bar Charts. When you hover over the graph you can view the Date and Time, Median, Likely Range, Min-Max Range of the parameters. To view specific information on the graph, click and drag the portion. The selected portion would zoom in. To restore to normal view, click the **Reset zoom** button.

To display specific information, click the settings button. The Settings - Performance window pops up. In **Show top**, enter the number of APs to be analysed and choose the AP identity display.

## Viewing AP Connection Failures

Click the Connection Failure tab to analyze the following parameters

- Total - Measurement of unsuccessful connectivity attempts by clients
- Authentication - Measurement of client connection attempts that failed at the 802.11 open authentication stage
- Association - Measurement of client connection attempts that failed at the 802.11 association stage
- EAP - Measurement of client connection attempts that failed during and EAP exchange
- RADIUS - Measurement of RADIUS exchanges that failed due to AAA client/server communication issues or errors
- DHCP - Measurement of failed IP address assignment to client devices

You can view the parameters based on specific:

- Duration: 1 hour, 24 hours, 7 days, and 14 days
- Radio: Total, 2.4 GHz, 5GH

The parameters are displayed as Graphs and Bar Charts. When you hover over the graph you can view the Date and Time, Median, Likely Range, Min-Max Range of the parameters. To view specific information on the graph, click and drag the portion. The selected portion would zoom in. To restore to normal view, click the **Reset zoom** button.

To display specific information, click the Settings button. The Settings - Performance window pops up. In **Show top**, enter the number of APs to be analysed and choose the AP identity display.

## Viewing Switches on the Dashboard

The wired dashboard displays detailed information about the health of the switch and graphs indicating traffic trends.

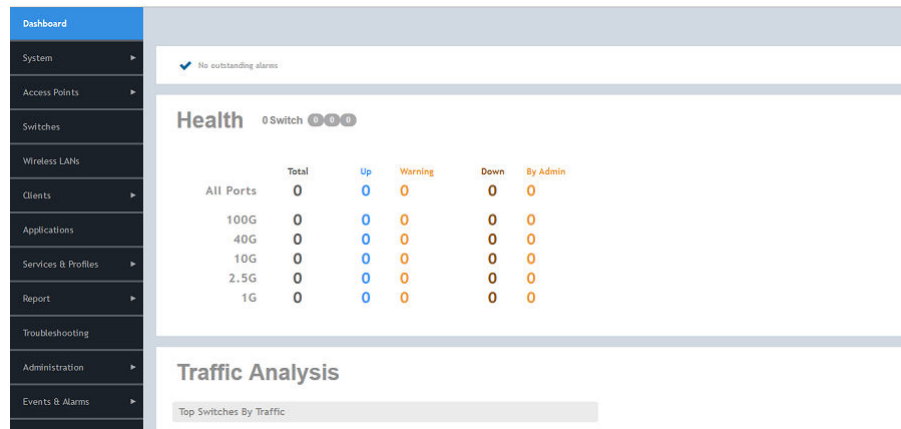
1. From the SmartZone interface, click **Dashboard** in the left menu.

The **Dashboard** page is displayed.

2. Click **Wired**.

The **Wired** page is displayed as shown in the following example.

**FIGURE 18** Wired Devices



The **Health** section displays the number of switches that are online, offline, and flagged. It also displays the number of ports by speed and indicates whether they are Up, Warning, Down, or Down By Admin.

The **Traffic Analysis** section displays the following information:

- Top switches based on traffic
- Top ports based on traffic
- Top switches based on port errors
- Top switches based on PoE utilization

## Traffic Analysis

You can analyze network traffic for APs, WLANs and clients.


From the traffic analysis tab, you can choose to analyze data using the following filters:

- **Channel Range**
  - Total
  - 2.4GHz
  - 5GHz
- **Throughput**
  - **TX+RX**—Number of bytes sent and received
  - **TX**—Number of bytes sent
  - **RX**—Number of bytes received
- **Group**

The parameters are displayed as Graphs and Bar Charts. When you hover over the graph you can view the Date and Time, Median, Likely Range, Min-Max Range of the parameters. To view specific information on the graph, click and drag the portion. The selected portion would zoom in. To restore to normal view, click the **Reset zoom** button.

## Customizing Traffic Analysis

You can customize the traffic analysis page to display specific traffic information.


1. From **Dashboard > Traffic Analysis**, click the settings  button. The Settings - Traffic Analysis form appears.
2. In the **Refresh every** drop-down, select the refresh interval.
3. Select the required check boxes from the following options:
  - **Traffic Trend**
  - **Client Trend**
  - **Access Points**
  - **WLANS**
  - **Clients**
4. Click **OK**. You have customized the traffic analysis page.

## Configuring Traffic Analysis Display for APs

Using traffic analysis you can measure the total volume of traffic sent or received by an Access Point (AP).

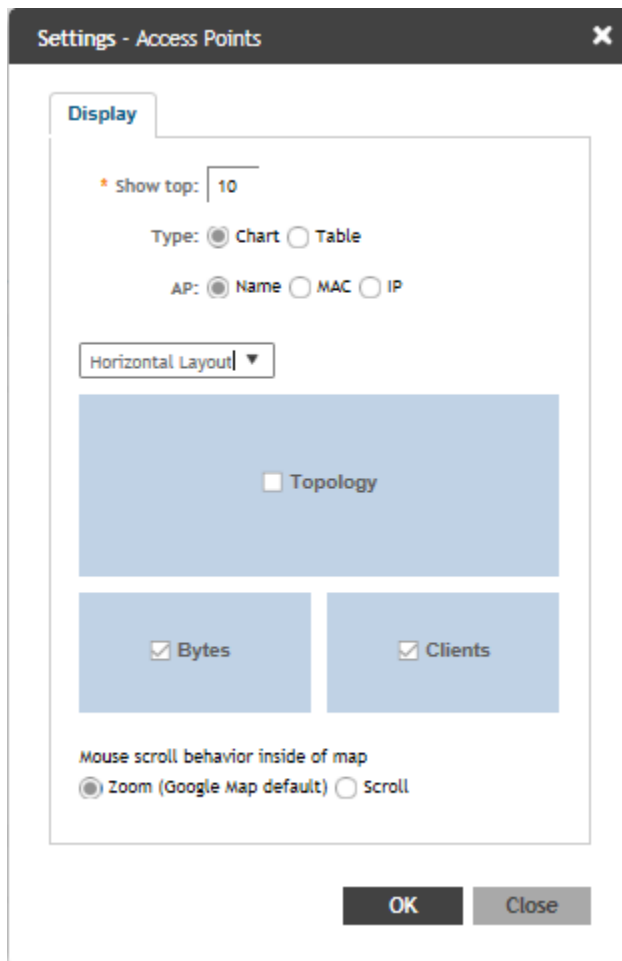
You can view historical and real-time data of the AP. Throughput and the number of clients connected to the AP are displayed in a bar chart. You can view the count of AP model details supported on the system in a pie chart. You must configure the AP settings to view its traffic analysis.

To configure the AP settings:

1. From the Access Points area, click settings .

The AP setting form displays.

**FIGURE 19** AP Settings Form



2. In the **Show top** box, enter the number of APs for which the traffic must be analyzed. Range: 5 through 20.
3. Select the **Type** radio button for the type of display you want to view. The choices are **Chart** or **Table**.
4. Select the **AP** identification option to be displayed. The choices are **Name**, **MAC**, or **IP**.
5. From the drop-down, select the required display layout. The choices are **Horizontal Layout** or **Vertical Layout**.
6. Select or clear the required options that must be displayed in the Content area.
  - a) **Topology**—To view the location map.
  - b) **Bytes**—To view the location map.
  - c) **Clients**—To view the location map.
  - d) **AP Models**—To view the location map.




7. Select the following mouse-scroll behavior when you point the mouse over a map.
  - a) **Zoom**
  - b) **Scroll**
8. Click **OK**.

## Configuring Traffic Analysis Display for WLANs

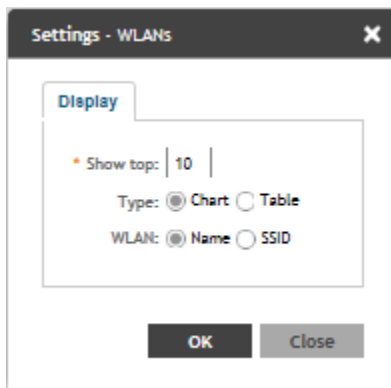
Using traffic analysis you can measure the total volume of traffic sent or received by WLANs.

You can view historical and real-time data of the WLANs. Throughput and the number of clients connected to the WLANs are displayed in a bar chart. You must configure the WLAN settings to view its traffic analysis.

To configure the WLAN settings:

1. From the WLAN area, click settings .
- The WLAN settings form displays.

**FIGURE 20** WLAN Settings Form



2. In the **Show top** box, enter the number of WLANs for which the traffic must be analyzed. Range: 5 through 20.
3. Select the **Type** radio button for the type of display you want to view. The choices are **Chart** or **Table**.
4. Select the **WLAN** identification option to be displayed. The choices are **Name** or **SSID**.
5. Click **OK**.


## Configuring Traffic Analysis Display for Top Clients

Using traffic analysis you can measure the total volume of traffic sent or received by clients.

Using traffic analysis you can measure the total volume of traffic sent or received by Clients. You must configure the Client settings to view the traffic analysis. You can view historical and real-time data of the Clients. The chart displays:

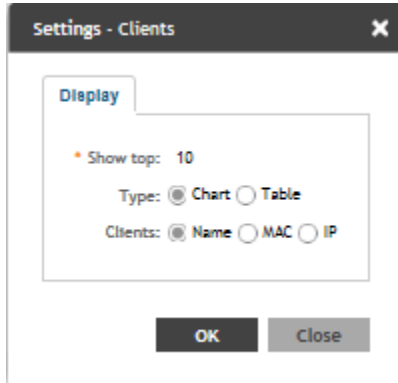
- Bytes—Frequency and number of clients connected to the AP
- OS Type—Types of OS the associated clients are using
- Application—Throughput the applications use

To configure the Client settings:

1. From the WLAN area, click settings .

The Client settings form displays.

**FIGURE 21** Client Setting Form



2. In the **Show top** box, enter the number of Clients for which the traffic must be analyzed. Range: 5 through 20.
3. Select the **Type** radio button for the type of display you want to view. The choices are **Chart** or **Table**.
4. Select the **WLAN** identification option to be displayed. The choices are **Name**, **MAC**, or **IP**.
5. Click **OK**.

## SmartCell Insight Report on Actual Traffic Rate for APs and Client

SmartZone (SZ) reports the total traffic statistics at an interval of every three minutes or 15 minutes to SmartCell Insight (SCI).

For traffic rate calculation, SCI divides the total traffic by time. But, this is not sufficient to accurately calculate airtime efficiency, as APs may not be sending or receiving the traffic all the time in the 15 minute interval. In other words, the SCI reporting of *traffic rate* needs to be across two dimensions:

1. **Traffic Over Time:** This is the current metric, and effectively captures how much traffic was sent or received over a period of time. The goal of this metric is to capture traffic, so that network operators can identify how much the network is being used in a time period.
2. **Traffic Efficiency:** This is the new metric, and effectively captures how much airtime was required to send receive traffic over time. The goal of this metric is to capture traffic efficiency, so that network operators can identify network performance in a time period.

To accomplish the efficiency calculation, information about both traffic and airtime usage (Tx,Rx, and busy), are measured as counters in a reporting interval. For SCI to do this, SZ will send the following information to SCI at the AP level.

- **Total traffic** Uplink and downlink time
- **Total Tx Time:** How much time did the AP spend transmitting traffic
- **Total Rx Time:** How much time did the AP spend receiving traffic for the AP's basic service set identifier (BSSIDs)
- **Other Rx Time:** How much time did the AP spend receiving broadcast traffic and traffic for other BSSIDs

**NOTE**

The reason for this metric is to distinguish between AP traffic and environmental traffic, where environmental traffic does affect airtime availability, but is not incorporated into the traffic efficiency calculation.

- **Total Tx/Rx Time:** How much time did the AP spend receiving and sending traffic in total for its BSSIDs
- **Idle Time:** How much time did the AP spend idle

SZ will send the following information to SCI at the Client level.

- **Total traffic** Uplink and downlink time
- **Total Tx Time:** How much time did the client spend transmitting traffic
- **Total Rx Time:** How much time did the client spend receiving traffic for the AP's basic service set identifier (BSSIDs)
- **Total Tx/Rx Time:** How much time did the client spend receiving and sending traffic in total for its BSSIDs



# Configuring General Settings

---

• Viewing System Settings.....	41
• Configuring System Time.....	43
• Configuring the Remote Syslog Server.....	43
• Configuring Northbound Data Streaming Settings.....	45
• Setting the Northbound Portal Password.....	46
• Enabling Global SNMP Notifications.....	46
• Configuring SMTP Server Settings.....	48
• Configuring FTP Server Settings.....	49
• Configuring the SMS Gateway Server.....	50
• Location Service.....	50
• Working with Maps.....	52

## Viewing System Settings

You can view the system information such as the controller version, firmware version, license information, control and data plane details from the **General Settings** tab.

To view the system settings, from the left pane, select **System > General Settings > About**. The following system information is displayed:

- Controller Version
- Control Plane Software Version
- Data Plane Software Version
- AP Firmware Version (hover over the field to see the firmware type)
- Cluster Name
- Number of Planes
- System Name
- System Uptime
- Serial Number
- System Capacity of Cluster
- AP Capacity License
- AP Direct Tunnel License
- Data Plane Capacity License

FIGURE 22 General Settings - SZ300

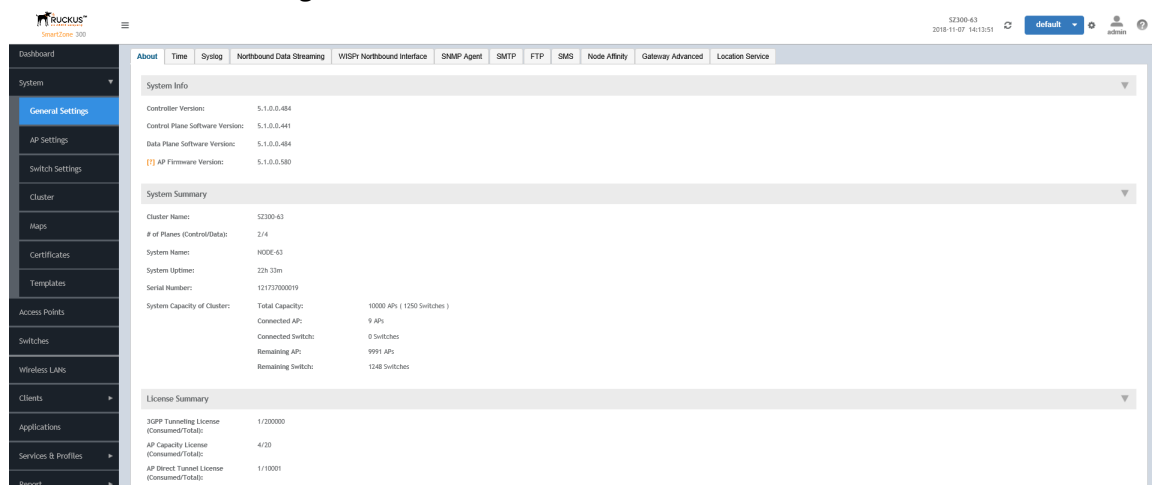
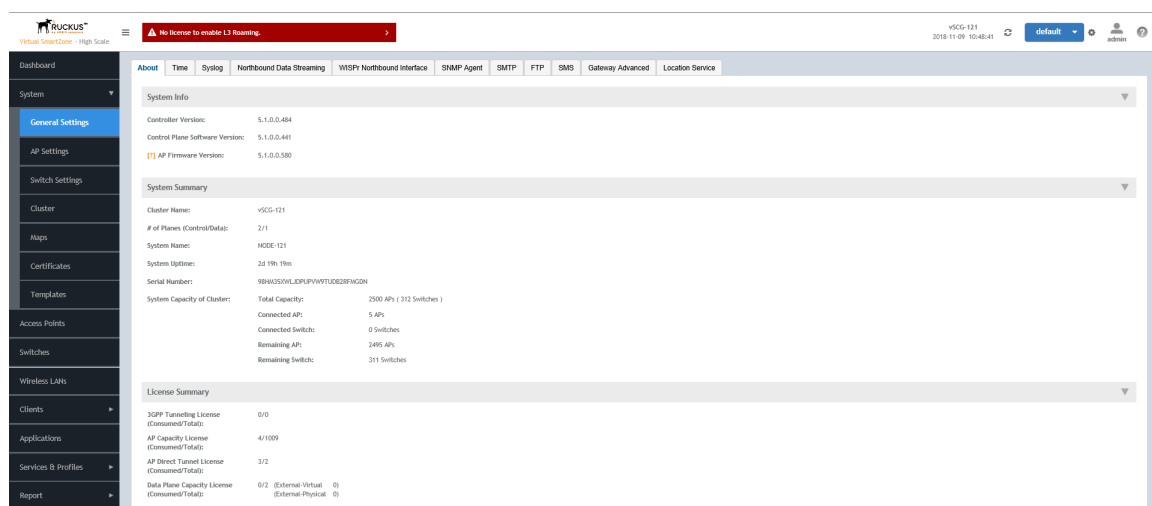


FIGURE 23 General Settings - vSZ-H



AP image signing involves digitally signing the Ruckus header and body of the AP firmware, and authenticating the firmware as valid to be installed on the AP. AP firmware images are available in the following types:

- **USI:** Un-Signed Images which do not have the capability to sign and verify. It only contains a Header and Body. The Body usually contains both the kernel and file system information.
- **IUI:** Intermediate Signed Image which has the capability to sign and verify, and it allows installation of both signed and unsigned images.
- **FSI:** Fully Signed Image which only allow Ruckus-signed firmware to be installed on the AP. It does not allow installation of unsigned or tampered images.

AP image signing is a two step upgrade or downgrade procedure where in the AP firmware can be upgraded from type USI to ISI, ISI to FSI and vice-versa in the same order.

### NOTE

You cannot upgrade an image from USI to FSI as the formats of these images are different. Attempting such an upgrade triggers an **AP image signing failed** event.

## Configuring System Time

The controller uses an external network time protocol (NTP) server to synchronize the times across cluster nodes and managed access points.

To edit the system time:

1. Go to **System > General Settings > Time**.
2. Enter the **NTP Server** address that you want to use. The default NTP server address is **ntp.ruckuswireless.com**.
3. Click **Sync Server** to enable an AP to join the controller and automatically synchronize its time every day.
4. Select the **System Time Zone**, from the drop-down that you want the controller to use. The default time zone is (GMT +0:00) UTC.
5. Click **OK**.

## Configuring the Remote Syslog Server

The controller maintains an internal log file of current events and alarms, but this internal log file has a fixed capacity. Configure the log settings so you can keep copies of the logs that the controller generates.

At a certain point, the controller will start deleting the oldest entries in log file to make room for newer entries. If you want to keep a permanent record of all alarms and events that the controller generated, you can configure the controller to send the log contents to a syslog server on the network.

Follow these steps to configure the remote syslog server:

1. Go to **System > General Settings > Syslog**.
2. Select the **Enable logging to remote syslog server** check box.
3. Configure the settings as explained in the following table.
4. Click **OK**.

**TABLE 5** Syslog Server Configuration Settings

Field	Description	Your Action
<b>Primary Syslog Server Address</b>	Indicates the syslog server on the network.	<ol style="list-style-type: none"> <li>Enter the server address.</li> <li>Enter the <b>Port number</b>.</li> <li>Choose the <b>Protocol type</b>.</li> <li>Click <b>Ping Syslog Server</b>. If the syslog server is reachable, a flashing green circle and the message <b>Success</b> appears after the button.</li> </ol>
<b>Secondary Syslog Server Address</b>	Indicates the backup syslog server on the network, if any, in case the primary syslog server is unavailable.	<ol style="list-style-type: none"> <li>Enter the server address.</li> <li>Enter the <b>Port number</b>.</li> <li>Choose the <b>Protocol type</b>.</li> <li>Click <b>Ping Syslog Server</b>. If the syslog server is reachable, a flashing green circle and the message <b>Success</b> appears after the button.</li> </ol>
<b>Application Logs Facility</b>	Indicates the facility for application logs.	<ol style="list-style-type: none"> <li>Select the option from the drop-down. Range: 0 through 7.</li> </ol>

**TABLE 5 Syslog Server Configuration Settings (continued)**

Field	Description	Your Action
		b. Select one of the following <b>Filter Severity</b> : 1. <b>Emerg</b> 2. <b>Alert</b> 3. <b>Crit</b> 4. <b>Error</b> 5. <b>Warning</b> 6. <b>Notice</b> 7. <b>Info</b> 8. <b>Debug</b> : Default option
<b>Administrator Activity Logs Facility</b>	Indicates the facility for administrator logs.	a. Select the option from the drop-down. Range: 0 through 7. b. Select one of the following <b>Filter Severity</b> : 1. <b>Emerg</b> 2. <b>Alert</b> 3. <b>Crit</b> 4. <b>Error</b> 5. <b>Warning</b> 6. <b>Notice</b> 7. <b>Info</b> 8. <b>Debug</b> : Default option
<b>Other Logs Filter Severity</b>	Indicates the facility for comprehensive logs.	Select one of the following <b>Filter Severity</b> : a. <b>Emerg</b> b. <b>Alert</b> c. <b>Crit</b> d. <b>Error</b> e. <b>Warning</b> f. <b>Notice</b> g. <b>Info</b> h. <b>Debug</b> : Default option
<b>Event Facility</b>	Indicates the facility for event logs.	Select the option from the drop-down. Range: 0 through 7.
<b>Event Filter</b>	Indicates the type of event that must be sent to the syslog server.	Choose the required option: <ul style="list-style-type: none"> <li>• <b>All events</b> — Send all controller events to the syslog server.</li> <li>• <b>All events except client association / disassociation events</b> — Send all controller events (except client association and disassociation events) to the syslog server.</li> <li>• <b>All events above a severity</b> — Send all controller events that are above the event severity to the syslog server.</li> </ul>
<b>Event Filter Severity</b> applies to <b>Event Filter &gt; All events above a severity</b>	Indicates the lowest severity level. Events above this severity level will be sent to the syslog server.	Select the option from the drop-down. a. <b>Critical</b> b. <b>Major</b>



**TABLE 5 Syslog Server Configuration Settings (continued)**

Field	Description	Your Action
		c. <b>Minor</b> d. <b>Warning</b> e. <b>Informational</b> f. <b>Debug</b> : Default option
<b>Priority</b>	Indicates the event severity to syslog priority mapping in the controller.	Choose the <b>Syslog Priority</b> among <b>Error</b> , <b>Warning</b> , <b>Info</b> and <b>Debug</b> , for the following event severities: <ul style="list-style-type: none"> <li>• <b>Critical</b></li> <li>• <b>Major</b></li> <li>• <b>Minor</b></li> <li>• <b>Warning</b></li> <li>• <b>Informational</b></li> <li>• <b>Debug</b></li> </ul>

## Configuring Northbound Data Streaming Settings

SmartCell Insight and other third-party GPB listeners use data from the controller to analyze performance and generate reports about the WiFi network. Configuring the Northbound Data Streaming settings in the controller enables data transfer from the controller to the Northbound Data Streaming server using the MQTT protocol.

Follow these steps to configure the Northbound Data Streaming server settings:

1. Go to **System > General Settings > Northbound Data Streaming**.
2. Select the **Enable Northbound Data Streaming** check-box to configure the Northbound Data Streaming server settings.
3. Click **Create**, the Create Northbound Data Streaming Profile form appears.

Enter the following details:

- Name—Profile name.
- Server Host—IP address to the Northbound Data Streaming host server.
- Server Port—Port number over which the Northbound Data Streaming server and controller can communicate and transfer data.
- User—Name for the user.
- Password—password for the respective user.
- System ID—ID of the Northbound Data Streaming system that should be accessed.

4. Click **OK**.
5. Select **All** or **Stream GPB data by Domain/Zone**.

Selecting **All** sends all the KPIs or stats for all zones or domains to SCI or other third-party GPB listeners.

Selecting **Stream GPB data by Domain/Zone** allows you to set any one of the nodes (Domain or Zone), and the AP message of that node is bypassed.

6. From **Settings**, select the domain or zone and enable **Stream GPB data in this node**. This will selectively send KPIs or stats for certain zones or domains to SCL or other third-party GPB listeners.

**NOTE**

You can also edit or delete an Northbound Data Streaming profile. To do so, select the Northbound Data Streaming profile from the list and click **Configure** or **Delete** as required.

## Setting the Northbound Portal Password

Third-party applications use the northbound portal interface to authenticate users and to retrieve user information during the UE association.

Follow these steps to configure the northbound portal interface:

1. Go to **System > General Settings > Northbound Interface**.
2. Select **Enable Northbound Interface Support**, and enter the **User Name** and **Password**.
3. Click **OK**.

## Enabling Global SNMP Notifications

The controller supports the Simple Network Management Protocol (SNMP v2 and v3), which allows you to query controller information, such as system status, AP list, etc., and to set a number of system settings using a Network Management System (NMS) or SNMP MIB browser.

You can also enable SNMP traps to receive immediate notifications for possible AP and system issues.

The procedure for enabling the internal SNMP agents depends on whether your network is using SNMPv2 or SNMPv3. SNMPv3 mainly provides security enhancements over the earlier version, and therefore requires you to enter authorization passwords and encryption settings, instead of simple clear text community strings.

Both SNMPv2 and SNMPv3 can be enabled at the same time. The SNMPv3 framework provides backward compatibility for SNMPv1 and SNMPv2c management applications so that existing management applications can still be used to manage the controller with SNMPv3 enabled.

## Configuring SNMP v2 Agent

To configure SNMP v2 Agent settings:

1. Go to **System > General Settings > SNMP Agent**.
2. Select the **Enable SNMP Notifications Globally** check box to send out notification messages.
3. To configure the SNMPv2 Agent, click **Create** and update the details as explained in the following table.

**TABLE 6** SNMP v2 Agent Settings

Field	Description	Your Action
<b>Community</b>	Indicates that applications which send SNMP Get-Requests to the controller (to retrieve information) will need to send this string along with the request before they will be allowed access.	Enter a name.

**TABLE 6 SNMP v2 Agent Settings (continued)**

Field	Description	Your Action
<b>Privilege</b>	Indicates the privileges granted to this community.	<p>Select the required privileges:</p> <ul style="list-style-type: none"> <li>• <b>Read</b>—Privilege only to read.</li> <li>• <b>Write</b>—Privilege only to read and write.</li> <li>• <b>Notification</b>—Privilege to: <ul style="list-style-type: none"> <li>– <b>Trap</b>—Choose this option to send SNMP trap notification.</li> <li>– <b>Inform</b>—Choose this option to send SNMP notification. <ul style="list-style-type: none"> <li>a. Enter the <b>Target IP</b> address.</li> <li>b. Enter the <b>Target Port</b> number.</li> <li>c. Click <b>Add</b>.</li> </ul> </li> </ul> </li> </ul>

**NOTE**

You can also edit or delete an SNMPv2 agent. To do so, select the SNMPv2 agent from the list and click **Configure** or **Delete** respectively.

4. Click **OK**.

## Configuring SNMP v3 Agent

1. Go to **System > General Settings > SNMP Agent**.
2. Select the **Enable SNMP Notifications Globally** check box to send out notification messages.
3. To configure the SNMPv3 Agent, click **Create** and update the details as explained in the following table.

**TABLE 7 SNMPv3 Agent Settings**

Field	Description	Your Action
<b>Community</b>	Indicates that applications which send SNMP Get-Requests to the controller (to retrieve information) will need to send this string along with the request before they will be allowed access.	Enter a name.
<b>Authentication</b>	Indicates the authentication method.	<p>Choose the required option:</p> <ul style="list-style-type: none"> <li>• <b>None</b>—Use no authentication.</li> <li>• <b>SHA</b>—Secure Hash Algorithm, message hash function with 160-bit output. <ul style="list-style-type: none"> <li>a. Enter the <b>Auth Pass Phrase</b>.</li> <li>b. Choose the <b>Privacy</b> option. <ul style="list-style-type: none"> <li>– <b>None</b>: Use no privacy method.</li> <li>– <b>DES</b>: Data Encryption Standard, data block cipher.</li> <li>– <b>AES</b>: Advanced Encryption Standard, data block cipher.</li> </ul> </li> <li>c. Enter a <b>Privacy Phrase</b>, 8 through 32 characters.</li> </ul> </li> </ul>

**TABLE 7 SNMPv3 Agent Settings (continued)**

Field	Description	Your Action
		<ul style="list-style-type: none"> <li>• <b>MD5</b>—Message-Digest algorithm 5, message hash function with 128-bit output. <ul style="list-style-type: none"> <li>a. Enter the <b>Auth Pass Phrase</b>.</li> <li>b. Choose the <b>Privacy</b> option. <ul style="list-style-type: none"> <li>– <b>None</b>: Use no privacy method.</li> <li>– <b>DES</b>: Data Encryption Standard, data block cipher.</li> <li>– <b>AES</b>: Advanced Encryption Standard, data block cipher.</li> </ul> </li> <li>c. Enter a <b>Privacy Phrase</b>, 8 through 32 characters.</li> </ul> </li> </ul>
<b>Privilege</b>	Indicates the privileges granted to this community.	<p>Select the required privileges:</p> <ul style="list-style-type: none"> <li>• <b>Read</b>—Privilege only to read.</li> <li>• <b>Write</b>—Privilege only to read and write.</li> <li>• <b>Notification</b>—Privilege to: <ul style="list-style-type: none"> <li>– <b>Trap</b>—Choose this option to send SNMP trap notification.</li> <li>– <b>Inform</b>—Choose this option to send SNMP notification.</li> </ul> </li> </ul> <ul style="list-style-type: none"> <li>a. Enter the <b>Target IP</b> address.</li> <li>b. Enter the <b>Target Port</b> number.</li> <li>c. Click <b>Add</b>.</li> </ul>

**NOTE**

You can also edit or delete an SNMPv3 agent. To do so, select the SNMPv3 agent from the list and click **Configure** or **Delete** respectively.

4. Click **OK**.

## Configuring SMTP Server Settings

If you want to receive copies of the reports that the controller generates or to email guest passes to users, you need to configure the SMTP server settings and the email address from which the controller will send the reports.

Follow these steps to configure the SMTP server settings:

1. Go to **System > General Settings > SMTP**.
2. Select **Enable SMTP Server**.
3. Enter the **Logon Name** or user name provided by your ISP or mail administrator. This might be just the part of your email address before the @ symbol, or it might be your complete email address. If you are using a free email service (such as Hotmail™ or Gmail™), you typically have to type your complete email address.
4. Enter the associated **Password**.
5. For **SMTP Server Host**, enter the full name of the server provided by your ISP or mail administrator. Typically, the SMTP server name is in the format **smtp.company.com**.

6. For **SMTP Server Port**, enter the SMTP port number provided by your ISP or mail administrator. Often, the SMTP port number is **25** or **587**. The default SMTP port value is **25**.
7. For **Mail From**, enter the source email address from which the controller sends email notifications.
8. For **Mail To**, enter the recipient email address to which the controller sends alarm messages. You can send alarm messages to a single email address.
9. Select the **Encryption Options**, if your mail server uses encryption.
  - **TLS**
  - **STARTTLS**Check with your ISP or mail administrator for the correct encryption settings that you need to set.
10. Click **Test**, to verify if the SMTP server settings are correct. The test completed successfully form appears, click **OK**.
11. Click **OK**.

## Configuring FTP Server Settings

The controller enables you to automatically back up statistics files, reports, and system configuration backups to an external FTP server.

However, before you can do this, you must add at least one FTP server to the controller.

Follow these steps to add an FTP server to which the controller will export data automatically:

1. Go to **System > General Settings > FTP**.
2. Click **Create**, the Create FTP Server form appears.
3. Enter an **FTP Name** that you want to assign to the FTP server that you are adding.
4. Select the required **Protocol**; **FTP** or **SFTP** (Secure FTP) protocol.
5. Enter the **FTP Host**, IP address of the FTP server.
6. Enter the **FTP Port**, number. The default FTP port number is 21.
7. Enter a **User Name** for the FTP account that you want to use.
8. Enter a **Password** that is associated with the FTP user name.
9. For **Remote Directory**, enter the remote FTP server path to which data will be exported from the controller. The path must start with a forward slash (/)
10. To verify that the FTP server settings and logon information are correct, click **Test**. If the server and logon settings are correct, a confirmation message stating, "**FTP server connection established successfully**" appears.
11. Click **OK**.

### NOTE

You can edit or delete an existing FTP setting. To do so, select the FTP setting from the list and click **Configure** or **Delete** respectively.

# Configuring the SMS Gateway Server

You can define the external gateway services used to distribute guest pass credentials to guests.

To configure an external SMS gateway for the controller:

1. Go to **System > General Settings > SMS**.
2. Select the **Enable Twilio SMS Server** check box to use an existing Twilio account for SMS delivery.
3. Enter the following Twilio Account Information:
  - **Server Name**, type the name of the server.
  - **Account SID**, type the account number.
  - **Auth Token**, type the token number to authenticate the external SMS gateway.
  - **From**, type the phone number from which the message must be sent.
4. Click **OK**.

You have completed adding an SMS gateway to the controller. You will receive a guest pass key from your Twilio Trial account.

## Location Service

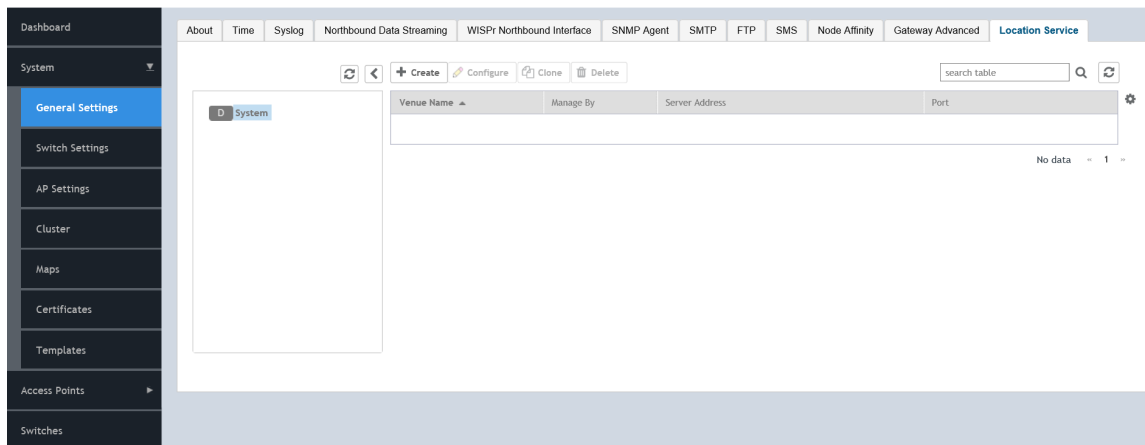
If your organization purchased the Ruckus Smart Positioning Technology (SPoT) location service, the controller must be configured with the venue information that is displayed in the SPoT Administration Portal.

After completing purchase of the SPoT location service, you will be given account login information that you can use to log into the SPoT Administration Portal. The Admin Portal provides tools for configuring and managing all of your venues (the physical locations in which SPoT service is deployed). After a venue is successfully set up, you will need to enter the same venue information in the controller.

1. Select **System > General Settings > Location Service**.

The **Location Service** page appears.

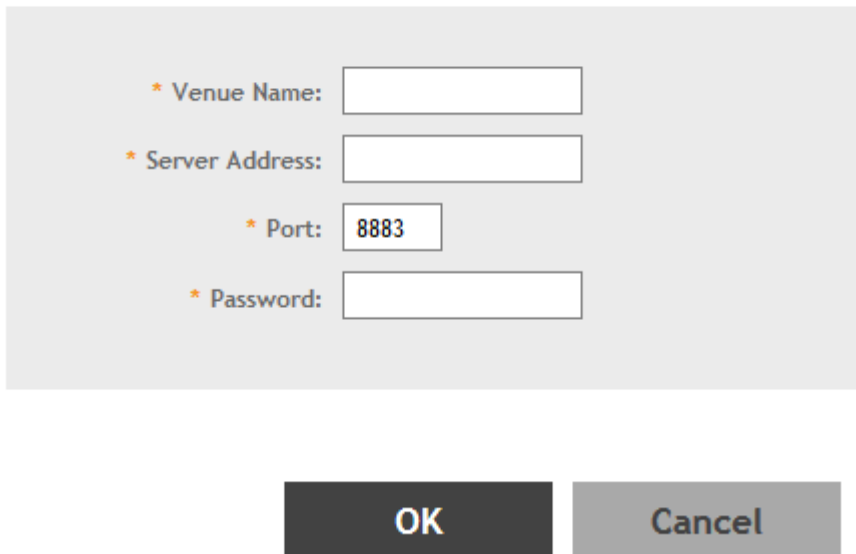
**FIGURE 24** Location Service



2. Click **Create**.  
The **Create LBS Server** page appears.

**FIGURE 25** Creating an LBS Server

## Create LBS Server



\* Venue Name:

\* Server Address:

\* Port:

\* Password:

**OK** **Cancel**

3. In the **Venue Name** field, enter the venue name for the server.
4. In the **Server Address** field, enter the venue name for the server.
5. In the **Port** field, enter the port number to communicate with the server.

**NOTE**

Default port number is 8883.

6. In the **Password** field, enter the password to access the server.
7. Click **OK**.

You have completed creating a location-based service on the controller.

**NOTE**

You can also edit, clone, and delete the location service by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Location Services** tab.

## Working with Maps

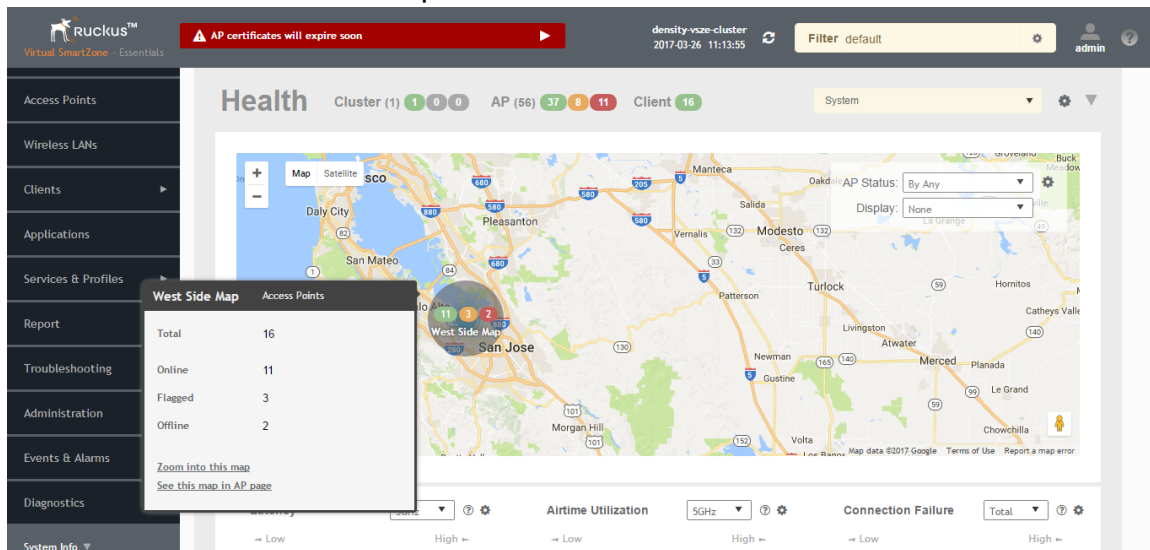
Importing floorplan maps into SmartZone allows you to further customize the information displayed on the Dashboard and Access Points pages, and monitor your APs, zones, groups, clients and traffic statistics all within the world map view on the Dashboard.

Additionally, you can use the maps to quickly locate more specific information on a venue or zone, and drag and drop APs onto the floor plan map to represent their locations in physical space in your venue.

Once a map is imported and GPS coordinates are entered, an icon representing the venue appears on the world map on the Dashboard. The icon displays the current number of APs (Online, Flagged and Offline). You can hover over the icon for more information.

Double-click the map icon or click **Zoom into this map** to view the imported map in the Dashboard.

**FIGURE 26** Once a floorplan map has been imported (with GPS coordinates), it is displayed on the world map on the Dashboard. Hover over the local map icon for more information.




## Importing a Floorplan Map

SmartZone provides a user-friendly workflow for importing a map of your venue floorplan, placing APs in their respective physical locations on the map, and scaling the map to match the actual dimensions of your venue.

Floorplan maps allow you to view site/venue/floor-specific details such as:

- AP status, performance, and health conditions
- Client connections to an AP
- Location-specific trouble spots related to AP or client connectivity

To import a floorplan map:

1. Go to **System > Maps**.
2. From the System tree hierarchy, select the location where you want to create a map and click the add  button. The **Add Map** form appears.
3. On the **Details** tab, enter a **Name** and optionally a **Description** to identify the map.



4. Enter a **Location** for the map. Alternatively, you can choose the location from the auto-completion options. Once you select the location, the GPS Coordinates are automatically updated.
5. For **GPS Coordinates**, you can enter the **Latitude** and **Longitude** values.

**FIGURE 27** The Add Map form

6. To add a **Map Image**, click **Browse** and select a site, venue, or floor map in jpg, jpeg, png, bmp or svg file formats.

**NOTE**

The maximum file size per indoor map is 5MB.

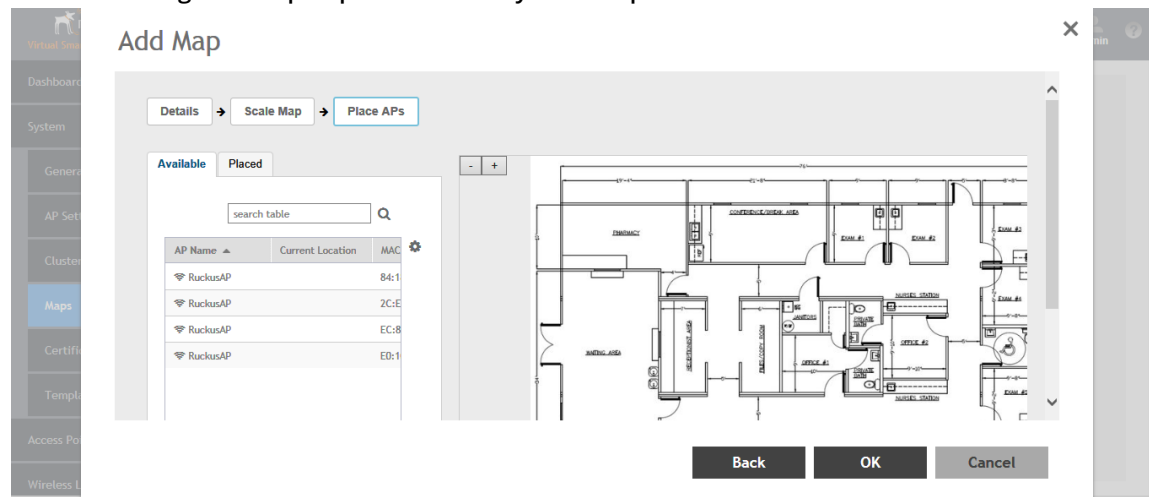
7. Click **Next**, the **Scale Map** tab appears.
8. Click two points on the map between which you know the distance. Blue dots appear to show the points you selected.

**FIGURE 28** Click two points on the map to define the map's scale

9. Enter the **Physical Distance** between the two points and select the unit of measurement (mm, cm, m, ft, yard).
10. Click **Save & Next**. The **Place APs** tab appears.

11. From the **Available** list, drag the APs and place them in their physical locations on the map. Click the **Placed** tab to see the list of placed APs.

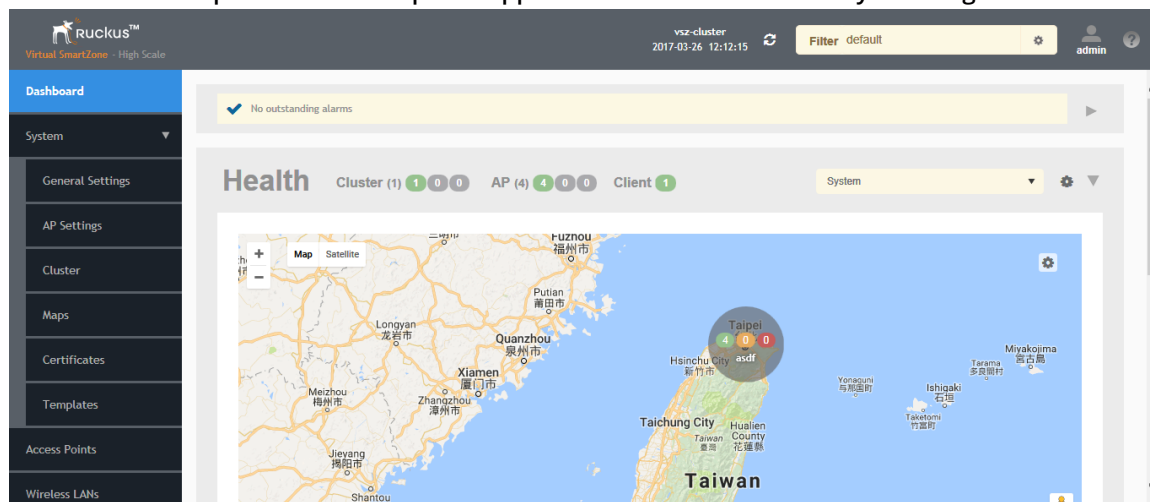
**FIGURE 29** Drag and drop to place APs onto your floorplan





12. Once you are happy with the placement of your APs on the map, click **OK** to save your map.

Your venue now appears as an icon on the world map on the Dashboard, located at your venue's actual physical location (if you entered the GPS coordinates correctly). The Dashboard icon that represents your venue provides an overview of the number of APs in the venue and their status. Hover over the icon to view more details, or click one of the links to zoom in to the venue floorplan map you imported.

**FIGURE 30** The imported venue map icon appears at the GPS coordinates you configured



#### NOTE

You can also edit or delete a map. To do so, select the map from the list and click the  **Edit** or  **Delete** buttons respectively.

## Viewing RF Signal Strength

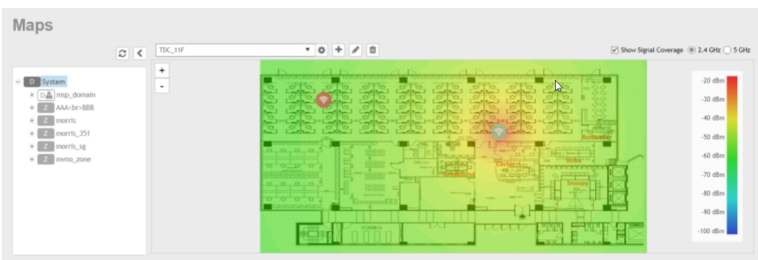
Radio Frequency (RF) signal strength can be viewed using a heat map for a specific location.

The heat map helps us identify the RF signal strength in a specific location. It provides heat maps using actual path loss information from the environment. You can view an indoor floor plan map for an AP.

To view the RF signal strength:

1. Go to **System > Maps**.
2. From the System tree hierarchy, select the location of the map that you want to view.
3. Select the **Show Signal Coverage** check box and choose the required RF frequency. For example, 2.4 GHz or 5 GHz. The heat map is displayed with a color-gradient legend. High signal strength appears in red. The color changes as the signal strength reduces.

**FIGURE 31** RF Coverage Heat Map



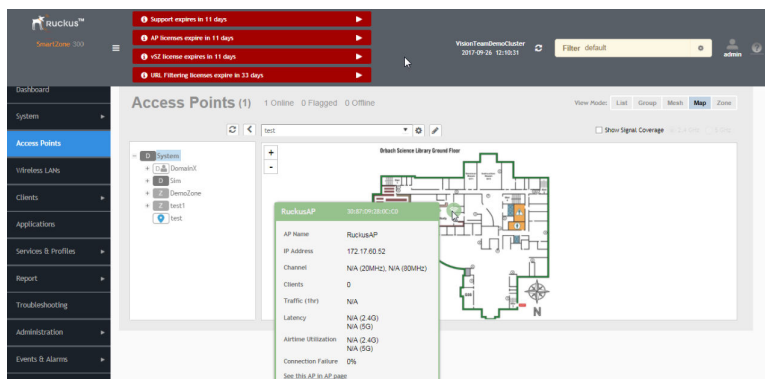
## Monitoring APs Using the Map View

Use the Map view on the **Access Points** page to monitor APs in relation to your venue's floorplan.

1. Go to **Access Points**.
2. In **View Mode**, click the **Map** button. The map view is displayed with your placed APs.

3. Hover over an AP to view the following AP-specific details:
  - **AP Name:** The name of the AP, if configured. If not, the default AP name is "RuckusAP."
  - **IP Address:** The current IPv4 or IPv6 address assigned to the AP.
  - **Channel:** Displays the channel (2.4 GHz / 5 GHz) in use, along with the channel width in parentheses.
  - **Clients:** The number of currently connected wireless clients.
  - **Traffic:** The total traffic volume over the last 1 hour.
  - **Latency:** The average time delay between AP and connected clients.
  - **Airtime Utilization:** Percent of airtime utilized, by radio.
  - **Connection Failure:** Percent of client connection attempt failures.

FIGURE 32 Hover over an AP to view details



4. To view more specific details on the AP, click the **See this AP in AP page** link.
5. To view the RF signal strength, select the **Show Signal Coverage** check box and choose the required RF frequency. For example, 2.4 GHz or 5 GHz.

The heat map is displayed with a color-gradient legend. High signal strength appears in red. The color changes as the signal strength reduces.

# Configuring AP Settings

---

• Approving APs.....	57
• Working with AP Registration Rules.....	57
• Tagging Critical APs.....	59
• Configuring the Tunnel UDP Port.....	60
• Setting the Country Code.....	60

## Approving APs

APs must be approved to join the system.

To approve an AP:

1. Go to **System > AP Settings > Approval**.
2. To approve each newly discovered APs
  - automatically, select the **Automatically approve all join requests from APs** check box.
  - manually, clear the **Automatically approve all join requests from APs** check box. This option enhances wireless security.
3. Click **OK**.

## Working with AP Registration Rules

Registration rules enable the controller to assign an AP to an AP zone automatically based on the rule that the AP matches.

### NOTE

A registration rule is only applied to an AP the first time it joins the controller. If an AP's MAC address already exists on the controller database (whether it is in connected or disconnected state and whether it belongs to the Staging Zone or any other zone), the controller will assign the AP to its last known AP zone.

## Creating an AP Registration Rule

You must create rules to register an AP.

To create an AP registration rule:

1. Go to **System > AP Settings > AP Registration**.
2. Click **Create**, the AP Registration Rule form appears.
3. Enter a **Rule Description**.
4. Select the **Zone Name** to which this rule applies.
5. In **Rule Type**, click the basis upon which you want to create the rule. Options include:

**NOTE**

The format of the IP address or addresses that you need to enter here depends on the AP IP mode that you selected when you created the AP zone to which this rule will be assigned. If you selected IPv4 Only, enter an IPv4 address. If you selected IPv6 Only, enter an IPv6 address.

- **IP Address Range:** If you select this option, enter the From (starting) and To (ending) IP address that you want to use.
- **Subnet:** If you select this option, enter the IP address and subnet mask pair to use for matching.
- **GPS Coordinates:** If you select this option, type the GPS coordinates to use for matching. Access points that have been assigned the same GPS coordinates will be automatically assigned to the AP zone that you will choose in the next step.

You can choose the Rule Type as GPS coordinates, wherein you must provide information about the latitude, longitude and distance to determine if the AP is within the defined area.

- **Provision Tag:** If the access points that are joining the controller have been configured with provision tags, click the Provision Tag option, and then type a tag name in the Provision Tag box. Access points with matching tags will be automatically assigned to the AP zone that you will choose in the next step.

**NOTE**

Provision tags can be configured on a per-AP basis from the access point's command line interface.

6. Click **OK**.

When the process is complete, the page refreshes, and then registration rule that you created appears on the AP Registration Rules page.

To create another registration rule, repeat the preceding steps. You can create as many registration rules as you need to manage the APs on the network.

**NOTE**

You can also edit, delete or clone an AP registration rule. To do so, select the rule profile from the list and click **Configure**, **Delete** or **Clone** respectively.

## Configuring Registration Rule Priorities

The controller applies registration rules in the same order as they appear in the AP Registration Rules table (highest to lowest priority).

If you want a particular registration rule to have higher priority, you must move it up the table. Once an AP matches a registration rule, the controller assigns the AP to the zone specified in the rule and stops processing the remaining rules.

Follow these steps to configure the registration rule priorities.

1. Go to **System > AP Settings > AP Registration**.
2. Select the rule from the list and click.
  - **Up**—To give a rule higher priority, move it up the table
  - **Down**—To give a rule lower priority, move it down the table
3. Click **Update Priorities** to save your changes.

# Tagging Critical APs

A critical AP is an AP that exceeds the daily traffic threshold (sum of uplink and downlink) data bytes configured on the controller web interface.

Follow these steps to tag critical APs (APs that exceed the data traffic threshold you have defined) automatically:

1. Go to **System > AP Settings > Critical AP Tagging**.
2. Select the **Enable Auto Tagging Critical APs** check box.
3. For **Auto Tagging Rules**, select **Daily Traffic Bytes Exceeds Threshold**.
4. For **Rule Threshold**:
  - In the first box, enter the value that you want to set as the traffic threshold. This value will be applied in conjunction with the data unit that you select in the second box.
  - In the second box, select the data unit for the threshold—**MB** for megabytes or **GB** for gigabytes.
5. Click **OK**.

Critical APs are marked with red dots next to its MAC Address for attention (refer the following image). APs that exceed the daily traffic threshold that you specified will appear highlighted on the Access Points page and the Access Point details page. Additionally, the controller will send an SNMP trap to alert you that an AP has been disconnected.

**FIGURE 33** APs Tagged as Critical

MAC Address	AP Name	Status	Alarm	Clients	Latency (2.4G)	Airtime Utilization (2.4G)	Latency (5G)	Airtime Utilization (5G)	Zone
38:FF:38:01:A2:10	Eddie R500	Offline	1	0	0	0	0	0	Eddies AP Zs...
58:86:33:36:98:70	SZ5.0DemoAP1	Online	1	0	0	0	0	0	SZ_Switch_D...
58:86:33:36:E9:60	SZ5.0DemoAP2	Online	1	0	0	0	0	0	SZ_Switch_D...
58:86:33:37:87:60	SZ5.0DemoAP3	Online	1	0	0	0	0	0	SZ_Switch_D...
E0:10:7F:18:52:00	RuckusAP	Offline	4	0	0	0	0	0	Laurent Home
E0:10:7F:38:7F:B0	Eddie R600	Offline	3	0	0	0	0	0	Eddies AP Zs...
E8:1D:A8:09:44:20	Silesia - RuckusAP	Offline	0	0	0	0	0	0	PlusPOsdemo
E8:1D:A8:09:44:90	Warszawa-RuckusAP	Offline	0	0	0	0	0	0	PlusPOsdemo
E8:1D:A8:09:45:90	Sosnowiec - RuckusAP	Offline	0	0	0	0	0	0	PlusPOsdemo
E8:1D:A8:09:46:10	GLIWICE - RuckusAP	Online	0	2	0	8%	0	1%	PlusPOsdemo
E8:1D:A8:09:46:20	Skoczow - RuckusAP	Online	0	1	0	3%	0	1%	PlusPOsdemo
E8:1D:A8:09:46:D0	JStawy- RuckusAP	Offline	0	0	0	0	0	0	PlusPOsdemo

## Configuring the Tunnel UDP Port

The tunnel UDP port is used by all GRE+UDP type tunnels.

To configuring the tunnel UDP port:

1. Go to **System > AP Settings > Tunnel UDP Port**.
2. Enter the **Tunnel UDP Port** number.
3. Click **OK**.

## Setting the Country Code

Different countries follow different regulations for radio channel usage.

To ensure that the APs use authorized radio channels:

1. Go to **System > AP Settings > Country Code**.
2. Select the **Country Code** for your location from the drop-down.
3. Click **OK**.

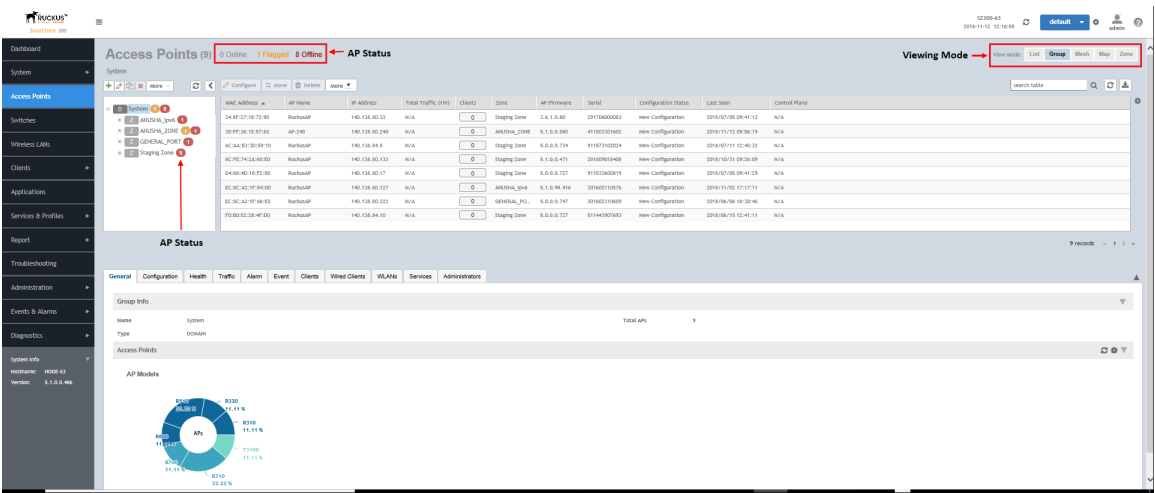


# Working With Access Points

- Understanding WLAN Services..... 61
- Viewing Modes.....82
- AP Status.....83
- Configuring Access Points..... 83
- Managing Access Points..... 93
- Multi-Tunnel Support for Access Points..... 102

The following image gives you an understanding of the Access Points home page.

FIGURE 34 Access Points



## Understanding WLAN Services

### Hierarchy Overview

The hierarchy helps in specifying which AP groups or APs provide which WLAN services.

You can virtually split them using the following hierarchy:

- System—Highest order that comprises of multiple zones
- Domains—Broad classification that comprises of multiple Zones.
- Zones—Comprises of multiple AP groups
- AP groups—Comprises of multiple APs
- APs—Individual access points.

## Working with AP Zones

An AP zone functions as a way of grouping Ruckus APs and applying a particular set of settings (including WLANs and their settings) to this group of Ruckus APs. Each AP zone can include up to 27 WLAN services.

By default, an AP zone named Staging Zone exists. Any AP that registers with the controller that is not assigned a specific zone is automatically assigned to the Staging Zone. This section describes how to use AP zones to manage devices.

### NOTE

When an AP is assigned or moved to the Staging Zone, the cluster name becomes its user name and password after the AP shows up-to-date state. If you need to log on to the AP, use the cluster name for the user name and password.

Before creating an AP zone, Ruckus recommends that you first set the default system time zone on the General Settings page. This will help ensure that each new AP zone will use the correct country. For information on how to set the default system time zone, see [Configuring System Time](#) on page 43.

### NOTE

In vSZ-E and SZ100, when the system is upgraded to release 3.5, the new UI and re-architected stats database will prevent the system from displaying AP and zone stats if the AP/zone is operating on 3.4 or prior releases. In order to make full use of the UI introduced in 3.5, zones and APs should be updated to 3.5 as well. Operationally, the zones will still work, but stats visibility will be impacted.

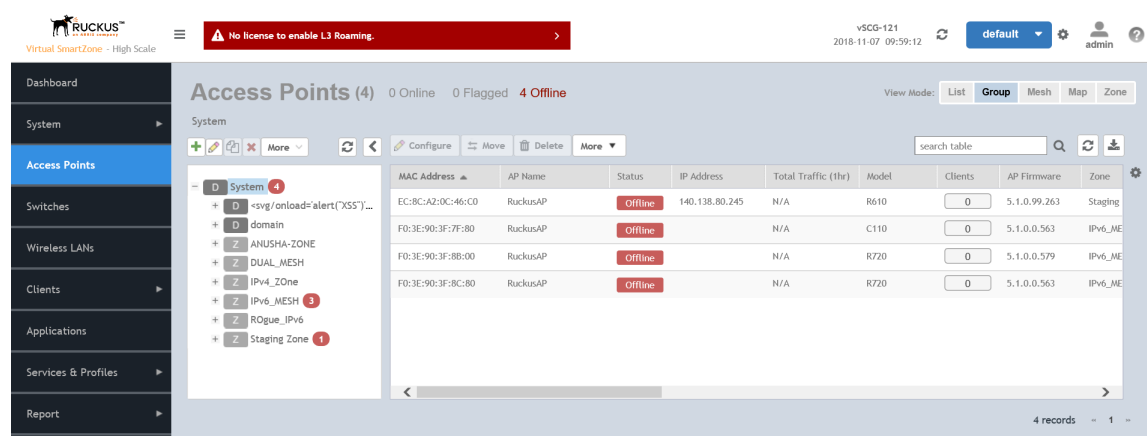
## Creating an AP Zone


An AP zone (or zone) functions as a way of grouping Ruckus APs and applying settings including WLANs to these groups of Ruckus APs. Each AP zone can include up to six WLAN services.

To create an AP zone

1. On the menu, click **Access Points**. The figure below appears.

**FIGURE 35** Access Points



2. From the **System** tree, select the location where you want to create the zone (for example, System or Domain), and then click .

**FIGURE 36** Create Groups

3. Configure the zone by completing the settings listed in the table below.
4. Click **OK**.

**TABLE 8** AP Zone Details

Field	Description	Your Action
<b>Name</b>	Indicates the name of the zone/AP group.	Enter a name.
<b>Description</b>	Indicates the short description assigned to the zone or AP group.	Enter a brief description
<b>Type</b>	Indicates if you are creating a domain, zone or an AP group.	Appears by default. You can also choose the option.
<b>Parent Group</b>	Indicates the parent AP group.	Appears by default.
<b>Configuration &gt; General Options</b>		
<b>AP Firmware</b>	Indicates the firmware to which it applies.	Select the firmware.
<b>Country Code</b>	Indicates the country code. Using the correct country code helps ensure that APs use only authorized radio channels.	Select the country code.
<b>Location</b>	Indicates the generic location of the zone.	Enter the location.
<b>Location Additional Information</b>	Indicates detailed location.	Enter additional location information.
<b>GPS Coordinates</b>	Indicates the geographical location.	Enter the following coordinates: <ul style="list-style-type: none"> <li>• <b>Longitude</b></li> <li>• <b>Latitude</b></li> <li>• <b>Altitude</b></li> </ul>
<b>AP Admin Logon</b>	Indicates the admin logon credentials.	Enter the <b>Logon ID</b> and <b>Password</b> .
<b>AP Time Zone</b>	Indicates the time zone that applies.	Select a time zone, and the enter the details as required.
<b>AP IP Mode</b>	Indicates the IP version that applies.	Select the IP version. IPv6, IPv4 and dual addressing modes are supported.

**TABLE 8 AP Zone Details (continued)**

Field	Description	Your Action
<b>Historical Connection Failures</b>	Allows the zone APs to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu.	Click the button.
<b>SSH Tunnel Encryption</b>	Specifies the encryption that reduces the load on controller control of SSH traffic.	Select the required option: <ul style="list-style-type: none"> <li><b>AES 128</b></li> <li><b>AES 256</b></li> </ul>
<b>Configuration &gt; Mesh Options</b>		
<b>Enable mesh networking in this zone</b>	Enables managed APs to automatically form a wireless mesh network, in which participant nodes (APs) cooperate to route packets.  Dual band APs can only mesh with other dual band APs, while single band APs can only mesh with other single band APs.	Click the button.
<b>Zero Touch Mesh</b>	Enables a new AP to join the network using wireless connection.	Click the button.
<b>Mesh Name (ESSID)</b>	Indicates the mesh name.	Type a name for the mesh network. Alternatively, do nothing to accept the default mesh name that the controller has generated.
<b>Mesh Passphrase</b>	Indicates the passphrase used by the controller to secure the traffic between Mesh APs.	Type a passphrase that contains at least 12 characters. Alternatively, click <b>Generate</b> to generate a random passphrase with 32 characters or more.
<b>Mesh Radio Option</b>	Indicates the channel range configured.	Select the channel option: 2.4 GHz or 5 GHz.
<b>Configuration &gt; Radio Options</b>		
<b>Channel Range (2.4G)</b>	Indicates that you want to override the 2.4GHz channel range that has been configured for the zone to which this AP group belong.	Select <b>Select Channel Range (2.4G)</b> check boxes for the channels on which you want the 2.4GHz radios of managed APs to operate. Channel options include channels 1 to 11. By default, all channels are selected.
<b>DFS Channels</b>	Allows ZoneFlex APs to use DFS channels.	Select the check box.
<b>5.8 Ghz Channels</b>	Provides C-band support for all Outdoor APs and the following Indoor APs: R310, R510, R710 .  <b>NOTE</b> This feature is available only for countries that support 5.8Ghz channel. For example, UK provides indoor AP—5.8Ghz channel support.	Select the <b>Allow 5.8Ghz channels</b> check box.
<b>5.8 Ghz Channels License</b>	Enables full TX Power Adjustment for C-band channels.  <b>NOTE</b> This feature is supported only for UK.	Select the <b>Allow 5.8Ghz channels use full power</b> check box.
<b>Channel Range (5G) Indoor</b>	Indicates the channels on the 5GHz radio that you want managed indoor APs to operate.	Select the check boxes.
<b>Channel Range (5G) Outdoor</b>	Indicates the channels on the 5GHz radio that you want managed outdoor APs to operate.	Select the check boxes.

**TABLE 8 AP Zone Details (continued)**

Field	Description	Your Action
<b>Radio Options b/g/n (2.4 GHz)</b>	Indicates the configuration options for the 2.4 GHz radio.	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20</b> or <b>40</b> (MHz), or select <b>Auto</b> to set it automatically.</li> <li>• <b>Channel</b>—Select the channel to use for the b/g/n (2.4GHz) radio, or select <b>Auto</b> to set it automatically.</li> <li>• <b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option, disables the TX Power Adjustment configuration.</li> </ul> <p><b>NOTE</b> Ensure that <b>Background Scan</b> is enabled.</p> <ul style="list-style-type: none"> <li>• <b>TX Power Adjustment</b>—Select the preferred TX power, if you want to manually configure the transmit power on the 2.4GHz radio. By default, TX power is set to <b>Full</b> on the 2.4GHz radio.</li> </ul> <p><b>NOTE</b> If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p>
<b>Radio Options a/n/ac (5 GHz)</b>	Indicates the configuration options for the 5 GHz radio.	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20, 40, 80, 80+80, 160</b> (MHz), or select <b>Auto</b> to set it automatically.</li> <li>• <b>Channel</b>—For <b>Indoor</b> and <b>Outdoor</b>, select the channel to use for the a/n/c (5GHz) radio, or select <b>Auto</b> to set it automatically.</li> <li>• <b>Secondary Channel (80+80)</b>—For <b>Indoor</b> and <b>Outdoor</b>, the default secondary channel to use for the a/n/c (5GHz) radio, is set as <b>Auto</b>.</li> <li>• <b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option, disables the TX Power Adjustment configuration.</li> </ul>

**TABLE 8 AP Zone Details (continued)**

Field	Description	Your Action
		<p><b>NOTE</b> Ensure that <b>Background Scan</b> is enabled.</p> <ul style="list-style-type: none"> <li>• <b>TX Power Adjustment</b>—Select the preferred TX power, if you want to manually configure the transmit power on the 5GHz radio. By default, TX power is set to <b>Full</b> on the 5GHz radio.</li> </ul> <p><b>NOTE</b> If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p>
<b>Configuration &gt; AP GRE Tunnel Options</b>		
<b>Tunnel Type</b>	Indicates the supported tunnel type (Ruckus GRE, SoftGRE and SoftGRE+IPsec)	<p>Choose :</p> <ul style="list-style-type: none"> <li>• <b>Ruckus GRE</b> and select the <b>GRE Tunnel Profile</b>.</li> <li>• <b>SoftGRE</b> and <ul style="list-style-type: none"> <li>- select the <b>GRE Tunnel Profile</b></li> <li>- select <b>AAA Affinity</b>, which is applicable only for proxy AAA.</li> </ul> </li> </ul> <p><b>NOTE</b> If you select <b>AAA Affinity</b>, you must enable <b>Force Disassociate Client</b> while creating the Soft GRE Profile.</p> <ul style="list-style-type: none"> <li>• <b>SoftGRE+IPsec</b> and <ul style="list-style-type: none"> <li>- select the <b>GRE Tunnel Profile</b></li> <li>- select <b>SoftGRE+IPsec</b></li> </ul> </li> </ul>
<b>Configuration &gt; Syslog Options</b>		
<b>Enable external syslog server for APs</b>	Indicates if an external syslog server is enabled.	<p>Select the check box and update the following details for the AP to send syslog messages to syslog server. If the primary server goes down, the AP send syslog messages to the secondary server as backup:</p> <ul style="list-style-type: none"> <li>• <b>Primary Server Address</b></li> <li>• <b>Secondary Server Address</b></li> <li>• <b>Port</b> for the respective servers</li> <li>• <b>Portocol</b>: select between UDP and TCP protocols</li> <li>• <b>Event Facility</b></li> <li>• <b>Priority</b></li> <li>• <b>Send Logs</b>: you can choose to send the General Logs, Client Logs or All Logs</li> </ul>
<b>Configuration &gt; AP SNMP Options</b>		

**TABLE 8 AP Zone Details (continued)**

Field	Description	Your Action
<b>Enable AP SNMP</b>	Indicates if the AP SNMP option is enabled.	Select the check box.
<b>SNMPv2 Agent</b>	Indicates if the SNMPv2 agent is enabled.	<p>If the SNMPv2 agent is enabled, configure the community settings.</p> <ol style="list-style-type: none"> <li>1. Click <b>Create</b> and enter <b>Community</b>.</li> <li>2. Select the required <b>Privilege</b>. If you select <b>Notification</b> enter the <b>Target IP</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
<b>SNMPv3 Agent</b>	Indicates SNMPv3 Agent is applied.	<p>If the SNMPv3 agent is enabled, configure the community settings.</p> <ol style="list-style-type: none"> <li>1. Click <b>Create</b> and enter <b>User</b>.</li> <li>2. Select the required <b>Authentication</b>.</li> <li>3. Enter the <b>Auth Pass Phrase</b>.</li> <li>4. Select the <b>Privacy</b> option.</li> <li>5. Select the required <b>Privilege</b>. If you select <b>Notification</b> select the option <b>Trap</b> or <b>Inform</b> and enter the <b>Target IP</b> and <b>Target Port</b>.</li> <li>6. Click <b>OK</b>.</li> </ol>
<b>DHCP Service for Wi-Fi Clients</b>		
<b>Enable DHCP Service in this zone</b>	Enables the DHCP service for this zone.	Select the check box.
<b>Configuration &gt; Advanced Options</b>		
<b>Channel Mode</b>	Indicates if location-based service is enabled. If you want to allow indoor APs that belong to this zone to use wireless channels that are Channel Mode regulated as indoor-use only.	Select the <b>Allow indoor channels</b> check box.
<b>Auto Channel Selection</b>	Indicates auto-channel settings.	Select the check box and choose the option.
<b>Background Scan</b>	Runs a background scan.	<p>Select the respective check boxes and enter the duration in seconds:</p> <ul style="list-style-type: none"> <li>• <b>Background Scanning</b>—Changes the AP channel if there is interference.</li> <li>• <b>ChannelFly</b>—Continuously monitors potential throughput and changes the AP channel to minimize interference and optimize throughput.</li> </ul>
<b>Smart Monitor</b>	Indicates AP interval check and retry threshold settings.	Select the check box and enter the interval and threshold.
<b>AP Ping Latency Interval</b>	Measures the latency between the controller and AP periodically, and send this data to SCI	Enable by moving the radio button to ON to measure latency.
<b>AP Management VLAN</b>	Indicates the AP management VLAN settings.	<p>Choose the option. Click <b>VLAN ID</b>, and then type the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID that has been configured on the AP, click Keep AP's settings.</p> <p><b>NOTE</b> For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.</p>
<b>Rogue AP Detection</b>	Indicates rogue AP settings.	Enable the option.

**TABLE 8 AP Zone Details (continued)**




Field	Description	Your Action
<b>Rogue Classification Policy</b>	Indicates the parameters used to classify rogue APs. This option is available only if you enable the <b>Rogue AP Detection</b> option.	<p>Select the options for rogue classification policy:</p> <ul style="list-style-type: none"> <li>– <b>Enable events and alarms for all rogue devices</b></li> <li>– <b>Enable events and alarms for malicious rogues only</b></li> <li>• <b>Report RSSI Threshold</b> - enter the threshold. Range: <b>0</b> through <b>100</b>.</li> <li>• <b>Protect the network from malicious rogue access points</b> - Enable the option and choose one of the following: <ul style="list-style-type: none"> <li>– <b>Aggressive</b></li> <li>– <b>Auto</b></li> <li>– <b>Conservative</b></li> </ul> </li> <li>• <b>Radio Jamming Detection</b> - enable the option and enter the <b>Jamming Threshold</b> in percentage.</li> </ul>
<b>DoS Protection</b>	Indicates settings for blocking a client.	Select the check box and enter the duration in seconds.
<b>Client Load Balancing</b>	Balances the number of clients across APs.	Select the check box and enter the threshold.
<b>Band Balancing</b>	Balances the bandwidth of the clients.	<p>You can use the slider to actively control associated stations to meet certain band distribution requirements allowing for dynamic band balancing:</p> <ul style="list-style-type: none"> <li>• Disable: disables band balancing</li> <li>• Basic (default): during heavy load conditions, this option withholds probe and authentication responses in order to balance clients.</li> <li>• Proactive: this is a dynamic form of band balancing where the clients are re-balanced on the AP utilizing the 802.11v BTM standard. The AP sends a BTM message to the client to change the bands and it is left to the client's discretion to make a decision on changing the bands.</li> <li>• Strict: this is an aggressive form of band balancing where the clients are forced to re-balance utilizing the 802.11v BTM standard. The AP sends a BTM message to the client to change the bands. If the client does not change the band, the client is forced to disconnect after 10 seconds.</li> </ul> <p><b>NOTE</b> The band change is applicable only for those connected clients that support 802.11v standard.</p> <p>Enter the percentage of client load on the 2.4 GHz band.</p>
<b>Location Based Service</b>	Indicates that the location based service is enabled.	<ul style="list-style-type: none"> <li>• Select the check box and choose the options.</li> <li>• Click Create, In the Create LBS Server form: <ol style="list-style-type: none"> <li>1. Enter the <b>Venue Name</b>.</li> <li>2. Enter the <b>Server Address</b>.</li> </ol> </li> </ul>



**TABLE 8 AP Zone Details (continued)**

Field	Description	Your Action
		3. Enter the <b>Port number</b> . 4. Enter the <b>Password</b> .
<b>Client Admission Control</b>	Indicates the load thresholds on the AP at which it will stop accepting new clients.	Select the check box and update the following settings: <ul style="list-style-type: none"> <li>• <b>Min Client Count</b></li> <li>• <b>Max Radio Load</b></li> <li>• <b>Min Client Throughput</b></li> </ul>
<b>Protection Mode</b>	Indicates the mechanism to reduce frame collision.	Choose one of the following options: <ul style="list-style-type: none"> <li>• None</li> <li>• RTS/CTS</li> <li>• CTS Only</li> </ul>
<b>AP Reboot Timeout</b>	Indicates the AP reboot settings.	Choose the required option for: <ul style="list-style-type: none"> <li>• <b>Reboot AP if it cannot reach default gateway after</b></li> <li>• <b>Reboot AP if it cannot reach the controller after</b></li> </ul>
<b>Recovery SSID</b>	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable <b>Recovery SSID Broadcast</b>

**NOTE**

You can also edit, clone or delete an AP Zone by selecting the options Configure , Clone  or Delete  respectively, from the Access Points page.

## Auto Cell Sizing

**NOTE**

Ensure that **Background Scan** is enabled.

When Wi-Fi is deployed in a high-density environment, despite the use of auto-channel selection, multiple APs operating on the same channel face a significant overlap of coverage regions. This could happen more so in a 2.4 GHz band where there is limited number of available channels and band path loss is lower than 5 GHz band. In such circumstances, the performance could be affected by AP to AP co-channel interference. To overcome this circumstance, the Auto Cell Sizing feature uses AP to AP communication to share information on the degree of interference seen by each other. Based on this information, the APs dynamically adjust their radio Tx power and Rx parameters (or cell size) to mitigate interference. Enabling the Auto Cell Sizing option, disables the TX Power Adjustment configuration.

## ChannelFly and Background Scanning

SmartZone controllers offer the ChannelFly and Background Scanning automatic channel selection methods for spectrum utilization and performance optimization. While Background Scanning must be enabled for rogue AP detection, AP location detection and radio power adjustment, either can be used for automatic channel optimization.

The main difference between ChannelFly and Background Scanning is that ChannelFly determines the optimal channel based on real-time statistical analysis of actual throughput measurements, while Background Scanning uses channel measurement and other techniques to estimate the impact of interference on Wi-Fi capacity based on progressive scans of all available channels.

#### **NOTE**

If you enable ChannelFly, Background Scanning can still be used for adjusting radio power and rogue detection while ChannelFly manages the channel assignment. Both cannot be used at the same time for channel management.

#### **Benefits of ChannelFly**

With ChannelFly, the AP intelligently samples different channels while using them for service. ChannelFly assesses channel capacity every 15 seconds and changes channel when, based on historical data, a different channel is likely to offer higher capacity than the current channel. Each AP makes channel decisions based on this historical data and maintains an internal log of channel performance individually.

When ChannelFly changes channels, it utilizes 802.11h channel change announcements to seamlessly change channels with no packet loss and minimal impact to performance. The 802.11h channel change announcements affect both wireless clients and Ruckus mesh nodes in the 2.4 GHz and/or 5 GHz bands.

Initially (in the first 30-60 minutes) there will be more frequent channel changes as ChannelFly learns the environment. However, once an AP has learned about the environment and which channels are most likely to offer the best throughput potential, channel changes will occur less frequently unless a large measured drop in throughput occurs.

ChannelFly can react to large measured drops in throughput capacity in as little as 15 seconds, while smaller drops in capacity may take longer to react to.

#### **Disadvantages of ChannelFly**

Compared to Background Scanning, ChannelFly takes considerably longer for the network to settle down. If you will be adding and removing APs to your network frequently, Background Scanning may be preferable. Additionally, if you have clients that do not support the 802.11h standard, ChannelFly may cause significant connectivity issues during the initial capacity assessment stage.

You can enable/disable ChannelFly per band. If you have 2.4 GHz clients that do not support 802.11h, Ruckus recommends disabling ChannelFly for 2.4 GHz but leaving it enabled for the 5 GHz band.

#### **Background Scanning**

Using Background Scanning, SmartZone controllers regularly samples the activity in all Access Points to assess RF usage, to detect rogue APs and to determine which APs are near each other for mesh optimization. These scans sample one channel at a time in each AP so as not to interfere with network use. This information is then applied in AP Monitoring and other controller monitoring features. You can, if you prefer, customize the automatic scanning of RF activity, deactivate it if you feel it's not helpful, or adjust the frequency, if you want scans at greater or fewer intervals.

#### **NOTE**

Background Scanning must be enabled for SmartZone controllers to detect rogue APs on the network.

#### **VLAN Pooling**

When Wi-Fi is deployed in a high density environment (such as a stadium) or on a university campus to provide access for students, the number of IP addresses required for client devices can easily run into several thousands.

Allocating a single large subnet results in a high probability of degraded performance due to factors like broadcast/multicast traffic.

To address this problem, VLAN pooling provides a method by which administrators can deploy pools of multiple VLANs from which clients are assigned, thereby automatically segmenting large groups of clients into smaller subgroups, even when connected to the same SSID.

As the client device joins the Wi-Fi network, the VLAN is assigned based on a hash of the client's MAC address (by default).

## Working with AP Groups

AP (access point) groups can be used to define configuration options and apply them to groups of APs at once, without having to individually modify each AP's settings.

For each group, administrators can create a configuration profile that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group or for all APs of a specific model in the group. AP groups are similar to WLAN groups (see Working with WLAN Groups for more information). While WLAN groups can be used to specify which WLAN services are served by which APs, AP groups are used for more specific fine-tuning of how the APs themselves behave.

### NOTE

AP group configuration settings can be overridden by individual AP settings. For example, if you want to set the transmit power to a lower setting for only a few specific APs, leave the Tx Power Adjustment at **Auto** in the AP group configuration page, then go to the individual AP configuration page (**Access Points > Access Points > Edit [AP MAC address]**) and set the **Tx Power Adjustment** to a lower setting.

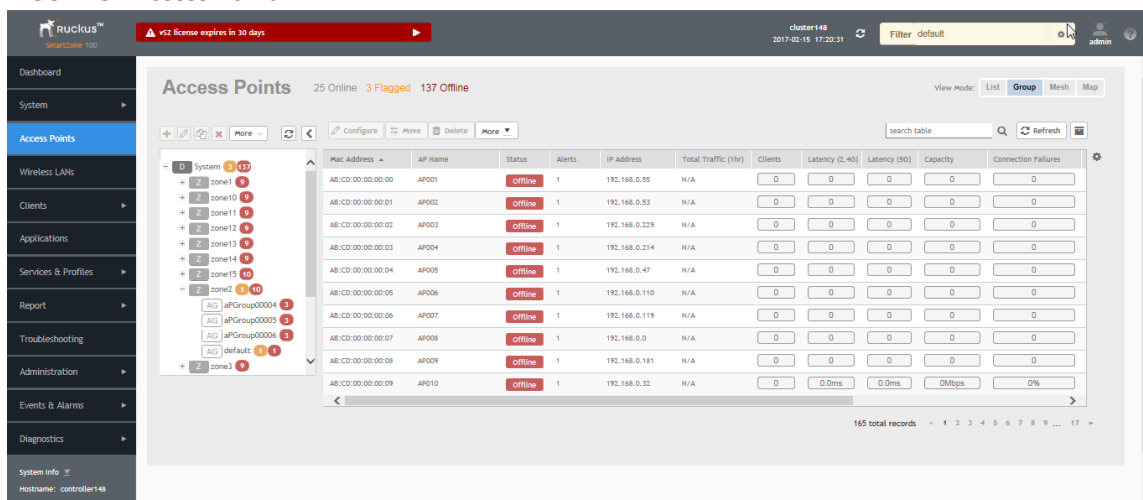
## Creating an AP Group


Creating an AP group means creating a configuration profile that defines the channels, radio settings, Ethernet ports and other configurable fields for all members of the group or for all APs of a specific model in the group.

Follow these steps to create an AP group.

1. From the left pane, select **Access Points**. The below figure appears.

FIGURE 37 Access Point




2. From the System tree hierarchy, select the location (for example: System, Domain, Zone) and click . The following figure appears.

**FIGURE 38** Create Groups

- Enter the details as explained in the following table.

**NOTE**

You can also edit the configuration of default APs by selecting the AP and clicking the  icon.

- Click **OK**.

**TABLE 9** AP Group Details

Field	Description	Your Action
<b>Name</b>	Indicates a name for the Zone/AP group.	Enter a name.
<b>Description</b>	Indicates a short description.	Enter a brief description
<b>Type</b>	Indicates if you are creating a domain, zone or an AP group.	Appears by default. You can also choose the option.
<b>Parent Group</b>	Indicates the parent group that this AP group belongs.	Appears by default.
<b>Configuration &gt; General Options</b>		
<b>Location</b>	Indicates generic location.	Enter the location.
<b>Location Additional Information</b>	Indicates detailed location.	Enter additional location information.
<b>GPS Coordinates</b>	Indicates the geographical location.	Enter the following coordinates in meters or floor: <ul style="list-style-type: none"> <li><b>Longitude</b></li> <li><b>Latitude</b></li> <li><b>Altitude</b></li> </ul>
<b>Configuration &gt; Group Members</b>		
<b>Members</b>	Displays the list of APs that belong to the group.	Select the members from the list and click <b>Move to</b> to assign them to the required group.
<b>Access Points</b>	Displays the list of APs that belong to the zone.	Select the <b>Access Points</b> from the list and click <b>Add to Group</b> .
<b>Configuration &gt; Radio Options</b>		

**TABLE 9** AP Group Details (continued)

Field	Description	Your Action
<b>Channel Range (2.4G)</b>	Indicates that you want to override the 2.4GHz channel range that has been configured for the zone to which this AP group belong.	Select <b>Select Channel Range (2.4G)</b> check boxes for the channels on which you want the 2.4GHz radios of managed APs to operate. Channel options include channels 1 to 11. By default, all channels are selected.
<b>5.8 Ghz Channels</b>	Provides C-band support for all Outdoor APs and the following Indoor APs: R310, R510, R710.  <b>NOTE</b> This feature is available only for countries that support 5.8Ghz channel. For example, UK provides indoor AP—5.8Ghz channel support.	Select the <b>Allow 5.8Ghz channels</b> check box.
<b>5.8 Ghz Channels License</b>	Enables full TX Power Adjustment for C-band channels.  <b>NOTE</b> This feature is supported only for UK.	Select the <b>Allow 5.8Ghz channels use full power</b> check box.
<b>Channel Range (5G) Indoor</b>	Indicates for what channels want the 5GHz radios of managed indoor APs to operate.	Select the check boxes.
<b>Channel Range (5G) Outdoor</b>	Indicates for what channels want the 5GHz radios of managed outdoor APs to operate.	Select the check boxes.
<b>Radio Options b/g/n (2.4 GHz)</b>	Indicates the radio option 2.4 GHz configurations.	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20</b> or <b>40</b> (MHz), or select <b>Auto</b> to set it automatically.</li> <li>• <b>Channel</b>—Select the channel to use for the b/g/n (2.4GHz) radio, or select <b>Auto</b> to set it automatically.</li> <li>• <b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option, disables the TX Power Adjustment configuration.</li> </ul> <p><b>NOTE</b> Ensure that <b>Background Scan</b> is enabled.</p> <ul style="list-style-type: none"> <li>• <b>TX Power</b>—Select the preferred TX power, if you want to manually configure the transmit power on the 2.4GHz radio. By default, TX power is set to <b>Full</b> on the 2.4GHz radio</li> <li>• <b>WLAN Group</b>—Specifies to which WLAN group this AP group belongs.</li> </ul>

**TABLE 9** AP Group Details (continued)

Field	Description	Your Action
<b>Radio Options a/n/ac (5 GHz)</b>	Indicates the radio option 5 GHz configurations.	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20, 40, 80, 80+80, 160</b> (MHz), or select <b>Auto</b> to set it automatically.</li> <li>• <b>Channel</b>—For <b>Indoor</b> and <b>Outdoor</b>, select the channel to use for the a/n/c (5GHz) radio, or select <b>Auto</b> to set it automatically.</li> <li>• <b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Enabling this option, disables the TX Power Adjustment configuration.</li> </ul> <p><b>NOTE</b> Ensure that <b>Background Scan</b> is enabled.</p> <ul style="list-style-type: none"> <li>• <b>TX Power</b>—Select the preferred TX power, if you want to manually configure the transmit power on the 5GHz radio. By default, TX power is set to <b>Full</b> on the 5GHz radio.</li> <li>• <b>WLAN Group</b>—Specify to which WLAN group this AP group belongs.</li> </ul>
<b>Configuration &gt; AP SNMP Options</b>		
<b>Override zone configuration</b>	Indicates that the AP Group configuration overrides the zone configuration.	Select the check box.
<b>Enable AP SNMP</b>	Indicates if the AP SNMP option is enabled.	Select the check box.
<b>SNMPv2 Agent</b>	Indicates SNMPv2 Agent is applied.	<ol style="list-style-type: none"> <li>1. Click <b>Create</b> and enter <b>Community</b>.</li> <li>2. Select the required <b>Privilege</b>. If you select <b>Notification</b> enter the <b>Target IP</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
<b>SNMPv3 Agent</b>	Indicates SNMPv3 Agent is applied.	<ol style="list-style-type: none"> <li>1. Click <b>Create</b> and enter <b>User</b>.</li> <li>2. Select the required <b>Authentication</b>.</li> <li>3. Enter the <b>Auth Pass Phrase</b>.</li> <li>4. Select the <b>Privacy</b> option.</li> <li>5. Select the required <b>Privilege</b>. If you select <b>Notification</b> select the option <b>Trap</b> or <b>Inform</b> and enter the <b>Target IP</b> and <b>Target Port</b>.</li> <li>6. Click <b>OK</b>.</li> </ol>
<b>Configuration &gt; Model Specific Options</b>		
<p><b>NOTE</b> Select the <b>Override</b> check box for that setting, and then configure the setting.</p>		
<b>AP Model</b>	Indicate the AP model for which you are configuring.	Select the option.




**TABLE 9 AP Group Details (continued)**

Field	Description	Your Action
<b>Status LEDs</b>	Disable the status LED on the selected AP model.	Select the option.
<b>LLDP</b>	Enables the Link Layer Discovery Protocol (LLDP) on the selected AP model.	Select the option and enter the following details: <ul style="list-style-type: none"> <li>• <b>Advertise Interval</b>—Enter the duration in seconds.</li> <li>• <b>Hold Time</b>—Enter the duration in seconds.</li> <li>• <b>Enable Management IP TLV</b>—Select the check box.</li> </ul>
<b>External Antenna (2.4 GHz)</b>	Enables the external 2.4 GHz antenna on the selected AP model.	Select the <b>Enable external antenna</b> check box, and then set the gain value (between 0 and 90dBi) in the box provided.
<b>External Antenna (5 GHz)</b>	Enables the external 5 GHz antenna on the selected AP model.	Select the <b>Enable external antenna</b> check box, and then set the gain value (between 0 and 90dBi) in the box provided.
<b>Port Settings</b>	Indicates the port settings.	Select the option and choose the required LAN option.
<b>PoE out port</b>	Enables PoE out mode.	Select the Enable PoE out ports (specific ZoneFlex AP models only) check box.
<b>PoE Operating Mode</b>	Indicates the PoE operating mode of the selected AP model	Choose the option. <p><b>NOTE</b> When this option is selected, some AP features are disabled to reduce power consumption, such as the USB port and one of the Ethernet ports.</p>
<b>Internal Heater</b>	Enables the heater that is built into the selected AP model	Select the Enable internal heaters (specific AP models only) check box.
<b>USB Port</b>	Disables the USB port. USB ports are enabled by default.	Select the Disable USB port check box.
<b>Configuration &gt; Advanced Options</b>		
<b>Location Based Service</b>	Enables location-based service for the AP group.	<ul style="list-style-type: none"> <li>• Select the <b>Override zone configuration</b> check box.</li> <li>• Select the <b>Enable LBS Service</b> check box.</li> <li>• <b>Select an LBS Server</b> from the drop-down.</li> </ul>
<b>Hotspot 2.0 Venue Profile</b>	Indicates the hotspot profile that you want to assign to the group.	Select the required option or click <b>Create</b> and update the following details: <ul style="list-style-type: none"> <li>• Enter the <b>Name</b>.</li> <li>• Enter the <b>Description</b>.</li> <li>• Enter the <b>Venue Names</b>.</li> <li>• Select the <b>Venue Category</b>.</li> <li>• Select the <b>Type</b>.</li> <li>• Enter the <b>WLAN Metrics</b>.</li> </ul>
<b>AP Management VLAN</b>	Indicates the AP management VLAN settings.	Choose the option. Click <b>VLAN ID</b> , and then type the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID that has been configured on the AP, click <b>Keep AP's settings</b> .

**TABLE 9** AP Group Details (continued)

Field	Description	Your Action
		<p><b>NOTE</b> For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.</p>
<b>Auto Channel Selection</b>	Indicates auto-channel settings.	Select the check box and choose the option.
<b>Client Admission Control</b>	Indicates the load thresholds on the AP at which it will stop accepting new clients.	<p>Select the <b>Override</b> check box respective to <b>2.4 GHz Radio</b> or <b>5 GHz Radio</b> and update the following details:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b></li> </ul> <p><b>NOTE</b> Client load balancing and band balancing will be disabled for this AP group.</p> <ul style="list-style-type: none"> <li>• <b>Min Client Count</b></li> <li>• <b>Max Radio Load</b></li> <li>• <b>Min Client Throughput</b></li> </ul>
<b>Protection Mode</b>	Indicates the mechanism to reduce frame collision.	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• RTS/CTS</li> <li>• CTS Only</li> </ul>
<b>Rogue Classification Policy</b>	Indicates the parameters used to classify rogue APs. This option is available only if you enable the <b>Rogue AP Detection</b> option.	<p>Select the options for rogue classification policy:</p> <ul style="list-style-type: none"> <li>• Enable the <b>Override</b> option and select the rogue classification policy from the list to override for this group.</li> <li>• Enable the <b>Override</b> option and enter the <b>Report RSSI Threshold</b>. Range: <b>0</b> through <b>100</b>.</li> <li>• Enable the <b>Override</b> option to override the aggressiveness of protecting the network and choose one of the following: <ul style="list-style-type: none"> <li>- <b>Aggressive</b></li> <li>- <b>Auto</b></li> <li>- <b>Conservative</b></li> </ul> </li> <li>• Enable the <b>Override</b> option and enter the <b>Jamming Threshold</b> in percentage.</li> </ul>
<b>Recovery SSID</b>	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable <b>Recovery SSID Broadcast</b>
<b>Direct Multicast</b>	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	<p>Select one or more of the following:</p> <ul style="list-style-type: none"> <li>• <b>Multicast Traffic from Wired Client</b></li> <li>• <b>Multicast Traffic from Wireless Client</b></li> <li>• <b>Multicast Traffic from Network</b></li> </ul>

**NOTE**

You can also edit, clone or delete an AP Group by selecting the options Configure , Clone  or Delete  respectively, from the Access Points page.



## Configuring Model-Based Settings

If you want to apply a set of settings to all APs of a particular model, use the Model-Based Settings option.

Follow the steps to configure the model based settings.

1. From the left-pane, click **Access Points**. The Access Points page appears.
2. From the list, select the AP for which you want to apply the model-based settings and click **Configure**. The Edit AP form appears.
3. Scroll down to **Model Specific Options** section, and then expand the section.
4. In **Model Specific Control**, select the **Override zone config** check box. The settings available for the AP model appear.
5. In the General Options section, configure the following settings:

### NOTE

The options that appear in the **Model Specific Options** section depend on the AP model that you select. Not all the options described in the table below will appear for every AP model.

Option	Description
<b>USB Port</b>	To disable the USB port on the selected AP model, select the <b>Disable USB port</b> check box. USB ports are enabled by default.
<b>Status LEDs</b>	To disable the status LED on the selected AP model, select the <b>Disable Status LEDs</b> check box.
<b>LLDP</b>	To enable the Link Layer Discovery Protocol (LLDP) on the selected AP model, select the <b>Enable Link Layer Discovery Protocol</b> check box. <ul style="list-style-type: none"> <li>• Enter the <b>Advertise Interval</b> duration in seconds</li> <li>• Enter the <b>Hold Time</b> duration in seconds</li> <li>• Select the <b>Enable Management IP TLV</b> check box</li> </ul>
<b>PoE Operating Mode</b>	Select the PoE operating mode of the selected AP model. Available options include Auto (default), 802.3af and 802.3at mode. If 802.3af PoE Operating Mode PoE is selected, this AP model will operate in 802.3af mode and will consume less power than in 802.3at mode. However, when this option is selected, some AP features are disabled to reduce power consumption, such as the USB port and one of the Ethernet ports.
<b>PoE out port</b>	To enable the PoE out port on the selected AP model, select the <b>Enable PoE out ports (specific ZoneFlex AP models only)</b> . <p><b>NOTE</b> If the controller country code is set to United Kingdom, an additional Enable 5.8 GHz Channels option will be available for outdoor 11n/11ac APs. Enabling this option allows the use of restricted C-band channels. These channels are disabled by default and should only be enabled by customers with a valid license to operate on these restricted channels.</p>
<b>Internal Heater</b>	To enable the heater that is built into the selected AP model, select the <b>Enable internal heaters (specific AP models only)</b> check box.
<b>External Antenna (2.4 GHz)</b>	To enable the external 2.4 GHz antenna on the selected AP model, select the <b>Enable external antenna</b> check box, and then set the gain value (between 0 and 90dBi) in the box provided.
<b>External Antenna (5 GHz)</b>	To enable the external 5 GHz antenna on the selected AP model, select the <b>Enable external antenna</b> check box, and then set the gain value (between 0 and 90dBi) in the box provided.

### NOTE

For H series AP models such as H500 and H510, you can disable LAN5.

6. In the **Port Settings** section, configure the following options for each LAN port.

#### NOTE

The number of LAN ports that appear in this section correspond to the physical LAN ports that exist on the selected AP model.

#### NOTE

When trunk port limitation is enabled, the controller does not validate the port settings configured in the AP or the AP group with no members.

Option	Description
<b>Enable</b>	Use this option to enable and disable this LAN port on the selected AP model. By default, this check box is selected. To disable this LAN port, clear this check box.
<b>Profile</b>	<p>Use this option to select the Ethernet port profile that you want this LAN port to use. Two default Ethernet port profile exist: <b>Default Trunk Port</b> (selected by default) and <b>Default Access Port</b>. If you created Ethernet port profiles (see <a href="#">Creating an Ethernet Port Profile</a> on page 317), these profiles will also appear on the drop-down list.</p> <p><b>NOTE</b> If you recently created an Ethernet port profile and it does not appear on the drop-down menu, click <b>Reload</b> on the drop-down menu to refresh the Ethernet port profile list.</p>
<b>Overwriter VLAN</b>	<p>Select the check box and enter:</p> <ul style="list-style-type: none"> <li>• <b>Untag ID</b>—Default: 1</li> <li>• <b>Members</b>—Range: 1 through 4094.</li> </ul>

7. Click **OK**.

### Supported LLDP Attributes

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral Layer 2 protocol that allows a network device (for example, a Ruckus AP) to advertise its identity and capabilities on the local network.

LLDP information is sent by devices from each of their interfaces at a fixed interval (default is 30 seconds), in the form of an Ethernet frame. Each LLDP Ethernet frame contains a sequence of type-length-value (TLV) structures starting with Chassis ID, Port ID and Time to Live (TTL) TLV. Table 2 lists the LLDP attributes supported by the controller.

LLDP information is sent by devices from each of their interfaces at a fixed interval (default is 30 seconds), in the form of an Ethernet frame. Each LLDP Ethernet frame contains a sequence of type-length-value (TLV) structures starting with Chassis ID, Port ID and Time to Live (TTL) TLV. The following table lists the LLDP attributes supported by the controller.

Attribute (TLV)	Description
Chassis ID	Indicates the MAC address of the AP's br0 interface
Port ID	Identifies the port from which the LLDP packet was sent
Time to Live	Same as LLDP Hold Time. Indicates the length of time (in seconds) that a receiving device will hold the LLDP information sent by the selected AP model before discarding it. The default value is 120 seconds.
System Name	Indicates the name assigned to the AP. The default name of Ruckus APs is RuckusAP.
System Description	Indicates the AP model plus software version
System Capabilities	Indicates the AP's capabilities (Bridge, WLAN AP, Router, Docsis), and which capabilities are enabled
Management Address	Indicates the management IP address of the AP
Port Description	Indicates the description of the port in alphanumeric format

## Configuring the Port Settings of a Particular AP Model

Use Port Settings in the AP Model-Specific Configuration section to configure the Ethernet ports of a particular AP model.

Follow these steps to configure the port settings of a certain AP model.

1. All ports are enabled by default (the Enable check boxes are all selected). To disable a particular port entirely, clear the Enable check box next to the port name (LAN1, LAN2, etc.)
2. For any enabled ports, you can choose whether the port will be used as a Trunk Port, Access Port, or General Port.

The following restrictions apply:

- All APs must be configured with at least one Trunk Port.

### NOTE

You cannot move an AP model to an AP group and configure the AP model to use a trunk port at the same time, if general ports are enabled when trunk port limitation is disabled. You must configure the selected AP model to use at least one trunk port, and then move the AP model to the AP group.

- For single port APs, the single LAN port must be a trunk port and is therefore not configurable.
- For ZoneFlex 7025/7055, the LAN5/Uplink port on the rear of the AP is defined as a Trunk Port and is not configurable. The four front-facing LAN ports are configurable.
- For all other APs, you can configure each port individually as either a Trunk Port, Access Port, or General Port. See [Designating an Ethernet Port Type](#) on page 79 for more information.

## Designating an Ethernet Port Type

Ethernet ports can be configured as access ports, trunk ports, or general ports.

Trunk links are required to pass VLAN information between switches. Access ports provide access to the network and can be configured as members of specific VLANs, thereby separating the traffic on these ports from traffic on other VLANs. General ports are user-defined ports that can have any combination of up to 20 VLAN IDs assigned.

For most ZoneFlex APs, you can set which ports you want to be your Access, Trunk and General Ports from the controller web interface, as long as at least one port on each AP is designated as a Trunk Port.

By default, all ports are enabled as Trunk Ports with Untag VLAN set as 1 (except for ZoneFlex 7025, whose front ports are enabled as Access Ports by default). If configured as an Access Port, all untagged ingress traffic is the configured Untag VLAN, and all egress traffic is untagged. If configured as a Trunk Port, all untagged ingress traffic is the configured Untag VLAN (by default, 1), and all VLAN-tagged traffic on VLANs 1-4094 will be seen when present on the network.

The default Untag VLAN for each port is VLAN 1. Change the Untag VLAN to:

- Segment all ingress traffic on this Access Port to a specific VLAN.
- Redefine the native VLAN on this Trunk Port to match your network configuration.

When trunk port limitation is disabled using the `eth-port-validate-one-trunk disable` command, validation checks are not performed for the VLAN members and the AP Management VLAN. If the AP configuration for general ports and access ports does not include a member of an AP management VLAN, or the VLAN of a WAN interface configured through CLI, the AP will disconnect and the Ethernet port stops transmitting data. Make sure that you configure the correct VLAN member in the ports (general/access) and the AP management VLAN.

### NOTE

Ensure that at least one of the general port VLANs is the same as a Management VLAN of the AP.

## Configuring Client Admission Control

As an administrator, you can help maintain a positive user experience for wireless users on the network by configuring the following client admission control settings:

- Minimum client count
- Maximum radio load
- Minimum client throughput

Client admission control is implemented on a per radio basis and is supported on 802.11n and 802.11ac APs.

## Monitoring Domains, Zones, and AP Groups

When you select a System, Domain, Zone, or AP Group from the hierarchy tree, respective contextual tabs appear at the bottom of the page.

These tabs are used to monitor the selected group. The following table lists the tabs that appear for System, Domain, Zone, and AP Group.

**TABLE 10** System, Domain, Zone, and AP Groups Monitoring Tabs

Tabs	Description	System	Domain	Zone	AP Groups
<b>General</b>	Displays group information	Yes	Yes	Yes	Yes
<b>Configuration</b>	Displays group configuration information.	Yes	Yes	Yes	Yes
<b>Health</b>	Displays historical health information.	Yes	Yes	Yes	Yes
<b>Traffic</b>	Displays historical traffic information.	Yes	Yes	Yes	Yes
<b>Alarm</b>	Displays alarm information.	Yes	Yes	Yes	Yes
<b>Event</b>	Displays event information.	Yes	Yes	Yes	Yes
<b>Clients</b>	Displays client information.  <b>NOTE</b> Selecting the <b>Enable client visibility regardless of 802.1X authentication</b> check box bypasses 802.1X authentication for client visibility. This option allows you to view statistical information about wired clients even without enabling 802.1X authentication.	Yes	Yes	Yes	Yes
<b>WLANs</b>	Displays WLAN information.	Yes	Yes	Yes	NA
<b>Services</b>	Displays information on the list of services.	Yes	Yes	Yes	NA
<b>Administrators</b>	Displays administrator account information.	Yes	NA	NA	NA

Additionally, you can select System, Domain, or Zone and click **More** to perform the following operations as required:

- **Move**
- **Create New Zone from Template**
- **Extract Zone Template**
- **Apply Zone Template**
- **Change AP Firmware**
- **Switchover Cluster**

- **Trigger Preferred Node**

### ***Moving an AP Zone Location***

Follow these steps to move an AP zone to a different location:

1. From the Access Points page, locate the AP zone that you want to move to a different location.
2. Click **Move**, the **Select Destination Management Domain** dialog box appears.
3. Select the destination and click **OK**, a confirmation dialog box appears.
4. Click **Yes**, the page refreshes and AP zone is moved to the selected destination.

### ***Creating a New Zone using a Zone Template***

Follow these steps to create a new zone using a template:

1. From the Access Points page, locate the zone from where you want to create a new zone.
2. Click **More** and select **Create New Zone from Template**, a dialog box appears.
3. In **Zone Name**, enter a name for the new AP zone.
4. Select the required template from the **Template Name** drop-down.
5. Click **OK**. The page refreshes and the new zone is created.

### ***Extracting a Zone Template***

You can extract the current configuration of a zone and save it as a zone template.

Follow these steps to extract the configuration of a zone to a zone template:

1. From the Access Points page, locate the zone from where you want to extract the WLAN template.
2. Click **More** and select **Extract Zone Template**, the **Extract Zone Template** dialog box appears.
3. In **Zone Template Name**, enter a name for the Template.
4. Click **OK**, a message appears stating that the zone template was extracted successfully.
5. Click **OK**. You have completed extracting a zone template.

The extracted Zone template can be viewed under **System > Templates > Zone Templates**.

### ***Applying a Zone Template***

You can apply an AP zone configuration template to a zone.

Follow these steps to apply a zone template:

1. From the Access Points page, locate the zone where you want to apply the zone template.
2. Click **More** and select **Apply Zone Template**, the **Import Zone Template** dialog box appears.
3. From the **Select a Zone template** drop-down, select the template.
4. Click **OK**, a confirmation message appears asking to apply the zone template to the AP zone.
5. Click **Yes**. The zone template was applied successfully.

You have completed applying zone template to the AP zone.

## Changing the Zone's AP Firmware Version

The controller supports multiple firmware version. You can manually upgrade or downgrade the zone's AP firmware version.

Follow these steps to change the zone's AP firmware version:

1. From the Access Pointss page, locate the zone for which you want to upgrade the AP firmware version.
2. Click **More** and select **Change AP Firmware**, the **Change AP Firmware** dialog box appears.
3. The Current AP Firmware version is displayed. Select the firmware version you need. If you upgrade to a new firmware, a backup configuration file will be created. You can use this backup file to downgrade to original firmware.
4. Click **Yes**, a confirmation message appears stating that the firmware version was updated successfully.
5. Click **OK**. You have completed upgrading the zone's AP firmware version.

## Rehoming Managed APs and Data Planes

Rehoming is the process of returning the APs and external data planes that have failed over to the standby cluster back to their original cluster (once it becomes available). Rehoming must be done manually. APs and external data planes that have failed over will continue to be managed by the failover cluster until you rehome them.

### NOTE

You can rehome managed APs and external data planes, only in a cluster redundancy environment. When APs or external data planes of a certain active cluster failover to a standby cluster, you must manually restore them to the original cluster, once the active cluster is fixed and back to service.

Rehoming APs or external data planes must be done on a per-cluster basis. Follow these steps to rehome managed APs to the original cluster:




1. From the **Access Points** page, select the **System** to activate rehome operation.
2. Click **More** and select **Rehome Active Clusters**.  
A confirmation dialog box appears.
3. Click **Yes**, you have set all APs in the standby cluster to rehome to the active cluster to which they were previously connected

# Viewing Modes

You can view System, Zone, and AP Group-level information by selecting one of the following **View Mode** options:

- **List**—Displays the list of all APs irrespective of the Zone or Group they belong.
- **Group**—Displays the list of APs in a hierarchy format. The is the default viewing mode.
- **Mesh**—Lists AP details.
- **Map**—Displays the location map of the APs.
- **Zone**—Lists zone details. There will be 10,000 zones in a system.

### NOTE

You can also edit, clone or delete a zone by selecting the options Configure , Clone  or Delete  respectively from the Access Points page.

# AP Status

The real-time status of the Access Points are classified as follows:

The status of Access Points can be one of the following:

- **25 Online**—Number of Access Points that are online.
- **3 Flagged**—Number of Access Points that are flagged.
- **137 Offline**—Number of Access Points that are offline.

## NOTE

APs that exceed their health threshold and that require your attention are flagged. See [Understanding Cluster and AP Health Icons](#) on page 23.

# Configuring Access Points

You can configure an Access Point.

To configure an Access Point:

1. From the list, select the Access Point that you want to configure and click **Configure**. The Edit AP page appears.
2. Edit the parameters as explained in [Table 11](#).
3. Click **OK**.

## NOTE

Select the **Override** check box if you want to configure new settings.

**TABLE 11** Access Point Edit Parameters

Field	Description	Your Action
<b>AP Configuration &gt; General Options</b>		
<b>AP Name</b>	Indicates the name of the AP.	Enter a name.
<b>Description</b>	Gives a short description of the AP.	Enter a short description.
<b>Location</b>	Indicates generic location.	Select the check box and enter the location.
<b>Location Additional Information</b>	Indicates specific location.	Select the check box and enter the location.
<b>GPS Coordinates</b>	Indicates the geographical location.	Select the option. For Manual option, enter the following details: <ul style="list-style-type: none"> <li>• <b>Latitude</b></li> <li>• <b>Longitude</b></li> <li>• <b>Altitude</b></li> </ul>
<b>User Location Information</b>	Indicates the demographic information.	Enter the <b>Area Code</b> and <b>Cell Identifier</b> .
<b>AP Admin Logon</b>	Indicates the admin logon credentials.	Select the check box and enter the <b>Logon ID</b> and <b>Password</b> .
<b>AP Configuration &gt; Radio Options</b>		
<b>Channel Range (2.4G)</b>	Indicates that you want to override the 2.4GHz channel range that has been configured for the zone to which this AP group belong.	Select <b>Select Channel Range (2.4G)</b> check boxes for the channels on which you want the 2.4GHz radios of managed APs to operate. Channel options include channels 1 to 11. By default, all channels are selected.

**TABLE 11** Access Point Edit Parameters (continued)

Field	Description	Your Action
<b>Channel Range (5G)</b>	Indicates that you want to override the 5GHz channel range that has been configured for the zone to which this AP group belong.	Select <b>Select Channel Range (5G)</b> check boxes for the channels on which you want the 5GHz radios of managed APs to operate.
<b>Radio Options b/g/n (2.4 GHz)</b>	Indicates the radio option 2.4 GHz configurations.	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20</b> or <b>40</b> (MHz), or select <b>Auto</b> to set it automatically.</li> <li>• <b>Channel</b>—Select the channel to use for the b/g/n (2.4GHz) radio, or select <b>Auto</b> to set it automatically.</li> <li>• <b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Selecting the <b>Enable</b> option, disables the <b>TX Power Adjustment</b> configuration.</li> </ul> <p><b>NOTE</b> Ensure that <b>Background Scan</b> is enabled.</p> <ul style="list-style-type: none"> <li>• <b>TX Power Adjustment</b>—Select the required option.</li> </ul> <p><b>NOTE</b> If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p> <ul style="list-style-type: none"> <li>• <b>WLAN Group</b>—Select the WLAN group to which this AP belongs.</li> <li>• <b>WLAN Services</b>—Select the check box to enable WLAN services in this radio.</li> </ul>
<b>Radio Options a/n/ac (5 GHz)</b>	Indicates the radio option 5 GHz configurations.	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20, 40, 80</b> (MHz), or select <b>Auto</b> to set it automatically.</li> <li>• <b>Channel</b>—Select the channel to use for the a/n/c (5GHz) radio, or select <b>Auto</b> to set it automatically.</li> </ul>



**TABLE 11** Access Point Edit Parameters (continued)

Field	Description	Your Action
		<ul style="list-style-type: none"> <li>• <b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Selecting the <b>Enable</b> option, disables the <b>TX Power Adjustment</b> configuration.</li> </ul> <p><b>NOTE</b> Ensure that <b>Background Scan</b> is enabled.</p> <ul style="list-style-type: none"> <li>• <b>TX Power Adjustment</b>—Select the required option.</li> </ul> <p><b>NOTE</b> If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p> <ul style="list-style-type: none"> <li>• <b>WLAN Group</b>—Select the WLAN group to which this AP belongs.</li> <li>• <b>WLAN Services</b>—Select the check box to enable WLAN services in this radio.</li> </ul>
<b>Configuration &gt; AP GRE Tunnel Options</b>		
<b>Ruckus GRE Forwarding Broadcast</b>	Forwards broadcast traffic from network to tunnel.  <b>NOTE</b> ARP and DHCP traffic are allowed even if this option disabled	Click <b>Override</b> to enable the Ruckus GRE broadcast forwarding option.  Click the <b>Enable Forwarding Broadcast</b> option to forward the broadcast traffic.
<b>AP Configuration &gt; AP SNMP Options</b>		
<b>Override zone configuration</b>	Allows you to override the existing zone configuration	Select the check box
<b>Enable AP SNMP</b>	Enables you to configure SNMP settings.	Select the check box
<b>SNMPv2 Agent</b>	Allows you to add users to SNMPv2 Agent.	<ol style="list-style-type: none"> <li>1. Click <b>Create</b> and enter <b>Community</b>.</li> <li>2. Select the required <b>Privilege</b>. If you select <b>Notification</b> enter the <b>Target IP</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>

**TABLE 11** Access Point Edit Parameters (continued)

Field	Description	Your Action
<b>SNMPv3 Agent</b>	Allows you to add users to SNMPv3 Agent.	<ol style="list-style-type: none"> <li>1. Click <b>Create</b> and enter <b>User</b>.</li> <li>2. Select the required <b>Authentication</b>.</li> <li>3. Enter the <b>Auth Pass Phrase</b>.</li> <li>4. Select the <b>Privacy</b> option.</li> <li>5. Select the required <b>Privilege</b>. If you select <b>Notification</b> select the option <b>Trap</b> or <b>Inform</b> and enter the <b>Target IP</b>.</li> <li>6. Click <b>OK</b>.</li> </ol>
<b>AP Configuration &gt; Model Specific Options</b>		
<b>Model Specific Control</b>	Indicates that the model overrides the AP settings.	Select the check box.
<b>USB Port</b>	Disables the USB port on the selected AP model.	Select the option. USB ports are enabled by default.
<b>Status LEDs</b>	Disable the status LED on the selected AP model.	Select the option.
<b>LLDP</b>	Enables the Link Layer Discovery Protocol (LLDP) on the selected AP model.	Select the option and enter the following details: <ul style="list-style-type: none"> <li>• <b>Advertise Interval</b>—Enter the duration in seconds.</li> <li>• <b>Hold Time</b>—Enter the duration in seconds.</li> <li>• <b>Enable Management IP TLV</b>—Select the check box.</li> </ul>
<b>PoE Operating Mode</b>	Allows you to operate using PoE mode.	Select the option.
<b>Port Settings</b>	Indicates the port settings.	Select the option and choose the required LAN option.
<b>AP Configuration &gt; Advanced Options</b>		
<b>Network Settings</b>	Determines the network settings.	Select the IPv4 Settings from the following: <ul style="list-style-type: none"> <li>• <b>Static</b>—Enter the <b>IP Address, Network Mask, Gateway, Primary DNS, Secondary DNS</b>.</li> <li>• <b>Dynamic</b></li> <li>• <b>Keep the AP's Setting</b></li> </ul>
<b>Smart Monitor</b>	Indicates AP interval check and retry threshold settings.	Select the required check boxes.
<b>Syslog Options</b>	Determines if external syslog server settings is applicable.	Select the check box and update the following details for the AP to send syslog messages to syslog server. If the primary server goes down, the AP send syslog messages to the secondary server as backup: <ul style="list-style-type: none"> <li>• <b>Primary Server Address</b></li> <li>• <b>Secondary Server Address</b></li> <li>• <b>Port</b> for the respective servers</li> <li>• <b>Portocol</b>: select between UDP and TCP protocols</li> <li>• <b>Event Facility</b></li> </ul>

**TABLE 11** Access Point Edit Parameters (continued)

Field	Description	Your Action
		<ul style="list-style-type: none"> <li>• <b>Priority</b></li> <li>• <b>Send Logs:</b> you can choose to send the General Logs, Client Logs or All Logs</li> </ul>
<b>Hotspot 2.0 version Profile</b>	Indicates the hotspot profile that you want to assign to the group.	<p>Select the required option or click <b>Create</b> and update the following details:</p> <ul style="list-style-type: none"> <li>• Enter the <b>Name</b>.</li> <li>• Enter the <b>Description</b>.</li> <li>• Enter the <b>Venue Names</b>.</li> <li>• Select the <b>Venue Category</b>.</li> <li>• Select the <b>Type</b>.</li> <li>• Enter the <b>WLAN Metrics</b>.</li> </ul>
<b>AP Management VLAN</b>	Indicates the AP management VLAN settings.	<p>Select the check box and choose the option.</p> <p><b>ATTENTION</b> For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.</p>
<b>Auto Channel Selection</b>	Indicates auto-channel settings.	Select the check box and choose the option.
<b>Client Admission Control</b>	Indicates the load thresholds on the AP at which it will stop accepting new clients.	<p>Select the check boxes and update the following details:</p> <ul style="list-style-type: none"> <li>• <b>Min Client Count</b></li> <li>• <b>Max Radio Load</b></li> <li>• <b>Min Client Throughput</b></li> </ul>
<b>Rogue Classification Policy</b>	Indicates the parameters used to classify rogue APs. This option is available only if you enable the <b>Rogue AP Detection</b> option.	<p>Select the options for rogue classification policy:</p> <ul style="list-style-type: none"> <li>• Enable the <b>Override</b> option and enter the <b>Report RSSI Threshold</b>. Range: <b>0</b> through <b>100</b>.</li> <li>• Enable the <b>Override</b> option to override the aggressiveness of protecting the network and choose one of the following: <ul style="list-style-type: none"> <li>- <b>Aggressive</b></li> <li>- <b>Auto</b></li> <li>- <b>Conservative</b></li> </ul> </li> <li>• Enable the <b>Override</b> option and enter the <b>Jamming Threshold</b> in percentage.</li> </ul>
<b>Recovery SSID</b>	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable <b>Recovery SSID Broadcast</b>
<b>Direct Multicast</b>	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	<p>Select one or more of the following:</p> <ul style="list-style-type: none"> <li>• <b>Multicast Traffic from Wired Client</b></li> <li>• <b>Multicast Traffic from Wireless Client</b></li> <li>• <b>Multicast Traffic from Network</b></li> </ul>
<b>Swap Configuration</b>		

**TABLE 11** Access Point Edit Parameters (continued)

Field	Description	Your Action
<b>Add Swap-In AP</b>	Allows to swap APs.	Select the check box and enter the <b>Swap-in AP MAC</b> details.

**NOTE**

You can also move the location of an AP or delete an AP. To do so, select the AP from the list and click **Move** or **Delete** as required.

## Configuring the M510 AP

The M510 Access Point (AP) is an 802.11ac Wave 2 access point with LTE backhaul in addition to providing better performance, power efficiency, and is cost-effective.

SmartZone supports the M510 AP with cellular backhaul connections. Model-specific configurations including settings for cellular radio are introduced to configure the AP behavior.

1. From the list, select the M510 Access Point and click **Configure**. The **Edit AP** page appears.
2. Edit the parameters as explained in the table below.
3. Click **OK**.

**NOTE**

Select the **Override** check box if you want to configure new settings.

**TABLE 12** Access Point Edit Parameters

Field	Description	Your Action
<b>AP Configuration &gt; General Options</b>		
<b>AP Name</b>	Indicates the name of the AP.	Enter a name.
<b>Description</b>	Gives a short description of the AP.	Enter a short description.
<b>Location</b>	Indicates generic location.	Select the check box and enter the location.
<b>Location Additional Information</b>	Indicates specific location.	Select the check box and enter the location.
<b>GPS Coordinates</b>	Indicates the geographical location.	Select the option. For Manual option, enter the following details: <ul style="list-style-type: none"> <li>• <b>Latitude</b></li> <li>• <b>Longitude</b></li> <li>• <b>Altitude</b></li> </ul>
<b>User Location Information</b>	Indicates the demographic information.	Enter the <b>Area Code</b> and <b>Cell Identifier</b> .
<b>AP Admin Logon</b>	Indicates the admin logon credentials. For the Default Zone, the SZ cluster name is used as the default logon ID and password.	Select the check box and enter the <b>Logon ID</b> and <b>Password</b> .
<b>AP Configuration &gt; Radio Options</b>		
<b>Channel Range (2.4G)</b>	Indicates that you want to override the 2.4GHz channel range that has been configured for the zone to which this AP group belong.	Select <b>Select Channel Range (2.4G)</b> check boxes for the channels on which you want the 2.4GHz radios of managed APs to operate. Channel options include channels 1 to 11. By default, all channels are selected.
<b>Channel Range (5G)</b>	Indicates that you want to override the 5GHz channel range that has been configured for the zone to which this AP group belong.	Select <b>Select Channel Range (5G)</b> check boxes for the channels on which you want the 5GHz radios of managed APs to operate.

**TABLE 12** Access Point Edit Parameters (continued)

Field	Description	Your Action
<b>Radio Options b/g/n (2.4 GHz)</b>	Indicates the radio option 2.4 GHz configurations.	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20</b> or <b>40</b> (MHz), or select <b>Auto</b> to set it automatically.</li> <li>• <b>Channel</b>—Select the channel to use for the b/g/n (2.4GHz) radio, or select <b>Auto</b> to set it automatically.</li> <li>• <b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Selecting the <b>Enable</b> option, disables the <b>TX Power Adjustment</b> configuration.</li> <li>• <b>TX Power Adjustment</b>—Select the required option.</li> </ul> <p><b>NOTE</b> If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p> <ul style="list-style-type: none"> <li>• <b>WLAN Group</b>—Select the WLAN group to which this AP belongs.</li> <li>• <b>WLAN Services</b>—Select the check box to enable WLAN services in this radio.</li> </ul>
<b>Radio Options a/n/ac (5 GHz)</b>	Indicates the radio option 5 GHz configurations.	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20</b>, <b>40</b>, <b>80</b> (MHz), or select <b>Auto</b> to set it automatically.</li> <li>• <b>Channel</b>—Select the channel to use for the a/n/c (5GHz) radio, or select <b>Auto</b> to set it automatically.</li> <li>• <b>Auto cell sizing</b>— Select this option to enable APs to share information on interference seen by each other and dynamically adjust their radio Tx power and Rx parameters to minimize interference. Selecting the <b>Enable</b> option, disables the <b>TX Power Adjustment</b> configuration.</li> </ul>

**TABLE 12** Access Point Edit Parameters (continued)

Field	Description	Your Action
		<ul style="list-style-type: none"> <li>• <b>TX Power Adjustment</b>—Select the required option.</li> </ul> <p><b>NOTE</b> If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p> <ul style="list-style-type: none"> <li>• <b>WLAN Group</b>—Select the WLAN group to which this AP belongs.</li> <li>• <b>WLAN Services</b>—Select the check box to enable WLAN services in this radio.</li> </ul>
<b>AP Configuration &gt; AP SNMP Options</b>		
<b>Override zone configuration</b>	Allows you to override the existing zone configuration	Select the check box
<b>Enable AP SNMP</b>	Enables you to configure SNMP settings.	Select the check box
<b>SNMPv2 Agent</b>	Allows you to add users to SNMPv2 Agent.	Click <b>Create</b> and enter <b>Community</b> . <ol style="list-style-type: none"> <li>1. Select the required <b>Privilege</b>. If you select <b>Notification</b> enter the <b>Target IP</b>.</li> <li>2. Click <b>OK</b>.</li> </ol>
<b>SNMPv3 Agent</b>	Allows you to add users to SNMPv3 Agent.	Click <b>Create</b> and enter <b>User</b> . <ol style="list-style-type: none"> <li>1. Select the required <b>Authentication</b>.</li> <li>2. Enter the <b>Auth Pass Phrase</b>.</li> <li>3. Select the <b>Privacy</b> option.</li> <li>4. Select the required <b>Privilege</b>. If you select <b>Notification</b> select the option <b>Trap</b> or <b>Inform</b> and enter the <b>Target IP</b>.</li> <li>5. Click <b>OK</b>.</li> </ol>
<b>AP Configuration &gt; Model Specific Options</b>		
<b>Model Specific Control</b>	Indicates that the model overrides the AP settings.	Select the check box.
<b>USB Port</b>	Disables the USB port on the selected AP model.	Select the option. USB ports are enabled by default.
<b>Status LEDs</b>	Disable the status LED on the selected AP model.	Select the option.

**TABLE 12** Access Point Edit Parameters (continued)

Field	Description	Your Action
<b>LLDP</b>	Enables the Link Layer Discovery Protocol (LLDP) on the selected AP model.	Select the option and enter the following details: <ul style="list-style-type: none"> <li>• <b>Advertise Interval</b>—Enter the duration in seconds.</li> <li>• <b>Hold Time</b>—Enter the duration in seconds.</li> <li>• <b>Enable Management IP TLV</b>—Select the check box.</li> </ul>
<b>Cellular Radio Settings</b>	Indicates the settings you can configure for the cellular connection	Select the following options: <ul style="list-style-type: none"> <li>• <b>APN for Primary SIM</b>: type the name of the AP for the primary SIM</li> <li>• <b>APN for Secondary SIM</b>: type the name of the AP for the second SIM</li> <li>• <b>SIM Card Usage</b>: you can priorities the SIM card usage by selecting only one of them or both</li> <li>• <b>3G/4G Selection</b>: you can select either 3G or 4G internet speeds</li> <li>• <b>Data Roaming</b>: this can be enabled or disabled by moving the radio button</li> <li>• <b>WAN connection</b>: the AP can be connected to the WAN either through the Ethernet or cellular data, and only from the primary SIM card. The options available are: <ul style="list-style-type: none"> <li>- Ethernet primary with cellular failover - the AP is connected to the Ethernet if LTE fails</li> <li>- Cellular primary with Ethernet failover- the AP is connected to LTE if Ethernet connection fails.</li> <li>- Ethernet only</li> <li>- Cellular only</li> </ul> </li> </ul>
<b>PoE Operating Mode</b>	Allows you to operate using PoE mode.	Select the option.
<b>Port Settings</b>	Indicates the port settings.	Select the option and choose the required LAN option.
<b>AP Configuration &gt; Advanced Options</b>		
<b>Network Settings</b>	Determines the network settings.	Select the IPv4 Settings from the following: <ul style="list-style-type: none"> <li>• <b>Static</b>:Enter the <b>IP Address, Network Mask, Gateway, Primary DNS, Secondary DNS</b>.</li> <li>• <b>Dynamic</b></li> <li>• <b>Keep the AP's Setting</b></li> </ul>
<b>Smart Monitor</b>	Indicates AP interval check and retry threshold settings.	Select the required check boxes.
<b>Syslog Options</b>	Determines if external syslog server settings is applicable.	Select the required check boxes. For <b>Enable external syslog server</b> option, update the following information: <ul style="list-style-type: none"> <li>• <b>Server Address</b></li> <li>• <b>Port</b></li> </ul>

**TABLE 12** Access Point Edit Parameters (continued)

Field	Description	Your Action
		<ul style="list-style-type: none"> <li>• <b>Facility for Event</b></li> <li>• <b>Priority</b></li> </ul>
<b>Hotspot 2.0 version Profile</b>	Indicates the hotspot profile that you want to assign to the group.	<p>Select the required option or click <b>Create</b> and update the following details:</p> <ul style="list-style-type: none"> <li>• Enter the <b>Name</b>.</li> <li>• Enter the <b>Description</b>.</li> <li>• Enter the <b>Venue Names</b>.</li> <li>• Select the <b>Venue Category</b>.</li> <li>• Select the <b>Type</b>.</li> <li>• Enter the <b>WLAN Metrics</b>.</li> </ul>
<b>AP Management VLAN</b>	Indicates the AP management VLAN settings.	<p>Select the check box and choose the option.</p> <p><b>ATTENTION</b> For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.</p>
<b>Auto Channel Selection</b>	Indicates auto-channel settings.	Select the check box and choose the option.
<b>Client Admission Control</b>	Indicates the load thresholds on the AP at which it will stop accepting new clients.	<p>Select the check boxes and update the following details:</p> <ul style="list-style-type: none"> <li>• <b>Min Client Count</b></li> <li>• <b>Max Radio Load</b></li> <li>• <b>Min Client Throughput</b></li> </ul>
<b>Protection Mode</b>	Indicates the protection mode settings for the AP	<p>You can override the protection mode settings at 2.4 GHz, and select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>RTS/CTS (Request to Send/ Clear to Send flow control mechanism that allows receiver and the transmitter to alert each other to their state)</b></li> <li>• <b>CTS Only</b></li> </ul>
<b>Venue Code</b>	Indicates the venue code	You can choose to override this setting and type the code in the box provided.
<b>Recovery SSID</b>	Indicates the recovery SSID you can use	You can also <b>Enable Recovery SSID Broadcast</b> for the AP to broadcast the SSID so it can be visible during discovery.
<b>Direct Multicast</b>	Indicates the direction in which multicast traffic can be sent	You can configure the AP to multicast traffic from wired clients, wireless clients and from the network
<b>Swap Configuration</b>		
<b>Add Swap-In AP</b>	Allows to swap APs.	Select the check box and enter the <b>Swap-in AP MAC</b> details.

**NOTE**

You can also move the location of an AP or delete an AP. To do so, select the AP from the list and click **Move** or **Delete** as required.



# Managing Access Points

## Overview of Access Point Configuration

Once you have created registration rules and the AP zones to which joining access points can be assigned automatically, access points will be able to join or register with the controller automatically.

Whenever a new AP connects to the controller and before it gets approval, the AP registration is moved to "Pending" state determining there is communication between the AP and controller. Every time an unapproved AP attempts to register, a "AP reject" event is generated and can be exported to syslog server if there is one configured.

### NOTE

AP reject event is generated only once since subsequent events are suppressed to reduce resource usage.

After an access point registers successfully with the controller, you can update its configuration by following the steps described in this section.

## Viewing Managed Access Points

After an access point registers successfully with the controller, it appears on the Access Points page, along with other managed access points.

Follow these steps to view a list of managed access points.

1. Click **Access Points**, a list of access points that are being managed by the controller appears on the Access Points page. These are all the access points that belong to all management domains.

The list of managed access points displays details about each access point, including its:

- AP MAC address
- AP name
- Zone (AP zone)
- Model (AP model)
- AP firmware
- IP address (internal IP address)
- External IP address
- Provision Method
- Provision State
- Administrative Status
- Status
- Configuration Status
- Registered On (date the access point joined the controller network)
- Registration Details
- Registration State
- Actions (actions that you can perform)

#### NOTE

By default, the Access Points page displays 20 access points per page (although you have the option to display up to 250 access points per page). If the controller is managing more than 20 access points, the pagination links at the bottom of the page are active. Click these pagination links to view the succeeding pages on which the remaining access points are listed.

2. To view access points that belong to a particular administration domain, click the name of the administration domain in the domain tree (on the sidebar).

The page refreshes, and then displays all access points that belong to that management domain.

## Downloading the Support Log from an Access Point

If you are experiencing issues with an access point, Ruckus Support Team may request you to download the support log from the access point.

The support log contains important technical information that may help Ruckus Support Team troubleshoot the issue with the access point. Follow these steps to download the support log from an access point.

To download a support log from an AP:

- Select the AP and click **More > Download Support Log**. The following message appears: Do you want to open or save **SupportLog\_{random-string}.log**.

Save the file and use a text editor (for example, Notepad) to view the contents of the text file. Send the support log file to Ruckus Support Team, along with your support request.

## Provisioning and Swapping Access Points

The controller supports the provisioning and swapping of access points.

As an administrator you can:

- Upload a file containing list of AP and the pre-provisioned configuration data for each AP. The controller processes the file and provides details on regarding the import results (including a list of failed APs and failure reasons).
- Modify or delete pre-provisioning data if AP does not connect to the controller
- Monitor the status and stage of the pre-provisioned APs
- Manually lock or unlock APs
- Upload a file containing list of AP pairs for swapping. The controller processes the file and provide the detailed import result (including a list of failed APs and failure reasons).
- Manually enter the AP swap pair
- Delete the swap configuration if AP fails to contact the controller
- Monitor the status and stage of the swapping AP pairs
- Manually swap the APs

## Options for Provisioning and Swapping APs

The controller supports the provisioning and swapping of access points.

Use the following buttons on the AP List page to perform the AP provisioning and swapping.

- **Import Batch Provisioning APs:** Select this option to import the provisioning file. The controller displays the import results. Any errors that occur during the import process will be listed by the controller.
- **Export All Batch Provisioning APs:** Select this option to download a CSV file that lists all APs that have been provisioned. The exported CSV contains the following information:
  - AP MAC Address
  - Zone Name
  - Model
  - AP Name
  - Description
  - Location
  - GPS Coordinates
  - Logon ID
  - Password
  - Administrative State
  - IP Address
  - Network Mask
  - Gateway
  - Primary DNS
  - Secondary DNS
  - Serial Number
  - IPv6 Address
  - IPv6 Gateway
  - IPv6 Primary DNS
  - IPv6 Secondary DNS

### NOTE

The exported CSV file for all batch provisioned APs only contains pre-provisioned APs. It does not contain swapping APs or auto discovered APs.

If no APs have been pre-provisioned, you will still be able to export the CSV file but it will be empty (except for the column titles).

- **Import Swapping APs:** Manually trigger the swapping of two APs by clicking the swap action in the row. You can also edit the pre-provision configuration only if the AP does not connect to the controller. Click the AP MAC address to bring up the configuration edit form, and then select Pre-provision Configuration.
- **Export All Batch Swapping APs:** Select this option to download a CSV file that lists all APs that have been swapped. The exported CSV contains the following information:
  - Swap In AP MAC
  - Swap In AP Model
  - Swap Out AP MAC

### NOTE

The exported CSV file for batch swapping APs only contains swapping APs. It does not contain pre-provisioned APs or auto discovered APs.

## Understanding How Swapping Works

The following table lists how the controller handles swapping by detailing each stage. For example, you have entered swap configuration as Swap In: A and Swap out: B.

**TABLE 13** AP swapping stages

Stage	State A	Stage A	State B	Stage B
1. Enter data	Swapping	Not Registered	Approved	Waiting for swap in AP registration
2. AP register	Swapping	Waiting for swapping in	Approved	Waiting for swapping out
3. User swap	Approved	Swapped in	Swapping	Swapped out
4. Second swap	Swapping	Swapped out and waiting for swapping in	Approved	Swapped in and waiting for swapping out

## Editing Swap Configuration

The controller supports the swapping or replacement of a managed AP with a new AP of the same model. This feature is useful when you want to avoid service interruption because you need to replace an AP in the field.

By configuring the swap settings, you can easily and automatically export and apply the settings of the old AP to the new AP.

Follow these steps to configure the swap settings of an AP.

1. On the Access Points page, locate the access point whose swap configuration you want to update.
2. Click **Configure**, the Edit AP page appears.
3. Click the **Swap Configuration** tab.
4. Select the **Add Swap-In AP** check box.
5. Enter the **Swap-In AP MAC** address.
6. Click **OK**.

You have completed editing the swap configuration.

## Approving Mesh APs

You can approve mesh APs that join the network using wireless connection.

To approve mesh APs:

1. Go to the Access Points page. On the upper-right corner of the page, select the **Mesh** option from **View Mode**.  
The mesh APs are listed. The **Mesh Role** field, displays the status of the APs.

### NOTE

To view the list of APs pending for approval, click the **Unapproved APs** below the left pane.

2. From the list, select the AP which is not assigned to a Staging Zone and click **Approve**.  
The **Approve Mesh AP** form appears.
3. From the **AP Zone** drop-down, select the zone.
4. In **Last 4 digit of AP S/N**, enter the last four digit serial number of the AP.

- Click **Approve**, to manually approve the APs that join the network using Zero Touch Mesh (ZTM).

After approval, Zero Touch Mesh (ZTM) AP changes mesh role to “approved”, and the AP will show up in AP list for waiting AP join.

## Moving a Single Access Point to a Different AP Zone

Follow these steps to move a single access point from its current AP zone to a different one.

### NOTE

The AP that you move will inherit the configuration of the new AP zone.

- From the Access Points page, locate the access point that you want to move to a different AP zone.
- Click **Move**, the Select Destination AP Zone form appears.
- Select the AP zone to which you want to move the access point.
- Click **OK**.

You have completed moving an access point to a new AP zone.

## Monitoring Access Points

When you select an AP from the list, contextual tabs appear at the bottom of the page.

The following table helps you to understand the real-time information about the AP.

**TABLE 14** Access Point Monitoring Tabs

Tabs	Description
<b>General</b>	Displays group information
<b>Configuration</b>	Displays group configuration information.
<b>Health</b>	Displays historical health information.
<b>Traffic</b>	Displays historical traffic information.
<b>Alarm</b>	Displays alarm information.
<b>Event</b>	Displays event information.
<b>Clients</b>	Displays client information.
<b>Pool Stats</b>	Displays DHCP pool data.
<b>Stats Counter</b>	Displays AP statistics that can be exported to CSV format.

Additionally, you can select an AP and click **More** to perform the following operations as required:

- Select ALL** - Selects all the APs in the list.
- Deselect All** - Clears all selection from the list.
- Troubleshooting > Client Connection** - Connects to client devices and analyze network connection issues in real-time. See, [Troubleshooting Client Connections](#) on page 353
- Troubleshooting > Spectrum Analysis** - Troubleshoots issues remotely, identify sources of interferences within the network and allow administrators access to the RF health of the network environment. See, [Troubleshooting through Spectrum Analysis](#) on page 355
- Restart** - Restarts an access point remotely from the web interface.

- **Lock** - Disables all WLAN services on the AP and disconnect all wireless users associated with those WLAN services temporarily.
- **Unlock** - Makes all WLAN services available.
- **Import Batch Provisioning APs** - Import the provisioning file. See, [Options for Provisioning and Swapping APs](#) on page 95
- **Import Swapping APs** - Manually trigger the swapping of two APs by clicking the swap action in the row. See, [Options for Provisioning and Swapping APs](#) on page 95
- **Export All Batch Provisioning APs** Downloads a CSV file that lists all APs that have been provisioned.. See, [Options for Provisioning and Swapping APs](#) on page 95
- **Export All Swapping APs** - Downloads a CSV file that lists all APs that have been swapped. See, [Options for Provisioning and Swapping APs](#) on page 95
- **Download Support Log** - Downloads support log.
- **Trigger AP Binary Log** - Triggers binary log for the selected AP.
- **Download CM Support Log** - Downloads Cable Modem support log.
- **Restart Cable Modem** - Restarts the cable modem. The AP will disconnect from the network for a short period. The AP will disconnect from the network for a short period.
- **Reset Cable Modem** - Resets the cable modem.
- **Reset Cable Modem to Factory Default** - Resets the cable modem to factory default settings.
- **Untag Critical APs** - Stating APs as non-critical. See, [Tagging Critical APs](#) on page 59.
- **Swap** - Swaps current AP to swap-in AP. See, [Editing Swap Configuration](#) on page 96
- **Switch Over Clusters** - Moves APs between clusters. See [Configuring AP Switchover](#) on page 101.
- **Approve** - Approves AP and completes registering. See, [Working with AP Registration Rules](#) on page 57.

## Viewing Neighbor APs in a Non-Mesh Zone


To view neighbor APs in a Non-Mesh zone:

1. From the Access Points page, select an AP from the list which is not assigned to a Staging Zone.
2. Scroll down to the bottom of the page. In the Neighbors area, click **Detect**.

The list of neighboring APs are displayed in the table.

**FIGURE 39** Neighbor APs for a Non-Mesh Zone

Neighbors								
<div> <div>Detect</div> <div>search table</div> <div></div> </div>								
AP name	MAC Address	Status	Model	Zone Name	IPv4 Address	IPv6 Address	Channel(2,4G)	Channel(5G)
RuckusAP	F0:3E:90:3F:7F:80	Flagged	C110	430-ZONE-IPV6	N/A	2008::186	8 (20MHz)	44 (80MHz)
RuckusAP	F8:E7:1E:0C:A8:C0	Flagged	R310	ZONE-AB	140.138.80.126	N/A	4 (20MHz)	153 (80MHz)
RuckusAP	1C:B9:C4:23:01:90	Online	H510	430-ZONE-IPV4	10.1.13.212	N/A	1 (20MHz)	161 (80MHz)
RuckusAP	F0:3E:90:3F:88:00	Online	R720	430-ZONE-IPV6	N/A	2008::226	11 (20MHz)	36 (80MHz)

3. To refresh the list, click the Refresh  button.

## Viewing LLDP Neighbors

You can view basic information, and detailed information about the LLDP neighbor of an AP from the controller interface.

1. From the **Access Points** page, select an AP from the list.
2. Scroll down to the bottom of the page. In the **LLDP Neighbors** area, click **Detect**.

The list of neighboring LLDP APs are displayed in the table.

**FIGURE 40** Neighbor LLDP APs for a Non-Mesh Zone

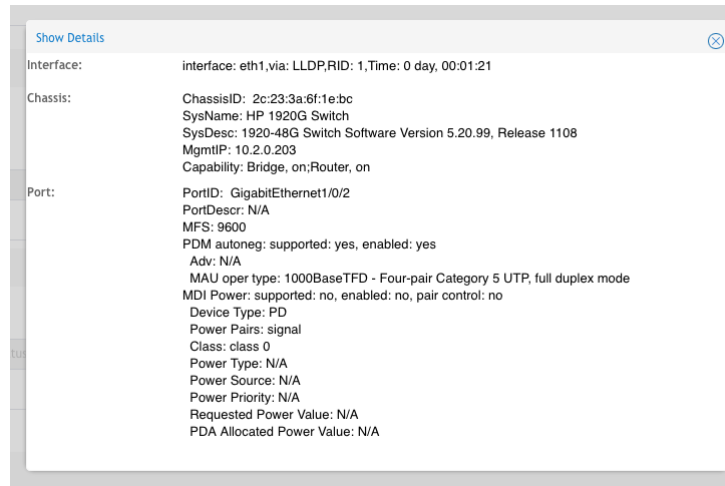
Interface	Time	System Name	System Description	System MAC	Mgmt IP	Capability	Port Description	Port ID	MDI Power Device Type	Power Class	PD Requested Power
eth1	0 day, 00:01:21	HP 1920G Switch	HP 1920G Switch	3c:23:3a:6f:1e:3c	10.2.0.203	Bridge, en_R	GigabitEthernet1/0/2		PD	class 0	N/A

You can view basic information about the LLDP AP neighbor such as:

- **Interface:** displays the interface on the AP from which the LLDP neighbor is detected
- **Time:** displays the matching time output in current LLDP command
- **System Name:** displays the name of the system such as a switch or router
- **System Description:** displays a short description about the system
- **Chassis ID:** displays the chassis ID of the system
- **Mgmt IP:** displays the management IP address of the LLDP neighbor
- **Capability:** displays the capability of the LLDP neighbor such as Bridging or Routing capabilities
- **Port Description:** displays the port type and capacity such as Gigabit Ethernet port
- **Port ID:** displays the port ID
- **MDI Power Device Type:** indicates whether the device is a power sourcing equipment (PSE) or a powered device (PD). PSE is the source of the power, or the device that integrates the power onto the network. PD is the Ethernet device that requires power and is situated on the other end of the cable connected to the PSE.
- **Power Class:** displays the power-class of the device ranging from 0 to 4 (IEEE 802.3at power-classes).
- **PD Requested Power:** displays power (in watts) requested by the Powered Device
- **PSE Allocated Power:** displays power (in watts) allocated by the Power Sourcing Equipment to the Powered Device

3. Click **Show Details** to view detailed information about the LLDP AP neighbor such as the interface, chassis and ports.

**FIGURE 41** Additional LLDP AP Neighbor Details



4. To refresh the list, click the Refresh  button.

## Viewing AP Health Indicators

You can monitor the performance and connection failures of an AP from the Health tab page.

### Performance

- Latency - It is the measurement of average delay required to successfully deliver a Wi-Fi frame.
- Airtime Utilization - It is a measurement of airtime usage on the channel measuring the total percentage of airtime usage on the channel.
- Capacity - It is a measurement of potential data throughput based on recent airtime efficiency and the performance potential of the AP and its currently connected clients.


### Connection Failure

- Total - It is a measurement of unsuccessful connectivity attempts by clients.
- Authentication - It's a measurement of client connection attempts that failed at the 802.11 open authentication stage.
- Association - It is a measurement of client connection attempts that failed at the 802.11 association stage, which happens before user/device authentication.
- EAP - It is a measurement of client connection attempts that failed during an EAP exchange.
- RADIUS - It's a measurement of RADIUS exchange failures due to AAA client /server communication.
- DHCP - It's a measurement of failed IP address assignment to client devices.

To customize Health Performance settings:

1. From the Access Points page, select the required AP from the list.
2. Scroll Down and select the **Health** tab.



3. On the **Performance** bar, select the Setting  icon. The **Settings - Performance** pop-up appears. Customize the following:
  - **Show top**: Enter the number of performance failures to be displayed.
  - **Display Channel Change**: Select the required options. For example: **2.4G, 5G**.
  - **AP**: Choose how the AP details must be displayed. For example: **Name, MAC, IP**.
4. Click **OK**.

Performance details of the AP are listed according to the settings.

## Viewing AP Traffic Indicators

You can monitor the performance and connection failures of an AP from the Traffic tab page.


You can view:

- Historical or Real Time traffic
- WLAN traffic

Traffic indicators can be filtered based on the following parameters:

- Rate, Packets, Rate
- Total, Downlink-From AP to client, Uplink-From client to AP

To customize Traffic settings:

1. From the Access Points page, select the required AP from the list.
2. Scroll Down and select the **Traffic** tab.
3. On the respective section bar, select the Settings  icon. The **Settings - Clients** pop-up appears. Customize the following:
  - **Type**: Choose the Display format. For example: **Chart, Table**.
  - **Display Channel Change**: Select the required options. For example: **2.4G, 5G**.

### NOTE

This field is available only for the Clients Tab when you select the Display Type as Chart.

- **AP**: Choose the AP display format. For example: **Name, MAC, IP**.
4. Click **OK**.

Performance details of the AP are listed according to the settings.

## Configuring AP Switchover

AP switchover is moving APs between clusters, not confined to clusters that enable cluster redundancy. For normal clusters, you can switchover APs with firmware later or equal to R5.0, no matter it is in Staging Zone or Non-staging Zone. But for a standby cluster in cluster redundancy, APs in Staging Zone can only be moved to another cluster by switchover.

To configure APs to switchover clusters:

1. From the **Access Points** page, select the AP from the list.
2. Click **More** and select **Switch Over Clusters**.

The specify **Destination Cluster** dialog box appears.

3. Enter the **Control IP** or **FQDN**
4. Click **OK**. A confirmation dialog to trigger the AP switchover appears.
5. Click **Yes**.

You configured AP switchover.

## Configuring Packet Capture for APs

User can enable packet streaming feature on both wired and wireless interfaces on specified APs using web UI. You must enable this feature on a per-AP basis. It allows multiple users to execute AP packet capturing, but only a single AP can execute one capturing task at a time. For a single user can capture tasks in multiple APs, but batch operation is not allowed. Only users with full access permission can execute AP packet capturing.

To configure Packet Capture:

1. From the **Access Points** page, select the AP from the list.
2. Click **More** and select **Packet Capture**.  
The **Packet Capture** dialog box appears.
3. Configure the **Capture Mode**:
  - **Stream to Wireshark**
    - **Capture Interface** Select the required wireless or wired interface
      - › For 2.4 GHz/5 GHz, update the following details:  
**Wireshark station IP**: Enter the IP address.  
**MAC Address Filter**: Enter the MAC address.  
**Frame Type Filter**: Click the required options from Management, Control, and Data.
      - › For Wired Interface, update the following details:  
**Wireshark station IP**: Enter the IP address.  
**LAN Port**: Choose the LAN port.
  - **Save to file**
    - **Capture Interface** Select the required wireless or wired interface
      - › For 2.4 GHz/5 GHz, update the following details:  
**MAC Address Filter**: Enter the MAC address.  
**Frame Type Filter**: Click the required options from Management, Control, and Data.
      - › For Wired Interface, update the following details:  
**MAC Address Filter**: Enter the MAC address.  
**LAN Port**: Choose the LAN port.
4. Click **Start**.

## Multi-Tunnel Support for Access Points

In prior Ruckus solutions, APs could only support a single tunnel to a data plane, as well as a local break out. In this release, we're adding support for Ruckus APs to provide multiple simultaneous tunnels to different data planes.

For 5.0, the AP will support a single Ruckus GRE tunnel (with or without encryption) while supporting up to three SoftGRE (without encryption) tunnels, in addition to local breakout option. The tunneling will be based on SSID configurations on the AP.

This feature is designed to help in common MSP (Managed Service Provider) use cases, where each of the MSP's customer will have the possibility to get its own tunnel directly to the data center.

Before configuring multiple tunnels, consider the following configuration prerequisites:

- Ensure that there is a reachable SoftGRE gateway and also verify that there is network connectivity.
- Ensure that the zone is configured with correct SoftGRE gateway information.
- Verify that the SSID to SoftGRE tunnel mapping is correct.
- Verify the SoftGRE tunnel configuration and run time status using the command **get softgre tunnel-index**. The tunnel index can be 1, 2, or 3.

## Configuring Multiple Tunnels for Zone Templates

Multiple tunnels can be configured for a zone template.

Perform the following steps to select a tunnel profile for a zone template.

1. From the application, go to **System > Templates > Zone Templates**.
2. Click **Create**.

The **Create Zone Template** form appears.

**FIGURE 42** Configuring a Ruckus GRE Profile

### Create Zone Template

The screenshot shows the 'Create Zone Template' form. The 'AP GRE Tunnel Options' section is expanded, showing the following fields:

- Ruckus GRE Profile:** A dropdown menu with 'Default Tunnel Profile' selected, and '+' and '-' icons.
- SoftGRE Profiles:** A table with columns 'Name' and 'AAA Affinity'. There is a 'Select' button above the table.
- IPsec Profiles:** A table with a column 'Name'. There is a 'Select' button above the table.

The form also has 'Radio Options' at the top and 'Syslog Options' at the bottom, both with expand/collapse arrows.

3. Navigate to the **AP GRE Tunnel Options** section.
4. For the **Ruckus GRE Profile** select a profile from the drop-down menu.  
Click the **+** icon to create a new Ruckus GRE profile.

5. Click the **Select** checkbox above the SoftGRE Profiles box.

A form appears from which you can select the SoftGRE profiles that you want to apply to the zone. The profiles you can select are displayed under **Available Profiles**. Select the profile and click the -> icon to choose it. The profile is now listed under the **Selected Profiles** area.

**FIGURE 43** SoftGRE Profiles Form

## Select Soft GRE Tunnel Profiles

You can also click the + icon to create a new SoftGRE profile.

If you wish to deselect a profile, select it and click the <- icon. The profile will be moved back to the **Available Profiles** area and will not be applied to that zone.

6. Click **OK**.

Your multiple tunnel configuration for the zone template is saved.

## Configuring Multiple Tunnels for Zone

Multiple tunnels can be configured for a zone.

To configure the tunnel types for an AP zone, perform the following steps.

1. From the dashboard, go to **Access Points**.

2. From the System tree, select the location where you want to create the zone. For example, System or Domain. Click + icon.

The **Create Group** page appears.

3. Under **Type**, select **Zone**.
4. Navigate to the **AP GRE Tunnel** section.
5. For the **Ruckus GRE Profile** select a profile from the drop-down menu.  
Click the + icon to create a new Ruckus GRE profile.
6. Click the **Select** checkbox above the SoftGRE Profiles box.

A form appears from which you can select the SoftGRE profiles that you want to apply to the zone. The profiles you can select are displayed under **Available Profiles**. Select the profile and click the -> icon to choose it. The profile is now listed under the **Selected Profiles** area.

**FIGURE 44** SoftGRE Profiles Form

## Select Soft GRE Tunnel Profiles

You can also click the + icon to create a new SoftGRE profile.

If you wish to deselect a profile, select it and click the <- icon. The profile will be moved back to the **Available Profiles** area and will not be applied to that zone.

7. Click **OK**.

Your multiple tunnel configuration for the zone is saved.

## Configuring Multiple Tunnels in WLANs

In WLANs where there is an option to tunnel the traffic, you can choose the tunneling profile the WLAN can use.

Perform the following steps to enable tunneling in WLANs.

1. In the Wireless LANs page, from the **System tree hierarchy**, select the **Zone** where you want to create a WLAN.
2. Click **Create**.

The **Create WLAN Configuration** page appears.

**FIGURE 45** Tunneling Options while Creating a WLAN Configuration

### Create WLAN Configuration

The screenshot shows the 'Create WLAN Configuration' page. At the top, there is a 'Zone' dropdown menu set to 'Z shol\_zone' and a 'WLAN Group' dropdown menu set to 'default' with a '+ Create' button. Below these are three main sections: 'Authentication Options', 'Encryption Options', and 'Data Plane Options'. The 'Authentication Options' section includes 'Authentication Type' with radio buttons for 'Standard usage (For most regular wireless networks)', 'Hotspot (WISPr)', 'Guest Access', 'Web Authentication', 'Hotspot 2.0 Access', 'Hotspot 2.0 Onboarding', and 'WeChat'. It also includes a 'Method' section with radio buttons for 'Open', '802.1X EAP', 'MAC Address', and '802.1X & MAC'. The 'Encryption Options' section includes a 'Method' section with radio buttons for 'WPA2', 'WPA-Mixed', 'WEP-64 (40 bits)', 'WEP-128 (104 bits)', and 'None'. The 'Data Plane Options' section includes an 'Access Network' section with a checked checkbox for 'Tunnel WLAN traffic', a 'Core Network' section with radio buttons for 'Bridge' and 'L2oGRE', and a 'Tunnel Profile' dropdown menu set to 'SoftGre1'.

3. In the **Data Plane Options** section, and next to **Access Network:** text check the **Tunnel WLAN traffic** box to tunnel the data traffic to a central data plane. Clear the check box if you want APs to perform local breakouts.
4. Next to the **Core Network:** option, click the radio button for Bridge.
5. Next to the **Tunnel Profile:** option, use the drop-down menu to select one of the tunnelling profiles—either **SoftGRE** or **Ruckus GRE**.

You have successfully configured the tunneling option to forward traffic in a WLAN.

# Viewing the System Cluster Overview

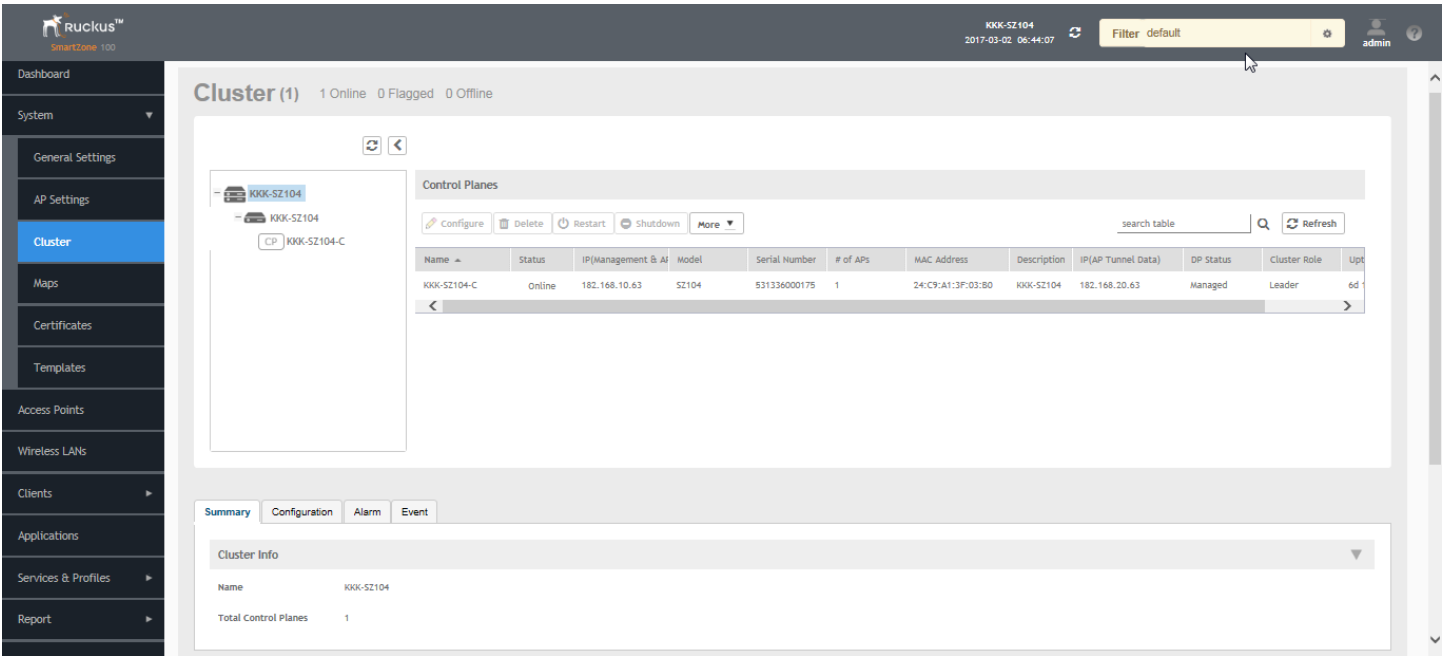
- Control Planes and Data Planes..... 107
- Interface and Routing..... 108
- Displaying the Chassis View of Cluster Nodes..... 109
- Configuring the Control Plane..... 110
- Monitoring Cluster Settings..... 114
- Creating DP Zone Affinity Profile..... 115
- Enabling Flexi VPN..... 116
- Enabling L3 Roaming Criteria for DP..... 117

The system cluster overview provides summary information of the controller cluster.

To view the cluster settings:

- From the left pane of the application, click **System > Cluster**. The **Cluster** page appears.

FIGURE 46 System Cluster Overview - SZ100



## Control Planes and Data Planes

Control planes and data planes are used to control traffic.

The control plane manages and exchanges routing table information. The control plane packets are processed by the router to update the routing table information. The data plane forwards the traffic along the path according to the logic of the control plane.

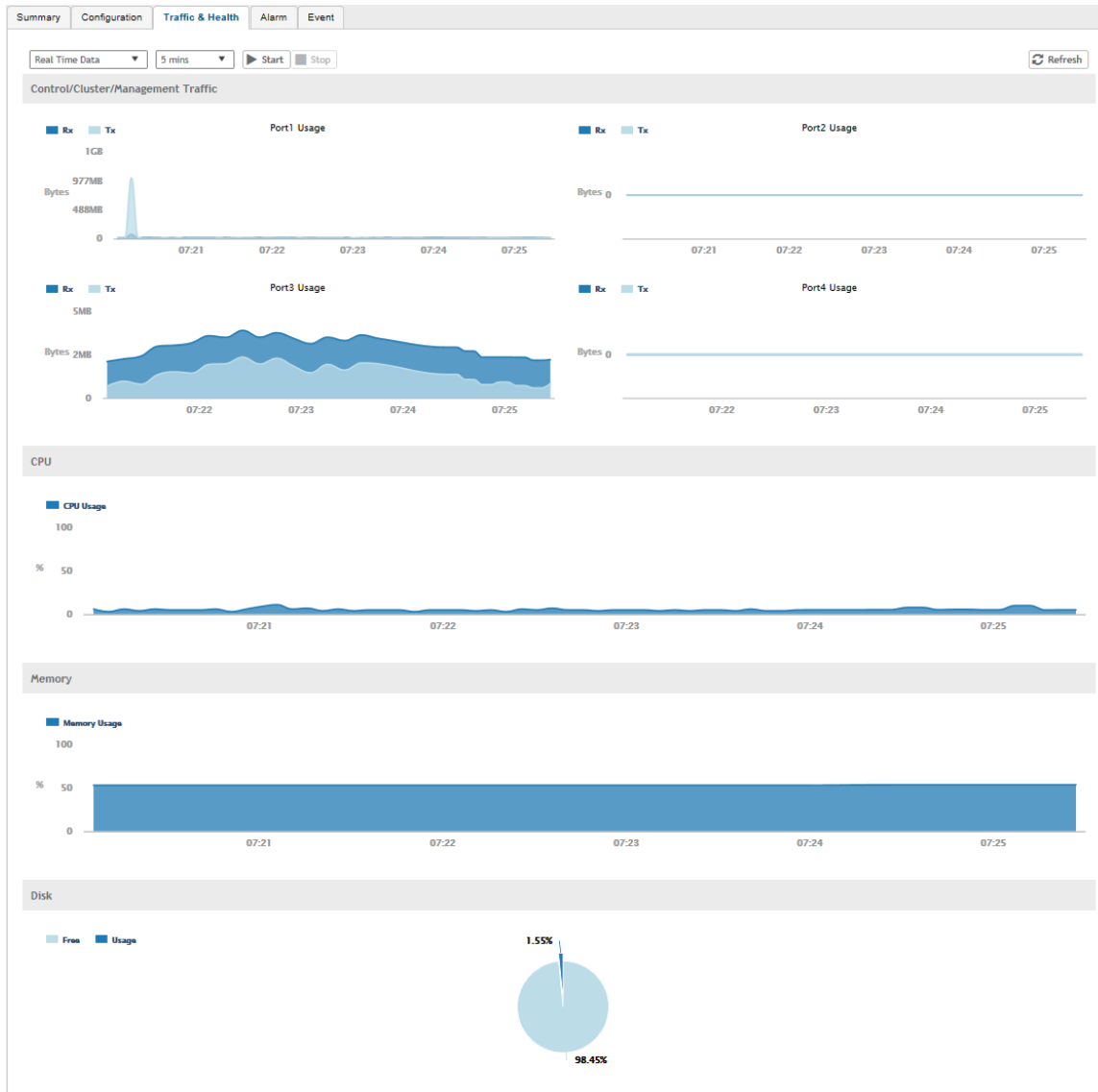
You can view historical and real time traffic of the nodes. To view the traffic:

- From the Controller page, select the node.

2. Click the Traffic & Health from the lower end of the page.
3. Select the option from the drop-down:
  - **Historical Data**, and enter the time frame for which you want.
  - **Real Time Data**, enter the duration in minutes and click **Start**.

The Cluster Node Traffic and Health tab displays as shown in the diagram below.

**FIGURE 47** Cluster Node Traffic and Health.



## Interface and Routing

To configure a cluster node, you must define interface and routing information.

### Interface



You can only create one user defined interface, and it must be for a hotspot service and must use the control interface as its physical interface. The control plane and the UDI must be on different subnets. If the control plane and UDI are on the same subnet, and assigned with the same IP address, APs will be unable to communicate with the control plane. If the control plane and UDI are on the same subnet and assigned different IP addresses, hotspot clients will not be redirected to the logon URL for user authentication.

**NOTE**

The user defined interface (UDI) is unavailable in Virtual SmartZone (High-Scale and Essentials).

**Static Routing**

Static routing is used to manually configure routing entry. Static routes are fixed and do not change if the network is changed or reconfigured. Static routing are usually used to maximize efficiency and to provide backups in the event that dynamic routing information fails to be exchanged.

## Displaying the Chassis View of Cluster Nodes

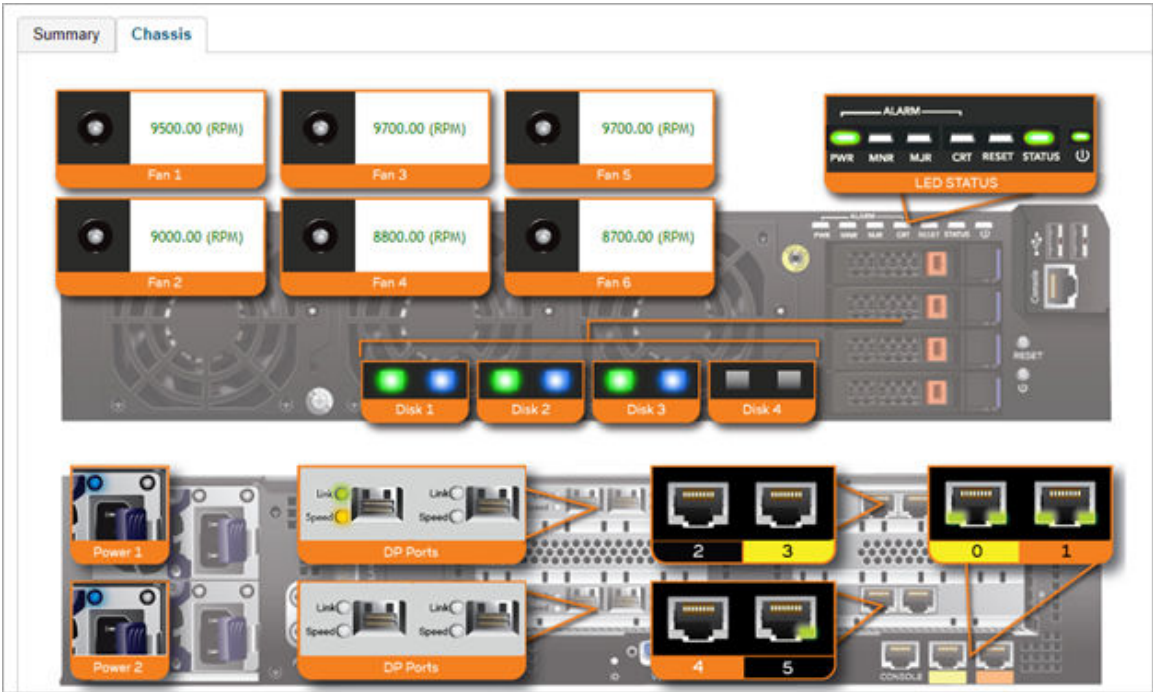
The chassis view provides a graphical representation of the control panel (on the front panel of the controller), including the LEDs.

Use the LEDs to check the status of the ports and power supplies on the controller. Fan status is also displayed on the chassis view.

To view the chassis of the cluster node:

1. From the Cluster page, select the node.
2. From the lower-left side of the page, click the **Chassis** tab to display the Chassis tab information.

FIGURE 48 Cluster Node Chassis



- port 1 and 2 are management ports
- ports (3-4 or 3-6) are data ports

## Configuring the Control Plane

Control Plane configuration includes defining the physical interface, user defined interface and static routes.

To configure a control plane:

1. Go to **System > Cluster > Control Planes**.
2. Select the control plane from the list and click **Configure**. The Edit Control Plane Network Settings form appears.
3. Configure the settings as explained in the table below.
4. Click **OK**.

**NOTE**

You must configure the **Control** interface, **IPv4 Cluster** interface, and **Management** interface to be on three different subnets. Failure to do so may result in loss of access to the web interface or failure of system functions and services.

TABLE 15 Configuring Control Plane

Field	Description	Your Action
<b>Physical Interfaces</b>		

**TABLE 15** Configuring Control Plane (continued)

Field	Description	Your Action
<b>IPv4-Control Interface</b>	Indicates the management and IP control settings.	<p>Select the <b>IP Mode</b>:</p> <ul style="list-style-type: none"> <li>• <b>Static (recommended)</b>—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> <li>- Enter the <b>IP Address</b>.</li> <li>- Enter <b>Subnet Mask</b>.</li> <li>- Enter the <b>Gateway</b> router address.</li> <li>- Enter <b>Control NAT IP</b> address.</li> </ul> </li> <li>• <b>DHCP</b>—To automatically obtain an IP address from a DHCP server on the network. <ul style="list-style-type: none"> <li>- Enter <b>Control NAT IP</b>.</li> </ul> </li> </ul>
<b>IPv4-Cluster Interface</b>	Indicates the IPv4 cluster interface settings	<p>Select the <b>IP Mode</b>:</p> <ul style="list-style-type: none"> <li>• <b>Static (recommended)</b>—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> <li>- Enter the <b>IP Address</b>.</li> <li>- Enter <b>Subnet Mask</b>.</li> <li>- Enter the <b>Gateway</b> router address.</li> </ul> </li> <li>• <b>DHCP</b>—To automatically obtain an IP address from a DHCP server on the network.</li> </ul>
<b>IPv4-Management Interface</b>	Indicates the IPv4 management interface settings	<p>Select the <b>IP Mode</b>:</p> <ul style="list-style-type: none"> <li>• <b>Static (recommended)</b>—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> <li>- Enter the <b>IP Address</b>.</li> <li>- Enter <b>Subnet Mask</b>.</li> <li>- Enter the <b>Gateway</b> router address.</li> </ul> </li> <li>• <b>DHCP</b>—To automatically obtain an IP address from a DHCP server on the network.</li> </ul>
<b>IPv6-Control Interface</b>	Indicates the IPv6 control interface settings	<p>Select the <b>IP Mode</b>:</p> <ul style="list-style-type: none"> <li>• <b>Static (recommended)</b>—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> <li>- Enter the IPv6 <b>IP Address</b> (global only) with a prefix length (for example, 1234::5678:0:C12/123) is required. Link-local addresses are unsupported.</li> <li>- Enter the IPv6 <b>Gateway</b> address (global or link-local) without a prefix length. For example, 1234::5678:0:C12 (global address without a prefix length) and fe80::5678:0:C12 (link-local address without a prefix length).</li> </ul> </li> </ul>

**TABLE 15** Configuring Control Plane (continued)

Field	Description	Your Action
		<ul style="list-style-type: none"> <li>• <b>Auto</b>—To automatically obtain an IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network.</li> </ul>
<b>IPv6-Management Interface</b>	Indicates the IPv6 management interface settings	<p>Select the <b>IP Mode</b>:</p> <ul style="list-style-type: none"> <li>• <b>Static</b> (<i>recommended</i>)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> <li>– Enter the IPv6 <b>IP Address</b> (global only) with a prefix length (for example, 1234::5678:0:C12/123) is required. Link-local addresses are unsupported.</li> <li>– Enter the IPv6 <b>Gateway</b> address (global or link-local) without a prefix length. For example, 1234::5678:0:C12 (global address without a prefix length) and fe80::5678:0:C12 (link-local address without a prefix length).</li> </ul> </li> <li>• <b>Auto</b>—To automatically obtain an IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network.</li> </ul>
<b>Access &amp; Core Separation</b>	Indicates that the management interface (core side) to be the system default gateway and the control interface (access side) to be used only for access traffic.	Select the <b>Enable</b> check box.
<b>IPv4 Default Gateway &amp; DNS</b>	<p>Indicates the IPv4 gateway that you want to use - Control, Cluster, and Management.</p> <p><b>NOTE</b> When <b>Access &amp; Core Separation</b> is enabled, the <b>Default Gateway</b> field is hidden.</p>	<ol style="list-style-type: none"> <li><b>Default Gateway</b>—Choose the Interface for which you want to assign the default gateway setting.</li> <li><b>Primary DNS Server</b>—Enter the server details.</li> <li><b>Secondary DNS Server</b>—Enter the server details.</li> </ol>
<b>IPv6 Default Gateway &amp; DNS</b>	<p>Indicates the IPv6 gateway that you want to use - Control, Cluster, and Management.</p> <p><b>NOTE</b> When <b>Access &amp; Core Separation</b> is enabled, the <b>Default Gateway</b> field is hidden.</p>	<ol style="list-style-type: none"> <li><b>Default Gateway</b>—Choose the Interface for which you want to assign the default gateway setting.</li> <li><b>Primary DNS Server</b>—Enter the server details.</li> <li><b>Secondary DNS Server</b>—Enter the server details.</li> </ol>
<b>User Defined Interfaces</b> <p><b>NOTE</b> The control plane and the UDI must be on different subnets. If the control plane and UDI are on the same subnet, and assigned the same IP address, APs will be unable to communicate with the control plane. If the control plane and UDI are on the same subnet and assigned different IP addresses, hotspot clients will not be redirected to the logon URL for user authentication.</p>		
<b>Name</b>	Indicates the name of the interface.	Enter a name.

**TABLE 15** Configuring Control Plane (continued)

Field	Description	Your Action
<b>Physical Interfaces</b>	Indicates the physical interface.	Select <b>Control Interface</b> .
<b>Service</b>	Indicates the service.	Select <b>Hotspot</b> , the hotspot must use the control interface as its physical interface.
<b>IP Address</b>	Indicates the IP address that you want to assign to this interface.	Enter the IP address.
<b>Subnet Mask</b>	Indicates the subnet mask for the IP address.	Enter the subnet mask.
<b>Gateway</b>	Indicates the IP address of the gateway router.	Enter the gateway IP address.
<b>VLAN</b>	Indicates the VLAN ID that you want to assign to this interface.	Enter the VLAN ID.
<b>Add</b>	Adds the interface settings.	Click <b>Add</b> .
<b>Static Routes</b>		
<b>Network Address</b>	Indicates the destination IP address of this route.	Enter the IP address.
<b>Subnet Mask</b>	Indicates a subnet mask for the IP address.	Enter the subnet mask.
<b>Gateway</b>	Indicates the IP address of the gateway router.	Enter the IP address of the gateway router.
<b>Interface</b>	Indicates the physical interface to use for this route.	Select the interface.
<b>Metric</b>	Represents the number of routers between the network and the destination.	Enter the number of routers.
<b>Add</b>	Adds the static route settings.	Click <b>Add</b> .

**NOTE**

You can also delete or restart a control plane. To do so, select the control plane from the list and click **Delete** or **Restart** respectively.

## Rebalancing APs

AP rebalancing helps distribute the AP load across nodes that exist within a cluster.

When a multi-node cluster is upgraded, the node that reboots the last typically does not have any APs associated with it.

When you click **Rebalance APs**, the following process is triggered:

1. The controller calculates the average AP count based on the number of available control planes and data planes.
2. The controller calculates how many APs and which specific APs must be moved to other nodes to distribute the AP load.
3. The controller regenerates the AP configuration settings based on the calculation result.
4. The web interface displays a message to inform the administrator that the controller has completed its calculations for rebalancing APs.
5. Each AP that needs to be moved to a different node retrieves the updated AP configuration from the controller, reads the control planes and data planes to which it must connect, and then connects to them.

When the AP rebalancing process is complete, which typically takes 15 minutes, one of the following events is generated:

- **Event 770: Generate ApConfig for plane load rebalance succeeded.**

- **Event 771: Generate ApConfig for plane load rebalance failed.**

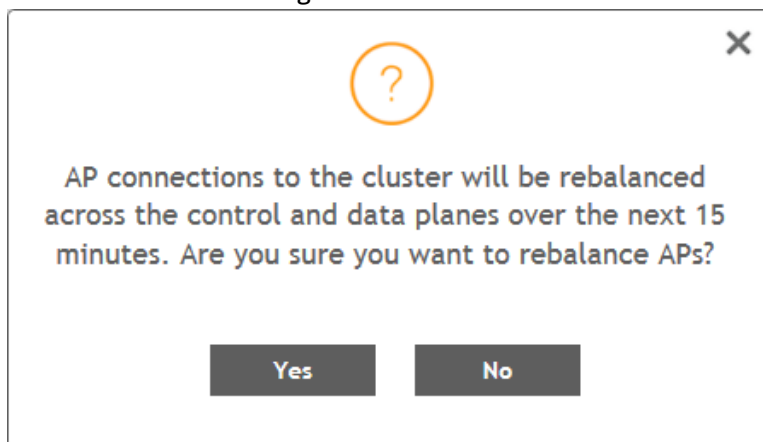
**NOTE**

- APs may recreate the Ruckus-GRE tunnel to a different data plane.
- Devices associated with an AP that uses the Ruckus-GRE tunnel may temporarily lose network connection for a short period of time (typically, around five minutes) during the AP rebalancing process.
- When node affinity is enabled, AP rebalancing is disallowed on those nodes.
- When data plane grouping is enabled, AP rebalancing is disallowed on those data planes.
- AP rebalancing only supports APs running release 3.2 firmware. APs running on legacy firmware will not be rebalanced.

To rebalance APs across the nodes:

1. Go to **System > Cluster > Control Planes > More > Rebalance APs**.

**FIGURE 49** AP Rebalancing Form



2. Click **Yes**, the controller rebalances AP connections across the nodes over the next 15 minutes.

**NOTE**

If you want to repeat this procedure, you must wait 30 minutes before the controller will allow you to rebalance APs again.

## Monitoring Cluster Settings

This section provides information on how to view the status of the cluster settings.

You can select the following tabs for more information:

- **Summary**—Details such as Name, model, IP details, memory usage, disk usage.
- **Network Settings**—Details such as control interface, cluster interface, management interface, DNS Server, Routes.
- **Configuration**—Details such as physical interfaces, User defined interfaces, Static Routes Interface.
- **Traffic & Health**—Details such as CPU usage, memory usage, disk usage, interface, port usage.
- **Alarm**—Details of alarms generated. You can Clear Alarm or Acknowledge Alarm that are generated.
- **Event**—Details of events that are generated.

## Clearing or Acknowledging Alarms

You can clear or acknowledge an alarm.

To Clear an alarm:

1. From the **Alarm** tab, select the alarm from the list.
2. Click **Clear Alarm**, the Clear Alarm form appears.
3. Enter a comment and click **Apply**.


To acknowledge an alarm:

1. From the **Alarm** tab, select the alarm from the list.
2. Click **Acknowledge Alarm**, the Are you sure you want to acknowledge the selected form appears.
3. Click **Yes**.

## Filtering Events

You can view a list of events by severity or date and time.

To apply filters:

1. From the **Event** tab, select the  icon. The Apply Filters form appears.
2. Select any or both the following criteria:
  - **Severity**: Select the severity level by which you want to filter the list of events.
  - **Date and Time**: Select the events by their **Start** and **End** dates.

### NOTE

You can filter events that generated in the last seven days.

3. Click **OK**, all the events that meet the filter criteria are displayed on the Event page.

## Creating DP Zone Affinity Profile

The vSZ-D version in the same zone affinity profile must be the same for consistent AP/DP functioning.

### NOTE

This feature is supported only for vSZ-E and vSZ-H platforms.

To create DP zone affinity profile:

1. Go to **System > Cluster > DP Zone Affinity**.
2. Click **Create**, the Create New DP Zone Affinity form appears.
3. Enter a **Name** and **Description** for the zone affinity.
4. Click **Add**, the Add DP form appears. Profiles with only one or two Data Planes are listed in the drop-down.
5. Choose a Data Plane from the drop-down and click **OK**.
6. Click **OK**.

You have created a DP zone affinity profile.

**NOTE**

You can also edit or delete a zone affinity profile. To do so, select the profile from the list and click **Configure** or **Delete** as respectively.

## Verifying DP and Profile Version Match

From the list, the **DP(s) Version Match** column indicates **Yes** if the DP Profile and the DP have the same version and **No** if they have a different version. You can click the **DPs** tab to check the version of the DP.

## Verifying Zone and Profile Version Match

The Zone version must match the version of the Zone Affinity Profile. Click the Zones tab to view the list of zones and its versions. Click the **Show version mismatched zone(s) only** button to view zones with version difference.

## Enabling Flexi VPN

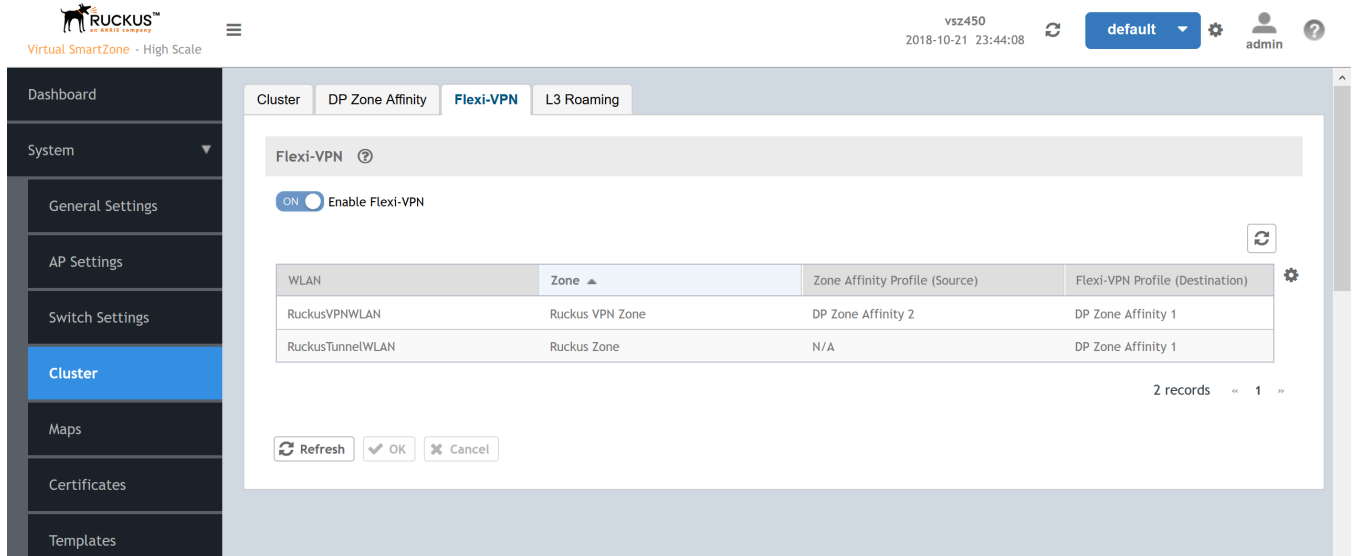
You can enable Flexi-VPN and limit the network resources that a UE can access. Flexi-VPN allows an administrator to customize the network topology, and is thereby able to control the network resources accessible to the end-user. This feature is only supported on vSZ-E and vSZ-H, and is enabled by purchasing the Flexi-VPN license.

1. Go to **System > Cluster**.



2. Select the **Flexi-VPN** tab.  
The page with Flexi-VPN settings appears.

**FIGURE 50** Enabling Flexi-VPN



**NOTE**

The Flexi-VPN option is available only if the Access-VLAN ID is configured in manual mode, and when VLAN Pooling, Dynamic VLAN and Core Network VLAN options, and Tunnel NAT are disabled.

**NOTE**

You can only apply 1024 WLAN IDs to a Flexi-VPN profile.

Flexi-VPN supports IPv4 addressing formats and Ruckus GRE tunnel protocol. It does not support IPv6 addressing formats.

3. Select a virtual data plane for which you want to enable the Flexi-VPN feature, and then select the **Enable Flexi-VPN** check-box.

The following information is displayed:

- **WLAN:** displays the name of the WLAN
- **Zone:** displays the name of the zone
- **Zone Affinity Profile:** displays the name of the source data plane from which tunneled traffic starts
- **Flexi-VPN Profile:** displays the name of the destination data plane to where the tunneled traffic terminates

4. Click **OK**.

You have successfully enabled the Flexi-VPN feature on the selected vDP.

## Enabling L3 Roaming Criteria for DP

Using the layer 3 roaming feature, clients can roam across APs in the network (from one data plane to another data plane). This is typically required when the number of clients in the network increases and clients have to roam from a network that they were connected to, to another WLAN network with similar access settings. This feature enables seamless roaming and ensures session continuity between the client and the network.

#### NOTE

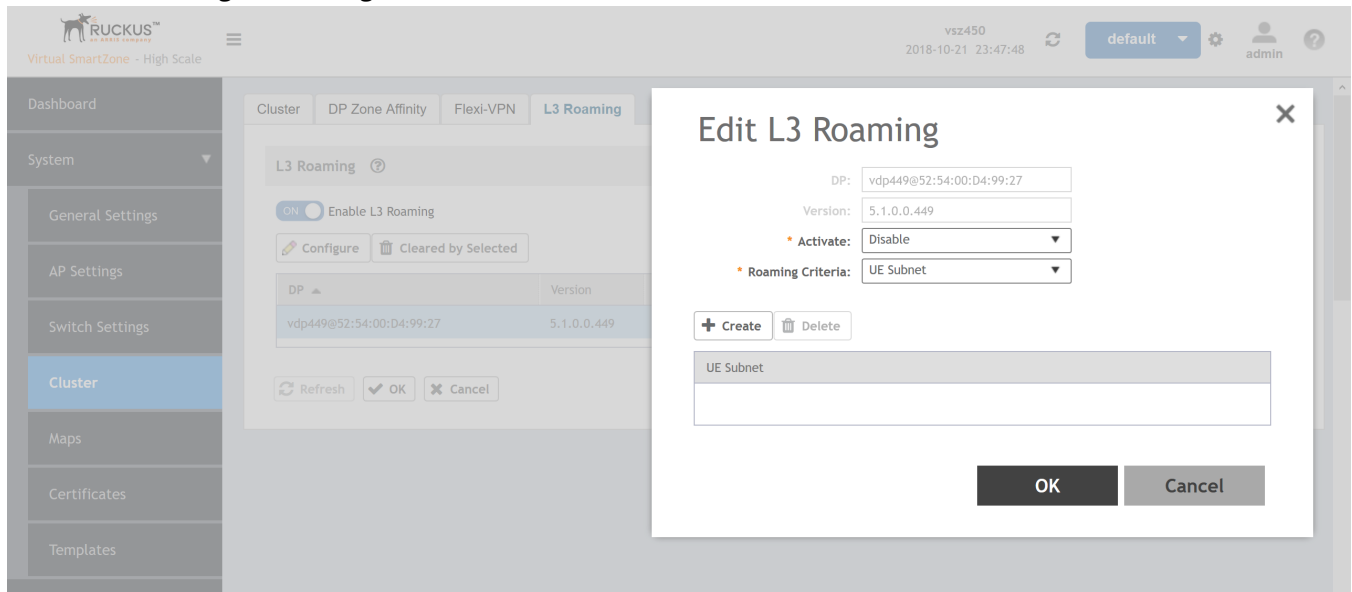
L3 roaming is only supported on vSZ-H and vSZ-E.

You can configure the roaming criteria for a DP so that it uses one of these two options - UE subnet or WLAN VLAN to access another DP to connect to, within a network. Before this, you must ensure that the L3 roaming feature is enabled in the DP.

1. Go to **System > Cluster**.
2. Select the **L3 Roaming** tab.

The page with L3 Roaming settings appears.

**FIGURE 51** Enabling L3 Roaming



3. Select the **Enable L3 Roaming** check-box.
4. You can edit the L3 Roaming settings by clicking **Configure**.

The **Edit L3 Roaming** page appears.

5. From **Activate**, you can enable the feature for the vSZ-D by selecting Enable or Disable from the drop-down menu.
6. From the **Roaming Criteria** drop-down, select one of these options to define the data format to establish connection between DPs: UE Subnet or WLAN VLAN.
7. Click **OK**.

You have successfully enabled L3 roaming, and also set the roaming criteria based on which DPs would connect within the network.

#### NOTE

A fresh controller software installation or upgrade from a version that does not support L3 roaming resets the L3 roaming configuration and it remains disabled. You must enable L3 roaming on a DP again.

# Certificates

---

• Importing New Certificates.....	119
• Assigning Certificates to Services.....	120
• Generating Certificate Signing Request (CSR).....	120
• Managing AP Certificates.....	121
• Importing Trusted CA Certificates.....	123

All the security certificates that the controller uses for its web interface, AP portal, and hotspots are managed from a central storage.

By default, a Ruckus-signed SSL certificate (or security certificate) exists in the controller. However, because this default certificate is signed by Ruckus and is not recognized by most web browsers, a security warning appears whenever you connect to the web interface or users connect to the AP portal or a hotspot. To prevent these security warnings from appearing, you can import an SSL certificate that is issued by a recognized certificate authority.

If you are implementing Hotspot 2.0 on the network and you want to support anonymous authentication using OSU Server-Only Authenticated L2 Encryption Network (OSEN), you will need to import a trust root certificate, server or intermediate certificate and private key.

## Importing New Certificates

When you have an SSL certificate issued by an SSL certificate provider, you can import it into the controller and use it for HTTPS communication.

To complete this procedure, you will need the following:

- The signed server certificate
- The intermediate CA certificate (at least one)
- The private key file

### NOTE

The file size of each signed certificate and intermediate certificate must not exceed 8192 bytes. If a certificate exceeds 8192 bytes, you will be unable to import it into the controller.

Follow these steps to import a signed server certificate:

1. Copy the signed certificate file, intermediate CA certificate file, and private key file to a location (either on the local drive or a network share) that you can access from the controller web interface.
2. From the application select, **System > Certificates > Installed Certs**.
3. Click **Import**, the Import Certificate form appears.
4. Enter a **Name** to identify the certificate.
5. Enter a **Description** about the certificate.
6. For **Service Certificates**, click **Browse** and select the location where the certificate is saved.
7. For **Intermediate CA certificates**, click **Browse** and select the location where the certificate is saved. If you need to upload additional intermediate CA certificates to establish a chain of trust to the signed certificate, you can select up to four certificates.

8. If you are using this SSL certificate for a Hotspot 2.0 configuration, you must also import a root CA certificate. To import **Root CA Certificate**, click **Browse** and select the location where the certificate is saved.
9. You can import the **Private Key** file either by
  - uploading file—choose **Upload** and click **Browse** to select the location.
  - using CSR—choose **Using CSR** and select the CSR that you generated earlier.
10. Enter the **Key Passphrase** that has been assigned to the private key file.
11. Click **OK**.

#### NOTE

You can also edit or delete a certificate by selecting the options **Configure** or **Delete** respectively.

## Assigning Certificates to Services

You can map certificates to services

To specify the certificate that each secure service will use:

1. From the application select, **System > Certificates > Service Certs**.
2. Select the certificate that you want to use for each of the following services:
  - **Management Web**—Used by Web UI and Public API traffic.
  - **AP Portal**—Used by Web Auth WLAN and Guest Access WLAN control traffic.
  - **Hotspot (WISPr)**—Used by WISPr WLAN control (Northbound Interface, Captive Portal, and Internal Subscriber Portal) traffic.
  - **Communicator**—Used by AP control traffic.
3. To view the public key, click **View Public Key**, the Certificate Public Key form appears with the public key.
4. Click **OK**.

## Generating Certificate Signing Request (CSR)

If you do not have an SSL certificate, you will need to create a certificate signing request (CSR) file and send it to an SSL certificate provider to purchase an SSL certificate.

To create a CSR file:

1. From the application select, **System > Certificates > CSR**.
2. Click **Generate**, the Generate CSR form appears.
3. Enter the following details:
  - **Name**—A name for this CSR.
  - **Description**— A short description for this CSR.
  - **Common Name**—A fully qualified domain name of your Web server. This must be an exact match (for example, **www.ruckuswireless.com**).
  - **Email**—An email address (for example, **joe@ruckuswireless.com**).

- **Organization**—Complete legal name of your organization (for example, **Google, Inc.**). Do not abbreviate your organization name.
  - **Organization Unit**—Name of the division, department, or section in your organization that manages network security (for example, **Network Management**).
  - **Locality/City**—City where your organization is legally located (for example, **Sunnyvale**).
  - **State/Province**—State or province where your organization is legally located (for example, **California**) Do not abbreviate the state or province name.
4. Select the **Country**
  5. Click **OK**, the controller generates the certificate request. When the certificate request file is ready, your web browser automatically downloads it.
  6. Go to the default download folder of your Web browser and locate the certificate request file. The file name is **myreq.zip**.
  7. Use a text editor (for example, Notepad) to open the certificate request file.
  8. Go to the website of your preferred SSL certificate provider, and then follow the instructions for purchasing an SSL certificate.
  9. When you are prompted for the certificate signing request, copy and paste the entire content of **myreq.csr**, and then complete the purchase.
  10. After the SSL certificate provider approves your CSR, you will receive the signed certificate via email.
  11. Copy the content of the signed certificate, and then paste it into a text file.
  12. Save the file.

**NOTE**

You can also edit, clone, download or delete a CSR by selecting the options **Configure**, **Clone**, **Download** or **Delete** respectively.

## Managing AP Certificates

AP certificates are valid for a period of time and have to be replaced when they expire.

**NOTE**

Although AP Certificate Expire Check is enabled by default, when an AP with an expired certificate joins the controller, this check automatically gets disabled. To restore security:

- All APs with expired certificates need to be replaced with a new valid certificate
- Manually enable certificate check using `ap-cert-expired-check` CLI command in the config mode

You must get AP Certificate Replacement before your AP certificate expires. The system generates an *apCertificateExpireSystem* alarm and event when an AP certificate expires.

To get an AP Certificate replacement:

1. From the application select, **System > Certificates > AP Certificate Replacement**.
2. In the AP Request List area, those APs with the **Need Export** column marked **Yes** needs certificate replacement. Those marked with **No** means that the certificate request has already been exported.

**NOTE**

Use the Search terms option to look for APs by name, model, serial number, or description.

3. Click **Export** and select one of the following options:

- **Export All APs Certificate Request**—Exports the certificates for all the AP
- **New APs**—Exports the certificates for new APs or APs that need to regenerate their certificates.

**NOTE**

All exported AP Certificate request (.req) files generated from a cluster include its name. To manage multiple export request files, change the file name before uploading it to uniquely identify the file.

4. Login <https://support.ruckuswireless.com/> with your credentials.
5. From the right pane go to **Tools > Certificate Renewal**. The Certificate Renewal Requests page appears.
6. Click **Browse** to select the .req file exported from Certificate Refresh page.
7. Enter the Email address for communication.
8. Click **Upload**, you will receive an e-mail acknowledgment from Ruckus.
9. From the Certificate Renewal Request page, check the **Status** column of your request. After the request is processed, you will receive the response from Ruckus, with a link to the .res response file for Import on the Certificate Refresh page.
10. From the AP Certificate Replacement page of the application, click **Import AP certificate Response (.res) file**. The Import AP certificate for replacement form appears.
11. Click **Browse** and select the file.
12. Click **OK**.

**NOTE**

All APs included in the imported response (.res) file reboot after their certificate is refreshed.

13. From the Certificate Status area, check the **Status** column of the AP. If the status is:
  - **Updating**—Controller is in the process of updating the certificate.
  - **Update Failed**—Controller failed to update the certificate.

**NOTE**

The AP reports to the controller at 15-minute intervals. As a result, it may take up to 15 minutes for the AP to update its certificate status on the web interface.

14. Click **Reset Update Failed AP**, to reset the status of the APs for which certification update failed. The status of the AP will change.
15. Check the **Update Stats** to know the status of the AP certificates.
16. Once all the APs are updated with the new certificates, manually enable the `ap-cert-expired-check` CLI command in the config mode to restore security and reject APs that try to connect with expired certificate

# Importing Trusted CA Certificates

When a controller receives a server's certificate, it matches the server's CA against the list of trusted CAs it has. If there is no match, the controller sends an error.

To import a CA certificate:

1. From the application select, **System > Certificates > Trusted CA Certs (Chain)**.
2. Click **Import**, the Import CA Certs (Chain) form appears.
3. Enter a **Name**.
4. Enter a **Description** of the certificate.
5. For **Intermediate CA Certificates**, click **Browse** and select the file. If you need to upload additional intermediate CA certificates to establish a chain of trust to the signed certificate, you can select up to four certificates.
6. For **Root CA Certificate**, click **Browse** and select the file.
7. Click **OK**.

## NOTE

You can also edit or delete a CA certificate by selecting the options **Configure** or **Delete** respectively.





# Configuring Templates

- [Working with Zone Templates.....](#) 125
- [Working with WLAN Templates.....](#) 131

## Working with Zone Templates

You can create, configure, and clone zone templates

### Creating Zone Templates

To create a zone template:

1. From the application select, **System > Templates > Zone Templates**.
2. Click **Create**, the Create Zone Template form appears.
3. Enter the template details as explained in the following table.
4. Click **OK**.

**TABLE 16** Zone Template Details

Field	Description	Your Action
<b>General Options</b>		
<b>Zone Name</b>	Indicates a name for the Zone.	Enter a name.
<b>Description</b>	Indicates a short description.	Enter a brief description
<b>AP Firmware</b>	Indicates the firmware to which it applies.	Select the firmware.
<b>Country Code</b>	Indicates the country code to ensure that this zone uses authorized radio channels.	Select the country code.
<b>Location</b>	Indicates generic location.	Enter the location.
<b>Location Additional Information</b>	Indicates detailed location.	Enter additional location information.
<b>GPS Coordinates</b>	Indicates the geographical location.	Enter the following coordinates in meters or floor: <ul style="list-style-type: none"><li>• <b>Longitude</b></li><li>• <b>Latitude</b></li><li>• <b>Altitude</b></li></ul>
<b>AP Admin Logon</b>	Indicates the admin logon credentials. For the Default Zone, the SZ cluster name is used as the default login ID and password.	Enter the <b>Logon ID</b> and <b>Password</b> .
<b>Time Zone</b>	Indicates the time zone that applies.	Select the option: <ul style="list-style-type: none"><li>• <b>System Defined:</b> Select the time zone.</li><li>• <b>User defined:</b><ol style="list-style-type: none"><li>1. Enter the <b>Time Zone Abbreviation</b>.</li><li>2. Choose the <b>GMT Offset time</b>.</li><li>3. Select <b>Daylight Saving Time</b>.</li></ol></li></ul>
<b>AP IP Mode</b>	Indicates the IP version that applies.	Select the option: <ul style="list-style-type: none"><li>• <b>IPv4 only</b></li><li>• <b>IPv6 only</b></li></ul>

**TABLE 16** Zone Template Details (continued)

Field	Description	Your Action
		<ul style="list-style-type: none"> <li>• <b>Dual</b></li> </ul>
<b>Historical Connection Failures</b>	Allows the zone APs to report client connection failures so that the administrator can view past connection problems from the Troubleshooting menu.	Click the button.
<b>DP Zone Affinity Profile</b>	Specifies the DP affinity profile for the zone.  <b>NOTE</b> This option is supported only on vSZ-H.	Select the zone affinity profile from the list.
<b>SSH Tunnel Encryption</b>	Specifies the encryption that reduces the load on control of SSH traffic.	Select the required option: <ul style="list-style-type: none"> <li>• <b>AES 128</b></li> <li>• <b>AES 256</b></li> </ul>
<b>Cluster Redundancy</b>	Provides cluster redundancy option for the zone.  <b>NOTE</b> Cluster redundancy is supported only on SZ300 and vSZ-H.	Select the required option: <ul style="list-style-type: none"> <li>• <b>Zone Enable</b></li> <li>• <b>Zone Disable</b></li> </ul>
<b>Radio Options</b>		
<b>Channel Range</b>	Indicates that you want to override the 2.4GHz channel range that has been configured for the zone.	Select <b>Select Channel Range (2.4G)</b> check boxes for the channels on which you want the 2.4GHz radios to operate. Channel options include channels 1 to 11. By default, all channels are selected.
<b>DFS Channels</b>	Allows ZoneFlex APs to use DFS channels.	Select the check box.
<b>Channel Range (5G) Indoor</b>	Indicates for what channels want the 5GHz radios to operate.	Select the check boxes.
<b>Channel Range (5G) Outdoor</b>	Indicates for what channels want the 5GHz radios to operate.	Select the check boxes.
<b>Radio Options b/g/n (2.4 GHz)</b>	Indicates the radio option 2.4 GHz configurations.	Select the following options: <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20</b> or <b>40</b> (MHz), or select <b>Auto</b> to set it automatic.</li> <li>• <b>Channel</b>—Select the channel to use for the b/g/n (2.4GHz) radio, or select <b>Auto</b> to set it automatic.</li> <li>• <b>TX Power Adjustment</b>—Select the preferred TX power, if you want to manually configure the transmit power on the 2.4GHz radio. By default, TX power is set to <b>Full/Auto</b> on the 2.4GHz radio.</li> </ul>

**TABLE 16** Zone Template Details (continued)

Field	Description	Your Action
		<p><b>NOTE</b> If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p>
<b>Radio Options a/n/ac (5 GHz)</b>	Indicates the radio option 5 GHz configurations.	<p>Select the following options:</p> <ul style="list-style-type: none"> <li>• <b>Channelization</b>—Set the channel width used during transmission to either <b>20, 40, 80, 80+80</b> or select <b>Auto</b>.</li> <li>• <b>Channel</b>—For Indoor and Outdoor, select the channel to use for the a/n/c (5GHz) radio, or select <b>Auto</b>.</li> <li>• <b>TX Power Adjustment</b>—Select the preferred TX power, if you want to manually configure the transmit power on the 5GHz radio. By default, TX power is set to <b>Full/Auto</b> on the 5GHz radio.</li> </ul> <p><b>NOTE</b> If you choose Min, the transmit power is set to 0dBm (1mW) per chain for 11n APs, and 2dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the max allowable value according to the AP's capability and the operating country's regulations.</p>
<b>AP GRE Tunnel Options</b>		
<b>Tunnel Type</b>	Indicates the support for NAT.	<p>Choose the required tunnel type:</p> <ul style="list-style-type: none"> <li>• <b>Ruckus GRE</b> and select the <b>GRE Tunnel Profile</b>.</li> <li>• <b>SoftGRE</b> and <ul style="list-style-type: none"> <li>- select the <b>GRE Tunnel Profile</b></li> <li>- select <b>AAA Affinity</b>, which is applicable only for proxy AAA.</li> </ul> </li> </ul> <p><b>NOTE</b> If you select <b>AAA Affinity</b>, you must enable <b>Force Disassociate Client</b> while creating the Soft GRE Profile.</p> <ul style="list-style-type: none"> <li>• <b>SoftGRE+IPsec</b> and <ul style="list-style-type: none"> <li>- select the <b>GRE Tunnel Profile</b></li> <li>- select <b>IPSec Tunnel Profile</b></li> </ul> </li> </ul>
<b>Syslog Options</b>		
<b>Enable external syslog server for Aps</b>	Indicates if an external syslog server is enabled.	Select the check box and update the following details for the AP to send syslog messages to syslog

**TABLE 16** Zone Template Details (continued)

Field	Description	Your Action
		<p>server. If the primary server goes down, the AP send syslog messages to the secondary server as backup:</p> <ul style="list-style-type: none"> <li>• <b>Primary Server Address</b></li> <li>• <b>Secondary Server Address</b></li> <li>• <b>Port</b> for the respective servers</li> <li>• <b>Protocol</b>: select between UDP and TCP protocols</li> <li>• <b>Event Facility</b></li> <li>• <b>Priority</b></li> <li>• <b>Send Logs</b>: you can choose to send the General Logs, Client Logs or All Logs</li> </ul>
<b>AP SNMP Options</b>		
<b>Enable AP SNMP</b>	Indicates if the AP SNMP option is enabled.	Select the check box.
<b>SNMPv2 Agent</b>	Indicates SNMPv2 Agent is applied.	<ol style="list-style-type: none"> <li>1. Click <b>Create</b> and enter <b>Community</b>.</li> <li>2. Select the required <b>Privilege: Read or Write</b>.</li> <li>3. Click <b>OK</b>.</li> </ol>
<b>SNMPv3 Agent</b>	Indicates SNMPv3 Agent is applied.	<ol style="list-style-type: none"> <li>1. Click <b>Create</b> and enter <b>User</b>.</li> <li>2. Select the required <b>Authentication</b>: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>SHA</b> <ol style="list-style-type: none"> <li>a. Enter the <b>Auth Pass Phrase</b></li> <li>b. Select the <b>Privacy</b> option. For <b>DES</b> and <b>AES</b> options, Enter the <b>Privacy Phrase</b>.</li> </ol> </li> <li>• <b>MD5</b> <ol style="list-style-type: none"> <li>a. Enter the <b>Auth Pass Phrase</b></li> <li>b. Select the <b>Privacy</b> option. For <b>DES</b> and <b>AES</b> options, Enter the <b>Privacy Phrase</b>.</li> </ol> </li> </ul> </li> <li>3. Select the required <b>Privilege: Read or Write</b>.</li> <li>4. Click <b>OK</b>.</li> </ol>
<b>Advanced Options</b>		
<b>Channel Mode</b>	Indicates if location-based service is enabled.	Select the check box and choose the option.
<b>Auto Channel Selection</b>	Indicates auto-channel settings.	Select the required check boxes and choose the option.
<b>Background Scan</b>	Runs a background scan.	Select the respective check boxes and enter the duration in seconds.
<b>Smart Monitor</b>	Indicates AP interval check and retry threshold settings.	Select the check box and enter the duration and threshold.
<b>AP Ping Latency Interval</b>	Measures the latency between the controller and AP periodically, and send this data to SCI	Enable by moving the radio button to ON to measure latency.
<b>AP Management VLAN</b>	Indicates the AP management VLAN settings.	Choose the option. If you select <b>VLAN ID</b> , enter the VLAN ID that you want to assign (valid range is from 1 to 4094). To keep the same management VLAN ID

**TABLE 16** Zone Template Details (continued)

Field	Description	Your Action
		that has been configured on the AP, click <b>Keep AP's settings</b> .  <b>NOTE</b> For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.
<b>Rogue AP Detection</b>	Indicates rogue AP settings.	Enable the option.
<b>Rogue Classification Policy</b>	Indicates the parameters used to classify rogue APs. This option is available only if you enable the <b>Rogue AP Detection</b> option.	Select the options for rogue classification policy: <ul style="list-style-type: none"> <li>• <b>Enable events and alarms for all rogue devices</b></li> <li>• <b>Enable events and alarms for malicious rogues only</b></li> <li>• <b>Report RSSI Threshold</b> - enter the threshold. Range: <b>0</b> through <b>100</b>.</li> <li>• <b>Protect the network from malicious rogue access points</b> - Enable the option and choose one of the following: <ul style="list-style-type: none"> <li>• <b>Aggressive</b></li> <li>• <b>Auto</b></li> <li>• <b>Conservative</b></li> </ul> </li> <li>• <b>Radio Jamming Detection</b> - enable the option and enter the <b>Jamming Threshold</b> in percentage.</li> </ul>
<b>DoS Protection</b>	Indicates settings for blocking a client.	Select the check box and enter the: <ul style="list-style-type: none"> <li>• duration in seconds to Block a client for</li> <li>• number of <b>repeat authentication failures</b></li> <li>• duration in <b>seconds</b> to be blocked for every repeat authentication failures.</li> </ul>
<b>Load Balancing</b>	Balances the number of clients across APs.	Select one of the following options and enter the threshold: <ul style="list-style-type: none"> <li>• <b>Based on Client Count</b></li> <li>• <b>Based on Capacity</b></li> <li>• <b>Disabled</b></li> </ul> <b>NOTE</b> If <b>Based on Capacity</b> is selected, <b>Band Balancing</b> is disabled.
<b>Band Balancing</b>	Balances the bandwidth of the clients.	Select the check box and enter the percentage.
<b>Location Based Service</b>	To disable the LBS service for this AP group, clear the Enable LBS service check box. To use a different LBS server for this AP group, select the Enable LBS service check box, and then select the LBS server that you want to use from the drop-down list.	Select the check box and choose the options.
<b>Client Admission Control</b>	Indicates the load thresholds on the AP at which it will stop accepting new clients.	Select the <b>Enable</b> check box 2.4 GHz Radio or 5GHz Radio and update the following details: <ul style="list-style-type: none"> <li>• <b>Min Client Count</b></li> <li>• <b>Max Radio Load</b></li> <li>• <b>Min Client Throughput</b></li> </ul>

**TABLE 16** Zone Template Details (continued)

Field	Description	Your Action
	<p><b>NOTE</b> Client admission cannot be enabled when client load balancing or band balancing is enabled.</p>	
<b>AP Reboot Timeout</b>	Indicates AP reboot settings.	Choose the required option for: <ul style="list-style-type: none"> <li>• <b>Reboot AP if it cannot reach default gateway after</b></li> <li>• <b>Reboot AP if it cannot reach the controller after</b></li> </ul>
<b>Recovery SSID</b>	Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller.	Enable <b>Recovery SSID Broadcast</b>
<b>Direct Multicast</b>	Indicates whether multicast traffic is sent from a wired device, wireless device or from the network.	Select one or more of the following: <ul style="list-style-type: none"> <li>• <b>Multicast Traffic from Wired Client</b></li> <li>• <b>Multicast Traffic from Wireless Client</b></li> <li>• <b>Multicast Traffic from Network</b></li> </ul>

**NOTE**

You can select a zone from the list and edit, clone or delete its template by selecting the options **Configure**, **Clone** or **Delete** respectively.

## Applying Zone Templates

To apply a zone template:

1. From the application select, **System > Templates > Zone Templates**.
2. From the list, select the zone template that you want to apply and click **Apply**. The Apply Zone Templates form appears.
3. From **Select AP Zone**, select the required zone.
4. Click **Apply**.

## Exporting Zone Templates

You can export a zone template.

To export a zone template:

1. From the application select, **System > Templates > Zone Templates**.
2. Select the zone template that you want to export and click **Export Template**.
3. A pop-up appears prompting you to **Open** or **Save** the zone template file with **.bak** extension. Click:
  - **Open**—To view the template file
  - **Save**—Select the destination folder where you want to save the template file and then click **Open** to view it.

## Importing Zone Templates

You can import zone templates and upload them to the system.

### NOTE

Configuration references to global services or profiles cannot be imported, manually configure it after importing.

To import a zone template:

1. From the application select, **System > Templates > Zone Templates**.
2. Click **Import**, the Import Zone Templates form appears.
3. Click **Browse** and select the template file.
4. Click **Upload**.

## Working with WLAN Templates

You can create, configure and clone a WLAN template.

### Creating WLAN Templates

To create a WLAN template:

1. From the application select, **System > Templates > WLAN Templates**.
2. Click **Create**, the Create WLAN Template form appears.
3. Enter a **Template Name**.
4. Enter a **Description**.
5. Select the **Template Firmware**.
6. Choose the **AP IP Mode**.
7. Select **AP SoftGRE Tunnel** to enable all WLANs defined in this template to tunnel traffic to SoftGRE through the AP.
8. Click **OK**.

### NOTE


You can select a WLAN and edit, clone or delete its template by selecting the options **Configure**, **Clone** or **Delete** respectively.

### Applying a WLAN Template

You can apply the WLAN template to zones where the AP's firmware version is later than the Zone templates firmware version. An unsupported firmware version of the WLAN template is automatically upgraded to its next version before being upgraded to the current version.

To Apply a WLAN template to a zone:

1. From the application select, **System > Templates > WLAN Templates**.
2. From the list, select the WLAN template that you want to apply and click **Apply**. The Apply WLAN Template to selected zones form appears.

3. From **Available AP Zones**, select the required zone and click the  Move button.
4. Click **Next**, the **Apply WLAN template to selected zones** form appears.
5. Select the required options:
  - Create all WLANs and WLAN profiles from the template if they don't already exist in the target zone(s)
  - If the target zone(s) has WLANs or WLAN profile with the same name as the template, overwrite current settings with settings from the template.
6. Click **OK**, you have applied the template to the zone.



# Managing ICX Switches

---

- Overview of ICX Switch Management..... 133

## Overview of ICX Switch Management

Beginning with SmartZone release 5.0, the administrator can monitor and manage switches and routers in the ICX 7000 series or above.

ICX switch management allows you to monitor status, view usage statistics, and perform some basic management operations, including configuration backup and firmware management. The following capabilities are supported:

- ICX switch registration and authentication
- Switch inventory (for example, model, firmware version, and last backup)
- Health and performance monitoring (status, traffic stats, errors, clients etc) with alarms
- Switch configuration file backup and restore
- Firmware upgrade to FastIron release 08.0.80 GA.

## Preparing ICX Devices to be Managed by SmartZone

### NOTE

For more information on ICX device capabilities and configuration, refer to the Ruckus FastIron documentation set available at the following URL:

<https://support.ruckuswireless.com>. On the site, select **Products > Ruckus ICX Switches > Technical Documents**, and choose the platform and document of interest.

ICX devices running either router or switch images can be managed by SmartZone. The following items are required to manage ICX devices:

- The ICX switch must be running FastIron software version 08.0.80 or higher.
- Smartzone's IP address should be reachable by the ICX device through the Management interface or through router interfaces.
- The ICX device must be made aware of the configured SmartZone IP address in one of two ways:
  - configuring the DHCP server to use DHCP option 43
  - issuing the following command at the global configuration level:

```
ICX(conf)# sz active-list < SmartZone_Control_IP_Address >
```

- On some ICX 7250, ICX 7450, or ICX 7750 devices, self-signed certificates are used. SmartZone honors these certificates when the following option is configured on the SmartZone console: **non-tpm-switch-cert-validate** as shown in the following example.

**FIGURE 52** Sample Commands and Parameters

```
SZ# T.onf
SZ(config)# non-tpm-switch-cert-validate
Successful operation

SZ(config)# end
SZ#
```

**NOTE**

ICX 7150, ICX 7650, and ICX 7850 devices are shipped with embedded certificates that are used for authentication with SmartZone.

- When SmartZone or ICX devices are behind NAT, be sure to forward TCP ports 443 and 22 through NAT.
- The following table lists virtual platforms requirements for supporting ICX devices.

**NOTE**

SmartZone can monitor ICX stacks; however, the stack must be configured and enabled locally before it connects to SmartZone.

**NOTE**

Each unit in a stack is considered as a separate switch unit for capacity management purposes.

**TABLE 17** Virtual Platform Requirements for Supporting ICX Devices

Platform	Number of Switches	RAM	vCPU	Disk Storage
vSZ-E	50	18 GB	4	100 GB
vSZ-H	500	30 GB	12	300 GB

# ICX Switch Configuration and Behavior

• ICX Switch Behavior with SmartZone.....	135
• Enabling an ICX Device to be Managed by SmartZone.....	135
• Displaying the SmartZone Connection Status.....	136
• Disconnecting the Switch Connection with SmartZone.....	137
• Disabling SmartZone Management on the ICX Switch.....	137

## ICX Switch Behavior with SmartZone

When an ICX switch is managed by SmartZone, the following behaviors apply:

- All local configuration methods continue to be available to the local administrator, which means the switch can be configured through the console, Telnet, SSH, SNMP, and the web.
- It is recommended that the switch be configured with the same NTP server as SmartZone.
- In an ICX stack, if a stack switchover or failover occurs, the original connection to SmartZone is closed, and the new active unit initiates a connection with SmartZone.

## Enabling an ICX Device to be Managed by SmartZone

There are two ways to make an ICX device aware of the SmartZone's IP address. One is using DHCP option 43, and the other is using manual configuration via ICX commands. Both of these methods can be used for new switches with no configuration and for switches with existing configuration.

## Manually Configuring the SmartZone IP Address on an ICX Switch

Perform this task to configure a list of SmartZone IP addresses on the ICX device.

1. Enter the **sz active-list** followed by one or more priority IP addresses for the SmartZone as shown in the following example.

IP addresses are examples only.

```
ICX# configure terminal
ICX(config)# sz active-list 192.168.11.200 192.168.11.201 192.168.11.202
```

2. Use the **sz passive-list ip-address ip-address** command to configure the SmartZone IP addresses to be used for redundancy.

```
ICX(config)# sz passive-list 10.176.160.118
```

## Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch

The following example shows how a DHCP server can be configured to send SmartZone IP addresses to ICX devices using DHCP Option 43.

Configure DHCP Option 43 on the DHCP server, using **RKUS.scg-address** to identify the SmartZone IP addresses.

A single SmartZone IP address or a comma-separated list can be configured. SmartZone IP addresses are sent with a sub-option value of 6. The ICX device ignores all other data in DHCP Option 43 if SmartZone IP addresses are present.

The following example shows a DHCP Option 43 configuration on a DHCP server. The IP addresses listed are examples only.

```
subnet 192.168.12.0 netmask 255.255.255.0 {  
    range 192.168.12.100 192.168.12.199;  
    option routers 192.168.12.1;  
    option subnet-mask 255.255.255.0;  
    option broadcast-address 192.168.12.255;  
    option ntp-servers 192.168.11.22;  
    class "Ruckus AP" {  
        match if option vendor-class-identifier = "Ruckus CPE";  
        option vendor-class-identifier "Ruckus CPE";  
        default-lease-time 86400;  
        vendor-option-space RKUS;  
        option RKUS.scg-address "192.168.11.200, 192.168.11.201, 192.168.11.202";  
    }  
}
```

## Displaying the SmartZone Connection Status

The status of the ICX switch connection with SmartZone can be displayed using the **show sz status** command.

Use the **show sz status** command to display the SmartZone IP address lists and information about the status of the connection.

```
ICX# show sz status  
  
=====      SZ Agent State Info      =====  
Config Status: None      Operation Status: Enabled  
State: SZ SSH CONNECTED      Prev State: SZ SSH CONNECTING      Event: CONF  
  
Active List      : 10.176.160.118  
DHCP Option 43   : Yes  
DHCP Opt 43 List : 10.176.160.115  
Passive List     : 10.176.160.118  
Merged List      : 10.176.160.118, 10.176.160.115  
Merged Idx: 0    IP : 10.176.160.118  
  
SZ IP Used       : 10.176.160.118  
SZ Query Status  :  
    Response Received  
  
SSH Tunnel Status - :  
    Tunnel Status   : Established  
    CLI IP/Port     : 127.255.255.253/53704  
    SNMP IP/Port    : 127.255.255.254/53704  
    Syslog IP/Port   : 127.0.0.1/20514  
  
Timer Status     : Not Running
```

## Disconnecting the Switch Connection with SmartZone

The **sz disconnect** command can be used to disconnect the ICX switch from the current connection with SmartZone and initiate a new connection based on the currently available list of SmartZone IP addresses.

Enter the **sz disconnect**.

This command can be executed on the local terminal.

```
ICX# sz disconnect
SZ Disconnect initiated...
```

## Disabling SmartZone Management on the ICX Switch

When SmartZone management is disabled on the switch, the switch will not initiate a connection with SmartZone even if a SmartZone IP address is available.

Enter the **sz disable** command to disable SmartZone management on the ICX switch.

```
ICX(config)# sz disable
```



# SmartZone Switch Management

- Using SmartZone Settings to Manage ICX Switch Groups..... 139
- Creating ICX Switch Groups..... 139
- Creating Switch Registration Rules..... 140
- Moving the Switches between Groups..... 142
- Deleting Switches..... 143
- Backing up and Restoring ICX Switch Configuration..... 143
- Scheduling a Firmware Upgrade..... 144
- Viewing Switch Information..... 146
- Viewing Switch Configuration Information..... 148
- Viewing Port Details..... 149
- Viewing Switch Health..... 153
- Viewing Alarms..... 156
- Viewing Events..... 158
- Viewing LLDP Neighbor Information..... 159
- Viewing Traffic Trends in the Switch..... 159
- Viewing Firmware History of the Switch..... 161

## Using SmartZone Settings to Manage ICX Switch Groups

SmartZone allows you to create switch groups, similar to AP zones. ICX switches connecting to Smartzone can be placed in one of these logical groups for better manageability. A Default Group is created by SmartZone automatically. All ICX switches are placed in this group when they initially join SmartZone. You have the option to create additional groups. Using registration rules, you can specify which group the switch should be placed into. Refer to [Creating ICX Switch Groups](#) on page 139 and [Creating Switch Registration Rules](#) on page 140 for additional information.

## Creating ICX Switch Groups

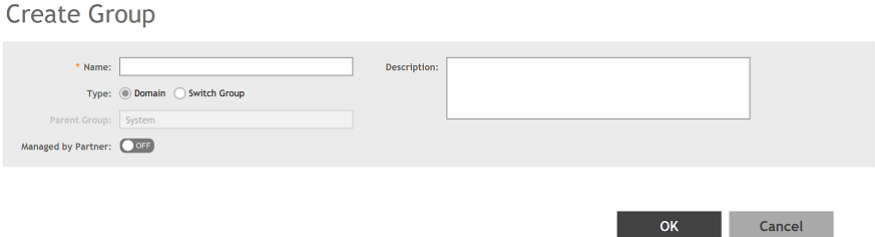
You can group switches based on your need, for example, you can group switches based on their size or their location. You can only create a maximum of two levels within the group hierarchy. By default, all the switches are placed under the default switch group. You can create a group or sub-group and then move the switch under it. You can also modify or delete a group at any time. After the switch is registered with the SmartZone interface, you can monitor, view status or usage, and perform some basic management, including configuration backups and firmware management. However, you cannot configure the switch from the interface.

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.

2. Click .

The **Create Group** page appears.

**FIGURE 53** Creating switch groups



The 'Create Group' dialog box is shown. It has a title bar 'Create Group' with a close button. The form contains the following fields and controls:

- Name:** A text input field.
- Description:** A text input field.
- Type:** Radio buttons for **Domain** (selected) and **Switch Group**.
- Parent Group:** A dropdown menu showing 'System'.
- Managed by Partner:** A toggle switch currently set to **OFF**.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

Configure the following:

- **Name:** type the name of the switch group that you want to create
- **Description:** enter a brief description for the switch group
- **Type:** select **Switch Group**. For enterprise devices such as SZ-300 and vSZ-H, you also have the option to select **Domain**.
- **Parent Group:** displays the parent group under which the switch group resides
- **Managed by Partner:** this option is available if you select the group type as **Domain**. You can slide the radio button to ON or OFF to enable or disable partners from managing the switches.

3. Click **OK**.

The switch group is created under the selected parent group.

## Creating Switch Registration Rules

You can create registration rules for switch groups which are identified and approved by the controller to establish connection. Typically, the switch is registered with the controller using an IP address, subnet or model number.

Follow these steps to create a registration rule:

1. Go to **System > Switch Settings**

The **Switch Registration** page appears.



2. Click **Create**.

The **Switch Registration Rule** page appears. Configure the following:

- Rule Description: provide a brief description about the registration rule you are creating in order to put the switches into specific groups.
- Group Name: from the drop-down menu, select the switch group that you want to apply this rule to.
- Rule Type: you can apply this rule to switches based on their IP Address Range, Subnet or Model Number. Select one of the options as appropriate.

If you select IP Address Range, you must provide the range of the IP address for which this rule will apply. If you select Subnet, you must provide the network address and subnet mask that will apply to the rule. If you select Model Number, you must provide the model number of the device.

**FIGURE 54** Creating registration rules

## Switch Registration Rule

3. Click **OK**.

You can edit, clone and delete the rule by selecting the rule and clicking **Configure**, **Clone** and **Delete** respectively.

The registration rule is created. The rules that are created can be rearranged using the **Up** and **Down** options. They can be arranged in an order of priority. After the order of priority for the list of rules is finalized, click **Update Priority** to confirm.

## Approving ICX Switches

The ICX switch must be approved so that it can be discovered and monitored by the SmartZone controller.

- Switches that are not registered through registration rules are automatically moved under the Default group.

- If there are no registration rules, the switch is moved to the Default group and approved but left in the offline state.
- After it is successfully registered with the controller, the switch joins the controller's Default group. To approve the switch manually, you must move it to a specific group. Refer to [Moving the Switches between Groups](#) on page 142 for more information.

#### NOTE

A switch capacity license (CAPACITY-SWITCH-DEFAULT) is available for controllers and ICX switches managed by the controllers. The license is activated for devices running SmartZone 5.1 or later. Upgrading to SmartZone 5.1 from an earlier version activates the license by default. A 90 day version is then available for trial or purchase. The controller manages switches only as defined in the Switch Capacity license and rejects individual switches or stacks when license capacity is reached. Any switch that exceeds license limits is moved to the service group, where it cannot be configured. When license capacity is again available, the controller accepts the switch for management.

Follow these steps to automatically approve a switch:

1. Create a registration rule for the switch. Refer to [Creating Switch Registration Rules](#) on page 140 for more information.
2. Configure the switch to register and join the SmartZone controller. Refer to *ICX Switch Configuration and Behavior* for more information.

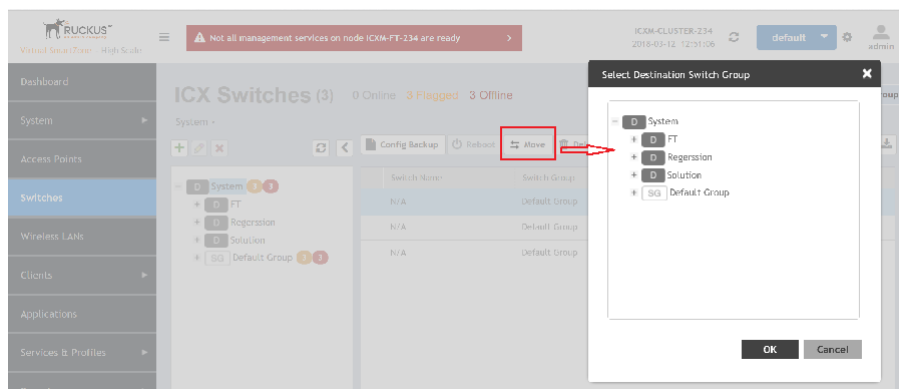
The switch must join the specific group as configured in the registration rule.

## Moving the Switches between Groups

You can move the switches within any group or sub-group in the system hierarchy to manage it.

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.
2. From the **ICX Switches** page, select the switch that you want to move and click **Move**.  
The **Select Destination Switch Group** page appears. It displays the system hierarchy from which you can select the group under which you want to move the switch.

**FIGURE 55** Moving the switch



#### Approval of Switches

- Switches which are not registered through Registration Rules are moved under the Default Group.
- If Registration Rules are not present, the switch is moved to System Domain.

- These switches are not approved in the System Domain and are in the offline state.
- To approve the switch, you must manually move it from System, to another domain or subgroup, or ensure that registration rule matches.
  3. Select the destination group and Click **OK**  
A confirmation message appears
  4. Click **Yes**. The switch is moved to the destination location.

## Deleting Switches

You can delete switches that you do not want the SmartZone controller to manage anymore.

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.
2. Select the switch you want to delete and click **Delete**.  
The selected switch is deleted, and it will not be managed by the SmartZone interface.

## Backing up and Restoring ICX Switch Configuration

SmartZone can back up the switch's running configuration. By default, SmartZone makes a backup of switch configuration on a daily basis. When needed, these backups can be restored to the switch. While performing network maintenance, you can initiate a backup without having to wait for the daily backup.

Perform the following steps to configure ICX switch backups.

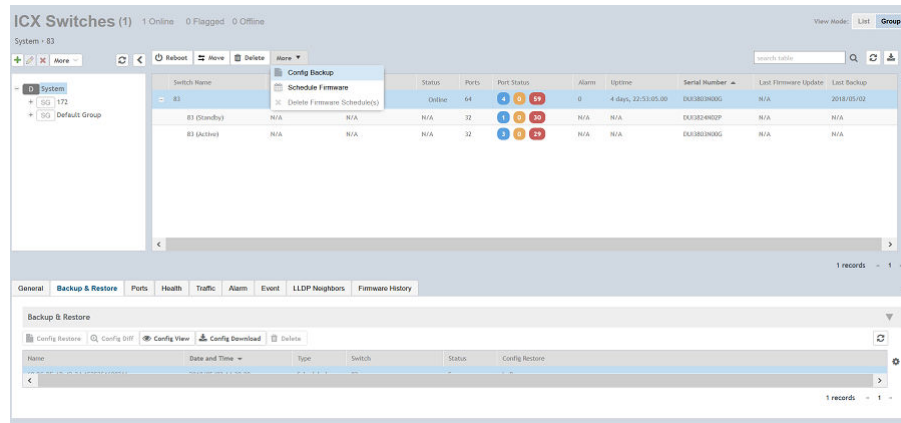
### NOTE

Be sure to sync the controller to the NTP server during installation. You can also do this from **System > General Setting > Time**.

1. From the left pane, select **Switches**.  
The **ICX Switches** page is displayed.

- From the **ICX Switches** page, select the switch for which you want to backup the configuration and click **More**.

**FIGURE 56** Configuring Backup



- From the drop-down menu, select **Config Backup**.  
A confirmation message is displayed asking whether to continue with the backup.
- Click **Yes**. A message is displayed confirming that the backup process has been initiated.  
After the backup is completed, the status is recorded in the **Backup & Restore** tab.

**NOTE**

- As soon as the switch connects to the controller, and when it is online, the controller retrieves all the information about the switch.
- The controller maintains seven of the latest configuration backups for each ICX switch.
- The controller automatically backs up the configuration of each switch, once, every 24 hours.
- If a previous switch configuration matches the current configuration, the latest configuration is saved and the old configuration is removed.

You can restore an individual switch to its previous configuration by clicking **Config Restore**. A message is displayed stating the restore operation is initiated and that the system must be rebooted for the configuration changes to take effect.

For switches, you can click **Config Diff** to view differences in configuration details, click **Config View** to see the configuration details from the **Switch Config View** screen and click **Config Download** to download the copy of the configuration file.

You can delete a configuration file by selecting it and clicking **Delete**.

## Scheduling a Firmware Upgrade

You can upgrade or downgrade the firmware version of a switch or multiple switches that you are monitoring. You can upgrade the firmware on demand or schedule a firmware update for a list of selected ICX switches.

Upload a valid ICX firmware which is greater than version 8.0.80 to the controller.

**NOTE**

Ensure you sync the controller to the NTP server during installation. You can also do this from **System > General Setting > Time**.

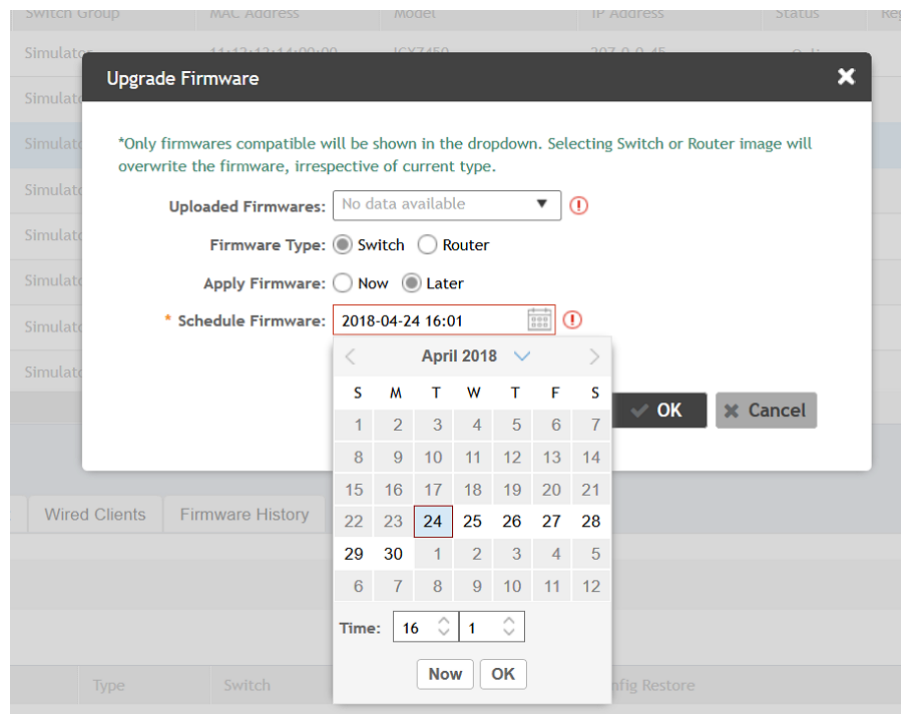
To upgrade the firmware for a group of switches, you must select multiple switches at the same time and perform steps 3 to 7. For more information on uploading the switch firmware, see [Uploading the Switch Firmware to the Controller](#) on page 396

**NOTE**

Only firmware versions later than ICX 8.0.80 are supported.

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.
2. From the **ICX Switches** page, select the switch that you want to upgrade and click **More**.
3. From the drop-down menu, select **Schedule Firmware**.  
The **Upgrade Firmware** page appears.

**FIGURE 57** Scheduling Firmware Upgrade



4. From **Uploaded Firmware**, select the firmware version that you want the switch to be upgraded to
5. In **Firmware Type**, select type of firmware you want to upload to the switch. Options include Switch and Router images.
6. In **Apply Firmware**, set when you want to apply the new firmware version to the switch. You can select Now or Later to schedule your upload. If you select Later, then you must select the date from the **Schedule Firmware** field.
7. Click **OK**.

If you want to delete the schedule you created; From **More**, click **Deleted Firmware Schedule(s)**.

# Viewing Switch Information

Details such as switch status, firmware version, and IP address are available for individual switches, stacks, and switch groups.

To view information on a switch, a stack, or a switch group, perform these steps.

1. From the left pane, select **Switches**.

The **ICX Switches** page is displayed as shown in the following example.

**FIGURE 58** ICX Switches Page

Switch Name	Switch Group	MAC Address	IP Address	Serial Number	Model	Status	Ports	Port Status	Uptime	Firmware	Last F
N/A	Karen	CC:4E:24:0C:D7:80	10.177.130.20	CYU3316K00C	ICX7450-24-HP0E	Online	0	0 0 29	N/A	SPR08080q13.bin	N/A
N/A	Rack_A30	00:00:00:00:01:70	10.176.137.154	CYR3347X00Y	ICX7450	Online	0	28 0 164	N/A	SPR0808085.bin	N/A
N/A	Malik_team	CC:4E:24:38:D9:80	10.177.131.148	CRJ3302K045	ICX7750-48C	Online	0	3 1 57	N/A	SWR0808085.bin	N/A
N/A	Sridhar	60:9C:9F:504:59:C4	10.176.151.13	DUH3805M07F	ICX7250-24	Online	0	0 0 32	N/A	SPR0809061-no...	N/A
N/A	Malik_team	60:9C:9F:1F:5F:00	10.177.131.146	CRH3346L008	ICX7750-48F	Online	0	4 0 50	N/A	SWR0808085.bin	N/A
N/A	Malik_team	60:9C:9F:1F:50:80	10.177.131.147	CRH3346L008	ICX7750-48F	Online	0	4 5 50	N/A	SWR0808085.bin	N/A
N/A	Gobu	CC:4E:24:8E:48:80	10.176.152.166	CRH3326K089	ICX7750-48F	Online	0	2 0 58	N/A	SWR080808q16.bin	N/A
CCEP-122-SPATHA	Rack_A29	CC:4E:24:88:D3:28	10.176.141.22	CYU3333K017	ICX7450	Online	138	19 0 113	6 days, 21:21:35.00	SPR0808085	N/A
CEP-120-SDW	Rack_A29	00:00:00:00:01:20	10.176.141.138	CRH3319L01J	ICX7750	Online	60	5 0 95	6 days, 22:14:53.00	SWR0808085	N/A
N/A	Testsuya_Namba	CC:4E:24:38:36:80	10.176.190.47	CRK2235J00H	ICX7750-26Q	Online	0	5 0 32	N/A	SWR08080b1_v...	Fail

2. Select a switch to display information specific to it. Then select the **General** tab to display the information shown in the following example.

**FIGURE 59** Switch Stack and General Information

Switch Name	MAC Address	IP Address	Status	Ports	Port Status	Alarm	Uptime	Last Firmware Update	Last Backup
HQ-DEV-Stack6	CC:4E:24:8B:19:D8	10.150.22.84	Online	68	3 0 65	0	2:18:22.00	N/A	2018/05/09
HQ-DEV-Stack6 (Active)	N/A	N/A	N/A	30	2 0 28	N/A	N/A	N/A	N/A
HQ-DEV-Stack6 (Standby)	N/A	N/A	N/A	38	1 0 37	N/A	N/A	N/A	N/A

General

Backup & Restore

Ports

Health

Traffic

Alarm

Event

LLDP Neig

**Info**

Switch Name: icx321

MAC Address: 13:12:11:11:01:41

Serial Number: 9999999321

IP Address: 207.0.11.72

Gateway: 10.1.200.254

Model: ICX7250

Switch/Stack: Switch

Number of Switch Units: 1

Firmware Version: 1.0.0

**Status Summary**

Status: Online

Registration State: Approved

No of Alarms: 23

Uptime: 0:17:56.44

Last Configuration Backup: 2018/05/29 06:30:05

Switch Group: Simulator

Switch Stack ↑

The following information about the selected switch is displayed in the **General** tab:

- Switch Name: The name of the switch or group
- MAC Address: The MAC address of the switch
- Serial Number: The serial number assigned to the switch
- IP Address: The IP of the controller that monitors the switch
- Gateway: The gateway IP address through which the switch, group, or stack forwards data
- Model: The model number of the switch
- Switch/Stack: Whether the selected system is a standalone switch or a stack of switches
- Number of Switch Units: The number of switches in a group or stack

- **Firmware Version:** The firmware version uploaded to the selected switch
- **Status:** The status of the switch, such as Online, Offline, or Flagged
- **Registration State:** The status of the switch, such as Approved, Offline, Online, or Flagged (when an event or alarm is triggered)
- **Number of Alarms:** The number of alarms generated for the selected switch or stack
- **Uptime:** The time that has elapsed since reboot
- **Last Configuration Backup:** The time the switch or stack configuration was last backed up
- **Switch Group:** The name of the group to which the switch belongs
- **PoE Utilization (watts):** The total switch PoE utilization. For example, if the total PoE allocation for the switch is 520 Watts, and 300 Watts are used, the column displays 300/520 W.

## Viewing Switch Configuration Information

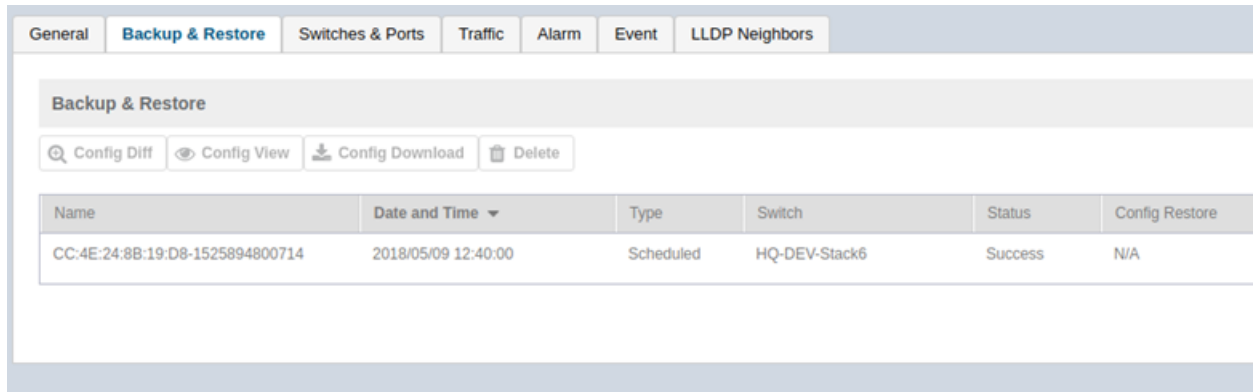
You can view configuration information about the switch, and backup or restore switch configuration as necessary. You can also view the difference between two configuration files.

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.



2. Select the switch and then the **Backup & Restore** tab.

**FIGURE 60** ICX Switch Backup & Restore Tab



The following information about the selected configuration file is displayed in the **Backup & Restore** tab:

- Name: displays the name of the configuration file
- Date and Time: displays the time when the file was created
- Type: displays whether the configuration was created scheduled or on demand
- Switch: displays the model number of the switch
- Status: displays whether the configuration was successful or failed
- Config Restore: displays whether the configuration for the selected switch was restored

To view the difference between two configuration files, select the fields and click **Config Diff**. A **Switch Config Diff** page appears displaying the difference between both files.

To delete a configuration file, select it and click **Delete**.

## Viewing Port Details

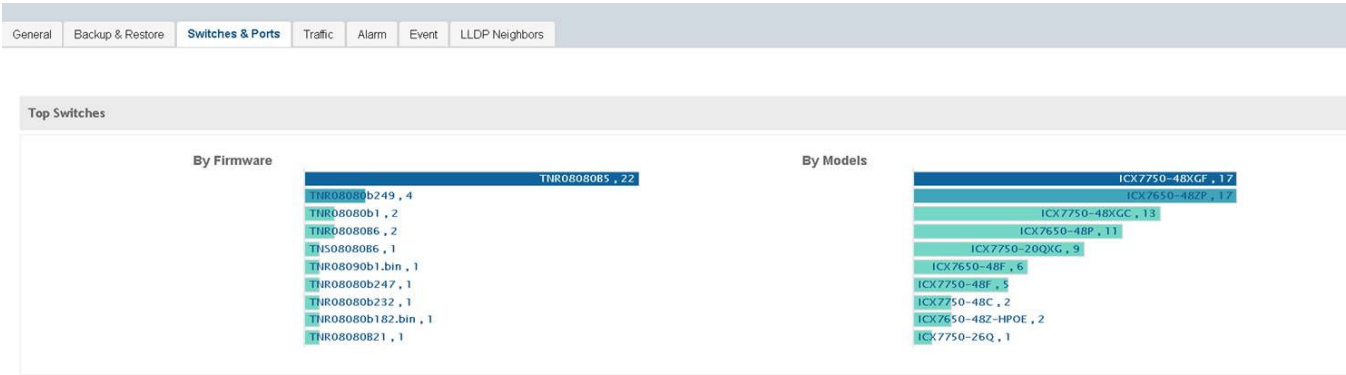
Details on port use are available for individual switches, stacks, and switch groups.

Perform these steps to display information on ports for a switch, stack, or switch group.

1. From the left pane, select **Switches**.  
The **ICX Switches** page is displayed.

2. Select the switch or group. Then select the **Ports** tab.
- For a switch group, a **Top Switches** page similar to the following example is displayed. The graphs provide information on top switches based on firmware and model.

FIGURE 61 Top Switches



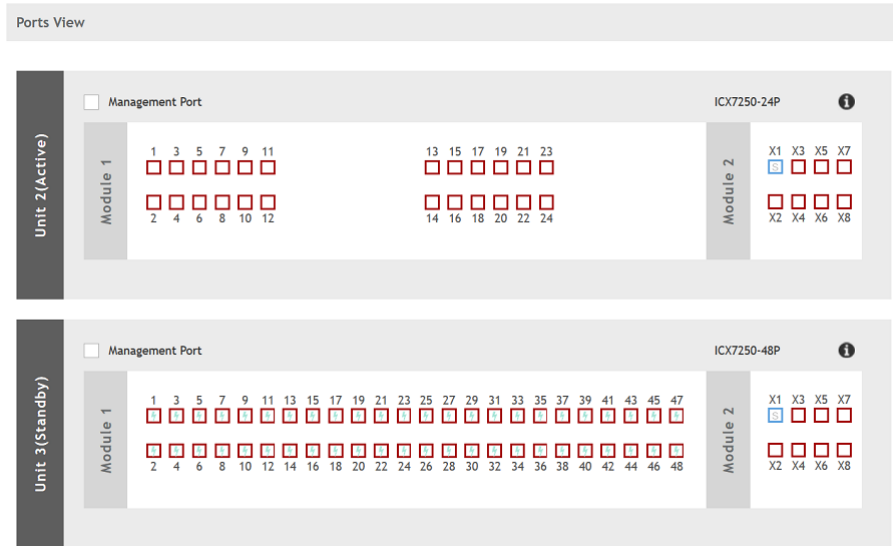
For standalone switches, the **Port Summary** page is displayed in the **Ports** tab as shown in the following example. The **Ports Summary** page provides information on the ports for the selected switch or group, including the total number of ports connected to the switch or stack, the number of ports active at various speeds, operational status of the ports (Up or Down), warnings associated with ports when alarms or events are triggered, and the number of ports managed by an administrator.

FIGURE 62 Port Summary

Ports Summary					
	Total	Up	Warning	Down	By Admin
All Ports	210	26	0	184	0
100G	0	0	0	0	0
40G	2	0	0	2	0
10G	28	6	0	22	0
2.5G	40	0	0	40	0
1G	140	20	0	120	0

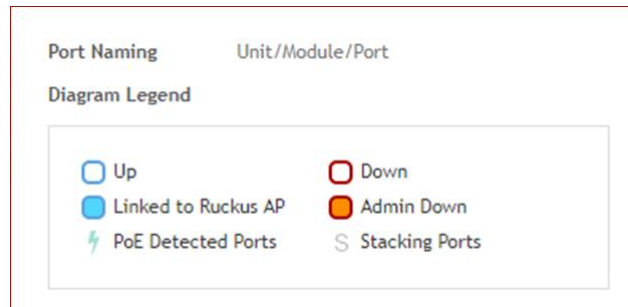
- Click the switch to obtain the **Ports View** page for additional port information as shown in the following example.  
The **Ports View** page provides information on the state of all ports in each switch module, for example port Up, Down, or Administratively Down.

**FIGURE 63 Ports View**



The following figure defines the colors used in the Ports View.

**FIGURE 64 Legend**



The following list further describes items in the Ports View legend.

- Up: Ports that are up or active
- Warning: Ports that have packet errors
- Down: Ports that are down or inactive
- By Admin: Ports that have been manually disabled by the network administrator

- Click the switch to obtain the **Port Details** page as shown in the following example.


**FIGURE 65 Port Details**

Port Details									
<div> Filter Off search table </div>									
Port Name	Status	Admin Status	Speed	PoE Usage (u	VLANs	Bandwidth IN (%)	Bandwidth OUT (%)	Neighbor Name	LAG Name (Type)
10Gigabi...	Down	Up	Link dow...			0.00	0.00		
10Gigabi...	Down	Up	Link dow...		1	0.00	0.00		
10Gigabi...	Up	Up	10 Gbits ...			0.00	0.00		
10Gigabi...	Down	Up	Link dow...		1	0.00	0.00		
10Gigabi...	Down	Up	Link dow...		1	0.00	0.00		
10Gigabi...	Down	Up	Link dow...		1	0.00	0.00		
10Gigabi...	Down	Up	Link dow...		1	0.00	0.00		
10Gigabi...	Down	Up	Link dow...		1	0.00	0.00		

The **Port Details** page provides the following information on each port.

- 
- Port Name: The port name
- Port Number: The port number
- Status: Whether the port is operationally Up or Down
- Admin Status: Whether the port has been set to Up or Down by the network administrator
- Speed: The speed of the port
- PoE Device Type: Inline Power device type, such as 802.3af, 802.3at or Legacy device.
- PoE Usage (used/total watts): The PoE power usage compared to the allocated power
- VLANs: The VLAN(s) to which the port is connected
- Bandwidth IN (%): The bandwidth utilization for incoming traffic
- Bandwidth OUT (%): The bandwidth utilization of the port for outgoing traffic
- LAG Name: The name of the Link Aggregation Group (LAG)
- Optics: The type of optic
- Neighbor Name: When LLDP is enabled, the name of the neighboring device, such as an AP or another switch or router
- Incoming Multicast Packets: The total number of incoming multicast data packets
- Outgoing Multicast Packets: The total number of outgoing multicast data packets
- Incoming Broadcast Packets: The total number of incoming broadcast data packets
- Outgoing Broadcast Packets: The total number of outgoing broadcast data packets
- In Errors: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
- Out Errors: The number of outbound packets that could not be transmitted because of errors.
- CRC Errors: Indicates that the checksum calculated does not match between the data sender side and received side. It usually depicts network transmission problems.

- In Discard: The number of inbound packets which were chosen to be discarded (even though no errors are detected) to prevent their being deliverable to a higher-layer protocol. Some reasons for discarding such a packet could be to free up buffer space.
- Switch Name: The name of the switch connected to the port
- Switch Group: The name of the switch group connected to the port

You can also filter the list of ports by the VLANs associated with them. Click  to set the filters.

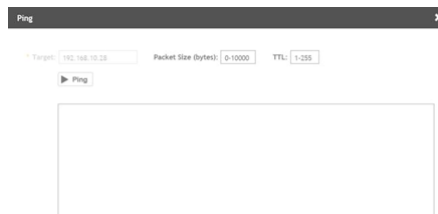
## Viewing Switch Health

Health information displayed for a switch is based on memory usage and CPU usage statistics.

To view information on the health of a switch or the active controller of a stack, perform the following steps.

1. From the left pane, select **Switches**.  
The **ICX Switches** page is displayed.
2. Select the switch and then the **Health** tab.
3. Click **Ping**.  
The **Ping** page is displayed.
4. On the **Ping** page, the IP address of the target switch is populated. Type the packet size and the TTL (Time to Live) value after which a packet is discarded from the network. As shown in the following example, after the ping, the page displays the number of data packets transmitted, received, and lost and the time required following the ping from the controller to the switch to establish communication.

**FIGURE 66** Pinging the switch



5. Click **Trace Route**.  
The **Trace Route** page is displayed.

- On the **Trace Route** page, enter the TTL (Time to Live) value after which the packet is discarded from the network.  
As shown in the following example, the page displays the IP address of the hops the packet takes as it traverses the network between the switch and the controller.

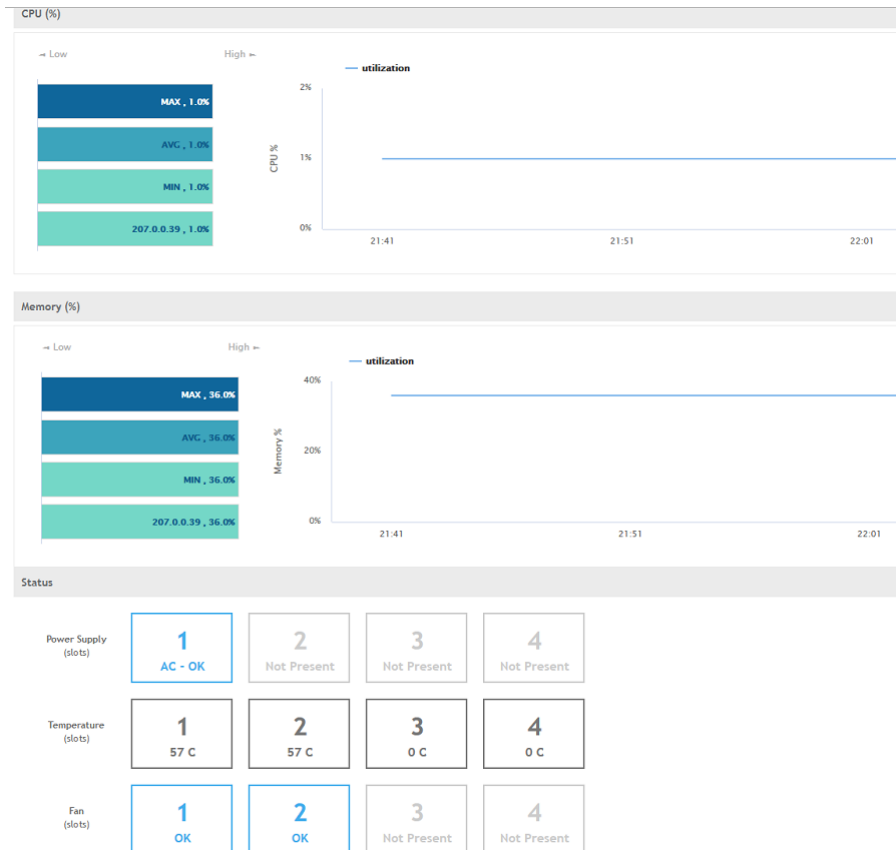
**FIGURE 67** Tracing the packet route through the network



- From the drop-down menu, select the duration for which you want to view the switch health.


As shown in the following example, information on switch health is displayed on the **Health** Tab, based on your selections.

**FIGURE 68** Health Tab



The following information is displayed based on the duration selected:

- CPU (%):** The CPU usage of the switch, including the minimum, maximum, average, and current CPU usage trends of the switch.
- Memory (%):** The memory usage of the switch, including the minimum, maximum, average, and current memory usage trends of the switch.
- Status:** The health status of the power supply, temperature, and the fans for up to four switch modules are displayed. OK indicates the parameter and components are in good health.

You can click  to modify the display settings. You can view the trend as a graph or a table. You can also modify the display to reflect the switch name, MAC address, or IP address.

## Viewing Alarms

Syslog messages from the switch are sent to the controller to periodically communicate switch health and status. It also brings your attention to issues that may need resolution at the switch level. You can view these details from the **Alarms** tab for individual switches, stacks and switch groups.

Syslog messages from the switch are categorized as **Major** and **Critical**, and are displayed as **events** in the SZ controller. From these events, the following messages are displayed as **alarms** in the controller interface:

- Power Supply failure
- Fan failure
- Module Insertion or removal
- Temperature above the threshold warning
- Stack member unit failure
- PoE power allocation failure
- DHCP offer dropped message
- Port put into error disable state

The remaining syslog messages which are categorized by other severity levels are listed in the `switchevent.log` file available in **Diagnostics > Application Logs**.

The alarms generate for the switch also reflect in the **Events & Alarms > Alarms** page.

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.



2. Select the switch or group. Then select the **Alarms** tab.

**FIGURE 69** ICX Alarms Tab

Date and Time	Code	Alarm Type	Severity	Status	Activity	Acknowledged On
2018/05/15 16:38:05	20004	Temperature above thres...	Critical	Outstanding	[DUI3839L0WS / ABHI-ICX] Temperature is over warning level on unit 1	N/A
2018/05/15 16:38:05	20004	Temperature above thres...	Critical	Outstanding	[DUI3839L0WS / ABHI-ICX] Stack unit 1 Temperature 72.0 C degrees, warning level 1.0 ...	N/A
2018/05/15 15:43:50	20004	Temperature above thres...	Critical	Outstanding	[DUI3839L0WS / ABHI-ICX] Stack unit 1 Temperature 71.0 C degrees, warning level 1.0 ...	2018/05/15 15:44:20
2018/05/15 14:18:05	20004	Temperature above thres...	Critical	Outstanding	[DUI3839L0WS / ABHI-ICX] Stack unit 1 Temperature 70.0 C degrees, warning level 1.0 ...	N/A
2018/05/15 12:13:50	20004	Temperature above thres...	Critical	Outstanding	[DUI3839L0WS / noSuchInstance] Stack unit 1 Temperature 70.0 C degrees, warning le...	N/A
2018/05/15 12:13:50	20004	Temperature above thres...	Critical	Outstanding	[DUI3839L0WS / noSuchInstance] Temperature is over warning level on unit 1	N/A
2018/05/15 11:53:27	20004	Temperature above thres...	Critical	Outstanding	[DUI3839L0WS / noSuchInstance] Stack unit 1 Temperature 69.0 C degrees, warning le...	N/A
2018/05/15 11:37:05	20004	Temperature above thres...	Critical	Outstanding	[DUI3839L0WS / ABHI-ICX] Stack unit 1 Temperature 69.0 C degrees, warning level 1.0 ...	N/A

The following information is displayed in the **Alarms** tab:

- **Date and Time:** Displays the date and time when the alarm was triggered
- **Code:** Displays the alarm code (see the Alarm and Reference Guide for your controller platform for more information).
- **Alarm Type:** Displays the type of alarm event that occurred (for example, switch reset to factory settings).
- **Severity:** Displays the severity level assigned to the events such as Critical, Major, Minor and Warning.
- **Status:** Indicates whether the alarm has already been cleared or still outstanding.
- **Activity:** Displays additional details about the alarm, such as how long was the switch offline for
- **Acknowledged On:** Displays the date and time when the administrator acknowledge the alarm
- **Cleared By:** Displays information about who cleared the alarm
- **Cleared On:** Displays the date and time when the alarm was cleared
- **Comments:** Displays administrator notes recorded during alarm management



Click to export the alarms details to a CSV file. Check the default download folder of your web browser and look for a file named *alarms.csv* and view it using a spreadsheet application

Clearing an alarm removes the alarm from the list but keeps it on the controller's database. Select the alarm from the list and click **Clear Alarm**. The **Clear Alarm** page appears. Type your comments and select **Apply**.

Acknowledging an alarm lets other administrators know that you have examined the alarm. Click **Acknowledge Alarm** to acknowledge an alarm. After you acknowledge an alarm, it will remain on the list of alarms and will show the date and time that you acknowledged it.



You can also view alarms by their severity, status, date and time stamp. Click to apply filters.

## Viewing Events

Events are triggered by an occurrence or the detection of certain conditions in the switch. For example, when the temperature of the device reaches warning levels, or when the fan speed changes, an event is triggered. You can view these details from the **Events** tab for individual switches, stacks and switch groups.

The alarms generate for the switch also reflect in the **Events & Alarms > Events** page.

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.
2. Select the switch or group. Then select the **Events** tab.


**FIGURE 70** ICX Events Tab

Date and Time	Code	Type	Severity	Activity
2018/05/15 16:38:05	20001	Switch Alert Message	Major	[DUI3839L0WS / ABHI-ICX] Temperature is over warning level on unit 1
2018/05/15 16:38:05	20001	Switch Alert Message	Major	[DUI3839L0WS / ABHI-ICX] Stack unit 1 Temperature 72.0 C degrees, warning level 1.0 C degrees, shutdown level 105.0 C degrees
2018/05/15 16:36:20	20001	Switch Alert Message	Major	[DUI3839L0WS / ABHI-ICX] Temperature is over warning level on unit 1
2018/05/15 16:36:20	20001	Switch Alert Message	Major	[DUI3839L0WS / ABHI-ICX] Stack unit 1 Temperature 72.0 C degrees, warning level 1.0 C degrees, shutdown level 105.0 C degrees
2018/05/15 16:34:35	20001	Switch Alert Message	Major	[DUI3839L0WS / ABHI-ICX] Temperature is over warning level on unit 1
2018/05/15 16:34:35	20001	Switch Alert Message	Major	[DUI3839L0WS / ABHI-ICX] Stack unit 1 Temperature 72.0 C degrees, warning level 1.0 C degrees, shutdown level 105.0 C degrees
2018/05/15 16:32:50	20001	Switch Alert Message	Major	[DUI3839L0WS / ABHI-ICX] Temperature is over warning level on unit 1
2018/05/15 16:32:50	20001	Switch Alert Message	Major	[DUI3839L0WS / ABHI-ICX] Stack unit 1 Temperature 72.0 C degrees, warning level 1.0 C degrees, shutdown level 105.0 C degrees

The following information is displayed in the **Events** tab:

- **Date and Time:** Displays the date and time when the event occurred
- **Code:** Displays the event code (see the Alarm and Event Reference Guide for your controller platform more information)
- **Type:** Displays the type of event that occurred (for example, Switch configuration updated)
- **Severity:** Displays the severity level assigned to the events such as Critical, Debug, Informational, Warning, Major etc .
- **Activity:** Displays additional details about the event



Click  to export the events details to a CSV file. Check the default download folder of your web browser and look for a file named *events.csv* and view it using a spreadsheet application



You can also view alarms by their severity, date and time. Click  to apply filters.

## Viewing LLDP Neighbor Information

You can view information about the LLDP neighbors such as printers, VOIP devices, or other user equipment connected to the switch, in addition to the LLDP AP neighbors connected to the switch. Link layer discovery protocol or LLDP is used to discover and identify the clients.

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.
2. Select the switch or group. Then select the **LLDP Neighbors** tab.

**FIGURE 71** LLDP Neighbors Connected to the Switch

Device Name	Remote MAC	Device Type	Remote Port	Local Port	Local MAC	Remote Device Description
RuckusAP	08:00:27:1e:fa:02	Bridge, Ruckus...	vst0	GigabitEthernet1/0/6	809c:1e:1da:b3:03	Ruckus 1812 RuckusMedia Protocol Wireless AP/MP Version: 1.8.9.0.08
RuckusAP	08:00:27:1e:fa:04	Bridge, Ruckus...	vst0	GigabitEthernet1/0/4	809c:1e:1da:b3:03	Ruckus 1812 RuckusMedia Protocol Wireless AP/MP Version: 1.8.9.0.08
RuckusAP	08:00:27:1e:fa:06	Bridge, Ruckus...	vst0	GigabitEthernet1/0/2	809c:1e:1da:b3:03	Ruckus 1812 RuckusMedia Protocol Wireless AP/MP Version: 1.8.9.0.08
RuckusAP	08:00:27:1e:fa:08	Bridge, Ruckus...	vst0	GigabitEthernet1/0/8	809c:1e:1da:b3:03	Ruckus 1812 RuckusMedia Protocol Wireless AP/MP Version: 1.8.9.0.08

Device Name	Remote MAC	Device Type	Remote Port	Local Port	Local MAC	Remote Device Description
BRD-CORE	08:00:27:1e:fa:03	Bridge, Router	GigabitEthernet1/1/2	GigabitEthernet1/0/8	809c:1e:1da:b3:03	BRD
POE	08:00:27:1e:fa:05	Bridge, Router	Port 1/0/1	GigabitEthernet1/0/5	809c:1e:1da:b3:03	OSW7209 24 Port Gigabit Layer 2 PoE Managed Switch with Static Routing
usb-video44100	18:05:7b:06:7b:08	Bridge, Ruckus...	vst0	GigabitEthernet1/0/8	809c:1e:1da:b3:03	Ubiquiti 16.34.2 LTS Linux 4.4.0-20-generic 691 Ubuntu 5.0P Thu Apr 27 05:28:09 UTC 2017 x86_64
usb-video44100	18:05:7b:06:7b:08	Bridge, Ruckus...	vst0	GigabitEthernet1/0/9	809c:1e:1da:b3:03	Ubiquiti 16.34.2 LTS Linux 4.4.0-20-generic 691 Ubuntu 5.0P Thu Apr 27 05:28:09 UTC 2017 x86_64

The following information is displayed in the **LLDP Neighbors** tab for devices to the switch:

- Device Name: displays the name of the LLDP neighbor or AP neighbor connected to the switch
- Remote MAC: displays the remote MAC address of the device
- Device Type: displays the name of the device type (for example, Router)
- Local Port: displays the local port the device is connected to
- Local MAC: displays the local MAC address of the device
- Remote Port: displays the remote port to which the device is connected
- Remote Device: displays the name of the remote device

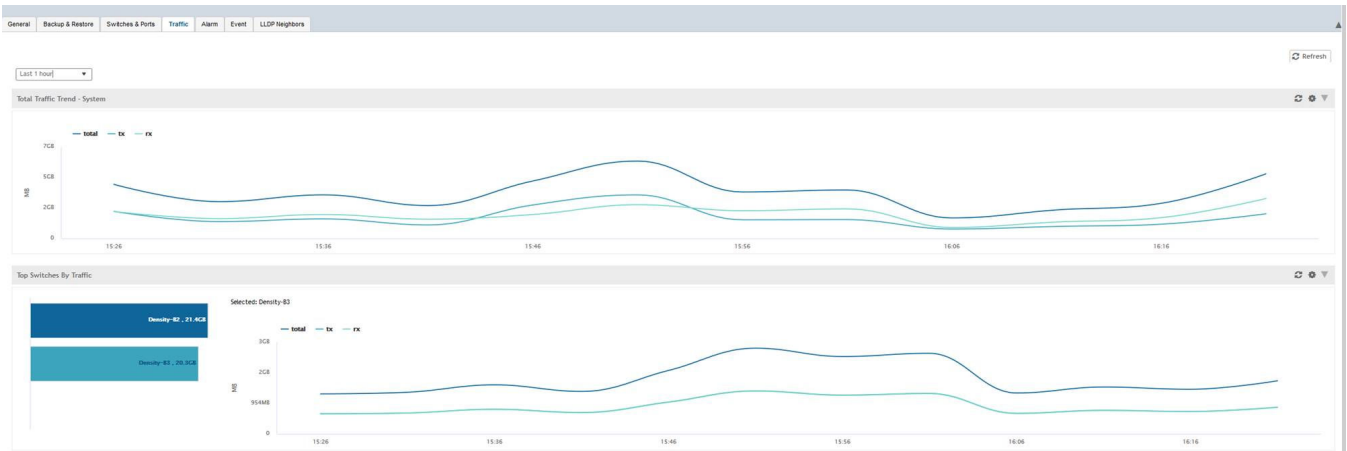
## Viewing Traffic Trends in the Switch

You can view statistical information about how traffic is handled at the switch level. These details are available for individual switches, stacks and switch groups.

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.

2. Select the switch or group. Then select the **Traffic** tab.

**FIGURE 72** Traffic Trend for a Switch Group



**FIGURE 73** Traffic Trend for a Switch



The following information is displayed in the **Traffic** tab. You can view the traffic trend for the last 1 hour or 24 hours:

- **Total Traffic Trend:** provides a graphical representation of the network traffic usage over a period of time in the switch or switch group. It also indicates the amount of traffic or data transmitted (tx) and received (rx) by the group in MB, at a certain time and date.
- **Top Switch by Traffic:** provides a graphical representation of the top switches that handled maximum network traffic over a period of time, in the switch group. You can click on the switch address to view the traffic trend. This trend is only available for switch groups.
- **Top Ports by Traffic:** provides a graphical representation of the top ports that handled maximum network traffic over a period of time, for a switch. You can click on the port address to view the traffic trend. This trend is only available for individual switches.

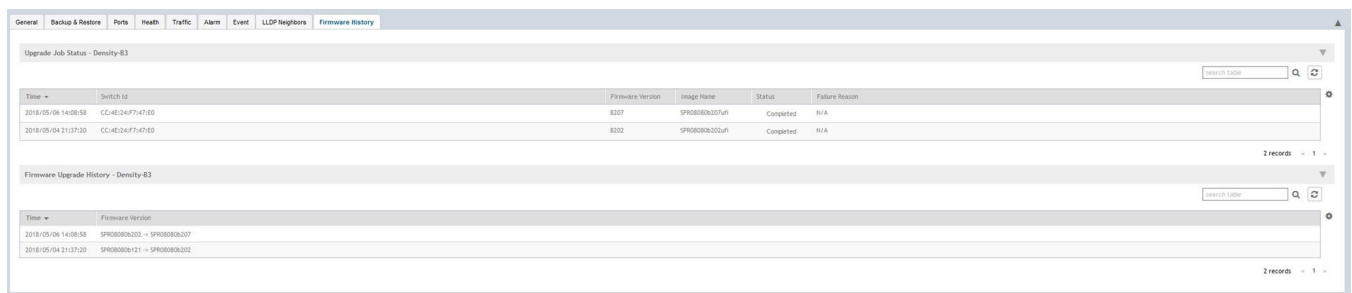
# Viewing Firmware History of the Switch

You can view the detailed status and result of the firmware update to a switch. You can also view a history of firmware upgrades that were previously carried out on the switch.

You must have upgraded the firmware of the switch as described in [Scheduling a Firmware Upgrade](#) on page 144

1. From the left pane, select **Switches**.  
The **ICX Switches** page appears.
2. Select the switch or group. Then select the **Firmware History** tab.  
The **Firmware History** tab is displayed.

**FIGURE 74** Viewing Firmware History



Time	Switch ID	Firmware Version	Image Name	Status	Failure Reason
2018/05/04 14:08:58	CC4E24A774789	8307	SP808080207u	Completed	N/A
2018/05/04 21:07:20	CC4E24A774789	8302	SP808080207u	Completed	N/A

Time	Firmware Version
2018/05/04 14:08:58	SP808080202 → SP808080207
2018/05/04 21:07:20	SP808080207 → SP808080202

You can verify the status of the upgrade from the **Upgrade Job Status** section which displays the time, switch ID, firmware version, image name, status and failure reasons (if any) for the upgrade.

The **Firmware Upgrade History** section displays the time of the pervious upgrade operations, and firmware versions to which the upgrade was done.



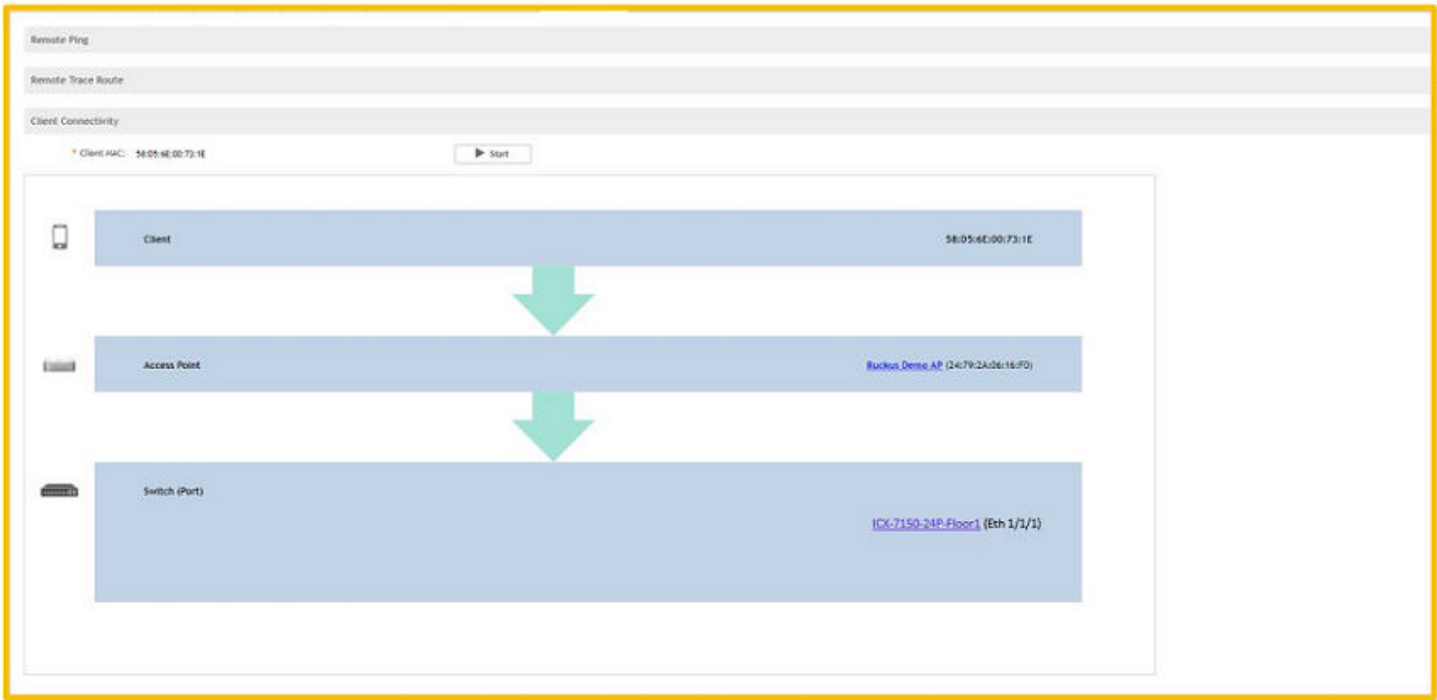
# Troubleshooting Switch Issues

- Troubleshooting Using Custom Events..... 164
- Troubleshooting Using Remote Operations..... 164

You can troubleshoot issues related to wired and wireless clients connected to the switch at the system level from the **Troubleshooting** tab. You can use Remote operations, Client Connectivity and Custom Events to troubleshoot issues with switches or switch groups.

To troubleshoot issues with an AP client, use the MAC address of the client on the **Troubleshooting** tab of a switch or switch group. Once you enter the MAC address of the client, SmartZone displays how the client is connected to the network, including the AP, the switch, and the switch port on which the client MAC is learned. As an example, if a printer is connected to an AP, which in turn is connected to a switch that is managed by a SmartZone controller, you can troubleshoot any connectivity issues between the devices from the **Troubleshooting** tab by providing the MAC address of the printer.

**FIGURE 75** Client MAC Search

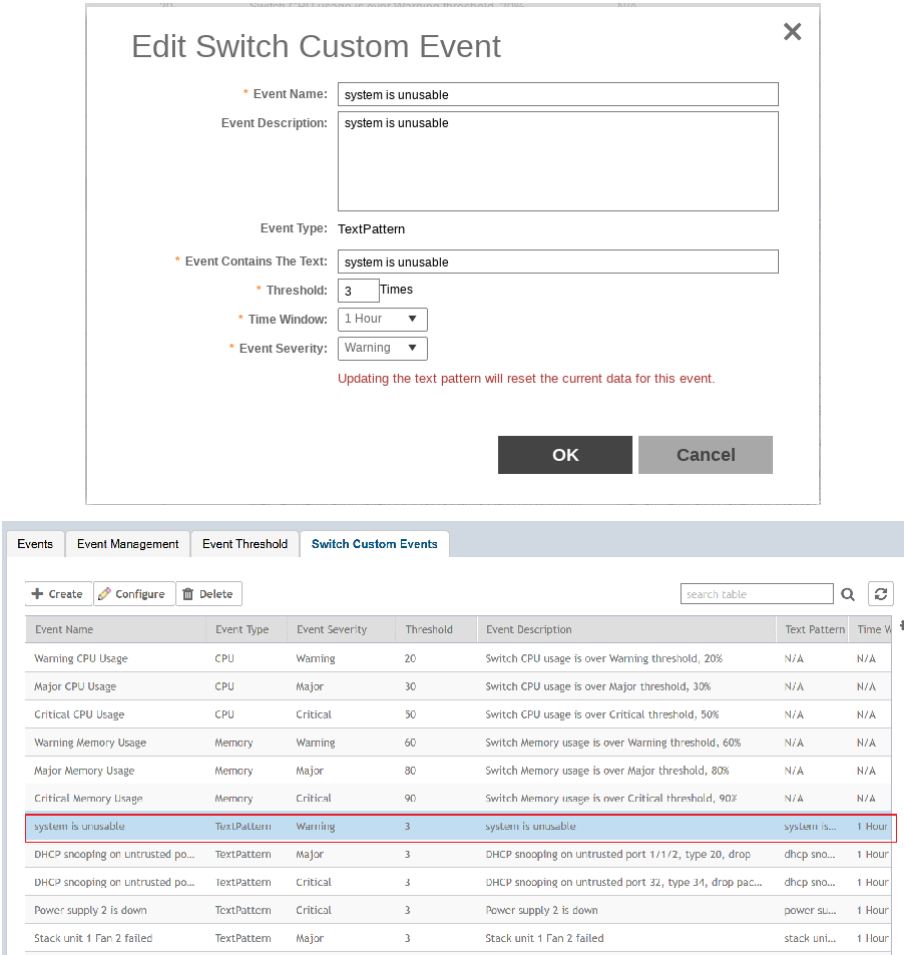


# Troubleshooting Using Custom Events

You can create custom events to define failure scenario and use them to generate troubleshoot switch issues.

For example, you can create a "system is unusable" event with the following settings. Based on this event definition and configuration, if any switch sends this message thrice in one hour, the controller triggers a Custom Event. You can view the "system unavailable" event from the **Switch Custom Events** page. For more information on custom events, see [Creating Custom Events for ICX Switches](#) on page 359

FIGURE 76 Troubleshooting switch issues through custom events



# Troubleshooting Using Remote Operations

You can use the **Remote Ping** and **Remote Trace Route** options to identify issues with individual switches.

Follow these steps to troubleshoot switch issues using remote ping and traceroute.

- From the left pane, select **Switches**.  
The **ICX Switches** page is displayed.
- Select a switch.



3. Click the **Troubleshooting** tab.

4. Click **Remote Ping**.

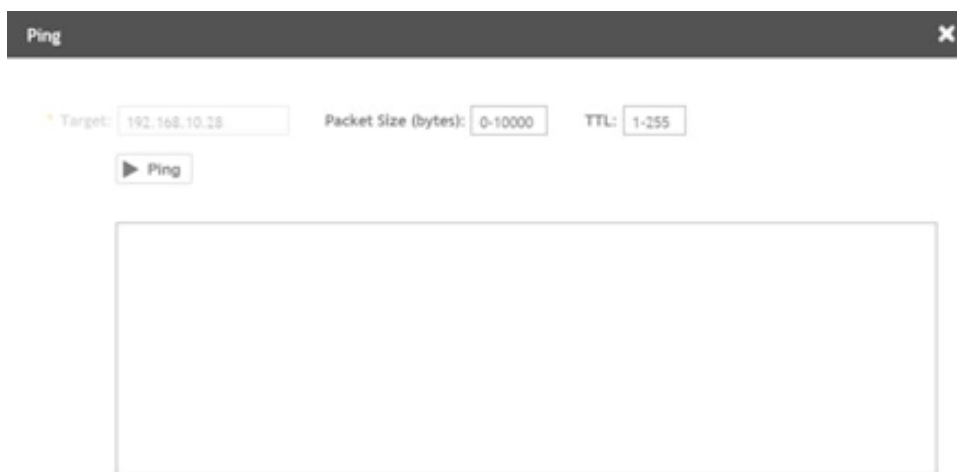
The **Ping** page is displayed.

5. On the **Ping** page, enter the IP address of the destination (target) you are checking, along with the packet size and the TTL (Time to Live) value after which the packet is discarded from the network.

6. Click **Ping**.

The controller pings the ICX switch at the destination IP address provided. As shown in the following example, the results displayed include the number of data packets transmitted, received, and lost and the time required for the controller to ping the switch to establish communication.

**FIGURE 77** Pinging the switch



The screenshot shows a web interface for the 'Ping' function. At the top, there is a dark header bar with the word 'Ping' on the left and a close button (X) on the right. Below the header, there are three input fields: 'Target:' with the value '192.168.10.25', 'Packet Size (bytes):' with the value '0-10000', and 'TTL:' with the value '1-255'. Below these fields is a button with a play icon and the text 'Ping'. At the bottom of the form is a large, empty rectangular box intended for displaying the results of the ping test.

7. Click **Remote Trace Route**.

The **Trace Route** page is displayed.

8. Enter the IP address of the destination being checked for connectivity and the TTL (Time to Live) value after which the packet is discarded from the network.

9. Click **Trace Route**.

As shown in the following example, the **Trace Route** page displays the IP address of the hops the packet traverses through the network between the switch and the controller.

**FIGURE 78** Tracing the packet route through the network



# Viewing Switches on the Dashboard

The wired dashboard displays detailed information about the health of the switch and graphs indicating traffic trends.

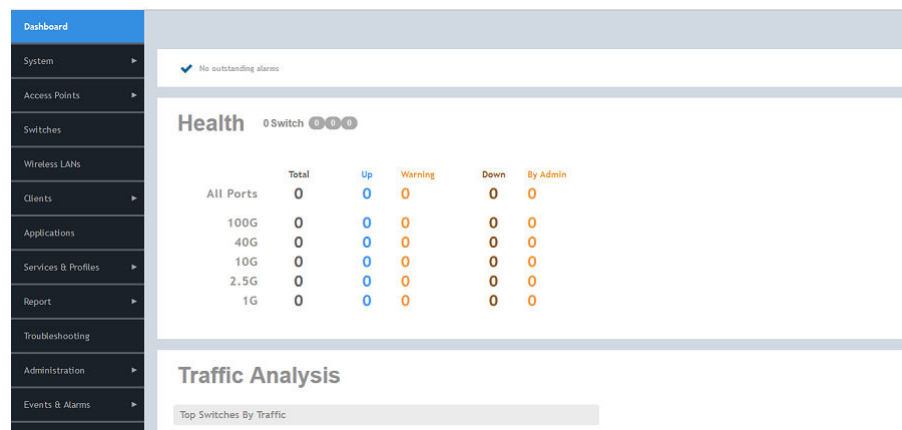
1. From the SmartZone interface, click **Dashboard** in the left menu.

The **Dashboard** page is displayed.

2. Click **Wired**.

The **Wired** page is displayed as shown in the following example.

**FIGURE 79** Wired Devices



The **Health** section displays the number of switches that are online, offline, and flagged. It also displays the number of ports by speed and indicates whether they are Up, Warning, Down, or Down By Admin.

The **Traffic Analysis** section displays the following information:

- Top switches based on traffic
- Top ports based on traffic
- Top switches based on port errors
- Top switches based on PoE utilization



# Working with WLANs and WLAN Groups

---

• Zones, AP Groups, and WLANs.....	169
• Viewing Modes.....	169
• WLAN Groups.....	170
• Creating a WLAN Configuration.....	171
• Managing WLANs.....	189

## Zones, AP Groups, and WLANs

If your wireless network covers a large physical environment (for example, multi-floor or multi-building office) and you want to manage and provide different WLAN services to different areas of your environment, you can virtually split them using the following hierarchy:

- Zones—Comprises of multiple WLAN groups
- WLAN Groups—Comprises of multiple WLANs
- WLANs—Wireless network service

### NOTE

In vSZ-E and SZ100, when the system is upgraded to release 3.5, the new UI and re-architected stats database will prevent the system from displaying AP and zone stats if the AP/zone is operating on 3.4 or prior releases. In order to make full use of the UI introduced in 3.5, zones and APs should be updated to 3.5 as well. Operationally, the zones will still work, but stats visibility will be impacted.

## Viewing Modes

The **View Mode** on upper-right corner of the page provides two options to view the WLANs available in the system:

- **List**—Displays the list of all WLANs irrespective of the Zone or Group they belong.
- **Group**—Displays the list of WLANs that belong to a specific Zone or Group.

The following WLAN details can be viewed regardless of the mode selected:

- **Name**
- **Alert**
- **SSID**
- **Auth Method**
- **Encryption Method**
- **Clients**
- **Traffic**
- **VLAN**
- **Application Recognition**
- **Tunneled**

## WLAN Groups

A WLAN group is a way of specifying which APs or AP groups provide which WLAN services. For example, if your wireless network covers three floors of a building and you need to provide wireless access to visitors only on the first floor:

1. Create a WLAN service (for example, **Guest Only Service**) that provides guest-level access only.
2. Create a WLAN group (for example, **Guest Only Group**), and then assign **Guest Only Service** (WLAN service) to **Guest Only Group** (WLAN group).
3. Assign APs on the 1st Floor (where visitors need wireless access) to your **Guest Only Group**.



Any wireless client that associates with APs assigned to the **Guest Only Group** will get the guest-level access privileges defined in your **Guest Only Service**. APs on the 2nd and 3rd floors can remain assigned to the default WLAN Group and provide normal-level access.

### NOTE



- WLAN groups are configured at the zone level.
- Creating WLAN groups is optional. If you do not need to provide different WLAN services to different areas in your environment, you do not need to create a WLAN group.
- A default WLAN group called **default** exists. The first 27 WLANs that you create are automatically assigned to this default WLAN group.
- A WLAN group can include a maximum of 27 member WLANs. For dual radio APs, each radio can be assigned to only one WLAN group (single radio APs can be assigned to only one WLAN group).

## Creating a WLAN Group

To create a WLAN group:




1. In the Wireless LANs page, from the **System** tree hierarchy, select the zone where you want to create a WLAN Group.
2. Click the add  button. The Create WLAN Group page appears.
3. Enter a **Name** and **Description** for the WLAN group.
4. From the **Available WLANs** list perform one of the following option:
  - select the required WLAN and click the Move button. It will appear in the **Selected WLANs** list.
  - click the add  button to create a new WLAN service. The Create WLAN Configuration page appears. Refer [Creating a WLAN Configuration](#) on page 171.

### NOTE

To edit or delete a WLAN configuration, select the WLAN from the Available WLANs list and click Configure  or Delete  respectively.

5. Click **Next**, The Create WLAN Group form appears.
6. Click **OK**.

### NOTE

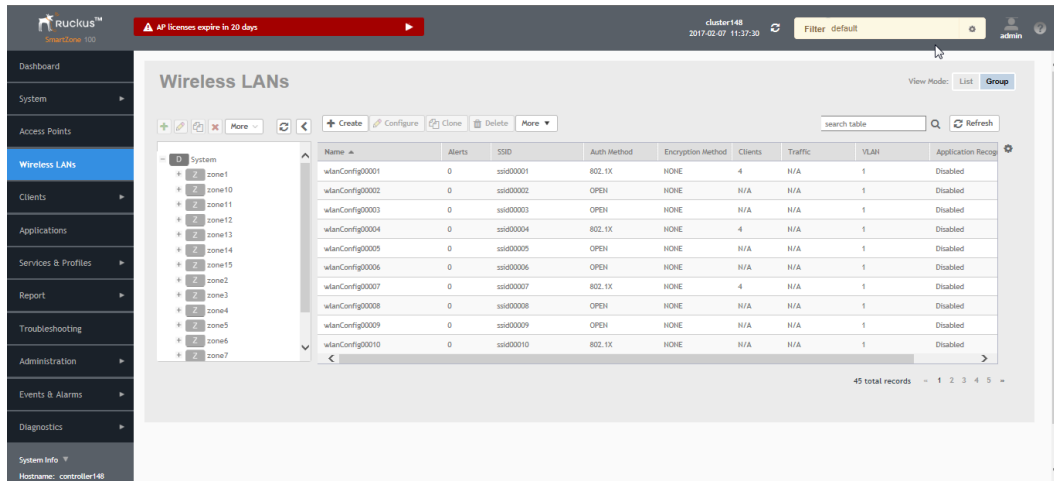
You can also edit, clone, and delete WLAN group by selecting the options Configure , Clone , and Delete  respectively, from the Wireless LANs page.

# Creating a WLAN Configuration

To create a WLAN configuration:

1. In the Wireless LANs page, from the **System** tree hierarchy, select the **Zone** where you want to create a WLAN.

**FIGURE 80** Wireless LANs



2. Click **Create**, [Figure 81](#) appears.

**FIGURE 81** Create WLAN Configuration

## Create WLAN Configuration

General Options

Name:

SSID:

Description:

Zone:

WLAN Group: No data available

+ Create

Authentication Options

Authentication Type:

☒ Standard usage (For most regular wireless networks)
 ☐ Hotspot (WISPr)
 ☐ Guest Access
 ☐ Web Authentication

☐ Hotspot 2.0 Access
 ☐ Hotspot 2.0 Onboarding
 ☐ WeChat

Method:

☒ Open
 ☐ 802.1X EAP
 ☐ MAC Address
 ☐ 802.1X & MAC

OK

Cancel

3. Set the required configurations as explained in the below table.

4. Click **OK**.

**TABLE 18 WLAN Configurations**



Field	Description	Your Action
<b>General Options</b>		
<b>Name</b>	Indicates the user-friendly administrative name for the WLAN.	Enter a name.
<b>SSID</b>	Indicates the SSID for the WLAN.	Enter the SSID
<b>Description</b>	Indicates a user-friendly description of the WLAN's settings or function.	Enter a short description.
<b>Zone</b>	Indicates the zone to which the WLAN belongs.	Select the Zone to which the WLAN settings apply.
<b>WLAN Groups</b>	Indicates the WLAN group(s) to which the WLAN applies.	Select the WLAN Groups.
<b>Authentication Options</b>		
<b>Authentication Type</b>	<p>Defines the type of authentication flow for the WLAN.</p> <p><b>NOTE</b> Authentication types such as WeChat, Web Authentication and Guest Access are not supported by APs in IPv6 mode.</p>	<p>Select the required option:</p> <ul style="list-style-type: none"> <li>• <b>Standard Usage</b>—This is a regular WLAN suitable for most wireless networks.</li> <li>• <b>Hotspot (WISPr)</b>—Click this option if want to use a hotspot service (use this type for external captive portal workflows) or WISPr.</li> </ul> <p><b>NOTE</b> Hotspot (WISPr) applies to WLAN traffic that is tunneled and not tunneled.</p> <ul style="list-style-type: none"> <li>• <b>Guest Access</b>—Click this option if you want guest users to use this WLAN. After you complete creating this WLAN for guest access, you can start generating guest passes.</li> </ul> <p>For more information about Hotspot 2.0 online signup, see the Hotspot 2.0 Reference Guide for this release.</p> <ul style="list-style-type: none"> <li>• <b>Web Authentication</b>—Click this option if you want to require all WLAN users to complete a web-based logon to this network every time they attempt to connect.</li> <li>• <b>Hotspot 2.0 Access</b>—Click this option if you want a Hotspot 2.0 operator profile that you previously created to use this WLAN. See the Hotspot 2.0 Reference Guide for this release.</li> <li>• <b>Hotspot 2.0 Onboarding</b>—Click this option if you want to use this WLAN for Hotspot 2.0 onboarding. See the Hotspot 2.0 Reference Guide for this release for more information. Hotspot 2.0 onboarding allows for Open and 802.1x EAP authentication methods.</li> <li>• <b>WeChat</b>—Click this option if you want the WLAN usage through WeChat.</li> </ul>
<b>Authentication Options</b>		
<b>Method</b>	Specifies the authentication mechanism.	<p>Select the following option:</p> <ul style="list-style-type: none"> <li>• <b>Open</b> (Default)—No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication.</li> </ul> <p>If you clicked <b>Web Authentication</b> in <b>Authentication Type</b>, <b>Open</b> is the only available authentication</p>



**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
		<p>option, even though PSK-based encryption can be supported.</p> <ul style="list-style-type: none"> <li>• <b>802.1x EAP</b>—A very secure authentication/encryption method that requires a back-end authentication server, such as a RADIUS server. Your choice mostly depends on the types of authentication the client devices support and your local network authentication environment. If you select <b>Enable RFC Location Delivery Support for Authentication &amp; Accounting Server</b>, enter the <b>Operator Realm</b>.</li> </ul> <p>Selecting the authentication method as Hotspot (WISPr), also allows you to select 802.1x EAP as an authentication option. This enables a two-step authentication method when shared and pre-authenticated devices are used, or when user equipment is shared among multiple users. The device access is successful when both authentication processes are completed successfully - 802.1x EAP authentication first, followed by Hotspot (WISPr) authentication.</p> <ul style="list-style-type: none"> <li>• <b>802.1x EAP with MAC address</b>—Selecting this option indicates that the 802.1x EAP and MAC address authentication methods must both pass for a user to successfully authenticate. First, MAC address authentication is verified, if that passes, 802.1x EAP authentication is processed. After this two authentication methods succeed, the user equipment gains access to the WLAN. Authentication is done by a back-end RADIUS server.</li> </ul> <p>When this authentication method is selected, the MAC Authentication and MAC Address Format fields will be shown within the Authentication Options section.</p> <ul style="list-style-type: none"> <li>• <b>MAC Address</b>—Authenticate clients by MAC address. <ul style="list-style-type: none"> <li>– <b>MAC Authentication</b>—Requires a RADIUS server and uses the MAC address as the user logon name and password. <ul style="list-style-type: none"> <li>› Select <b>Use user defined text as authentication password</b> (default is device MAC address) and enter the format.</li> </ul> </li> <li>– <b>MAC Address Format</b>—Choose the MAC address format from the drop-down.</li> </ul> </li> </ul>
<b>Encryption Options</b>		
<b>Method</b>	Specifies the encryption method. WPA and WPA2 are both encryption methods certified by the Wi-Fi Alliance; WPA2 with AES is the recommended encryption method. The Wi-Fi Alliance will be mandating the removal of WEP due to its security vulnerabilities, and Ruckus recommends against using WEP if possible.	<p>Select the option:</p> <ul style="list-style-type: none"> <li>• <b>WPA2</b>—Enhanced WPA encryption using AES encryption algorithm. <ol style="list-style-type: none"> <li>1. Choose <b>Algorithm</b>: <ul style="list-style-type: none"> <li>– <b>AES</b>: <ol style="list-style-type: none"> <li>a. Enter <b>PassPhrase</b></li> <li>b. Select or clear <b>Show</b></li> <li>c. Select <ul style="list-style-type: none"> <li>› the <b>Enable 802.11 Fast BSS Transition</b> check box and enter the <b>Mobility Domain ID</b>.</li> <li>› the required <b>802.11w MFP</b> option.</li> </ul> </li> </ol> </li> </ul> </li> </ol> </li> </ul>

**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
		<ul style="list-style-type: none"> <li>- <b>AUTO:</b> <ul style="list-style-type: none"> <li>a. Enter <b>PassPhrase</b></li> <li>b. Select or clear <b>Show</b></li> </ul> </li> <li>• <b>WPA-Mixed</b>—Allows mixed networks of WPA and WPA2 compliant devices. Use this setting if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.               <ul style="list-style-type: none"> <li>1. Choose <b>Algorithm: AES</b> or <b>AUTO</b></li> <li>2. Enter <b>PassPhrase</b></li> <li>3. Select or clear <b>Show</b></li> <li>4. Select <b>Enable 802.11 Fast BSS Transition</b>.</li> <li>5. Enter the <b>Mobility Domain ID</b>.</li> </ul> </li> <li>• <b>WEP-64 (40 bits)</b>—Provides a lower level of encryption, and is less secure, using 40-bit WEP encryption.               <ul style="list-style-type: none"> <li>1. Choose the <b>WEP Key</b>.</li> <li>2. Enter <b>HEX</b> value.</li> </ul> </li> <li>• <b>WEP-128 (104 bits)</b>—Provides a higher level of encryption than WEP-64, using a 104-bit key for WEP encryption. However, WEP is inherently less secure than WPA.               <ul style="list-style-type: none"> <li>1. Choose the <b>WEP Key</b>.</li> <li>2. Enter <b>HEX</b> value.</li> </ul> </li> <li>• <b>None</b></li> </ul>
<b>Data Plane Options</b>		
<b>Access Network</b>	Defines the data plane tunneling behavior.	<p>Enable <b>Tunnel WLAN traffic through Ruckus GRE</b>. Configure the following options as appropriate:</p> <ul style="list-style-type: none"> <li>• <b>GRE Tunnel Profile:</b> Manages AP traffic. Select the profile from the list.</li> <li>• <b>Split Tunnel Profile:</b> Enables split tunneling to manage user traffic between corporate and local traffic. Enable the profile from the list. Click  to create a new profile or click  to edit a profile. By default, the option is disabled.</li> </ul> <p><b>NOTE</b> RuckusGRE or SoftGRE must be enabled on the WLAN before mapping it to a Split Tunnel Profile.</p>
<b>vSZ-D DHCP/NAT</b>	Enables tunneling option for DHCP/NAT.	<p>Select the required check boxes:</p> <ul style="list-style-type: none"> <li>• <b>Enable Tunnel NAT</b></li> <li>• <b>Enable Tunnel DHCP</b></li> </ul>
<b>RADIUS based DHCP/NAT</b>	Enables RADIUS-based DHCP/NAT settings. DHCP server authorizes remote clients and allocates addresses based on replies from a RADIUS server.	<p>Select the required check boxes:</p> <ul style="list-style-type: none"> <li>• <b>Enable RADIUS based NAT</b></li> <li>• <b>Enable RADIUS based DHCP</b></li> </ul>
<b>Authentication &amp; Accounting Server (for WLAN Authentication Type: Standard usage)</b>		

**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
<b>Authentication Server</b>	Specifies the server used for authentication on this network. By enabling Proxy, authentication requests will flow through the controller. In a non-proxy mode, the AP will communicate directly with the authentication server without going through the controller.	<ol style="list-style-type: none"> <li>1. Select the <b>Use controller as proxy</b> check box.</li> <li>2. Select the server from the drop-down menu.</li> <li>3. Select the <b>Enable RFCLocationDeliverySupport</b>.</li> </ol>
<b>Accounting Server</b>	Specifies the server used for accounting messages. By enabling Proxy, accounting messages are sent by the controller. In a non-proxy mode, the AP will communicate accounting messages directly.	<ol style="list-style-type: none"> <li>1. Select the <b>Use controller as proxy</b> check box.</li> <li>2. Select the server from the drop-down.</li> </ol>
<b>Hotspot Portal (for WLAN Authentication Type: Hotspot (WisPr))</b>		
<b>Hotspot (WISPr) Portal</b>	Defines hotspot behavior, like redirects, session timers, and location information, among others.	Select the hotspot portal profile that you want this WLAN to use.
<b>Bypass CNA</b>	Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN.	Select the <b>Enable</b> check box.
<b>Authentication Server</b>	Indicates the authentication server that you want to use for this WLAN.	<p>Choose the option. Options include <b>Local DB</b>, <b>Always Accept</b>, and any AAA servers that you previously added. Additionally, if you want the controller to proxy authentication messages to the AAA server, select the <b>Use Controller as Proxy</b> check box. When the SSH tunnel between the AP and the controller is down, you can enable <b>Backup Authentication Service</b> to back up the AP's authentication services to a secondary device.</p> <p><b>NOTE</b> For WISPr survivability, the customer portal must use the AP WISPr ZD-Style API/Backup AAA authentication to continue the WISPr service.</p>
<b>Accounting Server</b>	Indicates the RADIUS Accounting server that you want to use for this WLAN.	<p>Choose the option. You must have added a RADIUS Accounting server previously. Additionally, if you want the controller to proxy accounting messages to the AAA server, select the <b>Use the Controller as Proxy</b> check box. When the SSH tunnel between the AP and the controller is down, you can enable <b>Backup Accounting Service</b> to back up the AP's accounting services to a secondary device.</p> <p><b>NOTE</b> For WISPr survivability, the customer portal must use the AP WISPr ZD-Style API/Backup AAA authentication to continue the WISPr service.</p>
<b>Guest Access Portal (for WLAN Authentication Type: Guest Access)</b>		
<b>Guest Portal Service</b>	Indicates the guest access portal to be used on this WLAN.	Choose the guest portal service.
<b>Bypass CNA</b>	Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN.	Select the <b>Enable</b> check box.









**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
<b>Guest Authentication</b>	Manages guest authentication.	Select: <ul style="list-style-type: none"> <li><b>Guest</b> to require users to enter their guest pass credentials. Guest passes are managed directly on the controller.</li> <li><b>Always Accept</b> to allow users without guest credentials to authentication.</li> </ul>
<b>Guest Accounting</b>	Indicates the RADIUS Accounting server that you want to use for this WLAN.	Choose the server. You must have added a RADIUS Accounting server previously. Additionally, if you want the controller to proxy accounting messages to the AAA server, select the <b>Use the Controller as Proxy</b> check box.
<b>Authentication &amp; Accounting Server (for WLAN Authentication Type: Web Authentication)</b>		
<b>Web Authentication Portal</b>	Indicates the web authentication portal to use for this WLAN.	Choose the web authentication portal from the drop-down.
<b>Bypass CNA</b>	Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN.	Select the <b>Enable</b> check box.
<b>Authentication Server</b>	Indicates the authentication server that you want to use for this WLAN.	Choose the option. Options include <b>Local DB</b> , <b>Always Accept</b> , and any AAA servers that you previously added. Additionally, if you want the controller to proxy authentication messages to the AAA server, select the <b>Use the Controller as Proxy</b> check box.
<b>Accounting Server</b>	Indicates the RADIUS Accounting server that you want to use for this WLAN.	Choose the server. You must have added a RADIUS Accounting server previously. Additionally, if you want the controller to proxy accounting messages to the AAA server, select the <b>Use the Controller as Proxy</b> check box.
<b>Hotspot 2.0 Profile (for WLAN Authentication Type: Hotspot 2.0 Access)</b>		
<b>Hotspot 2.0 Profile</b>	Indicates the profile, which includes operator and identify provider profiles.	Choose the profile.
<b>Authentication Server RFC 5580</b>	Supports RFC 5580 location delivery on the WLAN, which carries location information in RADIUS exchanges.	Select the check box.
<b>Accounting Server Updates</b>	Indicate the frequency to sends interim updates. Configure the account update interval for accounting servers defined in the Hotspot 2.0 Identity Provider profile.	Enter the duration in minutes. <i>Range:</i> 0 through 1440.
<b>We Chat Portal (for WLAN Authentication Type: We Chat)</b>		
<b>We Chat Portal</b>	Defines the We Chat authentication URL, DNAT destination, and other information.	Select a We Chat portal service.
<b>Accounting Server</b>	Indicates the RADIUS Accounting server that you want to use for this WLAN.	Choose the server. You must have added a RADIUS Accounting server previously. Additionally, if you want the controller to proxy accounting messages to the AAA server, select the <b>Use the Controller as Proxy</b> check box.
<b>Forwarding Profile ( for WLAN Usage &gt; Access Network)</b>		
<b>Forwarding Policy</b>	Defines special data packet handling to be taken by the data plane when the traffic is tunneled.	<b>Forwarding Profile is Factory Default.</b> It is disabled.
<b>Options</b>		
<b>Wireless Client Isolation</b>	Prevents wireless clients from communicating with each other.	Enable <b>Isolate wireless client traffic from all hosts on the same VLAN/subnet</b>

**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
		<p>Enable the following required options as appropriate:</p> <ul style="list-style-type: none"> <li>• <b>Isolate unicast packets:</b> Isolates only unicast packets between a client isolation-enabled client and other clients of AP. By default, the option is enabled.</li> <li>• <b>Isolate multicast packets:</b> Isolates only multicast packets between a client isolation-enabled client and other clients of AP. By default, the option is disabled.</li> <li>• <b>Automatic support for VRRP:</b> Isolates packets in VRRP deployment. By default, the option is disabled indicating that the AP is not in a VRRP deployment.</li> </ul>
<b>Isolation Whitelist</b>	Defines wired destinations on the local subnet that can be reached, even if client isolation is enabled.	Select the option.
<b>Priority</b>	Determines high vs low transmit preference of one WLAN compared to another. Traffic for high priority WLAN is always sent before low priority WLANs in the same QoS category (background, best effort, video, voice).	<p>Choose the priority:</p> <ul style="list-style-type: none"> <li>• <b>High</b></li> <li>• <b>Low</b></li> </ul>
<b>RADIUS Option</b>		
<b>NAS ID</b>	Defines the ID sent to the RADIUS server, which will identify the AP.	<p>Choose the option:</p> <ul style="list-style-type: none"> <li>• <b>WLAN BSSID</b></li> <li>• <b>AP MAC</b></li> <li>• <b>User-defined</b></li> </ul>
<b>NAS Request Timeout</b>	Indicates the duration after which an expected RADIUS response message is considered to have failed.	<p>Enter the timeout period (in seconds).</p> <p><b>NOTE</b> It is recommended to configure the same values for <b>NAS Request Timeout</b>, <b>NAS Max Number of Retries</b>, and <b>NAS Reconnect Primary</b>.</p>
<b>NAS MAX Number of Retries</b>	Indicates the maximum number of failed connection attempts after which the controller will fail over to the backup RADIUS server.	<p>Enter the maximum number of failed connection attempts.</p> <p><b>NOTE</b> It is recommended to configure the same values for <b>NAS Request Timeout</b>, <b>NAS Max Number of Retries</b>, and <b>NAS Reconnect Primary</b>.</p>
<b>NAS Reconnect Primary</b>	Indicates the time interval after which the controller will recheck if the primary RADIUS server is available when the controller has failed over to the backup RADIUS server.	<p>Enter the duration in minutes. <i>Range:</i> 1 through 60 minutes. The default interval is 5 minutes.</p> <p><b>NOTE</b> It is recommended to configure the same values for <b>NAS Request Timeout</b>, <b>NAS Max Number of Retries</b>, and <b>NAS Reconnect Primary</b>.</p>
<b>Called Station ID</b>	Indicates the format for the called station ID, which is sent to the RADIUS server as an attribute, and can be used in policy decision	<p>Select a format:</p> <ul style="list-style-type: none"> <li>• <b>WLAN BSSID</b></li> <li>• <b>AP MAC</b></li> <li>• <b>AP GROUP</b></li> <li>• <b>NONE</b></li> </ul>
<b>Single Session ID Accounting</b>	Enabling this feature allows the APs to maintain one accounting session for a client roaming between APs. If the	Select the <b>Enable</b> check box to use this feature.

**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
	client roams from one AP to another, the accounting session ID and stats will be carried while roaming from one AP to the other. If the feature is not enabled, the accounting session ID is re-generated and stats is also reset, essentially resetting the accounting.	
<b>NAS IP</b>	Indicates the NAS IP address.	Select the option: <ul style="list-style-type: none"> <li>• <b>Disabled</b></li> <li>• <b>SZ Control IP</b></li> <li>• <b>SZ Management IP</b></li> <li>• <b>User-defined</b></li> </ul>
<b>Advanced Options</b>		
<b>User Traffic Profile</b>	Defines the traffic policy that will be applied to users on this WLAN. The default UTP allows all with no rate limits. UTPs can define rate limits as well as L3-7 ACLs and policies.	Select the required option. Click  to add a new profile or click  to edit a profile.
<b>L2 Access Control</b>	Enables the WLAN to blacklist or whitelist a specific set of MAC addresses based on a L2 access control policy.	Select the required option. Click  to add a new policy or click  to edit a policy.
<b>OS Policy</b>	Enables the WLAN to apply a unique policy to a device based on OS type. Use a precedence profile to determine whether a role-based, AAA-based, or OS-based policy will take precedence.	Select the required option. Click  to add a new policy or click  to edit a policy.
<b>Application Recognition and Control</b>	Enables DPI-based L7 application recognition, and if enabled, an application control policy. Recognition and control are performed on the AP.	Select the <b>Enable</b> check box.
<b>URL Filtering</b>	Enables URL filtering on the WLAN controller to block or allow access to specific web sites or web pages.	Click the button and select the URL Filtering Profile. Select the required option. Click  to add a new profile or click  to edit a profile.
<b>Client Fingerprinting</b>	Enables the AP to attempt utilize DHCP fingerprinting to identify client devices by their operating system, device type, and host name.	Select the check box.
<b>Access VLAN</b>	Tags the WLAN traffic with a VLAN ID between 2-4094. By default, all client traffic will be assigned to the native (untagged) VLAN on the AP's Ethernet port, which we represent as VLAN ID 1.	Select the check box and enter the <b>VLAN ID</b> .
<b>Hotspot 2.0 Onboarding</b>	Allows devices to connect to a WiFi network automatically, where in the service providers engage in roaming partnerships to provide seamless access to WiFi networks. The devices are authenticated using credentials or certificates.	Select the check box to allow Hotspot 2.0 Onboarding for the WISPr WLAN.
<b>Hide SSID</b>	Removes the SSID from Beacon frames. By removing the SSID, in most cases, clients will not show this SSID in	Select the check box.

**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
	their scan list unless the device is already configured to connect. This can simplify the network decision for an end user.	
<b>Client Load Balancing</b>	Disables client load balancing on this WLAN if the option is selected.	Select the check box to disable client load balancing on this WLAN.
<b>Proxy ARP</b>	Enables proxy ARP. When proxy ARP is enabled on a WLAN, the AP provides proxy service for stations when receiving neighbor discovery packets (for example, ARP request and ICMPv6 Neighbor Solicit messages), and acts on behalf of the station in delivering ARP replies. When the AP receives a broadcast ARP/Neighbor Solicit request for a known host, the AP replies on behalf of the host. If the AP receives a request for an unknown host, it forwards the request.	Select the check box.
<b>MAX Clients</b>	Limits the number of clients that can associate with this WLAN per AP radio (default is 100). Every connection attempt after this max value will not be permitted to connect.	Enter the number of clients allowed.
<b>802.11d</b>	Adds additional regulatory information to AP beacons and probe responses. This compliance information provides country-specific guidance like permitted channels and transmit power, to ensure that the devices operate within the legal boundaries of the country. 11d is helpful for many devices that cannot independently determine their operating country.	Select the check box to enable this option.
<b>802.11k Neighbor Report</b>	Enhances roaming by providing a list of neighbor APs to the client device. APs build a neighbor AP list via background scanning, and when the client plans to roam, it will request this list from the AP. This list is then used to perform efficient scanning to find a roaming candidate.	Select the check box.
<b>Anti-spoofing</b>	Prevents attacks on genuine clients from rogue clients that could lead to service disruption, data loss and so on. This is achieved by matching the MAC address or IP address (IPv4) of the client with the address in the Ruckus database. If the addresses do not match, the packet is dropped. These checks are also performed on ingress data packets to catch spoofed data packets early.	<p>Enable the option. By default, the following options are also enabled:</p> <ul style="list-style-type: none"> <li>• ARP request rate limit: type the packets to be reviewed for ARP (Address Resolution Protocol) attacks, per minute. In ARP attacks, a rouge clients send messages to a genuine client to establish connection over the network.</li> <li>• DHCP request rate limit: type the packets to be reviewed for DHCP pool exhaustion, per minute. When rouge clients send a DHCP request with a spoofed address, an IP address from the DHCP pool is assigned to it. If this happens repeatedly, the IP addresses in</li> </ul>

**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
		<p>the DHCP pool are exhausted, and genuine clients might miss out on obtaining the IP addresses.</p> <p><b>NOTE</b> When you enable anti-spoofing, an ARP request and DHCP request rate limiter is automatically enabled with default values (in ppm or packets per minute) which are applied per client; Implying that each client connected to an interface enabled with anti-spoofing is allowed to send a maximum of "X" ARP/DHCP request ppm. The value "X" is configured on the interface that the client is connected to.</p> <p><b>NOTE</b> The Force-DHCP option will be enabled by default when the Anti-spoofing feature is enabled, and it cannot be changed after Anti-Spoofing is enabled.</p>
<b>Force DHCP</b>	Requires the clients to obtain a valid IP address from DHCP within the specified number of seconds. This prevents clients configured with a static IP address from connecting to the WLAN. Additionally, if a client performs Layer 3 roaming between different subnets, in some cases the client sticks to the former IP address. This mechanism optimizes the roaming experience by forcing clients to request a new IP address.	Select the check box.
<b>DHCP Option 82</b>	Enables an AP to encapsulate additional information (such as VLAN ID, AP name, SSID and MAC address) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.	Select the check box.
<b>DHCP Option 82 Format</b>	Enables an AP to encapsulate additional information (such as VLAN ID, AP name, SSID and MAC address) into the DHCP request packets before forwarding them to the DHCP server. The DHCP server can then use this information to allocate an IP address to the client from a particular DHCP pool based on these parameters.	<p>Choose the required option:</p> <ul style="list-style-type: none"> <li>• <b>Default</b></li> <li>• <b>Option-A</b></li> <li>• <b>Option-B</b></li> </ul>
<b>DTIM Interval</b>	Indicates the frequency at which the DTIM (Delivery Traffic Indication Message) will be included in Beacon frames.	<p>Enter the frequency number. Range: 1 through 255.</p>
<b>Directed MC/BC Threshold</b>	Defines the per radio client count at which an AP stops converting group-addressed data traffic to unicast. However, the Directed Threshold logic is only one part of the access points' multicast handling logic, which means	<p>Enter the client count number. Range: 0 through 128.</p>







**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
	there may be other factors that determine whether a frame is transmitted as unicast or multicast. APs support a feature called Directed Multicast (configurable only on AP CLI, enabled by default), which adds additional logic to the multicast flow. If Directed Multicast is disabled, the AP uses the Directed Threshold as the only criteria to determine whether to transmit a multicast packet as unicast. However, when Directed Multicast is enabled, the flow is changed. Directed Multicast is a feature that checks to see if a multicast packet is well-known or not. For well-known multicast packets, for example: Bonjour, uPNP, most IPv6 link- and node-local, Spectralink, the AP still applies the directed-threshold logic to determine conversion to unicast. For non well-known types, the AP monitors and maintains a database of client subscriptions using IGMP and MLD. If associated clients are subscribed to the multicast stream, then the AP always converts these packets to unicast, regardless of the Directed Threshold configuration. If there are no clients subscribed to the multicast stream, the AP drops these packets. It is important to be aware of this behavior when validating multicast operation in a deployment.	
<b>Client tx/Rx Statistics</b>	Stops the controller from monitoring traffic statistics for unauthorized clients.	Select the check box.
<b>Inactivity Timeout</b>	Indicates the duration after which idle clients will be disconnected.	Enter the duration in seconds.
<b>OFDM Only</b>	Disconnects 802.11b devices to the WLAN and all devices are forced to use higher data rates for more efficient airtime usage. This setting only affects the 2.4GHz radio. OFDM is used by 802.11a/g/n/ac, but is not supported by 802.11b.	Select the check box.
<b>BSS Min Rate</b>	Forces client devices to both be closer to the AP and to use higher, more efficient rates when you increase the BSS min rate above the default (all rates) setting. The BSS minimum rate is the lowest data rate supported on the WLAN. When OFDM-only is enabled, it takes higher priority than BSS min rate settings.	Select the option.

**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
<b>Mgmt Tx Rate</b>	Sets the transmit rate for management frames type such as beacon and probes.	Select the value.
<b>Service Schedule</b>	<p>Controls when the WLAN service is active. The purpose of this setting is to automatically enable or disable a WLAN based on a pre-determined schedule. By default, the service is Always On. Always Off can be checked in order to create a WLAN and apply it, but prevent it from advertising until ready. The "specific" setting allows a configurable schedule based on time of day and days of the week.</p> <p><b>NOTE</b> When a service schedule is created it is saved by the SZ and AP using the browser's time zone. When it is enforced by the AP, the AP will enforce it according to the time zone of the browser when it was configured.</p>	<p>Choose the option:</p> <ul style="list-style-type: none"> <li>• <b>Always On</b></li> <li>• <b>Always Off</b></li> <li>• <b>Specific</b> and select a schedule profile from the drop-down list.</li> </ul>
<b>Band Balancing</b>	Disables band balancing only for this WLAN, if you select the check box.	Select the <b>Disable band balancing for this WLAN service</b> check box.
<b>Qos Map Set</b>	<p>Reprioritizes downlink packets based on the configured mappings. When an AP receives a downlink packet, it checks the existing DSCP (L3 QoS) marking, compares it to this map set and then changes the user priority (L2 QoS) values for transmission by the AP.</p> <p>TO configure this feature, select the User Priority (UP) from the table (0-7) and configure the DSCP (0-64) range that will be mapped to this UP.</p> <p>Exceptions can also be added such that the original DSCP and UP tagging are preserved the honored by the AP.</p>	Select <b>Enable QOS Map Set</b> .
<b>SSID Rate Limiting</b>	Enforces an aggregate rate limit for all users of the WLAN. The purpose of this feature is to prevent the combined throughput from all users of an SSID from exceeding this threshold. This feature is different from per-user rate limiting, which enforces the same rate limit for each individual device.	Select <b>Uplink</b> and <b>Downlink</b> check boxes and enter the limiting rate in mbps respectively. <i>Range:</i> 1 mbps through 200 mbps.
<b>DNS Server Profile</b>	Allows the AP to inspect DHCP messages and overwrite the DNS server(s) with the DNS server configured in this profile. This allows for policy-based DNS application in	Select a profile from the drop-down menu. Select Disable from the drop-down menu if you want to disable the DNS Server

**TABLE 18 WLAN Configurations (continued)**

Field	Description	Your Action
	which unique users/roles should use a different DNS server than others.	profile for the WLAN service. Click  to add a new profile or click  to edit a profile.
<b>Precedence Profile</b>	Defines the relative policy assignment priority for some specific settings. For example, if a WLAN is configured to use VLAN 10, and a AAA/role policy is configured for VLAN 20, and a device OS policy is configured for VLAN 30, and a user/device connects to the WLAN matching all of these policies, which VLAN should be assigned? The precedence policy determines which setting takes priority.	Select the required option. Click  to add a new profile or click  to edit a profile.
<b>Client Flow Data Logging</b>	Sends a log message with source MAC, destination MAC, source IP, destination IP, source port, destination port, L4 protocol and AP MAC of each packet session to the external syslog server. This function is provided by the AP syslog client (not the SZ's syslog client), which must be enabled at the zone level in order to support this client flow logging.	Select the check box to log the client-flow data to the external syslog server. Then enable AP syslog functionality from the Zone settings.
<b>Airtime Decongestion</b>	Mitigates airtime congestion caused by management frames in high density deployments.	Select the check box.
<b>Join RSSI threshold</b>	Indicates the signal threshold that could connect to the WiFi. If <b>Airtime Decongestion</b> is enabled, <b>Join RSSI threshold</b> is automatically disabled.	Enter the Client RSSI threshold to allow joining. Range: -60 through -90 dBm.
<b>Transient Client Management</b>	Discourages transient clients from joining the network.	Select the <b>Enable Transient Client Management</b> check box and set the following parameters: <ul style="list-style-type: none"> <li>• <b>Join wait time</b>—Enter the wait time before a client can be permitted to join. Range: 1 through 60 secs.</li> <li>• <b>Join expire time</b>—Enter the time during which a rejoin request is accepted without delay. Range: 1 through 300 secs.</li> <li>• <b>Join wait threshold</b>—Enter the number of join attempts after which a client is permitted to join even before the join wait time expires.</li> </ul>
<b>Optimized Connectivity Experience (OCE)</b>	OCE enables probe response suppression and prevents devices with marginal connectivity from joining the network. Optimizes the connectivity experience for OCE-enabled APs and stations.	Select <b>Optimized Connectivity Experience (OCE)</b> and set the following parameters: <ul style="list-style-type: none"> <li>• <b>Broadcast Probe Response Delay</b> - Indicates the time delay to transmit probe response frames in milliseconds.</li> <li>• <b>RSSI-based Association Rejection Threshold</b> - Indicates the minimum threshold value to connect to the network (in dBm). If the value entered is less than the minimum threshold value, then any RSSI-based association is rejected.</li> </ul>

#### NOTE

You can also edit, clone and delete WLANs by selecting the options **Configure**, **Clone** and **Delete** respectively, from the Wireless LANs page.

## 802.11 Fast BSS Transition

802.11r Fast BSS Transition is a fast roaming protocol that reduces the number of frame exchanges required for roaming and allows the clients and APs to reuse the master keys obtained during a prior authentication exchange. 11r is most helpful for 802.1X networks. Client support is required for 11r to work.

## 802.11w MFP

802.11w Management Frame Protection provides additional security measures for management frames. Not all client devices support 802.11w.

Check your client devices before enabling 11w. If “Required” is selected, clients must support 11w in order to connect. If “Capable” is selected, clients with or without 11w should be able to connect. However, note that some clients with poor driver software may have connection problems even if 11w is set to Capable.

## Airtime Decongestion

#### NOTE

Ensure that **Background Scan** is enabled.

The Airtime Decongestion feature optimized the Wi-Fi management traffic in a network where the amount of management traffic can potentially consume a significant portion of airtime thereby reducing the amount of time available for traffic. This feature controls the RSSI threshold setting for Transient Client Management. Enabling this feature disables the **RSSI threshold** configuration in **Transient Client Management**.

## Band Balancing

Band balancing balances the client load on radios by distributing clients between the 2.4 GHz and 5 GHz radios.

This feature is enabled by default and set to a target of 25% of clients connecting to the 2.4 GHz band. To balance the load on a radio, the AP encourages dual-band clients to connect to the 5 GHz band when the configured percentage threshold is reached.

## Bypassing Apple CNA

Some Apple® iOS and OS X® clients include a feature called Captive Network Assistant (CNA), which allows clients to connect to an open captive portal WLAN without displaying the logon page.

When a client connects to a wireless network, the CNA feature launches a pre-browser login utility and it sends a request to a success page on the Apple® website. If the success page is returned, the device assumes it has network connectivity and no action is taken. However, this login utility is not a fully functional browser, and does not support HTML, HTML5, PHP or other embedded video. In some situations, the ability to skip the login page for open WLANs is a benefit. However, for other guest or public access designs, the lack of ability to control the entire web authentication process is not desirable.

The controller provides an option to work around the Apple® CNA feature if it is not desirable for your specific deployment. With CNA bypass enabled, captive portal (web-based authentication) logon must be performed by opening a browser to any unauthenticated page (HTTP) to get redirected to the logon page.

## Client Admission Control

Client admission control allows APs to adaptively allow or deny the association of clients based on the potential throughput of the currently associated clients. This helps prevent APs from becoming overloaded with clients and improves user experience for wireless users.

As an administrator, you can help maintain a positive user experience for wireless users on the network by configuring the following client admission control settings:

- Minimum client count
- Maximum radio load
- Minimum client throughput

Client admission control is implemented on a per radio basis and is supported on 802.11n and 802.11ac APs.

## Client Load Balancing

Enabling load balancing can improve WLAN performance by helping to spread the wireless client load between nearby access points, so that one AP does not get overloaded while another sits idle.

The load balancing feature can be controlled from within the controller web interface to balance the number of clients per radio on adjacent APs.

Adjacent APs are determined by the controller at startup by measuring the RSSI during channel scans. After startup, the controller uses subsequent scans to update the list of adjacent radios periodically and when a new AP sends its first scan report. When an AP leaves, the controller immediately updates the list of adjacent radios and refreshes the client limits at each affected AP.

Once the controller is aware of which APs are adjacent to each other, it begins managing the client load by sending the configured client limits to the APs. These limits are soft values that can be exceeded in several scenarios, including:

- When a client's signal is so weak that it may not be able to support a link with another AP
- When a client's signal is so strong that it really belongs on this AP.

The APs maintain these configured client limits and enforce them once they reach the limits by withholding probe responses and authentication responses on any radio that has reached its limit.

### Key Points About Client Load Balancing

Before you enable load balancing, keep the following considerations in mind:

- The load balancing rules apply only to client devices; the AP always responds to another AP that is attempting to set up or maintain a mesh network.
- Load balancing does not disassociate clients already connected.
- Load balancing takes action before a client association request, reducing the chance of client misbehavior.
- The process does not require any time-critical interaction between APs and the controller.
- Provides control of adjacent AP distance with safeguards against abandoning clients.
- Can be disabled on a per-WLAN basis. For instance, on a voice WLAN, load balancing may not be desired due to voice roaming considerations.

- Background scanning must be enabled on the WLAN for load balancing to work.

## Mobility Domain ID

A Mobility Domain ID is used by 802.11r to define a scope of the network in which an 11r fast roam is supported. Master keys are shared within the Mobility Domain, allowing clients to support a fast roam.

## Portal-based WLANs

There are many types of portal-based WLANs and they can be distinguished based on where the user credentials are stored, and where the portal page is hosted.

**TABLE 19** Portal-based WLANs

WLAN Type	User Credential	Portal on which WLAN is Hosted
Guest	Guest passes on the controller	AP
Hotspot (WISPr)	RADIUS server. LDAP/Active Directory from SmartZone release 3.2 and later	External portal server or internal portal on the controller
Web Auth	RADIUS/LDAP/Active Directory	AP

Guest and WebAuth WLAN portals are hosted on the controller AP with limited customization. WISPr WLANs are usually hosted on external portal servers providing the flexibility to customize. WISPr WLANs allow for sophisticated customization such as providing a customized login page which could include locale information, advertisements etc.

WISPr WLANs can also be configured to bypass the authentication portal such that if an end user device's MAC address (as a credential) is stored on a RADIUS server, there is no need to redirect the end user to the portal server for authentication.

### Characteristics of portal-based WLANs

Portal-based WLANs have the following characteristics:

- WebAuth WLAN
  - Does not provide an option to modify the portal (WYSIWYG)
  - User authentication is done by the RADIUS server, LDAP and Active Directory
  - Allows redirecting user web pages
- Guest WLAN
  - Provides an option to modify the portal elements such as the logo, Terms and Conditions, title etc
  - User authentication is by using guest passphrases or select the **Always Accepted** option
  - Allows redirecting user web pages
  - Does not possess a local database, LDAP, Active Directory or RADIUS server
- Hotspot (WISPr) WLAN
  - Internal Portal
    - › Provides an option to modify the portal elements such as the logo, Terms and Conditions, title etc
    - › Allows redirecting user web pages
    - › User authentication is by the local database, LDAP, Active Directory, RADIUS server or rendered by selecting the **Always Accepted** option
    - › Supports the Walled Garden approach to allow user access to specific areas within the network
  - External Portal
    - › Allows customization of the portal pages through external services

- › Supports Northbound Portal Interface for authentication
- › User authentication is by the local database, LDAP, Active Directory, RADIUS server or rendered by selecting the **Always Accepted** option
- › Supports the Walled Garden approach to allow user access to specific areas within the network
- › Allows redirecting user web pages

## Rate Limiting Ranges for Policies

You can define and apply rate limit values for user devices to control the data rate and types of network traffic the device transmits.

### NOTE

For SmartZone release 3.4 and 3.2.x, the APs support the following rate limiting values:

- 0.10Mbps
- 0.25Mbps - 20.00Mbps (increments by 0.25Mbps)
- 21.00Mbps - 200.00Mbps (increments by 1.00Mbps)

For example, typing 6.45 Mbps maps to the closest predefined rate value, so 6.45Mbps will be rendered as 6.50Mbps.

### NOTE

For SmartZone release 3.1.x, the APs support the following rate limiting values:

- 0.10Mbps
- 0.25Mbps - 20.00Mbps (increments by 0.25Mbps)
- 30.00Mbps
- 40.00Mbps
- 50.00Mbps

For example, typing 31.50 Mbps maps to the closest predefined rate value, so 31.50 Mbps will be rendered as 40 Mbps. Any rate greater than 50.00Mbps would be mapped to the maximum rate which is 50.00Mbps.

**TABLE 20** Rate Limiting ranges for different controller policies

Policy	Global or Zone	Rate limit range for zone running SmartZone 3.4	Rate limit range for zone running SmartZone 3.2.x	Rate limit range for zone running SmartZone 3.1.x
Device Policy	Zone	0.1 Mbps to 200 Mbps Support uni-direction (Uplink and Downlink need not be enabled or disabled at the same time)	0.1 Mbps to 200 Mbps No support for uni-direction (Uplink and Downlink need not be enabled or disabled at the same time)	0.1 Mbps to 200 Mbps. But any rate greater than 50Mbps will be mapped to 50 Mbps implicitly on the AP side when the rate is applied. No support for uni-direction
User Traffic Profile	Global	0.1 Mbps to 200 Mbps No support for uni-direction because this is Global profile that is used by 3.2.x and 3.1.x APs	0.1 Mbps to 200 Mbps No support for uni-direction	But any rate greater than 50Mbps will be mapped to 50 Mbps implicitly on the AP side when the rate is applied. No support for uni-direction

## Transient Client Management

The Transient Client Management feature allows only those clients that stay within the AP's coverage region for a minimum period of time to associate with the AP and use the service. For example, in a train station or downtown area there may be passerby who do not intend to connect and utilize the network service. However, their Wi-Fi devices may do an active/passive scanning and could be roaming either from cellular to Wi-Fi or from one Wi-Fi AP to another Wi-Fi AP or from Wi-Fi to cellular, which could compromise the experience of users who are connected and using the service. First-time client association may be delayed.

Transient Client management uses statistical methods to delay the association of transient clients to an AP. Venue administrators will be able to tune configuration parameters based on typical observed dwell times and RSSI of transient clients. This feature delivers efficient airtime utilization and minimizes Cellular to Wi-Fi handoffs, AP to AP roaming of Transient clients.

## Optimized Connectivity Experience

Optimized Connectivity Experience (OCE) delivers a better overall connectivity experience by enabling probe response suppression and by preventing devices with marginal connectivity to join the network.

When OCE is enabled, the affected APs and stations are excluded from Airtime Decongestion and Transient Client Management, resulting in reduction in probe response. Probe response suppression optimizes airtime for data traffic. OCE solves connectivity issues by rejecting any association with clients with poor signals.

## Working with WLAN Schedule Profiles

A WLAN schedule profile specifies the hours of the day or week during which a WLAN service will be enabled or disabled.

For example, a WLAN for student use at a school can be configured to provide wireless access only during school hours. Create a WLAN schedule profile, and then when you configure a WLAN, select the schedule profile to enable or disable the WLAN service during those hours/days.

### NOTE

This feature will not work properly if the system does not have the correct time. To ensure that the system always maintains the correct time, configure an NTP server and point the system to the NTP server's IP address, as described in [Configuring System Time](#) on page 43.

### NOTE

WLAN service schedule times should be configured based on your browser's current timezone. If your browser and the target AP/WLAN are in different timezones, configure the on/off times according to the desired schedule according to your local browser. For example if you wanted a WLAN in Los Angeles to turn on at 9 AM and your browser was set to New York time, please configure the WLAN service schedule to enable the WLAN at noon. When configuring the service schedule, all times are based on your browser's timezone setting.

## Creating a WLAN Schedule Profile

Follow these steps to create a WLAN schedule profile.

1. From the Wireless LANs page, select the WLAN for you want to create a WLAN Schedule profile.
2. Click **Configure**, the Edit WLAN Config page appears.
3. Scroll down to the Advanced Options section.
4. In the **Service Schedule** field, select **Specific**.



5. Click **Create**, the Create Time Schedules Table form appears.
6. In General Options, enter the **Schedule Name** and **Schedule Description**.
7. To set a WLAN schedule:
  - To enable or disable the WLAN for an entire day, click the day of the week under the **Time** column.
  - To enable or disable the WLAN for specific hour of a specific day, click the squares in the table. A single square represents 30 minutes (two-15 minute blocks).

Blue-colored cells indicate the hours when the WLAN is enabled. Clear (or white) cells indicate the hours when the WLAN is disabled.
8. Click **Create**, the page refreshes, and then the schedule you created appears in the drop-down list.

## Managing WLANs

When you select a System, Zone, or WLAN Group from the hierarchy tree, respective contextual tabs appear at the bottom of the page.

These tabs are used to monitor the selected group. The following table lists the tabs that appear for System, Zone, and WLAN Group.

**TABLE 21** System/Zone/WLAN Groups Monitoring Tabs

Tabs	Description	System	Zone	WLAN Groups
<b>Configuration</b>	Displays the respective configuration information.	Yes	Yes	Yes
<b>Traffic</b>	Displays the respective historical traffic information.	Yes	Yes	Yes
<b>Alarm</b>	Displays the respective alarms information.	Yes	Yes	Yes
<b>Event</b>	Displays the respective event information.	Yes	Yes	Yes
<b>APs</b>	Displays the respective AP information.	Yes	Yes	NA
<b>Clients</b>	Displays the respective client information.	Yes	Yes	NA
<b>Services</b>	Displays the respective Services information.	Yes	Yes	NA
<b>Administrators</b>	Displays the respective administrator account information.	Yes	NA	NA

When you can select a Zone and click **More** you can perform the following operations:

- **Extract WLAN Template**
- **Apply WLAN Template**
- **Change AP Firmware**
- **Switchover Cluster**

## Extracting a WLAN Template

You can extract only WLAN-related configuration of an AP to a WLAN template.

Follow these steps to extract a WLAN template:

1. From the Wireless LANs page, locate the zone from where you want to extract the WLAN template.
2. Click **More** and select **Extract WLAN Template**, the Extract WLAN Template form appears.

3. In **WLAN Template Name**, enter a name for the Template.
4. Click **OK**, a message appears stating that the WLAN template was extracted successfully.
5. Click **OK**.

The extracted WLAN template can be viewed under **System > Templates > WLAN Templates**.

## Applying a WLAN Template

You can apply only WLAN-related configuration to an AP zone using a WLAN template. You can apply the WLAN template to zones where the AP's firmware version is later than the Zone templates firmware version. Unsupported firmware version of the WLAN template is automatically upgraded to its next version before being upgraded to the current version.

Follow these steps to apply a WLAN template:

1. From the Wireless LANs page, locate the zone where you want to apply the WLAN template.
2. Click **More** and select **Apply WLAN Template**, the **Apply WLAN Template** dialog box appears.
3. From the **Select a WLAN template** drop-down, select the template.
4. Click **Next**, the **Apply WLAN template to selected zones** form appears..
5. Click the required options:
  - Create all WLANs and WLAN profiles from the template if they don't already exist in the target zone(s)
  - If the target zone(s) has WLANs or WLAN profile with the same name as the template, overwrite current settings with settings from the template.
  - Click **OK**. A confirmation dialog appears.
6. Click **OK**. You have applied the WLAN template to the zone.

## How Dynamic VLAN Works

Dynamic VLAN can be used to automatically and dynamically assign wireless clients to different VLANs based on RADIUS attributes.

Dynamic VLAN Requirements:

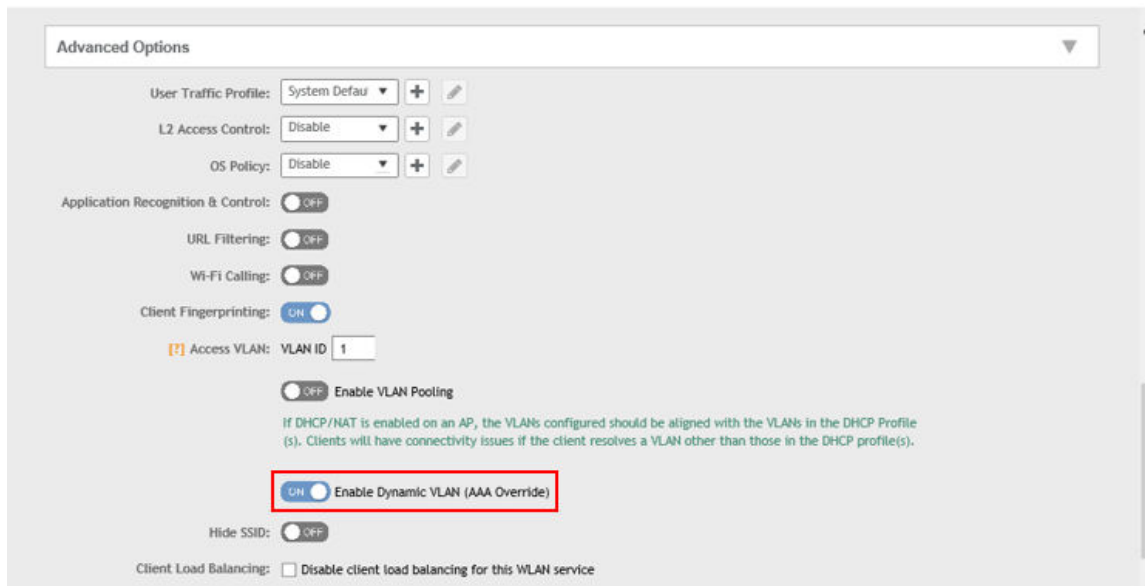
- A RADIUS server must have already been added to the controller
- WLAN authentication method must be set to 802.1X, MAC address or 802.1X + MAC address

To enable Dynamic VLAN for a WLAN:

1. Go to **Wireless LANs**.
2. Click **Configure** for to the WLAN you want to configure.
3. In **Authentication Server**, select the AAA profile.
4. Expand the **Advanced Settings** section and click the **Enable Dynamic VLAN box** next to Access VLAN.

- Click **OK** to save your changes.

**FIGURE 82** Enabling Dynamic VLAN



## How It Works

- User associates with a WLAN on which Dynamic VLAN has been enabled.
- The AP requires the user to authenticate with the RADIUS server.
- When the user completes the authentication process, the AP will approve the user along with the VLAN ID that has been assigned to the user on the RADIUS server.
- User joins the AP and is segmented to the VLAN ID that has been assigned to him.

## Required RADIUS Attributes

For dynamic VLAN to work, you must configure the following RADIUS attributes for each user:

- Tunnel-Type:** Set this attribute to VLAN.
- Tunnel-Medium-Type:** Set this attribute to IEEE-802.
- Tunnel-Private-Group-ID:** Set this attribute to the VLAN ID to which you want to segment this user.

Depending on your RADIUS setup, you may also need to include the user name or the MAC address of the wireless device that the user will be using to associate with the AP. The following table lists the RADIUS user attributes related to dynamic VLAN.

**TABLE 22** RADIUS user attributes related to dynamic VLAN

Attribute	Type ID	Expected Value (Numerical)
Tunnel-Type	64	VLAN (13)
Tunnel-Medium-Type	65	802 (6)
Tunnel-Private-Group-Id	81	VLAN ID

Here is an example of the required attributes for three users as defined on Free RADIUS:

```
0018ded90ef3
  User-Name = user1,
  Tunnel-Type = VLAN,
  Tunnel-Medium-Type = IEEE-802,
  Tunnel-Private-Group-ID = 0014
00242b752ec4
  User-Name = user2,
  Tunnel-Type = VLAN,
  Tunnel-Medium-Type = IEEE-802,
  Tunnel-Private-Group-ID = 0012
013469acee5
  User-Name = user3,
  Tunnel-Type = VLAN,
  Tunnel-Medium-Type = IEEE-802,
  Tunnel-Private-Group-ID = 0012
```

**NOTE**

The values in bold are the users' MAC addresses.

# Managing Clients

- Working with Wireless Clients..... 193
- Working with Wired Clients..... 196
- Working with Users and Roles..... 197
- Working with Guest Passes..... 211
- Working with Dynamic PSKs..... 224

## Working with Wireless Clients

Wireless clients are client devices that are connected to the wireless network services that your managed APs provide. Wireless clients can include smart phones, tablets, and notebook computers equipped with wireless network adapters.

### Viewing a Summary of Wireless Clients

View a summary of wireless clients that are currently associated with all of your managed access points.

Go to **Clients > Wireless Clients**. The **Wireless Clients** page appears and displays a table that lists all clients that are currently associated with your managed access points.

To view only wireless clients that belong to a particular zone, click the zone name in the zone tree. The table refreshes and displays only the clients that belong to the zone you selected.

The following table lists the wireless client details.

#### NOTE

Not all of the columns listed below are displayed by default. To display column that are currently hidden, click the gear icon in the upper-right corner of the table, and then select the check boxes for the columns that you want to display.

You can view the clients listed in the table in two view modes - **No TTG** (without TTG) and **TTG** (with TTG).



Click the  icon to export all the data into a CSV file.

**TABLE 23** Wireless client details

Column Name	Description
Hostname	Displays the hostname of the wireless client
OS Type	Displays the operating system that the wireless client is using
IP Address	Displays the IP address assigned to the wireless client
MAC Address	Displays the MAC address of the wireless client
WLAN	Displays the name of the WLAN with which the client is associated
AP Name	Displays the name assigned to the access point
AP MAC	Displays the MAC address of the AP
Traffic (Session)	Displays the total traffic (in KB/MB/GB/TB) for this client in this session
Traffic (Uplink)	Displays the total uplink traffic (in KB/MB/GB/TB) for this client in this session
Traffic (Downlink)	Displays the total downlink traffic (in KB/MB/GB/TB) for this client in this session

**TABLE 23** Wireless client details (continued)

Column Name	Description
RSSI	Displays the Received Signal Strength Indicator (RSSI), which indicates how well a wireless client can receive a signal from an AP. The RSSI value is shown in decibels (dB) and displayed as either the real-time value or the average value over the past 90 seconds.
SNR	Displays the Signal-to-Noise Ratio (SNR), which indicates the signal strength relative to background noise. The SNR value is shown in decibels (dB) and displayed as either the real-time value or the average value over the past 90 seconds.
Radio Type	Displays the type of wireless radio that the client supports. Possible values include 11b, 11g, 11g/n, 11a, 11a/g/n, and 11ac.
VLAN	Displays the VLAN ID assigned to the wireless client
Channel	Displays the wireless channel (and channel width) that the wireless client is using
User Name	Displays the name of the user logged on to the wireless client
Effective Data Rate	Displays the real traffic transmit rate of the wireless client
Auth Method	Displays the authentication method used by the AP to authenticate the wireless client
Auth Status	Indicates whether the wireless client is authorized or unauthorized to access the WLAN service
Encryption	Displays the encryption method used by the AP
Control Plane	Displays the name of SmartZone node to which the AP's control plane is connected
Packets to	Displays the downlink packet count for this session
Packets from	Displays the uplink packet count for this session
Packets dropped	Displays the downlink packet count for this client that have been dropped
Session start time	Indicates the session creation time

**NOTE**

The client is automatically unauthenticated by the WLAN if the client is connected for 48 hours in the *Standard+Open/Standard+MAC Auth* authentication method, and for 12 hours in the *Standard+802.1x EAP* authentication method.

## Viewing Information about a Wireless Client

You can view more information about a wireless client, including its IP address, MAC address, operating system, and even recent events that have occurred on it.

Follow these steps to view information about a wireless client.

1. Go to **Clients > Wireless Clients**.
2. From the list of wireless clients, locate the client whose details you want to view.
3. Under the **MAC Address** column, click the MAC address of the wireless client.

The **Associated Client** page appears and displays general information about the wireless client.

- **General:** Displays general client information.
- **Health:** Displays information about the real-time health of the client. It displays graphical trends based on the signal-to-noise ratio (SNR) and data rate. You can use the **Start** and **Stop** option to review client health at real time.
- **Traffic:** Displays historical and real-time traffic information.
- **Event:** Displays information about events associated with the client.

## Deauthorizing a Wireless Client

If you want to force wireless clients that joined the wireless network through an authentication portal (for example, a hotspot, guest access or web authentication portal) to reauthenticate themselves, you can deauthorize them. Deauthorized wireless clients remain connected to the wireless network, but these clients will be redirected to the authentication portal whenever they attempt to access network resources.

Follow these steps to deauthorize a wireless client.

1. On the menu, click **Clients > Wireless Clients**.
2. From the list wireless clients, locate the client that you want to deauthorize. If you have a large number of wireless clients and you know the MAC address of the client, enter the MAC address in the search box, and then press Enter to search for the client.
3. When you have located the client, select it, and then click the **Deauthorize** button above the table.  
The table refreshes, and then the client that you deauthorized disappears from the list.

## Blocking a Wireless Client

When a user associates a wireless client device with an AP that the controller is managing, the client device is recorded and tracked. If, for any reason, you need to block a client device from accessing the network, you can do so from the web interface.

A few reasons why you might consider blocking a wireless client device include:

- Network abuse
- Violation of acceptable use policy
- Theft
- Security compromise

Follow these steps to block a wireless client from accessing the SmartZone network.

1. On the menu, click **Clients > Wireless Clients**.
2. From the list wireless clients, locate the client that you want to block. If you have a large number of wireless clients and you know the MAC address of the client, enter the MAC address in the search box, and then press <Enter> to search for the client.
3. When you have located the client, select it, and then click the **Block** button above the table.

You have completed blocking a wireless client.

## Unblocking a Wireless Client

If you want to allow a client that you previously blocked to access the SmartZone network, you can unblock it.

Follow these steps to unblock a wireless client.

1. On the menu, click **Services and Profiles > Access Control**.
2. Click the **Blocked Client** tab.
3. From the list of blocked clients, locate the client that you want to unblock. If you have a large number of blocked clients and you know the MAC address of the client, enter the MAC address in the search box, and then press <Enter> to search for the client.
4. When you have located the client, select it, and then click the **Delete** button above the table.  
The table refreshes, and then the client that you want to unblock disappears from the list.

You have completed unblocking a wireless client.

## Disconnecting a Wireless Client

If you need to temporarily disconnect a wireless client from the wireless network, you can do so from the web interface. For example, if you are troubleshooting problematic network connections, you might have to manually disconnect wireless clients as part of the troubleshooting process.

Follow these steps to disconnect a wireless client from the WLAN to which it is connected.

1. On the menu, click **Clients > Wireless Clients**.
2. From the list wireless clients, locate the client that you want to disconnect. If you have a large number of wireless clients and you know the MAC address of the client, enter the MAC address in the search box, and then press <Enter> to search for the client.
3. When you have located the client, select it, and then click the **Disconnect** button above the table.

The table refreshes, and then the client that you disconnected disappears from the list.

## Working with Wired Clients

Wired clients are client devices that are connected to the Ethernet ports of APs managed by the controllers, and thereby are connected to the wired network services that your managed APs provide.

### Viewing a Summary of Wired Clients

View a summary of wired clients that are currently associated with all of your managed access points.

Go to **Clients > Wired Clients**. The **Wired Clients** page appears and displays a table that lists all clients that are currently associated with your managed access points.

To view only wired clients that belong to a particular zone, click the zone name in the zone tree. The table refreshes and displays only the clients that belong to the zone you selected.

The following table lists the wired client details.

**TABLE 24** Wired client details

Column Name	Description
MAC Address	Displays the MAC address of the wired client
Username	Displays the name of the user logged on to the wire client
IP Address	Displays the IP address assigned to the wired client
AP MAC	Displays the MAC address of the AP
AP Name	Displays the name assigned to the access point
LAN	Displays the LAN ID assigned to the wired client
VLAN	Displays the VLAN ID assigned to the wired client
Auth Status	Indicates whether the wired client is authorized or unauthorized to access the WLAN service

To know more about how the 802.1X configuration works for the port refer [Creating an Ethernet Port Profile](#) on page 317.



## Viewing Information about a Wired Client

You can view more information about a wired client, including its IP address, MAC address and even recent events that have occurred on it.

Follow these steps to view information about a wired client.

1. Go to **Clients > Wired Clients**.
2. From the list of wired clients, locate the client whose details you want to view.
3. Under the **MAC Address** column, click the MAC address of the wired client.

The **Associated Client** page appears and displays general information about the wired client.

- **General:** Displays general client information.

### NOTE

Selecting the **Enable client visibility regardless of 802.1X authentication** check box bypasses 802.1X authentication for client visibility. This option allows you to view statistical information about wired clients even without enabling 802.1X authentication.

- **Configuration:** Displays detailed configuration information for the zones, tunnel options, radio options, mesh links and model.
- **Event:** Displays information about events associated with the client.

## Deauthorizing a Wired Client

If you want to force wired clients that joined the wired network through an authentication portal to reauthenticate themselves, you can deauthorize them. Deauthorized wired clients remain connected to the wired network, but these clients will be redirected to the authentication portal whenever they attempt to access network resources.

Follow these steps to deauthorize a wired client.

1. On the menu, click **Clients > Wired Clients**.
2. From the list wired clients, locate the client that you want to deauthorize. If you have a large number of wired clients and you know the MAC address of the client, enter the MAC address in the search box, and then press **Enter** to search for the client.
3. When you have located the client, select it, and then click the **Deauthorize** button above the table.

The table refreshes, and then the client that you deauthorized disappears from the list.

## Working with Users and Roles

The controller provides a default role (named **Default**) that is automatically applied to all new user accounts.

By default, this role links all users to the internal WLAN and permits access to all WLANs. As an alternative, you can create additional roles that you can assign to select wireless network users, to limit their access to certain WLANs, to allow them to log on with non-standard client devices, or to grant permission to generate guest passes. (You can then edit the default role to disable the guest pass generation option.)

## Creating a User Role

Use user roles to limit user access to certain WLANs, to allow them to log on with non-standard client devices.

Follow these steps to create a user role.

1. Go to **Clients > Users & Roles**.
2. Select the **User Roles** tab, and then select the zone for which you want to create the role.
3. Click **Create**.

The **Create User Role** page appears.

**FIGURE 83** Create User Role

**Create User Role**

\* Role Name:

Description:

\* User Traffic Profile:

Access VLAN: VLAN ID

☐ Enable VLAN Pooling

4. Configure the options in the **Create User Role** form.
  - Role Name: Type a name for this user role.
  - Description: Type a description for this user role.
  - User Traffic Profiles: Select the user traffic profile from the drop-down menu. You can also create the user traffic profile. For more information, see [Creating a User Traffic Profile](#) on page 254.
  - Access VLAN: Provide the VLAN ID.  
  
You can also select the Enable VLAN Pooling check-box and select the VLAN ID from the drop-down list. You can also create a VLAN Pooling profile. For more information, see [Creating a VLAN Pooling Profile](#) on page 261.
5. Click **OK**.

You have completed creating a user role.

### NOTE

You can also edit, clone and delete user roles by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **User Roles** tab.

## User Group Permissions in SmartZone Devices

By combining the all resource groups with a permission level for each group, you can customize the administrator's privileges.

Resources are divided into the following groups:

- SmartZone Management
- AP Management
- WLAN Management
- User/Device/Application Management
- Administrator Management
- Managed Service or MVNO Management
- Switch Management

There are four permission levels in each group:

- No access
- Read (read only permission level)
- Modify (read and modify existing resources, cannot create new resource or delete existing resource)
- Full access

Though resource groups are associated with domains, not all resource groups can be associated with any domain. Following are some restrictions:

**TABLE 25 Resource Group-Domain Restrictions**

Resource Group	Domain Allowed
AP Management	All Domains
WLAN Management	All Domains
SmartZone Management	System (MSP root)
Managed Service or MVNO Management	System (MSP root)
User/Device/Application Management	System (MSP root), Partner managed domains (Partner root)
Administrator Management	System (MSP root), Partner managed domains (Partner root)

**TABLE 26 Predefined Administrator Roles**

Predefined Permissions	Management					
	SmartZone	AP	WLAN	User/Device/Application	Administrator	Managed Service or MVNO
Super Admin	Full Access	Full Access	Full Access	Full Access	Full Access	Full Access
System Admin	Full Access	Read	Read	Read	Full Access	No Access
Read-Only System Admin	Read	Read	Read	Read	Read	No Access
Network Admin	Read	Full Access	Full Access	Full Access	No Access	No Access
Read-Only Network Admin	Read	Read	Read	Read	No Access	No Access
AP Admin	No Access	Modify	Modify	Read	No Access	No Access
Guest Pass Admin	No Access	No Access	No Access	Full Access (Guest Pass, Guest Template, Subscription Package, Identity User)	No Access	No Access

**TABLE 27 Relationship between Resource, Operation -Resource Group and Permission Levels**

Resource	Operation	Resource Group	Permission Levels
Dashboard	Settings - Global Notification	SZ Management	Modify
	Settings - Health Dashboard > Cluster	SZ Management	Modify
	Settings - Health Dashboard > AP	SZ Management	Modify
	Settings - Others	SZ Management	
	Settings - User Preference	Permitted after login	
Cluster	Cluster Backup	SZ Management	Full Access
	Cluster Restore	SZ Management	Full Access
	SZ Upgrade and AP firmware Upgrade	SZ Management	Full Access
	Configuration Backup	SZ Management	Full Access
	Configuration Restore	SZ Management	Full Access
	Modify License Server Configuration	SZ Management	Modify
	Update License (manual upload or manual sync with License Server)	SZ Management	Modify
	View License Information (download, status, usage, installed licenses)	SZ Management	Read
	AP Certificate Replacement	SZ Management	Modify
	Restart/shutdown SZ	SZ Management	Full Access
Cluster Level Configuration			
<ul style="list-style-type: none"> <li>System Time</li> <li>Syslog Server</li> <li>SCI</li> <li>northbound portal</li> </ul>	View configuration content	SZ Management	Read
<ul style="list-style-type: none"> <li>SMTP</li> <li>FTP server for upload stats</li> <li>Critical AP rules</li> <li>Q-in-Q Ether Type</li> <li>Gateway Advanced Options</li> <li>Certificate Store</li> </ul>	Modify configuration content	SZ Management	Modify
<ul style="list-style-type: none"> <li>Cluster Redundancy(3.6)</li> <li>SNMP Agent</li> <li>Event Management</li> <li>Event Threshold</li> <li>Management Interface ACL</li> <li>Hosted AAA services (EAP-SIM, EAP-AKA)</li> <li>MNC-NDC Mappings</li> <li>FTP</li> <li>SMS Server</li> <li>Approval (System &gt; AP Settings &gt; Approval)</li> <li>AP Switchover</li> </ul>	Create new configuration entity Event Management : Disable/Enable Cluster Redundancy - Rehome Per cluster, Restore Config, Switchover	SZ Management	Full Access

**TABLE 27 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)**

Resource	Operation	Resource Group	Permission Levels
<ul style="list-style-type: none"> <li>EPVOT (Ethernet Port Validate On Trunk)</li> <li>Gateway advanced</li> <li>ZeroIT</li> <li>lwapp2scg</li> </ul>			
CP/DP Node	View node configuration	SZ Management	Read
	Modify node configuration	SZ Management	Modify
	Reset/Reboot/Remove Node	SZ Management	Full Access
	Node level realtime monitor	SZ Management	Read
	Node level historical stats	SZ Management	Full Access
Administrator	Modify account	Administrator Management	Read
	Create/Delete account	Administrator Management	Modify
	View account content	Administrator Management	Modify
	View Login captcha settings	Administrator Management	Full Access
	Modify Login captcha settings	Administrator Management	Read
Administrator Group	Modify administrator group	Administrator Management	Modify
	Create/Delete	Administrator Management	Full Access
	View administrator group content	Administrator Management	Read
Management Domain	Modify domain	Administrator Management	Modify
	Create/Delete	Administrator Management	Full Access
	Move zone in/out of domain	Administrator Management	Modify
	View group tree (hierarchical relationship among domain, zone and AP, limited information about domain, zone and AP such as id, name, MAC)	Administrator Management Managed Service/MVNO Management AP Management WLAN Management User/Device/Application Management	Read
	View domain List (limited information about the domain such as id and name)	Administrator Management Managed Service/MVNO Management AP Management WLAN Management User/Device/Application Management	Read
Partner/Venue/MVNO	Modify Partner, Venue, MVNO account	Managed Service/MVNO Management	Modify
	Create/Delete	Managed Service/MVNO Management	Full Access
	View Partner, Venue, MVNO account, Third Party UE	Managed Service/MVNO Management	Read
	Partner, Venue, MVNO related historical stats	Managed Service/MVNO Management	Full Access
Zone/Zone Template	Modify Zone	AP Management	Modify

**TABLE 27 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)**

Resource	Operation	Resource Group	Permission Levels
	Create/Delete	AP Management	Full Access
	View	AP Management	Read
	Apply zone template (grid action button)	AP Management	Read
	Apply zone template	AP Management	Full Access
Zone related service/profile <ul style="list-style-type: none"> <li>Node affinity</li> <li>Ruckus GRE Tunnel</li> <li>SoftGRE Tunnel</li> <li>IPsec Tunnel</li> <li>LBS</li> <li>Hotspot 2.0 Venue Profile</li> <li>Ethernet Port Profile</li> </ul>	Modify	AP Management	Modify
	Create/Delete	AP Management	Full Access
	View configuration content	AP Management	Read
	Move AP in/out zone	AP Management	Full Access
	Get by Zone ID	AP Management	Read
AP Group	Modify	AP Management	Modify
	Create/Delete	AP Management	Full Access
	View configuration content	AP Management	Read
	Move AP in/out AP group	AP Management	Full Access
	Modify associated WLAN group	AP Management and WLAN Management	Modify
AP Group related service/profile			
LBS	Modify	AP Management	Modify
Hotspot 2.0 Venue Profile	Create/Delete	AP Management	Full Access
Ethernet Port Profile	View configuration content	AP Management	Read
WLAN or WLAN Template	Modify WLAN	WLAN Management	Modify
	Create/Delete	WLAN Management	Full Access
	View WLAN configuration content	WLAN Management	Read
	Apply WLAN template (grid action button)	WLAN Management AP Management : READ &&WLAN Management : FULL_ACCESS	Read
	Apply WLAN template	WLAN Management AP Management : READ &&WLAN Management : FULL_ACCESS	Full Access
WLAN related zone level service/profile			
<ul style="list-style-type: none"> <li>AAA</li> <li>Hotspot</li> <li>WeChat</li> <li>Guest Access</li> </ul>	Modify Test AAA	WLAN Management	Modify
<ul style="list-style-type: none"> <li>Web Auth</li> <li>Hotspot 2.0 WLAN Profile</li> <li>WLAN scheduler</li> <li>Device Policy</li> </ul>	Create/Delete	WLAN Management	Full Access
<ul style="list-style-type: none"> <li>L2 Access Control</li> <li>DiffServ</li> <li>VLAN Pooling</li> </ul>	View configuration content	WLAN Management	Read

**TABLE 27 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)**

Resource	Operation	Resource Group	Permission Levels
WLAN related level service/profile global <ul style="list-style-type: none"> <li>• Authentication/Accounting Profile</li> <li>• AAA (authentication/accounting services)</li> <li>• Hotspot 2.0 Wi-Fi Operator</li> <li>• Hotspot 2.0 Wi-Fi Provider</li> <li>• Online Signup Portal</li> <li>• User Traffic Profile</li> <li>• Forwarding Profile (all types, e.g. Bridge,L2oGRE...)</li> <li>• Application Control (AVC)</li> <li>• DNS server services</li> <li>• URL Filtering</li> </ul>	Modify Test AAA	WLAN Management	Modify
	Create/Delete	WLAN Management	Full Access
	View configuration content	WLAN Management	Read
	Signature Package upload	WLAN Management	Full Access
	Signature Package content	WLAN Management	Read
	View Url Filtering Block Categories	Permitted after login	
	View Url Filtering All Level	Permitted after login	
WLAN Group	Modify	WLAN Management	Modify
	Create/Delete	WLAN Management	Full Access
	View configuration content	WLAN Management	Read
	Add/Remove WLAN group member	WLAN Management	Modify
AP	Pre-provision AP, Delete AP, Move AP, Manual Approve AP and Reboot AP(cable modem)	AP Management	Full Access
	Modify AP level configuration	AP Management	Modify
	View AP level configuration content	AP Management	Read
	Zone level: Extract zone template, Apply zone template, Change AP firmware and Trigger preferred node	AP Management	Full Access
	AP Table: <ul style="list-style-type: none"> <li>• Lock</li> <li>• Unlock</li> <li>• Import Batch Provisioning APs</li> <li>• Import Swapping APs</li> <li>• Trigger Preferred Node</li> <li>• Restart Cable Modem</li> <li>• Reset Cable Modem</li> <li>• Swap</li> <li>• Approve</li> </ul>	AP Management	Full Access
	AP Table: <ul style="list-style-type: none"> <li>• Export All Batch Provisioning APs</li> <li>• Export All Swapping APs</li> <li>• Download Support Log</li> <li>• Trigger AP Binary Log</li> <li>• Download CM Support Log</li> </ul>	AP Management	Read

**TABLE 27 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)**

Resource	Operation	Resource Group	Permission Levels
	Untag Critical APs	AP Management	Modify
	Get All APs Firmware	AP Management	Read
	Get AP Binary Log	AP Management	Read
AP Routine Status	View Status/Config Interval	SZ Management	Read
	Modify Status/Config Interval	SZ Management	Modify
AP related zone-level service/profile: <ul style="list-style-type: none"> <li>Bonjour Gateway</li> <li>WIPS (Rogue AP Policy)</li> </ul>	Modify	AP Management	Modify
	Create/Delete	AP Management	Full Access
	View configuration content	AP Management	Ready
	Mark/Unmark Rogue APs	AP Management	Modify
AP Registration Rule	Create/Modify/Delete	AP Management	Full Access
	View configuration content	AP Management	Read
AP zero touch	Execute action on AP through Mesh network	AP Management	Full Access
	List discovered AP through Mesh network	AP Management	Read
User/Subscription Package	Modify	User/Device/Application Management	Modify
	Create/Delete	User/Device/Application Management	Full Access
	View configuration content	User/Device/Application Management	Read
Guest Pass	Print	User/Device/Application Management	Read
	Export		
	Email		
	Mobile		
	Modify	User/Device/Application Management	Modify
	Enable	User/Device Application Management	Full Access
	Disable		
	Create/Delete/Upload	User/Device Application Management	Full Access
	View, print, text guest pass	User/Device/Application Management	Read
User Role	Modify	User/Device/Application Management	Modify
	Create	User/Device/Application Management	Full Access
	View configuration content	User/Device/Application Management	Read
Client/Managed Devices	Delete/Block/Test Speed client or managed devices	User/Device/Application Management	Full Access
	Client page: stop/start real time chart		
	Disconnect	User/Device/Application Management	Read
	View client or managed devices		



**TABLE 27 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)**

Resource	Operation	Resource Group	Permission Levels
Dynamic PSK (DPSK)	Batch Generate	User/Device/Application Management	Full Access
	Import CSV		
	Delete		
	Modify expired DPSK auto purge policy		
	View	User/Device/Application Management	Read
	View expired DPSK auto purge policy		
	Modify user name		
	Export CSV	User/Device/Application Management	Read
Rogue Device		AP Management	Read
Admin Activity Log		Administrator Management	Read
Admin > Access Control List		SZ Management	Full Access
Events & Alarms	View	All admin	Read
	Clear	Permitted after login	
	Acknowledge	Permitted after login	
	Create/Delete	Permitted after login	
Saved Report		AP Management WLAN Management SZ Management	Modify
Diagnostics > Scripts > Patch Scripts		Super Admin only	Full Access
Diagnostics > Scripts > Diagnostics Scripts			
Diagnostics > Scripts > AP CLI Scripts		AP Management	Full Access
Diagnostics > Scripts > Applications Logs	Download log	SZ Management	Read
	Set log level	SZ Management	Modify
Diagnostics > Others		SZ Management	Read
Historical Client Statistics	View	User/Device/Application Management	Read
		AP management	
Core Tunnel Statistic (generated By DP)		SZ Management	Read
<ul style="list-style-type: none"> <li>Core Network Tunnel Stats &gt; SoftGRE</li> <li>Core Network Tunnel Stats &gt; GRE</li> <li>Core Network Tunnel Stats &gt; GTP</li> <li>Core Network Tunnel Stats &gt; PMIPv6</li> </ul>			
Access Tunnel Statistics (generated By DP)		SZ Management	Read

**TABLE 27 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)**

Resource	Operation	Resource Group	Permission Levels
Access Tunnel Statistics (generated by AP) <ul style="list-style-type: none"> <li>Ruckus AP Tunnel Stats &gt; Ruckus GRE</li> <li>Ruckus AP Tunnel Stats &gt; SOFT GRE</li> <li>Ruckus AP Tunnel Stats &gt; SoftGRE + IPSec</li> </ul>		AP Management	Read
3rd Party AP Zone	Modify 3rd party AP zone	AP Management/ SZ Management	Modify
	Create/Delete	AP Management/ SZ Management	Full Access
	View 3rd party zone configuration	AP Management/ SZ Management	Read
	Session data of the UE in that zone	User/Device/Application Management	Full Access
	Historical session data of the UE in that zone	User/Device/Application Management	Full Access
3rd Party > Hotspot		AP Management/ SZ Management	
3rd Party > Network Traffic Profile		AP Management/ SZ Management	
3rd Party > Q-in-Q Ether Type	Create	AP Management/ SZ Management	Full Access
3rd Party > L2oGRE	Create	AP Management/ SZ Management	Full Access
3rd Party WLAN	Create/Delete	AP Management/ SZ Management	Full Access
	Modify 3rd Party WLAN	AP Management/ SZ Management	Modify
Indoor Map	Modify	AP Management	Modify
	Create/Delete	AP Management	Full Access
	View configuration content	AP Management	Read
Troubleshooting	Client to AP	AP Management	Read
Manage User Agent Blacklist		WLAN Management	
Services & Profiles > Access Control > Client Isolation Whitelist		WLAN Management	
Services & Profiles > Access Control > Blocked Clients		User/Device/Application Management	
Services & Profiles > DHCP & NAT	DHCP Setting (AP)	AP Management, WLAN Management and SZ Management	Full Access
	DHCP Pools (AP)		
Administration > ZD Migration	Detail	SZ Management	Read
Data Plane	Upload/Update - Calea Mac Setting/ Customized Config	SZ Management	Modify
	Create/Delete - Calea Related Setting/Customized Config	SZ Management	Full Access

**TABLE 27** Relationship between Resource, Operation -Resource Group and Permission Levels (continued)

Resource	Operation	Resource Group	Permission Levels
	View - Calea Related Setting/ Customized Config/ DP Key	SZ Management	Read
	Modify Zone Affinity Profile	SZ Management/AP Management	Modify
	Create/Delete Zone Affinity Profile	SZ Management/AP Management	Full Access
	View Zone Affinity Profile	SZ Management/AP Management	Read

## Creating a User Role with Active Directory Authentication

Configuring user roles using AD authentication provides broad range of directory-based identity-related services.

To create a User Role with AD authentication:

1. Create a new UTP for a particular role, refer [Creating a User Traffic Profile](#) on page 254.
2. Create a role, refer [Creating a User Role](#) on page 198.

3. **NOTE**  
Non-proxy Auth servers are not supported.

Create a new Proxy AD server and apply the UTP. Refer [Creating Proxy AAA Servers for Standby Cluster](#) on page 291.

4. **NOTE**  
In step 4 of the authentication test, for the **Service Protocol** option, choose **Active Directory** and proceed.

Perform an authentication test to ensure that the user gets assigned the correct Role. Refer [Testing AAA Servers](#) on page 296.

5. Create a web authentication portal WLAN configuration and assign the Non-proxy AD server to it. Refer [Creating a WLAN Configuration](#) on page 171.
  - a) Choose **WLAN Usage > Authentication Type > Web Authentication**.
  - b) Configure the following for **Authentication & Accounting Server**:

**Web Authentication Portal:** choose the option from the drop-down.

**Authentication Server:** select the Use the Controller Proxy check box and choose the authentication service from the drop-down.

## Creating a User Role with 802.1x Authentication

To create a User Role with 802.1x authentication:

1. Create a new UTP for a particular role, see [Creating a User Traffic Profile](#) on page 254 .
2. Create a role, refer [Creating a User Role](#) on page 198.

3. **NOTE**  
Non-proxy Auth servers are not supported.

**NOTE**  
In step 4 of this procedure, for the **Service Protocol** option, choose **RADIUS** and proceed.

Create a new Proxy RADIUS server and apply the UTP. Refer [Creating Proxy AAA Servers for Standby Cluster](#) on page 291.

4. Perform an authentication test to ensure that the user gets assigned the correct Role. Refer [Testing AAA Servers](#) on page 296.
5. Create a web authentication portal WLAN configuration and assign the Non-proxy RADIUS server to it. Refer [Creating a WLAN Configuration](#) on page 171.
  - a) Choose **WLAN Usage > Authentication Type > Web Authentication**.
  - b) Go to **Authentication Options > Methods**, choose **802.1x EAP** and proceed.

## Limitations Applying Role Policies to Users

You must be aware of some limitations in applying roles to a user.

Specifically, user role policies are only supported in proxy-mode AAA WLANs. Also, you configure the user-attribute-to-role mapping in AAA profiles. Also, there are some components that will not work in 3.5, even though the GUI would lead us to believe they do. Precedence policies are configurable at the WLAN level, but have an impact on the way that roles are assigned. Finally, we should talk about the difference between assigning UEs to roles via RADIUS and using RADIUS attributes to apply some specific policy, like rate limit, VLAN, or ACL. RADIUS attribute will always take precedence over the role assignment.

## Creating a Local User

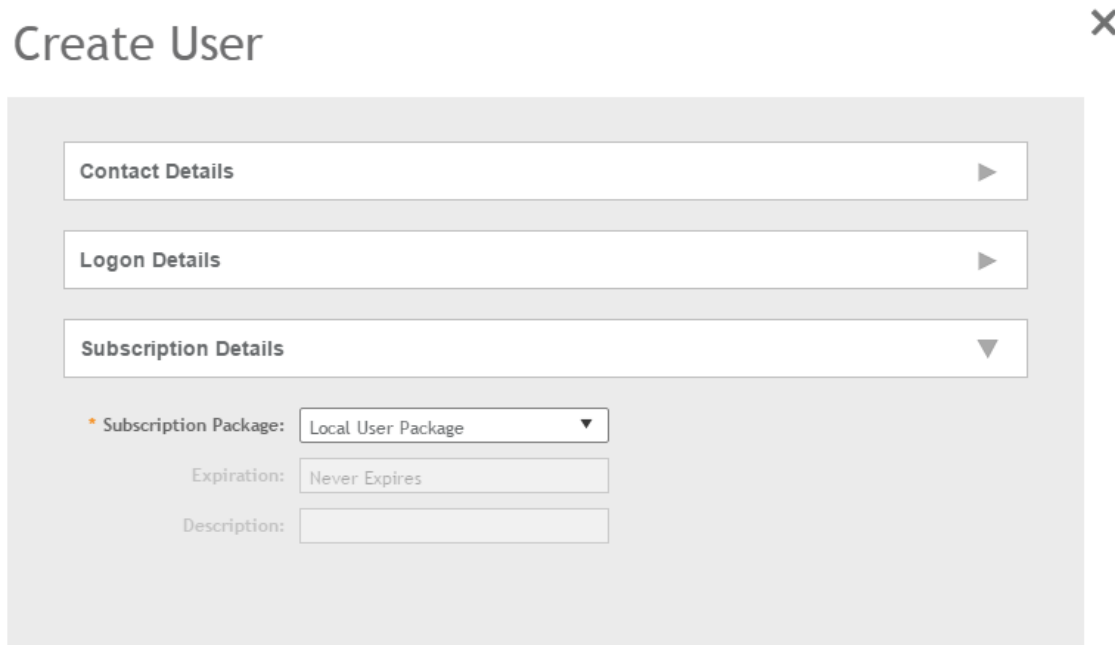
A local user in the controller refers to a registered user who may be given access to the controller hotspot. A user account contains a user's personal information, logon information, and the subscription package that he or she has been assigned. The controller's local user database can include 802.1X, WISPr, and Zero-IT users.

When you create a user account, you will be required to assign a subscription package to the user. Before creating a user account, Ruckus recommends creating at least one subscription package. See [Creating a VLAN Pooling Profile](#) on page 261 for more information.

1. Go to **Clients > Users & Roles**.
2. Select the **Local Users** tab, and then select the zone for which you want to create the local user.

3. Click **Create**.  
The **Create User** page appears.

**FIGURE 84** Create User




The screenshot shows the 'Create User' form. At the top, there is a title 'Create User' and a close button 'X'. Below the title, there are three expandable sections: 'Contact Details', 'Logon Details', and 'Subscription Details'. The 'Subscription Details' section is expanded, showing a 'Subscription Package' dropdown menu with 'Local User Package' selected, an 'Expiration' field with 'Never Expires', and a 'Description' field.


4. Configure the options in the **Create User** form.
  - a. In the **Contact Details** section, fill the following:
    - First Name
    - Last Name
    - Email
    - Phone
    - Address
    - City
    - State
    - Zip Code
    - Country
    - Remark
  - b. In the **Login Details** section, fill out the following boxes to create the logon credentials of this user:
    - User Name: Type a name for this user. The user name is not case-sensitive and will always be displayed in lowercase characters.
    - Password: Type a password for this user. The password must be at least eight characters in length.
    - Confirm Password: Retype the password above.
  - c. In the **Subscription Details** section, select a subscription package that you want to assign to this user. See [Creating a Subscription Package](#) on page 210, for more information.
5. Click **OK**.


You have completed creating a local user.

Select **Enable** to enable this user profile or select **Disable**.

You can view the list of local users by applying filters. Click the  icon to do so.

The following information is displayed when you click on the user:

- **Summary:** Displays a summary of information about the user.
- **Admin Activities:** Displays information about the administrator activities.
- **Event:** Displays information about events associated with the user. Click the  icon to apply filters.

Click the  icon to export all the data into a CSV file.

**NOTE**

You can also edit, clone and delete user by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Local Users** tab.

## Creating a Subscription Package

A subscription package defines the characteristics of a subscription that has been created for a registered user. These characteristics include the expiration date of the subscription.

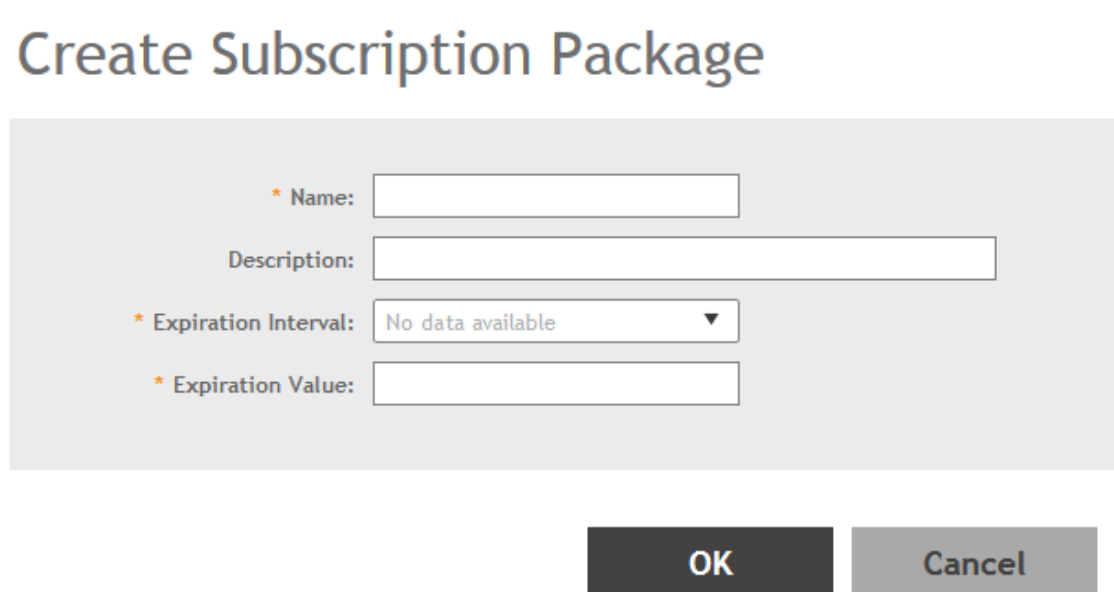
If the user is connected at the time when his or her subscription expires, the user will get disconnected from the AP and any attempts to re-authenticate will fail.

1. Go to **Clients > Users & Roles**.
2. Select the **Subscription Package** tab, and then select the zone for which you want to create the package.

3. Click **Create**.

The **Create Subscription Package** page appears.

**FIGURE 85** Create Subscription Package



**Create Subscription Package**

\* Name:

Description:

\* Expiration Interval:

\* Expiration Value:

**OK** **Cancel**

4. Configure the options in the **Create Subscription Package** form.
  - Name: Type a name for the subscription package that you are creating.
  - Description: Type a description for this package.
  - Expiration Interval: Set the time unit to use for the package expiration. Options include: Hour, Day, Week, Month, Year and Never.
  - Expiration Value: Set the actual value to use in combination with the Expiration Time.
5. Click **OK**.

You have completed creating a subscription package.

**NOTE**

You can also edit and delete a package by selecting the options **Configure** and **Delete** respectively, from the **Subscription Package** tab.

## Working with Guest Passes

Similar to user accounts, guest passes in the controller allow users to gain access to the controller hotspots. However, unlike user accounts, guest pass users are not required to provide personal information to access the controller hotspots and can therefore remain anonymous.

Guest passes are generated for specific WLANs only – guest pass users will only be able to gain access to the WLANs for which the guest pass was generated.

## Generating Guest Passes

Generating guest passes involves four steps:

[Step 1: Create a Guest Access Service](#) on page 212

[Step 2: Create a Guest Access WLAN](#) on page 212

[Step 3: Generate a Guest Pass](#) on page 213

[Step 4: Send Guest Passes to Guest Users](#) on page 215

### *Step 1: Create a Guest Access Service*

1. Follow the instructions in [Creating a Guest Access Portal](#) on page 235 to create at least one guest access service in Guest Access Portal.
2. When you finish creating a guest access service, continue to the next task.

### *Step 2: Create a Guest Access WLAN*

Guest passes are generated for specific WLANs only. Guest pass users will only be able to gain access to the WLANs for which the guest pass is generated.

Follow these steps to create a WLAN that will be used for guest access only.

1. Click **Wireless LANs**.  
The **Wireless LANs** page appears.
2. Click **Create**.  
The **Create WLAN Configuration** page appears.
3. In **General Options**, configure the following:
  - **Name**
  - **SSID**
  - **Description**
  - **Zone**
  - **WLAN Group**
4. In **WLAN Usage**, configure the following:
  - a) In **Access Network**, select the **Tunnel WLAN traffic through Ruckus GRE** check box if you want to tunnel the traffic from this WLAN back to the controller.
  - b) In **Authentication Type**, click **Guest Access**.
5. Configure the rest of the WLAN settings.  
For details on each setting, see the Working with WLANs section.



- When you finish creating a guest access WLAN, continue to the next step.

**FIGURE 86** Creating a WLAN for guest access only

The screenshot shows a configuration interface for a WLAN. It has two main sections: 'Encryption Options' and 'Guest Access Portal'. In the 'Encryption Options' section, the 'Method' is set to 'None' with radio buttons for WPA2, WPA-Mixed, WEP-64 (40 bits), WEP-128 (104 bits), and None. The 'Guest Access Portal' section includes a 'Guest Portal Service' dropdown set to 'Select a guest access' with a '+ Create' button. Below this, 'Bypass CNA' is checked and labeled 'Enable'. 'Guest Authentication' is set to 'Select an authentication se'. At the bottom, 'Guest Accounting' is checked and labeled 'Use the Controller as Proxy', with a dropdown set to 'KHK-ACCT' and a '+ Create' button. To the right, 'Send interim update every' is set to '1' with a unit of 'Minutes (0-144)'.

### Step 3: Generate a Guest Pass

Follow these steps to generate a guest pass.

- Click **Clients > Guests**.  
The **Guest Pass** page appears.
- Click **Generate Guest Pass**.  
The **Generate Guest Pass** form appears.
- Configure the following options:
  - Guest Name:** Type a name that you want to assign to the guest user.
  - Guest WLAN:** Select the guest WLAN that you created in [Step 2: Create a Guest Access WLAN](#) on page 212.
  - Number of Passes:** Type the number of guest passes that you want to generate.
  - Pass Valid For:** Set the validity period for the guest pass by filling in the two boxes. For example, if you want the guest pass to be valid for seven days, type **7** in the first box, and then select **Days** in the second box.

4. Configure the advanced options:

- a) **Pass Generation:** Select the **Auto Generate** check box if you want the controller to generate the guest pass key automatically.

If you want to generate the guest pass manually, clear the **Auto Generate** check box.

If you are generating more than one guest pass, the Auto Generate check box is selected automatically and is not configurable.

- b) **Pass Effective Since:** Set the guest pass validity period by selecting one of the following options:

- **Effective from the creation time:** This type of guest pass is valid from the time it is first created to the specified expiration time, even if it is not being used by any end user.
- **Effective from first use:** This type of guest pass is valid from the time the user uses it to authenticate with the controller until the specified expiration time. An additional parameter (Guest Pass will expire in X days) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
- **Expire guest pass if not used within [ ] days:** If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).

- c) **Max Devices Allowed:** Set the number of users that can share this guest pass.

- **Limited to [ ]:** If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
- **Unlimited:** If you want an unlimited number of users to share this guest pass, click this option.
- **Session Duration:** If you clicked **Unlimited**, this option appears. If you want require users to log on again after their sessions expire, select the **Require guest re-login after [ ]** check box, and then select a time increment. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.

- d) In **Remarks** (optional), type your notes about this guest pass, if any.

5. Click **Generate**.

The page refreshes, and then the guest pass you generated appears in a table, along with other guest passes that exist on the controller.

Click **Enable** to enable the guest pass for a user, and **Disable** to revoke the guest pass for a particular user.

You have completed generating a guest pass. You are now ready to send the guest pass to guest users. See [Step 4: Send Guest Passes to Guest Users](#) on page 215 for information.

You can view the list of guest passes by applying filters. Click the  icon to do so.

The following information is displayed when you click on the guest pass created:

- **Summary:** Displays a summary of information about the user and credentials.
- **Admin Activities:** Displays information about the administrator activities.
- **Event:** Displays information about events associated with the user.

Click the  icon to apply filters. Click the  icon to export all the data into a CSV file.

**FIGURE 87** Generating a guest pass

## Generate Guest Pass ✕

\*

 Guest Name:

\*

 Guest WLAN:

\*

 Number of Passes:

\*

 Pass Valid For:

Advanced Options

▼

Pass Generation:

☒ Auto Generate

\*

 Pass Value:

Pass Effective Since:

☒ Effective from the creation time

☐ Effective from first use

\*

 Expire new guest pass if not used within:

days

\*

 Max Devices Allowed:

☒ Limited to

☐ Unlimited

Remarks:

Generate

Cancel

### **Step 4: Send Guest Passes to Guest Users**

Deliver the guest passes to guest users as per the delivery options that you choose.

The page that appears after you generate a guest pass contains options for delivering the guest pass to guest users (see the following image).

**FIGURE 88** Options for delivering guest passes to guest users

Here are the generated guest passes ▼

Print Selected	Export Selected	Email	SMS	Delete	<input checked="" type="checkbox"/> Enable	<input type="checkbox"/> Disable	More ▾	Filter Off		search table		
Guest Name ▲	Manage By	Key	Remarks	Generated	Expiration Date	WLAN						
Sam	System	Wv3QSH6q	One day pass	2017/03/08 17:41:30	2017/03/09 17:41:30	[SZ-300-GUEST] of [TEST-JL...						
Sen	System	sajeXkCg	N/A	2017/03/08 18:45:26	N/A	[SZ-300-GUEST] of [TEST-JL...						
test2	System	DNp2u8D3	N/A	2017/01/18 14:19:18	2017/01/19 14:19:18	[SZ-300-GUEST] of [TEST-JL...						

3 total records    1    »

## Creating a Guest Pass Template

A guest pass template is a HTML file which contains variables for the information that guest users need to connect to the controller hotspots (for example, guest name, key, and WLAN name), and actual instructions for connecting to the guest WLAN.

A default printout template exists in the controller. If you want to create your own printout template, follow these steps.

1. Go to **Clients > Guests**.
2. Click **Guest Pass Template**.

The **Guest Pass Template** page appears.

3. In the **Guest Instruction HTML Template** section, click `default.html`, which is the default guest pass printout template.

The content of the default guest pass printout template appears in the *Name: default.html*.

4. Click **Download** below the template preview area to download a copy of the template to your computer.
5. Using an HTML editor, create a new HTML file.
6. Add content to the file.

Typically, a printout template contains instructions for connecting to the controller hotspot. See the following image for the content of the default printout template.

**FIGURE 89** Content of the default printout template

### Connecting as a Guest to the Corporate Wireless Network

Greetings, {GP\_GUEST\_NAME}

You have been granted access to the company wireless network, which you can use to access both the World Wide Web and Internet, and to check your personal email.

Your guest pass key is: {GP\_GUEST\_KEY}

This guest pass is valid until {GP\_VALID\_TIME}

Connect your wireless-ready PC to the following network(s): {GP\_GUEST\_WLAN}, as detailed in the instructions printed below.

Before you start, please review the following requirements.

---

7. Insert the following variables into the content of your template:
  - `{GP_GUEST_NAME}`: This is the guest pass user name.
  - `{GP_GUEST_KEY}`: This is the guest pass key.
  - `{GP_VALID_TIME}`: This is the expiration date and time of the guest pass.
  - `{GP_GUEST_WLAN}`: This is the WLAN with which the guest user can associate using the guest name and guest key.
8. Save the file.
9. In the **Guest Instruction HTML Template** page, click the **Upload** button for the template that you are creating.  
The **Upload a Template File** form appears on the right side of the page.
10. Configure the **Upload a Template File** options:
  - **Template Name**: Type a name for the template that you are uploading.
  - **Template File**: Click **Browse**, and select the template file you created.
11. Click **Upload**.  
An information message box appears and informs you that the template file has been uploaded successfully.
12. Click **OK**.  
The template file you uploaded now appears in the list of templates.

**FIGURE 90** The Upload a Template File form

Guest Instruction HTML Templates	
<div> <div> <div>Upload</div> <div>Delete</div> </div> <div> <input type="text" value="search table"/> <div>Q</div> <div>Refresh</div> </div> </div>	
Name	Manage By
default.html	System
Sha1	System

## Creating a Guest Instruction SMS Template

A guest SMS template is a text file which contains variables for the information that guest users need to connect to the controller hotspots (for example, guest name, key, and WLAN name), and actual instructions for connecting to the guest WLAN.

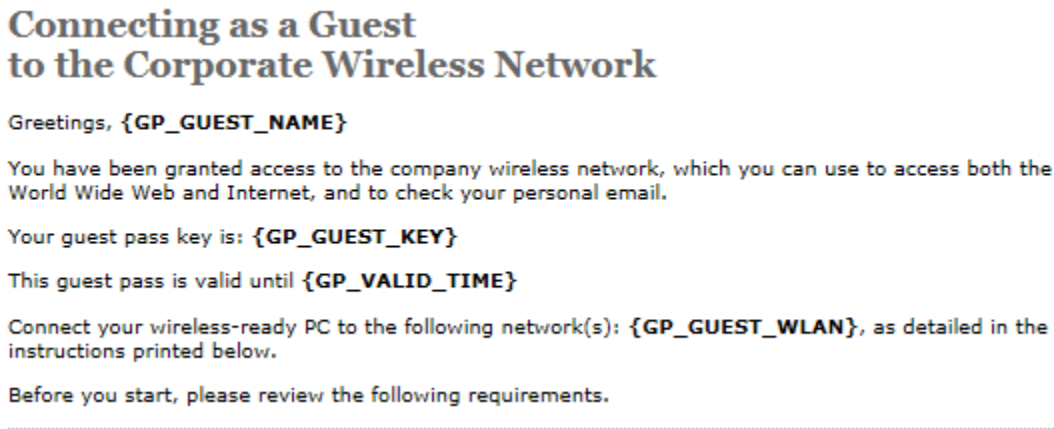
A default printout template exists in the controller. If you want to create your own printout template, follow these steps.

1. Go to **Clients > Guests**.
2. Click **Guest Pass Template**.  
The **Guest Pass Template** page appears.
3. In the **Guest Instruction SMS Template** section, click `default.txt`, which is the default guest pass printout template.  
The content of the default guest pass printout template appears in the *Name: default.txt*.
4. Click **Download** below the template preview area to download a copy of the template to your computer.
5. Using an HTML editor, create a new text file.

6. Add content to the file.

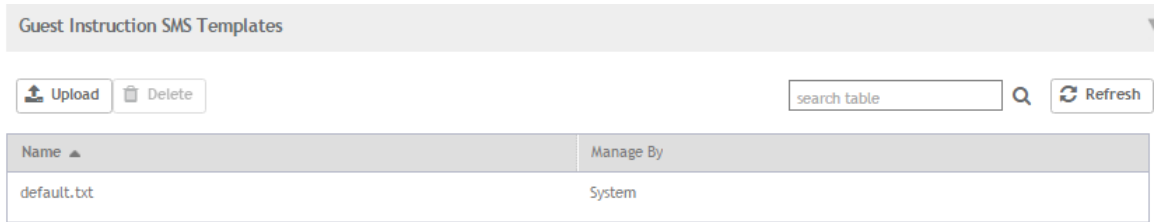
Typically, a printout template contains instructions for connecting to the controller hotspot. See the following image for the content of the default printout template.

**FIGURE 91** Content of the default printout template



7. Insert the following variables into the content of your template:
- {GP\_GUEST\_NAME}: This is the guest pass user name.
  - {GP\_GUEST\_KEY}: This is the guest pass key.
  - {GP\_VALID\_TIME}: This is the expiration date and time of the guest pass.
  - {GP\_GUEST\_WLAN}: This is the WLAN with which the guest user can associate using the guest name and guest key.
8. Save the file.
9. In the **Guest Instruction SMS Template** page, click the **Upload** button for the template that you are creating.
- The **Upload a Template File** form appears on the right side of the page.
10. Configure the **Upload a Template File** options:
- **Template Name:** Type a name for the template that you are uploading.
  - **Template File:** Click **Browse**, and select the template file you created.
11. Click **Upload**.
- An information message box appears and informs you that the template file has been uploaded successfully.
12. Click **OK**.
- The template file you uploaded now appears in the list of templates.

**FIGURE 92** The Upload a Template File form



## Exporting the Guest Pass to CSV

Follow these steps to export the last generated guest passes to a comma-separated value (CSV) file.

1. From the generate guest pass list, select the guest passes that you want to export to CSV.
2. Click **Export Selected**.

Your web browser downloads the CSV file to its default download location.

3. Go to your web browser's default download location and look for a file named `guestpass.csv`.
4. Using Microsoft Excel or a similar application, open the CSV file. The CSV file displays the details of the guest passes, including:
  - Guest Name
  - Key
  - Remarks
  - Generated
  - Expiration Date
  - WLAN

You have completed exporting the last generated guest passes to CSV.

**FIGURE 93** A sample CSV of generated guest passes when opened in Excel

	A	B	C	D	E	F	G	H	I	J	K	L
1	Guest Name	Key	Remarks	Generated	Expiration Date	WLAN						
2	test2	DNp2u8D3		18-01-2017 14:19	19-01-2017 14:19	[SZ-300-GUEST] of [TEST-JILANI]						
3												
4												
5												
6												
7												
8												
9												
10												
11												
12												

## Generating Guest Passes from an Imported CSV

You can also manually define the guest passes that you want to generate in a comma-separated value (CSV) file (a sample of which is available for download from the **Guest Pass** page).

Follow these steps to generate guest passes from an imported CSV file.

1. Click **Clients > Guests**.

The **Guest Pass** page appears.

2. Click **Import Guest Pass**,

The **Import Guest Pass** form appears.

3. Look for the following text under Browse:

To download a sample guest pass, click here.

4. Click the **here** link to download the sample CSV file.

5. Using Microsoft Excel or a similar application, open the CSV file.

6. In the CSV file, fill out the following columns:

- **#Guest Name (Must):** Assign a user name to the guest pass user.
- **Remarks (Optional):** Add some notes or comments about this guest pass.
- **Key:** Enter a guest pass key or leave it blank so the controller can generate the key automatically.

**FIGURE 94** The sample CSV file when opened in Excel

A6			
	A	B	C
1	#Guest Name (Must)	Remarks	Key (Empty implies random key)
2	Batch-Guest-1	Batch generation	AAAAAAAA
3	Batch-Guest-2	Batch generation	
4	Batch-Guest-3		
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			

7. Save the CSV file.

8. Go back to the **Import Guest Pass** page, and then configure the following settings on the Common Guest Pass Settings:

- **Guest WLAN:** Select the guest WLAN that you created in [Step 2: Create a Guest Access WLAN](#) on page 212.
- **Pass Valid For:** Set the validity period for the guest pass by filling in the two boxes. For example, if you want the guest pass to be valid for seven days, type **7** in the first box, and then select **Days** in the second box.



9. Configure the advanced options:

a) **Pass Effective Since:** Set the guest pass validity period by selecting one of the following options:

- **Effective from the creation time:** This type of guest pass is valid from the time it is first created to the specified expiration time, even if it is not being used by any end user.
- **Effective from first use:** This type of guest pass is valid from the time the user uses it to authenticate with the controller until the specified expiration time. An additional parameter (**Guest Pass will expire in X days**) can be configured to specify when an unused guest pass will expire regardless of use. The default is 7 days.
- **Expire guest pass if not used within [ ] days:** If you want this guest pass to expire if it is unused after you generated it, type the number of days in the box (maximum value is 365 days).

b) **Max Devices Allowed:** Set the number of users that can share this guest pass.

- **Limited to [ ]:** If you want a limited number of users to share this guest pass, click this option, and then type the number in the box.
- **Unlimited:** If you want an unlimited number of users to share this guest pass, click this option.
- **Session Duration:** If you clicked **Unlimited**, this option appears. If you want require users to log on again after their sessions expire, select the **Require guest re-login after [ ]** check box, and then select a time increment. If this feature is disabled, connected users will not be required to re-log in until the guest pass expires.

10. In **Guest List CSV File** (at the top of the page), click **Browse**, and then select the CSV file you edited earlier.

The page refreshes, and the number of guest passes that the controller has identified in the CSV file appears below the **Browse** button.

11. Click **Import**.

The page refreshes, and then the guest pass you generated appears in a table, along with other guest passes that exist on the controller.

You have completed generating a guest pass. You are now ready to send the guest pass to guest users. See [Step 4: Send Guest Passes to Guest Users](#) on page 215 for information.

**FIGURE 95** The Guest Pass page for importing a CSV file

Here are the generated guest passes ▼

Print Selected	Export Selected	Email	SMS	Delete	Enable	Disable	More ▾	Filter Off		search table	
Guest Name ▲	Manage By	Key	Remarks	Generated	Expiration Date	WLAN					
Sam	System	Wv3QSH6q	One day pass	2017/03/08 17:41:30	2017/03/09 17:41:30	[SZ-300-GUEST] of [TEST-JL...					
Sen	System	sajeXkCg	N/A	2017/03/08 18:45:26	N/A	[SZ-300-GUEST] of [TEST-JL...					
test2	System	DNp2u8D3	N/A	2017/01/18 14:19:18	2017/01/19 14:19:18	[SZ-300-GUEST] of [TEST-JL...					

3 total records 1

## Printing the Guest Pass

After you generate the guest pass, you can print the guest pass information, which contains the guest user information and instructions on how to connect to the hotspot, and give it to the guest user.

### NOTE

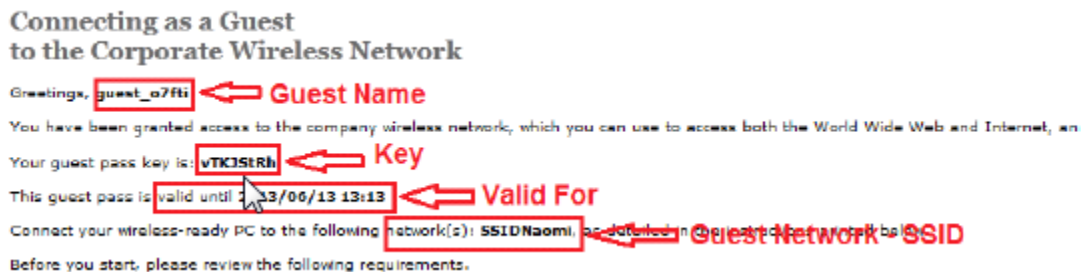
If your browser is blocking pop-ups, make you temporarily disable the pop-up blocker so you can view and print the guest pass.

Follow these steps to print a guest pass.

1. From the generated guest passes list, select the guest passes that you want to print.
2. In **Guest Instruction HTML Template**, select a printout template to use.  
The default printout template (default.html) is selected by default. If you created custom printout templates (see [Creating a Guest Pass Template](#) on page 216), they will appear in the drop-down menu.
3. Click **Print Selected**.  
A new browser page appears, which displays the guest pass and available printing options.
4. Configure your printer settings, and then print the guest passes.

You have completed printing the guest passes.

**FIGURE 96** What a guest pass printout looks like



## Sending the Guest Pass via Email

To send guest passes via email, you must have added an external email server to the controller.

Follow these steps to send the guest pass via email.

1. From the generated guest passes list, select the guest passes that you want to send via email.
2. Click **Email**.  
The Recipient Email form appears on the right side of the page (see [Figure 97](#)).
3. Click **Add New**.
4. In the box that appears below, type the email address to which you want to send the guest passes.
5. To add another recipient, click **Add New** again, and then type another email address.
6. When you have finished adding all the email recipients, click **Send Email**.

A dialog box appears and informs you that the emails have been sent to the message queue successfully

7. Click **OK** to close the dialog box.

You have completed sending guest passes via email.

**FIGURE 97** Use the Recipient Email form to specify who will receive the guest passes via email

Here are the generated guest passes ▼

☒ Enable
 ☐ Disable

Guest Name ▲	Manage By	Key	Remarks	Generated	Expiration Date	WLAN
Sam	System	Wv3Q5H6q	One day...	2017/03/08 17:41:30	2017/03/09 17:41:30	[SZ-300-GUES
Sen	System	saJeXkCg	N/A	2017/03/08 18:45:26	N/A	[SZ-300-GUES
test2	System	DNp2u8D3	N/A	2017/01/18 14:19:18	2017/01/19 14:19:18	[SZ-300-GUES

3 total records < 1 >

Recipient Email

sama@yahoo.co

## Sending the Guest Pass via SMS

To send guest passes via sms, you must have added an external SMS gateway to the controller.

Follow these steps to send the guest pass via email.

1. From the generated guest passes list, select the guest pass that you want to send via SMS.
2. Click **SMS**.

SMS options appear on the right side of the page (see [Figure 98](#)).

3. In Guest Instruction SMS Template, select the SMS template that you want to use.
4. Click **Add New**.
5. In the box that appears below, type the phone number to which you want to send the guest passes via SMS.
6. To add another SMS recipient, click **Add New** again, and then type another phone number.
7. When you have finished adding all the SMS recipients, click **Send SMS**.

A dialog box appears and informs you that the SMS messages have been sent to the message queue successfully

8. Click **OK** to close the dialog box.

You have completed sending guest passes via SMS.

**FIGURE 98** Options for sending guest passes via SMS

Here are the generated guest passes ▼

Print Selected Export Selected Email SMS Delete Enable Disable

Guest Name	Manage By	Key	Remarks	Generated	Expiration
Sam	System	Wv3QSH6q	One day...	2017/03/08 17:41:30	2017/03/09 17:41:30
Sen	System	sajeXkCg	N/A	2017/03/08 18:45:26	N/A
test2	System	DNp2u8D3	N/A	2017/01/18 14:19:18	2017/01/19 14:19:18

3 total records < 1 >

Guest Instruction SMS Template: default.txt

Recipient Phone Number 9876543210 x Add New Remove

Send SMS

## Working with Dynamic PSKs

Dynamic PSKs (DPSKs) are unique pre-shared keys assigned to a user or device. DPSKs are used to provide secure wireless access, which helps avoid manual wireless configuration and managing encryption keys.

DPSK is a form of PSK (static key) in a WPA2 WLAN and its purpose is to provide each user device with a unique dynamic PSK to associate to a WLAN without any modifications to the WLAN configuration. For example, a school administrator provides a time-limited DPSK for student's device so that the student can access the school's WLAN for the period their DPSK is valid. After the validity period ends, the DPSK expires and the student's device can no longer access the school's WLAN. Without the use of DPSKs, the school administrator would have to change the default static key to prevent the student from using the WLAN resources, which in turn would impact all other users of that WLAN.

Individual DPSKs can be deleted in the event of a student leaving the school, or their device being lost or stolen without impacting other users of the WLAN.

A "bound" DPSK is one which is assigned to the MAC address of a user device at the time of creation. No other user device can utilize this DSPK. Bound DPSKs are stored in on APs.

An "unbound" DPSK is not assigned to a device's MAC address during creation, but upon its first use (that is, when the device first connects to a WLAN and the DPSK is entered as the WLAN security key). Once a DPSK becomes assigned to a user device, it becomes bound and no other user device can use it.

### NOTE

If you generate a single unbound DPSK, then only one device can be connected to the DPSK WLAN by the key, since other devices can still use "admin" PSK to connect to the DPSK WLAN. However, when devices from different APs try to use the same unbound DPSK simultaneously, for a short period, they could both connect to the WLAN successfully, but the later device will be disconnected by the controller. If the AP happens to disconnect from the controller, the device could stay connected until the AP connects back to the controller.

When DPSKs are created, there are some prevented behaviors that are considered database conflicts such as the following:

- You cannot create two unbound DPSKs with the same passphrase.
- You cannot create two bound DPSKs for the same MAC address and passphrase. Create two DPSKs for the same MAC address, the former will be replaced. However, you can create multiple bound DPSKs with different MAC addresses and the same passphrase.
- You can also create bound DPSKs and a single unbound DPSK with the same passphrase.

UEs within a PSK WLAN use the same shared key to encrypt data traffic, but if the key is compromised by even one WLAN user, the entire user traffic can be accessed/hacked. Therefore, a secure tunnel is created for each user connected to the WLAN, by configuring the PSK WLAN as an *Internal* or *External* DPSK.

In Internal DPSKs, the controller manages and records the DPSK for each individual user and a limited number of DPSKs are supported.

In External DPSKs, the DPSK is maintained by the Radius Server (AAA) and Radius protocols are used to authenticate the UE. The UE is authenticated by the open authentication WLAN - WPA/WPA2 encryption where in, the controller uses the RADIUS interface with the RADIUS server (AAA includes the DPSK in the Radius response or Access Accept message and sends it to the AP) so that the DPSK is maintained in one place. There is no limitation on the number of DPSK supported in this mode.

**NOTE**

Only proxy AAA authentication is supported for External DPSK.

**NOTE**

External DPSKs are supported only on bounded DPSKs.

## Viewing Dynamic PSKs

You can view the DPSKs that have been generated on the controller.

The following information about DPSKs is available:

- User Name
- MAC Address
- WLAN (SSID)
- User Role
- VLAN ID
- Created Date
- Expiration Date
- Expired - Lists the DPSKs that have expired.
- Group DPSK - Specifies which DPSK is a group DPSK.

Complete the following steps to view the DPSKs:

1. Select **Clients > Dynamic PSK**.

The **Dynamic PSK** page appears listing the DPSKs that have been generated.

**NOTE**

You can sort the list of DPSKs or export the listed DPSKs to a CSV file.

**NOTE**

You can search for DPSKs by performing a full text search using the following fields: **User Name**, **MAC Address**, and **VLAN ID**.

2. (Optional) Click the **Delete Expired DPSKs** arrow and select one of the following options:
  - **Never**: No action must be taken for the expired DPSKs.
  - **After 1 day**: Auto-deletes DPSKs that have expired after one day.
  - **After 6 months**: Auto-deletes DPSKs that have expired after 6 months.

You have completed viewing the list of DPSKs.

## Generating Dynamic PSKs

You can generate new dynamic PSKs to secure the WiFi network.

Follow these steps to generate the dynamic PSKs (DPSKs):

1. Click **Clients > Dynamic PSK**.

The **Dynamic PSK** page appears listing the PSKs that were generated.

2. Click **Generate DPSKs**.

The **Generate DPSKs** dialog box appears.

3. Provide the following information:

- **WLAN:** From the drop-down list, select a DPSK-enabled WLAN.
- **Number of DPSKs:** Type the number of PSKs you want to create in a zone. You can generate up to a maximum of 500 Unbound or Group DPSKs.

There are three types of DPSKs:

- Unbound DPSK (DPSK not binding to a specific device yet)

Once an unbound DPSK is used by a device, it will become bound DPSK and release one slot from the maximum limit of 500.

- Group DPSK (DPSK that can be shared between devices)

A group DPSK will never become bound, it always occupy one slot from the 500 limit, until the Admin deletes it.

- Bound DPSK (DPSK bound to a specific device)

An Admin can import Bound DPSKs using CSV by specifying the **MAC Address** and create Bound DPSKs regardless of the 25,000 limitation.

SZ version	Max DPSK per zone	Max Unbound DPSK per zone	Max Group DPSK per zone
3.4.x	10K	256	X
3.5.x	10K	256	64
3.6.x	10K	Share 320 slots for Unbound and Group DPSKs	
5.1	25K	Share 500 slots for Unbound and Group DPSKs	


### NOTE

For SZ100/vSZ-E platform, the maximum number of DPSKs is 25,000 per zone or system.

- **User Name:** Leave it blank if you want the controller to auto-generate the user name, or enter the user name manually.
- **Passphrase:** Leave it blank if you want the controller to auto-generate the passphrase, or enter the passphrase manually.
- **User Role:** If you have created user roles, select the user role that you want to assign to the device that connects to the SmartZone network using this DPSK. The device will be assigned the same attributes and permissions (VLAN, UTP, time restrictions, etc.) that have been defined for the assigned user role.
- **VLAN ID:** Type a VLAN ID within the range 1-4094.
- **Group DPSK:** If you want multiple devices to be able to use this DPSK, click **Yes**. If you want only a single device to use this DPSK (bound DPSK), click **No**.

4. Click **Generate**.

You have completed creating dynamic PSKs.

To delete a DPSK, click the DPSK from the list, and then click the  **Delete** icon.

## Importing Dynamic PSKs

You can import CSV files to create DPSKs to secure the WiFi network.

Follow these steps to import dynamic PSKs (DPSKs):

1. Click **Clients > Dynamic PSK**.

The **Dynamic PSK** page appears and lists the DPSKs that have been generated.

2. Click the **Download Sample (CSV)** link to download the CSV template for generating DPSKs.

A sample CSV file is displayed as show in the figure.

**FIGURE 99** Sample CSV file

A	B	C	D	E	F
User Name	MAC Address	VLAN ID	User Role	Passphrase	Group DPSK
DPSK-User-1	00:11:22:33:44:44				
DPSK-User-2	00:11:22:33:44:55	1		passphrase02	
DPSK-User-3	11:22:33:44:55:66	2	testUserRole	passphrase03	
Group-DPSK-1					Y

3. Modify the CSV file as appropriate and save it. The following are the fields that need to be completed in the CSV file:
  - **User Name** (mandatory field): Enter the user name.
  - **MAC Address** (optional): Enter the MAC address of the device for which to generate a DPSK (bound DPSK). If you leave the MAC address field empty, the controller will generate an unbound DPSK.
  - **VLAN ID** (optional): Enter a value to override the WLAN VLAN ID, or leave it empty if you do not want to override the WLAN VLAN ID.
  - **User Role** (optional): If you have created user roles, type the name of the user role that you want to assign to the device that connects to the SmartZone network using this DPSK. The device will be assigned the same attributes and permissions (VLAN, UTP, time restrictions, etc.) that have been defined for the assigned user role.
  - **Passphrase** (optional): Leave it blank if you want the controller to auto-generate the passphrase, or enter the passphrase manually.
  - **Group DPSK** (optional): Enter **Y** to indicate the entry is a Group DPSK if you want multiple devices to use this DPSK.
4. Click **Import CSV**.

The **Import CSV** dialog box appears.

### NOTE

Importing a CSV file that contains a MAC address to which an existing DPSK (on the same target WLAN) is already assigned will replace the existing DPSK on the controller database.

5. In **DPSK Enabled WLAN**, select a WLAN from the drop-down list. Only WLANs that support DPSK must be selected.

6. In **Choose File**, click **Browse** to choose the CSV file.

Click **Clear** if you want to replace the CSV file.

You can also specify **Group DPSK** in the CSV file.

7. Click **Upload**.

The generated DPSKs appear in the table on the **Dynamic PSK** page.

**NOTE**

You can import up to 1,000 DPSKs (not over 25K unbound + group DPSKs) at a time.

8. Click **Download CSV** to download a CSV that contains the generated DPSKs.

The CSV file appears in the following format.

**FIGURE 100** New CSV format

User Name	MAC	WLAN (SSID)	Passphrase	VLAN ID	Created Date	Expiration Date
DPSK-User-1	00:11:22:33:44:44	joe-wlan (joe-wlan)	4#4BSXMe		3/17/2016 18:55	Unlimited
DPSK-User-2	00:11:22:33:44:55	joe-wlan (joe-wlan)	rE<r0[]y	1	3/17/2016 18:55	Unlimited
DPSK-User-3	11:22:33:44:55:66	joe-wlan (joe-wlan)	'q=7vqfE	2	3/17/2016 18:55	Unlimited

You have completed generating DPSKs.

**NOTE**

Click **Export All** to export all the dynamic PSKs to a CSV file. You can also export specific dynamic PSKs by selected them and clicking **Export Selected**.

## Creating an External DPSK Over RADIUS WLAN

External DPSKs use the radius interface with the RADIUS Server (AAA) to maintain the DPSKs centrally. There is no limitation in the number of DPSKs that are supported.

To create an external DPSK over RADIUS WLAN:

1. Create an Authentication Service. Refer, [Creating Non-Proxy Authentication AAA Servers for Standby Cluster](#) on page 289.
2. Create an Accounting Service. Refer, [Creating Proxy Accounting AAA Servers for Standby Cluster](#) on page 303.
3. Create Zone Configuration. Refer, [Creating an AP Zone](#) on page 62.



4. Create a WLAN Configuration for DPSK. Refer, [Creating a WLAN Configuration](#) on page 171.

**FIGURE 101** External DPSK Configuration

**Create WLAN Configuration**

**WLAN Usage**

Access Network: ☐ Tunnel WLAN traffic through Ruckus GRE

Authentication Type: ☒ Standard usage (For most regular wireless networks) ☐ Hotspot (WISPr) ☐ Guest Access ☐ Web Authentication  
☐ Hotspot 2.0 Access ☐ Hotspot 2.0 Secure Onboarding (OSEN) ☐ WeChat

**Authentication Options**

Method: ☒ Open ☐ 802.1x EAP ☐ MAC Address

**Encryption Options**

Method: ☒ WPA2 ☐ WPA-Mixed ☐ WEP-64 (40 bits) ☐ WEP-128 (104 bits) ☐ None

Algorithm: ☒ AES ☐ AUTO

802.11w MFP: ☒ Disabled ☐ Capable ☐ Required

Dynamic PSK: ☐ Disable ☐ Internal ☒ External

**Authentication & Accounting Service**

Authentication Service: ☒ Use the controller as proxy

Accounting Service: ☐ Use the controller as proxy

**OK** **Cancel**

**NOTE**

- To connect to an external DPSK SSID, we need to generate hexadecimal keys using an external tool.
- The derived keys should match the mathematical formula: Key = PBKDF2 (passphrase, ssid, 4096, 256). (Here, we can also have reference to RFC2898).
- Pre-pend 0x00 to the calculated value of the key.



# Application Recognition and Control

---

- [Monitoring Applications.....](#) 231

Application Recognition and Control enables you to identify, monitor and control the applications that are running on wireless clients associated with managed APs.

## Monitoring Applications

If you have enabled Application Recognition and Control for at least one WLAN, you can monitor the applications that run on wireless clients associated with that WLAN.

### NOTE

To configure application recognition and control policies, go to **Services and Profiles > Application Control**. For more information, see [Configuring Application Controls](#) on page 271.

To monitor the top applications by traffic consumption on the wireless network:

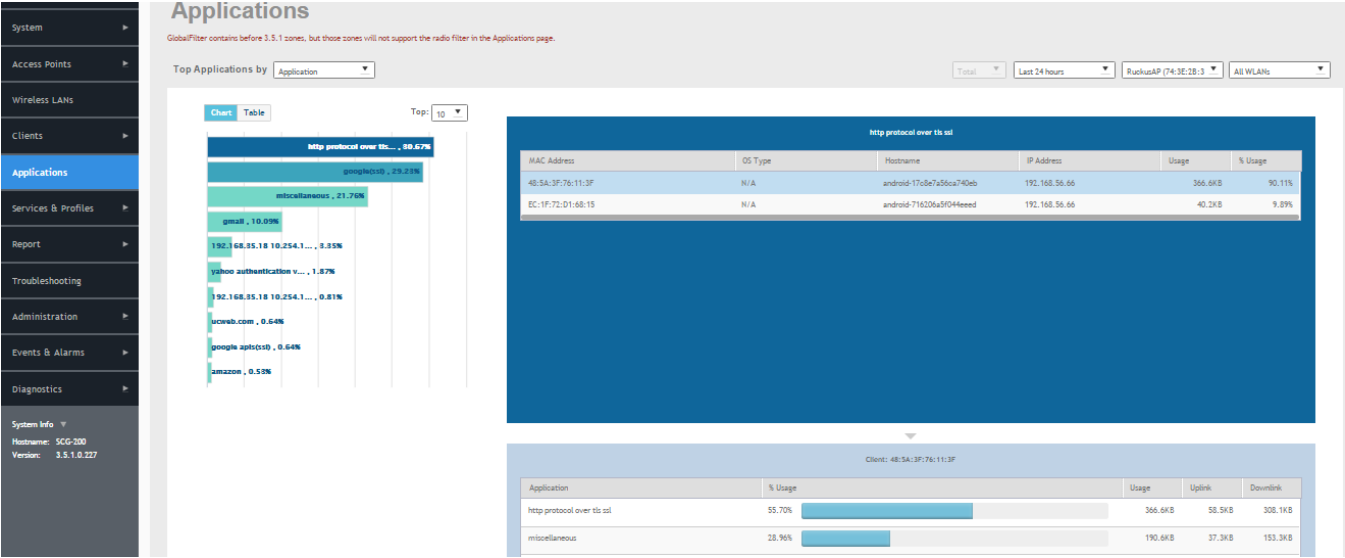
1. Go to **Applications** on the main menu.
2. Select whether to view the **Top Applications** by **Application** or **Port**, select a time period to display, and optionally filter the data by AP MAC address and WLAN name using the drop-down menus.

3. Select whether to display the Top 10 or Top 25 applications in **Chart** or **Table** format.

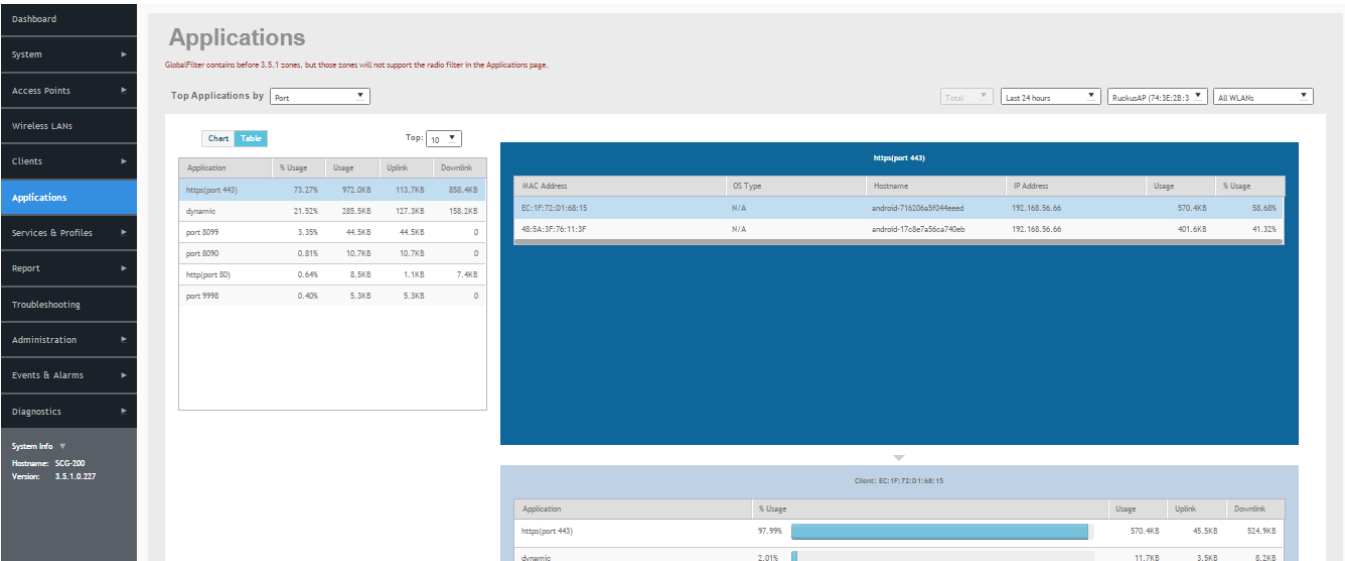
**NOTE**

If Application Recognition and Control is unable to find an application name, it displays the source and destination IP: port address of the application

**FIGURE 102** Top Applications - Chart View

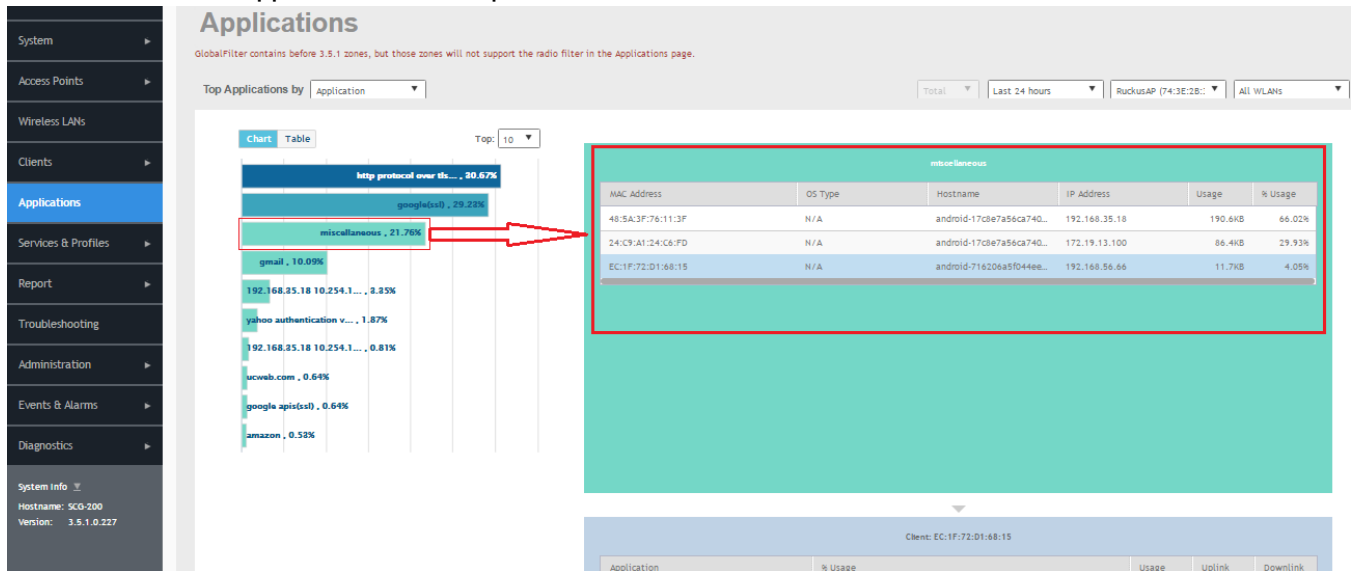


**FIGURE 103** Top Applications by Port - Table View



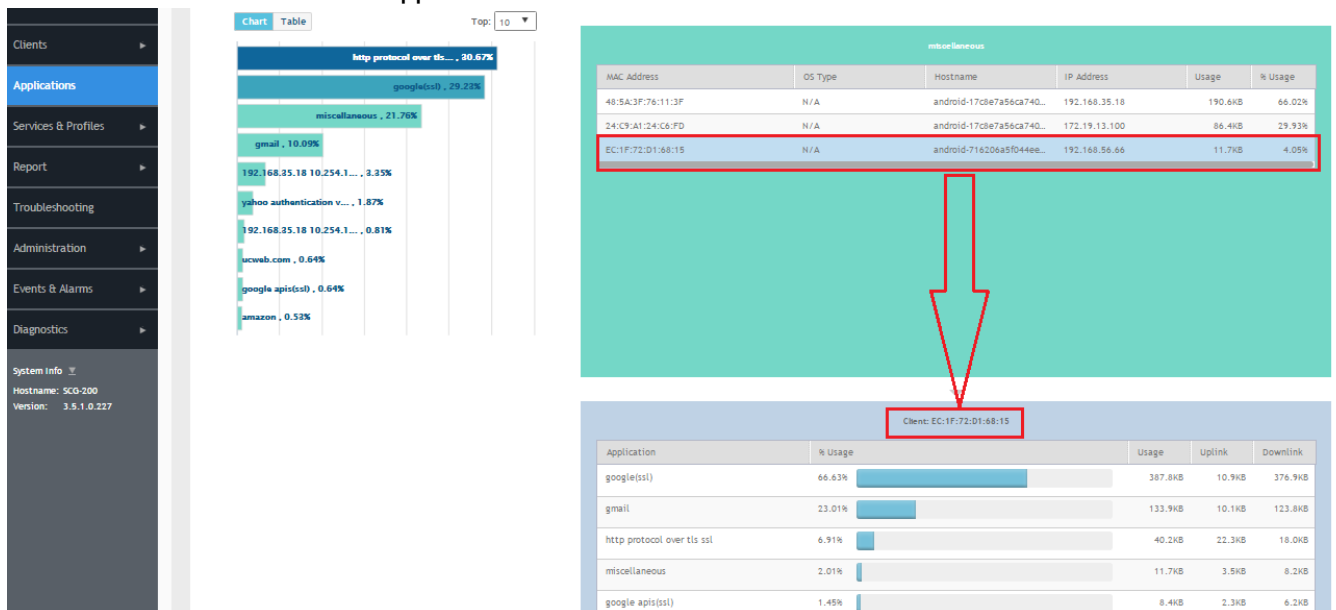
- Click on an application from the list on the left (either Chart or Table view) to view a list of the top clients using the selected application in the list on the right. The client list displays the client's MAC address, OS, hostname, IP address (IPv4 and IPv6), and application usage volume and percent of application traffic generated by the client. From the Total option, you can also filter the data based on the radio frequencies (2.4 GHz and 5 GHz).

**FIGURE 104** Click an application to view top client details



- Click on a client in the list on the right, and scroll down to the client specific details table on the bottom right to view the top 10 applications used by the client.

**FIGURE 105** Click a client to view application details



**NOTE**

You can configure application control policies (denial, rate limiting, and QoS) using the **Services and Profiles > Application Control** page. For more information, see [Configuring Application Controls](#) on page 271.

# Services and Profiles

---

- Working with Hotspots and Portals..... 235
- Configuring Access Control..... 254
- Configuring Application Controls..... 271
- URL Filtering..... 279
- Understanding WiFi Calling..... 286
- Authentication..... 289
- Accounting..... 301
- Classifying Rogue Policy..... 305
- Bonjour..... 306
- Working with Tunnels and Ports..... 312
- DHCP/NAT..... 325
- 3rd Party Service.....340

The Services and Profiles menu provides options for monitoring and configuring services such as guest access, access controls, authentication servers, application recognition and control, Bonjour services, tunneling, location services and DHCP server configuration.

## Working with Hotspots and Portals

### Creating a Guest Access Portal

Using the controller's Guest Access features, you can provide visitors to your organization limited access to a guest WLAN with configurable guest policies. The following sections describe how to configure guest WLANs and access policies that control guest use of your network.

Each guest WLAN must be associated with a Guest Access service portal, which defines the behavior of the guest WLAN interface. Follow these steps to create a guest access service.

1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **Guest Access** tab, and then select the zone for which you want to create the portal.

3. Click **Create**.  
The **Create Guest Access Portal** page appears.

**FIGURE 106** Creating a Guest Access Portal

**Create Guest Access Portal**

**General Options**

\* Portal Name:

Portal Description:

\* Language:

**Redirection**

Start Page: After user is authenticated,

☒ Redirect to the URL that user intends to visit. ☐ Redirect to the following URL:

\*

**Guest Access**

\* Guest Pass SMS Gateway:

Terms and Conditions: ☐ ON

Terms of Use

By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement.  
(\*) The wireless network service is provided by the property owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason.  
(\*) You agree not to use the wireless network for any purpose that is unlawful or otherwise prohibited and you are fully responsible for your use.  
(\*) The wireless network is provided "as is" without warranties of any kind, either expressed or

[?] Web Portal Logo:



4. Configure the following:
  - a. General Options
    - Portal Name: Type a name for the guest access service portal that you are creating.
    - Portal Description: Type a short description of the guest access service portal.
    - Language: Select the display language to use for the buttons on the guest access logon page.
  - b. Redirection: select where to redirect the user after successfully completing authentication.
    - Redirect to the URL that the user intends to visit: Allows the guest user to continue to their destination without redirection.
    - Redirect to the following URL: Redirect the user to a specified web page (entered into the text box) prior to forwarding them to their destination. When guest users land on this page, they are shown the expiration time for their guest pass.  
  
Enter a domain name or IP address to be redirected.
  - c. Guest Access
    - Guest Pass SMS Gateway: You can deliver the guest pass to the user using Short Message Service (SMS). But first you need to configure an SMS server. If you previously configured an SMS server, you can select it here or you can select **Disable**.
    - Terms and Conditions: To require users to read and accept your terms and conditions prior to use, **Show Terms and Conditions** check box. The box below, Terms and Conditions which contains the default Terms of Use text, becomes editable. Edit the text or leave it unchanged to use the default text.
    - Web Portal Logo: By default, the guest hotspot logon page displays the Ruckus logo. To use your own logo, click the **Browse** button, select your logo Web Portal Logo (recommended size is 138 x 40 pixels, maximum file size is 20KB), and then click **Open**.
    - Web Portal Title: Type your own guest hotspot welcome text or accept the default welcome text (Welcome to the Guest Access login page).
  - d. User Session
    - Session Timeout: Specify a time limit after which users will be disconnected and required to log on again.
    - Grace Period: Set the time period during which clients will not need to re-authenticate after getting disconnected from the hotspot. Enter a number (in minutes) between 1 and 14399.
5. Click **OK**.

You have completed creating a guest access service.

#### NOTE

You can also edit, clone and delete a guest access portal by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Guest Access** tab.

## Working with Hotspot (WISPr) Services

A hotspot is a venue or area that provides Internet access to devices with wireless networking capability such as notebooks and smart phones.

Hotspots are commonly available in public venues such as hotels, airports, coffee shops and shopping malls. Configure a traditional (WISPr 1.0) hotspot service to provide public access to users via its WLANs. In addition to the controller and its managed APs, you will need the following to deploy a hotspot:

**Captive Portal:** A special web page, typically a login page, to which users that have associated with your hotspot will be redirected for authentication purposes. Users will need to enter a valid user name and password before they are allowed access to the Internet through the hotspot.

**RADIUS Server:** A Remote Authentication Dial-In User Service (RADIUS) server through which users can authenticate.

For installation and configuration instructions for the captive portal and RADIUS server software, refer to the documentation that was provided with them. After completing the steps below, you will need to edit the WLAN(s) for which you want to enable Hotspot service. The controller supports up to 32 WISPr hotspot service entries, each of which can be assigned to multiple WLANs.

## Creating a Hotspot (WISPr) Portal

To create a hotspot service, you must define the required basic settings.

SZ supports only one grace period, session timeout, UTP, VLAN and all UE session related configuration. These configurations for the first WLAN do not work when the UE joins the second WLAN. The configuration works only when the UE roams within the cluster node. The configurations do not work when the client roams from one zone to another zone or from one cluster to another cluster.

Before creating a hotspot, you need to create a user defined interface.

1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **Hotspot (WISPr)** tab, and then select the zone for which you want to create the portal.
3. Click **Create**.

The **Create Hotspot (WISPr) Portal** page appears.

**FIGURE 107** Creating a Hotspot (WISPr) Portal

### Create Hotspot Portal

The screenshot shows the 'Create Hotspot Portal' configuration page. It features two main sections: 'General Options' and 'Redirection'. The 'Redirection' section is expanded, revealing various settings. 'Smart Client Support' has three radio buttons: 'None' (selected), 'Enable', and 'Only Smart Client Allowed'. 'Logon URL' has two radio buttons: 'Internal' and 'External' (selected). Under 'Redirect unauthenticated user', there are two text input fields for 'Primary' and 'Secondary' URLs. 'Redirected MAC Format' is a dropdown menu showing 'AA:BB:CC:DD:EE:FF'. The 'Start Page' section has a label 'After user is authenticated,' followed by two radio buttons: 'Redirect to the URL that user intends to visit.' (selected) and 'Redirect to the following URL:'. Below this is a text input field. At the bottom, 'HTTPS Redirect' is a toggle switch set to 'ON', with a note: 'The AP will try to redirect HTTPS requests to the hotspot portal'.

4. Under **General Options**, enter portal name and portal description.

5. Under **Redirection**, select where to redirect the user after successful authentication.

a. For **Smart Client Support**, select one of the following options:

- **None**: Disables Smart Client Support on the hotspot service.
- **Enable**: Enables Smart Client Support.
- **Only Smart Client Allowed**: Allows only Smart Clients to connect to the hotspot service.

b. For **Logon URL**, select one of the following options:

- **Internal**: Indicates the internal URL of the subscriber portal (where hotspot users can log in to the service).
- **External**: Indicates the external URL of the subscriber portal.

Selecting **External** provides an option to reroute an unauthorized user to a primary location. You can set the primary location in **Redirect unauthenticated user**. If an unauthorized user is rerouted, the AP redirects the UE to a backup portal.

The AP subscriber portal supports ZD-style API to login and logout. A customer can use AP IP address to submit the login or logout request.

- **Redirect unauthenticated user**: APs can perform WISPr redirection. Native WISPr support is available on SZ-managed APs even if access to SZ is not available. It supports external portal redirection with survivability when APs cannot reach the centralized SZ. It also supports backup portal redirection if primary portal is down. The WISPr authentication load can be distributed to AP or use an AP as a WISPr authentication backup.

WISPr redirection and survivability is supported only on Ruckus 11AC Wave 1 and later APs. Only ZD-style external WISPr is supported. No NBI is supported for backup.

- **Primary**: Redirects an unauthenticated user to a specified URL for authentication.
- **Secondary**: Redirects an unauthenticated user to the backup external portal if the primary URL is down. The AP periodically accesses the primary portal URL to detect and check the availability of the primary URL.

**NOTE**

An AP and the primary portal must be in the same VLAN for the AP to access the primary portal.

- In the **Redirected MAC Format** field, enter the format of the redirection MAC address.
- For **Start Page**, select one of the following options:
  - **Redirect to the URL that the user intends to visit**: Redirects users to the page that they want to visit.
  - **Redirect to the following URL**: Sets a different page where users will be redirected (for example, your company website). Enter a domain name or an IP address to be redirected.
- Enable **HTTPS Redirect** if you want the AP to redirect HTTPS requests to the hotspot portal. HTTPS requests are dropped if this option is disabled.

6. Under **User Session**, set the session timeout and grace period.

- **Session Timeout**: Sets a time limit (in minutes) after which users will be disconnected from the hotspot service and required to log in again.
- **Grace Period**: Sets the time period (in minutes) during which disconnected users are allowed access to the hotspot service without logging in again.

7. Under **Location Information**, set the location ID and location name.
  - a. In **Location ID**, enter the ISO and ITU country and area code that the AP includes in accounting and authentication requests. The code includes the following requirements:
    - isocc (ISO-country-code): The ISO country code that the AP includes in RADIUS authentication and accounting requests.
    - cc (country-code): The ITU country code that the AP includes in RADIUS authentication and accounting requests.
    - ac (area-code): The ITU area code that the AP includes in RADIUS authentication and accounting requests.
    - network: Name of the network.The following example illustrates a proper location ID entry: isocc=us,cc=1,ac=408,network=Ruckus
  - b. For **Location Name**, enter the name of the location of the hotspot service.
8. Under **Walled Garden**, click **Add** to add a user to a walled garden and provide access.
9. Click **Import CSV** to import the CSV file with the user information.
10. Select **Traffic Class Profile** and click + to create a traffic class profile. Refer to **Creating a Traffic Class Profile** section in the Administration guide.
11. Under **Advanced Options**, select the required options:
  - a. Click **Use Token Redirect URL** and enter a signature signing key.
  - b. Click **Enable Internal Node** and enter the internal node.

**NOTE**

If an **Internal node** is enabled, then only one IP is used and the IP domain name and IP ranges are not supported.

12. Click **OK**.

You have completed creating a Hotspot (WISPr) portal.

**NOTE**

If **Traffic Class Profile** or **Use Token Redirect URL** is enabled, **Smart Client Support** is set to **None**.

**NOTE**

You can also edit, clone, and delete a Hotspot (WISPr) portal by selecting the **Configure**, **Clone**, and **Delete** options respectively from the **Hotspot (WISPr)** tab.

## Creating a Web Authentication Portal

Web authentication (also known as a “captive portal”) redirects users to a logon web page the first time they connect to this WLAN, and requires them to log on before granting access to use the WLAN.

1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **Web Auth** tab, and then select the zone for which you want to create the portal.

3. Click **Create**.

The **Create Web Authentication Portal** page appears.

**FIGURE 108** Creating a Web Authentication Portal

## Create Web Authentication Portal

General Options

\* Portal Name:

Portal Description:

\* Language:

English

Redirection

Start Page: After user is authenticated,

☒ Redirect to the URL that user intends to visit. ☐ Redirect to the following URL:

\*

User Session

\* Session Timeout:

1440

Minutes (2-14400)

\* Grace Period:

60

Minutes (1-14399)

OK

Cancel

4. Configure the following:
  - a. General Options
    - Portal Name: Type a name for the hotspot service portal that you are creating.
    - Portal Description: Type a short description of the hotspot service portal.
    - Language: Select the display language that you want to use on the web authentication portal.
  - b. Redirection: select where to redirect the user after successfully completing authentication.
    - Start Page: select one of the following
      - Redirect to the URL that the user intends to visit: Allows the guest user to continue to their destination without redirection.
      - Redirect to the following URL: Redirect the user to a specified web page (entered into the text box) prior to forwarding them to their destination. When guest users land on this page, they are shown the expiration time for their guest pass.  
  
Enter a domain name or IP address to be redirected.
  - c. User Session
    - Session Timeout: Set a time limit (in minutes) after which users will be disconnected from the hotspot service and will be required to log on again.
    - Grace Period: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot service without having to log on again.
5. Click **OK**.

You have completed creating a Web Auth service portal.

**NOTE**

You can also edit, clone and delete a Web Auth service portal by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Web Auth** tab.

## Creating a WeChat Portal

WeChat is a mobile app from Tenecent that enables its users to call and send text messages to one another. If you have WeChat users on the network and you want your WLANs to support WeChat services, you can create a WeChat portal that WeChat users can use.

A WeChat portal defines the third party authentication server, also known as the equipment service provider (ESP) server, to which the controller will forward all WeChat authentication requests from wireless devices that are associated with controller-managed APs. In turn, the third party authentication server will forward these authentication requests to the WeChat server.

1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **WeChat** tab, and then select the zone for which you want to create the portal.

3. Click **Create**.  
The **Create WeChat Portal** page appears.

**FIGURE 109** Creating a WeChat Portal

Create WeChat Portal

General Options

Portal Settings

Whitelist

DNAT Port Mapping

OK

Cancel

4. Configure the following:
  - a. General Options
    - Name: Type a name for the portal that you are creating.
    - Description: Type a short description of the portal.
  - b. Portal Settings: configure the following
    - Authentication URL: Type the authentication interface URL on the third party authentication server. When a managed AP receives a WeChat logon request from a client device, it will send the request to this authentication URL and get the authorization result.
    - DNAT Destination: Type the DNAT destination server address to which the controller will forward HTTP requests from unauthenticated client devices. The DNAT destination server and the authentication server (above) may or may not be the same server.
    - Grace Period: Type the number of minutes during which disconnected users who were recently connected will be allowed to reconnect to the portal without needing to re-authenticate. The default grace period is 60 minutes (range is between 1 and 14399 minutes).
    - Blacklist: Type network destinations that the controller will automatically block associated wireless clients from accessing. Use a comma to separate multiple entries.
  - c. Whitelist: Type network destinations that the controller will automatically allow associated wireless clients to access. You can add a single entry or multiple entries.

To add a single entry, type the entry in **Wall Garden Entry**, and then click **Add**. The entry you added appears in the table below. To add multiple entries, in a comma-separated value (CSV) file, type all the network destinations that you want to add to the whitelist, and then save the CSV file. In the Whitelist section, click **Import CSV**, and then select the CSV file you created. Click **Open**. The entries in the CSV file are added to the whitelist.
  - d. DNAT Port Mapping: specify at least one pair of source-to-destination port mapping. To add a port mapping, type the source and destination ports in the boxes provided, and then click **Add**. The AP will use this information to drop or forward HTTP requests from associated clients to specified ports on the DNAT server. For example, if an HTTP request from a wireless client does not originate from the specified source (from) port, the AP will discard the HTTP request. By default, a port mapping of 80-80 (source-destination) exists.
5. Click **OK**.

You have completed creating a WeChat portal.

**NOTE**

You can also edit, clone and delete a WeChat service portal by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **WeChat** tab.

## Working with Hotspot 2.0 Services

You must be aware of Hotspot 2.0 - a Wi-Fi Alliance specification that allows for automated roaming between service provider access points when both the client and access gateway support the newer protocol.

Hotspot 2.0 (also known as Passpoint™, the trademark name of the Wi-Fi Alliance certification) aims to improve the experience of mobile users when selecting and joining a Wi-Fi hotspot by providing information to the station prior to association.

This information can then be used by the client to automatically select an appropriate network based on the services provided and the conditions under which the user can access them. In this way, rather than being presented with a list of largely meaningless SSIDs to choose from, the Hotspot 2.0 client can automatically select and authenticate to an SSID based on the client's configuration and services offered, or allow the user to manually select an SSID for which the user has login credentials.



The controller's Hotspot 2.0 implementation complies with the IEEE 802.11u standard and the Wi-Fi Alliance Hotspot 2.0 Technical Specification.

See the *Hotspot 2.0 Reference Guide for SmartZone* for information on configuring Hotspot 2.0 services, including:

- Working with Hotspot 2.0 operator profiles
- Working with Hotspot 2.0 identity providers
- Creating a Hotspot 2.0 online signup portal

## Creating a Hotspot 2.0 WLAN Profile

You can assign a Hotspot 2.0 service to a Hotspot 2.0 WLAN, for which you must create a Hotspot 2.0 WLAN profile.

Follow these steps to create a Hotspot 2.0 WLAN profile.

1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **Hotspot 2.0** tab, and then select the zone for which you want to create the profile.
3. Click **Create**.

The **Create Hotspot 2.0 WLAN Profile** page appears.

**FIGURE 110** Creating a Hotspot 2.0 WLAN Profile

### Create Hotspot 2.0 WLAN Profile

\* Name:

Description:

\* Operator:

\* Identity Providers: \* Identity Provider

Identity Provider	Online Signup Service	Default
<input type="text"/>		

You can configure Onboarding SSID when you add an identity provider which enable Online Signup & Provisioning

Advanced Options

4. Configure the following:

- a. Name: Enter a name for this WLAN profile. This name identifies the WLAN profile when assigning an HS2.0 service to a HS2.0 WLAN.
- b. Description: Enter a description for the WLAN profile.
- c. Operator: Select the operator profile. This name identifies the service operator when assigning an HS2.0 service to a HS2.0 WLAN.

You can also click **Create** to create a Hotspot 2.0 WiFi operator. See [Creating a Hotspot 2.0 WiFi Operator Profile](#) on page 246 for more information.

- d. Identity Provider: Choose one or more identity providers. Choose the identity provider. You can configure an OSU SSID when you add an Identity Provider which enables OSU and provisioning. Since there may be more than one identity provider per Hotspot 2.0 profiles having its own authentication profile, the No Match and Unspecified mapping could be duplicated. To avoid duplication, the default identity provider is taken as the correct configuration for No Match and Unspecified mapping. OSUSSID can be OSEN or OPEN [Guest].

You can also click **Create** to create a Hotspot 2.0 WiFi operator. See [Creating a Hotspot 2.0 Identity Provider](#) on page 247 for more information.

e. Advanced Options:

- Internet Options: Specify if this HS2.0 network provides connectivity to the Internet.
- Access Network Type: Access network type (private, free public, chargeable public, etc.), as defined in IEEE802.11u.
- IPv4 Address: Select IPv4 address type availability information, as defined in IEEE802.11u
- IPv6 Address: Select IPv6 address type availability information, as defined in IEEE802.11u
- Connection Capabilities: Provides information on the connection status within the hotspot of the most commonly used communications protocols and ports.

Provide the **Protocol Name**, **Protocol Number**, **Port Number** and **Status** to **Add** a new connection.

- Custom Connection Capabilities: Allows addition of custom connection capability rules. Up to 21 custom rules can be created.

Provide the **Protocol Name**, **Protocol Number**, **Port Number** and **Status** to **Add** a new connection.

5. Click **OK**.

You have completed creating a Hotspot 2.0 WLAN profile.

**NOTE**

You can also edit, clone and delete a Hotspot 2.0 WLAN profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **WLAN Profile** section in the **Hotspot 2.0** tab.

### Creating a Hotspot 2.0 WiFi Operator Profile

An operator profile defines all the properties pertaining to an operator while a service profile defines the properties related to a service provider. If a WLAN is configured to provide Hotspot 2.0 service, it must be linked exactly like a Hotspot 2.0 operator profile.

1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **Hotspot 2.0** tab, and then select the device for which you want to create the profile.

3. Click **Create**.

The **Creating Hotspot 2.0 WiFi Operator Profile** page appears.

**FIGURE 111** Creating a hotspot 2.0 WiFi operator profile

## Create Hotspot 2.0 Wi-Fi Operator Profile

The screenshot shows a web form titled "Create Hotspot 2.0 Wi-Fi Operator Profile". The form contains several sections:

- Name:** A single-line text input field.
- Description:** A single-line text input field.
- Domain Names:** A section with a table for managing domain names. The table has columns for "Domain Name", "Add", "Cancel", and "Delete". Below the table is a "Domain Name" label and a text input field.
- Signup Security:** A checkbox labeled "Support Anonymous Authentication (OSEN)".
- Certificate:** A dropdown menu showing "No data available" and a "Create" button.
- Friendly Names:** A section with a table for managing friendly names. The table has columns for "Language", "Name", "Add", "Cancel", and "Delete". Below the table is a "Language" label and a text input field.

At the bottom of the form are two large buttons: "Create" and "Cancel".

4. Configure the following:
  - a. **Name:** Enter a name for this Wi-Fi operator profile.
  - b. **Description:** Enter a description for the venue profile.
  - c. **Domain Names:** HS2.0 operator's domain name is a mandatory field, which specifies the operator's domain name. Hotspot 2.0 AP broadcasts the domain name to indicate the home Wi-Fi providers.
  - d. **Signup Security:** This is an optional field and is disabled by default. Enabling would mean that operator supports secure onboarding (OSEN).
  - e. **Certificate:** Select the certificate for the operator - AAA. This can be the same certificate as the one used with OSU service.
  - f. **Friendly Names:** HS2.0 operator's friendly name is a mandatory field. Operator's friendly name is displayed on mobile client's screen. It is also used for operator verification during secure onboarding (OSEN). Select the display language from the drop down list.
5. Click **OK**.

### Creating a Hotspot 2.0 Identity Provider

The Hotspot 2.0 Identity provider provides authentication, accounting and online sign-up service. There can be one or more identity providers per Hotspot 2.0 access WLAN.

To configure the HS 2.0 identity provider, you must configure the following:

#### Network Identifier

Follow these steps to create a Hotspot 2.0 Identity Provider - Network Identifier.

1. Configure the following:
  - a. Name: Enter a name or this network identifier profile.
  - b. Description: Enter a description for the network identifier profile.
  - c. PLMNs: Each record contains MCC and MNC.

MCC: Set the correct country code for the geographical location. This is required when the controller sends MAP authentication information. Type the mobile country code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.

MNC: Set the mobile network code based on the geographical location. This is required when controller sends MAP authentication information. Type the mobile network code digits. Decimal digit strings with maximum length of 3 and minimum length of 2.
  - d. Realms: List of NAI realms corresponding to service providers or other entities whose networks or services are accessible via this AP. Up to 16 NAI realm entries can be created. Each NAI realm entry can contain up to four EAP methods. You can add a realm by providing the realm **Name, Encoding technique** (choose between RFC-4282 and UTF-8) and **EAP Methods**.
  - e. Home OIs: Organization Identifier (OI) is a unique value assigned to the organization. User can configure a maximum of 12 OI values and can adjust the order since the AP takes only 3 OIs in the beacon.
2. Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Network Identifier.

### Online Signup and Provisioning

Follow these steps to create a Hotspot 2.0 Identity Provider - Online Signup and Provisioning.

1. Configure the following:
  - a. Provisioning Options
    - Provisioning Service: The provisioning service is responsible for any subscription provisioning process in which messages are communicated between the UE and the SZ resulting in a PPS-MO provisioned into the UE. The provisioning supports both SOAP-XML and OMA-DM as communication protocols for the process based on the initial request coming from the UE. The provisioning service supports sign-up; remediation and policy update flows where the UE is provisioned with a full PPS -MO or only with internal node/s of the PPS-MO. Administrator can only set External Internal Provisioning Services. , where the administrator is required to fill the external OSU server URL.
    - Provisioning Protocol: Select communication protocols OMA-DM or SOAP-XML.
  - b. Online Signup Options
    - OSU NAI Realm: This configuration is only for External Provision Service. In case of Internal Provisioning Service, the NAI realm should be configured per authentication service, which is available during on-boarding.
    - Common Language Icon: This is the default icon presented in the device for this identity provider in case the device does not find any match for other icons per language in the table.
    - OSU Service Description: This table configures the friendly name, description and icon per language. This information is presented on the device when it receives ANQP message which includes OSU providers. Friendly names, which are required to be part of the OSU certificate is automatically populated in this table. In case description is also included in the OSU certificate it is automatically populated into the table. Administrators are required to set the matched icon per language as included in the OSU certificate.
    - Whitelisted Domain: Add the domain names of the External Portal domain.
2. Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Online Signup and Provisioning.

### **Authentication**

Follow these steps to create a Hotspot 2.0 Identity Provider - Authentication.

1. Configure the following:
  - a. Realm: configure the realm mapping to the authentication service.
  - b. Auth Service: map the realm to an external RADIUS server which should be pre-configured.
  - c. Dynamic VLAN ID: type the VLAN ID.
2. Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Authentication.

### **Accounting**

Follow these steps to create a Hotspot 2.0 Identity Provider - Accounting.

1. Configure the following:
  - a. Realm: if the authentication's realm is set as remote credential type, administrator should set this realm here to the customer's external accounting server.
  - b. Accounting Service: select the accounting service.
2. Click **Next**.

You have completed creating a Hotspot 2.0 Identity Provider - Accounting.

### **Review**

Review the configuration on the page before committing the changes to the server. Click **Create** to create the Hotspot 2.0 Identity Provider.

## **Creating a Hotspot 2.0 Venue Profile**

The Hotspot 2.0 technology allows users to seamlessly roam between the provider's home Wi-Fi network and the visited Wi-Fi network in a different location. A Wi-Fi provider can partner with several roaming partners to provide Wi-Fi access to partner's subscribers. Public venues such as institutions, restaurants, and stadiums are considered roaming partners.

1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **Hotspot 2.0** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

The **Create Hotspot 2.0 Venue Profile** page appears.

**FIGURE 112** Creating a Hotspot 2.0 Venue Profile

## Create Hotspot 2.0 Venue Profile

The screenshot shows the 'Create Hotspot 2.0 Venue Profile' form. It has the following elements:

- Name:** A text input field.
- Description:** A text input field.
- Venue:** A dropdown menu.
- Venue Names:** A table with two columns: **Language** and **Name**. The first row shows 'English' in the Language column. To the right of the table are buttons: **+ Add**, **x Cancel**, and **trash Delete**.
- Venue Category:** A dropdown menu with 'Group' selected and 'Unspecified' as the value.
- Type:** A dropdown menu with 'Unspecified' as the value.
- Buttons:** **OK** and **Cancel** buttons at the bottom right.

4. Configure the following:

- Name:** Enter a name for this venue profile. This name identifies the venue profile when assigning an HS2.0 service to a HS2.0 venue.
- Description:** Enter a description for the venue profile.
- Venue:**
  - Venue Names:** Create a new venue name. Select the language and enter the venue name in that language.
  - Venue Category:** Select venue group and venue type as defined in IEEE802.11u, Table 7.25m/n.
  - WAN Metrics:** Provides information about the WAN link connecting an IEEE 802.11 access network and the Internet; includes uplink/downlink speed estimatesSelect the operator profile. This name identifies the service operator when assigning an HS2.0 service to a HS2.0 WLAN.

5. Click **OK**.

You have completed creating a Hotspot 2.0 WLAN profile.

**NOTE**

You can also edit, clone and delete a Hotspot 2.0 venue profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Venue Profile** section in the **Hotspot 2.0** tab.

## Creating a UA Blacklist Profile

The controller automatically blocks certain user agents (or software used by a user) from accessing hotspots provided by controller-managed APs. When the controller blocks any of these user agents, an error message appears on the user device. You can add to or remove user agents from this blacklist.

Following are some of the blocked user agents:

- ZoneAlarm

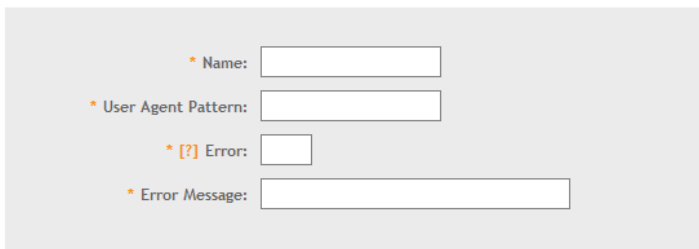
- VCSOAPClient
- XTier NetIdentity
- DivX Player
- Symantec LiveUpdate
- Windows Live Messenger
- StubInstaller
- windows-update-agent
- Windows Live Essentials
- Microsoft Dr. Watson for Windows (MSDW)
- Avast Antivirus Syncer
- Microsoft Background Intelligent Transfer Service (BITS)
- Google Update
- TrendMicro client
- Skype WISPr

1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **UA Blacklist** tab, and then select the zone for which you want to create the portal.
3. Click **Create**.

The **Creating a UA Blacklist Profile** page appears.

**FIGURE 113** Creating a UA Blacklist Profile

## Create UA Blacklist Profile



OK

Cancel

4. Configure the following:
  - a. Name: Type a name of the user agent.
  - b. User Agent Pattern: Type the agent pattern.
  - c. Error: Specify the error message number.
  - d. Error Message: Specify the error message.
5. Click **Create**.

You have completed creating a UA Blacklist Profile

NOTE

You can also edit, clone and delete a UA blacklist profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **UA Blacklist** tab.

Creating a Portal Detection and Suppression Profile

To restrict an unauthorized user in a walled garden, a service operator must set defined policy rules by creating a portal detection and suppression profile.

- 1. Select **Services & Profiles > Hotspots & Portals**.
- 2. Click the **Portal Detection and Suppression** tab.
- 3. Select a zone and click **Create** to add a portal detection and suppression profile.

The **Create a Portal Detection Profile** page is displayed.

FIGURE 114 Creating Portal Detection Profile

Create Portal Detection Profile

General Options

Name:

Description:

Portal Detection Patterns

+ Create

Configure

Clone

Delete

Name	User Agent Pattern	HTTP Code	HTTP Response Body

OK

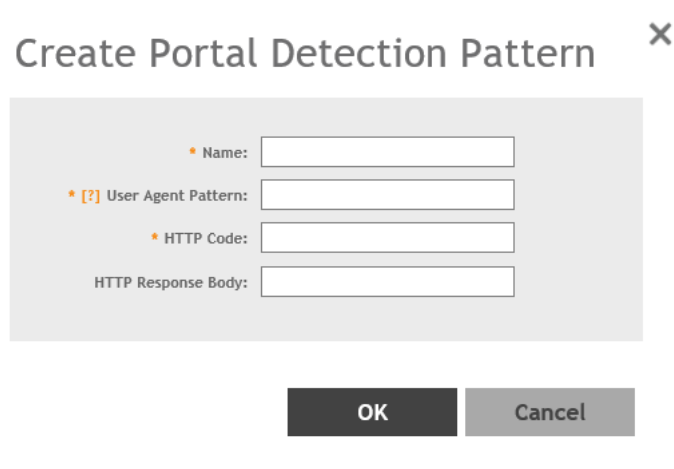
Cancel

- 4. Under **General Options**, enter a policy list name and description.



- Under **Portal Detection Patterns**, click **Create** to create a portal detection pattern.  
The **Create a Portal Detection Pattern** page is displayed.

**FIGURE 115** Creating Portal Detection Pattern



The screenshot shows a modal dialog titled "Create Portal Detection Pattern" with a close button (X) in the top right corner. The dialog contains four input fields, each with a label and a required field indicator (an asterisk):

- Name:** A text input field.
- \* [?] User Agent Pattern:** A text input field.
- \* HTTP Code:** A text input field.
- HTTP Response Body:** A text input field.

At the bottom of the dialog, there are two buttons: **OK** and **Cancel**.

- In the **Name** field, enter the name of the portal detection pattern.
- In the **User Agent Pattern** field, enter the user agent pattern.

**NOTE**

The user agent pattern must follow a regular expression format, starting and ending with .\* (for example, .\*Android-WiFi.\*). The default Captive Portal Detection may not support all the Android devices and the new Microsoft phone if different user agent patterns are used. In this case, new rules must be created to cover such patterns. Using an improper user agent pattern may impact browser behaviors.

- In the **HTTP Code** field, enter the code.

**NOTE**

The HTTP code range must be from 100 through 599.

- In the **HTTP Response Body** field, enter the HTML string.
- Click **OK**.

**NOTE**

To select a **Portal Detection Pattern** profile, **Bypass CNA** must be enabled in the WLAN configuration page. Use **Bypass CNA** to enable or disable Portal Detection Service for HotSpot, Web Authentication, and Guest Access WLAN.

# Configuring Access Control

SmartZone's Access Control features provide a wide range of options to control access and utilization of the wireless network.

## Creating a User Traffic Profile

A User Traffic Profile (UTP) can be created to block or limit user traffic based on a number of factors, including Source IP address, Port, Destination IP address, Protocol, etc. Additionally, a UTP can be created to shape traffic according to a configurable Application Control Policy.

Once the UTP is created, it can be applied to any WLAN from the **Wireless LANs** page.

1. Select **Services & Profiles > Access Control**.
2. Select the **User Traffic** tab.
3. Click **Create**. The **Create User Traffic Profile** page appears.

**FIGURE 116** Creating User Traffic Profile

**Create User Traffic Profile**

Name:

Description:

Rate Limiting: Uplink ☐ OFF  Mbps (0.1~200)

Downlink ☐ OFF  Mbps (0.1~200)

Traffic Access Control List

Application Recognition and Control

Application Policy:

Application Policy (Earlier Firmware Versions):

URL Filtering Control

OK Cancel

4. In the **Name** field, enter a UTP name.
5. In the **Description** field, enter a short description for the UTP.
6. In the **Rate Limiting** field, select the required option to specify and apply rate limit values for the UTP to control the data rate.
  - Uplink
  - Downlink
7. Under **Traffic Access Control List**, complete the following steps:
  - a. Under **Default Access**, select **Allow** or **Block** if no rule is matched.
  - b. Click **Create** to create and configure traffic control rules. Refer to [Creating a User Traffic Access Control Rule](#) on page 255 for more information.

8. Under **Application Recognition and Control**, select an **Application Policy** from the list or click **Create** to create a new policy. Refer to [Configuring Application Controls](#) on page 271 for more information.
9. Click **OK** to save the UTP.

You have completed creating a UTP. You can now assign this UTP to a WLAN from the **Wireless LANs** page.

#### NOTE

You can also edit, clone, and delete a UTP by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **User Traffic** tab.

## Creating a User Traffic Access Control Rule

User Traffic Profiles consist of multiple traffic control rules, which can be enforced in any order you prefer (click up or down arrows to rearrange rules).

To create a user traffic control rule:

1. Click **Create**. The **Create User Traffic Access Control Rule** page appears.

**FIGURE 117** Creating a User Traffic Access Control Rule

✕

### Create User Traffic Access Control Rule

Description:

\* Access: Allow

\* Type: ☒ IPv4 ☐ IPv6

Source IP: UN ☐ Subnet ☐ Network Address:  Subnet Mask:

Source Port: UN ☐ Range  -

Destination IP: UN ☐ Subnet ☐ Network Address:  Subnet Mask:

Destination Port: UN ☐ Range  -

Protocol: No data available

Direction: Only upstream rules supported

OK
Cancel

2. Configure the following:
  - **Description:** Type a short description for the user traffic rule.
  - **Access:** Select Allow or Block depending on whether you want to set this rule as the default rule.
  - **Type:** Choose the IP version, IPv4 or IPv6.
  - **Source IP:** Enable the option and specify the source **Subnet Network Address** and **Subnet Mask** for IPv4 option type or enter **IPv6 Network** address for IPv6 option type.
  - **Source Port:** Enable the option and specify the source port to which this rule will apply. To apply this rule to a port range, type the starting and ending port numbers in the two boxes.
  - **Destination IP:** Enable the option and specify the destination **Subnet Network Address** and **Subnet Mask** for IPv4 option type or enter **IPv6 Network** address for IPv6 option type.
  - **Destination Port:** Enable the option and specify the source port to which this rule will apply. To apply this rule to a port range, type the starting and ending port numbers in the two boxes.
  - **Protocol:** Select the network protocol to which this rule will apply. Supported protocols include TCP, UDP, UDPLITE, ICMP (ICMPv4), ICMPv6, IGMP, ESP, AH, SCTP.
3. Click **OK** to save your changes.

## Creating an Application Control Policy

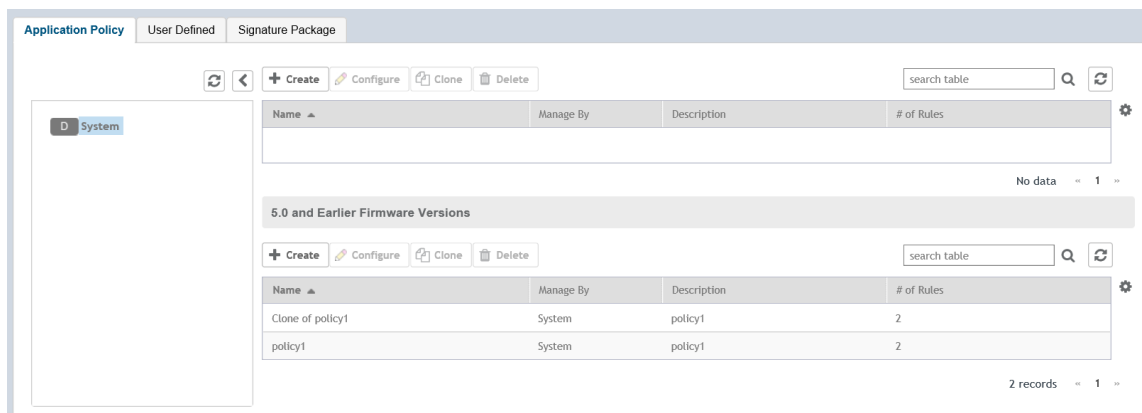
You must create an application policy to limit traffic by application, to classify traffic into priority queues using QoS traffic shaping rules, or to completely block access to an application.

Complete the following steps to create an application control policy:

1. Select **Services & Profiles > Application Control**.
2. Click the **Application Policy** tab.

The **Application Policy** page appears.

**FIGURE 118** Viewing Application Policy



3. Click **Create**.

The **Create Application Policy** page appears.

**FIGURE 119** Creating an Application Policy

## Create Application Policy

Note: Please ensure that configuration is consistent with URL filtering policy. The URL filtering policy will take precedence.

General Options ▼

Name:

Description:

Rules ▼

+ Create

Configure

Delete

#	Rule Type ▲	Content
<div></div>		

Logging ▼

[?] Send App Logs to SZ:

☐ Allow the AP to log every application event and end the events to SmartZone

[?] Enable Remote Syslog:

☐ Allow the AP to log every application event and end the events to external syslog

OK

Cancel

4. Under **General Options**, enter a policy name and policy description.

- Under **Rules**, click **Create** to create a new rule.

**NOTE**

Each application policy can contain up to 128 rules.

The **Create Application Policy Rule** page appears.

**FIGURE 120** Creating an Application Policy Rule

Create Application Policy Rule

\* Rule Type: Denial Rules

\* Application Type: System Defined

\* Application: Antivirus

All

Reload...

All

Lookout Mobile Security

Sophos update

ZoneAlarm

ZoneAlarm Updates

App Logs to SZ: OFF Allow the AP to log every application event and

- In the **Rule Type** field, select one of the following options:
  - Denial Rules**
  - QoS**
  - Rate Limiting**
- In the **Application Type** field, select the type of application.
- In the **Application** field, select the application for which you want to create a policy rule.

For example, if you select **All** in the application category and save the application rule, the application rule list reflects all Antivirus applications and is selected as a single entry in the rule list. A full category is counted as one rule in the allotment of 128 Layer 7 rules in a Layer 7 policy.

- Click **OK** to save the rule.

If a rule is already created, you can edit its configuration settings by selecting the rule and clicking **Configure** on the **Create Application Policy** page.

- Under **Logging**, select the appropriate option for the APs to log events:
  - Allow the AP to log every application event and end the events to SmartZone**
  - Allow the AP to log every application event and end the events to external syslog**
- Click **OK** to save the application control policy.

You have created an application control policy.

You can continue to apply the application control policy to user traffic, as described in [Implementing an Application Control Policy](#) on page 274.

## Creating OS Policy Service

You can control how devices installed with certain OS configurations can be connected to the network, and also control what they can be allowed to do within the network. Using the OS policy service, the system can identify the type of client attempting to connect, and perform control actions such as allow/block, rate limiting, and VLAN tagging based on the OS rule.

1. Go to **Services & Profiles > Access Control**.
2. Select the **OS Policy** tab, and then select the zone for which you want to create the policy.
3. Click **Create**.

The **Create OS Policy Service** page appears.

**FIGURE 121** Creating an OS Policy Service

### Create OS Policy Service

**General Options**

\* Name:

Description:

\* Default Access: Default access if no rule is matched: ☒ Allow ☐ Block

**Rules**

+ Create Configure Clone Delete

Description	Device Type	Access	Uplink Rate Limit	Downlink Rate Limit	VLAN

OK Cancel

4. Configure the following:
  - a. Name: Type a name for the OS policy.
  - b. Description: Type a short description for this OS policy.
  - c. Default Access: select either Allow or Block. This is the default action that the system will take if no rules are matched.
  - d. Rules: Define the OS Policy rules. For more information see, [Creating OS Policy Rules](#) on page 260
  - e. Click **OK**.

You have created the OS policy service.

#### NOTE

You can also edit, clone and delete a service by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **OS Policy** tab.

## Creating OS Policy Rules

You can create rules for every OS policy service that you create.

1. Click **Create**. The **Create OS Policy Rule** page appears.

**FIGURE 122** Create OS Policy Rule

### Create OS Policy Rule

\* Description:

\* Action:

\* Device Type:

Rate Limiting: **Uplink** ☐ Enable  Mbps (0.1~200)

**Downlink** ☐ Enable  Mbps (0.1~200)

VLAN:

**OK** **Cancel**

2. Configure the following:
  - Description: Type a short description for the rule.
  - Access: Select Allow or Block. This is the action that the system will take if the client matches any of the attributes in the rule.
  - Device Type: Select from any of the supported OS types.
  - Rate Limiting: Specify and apply rate limit values for the device.  
Select the **Enable** check-box to set the *Uplink* and *Downlink* rate limit values.
  - VLAN: Segment this client type into a specified VLAN (1~4094; if no value is entered, this policy does not impact device VLAN assignment).
  - Click **OK**.

You have created the OS policy rule.

## VLAN Pooling

When Wi-Fi is deployed in a high density environment such as a stadium or a university campus, the number of IP addresses required for client devices can easily run into the thousands. Placing thousands of clients into a single large subnet or VLAN can result in degraded performance due to factors like broadcast and multicast traffic. VLAN pooling is adopted to address this problem.



VLAN pooling allows administrators to deploy a pool of multiple VLANs to which clients are assigned, thereby automatically segmenting large groups of clients into multiple smaller subgroups, even when connected to the same SSID. As the client device joins the WLAN, the VLAN is assigned to one of the VLANs in the pool based on a hash of the client's MAC address. To use the VLAN pooling feature, you first need to create a VLAN pooling profile, and then you can assign the profile to a specific WLAN or override the VLAN settings of a WLAN group.

**NOTE**

AP model: 11ac wave 2 supports a maximum of 64 VLANs. Other AP models support up to 32 VLANs.

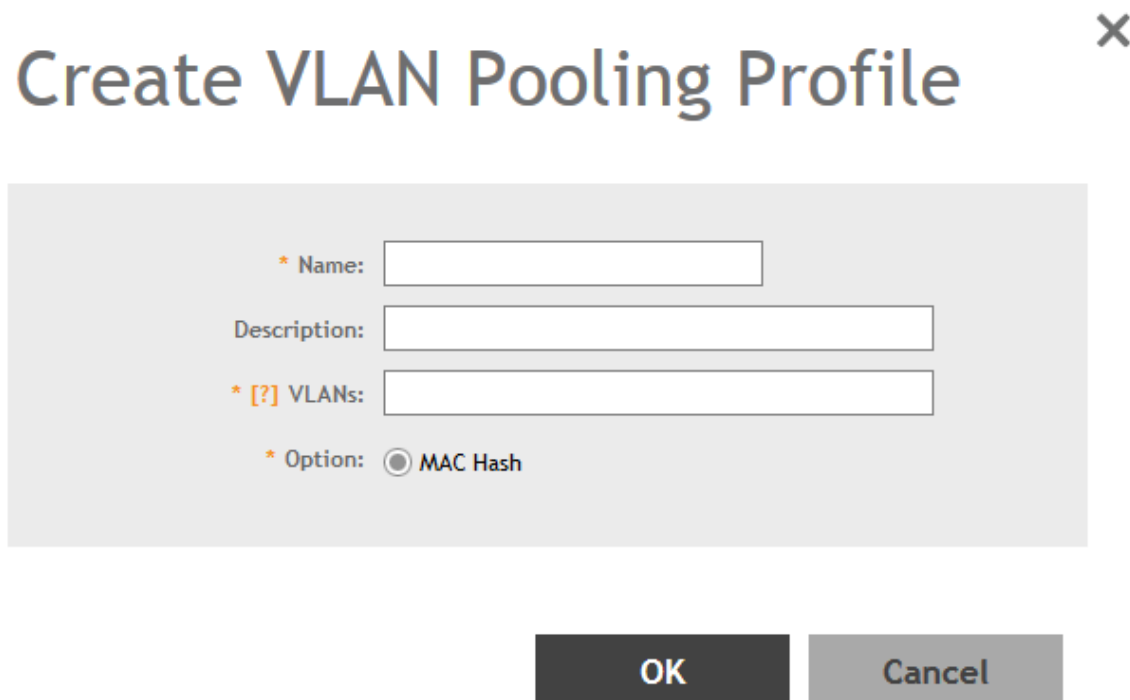
### ***Creating a VLAN Pooling Profile***

Each VLAN pool can contain up to 16 VLANs, and a maximum of 64 VLAN pools can be created. Each WLAN can be configured with a single VLAN pool.

1. Go to **Services & Profiles > Access Control**.
2. Select the **VLAN Pooling** tab, and then select the zone for which you want to create the profile.
3. Click **Create**.

The **Create VLAN Pooling** page appears.

**FIGURE 123** Creating a VLAN Pooling Profile



×

## Create VLAN Pooling Profile

\* Name:

Description:

\* [?] VLANs:

\* Option: ☒ MAC Hash

OK
Cancel

4. Configure the following:
  - a. Name: Type a name for the VLAN profile.
  - b. Description: Type a short description for this profile.
  - c. VLANS: Type the VLAN IDs to be assigned to this pool. VLAN IDs can be separated by hyphens, commas, or a combination (for example, 7-10, 13, 17, 20-28).
  - d. Click **OK**.

You have created the VLAN Pooling profile.

**NOTE**

You can also edit, clone and delete a profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **VLAN Pooling** tab.

## Create Precedence Profile

Clients are assigned to VLANs by various methods, and there is an order of precedence by which VLANs are assigned. The assignment is commonly done from lowest to highest precedence. You can also set precedence for Rate limiting attribute of the profile.

**NOTE**

Each WLAN has a default precedence.

1. Go to **Services & Profiles > Access Control**.
2. Select the **Precedence** tab, and then select the zone for which you want to create the policy.

3. Click **Create**.

The **Create Precedence Profile** page appears.

**FIGURE 124** Creating a Create Precedence Profile

## Create Precedence Profile

\* Name:

VLAN Precedence ▼

Priority	Description
1	AAA
2	DEVICE
3	WLAN

4. Configure the following:
  - a. Name: Type the name of the profile.
  - b. VLAN Precedence: Use the Up and Down options to set the VLAN priority.
  - c. Rate Limiting Precedence: Use the Up and Down options to set the Rate Limit priority.

**NOTE**

When SSID Rate Limiting (restricts total usage on WLAN) is enabled, per-user rate limiting is disabled.

- d. Click **OK**.

You have created the Precedence profile.

**NOTE**

You can also edit, clone and delete a profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Precedence** tab.

## Creating an L2 Access Control Service

Another method to control access to the network is by defining Layer 2/MAC address access control lists (ACLs), which can then be applied to one or more WLANs or WLAN groups. L2 ACLs are either allow-only or deny-only; that is, an ACL can be set up to allow only specified clients or to deny only specified clients. MAC addresses that are in the deny list are blocked at the AP.

1. Go to **Services & Profiles > Access Control**.
2. Select the **L2 Access Control** tab, and then select the zone for which you want to create the access control service.
3. Click **Create**.

The **Create L2 Access Control Service** page appears.

**FIGURE 125** Creating an L2 Access Control Service

### Create L2 Access Control Service

**General Options**

\* Name:

Description:

\* Restriction: ☒ Allow only the stations listed below ☐ Block only the stations listed below

**Rules**

\* MAC Address

MAC Address

4. Configure the following:
  - a. General Options:
    - Name: Type a name for this policy.
    - Description: Type a short description for this policy.
    - Restriction: Select the default action that the controller will take if no rules are matched. Available options include: **Allow only the stations listed below** or **Block only the stations listed below**.
  - b. Rules:
    - MAC Address: Type the MAC address to which this L2 access policy applies.
  - c. Click **OK**.

You have created an L2 access policy.

#### NOTE

You can also edit, clone and delete a policy by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **L2 Access Control** tab.

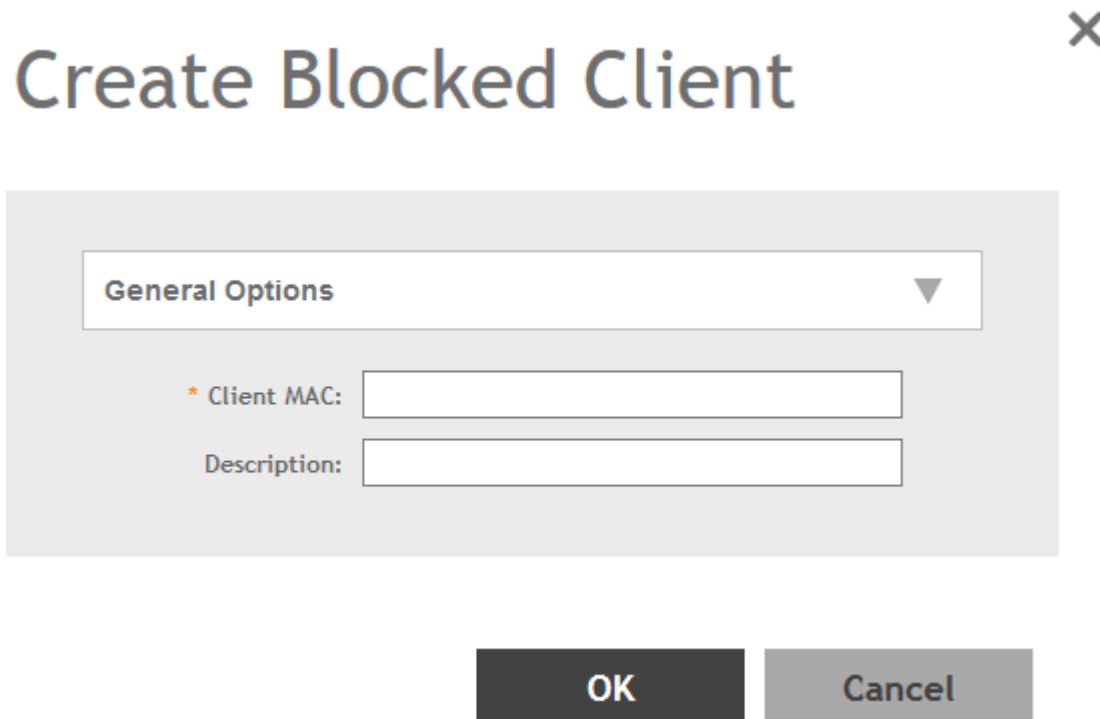
## Creating Blocked Clients

You can deny access to the network for certain clients by using the block client access control feature.

1. Go to **Services & Profiles > Access Control**.
2. Select the **Blocked Client** tab, and then select the zone for which you want to block the client access.
3. Click **Create**.

The **Create Blocked Client** page appears.

**FIGURE 126** Create Blocked Client



**Create Blocked Client**

**General Options**

\* Client MAC:

Description:

**OK** **Cancel**

4. Configure the following:
  - a. Client MAC: Type MAC address of the client that you want to block.
  - b. Description: Type a short description for client.
  - c. Click **OK**.

You have created the blocked client list.

### NOTE

You can also edit, clone and delete a list by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Blocked Client** tab.

## Creating a Client Isolation Whitelist

This feature allows the administrator to manually specify an approved list of wired destinations that may be reachable by wireless clients.

**NOTE**

The whitelist only applies to destinations that are on the wired network, and it will not work on wireless destinations.

1. Go to **Services & Profiles > Access Control**.
2. Select the **Client Isolation Whitelist** tab, and then select the zone for which you want to specify the list of approved clients.
3. Click **Create**.

The **Create Client Isolation Whitelist** page appears.

**FIGURE 127** Creating a Client Isolation Whitelist

### Create Client Isolation Whitelist

\* Name:

Description:

Auto Whitelist: ☐ APs will auto-discovery gateway devices and add them to the isolation whitelist.

Client Entries ▼

+ Create    Configure    Delete

MAC	IP Address	Description
<input type="text"/>		

OK    Cancel

4. Configure the following:
  - a. Name: Type a name for the client.
  - b. Description: Type a short description about the client.
  - c. Auto Whitelist: Select this check-box if you want the AP to automatically scan for devices and include them to the whitelist.
  - d. Client Entries: To add the clients to the list, click **Create** and provide client information such as MAC address (mandatory), IP address and Description.
  - e. Click **OK**.

You have created the list of whitelisted clients that can access the network.

**NOTE**

You can also edit, clone and delete the list by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Client Isolation Whitelist** tab.

## Creating Time Schedules

You can control client access to the network by providing a time schedule within which the device can access the network.

1. Go to **Services & Profiles > Access Control**.
2. Select the **Time Schedule** tab, and then select the zone for which you want to create the schedule.
3. Click **Create**.

The **Create Time Schedule Table** page appears.

**FIGURE 128** Creating a Time Schedule Table

### Create Time Schedules Table

\* Schedule Name:

Schedule Description:

	AM											PM											
Time	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Sun																							
Mon																							

4. Configure the following:
  - a. Schedule Name: Type a name for the schedule you want to create.
  - b. Schedule Description: Type a short description for this schedule.
  - c. Draw the schedule table.
  - d. Click **OK**.

You have created the schedule.

**NOTE**

You can also edit, clone and delete the schedule by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Time Schedule** tab.

## Creating a DNS Server Profile

By creating a DNS server profile, you can specify the primary and secondary address of the DNS server that will be used to transmit data packets to the DNS server.

1. Go to **Services & Profiles > Access Control**.
2. Select the **DNS Servers** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

The **Create DNS Server Profile** page appears.

**FIGURE 129** Creating a DNS Server Profile

## Create DNS Server Profile

\* Name:

Description:

\* Primary DNS IP:

Secondary DNS IP:

**OK** **Cancel**

4. Configure the following:
  - a. Name: Type a name for the DNS server profile.
  - b. Description: Type a short description for profile.
  - c. Primary DNS IP: Type the primary DNS IP address.
  - d. Secondary DNS IP: Type the secondary DNS IP address.
  - e. Click **OK**.

You have created the DNS Server Profile.

**NOTE**

You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **DNS Servers** tab.

## Creating a Traffic Class Profile

To create a traffic class profile, you must define the basic required settings.

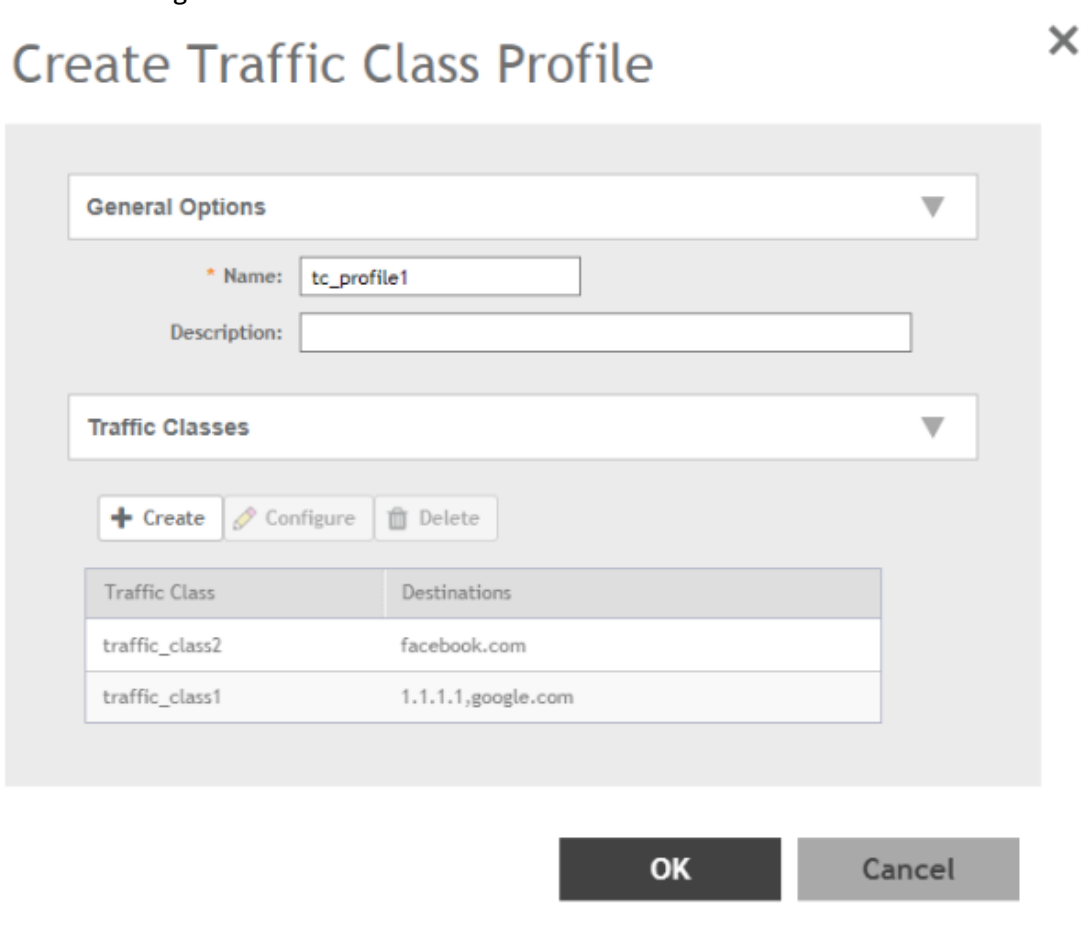
1. Go to **Services & Profiles > Access Control**.
2. Select the **Traffic Classes** tab, and then select the zone for which you want to create the profile.



3. Click **Create**.

The **Create Traffic Class Profile** page appears.

**FIGURE 130** Creating a Traffic Class Profile



## Create Traffic Class Profile

General Options

\* Name: tc\_profile1

Description:

Traffic Classes

+ Create

Configure

Delete

Traffic Class	Destinations
traffic_class2	facebook.com
traffic_class1	1.1.1.1,google.com

OK

Cancel

4. Under **General Options**, enter traffic class profile name and description.

- Under **Traffic Classes**, click **Create** to add a traffic class.

**NOTE**

Only four traffic classes can be added in a single **Traffic Class** profile.

The **Traffic Class** page appears.

**FIGURE 131** Creating a Traffic Class

\* Name:

Destination Addresses

\* Access Control Rule Entry  **+ Add** **Import CSV** **Cancel** **Delete**

Access Control Rule Entry

The following format are allowed for access control rule entry.  
Format:  
- IP (e.g. 10.11.12.13)  
- IP Range (e.g. 10.11.12.13-10.11.12.15)  
- CIDR (e.g. 10.11.12.100/28)  
- IP and mask (e.g. 10.11.12.13 255.255.255.0)  
- Precise web site (e.g. www.ruckus.com)  
- Web site with special regular expression like  
- \*.amazon.com  
- \*.com

**OK** **Cancel**

- Enter the name of the traffic class profile.
- In the **Access Control Rule Entry** field, enter an access control rule in the proper format.
- Click **Add** to add an access control rule or click **Import CSV** to import an access control list.

**NOTE**

Click the **Import CSV** arrow and select **Download Sample (CSV)** to download the CSV template.

**NOTE**

To delete an access control rule, select an entry and click **Delete**.

- Click **OK**.

You have created a Traffic Class Profile.

**NOTE**

IP destination is reachable only when IP is not part of Traffic Class, but present under Split Tunnel. Split-tunnel policy is effective only when both **Split Tunnel** and **Traffic Class** features are enabled together.

# Configuring Application Controls

Using the **Application Control** screen, you can identify, control, and monitor applications that are running on wireless clients associated with managed APs, and you can also apply filtering policies to prevent users from accessing certain applications.

Additionally, you can create your own user-defined applications, import an updated application signature package, and configure rate limiting and QoS traffic shaping policies based on system-defined or user-defined applications.

## Creating an Application Control Policy

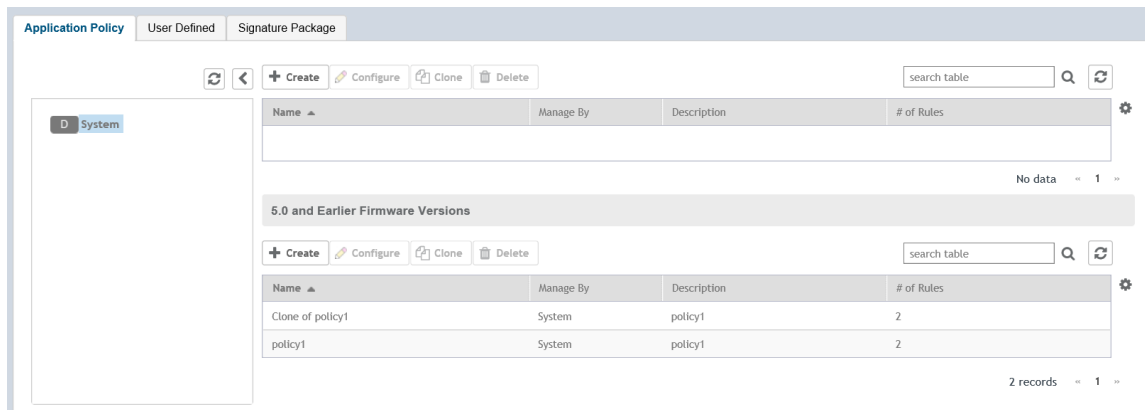
You must create an application policy to limit traffic by application, to classify traffic into priority queues using QoS traffic shaping rules, or to completely block access to an application.

Complete the following steps to create an application control policy:

1. Select **Services & Profiles > Application Control**.
2. Click the **Application Policy** tab.

The **Application Policy** page appears.

**FIGURE 132** Viewing Application Policy



- 3. Click **Create**.  
The **Create Application Policy** page appears.

**FIGURE 133** Creating an Application Policy

## Create Application Policy

Note: Please ensure that configuration is consistent with URL filtering policy. The URL filtering policy will take precedence.

General Options

Name:

Description:

Rules

+ Create

Configure

Delete

#	Rule Type	Content

Logging

[?] Send App Logs to SZ:

☐ Allow the AP to log every application event and end the events to SmartZone

[?] Enable Remote Syslog:

☐ Allow the AP to log every application event and end the events to external syslog

OK

Cancel

- 4. Under **General Options**, enter a policy name and policy description.

5. Under **Rules**, click **Create** to create a new rule.

**NOTE**

Each application policy can contain up to 128 rules.

The **Create Application Policy Rule** page appears.

**FIGURE 134** Creating an Application Policy Rule

6. In the **Rule Type** field, select one of the following options:
  - **Denial Rules**
  - **QoS**
  - **Rate Limiting**
7. In the **Application Type** field, select the type of application.
8. In the **Application** field, select the application for which you want to create a policy rule.

For example, if you select **All** in the application category and save the application rule, the application rule list reflects all Antivirus applications and is selected as a single entry in the rule list. A full category is counted as one rule in the allotment of 128 Layer 7 rules in a Layer 7 policy.

9. Click **OK** to save the rule.
 

If a rule is already created, you can edit its configuration settings by selecting the rule and clicking **Configure** on the **Create Application Policy** page.
10. Under **Logging**, select the appropriate option for the APs to log events:
  - **Allow the AP to log every application event and end the events to SmartZone**
  - **Allow the AP to log every application event and end the events to external syslog**
11. Click **OK** to save the application control policy.

You have created an application control policy.

You can continue to apply the application control policy to user traffic, as described in [Implementing an Application Control Policy](#) on page 274.

## Implementing an Application Control Policy

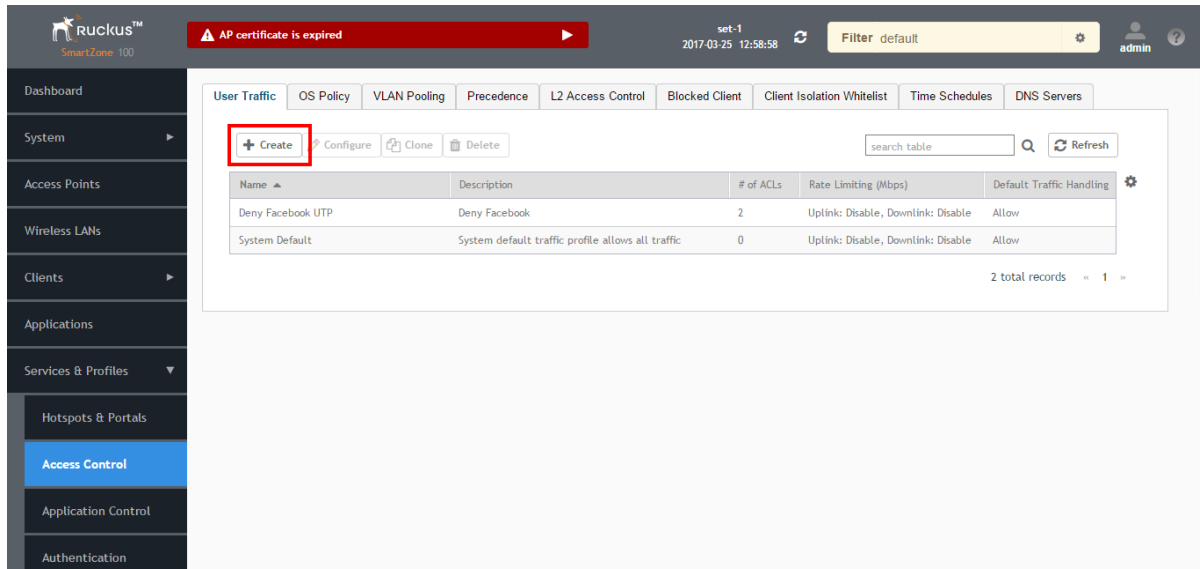
Deploying an application control policy involves configuring a User Traffic Profile (UTP) with the policy, and then applying that profile to a WLAN.

To implement an Application Control Policy:

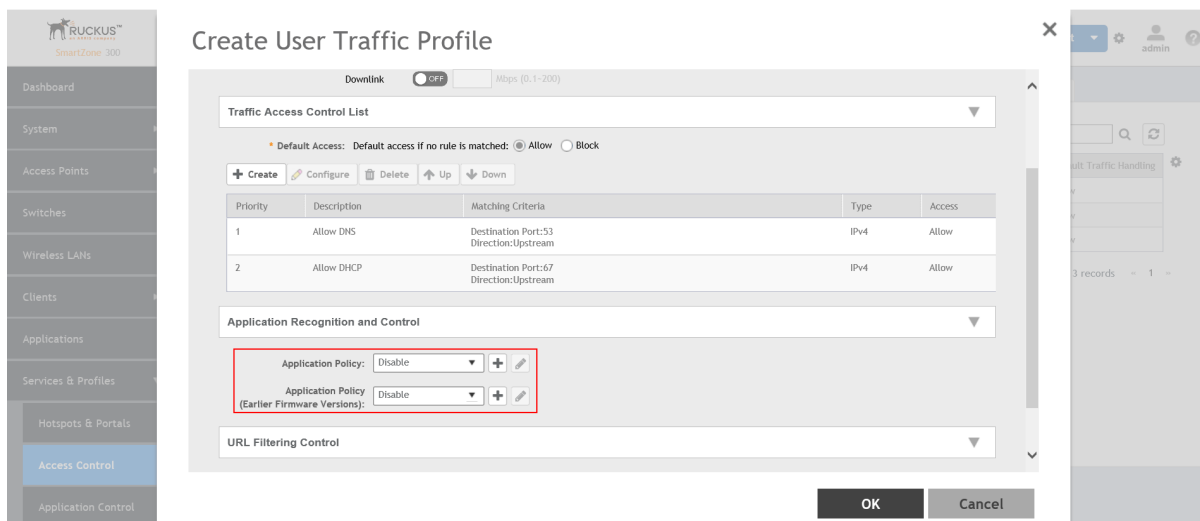
1. Go to **Services and Profiles > Access Control > User Traffic**.
2. Click **Create**. The **Create User Traffic Profile** page appears.
3. Enter a **Name**, and optionally a **Description** for the UTP.
4. Under **Application Recognition and Control**, select an **Application Policy** from the drop-down list. Alternatively, click **Create** to create a new policy.
5. Click **OK** to save the UTP.
6. Go to **Wireless LANs**.
7. Locate the WLAN for which you want to apply the application policy, and select it from the list.
8. Click **Configure**. The **Edit WLAN [WLAN Name]** page appears.
9. Under **Advanced Options**, select a user traffic profile you created from the drop-down list. Alternatively, click **Create** to create a new UTP.

- Click **OK** to save your WLAN changes.

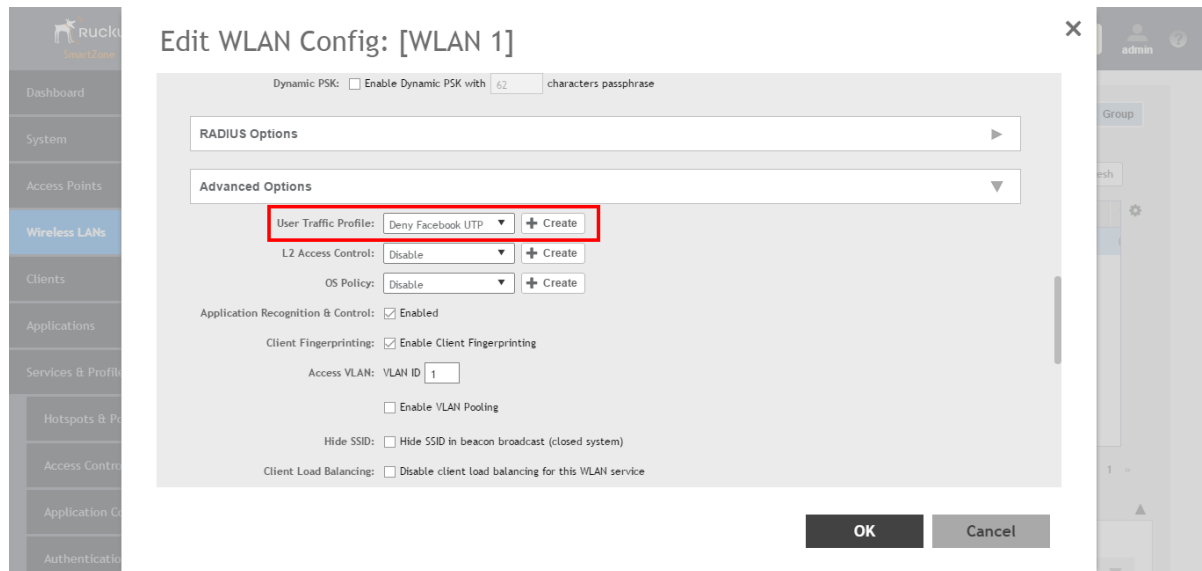
**FIGURE 135** Create a User Traffic Profile (UTP)



**FIGURE 136** Select an Application Policy to apply to this UTP



**FIGURE 137** Apply the UTP to a WLAN



## Creating a User Defined Application

When an application is unrecognized and generically (or incorrectly) categorized, the controller will be unable to monitor its traffic, unless you configure an explicit application identification policy based on IP address/mask, port and protocol.

To configure a user-defined application:

1. Go to **Services & Profiles > Application Control**.
2. Select the **User Defined** tab.



3. Click **Create**.  
The **Create User Defined Application** page appears.

**FIGURE 138** Creating a User Defined Application

**Create User Defined Application** X

\* Name:

\* Type: ☒ Default ☐ Port Mapping Only

\* Destination IP:

\* Netmask:

\* Destination Port:

\* Protocol: TCP ▼

OK Cancel

4. Configure the following:
  - a. **Name:** Type a name for the application. This is the name that will identify this application on the dashboard.
  - b. **Type:** Select Default or Port Mapping Only (destination port).
  - c. **Destination IP:** Type the destination IP address of the application.
  - d. **Netmask:** Type the netmask of the destination IP address.
  - e. **Destination Port:** Type the destination port for the application.
  - f. **Protocol:** Select the protocol used by the application. Options include TCP and UDP.
  - g. Click **OK**.

You have created the user defined application.

**NOTE**

You can also edit, clone and delete the application policy by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **User Defined** tab.

# Working with Application Signature Package

Ruckus will periodically release and make new application signature packages available for download.

## Step 1: Uploading the Signature Package

Once you have downloaded a new signature package, you can import it into SmartZone using the following procedure:

- 1. Select **Services & Profiles > Application Control**.
- 2. Select the **Signature Package** tab.

FIGURE 139 Viewing and Uploading Signature Package File Information

Application PolicyUser DefinedSignature Package

Current Signature Package Info

File Name	RuckusSigPack-v2-1.380.0-40
File Size	6.7MB
Version	1.380.0-40

Upload Signature Package

Upload the Application Signature Package file (\*.tar.gz).

Browse

Upload

5.0 and Earlier Firmware Versions

Current Signature Package Info

File Name	RuckusSigPack-1.074
File Size	591.2KB
Version	1.74

Upload Signature Package

Upload the Application Signature Package file (\*.tar.gz).

Browse

Upload

The **Current Signature Package Info** section displays the information about the file name, file size, and version of the signature package.

- 3. Under **Upload Signature Package**, click **Browse** to select the signature package file.
- 4. Click **Upload** to upload the signature package file.

Once the import is complete, the list of system-defined applications is updated immediately.

## Step 2: Validating the Signature Package

The application updates the latest signature package in all the connected APs. To validate the latest version follow the procedure:

- 1. In the Access Point, enter the Privileged EXEC mode using CLI.

2. Enter the following CLI command, which displays the latest version of the signature package.

```
rksccli:get tdt-sigpack
```

Current TDTs Signature Package is Ruckus-SigPack-Ver-x.xx.trf

OK

## Managing Signature Package Upgrading Conflicts

Upgrading a Signature package from lower version to a higher version fails when an Access Control Policy and an Application Control Policy already exists and the Application Signature in the AVC Policy of lower version conflicts with the one in higher version. In such a case, SZ displays an error message. Perform the following procedure to avoid this error.

To overcome Signature Package upgrade conflicts:

### Step 1: Delete the User Traffic Profile:

1. Go to **Services & Profiles > Access Control > User Traffic**.
2. Take a note of the profile details that you want to delete; click **Configure** to get more details of the profile for future reference.
3. Select the profile and click **Delete**.

### Step 2: Delete the Application Control Policy:

1. Go to **Services & Profiles > Application Control > Application Policy**.
2. Take a note of the policy details that you want to delete; click **Configure** to get more details of the profile for future reference.
3. Select the policy and click **Delete**.

### Step 3: Upgrade the Signature Package

1. Go to **Services & Profiles > Application Control -> Signature Package**.
2. Click **Browse**, and choose the Signature Package file.
3. Click **Upload**.

After the Signature Package is successfully applied the package file name, file size and the version will be visible in the UI.

### Step 4: Create a new User Traffic Profile with the details of the profile deleted.

### Step 5: Create a new Application Control Policy with the details of the policy deleted.

## URL Filtering

Administrators can use the URL filtering feature to block access to inappropriate websites. The Web pages available on the internet are classified into different categories, and those identified to be blocked can be configured based on available categories. Administrators can also create policies based on these categories, to allow or deny user access.

After categorizing websites accessed by the clients connected to the AP, a third-party cloud-hosted URL categorization service is used to categorize the live web traffic generated from the client devices. By default, traffic which is not categorized is allowed. The packets from the client device are dropped only after the URL is successfully categorized, and DENY is configured for the client in the policy.

The AP periodically generates statistics such as the Top 10 Denied URLs/categories, Top 10 URLs/categories by traffic and sends them to controller which collects this information and maintains it based on the filters applied per zone and WLAN.

URLs are typically classified by third-party applications to enhance internet security and usage. To categorize the web page or URL, the network packets must be analyzed. In HTTP packets, the complete URL value is extracted and in HTTPS packets, the domain name of the URL is extracted for URL web page categorization. The AP remembers the signature of the packet it forwards and when the packet is identified as HTTP or HTTPS, it receives the domain name/URL from the packet and sends it to the third-party URL categorization engine to verify the Web category. If the retrieved category is blocked as per the configured policy, packets with the same signature are blocked. Blocked HTTP browser traffic redirects the user to a web page that provides information on why the access to the website was denied. This feature is not applicable to HTTPS traffic and mobile application traffic.

The AP maintains a cache of up to 80000 URL entries and attempts to find the URL category from the local cache. It contacts the third-party URL categorization server only when the URL is not available in the local cache.

## Viewing a Summary of URL Filters

The **Summary** page provides administrators with a view to analyze URL traffic based on the user activity over the network.

You can view the top ten URLs by:

- Traffic - displays all URLs accessed (including blocked URLs) the most
- Categories Traffic - displays all categories accessed (including blocked categories) the most
- Clients Traffic - displays all clients accessed (including blocked clients) the most
- Blocked URLs - displays the URLs that have been denied access the most
- Blocked Categorize - displays the URL categories that have been denied the most
- Blocked Clients - displays the clients that have been denied access the most

## Creating a URL Filtering Policy

Administrators can create URL filtering policies and reuse them across WLAN controllers. You can define the policy based on the web page categorization, whitelist, blacklist and web search.

Policies can also be created based on the role assigned to the user. Users can be allowed or denied access to a particular URL based on the role assigned, and the SSID login details for that role.

Follow these steps to create a URL filtering policy:

1. Go to **Services & Profiles > URL Filtering**.

2. Select the **Profiles** tab, and then click **Create**.  
The **Create URL Filtering Policy** page appears.

**FIGURE 140** Creating a URL Filtering Policy

## Create URL Filtering Policy

**General Options**

**Blocked Categories**

☒ No adult content  
☐ Clean and safe  
☐ Child and student friendly  
☐ Strict  
☐ Custom

No adult content or nudity  
 No adult content plus, no malware, spyware, phishing, botnet or spamware  
 Clean and safe plus no alcohol, intimate apparel, dating, or weapons  
 Child and student friendly plus no streaming media, personal storage and, games  
 Please chose the contents you want to block in below checkbox group

**Blocked Categories**

[Select All](#) [None](#)

<input checked="" type="checkbox"/> Abortion	<input type="checkbox"/> Entertainment and Arts	<input type="checkbox"/> Job Search	<input type="checkbox"/> Personal Storage	<input type="checkbox"/> Society
<input type="checkbox"/> Abused Drugs	<input type="checkbox"/> Fashion and Beauty	<input checked="" type="checkbox"/> Keyloggers and Monitoring	<input type="checkbox"/> Personal sites and Blogs	<input type="checkbox"/> Sports
<input checked="" type="checkbox"/> Adult and Pornography	<input type="checkbox"/> Financial Services	<input type="checkbox"/> Kids	<input type="checkbox"/> Philosophy and Political Advocacy	<input checked="" type="checkbox"/> Spyware and Adware
<input type="checkbox"/> Alcohol and Tobacco	<input type="checkbox"/> Food and Dining	<input type="checkbox"/> Legal	<input checked="" type="checkbox"/> Phishing and Other Frauds	<input type="checkbox"/> Stock and Advice Tools
<input type="checkbox"/> Auctions	<input type="checkbox"/> Gambling	<input type="checkbox"/> Local Information	<input type="checkbox"/> Private IP Addresses	<input type="checkbox"/> Streaming Media
<input type="checkbox"/> Bot Nets	<input type="checkbox"/> Games	<input checked="" type="checkbox"/> Malware Sites	<input type="checkbox"/> Proxy Avoidance and	<input type="checkbox"/> Swimsuits & Intimate Apparel

**Blacklist & Whitelist**

Blacklist: \* Domain Name

Domain Name

Whitelist: \* Domain Name

Domain Name

**Safe Search**

Google Safe Search: ☐ Enable

YouTube Safe Search: ☐ Enable

Bing Safe Search: ☐ Enable

Configure the following:

- General Options  
Name: type the name of the policy you want to create.

Description: type a brief description for the policy to identify

- **Blocked Categories:** select one of the categories to block. Choosing the Custom option allows the administrator to customize the list of categories to block for the user. You can also use Select All to choose all of the categories listed, or None to set no filters for the user to access - user can access any URL in this case as no web page is blocked.
- **Blacklist and Whitelist:** If web content categorization is unable to classify URLs that the user, organization or institution needs, then Whitelist or Blacklist profiles can be created by the administrator. The URLs listed by the administrator under Blacklist are blocked and those listed under Whitelist are allowed access. The domain names under the Blacklist and Whitelist take precedence over the default allow or deny action of the URL filter.

The AP matches the URL pattern against all the configured Whitelist and Blacklists through the *egrep* (Extended Global Regular Expressions Print) program which performs a line-by-line scan of the file and returns lines that contain a pattern matching the given expression. Currently, the exact URL name or a wildcard at the beginning of the URL is used to match the pattern.

Administrators can also add specific IP addresses or wildcard domain names under Whitelist and Blacklist.

In **Domain Name**, type the domain name of the web page that you want to deny user access to in the **Blacklist** tab, and provide user access to in the **Whitelist** tab. You can define up to 16 domains.

Click **Add**. The domain name/web page is listed in the corresponding tab.

Click **Cancel** to remove the domain name you have entered in the field.

If you want to delete the domain name from the *Blacklist* or *Whitelist* tab, select the URL and click **Delete**.

- **Safe Search:** Administrators can configure the policy to include a safe search option when users access Google, YouTube or Bing to search on the internet. Select the **Enable** check box to set the safe search feature to ON. Enabling this option will mandate all users using this policy on the network to use safe search on Google, YouTube and Bing. This option provides a secure connection via HTTPS while still allowing access to the internet. Enabling safe search on the browser displays the virtual IP address of the browser.

3. Click **OK**.

The **URL Filtering Policy** form is submitted with the specified configuration settings.

You have created the URL filtering policy. The newly created policy is displayed on **Profiles** page.

If you click on the policy, it displays the following information:

- Name
- Managed By
- Description
- Filtering Level
- # of Blocked Categorize
- # of Blacklist
- #of Whiltelist
- Last Modified By
- Last Modified On

Click **Configure** to edit the policy. Click **Clone** to create a duplicate of the policy, or to make modifications to the existing settings of the clone.

Click **Delete** to delete the policy from the URL Filtering Profile.

## Enabling URL Filtering on the Controller

You can enable the URL filtering feature on the WLAN controller to block or allow access to specific web sites or web pages.

By configuring the controller, the administrator can create a wireless network SSID and allow or deny access to a category of websites for all users that join this SSID.

Follow these steps to enable URL filtering on the controller:

1. In the **Wireless LANs** page, from the System tree hierarchy, select the domain, zone or WLAN system for which you want to enable URL.

2. Click **Create**.

The **Wireless LANs** page appears.

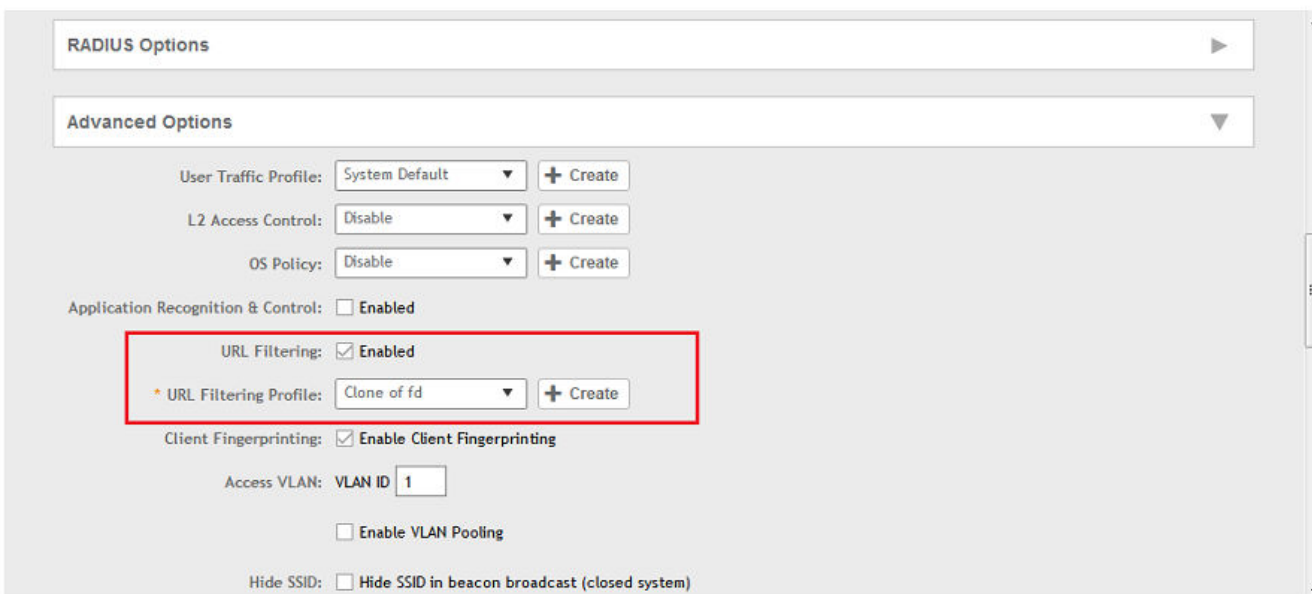
3. In **Advance Options**, select the **Enabled** check-box against the **URL Filtering** option.

The **URL Filtering Profile** field appears. Select a profile from a list of existing URL filtering profiles displayed in the drop-down menu. You can also click **Create** to create a new URL filtering profile.

For more information, see [Creating a URL Filtering Policy](#) on page 280.

**FIGURE 141** Enabling URL Filtering

### Create WLAN Configuration



The screenshot shows the 'Create WLAN Configuration' page. The 'Advanced Options' section is expanded. The 'URL Filtering' checkbox is checked and highlighted with a red box. The 'URL Filtering Profile' dropdown is set to 'Clone of fd'. Other options include 'User Traffic Profile' (System Default), 'L2 Access Control' (Disable), 'OS Policy' (Disable), 'Application Recognition & Control' (unchecked), 'Client Fingerprinting' (checked), 'Access VLAN' (VLAN ID 1), 'Enable VLAN Pooling' (unchecked), and 'Hide SSID' (unchecked).

#### NOTE

Application rules are applied based on the following priority, and user defined rules take precedence over URL filtering.

- a. User defined ARC profile
- b. URL Filtering
- c. ARC

You have enabled URL filtering on the controller.

## Enabling URL Filtering in the User Traffic Profile

A User Traffic Profile (UTP) can be created to block or limit user traffic based on a number of factors, including URL filtering in addition to Source IP address, Port, Destination IP address, Protocol, etc. A UTP can be created to shape traffic according to a configurable Application Control Policy.

After the UTP is created, it can be applied to any WLAN from the **Wireless LANs** page.

1. Go to **Services & Profiles > Access Control**.
2. Select the **User Traffic** tab, and then select the zone for which you want to create the profile.
3. Click **Create**.

The **Create User Traffic Profile** page appears.

4. In **URL Filtering Control**, select the **URL Filtering Profile** from the drop-down menu.

You can also create a URL filtering profile by clicking **Create**. For more information, refer to [Creating a URL Filtering Policy](#) on page 280.

**NOTE**

You must select a UTP in which URL filtering is enabled, and also ensure URL filtering is enabled within the same WLAN configuration.

**FIGURE 142** UTP Page

### Create User Traffic Profile

Default Access: Default access if no rule is matched: ☒ Allow ☐ Block

+ Create

Configure

Delete

Up

Down

Priority	Description	Matching Criteria	Access
1	Allow DNS	Destination Port:53 Direction:Upstream	Allow
2	Allow DHCP	Destination Port:67 Direction:Upstream	Allow

Application Recognition and Control

Application Policy: No data available + Create

URL Filtering Control

URL Filtering Profile: No data available + Create

You have successfully enable URL filtering in the UTP.



## Managing URL Filtering Licenses

URL Filtering license for the selected partners-to use the content database is issued for a duration of one year for an AP. Dashboard warnings are issued thirty days before the end of the license term.

You can add licenses over time. For example, you can purchase 100 one-year licenses on January 1st and add another 200 one-year licenses in May. The controller receives a new expiry date for the combined license count of 300 APs.

To view license details such as start date, end date, and capacity, go to **Administration > Licenses > Installed Licenses** tab. For more information on importing installed licenses, synchronizing the controller with the license server, and downloading license files, refer *Managing Licenses*.

When the license capacity is exhausted, event code 1281 is triggered. When the license period expires, alarm code 8003 is generated which indicates that the URL filtering server is unreachable. For more information, refer *Managing Events and Alarms*.

### NOTE

A permissive license similar to the BSD 2-Clause License, but with a 3rd clause that prohibits others from using the name of the project or its contributors to promote derived products without written consent.

Copyright (c) 2005, Google Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

### ATTENTION

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

URL filtering feature is supported only on APs that have a minimum of 256MB RAM.

**TABLE 28** List of APs with 256MB or more

E510	T811-CM	T310c/d/n/s	H320
R720	T610/T610s	C110	R610
R500e	H510	T710 / T710s	R510
R310	T504	R710	R600
T300	T301n	T301s	T300e
FZM300 & FZP300	R500	R700	

# Understanding WiFi Calling

Mobile service providers offer services where you can make voice calls or send and receive text messages from their mobile phones using a WiFi network, without changing the mobile number.

Built-in software applications on smart phones provide seamless authentication of the device when on the Wi-Fi network with the mobile carrier network. When WiFi calling is enabled by the mobile carrier, an IPSec tunnel is established between the phone and the mobile network through which calls are routed.

Due to increasing use of Wi-Fi for device connections, WiFi Calling is seeing high demand by many service providers worldwide, which allows them to differentiate their WiFi access. Though the end-user device and Mobile Packet Core communicate directly over encrypted tunnels, it is important for the Wi-Fi network to detect and prioritize this type of traffic for an optimal application experience.

This feature supports WiFi calling traffic recognition and prioritization above other network traffic, with visibility for Wi-Fi calling stats for the network operator. Following are some benefits of using WiFi calling in Ruckus networks:

- QoS ensures advanced identification rules prioritize voice traffic over data traffic
- Seamless roaming across APs
- Voice call analytics and reporting aid in planning network resource and troubleshooting
- Accurate classification and prioritization of voice calls over WiFi on WLANs
- Enables users to define priorities for voice, video, background and best effort on the WiFi calls generated from a particular carrier phone. For example, you can prioritize your choice of carriers WiFi calls over other WiFi calls.
- Easy to setup and offers the flexibility to add more than one ePDG FQDN/address for a carrier
- WiFi call prioritization when mobile phones roams from one AP to another

## Creating a WiFi Calling Profile

You can classify the voice packets in a WiFi call based on the carrier, by creating a WiFi calling profile.

1. Go to **Services & Profiles > WiFi Calling > Profiles**.
2. Click **Create**.

The **WiFi Calling Profile** page appears.

**FIGURE 143** Creating a WiFi Calling Profile

The screenshot displays the Ruckus SmartZone web interface. On the left is a navigation sidebar with the Ruckus logo at the top and a list of menu items: Dashboard, System, Access Points, Switches, Wireless LANs, Clients, Applications, Services & Profiles (which is highlighted), Hotspots & Portals, and Access Control. The main content area is titled 'Create Wi-Fi Calling Policy'. It contains a 'General Options' section with fields for 'Carrier Name', 'Description', and a 'QoS Priority' dropdown menu set to 'Voice'. Below this is an 'Evolved Packet Data Gateway (ePDG)' section with a table for adding domain names and IP addresses. The table has two columns: 'Domain Name' and 'IP Address'. There are '+ Add', 'X Cancel', and 'Delete' buttons for the table. At the bottom right of the form are 'OK' and 'Cancel' buttons.

3. In **General Options**, configure the following:  
 Carrier Name: Type the name of the carrier based on which you want to create a rule to prioritize the voice calls  
 Description: Provide a brief description about the profile  
 QoS Priority: From the drop-down menu, select the Quality of Service feature based on which you want to prioritize the calls
4. In **Evolved Packet Data Gateway (ePDG)**, configure the following:  
 Domain Name: Type the domain name. For example, epdg.epc.att.net  
 IP Address (optional): Type the IP address for the domain. Providing the IP address enables better WiFi calling QoS during roaming.
5. Click **Add** to include the domain.  
 The AP will verify the domain IP address before qualifying the WiFi call.
6. Click **OK**.  
 The WiFi calling profile is created and displayed with its name, QoS priority, number of ePDGs associated and management domain.

**NOTE**

You can edit, clone and delete the profile by clicking **Configure**, **Clone** and **Delete**, respectively.

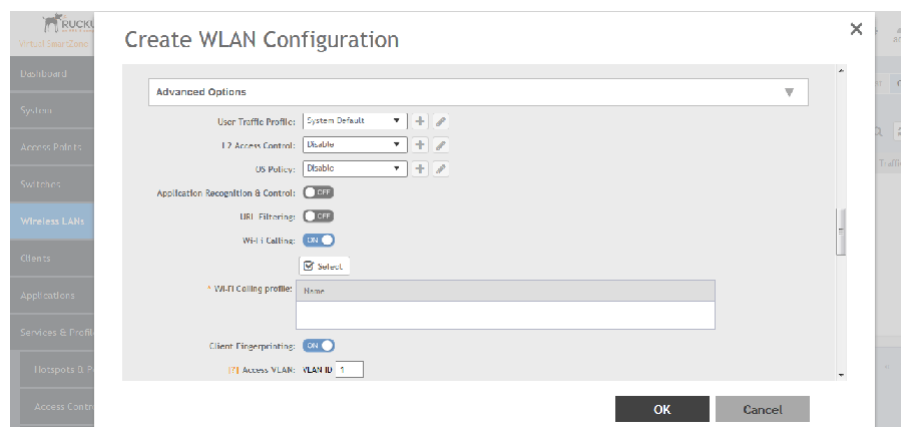
## Configuring WiFi Calling in WLAN

You can also edit the WLAN configuration to select a WiFi calling profile.

1. Go to **Wireless LANs**.
2. Select the WLAN for which you want to enable WiFi calling and click **Configure**.

The **Edit WLAN Configuration** page appears. You can also enable WiFi calling when you create a fresh WLAN configuration, by clicking **Create**.

**FIGURE 144** Configuring WiFi Calling in a WLAN



- 3.
4. In **Advanced Options**, move the **WiFi Calling** radio button to ON. WiFi calling is enabled.

5. Click **Select**.

The **WiFi Calling Policies** page appears.

From the list under **Available Profiles**, identify the ones you want and click the -> icon. The profile(s) is moved under **Selected Profiles**. You can use the <- icon to de-select the profile for the WLAN.

6. Click **OK**.

The profile(s) selected are displayed under the **WiFi Calling Profile** field.

You have selected the WiFi calling profile that you want to apply to the WLAN.

## Analyzing WiFi Calling Statistics

You can view a summary of the WiFi calling traffic by the top ten SSIDs by traffic and ePDGs by traffic. The trends provide information about the WiFi usage, uplink and downlink speeds.

Go to **Services & Profiles > WiFi Calling > Summary**.

The **WiFi Calling Clients** area provides the following information about clients that are using the WiFi calling feature, such as:

- Hostname: displays the name to the user equipment or device that is connected to the WiFi
- MAC Address: IP address of the user equipment
- Carrier Name: displays the name of the carrier network/service provider used by the user equipment such as ATT, Sprint, and TMobile etc.
- Priority: Displays the priority set for the WiFi call through this device such as voice, video, best effort and background
- Traffic Session: displays the amount of data that is transmitted during the WiFi call
- Traffic (uplink/downlink): displays the speed with which data is transmitted during the WiFi call

**FIGURE 145** Analysing WiFi Traffic



The Clients detail page provides following information about the client involved in the WiFi call:

- AP MAC: displays the MAC address of the AP
- Client IP: displays the IP address of the client
- Carrier Name: displays the name of the carrier, for example, epdg.epc.att.net
- Start Time: displays the time when the client initiated the WiFi call
- End Time: displays the time when the client completed the WiFi call

- Traffic (uplink/downlink): displays the speed with which the data is transmitted during the WiFi call session

**FIGURE 146** WiFi Calling Client Details

WiFi Calling Clients

search table

Hostname	MAC Address	Carrier Name	Priority	Traffic (session)	Traffic (uplink)	Traffic (downlink)
flvikiranMottapart	24:F3:94:96:D5:D7	att	Voice	3.6MB	2.0MB	1.6MB
Samsung Galaxy S7 edge	2C:5E:3C:39:8F:8D	tmobile	Voice	2.5MB	1.2MB	1.3MB

2 records

Client Detail:

search table

AP MAC	Client IP	Carrier Name	Start time	End time	Traffic (uplink)	Traffic (downlink)
1C:8A:14:2A:8F:3D	10.150.3.154	epdg.epc.att.net	19/01/18 19:12:24	N/A	1.1MB	842.3MB

1 records

## Authentication

You can add AAA servers to the controller in order to use them to authenticate users attempting to associate with controller-managed APs.

### Creating Non-Proxy Authentication AAA Servers for Standby Cluster

A non-proxy AAA server is used when the APs connect to the external AAA server directly.

1. Go to **Services & Profiles > Authentication**.
2. Select the **Non-Proxy (AP Authenticator)** tab, and then select the zone for which you want to create the AAA server.
3. Click **Create**.

The **Create AAA Server** page is displayed.

**FIGURE 147** Creating an AAA Server

Create AAA Server

General Options

Name:

Description:

Type: ☒ RADIUS ☐ Active Directory ☐ LDAP

ClusterRedundancy: ☐ OFF ☐ Enable Service for Standby Cluster

Backup RADIUS: ☐ OFF ☐ Enable Secondary Server

OK Cancel

4. Configure the following:
  - a. General Options
    - Name: Type a name for the AAA server that you are creating.
    - Description: Type a short description of the AAA server.
    - Type: Select the type of AAA server that you are creating. Options include RADIUS, Active Directory and LDAP.
    - Cluster Redundancy: Select the **Enable Service for Standby Cluster** option to enable cluster redundancy.
    - Backup RADIUS (appears if you clicked RADIUS above): Select the **Enable Secondary Server** check box if a secondary RADIUS server exists on the network.
    - Global Catalog (appears if you clicked Active Directory above): Select the **Enable Global Catalog support** if you the Active Directory server to provide a global list of all objects.
  - b. Primary Server
    - If you selected RADIUS, configure the following options in the Primary Server section:
      - IP Address: Type the IP address of the AAA server. Both IPv4 and IPv6 addressing formats are supported.
      - Port: Type the port number of the AAA server. The default RADIUS server port number is 1812.
      - Shared Secret: Type the AAA shared secret.
      - Confirm Secret: Retype the shared secret to confirm.

If you have enabled **Backup RADIUS** to the **Secondary Sever**, you must provide similar information as in the primary server.

See [RADIUS Service Options](#) on page 294 for more information.
    - If you selected Active Directory, configure the following options in the Primary Server section:
      - IP Address: Type the IPv4 address of the AD server.
      - Port: Type the port number of the AD server. The default port number (389) should not be changed unless you have configured the AD server to use a different port.
      - Windows Domain Name: Type the Windows domain name assigned to the AD server (for example, domain.ruckuswireless.com).
    - If you selected LDAP, configure the following options:
      - IP Address: Type the IPv4 address of the LDAP server.
      - Port: Type the port number of the LDAP server. Default is 389.
      - Base Domain Name: Type the base DN in LDAP format for all user accounts (for example, dc=ldap,dc=com).
      - Admin Domain Name: Type the admin DN in LDAP format (for example, cn=Admin;dc=<Your Domain>,dc=com).
      - Admin Password: Type the administrator password for the LDAP server.
      - Confirm Password: Retype the administrator password to confirm.
      - Key Attribute: Type a key attribute to denote users (for example, default: uid)
      - Search Filter: Type a search filter (for example, objectClass=Person).
5. Under **User Role Mapping**, click **Create** to create a user traffic profile mapping.
  - a) In the **Group Attribute Value** field, enter the value.
  - b) Select a user role from the **User Role** list or click **+** to create a user role. For more information, refer to **Creating a User Role** section in the Administration guide.
6. Click **OK**.

You have completed creating a Non-proxy AAA server.

#### NOTE

You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Non-Proxy (AP Authenticator)** tab.

### Testing AAA Server (Auth)

To ensure that the controller administrators will be able to authenticate successfully with the RADIUS server type that you selected, Ruckus strongly recommends testing the AAA server after you set it up.

The test queries the RADIUS server for a known authorized user and return groups associated with the user that can be used for configuring roles within the controller.

1. Go to **Services & Profiles > Authentication**.
2. Select the **Non-Proxy (AP Authenticator)** tab, and then select the zone for which you want to test the AAA server.
3. Click **Test AAA**.

The **Test AAA Server** page appears.

4. Configure the following:
  - a. Name: Select one of the AAA servers that you previous created.
  - b. User Name: Type an existing user name on the AAA server that you selected.
  - c. Password: Type the password for the user name you specified.
5. Click **Test**.

If the test was unsuccessful, there are two possible results (other than success) that will be displayed to inform you if you have entered information incorrectly: **Admin invalid** or **User name or password invalid**. These results can be used to troubleshoot the reasons for failure to authenticate administrators with an AAA server through the controller.

You have completed testing the non-proxy AAA servers that you created.

### Creating Proxy AAA Servers for Standby Cluster

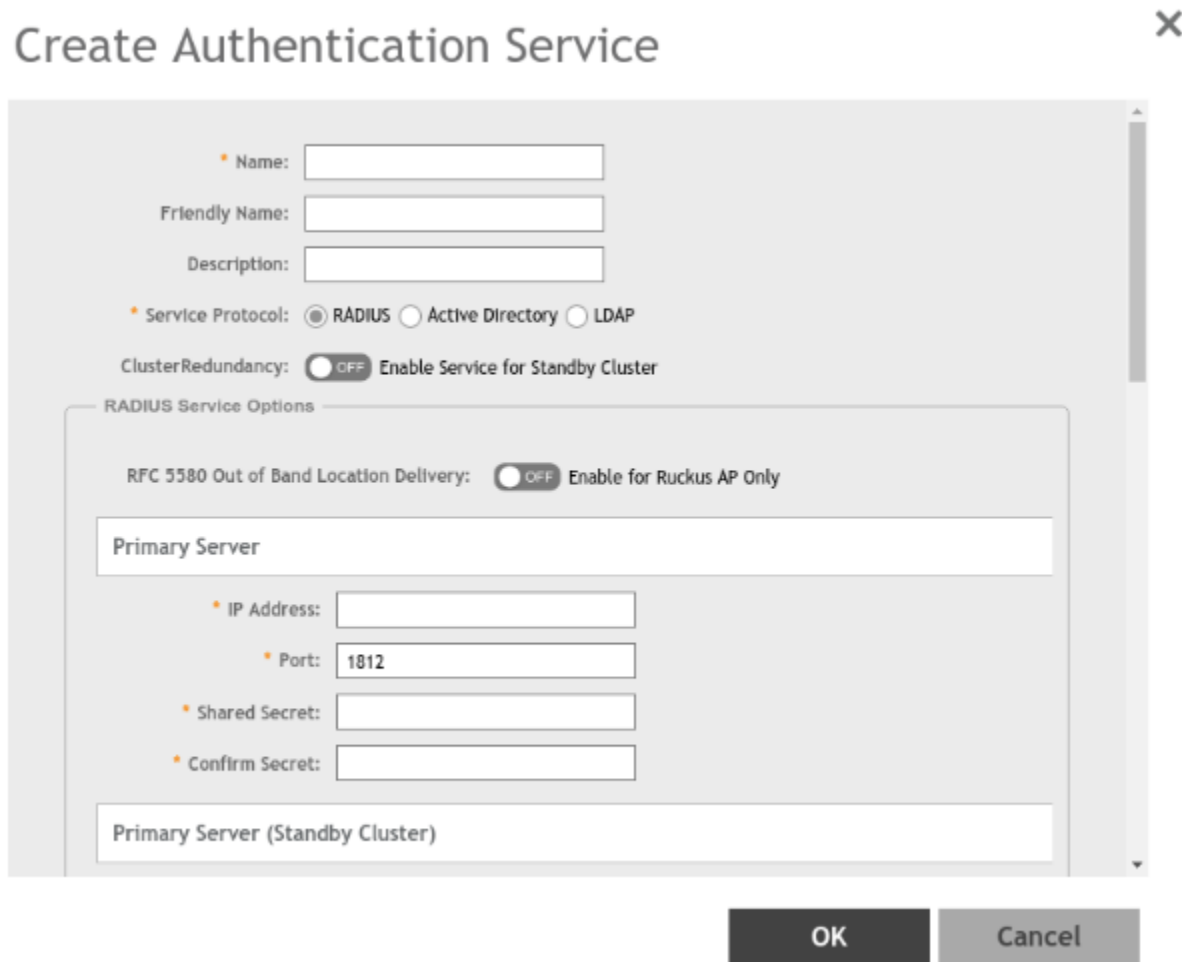
A proxy AAA server is used when APs send authentication/accounting messages to the controller and the controller forwards these messages to an external AAA server.

1. Go to **Services & Profiles > Authentication**.
2. Select the **Proxy (SZ Authenticator)** tab, and then select the zone for which you want to create the AAA server.

3. Click **Create**.

The **Create Authentication Service** page appears.

**FIGURE 148** Creating an Authentication Service



The image shows a 'Create Authentication Service' dialog box with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Name:** A text input field.
- Friendly Name:** A text input field.
- Description:** A text input field.
- Service Protocol:** Radio buttons for **RADIUS** (selected), **Active Directory**, and **LDAP**.
- ClusterRedundancy:** A toggle switch set to **OFF** with the text 'Enable Service for Standby Cluster'.
- RADIUS Service Options:** A section containing:
  - RFC 5580 Out of Band Location Delivery:** A toggle switch set to **OFF** with the text 'Enable for Ruckus AP Only'.
  - Primary Server:** A text input field.
  - IP Address:** A text input field.
  - Port:** A text input field with the value **1812**.
  - Shared Secret:** A text input field.
  - Confirm Secret:** A text input field.
  - Primary Server (Standby Cluster):** A text input field.

At the bottom right of the dialog are two buttons: **OK** and **Cancel**.



4. Configure the following:
  - a. Name: Type a name for the authentication service that you are adding.
  - b. Friendly Name: Type an alternative name that is easy to remember.
  - c. Description: Type a description for the authentication service.
  - d. Service Protocol: If you select
    - RADIUS, see [RADIUS Service Options](#) on page 294 for more information.
    - Active Directory, configure the following:
      1. Global Catalog: Select the **Enable Global Catalog** support if you the Active Directory server to provide a global list of all objects.
      2. Primary Server:
        - Encryption: Select the **Enable TLS Encryption** check box if you want to use the *Transport Layer Security* (TLS) protocol to secure communication with the server.

**NOTE**

You must also configure the Trusted CA certificates to support TLS encryption.

3. IP Address: Type the IPv4 address of the AD server.
4. Port: Type the port number of the AD server. The default port number (389) should not be changed unless you have configured the AD server to use a different port.
5. Windows Domain Name: Type the Windows domain name assigned to the AD server (for example, domain.ruckuswireless.com).
- LDAP, configure the following:
  1. Select the **Enable TLS Encryption** check box if you want to use the *Transport Layer Security* (TLS) protocol to secure communication with the server.

**NOTE**

You must also configure the Trusted CA certificates to support TLS encryption.

2. IP Address: Type the IPv4 address of the LDAP server.
3. Port: Type the port number of the LDAP server.
4. Base DN: Type the base DN in LDAP format for all user accounts (for example, dc=ldap,dc=com).
5. Admin DN: Type the admin DN in LDAP format (for example, cn=Admin;dc=<Your Domain>,dc=com).
6. Admin Password: Type the administrator password for the LDAP server.
7. Confirm Password: Retype the administrator password to confirm.
8. Key Attribute: Type a key attribute to denote users (for example, default: uid)
9. Search Filter: Type a search filter (for example, objectClass=Person).
- e. Cluster Redundancy: Click the **Enable Service for Standby Cluster** option to enable cluster redundancy.
- f. Advanced Options - Domain name: Type the whitelisted domain name that you want to add.
- g. User Traffic Profile Mapping:
  1. Type a **Group Attribute Value**.
  2. Select a **User Role** from the drop-down list.
  3. Click **Add**.

The mapped user profile is listed.

5. Click **OK**.

You have completed creating a Proxy AAA server.

**NOTE**

You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Proxy (SZ Authenticator)** tab.

## RADIUS Service Options

These are the Radius service options available for the primary and secondary servers.

RFC 5580 Out of Band Location Delivery: If you want out-of-band location delivery (RFC 5580) to apply only to Ruckus APs, select the **Enable for Ruckus AP Only** check box.

Configure the primary RADIUS server settings as shown in the following table.

Configure the primary RADIUS server settings.

**TABLE 29 Primary Server Options**

Option	Description
IP Address	Type the IP address of the RADIUS server. IPv4 and IPv6 addressing formats are supported.
Port	Type the port number of the RADIUS server. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
Shared Secret	Type the RADIUS shared secret.
Confirm Secret	Retype the shared secret to confirm.

If you have a secondary RADIUS server on the network that you want to use as a backup, select the Enable Secondary Server check box, and then configure the settings in the following table.

**TABLE 30 Secondary Server Options**

Option	Description
Backup RADIUS	Select <b>Enable Secondary Server</b> . When a secondary RADIUS server is enabled and the primary RADIUS server becomes unavailable, the secondary Automatic Fallback Disable server takes over the handling of RADIUS requests. When the primary server becomes available again, it takes back control over RADIUS requests from the secondary server. If you want to prevent the primary server from retaking control over RADIUS requests from the secondary server, select the <b>Automatic Fallback Disable</b> check box.
IP Address	Type the IP address of the secondary AAA server. IPv4 and IPv6 addressing formats are supported.
Port	Type the port number of the secondary AAA server port number. The default RADIUS server port number is 1812 and the default RADIUS Accounting server port number is 1813.
Shared Secret	Type the AAA shared secret.
Confirm Secret	Retype the shared secret to confirm.

The following options define the health monitoring settings of the primary and secondary RADIUS servers, when the controller is configured as RADIUS proxy for RADIUS Authentication and Accounting messages.

**TABLE 31 Health Check Policy**

Option	Description
Response Window	<p>Set the time (in seconds) after which, if the AAA server does not respond to a request, the controller will initiate the zombie period (see below). Response Window</p> <p>If the primary AAA server does not respond to RADIUS messages sent after Response Window expires, the controller will forward the retransmitted RADIUS messages to the secondary AAA server.</p> <p><b>NOTE</b> The zombie period is not started immediately after the Response Window expires, but after the configured Response Window plus <math>\frac{1}{4}</math> of the configured Zombie Period. The default Response Window is 20 seconds</p>
Zombie Period	<p>Set the time (in seconds) after which, if the AAA server does not respond to ANY packets during the zombie period, it will be considered to inactive or unreachable.</p> <p>An AAA server that is marked zombie (inactive or unreachable) will be used to proxy with a low priority. If there are other live AAA servers, the controller will attempt to use these servers first instead of the zombie AAA server.</p> <p>The controller will only proxy requests to a zombie server only when there are no other live servers. Any request that is sent as a proxy to an AAA server will continue to be sent to that AAA server until the home server is marked inactive or unreachable. At that point, the request will fail over to another server, if a live AAA server is available. The default Zombie Period is 40 seconds.</p>
Revive Interval	<p>Set the time (in seconds) after which, if no RADIUS messages are sent as proxy to the AAA server after it has been marked as inactive or unreachable, the controller will mark the AAA server as active again (and assume that it has become reachable again). The default Revive Interval is 120 seconds.</p>
No Response Fail	<p>Click <b>Yes</b> to respond with a reject message to the NAS if no response is received from the RADIUS server. Click <b>No</b> to skip sending a response.</p>

**NOTE**

To ensure that the RADIUS fail-over mechanism functions correctly, either accept the default values for the Response Window, Zombie Period, and Revive Interval, or make sure that the value for Response Window is always higher than the value for RADIUS NAS request timeout multiplied by the value for RADIUS NAS max number of retries. For third party APs, you must ensure that the configured Response Window on the controller is higher than the RADIUS NAS request timeout multiplied by the RADIUS value. The maximum number of retries is configured at the 3rd party controller/AP.

Configure the following options.

**TABLE 32 Rate Limiting**

Options	Description
Maximum Outstanding Requests (MOR)	<p>Set the maximum outstanding requests per server. Type 0 to disable it, or set a value between 10 and 4096.</p>
Threshold (% of MOR)	<p>Set a percentage value of the MOR at which (when reached) the controller will generate an event. Threshold (% of MOR)</p> <p>For example, if the MOR is set to 1000 and the threshold is set to 50%, the controller will generate an event when the number of outstanding requests reaches 500.</p>

**TABLE 32** Rate Limiting (continued)

Options	Description
Sanity Timer	Set a timer (in seconds) that will be started whenever a condition that generates an event is reached. This helps prevent conditions that trigger events which occur frequently.

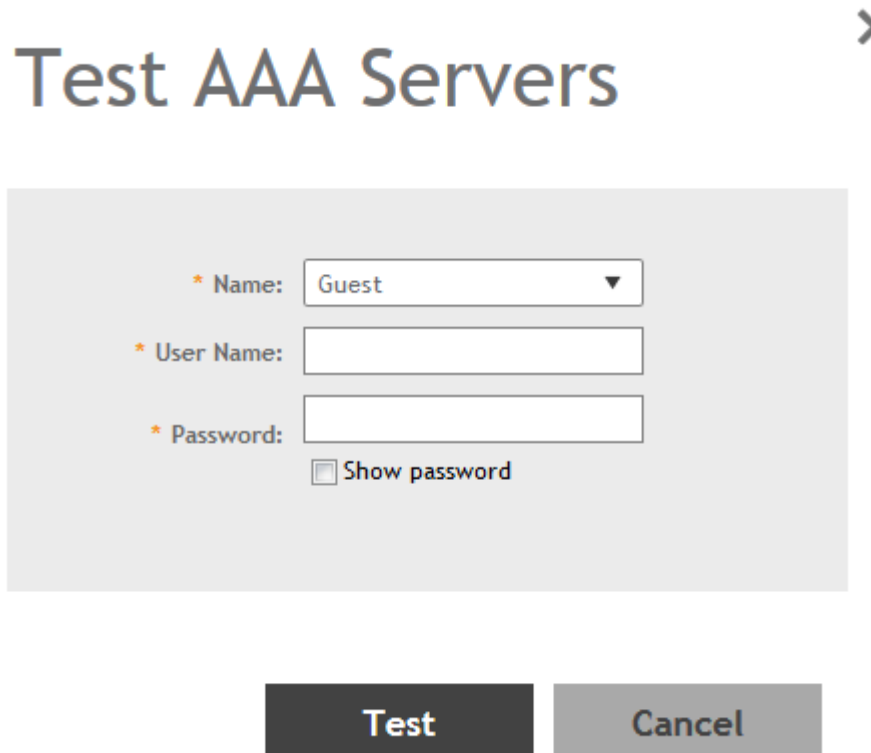
## Testing AAA Servers

To ensure that the controller administrators will be able to authenticate successfully with the RADIUS server type that you selected, Ruckus strongly recommends testing the AAA server after you set it up.

1. Go to **Services & Profiles > Authentication**.
2. Select the **Proxy (SZ Authenticator)** tab, and then select the zone for which you want to test the AAA server.
3. Click **Test AAA**.

The **Test AAA Server** page appears.

**FIGURE 149** Testing an AAA Server



Test AAA Servers

\* Name: Guest ▼

\* User Name:

\* Password:

☐ Show password

Test Cancel

4. Configure the following:
  - a. Name: Select one of the AAA servers that you previously created.
  - b. User Name: Type an existing user name on the AAA server that you selected.
  - c. Password: Type the password for the user name you specified.

5. Click **Test**.

If the controller was able to connect to the authentication server and retrieve the configured groups/attributes, the information appears at the bottom of the page. If the test was unsuccessful, there are two possible results (other than success) that will be displayed to inform you if you have entered information incorrectly: **Admin invalid** or **User name or password invalid**. These results can be used to troubleshoot the reasons for failure to authenticate administrators with an AAA server through the controller.

## Authentication Support Matrix

It is important to understand the compatibility between AAA servers and different WLANs.

### Proxy Mode

In proxy mode, authentication requests are set through the controller.

**TABLE 33 Proxy Mode Compatibility**

Authentication Source	802.1X	HS 2.0 Secure	Web Auth	Hotspot/WISPr
Local Database	No	Yes	No	Yes
IDM-Provisioned Local DB	Yes	Yes	NA	NA
Active Directory	No*	No	Yes	Yes
RADIUS	Yes	Yes	Yes	Yes
LDAP	Yes	No	Yes	Yes

**NOTE**

To support 802.1X with Active Directory, an external RADIUS server (such as NPS) must be used.

**NOTE**

IDM Provisioned username (also called local cache credential) is relevant only in secure access after Onboarding.

**NOTE**

802.1X (MSCHAPv2 via built-in RADIUS using AD-NPS), WebAuth, and WISPr support AD authentication from SmartZone release in 3.2.

**NOTE**

802.1X, WebAuth, and WISPr support LDAP authentication from SmartZone release in 3.2. For 802.1X authentication, the user password must be in clear text in the LDAP database.

### Non-proxy Mode

In the Non-proxy mode, authentication requests are sent directly by AP and not through the controller. The local database is stored on the controller, therefore, authentication sources such as local database and IDM-provisioned local databases are not supported.

**TABLE 34 Non-proxy Mode Compatibility**

Authentication Source	802.1X	Zero-IT Onboard	HS 2.0 Onboard	HS 2.0 Secure	Web Auth	Hotspot/WISPr
Active Directory	No	No*	No*	No	Yes	No
RADIUS	Yes	No*	No*	No	Yes	Yes*
LDAP	No	No*	No*	No	Yes	No

(\*) From the configuration it may seem like non-proxy RADIUS is supported in WISPr, but the call flow goes through the controller.

#### Profile Configuration

The following table details proxy and non-proxy AAA server configurations against various platforms.

**TABLE 35 Profile Configuration**

Feature	SZ100	vSZ-E	vSZ-H	Description
Per-Zone ProxyAAA Profiles	NA	NA	NA	Ability to configure a ProxyAAA profile in a specific zone
Global ProxyAAA Profiles	Yes	Yes	Yes	Ability to configure a ProxyAAA profile globally and then use it across zones
Per-Zone NonProxy AAA Profiles	NA	NA	Yes	Ability to configure a NonProxyAAA profile in a specific zone
Global NonProxy AAA Profiles	Yes	Yes	No	Ability to configure a NonProxy AAA profile globally and then use it across zones

#### Dynamic Policy Assignment (Proxy Authentication Types)

The following table details dynamic policy assignments across authentication types.

**TABLE 36 Dynamic Policy Assignment (Proxy)**

Feature	802.1X	Zero-IT Onboard	HS 2.0 Onboard	HS 2.0 Secure	Web Auth	Hotspot/WISPr	MAC Auth	Description
Dynamic Role Assignment	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Ability to assign a user to a particular local Role via a group/role attribute from RADIUS, AD, LDAP. From SmartZone 3.4, Role can contain UTP. Therefore, , when you assign a role, you also get the ACL and Rate Limiting policies.
Dynamic VLAN / VLAN Pool	Yes	NA	NA	NA	No	No	Yes	Ability to assign a user to a VLAN through a VLAN attribute from RADIUS, AD, LDAP. From SmartZone release 3.5, you

**TABLE 36 Dynamic Policy Assignment (Proxy) (continued)**

Feature	802.1X	Zero-IT Onboard	HS 2.0 Onboard	HS 2.0 Secure	Web Auth	Hotspot/WISPr	MAC Auth	Description
								can also assign VLANs and VLAN pools based on the user role.
Dynamic UTP	Yes				Yes	Yes	Yes	Ability to assign a user to a UTP through an attribute from an authentication source.
Dynamic ACL	Yes	Yes	Yes	No	Yes	Yes	Yes	Ability to assign a specific ACL to a user through an attribute from RADIUS, AD, LDAP.
Dynamic Rate Limit	Yes	Yes	Yes			Yes	Yes	Ability to assign a specific Rate Limit to a user through an attribute from RADIUS, AD, LDAP.

**NOTE**

In dynamic ACL and Rate limit, since ACL and rate limit are associated with a UTP, assigning a UTP also assigns an ACL or rate limit.

Dynamic Policy Assignment (Non-Proxy Authentication Types)

The following table details dynamic policy assignments across authentication types.

**TABLE 37 Dynamic Policy Assignment (Non-Proxy)**

Feature	802.1X	HS 2.0 Secure	Web Auth	Description
Dynamic Role Assignment	No			Ability to assign a user to a local Role through a group/role attribute from the authentication source.
Dynamic VLAN / VLAN Pool				Ability to assign a user to a VLAN through a VLAN attribute from the authentication source.
Dynamic UTP				Ability to assign a user to a UTP through an attribute from the authentication source.  <b>NOTE</b> From SmartZone release 3.4, UTP contains ACL and rate limit.

**TABLE 37 Dynamic Policy Assignment (Non-Proxy) (continued)**

Feature	802.1X	HS 2.0 Secure	Web Auth	Description
Dynamic ACL				<p>Ability to assign a specific ACL to a user through an attribute from the authentication source.</p> <p><b>NOTE</b> ACLs are a part of a UTP. If you configure a UTP without a rate limit, you effectively only have an ACL.</p>
Dynamic Rate Limit				<p>Ability to assign a specific Rate Limit to a user through an attribute from the authentication source.</p> <p><b>NOTE</b> Rate limiting is also a part of a UTP. If you configure a UTP without ACL, you effectively only have a rate limiting policy.</p>

#### Other Authentication Features

The following table details authentication support for various authentication features.

**TABLE 38 Authentication Features**

Feature	Supported	Description
Test AAA - RADIUS	Yes	Ability to test a specific username/password against a configured RADIUS serve.
Test AAA - Active Directory	Yes	Ability to test a specific username/password against a configured AD serve.
Test AAA - LDAP	Yes	<p>Ability to test a specific username/password against a configured LDAP serve.</p> <p><b>NOTE</b> Only Non-Proxy LDAP is supported at the Zone Level.</p>
Test AAA - Return a Role	Yes - supported by RADIUS, AD and LDAP	Ability to return a role assignment when testing a AAA server.
RADIUS CoA - Change Role		Ability to change a user's Role through a Change of Authorization (CoA).
RADIUS CoA - Change VLAN		Ability to change a user's VLAN through a Change of Authorization (CoA).
RADIUS CoA - Change ACL		Ability to change a user's ACL through a Change of Authorization (CoA).
RADIUS CoA - Change Rate Limit		Ability to change a user's rate limit through a Change of Authorization (CoA).
RADIUS CoA - Change Authorization		Ability to authorize or deauthorize a user through a Change of Authorization (CoA).



## PAP/CHAP Support

The following table details PAP and CHAP support for various authentication features.

**TABLE 39** PAP/CHAP Support

Feature	802.1X	Web Auth	Hotspot/ WISPr	MAC Auth	Notes
Proxy-Mode					
Active Directory	Yes	Yes*	Yes	No	PAP / CHAP is supported for Web Authentication and HotSpot/WISPr. NPS interface (AD) is required for WebAuthenticaiton (CHAP) and 802.1X (MSCHAPv2).
RADIUS	Yes	Yes*	Yes	Yes	
LDAP	Yes	Yes*	Yes	No	PAP / CHAP is supported for Web Authentication and HotSpot/WISPr
LDAP-TLS	Yes	Yes*	Yes	No	This support is available from SmartZone version 3.5.
Active Directory (TLS)	Yes	Yes*	Yes	No	This support is available from SmartZone version 3.5. NPS interface (AD) is required for WebAuthenticaiton (CHAP) and 802.1X (MSCHAPv2).
Non-proxy Mode					
Active Directory	No	Yes*	Yes	No	
RADIUS	Yes	Yes*	Yes	Yes	
LDAP	No	Yes*	Yes	No	

**NOTE**

(\*) This is an AP CLI setting:

```
set aaa auth-method pap|chap
```

It is a global setting for all WebAuth WLANs on the AP. The default is CHAP.

## Accounting

### Creating Non-Proxy Accounting AAA Servers for Standby Cluster

A non proxy AAA server is used when the APs connect to the external AAA server directly.

1. Go to **Services & Profiles > Accounting**.

2. Select the **Non-Proxy** tab, and then select the zone for which you want to create the AAA server.
3. Click **Create**.

The **Create AAA Server** page appears.

**FIGURE 150** Creating an AAA Server



The image shows a 'Create AAA Server' dialog box with a close button (X) in the top right corner. The dialog is divided into three sections: 'General Options', 'Primary Server', and 'Primary Server (Standby Cluster)'. The 'General Options' section includes fields for 'Name' and 'Description', a 'Type' dropdown set to 'RADIUS Accounting', and two toggle switches: 'ClusterRedundancy' (set to OFF) and 'Backup RADIUS' (set to OFF). The 'Primary Server' section includes fields for 'IP Address', 'Port' (set to 1813), 'Shared Secret', and 'Confirm Secret'. The 'Primary Server (Standby Cluster)' section is currently empty. At the bottom are 'OK' and 'Cancel' buttons.

**Create AAA Server**

**General Options**

Name:

Description:

Type: ☒ RADIUS Accounting

ClusterRedundancy: ☐ OFF Enable Service for Standby Cluster

Backup RADIUS: ☐ OFF Enable Secondary Server

**Primary Server**

IP Address:

Port:

Shared Secret:

Confirm Secret:

**Primary Server (Standby Cluster)**

OK Cancel

4. Configure the following:
  - a. General Options
    - Name: Type a name for the AAA server that you are creating.
    - Description: Type a short description of the AAA server.
    - Type: Select **RADIUS Accounting**.
    - Cluster Redundancy: Click the **Enable Service for Standby Cluster** option to enable cluster redundancy.
    - Backup RADIUS (appears if you clicked RADIUS above): Click the **Enable Secondary Server** check box if a secondary RADIUS server exists on the network.
  - b. If you selected RADIUS, configure the following options in the Primary and Secondary server sections:
    - IP Address: Type the IP address of the AAA server.
    - Port: Type the port number of the AAA server. The default RADIUS server port number is 1813.
    - Shared Secret: Type the AAA shared secret.
    - Confirm Secret: Retype the shared secret to confirm.
5. Click **OK**.

You have completed creating a Non-proxy Accounting AAA server.

For information on how to test this server, see [Testing AAA Servers](#) on page 296

#### NOTE

You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Non-Proxy** tab.

## Creating Proxy Accounting AAA Servers for Standby Cluster

A proxy AAA server is used when APs send authentication/accounting messages to the controller and the controller forwards these messages to an external AAA server.

1. Go to **Services & Profiles > Accounting**.
2. Select the **Proxy** tab, and then select the zone for which you want to create the AAA server.

3. Click **Create**.

The **Create Accounting Service** page appears.

**FIGURE 151** Creating an Accounting Service

**Create Accounting Service**

Name:

Description:

Service Protocol: ☒ RADIUS Accounting

ClusterRedundancy: ☐ OFF Enable Service for Standby Cluster

**RADIUS Service Options**

Primary Server

IP Address:

Port:

Shared Secret:

Confirm Secret:

Primary Server (Standby Cluster)

OK Cancel

4. Configure the following:
  - a. Name: Type a name for the authentication service that you are adding.
  - b. Description: Type a description for the authentication service.
  - c. Service Protocol: By default, the RADIUS Accounting selected. For more information, see [RADIUS Service Options](#) on page 294.
  - d. Cluster Redundancy: Click the **Enable Service for Standby Cluster** option to enable cluster redundancy.
5. Click **OK**.

You have completed creating a Proxy Accounting AAA server.

For information on how to test this server, see [Testing AAA Servers](#) on page 296

**NOTE**

You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Proxy** tab.

# Classifying Rogue Policy

You can create rogue classification policy with rules at the zone-level. This helps in automatic classification behavior when a specific-rogue detection criteria are met.

To create a rogue classification policy:

1. Go to **Services & Profiles > WIPS**.
2. In the **Policy** tab, select the zone for which you want to create the policy.
3. Click **Create**.

The Create Rogue Classification Policy page appears.

4. Configure the following:
  - a) **Name** : Type a name for the policy.
  - b) **Description** : Type a description for the policy.
  - c) **Rogue Classification Rules** : Create the policy rule by configuring the following :
    - Click **Create**. The Create Rogue Classification Rules page appears.
    - Configure the following options:
      - **Name**: Enter a name for the rule.
      - **Rule Type**: Select one of following the rule type for the Classification:
        - › Low RSSI
        - › MAC OUI
        - › MAC Spoofing
        - › Same Network
        - › SSID
        - › SSID Spoofing
      - **Signal Threshold**: Enter the RSSI threshold in dBm. This option is available only for **Low RSSI** rule type.
      - **MAC OUI**: Enter the first three octets of the MAC. For example, 11:22:33. This option is available only for **MAC OUI** rule type.
      - **SSID**: Enter the SSID. This option is available only for **SSID** rule type.
      - **Classification**: Select one of the following action for the selected **Rule Type**:
        - › Ignore
        - › Know
        - › Malicious
        - › Rogue
    - Click **OK**. You have created a Rogue classification rule.

5. Click **OK**.

You have created Rogue classification policy.

## NOTE

You can also edit or delete a Rogue classification policy. To do so, select the rogue classification from the list and click **Configure** or **Delete** as required.

## NOTE

To prioritize the classification rule, select the rule from the list and click **UP** or **Down** to position the rule.

# Bonjour

Bonjour is Apple's implementation of a zero-configuration networking protocol for Apple devices over IP.

Bonjour allows OS X and iOS devices to locate other devices such as printers, file servers and other clients on the same broadcast domain and use the services offered without any network configuration required.

Multicast applications such as Bonjour require special consideration when being deployed over wireless networks. Bonjour only works within a single broadcast domain, which is usually a small area. This is by design to prevent flooding a large network with multicast traffic. However, in some situations, a user may want to offer Bonjour services from one VLAN to another.

SmartZone provides two features for controlling how and where Bonjour services are available to clients:

- [Bonjour Gateway](#) on page 306: Bridge Bonjour services from one VLAN to another.
- [Bonjour Fencing](#) on page 308: Limit the range in physical space at which Bonjour services are available to clients.

## Bonjour Gateway

Bonjour Gateway policies enable APs to provide Bonjour services across VLANs.

The controller's Bonjour gateway feature provides an mDNS proxy service configurable from the web interface to allow administrators to specify which types of Bonjour services can be accessed from/to which VLANs.

In order for the Bonjour Gateway to function, the following network configuration requirements must be met:

- The target networks must be segmented into VLANs.
- VLANs must be mapped to different SSIDs.
- The controller must be connected to a VLAN trunk port.

Additionally, if the VLANs to be bridged by the gateway are on separate subnets, the network has to be configured to route traffic between them.

### *Creating Bonjour Gateway Policies*

A Bonjour Gateway policy must be created for an AP zone before the policy can be deployed to an AP or group of APs.

To create a Bonjour Gateway policy:

1. Go to **Services & Profiles > Bonjour**.
2. Select the **Gateway** tab, and then select the zone for which you want to create the policy.

3. Click **Create**.

The **Create Bonjour Policy** page appears.

**FIGURE 152** Creating a Bonjour Gateway Policy

## Create Bonjour Policy

4. Configure the following:

- a. **Name:** Type a name for the policy.
- b. **Description:** Type a description for the policy.
- c. **Rules:** Create the policy rule by configuring the following
  1. Click **Create**. The **Create Bonjour Policy Rule** page appears.
  2. Configure the following options:
    - **Bridge Service:** Select the Bonjour service from the list.
    - **From VLAN:** Select the VLAN from which the Bonjour service will be advertised.
    - **To VLAN:** Select the VLAN to which the service should be made available.
    - **Notes:** Add optional notes for this rule.

3. Click **OK**.

You have created a Bonjour policy rule.

- d. Click **OK**.

You have created a Bonjour policy with a rule.

### NOTE

You can also edit, clone and delete the policy by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Gateway** tab.

You may now continue to apply this Bonjour gateway policy to an AP or AP group, as described in [Applying a Bonjour Gateway Policy to an AP or AP Group](#) on page 308.

## Applying a Bonjour Gateway Policy to an AP or AP Group

Once a Bonjour Gateway policy is created, you can select which AP (or AP group) will serve as the gateway for Bonjour services.

To apply a Bonjour Gateway policy to an AP or AP group:

1. Go to **Access Points > Access Points**.
2. Select the AP or AP group that you want to configure from the zone in which the AP/group exists.
3. Click **Configure**.
4. Expand the **Advanced Options**, and in **Bonjour Gateway**, enable the check box next to **Enable as Bonjour Gateway with policy**, and select the policy you created from the drop-down list.
5. Click **OK** to save your changes.

## Bonjour Fencing

Bonjour Fencing provides a mechanism to limit the scope of Bonjour (mDNS) service discovery in the physical/spatial domain.

While Bonjour Fencing is related to Bonjour Gateway, they are two separate features designed for different purposes. Bonjour Gateway bridges mDNS services across VLANs, and is useful because mDNS/Bonjour packets are restricted to the same VLAN/subnet and cannot be routed to other VLANs. Bonjour Fencing limits the range of Bonjour service discovery within physical space, which is useful because logical network boundaries (e.g. VLANs) do not always correlate well to physical boundaries within a building/floor.

The following considerations should be taken into account before deploying Bonjour fencing policies:

- Bonjour fencing is not supported on Mesh APs.
- Switch interfaces to which APs are connected must be configured in VLAN trunk mode so that Bonjour traffic gets forwarded across VLANs based on Bonjour Gateway Policies.
- Bonjour fencing is implemented at the AP, not at the controller.
- Fencing policies can be applied on a zone level only, and cannot be configured per AP group.
- In order for a wired fencing policy to work properly, wireless fencing for the same mDNS service should also be enabled. If wired fencing is enabled but wireless is disabled, APs that are not the "closest AP" will be unable to determine whether the source of the mDNS advertisement was wired or wireless.
- Bonjour fencing will work for local breakout scenarios, but will not work for tunnel based configuration. (This feature is supported only for SZ300 controllers)

## Creating Bonjour Fencing Policies

Bonjour Fencing policies can be created and applied to a zone at the same time using the Fencing tab on the **Services and Profiles > Bonjour** screen.

To create a Bonjour Fencing policy:

1. Go to **Services & Profiles > Bonjour**.
2. Select the **Fencing** tab, and then select the zone for which you want to create the policy.



3. Click **Create**.  
The **Create Bonjour Fencing Policy** page appears.

**FIGURE 153** Creating a Bonjour Fencing Policy

Create Bonjour Fencing Policy

Name:

Description:

Fencing Rule

Create

Configure

Delete

Device Type	Device MAC	Closest AP	Service	Fencing Range	Description
Wireless	N/A	N/A	Other (asdsds)	Same AP	N/A

Custom Services Mapping

Create

Configure

Delete

Service	Custom String List
AirPlay	"_sdsd_tcp."

OK

Cancel

4. Configure the following:
  - a. **Name:** Type a name for the policy.
  - b. **Description:** Type a description for the policy.
  - c. **Fencing Rule:** Create the policy rule by configuring the following:

FIGURE 154 Fencing Rule

**Fencing Rule**

\* [?] Device Type: Wired

\* Closest AP: No data available

\* Service: Other

\* Custom Service Name:

\* Fencing Range: Same AP

Description:

\* [?] Device MAC: \* MAC + Add X Cancel Delete

MAC

OK Cancel

1. Click **Create**. The **Fencing Rule** page appears.
2. Configure the following options:
  - **Device Type:** Select the Wireless or Wired network connection method for the device advertising Bonjour services.
  - **Closest AP:** Select the closest AP to create a physical anchor point for fencing, and the closest AP is auto-detected for wireless devices, based on the AP association.
  - **Service:** Select one of the Bonjour services from the drop-down list. In 5.0, two new services, **Chromecast** and **Other** are added. Chromecast behaves as the standard service. If you select **Other**, the **Custom Service Name** appears which is used for service mapping. Regardless of the device type selected only three services for Other option.
  - **Custom Service Name:** For mapping services other than the custom services regardless of the Device Type. You can create a maximum of three service with the same custom service name.
  - **Fencing Range:** Select the fencing range to be the Same AP or 1-Hop AP Neighbors.
  - **Description:** Specify any notes you may need to refer.

- **Device MAC:** Specify the MAC address of the device advertising Bonjour services. This option is available only for Wired Device Type. It supports up to four wired MAC addresses.
3. Click **OK** to save the rule.

You have created a Bonjour fencing rule. Each policy can contain up to 32 rules.

- d. **Custom Services Mapping:** Create services mapping by configuring the following:

**FIGURE 155** Create Custom Services Mapping

1. Click **Create**. The **Custom Services Mapping** page appears.
2. Configure the following options:
  - **Service:** Select one of the Bonjour services from the drop-down list.  
Per Service, has only one entry for Custom Services Mapping. For example: AppleTV and Chromecast, have only one entry with custom strings (three at most) and Other type has one entry with custom strings (three at most) because it allows three Other rules.
  - **Custom Service Name:** Lists all **Custom Service Name** with Service type **Other** created in the Fencing Rule. This field is available if you select the **Other** option from the **Service** drop-down.
  - **Custom String List:** Enter the name in the format **\_xxxx.\_xtcp** or **\_xxxx.\_xudp**. You can create only one entry for Custom service and three entries for other service.
3. Click **OK** to save the services mapping policy.

You have created a Custom Services Mapping policy.

- e. Click **OK** to save the policy.

You have created a Bonjour fencing policy.

**NOTE**

You can also edit or delete the policy by selecting the options **Configure** or **Delete** respectively, from the **Fencing** tab.

## Working with Tunnels and Ports

### Creating a Ruckus GRE Profile

You can configure the Ruckus GRE tunnel profile of the controller to manage AP traffic.

**NOTE**

You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Ruckus GRE** tab.

1. Go to **Services & Profiles > Tunnels and Ports**.
2. Select the **Ruckus GRE** tab, and then select the zone for which you want to create the profile.
3. Click **Create**.

The **Create Ruckus GRE Profile** page appears.

**FIGURE 156** Creating a Ruckus GRE Profile

Create Ruckus GRE Profile

\* Name:

Description:

\* Ruckus Tunnel Mode:  Support for APs behind NAT.

\* Tunnel Encryption: ☒ Disable ☐ AES 128 ☐ AES 256

\* Tunnel MTU: ☒ Auto ☐ Manual  bytes (IPv4:850-1500, IPv6:1384-1500)

OK Cancel

4. Type a name for the profile in the **Name** box.
5. Type a description for the profile in the **Description** box.
6. Select a protocol to use for tunneling WLAN traffic back to the controller by choosing one of the following after clicking the drop-down arrow in the **Ruckus Tunnel Model** box:
  - **GRE + UDP**—Select this option to allow APs behind a NAT server to tunnel WLAN traffic back to the controller.
  - **GRE**—Select this option to tunnel regular WLAN traffic only.

7. To allow managed APs to decrypt 802.11 packets, and then use an AES encrypted tunnel to send them to the controller. select one of the **Tunnel Encryption** options:
  - Click the **Disable** radio button to allow only the management traffic to be encrypted; data traffic is unencrypted. This is the default option.
  - Click the **AES 128** radio button to use an AES 128-byte encryption tunnel.
  - Click the **AES 256** radio button to use an AES 256-byte encryption tunnel.

MTU is the size of the largest protocol data unit that can be passed on the controller network.
8. Set the maximum transmission unit (MTU) for the tunnel using one of the **Tunnel MTU** options:
  - Click the **Auto** radio button. This is the default option.
  - Click the **Manual** radio button and enter the maximum number of bytes. For IPv4 traffic the range is from 850-1500 bytes, for IPv6 traffic the range is from 1384 to 1500 bytes.

MTU is the size of the largest protocol data unit that can be passed on the controller network.
9. Click **OK**.

You have created the Ruckus GRE profile.

## Creating a Soft GRE Profile

You can configure the Soft GRE tunnel profile of the controller to manage AP traffic.

1. Select **Services & Profiles > Tunnels and Ports**.
2. Select **Soft GRE** and click **Create**.

The **Create Soft GRE Profile** page is displayed.

**FIGURE 157** Creating a Soft GRE Profile

**Edit SoftGRE Profile [l2gre\_dev]**

Name:

Description:

Gateway IP Mode: ☒ IPv4 ☐ IPv6

Primary Gateway Address:

Secondary Gateway Address:

Gateway Path MTU: ☒ Auto ☐ Manual  bytes (IPv4:850-1500, IPv6:1384-1500)

ICMP Keep Alive Period (secs):  (1-180)

ICMP Keep Alive Retry:  (2-70)

Force Disassociate Client: ☒ Disassociate client when AP fails over to another tunnel.

**OK** **Cancel**

3. Enter profile name and description.
4. Under **Gateway IP Mode**, select **IPv4** or **IPv4** addressing.
5. In the **Primary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the primary gateway server.
6. In the **Secondary Gateway Address** field, enter the IP address or fully-qualified domain name (FQDN) of the secondary gateway server.

**NOTE**

If the controller is unable to reach the primary gateway server, the controller automatically attempts to reach the secondary gateway address at the IP address specified by you.

7. For **Gateway Path MTU**, set the maximum transmission unit (MTU) for the gateway path.  
Select one of the following options:
  - **Auto**: This is the default option.
  - **Manual**: The transmission range is from 850 through 1500 bytes.
8. In the **ICMP Keep Alive Period** field, enter the time interval in seconds.

**NOTE**

Time interval is the time taken by the APs to send a keepalive message to an active third party WLAN gateway. The range is from 1 through 180 seconds. The default value is 10 seconds.

9. In the **ICMP Keep Alive Retry** field, enter the number of keepalive attempts.

**NOTE**

Keepalive attempts are the number of attempts that the APs wait for a response from the active third party WLAN gateway before failing over to the standby WLAN gateway. The range is from 2 through 10 attempts. The default value is 5 attempts.

10. Under **Force Disassociate Client**, enable **Disassociate client when AP fails over to another tunnel** if you want to disassociate the client when AP fails over to another tunnel.

**NOTE**

You must select this option if you have enabled **AAA Affinity** while configuring the zone.

11. Click **OK**.

You have created the Soft GRE profile.

**NOTE**

You can also edit, clone, and delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Soft GRE** tab.

## Creating an IPsec Profile

1. Go to **Services & Profiles > Tunnels and Ports**.
2. Select the **IPsec** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

The **Create IPsec Profile** page appears.

**FIGURE 158** Creating an IPsec Profile

## Create IPsec profile

**General Options** ▼

\* Name:

Description:

Security Gateway:

**Authentication** ▶

**Security Association** ▶

**OK** **Cancel**

4. Configure the following:
  - a. Name: Type a name for the profile.
  - b. Description: Type a description for the profile.
  - c. Security Gateway: Type the IP address or FQDN of the IPsec server. If you use the IP address, the IP address format that you must enter will depend on the IP mode that is configured on the controller.
  - d. IP Mode: Select IPv4 or IPv6 addressing modes.

**NOTE**

This option is only applicable to SZ300.

- e. Authentication: Select Preshared Key to use PSK for authentication or Certificate to use an X.509 certificate on the certificate authority (CA) or registration authority (RA) server. The controller uses the CMPv2 protocol to obtain the signed certificate from the CA/RA server.

If you selected Preshared Key, type the PSK in this box. The PSK must be eight to 128 ASCII characters in length.

- f. Security Association
  1. IKE Proposal Type: Select Default to use the default Internet Key Exchange (IKE) security association (SA) proposal type or select Specific to manually configure the IKE SA proposal. If you clicked Specific, you will need to configure the following settings:
    - Encryption Algorithm: Options include 3DES, AES128, AES192, and AES256.
    - Integrity Algorithm: Options include MD5, SHA1, AES-XCBC, SHA256, SHA384, and SHA512.
    - Pseudo-Random Function: Options include Use integrity ALG, PRF-MD5, PRF-SHA1, PRF-AES-XCBC, PRF-AES-CMAC, PRF-SHA256, and PRF-SHA384.
    - DH Group: Options for Diffie-Hellman groups for IKE include modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, and modp8192.
  2. ESP Proposal Type: Click Default to use the default Encapsulating Security Payload (ESP) SA proposal type or click Specific to manually configure the ESP proposal. If you clicked Specific, you will need to configure the following settings:
    - Encryption Algorithm: Options include 3DES, AES128, AES192, AES256, and NONE.
    - Integrity Algorithm: Options include MD5, SHA1, AES-XCBC, SHA256, SHA384, and SHA512.
    - DH Group: Options for Diffie-Hellman groups for ESP include None, modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, and modp8192.
- g. Rekey Options
  1. Internet Key Exchange: To set time interval at which the IKE key renews, select a time unit (day, hour, or minute) from the drop-down list, and then type a number in the box. To disable IKE rekey, select the Disable check box. SmartZone 100/Virtual SmartZone Essentials for Release 3.4 Administrator Guide 82 Configuring the Wireless Network Configuring Access Points.
  2. Encapsulating Security Payload: To set time interval at which the ESP key renews, select a time unit (day, hour, or minute) from the drop-down list, and then type a number in the box. To disable ESP rekey, select the Disable check box.
- h. Certificate Management Protocol
  1. DHCP Option 43 Sub Code for CA/RA Address: Set the DHCP Option 43 subcode that will be used to discover the address of the CA/RA server on the network. The default subcode is 8.
  2. CA/RA Address: Type the IP address or FQDN of the CA/RA server. If you use the IP address, the IP address format that you must enter will depend on the IP mode that is configured on the controller.



3. Server Path: Type the path to the X.509 certificate on the CA/RA server.
4. DHCP Option 43 Sub Code for Subject Name of CA/RA: Set the DHCP Option 43 subcode that will be used to discover the subject name of the CA/RA server on the network. The default subcode is 5.
5. Subject Name of CA/RA: Type an ASCII string that represents the subject name of the CA/RA server.
- i. Advanced Options
  1. DHCP Option 43 Sub Code for Security Gateway: Set the DHCP Option 43 subcode that will be used to discover the address of the security gateway on the network. The default subcode is 7.
  2. Retry Limit: Set the number of times that the controller will attempt to discover the address of the security gateway. The default retry count is 5. Accepted values are 0 (disable) to 16.
  3. Replay Window: Set the ESP replay window (in packets). The default size is 32 packets. Accepted values are 0 (disable) to 32 packets.
  4. IP Compression: To enable IP Payload Compression Protocol (IPComp) compression before encryption, click Enable. The default value is Disable.
  5. Force NAT-T: To enforce UDP encapsulation of ESP packets, click Enable. The default value is Disable.
  6. Dead Peer Detection: By default, the IKE protocol runs a health check with remote peer to ensure that it is alive. To disable this health check, click Disable.
  7. NAT-T Keep Alive Interval: To set the keep alive interval (in seconds) for NAT traversal, type a value in the box. The default keep alive interval is 20 seconds. Accepted values are 1 to 65536. To disable the keep alive interval, click Disable.
  8. FailOver Options: To configure the failover settings when APs are unable to connect, configure the following:
  9. Retry Period: Set the number of days (minimum 3 days) during which APs will keep attempting to connect. To keep try indefinitely, select the **Forever** check box.
  10. Retry Interval: Set the interval (in minutes) between each retry attempt. The default retry interval is 1 minute. Accepted values are from 1 to 30 minutes.
  11. Retry Mode: If you want APs to fall back to the specified primary security gateway, click Revertive. If you want APs to maintain connectivity with the security gateway to which they are currently connected, click **Non-revertive**.
- j. Click **OK**.

You have created the IPsec GRE profile.

#### NOTE

You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **IPsec GRE** tab.

## Creating an Ethernet Port Profile

An Ethernet port profile contains settings that define how an AP will handle VLAN packets when its port is designated as either trunk, access, or general port. By default, three Ethernet port profiles exist: General Port, Access Port and Trunk Port.

1. Go to **Services & Profiles > Tunnels and Ports**.
2. Select the **Ethernet Port** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

The Create Ethernet Port page appears.

**FIGURE 159** Creating a Ethernet Port Profile

## Create Ethernet Port

**General Options** ▶

**Ethernet Port Usage** ▶

**Authentication Options** ▼

802.1X: ☒ Enable 802.1X authentication

\* 802.1X Role: Port-based Authentica ▼

☒ Enable client visibility regardless 802.1X authentication

**Authentication & Accounting Service** ▼

\* Authentication Server: ☐ Use the controller as proxy Select an authenticat ▼

Accounting Server: ☐ Use the controller as proxy Disable ▼

☐ Enable MAC authentication bypass (Use device MAC address as username and password)

**OK** **Cancel**

4. Configure the following:

a. General Options

1. Name: Type a name for the Ethernet port profile that you are creating.
2. Description: Type a short description about the profile.
3. Type: The Ethernet port type defines how the AP will manage VLAN frames. You can set Ethernet ports on an AP to one of the following types: Trunk Port, Access Port or General Port.

By selecting the appropriate port type, authentication method, and 802.1X Role, administrator can configure the ethernet ports to be used for the wired client. Up to 16 devices can be configured to connect to one ethernet port. After configuring the ports, the wired clients and their stats are displayed in the **Clients > Wired Clients** page. You can also delete a wired client from this page.

b. Ethernet Port Usage

1. Access Network: Select this check box to enable tunneling on the Ethernet port.
2. VLAN Untag ID: Type the ID of the native VLAN (typically, 1), which is the VLAN into which untagged ingress packets are placed upon arrival. If your network uses a different VLAN as the native VLAN, configure the AP Trunk port's VLAN Untag ID with the native VLAN used throughout your network.
3. VLAN Members: Type the VLAN IDs that you want to use to tag WLAN traffic that will use this profile. You can type a single VLAN ID or a VLAN ID range (or a combination of both). The valid VLAN ID range is 1 to 4094.
4. Enable Dynamic VLAN: Select this check box if you want the controller to assign VLAN IDs on a per-user basis. Before enabling dynamic VLAN, you need to define on the RADIUS server the VLAN IDs that you want to assign to users.

**NOTE**

This option is only available when Type is set to Access Port and 802.1X authentication is set to MAC-based Authenticator.

**NOTE**

If you enable client visibility, a maximum of 16 clients can be connected to a port regardless of the 802.1X authentication. The same limitation applies when 802.1X authentication is enabled and client visibility is not enabled.

- c. Guest VLAN: If you want to assign a device that fails authentication to still be able to access the Internet but to internal network resources, select this check box.

**NOTE**

This check box only appear when the Enable Dynamic VLAN check box is selected.

- d. Anti-spoofing: Prevents attacks on genuine clients from rogue clients that could lead to service disruption, data loss and so on. This is achieved by matching the MAC address or IP address (IPv4) of the client with the address in the Ruckus database. If the addresses do not match, the packet is dropped. These checks are also performed on ingress data packets to catch spoofed data packets early.
- ARP request rate limit: type the packets to be reviewed for ARP (Address Resolution Protocol) attacks, per minute. In ARP attacks, a rouge clients send messages to a genuine client to establish connection over the network.
  - DHCP request rate limit: type the packets to be reviewed for DHCP pool exhaustion, per minute. When rouge clients send a DHCP request with a spoofed address, an IP address from the DHCP pool is assigned to it. If this happens repeatedly, the IP addresses in the DHCP pool are exhausted, and genuine clients might miss out on obtaining the IP addresses.

**NOTE**

When you enable anti-spoofing, an ARP request and DHCP request rate limiter is automatically enabled with default values (in ppm or packets per minute) which are applied per client; Implying that each client connected to an interface enabled with anti-spoofing is allowed to send a maximum of "X" ARP/DHCP request ppm. The value "X" is configured on the interface that the client is connected to.

**NOTE**

The Force-DHCP option will be enabled by default when the Anti-spoofing feature is enabled, and it cannot be changed after Anti-Spoofing is enabled.

e. Authentication Options

1. 802.1X: Select this check box to enable 802.1X authentication.
2. Enable client visibility regardless of 802.1X authentication: select this check box to bypass 802.1X authentication for client visibility.

**NOTE**

You can view statistical information about wired clients even without enabling 802.1X authentication.

3. 802.1X Role: Select the authenticator role from the drop-down menu. Options include Supplicant, MAC-based Authenticator and Port-based Authenticator. When you select Supplicant, you can customize the username and password to authenticate as a supplicant role or use the credentials of the AP MAC address. When you select Port-based Authenticator, only a single MAC host must be authenticated for all hosts to be granted access to the network. If you select MAC-based Authenticator, each MAC address host is individually authenticated. Each newly-learned MAC address triggers an EAPOL request-identify frame.

f. Authentication and Accounting Services

1. Authentication Server: Select the check-box and a controller from the drop-down menu to use the controller as a proxy authentication server.
2. Accounting Server: Select the check-box and a controller from the drop-down menu to use the controller as a proxy accounting server.
3. Enable MAC authentication bypass: Select this check-box if you want to use the device MAC address as access credentials (username and password).

g. RADIUS Options

1. NAS ID: Set the NAS ID for the AP to communicate with the RADIUS server. Options include using the AP MAC address or any User-defined address.
2. Delimiter: If AP MAC is selected to configure the NAS ID, then you can choose between Dash or Colon as delimiters to separate.

h. Click **OK**.

You have created the Ethernet Port profile.

**NOTE**

You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Ethernet Port** tab.

## Creating a Tunnel DiffServ Profile

If you need to configure the type of traffic (ToS) bit settings for the access side traffic from Ruckus APs, follow these steps to create a Differentiated Services (DiffServ) profile. This profile can only be applied to Ruckus GRE and SoftGRE traffic.

1. Go to **Services & Profiles > Tunnels and Ports**.
2. Select the **DiffServ** tab, and then select the zone for which you want to create the profile.
3. Click **Create**.

The **Create Tunnel DiffServ Profile** page appears.

**FIGURE 160** Creating a Tunnel DiffServ Profile

### Create Tunnel DiffServ profile

\* Name:

Description:

\* Tunnel DiffServ: ☐ Set Uplink DiffServ

☐ Set Downlink DiffServ  Downlink DiffServ only applies to RuckusGRE tunnel

Preserved DiffServ:   Up to 8 preserved DiffServ allowed

4. Configure the following:
  - a. Name: Type a name for the DiffServ profile that you are creating.
  - b. Description: Type a brief description for the DiffServ profile.
  - c. Tunnel DiffServ: configure the following options.
    1. Set Uplink DiffServ: Select the check box if you want to set the Differentiated Services field for uplink user traffic from Ruckus APs towards either the controller or a third SmartCell Gateway 200/Virtual SmartZone High-Scale for Release 3.4.1 Administrator Guide 92 Managing Ruckus AP Zones Creating a DiffServ Profile party gateway via SoftGRE. Configure the desired value to be set by the Ruckus AP.
    2. Set Downlink DiffServ: Select the check box if you want to set the Differentiated Services field for downlink user traffic from the controller towards the AP, and then configure the desired value to be set by the Ruckus AP.
  - d. Preserved DiffServ: Configure up to eight (8) entries in the preserved DiffServ list. The Preserved DiffServ list allows the preservation of values that have been already marked in incoming packets either in uplink or downlink traffic.
  - e. Click **OK**.

You have created the DiffServ profile.

**NOTE**

You can also edit, clone and delete the profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **DiffServ** tab.

## Split Tunnel Profile

A Split Tunnel Profile can be created to manage corporate and local traffic by sending only corporate traffic to the controller. A split tunnel ensures that local traffic does not incur the overhead of the round trip to the controller, which decreases traffic on the WAN link and minimizes latency for local application traffic. Using a split tunnel, a remote user is associated with a single SSID (rather than multiple SSIDs) to access corporate resources, such as a mail server and local resources (for example, a local printer).

### *Split Tunnel Profile Limitations*

Before enabling the Split Tunnel Profile, consider the following limitations:

- Split Tunnel Profile does not support a zone where mesh-enabled APs are present.
- Split Tunnel Profile and Express Wi-Fi are not supported together on the same WLAN.
- For both features to work properly, the configured IP rules for a split tunnel and a walled garden must be different.
- Split Tunnel Profile does not support DHCP/NAT.
- Split Tunnel Profile does not support wired clients.
- The limitations applicable to DHCP/NAT also apply to Split Tunnel Profile.

### *Creating a Split Tunnel Profile*

Complete the following steps to configure a split tunnel profile:

1. Select **Services & Profiles > Tunnels and Ports**.
2. Select the **Split Tunnel** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.  
The **Create Split Tunnel Profile** window is displayed.

**FIGURE 161** Creating a Split Tunnel Profile

4. Enter the split tunnel profile information:

**NOTE**

RuckusGRE or SoftGRE must be enabled on the WLAN before mapping it to a Split Tunnel Profile.

- a. In the **Name** field, type a name for the split tunnel profile.
- b. In the **Description** field, type a short description for the split tunnel profile.
- c. In the **IP Address** field, enter the destination IP address.
- d. In the **Subnet Mask** field, enter the destination IP subnet mask.
- e. Click **Add** to add the destination IP details.
- f. Click **OK**.

**NOTE**

You can also edit, clone or delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively from the **Split Tunnel** tab.

## Enabling Tunnel Encryption

You can use the tunnel encryption feature to encrypt data for a private network, through a public network. This feature is available in vSZ-H and vSZ-E.

1. Go to **Services & Profiles > Tunnels and Ports**.

2. Select the **Tunnel Encryption(DP)** tab, and then select the zone for which you want to create the profile.  
The **Tunnel Encryption (DP)** page appears.

**FIGURE 162** Tunnel Encryption (DP)



3. Select the **Enable Tunnel Encryption** check-box.
4. Click **OK**.

You have successfully enabled tunnel encryption.

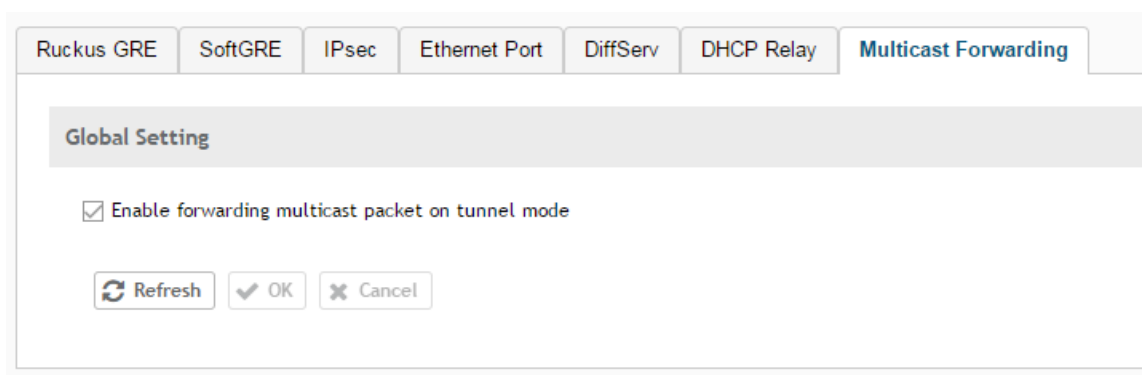
## Forwarding Multicast Packets

In multicast forwarding, a group of hosts are typically grouped under a multicast IP address. Data can then be transmitted from the source to the IP address which in turn transmits data to the various hosts assigned to the multicast IP. This is a point-to-multipoint data transmission. You can forward multicast traffic on vDP by enabling the multicast forwarding feature in tunnel mode, but you must make sure that the hosts are connected to the vDP and that Ruckus GRE tunnel is configured in the vDP. This feature is only available in SZ100.

1. Go to **Services & Profiles > Tunnels and Ports**.
2. Select the **Multicast Forwarding** tab.

The **Multicast Forwarding** page appears.

**FIGURE 163** Forwarding Multicast Packets



3. In **Global Setting**, select the **Enable forwarding multicast packet on tunnel mode** check-box.
4. Click **OK**. The form is submitted and multicast packet forwarding is enabled.

You have successfully enabled multicast forwarding for data packets in the tunnel mode.



# DHCP/NAT

DHCP/NAT functionality on SZ-managed APs and DPs (data planes) allows customers to reduce costs and complexity by removing the need for DHCP server/NAT router to provide IP addresses to clients. For data traffic aggregation and services delivery you can choose appropriate user profile for DHCP and NAT services on vSZ-D.

## AP-based DHCP/NAT

In highly distributed environments, particularly those with only a few APs per site, the ability for an AP or a set of APs to provide DHCP/NAT support to local client devices simplifies deployment by providing all-in-one functionality on the AP, which eliminates the need for a separate router and DHCP server for each site. It also eases site management by providing central control and monitoring of the distributed APs and their clients.

Three general DHCP scenarios are supported:

- SMB Single AP: DHCP is running on a single AP only. This AP also functions as the Gateway AP.
- SMB Multiple APs (<12): DHCP service is running on all APs, among which two of the APs will be Gateway APs. These two Gateway APs will provide the IP addresses as well as Internet connectivity to the clients via NAT.
- Enterprise (>12): For Enterprise sites, an additional on site vSZ-D will be deployed at the remote site which will assume the responsibilities of performing DHCP/NAT functions. Therefore, DHCP/NAT service will not be running on any APs (they will serve clients only), while the DHCP/NAT services are provided by the onsite vSZ-D.

## Profile-based DHCP

The DHCP Server is designed in-line in the data plane and provides extreme scale in terms of IP address assignment to clients. This feature is especially useful in high density and dynamic deployments like stadiums, train stations where large number of clients continuously move in & out of WiFi coverage. The DHCP server in the network needs to scale to meet these challenging requirements. The DHCP server on the vSZ-D provides high scale IP assignment and management with minimal impact on forwarding latency. The DHCP server allows IP assignment only when a DHCP license assignment policy is created for a specific vSZ-D. A maximum of 101k IP assignments are allowed for each vSZ-D. Additional IP assignments requires additional licensing.

### NOTE

DHCP Server/NAT function if enabled is supported only for wireless client IPv4 address assignment.

## Profile-based NAT

With NAT service enabled, all the WiFi client traffic is NATed by the vSZ-D before being forwarded to the core network. The NAT license assignment policy for specific vSZ-D must be created. Each vSZ-D supports up to 2000K NAT ports (traffic sessions) and 128 public IP addresses for NAT. This feature essentially reduces the network overhead significantly since this reduces the MAC-table considerations on the UP-stream switches significantly. Again, very useful in high density deployments.

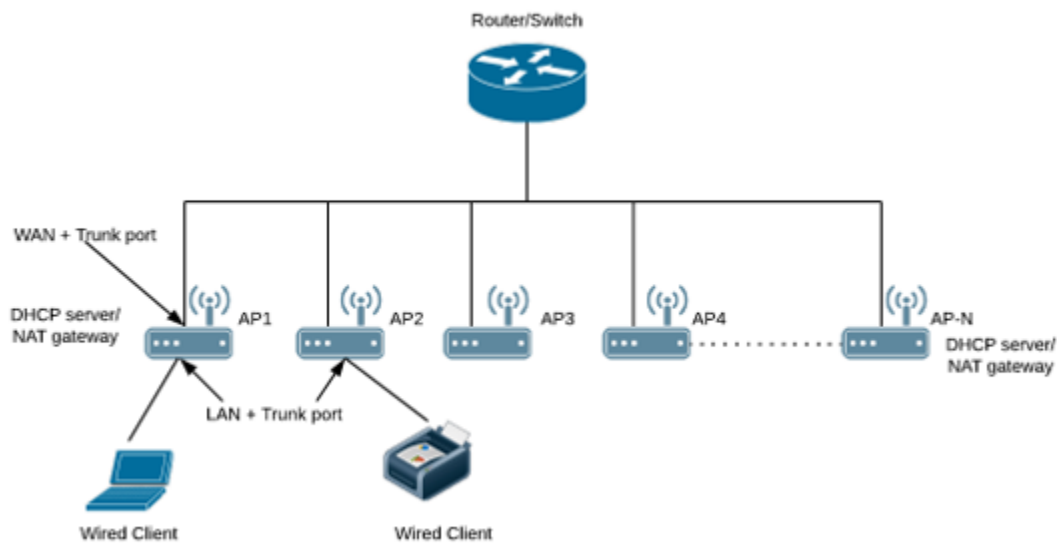
## Network Topology

There are three types of network topologies for APs. They are:

### Single AP Topology

All the APs in the zone get their IP from the WAN router and provides the DHCP/NAT service. If H510/H320 is configured as GAP by manual port selection, then LAN1 and LAN2 configuration will be pushed to eth1 and eth2 ports of H510/H320 APs instead of eth0 and eth1 ports.

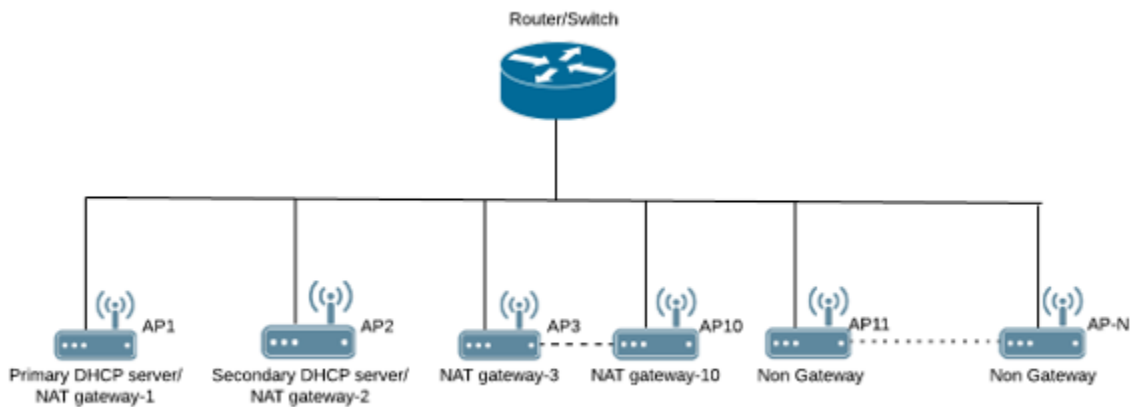
**FIGURE 164** Single AP Topology



### Multiple AP (Flat Network) Topology

All the APs in the zone get their IP from the WAN router and designated APs provide the DHCP/NAT service. A maximum of two APs be can select for DHCP service (Primary and Secondary) and ten APs for NAT Gateway.

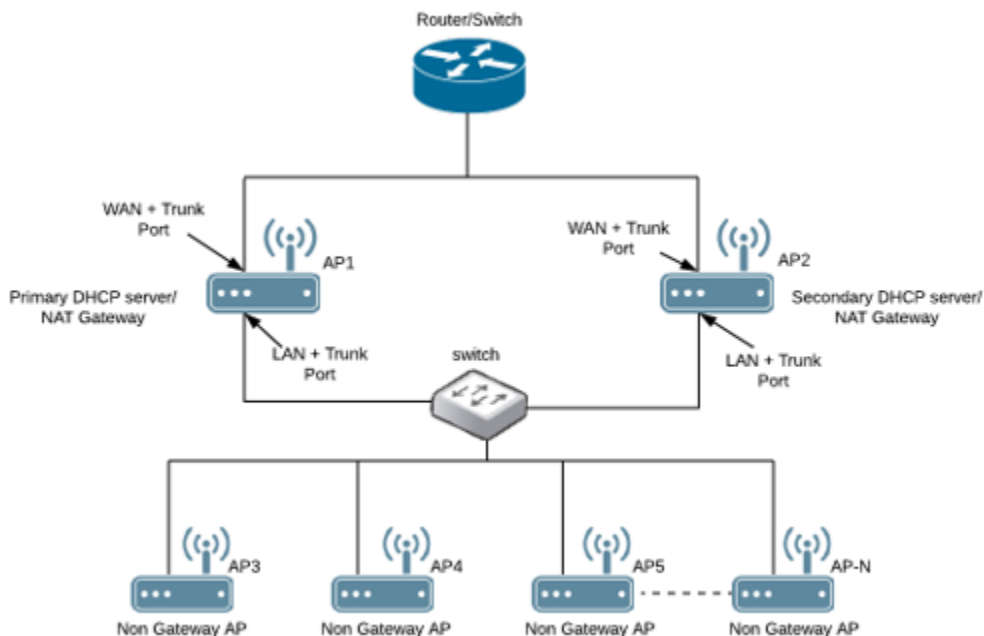
**FIGURE 165** Multiple AP (Flat Network) Topology



### Hierarchical AP Topology

Designated APs provide the DHCP/NAT service. Gateway APs get the IP address from the WAN router and non-gateway APs get the IP from the Gateway APs. If H510/H320 is configured as GAP by manual port selection, then LAN1 and LAN2 configuration will be pushed to eth1 and eth2 ports of H510/H320 APs instead of eth0 and eth1 ports. In order to configure eth0 ports of H510/H320 the user needs to configure LAN5/LAN3 Ports respectively for the H510/H320 APs.

**FIGURE 166** Hierarchical AP Topology



## Hierarchical Network Topology

Hierarchical network topology along with DHCP/NAT runs on single and multiple APs. The Gateway APs can directly be connected to the service providers' route/switch and can get the public IPs. The NGAPs can get the private IPs from the GAP through the DHCP/NAT service. Wired client such as printers and laptops can be directly connected to the LAN port of the GAP or WAN ports of Non-GAPs and hence can be operational without the use of external DHCP/NAT. Basic Mesh Topology is supported where the GAP is root the AP and all other NGAP can be the Mesh APs.

The Dynamic WAN Port Detection (DWPD) algorithm detects the WAN port among eth0/eth1/eth2 of the APs and marks only one port of AP as LAN. LAN port selection is based on the availability of Port. If a port is GRE enabled then it will not be modified to LAN. Remaining other available port will be marked as LAN.

Expected behavior in case of a three port AP are as follows:

- Eth0: connected to WAN  
Final result after DWPD: Eth0=WAN, ETH1=LAN, ETH2=WAN
- Eth1: connected to WAN  
Final result after DWPD: Eth0=LAN, ETH1=WAN, ETH2=WAN
- Eth2: connected to WAN  
Final result after DWPD: Eth0=LAN, ETH1=WAN, ETH2=WAN

Using DWPD you can do plug-n-play without worrying about the configuration of WAN or LAN ports. Wired client connectivity for each AP where all the APs in the zone run DHCP/NAT service. All ethernet ports can be configured as LAN port and wired clients can be used to connect. LAN port profile enables APs with multiple ethernet ports to be configured as LAN ports. Hence there is no need for a separate switch if the multi-port AP is GAP and all the required wired and NGAP AP can be connected directly to the number of available ethernet ports.

## Configuring AP-based DHCP Service Settings

Using DHCP service settings, you can configure an AP to assign private IP addresses to Wi-Fi clients without the need for a separate DHCP server (router).

Before you configure the DHCP Service, consider the following:

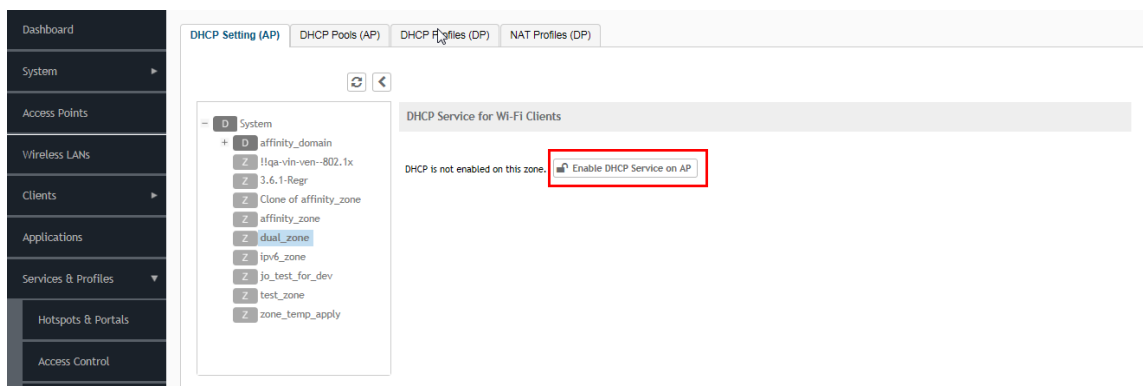
- There must be minimum one and maximum two APs acting as Gateway AP (GAP). There is no count in the number of APs acting as Non-Gateway APs (NGAP).
- For a single non-Gateway AP (NGAP) you can connect eth0 of NGAP to LAN port (usually eth1) of GAP.
- For more than one NGAP you need a minimum L2 switch to connect the LAN port of GAP to all the NGAPs
- For APs having more than 2 ethernet ports, all the eth ports except the WAN backhaul (usually eth0) can be configured as LAN ports. In such case a separate switch may not be required.

To configure DHCP services:

1. Go to **Services & Profiles > DHCP & NAT**.
2. Select the **DHCP Setting (AP)** tab, and select the zone for which you want to configure the settings.

3. Select a Zone from the zone list on the left side of the screen, and click **Enable DHCP Service on AP**.

**FIGURE 167** Enabling DHCP Service



4. Click **Edit DHCP Service on AP**. The **DHCP Settings** wizard appears.

**FIGURE 168** DHCP Settings wizard

## DHCP Settings

Base Settings

Select Pools

Select APs

Review

\* DHCP Configuration:

☒ Enable on Each AP

☐ Enable on Multiple APs

☐ Enable on Hierarchical APs

Each AP in this zone is running it's own DHCP server instance. Typically configured when APs are at different sites and roaming is not required.

Designated APs in this zone are running the DHCP Server instance. Typically configured when multiple APs are at the same site and roaming across APs is needed.

Designated APs in this zone are running the DHCP Server instance. The DHCP server APs connected to the WAN, the rest of APs get their Private IP address from a local IP Pool with VLAN ID 1 from the DHCP Server AP.

\* DHCP AP Port Selection:

☒ Dynamic WAN Port Detection

☐ WAN Port Selection

The port which is reachable to SZ will be marked as WAN and rest of the ports will be marked as LAN.

Assign the specific port to WAN or LAN. This setting will override your original port configuration of Zone. If the option is changed from WAN to LAN then there could be loss of connectivity with SZ.

LAN1:

Default Trunk Port(WAN)

LAN2:

Default Trunk Port(LAN)

Next

Cancel

330

Ruckus SmartZone 100 and Virtual SmartZone-Essentials Administrator Guide, 5.1  
Part Number: 800-71965-001 Rev E

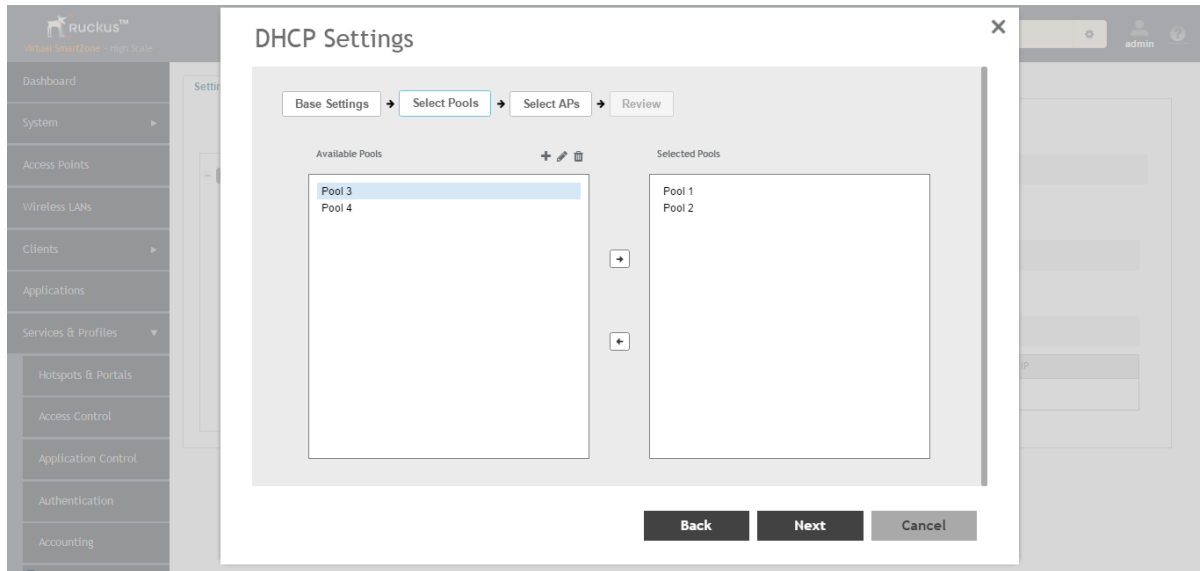
5. On the first page of the wizard (**Base Settings**), configure the **DHCP Configuration** as follows:
  - **Enable on Each AP:** Each AP in this zone runs its own DHCP server instance. This option is typically used when APs are at different sites and roaming is not required. Now configure the **DHCP AP Port Selection** by selecting one of the following:
    - **Dynamic WAN Port Detection**—WAN is automatically identified by default and the LAN will be selected.
    - **WAN Port Selection**—Manually assign port to WAN and LAN. This setting overrides the original port configuration of a zone. Select the **LAN1** and **LAN2** options from the drop-down.
  - **Enable on Multiple APs:** Designate which APs will provide DHCP/NAT service. This option is typically used when multiple APs are at the same site and roaming is required. This option also allows you to choose whether to automatically or manually specify which APs will provide DHCP service. Now configure the **DHCP AP Port Selection** by selecting one of the following:
    - **Dynamic WAN Port Detection**—WAN is automatically identified by default and the LAN will be selected.
    - **WAN Port Selection**—Manually assign port to WAN and LAN. This setting overrides the original port configuration of a zone. Select the **LAN1** and **LAN2** options from the drop-down.
  - **Enable on Hierarchical APs**— Designate which APs will provide DHCP/NAT service. The DHCP Server AP connect to the WAN and the other AP get its private IP address from the local IP pool with VLAN ID 1 from the DHCP Server AP. Now configure the **DHCP AP Port Selection** by selecting one of the following:
    - **Dynamic WAN Port Detection**—WAN is automatically identified by default and the LAN will be selected.
    - **WAN Port Selection**—Manually assign port to WAN and LAN. This setting overrides the original port configuration of a zone. Select the **LAN1** and **LAN2** options from the drop-down.

- On the next wizard screen, (**Select Pools**), select up to four DHCP pools from which to assign client IP addresses.

**NOTE**

For the **Enable on Hierarchial APs** DHCP configuration, one of the pools must be VLAN ID 1.

**FIGURE 169** Selecting Pools



**NOTE**

If you have not already created DHCP pools, you can do so from within the wizard. Click the Plus (+) icon and configure the IP address pools as described in the [Creating an AP DHCP Pool](#) on page 334.

- Click **Next**. The **Select APs** screen appears.

**NOTE**

If you selected **Auto Select AP** on the first wizard screen, this configuration screen will be skipped.



8. On the **Select APs** wizard screen, select the AP(s) that you want to set as the primary and secondary DHCP servers (if you previously selected **Enable on Multiple APs**).

**NOTE**

For the **Enable on Hierarchial APs** DHCP configuration, you can select only two APs.

**FIGURE 170** Selecting APs

## DHCP Settings

Base Settings → Select Profiles → **Select APs** → Review

Available APs

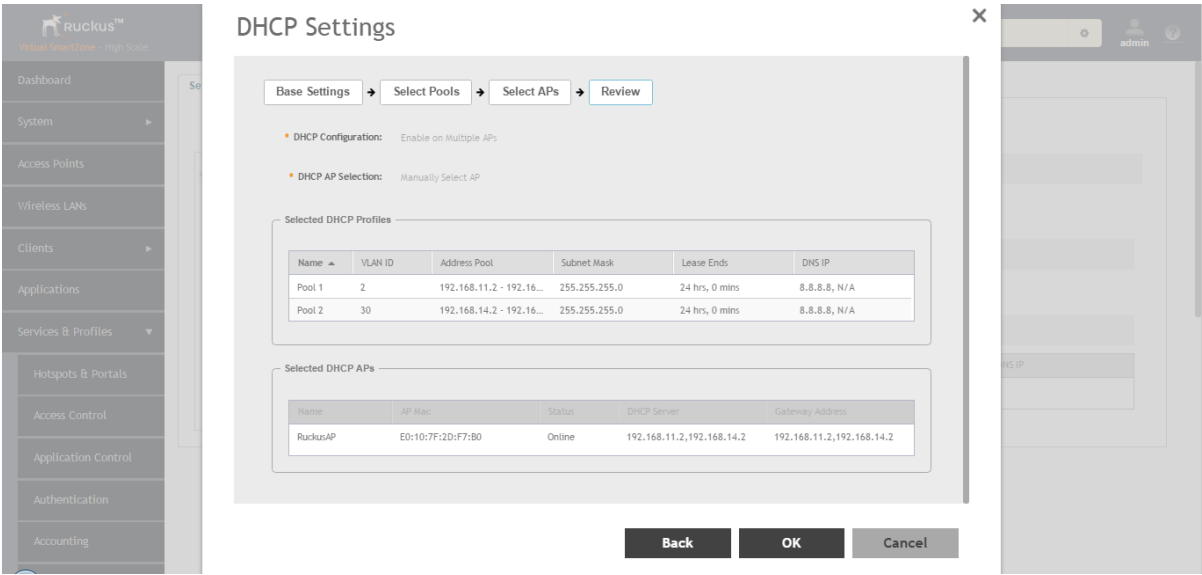
Selected APs

	Primary Server	Backup Server	Gateway
AP02	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
RuckusAP	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>

9. Click **Next**.

10. On the **Review** screen, review your settings to make sure everything is correct. Once you are satisfied with your settings, click **OK** to confirm.

**FIGURE 171** Review DHCP settings



You have configured the DHCP server settings and applied them to an AP (or multiple APs). These APs will now provide DHCP/NAT functionality and assign IP addresses to wireless clients from the DHCP address pools you specified.

## Creating an AP DHCP Pool

Creating a DHCP pool is necessary for assigning IP addresses to clients. Multiple address pools can be created and assigned to APs that are running DHCP services. Then, when a client connects to the wireless network, it will be assigned an address from the DHCP pool(s) you specified.

To configure a DHCP pool for IP address allocation:

1. Go to **Services & Profiles > DHCP & NAT**.
2. Select the **DHCP Pools (AP)** tab, and then select the zone for which you want to create the pool.

3. Click **Create**.  
The **Create DHCP Pool** page appears.

**FIGURE 172** Creating a DHCP Pool

X

## Create DHCP Pool

\* Name:

Description:

\* VLAN ID:  (Range: 2~4094)

\* Subnet / Network Address:

\* Subnet Mask:

\* Pool Start Address:

\* [?] Pool End Address:

Primary DNS IP:

Secondary DNS IP:

\* Lease Time:  Hours  Minutes

OK
Cancel

4. Configure the following:
  - **Name:** Type a name for the pool you want to create.
  - **Description:** Type a description of the pool you want to create.
  - **VLAN ID:** Type the vlan id for the pool.
  - **Subnet Network Address:** Type the IP subnet network address (e.g., 192.168.0.0).
  - **Subnet Mask:** Type the subnet mask address (e.g., 255.255.255.0).
  - **Pool Start Address:** Type the first IP address to be allocated to clients from the pool (e.g., 192.168.0.1).
  - **Pool End Address:** Type the last IP address to be allocated to clients from the pool (e.g., 192.168.0.253).
  - **Primary DNS IP:** Type the primary DNS server IP address.
  - **Secondary DNS IP:** Type the secondary DNS server IP address.
  - **Lease Time:** Enter the IP address lease time, after which clients will have to renew or request new IP addresses.
5. Click **OK**.

You have created a DHCP address pool. You can now apply this address pool to a DHCP service, as described in [Configuring AP-based DHCP Service Settings](#) on page 328.

**NOTE**

You can also edit, clone and delete the address pool by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Pool** tab.

## Creating Profile-based DHCP

DHCP profile can be applied to vDP and the vDP server can assign IP to the UE based on the profile rule. Different pools with the same subnet can be created without overlapping IP range.

**NOTE**

DHCP supports only access-side network.

- [Configuring Global Settings](#) on page 336
- [Configuring DHCP Pool Settings](#) on page 337

## Configuring Global Settings

To configure Profile-based DHCP Global settings:

1. Go to **Services & Profiles > DHCP & NAT > DHCP Profiles (DP)**.
2. Click **Create**, the Create DHCP Profile page appears.

3. Configure the following:
  - **Profile Name:** Type a name for the DHCP profile you want to create. AP supports 32 bytes.
  - **Description:** Type a description of the settings you want to create.
  - **Domain Name:** Type the domain name address.
  - **Primary DNS Server:** Type the primary domain name server address.
  - **Secondary DNS Server:** Type the secondary domain name server address.
  - **Lease Time:** Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
  - **DHCP Option43 Space:** Click **Create**, the Create DHCP Option43 Space form appears. Configure the following:
    - **Space Name:** Type a name for Option43 space.
    - **Description:** Type a description for Option43 space.
    - Under **Option43 Sub Option**, click **Create** and configure the following:
      - › **Sub Option Name:** Type a sub option name.
      - › **Type:** Select the required option from the drop-down.
      - › **Code:** Enter a code. Range: 1 through 254.
      - › **Click OK**, you have created Option43 Sub Option.
    - Click **OK**, you have created Option43 Space.
  - **Hosts:** Click **Create**, the Create Host Configuration form appears. Configure the following:
    - **General Options**
      - › **Host:** Type a name for the host settings that you want to create.
      - › **Description:** Type a description for the host settings that you want to create.
    - **Policy Options**
      - › **Mac Address:** Type the MAC address of the DHCP host.
    - **Assigning Options**
      - › **Broadcast Address:** Type the broadcast IP address.
      - › **Fixed Address:** Type the fixed IP address of the host.
      - › **Gateway:** Type the gateway IP address.
      - › **DNS Server:** Type the IP address of the DNS server.
      - › **Domain Name:** Type the domain name.
      - › **Host Name:** Type the host name.
      - › **Lease Time:** Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
    - Click **OK**, you have created DHCP Host configuration.
4. Click **OK**.

You have created DHCP Profile settings.

## Configuring DHCP Pool Settings

To configure DHCP pool settings:

1. Go to **Services & Profiles > DHCP & NAT > DHCP Profiles (DP)**.
2. Select the DHCP profile from the list for which you want to configure the pool settings.
3. Select the **Pools** tab page.

4. Click **Create** and configure the following:
  - **General Options**
    - **Pool Name:** Type a name for the pool configuration.
    - **Description:** Type a description for the pool configuration.
  - **Policy Options**
    - **VLAN Range:** Type the VLAN range. Range: 1, 2 through 4095. For example: 1, 2 or 2-3.
    - **QinQ VLAN:** Select the check box and update the following:
      - › **QinQ SVLAN Range:** Type a SVLAN range. Range: 2 through 4095.
      - › **QinQ CVLAN Range:** Type a CVLAN range. Range: 2 through 4095.
  - **Assigning Options**
    - **Subnet:** Type the IP address.
    - **Subnet Mask:** Type the network address.
    - **Broadcast Address:** Type the broadcast IP address.
    - **Pool Range:** Type the address range for the pool.
    - **Exclude Pool:** Type the address range that must be excluded.
    - **Primary Gateway:** Type the primary gateway IP address.
    - **Secondary Gateway:** Type the secondary gateway IP address.
    - **Primary DNS Server:** Type the IP address of the primary DNS server.
    - **Secondary DNS Server:** Type the IP address of the secondary DNS server.
    - **Domain Name:** Type the domain name.
    - **Host Name:** Type the host name.
    - **Lease Time:** Type the duration in Hours, Minutes and Seconds. Range: 1 through 86400 seconds.
  - **Option43 Value**
    - Click **Create**, the Create Option43 value form appears. Configure the following:
      - › Choose the **Space** Name or click **Create** to configure Option 43 Space Name.
      - › Enter a **Description**.
    - Click **OK**, you have configured Option43 value.
5. Click **OK**.

You have created DHCP pool configuration.

## Creating Profile-based NAT

A NAT Profile could be applied to a vDP. The NAT server settings work independently. You must configure the following settings to create a NAT profile:

### NOTE

NAT does not support multiple public subnet/VLAN.

- [Configuring NAT Global Settings](#) on page 339
- [Configuring NAT Pool Setting](#) on page 339

## Configuring NAT Global Settings

To create a NAT global setting:

1. Go to **Services & Profiles > DHCP & NAT > NAT Profiles (DP)**.
2. Click **Create**, the Create NAT Profile page appears.
3. Configure the following:
  - **Profile Name:** Type a name for the NAT profile that you want to create. AP supports 32 bytes.
  - **Description:** Type a description for the profile that you want to create.
  - **Subnet:** Type the IP address.
  - **Prefix:** Type a prefix value. Maximum range: 31.
  - **Public VLAN:** Type the VLAN range. Range: 2 through 4095.
  - **Gateway:** Type the gateway IP address.
4. Click **OK**.

You have created a NAT Profile.

## Configuring NAT Pool Setting

To configure NAT pool settings

1. Go to **Services & Profiles > DHCP & NAT > NAT Profiles (DP)**.
2. Select the NAT profile from the list and click the **Pools** tab.
3. Click **Create**, the Create Pool Configuration page appears.
4. Configure the following:
  - **General Options**
    - **Pool Name:** Type a name for the NAT pool settings that you want to create.
    - **Description:** Type a description for the pool settings that you want to create.
  - **Policy Options**
    - **Private VLAN Range:** Type the VLAN range and click **Add**. Range: 1 through 4095. For example: 1 or 1-2.
    - **Private QinQ VLAN Range:** Type **SVLAN** range, **CVLAN** range and click **Add**. Range: 2 through 4095. For example: 2 or 2-3.
  - **Translation Options**
    - **Port Range:** Type the port range. Range: 10000 through 65534. For example: 10000-20000.
    - **Public Address Range:** Type the public address range.

Note: This public address must not be duplicated with the other public address in the same subnet, which includes applied NAT Profile and vSZ-D's Access and Core Interface Address.
5. Click **OK**.

You have created a NAT pool setting.

## Configuring DHCP/NAT with Mesh Options

To configure DHCP/NAT with mesh option:

1. Enable Mesh Option in zone level. Refer to **Mesh Options** in [Creating an AP Zone](#) on page 62.

2. From the Access Points Page, select the AP to be assigned as the Root AP > Click the **Configure** button > select Mesh specific options > and select Root AP mode.
3. Multiple address pools can be created and assigned to APs that are running DHCP services. Refer, [Creating an AP DHCP Pool](#) on page 334.
4. From the Services & Profiles page, enable DHCP on the zone. Edit the DHCP Service on the AP by selecting the required VLANs and APs as Gateway APs. Refer, [Configuring AP-based DHCP Service Settings](#) on page 328.

## 3rd Party Service

SZ supports integration for Ekahau and Aeroscout/Stanley tags and information is forwarded to the Ekahau and Aeroscout servers respectively. This enhancement provides support for Real-Time Location Service (RTLS) tags without requiring them to be associated to the network.

### Enabling Ekahau and Aeroscout/Stanley RTLS Tags

To locate tag positions, SZ allows you to enable Ekahau and Aeroscout/Stanley RTLS tags.

1. Select **Services and Profiles** > **3rd Party Service**.
2. Click the **RTLS** tab.

The **RTLS** page is displayed.

**FIGURE 173** Enabling Ekahau and Aeroscout/Stanley Tag Support

**Real Time Location Service**

**Ekahau Tag Support:** ☒ ON

\* **Server IP Address:**

\* **Server Port:**

**Stanley Tag Support:** ☒ ON

3. Select a zone to enable the tags.
4. To enable Ekahau tag support, set **Ekahau Tag Support** to **ON**.



5. In the **Server IP Address** field, enter the IP address of the server to which data is forwarded.
6. In the **Server Port** field, enter the server port to which data is forwarded.
7. To enable Stanley tag support, set **Stanley Tag Support** to **ON**.
8. Click **OK**.



# Working with Reports

---

- Types of Reports.....343
- Managing Report Generation..... 344
- Rogue Access Points..... 346
- Historical Client Stats..... 348
- Ruckus AP Tunnel Stats..... 349

## Types of Reports

The controller provides the following types of reports:

### Client Number Report

The **Client Number** report shows a historical view of the maximum and minimum number of clients connect to the system. Client number can be shown in different time intervals for a specified duration. The report can be generated based on a specific AP, SSID, or radio.

### Client Number vs Airtime Report

The **Client Number vs Airtime** report shows a historical view of the average number of clients connected to the system and the corresponding airtime (TX, RX, Busy). Client number and airtime can be shown in different time intervals for a specified duration. The report can be generated based on a specific AP or radio.

### Continuously Disconnected APs Report

The Continuously Disconnected APs report shows a list of access points disconnected within the specified time range.

### Failed Client Associations Report

The **Failed Client Associations** report shows a historical view of the number of failed client associations. Failed client associations can be shown in different time intervals for a specified duration. The report can be generated based on a specific AP, SSID, or radio.

### New Client Associations Report

The **New Client Associations** report shows a historical view of the number of new client associations. New client Associations can be shown in different time intervals for a specified duration. The report can be generated based on a specific AP, SSID, or radio.

## System Resource Utilization Report

The **System Resource Utilization** report shows a historical view of the CPU and memory usage of the system. The CPU and memory usage can be shown in different time intervals for a specific duration. The report can be generated based on specific plane.

## TX/RX Bytes Report

The **TX/RX Bytes** report shows a historical view of the transmitted (TX) and received (RX) bytes of the system. The transmitted and received bytes can be shown in different time intervals for a specified duration. The report can be generated based on a specific AP, SSID or radio.

# Managing Report Generation

You can create and manage reports.

### NOTE

Global filter settings does not apply to the Reports feature.

As reports are segmented by individual administrators, each administrator's reports are unique and applies only to them.

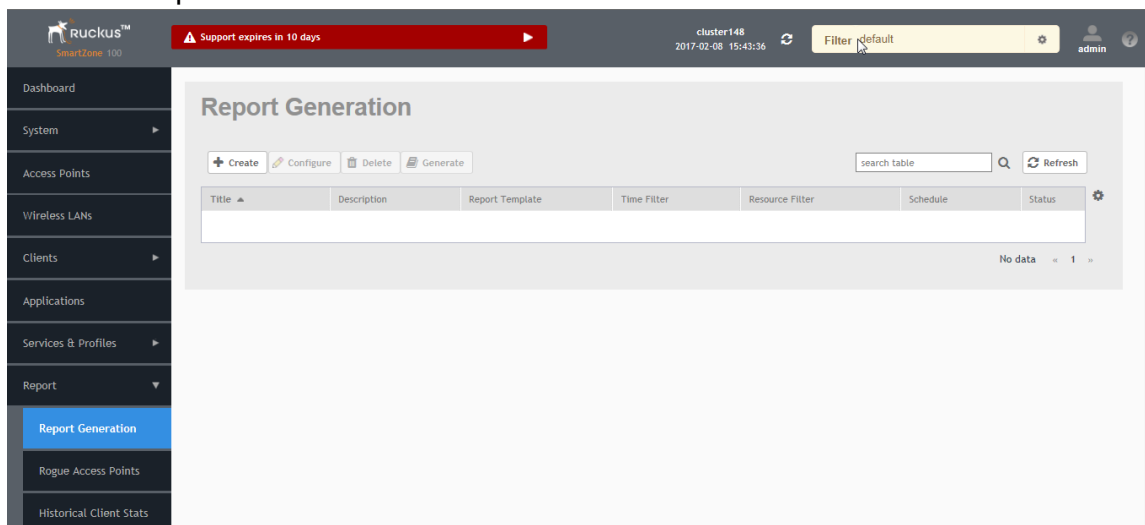
## Creating Reports

You can create reports to obtain a historical view of the maximum and minimum number of clients connect to the system, to view client number at different time intervals and to view the traffic statistics of switches.

To create a new report:

1. From the left pane, select **Report > Report Generation**. [Figure 174](#) appears.

**FIGURE 174** Report Generation Screen



2. Click **Create**, [Figure 175](#) appears.

**FIGURE 175** Create Reports Screen  
Create Report

The screenshot shows the 'Create Report' screen. At the top, there's a 'General Information' tab. Below it, the 'Management Domain' is set to 'Administration Domain'. There are input fields for 'Title' and 'Description'. The 'Report Category' is set to 'Switch' (radio button). The 'Report Type' is set to 'Switch Traffic Statistics' (dropdown menu). Below this, a descriptive text states: 'This report shows the traffic statistics of switches, including the packets of InFrame, OutFrame, InMulticast, OutMulticast, InBroadcast, and OutBroadcast. The numbers of InError, OutError, CrcError, and InDiscard are also included.' The 'Output Format' is set to 'PDF' (radio button). At the bottom, there's a 'Resource Filter Criteria' section.

3. Enter the required parameters as explained in [Table 40](#).
4. Click **OK**.

**TABLE 40** Report Parameters

Field	Description	Your Action
<b>General Information</b>		
<b>Title</b>	Indicates the report name.	Enter a title for the report.
<b>Description</b>	Describes the report type.	Enter a short description.
<b>Report Category</b>	Provides an option to generate reports for System or Switch devices in the network.	Select System or Switch as appropriate.
<b>Report Type</b>	Specifies the report type	Select the required report.
<b>Output Format</b>	Specifies the report output format.	Select the required report output format.
<b>Resource Filter Criteria</b>		
<b>Device</b>	Indicates the level of resource filtering for which you want to generate the report. For example: Management Domains, AP Zone or Access Point (if you select System option) and Switch.	Enter the device/switch name or select the device/switch from the list and choose the option.
<b>SSID</b>	Indicates the SSID for which you want to generate the report.	Select the check box and choose the SSID for which you want the report. You can select <b>All SSIDs</b> to generate reports for all the SSIDs available. This option is convenient as you do not have to update the resource filter criteria periodically.
<b>Radio</b>	Indicates the frequency for which you want to generate the report.	Select the check box and choose the required frequency: <ul style="list-style-type: none"> <li>• <b>2.4G</b></li> <li>• <b>5G</b></li> </ul>
<b>Time Filter</b>		
<b>Time Interval</b>	Defines the time interval at which to generate the report.	Select the required time interval.

**TABLE 40** Report Parameters (continued)

Field	Description	Your Action
<b>Time Filter</b>	Defines the time duration for which to generate the report.	Select the required time filter.
<b>Schedules</b>		
<b>Enable/Disable</b>	Specifies the scheduled time when a report must be generated. By default, the current system time zone is also displayed.	By default the option is disabled. Select <b>Enable</b> and select the <b>Interval</b> , <b>Hour</b> and <b>Minute</b> . You can add multiple schedules. You can also click <b>Add New</b> to include more schedules.
<b>Email Notification</b>		
<b>Enable/Disable</b>	Triggers an email notification when the report is generated.	By default the option is disabled. Select <b>Enable</b> and click the <b>Add New</b> and enter the email address. You can add multiple email addresses.
<b>Export Report Results</b>		
<b>Export Report Results, Enable/Disable</b>	Uploads the report results to an FTP server.	By default the option is disabled. Select <b>Enable</b> and select the <b>FTP Server</b> . Click <b>Test</b> to ping the FTP server and test if you are able to establish a connection.

**NOTE**

You can also edit or delete a report by selecting the options **Configure** or **Delete** respectively.

## Generating Reports

To generate a report:

1. From the left pane, select **Report > Report Generation**. [Figure 174](#) on page 344 appears.
2. Select the required report from the list and click **Generate**. The Report Generated form appears.
3. Click **OK**, the report will be generated and listed in the Report Results area.
4. Select the required format from the **Result Links** column and click **Open**.

## Rogue Access Points

### Viewing Rogue Access Points

Rogue (or unauthorized) APs pose problems for a wireless network in terms of airtime contention, as well as security.

Usually, a rogue AP appears in the following way: an employee obtains another manufacturer's AP and connects it to the LAN, to gain wireless access to other LAN resources. This would potentially allow even more unauthorized users to access your corporate LAN - posing a security risk. Rogue APs also interfere with nearby Ruckus APs, thus degrading overall wireless network coverage and performance.

The controller's rogue AP detection options include identifying the presence of a rogue AP, categorizing it as either a known neighbor AP or as a malicious rogue.


If you enabled rogue AP detection when you configured the common AP settings (see Configuring APs), click **Report > Rogue Access Points**. The Rogue Access Points page displays all rogue APs that the controller has detected on the network, including the following information:

- **Rogue MAC:** MAC address of the rogue AP.
- **Type:** Rogue, a normal rogue AP, not yet categorized as malicious or non-malicious.
- **Channel:** Radio channel used by the rogue AP.
- **Radio:** WLAN standards with which the rogue AP complies.
- **SSID:** WLAN name that the rogue AP is broadcasting.
- **Detecting AP Name:** Name of the AP.
- **Zone:** Zone to which the AP belongs.
- **RSSI:** Radio signal strength.
- **Encryption:** Indicates whether the wireless signal is encrypted or not.
- **Last Detected:** Date and time when the rogue AP was last detected by the controller.

### Filtering Rogue Access Points

From the list of Rogue Access Points you can filter the required rogue APs based on Rogue MAC or Type.

To filter rogue APs:

1. From the Rogue Access Points page, click Settings  button. The Apply Filters form appears.
2. Enter the **Rogue MAC** ID or select the rogue AP **Type** from the drop-down.
3. Click **OK**. Filtered rogue APs appear in the list.

### Marking Rogue Access Points

You can mark a Rogue (or unauthorized) AP as known.

To mark a Rogue AP as known:

1. From the left pane, click **Report** and **Rogue Access Points**. The Rogue Access Points page appears.
2. Select the Rogue AP from the list and click **Mark as Known**. The classification **Type** of the Rogue AP changes to **Known**. You can also select the Rogue AP from the list and click **Unmark**, to change the classification.

### Locating a Rogue Access Point

You can identify the estimated location area of a rogue AP on a map. Managed APs that detect the rogue APs are also visible in the map.

To locate the Rogue AP:

1. From the left pane, click **Report** and **Rogue Access Points**. The Rogue Access Points page appears.

2. Select the Rogue AP from the list and click Locate Rogue. The Rogue AP Location pop-up window appears locating the rogue AP.
  - a) You can select:
    - **Map**—to view the location in street view
    - **Satellite**—to view the location as satellite imagery
    - **+**—to zoom in the location
    - **-**—to zoom out the location.
  - b) You can find the following information:
    - Rogue APs: MAC, Type, and SSID
    - Detecting APs: MAC, Name, and RSSI
3. Click **OK**.

## Historical Client Stats

### Viewing AP Client Statistics

AP Client Statistics is a cumulative value per session and one entry is created per session. Data is reported every 60 seconds and is not bin data. The user interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, the total counters per DP or per GGSN IP for each bin is precalculated.

To view AP Client Statistics:

1. From the left pane, select **Report > Historical Client Stats**. The Ruckus AP Client page appears.
2. Update the parameters as explained in [Table 41](#).
3. Click:
  - **Load Data**— To view the report in the workspace.
  - **Export CSV**—To open or save the report in CSV file format.

**TABLE 41** AP Client Statistics Report Parameters

Field	Description	Your Action
<b>Time Period</b>	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
<b>Zone Name</b>	Specifies the zone for which you want to view the report.	Enter the zone name or choose the zone from the list.
<b>Client MAC</b>	Specifies the MAC.	Enter the client MAC.
<b>Client IP</b>	Indicates the client IP.	Enter the client IP address.
<b>MVNO Name</b>	Indicates the mobile virtual network operator name.	Choose the MVNO.

[Table 42](#) contains historical client statistics report based on the UE session statistics.

**TABLE 42** AP Client Statistics Report Attributes

Attribute	Type	Description
<b>Start</b>	Long	Indicates the session creation time.



**TABLE 42** AP Client Statistics Report Attributes (continued)

Attribute	Type	Description
<b>End</b>	Long	Indicates the session end time.
<b>Client MAC</b>	String	Indicates the Mac address of the client.
<b>Client IP Address</b>	String	Indicates the IP address of the client.
<b>Core Type</b>	String	Indicates the core network tunnel type.
<b>MVNO Name</b>	String	Indicates the mobile virtual network operator name.
<b>AP MAC</b>	String	Indicates the Client AP MAC.
<b>SSID</b>	String	Indicates the SSID
<b>Bytes from Client</b>	Long	Indicates the number of bytes received from the client.
<b>Bytes to Client</b>	Long	Indicates the number of bytes sent to the client.
<b>Packets from Client</b>	Long	Indicates the number of packets received from the client.
<b>Packets to Client</b>	Long	Indicates the number of packets sent to the client.
<b>Dropped Packets from Client</b>	Long	Indicates the number of packets dropped from the client.
<b>Dropped Packets to Client</b>	Long	Indicates the number of packets dropped to the client.

# Ruckus AP Tunnel Stats

## Viewing Statistics for Ruckus GRE Tunnels

The web interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, the total counters per DP or per AP for each bin may be pre-calculated.

To view the Ruckus GRE Tunnel Statistics:

1. From the left pane, select **Report > Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Update the parameters as explained in [Table 43](#).
3. Click:
  - **Load Data**— To view the report in the workspace.
  - **Export CSV**—To open or save the report in CSV file format.

**TABLE 43** Ruckus GRE Report Parameters

Field	Description	Your Action
<b>Time Period</b>	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
<b>Data Plane</b>	Indicates the Data Plane.	Select the Data Plane.
<b>AP MAC or IP Address</b>	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or IP address.

**TABLE 43** Ruckus GRE Report Parameters (continued)

Field	Description	Your Action
<b>Zone Name</b>	Specifies the zone for which you want to view the report.	Enter the zone name or select the zone from the list.

Table 44 contains the report based on the statistics for Ruckus GRE. Each entry contains the 15 minutes cumulative data.

**TABLE 44** Ruckus GRE report attributes

Attribute	Type	Description
<b>Time</b>	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
<b>TXBytes</b>	Long	Indicates the number of bytes sent.
<b>RXBytes</b>	Long	Indicates the number of bytes received.
<b>TXPkts</b>	Long	Indicates the number of packets sent.
<b>RXPkts</b>	Long	Indicates the number of packets received.
<b>Dropped Packets</b>	Long	Indicates the number of packets dropped.

## Viewing Statistics for SoftGRE Tunnels

The web interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, the total counters per DP or per AP for each bin may be pre-calculated.

To view the SoftGRE Tunnel Statistics:

1. From the left pane, select **Report > Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Select **SoftGRE**. Update the parameters as explained in Table 45.
3. Click:
  - **Load Data**—To view the report in the workspace.
  - **Export CSV**—To open or save the report in CSV file format.

**TABLE 45** SoftGRE Report Parameters

Field	Description	Your Action
<b>Time Period</b>	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
<b>Zone Name</b>	Specifies the zone for which you want to view the report.	Select the required zone.
<b>Gateway Address</b>	Specifies the gateway address	Enter the gateway address.
<b>AP MAC or IP Address</b>	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or IP address.

Table 46 contains the report based on the statistics for SoftGRE. Each entry contains the 15 minutes cumulative data.

**TABLE 46** SoftGRE Report Attributes

Attribute	Type	Description
<b>Time</b>	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
<b>TXBytes</b>	Long	Indicates the number of bytes sent.
<b>RXBytes</b>	Long	Indicates the number of bytes received.
<b>TXPkts</b>	Long	Indicates the number of packets sent.

**TABLE 46** SoftGRE Report Attributes (continued)

Attribute	Type	Description
<b>RXPkts</b>	Long	Indicates the number of packets received.
<b>RX Dropped Packets</b>	Long	Indicates the number of packets dropped.
<b>TX Dropped Packets</b>	Long	Indicates the number of packets dropped.
<b>TX Error Packets</b>	Long	Indicates the number of packets with a header error.
<b>RX Error Packets</b>	Long	Indicates the number of packets with a header error.

## Viewing Statistics for SoftGRE IPsec Tunnels

The web interface displays the table and its corresponding graph chart. The two representations are synchronized and controlled by the search criteria. For performance reasons, total counters per DP or per AP for each bin may be pre-calculated.

To view the SoftGRE IPsec Tunnel Statistics:

1. From the left pane, select **Report > Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
2. Select **SoftGRE + IPsec**. Update the parameters as explained in [Table 47](#).
3. Click:
  - **Load Data**— To view the report in the workspace.
  - **Export CSV**—To open or save the report in CSV file format.

**TABLE 47** SoftGRE + IPsec Report Parameters

Field	Description	Your Action
<b>Time Period</b>	Indicate the time period for which you want to view the report.	Move the slider to set the duration.
<b>Zone Name</b>	Specifies the zone for which you want to view the report.	Select the required zone.
<b>Gateway Address</b>	Specifies the gateway address	Enter the gateway address.
<b>AP MAC or IP Address</b>	Indicates the MAC of the Access Point or IP Address.	Enter the AP MAC or IP address.

[Table 48](#) contains the report based on the statistics for access point IPsec. Each entry contains the 15 minutes cumulative data.

**TABLE 48** SoftGRE + IPsecReport Attributes

Attribute	Type	Description
<b>Time</b>	Long	Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15.
<b>TXBytes</b>	Long	Indicates the number of bytes sent.
<b>RXBytes</b>	Long	Indicates the number of bytes received.
<b>TXPkts</b>	Long	Indicates the number of packets sent.
<b>RXPkts</b>	Long	Indicates the number of packets received.
<b>TX Dropped Packets</b>	Long	Indicates the number of packets dropped.
<b>RX Dropped Packets</b>	Long	Indicates the number of packets dropped.



# Troubleshooting

- Troubleshooting Client Connections.....353
- Troubleshooting through Spectrum Analysis..... 355

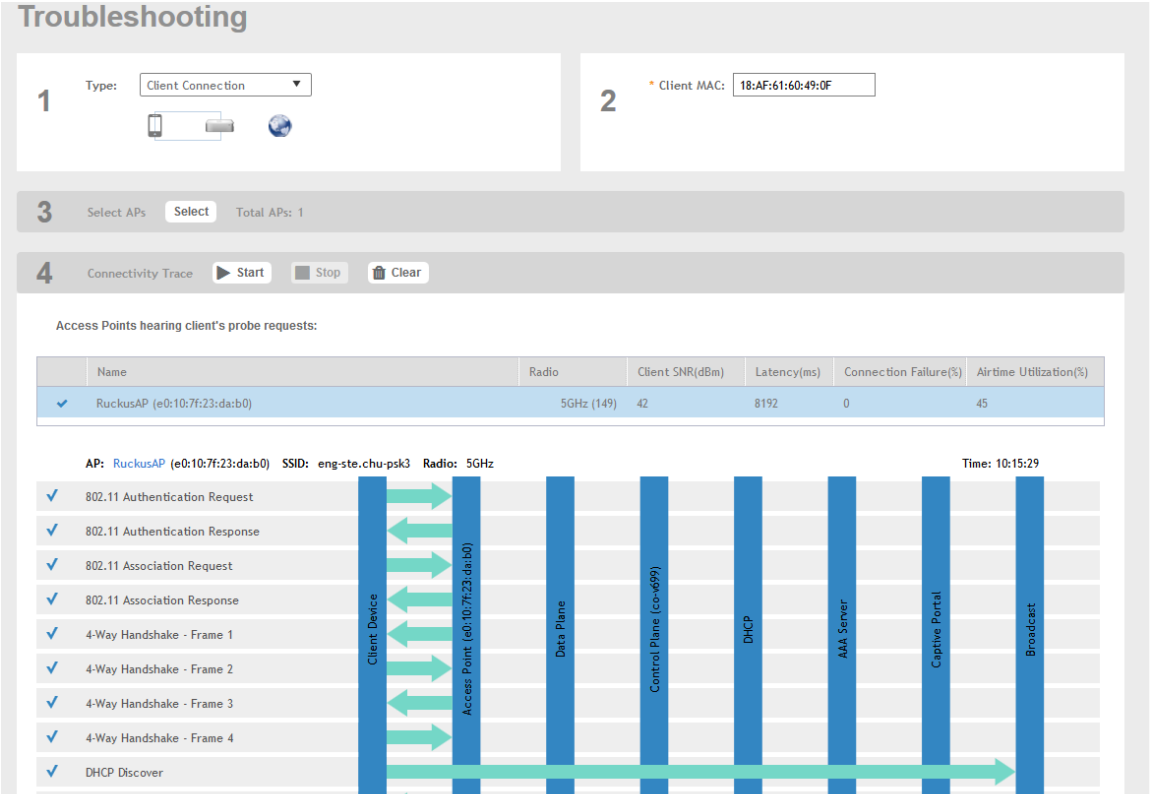
## Troubleshooting Client Connections

Network administrators can connect to client devices and analyze network connection issues in real time. The network administrator types the MAC address of the client device and starts services to identify the connectivity issue. The APs assigned to the client device relay data frames from the device to the controller. The administrator can analyze these frames to determine which stage of the connection is causing problems.

Perform the following steps to troubleshoot client connections.

1. Go to **Troubleshooting**.  
The **Troubleshooting** page is displayed as shown in the following example.

FIGURE 176 Troubleshooting - Client Connections



2. In Type, select **Client Connection** from the drop-down menu.
3. In **Client MAC**, click  settings, and choose **Historical Client** or **Connected Client** to view the client list.

4. Enter the MAC address of the client device with connectivity issues, or select the client device from the drop-down, which lists the **MAC Address**, **Hostname**, and **OS Type**.

You can search or sort the drop-down list by Client MAC, Hostname, or OS Type.

5. In Select APs, click **Select**.

The **Select APs** page is displayed.

6. Select an AP to communicate between the client and the controller, and then click **OK**.

7. In Connectivity Trace, click **Start**.

The controller configures the APs to receive data frames from the target client and relay frames to the controller based on the client filter.

The APs that receive probe requests from the target client are listed in a table, along with the AP's operating channel and the RSSI at which the client's frames were received. This stage of the connection identifies whether there are acceptable APs for the client to connect to.

The following items are displayed:

- AP Name and MAC Address
- Radio: The 2.4 or 5 GHz radio of the AP and the channel number the radio is operating on
- Client SNR: The signal-to-noise ratio received, in dB
- Latency: Time delay in connecting the AP to the client
- Connection Failures: The percentage of AP-client connection attempts that failed
- Airtime Utilization: The percentage of air time that was used by the client to transfer data

At this stage, the tool displays the statuses `Client is in a discovery state and not currently connected` (when the tool starts or when the client is already connected to an AP) and `Client is attempting a new connection` (when the target client sends an 802.11 authentication request frame to an AP to initiate a connection).

Use the list of APs that communicated with the client to determine whether the client chose the best AP based on signal quality and other health metrics.

When the client sends an 802.11 authentication request frame, a flow diagram depicting different stages of the AP-client connection is initiated. This sends a trigger frame to the AP, and it is highlighted from the list for reporting APs.

The Flow ladder in the diagram shows the step-by-step exchange of information between devices during the connection process. As the steps are completed, colored arrows are displayed when the step depicts a warnings (yellow) or event (for example, red for failure). Typical warning scenarios include time delays or a failed negotiation for an unsupported EAP type. Failure conditions are also highlighted as red arrows, typically when the connection itself fails.

#### NOTE

The following authentication types are supported:

- Open
- PSK (WPA2-Personal)
- 802.1X (PEAP, TTLS, TLS, SIM)
- WISPr

8. Click **Stop** to terminate the connection between the AP and the client.

# Troubleshooting through Spectrum Analysis

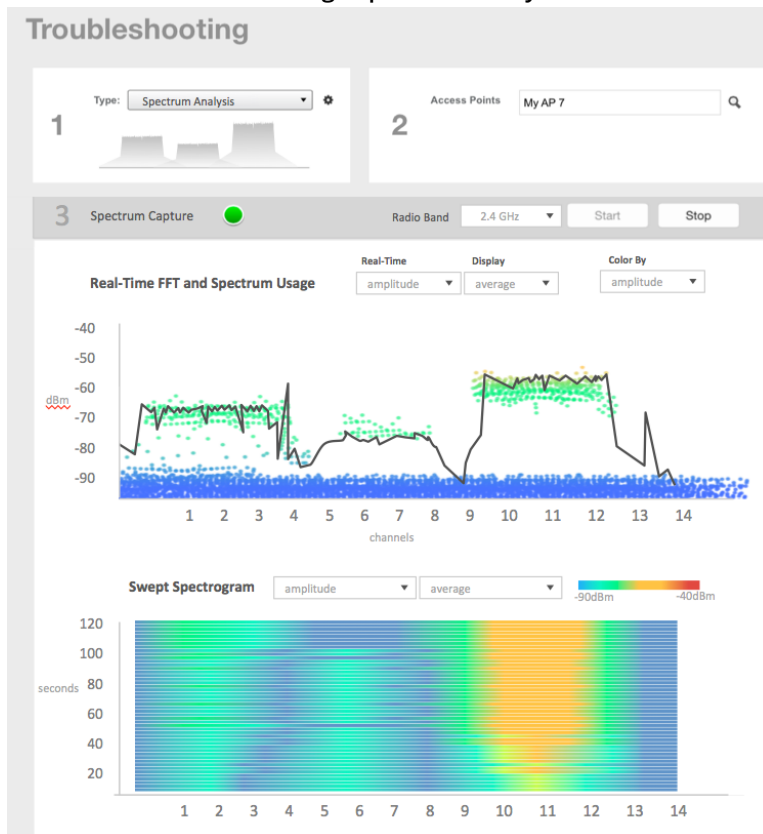
Interference between wireless devices is seen to increase dramatically due to the increase in the number of device used, and the availability of only three non-interfering channels in 802.11. This reduces the performance of the wireless network, therefore, it is important to monitor the spectrum usage in a particular area and efficiently allocate the spectrum as needed to wireless devices.

In addition, spectrum analysis provides the flexibility to troubleshoot issues remotely, identify sources of interferences within the network and allow administrators access to the RF health of the network environment.

APs which are put in spectrum-mode transmit data to the controller, which in turn displays the data in specturm-mode for analysis.

1. Go to **Troubleshooting**.  
The **Troubleshooting** page appears.

**FIGURE 177** Troubleshooting - Spectrum Analysis



2. In Type, select **Spectrum Analysis** from the drop-down menu.
3. In AP MAC Address, select the AP that needs to be in the spectrum analysis-mode.

4. In Spectrum Capture, select the radio frequency values (2.4GHz or 5GHz) for the analysis from the **Radio** option.  
The 2.4GHz band spans from 2400 - 2480 GHz and 5GHz band spans from 5.15 - 5.875 GHz.

You can select and view the spectrum analysis trends in these graphs:

- **Spectrum Usage:** This chart uses a color-based view to show collections of data points over time. As more data samples are measured at a specific frequency and amplitude coordinate, the color shown at that coordinate will change. If you choose to view colors by amplitude, the warm colors depict higher amplitude and cool colors lower amplitudes. If you view the colors by density, the warm colors depict a high number of samples at a given coordinate and cool colors show low number of samples at a given coordinate.
  - **Real-Time FFT :** This chart is a second-by-second (2sec) update of measured data across the band. If you view by Amplitude (signal strength), then the chart displays both average and maximum amplitudes of energy measured across the band for that sample period. If you view by Utilization (duty cycle), then the chart displays the percentage (%) of time at which the frequency is utilized at an amplitude above N. The amplitude threshold is configurable but the default is -85dBm.
  - **Swept Spectrogram:** This chart displays a waterfall of color over time, where each horizontal line in the waterfall represents one sample period (e.g. 2 seconds), and the full waterfall display spans 2 minutes of time (60 sample bins of 2sec each). There are two display options for the spectrogram chart:
    - **Amplitude:** Shows both average and maximum amplitude of energy measured across the band for that sample period.
    - **Utilization:** Shows the percentage of time at which the frequency is utilized at an amplitude above N. The amplitude threshold is configurable but the default is -85dBm.
5. After you select the parameters that you want to use to view the graphs, click **Start**.
  6. Click **Stop** to terminate viewing spectrum analysis trends.



# Managing Events and Alarms

---


• Viewing Events.....	357
• Sending SNMP Traps and Email Notifications for Events.....	357
• Configuring Event Threshold.....	358
• Creating Custom Events for ICX Switches.....	359
• Configuring Alarms.....	361

## Viewing Events

An event is an occurrence or the detection of certain conditions in and around the network. An AP being rebooted, an AP changing its IP address, and a user updating an AP's configuration are all examples of events.

Go to **Events and Alarms > Events**.

The **Events** page appears displaying the following information:

You can also click the  icon to apply filters, to display events based on time and severity.

- Date and Time: Displays the date and time when the event occurred
- Code: Displays the event code (see the Alarm and Event Reference Guide for your controller platform more information).
- Type: Displays the type of event that occurred (for example, AP configuration updated).
- Severity: Displays the severity level assigned to the events such as Critical, Debug, Informational, Warning, Major etc.
- Activity: Displays additional details about the event, including (if available) the specific access point, control plane, or data plane that triggered the event.

## Sending SNMP Traps and Email Notifications for Events

By default, the controller saves a record of all events that occur to its database. You can configure the controller to also send SNMP traps and email notifications for specific events whenever they occur.

Verify that global SNMP traps are enabled to ensure that the controller can send SNMP traps for alarms.

You can also manage notifications of the event for each zone by clicking the zones displayed in the tree structure. Event configuration for each zone is independent including:

- Enabling or disabling E-mail notification settings
- Recipient E-mail address
- Enabling or disabling DB persistence settings
- Enabling or disabling SNMP trap settings

You can also manually trigger SNMP traps without generating events using CLI. You can use the **#trigger-trap <event code>** command to trigger traps for respective events with their default attributes.

You can acquire the status of a specific client MAC address by using the query RUCKUS-CTRL-MIB. For more information, see the *SmartZone SNMP MIB Reference Guide*.

1. Go to **Events and Alarms > Events**.
2. Click the **Event Management** tab.

The **Event Management** page appears displaying the following information:

- Email Notification: Select the **Enable** check box, and then type an email address or email addresses in the **Mail To** box. If you want to send notifications to multiple recipients, use a comma to separate the email addresses. Then, click **OK**.
- Events: View the table and select the events for which you want to send traps or email notifications (or both). Select the **Enable** or **Disable** options from the drop-down menu, and configure the following:
  - Enable SNMP Notification: Click this link to enable SNMP trap notifications for all selected events.
  - Enable Email: Click this link to enable email notifications for all selected events.
  - Enable DB Persistence: Click this link to enable saving of all selected events to the controller database. If an event is already currently enabled, it will stay enabled after you click this link.

Following information related to the event are displayed:

- Code: displays the event code.
- Severity: displays the severity of the event such as Information, Minor and so on.
- Category: displays the category under which the event falls under, such as AP communication.
- Type: displays the event type such as AP managed, Ap rejected and so on.
- Zone Override: display the override status of the zone.

## Configuring Event Threshold

An event threshold defines a set of conditions related to the controller hardware that need to be met before the controller triggers an event. You can accept the default threshold values or you can update the threshold values to make them more suitable to your deployment or controller environment.

1. Go to **Events and Alarms > Events**.
2. Click the **Event Threshold** tab.

This page displays the list of events with configurable thresholds including the event code, severity level, default value and accepted range, and unit of measurement for each event.

3. Identify the event threshold that you want to configure.
4. Click the event name under the **Name** column.

The threshold value for the event becomes editable. Next to the threshold value, the acceptable range is displayed.

5. Edit the threshold value.

For **Client Count**, you can also edit the **Trigger Criterion** value between the range 1000-999999. When the client count exceeds 1000 users and when the client count drop percentage is more than 50% within an hour, the **Threshold Value** range of 50%-95% is breached. This generates event 956 and alarm 956 which are displayed in the **Events** and **Alarms** dashboard.

6. Click **OK**.

# Creating Custom Events for ICX Switches

You can create custom events by specifying that a particular switch status, for example a particular CPU utilization, memory utilization, or text pattern, generates an alarm or an event. Therefore, there are 3 types of custom events - CPU, Memory and TextPattern.

Because the polling interval between the switch and the controller is 5 minutes, the switch status cannot be obtained in real time. However, you can monitor memory and CPU utilization by creating an event or alarm that is triggered when a particular threshold is reached. You can also create a custom event to monitor for switch events based on text patterns.

To create a customer event, perform the following steps.

## NOTE

DB Persistence must be enabled to generate custom events.

1. Go to **Events and Alarms > Events**.
2. Click the **Switch Custom Events** tab.

The **Switch Custom Events** page is displayed.

**FIGURE 178** Types of custom events available

Events   Event Management   Event Threshold   Switch Custom Events						
+ Create   Configure   Delete   Types of switch custom events						
search table						
Event Name	Event Type	Event Severity	Threshold	Event Description	Text Pattern	Time Window
Warning CPU Usage	CPU	Warning	20	Switch CPU usage is ov...	N/A	N/A
Major CPU Usage	CPU	Major	30	Switch CPU usage is ov...	N/A	N/A
Critical CPU Usage	CPU	Critical	50	Switch CPU usage is ov...	N/A	N/A
Warning Memory Usage	Memory	Warning	60	Switch Memory usage l...	N/A	N/A
Major Memory Usage	Memory	Major	80	Switch Memory usage l...	N/A	N/A
Critical Memory Usage	Memory	Critical	90	Switch Memory usage l...	N/A	N/A
system is unusable	TextPattern	Warning	3	system is unusable	system is unusable	1 Hour
DHCP snooping on untrusted po...	TextPattern	Major	3	DHCP snooping on untr...	dhcp snooping on untr...	1 Hour
DHCP snooping on untrusted po...	TextPattern	Critical	3	DHCP snooping on untr...	dhcp snooping on untr...	1 Hour
Power supply 2 is down	TextPattern	Critical	3	Power supply 2 is down	power supply 2 is down	1 Hour

3. Click **Create**.

The **Create Switch Custom Events** page is displayed as shown in the following example.

**NOTE**  
You can only create new TextPattern custom events. Custom events of CPU or Memory type can only be edited or configured, and cannot be created.

**FIGURE 179** Creating custom events for switches - TextPattern type

The screenshot shows a dialog box titled "Create Switch Custom Event". It contains several input fields and dropdown menus. The "Event Name" field is empty. The "Event Description" field is empty. The "Event Type" dropdown is set to "TextPattern". The "Event Contains The Text" field is empty. The "Threshold" dropdown is set to "Times". The "Time Window" dropdown is set to "1 Hour". The "Event Severity" dropdown is set to "Warning". There are "OK" and "Cancel" buttons at the bottom right.

Configure the following:

- Event Name: Enter the name of the event. For example, you can provide a name to identify the text pattern to be displayed in the event description.
- Event Description: Enter a detailed description of the event.
- Event Type: Displays the type of event. Here, Text Pattern.
- Event Contains The Text: Enter the text used in the event to be monitored.
- Threshold: Enter the number of times the user-defined status is achieved.
- Time Window: Select the time frame within which the threshold is achieved. You can select from a few hours to two days.
- Event Severity: Select the severity level of the custom event. Options include Warning, Major, and Critical.

**FIGURE 180** Editing custom events for switches - CPU/Memory type

The screenshot shows a dialog box titled "Edit Switch Custom Event". It contains several input fields and dropdown menus. The "Event Name" field is filled with "Warning CPU Usage". The "Event Description" field is filled with "Switch CPU usage is over Warning threshold, 20%". The "Event Type" dropdown is set to "CPU". The "Threshold" dropdown is set to "20 %". The "Event Severity" dropdown is set to "Warning". There are "OK" and "Cancel" buttons at the bottom right.

Configure the following:

- Event Name: Displays the name of the event.
- Event Description: Displays a detailed description of the event.
- Event Type: Displays the type of event. Here, CPU.
- Threshold: Enter the percentage of times the user-defined status is achieved.
- Event Severity: Displays the severity level of the custom event. Options include Warning, Major, and Critical.

4. Click **OK**.

## Configuring Alarms

Alarms are a type of event that typically warrants your attention. Alarms are generated by managed access points and the controller system (control plane and data plane).


Go to **Events and Alarms > Alarms**.

The **Alarms** page appears displaying the following information:

- Date and Time: Displays the date and time when the alarm was triggered.
- Code: Displays the alarm code (see the Alarm and Reference Guide for your controller platform for more information).
- Alarm Type: Displays the type of alarm event that occurred (for example, AP reset to factory settings).
- Severity: Displays the severity level assigned to the events such as Critical, Major, Minor and Warning.
- Status: Indicates whether the alarm has already been cleared or still outstanding.
- Activity: Displays additional details about the alarm, including (if available) the specific access point, control plane, or data plane that triggered the alarm.
- Acknowledged On: Displays the date and time when the administrator acknowledge the alarm.
- Cleared By: Displays information about who cleared the alarm.
- Cleared On: Displays the date and time when the alarm was cleared.
- Comments: Displays administrator notes recorded during alarm management.

### NOTE



Click  to export the alarms details to a CSV file. Check the default download folder of your web browser and look for a file named *alarms.csv* and view it using a spreadsheet application (for example, Microsoft Excel®).

## Clearing Alarms

Clearing an alarm removes the alarm from the list but keeps it on the controller's database.

To clear an alarm:

1. Select the alarm from the list and click **Clear Alarm**. The **Clear Alarm** page appears.
2. Type your comments and select **Apply**.

## Acknowledging Alarms

Acknowledging an alarm lets other administrators know that you have examined the alarm. After you acknowledge an alarm, it will remain on the list of alarms and will show the date and time that you acknowledged it.

To acknowledge an alarm:

1. Select the alarm from the list and click **Acknowledge Alarm**.

This message appears:

Are you sure you want to acknowledge the selected alarms?

.

2. Select **Yes**.

## Applying Filters

You can view a list of alarms by date, time, severity and status.

1. Click the  icon.

The **Apply Filters** page appears. Configure the following:

- a. **Severity:** Select the severity level by which you want to filter the list of alarms.
- b. **Status:** Select the status by which you want to filter the list of alarms.
- c. **Date and Time:** Select the alarms by their start and end dates.

2. Click **OK**.

All the alarms that meet the filter criteria are displayed on the **Alarms** page and the display changes to **Filter On**.

You can export the alarms into a CSV file by clicking the  icon.

# Administering the Controller

---

- Managing Administrator and Roles..... 363
- Backing Up and Restoring Clusters..... 381
- Upgrading the Controller..... 391
- Managing Licenses..... 396
- ZoneDirector to SmartZone Migration..... 403
- Monitoring Administrator Activities..... 403



## Managing Administrator and Roles






The controller must be able to manage various administrators and roles that are created within the network in order to assign tasks and functions, and to authenticate users.

### Creating User Groups

Creating user groups and configuring their access permissions, resources, and administrator accounts allows administrators to manage a large number of users.

1. Go to **Administration > Admins and Roles**.
2. Select the **Groups** tab.
3. Click **Create** after selecting the system domain.  
The **Create User Group** page appears.

4. Configure the following:
  - a. Permission
    1. Name: Type the name of the user group you want to create.
    2. Description: Type a short description for the user group you plan to create.
    3. Permission: Select one of the access permission for the user group, from the drop-down menu. You can also grant admin permission to generate guest passes. Select the **Custom** option to manually assign role-based permission in the **Resource** tab page.
    4. Account Security: Select the account security profile that you created to manage the administrator accounts.
    5. Click **Next**.
  - b. Resource: From **Select Resources**, choose the resources that you want to assign to this user group. If you have selected **Custom** permission option in the previous step, you can assign the required permission (**Read**, **Modify** or **Full Access**) to these resources. The resources available are SZ, AP, WLAN, User/Device/App, Admin, Guest Pass, MVNO and ICX. Click the  icon and they appear under **Selected Resources** now. Use the  icon to deselect the resources assigned to the group. To select the right set of resource permission, refer [Resource Group Details](#) on page 365.
- NOTE**

To create User Groups, migrating Domain User Roles prior to 3.5, with DPSK permissions, Users must be granted with "User/Device/App" resource.
- c. Click **Next**.
- d. Administrator: From **Available Users**, choose the users you want to assign to this user group. Click the  icon and they appear under **Selected Users** now. Use the  icon to deselect the users assigned to the group. You can also create Administrator Accounts by clicking the  icon. The **Create Administrator Account** page appears where you can configure the administrator account settings. You can edit the user settings by clicking the  icon and delete the user from the list by clicking  icon.
- e. Click **Next**.
- f. Review: Verify the configuration of the user group. Click **Back** to make modifications to the configuration settings.
- g. Click **OK** to confirm.

You have created the user groups.

**NOTE**

You can also edit and delete the group configuration by selecting the options **Configure**, and **Delete** respectively, from the **Groups** tab.



## Resource Group Details

The Resource Group table lists the resources available for each Resource Category. This helps the users to select the right set of resource permission for the Admin type.

**TABLE 49** Resource Group Table

Resource Category	Resources
SZ	<ul style="list-style-type: none"> <li>System Settings</li> <li>Cluster Settings and Cluster Redundancy</li> <li>Control Planes and Data Planes</li> <li>Firmware and Patches</li> <li>Cluster and Configuration Backups</li> <li>Licensing</li> <li>Cluster Stats and Health</li> <li>System Events and Alarms</li> <li>System Certificates</li> <li>Northbound Interface</li> <li>SCI Integration</li> </ul>
AP	<ul style="list-style-type: none"> <li>Zones and Zone Templates</li> <li>AP groups</li> <li>AP Settings</li> <li>AP Stats and Health</li> <li>Maps</li> <li>AP Events and Alarms</li> <li>Bonjour Policies</li> <li>Location Services</li> <li>Ethernet Port Profiles</li> <li>Tunneling Profiles and Settings</li> <li>AP Zone Registration</li> </ul>
WLAN	<ul style="list-style-type: none"> <li>WLANS</li> <li>WLAN Groups and Templates</li> <li>AAA Services</li> <li>L2-7 Policies</li> <li>Rate Limiting</li> <li>Application Policies</li> <li>Device OS Policies</li> <li>QoS Controls</li> <li>Hotspots and Portals</li> <li>Hotspot 2.0</li> <li>Service Schedules</li> <li>VLAN Pools</li> </ul>

**TABLE 49** Resource Group Table (continued)

Resource Category	Resources
User/Device/App	User Roles Local Users DPSK Guest Passes Application Usage Client and Device Details
Admin	Domains Administrators Administrative Groups Administrative Activity AAA for Admins
Guest Pass	Guest Pass Guest Pass Template
MVNO	MVNO
ICX Switch	ICX Switch Switch Group Registration Rule

## Creating Administrator Accounts

The controller supports the creation of additional administrator accounts. This allows you to share or delegate management and monitoring functions with other members of your organization. You can also modify the status of the administrator account by locking or unlocking it.

1. Go to **Administration > Admins and Roles**.
2. Select the **Administrators** tab.

3. Click **Create**.

The **Create Administrator Account** page appears.

**FIGURE 181** Creating an Administrator Account

## Create Administrator Account

\* Account Name:

Real Name:

\* Password:

\* Confirm Password:

Phone:

Email:

Job Title:

**OK** **Cancel**

4. Configure the following:
  - a. Account Name: Type the name that this administrator will use to log on to the controller.
  - b. Real Name: Type the actual name (for example, John Smith) of the administrator.
  - c. Password: Type the password that this administrator will use (in conjunction with the Account Name) to log on to the controller.
  - d. Confirm Password: Type the same password as above.
  - e. Phone: Type the phone number of this administrator.
  - f. Email: Type the email address of this administrator.
  - g. Job Title: Type the job title or position of this administrator in your organization.
  - h. Click **OK**.

You have created the administrator account.

### NOTE

You can also edit, delete, and unlock the admin account by selecting the options **Configure**, **Delete** and **Unlock** respectively, from the **Administrator** tab.

**NOTE**

Administrator users mapped to different domain other than system domain have to login using accountname@domain as the User.

## Unlocking an Administrator Account

When multiple user access authentications fail, the administrator account is locked. A super administrator can however unlock the administrator account.

Typically, the account gets locked when the user attempts to login with a wrong user ID or password multiple times, or when the time duration/session time to access the account has ended.

You must login as a super administrator in order to unlock the account.

1. Go to **Administration > Admins and Roles**.
2. Select the **Administrators** tab.
3. From the list of accounts, select the one which needs to be unlocked. The **Status** of such an account is displayed as *Locked*.
4. Click **Unlock**.

The administrator account is now unlocked, the **Status** field against the account now displays *Unlocked*.

## Configuring Administrator Accounts

To configure the account security of System Default Super Admin account, you can set session idle timeout, password expiration, and password reuse rules.

You must log in as a **System Default Super Admin** to set the rules.

1. Select **Administration > Admins and Roles**.
2. Click the **Administrators** tab.

3. Select the administrator account (admin) and click **Configure** to set the additional security enhancements.  
The **Edit Administrator Account** page appears.

**FIGURE 182** Configuring an Administrator Account

**Edit Administrator Account: admin** X

\* Account Name: admin

Real Name:

\* Password: .....

\* Confirm Password: .....

Phone:

Email:

Job Title:

Session Idle Timeout: ☒ ON 15 (1-1440) minutes

Password Expiration: ☒ ON Require password change every 90 (1-365) days

Password Reuse: ☒ ON Passwords cannot be the same as the last 4 (1-6) times

OK Cancel

4. Enable **Session Idle Timeout** and enter the timeout duration in minutes.  
**Session Idle Timeout** can be configured from the following locations:
  - **User Preferences:** Applicable for the currently logged in user. The user can be a System Default Super Admin or another administrator account.
  - **Account Security:** Other administrator accounts can configure this profile, but not the System Default Super Admin.
  - **Edit Administrator Account** page: Only the System Default Super Admin can configure the timeout from this page.For more information, refer to [Creating Account Security](#) on page 377.

**NOTE**

The **Session Timeout Settings** on the User Preferences page are disabled when **Session Idle Timeout** is enabled on the **Account Security** page or the **Edit Administrator Account** page.

5. Enable **Password Expiration** and enter the number of days for which the account password will be valid.

6. Enable **Password Reuse** and enter a number from 1 through 6.

**NOTE**

The default **Password Reuse** value is 4.

7. Click **OK**.

You have configured an administrator account.

## Working with AAA Servers

You can configure the controller to use external AAA servers to authenticate users.

To add and manage AAA servers that the controller can use to authenticate users, follow these steps:

1. Go to **Administration > Admins and Roles**.
2. Select the **AAA** tab.
3. Click **Create**.

The **Create Administrator AAA Server** page appears.

**FIGURE 183** Creating an Administrator AAA Server

Create Administrator AAA Server

\* Name:

\* Type: ☒ RADIUS ☐ TACACS+ ☐ Active Directory ☐ LDAP

\* Realm:   
Multiple realms supported. Use a comma (,) to separate realms (for example, home1,home2).

[?] Default Role Mapping: ☐ OFF

User Group:

Administrator:

Backup RADIUS: ☐ OFF Enable Secondary Server

\* IP Address:

\* Port:

\* Shared Secret:

\* Confirm Secret:

OK Cancel

4. Configure the following:
  - a. Name: Type a name for the RADIUS server.
  - b. Type: Select the type of AAA server that you have on the network. Options include:
    - RADIUS
    - TACACS+
    - Active Directory
    - LDAP
  - c. Realm/Service: Enter the realm or service. Multiple realms or services are supported, which must be separated with a comma.

**NOTE**

As the user login format (User Account + @ + Realm) includes the special character, the at symbol (@), the User Account must not include the at symbol (@) separately on AAA server.

- d. Default Role Mapping: Enable the option so that the AAA users can be automatically mapped to a default local admin user/group permission even if the AAA server does not use mapping attributes. If you disable the option, the AAA admin must be mapped to a local SZ Admin user with matching AAA attributes.
  - On a RADIUS server, the user data can use the **VSA Ruckus-WSG-User** attribute with a value depending on the SZ users or permissions you want the RADIUS user to map.
  - On a TACACS+ server, the user data can use the **user-name** attribute with the **user1** or **user2** or **user3** value depending on the SZ users or permissions you want the TACACS+ user to map.
  - On an AD or LDAP server, the user data can belong to the group **cn=Ruckus-WSG-{SZAdminName}** (for example, **cn=Ruckus-WSG-user1** depending on the SZ users or permissions you want the Active Directory or LDAP user to map.

**NOTE**

You can use the mapping attributes on AAA and enable the Default Role Mapping at the same time, but the mapping attributes override the Default Role Mapping.

- e. Backup RADIUS: Select the Enable backup RADIUS server check box if a secondary RADIUS server exists on the network. Configure the settings in *Step 7*.
- f. In the Primary Server section, configure the settings of the primary RADIUS server, TACACS+ server, Active Directory and LDAP.
  - IP Address: Type the IP address of the AAA server.
  - Port: Type the UDP port that the RADIUS server is using. The default port is 1812.
  - Shared Secret: Type the shared secret.
  - Confirm Secret: Retype the shared secret to confirm.
  - Windows Domain name: Type the domain name for the Windows server.
  - Base Domain Name: Type the name of the base domain.
  - Admin Domain Name: Type the domain name for the administrator.
  - Admin Password: Type the administrator password.
  - Confirm Password: Re-type the password to confirm.
  - Key Attribute: Type the key attribute such as UID.
  - Search Filter: Type filter by which you want to search such as objectClass=\*

- g. In the Secondary Server section, configure the settings of the secondary RADIUS server.
  - IP Address: Type the IP address of the AAA server.
  - Port: Type the UDP port that the RADIUS server is using. The default port is 1812.
  - Shared Secret: Type the shared secret.
  - Confirm Secret: Retype the shared secret to confirm.
- h. Click **OK**.

**NOTE**

You can also edit, clone and delete the server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Administrator** tab.

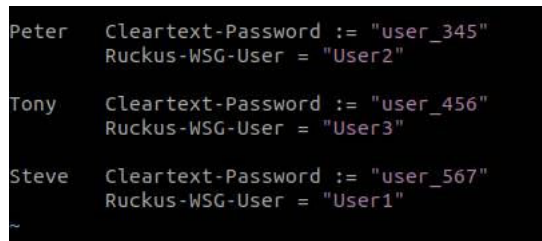
## About RADIUS Support

Remote Authentication Dial-In User Service (RADIUS) is an Authentication, Authorization, and Accounting protocol used to authenticate controller administrators.

In addition to selecting RADIUS as the server type, complete the following steps for RADIUS-based authentication to work on the controller.

1. Edit the RADIUS configuration file (**users**) on the RADIUS server to include the user names.

For example,



```
Peter  Cleartext-Password := "user_345"
      Ruckus-WSG-User = "User2"

Tony   Cleartext-Password := "user_456"
      Ruckus-WSG-User = "User3"

Steve  Cleartext-Password := "user_567"
      Ruckus-WSG-User = "User1"
```

2. On the controller web interface, select **Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

**NOTE**

Refer to [Creating Administrator Accounts](#) on page 366. In this example, RADIUS can use User1, User2, or User3.

3. Select **Administration > Admins and Roles > Groups** and assign an administrator role to the super administrator account.

**NOTE**

Refer to [Creating User Groups](#) on page 363.

4. When adding a server type for administrators, select RADIUS as the authentication server type.

**NOTE**

Refer to [Working with AAA Servers](#) on page 370.



5. Test the RADIUS server using the account **username@super-login**.

**NOTE**

The value of super-login depends on the realm configured for the AAA profile. Refer to [Creating Administrator Accounts](#) on page 366.

## About TACACS+ Support

Terminal Access Controller Access-Control System Plus (TACACS+) is one of the Authentication, Authorization and Accounting protocols used to authenticate controller administrators. TACACS+ is an extensible AAA protocol that provides customization and future development features, and uses TCP to ensure reliable delivery.

In addition to selecting TACACS+ as the server type, complete the following steps for TACACS+ based authentication to work on the controller.

1. Edit the TACACS+ configuration file (**tac\_plus.conf**) on the TACACS+ server to include the service user name.

For example,

```
key = test@1234
accounting file = /var/log/tac_acct.log
user = username {
    member = show
    login = cleartext "password1234!"
}
group = show {
    service = super-login {
        user-name = super <==mapped to the user account in the controller
    }
}
```

2. On the controller web interface, select **Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

**NOTE**

Refer to [Creating Administrator Accounts](#) on page 366.

3. Select **Administration > Admins and Roles > Groups** and assign an administrator role to the super administrator account.

**NOTE**

Refer to [Creating User Groups](#) on page 363.

4. When adding a server type for administrators, select TACACS+ as the authentication server type.

**NOTE**

Refer to [Working with AAA Servers](#) on page 370.

5. Test the TACACS+ server using the account **username@super-login**.

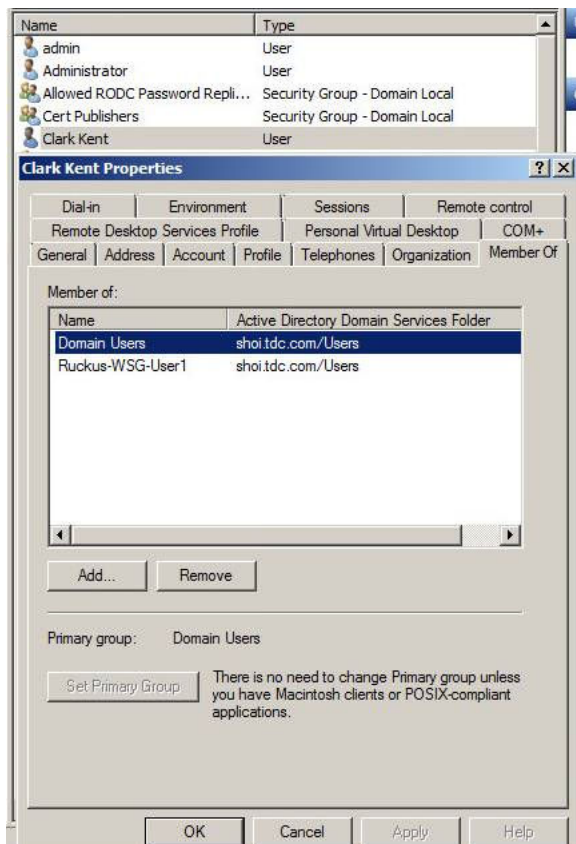
## About Active Directory (AD) Support

Active Directory is a domain service that authenticates and authorizes users in a Windows environment.

In addition to selecting AD as the server type, you must also complete the following steps for AD-based authentication to work on the controller.

1. Edit the AD configuration file on the AD server to include the service user name.

For example,



2. On the controller web interface, select **Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

### NOTE

Refer to [Creating Administrator Accounts](#) on page 366. In this example, AD can use User1 only.

3. Select **Administration > Admins and Roles > Groups**, and then assign an administrator role to the super administrator account.

### NOTE

Refer to [Creating User Groups](#) on page 363 .

4. When you add an AAA server for administrators, select **Active Directory** as the authentication server type.

### NOTE

Refer to [Working with AAA Servers](#) on page 370.

- Test the AD server using the account **username@super-login**.

**NOTE**

The value of super-login depends on the realm configured for the AAA profile. Refer to [Creating Administrator Accounts](#) on page 366.

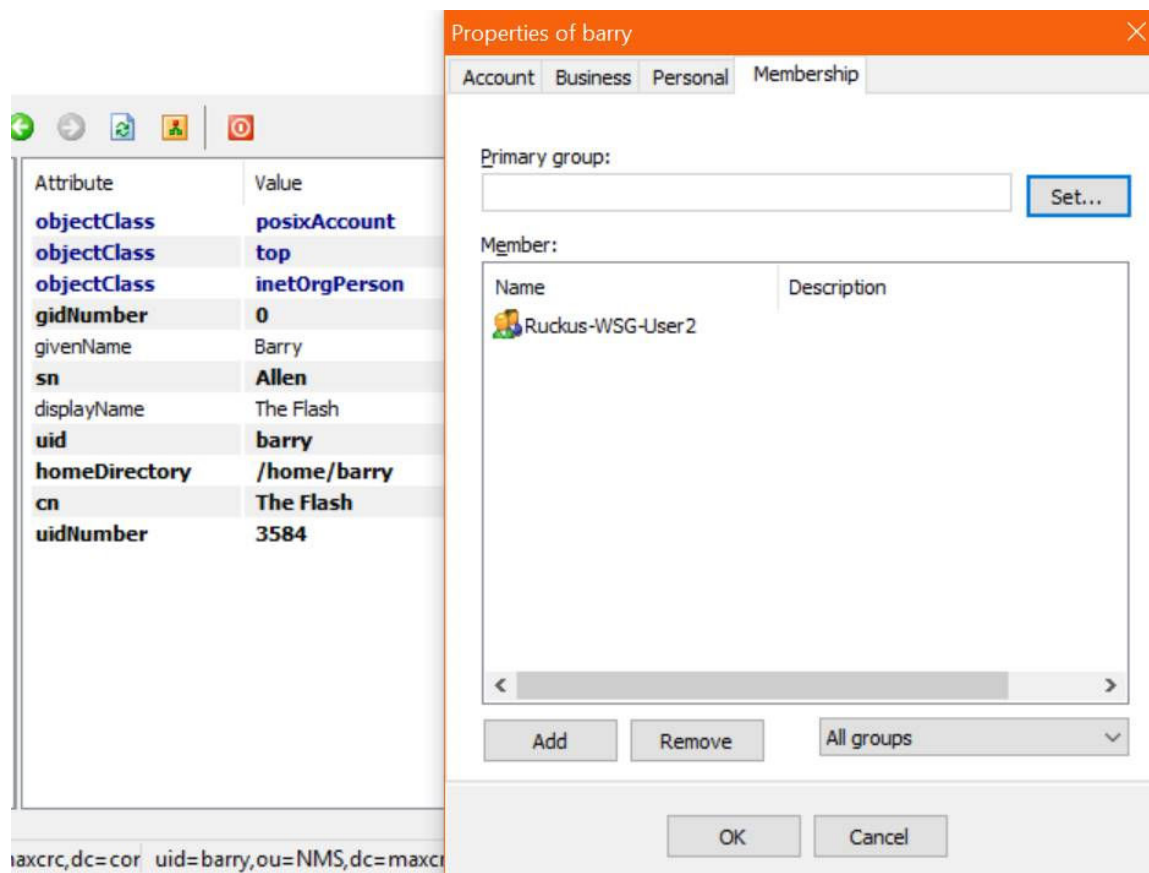
## About LDAP Support

Lightweight Directory Access Protocol (LDAP) is an application protocol used to access and maintain directory information services.

In addition to selecting LDAP as the server type, you must also complete the following steps for LDAP-based authentication to work on the controller.

- Edit the LDAP configuration file on the LDAP server to include the service user name.

For example,



- On the controller web interface, select **Administration > Admins and Roles > Administrators**, and click **Create** to create an administrator account with **super** as the user name.

**NOTE**

Refer to [Creating Administrator Accounts](#) on page 366. In this example, LDAP can use User2 only.

3. Select **Administration > Admins and Roles > Groups** and assign an administrator role to the super administrator account.

**NOTE**

Refer to [Creating User Groups](#) on page 363.

4. When you add an AAA server for administrators, select **LDAP** as the authentication server type.

**NOTE**

Refer to [Working with AAA Servers](#) on page 370.

5. Test the LDAP server using the account **username@super-login**.

**NOTE**

The value of super-login depends on the realm configured for the AAA profile. Refer to [Creating Administrator Accounts](#) on page 366.

## Enabling the Access Control List

You can control access to management interfaces from CLI or SSH.

1. Go to **Administration > Admins and Roles**.
2. Select the **Access Control List** tab.
3. Select **Enable**.
4. Click **Create**.

The **Management Interface Access Control Rule** page appears.

**FIGURE 184** Management Interface Access Control Rule

### Management Interface Access Control Rule

The screenshot shows a web form for configuring a Management Interface Access Control Rule. The form has a light gray background. At the top, there is a label '\* Name:' followed by a text input field. Below that is a label 'Description:' followed by a text input field. Further down is a label '\* Type:' followed by three radio button options: 'Single IP' (which is selected), 'IP Range', and 'Subnet'. Below the radio buttons, there is a section titled 'Single IP' with a label '\* IP Address:' followed by a text input field. At the bottom right of the form, there are two buttons: 'OK' and 'Cancel'.

5. Configure the following:
  - a. Name: Type the name that rule you want to create to access the management interface.
  - b. Description: Type a short description for the rule.
  - c. Type: Select one of the following
    - Single IP: Type the IP address of the interface that can be accessed per this rule.
    - IP Range: Type the range of IP address that will be allowed access.
  - d. Subnet: Type the network address and subnet mask address of the interface that will be allowed access.
  - e. Click **OK**.

You have created the access control list rule.

**NOTE**

You can also edit and delete the list by selecting the options **Configure** and **Delete** respectively, from the **Access Control List** tab.

## Creating Account Security

Creating an account security profile enables end-users to control administrative accounts to better manage admin accounts, passwords, login, and DoS prevention.

1. Go to **Administration > Admins and Roles**.
2. Select the **Account Security** tab.

3. Click **Create**.

The **Create Account Security** page appears.

**FIGURE 185** Creating Account Security

Create Account Security ✕

\*

Name:

Description:

Session Idle Timeout:

ON

15

(1-1440) minutes

Account Lockout:

ON

Lock account for

30

(1-1440) minutes

after

6

(1-100) failed authentication attempts

Password Expiration:

ON

Require password change every

90

(1-365) days

Password Reuse:

ON

Passwords cannot be the same as the last

4

(1-6) times

Two-Factor Authentication:

OFF

Require two-factor authentication via SMS

You have to verify your one-time code first to enable it

Send

Set SMS server

Disable Inactive Accounts:

ON

Lock admin accounts if they have not been used in the last

90

(1-1000) days

OK

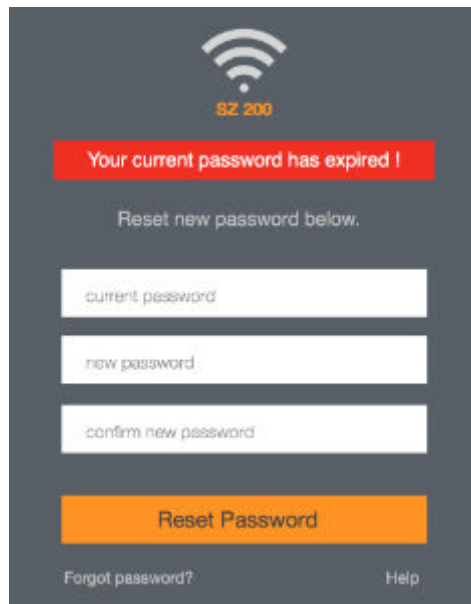
Cancel

4. Configure the following:

- **Name:** Type the name of the security profile that you want to create.
- **Description:** Provide a short description for the profile.
- **Session Idle Timeout:** Click the button and enter the timeout duration in minutes.
- **Account Lockout:** You can configure the security profile to lock the account based on the duration of the session or number of failed attempts to access the account. Provide the values as necessary. Click the button in order to enable the feature.
- **Password Expiration:** Click the button and type the number of days for which the account's password will be valid. After the configured number of days, the password will expire and render the account inaccessible. You must change the password before the expiration day to have continued access to the account. By default, the password is valid for a period of 90 days. It can be configured for validity from a minimum of 1 day, to a maximum of 365 days.

If your password has expired, you will be prompted to change or reset your password as soon as you login. Reset the password as shown in the figure.

**FIGURE 186** Resetting the old password



- **Password Reuse:** Prevents the reuse of passwords. Click the button to enable this option. By default, the value is 4 (last 4 passwords cannot be reused).
- **Two-Factor Authentication:** Provides username/password authentication and SMS authentication. To enable this option, click the button. You must have configured the SMS Gateway.

When a network admin logs in using the credentials, a prompt to enter a one-time SMS code appears. The SMS system generates a one-time code and sends it to the admin's phone number. Once the admin enters this SMS code access to the system is granted.

- **Disable Inactive Accounts:** Locks the admin user IDs that are inactive for the specified period of time. Click the button and specify the number of days.
- Click **OK**.

From **Global Security**, you can select the check-box to enable **Captcha for Login**. The captcha feature provides additional security to ensure a human is signing into the account, and not a robot. If this feature is enabled; when you login to the web interface, the captcha characters are displayed in the login page as shown.

**FIGURE 187** Captcha enabled in the login page



Type the characters as shown in the captcha picture and login. The characters in the captcha image are case sensitive and can be refreshed if not clear.

5. Click **OK** to submit the security profile/form.

The newly created profile is added under the **Account Security** section.

You have created the account security profile.

**NOTE**

You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **Administrator** tab.

With new enhancements to account security, SmartZone has a complete feature set to make PCI compliance very simple and straightforward. In addition to local PCI enforcement settings, SmartZone also integrates with SCI for reporting and analytics. SCI version 5.0 and above supports a PCI compliance report, which is based on the relevant PCI-related configuration settings throughout SmartZone. To facilitate the SmartCell Insight PCI report, the SmartZone is capable of sending the following information to SCI:

- Configuration messages as separated GPB messages.
- WLAN configuration
- Default configuration changes
- Controller information which identifies the SZ model
- Encryption details of communication, for example: CLI, SSH, telnet, Web, API.
- Inactive user IDs and session timeout
- Authentication mechanism enforced on user IDs.
- Enforcement of password.



- Supported mechanism on SZ that can be provided to SCL.
- User IDs that are locked after failed attempts.
- Authentication credentials that are unreadable and encrypted during transmission.
- Enforcement of password standards.
- Disallowing duplicate password feature is enabled.
- If rogue AP detection is enabled on each AP.

To learn more about SCL and the PCI compliance report it provides, check the product page (<https://www.ruckuswireless.com/products/smart-wireless-services/analytics>) and documentation on Ruckus support (<https://support.ruckuswireless.com>).

## Backing Up and Restoring Clusters

Back up the controller cluster periodically to ensure that you can restore the control plane, data plane, and AP firmware versions as well as the system configuration in the cluster if a system failure occurs.

### Creating a Cluster Backup

Backing up the cluster (includes OS, configuration, database and firmware) periodically enables you to restore it in the event of an emergency. Ruckus also recommends that you back up the cluster before you upgrade the controller software.

1. Go to **Administration > Backup and Restore**.
2. Select the **Cluster** tab.
3. In Cluster Backup and Restore, click **Backup Entire Cluster** to backup both nodes in a cluster.

The following confirmation message appears: Are you sure you want to back up the cluster?

4. Click Yes.

The following message appears: The cluster is in maintenance mode. Please wait a few minutes.

When the cluster backup process is complete, a new entry appears in the **Cluster Backups History** section with a **Created On** value that is approximate to the time when you started the cluster backup process.

### Restoring a Cluster Backup

You must be able to restore a cluster to its previous version in the case of a failure.

1. Go to **Administration > Backup and Restore**.
2. Select the **Cluster** tab.
3. In Cluster Backup History, select the cluster and click **Restore**.

The following confirmation message appears:

Are you sure you want to restore the cluster?

4. Click **Yes**.

The cluster restore process may take several minutes to complete. When the restore process is complete, the controller logs you off the web interface automatically.

#### ATTENTION

Do not refresh the controller web interface while the restore process is in progress. Wait for the restore process to complete successfully.

5. Log on to the controller web interface.  
If the web interface displays the message `Cluster is out of service. Please try again in a few minutes` appears after you log on to the controller web interface, wait for about three minutes. The dashboard will appear shortly. The message appears because the controller is still initializing its processes.
6. Go to **Administration > Upgrade**, and then check the **Current System Information** section and verify that all nodes in the cluster have been restored to the previous version and are all in service.
7. Go to **Diagnostics > Application Logs**, and then under **Application Logs & Status** check the **Health Status** column and verify that all of the controller processes are online.

You have completed restoring the cluster backup.

## Backing Up and Restoring the Controller's Network Configuration from an FTP Server

In addition to backing up and restoring the controller's network configuration from its own database, the controller supports backup and restore of its network configuration from an FTP server using the CLI.

This section describes the requirements for backing up and restoring the controller's network configuration from an FTP server, the information that is included in the backup file, and how to perform the backup and restore process.

To back up and restore the controller's network configuration from an FTP server, the controller must have already been set up and in service. In case of a multi-node cluster, all the nodes in the cluster must be in service.

The following table lists the network configuration that is backed up from the control and data planes when you perform a backup procedure to an FTP server.

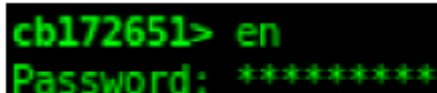
**TABLE 50** Information that is backed up to the FTP server

Control Plane	Data Plane
<ul style="list-style-type: none"><li>• Control interface</li><li>• Cluster interface</li><li>• Management interface</li><li>• Static routes</li><li>• User-defined interfaces</li></ul>	<ul style="list-style-type: none"><li>• Primary interface</li><li>• Static routes</li><li>• Internal subnet prefix</li></ul>

### Backing Up to an FTP Server

Follow these steps to back up the controller network configuration to an FTP server.

1. Log on to the controller from the controller's command line interface (CLI). For more information, see the corresponding *Command Line Interface Reference Guide* for your controller platform.
2. At the prompt, enter **en** to enable privileged mode.



```
cb172651> en
Password: *****
```

**FIGURE 188** Enable privileged mode

3. Enter - to display the statuses of the node and the cluster.

Before continuing to the next step, verify that both the node and the cluster are in service.

**FIGURE 189** Verify that both the node and the cluster are in service

```
cb172651# show cluster-state
Current Node Status : In service
Cluster Status      : In service
Cluster Operation   : None
System Mode         : None
```

4. Enter backup network to back up the controller network configuration, including the control plane and data plane information.

The controller creates a backup of its network configuration on its database.

**FIGURE 190** Run backup network

```
#####
#      Welcome to SCG      #
#####
Password:
Please wait. CLI initializing...

Welcome to the Ruckus SmartCell Gateway 200 Command Line Interface
Version: 2.5.0.0.402

cb172651> en
Password: *****

cb172651# backup network
Do you want to backup network configurations (or input 'no' to cancel)? [yes/no] yes
Starting to backup network configurations...
Successful operation
```

5. Enter show backup-network to view a list of backup files that have been created.

Verify that the **Created On** column displays an entry that has a time stamp that is approximate to the time you started the backup.

**FIGURE 191** Enter the show backup-network command

```
cb172651# show backup-network
```

No.	Created on	Patch Version	File Size
1	2013-10-23 11:01:14 GMT	2.5.0.0.402	1.2K
2	2013-10-24 02:40:22 GMT	2.5.0.0.402	1.2K

6. Enter **copy backup-network {ftp-url}**, where *{ftp-url}* (remove the braces) is the URL or IP address of the FTP server to which you want to back up the cluster configuration.

The **CLI** prompts you to choose the number that corresponds to the backup file that you want to export to the FTP server.

7. Enter the number of the backup file that you want to export to the FTP server.

The controller encrypts the backup file, and then exports it to the FTP server. When the export process is complete, the following message appears on the **CLI**:

```
Succeed to copy to remote FTP server
Successful operation
```

**FIGURE 192** Succeed to copy to remote FTP server indicates that you have exported the backup file to the FTP server successfully

```
cb172651# copy backup-network ftp://david-ko:AAAAa123@10.2.2.162
No.    Created on          Patch Version      File Size
-----
1      2013-10-23 11:01:14 GMT  2.5.0.0.402      1.2K
2      2013-10-24 02:40:22 GMT  2.5.0.0.402      1.2K

Please choose a backup to send to remote FTP server or 'No' to cancel: 2
Starting to copy the chosen backup to remote FTP server...
Starting to encrypt backup file...
Succeed to copy to remote FTP server
Successful operation
```

8. Using an FTP client, log on to the FTP server, and then verify that the backup file exists.

The file format of the backup file is `network_<YYYYMMDDHHmmss>_<controller-version>.bak`.

For example, if you created the backup file on October 24th 2013 at 02:40:22 and the controller version is 2.5.0.0.402, you should see a file named `network_20131024024022_2.5.0.0.402.bak` on the FTP server.

You have completed backing up the controller to an FTP server.

## Restoring from an FTP Server

Before you continue, take note of the following limitations with restoring a backup file of the controller network configuration from an FTP server:

- Only release 2.1 and later support restoring from an FTP server.
- In this current release, restoring the entire cluster from an FTP server is unsupported. The restore process must be performed on one node at a time.
- Restoring from an FTP server can only be performed using the **CLI**.



### CAUTION

**Restoring a backup file to the controller requires restarting all of the controller services.**

Follow these steps to restore a backup file of the controller's network configuration that you previously uploaded to an FTP back to the controller.

1. Log on to the controller from the **CLI**. For more information, see the corresponding *Command Line Interface Reference Guide* for your controller platform.

- At the prompt, enter **en** to enable privileged mode.

**FIGURE 193** Enable privileged mode

```
cb172651> en
Password: *****
```

- Enter **show cluster-state** to display the statuses of the node and the cluster.  
Before continuing to the next step, verify that both the node and the cluster are in service.

**FIGURE 194** Verify that both the node and the cluster are in service

```
cb172651# show cluster-state
Current Node Status : In service
Cluster Status      : In service
Cluster Operation   : None
System Mode         : None
```

- Enter the following command to log on to the FTP server and check for available backup files that can be copied to the controller:

**copy <ftp-url> backup-network**

- If multiple backup files exist on the FTP server, the **CLI** prompts you to select the number that corresponds to the file that you want to copy back to the controller.

If a single backup file exists, the **CLI** prompts you to confirm that you want to copy the existing backup file to the controller.

When the controller finishes copying the selected backup file from the FTP server back to the controller, the following message appears: Succeed to copy the chosen file from the remote FTP server

- Enter **show backup-network** to verify that the backup file was copied back to the controller successfully.

**FIGURE 195** Verify that the backup file was copied to the controller successfully

```
cb172651# copy ftp://david-ko:AAAAa123@10.2.2.162 backup-network
Only one NetworkBackup file (network_20131024024022_2.5.0.0.402.bak) is found. Do you want to copy (or input 'no' to cancel)? [yes/no] yes
Starting to copy the chosen NetworkBackup file (network_20131024024022_2.5.0.0.402.bak) from remote FTP server...
Succeed to copy the chosen file from remote FTP server

cb172651# show backup-network
```

No.	Created on	Patch Version	File Size
1	2013-10-24 02:40:22 GMT	2.5.0.0.402	1.2K

- Run **restore network** to start restoring the contents of the backup file to the current controller.

The **CLI** displays a list of backup files, and then prompts you to select the backup file that you want to restore to the controller.

8. Enter the number that corresponds to the backup file that you want to restore.

**FIGURE 196** Enter the number that corresponds to the backup file that you want to restore

```
cbl72651# restore network
No.    Created on          Patch Version      File Size
-----
1      2013-10-24 02:40:22 GMT  2.5.0.0.402      1.2K

Please choose a backup to restore or 'No' to cancel: 1
The matched network setting for current system serial number is found from the chosen backup as below:

[Control Plane Interfaces]
Interface  IP Mode  IP Address      Subnet Mask      Gateway
-----
Control    Dhcp
Cluster    Dhcp
Managemen  Dhcp
t

Default Gateway Interface : Management
Primary DNS Server       : 172.17.17.16
Secondary DNS Server      :
Internal Subnet Prefix    : 10.254.1

[Control Plane User Defined Interfaces]
Name      IP Address      Subnet Mask      Gateway      VLAN  Interface  Service
-----
v100      172.17.26.103   255.255.255.0    172.17.26.1   100    Control    Hotspot
v102      172.17.26.102   255.255.255.0    172.17.26.1   102    Control    Hotspot
v101      172.17.26.101   255.255.255.0    172.17.26.1   101    Managemen  Hotspot
t

Please confirm this network setting, and this action will restart all services that will cause current SSH connection closed. Do you want to continue (or input 'no' to cancel)? [yes/no] yes
Not all services are healthy. Do you want to continue (or input 'no' to cancel)? [yes/no] yes
Process had been started before and running...
Starting to stop all SCG services...
```

The **CLI** displays the network configuration that the selected backup file contains.

If the serial number of the current controller matches the serial number contained in one of the backup files, the **CLI** automatically selects the backup file to restore and displays the network configuration that it contains.

9. Type **yes** to confirm that you want to restore the selected backup file. The controller starts the restore process and performs the following steps:

- a) Stop all services.
- b) Back up the current network configuration.

This will enable the controller to roll back to the current configuration, in case there is an issue with the restore process.

- c) Clean up the current network configuration.

The controller deletes its previous network configuration, including static routes, name server, user defined interfaces, etc.

10. Restore the network configuration contained in the selected backup file.

## 11. Restart all services.

When the restore process is complete, the following message appears on the CLI: All services are up!

**FIGURE 197** The controller performs several steps to restore the backup file

```
cal72651# restore network
Process had been started before and running...
Starting to stop all SCG services...
Checking action...Done!
Checking type...Done!
Checking creator...Done!
Checking reason...Done!
service stop flag file already exists, skip create it
07:28:24.342 [main] INFO c.ruckuswireless.wsg.cluster.Cluster - Load cluster environment file [/opt/ruckuswireless/wsg/conf/configurableSetting.properties]
wait for (CaptivePortal,Cassandra,Communicator,Configurer,EventReader,Greyhound,Memcached,Northbound,Scheduler,SubscriberManagement) Down!
wait for (Cassandra,Communicator,Configurer,EventReader,Greyhound,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Cassandra,Configurer,Memcached) Down!
wait for (Configurer) Down!
All services are down!
Stop service SCG done!
Starting to restore current system network setting...
Starting to backup current network settings for rollback
Starting to restore network configuration
Starting to delete the routes of control plane
Starting to delete the user interfaces of control plane
Starting to update the IP settings of control plane
Starting to update the DNS of control plane
Starting to update the internal subnet of control plane
Restarting control plane network
Starting to update the user interfaces of control plane
Restarting control plane network
Succeed to restore network configuration
Starting to start all SCG services...
Checking action...Done!
Checking type...Done!
Checking creator...Done!
Checking reason...Done!
service start flag file already exists, skip create it
wait for (CaptivePortal,Cassandra,Communicator,EventReader,Greyhound,Memcached,Monitor,Northbound,Scheduler,SubscriberManagement,SubscriberPortal,Web) Up!
wait for (CaptivePortal,Communicator,EventReader,Greyhound,Memcached,Monitor,Northbound,Scheduler,SubscriberManagement,SubscriberPortal,Web) Up!
wait for (CaptivePortal,Communicator,EventReader,Greyhound,Memcached,Monitor,Northbound,Scheduler,SubscriberManagement,SubscriberPortal,Web) Up!
wait for (CaptivePortal,Communicator,EventReader,Greyhound,Memcached,Monitor,Northbound,Scheduler,SubscriberManagement,SubscriberPortal,Web) Up!
wait for (Communicator,EventReader,Greyhound,Monitor,Northbound,Scheduler,SubscriberManagement) Up!
wait for (Monitor) Up!
wait for (Monitor) Up!
wait for (Monitor) Up!
All services are up!
```

12. Do the following to verify that the restore process was completed successfully:
  - a) Run show cluster-state to verify that the node and the cluster are back in service.
  - b) Run show interface to verify that all of the network configuration settings have been restored.

**FIGURE 198** Verify that the node and cluster are back in service and that the network configuration has been restored successfully

```
cb172651# show cluster-state
Current Node Status : In service
Cluster Status      : In service
Cluster Operation   : None
System Mode         : None

cb172651# show interface
Interfaces
-----
Interface   : Control
IP Mode     : Dhcp
IP Address  : 10.2.7.155
Subnet Mask : 255.255.0.0
Gateway     : 10.2.0.1

Interface   : Cluster
IP Mode     : Dhcp
IP Address  : 10.2.2.215
Subnet Mask : 255.255.0.0
Gateway     : 10.2.0.1

Interface   : Management
IP Mode     : Dhcp
IP Address  : 172.17.26.51
Subnet Mask : 255.255.254.0
Gateway     : 172.17.26.1

Default Gateway Interface : Management
Primary DNS Server       : 172.17.17.16
Secondary DNS Server      :

User Defined Interfaces
-----
IP Address      : 172.17.26.101
Subnet Mask     : 255.255.255.0
Gateway         : 172.17.26.1
VLAN            : 101
Physical Interface : Management
Service         : Hotspot

IP Address      : 172.17.26.103
Subnet Mask     : 255.255.255.0
Gateway         :
VLAN            : 100
Physical Interface : Control
```

You have completed importing and applying the network configuration backup from the FTP server to the controller.



## Backing up Cluster Configuration

Ruckus strongly recommends that you back up the controller database periodically. This will help ensure that you can restore the system configuration settings easily if the database becomes corrupted for any reason.

The following are backed up in the system configuration backup file:

**TABLE 51** Contents of a cluster configuration backup file

Configuration Data	Administration Data	Report Data	Identity Data
AP zones	Cluster backup	Saved reports	Created profiles
Third-party AP zones	System configuration backups	Historical client statistics	Generated guest passes
Services and profiles	Upgrade settings and history	Network tunnel statistics	
Packages	Uploaded system diagnostic scripts		
System settings	Installed licenses		
Management domains			
Administrator accounts			
MVNO accounts			

A system configuration backup does not include control plane settings, data plane settings, and user-defined interface settings.

1. Go to **Administration > Backup and Restore**.
2. Select the **Configuration** tab.
3. In System Configuration Backup History, click **Backup**.

The following confirmation message appears: Are you sure you want to back up the controller's configuration?

4. Click **Yes**.

A progress bar appears as the controller creates a backup of the its database. When the backup process is complete, the progress bar disappears, and the backup file appears under the **System Configuration Backup History** section.

## Scheduling a Configuration Backup

You also have the option to configure the controller to backup its configuration automatically based on a schedule you specify.

1. Go to **Administration > Backup and Restore**.
2. Select the **Configuration** tab.
3. In Schedule Backup, you can configure the controller to backup its configuration automatically based on a schedule you specify.
  - a. In Schedule Backup, click **Enable**.
  - b. In Interval, set the schedule when the controller will automatically create a backup of its configuration. Options include: Daily, Weekly and Monthly.
  - c. Hour: Select the hour of the day when the controller must generate the backup.
  - d. Minute: Select the minute of the hour.
  - e. Click **OK**.

You have completed configuring the controller to create a backup automatically.

## Exporting the Configuration Backup to an FTP Server Automatically

In addition to backing up the configuration file manually, you can configure the controller to export the configuration file to an FTP server automatically whenever you click **Backup**.

Follow these steps to back up the configuration file to an FTP server automatically.

1. Go to **Administration > Backup and Restore**.
2. Select the **Configuration** tab.
3. In Auto Export Backup, you can configure the controller to export the configuration file to an FTP server automatically whenever you back up the configuration file.
  - a. In Auto Export Backup, click **Enable**.
  - b. FTP Server: Select the FTP server to which you want to export the backup file.
  - c. Click **Test**. The controller attempts to establish connection to the FTP server using the user name and password that you supplied. If the connection attempt is successful, a success message is displayed. If the connection attempt is unsuccessful, verify that the FTP server details (including the user name and password) are correct, and then click **Test** again.
  - d. Click **OK**.
4. After you verify the controller is able to connect to the FTP server successfully, click **OK** to save the FTP server settings.

You have completed configuring the controller to export the configuration backup file to an FTP server.

## Downloading a Copy of the Configuration Backup

After you create a configuration backup, you have the option to download the backup file from the **System Configuration Backups History** section.

1. Go to **Administration > Backup and Restore**.
2. Select the **Configuration** tab.
3. Locate the entry for the backup file that you want to download. If multiple backup files appear on the list, use the date when you created the backup to find the backup entry that you want.
4. Click **Download**.

Your web browser downloads the backup file to its default download folder. NOTE: When your web browser completes downloading the backup file, you may see a notification at the bottom of the page.
5. Check the default download folder for your web browser and look for a file that resembles the following naming convention: **{Cluster Name}\_BackupConf\_{MMdd}\_db\_{MM}\_{dd}\_{HH}\_{mm}.bak**

For example, if the controller cluster is named Cluster A and you created the configuration backup on September 7 at 11:08 AM, the backup file name will be: **ClusterA\_BackupConf\_0907\_db\_09\_07\_11\_08.bak**

You have completed downloading a copy of the configuration backup.

## Restoring a System Configuration Backup

In the event of a failure or emergency where you may need to go back to the previous version of a cluster, you will have to restore your system configuration backup and restart the cluster.

1. Go to **Administration > Backup and Restore**.
2. Select the **Configuration** tab.

3. Once you locate the backup file, click **Restore** that is in the same row as the backup file. A confirmation message appears.

**NOTE**

Take note of the backup version that you are using. At the end of this procedure, you will use the backup version to verify that the restore process was completed successfully.

4. Click **Yes**. The following message appears: `System is restoring. Please wait...` When the restore process is complete, the controller logs you off the web interface automatically.
5. Log on to the controller web interface.  
Check the web interface pages and verify that the setting and data contained in the backup file have been restored successfully to the controller.

You have completed restoring a system configuration backup file.

## Upgrading the Controller

Ruckus may periodically release controller software updates that contain new features, enhancements, and fixes for known issues. These software updates may be made available on the Ruckus support website or released through authorized channels.



**CAUTION**

**Although the software upgrade process has been designed to preserve all controller settings, Ruckus strongly recommends that you back up the controller cluster before performing an upgrade. Having a cluster backup will ensure that you can easily restore the controller system if the upgrade process fails for any reason.**



**CAUTION**

**Ruckus strongly recommends that you ensure that all interface cables are intact during the upgrade procedure.**



**CAUTION**

**Ruckus strongly recommends that you ensure that the power supply is not disrupted during the upgrade procedure.**

## Performing the Upgrade

Ruckus strongly recommends backing up the controller cluster before performing the upgrade. If the upgrade process fails for any reason, you can use the latest backup file to restore the controller cluster.

Before starting this procedure, you should have already obtained a valid controller software upgrade file from Ruckus Support Team or an authorized reseller.

Always back up the controller before attempting a software upgrade. If you are managing a multi-node cluster, back up the entire cluster, and then verify that the backup process completes successfully.

If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server.

1. Copy the software upgrade file that you received from Ruckus to the computer where you are accessing the controller web interface or to any location on the network that is accessible from the web interface.
2. Go to **Administration > Upgrade**.

3. Select the **Upgrade** tab.

In Current System Information, the controller version information is displayed.

**NOTE**

The **Upgrade History** tab displays information about previous cluster upgrades.

4. In Upload, select the **Run Pre-Upgrade Validations** check box to verify if the data migration was successful. This option allows you to verify data migration errors before performing the upgrade.
5. Click **Browse** to select the patch file.
6. Click **Upload** to upload the controller configuration to the one in the patch file.

The controller uploads the file to its database, and then performs file verification. After the file is verified, the **Patch for Pending Upgrade** section is populated with information about the upgrade file. If data migration was unsuccessful, the following error is displayed: `Exception occurred during the validation of data migration. Please apply the system configuration backup and contact system administrator.`

7. You can now:
  - Click **Upgrade** to start the upgrade process without backing up the current controller cluster or its system configuration, or
  - Click **Backup & Upgrade** to back up the controller cluster and system configuration before performing the upgrade.

When the upgrade (or backup-and-upgrade) process is complete, the controller logs you off the web interface automatically. When the controller log on page appears again, you have completed upgrading the controller.

In the **Current System Information** section, check the value for controller version. If the firmware version is newer than the firmware version that controller was using before you started the upgrade process, then the upgrade process was completed successfully.

**NOTE**

APs periodically send scheduled configuration requests to the controller, including the firmware version. Therefore, when an AP joins a zone for the first time, the firmware version is verified by the controller. If the firmware version is different from that which is configured for the zone, the controller responds with a request to upgrade it, after which the AP initiates a request to upgrade the firmware using HTTP.

## Uploading an AP Patch File

New AP models and firmware updates are supported without the need to upgrade the controller image by using the AP patch files supplied by Ruckus.

1. Go to **Administration > Upgrade**.
2. Select the **AP Patch** tab.
3. In Patch File Upload, click **Browse** to select the patch file (with extension .patch).
4. Click **Open**.
5. Click **Upload**. The upload status bar is displayed, and after the patch file is uploaded, the section is populated with the patch filename, size, firmware version, and supporting AP models.
6. Click **Apply Patch**. The apply patch status bar is displayed.

After the patch file is updated, you will be prompted to log out.

When you login again, the **AP Patch History** section displays information about the patch file such as start time, AP firmware and model.

You have successfully updated the AP models and AP firmware with the patch file, without having to upgrade the controller software.

## Verifying the Upgrade

You can verify that the controller upgrade was completed successfully.

1. Go to **Administration > Upgrade**.
2. In the **Current System Information** section, check the value for *Controller Version*. If the firmware version is newer than the firmware version that controller was using before you started the upgrade process, then the upgrade process was completed successfully.

### NOTE

APs periodically send scheduled configuration requests to the controller, including the firmware version. Therefore, when an AP joins a zone for the first time, the firmware version is verified by the controller. If the firmware version is different from that which is configured for the zone, the controller responds with a request to upgrade it, after which the AP initiates a request to upgrade the firmware using HTTP.

## Rolling Back to a Previous Software Version

There are scenarios in which you may want to roll back the controller software to a previous version.

Here are two:

- You encounter issues during the software upgrade process and the controller cannot be upgraded successfully. In this scenario, you can only perform the software rollback from the CLI using the `restore local` command. If you have a two-node controller cluster, run the `restore local` command on each of the nodes to restore them to the previous software before attempting to upgrade them again.
- You prefer a previous software version to the newer version to which you have upgraded successfully. For example, you feel that the controller does not operate normally after you upgraded to the newer version and you want to restore the previous software version, which was more stable. In this scenario, you can perform the software rollback either from the web interface or the CLI. If you have a two-node controller cluster, you must have cluster backup on both of the nodes.

To ensure that you will be able to roll back to a previous version, Ruckus strongly recommends the following before attempting to upgrade the controller software:

- Always back up the controller before attempting a software upgrade. If you are managing a multi-node cluster, back up the entire cluster, and then verify that the backup process completes successfully. See [Creating a Cluster Backup](#) on page 381 for the local backup instructions. If you have a local backup and you want to roll back the controller to a previous software version, follow the same procedure described in [Creating a Cluster Backup](#) on page 381.
- If you have an FTP server, back up the entire cluster and upload the backup files from all the nodes in a cluster to a remote FTP server. See [Backing Up to an FTP Server](#) on page 382 for remote backup instructions and [Restoring from an FTP Server](#) on page 384 for remote restore instructions.

## Upgrading the Data Plane

You can view and upgrade the virtual data plane version using patch files. This feature is applicable only for virtual platforms.

### Upgrading vSZ-D

vSZ support APs starting version 3.4. You must first upgrade vSZ before upgrading vSZ-D, because only a new vSZ can handle an old vSZ-D. There is no order in upgrading the AP zone or vSZ-D. During the vSZ upgrade, all tunnels stay up except the main tunnel which moves to the vSZ. Once the upgrade procedure is completed, allow ten minutes for the vSZ-D to settle.

Upgrade to R5.0 does not support data migration (statistics, events, administrator logs). Only the existing system and the network configuration is preserved. For more information, contact Ruckus support.

Upgrading from earlier versions to R5.0.x

SZ	vSZ-D	Upgrade Procedure
3.6.x	R3.6.x or R3.5.x or R3.4	<ol style="list-style-type: none"><li>1. R3.5.x/R3.4.x &gt; R3.6.x</li><li>2. R3.6. &gt; R5.0</li></ol>
3.5.x	R3.5.x or R3.4.x or R3.2.x	<ol style="list-style-type: none"><li>1. R3.4.x/R3.2.x &gt; R3.5.x</li><li>2. R3.5.x &gt; R3.6.x</li><li>3. R3.6.x &gt; R5.0.x</li></ol>
3.4.x	R3.4.x or R3.2.x	<ol style="list-style-type: none"><li>1. R3.2.x &gt; R3.4.x</li><li>2. R3.4.x &gt; R3.6.x</li><li>3. R3.6. x &gt; R5.0.x</li></ol>

Upgrading from R5.1.x (Long-term Support)/R5.0.x (Short-term Support) to R5.2.x (Short-term Support)

SZ	vSZ-D	Upgrade Procedure
R5.1.x (LTS)	R5.1.x or R5.0.x or R3.6	<ol style="list-style-type: none"><li>1. R5.0.x/R3.6.x &gt; R5.1.x</li><li>2. R5.1.x to R5.2.x</li></ol>
R5.0.x (STS)	R5.0.x or R3.6	<ol style="list-style-type: none"><li>1. R5.0.x/R3.6.x &gt; R5.1.x</li><li>2. R5.1.x to R5.2.x</li></ol>

### Upgrading SZ100-D

SZ100-D is shipped with 3.6.1 release version and you must upgrade it to 5.1 release version. As vSZ manages SZ100-D, ensure that vSZ has the same or later version than SZ100-D. Otherwise, upgrade vSZ before upgrading SZ100-D.

To Upgrade the Data Plane:

1. Go to **Administration > Upgrade**.

2. Select the **DP Patch** tab.  
The **DP Patch** page appears.

**FIGURE 199 DP Patch - Data Plane Upgrade**

vSZ-D

SZ-D

Patch Available for Upgrade

Patch File Name

sz100d-installer\_5.1.0.0.299.img

Patch File Size

220.1MB

Patch Version

5.1.0.0.299

Data Planes

Backup

Restore

Upgrade to 5.1.0.0.299

<input type="checkbox"/>	Name	DP MAC Address	Current Firmware	Backup Firmware	Last Backup Time	Process State	DP Status
<input type="checkbox"/>	SZ100-D	94:F6:65:2A:49:40	5.1.0.0.297	5.1.0.0.297	2018-08-08 14:54:17	Backup completed	Managed

3. In **Patch File Upload**, click **Browse** to select the patch file (.ximg file).
4. Click **Upload**. The patch files is uploaded.
- The controller automatically identifies the Type of DP (vSZ-D or SZ-D) and switches to the specific Tab page. Uploads the file to its database, and then performs file verification. After the file is verified, the **Patch for Pending Upgrade** section is populated with information about the upgrade file.
- The following details are displayed:
- Patch File Name: Displays the name of the patch file.
  - Patch File Size: Displays the size of the patch file.
  - Patch Version: Displays the version of the patch file.
5. In **Data Planes**, identify the data plane you want to upgrade, and then choose a patch file version from **Select upgrade version**.
6. Click **Apply** to apply the patch file version to the virtual data plane.

The following information about the virtual data plane is displayed after the patch file upgrade is completed.

- Name: Displays the name of the virtual data plane.
- DP MAC Address: Displays the MAC IP address of the data plane.
- Current Firmware: Displays the current version of the data plane that has been upgraded.
- Backup Firmware: Displays the backup version of the data plane.
- Last Backup Time: Displays the date and time of last backup.
- Process State: Displays the completion state of the patch file upgrade for the virtual data plane.
- DP Status: Displays the DP status.

You have successfully upgraded the virtual data plane.

NOTE

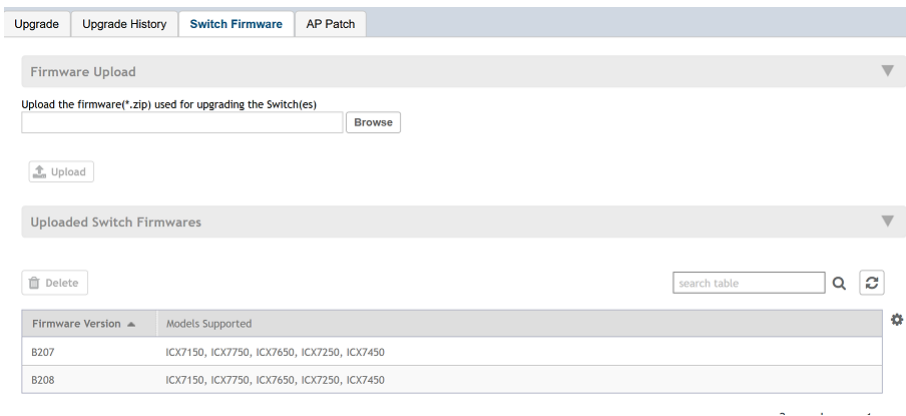
To have a copy of the data plane firmware or move back to the older version, you can select the data plane from the list and click **Backup** or **Restore** respectively.

Uploading the Switch Firmware to the Controller

You can upload the latest available firmware to a switch from the controller, thereby upgrading the firmware version of the switch.

- 1. Select **Administration > Upgrade**.
- 2. Select the **Switch Firmware** tab.

FIGURE 200 Upgrading the Switch Firmware



- 3. In Firmware Upload click **Browse** to select the firmware file for upgrading the switch.
- 4. Click **Open**.
- 5. Click **Upload**. The upload status bar is displayed, and after the firmware file is uploaded, the **Uploaded Switch Firmwares** section is populated with the firmware version and switch models it supports.

You have successfully uploaded the switch firmware to the controller.

Managing Licenses

Depending on the number of Ruckus APs that you need to manage with the controller, you may need to upgrade the controller license as your network expands.

The maximum number of access points that the controller can manage is controlled by the license file that came with the controller. If the number of access points on the network exceeds the limit in the license file, you will need to obtain an additional license file and upload it to the controller.

NOTE

For information on obtaining additional license files, contact Ruckus Support Team or an authorized Ruckus reseller.

The maximum number of access points that a license supports depends on its stock-keeping unit (SKU).



## Viewing Installed Licenses

You can synchronize the license data, import a license file into the controller if it is unable to connect to the Ruckus SmartLicense system, and release licenses bound to an offline controller by downloading a copy of the licenses.

Perform these steps to check installed licenses.

1. Go to **Administration > Licenses**.
2. Select the **Installed Licenses** tab.

The **List** view is displayed as shown in the following example.

3. Select **List** as the View Mode.

The license **List** view is displayed as shown in the following example.

**FIGURE 201** License List View

Name	Node	Start Date	Expiration Date	Capacity	Description
CAPACITY-AP	vSZ-H-R1	2015/12/08	2018/09/24	100	SZ/(v)SCG AP license for 1 AP
CAPACITY-AP	vSZ-H-R2	2015/12/08	2018/09/24	10	SZ/(v)SCG AP license for 1 AP
CAPACITY-AP-BUNDLED	vSZ-H-R2		Permanent	1	Default AP Capacity License for vSZ
CAPACITY-AP-BUNDLED	vSZ-H-R1		Permanent	1	Default AP Capacity License for vSZ
CAPACITY-DP-RWAG-DEFAULT	vSZ-H-R1	2018/07/10	2018/10/08	1	Default Third Party AP License for Data Plane. 1 license su...
CAPACITY-DP-RWAG-DEFAULT	vSZ-H-R2	2018/07/10	2018/10/08	1	Default Third Party AP License for Data Plane. 1 license su...

In the **List** view, the following information is displayed for licenses that have been uploaded to the controller:

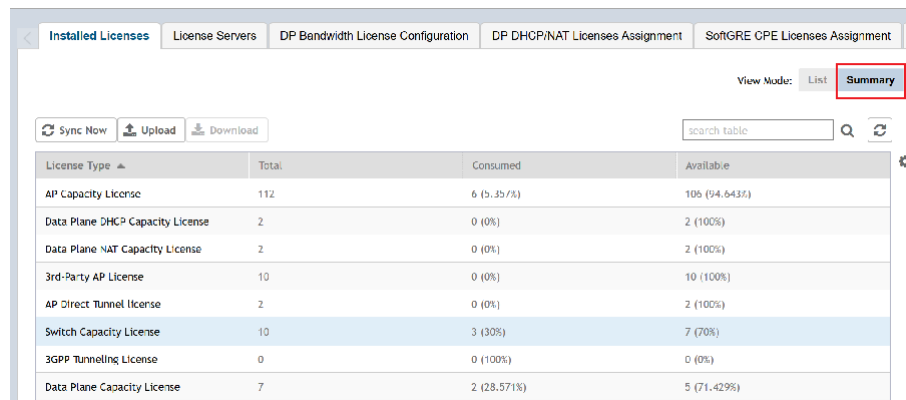
- **Name:** The name of the node to which the license was uploaded
- **Node:** The name of the controller node
- **Start Date:** The date when the license file was activated
- **Expiration Date:** For time-bound licenses, the date when the license file expires
- **Capacity:** The number of units or license seats that the license file provides
- **Description:** The type of license

4. Select **Summary** as the View Mode.

In the **Summary** view, the information shown in the following example is displayed for the licenses that have been uploaded to the controller.

- License Type: The type of license uploaded
- Total: The total licenses (both consumed and available)
- Consumed: The number of licenses consumed
- Available: The licenses available

**FIGURE 202** License Summary View



License Type	Total	Consumed	Available
AP Capacity License	112	6 (5.357%)	106 (94.643%)
Data Plane DHCP Capacity License	2	0 (0%)	2 (100%)
Data Plane NAT Capacity License	2	0 (0%)	2 (100%)
3rd-Party AP License	10	0 (0%)	10 (100%)
AP Direct Tunnel License	2	0 (0%)	2 (100%)
Switch Capacity License	10	3 (30%)	7 (70%)
3GPP Tunneling License	0	0 (100%)	0 (0%)
Data Plane Capacity License	7	2 (28.571%)	5 (71.429%)

## Importing Installed Licenses

If the controller is disconnected from the Internet or is otherwise unable to communicate with the Ruckus SmartLicense system (due to firewall policies, etc.), you can manually import a license entitlement file into the controller.

### NOTE

The option to import a license file manually into the controller is only available if the controller is using the cloud license server.

1. Obtain the license file. You can do this by logging on to your Ruckus Support account, going to the license management page, and then downloading the license file (the license file is in .bin format).
2. Log on to the controller web interface, and then go to **Administration > Licenses**.
3. Select the **Installed Licenses** tab.
4. Select the node for which you are uploading the license file and click **Upload**.

The **Upload License** page appears where you must provide the following information:

- Select Controller: Select the node for which you are uploading the license file.
- Select License File: Click **Browse**, locate the license file (.bin file) that you downloaded from your Ruckus Support account, and then select it.

The page refreshes, and the information displayed changes to reflect the updated information imported from the SmartLicense platform.

## Synchronizing Controller with the License Server

By default, the controller automatically synchronizes its license data with the selected license server every 24 hours. If you made changes to the controller licenses (for example, you purchased additional licenses) and you want the controller to download the updated license data immediately, you can trigger a manual synchronization.

1. Log on to the controller web interface, and then go to **Administration > Licenses**.
2. Select the **Installed Licenses** tab.
3. Click **Sync Now**.

When the sync process is complete, the message `Sync license with the license server successful` appears. If the previously saved license data are different the latest license data on the server, the information in the Installed Licenses section refreshes to reflect the latest data.

You have completed manually synchronizing the controller with the license server.

## Downloading License Files

If you need to release licenses bound to an offline controller and allow those licenses to be used elsewhere (on a different controller), you can download a copy of the controller licenses. The option to download a copy of the controller licenses is only available if the controller is using the Ruckus cloud license server.

1. Log on to the controller web interface, and then go to **Administration > Licenses**.
2. Select the **Installed Licenses** tab.
3. Click **Download**.

The **Download License** page appears. In **Select Controller**, select the controller node for which you want to download the license files.

### NOTE

You can upload and download license files only if the controller is using the Ruckus cloud license server.

4. Click **Download**. Your web browser downloads the license files from the controller.
5. When the download is complete, go to the default download folder that you have configured for your web browser, and then verify that the binary copy of the license files (with .bin extension) exists.

You have completed downloading copies of the controller licenses.

## Configuring the License Server

Ruckus provides two options for managing the licenses that you have purchased for the controller - Cloud License Server and Local License Server (LLS).

Cloud License Server also known as the SmartLicense server, this a cloud-based server that stores all of the licenses and support entitlements that you have purchased for the controller. For information on how to set up and activate your SmartLicense account, see the SmartLicense User Guide.

1. Go to **Administration > Licenses**.
2. Select the **License Server** tab.

The Server details and Synchronization history are displayed.

3. Click **Configure**.

The **License Server Configuration** page appears.

- Cloud License Server: Select this option to use the Ruckus SmartLicense server.
- Local License Server: Select this option to use an LLS that you have set up on the network, and then configure
  - Domain or IP: Type the FQDN or IP address of the LLS.
  - Port: Type the port number. Port range is from 0 to 65535 (default is 3333).

4. Click **OK**.

5. Click **Sync Now** and the controller saves the selected license server configuration, deletes all of its saved license data, and then automatically synchronizing the license information with the selected license server.

You have completed configuring the license server that the controller will use.

## Configuring License Bandwidth

You can assign a license bandwidth for a virtual data plane provided it is already approved. Each virtual data plane can be configured with only one bandwidth license. This feature is applicable only to virtual platforms.

1. Go to **Administration > Licenses**.
2. Select the **License Bandwidth Configuration** tab.

The **License Bandwidth Configuration** page appears.

**FIGURE 203** License Bandwidth Configuration

The screenshot shows the 'License Bandwidth Configuration' interface. At the top, there are three tabs: 'Installed Licenses', 'License Servers', and 'License Bandwidth Configuration'. The 'License Bandwidth Configuration' tab is selected. Below the tabs, there is a form with two main sections. The first section is for adding a new configuration, with a 'vSZ-D' field containing 'vSZ-D' and a 'Bandwidth' dropdown menu showing 'No data available'. There are 'Add', 'Cancel', and 'Delete' buttons next to this section. The second section is a table with two columns: 'vSZ-D' and 'Bandwidth'. The table contains one row with 'vSZ-D' as '8799-vDP' and 'Bandwidth' as '1Gbps'. Below the table, it indicates '1 total records'. At the bottom of the page, there are 'OK' and 'Cancel' buttons.

3. In **vSZ-D**, type the name of the virtual data plane.
4. From the **Bandwidth** drop-down menu, select the license bandwidth you want to assign to the virtual data plane. Default is 1Gbps.
5. Click **Add**. The vSZ-D with the assigned license bandwidth is displayed.
6. Click **OK**.

The message `Submitting form` appears, and the vSZ-D is assigned a bandwidth.

You have successfully assigned a license bandwidth to the virtual data plane.

## Configuring the DHCP/NAT License Assignment

### Configuring the DHCP/NAT License Assignment

License assignment specifies the capability of each Data Plane, which has the ability to assign IPs by DHCP feature and translate packets by NAT feature. Though these features already exist, starting 5.0, customers must purchase license to enable these features.

#### NOTE

This feature is supported only on virtual platform.

### Creating DHCP License Assignment

Licensing needs to be created on a per SZ Controller Cluster basis.

To create the DHCP License assignment:

1. Go to **Administration > Licenses**.
2. Select the **DP DHCP/NAT License Assignment** tab.
3. From the **DHCP License** area, click **Create**.

The **DHCP License** form appears.

- **License Usage:** Lists the details of license consumption and availability.
- **Data Plane 1:** Select the primary data plane from the drop-down. To remove the Data Plane from the DHCP license assignment, select **Clear**.
- **Data Plane 2:** Select the secondary data plane from the drop-down. To remove the Data Plane from the DHCP license assignment, select **Clear**.
- **License Count:** Enter the number of license. Range: 1 through 101.
- **IP Leases:** Lists the number of IPs assigned.
- **Description:** Enter a short description about the license assignment.

4. Click **OK**.

You have created the DHCP license assignment.

#### NOTE

To edit or remove the license assignment on the data plane, select the assignment from the list and click **Configure** or **Delete** respectively.

### Creating NAT License Assignment

Licensing needs to be created on a per SZ Controller Cluster basis.

To create the NAT License assignment:

1. Go to **Administration > Licenses**.
2. Select the **DP DHCP/NAT License Assignment** tab.

3. From the **NAT License** area, click **Create**.

The **NAT License** form appears.

- **License Usage:** Lists the details of license consumption and availability.
- **Data Plane:** Select the data plane from the drop-down. To remove the Data Plane from the NAT license assignment, select **Clear**.
- **License Count:** Enter the number of license for the data plane. Range: 1 through 20.
- **NAT Sessions/Flows:** Lists the number of NAT sessions/flows.
- **Description:** Enter a short description about the license assignment.

4. Click **OK**.

You have created the NAT license assignment.

#### NOTE

To edit or remove the license assignment on the data plane, select the assignment from the list and click **Configure** or **Delete** respectively.

## Configuring URL Filtering Licenses

You can configure the number of URL filtering licenses on an AP within the zone.

You can both limit the number of URL filtering licenses per zone, and also configure the AP to have unlimited licenses.

If an AP has URL filtering license enabled, then URL filtering can be enabled for all WLANs within the same zone.

If the URL filtering license is deleted in a zone, URL filtering services are disabled on all the WLANs within that zone. If you want to add the license back again, you simply have to enable URL filtering on the zone or WLAN.

If the license is limited to the zone, you cannot move or add more APs with URL filtering enabled to that zone. For example, if you have set the License limit to 3, you cannot add a fourth AP to the zone.

#### NOTE

Number of trial licenses for SZ100 and vSZ-E controllers is 1000.

1. Go to **Administration > Licenses**.
2. Select the **URL Filtering Licenses** tab.

The **URL Filtering Licenses** page displays the following:

**FIGURE 204** URL Filtering Licenses



URL Filtering Licenses (used0, unused20000)			
The URL Filtering license are distributed automatically to each zone when filtering is turned on a WLAN in that zone.			
<a href="#">Configure</a> <a href="#">Remove</a>		search table	<a href="#">Q</a> <a href="#">↺</a>
Zone Name	Number of Licenses	License Limit	WLANs with URL Filtering ON

- **Zone Name:** name of the zone within which APs are present
- **Number of Licenses:** displays the total licenses allocated to the zone
- **License Limit:** can be set to a value or can be Unlimited. This displays the number of APs (with URL filtering enabled) that can be accommodated within the zone.
- **WLANs with URL Filtering ON:** displays all the WLANs within the zone that have the URL filtering service enabled

3. Select the URL license and click **Configure**.  
The **URL Filtering Licenses** page appears.
4. Configure the License Limit as appropriate for the zone.
5. Click **OK**.

## ZoneDirector to SmartZone Migration

SmartZone controllers are better equipped to handle large WiFi deployments such as within campuses and when customers are vastly distributed; therefore, Ruckus recommends that you migrate existing ZoneDirector deployments to SmartZone controller deployments. You can migrate ZoneDirector AP configuration information to SmartZone controllers from the controller itself, using a migration tool.

The AP models should be supported by the controller.

### NOTE

ZD versions 9.13 and 10 are supported.

1. Go to **Administration > ZD Migration**.  
The **ZoneDirector Migration** page appears.
2. Configure the following:
  - a. ZoneDirector IP Address: Type the IP address of the ZD that you want to migrate.
  - b. Admin Credentials: Enter the username and password details to access/login to ZD.
  - c. Click **Connect**. Lists of APs connected to the ZD deployment are displayed.
  - d. Click **Select AP** to choose the AP information that you want to migrate from ZD.
  - e. Click **Migrate** to migrate the AP. The controller imports the ZD configuration and applies it to the selected AP.

The **ZoneDirector Migration Status** section displays the status of the migration. When completed successfully, a success message is displayed. If migration fails, a failure message is displayed and you can attempt the migration process again.

## Monitoring Administrator Activities

The controller keeps a record of all actions and configuration changes that administrators perform on the server. This feature enables you and other administrators in the organization to determine what changes were made to the controller and by whom.


1. Go to **Administration > Admin Activities**.

2. Select the **Admin Activities** tab. the **Admin Activities** page displays the administrator actions.

The following information is displayed:

- Date and Time: Date and time when the alarm was triggered
- Administrator: Name of the administrator who performed the action
- Source IP: Displays the IP address of the device from which the administrator manages the controller.
- Browser IP: IP address of the browser that the administrator used to log on to the controller.
- Action: Action performed by the administrator.
- Resource: Target of the action performed by the administrator. For example, if the action is Create and the object is Hotspot Service, this means that the administrator created a new hotspot service.
- Description: Displays additional details about the action. For example, if the administrator created a new hotspot service, this column may show the following: **Hotspot [company\_hotspot]** .



Click  to export the administrator activity list to a CSV file. You can view the default download folder of your web browser to see the CSV file named **clients.csv**. Use a spreadsheet application (for example, Microsoft® Excel®) to view the contents of the CSV file.



# Diagnostics

---

• Applying Scripts.....	405
• Uploading AP CLI Scripts.....	405
• Viewing and Downloading Logs.....	410
• RADIUS.....	411

## Applying Scripts

New AP models and firmware updates are supported without the need to upgrade the controller image by using AP patch files and diagnostic scripts.

1. Go to **Administration > Diagnostics > Scripts**.
2. Select the **Patch/Diagnostic Scripts** tab.
3. Select the **Upload to current node** check-box.
4. Click **Browse** to select a script that you want to upload to the controller.
5. Click **Upload**.

The script is listed in the **System Uploaded Scripts** section.

If you have uploaded a patch script, it is displayed in the **System Uploaded Patch Scripts** section with the following information:

- Name of the patch file
- Patch file description
- Supported AP firmware version
- AP model number

Click **Delete** to delete scripts.

6. Click **Apply Patch** to apply the patch file to the AP model or firmware as appropriate.

You have successfully applied scripts to the controller AP.

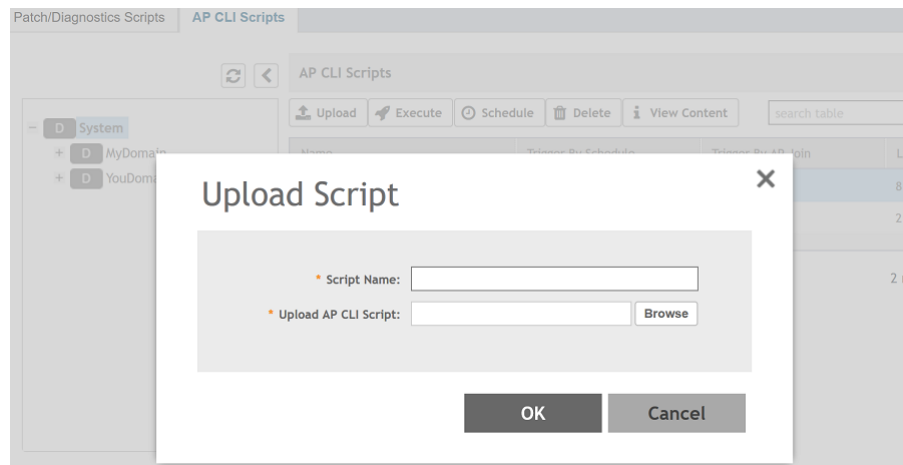
## Uploading AP CLI Scripts

You can upload AP CLI scripts to the controller which make the controller compatible with new AP models and new firmware without the need to upgrade the controller image.

1. Go to **Administration > Diagnostics > Scripts**.
2. Select the **AP CLI Scripts** tab.
3. From the domain tree, choose the AP zone for which you want to apply the script.

4. Click **Upload**.  
The Upload page appears.

**FIGURE 205** Uploading scripts



5. In **Script Name**, enter the name of the script you want to upload.
6. Click **Browse** to select an AP CLI script that you want to upload.
7. Click **OK** to apply the AP CLI script file to the AP zone.

You have successfully uploaded AP CLI scripts to the controller AP.

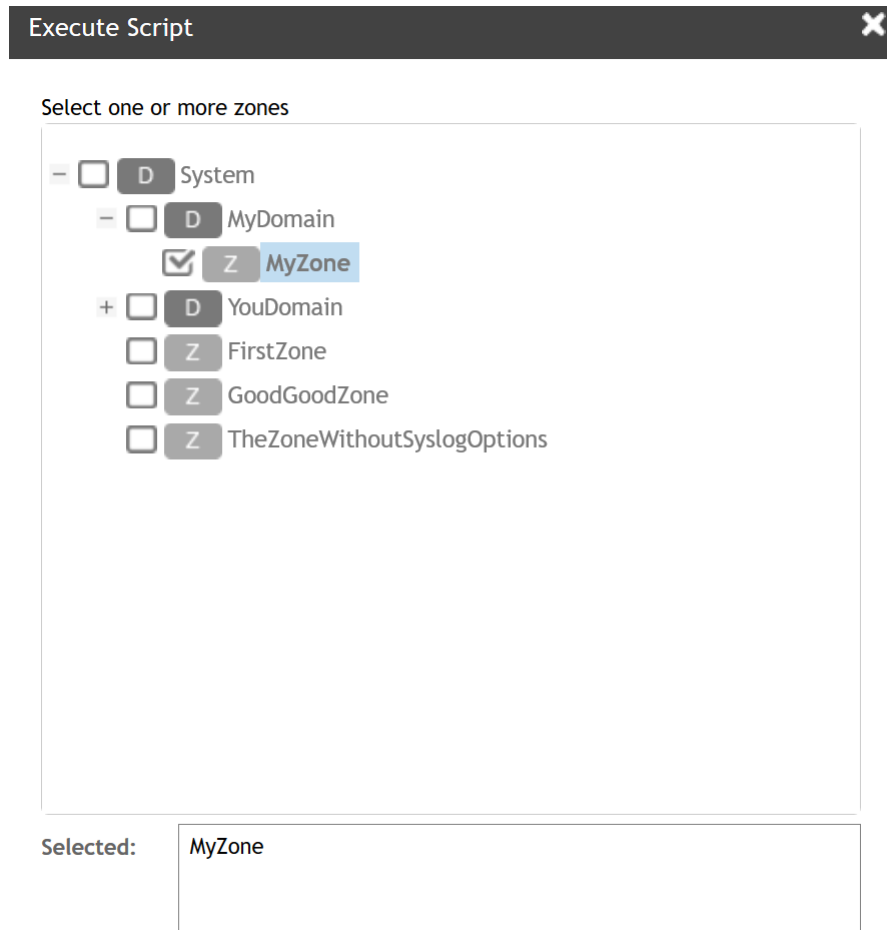
## Executing AP CLI Scripts

You can upload AP CLI Scripts to be run on APs within selected zones, and execute them immediately or on-demand.

1. Go to **Administration > Diagnostics > Scripts**.
2. Select the **AP CLI Scripts** tab.
3. From the domain tree, choose the domain in which the AP is present.
4. Select the script from the list of scripts in the **AP CLI Scripts** table.

- Click **Execute**.  
The **Execute Script** page appears.

**FIGURE 206** Executing script



- Select one or more zones from the domain tree.
- Click **OK** to run the AP CLI script on the AP zone.

The controller runs the selected script on the specified zone.

## Scheduling AP CLI Scripts

You can upload AP CLI Scripts to be run on APs within selected zones. You can also schedule the script to be run on the APs at a particular time or when the AP joins the zone.

- Go to **Administration > Diagnostics > Scripts**.
- Select the **AP CLI Scripts** tab.
- From the domain tree, choose the domain in which the AP is present.
- Select the script from the list of scripts in the **AP CLI Scripts** table.

5. Click **Schedule**.  
The **Schedule Script** page appears.

**FIGURE 207** Scheduling scripts

**Schedule Script**

Execute on a Schedule: ☒ ON

Current System Time Zone is (GMT+8:00) Asia/Taipei.

\* Interval:

\* Time:

AP Joins Zone: ☒ ON

Select Zones:

\* Selected:

6. Configure the following:
  - Execute on a Schedule: Enable this option to execute the script based on the current system time which is displayed.
  - Interval: select the time interval within which you want to schedule the execution. Options include Daily, Weekly and Monthly.
  - Time: from the drop-down menu, select the hours and minute when the script must be executed
  - AP Joins the Zone: enabling this will ensure the script is run on the AP when it joins a particular zone.
7. To select the zone, click **Select**.  
The **Select Zone** page appears. Identify and select the zone. The selected zone is populated in the **Selected** area.
8. Click **OK**.

The schedule is configured and the script will run on the AP as planned.

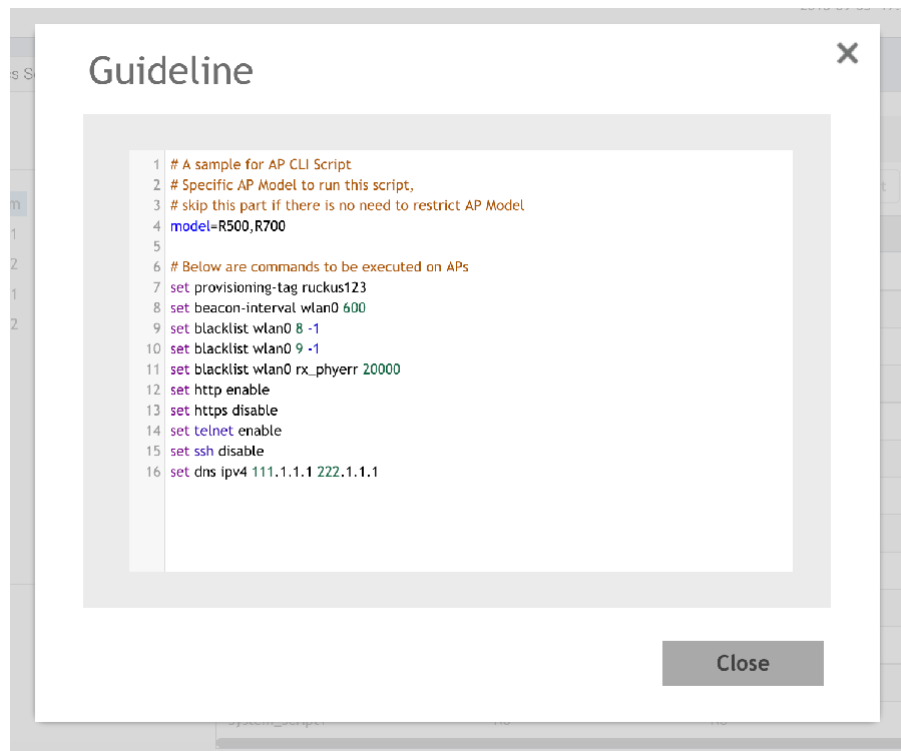
## Viewing Scripts

You can open the AP CLI script and view the script details.

1. Go to **Administration > Diagnostics > Scripts**.
2. Select the **AP CLI Scripts** tab.
3. From the domain tree, choose the domain in which the AP is present.
4. Select the script from the list of scripts in the **AP CLI Scripts** table.

- Click **View Content**.  
The script page appears.

**FIGURE 208** Viewing script details



- Click **Close**.

## Viewing Script Execution Summary

After an AP CLI script is executed on-demand or as per schedule, you can view details of the execution from the **History** tab.

- Go to **Administration > Diagnostics > Scripts**.
- Select the **AP CLI Scripts** tab.
- From the domain tree, choose the domain in which the AP is present.
- Select the script from the list of scripts in the **AP CLI Scripts** table.
- In the History tab below, you will see the list of scripts that were executed.

- To view the execution summary of a script, select a script from this list and click **View Execution Summary**.  
You will be able to view information such as the script name, number of execution attempts that were successful, failed and skipped, start and end time of the execution process, MAC address of the AP, AP and zone names, execution status and last line of the execution.

**FIGURE 209** Script execution summary

Start Time	End Time	MAC Address	AP Name	Zone Name	Execution Status	Last Execution Line
2018/08/24 09:40:09	2018/08/24 09:40:09	D8:3B:FC:22:FD:A0	Jacky's AP	MyZone	SKIPPED_AP_OFFLINE	0

- Click **Close**.

## Viewing and Downloading Logs

The controller generates logs for all the applications that are running on the server.

- Go to **Administration > Diagnostics > Application Logs**.  
The **Application Logs** page appears.
- From **Select the Control Plane**, select the control plane for which you want to download logs.
- Select the **Upload to current node** check-box.
- You can now opt to select:

Option

**Download Logs** To download all logs for the selected application.

**Download All** To download all available logs from the controller.

**Logs** Go to your web browsers default download location and verify that the TGZ file was downloaded successfully. You must use your preferred compression/decompression program to extract the log files from the TGZ file. When the log files are extracted (for example, `adminweb.log`, `cassandra.log`, `communicator.log`, etc.), use a text editor to open and view the log contents.

**Download Snapshot Logs** To download snapshot logs that contain system and configuration information, such as the AP list, configurations settings, event list, communicator logs, SSH tunnel lists, etc.

If you triggered the controller to generate a snapshot from the CLI, you have the option to download snapshot logs from the web interface.

Go to your browser's default download folder, and then verify that the snapshot log file or files have been downloaded successfully. Extract the contents of the tar file.

You have successfully completed downloading log files/snapshot logs from the controller.

## Available System Logs for platforms

The controller generates logs for all the applications that are running on the server.

The following table lists the controller applications that are running.

**TABLE 52** Controller applications and log types for SZ100

Application	Description
API	Stands for application program interface (API), this provides an interface for customers to configure and monitor the system
AUT	Manages the sessions in the controller's TTG module
CaptivePortal	Performs portal redirect for clients and manages the walled garden and blacklist
Cassandra	The controller's database server that stores most of the run-time information and statistical data
CNR	An application that obtains TTG configuration updates and applies the settings to related modules
Configurer	Performs configuration synchronization and cluster operations (for example, join, remove, upgrade, backup, and restore)
Diagnostics	An interface that customers can use to upload Ruckus scripts for performing troubleshooting or applying software patches
ElasticSearch	Scalable real-time search engine used in the controller
Memcached	The controller's memory cache that stores client authentication information for fast authentication or roaming
MemProxy	Replicates MemCached entries to other cluster nodes
Mosquitto	A lightweight method used to carry out messaging between LBS and APs
NC	The Node Controller, which monitors all of the controller's TTG processes
Northbound	Performs UE authentication and handles approval or denial of UEs to AP
RadiusProxy	Sets the RADIUS dispatch rules and synchronizes configuration to each cluster node
SMF	An application that monitors the health of TTG processes
SNMP	Provides a framework for the monitoring devices on a network. The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP.
SubscriberManagement	A process for maintaining local user credentials for WISPr authentication
SubscriberPortal	Internal portal page for WISPr (hotspot)
System	Collects and sends log information from all processes
Web	Runs the controller's management web server

## RADIUS

### Viewing RADIUS Proxy Settings

You must be aware of the RADIUS proxy settings on the controller to monitor the health of the controller.

Go to **Diagnostics > RADIUS**.

The **Proxy** page appears displaying the RADIUS settings.

**FIGURE 210** Diagnostics - RADIUS Proxy

Proxy

Refresh

MVNO Account	Control Plane	AAA IP	Created On	Last Modified On	NAS Type	Auth	Accounting	ACCESS Request	ACC



# Ports to Open for AP-Controller Communication

The table below lists the ports that must be opened in the network firewall to ensure that the vSZ-D/SZ/vSZ (controller), managed APs, and RADIUS servers can communicate with each other successfully.

**TABLE 53** Ports to open for AP-Controller Communication

Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Configurable from Web Interface?	Purpose
21	TCP	AP	Control plane of <ul style="list-style-type: none"> <li>SZ100</li> <li>SZ300</li> <li>SCG200</li> <li>vSZ</li> </ul>	No	ZD/Solo APs can download SZ AP firmware and converting themselves to SZ APs.
22	TCP	<ul style="list-style-type: none"> <li>AP</li> <li>vSZ-D</li> </ul>	vSZ control plane	No	SSH tunnel
49	TCP	TACACS+ server	vSZ control plane	Yes	TACACS+ based authentication of controller administrators
Port 91 (AP firmware version 2.0 to 3.1.x) and 443 (AP firmware version 3.2 and later)	TCP	AP	vSZ control plane	No	<p>AP firmware upgrade APs need Port 91 to download the Guest Logo and to update the signature package for the ARC feature.</p> <p><b>NOTE</b> Starting in release 3.2, the controller uses an HTTPS connection and an encrypted path for the firmware download. The port used for AP firmware downloads has also been changed from port 91 to 443 to distinguish between the two methods. To ensure that all APs can be upgraded successfully to the new firmware, open both ports 443 and 91 in the network firewall.</p>
9997	TCP	Client Device	SZ control Plane	No	Internal Subscriber Portal in HTTP protocol
443	TCP	<ul style="list-style-type: none"> <li>AP</li> <li>vSZ-D</li> </ul>	vSZ control plane	No	Access to the vSZ/SZ control plane over secure HTTPS
6868	TCP	vSZ-D	vSZ	No	Internal communication port
8443	TCP	Any	vSZ management plane	No	Access to the controller web interface via HTTPS

**TABLE 53** Ports to open for AP-Controller Communication (continued)

Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Configurable from Web Interface?	Purpose
<b>NOTE</b> The Public API port has changed from 7443 to 8443.					
23232	TCP	AP	controller (data plane)	No	GRE tunnel
23233	UDP and TCP	AP	Data plane	Yes	GRE tunnel (required only when tunnel mode is GRE over UDP)  <b>NOTE</b> On the vSZ-D, this port is used for both data and control in both UDP and TCP.
12222/12223	UDP	AP	vSZ control plane	No	LWAPP discovery  <b>NOTE</b> If your AP is within the same subnet as the controller, disable nat-ip-translation to establish a connection between the AP and the controller so that AP firmware upgrade progresses. If your AP is on the side of the NAT server and if the NAT server does not support PASV-Mode FTP, enable nat-ip-translation. If the NAT server supports PASV-Mode FTP, then disable nat-ip-translation for AP firmware upgrade to progress
1812/1813	UDP	AP	Radius servers (s)	Yes	AAA authentication and accounting
8022	No (SSH)	Any	Management interface	Yes	When the management ACL is enabled, you must use port 8022 (instead of the default port 22) to log on to the CLI or to use SSH.
8090	TCP	Any	vSZ control plane	No	Allows unauthorized UEs to browse to an HTTP website
8099	TCP	Any	vSZ control plane	No	Allows unauthorized UEs to browse to an HTTPS website
8100	TCP	Any	vSZ control plane	No	Allows unauthorized UEs to browse using a proxy UE
8111	TCP	Any	vSZ control plane	No	Allows authorized UEs to browse using a proxy UE

**TABLE 53** Ports to open for AP-Controller Communication (continued)

Port Number	Layer 4 Protocol	From (Sender)	To (Listener)	Configurable from Web Interface?	Purpose
9080	HTTP	Any	vSZ control plane	No	Northbound Portal Interface for hotspots
9443	HTTPS	Any	vSZ control plane	No	Northbound Portal Interface for hotspots
9998	TCP	Any	vSZ control plane	No	Hotspot WISPr subscriber portal login/logout over HTTPS
3333	TCP	Controller	License server	No	Local license server
3799	UDP	External AAA Server (free Radius)	SZ-RAC ( vSZ control plane)	No	Supports Disconnect Message and CoA (Change Of Authorization) which allows dynamic changes to a user session such as disconnecting users and changing authorizations applicable to a user session.
443	HTTPS	Controller	License server	No	Cloud license server
9996	TCP	Client	Controller interface	No	HotSpot 2.0 portal for onboarding and remediation
9999	TCP	Client	Controller interface	No	HotSpot 2.0 trust CA verification
7000	TCP/UDP	SZ	SZ	No	Cassandra (database) cluster communication and data replication
7800	TCP/UDP	SZ	SZ	No	Cluster node communication for cluster's operations

**NOTE**

The destination interfaces are meant for three interface deployments. In a single interface deployment, all the destination ports must be forwarded to the combined management/control interface IP address.

**NOTE**

Communication between APs is not possible across NAT servers.



# Web Server Support

The **<https://my.ruckus>** web page is a supplementary tool for reporting a problem without much understanding of the infrastructure.

This page is hosted on the AP's Web Server. This feature is independent of the controller being accessible to the AP and provides the first level information required by the support engineer to diagnose a problem. When the AP is managed by SZ, the web-server shall be turned off and the page may not be accessible. You can turn on the web-server by using the **set https enable** command, which the controller may turn off later to conserve memory on the AP.

When connected to an authenticated WLAN, you can enter **<https://my.ruckus>** on a web browser and view the following diagnostic information:

- Client Device
- AP
- AP's Neighbors (Wireless)
- AP's LLDP Neighbors (Wired)

**FIGURE 211** Viewing Diagnostic Information in WPA2 WLAN

The screenshot shows a web browser window with the address <https://my.ruckus/MyRuckusPages/mypage.asp>. The page displays diagnostic information for a Ruckus AP. The information is organized into four main sections: Client Device, AP, AP's Neighbors, and AP's LLDP Neighbors.

Client Device	
Device Name	MacBook-Pro
Your MAC	c4:b3:01:c6:8e:8d
Your SSID	ZZZ_R710_WPA2_WLAN2
Your IP Addr	10.47.210.12
Primary DNS	8.8.8.8
Secondary DNS	0.0.0.0
Device Type	Mac OS X
PHY Mode	11ac
Channel	36 (5180 Mhz)
Connect Duration	76 secs
Tx Bytes	96881
Rx Bytes	60250
RSSI seen by AP	49
MCS Idx/Wdth/Strm	MCS 0/80/3

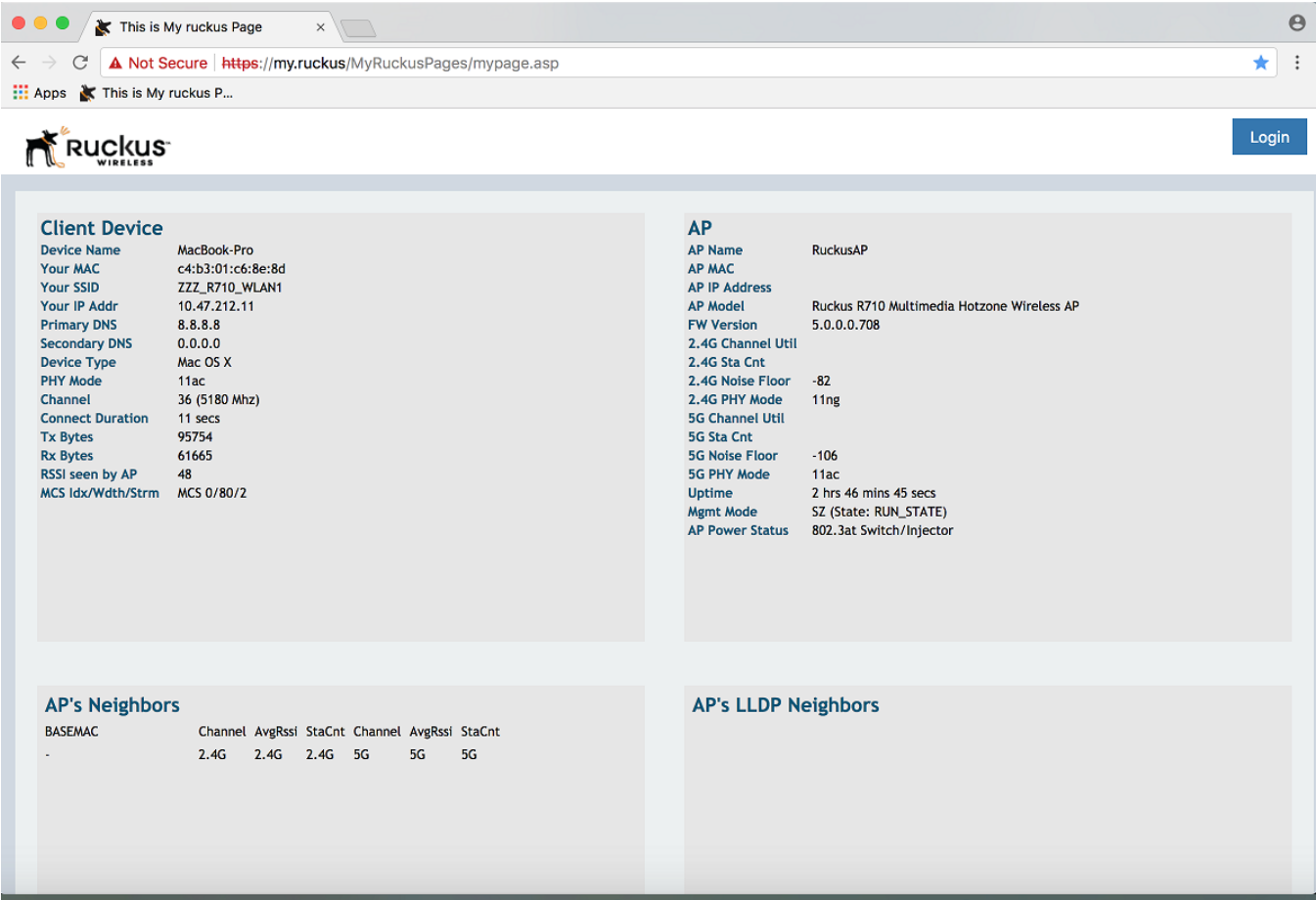
AP	
AP Name	RuckusAP
AP MAC	0C:F4:D5:12:FA:60
AP IP Address	10.47.214.137
AP Model	Ruckus R710 Multimedia Hotzone Wireless AP
FW Version	5.0.0.0.708
2.4G Channel Util	Tx: 2.60% Rx:69.10% Bz:17.50% Tot:90.10%
2.4G Sta Cnt	0
2.4G Noise Floor	-80
2.4G PHY Mode	11ng
5G Channel Util	Tx: 1.40% Rx:46.30% Bz: 6.60% Tot:55.20%
5G Sta Cnt	1
5G Noise Floor	-105
5G PHY Mode	11ac
Uptime	2 hrs 44 mins 7 secs
Mgmt Mode	SZ (State: RUN_STATE)
AP Power Status	802.3at Switch/Injector

AP's Neighbors						
BASEMAC	Channel	AvgRssi	StaCnt	Channel	AvgRssi	StaCnt
-	2.4G	2.4G	2.4G	5G	5G	5G

AP's LLDP Neighbors	
SysName:	ICX7650-48ZP Switch
MgmtIP:	10.150.6.27
PortDescr:	GigabitEthernet1/1/1

On entering <https://my.ruckus> when connected over an Open or WEP WLAN, the diagnostic information is restricted for security reasons.

FIGURE 212 Viewing Diagnostic Information in Open WLAN



# Appendix

---

- Copyright..... 419

## Copyright

Copyright (c) 2008, James Childers All rights reserved.

BSD License Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of SimpleCaptcha nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



© 2019 CommScope, Inc. All rights reserved.  
Ruckus Wireless, Inc., a wholly owned subsidiary of CommScope, Inc.  
350 West Java Dr., Sunnyvale, CA 94089 USA  
[www.ruckuswireless.com](http://www.ruckuswireless.com)