

RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide, 5.2.1

Supporting SmartZone Release 5.2.1

Copyright, Trademark and Proprietary Rights Information

© 2020 CommScope, Inc. All rights reserved.

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

Export Restrictions

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

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

Disclaimer

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

Limitation of Liability

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

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

| | |
|---|-----------|
| Preface | 13 |
| Document Conventions..... | 13 |
| Notes, Cautions, and Safety Warnings..... | 13 |
| Command Syntax Conventions..... | 13 |
| Document Feedback..... | 14 |
| RUCKUS Product Documentation Resources..... | 14 |
| Online Training Resources..... | 14 |
| Contacting RUCKUS Customer Services and Support..... | 15 |
| What Support Do I Need?..... | 15 |
| Open a Case..... | 15 |
| Self-Service Resources..... | 15 |
| About This Guide | 17 |
| What's New in This Document..... | 17 |
| Navigating the Dashboard | 19 |
| Setting Up the Controller for the First Time..... | 19 |
| Logging On to the Web Interface..... | 19 |
| Web Interface Features..... | 20 |
| Changing the Administrator Password..... | 22 |
| Setting User Preferences..... | 22 |
| Logging Off the Controller..... | 23 |
| Configuring Global Filters..... | 24 |
| Warnings and Notifications..... | 25 |
| Warnings..... | 25 |
| Setting Global Notifications..... | 26 |
| Health and Maps..... | 26 |
| Understanding Cluster and AP Health Icons..... | 27 |
| Customizing Health Status Thresholds..... | 27 |
| Using the Health Dashboard Map..... | 30 |
| Viewing Switches on the Dashboard..... | 37 |
| Traffic Analysis..... | 40 |
| Configuring Traffic Analysis Display for APs..... | 40 |
| Configuring Traffic Analysis Display for WLANs..... | 42 |
| Configuring Traffic Analysis Display for Top Clients..... | 42 |
| SmartCell Insight Report on Actual Traffic Rate for APs and Client..... | 43 |
| Configuring General Settings | 45 |
| Viewing System Settings..... | 45 |
| Configuring System Time..... | 47 |
| Configuring the Remote Syslog Server..... | 48 |
| Configuring Cloud Services..... | 50 |
| Configuring Northbound Data Streaming Settings..... | 51 |
| Setting the Northbound Portal Password..... | 52 |
| Enabling Global SNMP Notifications..... | 53 |
| Configuring SNMP v2 Agent..... | 53 |
| Configuring SNMP v3 Agent..... | 54 |
| Configuring SMTP Server Settings..... | 55 |

| | |
|--|-----------|
| Configuring FTP Server Settings..... | 55 |
| Configuring the SMS Gateway Server..... | 56 |
| Configuring Advanced Gateway Options..... | 56 |
| Configuring Node Affinity..... | 57 |
| Enabling Node Affinity..... | 57 |
| Disabling Node Affinity..... | 58 |
| Location Service..... | 58 |
| Working with Maps..... | 60 |
| Importing a Floorplan Map..... | 60 |
| Viewing RF Signal Strength..... | 64 |
| Monitoring APs Using the Map View..... | 64 |
| Configuring AP Settings..... | 67 |
| Working with AP Registration Rules..... | 67 |
| Creating an AP Registration Rule..... | 67 |
| Configuring Registration Rule Priorities..... | 68 |
| Tagging Critical APs..... | 68 |
| Configuring the Tunnel UDP Port..... | 69 |
| Setting the Country Code..... | 69 |
| Limiting the Number of APs in a Domain or Zone..... | 70 |
| Limiting the AP count for a Partner Domain or a System Zone..... | 70 |
| Limiting the AP count for a Zone in a Partner Domain..... | 71 |
| Creating an AP MAC OUI Address..... | 71 |
| AP Admin Password and Recovery SSID..... | 72 |
| Power Source in AP Configuration..... | 74 |
| POE tables for different 11 AC AccessPoint..... | 75 |
| POE tables for different 11 AX AccessPoint..... | 76 |
| Working With Access Points..... | 79 |
| Understanding WLAN Services..... | 79 |
| Hierarchy Overview..... | 79 |
| Creating an AP Domain..... | 80 |
| Working with AP Zones..... | 80 |
| Working with AP Groups..... | 92 |
| Monitoring WLAN Services..... | 105 |
| Viewing Modes..... | 109 |
| AP Status..... | 109 |
| Configuring Access Points..... | 110 |
| Configuring the M510 AP..... | 115 |
| Managing Access Points..... | 120 |
| Overview of Access Point Configuration..... | 120 |
| Viewing Managed Access Points..... | 121 |
| Downloading the Support Log from an Access Point..... | 121 |
| Debugging an AP Failure..... | 122 |
| Provisioning and Swapping Access Points..... | 122 |
| Editing Swap Configuration..... | 124 |
| Approving Mesh APs..... | 124 |
| Monitoring Access Points..... | 125 |
| Multi-Tunnel Support for Access Points..... | 132 |
| Configuring Multiple Tunnels for Zone Templates..... | 133 |
| Configuring Multiple Tunnels for Zone..... | 134 |

| | |
|---|------------|
| Configuring Multiple Tunnels in WLANs..... | 136 |
| Link Aggregation Control Protocol (LACP) support for R720 AP..... | 137 |
| Enabling the LACP Support for a Zone..... | 137 |
| Enabling LACP Support for an AP Group..... | 139 |
| Enabling LACP Support for an AP..... | 139 |
| Power Source in AP Configuration..... | 140 |
| POE tables for different 11 AC AccessPoint..... | 140 |
| POE tables for different 11 AX AccessPoint..... | 141 |
| Viewing the System Cluster Overview..... | 145 |
| Control Planes and Data Planes..... | 146 |
| Interface and Routing..... | 147 |
| Displaying the Chassis View of Cluster Nodes..... | 148 |
| Cluster Redundancy..... | 148 |
| How Cluster Redundancy Works..... | 151 |
| Enabling Cluster Redundancy..... | 152 |
| Viewing Cluster Configuration..... | 155 |
| Disabling Cluster Redundancy - Active-Standby from the Active Cluster..... | 156 |
| Disabling Cluster Redundancy - Active-Standby from the Standby Cluster..... | 156 |
| Deleting Cluster Redundancy - Active-Active from a target Active Cluster..... | 156 |
| Disabling Cluster Redundancy - Active-Active mode from a Current Target Active Cluster..... | 157 |
| Configuring the Control Plane..... | 157 |
| Rebalancing APs..... | 160 |
| Configuring the Data Plane..... | 161 |
| Monitoring Cluster Settings..... | 163 |
| Clearing or Acknowledging Alarms..... | 164 |
| Filtering Events..... | 164 |
| Creating a DP Zone Affinity Profile..... | 164 |
| Verifying DP and Profile Version Match..... | 166 |
| DP NAT License Assignment..... | 166 |
| Enabling Flexi VPN..... | 167 |
| Enabling L3 Roaming Criteria for DP..... | 168 |
| Powering Cluster Back..... | 169 |
| Certificates..... | 171 |
| Importing New Certificates..... | 171 |
| Assigning Certificates to Services..... | 172 |
| Generating Certificate Signing Request (CSR)..... | 172 |
| SZ as a Server Certificate..... | 173 |
| SZ as Client Certificate..... | 175 |
| Managing AP Certificates..... | 178 |
| Importing Trusted CA Certificates..... | 180 |
| Configuring Templates..... | 181 |
| Working with Zone Templates..... | 181 |
| Creating Zone Templates..... | 181 |
| Applying Zone Templates..... | 187 |
| Exporting Zone Templates..... | 187 |
| Importing Zone Templates..... | 187 |
| Working with WLAN Templates..... | 188 |
| Creating WLAN Templates..... | 188 |
| Applying a WLAN Template..... | 188 |

| | |
|--|------------|
| Managing ICX Switches from SmartZone..... | 191 |
| ICX-Management Feature Support Matrix..... | 191 |
| Supported ICX Models..... | 191 |
| Overview of ICX Switch Management..... | 193 |
| Preparing ICX Devices to be Managed by SmartZone..... | 193 |
| ICX Switch Behavior with SmartZone..... | 194 |
| Enabling an ICX Device to Be Managed by SmartZone..... | 195 |
| Configuring the ICX Source Address to Be Used by SmartZone..... | 195 |
| Setting up Switch Registrar Discovery..... | 196 |
| How Switch Registrar Discovery Works..... | 196 |
| Disabling or Enabling Switch Registrar Discovery..... | 196 |
| Confirming Successful Switch Registrar Discovery..... | 197 |
| Troubleshooting Switch Registrar Discovery..... | 197 |
| Preparing Stacking Devices to Connect to SmartZone..... | 198 |
| Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch..... | 198 |
| Manually Configuring the SmartZone IP Address on an ICX Switch..... | 199 |
| Displaying the SmartZone Connection Status..... | 199 |
| Disconnecting the Switch Connection with SmartZone..... | 200 |
| Disabling SmartZone Management on the ICX Switch..... | 200 |
| SmartZone Switch Management..... | 201 |
| Using Controller Settings to Manage Switch Groups..... | 201 |
| Creating Switch Groups..... | 201 |
| Creating Switch Registration Rules..... | 202 |
| Approving Switches..... | 203 |
| Moving the Switches between Groups..... | 204 |
| Deleting Switches..... | 205 |
| Backing up and Restoring Switch Configuration..... | 205 |
| Scheduling a Firmware Upgrade for Switch Group..... | 206 |
| Scheduling a Firmware Upgrade..... | 208 |
| Viewing Switch Information..... | 210 |
| Configuring the Switch..... | 212 |
| Zero Touch Provisioning using Group level Configuration..... | 212 |
| Copying Switch Group Configuration..... | 222 |
| Accessing AAA Settings for Switch Configuration..... | 222 |
| Viewing the Configuration History of Switches..... | 224 |
| Switch Level Configuration..... | 225 |
| Creating Switch Level Configuration..... | 225 |
| Copying Configuration..... | 233 |
| Port Settings..... | 234 |
| Configuring Port Settings for a Switch..... | 234 |
| Editing Ports Across Multiple Switches | 238 |
| Creating Routing Configurations..... | 241 |
| Managing Link Aggregation Groups (LAGs)..... | 244 |
| Creating a Switch Stack..... | 245 |
| Viewing Port Details..... | 246 |
| Viewing Switch Health..... | 249 |
| Viewing Alarms..... | 252 |
| Viewing Events..... | 254 |
| Viewing LLDP Neighbor Information..... | 255 |
| Viewing Traffic Trends in the Switch..... | 255 |

| | |
|--|------------|
| Viewing Firmware History of the Switch..... | 258 |
| Configuring the Group Firmware Settings..... | 258 |
| Accessing the switch CLI through SmartZone (Remote CLI)..... | 260 |
| Viewing PoE Utilization and Health Status of the Switch..... | 263 |
| Troubleshooting Switch Issues..... | 267 |
| Troubleshooting Using Custom Events..... | 268 |
| Troubleshooting Using Remote Operations..... | 269 |
| Viewing Switches on the Dashboard..... | 271 |
| Working with WLANs and WLAN Groups..... | 275 |
| Domains, Zones, AP Groups, and WLANs..... | 275 |
| Viewing Modes..... | 275 |
| Creating a WLAN Domain for an MSP..... | 276 |
| WLAN Groups..... | 276 |
| Creating a WLAN Group..... | 276 |
| Creating a WLAN Configuration..... | 277 |
| 802.11 Fast BSS Transition..... | 294 |
| 802.11w MFP..... | 294 |
| Airtime Decongestion..... | 294 |
| Band Balancing..... | 295 |
| Bypassing Apple CNA..... | 295 |
| Channel Mode..... | 295 |
| Client Admission Control..... | 295 |
| Client Load Balancing..... | 296 |
| Mobility Domain ID..... | 296 |
| Portal-based WLANs..... | 297 |
| Multicast Rate Filter..... | 298 |
| Rate Limiting Ranges for Policies..... | 299 |
| Transient Client Management..... | 300 |
| Optimized Connectivity Experience..... | 300 |
| Working with WLAN Schedule Profiles..... | 300 |
| Managing WLANs..... | 301 |
| Moving a Single WLAN to a Different WLAN Zone..... | 302 |
| Extracting a WLAN Template..... | 302 |
| Applying a WLAN Template..... | 302 |
| Triggering a Preferred Node..... | 303 |
| How Dynamic VLAN Works..... | 303 |
| Managing Clients..... | 305 |
| Working with Wireless Clients..... | 305 |
| Viewing Summary of Wireless Clients..... | 305 |
| Viewing Information about a Wireless Client..... | 306 |
| Deauthorizing a Wireless Client..... | 307 |
| Blocking a Wireless Client..... | 307 |
| Unblocking a Wireless Client..... | 307 |
| Disconnecting a Wireless Client..... | 308 |
| Working with Wired Clients..... | 308 |
| Viewing a Summary of Wired Clients..... | 308 |
| Viewing Information about a Wired Client..... | 309 |
| Deauthorizing a Wired Client..... | 309 |

| | |
|--|------------|
| Working with Users and Roles..... | 309 |
| Creating a User Role..... | 309 |
| Creating a User Role with Active Directory Authentication..... | 318 |
| Creating a User Role with 802.1x Authentication..... | 319 |
| Limitations Applying Role Policies to Users..... | 319 |
| Creating a Local User..... | 320 |
| Creating a Subscription Package..... | 321 |
| Working with Guest Passes..... | 322 |
| Generating Guest Passes..... | 323 |
| Creating a Guest Pass Template..... | 327 |
| Creating a Guest Instruction SMS Template..... | 328 |
| Exporting the Guest Pass to CSV..... | 330 |
| Generating Guest Passes from an Imported CSV..... | 330 |
| Printing the Guest Pass..... | 332 |
| Sending the Guest Pass via Email..... | 333 |
| Sending the Guest Pass via SMS..... | 334 |
| Working with Dynamic PSKs..... | 335 |
| Viewing Dynamic PSKs..... | 336 |
| Generating Dynamic PSKs..... | 336 |
| Importing Dynamic PSKs..... | 337 |
| Creating an External DPSK Over RADIUS WLAN..... | 339 |
| Application Recognition and Control..... | 341 |
| Monitoring Applications..... | 341 |
| Managing a Firewall Profile..... | 345 |
| Creating an L3 Access Control Policy..... | 346 |
| Creating an L3 Access Control Policy Rule..... | 347 |
| Creating an L2 Access Control Policy..... | 349 |
| Creating an L2 Access Control Service..... | 349 |
| Configuring Application Controls..... | 351 |
| Viewing Application Control Summary..... | 351 |
| Creating an Application Control Policy..... | 352 |
| Implementing an Application Control Policy..... | 355 |
| Creating a User Defined Application..... | 357 |
| Working with Application Signature Package..... | 358 |
| URL Filtering..... | 360 |
| Viewing a Summary of URL Filters..... | 360 |
| Creating a URL Filtering Policy..... | 360 |
| Enabling URL Filtering on the Controller..... | 364 |
| Managing URL Filtering Licenses..... | 365 |
| Creating a Device Policy..... | 366 |
| Creating Device Policy Rules..... | 367 |
| Enabling the Device Policy Service..... | 367 |
| Summary..... | 368 |
| Services and Profiles..... | 371 |
| Working with Hotspots and Portals..... | 371 |
| Creating a Guest Access Portal..... | 371 |
| Working with Hotspot (WISPr) Services..... | 374 |
| Creating a Web Authentication Portal..... | 377 |
| Creating a WeChat Portal..... | 379 |

| | |
|--|-----|
| Working with Hotspot 2.0 Services..... | 381 |
| Creating a UA Blacklist Profile..... | 387 |
| Creating a Portal Detection and Suppression Profile..... | 389 |
| Configuring Access Control..... | 391 |
| VLAN Pooling..... | 391 |
| Create Precedence Profile..... | 392 |
| Restricted Access..... | 394 |
| Creating Blocked Clients..... | 399 |
| Creating a Client Isolation Whitelist..... | 400 |
| Creating Time Schedules..... | 401 |
| Creating a DNS Server Profile..... | 402 |
| Creating a DNS Spoofing Profile..... | 404 |
| Creating a Traffic Class Profile | 404 |
| Understanding WiFi Calling..... | 407 |
| Creating a WiFi Calling Profile..... | 407 |
| Configuring WiFi Calling in WLAN..... | 408 |
| Analyzing Wi-Fi Calling Statistics..... | 409 |
| Authentication..... | 411 |
| Creating Non-Proxy Authentication AAA Servers for Standby Cluster..... | 411 |
| Creating Proxy AAA Servers for Standby Cluster..... | 414 |
| Authentication Support Matrix..... | 420 |
| Creating Realm Based Authentication Profile..... | 424 |
| Accounting..... | 426 |
| Creating Non-Proxy Accounting AAA Servers for Standby Cluster..... | 426 |
| Creating Proxy Accounting AAA Servers for Standby Cluster..... | 428 |
| Creating Realm Based Proxy..... | 429 |
| Wireless Intrusion Detection and Prevention Services..... | 430 |
| Classifying a Rogue Policy..... | 430 |
| Bonjour..... | 431 |
| Bonjour Gateway..... | 432 |
| Bonjour Fencing..... | 433 |
| Working with Tunnels and Ports..... | 438 |
| Creating a Ruckus GRE Profile..... | 438 |
| Creating a Soft GRE Profile..... | 439 |
| Creating an IPsec Profile..... | 441 |
| Creating an Ethernet Port Profile..... | 444 |
| Creating a Tunnel DiffServ Profile..... | 448 |
| Split Tunnel Profile..... | 449 |
| Communications Assistance for Law Enforcement Act (CALEA)..... | 450 |
| Enabling Tunnel Encryption..... | 451 |
| Managing Core Network Tunnels..... | 451 |
| Creating Bridge Forwarding Profiles..... | 451 |
| Creating L2oGRE Forwarding Profiles..... | 453 |
| Creating TTG+PDG Forwarding Profiles..... | 454 |
| Configuring the GGSN/PGW Service..... | 457 |
| DHCP/NAT..... | 458 |
| AP-based DHCP/NAT..... | 458 |
| Profile-based DHCP..... | 458 |
| Profile-based NAT..... | 459 |
| Network Topology..... | 459 |

| | |
|--|------------|
| Hierarchical Network Topology..... | 461 |
| Configuring AP-based DHCP Service Settings..... | 461 |
| Creating an AP DHCP Pool..... | 466 |
| Creating Profile-based DHCP..... | 468 |
| Creating Profile-based NAT..... | 470 |
| Configuring DHCP/NAT with Mesh Options..... | 472 |
| 3rd Party Service..... | 472 |
| Enabling Ekahau and Aer Scout/Stanley RTLS Tags..... | 472 |
| Vendor-Specific Attribute (VSA) Profile..... | 473 |
| Creating a Vendor-Specific Attribute Profile..... | 473 |
| Associating a VSA Profile to a WLAN Configuration..... | 475 |
| Working with Reports..... | 479 |
| Types of Reports..... | 479 |
| Client Number Report..... | 479 |
| Continuously Disconnected APs Report..... | 479 |
| Switch Traffic Statistics..... | 479 |
| System Resource Utilization Report..... | 479 |
| TX/RX Bytes Report..... | 479 |
| Managing Report Generation..... | 480 |
| Creating Reports..... | 480 |
| Generating Reports..... | 482 |
| Rogue Devices..... | 482 |
| Viewing Rogue Devices..... | 482 |
| Marking Rogue Access Points..... | 483 |
| Locating a Rogue Device..... | 484 |
| Historical Client Stats..... | 484 |
| Viewing AP Client Statistics..... | 484 |
| Ruckus AP Tunnel Stats..... | 485 |
| Viewing Statistics for Ruckus GRE Tunnels..... | 485 |
| Viewing Statistics for SoftGRE Tunnels..... | 486 |
| Viewing Statistics for SoftGRE IPsec Tunnels..... | 487 |
| Core Network Tunnel Stats..... | 488 |
| Viewing Statistics for L2oGRE Core Network Tunnel..... | 488 |
| Viewing Statistics for GTP Core Network Tunnel..... | 488 |
| Troubleshooting..... | 491 |
| Troubleshooting Client Connections..... | 491 |
| Troubleshooting through Spectrum Analysis..... | 493 |
| Managing Events and Alarms..... | 495 |
| Viewing Events..... | 495 |
| Sending SNMP Traps and Email Notifications for Events..... | 495 |
| Configuring Event Threshold..... | 496 |
| Creating Custom Events for ICX Switches..... | 497 |
| Configuring Alarms..... | 499 |
| Clearing Alarms..... | 499 |
| Acknowledging Alarms..... | 499 |
| Applying Filters..... | 500 |
| Statistics Files the Controller Exports to an FTP Server..... | 501 |
| Administering the Controller..... | 503 |

| | |
|---|------------|
| Managing Administrator and Roles..... | 503 |
| Creating User Groups..... | 503 |
| Creating Administrator Accounts..... | 506 |
| Configuring Administrator Accounts..... | 508 |
| Working with AAA Servers..... | 511 |
| Enabling the Access Control List..... | 522 |
| Creating Account Security..... | 522 |
| Managing Licenses..... | 526 |
| Viewing Installed Licenses..... | 527 |
| Configuring the License Server..... | 529 |
| Configuring License Bandwidth..... | 530 |
| Configuring the DHCP/NAT License Assignment..... | 530 |
| Configuring URL Filtering Licenses..... | 533 |
| Support AP Licensing for the Controller..... | 533 |
| ZoneDirector to SmartZone Migration..... | 534 |
| Monitoring Administrator Activities..... | 535 |
| Managing Mobile Virtual Network Operator (MVNO) Accounts..... | 536 |
| Terminating Administrator Sessions..... | 537 |
| Administrating the Cluster..... | 539 |
| SmartZone Cluster Mode..... | 539 |
| Crash mode..... | 539 |
| Suspend mode..... | 539 |
| Powering Cluster Back..... | 541 |
| Backing Up and Restoring Clusters..... | 541 |
| Disaster Recovery..... | 541 |
| Backing up Cluster Configuration..... | 541 |
| Creating a Cluster Backup..... | 544 |
| Backing Up and Restoring the Controller's Network Configuration from an FTP Server..... | 545 |
| Replacing a Controller Node..... | 552 |
| Replacing a Controller Node in Multi-Node Cluster | 552 |
| Replacing a Controller Node in Single Node Cluster | 552 |
| Performing a Wipe-out Upgrade for Controller Node..... | 553 |
| Upgrading the Controller..... | 553 |
| Performing the Upgrade..... | 554 |
| Uploading an AP Patch File..... | 555 |
| Verifying the Upgrade..... | 555 |
| Rolling Back to a Previous Software Version..... | 555 |
| Upgrading the Data Plane..... | 556 |
| Uploading the Switch Firmware to the Controller..... | 558 |
| Cautions & Limitations of Administrating a Cluster | 558 |
| Wipeout Upgrade..... | 558 |
| Cluster Upgrade..... | 558 |
| Cluster Restore..... | 559 |
| Diagnostics..... | 561 |
| Applying Scripts..... | 561 |
| Uploading AP CLI Scripts..... | 561 |
| Executing AP CLI Scripts..... | 562 |
| Scheduling AP CLI Scripts..... | 563 |
| Viewing Scripts..... | 564 |

| | |
|---|------------|
| Viewing Script Execution Summary..... | 565 |
| Viewing and Downloading Logs..... | 566 |
| Available System Logs for platforms..... | 567 |
| Viewing DHCP and NAT Information..... | 567 |
| GGSN..... | 569 |
| Viewing GGSN Connection Settings..... | 569 |
| Viewing GGSN/PGW GTP-C Session Settings..... | 569 |
| RADIUS..... | 570 |
| Viewing RADIUS Proxy Settings..... | 570 |
| Viewing RADIUS Server Settings..... | 570 |
| Ports to Open for AP-Controller Communication..... | 571 |
| SoftGRE Support..... | 577 |
| Overview of SoftGRE Support..... | 577 |
| Supported Deployment Scenario..... | 577 |
| SoftGRE Packet Format..... | 578 |
| Configuring And Monitoring AP Zones..... | 579 |
| SoftGRE SNMP MIBs..... | 580 |
| SoftGRE Events and Alarms..... | 581 |
| SoftGRE Events..... | 581 |
| SoftGRE Alarms..... | 582 |
| Replacing Hardware Components..... | 583 |
| Installing or Replacing Hard Disk Drives..... | 583 |
| Ordering a Replacement Hard Disk..... | 583 |
| Removing the Front Bezel..... | 583 |
| Removing an HDD Carrier from the Chassis..... | 584 |
| Installing a Hard Drive in a Carrier..... | 585 |
| Reinstalling the Front Bezel..... | 588 |
| Replacing PSUs..... | 589 |
| Replacing System Fans..... | 589 |
| vSZ-H SSID Syntax..... | 593 |
| SSIDs Supported in Release 1.1.x..... | 593 |
| SSIDs Supported in Release 2.1.x..... | 593 |
| SSIDs Supported in Release 2.5.x..... | 594 |
| SSIDs Supported in Release 3.0 and Above..... | 594 |
| ZoneDirector SSID Syntax..... | 595 |
| SSIDs Supported in Releases 9.8 and 9.7..... | 595 |
| Supported SSIDs in ZoneFlex Release 9.6..... | 595 |
| ZoneFlex AP SSID Syntax..... | 596 |
| Supported SSIDs in Releases 9.8, 9.7, and 9.6..... | 596 |
| Web Server Support..... | 597 |
| Appendix..... | 599 |
| Copyright..... | 599 |

Preface

- Document Conventions..... 13
- Command Syntax Conventions..... 13
- Document Feedback..... 14
- RUCKUS Product Documentation Resources..... 14
- Online Training Resources..... 14
- Contacting RUCKUS Customer Services and Support..... 15

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 | <code>device(config)# interface ethernet 1/1/6</code> |
| bold | User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names | On the Start menu, click All Programs . |
| <i>italics</i> | Publication titles | Refer to the <i>RUCKUS Small Cell Release Notes</i> for more information. |

Notes, Cautions, and Safety Warnings

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

NOTE

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

ATTENTION

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



CAUTION

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



DANGER

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

Command Syntax Conventions

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

| Convention | Description |
|------------------|--|
| bold text | Identifies command names, keywords, and command options. |

Preface

Document Feedback

| Convention | Description |
|--------------------|---|
| <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</i> [<i>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.

When contacting us, include the following information:

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

For example:

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

RUCKUS Product Documentation Resources

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

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

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

Online Training Resources

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

Contacting RUCKUS Customer Services and Support

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

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

What Support Do I Need?

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

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

Open a Case

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

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

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

Self-Service Resources

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

- Technical Documentation—<https://support.ruckuswireless.com/documents>
- Community Forums—<https://forums.ruckuswireless.com/ruckuswireless/categories>
- Knowledge Base Articles—<https://support.ruckuswireless.com/answers>
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—<https://support.ruckuswireless.com/security>

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

About This Guide

- [What's New in This Document](#)..... 17

What's New in This Document

TABLE 2 Summary of Enhancements in SmartZone Release 5.2.1

| Feature | Description | Location |
|--|--|--|
| URL filtering license for ethernet profile | Displays the ethernet port profile within the zone that have the URL filtering service enabled. | Refer to Configuring URL Filtering Licenses on page 533 and Creating an Ethernet Port Profile on page 444 for more information. |
| L2 ACL wired support | Enables user-defined ethernet port profile configuration. | Refer to Creating an L2 Access Control Service on page 349 and Creating an Ethernet Port Profile on page 444 for more information. |
| Configurable options to enable-disable my.ruckus | Supports tunneled-WLAN and non-default management VLAN. | Refer to Creating an AP Zone on page 80 for more information. |
| 11ax: ACLB | Automatically transfers client load across bands and APs. | Refer to Creating an AP Zone on page 80 for more information. |
| Group Firmware Upgrade | Enables upgrading the firmware version of a switch group. | Refer to Scheduling a Firmware Upgrade for Switch Group on page 206 for more information. |
| Remote CLI or SSH into the switch | Switch commands can be executed by accessing the console of switch through the controller interface. | Refer to Accessing the switch CLI through SmartZone (Remote CLI) on page 260 for more information. |
| Ability to configure protected ports | Displays the Protect Port filed in the Port settings. | Refer to Configuring Port Settings for a Switch on page 234 for more information. |
| Ability to change default VLAN | The default VLAN can now be changed to a different VLAN ID. | Refer to Creating Switch Level Configuration on page 225 for more information. |
| AP Admin Password & Recovery-SSID Enhancement | Describes the mitigation of security enhancement of the AP admin password management | Refer to AP Admin Password and Recovery SSID on page 72 for more information. |
| Channelfly improvements to reduce channel selection time | Describes the mapping of channelfly to new algorithm | Refer to ChannelFly and Background Scanning on page 90 for more information. |
| 11ax-Multicast Rate Limit | Describes the multicast rate limiter | Refer to Multicast Rate Filter on page 298 for more information. |
| Summary | Enhancement to Device Policy Service Summary. | Refer to Summary on page 368 for more information. |
| MCS Tx/Rx rate | Enhancement to view median of MCS Tx/Rx for Wireless Clients. | Refer to Viewing Summary of Wireless Clients on page 305 for more information. |
| Power Source in AP Configuraition | Describes the standardization applies when the AP is forced to a certain PoE power mode. | Refer to Power Source in AP Configuration on page 74 for more information. |

About This Guide

What's New in This Document

TABLE 2 Summary of Enhancements in SmartZone Release 5.2.1 (continued)

| Feature | Description | Location |
|---|--|---|
| Ability to save himem log into AP file system in rotating log | Saves HiMEM logs pertaining to the AP crash in the file system. | Refer to Debugging an AP Failure on page 122 for more information. |
| IPSec | Extends platform support to 11ax APs. | Refer to Creating an IPsec Profile on page 441 for more information. |
| Enable User-Agent for 11ax profile | Extends platform support to 11ax APs. | Refer to Creating a Device Policy on page 366 for more information. |
| Legacy Safe | Allows legacy Wi-Fi 5 clients with outdated drivers to interoperate with a Wi-Fi 6 AP. | Refer to Creating a WLAN Configuration on page 277 for more information. |
| User experience (QoE) enhancements | Displays Wi-Fi call quality statistics. | Refer to Analyzing Wi-Fi Calling Statistics on page 409 for more information. |
| ZAPd Enhancements | Measures APs' connection performance. | Refer to Configuring Access Points on page 110 and Running a Speed Test on page 131 for more information. |
| SZ GUI Enhancements for AP Info/Config | Provides additional information of the AP. | Refer to Viewing General AP Information on page 126 for more information. |
| SZ Onboarding US & EU | Provides control over a specific-region cluster. | Refer to Configuring Cloud Services on page 50 for more information. |
| Designate a VLAN as Management VLAN | Provides the ability to designate a VLAN on switches as Management VLAN. | Refer to Creating Switch Level Configuration on page 225 |
| Ability to change the Default VLAN. | Provides the ability to change the default VLAN for switch. | Refer to Creating Switch Level Configuration on page 225 |
| Protected Ports, PoE Budget and QoS settings. | Provides the ability to configure the protected ports, PoE budget and QoS settings for ports | Refer to Configuring Port Settings for a Switch on page 234 |
| Power supply status for stack members | Provides the ability to configure the PoE and Power utilization for stack members. | Refer to Viewing PoE Utilization and Health Status of the Switch on page 263 |
| Group Firmware Settings | Provides the ability to configure group firmware settings. | Refer to Configuring the Group Firmware Settings on page 258 |
| Syslog configuration | Provides the ability to configure syslog server. | Refer to Creating Common Configuration on page 213 |

Navigating the Dashboard

| | |
|---|----|
| • Setting Up the Controller for the First Time..... | 19 |
| • Logging On to the Web Interface..... | 19 |
| • Web Interface Features..... | 20 |
| • Changing the Administrator Password..... | 22 |
| • Setting User Preferences..... | 22 |
| • Logging Off the Controller..... | 23 |
| • Configuring Global Filters..... | 24 |
| • Warnings and Notifications..... | 25 |
| • Health and Maps..... | 26 |
| • Traffic Analysis..... | 40 |

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)

Navigating the Dashboard

Web Interface Features

- 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.

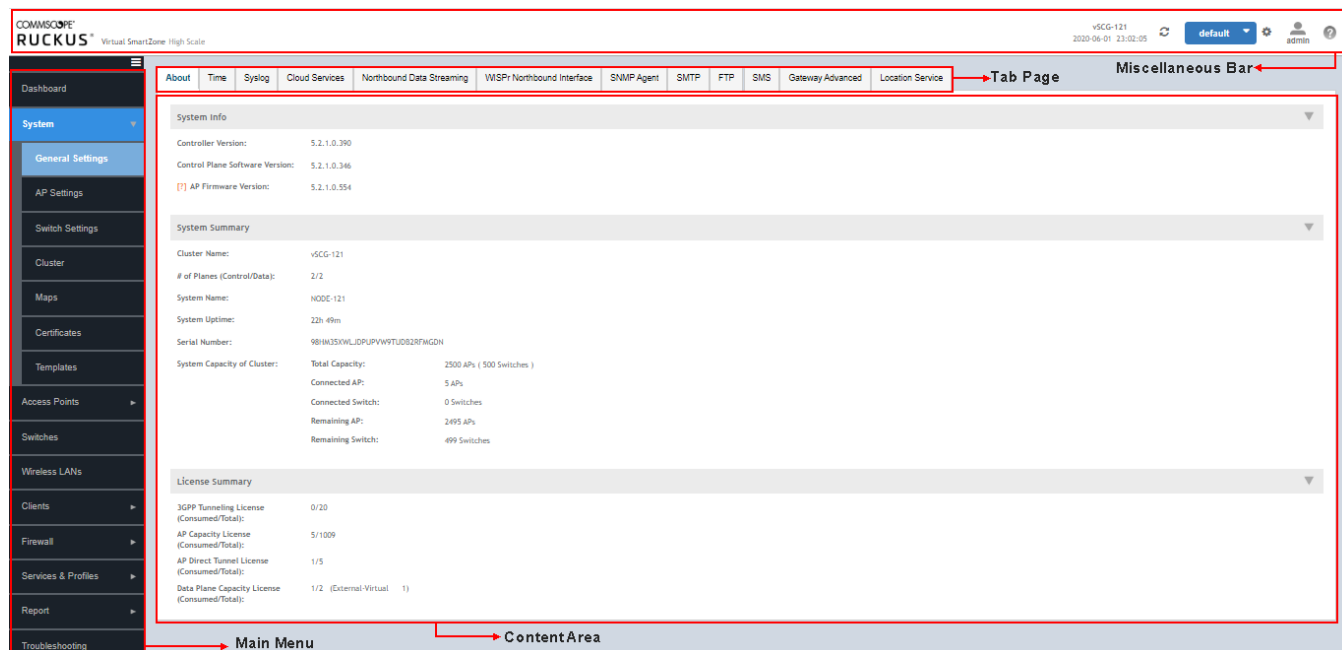
Web Interface Features

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 3 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"> Warning—Lists the critical issues to be resolved. System Date and time—Displays the current system date and time. Refresh—Refreshes the web page. Global filter—Allows you to set the preferred system filter. My Account link—Allows you to: <ul style="list-style-type: none"> Change password Set session preference View account activities such as login information and privilege changes Log off Online Help—Allows access to web help. |

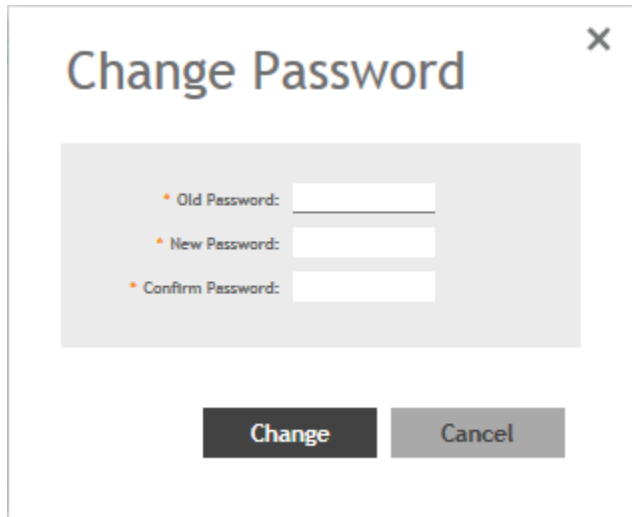
You can also use the  icon to expand and shrink the main menu. Shrinking the main menu increases the size of the content area for better readability and viewing.

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



The screenshot shows a modal window titled "Change Password" with a close button in the top right corner. Inside the window, there is a light gray rectangular area containing three input fields, each preceded by a red asterisk: "Old Password:", "New Password:", and "Confirm Password:". Below this area are two buttons: a dark gray "Change" button and a light gray "Cancel" button.

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.

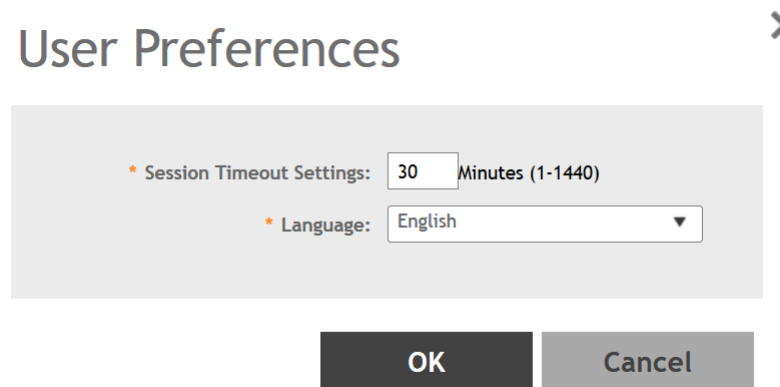
1. From the **Header** bar, click **admin**.
2. Select **Preferences** from the drop-down menu.
The **User Preferences** page appears.
3. In Session Timeout Setting, enter the duration the web interface session must last for, in minutes.

4. In Language, select the language that you want to view the web interface in.

The following languages are supported:

- Spanish
- Brazilian Portuguese
- French
- German
- Italian
- Russian
- Simplified Chinese
- Traditional Chinese
- Korean
- Japanese

FIGURE 3 User Preferences



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.

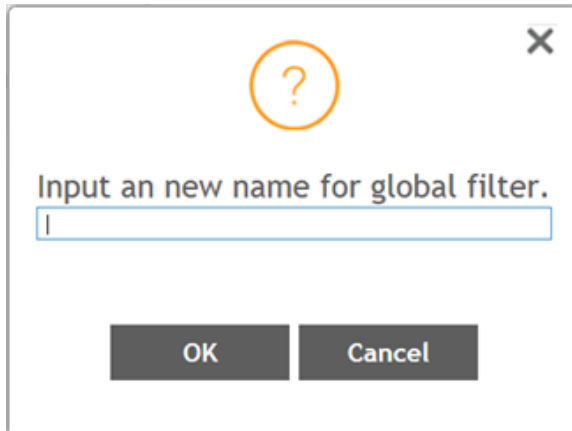
FIGURE 4 Global Filter Form



The screenshot shows a dialog box titled "Global Filter - default". At the top, there is a field labeled "Name:" with the value "default". Below this is a list of zones, each with a checked checkbox and a "Z" icon. The zones listed are zone13, zone14, zone15, zone2, zone3, zone4, zone5, zone6, zone7, zone8, and zone9. At the bottom of the dialog, there 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



Input an new name for global filter.

OK 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

Navigating the Dashboard

Health and Maps

- Suggested AP Limit Exceeded
- AP/DP version mismatch

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.

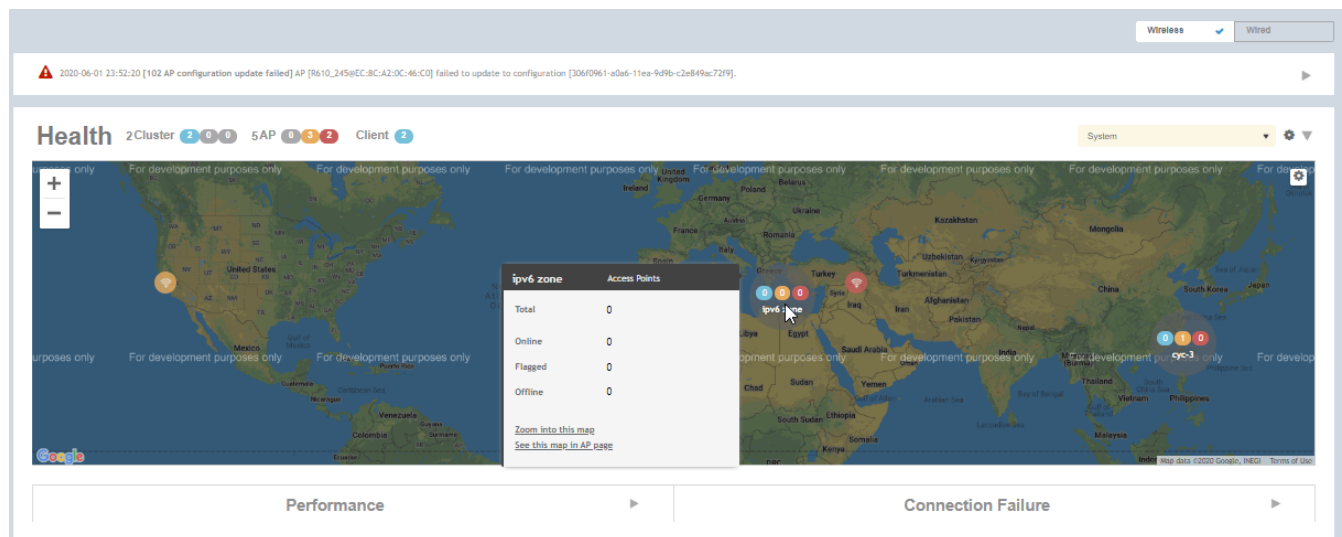
Health and Maps

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:

-  (Green): Online
-  (Orange): Flagged
-  (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 27.

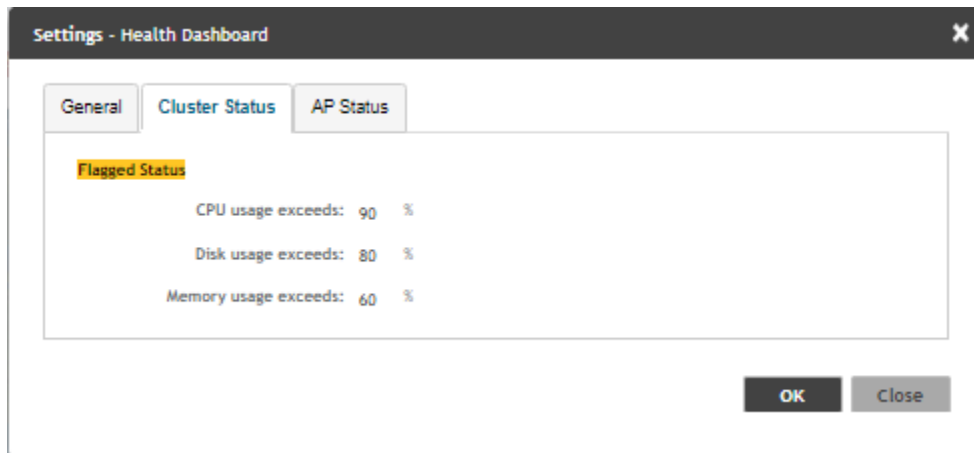
Customizing Health Status Thresholds

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



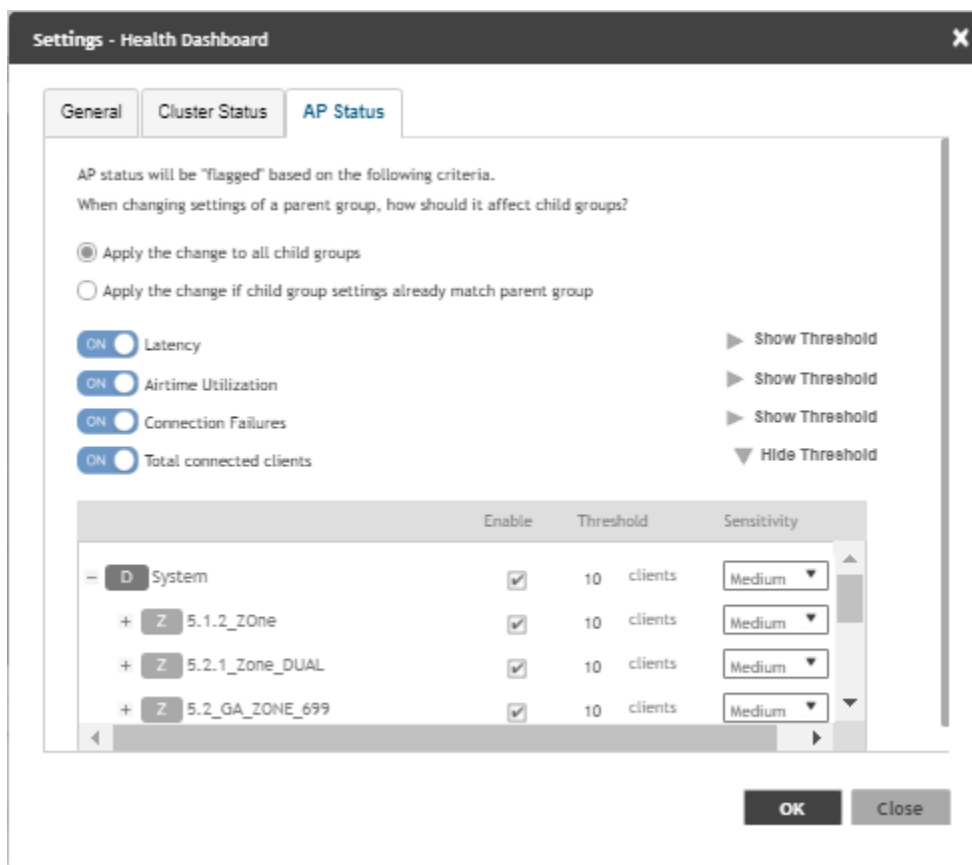
Customizing AP Flagged Status Thresholds

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 4 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

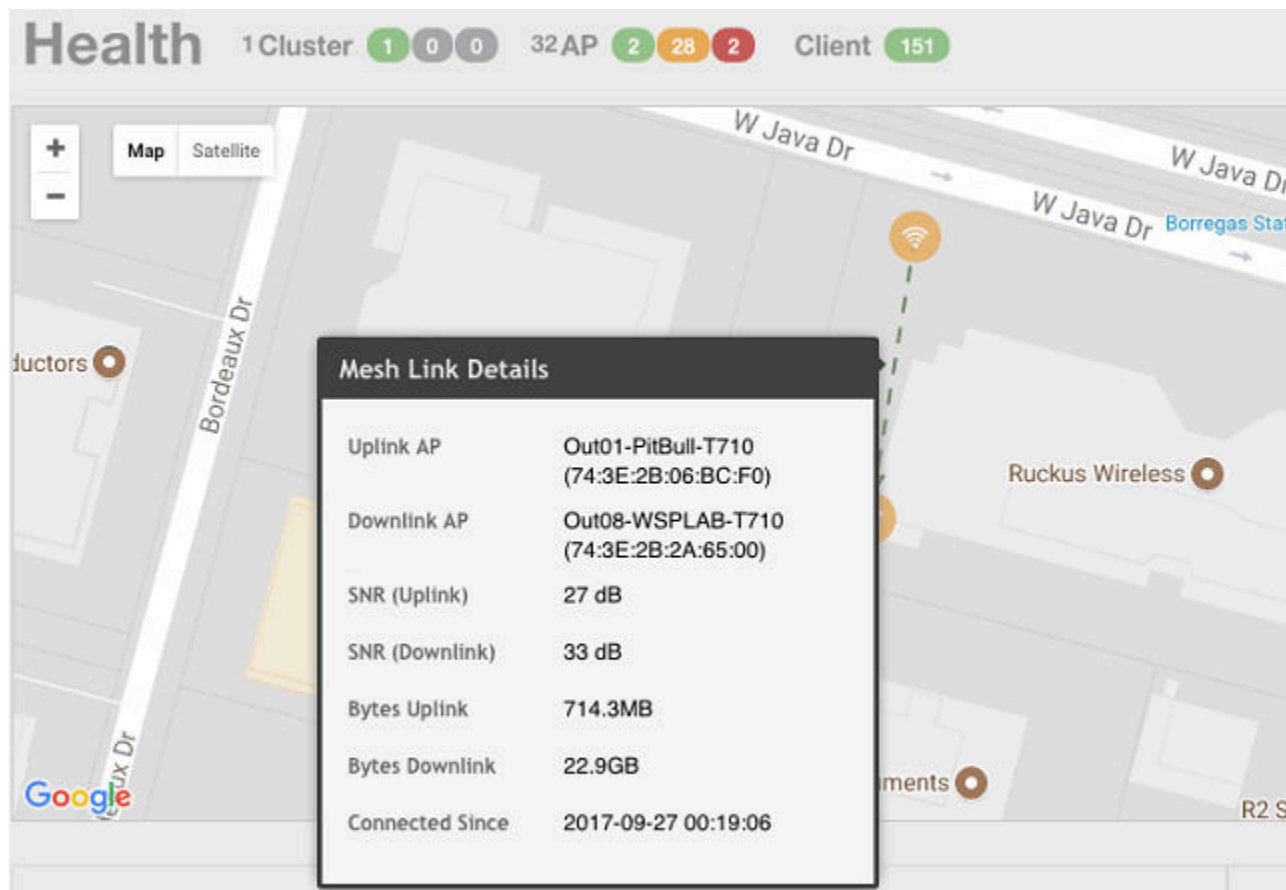
Use the Google Maps view just as you would normally use Google Maps - including zoom, satellite view, rotate and even street view icons. You can customize the AP icon information displayed on the map using the tools in the upper-right hand corner.

Use the **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.

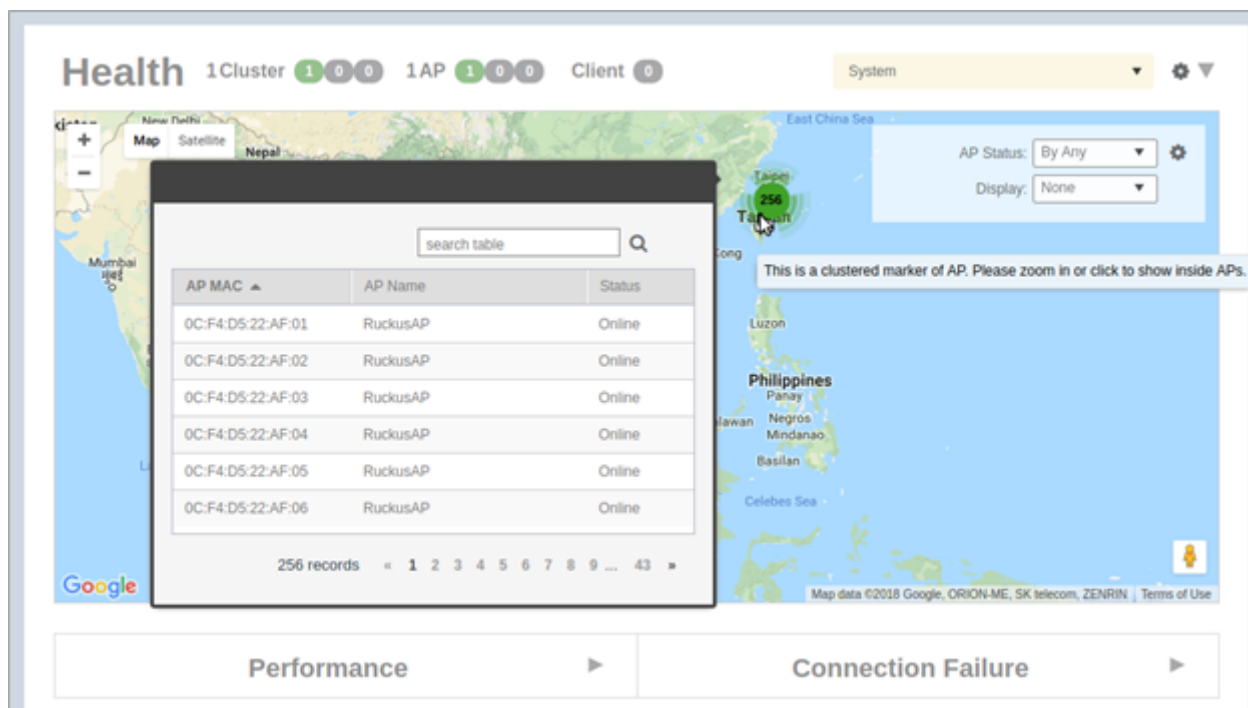
FIGURE 10 Mesh Link Details



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.

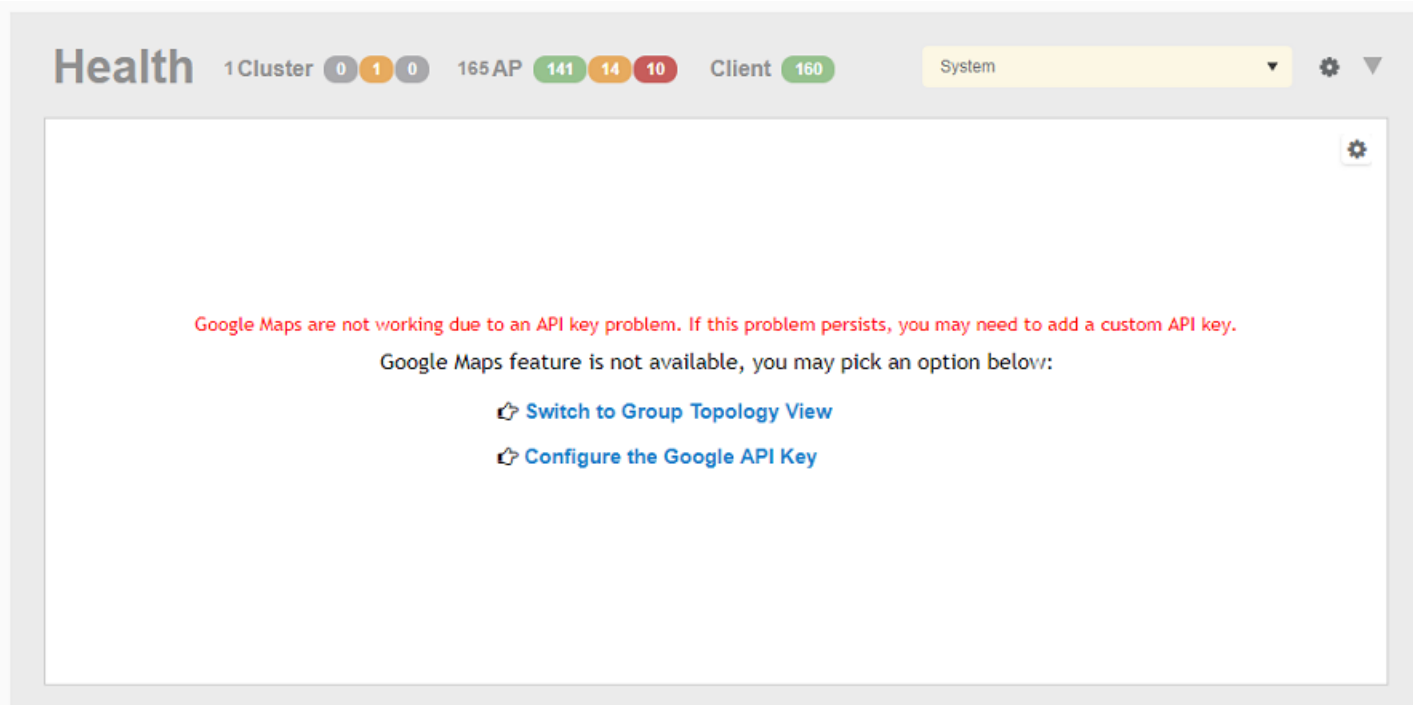
You would also have to generate an API key if you encounter errors such as

`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.

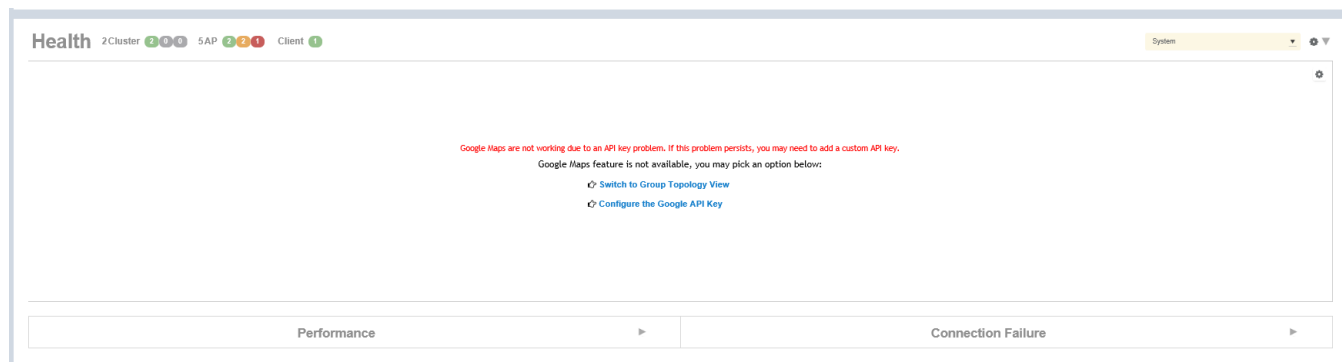
All administrators of the system can use the same API key, or apply a unique API key per administrator. Allowing an API key per administrator enables more flexibility when API usage is high, or in circumstances when each tenant must use their own API key.

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

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

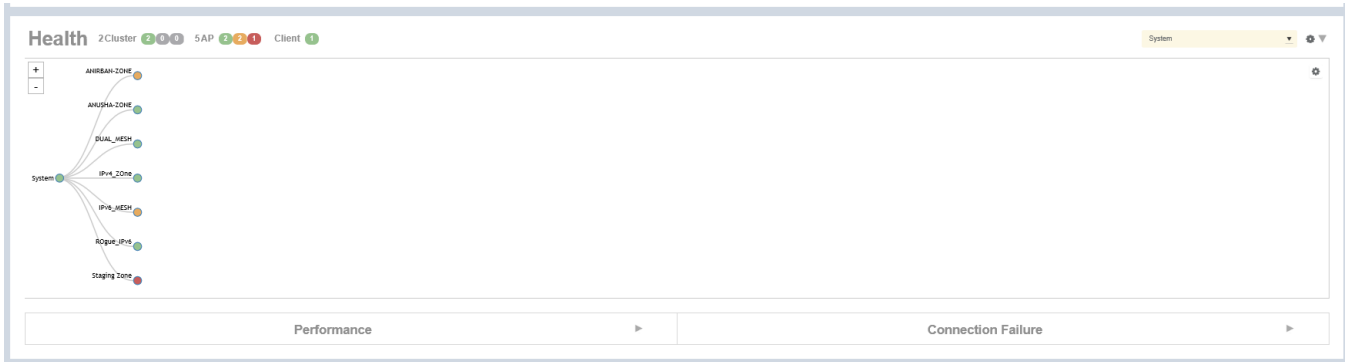
In **Health**, the map view appears if you are connected to a network. If you are not, then you might see the following screen and would have to view your network deployment as a topology diagram.

FIGURE 14 No Map View



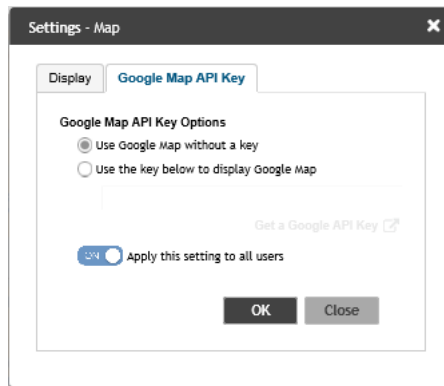
If you click the **Switch to Group Topology View**, a topology diagram similar to the following figure is displayed.

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 Get a Google API Key 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

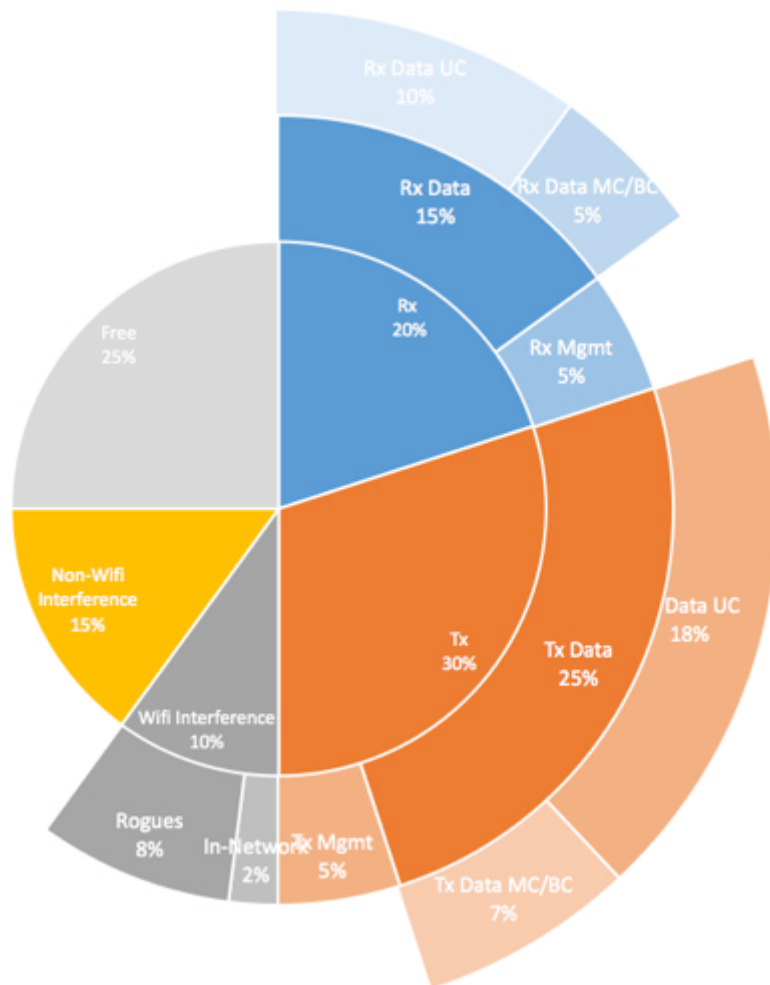
Click the Performance tab to analyze the following parameters:

- 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 5 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 displays charts illustrating traffic trends.

1. From the SmartZone interface, click **Dashboard** in the navigation pane.

The **Dashboard** page is displayed.

2. Click **Wired**.

The **Wired** page is displayed.

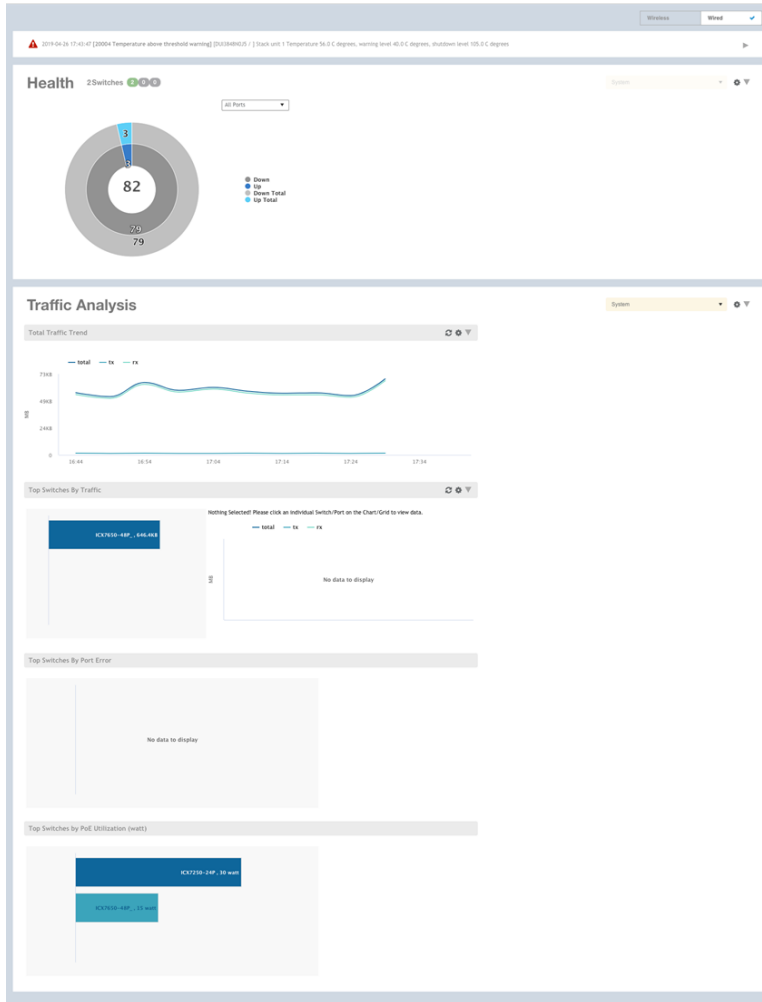
3. Click the Gear icon on the **Health** dashboard.

The **Settings-Health Dashboard** page is displayed.

4. Click the **Display** tab.

- From the **View Mode** , select either **Topology** or **Port** view to be displayed on the dashboard.

FIGURE 18 Showing Wired Devices Using Port View Mode



In the port view mode, the **Health** pane displays the number of switches that are online, offline, and flagged.

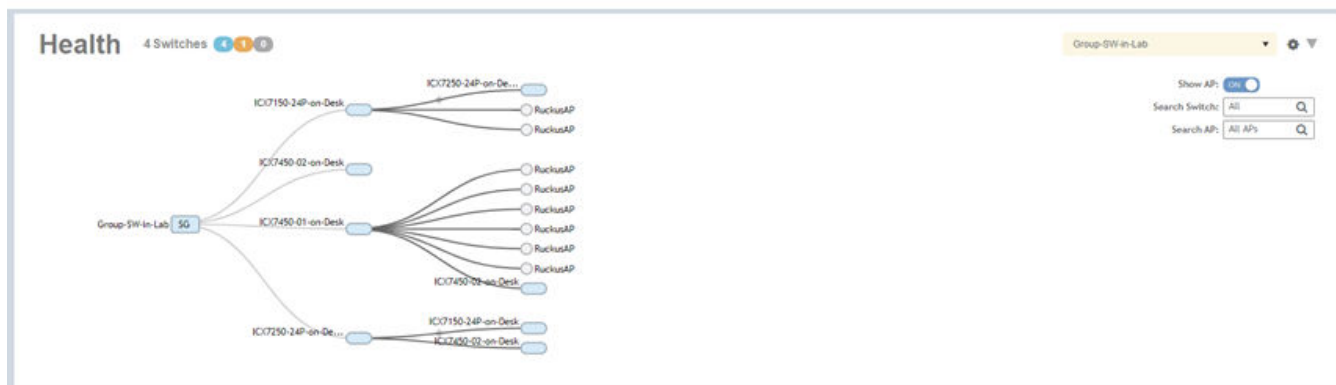
The **Health** pane also displays the number of ports for each port speed (1 Gbps, 2.5 Gbps, 10 Gbps, and so on) or all the ports, and indicates the status of the ports (Up, Down, Down by Admin, Down Total, and Up Total).

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

- Total Traffic Trend
- Top Switches By Traffic
- Top Switches By Port Error

- Top Switches by PoE Utilization (watt)

FIGURE 19 Showing Wired Devices Using Topology View Mode

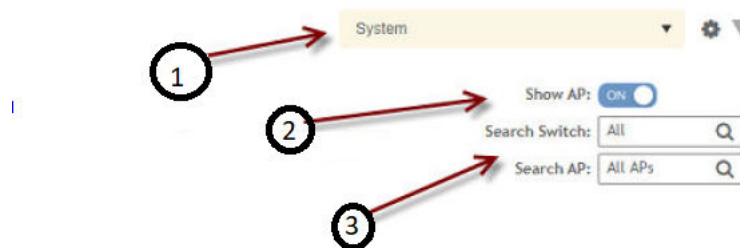


In the topology view mode, the **Health** pane consists of a filter combo box to display domain, sub-domain and switch group in the topology view. The **Show AP** button can be turned on or off to view either the switch or a combination of switch and AP, and **Search** box to search AP or switch based on the device name and MAC address. If you pause the pointer on a link in the topology view, the highlighted link shows the port and LAG information. If you pause the pointer on a device, the highlighted device shows device information such as name, model, MAC address, and IP address (for the switch only).

NOTE

The **Health** dashboard refreshes automatically every 15 minutes to show the latest topology view.

FIGURE 20 Showing Elements on the Health Dashboard



- 1 - Filter
- 2 - Topology Type Switch Button
- 3 - Search Bar

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.

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).

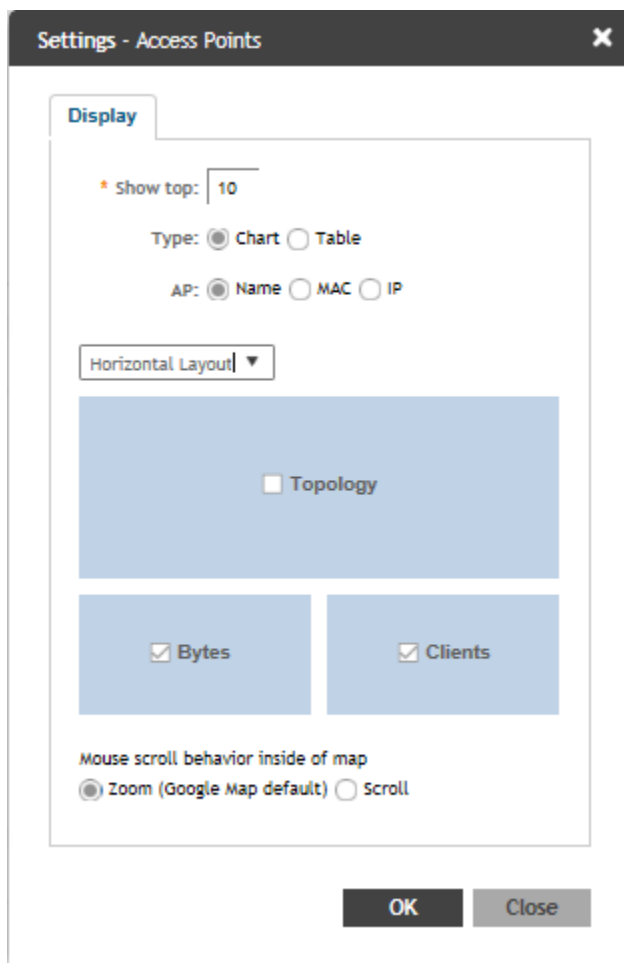
You can view historical and real-time data of the AP. Throughput and the number of clients connected to the AP are displayed in a bar chart. You can view the count of AP model details supported on the system in a pie chart. You must configure the AP settings to view its traffic analysis.

To configure the AP settings:

1. From the Access Points area, click settings .

The AP setting form displays.

FIGURE 21 AP Settings Form



The screenshot shows a window titled "Settings - Access Points" with a close button (X) in the top right corner. The window contains a "Display" tab. Inside the tab, there is a "Show top:" input field with the value "10". Below it are two radio buttons for "Type": "Chart" (selected) and "Table". Underneath are three radio buttons for "AP": "Name" (selected), "MAC", and "IP". A dropdown menu is set to "Horizontal Layout". Below the dropdown is a large blue rectangular area containing a "Topology" checkbox, which is currently unchecked. Below this area are two smaller blue rectangular areas, each containing a checked checkbox: "Bytes" and "Clients". At the bottom of the form, there is a section titled "Mouse scroll behavior inside of map" with two radio buttons: "Zoom (Google Map default)" (selected) and "Scroll". At the very bottom of the window are two buttons: "OK" and "Close".

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:


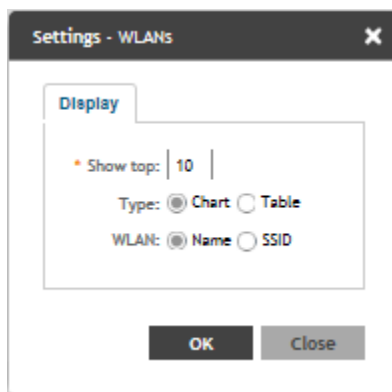
1. From the WLAN area, click settings .
The WLAN settings form displays.

FIGURE 22 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:


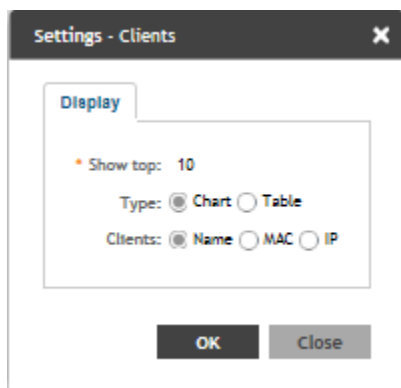
1. From the WLAN area, click settings .
The Client settings form displays.

FIGURE 23 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.

Navigating the Dashboard

Traffic Analysis

- **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..... | 45 |
| • Configuring System Time..... | 47 |
| • Configuring the Remote Syslog Server..... | 48 |
| • Configuring Cloud Services..... | 50 |
| • Configuring Northbound Data Streaming Settings..... | 51 |
| • Setting the Northbound Portal Password..... | 52 |
| • Enabling Global SNMP Notifications..... | 53 |
| • Configuring SMTP Server Settings..... | 55 |
| • Configuring FTP Server Settings..... | 55 |
| • Configuring the SMS Gateway Server..... | 56 |
| • Configuring Advanced Gateway Options..... | 56 |
| • Configuring Node Affinity..... | 57 |
| • Location Service..... | 58 |
| • Working with Maps..... | 60 |

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
- 3GPP Tunneling License
- AP Capacity License
- AP Direct Tunnel License
- Data Plane Capacity License

Configuring General Settings

Viewing System Settings

FIGURE 24 General Settings - SZ300

The screenshot displays the 'General Settings' page for an SZ300 device. The left sidebar contains navigation options: Dashboard, System (General Settings, AP Settings, Switch Settings, Cluster, Maps, Certificates, Templates), Access Points, Switches, Wireless LANs, Clients, Applications, Services & Profiles, and Report. The main content area is divided into three sections:

- System Info:**
 - Controller Version: 5.1.0.0.484
 - Control Plane Software Version: 5.1.0.0.441
 - Data Plane Software Version: 5.1.0.0.484
 - [?] AP Firmware Version: 5.1.0.0.580
- System Summary:**
 - Cluster Name: SZ300-63
 - # of Planes (Control/Data): 2/4
 - System Name: N00E-63
 - System Uptime: 22h 33m
 - Serial Number: 12173700019
 - System Capacity of Cluster:
 - Total Capacity: 10000 APs (1250 Switches)
 - Connected AP: 9 APs
 - Connected Switch: 0 Switches
 - Remaining AP: 9991 APs
 - Remaining Switch: 1248 Switches
- License Summary:**
 - 3GPP Tunneling License (Consumed/Total): 1/20000
 - AP Capacity License (Consumed/Total): 4/20
 - AP Direct Tunnel License (Consumed/Total): 1/10001

FIGURE 25 General Settings - vSZ-H

The screenshot displays the 'General Settings' page for a vSZ-H device. The left sidebar contains navigation options: Dashboard, System (General Settings, AP Settings, Switch Settings, Cluster, Maps, Certificates, Templates), Access Points, Switches, Wireless LANs, Clients, Firewall, Services & Profiles, and Troubleshooting. The main content area is divided into three sections:

- System Info:**
 - Controller Version: 5.2.1.0.390
 - Control Plane Software Version: 5.2.1.0.346
 - [?] AP Firmware Version: 5.2.1.0.554
- System Summary:**
 - Cluster Name: vSG-121
 - # of Planes (Control/Data): 2/2
 - System Name: N00E-121
 - System Uptime: 1d 10h 9m
 - Serial Number: 98IM35XWLDPUVWYU082RFMGDN
 - System Capacity of Cluster:
 - Total Capacity: 2500 APs (500 Switches)
 - Connected AP: 5 APs
 - Connected Switch: 0 Switches
 - Remaining AP: 2495 APs
 - Remaining Switch: 499 Switches
- License Summary:**
 - 3GPP Tunneling License (Consumed/Total): 0/20
 - AP Capacity License (Consumed/Total): 5/1009
 - AP Direct Tunnel License (Consumed/Total): 1/5
 - Data Plane Capacity License (Consumed/Total): 1/2 (External-Virtual 1)

NOTE

For the SZ300 and vSZ-H platforms, the AP to switch ratio is 5:1. For more details, refer to *SmartZone Upgrade Guide* and *Virtual SmartZone Getting Started Guide*.

Configuring System Time

The controller has three external Network Time Protocol (NTP) servers that are used to synchronize the time across Access Points, Cluster nodes, and vDPs.

NOTE

The controller supports version 4.2.6p5 of NTP. The controllers and Access Point does not accept broadcast and multicast NTP packets that would result in the timestamp, these packets are ignored by default.

To edit the system time:

1. Go to **System > General Settings > Time**.
2. Configure the following:
 - a. NTP Primary Server: Enter the primary NTP server address that you want to use.

FIGURE 26 Setting System Time

The screenshot displays the 'System Time' configuration page. At the top, it shows the current 'System Time' and 'System UTC Time' as 2020-07-20 10:56:00 UTC. Below this, there are three input fields for NTP servers: 'NTP Primary Server' (containing 10.1.200.135), 'NTP Secondary Server', and 'NTP Third Server'. A 'Sync Server' button is located to the right of the primary server field. A dropdown menu for 'System Time Zone' is set to '(GMT+0:00) UTC'. The page is divided into three sections for authentication: 'NTP Primary Server Authentication' (Key Type: MD5, Key ID: 9, Key: brocade!), 'NTP Secondary Server Authentication' (Key Type: None, Key ID: 1 - 65534, Key:), and 'NTP Third Server Authentication' (Key Type: None, Key ID: 1 - 65534, Key:). Each authentication section includes a note: 'The PSK is provided by the NTP server, please fill it accordingly'. At the bottom, there are 'Refresh', 'OK', and 'Cancel' buttons.

NOTE

By default, the address of NTP Primary Server is <http://ntp.ruckuswireless.com>.

Configuring General Settings

Configuring the Remote Syslog Server

- b. Click **Sync Server** to enable the controller to sync up with the NTP server configured and then to sync the cluster-follower nodes, APs, and vDPs with the controller time.
- c. System Time Zone: Select the time zone from the drop-down that you want the controller to use. The default time zone is (GMT +0:00) UTC.
- d. You can achieve secured communication with NTP servers after configuring them.

To establish this communication, in the **NTP Server Authentication** field, configure **Key Type** as MD5 or SHA1, **KEY ID** in the range of (1 to 65534, and **Key or PSK** as negotiated for each of the NTP servers.

3. 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 6 Syslog Server Configuration Settings

| Field | Description | Your Action |
|--|--|---|
| Primary Syslog Server Address | Indicates the syslog server on the network. | <ol style="list-style-type: none">a. Enter the server address.b. Enter the Port number.c. Choose the Protocol type.d. Click Ping Syslog Server. If the syslog server is reachable, a flashing green circle and the message Success appears after the button. |
| Secondary Syslog Server Address | Indicates the backup syslog server on the network, if any, in case the primary syslog server is unavailable. | <ol style="list-style-type: none">a. Enter the server address.b. Enter the Port number.c. Choose the Protocol type.d. Click Ping Syslog Server. If the syslog server is reachable, a flashing green circle and the message Success appears after the button. |

TABLE 6 Syslog Server Configuration Settings (continued)

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

TABLE 6 Syslog Server Configuration Settings (continued)

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

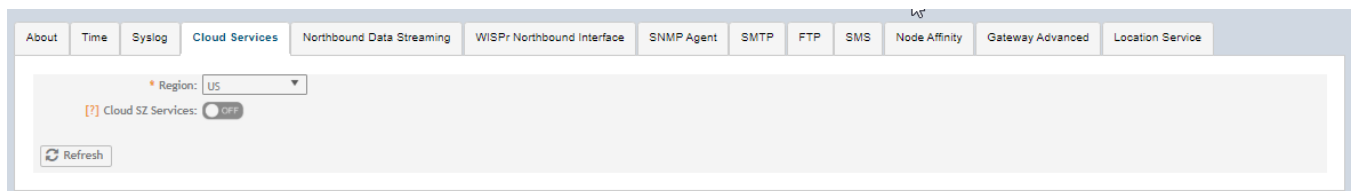
Configuring Cloud Services

Complete the following steps to enable cloud analytics on SmartZone.

1. Select **System > General Settings > Cloud Services**.

The **Cloud Services** page is displayed.

FIGURE 27 Configuring Cloud Services



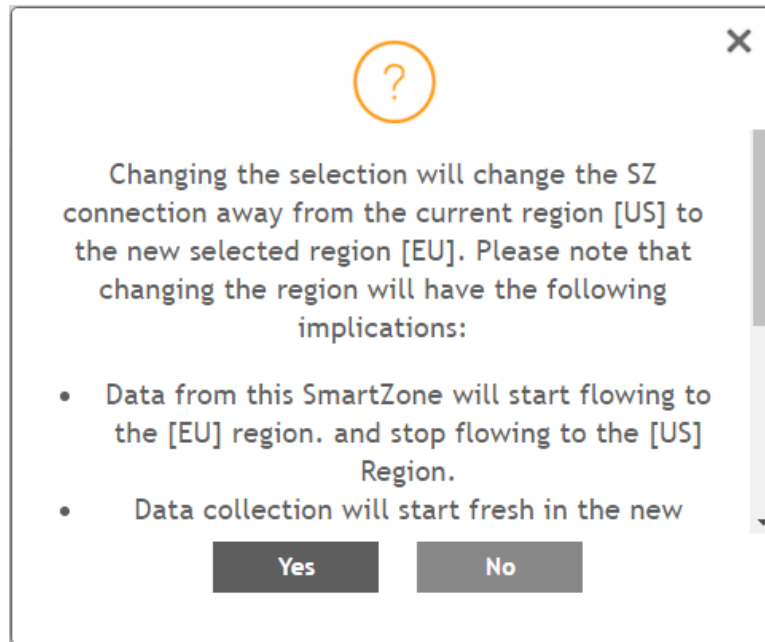
- For **Region**, select a specific cluster region to control. Options include US, EU, and Asia.

NOTE

The option to select a region is available only when **Cloud SZ Services** is disabled.

A confirmation dialog box is displayed.

FIGURE 28 Confirming Region Change



- Click **Yes** to confirm.

An error message is displayed if the cluster receives an unexpected response.

- Select **Cloud SZ Services**.

You are redirected to sign in to your Ruckus cloud account for authentication. The Ruckus cloud account name, connection status, and service details for Ruckus CloudFront are displayed.

NOTE

The **Service Details** within **Connection Status** display the list of SmartZone enabled and disabled services.

- Select **Cloud Analytics**.

The connection status for cloud analytics is displayed.

Configuring Northbound Data Streaming Settings

SmartCell Insight (SCI) 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:

Configuring General Settings

Setting the Northbound Portal Password

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.

You can create a maximum of two SCI profiles.

Enter the following details:

- Name—Profile name.
- Server Host—IP address to the Northbound Data Streaming host server.

NOTE

SCI profile supports only the IPv4 format.

- 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.
- Data Type—select the required options for specific data type.

4. Click **OK**.

The updated profile is listed in the table.

The **Status** column displays the current connection status of the SCI profile.

5. **NOTE**

This setting applies to all SCI profiles.

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. **NOTE**

This setting applies to all SCI profiles.

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 SCI 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 7 SNMP v2 Agent Settings

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

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 8 SNMPv3 Agent Settings

| Field | Description | Your Action |
|-----------------------|---|--|
| User | 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. |
| Authentication | Indicates the authentication method. | <p>Choose the required option:</p> <ul style="list-style-type: none"> • SHA—Secure Hash Algorithm, message hash function with 160-bit output. <ul style="list-style-type: none"> a. Enter the Auth Pass Phrase. b. Choose the Privacy option. <ul style="list-style-type: none"> – None: Use no privacy method. – DES: Data Encryption Standard, data block cipher. – AES: Advanced Encryption Standard, data block cipher. c. Enter a Privacy Phrase, 8 through 32 characters. • MD5—Message-Digest algorithm 5, message hash function with 128-bit output. <ul style="list-style-type: none"> a. Enter the Auth Pass Phrase. b. Choose the Privacy option. <ul style="list-style-type: none"> – None: Use no privacy method. – DES: Data Encryption Standard, data block cipher. – AES: Advanced Encryption Standard, data block cipher. c. Enter a Privacy Phrase, 8 through 32 characters. |
| Privilege | Indicates the privileges granted to this community. | <p>Select the required privileges:</p> <ul style="list-style-type: none"> • Read—Privilege only to read. • Write—Privilege only to read and write. • Notification—Privilege to: <ul style="list-style-type: none"> – Trap—Choose this option to send SNMP trap notification. – Inform—Choose this option to send SNMP notification. <ul style="list-style-type: none"> a. Enter the Target IP address. b. Enter the Target Port number. c. Click Add. |

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.

Configuring General Settings

Configuring the SMS Gateway Server

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.

Configuring Advanced Gateway Options

You can configure advanced gateway options. This feature no longer depend on flat file changes.

To configure advanced gateway options:

1. Go to **System > General Settings > Gateway Advanced**.
2. Configure the following options:
 - **Allow Session on Accounting Fail**—Allows the controller TTG to terminate calls if accounting response fails. The default setting is **Yes**.
 - **GTP Network Service Access Point Identifier [NSAPI]**—Selects NSAPI for GTP message. The default setting is **1**.
 - **Include IMEI IE in GTP Messages**—Enables or disables IMEI IE in GTP messages. The default setting is **No**.

NOTE

In IMEI IE, the controller will send the MAC address of the UE appended with FFFE.

- **Include ECGI in GTPV2 Messages**—Used only when the S5/S8 interface is used for GTPv2:
- **Include TAI in GTPV2 Messages**—Used only when the S5/S8 interface is used for GTPv2.

- **GTPv2 Interface Type**—Choose the interface type. S2a or S5_S8.

NOTE

The default GTPv2 interface for the controller is S2a.

- **Include SCG-RAI in GTPV2 Messages**—Enables or disables SCG-RAI in GTPV2 messages. The default setting is **No**.
- **Include SCG-SAI in GTPV2 Messages**—Enables or disables SCG-SAI in GTPV2 messages. The default setting is **No**.

3. Click **OK**.

Configuring Node Affinity

Node affinity enables administrators to manually configure the controller nodes to which APs will connect.

To do this, set the order of preferred nodes on the node affinity page. Node affinity is implemented at the AP zone level, which means that all APs that belong to a zone will have the same node affinity settings.

If you want APs that belong to the same zone to connect to the same node whenever possible, you can configure set the preferred node for a particular zone.

NOTE

An affinity profile defines the order of the nodes to which APs that belong to the same zone will connect.

NOTE

Node affinity profile works only if it is restored in the same cluster. If the configuration must be restored to a different cluster, disable node affinity and remove the node affinity profiles containing nodes that are not available in the new cluster.

NOTE

Node affinity is not supported on the vSZ-H and vSZ-D platforms.

Enabling Node Affinity

To enable and configure node affinity:

1. Go to **System > General Settings > Node Affinity**.
2. Select **Enable Node Affinity**. Node Affinity Profile appears.
3. To:
 - Create an new profile:
 - a. Click **Create**, the Create Node Affinity Profile form appears.
 - b. Enter a **Name** and **Description**.
 - c. In the **Node Order** list, select the node and click **Up** or **Down** to position the node in the required order.
 - d. Click **OK**.
 - Edit the default profile:
 - a. Select the profile from the list and click **Configure**. The Edit Node Affinity Profile form appears.
 - b. Edit the **Name** and **Description**.
 - c. In the **Node Order** list, select the node and click **Up** or **Down** to position the node in the required order.
 - d. Click **OK**.

NOTE

When you enable node affinity, disable cluster redundancy.

- To set the number of times an AP will attempt to connect to the preferred node, enter the **# of Node Retry for Preferred Node**.
The default value is 3 and the accepted range is 1 to 10. If the AP is unable to connect to the preferred node, it will attempt to connect to the node that is next in the order of node priority.
- In the **Zone Assignment** section, set the node affinity profile that you want each zone to use. Select the Zone from the list and click **Assign Profile**. The Assign Node Affinity Profile to Selected Zones form appears.
- Select the **Node Affinity Profile** from the drop-down and click **OK**.
- Click **OK**.

Disabling Node Affinity

Follow these steps to disable node affinity:

- From **System > General Settings > Node Affinity**.
- Clear the **Enable Node Affinity** check box.
- Click **OK**. You have disabled node affinity.

Location Service

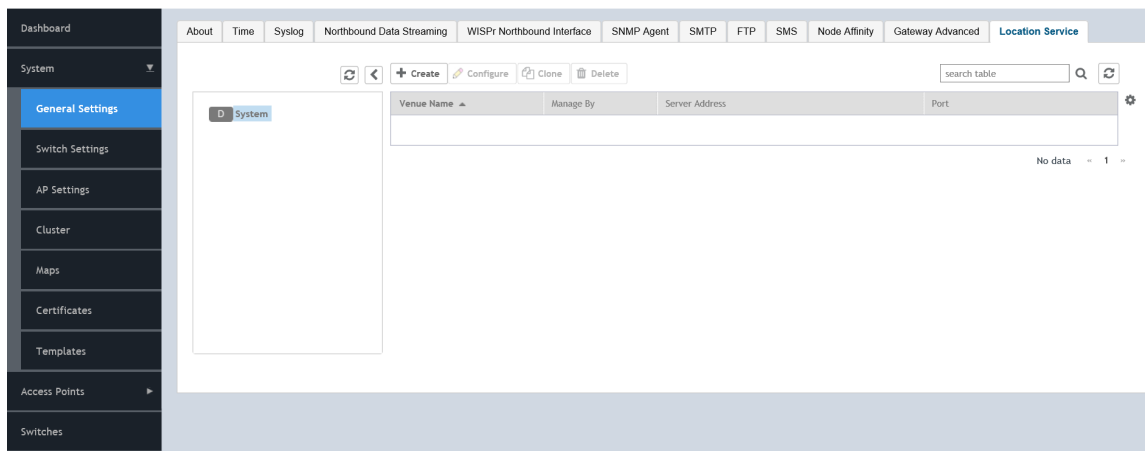
If your organization purchased the Ruckus Smart Positioning Technology (SPoT) location service, the controller must be configured with the venue information that is displayed in the SPoT Administration Portal.

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.

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

The **Location Service** page appears.

FIGURE 29 Location Service



2. Click **Create**.

The **Create LBS Server** page appears.

FIGURE 30 Creating an LBS Server

Create LBS Server

* Venue Name:

* Server Address: → IPv4 only

* 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.

NOTE

The server address must be entered in IPv4 format. The LBS server does not support configuration of IPv6 address.

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

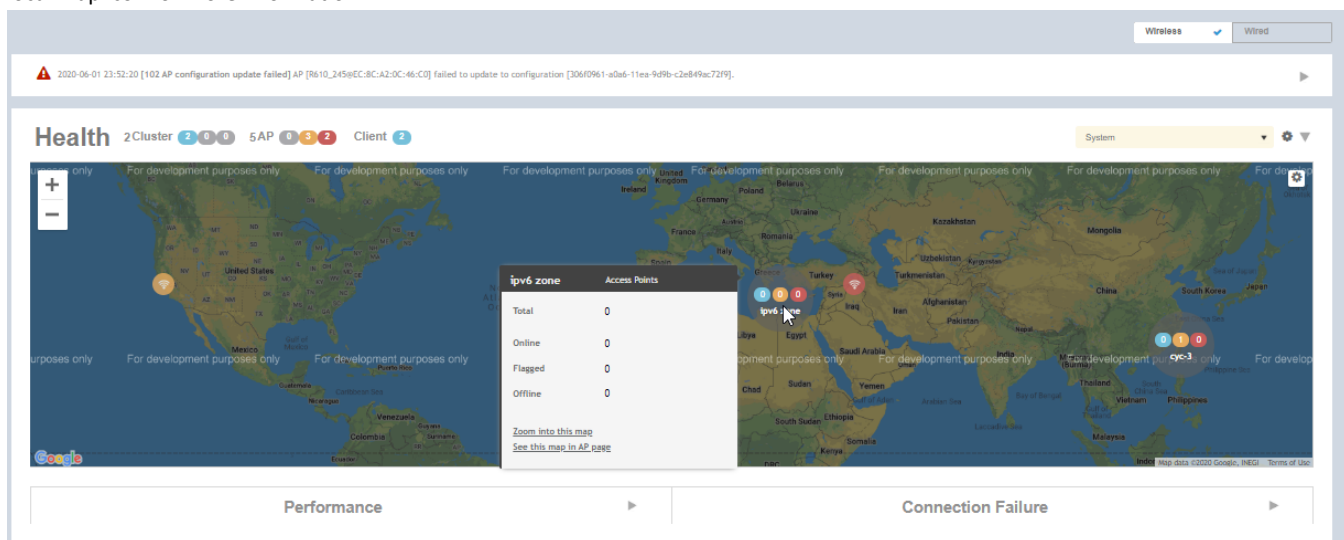
Importing floorplan maps into SmartZone allows you to further customize the information displayed on the Dashboard and Access Points pages, and monitor your APs, zones, groups, clients and traffic statistics all within the world map view on the Dashboard.

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 31 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.

- For **GPS Coordinates**, you can enter the **Latitude** and **Longitude** values.

FIGURE 32 The Add Map form

Add Map ✕

Details → **Scale Map** → **Place APs**

* Name:

Description:

* Location:

* GPS Coordinates: Latitude: Longitude: (example: 25.07858, 121.57141)

* Map Image:

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

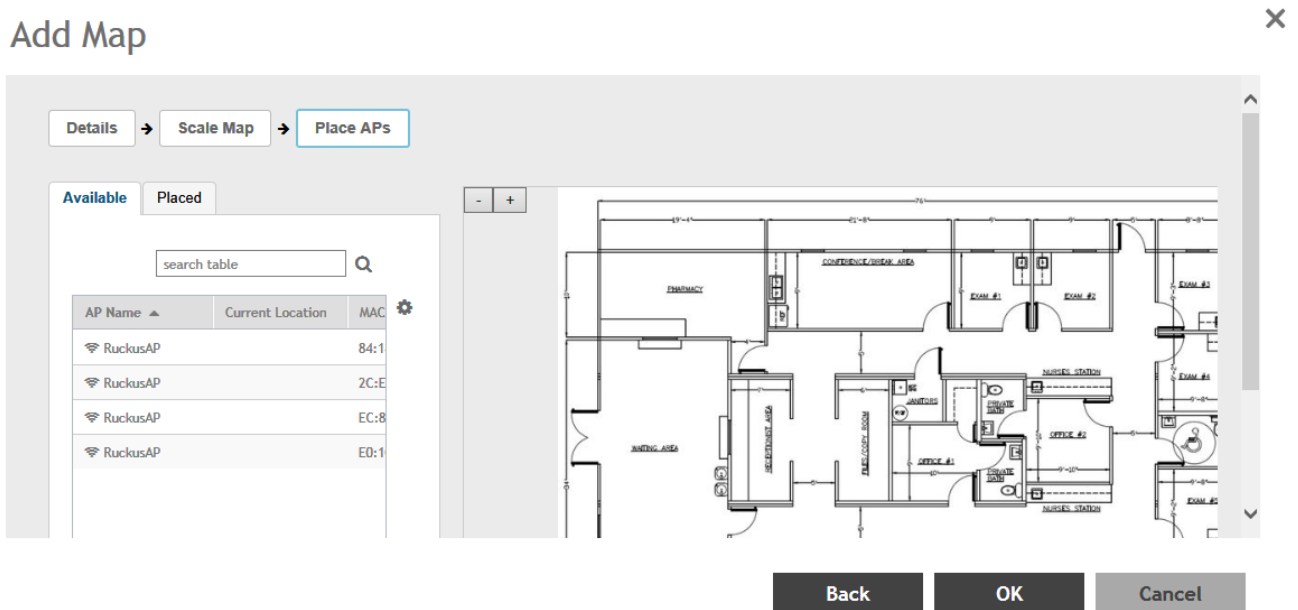
NOTE

The maximum file size per indoor map is 5MB.

- Click **Next**, the **Scale Map** tab appears.

- 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.

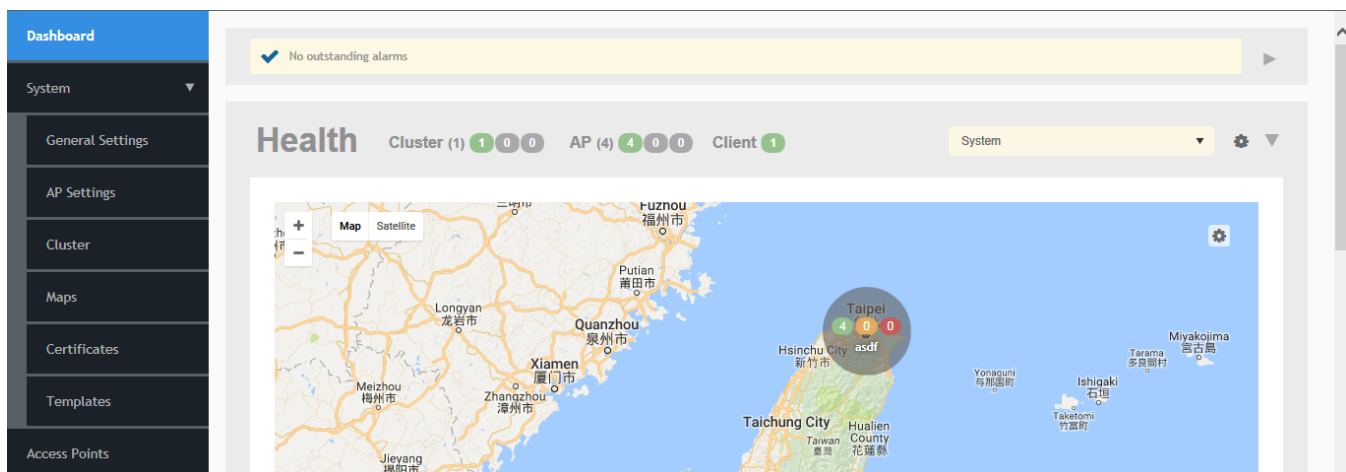
FIGURE 34 Drag and drop to place APs onto your floorplan





- 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 35 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

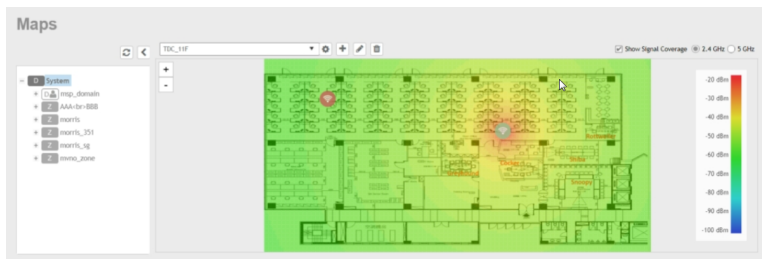
Radio Frequency (RF) signal strength can be viewed using a heat map for a specific location.

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 36 RF Coverage Heat Map



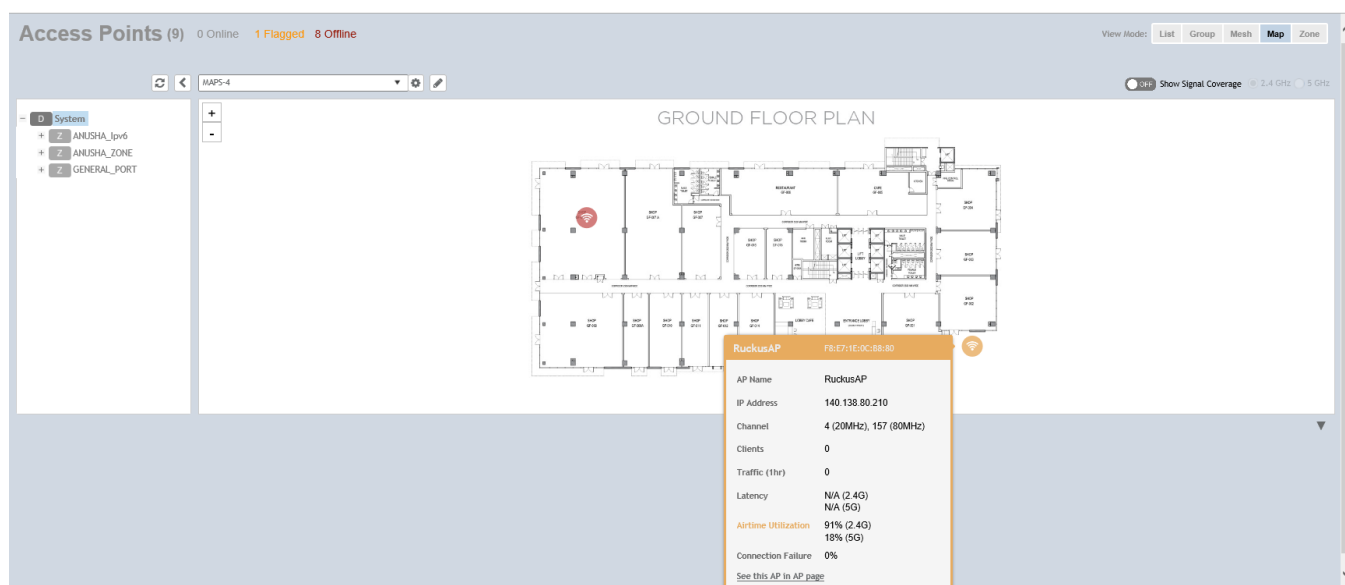
Monitoring APs Using the Map View

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 37 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

- Working with AP Registration Rules..... 67
- Tagging Critical APs..... 68
- Configuring the Tunnel UDP Port..... 69
- Setting the Country Code..... 69
- Limiting the Number of APs in a Domain or Zone..... 70
- Creating an AP MAC OUI Address..... 71
- AP Admin Password and Recovery SSID..... 72
- Power Source in AP Configuration..... 74

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 38 APs Tagged as Critical

Access Points (21) 9 Online 1 Flagged 11 Offline

System - Eddie R500 (38:FF:36:01:A2:10)

| MAC Address | AP Name | Status | Alarm | Clients | Latency (2.4G) | Airtime Utilization (2.4G) | Latency (5G) | Airtime Utilization (5G) | Zone |
|-------------------|----------------------|---------|-------|---------|----------------|----------------------------|--------------|--------------------------|----------------|
| 38:FF:36:01:A2:10 | Eddie R500 | Offline | 1 | 0 | 0 | 0 | 0 | 0 | Eddies AP Z... |
| 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:D0 | RuckusAP | Offline | 4 | 0 | 0 | 0 | 0 | 0 | Laurent Home |
| E0:10:7F:38:7F:80 | Eddie R600 | Offline | 3 | 0 | 0 | 0 | 0 | 0 | Eddies AP Z... |
| 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 | Zstawy - RuckusAP | Offline | 0 | 0 | 0 | 0 | 0 | 0 | PlusPOsdemo |

21 records - 1 2 -

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**.

Limiting the Number of APs in a Domain or Zone

You can limit the number of APs in a Partner-Managed Domain or a Zone. An MSP may have multiple customers each with their own zone and a number of APs. This feature ensures that their customers do not over-subscribe the licenses that they are entitled. MVNO domains do not have this option. When an AP joins a zone, where an AP number limitation has been applied to that zone, the controller checks the current capacity based on zone's limitation and:

- allows the new AP joining if the number of APs connected do not exceed the limit
- denies the new AP joining if there is no capacity in the domain or zone.

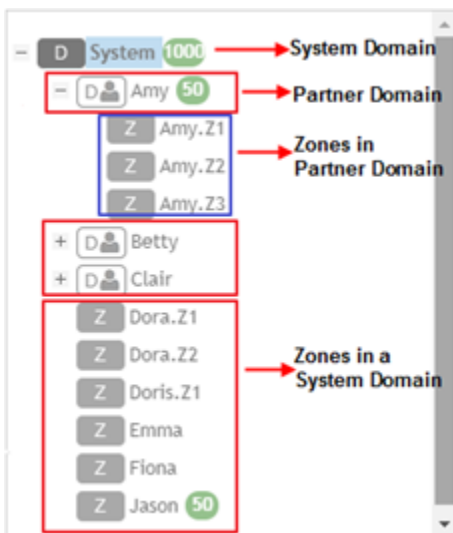
A scheduler task in the background periodically checks the AP number limitation against the number of APs connected. To avoid occupying the license capacity, the APs will be rejected in the following situations:

- If the AP number limitation of a Domain or a Zone is increased or reduced.
- If the license capacity is changed.

The following image gives a clarity on:

- System domain
- Partner domain
- Zones in a System domain
- Zones in a Partner domain

FIGURE 39 System Hierarchy



Limiting the AP count for a Partner Domain or a System Zone

Only super admin of the system domain is privileged to limit the number of APs in a partner domain or a system zone.

To limit the number of AP count for a partner domain or a system zone:

1. Log on to the controller web interface using super admin credentials of the system domain.

2. Follow the procedure to limit the number of APs in the partner domain or a zone in system domain:
 - a) Go to **System > AP Settings > AP Number Allocation**.
 - b) For **Enable AP Number Allocation**, select the **Enabled** check box and click **OK**. The Settings bar appears.
 - c) From the left pane, in the system tree hierarchy, select the partner-managed Domain or Zone for which you want to set the AP number limit.
 - d) On the right pane, select **Share Mode** or enter the **Number Limit**.
 - e) Click **OK**. You have set the AP number limit for the selected Domain or Zone.

Limiting the AP count for a Zone in a Partner Domain

To limit the number of AP count for a zone in a partner domain:

1. Create a super admin account for the partner domain. See the Administrating the Controller chapter.

2. **NOTE**

While creating user groups, in step 4 (l) c, for **Permission**, select Super Admin from the drop-down.

Create a user group and configure the access permissions, resources and administrator account. Refer [Creating User Groups](#) on page 503.

3. Log on to the controller web interface using the following logon details:

- **User Name:**

`Account Name@Domain`

The Account Name that you set when you created the Administrator Account and the Domain for which you created the Administrator Account. For example: If the partner domain is *TestDomain* and the Account Name is *User*, then the User Name is

`User@TestDomain`

- **Password** : The password that you set when you created the Administrator Account.

4. Follow the procedure to limit the number of APs for a zone in a partner-domain:
 - a) Go to **System > AP Settings > AP Number Allocation**.
 - b) Select the **Enable AP Number Allocation** check box and click **OK**. The Settings bar appears.
 - c) From the left pane, in the system tree hierarchy, select the partner-managed zone for which you want to set the AP number limit.
 - d) On the right pane, perform one of the following procedure:
 - Select **Share Mode**
 - Enter **Number Limit**
 - e) Click **OK**.

You have set the AP number limit for the selected partner-domain Zone.

Creating an AP MAC OUI Address

You must enable the AP MAC OUI validation for an AP with a specific organizationally unique identifier (OUI) to be allowed to connect to SZ. If the AP that is not in the OUI list connects to the SZ, then the AP is rejected and event code 186 is generated.

Perform the following procedure to create the MAC OUI address for an AP.

1. Select **System > AP Settings > AP MAC OUI Validation**.

Configuring AP Settings

AP Admin Password and Recovery SSID

2. Select **Enable AP MAC OUI Validation**.
3. Click **Create** to create the MAC OUI settings for an AP.

FIGURE 40 Creating an AP MAC OUI Address



Create MAC OUI

* **MAC OUI:**

Description:

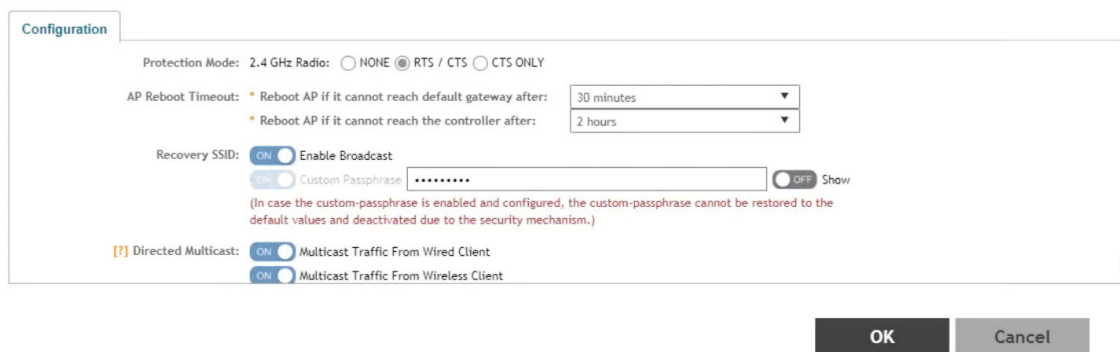
OK **Cancel**

4. Enter the MAC OUI.
5. Click **OK**.

AP Admin Password and Recovery SSID

This topic describes the mitigation of security enhancement of the AP admin password management.

Consider the following scenario while generating the configuration:



Configuration

Protection Mode: 2.4 GHz Radio: NONE RTS / CTS CTS ONLY

AP Reboot Timeout: * Reboot AP if it cannot reach default gateway after:

* Reboot AP if it cannot reach the controller after:

Recovery SSID: Enable Broadcast Custom Passphrase Show

(In case the custom-passphrase is enabled and configured, the custom-passphrase cannot be restored to the default values and deactivated due to the security mechanism.)

[?] Directed Multicast: Multicast Traffic From Wired Client Multicast Traffic From Wireless Client

OK **Cancel**

- Initial Installation: AP admin password need to be hashed in SHA-256 algorithm, stored in database and in configuration.

User can specify the Recovery SSID key in the Configuration Tab:

- The default of this Recovery SSID feature is enabled. The default passphrase is AP admin password in clear text format.
- If the user wants to change it, input the passphrase while enabling.

- The validation of passphrase, apply the same rule of WLAN passphrase.
- The passphrase can be clear text stored in the database and delivered to the AP in the GPB configuration by the way of secure channel (SSH channel).

The recovery SSID passphrase(key) will be delivered in GPB configuration as below:

- ccm_zone.proto
- message CcmCommon {
- /** recovery ssid
- */
- optional bool recovery_ssid_enabled = 26
- optional string recovery_ssid_psk_key = 27
- optional int32 server_loss_timeout = 28

When the Custom passphrase is disabled, the Custom passphrase filed is empty.

FIGURE 41 Custom Passphrase Disabled

The screenshot shows the configuration page for an AP. At the top, there is a 'Name' field with the value 'ssid_thesame_apapss' and a 'Description' field. Below this, there are radio buttons for 'Type' (Domain and Zone) and a 'Parent Group' dropdown set to 'System'. The 'Configuration' section is expanded, showing various settings. A red box highlights the 'Recovery SSID' section, which includes:

- 'Recovery SSID' toggle: ON
- 'Enable broadcast' radio button: selected
- 'Custom Passphrase' radio button: selected, with an empty text input field next to it.
- 'Show' toggle: OFF
- Footnote: (When the custom passphrase is enabled, passphrase cannot go back to the default settings.)

 Other visible settings include 'Location Based Service' (OFF), 'Hotspot 2.0 Venue Profile' (No data avail), 'Client Admission Control' for 2.4 GHz and 5 GHz radios (both OFF), 'Protection Mode' (RTS / CTS selected), 'AP Reboot Timeout' (30 minutes and 2 hours), and 'Directed Multicast' (all three options selected).

When the Custom passphrase is enabled, the Custom passphrase field is mandatory and should enter a passphrase.

FIGURE 42 Custom Passphrase Enabled

The screenshot shows the configuration page for an AP. At the top, there are fields for Name (custom-ssid-key), Description (postname-ipv4-zone), Type (Zone selected), and Parent Group (System). Below this is a 'Configuration' section with several options: Location Based Service (OFF), Hotspot 2.0 Venue Profile (No data avail), and Client Admission Control. The Client Admission Control section has two radio buttons for 2.4 GHz and 5 GHz, both set to OFF. Below these are settings for Protection Mode (RTS / CTS selected), AP Reboot Timeout (30 minutes and 2 hours), and Venue Code. A red box highlights the Recovery SSID section, which has 'Enable broadcast' selected and 'Custom Passphrase' entered as '*****'. Below this is a note: '(When the custom passphrase is enabled, passphrase cannot go back to the default settings.)'. At the bottom, there are three 'Directed Multicast' options, all set to ON.

Power Source in AP Configuration

The table below displays the PoE mode as per industry standards.

The currently used APs have AF, AT, AT+ convention modes. The standardization applies when the AP is forced to certain PoE power mode. If the AP is set to AUTO PoE mode, feedback displays PoE mode of the AP is currently configured.

The PoE mode as per the industry standards:

TABLE 9 Industry Standard PoE Modes

| Selection | Power@PSE | Power@AP (100M Cable) |
|-----------------|-----------|-----------------------|
| 802.3af | 15.4W | 12.95W |
| 802.3at | 30W | 25.5W |
| 802.3bt/Class 5 | 45W | 40W→35W |
| 802.3bt/Class 6 | 60W | 51W |
| 802.3bt/Class 7 | 75W | 62W |
| 802.3bt/Class 8 | 90W | 71.3W |

TABLE 10 Non-Standard High Power Solution Summary

| | Customers | Maximum Power Sourced |
|------|---|-----------------------|
| UPoE | Enterprise Switch | 60W |
| PoH | Consumer Customers, for example, audio systems) | 95W |

The SZ-GUI power mode drop-down has the following set of PoE mode configurations:

TABLE 11 PoE Mode Settings

| Name | Value |
|-----------------|-------|
| Auto | 0 |
| 802.3af | 1 |
| 802.3at | 2 |
| 802.3bt/Class 5 | 3 |
| 802.3bt/Class 6 | 4 |
| 802.3bt/Class 7 | 5 |

NOTE

The 802.3bt/Class5 is chosen for AP's with older software which advertise AT+.

NOTE

The below tables are applicable for stand alone APs as well. However, the IOT functionality is not available.

POE tables for different 11 AC AccessPoint

TABLE 12 R710

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT |
|--------------------------|----------------|------------|----------|-----------|----------|----------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled |
| AF | N/A | 2/4 | 4/4 | Enabled | Disabled | Disabled |
| AT | 25W | 4/4 | 4/4 | Enabled | Enabled | Enabled |
| Injector (Model 480125A) | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled |

TABLE 13 R610

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT |
|--------------------------|----------------|------------|----------|-----------|----------|----------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled |
| AF | N/A | 2/4 | 4/4 | Enabled | Disabled | Disabled |
| AT | 24W | 4/4 | 4/4 | Enabled | Enabled | Enabled |
| Injector (Model 480125A) | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled |

TABLE 14 R720

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT | Comments |
|----|----------------|------------|----------|-----------|----------|----------|-------------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | No comments |
| AF | N/A | 1/4 | 1/4 | Enabled | Disabled | Disabled | No comments |
| AT | 25W | 4/4 | 4/4 | Enabled | Disabled | Disabled | No comments |

TABLE 14 R720 (continued)

| | | | | | | | |
|----------------------------------|-----|-----|-----|---------|---------|---------|-------------------------------------|
| 3bt/class5 | 35W | 4/4 | 4/4 | Enabled | Enabled | Enabled | No comments |
| POE Injector (Model 480125A) 60W | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Force to 802.3bt/class5 from SZ GUI |

TABLE 15 M510

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT |
|--------------------------|----------------|------------|----------|-----------|----------|----------|
| DC | N/A | 2/2 | 2/2 | Enabled | Enabled | Enabled |
| AF | N/A | 2/2 | 2/2 | Enabled | Disabled | Disabled |
| AT | 25W | 2/2 | 2/2 | Enabled | Enabled | Enabled |
| Injector (Model 480125A) | N/A | 2/2 | 2/2 | Enabled | Enabled | Enabled |

TABLE 16 T610

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT |
|--------------------------|----------------|------------|----------|-----------|----------|----------------|
| DC | N/A | 3/3 | 3/3 | Enabled | Enabled | Enabled (0.5W) |
| AF | N/A | 2/3 | 3/3 | Enabled | Disabled | Disabled |
| AT | 25W | 3/3 | 3/3 | Enabled | Enabled | Enabled (0.5W) |
| Injector (Model 480125A) | N/A | 3/3 | 3/3 | Enabled | Enabled | Enabled (0.5W) |

POE tables for different 11 AX AccessPoint

TABLE 17 R730

| | LLDP | 2.4G tx/rx | 5G tx/rx | 5Gbps eth | 1Gbps eth | USB | IOT | Comments |
|----------------------------------|------|------------|----------|-----------|-----------|----------------|-------------|--|
| DC | N/A | 4/4 | 8/8 | Enabled | Enabled | Enabled | Enabled | No comments |
| AF | N/A | 1/4 | 1/8 | Enabled | Disabled | Disabled | N/ADisabled | Not supported via SZ-GUI, but we can AF mode via rkscli. |
| AT Mode = 0 | 25W | 4/4 | 4/8 | Enabled | Enabled | Enabled (0.5W) | Enabled | By default AT - mode = 0 |
| AT Mode = 1 | 25W | 4/4 | 8/8 | Enabled | Disabled | Disabled | Disabled | Set AT - mode = 1 via Rkscli |
| 802.3bt/class 5 | 35W | 4/4 | 8/8 | Enabled | Enabled | Enabled | Enabled | No comments |
| POE Injector (Model 480125A) 60W | N/A | 4/4 | 4/8 | Enabled | Enabled | Enabled | N/A | Force to 802.3bt/class5 from SZ GUI |

TABLE 18 R850

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 5Gbps eth | 1Gbps eth | USB | IOT | Comment |
|----|----------------|------------|----------|-----------|-----------|----------|----------|--|
| DC | N/A | 4/4 | 8/8 | Enabled | Enabled | Enabled | Enabled | No comments |
| AF | N/A | 1/4 | 1/8 | Enabled | Disabled | Disabled | Disabled | Not supported via SZ-GUI, but we can AF mode via rkscli. |

TABLE 18 R850 (continued)

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 5Gbps eth | 1Gbps eth | USB | IOT | Comment |
|----------------------------------|----------------|------------|----------|-----------|-----------|----------------|----------|-------------------------------------|
| AT (Mode=0) | 25W | 4/4 | 4/8 | Enabled | Enabled | Enabled (0.5W) | Enabled | By default at-mode=0 |
| AT (Mode=1) | 25W | 4/4 | 8/8 | Enabled | Disabled | Disabled | Disabled | Set at-mode=1 via Rkscli |
| 802.3bt/class5 | 35W | 4/4 | 8/8 | Enabled | Enabled | Enabled | Enabled | No comments |
| POE Injector (Model 480125A) 60W | N/A | 4/4 | 4/8 | Enabled | Enabled | Enabled | Enabled | Force to 802.3bt/class5 from SZ GUI |

TABLE 19 R750

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 2.5Gbps eth | 1Gbps eth | USB | IOT |
|----------------------------------|----------------|------------|----------|-----------------------|-----------|----------|----------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled |
| AF | N/A | 2/4 | 2/4 | Enabled | Disabled | Disabled | Disabled |
| AT | 25W | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled |
| POE Injector (Model 480125A) 60W | N/A | 4/4 | 4/4 | Enabled (1Gbps speed) | Enabled | Enabled | Enabled |

TABLE 20 T750

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 2.5Gbps eth | 1Gbps eth | USB | IOT | PSE | Comment |
|----------------------------------|----------------|------------|----------|-----------------------|-----------|----------|----------|----------|------------------------------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Enabled | No comments |
| AF | N/A | 1/4 | 1/4 | Enabled | Disabled | Disabled | Disabled | Disabled | Not supported operation mode |
| AT w/o USB | 25W | 4/4 | 4/4 | Enabled | Enabled | Disabled | Enabled | Disabled | No comments |
| AT with USB | 25W | 2/4 | 4/4 | Enabled | Disabled | Enabled | Enabled | Disabled | Set AT - mode = 1 via Rkscli |
| 802.3bt/class5 | 35W | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Disabled | No comments |
| 803.3bt/class6 | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Disabled | 51W by H/W negotiation |
| 802.3bt/class7 | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Enabled | 62W by H/W negotiation |
| POE 60W Injector (Model 480125A) | N/A | 4/4 | 4/4 | Enabled (1Gbps speed) | Enabled | Enabled | Enabled | Disabled | Force to 802.3bt/class5 |
| POE 90W Injector | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Enabled | Force to 802.3bt/class7 |

TABLE 21 R650

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 2.5Gbps eth | 1Gbps eth | USB | IOT |
|----|----------------|------------|----------|-------------|-----------|----------|----------|
| DC | N/A | 2/2 | 4/4 | Enabled | Enabled | Enabled | Enabled |
| AF | N/A | 2/2 | 2/4 | Enabled | Disabled | Disabled | Disabled |

Configuring AP Settings
 Power Source in AP Configuration

TABLE 21 R650 (continued)

| | | | | | | | |
|---------------------------------|-----|-----|-----|--------------------------|---------|---------|---------|
| AT | 25W | 2/2 | 4/4 | Enabled | Enabled | Enabled | Enabled |
| POE Injector (Model 480125A) | N/A | 2/2 | 4/4 | Enabled (1Gbps speed) | Enabled | Enabled | Enabled |

TABLE 22 R550

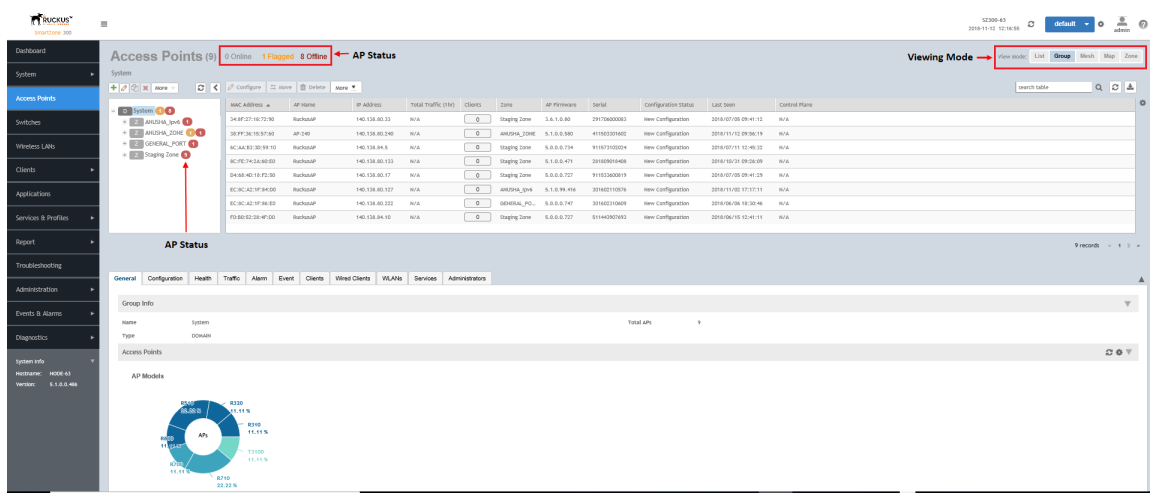
| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 2.5Gbps eth | 1Gbps eth | USB | IOT |
|---------------------------------|----------------|------------|----------|-------------|-----------|----------|----------|
| DC | N/A | 2/2 | 2/2 | Enabled | Enabled | Enabled | Enabled |
| AF | N/A | 2/2 | 2/2 | Enabled | Disabled | Disabled | Disabled |
| AT | 25W | 2/2 | 2/2 | Enabled | Enabled | Enabled | Enabled |
| POE Injector (Model 480125A) | N/A | 2/2 | 2/2 | Enabled | Enabled | Enabled | Enabled |

Working With Access Points

- Understanding WLAN Services..... 79
- Viewing Modes..... 109
- AP Status..... 109
- Configuring Access Points..... 110
- Managing Access Points..... 120
- Multi-Tunnel Support for Access Points..... 132
- Link Aggregation Control Protocol (LACP) support for R720 AP..... 137
- Power Source in AP Configuration..... 140

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

FIGURE 43 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.

Creating an AP Domain

To create an AP domain:

1. From the System tree hierarchy, select the location where you want to create the domain.
2. Click the **Create**  button, the Create Group form appears.
3. Configure the following details:
 - a. Enter a **Name** for the domain.
 - b. Enter a **Description** about the domain.
 - c. By default, the **Type** selected is **Domain**.
 - d. The **Parent Group** displays the group to which this domain will be tagged.
 - e. If you want to create a domain to manage MSP-related settings within that domain, in the **Managed by Partner** field, select the **Enable** check box.
4. Click **OK**.

NOTE

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

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 2048 WLAN services.

By default, an AP zone named Staging Zone exists in the SZ300/vSZH platforms and Default Zone in the SZ100/vSZE platforms. Any AP that registers with the controller that is not assigned a specific zone is automatically assigned to the Staging or Default Zone. This section describes how to use AP zones to manage devices.

NOTE

When an AP is assigned or moved to the Staging or Default 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 47.

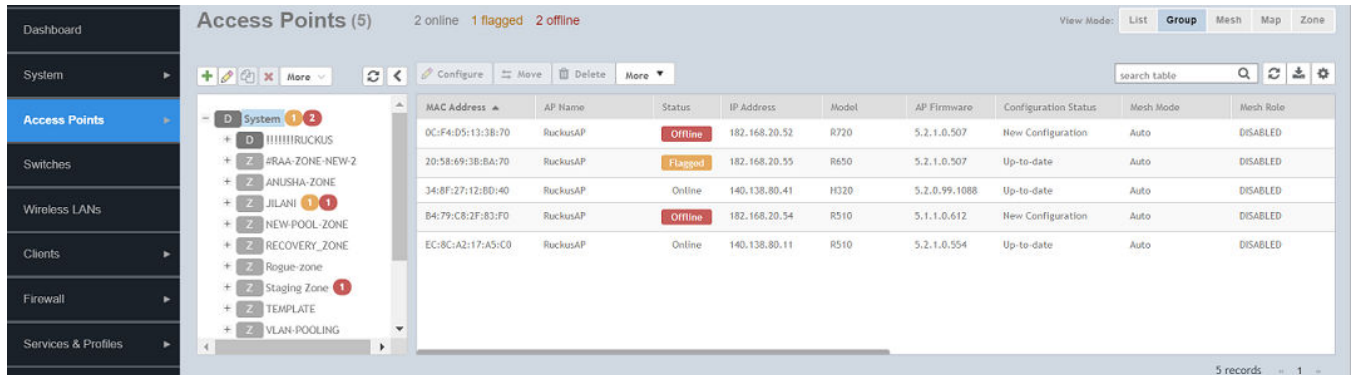
Creating an AP Zone

An AP zone (or zone) functions as a way of grouping Ruckus APs and applying settings, including WLANs to these groups of Ruckus APs.

To create an AP zone, complete the following steps.

1. On the menu, click **Access Points**.

FIGURE 44 Access Points Page




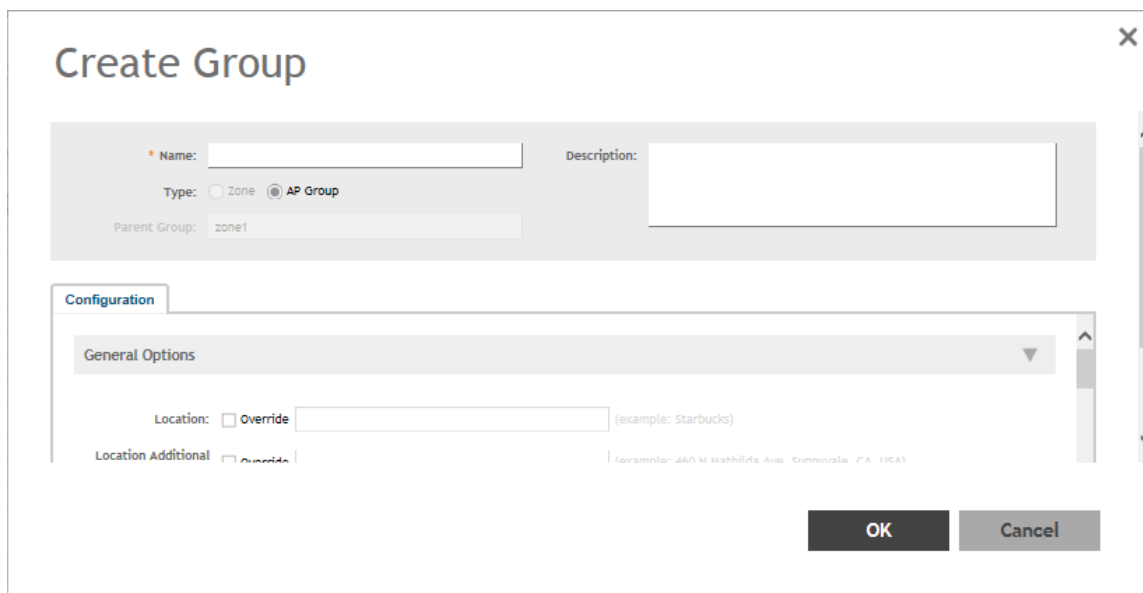
- From the **System** tree hierarchy, select the location where you want to create the zone (for example, System or Domain), and click .

FIGURE 45 Create Groups Page



- Configure the zone by completing the settings listed in the following table.

TABLE 23 AP Zone Details

| Field | Description | Your Action |
|---|---|---|
| Name | Indicates the name of the zone or an AP group. | Enter a name. |
| Description | Indicates the short description assigned to the zone or AP group. | Enter a brief description |
| Type | Indicates if you are creating a domain, zone, or an AP group. | Appears by default. You can also choose the option. |
| Parent Group | Indicates the parent AP group. | Appears by default. |
| Configuration > General Options | | |

TABLE 23 AP Zone Details (continued)

| Field | Description | Your Action |
|--|--|---|
| AP Firmware | Indicates the firmware to which it applies. | Select the firmware. |
| Country Code | Indicates the country code. Using the correct country code helps ensure that APs use only authorized radio channels. | Select the country code. |
| Location | Indicates the generic location of the zone. | Enter the location. |
| Location Additional Information | Indicates detailed location. | Enter additional location information. |
| GPS Coordinates | Indicates the geographical location. | Enter the following coordinates: <ul style="list-style-type: none"> • Longitude • Latitude • Altitude |
| AP Admin Logon | Indicates the administrator logon credentials. | Enter the Logon ID and Password . |
| AP Time Zone | Indicates the time zone that applies. | Select a time zone, and enter the details as required. |
| AP IP Mode | Indicates the IP version that applies. | Select the IP version. IPv6, IPv4, and dual addressing modes are supported. |
| Historical Connection Failures | 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. |
| DP Zone Affinity Profile | Specifies the DP affinity profile for the zone. NOTE This option is supported only on vSZ-H. | Select the zone affinity profile from the list. |
| SSH Tunnel Encryption | Specifies the encryption that reduces the load on controller control of SSH traffic. | Select the required option: <ul style="list-style-type: none"> • AES 128 • AES 256 |
| Cluster Redundancy | Provides cluster redundancy option for the zone. NOTE Cluster redundancy is supported only on SZ300 and vSZ-H. | Select the required option: <ul style="list-style-type: none"> • Zone Enable • Zone Disable |
| Configuration > Mesh Options | | |
| Enable mesh networking in this zone | 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. |
| Zero Touch Mesh | Enables a new AP to join the network using wireless connection. | Click the button. |
| Mesh Name (ESSID) | Indicates the mesh name. | Enter a name for the mesh network. Alternatively, do nothing to accept the default mesh name that the controller has generated. |
| Mesh Passphrase | Indicates the passphrase used by the controller to secure the traffic between Mesh APs. | Enter a passphrase that contains at least 12 characters. Alternatively, click Generate to generate a random passphrase with 32 characters or more. |
| Mesh Radio Option | Indicates the channel range configured. | Select the channel option: 2.4 GHz or 5 GHz. |
| Configuration > Radio Options | | |

TABLE 23 AP Zone Details (continued)

| Field | Description | Your Action |
|-----------------------------------|---|---|
| Channel Range (2.4G) | Indicates that you want to override the 2.4 GHz channel range that has been configured for the zone to which this AP group belongs. | Select Select Channel Range (2.4G) check boxes for the channels on which you want the 2.4 GHz radios of managed APs to operate. Channel options include channels 1 to 11. By default, all channels are selected. |
| DFS Channels | Allows ZoneFlex APs to use DFS channels. | Click to enable the option. |
| Channel 144 | Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 80+80 MHz and 160 MHz modes are supported if the AP supports these modes. Disabling this option provides Channel 140 support only to 20 MHz mode. NOTE This option is available for selection only if you enable the DFS Channels option. NOTE This feature is currently supported only in the United States. | Click to enable the option. |
| 5.8 Ghz Channels | Provides C-band support for all Outdoor APs and the following Indoor APs: R310, R510, and R710 . NOTE This feature is available only for countries that support 5.8 Ghz channel. For example, the UK provides indoor AP—5.8 Ghz channel support. | Select the Allow 5.8Ghz channels check box. |
| 5.8 Ghz Channels License | Enables full TX Power Adjustment for C-band channels. NOTE This feature is supported only for the UK. | Select the Allow 5.8Ghz channels use full power check box. |
| Channel Range (5G) Indoor | Indicates the channels on the 5 GHz radio that you want managed indoor APs to operate. | Select the check boxes. |
| Channel Range (5G) Outdoor | Indicates the channels on the 5 GHz radio that you want managed outdoor APs to operate. | Select the check boxes. |

TABLE 23 AP Zone Details (continued)

| Field | Description | Your Action |
|--------------------------------------|--|---|
| Radio Options b/g/n (2.4 GHz) | Indicates the configuration options for the 2.4 GHz radio. | <p>Select the following options:</p> <ul style="list-style-type: none"> Channelization—Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically. Channel—Select the channel to use for the b/g/n (2.4 GHz) radio, or select Auto to set it automatically. Auto cell sizing— 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. <p style="text-align: center;">NOTE Ensure that Background Scan is enabled.</p> TX Power Adjustment—Select the preferred TX power, if you want to manually configure the transmit power on the 2.4 GHz radio. By default, TX power is set to Full on the 2.4 GHz radio. <p style="text-align: center;">NOTE 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 maximum allowable value according to the AP's capability and the operating country's regulations.</p> |

TABLE 23 AP Zone Details (continued)

| Field | Description | Your Action |
|---|--|--|
| Radio Options a/n/ac (5 GHz) | Indicates the configuration options for the 5 GHz radio. | <p>Select the following options:</p> <ul style="list-style-type: none"> • Channelization—Set the channel width used during transmission to 20, 40, 80, 80+80, 160 (MHz), or select Auto to set it automatically. • Channel—For Indoor and Outdoor, select the channel to use for the a/n/c (5 GHz) radio, or select Auto to set it automatically. • Secondary Channel (80+80)—For Indoor and Outdoor, the default secondary channel to use for the a/n/c (5 GHz) radio, is set as Auto. • Auto cell sizing— 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. <p style="text-align: center;">NOTE Ensure that Background Scan is enabled.</p> <ul style="list-style-type: none"> • TX Power Adjustment—Select the preferred TX power, if you want to manually configure the transmit power on the 5 GHz radio. By default, TX power is set to Full on the 5 GHz radio. <p style="text-align: center;">NOTE 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 maximum allowable value according to the AP's capability and the operating country's regulations.</p> |
| Configuration > AP GRE Tunnel Options | | |
| Ruckus GRE Profile | Indicates the GRE tunnel profile. | Choose the GRE tunnel profile from the list. |
| Ruckus GRE Forwarding Broadcast | Forwards the broadcast traffic from network to tunnel. | Click the option to enable forwarding broadcast. |
| Soft GRE Profiles | Indicates the SoftGRE profiles that you want to apply to the zone. | <ol style="list-style-type: none"> Click the Select check box, a form is displayed. From the Available Profiles, select the profile and click the -> icon to choose it. You can also click the + icon to create a new SoftGRE profile. Click OK. |
| IPsec Tunnel Mode | Indicated the tunnel mode for the Ruckus GRE and SoftGRE profile. | <p>Select an option:</p> <ul style="list-style-type: none"> • Disable • SoftGRE • Ruckus GRE |

TABLE 23 AP Zone Details (continued)

| Field | Description | Your Action |
|--|---|---|
| IPsec Tunnel Profile | Indicates the tunnel profile for SoftGRE. NOTE Select the same tunnel type for IPsec tunnel profile in WLAN configuration. | Choose the option from the drop-down. |
| Configuration > Syslog Options | | |
| Enable external syslog server for APs | 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 the syslog server. If the primary server goes down, the AP sends syslog messages to the secondary server as backup: <ul style="list-style-type: none"> • Primary Server Address • Secondary Server Address • Port for the respective servers • Portocol: Select between UDP and TCP protocols • Event Facility • Priority • Send Logs: Choose to send the General Logs, Client Logs or All Logs |
| Configuration > AP SNMP Options | | |
| Enable AP SNMP | Indicates if the AP SNMP option is enabled. | Select the check box. |
| SNMPv2 Agent | Indicates if the SNMPv2 agent is enabled. | If the SNMPv2 agent is enabled, configure the community settings. <ol style="list-style-type: none"> Click Create and enter Community. Select the required Privilege. If you select Notification, enter the Target IP. Click OK. |
| SNMPv3 Agent | Indicates the SNMPv3 Agent is applied. | If the SNMPv3 agent is enabled, configure the community settings. <ol style="list-style-type: none"> Click Create and enter User. Select the required Authentication. Enter the Auth Pass Phrase. Select the Privacy option. Select the required Privilege. If you select Notification, select the option Trap or Inform and enter the Target IP and Target Port. Click OK. |
| Configuration > Cellular Options | | |

TABLE 23 AP Zone Details (continued)

| Field | Description | Your Action |
|--|---|---|
| LTE Band Lock | <p>Displays the list of LTE bands (4G/3G) and allows you to lock one or more bands from the list. Once a lock is enabled, the connection is established only to the specified bands.</p> <p>NOTE The list of bands is only applicable to:</p> <ul style="list-style-type: none"> • Domain • USA • Canada • Japan | <p>Select the check box and choose the band from:</p> <ul style="list-style-type: none"> • Primary Sim • Secondary Sim |
| Configuration > Advanced Options | | |
| Restricted AP Access Profile | <p>Restricted AP Access blocks access to the AP's standard well know open ports to protect the APs and enhance their security.</p> <p>NOTE This feature is available from 5.2 release and onwards.</p> | <p>Select the Restricted AP Access profile from the drop-down. You can also create a new profile by clicking + icon.</p> <p>NOTE By default this feature is disabled.</p> <p>NOTE You can add maximum five Restricted AP Access profiles for a zone.</p> |
| Channel Mode | <p>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.</p> | <p>Select the Allow indoor channels check box.</p> |
| Auto Channel Selection | <p>Indicates auto-channel settings.</p> | <p>Select the check box and choose the option.</p> |
| Background Scan | <p>Runs a background scan.</p> | <p>Select the respective check boxes and enter the duration in seconds:</p> <ul style="list-style-type: none"> • Background Scanning—Changes the AP channel if there is interference. • ChannelFly—Continuously monitors potential throughput and changes the AP channel to minimize interference and optimize throughput. |
| Smart Monitor | <p>Indicates AP interval check and retry threshold settings.</p> | <p>Select the check box and enter the interval and threshold.</p> |
| AP Ping Latency Interval | <p>Measures the latency between the controller and AP periodically, and sends this data to SCI.</p> | <p>Enable by moving the button to ON to measure latency.</p> |
| AP Management VLAN | <p>Indicates the AP management VLAN settings.</p> | <p>Choose the option. Click VLAN ID, 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>ATTENTION For standalone APs, set the AP Ethernet port to trunk before changing the AP Management VLAN settings.</p> |
| Rogue AP Detection | <p>Indicates rogue AP settings.</p> | <p>Enable the option.</p> |

TABLE 23 AP Zone Details (continued)

| Field | Description | Your Action |
|--|--|---|
| Rogue Classification Policy | Indicates the parameters used to classify rogue APs. This option is available only if you enable the Rogue AP Detection option. | <p>Select the options for rogue classification policy:</p> <ul style="list-style-type: none"> • – Enable events and alarms for all rogue devices – Enable events and alarms for malicious rogues only • Report RSSI Threshold: Enter the threshold. Range: 0 through 100. • Protect the network from malicious rogue access points: Enable the option and choose one of the following: <ul style="list-style-type: none"> – Aggressive – Auto – Conservative • Radio Jamming Detection: Enable the option and enter the Jamming Threshold in percentage. |
| DoS Protection | Indicates settings for blocking a client. | Select the check box and enter the duration in seconds. |
| Load Balancing | Balances the number of clients or the available capacity across APs. | <p>Select the required option:</p> <ul style="list-style-type: none"> • Based on Client Count • Based on Capacity • Disabled |
| Run load balancing on 2.4 GHz radio | Runs load balancing on 2.4 GHz band. | Select the option and enter the adjacent radio threshold. |
| Run load balancing on 5 GHz radio | Runs load balancing on 5 GHz band. | Select the option and enter the adjacent radio threshold. |
| Band Balancing | Balances the client distribution across frequency bands. | Enter the 2.4G client percentage to control the 2.4G clients limit and to enforce band balance. |
| Steering Mode | Controls the APs' steering behavior for load balancing and band balancing. | <p>Select the option and use the slider to actively control associated stations to meet the distribution requirements allowing band balancing and load balancing:</p> <ul style="list-style-type: none"> • Basic (default): During heavy load conditions, this option withholds probe and authentication responses in order to achieve load balance. • Proactive: This is a dynamic form of band balancing where some selected associated clients are rebalanced on the AP or across APs utilizing the 802.11v BTM. The AP sends a BTM message to the client to roam and it is left to the client's discretion to make its roaming decision. • Strict: This is an aggressive form of balancing where some selected associated clients are forced to rebalance utilizing the 802.11v BTM. The AP sends a BTM message to the client to roam. If the client does not roam, the client is forced to disconnect after 10 seconds. Additionally, some selected non-802.11v clients are forcefully disconnected directly to force them to roam. <p style="text-align: center;">NOTE The band change is applicable only for those connected clients that support the 802.11v standard.</p> <p>Enter the percentage of client load on the 2.4 GHz band.</p> |




TABLE 23 AP Zone Details (continued)

| Field | Description | Your Action |
|--|--|--|
| Location Based Service | Indicates that the location-based service is enabled. | <ul style="list-style-type: none"> Select the check box and choose the options. Click Create, In the Create LBS Server form: <ol style="list-style-type: none"> Enter the Venue Name. Enter the Server Address. Enter the Port number. Enter the Password. |
| Client Admission Control | 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"> Min Client Count Max Radio Load Min Client Throughput |
| Protection Mode | Indicates the mechanism to reduce frame collision. | Choose one of the following options: <ul style="list-style-type: none"> None RTS/CTS CTS Only |
| AP Reboot Timeout | Indicates the AP reboot settings. | Choose the required option: <ul style="list-style-type: none"> Reboot AP if it cannot reach default gateway after Reboot AP if it cannot reach the controller after |
| Recovery SSID | Allows you to enable or disable the Recovery (Island) SSID broadcast on the controller. | Enable Recovery SSID Broadcast . |
| My.Ruckus support for Tunnel-WLAN/ VLAN | By default, support for LBO, tunneled-WLAN, and non-default management VLAN is disabled because it adds an ACL which affects the LBO and tunneled-WLAN performance. Enabling this support may have a 10 percent impact on the Wi-Fi performance. | Enable the option for support. |

4. Click **OK**.

For SZ300 and vSZ-H, you can also migrate the Zone configuration from a regular Domain to a Partner Domain. For more information, see <https://support.ruckuswireless.com/answers/000006414>

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.

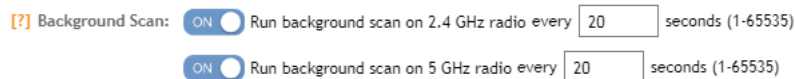
ChannelFly has undergone significant changes in SmartZone 5.2.1, combining the benefits of the Background Scanning method and the original Legacy ChannelFly. ChannelFly is the recommended method for all deployments.

TABLE 24

| Channel Selection Method | When to Use |
|---|--|
| ChannelFly | Preferred for most deployments |
| Background Scanning | For existing deployments that currently use Background Scanning |
| Legacy ChannelFly (Accessible only from AP CLI) | When Background Scan is not allowed – Legacy ChannelFly excels at avoiding excessive interference without the need of <i>Background Scan</i> |

NOTE

Both channel selection methods require *Background Scan*, ideally with the default 20 second scan interval. Background Scan is accessible from the zone configuration, advanced settings.

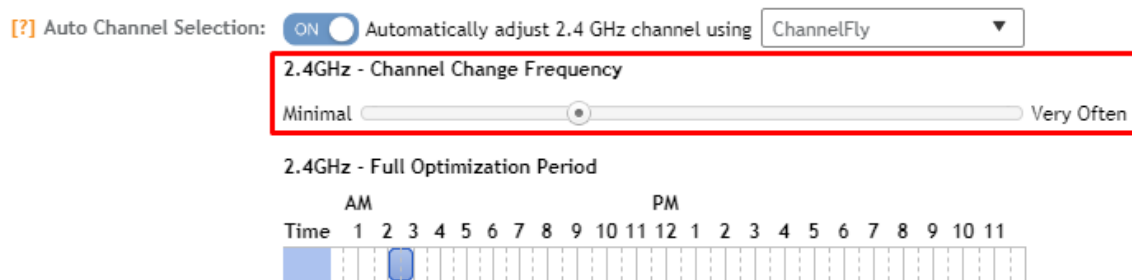


ChannelFly

ChannelFly uses Background Scan to collect information on the presence of neighboring APs and to assess how busy the channel is. The algorithm focuses on placing neighboring APs on different channels and avoiding busy channels. A Background Scan interval of 20 seconds is recommended for most deployments. In deployments where a larger interval is necessary, ChannelFly will still work but will take longer to settle upon a channel plan and may be less responsive to interference.

ChannelFly uses 802.11h channel change announcements to minimize the impact of channel changes on the wireless client. Despite 802.11h, channel changes still run the risk of disrupting wireless clients, and ChannelFly takes into the account the impact on associated clients.

The *Channel Change Frequency* (CCF) configuration allows the user to specify the responsive of ChannelFly to interference with consideration for the impact on associated clients. ChannelFly will avoid performing channel changes when a certain number of clients are associated to the AP on a per-radio basis. This threshold is defined by the CCF. **With the default CCF of 33, channel changes may occur only when the number of associate clients exceeds 3.** The CCF also affects the probability that a channel change occurs when a better channel is found. However, a channel change will only occur when the number of associate clients is below the client threshold as defined in Table 25.



The table below shows for each CCF, the number of associated clients that would bar ChannelFly from performing a channel change.

TABLE 25 Client Threshold Table

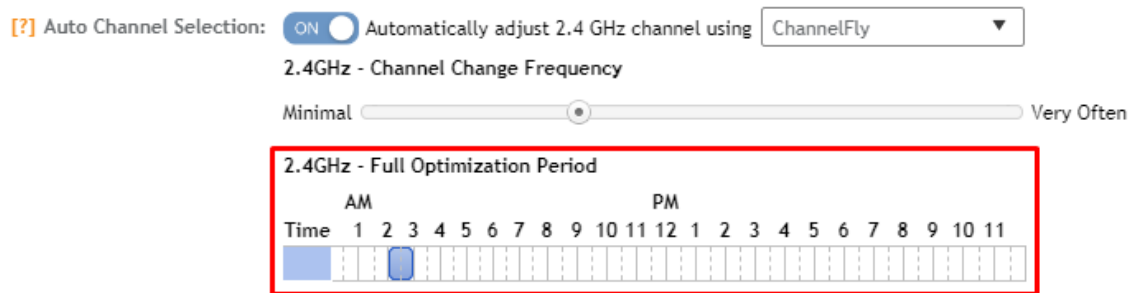
| | | | | | | | | | | | |
|------------------|-----|----|----|----|----|----|----|----|----|----|---|
| CCF | 100 | 90 | 80 | 70 | 60 | 50 | 40 | 30 | 20 | 10 | 1 |
| Client Threshold | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

For deployments where impact on the clients is less of a consideration and avoiding interference is paramount, higher values of CCF are recommended.

For deployments with low client counts, two or fewer associated clients per AP on average, a CCF of 10 or 20 is recommended. For deployments where channel changes are not allowed to impact any associate client, a CCF of 0 is recommended. For deployments where impact on clients is less of a consideration and avoiding interference is paramount, higher values of CCF are recommended.

The *Full Optimization Period* configuration specifies a period of time where ChannelFly is allowed to ignore the impact of channel changes on associated clients. During this time, preferably when the wireless network is not expected to be actively servicing clients such as the middle of the night, ChannelFly will be free to full optimize the channel plan. A higher number of channel changes may be observed during this time.

The *Full Optimization Period* can be specified by clicking and clicking-and-dragging the time bar. The time periods can be non-contiguous, and the period can be disabled entirely by clicking the blue box under *Time*.



For the first hour following the reboot of an AP, ChannelFly may perform up to six channel changes in order to quickly settle upon a channel plan. During this period, ChannelFly will ignore the impact of channel changes on associated clients.

The table below summarizes the channel change behavior for each of the ChannelFly states.

TABLE 26

| State | Behavior |
|--------------------------|--|
| AP reboot | Channel changes may occur at higher frequency for the first hour |
| Normal operation | Channel changes may occur only when the number of associated clients is greater than the client threshold based on the <i>Channel Change Frequency</i> |
| Full Optimization Period | Channel changes may occur at higher frequency |

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.

To revert to Legacy ChannelFly, first select ChannelFly in SmartZone, then from AP CLI:

```
rkscli: set channselectmode wifi[0/1] <mode> wifi0 – 2.4 GHz wifi1 – 5 GHz<mode> - 1: ChannelFly0: Legacy ChannelFly
```

```
rkscli: set channselectmode wifi[0/1] <mode>
```

```
wifi0 – 2.4 GHz
```

```
wifi1 – 5 GHz
```

```
<mode> - 1: ChannelFly
```

```
0: Legacy ChannelFly
```

Background Scanning

Background Scanning is a channel selection method, and *Background Scan* is the AP functionality where the AP briefly leaves the home channel to scan another channel.

Background Scanning uses Background Scan to collect information on the presence of neighboring APs. Background Scanning focuses on finding a channel with the fewest number of neighbors.

When the AP is rebooted, Background Scanning will enter a training period where the number of channel changes may be elevated in the first hour.

Background Scan is required, with the recommended default scan interval of 20 seconds. In situations where a larger scan interval is necessary, Background Scan will require a longer training period.

NOTE

Background Scan 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.

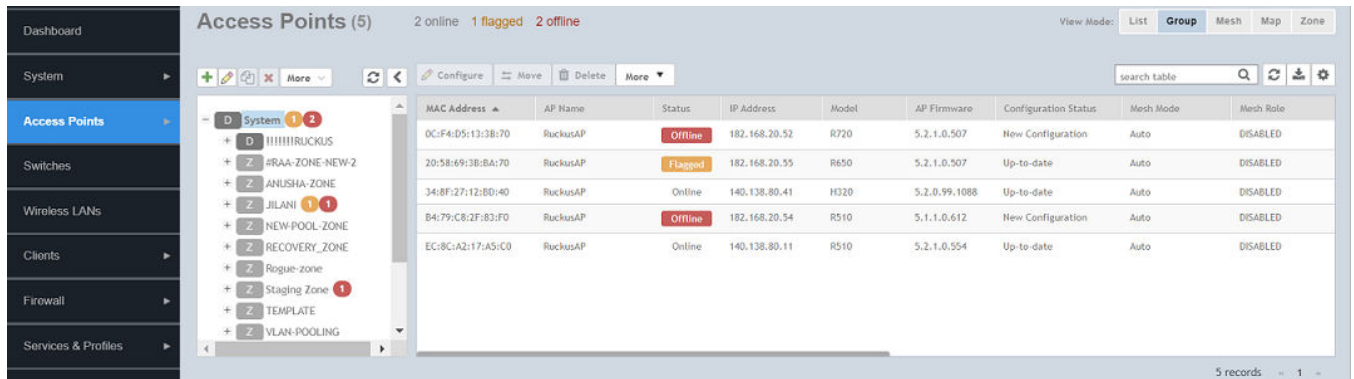
Creating an AP Group

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.

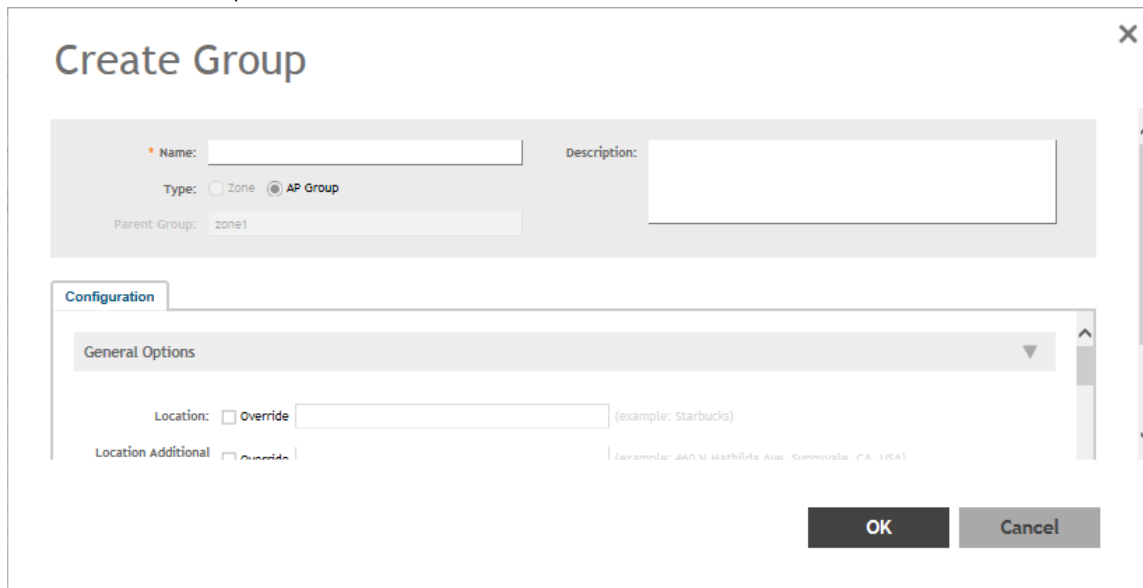
1. From the left pane, select **Access Points**. The below figure appears.

FIGURE 46 Access Point



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

FIGURE 47 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 27 AP Group Details

| Field | Description | Your Action |
|--------------------|--|---|
| Name | Indicates a name for the Zone/AP group. | Enter a name. |
| Description | Indicates a short description. | Enter a brief description |
| Type | Indicates if you are creating a domain, zone or an AP group. | Appears by default. You can also choose the option. |

TABLE 27 AP Group Details (continued)

| Field | Description | Your Action |
|---|--|--|
| Parent Group | Indicates the parent group that this AP group belongs. | Appears by default. |
| Configuration > General Options | | |
| Location | Indicates generic location. | Enter the location. |
| Location Additional Information | Indicates detailed location. | Enter additional location information. |
| GPS Coordinates | Indicates the geographical location. | Enter the following coordinates in meters or floor: <ul style="list-style-type: none"> • Longitude • Latitude • Altitude |
| Configuration > Group Members | | |
| Members | Displays the list of APs that belong to the group. | Select the members from the list and click Move to to assign them to the required group. |
| Access Points | Displays the list of APs that belong to the zone. | Select the Access Points from the list and click Add to Group . |
| Configuration > Radio Options | | |
| Channel Range (2.4G) | 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 Select Channel Range (2.4G) 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. |
| 5.8 Ghz Channels | Provides C-band support for all Outdoor APs and the following Indoor APs: R310, R510, R710. NOTE This feature is available only for countries that support 5.8Ghz channel. For example, UK provides indoor AP—5.8Ghz channel support. | Select the Allow 5.8Ghz channels check box. |
| 5.8 Ghz Channels License | Enables full TX Power Adjustment for C-band channels. NOTE This feature is supported only for UK. | Select the Allow 5.8Ghz channels use full power check box. |
| Channel Range (5G) Indoor | Indicates for what channels want the 5GHz radios of managed indoor APs to operate. | Select the check boxes. |
| Channel Range (5G) Outdoor | Indicates for what channels want the 5GHz radios of managed outdoor APs to operate. | Select the check boxes. |

TABLE 27 AP Group Details (continued)

| Field | Description | Your Action |
|---|--|--|
| Radio Options b/g/n (2.4 GHz) | Indicates the radio option 2.4 GHz configurations. | <p>Select the following options:</p> <ul style="list-style-type: none"> • Channelization—Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically. • Channel—Select the channel to use for the b/g/n (2.4GHz) radio, or select Auto to set it automatically. • Auto cell sizing— 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. <p style="text-align: center;">NOTE Ensure that Background Scan is enabled.</p> <ul style="list-style-type: none"> • TX Power—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 Full on the 2.4GHz radio • WLAN Group—Specifies to which WLAN group this AP group belongs. |
| Radio Options a/n/ac (5 GHz) | Indicates the radio option 5 GHz configurations. | <p>Select the following options:</p> <ul style="list-style-type: none"> • Channelization—Set the channel width used during transmission to either 20, 40, 80, 80+80, 160 (MHz), or select Auto to set it automatically. • Channel—For Indoor and Outdoor, select the channel to use for the a/n/c (5GHz) radio, or select Auto to set it automatically. • Auto cell sizing— 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. <p style="text-align: center;">NOTE Ensure that Background Scan is enabled.</p> <ul style="list-style-type: none"> • TX Power—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 Full on the 5GHz radio. • WLAN Group—Specify to which WLAN group this AP group belongs. |
| Configuration > AP GRE Tunnel Options | | |
| Ruckus GRE Forwarding Broadcast | <p>Forwards broadcast traffic from network to tunnel.</p> <p style="text-align: center;">NOTE ARP and DHCP traffic are allowed even if this option disabled</p> | <p>Click Override to enable the Ruckus GRE broadcast forwarding option.</p> <p>Click the Enable Forwarding Broadcast option to forward the broadcast traffic.</p> |
| Configuration > AP SNMP Options | | |

TABLE 27 AP Group Details (continued)

| Field | Description | Your Action |
|---|---|--|
| Override zone configuration | Indicates that the AP Group configuration overrides the zone configuration. | Select the check box. |
| Enable AP SNMP | Indicates if the AP SNMP option is enabled. | Select the check box. |
| SNMPv2 Agent | Indicates SNMPv2 Agent is applied. | <ol style="list-style-type: none"> 1. Click Create and enter Community. 2. Select the required Privilege. If you select Notification enter the Target IP. 3. Click OK. |
| SNMPv3 Agent | Indicates SNMPv3 Agent is applied. | <ol style="list-style-type: none"> 1. Click Create and enter User. 2. Select the required Authentication. 3. Enter the Auth Pass Phrase. 4. Select the Privacy option. 5. Select the required Privilege. If you select Notification select the option Trap or Inform and enter the Target IP and Target Port. 6. Click OK. |
| <p>Configuration > Model Specific Options</p> <p>NOTE Select the Override check box for that setting, and then configure the setting.</p> | | |
| AP Model | Indicate the AP model for which you are configuring. | Select the option. |
| Status LEDs | Disable the status LED on the selected AP model. | Select the option. |
| LLDP | 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"> • Advertise Interval—Enter the duration in seconds. • Hold Time—Enter the duration in seconds. • Enable Management IP TLV—Select the check box. |
| External Antenna (2.4 GHz) | Enables the external 2.4 GHz antenna on the selected AP model. | Select the Enable external antenna check box, and then set the gain value (between 0 and 90dBi) in the box provided. |
| External Antenna (5 GHz) | Enables the external 5 GHz antenna on the selected AP model. | Select the Enable external antenna check box, and then set the gain value (between 0 and 90dBi) in the box provided. |
| Port Settings | Indicates the port settings. | Select the option and choose the required LAN option. |
| PoE out port | Enables PoE out mode. | Select the Enable PoE out ports (specific ZoneFlex AP models only) check box. |




TABLE 27 AP Group Details (continued)

| Field | Description | Your Action |
|--|---|---|
| PoE Operating Mode | <p>Indicates the PoE operating mode of the selected AP model.</p> <p>NOTE You can set the PoE operating mode from the AP Configuration tab on the controller or using the get power-mode CLI command.</p> <ul style="list-style-type: none"> • R710 • R610 • T610 • R720 • R730 • R750 • M510 | <p>Choose the option.</p> <p>NOTE 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> |
| Internal Heater | Enables the heater that is built into the selected AP model | Select the Enable internal heaters (specific AP models only) check box. |
| USB Port | Disables the USB port. USB ports are enabled by default. | Select the Disable USB port check box. |
| Configuration > Cellular Options | | |
| LTE Band Lock | <p>Displays the list of LTE bands (4G/3G) and allows you to lock one or more bands from the list. Once a lock is enabled, the connection will be established only to the specified bands. The LTE band lock function is disabled by default.</p> <p>NOTE The list of bands is only applicable to:</p> <ul style="list-style-type: none"> • Domain • USA • Canada • Japan | <p>Select Override zone configuration to enable and choose the band from the following:</p> <ul style="list-style-type: none"> • Primary Sim • Secondary Sim |
| Configuration > Advanced Options | | |
| Location Based Service | Enables location-based service for the AP group. | <ul style="list-style-type: none"> • Select the Override zone configuration check box. • Select the Enable LBS Service check box. • Select an LBS Server from the drop-down. |
| Hotspot 2.0 Venue Profile | Indicates the hotspot profile that you want to assign to the group. | <p>Select the required option or click Create and update the following details:</p> <ul style="list-style-type: none"> • Enter the Name. • Enter the Description. • Enter the Venue Names. • Select the Venue Category. • Select the Type. • Enter the WLAN Metrics. |

TABLE 27 AP Group Details (continued)

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

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 Specific Options** section.

Complete the following 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** is displayed.
3. Scroll down to the **Model Specific Options** section, and expand the section.
4. In **Model Specific Control**, select the **Override zone config** check box. The settings available for the AP model are displayed.
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 following table are displayed for every AP model.

| Option | Description |
|-----------------------------------|--|
| USB Port | To disable the USB port on the selected AP model, select the Disable USB port check box. USB ports are enabled by default. |
| Status LEDs | To disable the status LED on the selected AP model, select the Disable Status LEDs check box. |
| LLDP | To enable Link Layer Discovery Protocol (LLDP) on the selected AP model, select the Enable Link Layer Discovery Protocol check box. <ul style="list-style-type: none"> • Enter the Advertise Interval duration in seconds. • Enter the Hold Time duration in seconds. • Select the Enable Management IP TLV check box. |
| PoE Operating Mode | 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, such as the USB port and one of the Ethernet ports, are disabled to reduce power consumption. For AP model R640, if 802.3at PoE Operating Mode PoE is selected and the USB Port option is enabled, the second Ethernet port and any devices running on that port will be disabled. |
| PoE out port | To enable the PoE out port on the selected AP model, select the Enable PoE out ports (specific ZoneFlex AP models only) . <p>NOTE If the controller country code is set to United Kingdom, an additional Enable 5.8 GHz Channels option will be available for outdoor 11n and 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> |
| Internal Heater | To enable the heater that is built into the selected AP model, select the Enable internal heaters (specific AP models only) check box. |
| External Antenna (2.4 GHz) | To enable the external 2.4-GHz antenna on the selected AP model, select the Enable external antenna check box, and then set the gain value (between 0 and 90dBi) in the field provided. |
| External Antenna (5 GHz) | To enable the external 5-GHz antenna on the selected AP model, select the Enable external antenna check box, and then set the gain value (between 0 and 90dBi) in the field 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 |
|------------------------|--|
| Enable | 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. |
| Profile | Use this option to select the Ethernet port profile that you want this LAN port to use. Two default Ethernet port profiles exist: Default Trunk Port (selected by default) and Default Access Port . If you created Ethernet port profiles (see Creating an Ethernet Port Profile on page 444), these profiles will also appear on the drop-down list. NOTE If you recently created an Ethernet port profile and it does not appear on the drop-down menu, click Reload on the drop-down menu to refresh the Ethernet port profile list. |
| Overwriter VLAN | Select the Overwriter VLAN check box and enter: <ul style="list-style-type: none"> • Untag ID—Default: 1 • Members—Range: 1 through 4094. |

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 103 for more information.

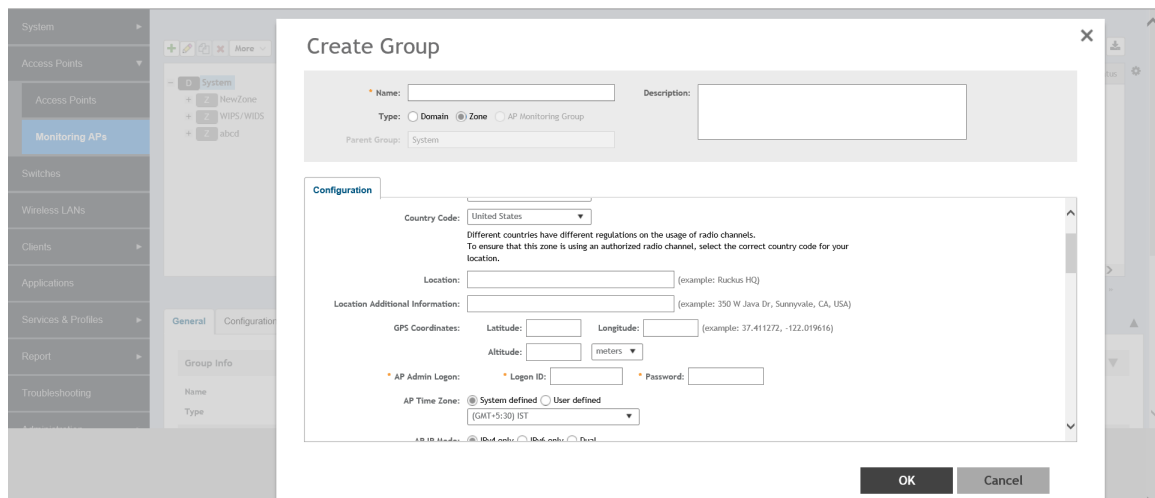
Creating a Monitoring AP Group

As a prerequisite, the monitoring AP must be connected to SZ.

Perform the following procedure to create a monitoring AP group.

1. From the left pane, select **Access Points > Monitoring APs** to create a zone.
2. Select **System** and click **+** to create a zone.

FIGURE 48 Creating a Zone



3. For **Type**, select **Zone**.

4. Select **General Options > AP Admin Logon**, enter the user name and password, and click **OK**.
5. Under **Advanced Options**, enable **Rogue Detection**.
6. For **Rogue Classification Policy**, configure the following options:
 - a) In the **Report RSSI Threshold** field, enter the threshold (the threshold ranges from 0 through 100).
 - b) Enable **Protect the network from malicious rogue access points** and select one of the following options:
 - **Aggressive**
 - **Auto**
 - **Conservative**

NOTE

An AP in a monitoring group cannot be used for prevention services. The monitoring AP will work only in passive mode.

- c) Enable **Radio Jamming Session** and enter the jamming threshold as a percentage.
 - d) Click **OK**.
7. On the **Access Points** page, select the created zone and click **+** to create the AP monitoring group.

FIGURE 49 Creating an AP Monitoring Group

Create Group [X]

Name: Description:

Type: Domain Zone AP Monitoring Group

Parent Group:

Configuration

Model Specific Options [▶]

Advanced Options [▼]

Location Based Service: OFF Override off Select an LBS server [v] [+] [✎]

AP Management VLAN: OFF Override Keep AP's settings VLAN ID

Venue Code: OFF Override

Rogue Classification Policy: ON Override [v] [+] [✎]

ON Override Report RSSI Threshold: (0-100)

ON Override Jamming Threshold: %

Please choose the frequency for scanning

Low Medium High

OK **Cancel**

8. Enter the group name.

9. Under **Advanced Options**, configure the following options:
 - a) Enable **Rogue Classification Policy** and select a rogue classification policy from the list.

NOTE

You can click + to create a rogue classification policy. Refer to [Classifying a Rogue Policy](#) on page 430.

- b) In the **Report RSSI Threshold** field, enter the threshold (the threshold ranges from 0 through 100).
- c) Enable **Radio Jamming Session** and enter the jamming threshold as a percentage.
- d) Select the frequency for scanning to detect rogue devices:
 - **Low** (20 seconds)
 - **Medium** (60 seconds)
 - **High** (120 seconds)

NOTE

You can configure **Jamming Threshold** and **Report RSSI Threshold** for individual APs.

10. To move the AP group to the **Monitoring APs** page, complete the following steps:
 - a) In the **Access Points** page, select the AP from the **Default Zone** and click **Move**.
 - b) In the **Select Destination Management Domain** page, select the AP monitoring group to where the selected AP must be moved and click **OK**.

Viewing Associated Events

- a. From the left pane, select **Monitoring APs**.
- b. Select the zone and the corresponding monitoring AP group and AP, and click **Event**.

The event table lists the rogue APs that are detected by the monitoring AP. Likewise, the rogue APs that are detected by the monitoring AP are listed on the **Rogue Devices** page.

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.

Access Ports

Access ports provide access to the network and can be configured as members of a specific VLAN, thereby separating the traffic on these ports from traffic on other VLANs.

All Access Ports are set to Untag (native) VLAN 1 by default. This means that all Access Ports belong to the native VLAN and are all part of a single broadcast domain. When untagged frames from a client arrive at an AP's Access Port, they are given an 802.1Q VLAN header with 1 as their VLAN ID before being passed onto the wired network.

When VLAN 1 traffic arrives destined for the client, the VLAN tag is removed and it is sent as plain (untagged) 802.11 traffic. When any tagged traffic other than VLAN 1 traffic arrives at the same Access Port, it is dropped rather than forwarded to the client.

To remove ports from the native VLAN and assign them to specific VLANs, select Access Port and enter any valid VLAN ID in the VLAN ID field (valid VLAN IDs are 2-4094).

The following table describes the behavior of incoming and outgoing traffic for Access Ports with VLANs configured.

TABLE 28 Access Ports with VLANs configured

| VLAN Settings | Incoming Traffic (from Client) | Outgoing Traffic (to Client) |
|----------------------------------|--|---|
| Access Port, Untag VLAN 1 | All incoming traffic is native VLAN (VLAN 1). | All outgoing traffic on the port is sent untagged. |
| Access Port, Untag VLAN [2-4094] | All incoming traffic is sent to the VLANs specified. | Only traffic belonging to the specified VLAN is forwarded. All other VLAN traffic is dropped. |

Trunk Ports

Trunk links are required to pass VLAN information between switches. Trunking is a function that must be enabled on both sides of a link.

If two switches are connected together, for example, both switch ports must be configured as trunk ports.

The trunk port is a member of all the VLANs that exist on the AP/switch and carries traffic for all VLANs between switches.

For a trunk port, the VLAN Untag ID field is used to define the native VLAN - 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.

General Ports

General ports are user-specified ports that can have any combination of up to 20 VLAN IDs assigned.

General ports function similarly to Trunk ports, except that where Trunk ports pass all VLAN traffic, General ports pass only the VLAN traffic that is defined by the user.

To configure an AP Ethernet port as a General port, select General Port and enter multiple valid VLAN IDs separated by commas or a range separated by a hyphen.

NOTE

You must also include the Untag VLAN ID in the Members field when defining the VLANs that a General port will pass. For example, if you enter 1 as the Untag VLAN ID and want the port to pass traffic on VLANs 200 and 300, you would enter: 1,200,300.

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 WLAN Services

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 29 System, Domain, Zone, and AP Groups Monitoring Tabs

| Tabs | Description | System | Domain | Zone | AP Groups |
|-----------------------|--|--------|--------|------|-----------|
| General | Displays group information | Yes | Yes | Yes | Yes |
| Configuration | Displays group configuration information. | Yes | Yes | Yes | Yes |
| Health | Displays historical health information. | Yes | Yes | Yes | Yes |
| Traffic | Displays historical traffic information. | Yes | Yes | Yes | Yes |
| Alarm | Displays alarm information. | Yes | Yes | Yes | Yes |
| Event | Displays event information. | Yes | Yes | Yes | Yes |
| Clients | Displays 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. | Yes | Yes | Yes | Yes |
| WLANs | Displays WLAN information. | Yes | Yes | Yes | NA |
| Services | Displays information on the list of services. | Yes | Yes | Yes | NA |
| Administrators | 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 AP Firmware Version of the Zone

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

Complete the following to change the AP firmware version of the zone.

1. For a single zone, from the **Access Point** page, locate a zone for which you want to upgrade the AP firmware version.

NOTE

To upgrade multiple zones, click the **Zone** view mode and select the zones by holding down the Ctrl key and clicking each of the zones.

2. Click **More** and select **Change AP Firmware**. The **Change AP Firmware** dialog box displays the current AP firmware version.
3. Select the firmware version you need. If you upgrade to a new firmware version, a backup configuration file will be created. You can use this backup file to downgrade to the original firmware version.

NOTE

If the multiple zones do not have the same supported firmware version, the dialog box displays the following message: `These Zones do not have same supported AP firmware available for upgrade/downgrade.`

4. Click **Yes**, and a confirmation message is displayed stating that the firmware version was updated successfully.

NOTE

If any zone fails to upgrade, a dialog box displays to download an error CSV list.

5. Click **OK**. You have completed changing the AP firmware version of the zone.

Switch Over Managed APs and External DPs

Switchover helps move APs / external DPs between clusters that are not confined to cluster, which enable cluster redundancy. For normal clusters you can switchover APs regardless of staging zone with firmware version 5.0 or later and external DPs with version 5.1 or later. For a standby cluster in cluster redundancy, APs in Staging Zone can only be moved to another cluster by switchover. You can switch over per AP or APs per Zone. However, you can switch over only per data plane.

Switch Over APs (per Zone)

To switch over APs per zone:

1. From the Access Points page, select the Zone.
2. Click **More** and select **Switch Over Clusters**. The **Switchover Cluster** dialog appears.
3. Choose the Target Cluster:
 - **Predefined Destination:** Available only when "Active-Active" mode cluster redundancy is enabled. Choose the **Cluster Name** of the switchover target from the list of target active clusters. The Control IPv4 List and Control IPv6 List is displayed.
 - **Custom Destination:** Enter the **Control IP/FQDN** of the switchover target cluster.
4. To delete the AP record after triggering a switchover, enable the **Delete selected Access Point after switchover** option.
5. Click **OK**, you have set all APs to disconnect from current cluster then connect to target cluster.

Switch Over APs (per AP)

To switch over per AP:

1. From the Access Points page, navigate the Zone and select the AP from the list.
2. Click **More** and select **Switch Over Clusters** . The **Specify Destination cluster** dialog appears.
3. Enter the **Control IP/FQDN** of the switchover target cluster.
4. Click **OK**, a confirmation dialog appears.
5. Click **OK** to confirm. You have set the AP to disconnect from current cluster then connect to target cluster.

Switch Over Data Planes (per data plane)

You can switch over external data planes.

To switch over external data planes:

1. Go to **System > Cluster**. From the Data Plane section, select the vSZ-D from the list.
2. Click **More** and select **Switch Over Clusters** . The **Switchover Cluster** dialog appears.
3. Choose the Target Cluster:
 - **Predefined Destination:** Available only when "Active-Active" mode cluster redundancy is enabled. Choose the **Cluster Name** of the switchover target from the list of target active clusters. The Control IPv4 List and Control IPv6 List is displayed.
 - **Custom Destination:** Enter the **Control IP/FQDN** of the switchover target cluster .
4. To delete the external data planes record after triggering a switchover, enable the **Delete selected Data Plane after switchover** option.
5. Click **OK**, you have set the external data plane to disconnect from current cluster then connect to target cluster.

Triggering a Preferred Node

You can trigger an AP that belongs to the current zone force go to their preferred node. For this, you must enable Node affinity, which gives AP the priority of preferred nodes.

Follow these steps to trigger a node:

NOTE

You must enable node affinity before triggering nodes.

1. From the Access Points page, locate the zone.
2. Click **More** and select **Trigger Preferred Node**, a confirmation stating that the node has been triggered appears.
3. Click **OK**. You have triggered the preferred node for the AP.

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. This 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 27.

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 30](#).
3. Click **OK**.

NOTE

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

TABLE 30 Access Point Edit Parameters

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

TABLE 30 Access Point Edit Parameters (continued)

| Field | Description | Your Action |
|--------------------------------------|--|--|
| Radio Options b/g/n (2.4 GHz) | Indicates the radio option 2.4 GHz configurations. | <p>Select the following options:</p> <ul style="list-style-type: none"> • Channelization—Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically. • Channel—Select the channel to use for the b/g/n (2.4GHz) radio, or select Auto to set it automatically. • Auto cell sizing— 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 Enable option, disables the TX Power Adjustment configuration. <p style="text-align: center;">NOTE Ensure that Background Scan is enabled.</p> <ul style="list-style-type: none"> • TX Power Adjustment—Select the required option. <p style="text-align: center;">NOTE 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"> • WLAN Group—Select the WLAN group to which this AP belongs. • WLAN Services—Select the check box to enable WLAN services in this radio. |

TABLE 30 Access Point Edit Parameters (continued)

| Field | Description | Your Action |
|---|--|---|
| Radio Options a/n/ac (5 GHz) | Indicates the radio option 5 GHz configurations. | <p>Select the following options:</p> <ul style="list-style-type: none"> • Channelization—Set the channel width used during transmission to either 20, 40, 80 (MHz), or select Auto to set it automatically. • Channel—Select the channel to use for the a/n/c (5GHz) radio, or select Auto to set it automatically. • Auto cell sizing— 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 Enable option, disables the TX Power Adjustment configuration. <p style="text-align: center;">NOTE Ensure that Background Scan is enabled.</p> <ul style="list-style-type: none"> • TX Power Adjustment—Select the required option. <p style="text-align: center;">NOTE 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"> • WLAN Group—Select the WLAN group to which this AP belongs. • WLAN Services—Select the check box to enable WLAN services in this radio. |
| Configuration > AP GRE Tunnel Options | | |
| Ruckus GRE Forwarding Broadcast | <p>Forwards broadcast traffic from network to tunnel.</p> <p style="text-align: center;">NOTE ARP and DHCP traffic are allowed even if this option disabled</p> | <p>Click Override to enable the Ruckus GRE broadcast forwarding option.</p> <p>Click the Enable Forwarding Broadcast option to forward the broadcast traffic.</p> |
| AP Configuration > AP SNMP Options | | |
| Override zone configuration | Allows you to override the existing zone configuration | Select the check box |
| Enable AP SNMP | Enables you to configure SNMP settings. | Select the check box |
| SNMPv2 Agent | Allows you to add users to SNMPv2 Agent. | <ol style="list-style-type: none"> 1. Click Create and enter Community. 2. Select the required Privilege. If you select Notification enter the Target IP. 3. Click OK. |

TABLE 30 Access Point Edit Parameters (continued)

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

TABLE 30 Access Point Edit Parameters (continued)

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

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

1. From the list, select the M510 AP and click **Configure**. The **Edit AP** is displayed.
2. Edit the parameters as explained in the following table.

TABLE 31 Access Point Edit Parameters

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

TABLE 31 Access Point Edit Parameters (continued)

| Field | Description | Your Action |
|---|--|--|
| <p>Radio Options b/g/n (2.4 GHz)</p> | <p>Indicates the 2.4 GHz radio option.</p> | <p>Select the following options:</p> <ul style="list-style-type: none"> • Channelization: Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatically. • Channel: Select the channel to use for the b/g/n (2.4 GHz) radio, or select Auto to set it automatically. • Auto cell sizing: 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 Enable option disables the TX Power Adjustment configuration. • TX Power Adjustment: Select the required option. <p style="text-align: center;">NOTE If you choose Min, the transmit power is set to 0 dBm (1 mW) per chain for 11n APs, and 2 dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the capability of the AP and the regulations of the operating country..</p> <ul style="list-style-type: none"> • WLAN Group: Select the WLAN group to which this AP belongs. • WLAN Services: Select the check box to enable WLAN services in this radio. |

TABLE 31 Access Point Edit Parameters (continued)

| Field | Description | Your Action |
|---|---|--|
| Radio Options a/n/ac (5 GHz) | Indicates the radio option 5 GHz configurations. | <p>Select the following options:</p> <ul style="list-style-type: none"> • Channelization: Set the channel width used during transmission to 20, 40, or 80 (MHz), or select Auto to set it automatically. • Channel: Select the channel to use for the a/n/c (5 GHz) radio, or select Auto to set it automatically. • Auto cell sizing: 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 Enable option disables the TX Power Adjustment configuration. • TX Power Adjustment: Select the required option. <p>NOTE If you choose Min, the transmit power is set to 0 dBm (1 mW) per chain for 11n APs, and 2 dBm per chain for 11ac APs. If you choose Max, the transmit power is set to the maximum allowable value according to the capability of the AP and the regulations of the operation country.</p> <ul style="list-style-type: none"> • WLAN Group: Select the WLAN group to which this AP belongs. • WLAN Services: Select the check box to enable WLAN services in this radio. |
| AP Configuration > AP SNMP Options | | |
| Override zone configuration | Overrides the existing zone configuration | Select the check box. |
| Enable AP SNMP | Configures SNMP settings. | Select the check box. |
| SNMPv2 Agent | Adds users to the SNMPv2 Agent. | <p>Click Create and enter Community.</p> <ol style="list-style-type: none"> Select the required Privilege. If you select Notification, enter the Target IP. Click OK. |
| SNMPv3 Agent | Adds users to the SNMPv3 Agent. | <p>Click Create and enter User.</p> <ol style="list-style-type: none"> Select the required Authentication. Enter the Auth Pass Phrase. Select the Privacy option. Select the required Privilege. If you select Notification, select the option Trap or Inform and enter the Target IP. Click OK. |
| AP Configuration > Model Specific Options | | |
| Model Specific Control | Indicates that the model overrides the AP settings. | Select the check box. |

TABLE 31 Access Point Edit Parameters (continued)

| Field | Description | Your Action |
|--------------------------------|--|---|
| USB Port | Disables the USB port on the selected AP model. | Select the option. USB ports are enabled by default. |
| Status LEDs | Disables the status LED on the selected AP model. | Select the option. |
| LLDP | 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"> • Advertise Interval: Enter the duration in seconds. • Hold Time: Enter the duration in seconds. • Enable Management IP TLV: Select the check box. |
| Cellular Radio Settings | Indicates the settings you can configure for the cellular connection. | Select the following options: <ul style="list-style-type: none"> • APN for Primary SIM: Enter the APN name for the primary SIM. If you choose to keep it blank, the controller sets NULL for APN. If you are not sure about the APN name, enter defaultapn. <p>NOTE For defaultapn, the AP internally searches for an appropriate apn name and sets it in the rpm key through the LTE chipset.</p> • APN for Secondary SIM: Enter the APN name for the secondary SIM. If you choose to keep it blank, the controller sets NULL for APN. If you are not sure about the APN name, then enter defaultapn. <p>NOTE For defaultapn, the AP internally searches for an appropriate apn name and sets it in the rpm key through the LTE chipset.</p> • SIM Card Usage: Select one or both SIM cards to prioritize SIM card usage. • 3G/4G Selection: Select either 3G or 4G internet speed. • Data Roaming: Enable or disable data roaming. • WAN connection: The AP can be connected to the WAN either through the Ethernet or cellular data, and only from the primary SIM card. The following options are available: <ul style="list-style-type: none"> – Ethernet primary with cellular failover (the AP is connected to the Ethernet if LTE fails) – Cellular primary with Ethernet failover (the AP is connected to LTE if the Ethernet connection fails) – Ethernet only – Cellular only |

TABLE 31 Access Point Edit Parameters (continued)

| Field | Description | Your Action |
|---|--|--|
| PoE Operating Mode | Allows you to operate using PoE mode. | Select the option. |
| Port Settings | Indicates the port settings. | Select the option and choose the required LAN option. |
| AP Configuration > Advanced Options | | |
| Network Settings | Determines the network settings. | Select the IPv4 settings from the following options: <ul style="list-style-type: none"> • Static: Enter the IP Address, Network Mask, Gateway, Primary DNS, and Secondary DNS. • Dynamic • Keep the AP's Setting |
| Smart Monitor | Indicates the AP interval check and retry threshold settings. | Select the required check boxes. |
| Syslog Options | Determines if external syslog server settings are applicable. | Select the required check boxes. For the Enable external syslog server option, update the following information: <ul style="list-style-type: none"> • Server Address • Port • Facility for Event • Priority |
| Hotspot 2.0 version Profile | Indicates the hotspot profile that you want to assign to the group. | Select the required option or click Create and update the following details: <ul style="list-style-type: none"> • Enter the Name. • Enter the Description. • Enter the Venue Names. • Select the Venue Category. • Select the Type. • Enter the WLAN Metrics. |
| AP Management VLAN | Indicates the AP management VLAN settings. | Select the check box and choose the option. <p>ATTENTION For standalone APs, set the AP Ethernet port to trunk before changing the AP management VLAN settings.</p> |
| Auto Channel Selection | Indicates auto-channel settings. | Select the check box and choose the option. |
| Client Admission Control | Indicates the load thresholds on the AP at which it will stop accepting new clients. | Select the check boxes and update the following details: <ul style="list-style-type: none"> • Min Client Count • Max Radio Load • Min Client Throughput |

TABLE 31 Access Point Edit Parameters (continued)

| Field | Description | Your Action |
|---------------------------|---|--|
| Protection Mode | Indicates the protection mode settings for the AP. | You can override the protection mode settings at 2.4 GHz, and select one of the following options: <ul style="list-style-type: none"> • None • RTS/CTS (Request to Send/Clear to Send flow control mechanism that allows receiver and the transmitter to alert each other to their state) • CTS Only |
| Venue Code | Indicates the venue code. | You can choose to override this setting and enter the code in the field provided. |
| Recovery SSID | Indicates the recovery SSID. | Select the Enable Recovery SSID Broadcast option for the AP to broadcast the SSID so it can be visible during discovery. |
| Direct Multicast | Indicates the direction in which multicast traffic can be sent. | Configure the AP to multicast traffic from wired clients, wireless clients, and from the network. |
| Swap Configuration | | |
| Add Swap-In AP | Allows swapping of APs. | Select the check box and enter the Swap-in AP MAC details. |

3. Click **OK**.

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.

NOTE

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

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.

Debugging an AP Failure

When an AP fails and reboots, himem logs pertaining to the failure are saved in the AP. These logs can be retrieved from the AP and the controller. From the AP support log, the **Himem Ring Buffer 0** section contains the himem rb0 logs. Log files can be exported to an external server for troubleshooting and debugging issues.

Complete the following steps to retrieve the himem logs from the controller.

1. From the navigation pane select **Access Points**.
The **Access Points** page is displayed.
2. Select an AP from the list.
3. Click **More** and select **Trigger AP binary log**.
4. When the **Trigger AP binary log successfully** dialog box is displayed, click **OK**.
5. From the left pane, select **Diagnostics > Application Logs**.
The **Application Logs** page is displayed.
6. From the **# of Logs** column, select the log corresponding to **AP Diagnostic Information** from the **Application Name** column.
7. Select the ap-dump-xxxxx.tar file to download it
8. Extract the file to get the himem rb0 logs .gz files.

NOTE

The most recent five himem log files can be viewed.

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 32 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 or Default 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.

5. 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.

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 33 Access Point Monitoring Tabs

| Tabs | Description |
|----------------------|---|
| General | Displays group information |
| Configuration | Displays group configuration information. |
| Health | Displays historical health information. |
| Traffic | Displays historical traffic information. |
| Alarm | Displays alarm information. |
| Event | Displays event information. |
| Clients | Displays client information. |
| Pool Stats | Displays DHCP pool data. |
| Stats Counter | Displays AP statistics that can be exported to CSV format. |
| GPS Location | Displays AP Historical GPS location information on a map NOTE For M510 AP, GPS location probe interval must be set to 5. |

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 491
- **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 493
- **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 123
- **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 123
- **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 123
- **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 123
- **Download Support Log** - Downloads support log.
- **Trigger AP Binary Log** - Triggers binary log for the selected AP.

- **Trigger Preferred Node** - Triggers an AP that belongs to the current zone to connect to the preferred node. See [Triggering a Preferred Node](#) on page 108.
- **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 68.
- **Swap** - Swaps current AP to swap-in AP. See, [Editing Swap Configuration](#) on page 124
- **Switch Over Clusters** - Moves APs between clusters. See [Configuring AP Switchover](#) on page 130.
- **Approve** - Approves AP and completes registering. See, [Working with AP Registration Rules](#) on page 67.

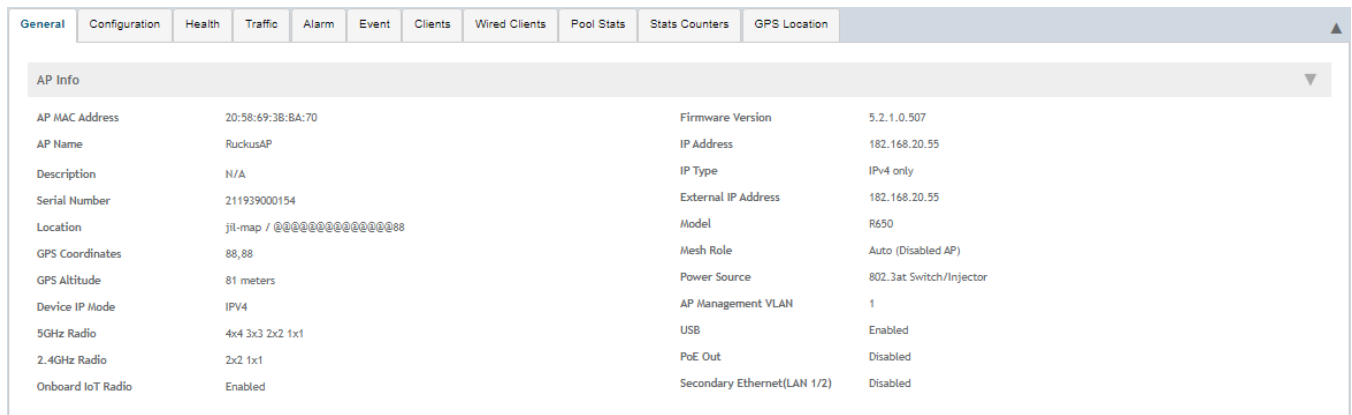
Viewing General AP Information

Complete the following steps to view general AP information.

1. From the **Access Points** page, select an AP.
2. In the **General** tab, scroll to the **AP Info** information.

You can view information specific to the selected AP.

FIGURE 50 General AP Information



| General | | | |
|-------------------|----------------------------|-----------------------------|-------------------------|
| Configuration | Health | Traffic | Alarm |
| Event | Clients | Wired Clients | Pool Stats |
| Stats Counters | GPS Location | | |
| AP Info | | | |
| AP MAC Address | 20:58:69:38:BA:70 | Firmware Version | 5.2.1.0.507 |
| AP Name | RuckusAP | IP Address | 182.168.20.55 |
| Description | N/A | IP Type | IPv4 only |
| Serial Number | 211939000154 | External IP Address | 182.168.20.55 |
| Location | jil-map / @@@@@@@@@@@@@@88 | Model | R650 |
| GPS Coordinates | 88,88 | Mesh Role | Auto (Disabled AP) |
| GPS Altitude | 81 meters | Power Source | 802.3at Switch/Injector |
| Device IP Mode | IPv4 | AP Management VLAN | 1 |
| 5GHz Radio | 4x4 3x3 2x2 1x1 | USB | Enabled |
| 2.4GHz Radio | 2x2 1x1 | PoE Out | Disabled |
| Onboard IoT Radio | Enabled | Secondary Ethernet(LAN 1/2) | Disabled |

Viewing Neighbor APs in a Non-Mesh Zone

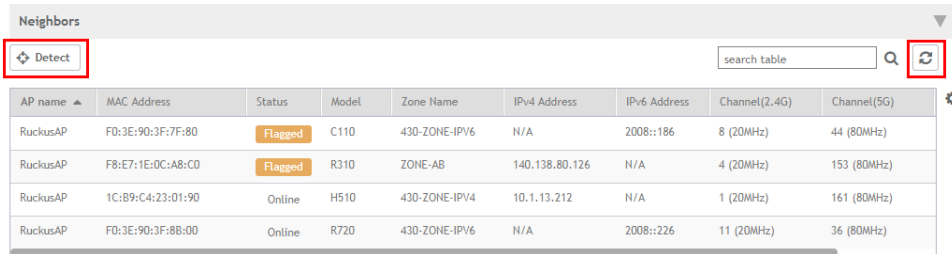
To view neighbor APs in a Non-Mesh zone:

1. From the Access Points page, select an AP from the list which is not assigned to a Staging or Default 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 51 Neighbor APs for a Non-Mesh Zone



| 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 52 Neighbor LLDP APs for a Non-Mesh Zone

| Interface | Time | System Name | System Description | System MAC | Mgmt IP | Capability | Port Description | Port MAC | MDI Power Device Type | Power Class | PD Requested Power |
|-----------|-----------------|-----------------|--------------------|-------------------|------------|-----------------|------------------|----------------------|-----------------------|-------------|--------------------|
| eth1 | 0 day, 00:01:21 | HP 1920G Switch | 1920-48G Switch... | 2c:23:3a:6f:1e:bc | 10.2.0.203 | Bridge, on,R... | GigabitEther... | 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 53 Additional LLDP AP Neighbor Details

```

Show Details
Interface: interface: eth1, via: LLDP, RID: 1, Time: 0 day, 00:01:21
Chassis: ChassisID: 2c:23:3a:6f:1e:bc
          SysName: HP 1920G Switch
          SysDesc: 1920-48G Switch Software Version 5.20.99, Release 1108
          MgmtIP: 10.2.0.203
          Capability: Bridge, on;Router, on
Port: PortID: GigabitEthernet1/0/2
       PortDescr: N/A
       MFS: 9600
       PDM autoneg: supported: yes, enabled: yes
       Adv: N/A
       MAU oper type: 1000BaseTFD - Four-pair Category 5 UTP, full duplex mode
       MDI Power: supported: no, enabled: no, pair control: no
       Device Type: PD
       Power Pairs: signal
       Class: class 0
       Power Type: N/A
       Power Source: N/A
       Power Priority: N/A
       Requested Power Value: N/A
       PDA Allocated Power Value: N/A
    
```

- 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:

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

- 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 the Staging or Non-staging Zone in High-scale platform and Default or Non-default Zone in the Essentials platform. But for a standby cluster in cluster redundancy, APs in Staging or Default 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**.

Running a Speed Test

You can run a speed test to measure the real-life uplink or downlink performance between the controller or wireless device and an AP in a specific environment.

To run a speed test from a wireless client to an AP, the Ruckus SpeedFlex application must be installed on the wireless client. The application can be downloaded from Google Play store for Android devices or the Apple App Store for iPhones. The following fields must be configured before performing a run test:

- Destination Address
- Source Address
- Link
- Protocol
- Test Duration

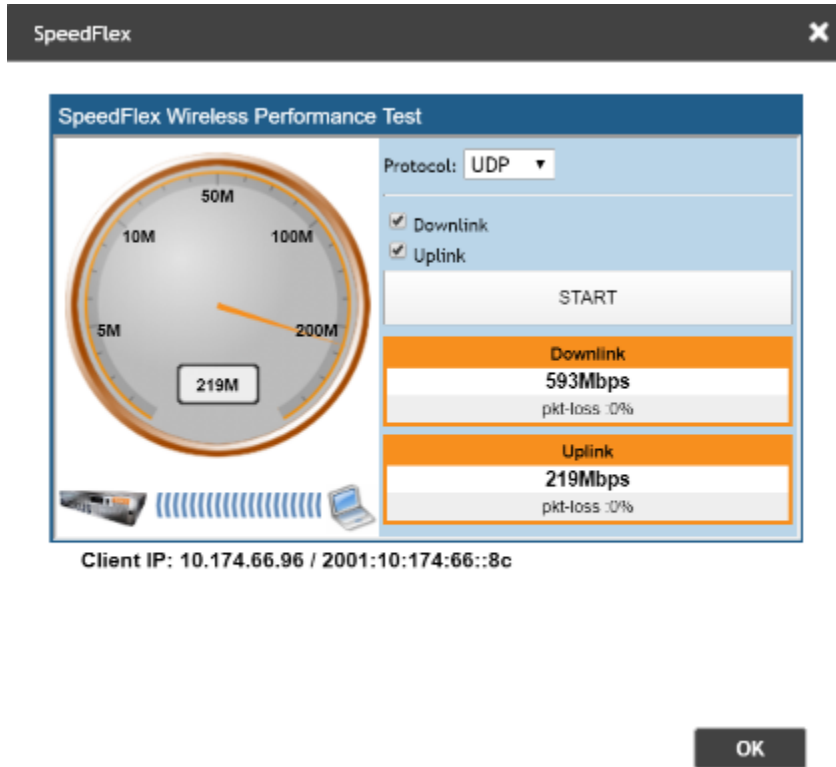
To run a speed test between an AP and the controller, perform the following steps.

1. From the navigation pane, select **Access Points**.
The **Access Points** page is displayed.
2. Select an AP from the list and then select the **Health** tab.
3. Click **Test Speed**.
The **SpeedFlex** page is displayed.

- Click **Start** to test the speed of UDP.

When the test is complete, the downlink and uplink results are displayed, along with packet loss percentages.

FIGURE 54 SpeedFlex Test Result



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 55 Configuring a Ruckus GRE Profile

Create Zone Template

The screenshot shows the 'Create Zone Template' form with the following sections and fields:

- Radio Options**: A section header with a right-pointing arrow.
- AP GRE Tunnel Options**: A section header with a downward-pointing arrow.
- Ruckus GRE Profile**: A field with a dropdown menu set to 'Default Tunnel Profile', a plus icon, and an edit icon. Below it is a 'Select' button with a checked checkbox.
- SoftGRE Profiles**: A table with two columns: 'Name' and 'AAA Affinity'. Below the table is a 'Select' button with a checked checkbox.
- IPsec Profiles**: A table with one column: 'Name'. Below the table is a 'Select' button with a checked checkbox.
- Syslog Options**: A section header with a right-pointing arrow.

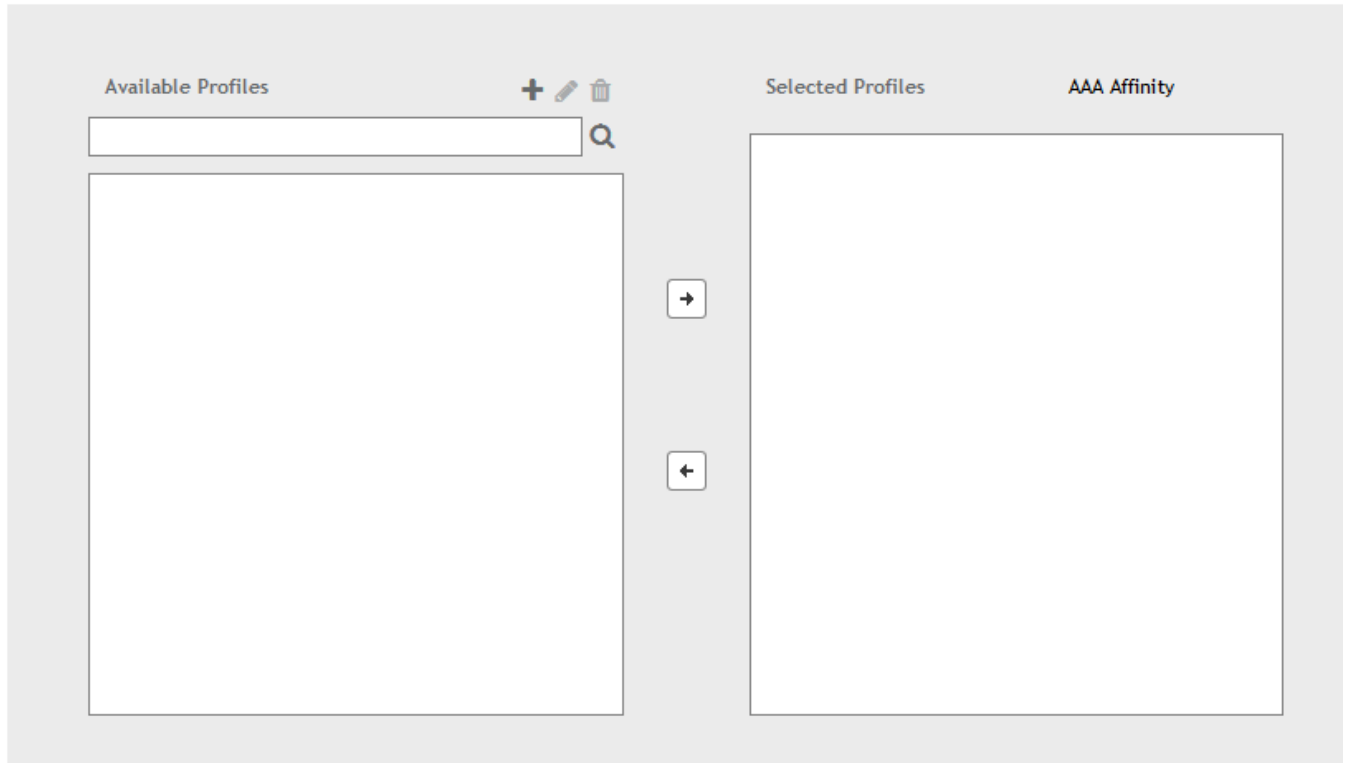
3. Navigate to the **AP GRE Tunnel Options** section.
4. For the **Ruckus GRE Profile** select a profile from the drop-down menu.
Click the + icon to create a new Ruckus GRE profile.

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 56 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.

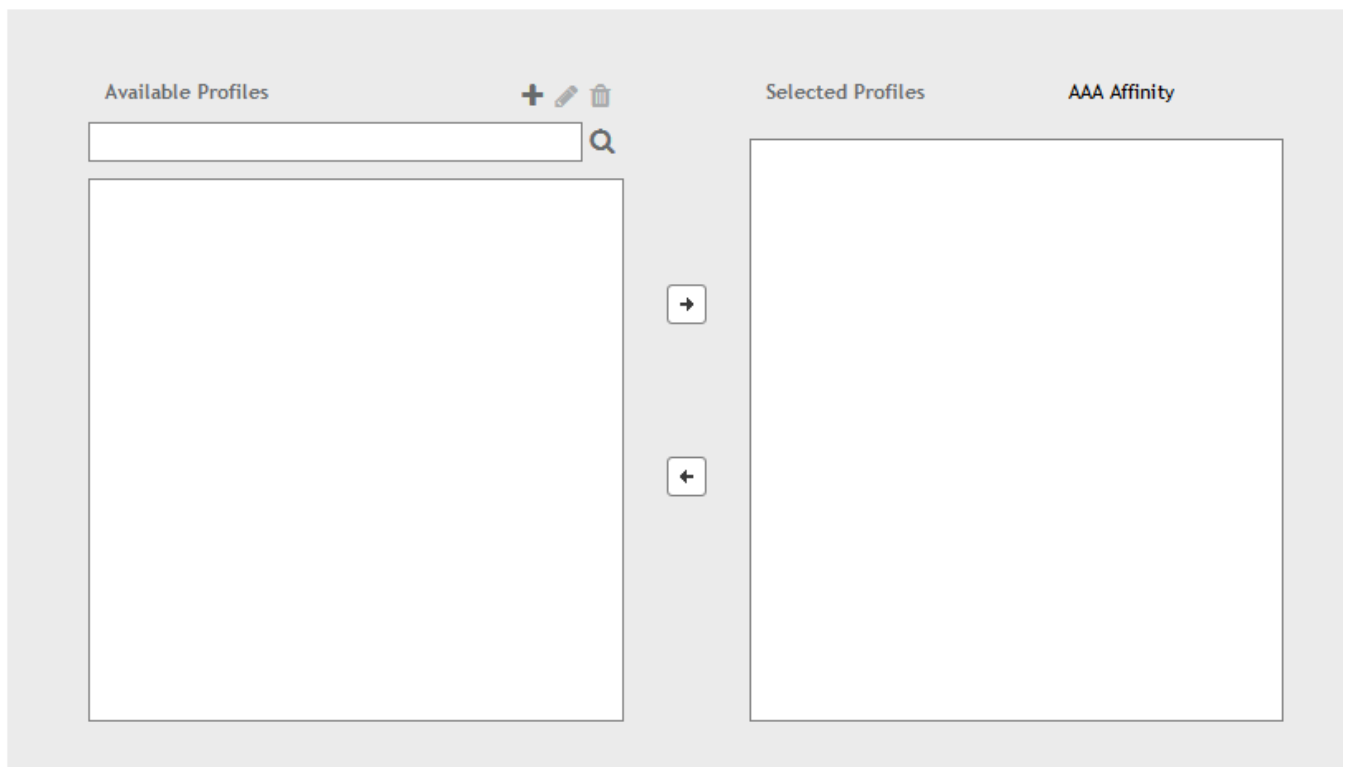
The **Create Group** page appears.

- Under **Type**, select **Zone**.
- Navigate to the **AP GRE Tunnel** section.
- For the **Ruckus GRE Profile** select a profile from the drop-down menu.
Click the **+** icon to create a new Ruckus GRE profile.
- 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 57 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.

- 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 58 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 shot_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'.
Under 'Authentication Options', there are radio buttons for 'Standard usage (For most regular wireless networks)', 'Hotspot (WISPr)', 'Guest Access', 'Web Authentication', 'Hotspot 2.0 Access', and 'Hotspot 2.0 Onboarding'. There is also a 'WeChat' option.
Under 'Encryption Options', there are radio buttons for 'Method: WPA2', 'WPA-Mixed', 'WEP-64 (40 bits)', 'WEP-128 (104 bits)', and 'None'.
Under 'Data Plane Options', there is a checkbox for 'Access Network: Tunnel WLAN traffic' which is checked. Below it are radio buttons for 'Core Network: Bridge' and 'L2oGRE'. At the bottom, there is 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.

Link Aggregation Control Protocol (LACP) support for R720 AP

The R720 AP is a four-stream 802.11ac Wave 2 access point. The AP can transmit to multiple Wave 2 clients in parallel, improving the RF efficiency in addition to faster connectivity and reliable network performance.

NOTE

LACP or Bonding feature is configurable using AP RKS CLI mode though the web user interface configuration option is limited to APs R720, R710 and R610.

NOTE

LACP or Bonding feature option enable or disable is a service-affecting feature configuration. This feature can be used during setup or maintenance mode only when there are no active downlink (DL) or uplink (UL) traffic in progress.

NOTE

To support LACP or Link Aggregation Group (LAG) feature on Ruckus APs, the administrator needs to ensure correct PoE power modes to Bring-Up LAN1 and 2 ports. For example, PoE-at+ for R720, PoE-at for R710, and so on. Refer to the respective AP product guides for details. LACP/LAG UL throughput is limited to around 1 Gbps.

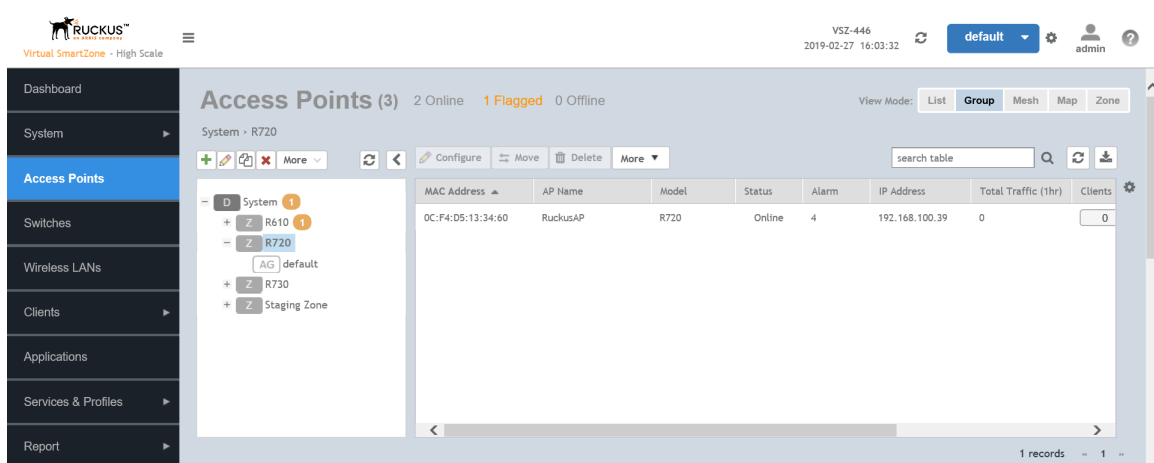
Enabling the LACP Support for a Zone

Perform the following procedure to enable the LACP support for a zone.

1. From the left panes, click **Access Points**.


The **Access Points** page is displayed.

FIGURE 59 Viewing the Access Points



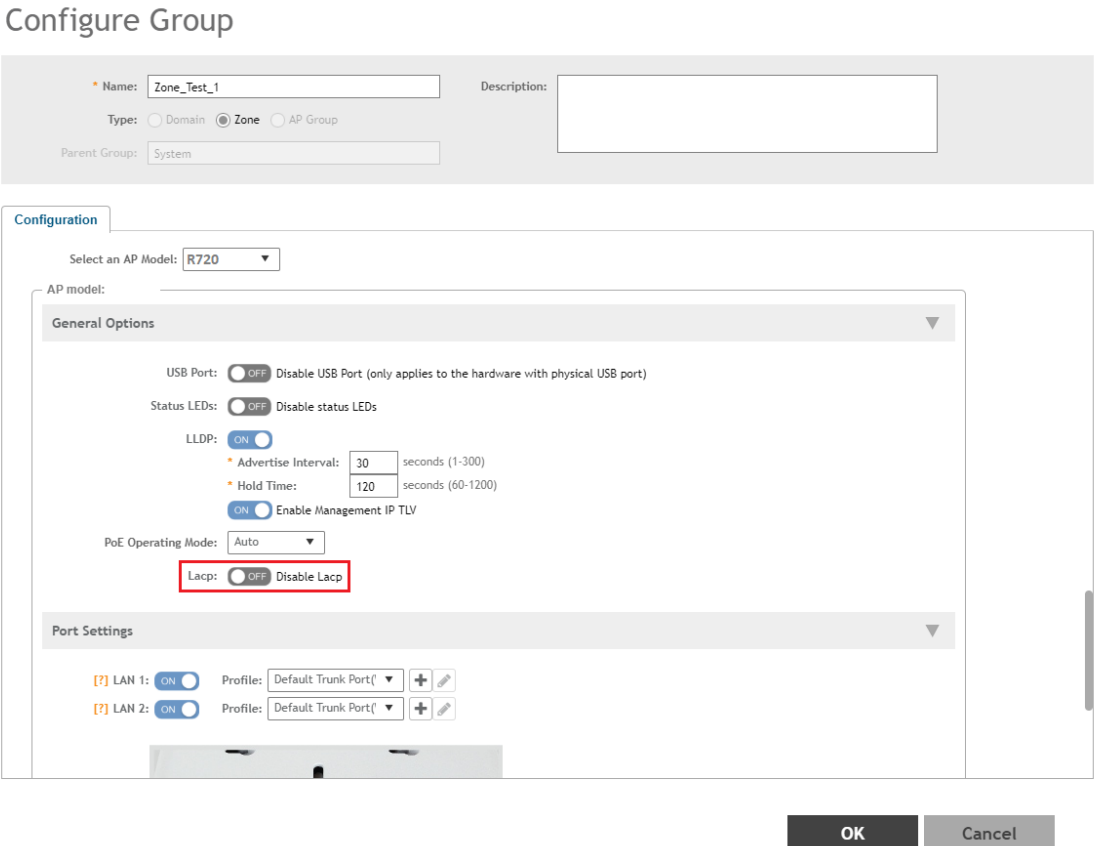
Working With Access Points

Link Aggregation Control Protocol (LACP) support for R720 AP

2. Select a zone and click .

The **Configure Group** page is displayed.

FIGURE 60 Enabling LACP Support for a Zone



The screenshot shows the 'Configure Group' interface. At the top, there is a 'Name' field with 'Zone_Test_1' and a 'Description' field. Below this, the 'Type' is set to 'Zone'. The 'Parent Group' is 'System'. The 'Configuration' section is expanded to show 'General Options'. Under 'General Options', the 'LACP' checkbox is highlighted with a red box and is currently set to 'OFF'. Other options include 'USB Port' (OFF), 'Status LEDs' (OFF), 'LLDP' (ON), 'Advertise Interval' (30 seconds), 'Hold Time' (120 seconds), and 'PoE Operating Mode' (Auto). The 'Port Settings' section shows two LAN ports (LAN 1 and LAN 2) both set to 'ON' with a profile of 'Default Trunk Port()'. At the bottom right, there are 'OK' and 'Cancel' buttons.

3. Enter the zone name.
4. Under **Configuration**, select **R720** from the **Select an AP Model** list.
5. Under **General Options**, enable **LACP**.

NOTE

By default, LACP is disabled.


NOTE

To support the LACP and LAG feature on Ruckus APs, ensure that the correct PoE mode is selected to bring up LAN1,2 ports. For example, PoE-at+ for R720, PoE-at for R710. The LACP and LAG UL throughput is limited to around 1Gbps.

6. Click **OK**.

Enabling LACP Support for an AP Group

Perform the following procedure to enable the LACP support for an AP group.

1. From the left pane, click **Access Points**.
2. Select an AP group from the zone and click .
3. In the **Configure** page, enter the name of the AP group.
4. Under **Configuration**, select **R720** from the **Select an AP Model** list.
5. Under **General Options**, enable **LACP**.

NOTE

By default, LACP is disabled. To enable LACP, both **LACP** and **Override** must be enabled.


NOTE

To support the LACP and LAG feature on Ruckus APs, ensure that the correct PoE mode is selected to bring up LAN1,2 ports. For example, PoE-at+ for R720, PoE-at for R710. The LACP and LAG UL throughput is limited to around 1Gbps.

6. Click **OK**.

Enabling LACP Support for an AP

Perform the following procedure to enable the LACP support for an AP.

1. From the left pane, click **Access Points**.
2. Select an AP group from the zone.
3. Select an AP and click .
4. In the **Edit AP** page, enter the AP name.
5. Under **Configuration**, select **R720** from the **Select an AP Model** list.
6. Under **General Options**, enable **LACP**.

NOTE

By default, LACP is disabled.

NOTE

To support the LACP and LAG feature on Ruckus APs, ensure that the correct PoE mode is selected to bring up LAN1,2 ports. For example, PoE-at+ for R720, PoE-at for R710. The LACP and LAG UL throughput is limited to around 1Gbps.

7. Click **OK**.

NOTE

When you enable or disable LACP, the corresponding status is updated in the **General** tab of the **Access Points** page.

Power Source in AP Configuration

The table below displays the PoE mode as per industry standards.

The currently used APs have AF, AT, AT+ convention modes. The standardization applies when the AP is forced to certain PoE power mode. If the AP is set to AUTO PoE mode, feedback displays PoE mode of the AP is currently configured.

The PoE mode as per the industry standards:

TABLE 34 Industry Standard PoE Modes

| Selection | Power@PSE | Power@AP (100M Cable) |
|-----------------|-----------|-----------------------|
| 802.3af | 15.4W | 12.95W |
| 802.3at | 30W | 25.5W |
| 802.3bt/Class 5 | 45W | 40W→35W |
| 802.3bt/Class 6 | 60W | 51W |
| 802.3bt/Class 7 | 75W | 62W |
| 802.3bt/Class 8 | 90W | 71.3W |

TABLE 35 Non-Standard High Power Solution Summary

| | Customers | Maximum Power Sourced |
|------|---|-----------------------|
| UPoE | Enterprise Switch | 60W |
| PoH | Consumer Customers, for example, audio systems) | 95W |

The SZ-GUI power mode drop-down has the following set of PoE mode configurations:

TABLE 36 PoE Mode Settings

| Name | Value |
|-----------------|-------|
| Auto | 0 |
| 802.3af | 1 |
| 802.3at | 2 |
| 802.3bt/Class 5 | 3 |
| 802.3bt/Class 6 | 4 |
| 802.3bt/Class 7 | 5 |

NOTE

The 802.3bt/Class5 is chosen for AP's with older software which advertise AT+.

NOTE

The below tables are applicable for stand alone APs as well. However, the IOT functionality is not available.

POE tables for different 11 AC AccessPoint

TABLE 37 R710

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT |
|----|----------------|------------|----------|-----------|----------|----------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled |
| AF | N/A | 2/4 | 4/4 | Enabled | Disabled | Disabled |
| AT | 25W | 4/4 | 4/4 | Enabled | Enabled | Enabled |

TABLE 37 R710 (continued)

| | | | | | | |
|--------------------------|-----|-----|-----|---------|---------|---------|
| Injector (Model 480125A) | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled |
|--------------------------|-----|-----|-----|---------|---------|---------|

TABLE 38 R610

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT |
|--------------------------|----------------|------------|----------|-----------|----------|----------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled |
| AF | N/A | 2/4 | 4/4 | Enabled | Disabled | Disabled |
| AT | 24W | 4/4 | 4/4 | Enabled | Enabled | Enabled |
| Injector (Model 480125A) | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled |

TABLE 39 R720

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT | Comments |
|----------------------------------|----------------|------------|----------|-----------|----------|----------|-------------------------------------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | No comments |
| AF | N/A | 1/4 | 1/4 | Enabled | Disabled | Disabled | No comments |
| AT | 25W | 4/4 | 4/4 | Enabled | Disabled | Disabled | No comments |
| 3bt/class5 | 35W | 4/4 | 4/4 | Enabled | Enabled | Enabled | No comments |
| POE Injector (Model 480125A) 60W | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Force to 802.3bt/class5 from SZ GUI |

TABLE 40 M510

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT |
|--------------------------|----------------|------------|----------|-----------|----------|----------|
| DC | N/A | 2/2 | 2/2 | Enabled | Enabled | Enabled |
| AF | N/A | 2/2 | 2/2 | Enabled | Disabled | Disabled |
| AT | 25W | 2/2 | 2/2 | Enabled | Enabled | Enabled |
| Injector (Model 480125A) | N/A | 2/2 | 2/2 | Enabled | Enabled | Enabled |

TABLE 41 T610

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 1Gbps eth | USB | IOT |
|--------------------------|----------------|------------|----------|-----------|----------|----------------|
| DC | N/A | 3/3 | 3/3 | Enabled | Enabled | Enabled (0.5W) |
| AF | N/A | 2/3 | 3/3 | Enabled | Disabled | Disabled |
| AT | 25W | 3/3 | 3/3 | Enabled | Enabled | Enabled (0.5W) |
| Injector (Model 480125A) | N/A | 3/3 | 3/3 | Enabled | Enabled | Enabled (0.5W) |

POE tables for different 11 AX AccessPoint

TABLE 42 R730

| | LLDP | 2.4G tx/rx | 5G tx/rx | 5Gbps eth | 1Gbps eth | USB | IOT | Comments |
|----|------|------------|----------|-----------|-----------|---------|---------|-------------|
| DC | N/A | 4/4 | 8/8 | Enabled | Enabled | Enabled | Enabled | No comments |

Working With Access Points

Power Source in AP Configuration

TABLE 42 R730 (continued)

| | | | | | | | | |
|----------------------------------|-----|-----|-----|---------|----------|----------------|-------------|--|
| AF | N/A | 1/4 | 1/8 | Enabled | Disabled | Disabled | N/ADisabled | Not supported via SZ-GUI, but we can AF mode via rkscli. |
| AT Mode = 0 | 25W | 4/4 | 4/8 | Enabled | Enabled | Enabled (0.5W) | Enabled | By default AT - mode = 0 |
| AT Mode = 1 | 25W | 4/4 | 8/8 | Enabled | Disabled | Disabled | Disabled | Set AT - mode = 1 via Rkscli |
| 802.3bt/class 5 | 35W | 4/4 | 8/8 | Enabled | Enabled | Enabled | Enabled | No comments |
| POE Injector (Model 480125A) 60W | N/A | 4/4 | 4/8 | Enabled | Enabled | Enabled | N/A | Force to 802.3bt/class5 from SZ GUI |

TABLE 43 R850

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 5Gbps eth | 1Gbps eth | USB | IOT | Comment |
|----------------------------------|----------------|------------|----------|-----------|-----------|----------------|----------|--|
| DC | N/A | 4/4 | 8/8 | Enabled | Enabled | Enabled | Enabled | No comments |
| AF | N/A | 1/4 | 1/8 | Enabled | Disabled | Disabled | Disabled | Not supported via SZ-GUI, but we can AF mode via rkscli. |
| AT (Mode=0) | 25W | 4/4 | 4/8 | Enabled | Enabled | Enabled (0.5W) | Enabled | By default at-mode=0 |
| AT (Mode=1) | 25W | 4/4 | 8/8 | Enabled | Disabled | Disabled | Disabled | Set at-mode=1 via Rkscli |
| 802.3bt/class5 | 35W | 4/4 | 8/8 | Enabled | Enabled | Enabled | Enabled | No comments |
| POE Injector (Model 480125A) 60W | N/A | 4/4 | 4/8 | Enabled | Enabled | Enabled | Enabled | Force to 802.3bt/class5 from SZ GUI |

TABLE 44 R750

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 2.5Gbps eth | 1Gbps eth | USB | IOT |
|----------------------------------|----------------|------------|----------|-----------------------|-----------|----------|----------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled |
| AF | N/A | 2/4 | 2/4 | Enabled | Disabled | Disabled | Disabled |
| AT | 25W | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled |
| POE Injector (Model 480125A) 60W | N/A | 4/4 | 4/4 | Enabled (1Gbps speed) | Enabled | Enabled | Enabled |

TABLE 45 T750

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 2.5Gbps eth | 1Gbps eth | USB | IOT | PSE | Comment |
|-------------|----------------|------------|----------|-------------|-----------|----------|----------|----------|------------------------------|
| DC | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Enabled | No comments |
| AF | N/A | 1/4 | 1/4 | Enabled | Disabled | Disabled | Disabled | Disabled | Not supported operation mode |
| AT w/o USB | 25W | 4/4 | 4/4 | Enabled | Enabled | Disabled | Enabled | Disabled | No comments |
| AT with USB | 25W | 2/4 | 4/4 | Enabled | Disabled | Enabled | Enabled | Disabled | Set AT - mode = 1 via Rkscli |

TABLE 45 T750 (continued)

| | | | | | | | | | |
|---|-----|-----|-----|-----------------------------|---------|---------|---------|----------|--------------------------------|
| 802.3bt/ class5 | 35W | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Disabled | No comments |
| 803.3bt/ class6 | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Disabled | 51W by H/W negotiation |
| 802.3bt/ class7 | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Enabled | 62W by H/W negotiation |
| POE 60W Injector (Model 480125A) | N/A | 4/4 | 4/4 | Enabled (1Gbps speed) | Enabled | Enabled | Enabled | Disabled | Force to 802.3bt/ class5 |
| POE 90W Injector | N/A | 4/4 | 4/4 | Enabled | Enabled | Enabled | Enabled | Enabled | Force to 802.3bt/ class7 |

TABLE 46 R650

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 2.5Gbps eth | 1Gbps eth | USB | IOT |
|---------------------------------|----------------|------------|----------|--------------------------|-----------|----------|----------|
| DC | N/A | 2/2 | 4/4 | Enabled | Enabled | Enabled | Enabled |
| AF | N/A | 2/2 | 2/4 | Enabled | Disabled | Disabled | Disabled |
| AT | 25W | 2/2 | 4/4 | Enabled | Enabled | Enabled | Enabled |
| POE Injector (Model 480125A) | N/A | 2/2 | 4/4 | Enabled (1Gbps speed) | Enabled | Enabled | Enabled |

TABLE 47 R550

| | LLDP Power Ask | 2.4G tx/rx | 5G tx/rx | 2.5Gbps eth | 1Gbps eth | USB | IOT |
|---------------------------------|----------------|------------|----------|-------------|-----------|----------|----------|
| DC | N/A | 2/2 | 2/2 | Enabled | Enabled | Enabled | Enabled |
| AF | N/A | 2/2 | 2/2 | Enabled | Disabled | Disabled | Disabled |
| AT | 25W | 2/2 | 2/2 | Enabled | Enabled | Enabled | Enabled |
| POE Injector (Model 480125A) | N/A | 2/2 | 2/2 | Enabled | Enabled | Enabled | Enabled |

Viewing the System Cluster Overview

- Control Planes and Data Planes.....146
- Interface and Routing.....147
- Displaying the Chassis View of Cluster Nodes.....148
- Cluster Redundancy.....148
- Configuring the Control Plane.....157
- Configuring the Data Plane.....161
- Monitoring Cluster Settings.....163
- Creating a DP Zone Affinity Profile.....164
- Enabling Flexi VPN.....167
- Enabling L3 Roaming Criteria for DP.....168
- Powering Cluster Back.....169

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 61 System Cluster Overview - SZ300

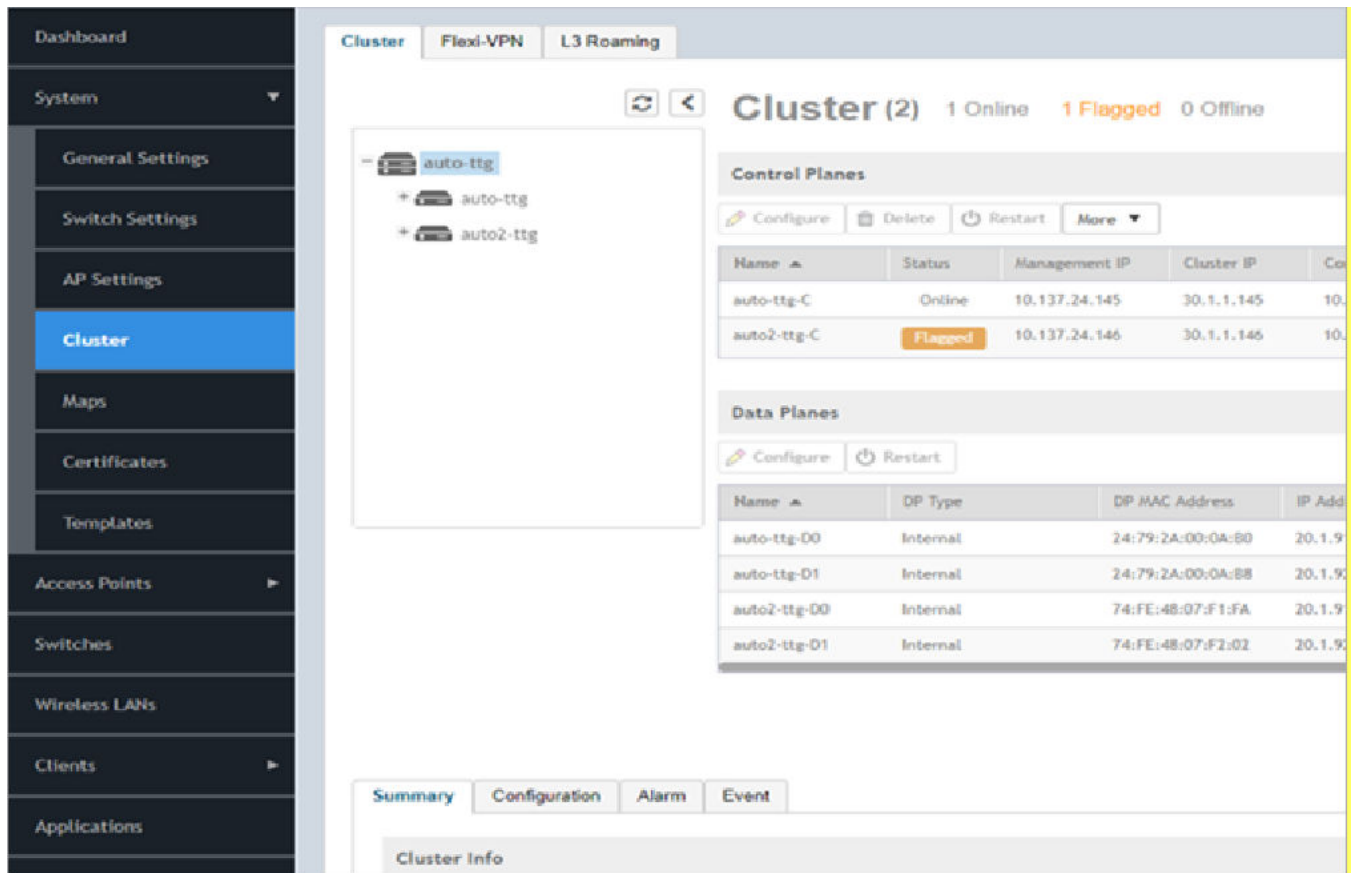
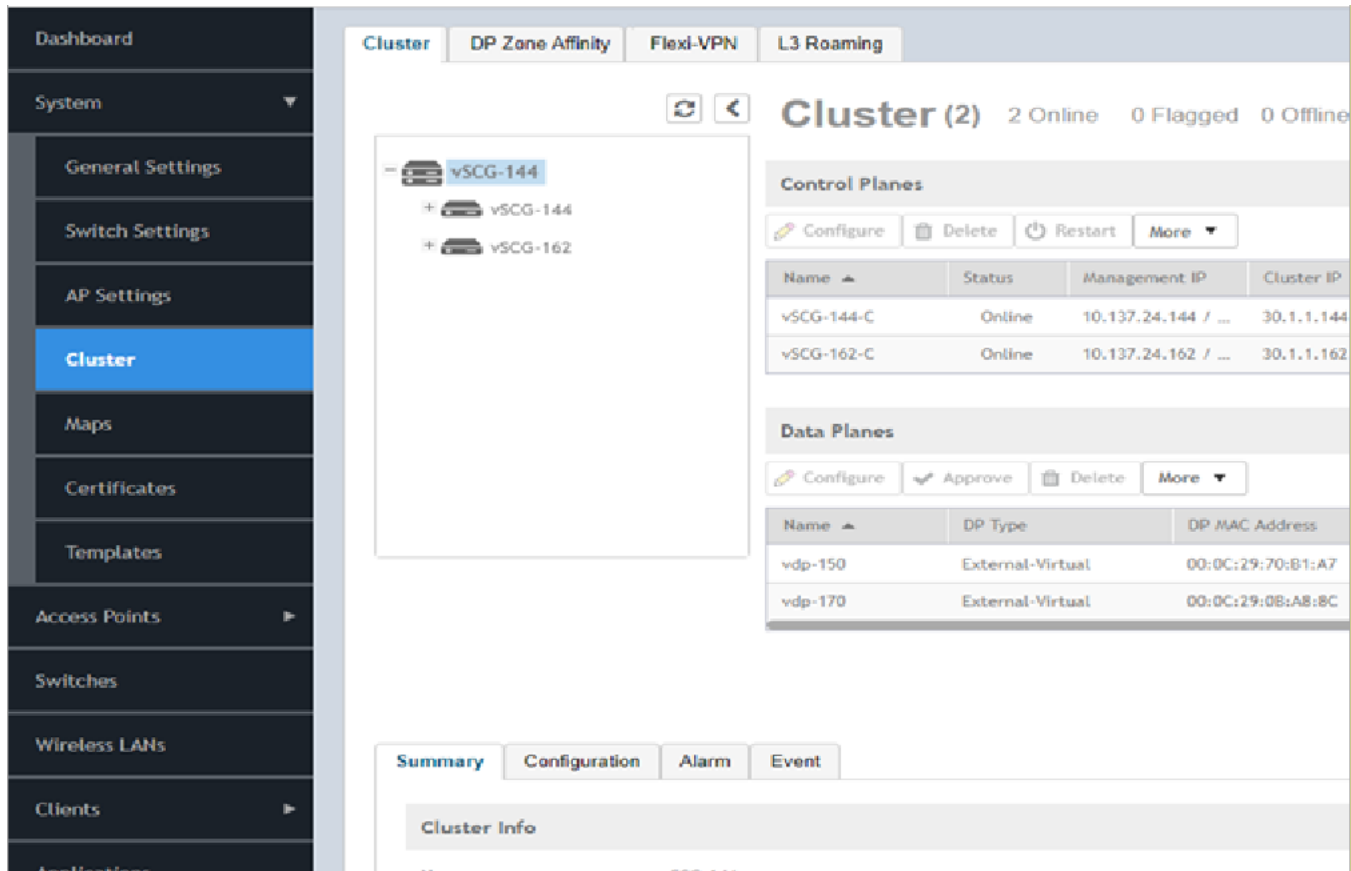


FIGURE 62 System Cluster Overview - vSZ-H



NOTE

The UDI is not accessible on the ESXi hypervisor as the default network driver of vSZ is VMXNET3 and it has a limitation for VLAN interface of VM. To resolve this issue, change the network driver to E1000.

Control Planes and Data Planes

Control planes and data planes are used to control traffic.

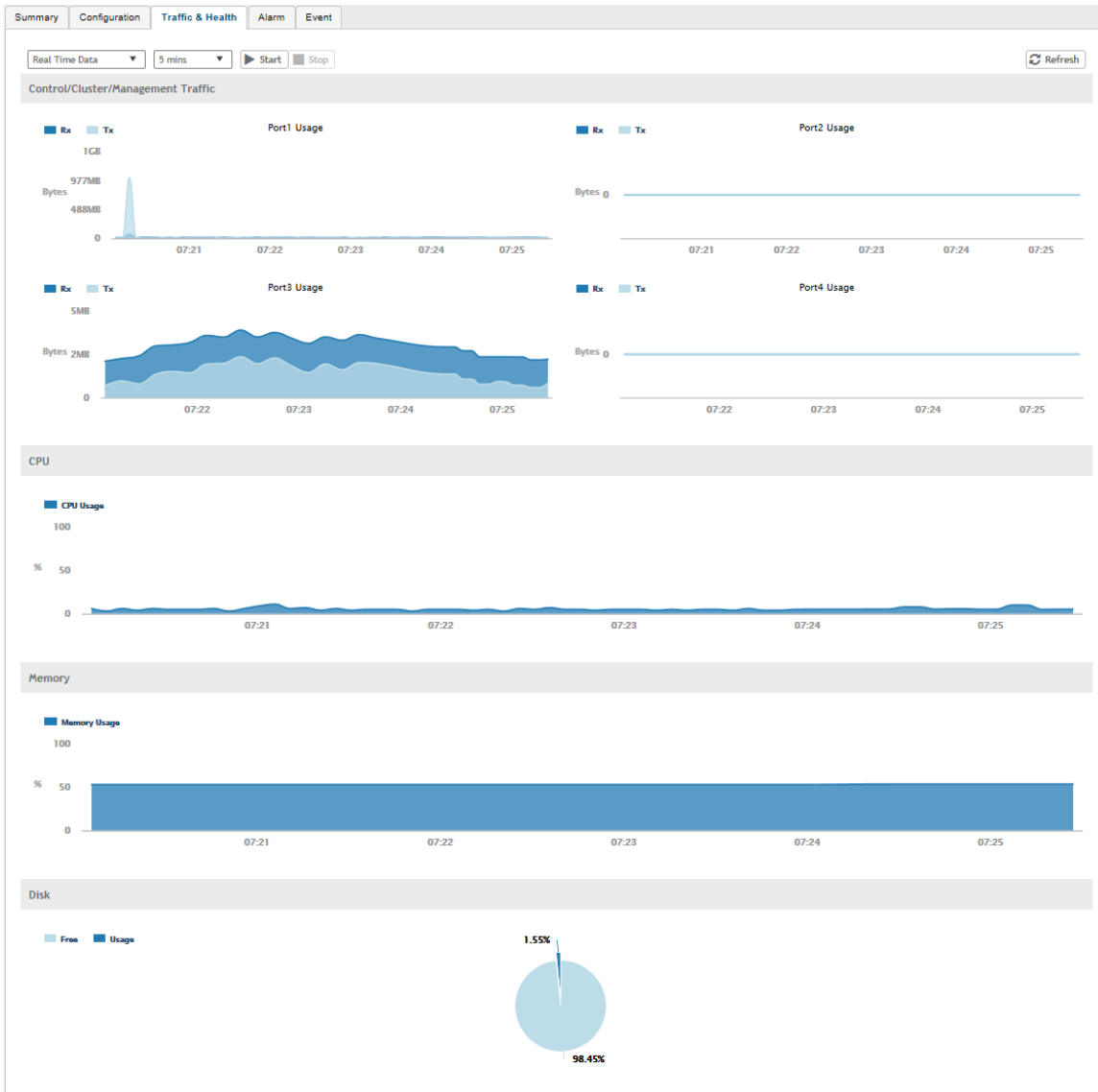
The control plane manages and exchanges routing table information. The control plane packets are processed by the router to update the routing table information. The data plane forwards the traffic along the path according to the logic of the control plane.

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

1. 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 63 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 available in Virtual SmartZone (High-Scale and Essentials) from release 5.1.1.

Viewing the System Cluster Overview

Displaying the Chassis View of Cluster Nodes

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

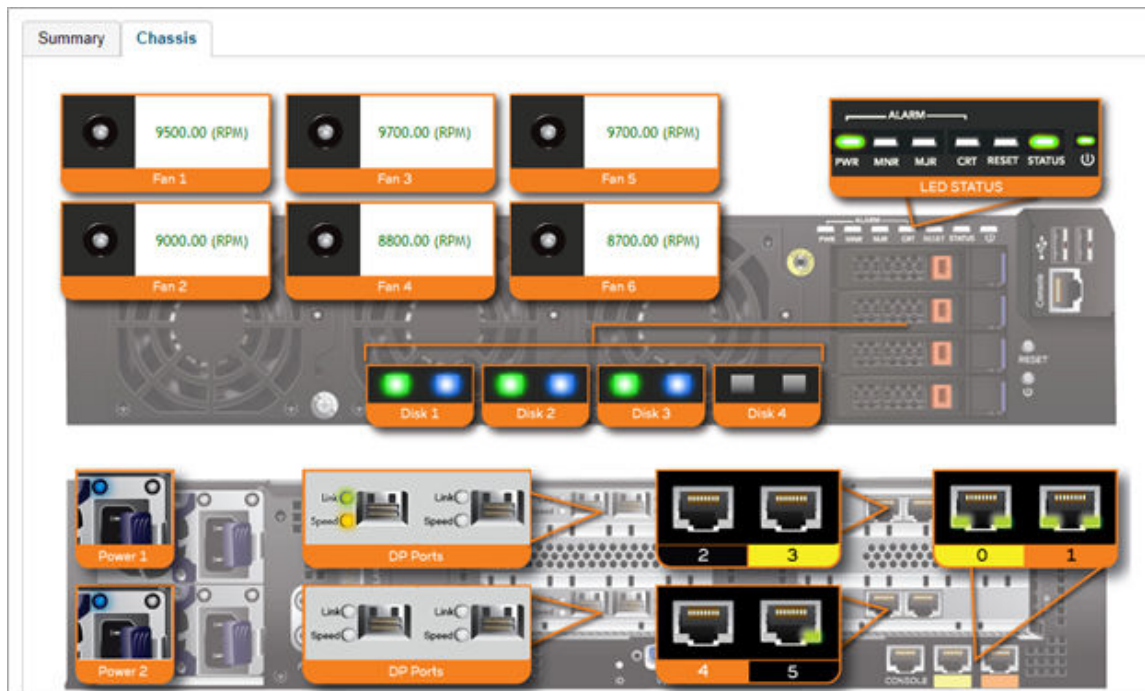
The chassis view provides a graphical representation of the control panel (on the front panel of the controller), including the LEDs.

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 64 Cluster Node Chassis



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

Cluster Redundancy

If you have multiple clusters on the network, you can configure cluster redundancy to enable APs managed by a particular cluster to failover automatically to another cluster if their parent cluster goes out of service or becomes unavailable.

Active-Standby mode

When an active cluster is inaccessible for APs and external DPs (vSZ-D and SZ100-D) for a while, a standby cluster restores the latest configuration of the Out-Of-Service (OOS) active cluster, then take over all external devices (including AP & external DPs) with AP capacity limited by AP HA licenses on Standby cluster and with services license limits coming from the failed Active cluster. When active cluster is back to in-service state, end-user can "rehome" all APs & external DPs back to the active cluster.

Behavior of the standby cluster changes automatically when there is a configuration change in the following deployment types:

- **One-to-one (one active cluster to one standby cluster) deployment**
Standby cluster restores configuration from active cluster every time after the configuration synchronisation is completed. Standby cluster is always in backup mode, ready to receive the APs (Access Points) and external-DPs (Data Plane) from the out-of-service active cluster.
- **Many-to-one (two or three active clusters to a standby cluster) deployment**
The time taken by Standby cluster from detecting Active cluster is out-of-service to it's being ready to serve APs and external-DPs is enhanced.

While upgrading from R3.6.x to R5.2 with geo-redundancy enabled, first upgrade the active cluster and then the standby cluster. Once both clusters are upgraded, from the geo-redundancy page of the active cluster, click **Sync Now** to synchronize the configuration of the active and standby clusters.

Active-Active mode

When there are multiple clusters, one cluster can be the configuration source cluster, and all other active cluster restores its configuration periodically to make sure the configuration between the clusters are synchronized constantly. When the active cluster becomes inaccessible for APs external DPs (vSZ-D and SZ100-D), they failover to the target active cluster with priority

NOTE

Cluster redundancy is supported only on SZ300 and vSZ-H and failover works only for external DPs (vSZ-D and SZ100-D).

A single standby cluster serves as a failover option for one or many distributed active clusters. Different AAA servers can be configured on active and standby clusters.

Precondition

- **Active-Standby mode**

Active-Standby cluster redundancy can be enabled only when matching the following conditions:

- All cluster nodes on both the Active and Standby clusters must be in service.
- System version of both clusters should be the same
- IP mode should be the same
- Both clusters should apply same KSPs on all nodes
- control interface of standby cluster can build connection to which of active cluster

- **Active-Active mode**

Active-Active cluster redundancy can be enabled only when the source active cluster and target active cluster match following conditions:

- All the cluster nodes must be in service.
- System version of both clusters should be the same
- Model (vSZ-H or SZ300) must be the same
- Network interface number should be equal
- IP mode should be the same
- Same KSPs should be applied to all nodes of both clusters
- "Schedule Configuration Sync" can be enabled only in one cluster.

Configuration

- **Active-Standby mode**

Viewing the System Cluster Overview

Cluster Redundancy

An active cluster can assign only one standby cluster and a standby cluster can monitor up to three active clusters.

- **Active-Active mode**

Each cluster in active-active redundancy can configure up-to three target clusters. "Schedule Configuration Sync" can be enabled only in one cluster.

It is highly recommended that you update the configuration from the source cluster till it is eventually synchronized.

Cluster status

- **Active-Standby mode**

Active cluster works as a normal cluster and the Standby cluster is in read-only mode. Only a few configurations can be configured on Standby cluster.

- **Active-Active mode**

All clusters work as normal cluster

Configuration backup

- **Active-Standby mode**

Active cluster can backup its configuration and push it to standby cluster periodically if scheduler task is configured.

- **Active-Active mode**

Source active cluster can backup its configuration and push it to target active cluster periodically if scheduler task is configured

Deployment Models

- **Active-Standby mode**

Starting SZ 5.1, following implementations are allowed for Active-Standby mode:

| | | |
|----------------------|-----------------------|----------------------------------|
| SZ300 (Active) | SZ300 (Standby) | LBO and Tunneled WLANs supported |
| vSZ-H (Active) | vSZ-H (Standby) | LBO Only |
| vSZ-H/vSZ-D (Active) | vSZ-H/vSZ-D (Standby) | LBO and Tunneled WLANs supported |
| SZ300 (Active) | vSZ-H (Standby) | LBO Only |

A standby cluster can be reset as a normal cluster if you set-factory after disabling cluster redundancy from active cluster. Once an Active cluster is set to factory default, it can only be made an Active cluster again either by restoring the entire cluster or by enabling cluster redundancy again. Once a Standby cluster is set to factory default, it can only be made as a Standby cluster again either by restoring the cluster or by clicking "Sync Now" on the active cluster. You can still enable the Active-Standby cluster redundancy again from the active cluster, to set Standby cluster after it has been set to factory default.

- **Active-Active mode**

Cluster in active-active mode must be running on either SZ300 or vSZ-H platforms.

License Management

- **Active-Standby mode**

You must manually sync the license on a Standby Cluster after it has been set as Standby cluster by the active cluster. The Standby cluster restores the latest configuration backup files from the Out-Of-Service Active cluster, and leverages the license with the active cluster profile except for the following type of licenses:

- Permanent AP Licenses
- Default Temporary AP Licenses
- Default Temporary AP License Period

NOTE

- High-availability (HA) AP licenses must be purchased for Standby cluster. The Standby cluster works only with High-availability (HA) AP licenses and do not sync or accept any regular AP licenses from any source.
- Active clusters do not accept High-availability (HA) AP licenses—only regular AP licenses must be used.

- **Active-Active mode**

Licenses in each active cluster are independent.

How Cluster Redundancy Works

The following simplified scenario describes how cluster redundancy works and how managed APs fail over from one controller cluster to another.

- **Active-Standby mode**

This mode offers limited UI configurations as most of them are read-only configurations on Standby cluster.

1. After you enable and configure cluster redundancy on the controller, managed APs will obtain IPs of all nodes in Active cluster as server list, and all IPs of all nodes in Standby cluster as failover list, which is shown in AP as:

```
{  
  "Server List":["IP_A1", "IP_A2", "IP_A3", "IP_A4"],  
  "Failover List":["IP_B1", "IP_B2", "IP_B3", "IP_B4"]  
}
```

2. If Cluster A goes out of service or becomes unavailable, APs managed by Cluster A will attempt to connect to the IP addresses (one node at a time) specified for Cluster A.
3. If managed APs are unable to connect to the IP addresses specified for Cluster A, they will attempt to connect to the IP addresses (one node at a time) specified for Cluster B.
4. If managed APs are able to connect to one of the IP address specified for Cluster B, they fail over to Cluster B. APs will move to the zone it belongs to when failover.

NOTE

The standby cluster to which APs fail over must have sufficient license seats to accommodate the new APs that it will be managing. If Standby cluster has insufficient license seats, some APs may not get HA license and these APs will be rejected by the standby cluster.

- **Active-Active mode**

Configurations can be made using the UI.

1. After you enable and configure cluster redundancy on the controller, the IPs of failover list come from all the target active clusters (up to 3) configured in current active cluster are prioritized per cluster, but the nodes in cluster are randomized.

For example, if you enable the cluster redundancy with active-active mode on current active cluster A and configure following active clusters with priority:

- a. Cluster B
- b. Cluster C
- c. Cluster D

The managed APs will obtain IPs of all nodes in cluster A as server list, and all IPs of all nodes in target active clusters as failover list, which is shown in AP as:

```
{
```

```
"Server List":["IP_A1", "IP_A2", "IP_A3", "IP_A4"],
```

```
"Failover List":["IP_B4", "IP_B2", "IP_B3", "IP_B1"], ["IP_C1", "IP_C4", "IP_C2", "IP_C3"], ["IP_D2", "IP_D1", "IP_D4", "IP_D3"]  
}
```

2. If Cluster A goes out of service or becomes unavailable, APs managed by Cluster A will attempt to connect to the IP addresses (one node at a time) specified for Cluster A.
3. If managed APs are unable to connect to the IP addresses specified for Cluster A, they will attempt to connect to the IP addresses (one node at a time) specified for Cluster B, and will try next Cluster C if APs unable to connect the IP address (one node at a time) specified for Cluster B.
4. If managed APs are unable to connect to the IP addresses specified for Cluster C, they will attempt to connect to the IP addresses (one node at a time) specified for Cluster D, and will start all over again from Cluster A if all IP addresses unable to connect.

Enabling Cluster Redundancy

Cluster redundancy enables APs to failover automatically to another cluster if their parent cluster goes out of service or becomes unavailable.

Before you configure cluster redundancy for Active-Standby mode, consider the following:

- Cluster redundancy is disabled by default.
- Super administrators and system administrators have the capability to configure the cluster redundancy settings.
- The Super admin / System admin, username & password can be different in the active & standby clusters.
- Active and standby cluster can use different passwords for super admin user.
- Up to three Active clusters are supported starting 5.0.
- The standby cluster can serve AP failover from one active cluster at a time.
- Some AAA configurations have secondary server which acts as the backup for the AAA feature. Hence, the AAA configuration feature for the standby cluster in geo-redundancy provides only the primary AAA configuration used on standby.
- Secondary server for non-proxy Radius and Proxy Radius does not support HA standby in 5.1.
- You require a "SUPPORT-HA-EU" license for upgrading a standby cluster.
- SZ support license cannot be used to upgrade the standby cluster.

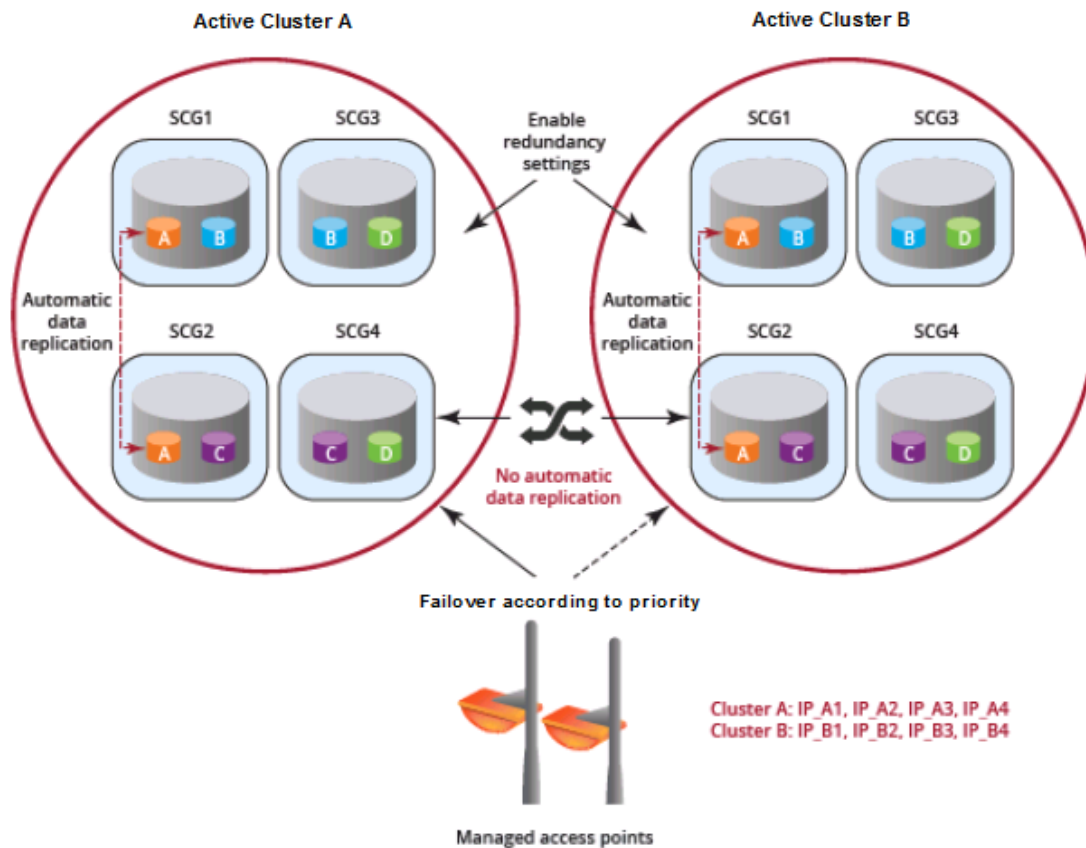
FIGURE 65 Cluster Redundancy for Active-Standby Mode



Before you configure cluster redundancy for Active-Active mode, consider the following:

- Cluster redundancy is disabled by default.
- Super administrators and system administrators have the capability to configure the cluster redundancy settings.
- The Super admin / System admin, username & password can be different in all active clusters.
- Each cluster in active-active redundancy can configure up to three target clusters.
- Allow only one cluster enable configuration scheduler sync.
- Licenses in source active cluster and target active cluster are independent.
- Following features will be disabled in target active cluster after they restore configuration from source active cluster:
 - Configuration FTP export
 - Configuration backup scheduler task
 - Cluster redundancy configuration sync scheduler task
- For adding external devices (AP and external DPs), the devices must be registered to the source active cluster (for which the **Schedule** option must be enabled in **Configuration Sync**) before dispatching these devices to the desired target active cluster.
- Target active clusters receive configuration backup file from the source active cluster and restore it periodically. It is Highly suggested to update the configuration from the source active cluster.

FIGURE 66 Cluster Redundancy for Active-Active Mode



Follow these steps to enable cluster redundancy:

1. Go to **System > Cluster**. The Cluster page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
3. On the right side of the Configuration area, click **Configure**. The Edit Cluster page appears.
4. In the Cluster Redundancy area, enable the **Enable Cluster Redundancy** option.
5. Choose one of the following **Type** to enable cluster redundancy:
 - **Active-Standby**: You can configure up to three active clusters and one standby cluster to support AP and vSZ-D failover to the standby cluster. Configure the following:
 - a. Enter the admin **Password** of the standby cluster.
 - b. Enter at least one **Management IP** address and **Port** of the standby cluster.
 - c. In **Configuration Sync**, the **Schedule** option is enabled by default.
 - d. Select the **Time** duration in HH:MM format from the drop-down to periodically sync the configurations.
 - e. Click **OK**. A confirmation dialog is displayed.
 - **Active-Active**: To support AP and vSZ-D failover from one active cluster to another active cluster, you can configure up to three target clusters to an active cluster.
 - a. Enter the admin **Password** of the active cluster.

- b. Enter at least one **Management IP** address and **Port** number of the active cluster and click **Add**.

NOTE

To prioritize the cluster, select the cluster from the list and **Up** or **Down** to position them. To remove the cluster from the list, select the cluster and click **Delete**.

- c. In **Configuration Sync**, the **Schedule** option is enabled by default.
 - d. Select the **Interval** to sync and restore configuration to target active clusters. If you select **Monthly** or **Weekly** option, select the respect day.
 - e. Select the **Hour** and **Minutes** to periodically sync the configurations.
 - f. Click **OK**. A confirmation dialog is displayed.
6. Click **OK**. You have enabled cluster redundancy.

NOTE

Once the standby cluster IP / port has been configured, the active cluster starts to sync configuration to the standby cluster.

NOTE

You can also edit the Standby Cluster by selecting **Configure** from the **Edit Cluster** page.

Viewing Cluster Configuration

After you have configured cluster redundancy, you can view details of the active and standby clusters.

NOTE

Cluster redundancy is supported only on SZ300 and vSZ-H.

Follow these steps to view the cluster configuration:

1. Go to **System > Cluster**.
The Cluster page appears.
2. Select the cluster, scroll down and click the **Configuration** tab. You can view the cluster details listed in the following table.

TABLE 48 Cluster Details

| Field | Description | Active Cluster | Standby Cluster |
|------------------------------|--|----------------|-----------------|
| Cluster Configuration | | | |
| IP Support | Displays IP support version | Yes | Yes |
| Cluster Redundancy | | | |
| Status | Displays the cluster redundancy status. | Yes | Yes |
| Cluster IP list | Displays cluster name, management IPs, and control IPs of standby cluster. | Yes | No |
| Schedule Configuration Sync | <ul style="list-style-type: none"> • Status—Displays sync status • System Time Zone—Displays the system time zone set • Time—Displays the sync time followed everyday • Last Trigger Time—Displays the date and time the clusters synced last. Applies to both scheduled sync or manually sync • Next Trigger Time—Displays the date and time of the next scheduled sync • Sync Now—Triggers manual configuration sync operation | Yes | No |
| State | Displays the system configuration sync state. | Yes | No |

TABLE 48 Cluster Details (continued)

| Field | Description | Active Cluster | Standby Cluster |
|-----------------|---|----------------|-----------------|
| Progress Status | Displays the progressive status of the system configuration sync. | Yes | No |

Disabling Cluster Redundancy - Active-Standby from the Active Cluster

To disable the cluster redundancy from the active standby cluster when the active cluster is in-service, perform these steps.

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

The **Cluster** page appears.

2. Select the cluster, scroll down and click the **Configuration** tab.
3. On the right side of the **Configuration** area, click **Configure**.

The **Edit Cluster** page appears.

4. In the **Cluster Redundancy** area, click the **Enable Cluster Redundancy** option, if this option is enabled and the button appears blue in color.
5. Click **OK**.

You have disabled cluster redundancy from active cluster when the active cluster is in Service.

If the active cluster is out-of-service, use the Disabling Cluster Redundancy - Active-Standby from the Standby Cluster task.

Disabling Cluster Redundancy - Active-Standby from the Standby Cluster

To disable the cluster redundancy from the standby cluster, perform these steps.

NOTE

Only an out-of-service active cluster can be deleted from the standby cluster.

1. Go to **System > Cluster**.
- The **Cluster** page appears.
2. Select the cluster, scroll down and click the **Configuration** tab.
 3. From the **Active Cluster** list, select the cluster and click **Delete**.

You have disabled cluster redundancy from the standby cluster when the active cluster is out-of-service.

Deleting Cluster Redundancy - Active-Active from a target Active Cluster

To delete a target active cluster form active-active cluster redundancy mode, perform these steps.

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

The **Cluster** page appears.

2. Select the cluster, scroll down and click the **Configuration** tab.
3. On the right side of the **Configuration** area, click **Configure**.

The **Edit Cluster** page appears.

4. In the Cluster Redundancy area, click the **Enable Cluster Redundancy** option, if this option is enabled and the button appears blue in color.

In **Type**, choose **Active-Active**.

- From the Target Active Cluster list, select the cluster and click **Delete**.

You have deleted cluster redundancy form the target active cluster.

Disabling Cluster Redundancy - Active-Active mode from a Current Target Active Cluster

You can disable a current target cluster in an active-active cluster redundancy mode. To do so, perform these steps:

- Go to **System > Cluster**.
The **Cluster** page appears.
- Select the cluster, scroll down and click the **Configuration** tab.
- On the right side of the **Configuration** area, click **Configure**.
The **Edit Cluster** page appears.
- In the Cluster Redundancy area, click the **Enable Cluster Redundancy** option to switch off the option.
- Click **OK**.

You have disabled cluster redundancy form the current target active cluster.

Configuring the Control Plane

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

To configure a control plane:

- Go to **System > Cluster > Control Planes**.
- Select the control plane from the list and click **Configure**. The Edit Control Plane Network Settings form appears.
- Configure the settings as explained in the table below.
- 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 49 Configuring Control Plane

| Field | Description | Your Action |
|-------------------------------|---|---|
| Physical Interfaces | | |
| IPv4-Control Interface | Indicates the management and IP control settings. | Select the IP Mode : <ul style="list-style-type: none"> • Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> – Enter the IP Address. – Enter Subnet Mask. – Enter the Gateway router address. – Enter Control NAT IP address. • DHCP—To automatically obtain an IP address from a DHCP server on the network. <ul style="list-style-type: none"> – Enter Control NAT IP. |

TABLE 49 Configuring Control Plane (continued)

| Field | Description | Your Action |
|----------------------------------|--|---|
| IPv4-Cluster Interface | Indicates the IPv4 cluster interface settings | <p>Select the IP Mode:</p> <ul style="list-style-type: none"> • Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> – Enter the IP Address. – Enter Subnet Mask. – Enter the Gateway router address. • DHCP—To automatically obtain an IP address from a DHCP server on the network. |
| IPv4-Management Interface | Indicates the IPv4 management interface settings | <p>Select the IP Mode:</p> <ul style="list-style-type: none"> • Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> – Enter the IP Address. – Enter Subnet Mask. – Enter the Gateway router address. • DHCP—To automatically obtain an IP address from a DHCP server on the network. |
| IPv6-Control Interface | Indicates the IPv6 control interface settings | <p>Select the IP Mode:</p> <ul style="list-style-type: none"> • Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> – Enter the IPv6 IP Address (global only) with a prefix length (for example, 1234::5678:0:C12/123) is required. Link-local addresses are unsupported. – Enter the IPv6 Gateway 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). • Auto—To automatically obtain an IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network. |
| IPv6-Management Interface | Indicates the IPv6 management interface settings | <p>Select the IP Mode:</p> <ul style="list-style-type: none"> • Static (recommended)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> – Enter the IPv6 IP Address (global only) with a prefix length (for example, 1234::5678:0:C12/123) is required. Link-local addresses are unsupported. – Enter the IPv6 Gateway 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). • Auto—To automatically obtain an IP address from Router Advertisements (RAs) or from a DHCPv6 server on the network. |

TABLE 49 Configuring Control Plane (continued)

| Field | Description | Your Action |
|---|--|---|
| Access & Core Separation | 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 Enable check box. |
| IPv4 Default Gateway & DNS | Indicates the IPv4 gateway that you want to use - Control, Cluster, and Management. NOTE When Access & Core Separation is enabled, the Default Gateway field is hidden. | <ol style="list-style-type: none"> Default Gateway—Choose the Interface for which you want to assign the default gateway setting. Primary DNS Server—Enter the server details. Secondary DNS Server—Enter the server details. |
| IPv6 Default Gateway & DNS | Indicates the IPv6 gateway that you want to use - Control, Cluster, and Management. NOTE When Access & Core Separation is enabled, the Default Gateway field is hidden. | <ol style="list-style-type: none"> Default Gateway—Choose the Interface for which you want to assign the default gateway setting. Primary DNS Server—Enter the server details. Secondary DNS Server—Enter the server details. |
| <p>User Defined Interfaces</p> <p>NOTE 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> | | |
| Name | Indicates the name of the interface. | Enter a name. |
| Physical Interfaces | Indicates the physical interface. | Select Control Interface . |
| Service | Indicates the service. | Select Hotspot , the hotspot must uses the control interface as its physical interface. |
| IP Address | Indicates the IP address that you want to assign to this interface. | Enter the IP address. |
| Subnet Mask | Indicates the subnet mask for the IP address. | Enter the subnet mask. |
| Gateway | Indicates the IP address of the gateway router. | Enter the gateway IP address. |
| VLAN | Indicates the VLAN ID that you want to assign to this interface. | Enter the VLAN ID. |
| Add | Adds the interface settings. | Click Add . |
| Static Routes | | |
| Network Address | Indicates the destination IP address of this route. | Enter the IP address. |
| Subnet Mask | Indicates a subnet mask for the IP address. | Enter the subnet mask. |
| Gateway | Indicates the IP address of the gateway router. | Enter the IP address of the gateway router. |
| Interface | Indicates the physical interface to use for this route. | Select the interface. |
| Metric | Represents the number of routers between the network and the destination. | Enter the number of routers. |
| Add | Adds the static route settings. | Click Add . |

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.**

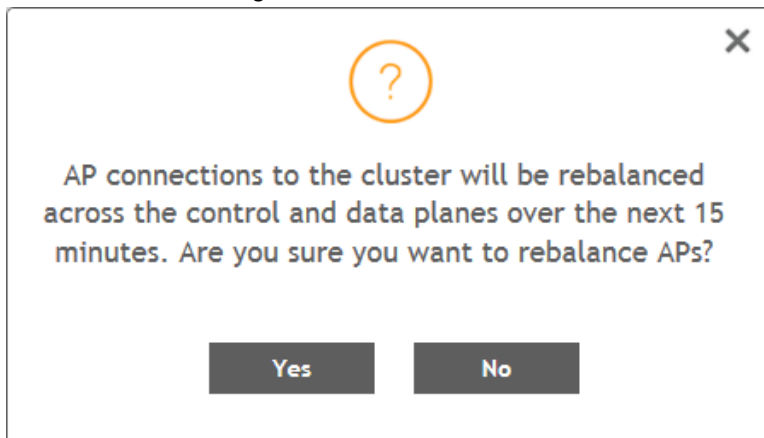
NOTE

- 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 67 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.

Configuring the Data Plane

By default, the controller sends traffic from its data plane from a single interface.

NOTE

This feature is managed only by vSZ-E and vSZ-H controllers.

If your organization's network requires separation of the access and core traffic, configure access and core separation on the controller.

To configure a data plane:

1. Go to **System > Cluster > Data Planes**.
2. Select the data plane from the list and click **Configure**. The Edit Data Plane Network Settings form appears.
3. Configure the settings as explained in [Table 50](#).
4. Click **OK**.

TABLE 50 Configuring Data Plane

| Field | Description | Your Action |
|--|----------------------------------|---|
| Network | | |
| Interface Mode | Indicates the traffic direction. | Choose the option: <ul style="list-style-type: none"> • Single Interface (default)—For the controller to send traffic from its data plane from a single interface. • Access and Core Interface—For the controller to send traffic to the access and core networks separately. <div style="margin-left: 20px;"> <p>NOTE To separate the access and core networks</p> <ul style="list-style-type: none"> – Use static routes, if the data plane is required to connect to IP addresses in the core network (for example, for DHCP relay or L2oGRE termination) and the destination IP addresses are not part of the core subnet. </div> • Keep original configuration—For the controller to keep the original manual Data Plane setup. |
| Network > Primary (Access) Interface | | |

TABLE 50 Configuring Data Plane (continued)

| Field | Description | Your Action |
|--|--|---|
| IP Mode | Indicates the mode of assigning the IP address to this interface. | <p>Select the option:</p> <ul style="list-style-type: none"> • Static (<i>recommended</i>)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> – Enter the IP Address. – Enter the Subnet Mask for the IP address. – Enter the Gateway router address. – Enter the Primary DNS Server IP address. – Enter the Secondary DNS Server IP address. – Enter VLAN ID to tag traffic. – Choose the Data NAT IP/Port Configured option. – Enter Data NAT IP address. – Enter Data NAT Port address. • DHCP—To automatically obtain an IP address from a DHCP server on the network. <ul style="list-style-type: none"> – Enter VLAN ID to tag traffic. – Choose the Data NAT IP/Port Configured option. |
| Network > IPv6 Primary (Access) Interface | | |
| IP Mode | Indicates the mode of assigning the IP address to this interface. | <p>Select the option:</p> <ul style="list-style-type: none"> • Static (<i>recommended</i>)—To manually assign an IP address to this interface manually. <ul style="list-style-type: none"> – Enter the IP Address. – Enter the Gateway router address. – Enter the Primary DNS Server IP address. – Enter the Secondary DNS Server IP address. • Auto—To automatically obtain an IP address from a DHCP server on the network. |
| Network > Secondary (Core) Interface (applicable for Interface Mode: Access and Core Interfaces) | | |
| IP Address | Indicates the IP address of the core network interface. | <p>Enter the IP address.</p> <p>NOTE The secondary/core interface IP address must be configured manually; DHCP is unsupported.</p> |
| Subnet Mask | Indicates the IP address of the subnet mask. | Enter the subnet mask. |
| VLAN | Indicates that the traffic is tagged with a VLAN ID. | <p>Enter the VLAN ID.</p> <p>NOTE If VLANs are configured on both the access and core networks, the VLAN ID that you enter here must be different from the one that you entered for the primary/access interface.</p> <p>NOTE You cannot configure the IP address and VLAN settings for a virtual Data Plane from the Primary (Access) and Secondary (Core) Interface sections. Only vSZ-H supports virtual Data Plane.</p> |
| Disconnect AP when core link down | Indicates that the AP is disconnected secondary core link is down. | Select the check box. |
| Static Routes | | |
| Network Address | Indicates the destination IP address of this route. | Enter the IP address. |
| Subnet Mask | Indicates a subnet mask for the IP address. | Enter the subnet mask. |

TABLE 50 Configuring Data Plane (continued)

| Field | Description | Your Action |
|---|--|---|
| Gateway | Indicates the IP address of the gateway router. | Enter the IP address of the gateway router. |
| Add | Adds the static route settings. | Click Add . |
| CALEA Relay | | |
| Mark this Data Plane as CALEA Relay (This feature is supported only for vSZ-E and vSZ-H controllers) | Indicates that the data plane uses CALEA relay. | Select the check box. |
| DHCP Profile | | |
| DHCP Profile | Indicates the data plane DHCP service profile. | Choose the DHCP service profile from the drop-down. |
| NAT Profile | | |
| NAT Profile | Indicates the data plane NAT service profile. | Choose the NAT service profile from the drop-down. |
| Syslog | | |
| Enable DHCP syslog | Enables syslog to record the DHCP logs. | Select the check box. |
| Enable NAT syslog | Enables syslog to record the NAT logs. | Select the check box. |
| Syslog Server IP | Indicates the IP address of the remote syslog server. | Enter the IP address of the remote syslog server. |
| Syslog Server Port | Indicates the port number of the remote syslog server. | Enter the Port number of the remote syslog server. |

NOTE

You can restart a data plane. To do so, select the data plane from the list and click **Restart**.

NOTE

You can approve or delete a data plane. To do so, select the data plane from the list and click **Approve** or **Delete** respectively. You can also download debug logs or switch over clusters. To do so, select the data plane from the list, click **More** and select **Download** or **Switch Over Clusters** respectively.

NOTE

All configuration changes applicable to vSZ-H are also applicable to SZ100-D.

Monitoring Cluster Settings

You can select the following tabs to view the status of the cluster settings:

- **Summary**—Details such as name, model, serial number, bandwidth, data driver, number of core, data interface details, management interface details, IP details, memory usage, and disk usage.
- **Network Settings**—Details such as control interface, cluster interface, management interface, DNS server, and routes. Appears only for Control Plane.
- **Configuration**—Details such as physical interfaces, user-defined interfaces, and static routes interfaces.
- **Traffic & Health**—Details on historical or real-time data such as CPU usage, memory usage, disk usage, disk IO utilization, interface, port usage for control planes and CPU-only usage, memory usage, and port usage for data planes. For control planes, the CPU usage data additionally provides information on the steal time, which is the percentage of time that a virtual CPU waits for a real CPU while the hypervisor serves another virtual processor. CPU and IO performance are measured at setup stage. The setup flow is blocked if the performance is lower than the threshold.
- **DHCP/NAT**—Details on DHP relay, TTG (DHCP proxy), and NAT statistics.

Viewing the System Cluster Overview

Creating a DP Zone Affinity Profile

- **System**—Details of process name and its health status. Appears only for Data Plane.
- **Alarm**—Details of alarms generated. You can clear alarms or acknowledge alarms that are generated.
- **Event**—Details of events that are generated.
- **DP Zone Affinity**—Details of the data plane, for example, name, profile version, version match information, DP count, and description. Appears only for Data Plane.

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 a DP Zone Affinity Profile

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

NOTE

Creating a DP zone affinity profile is supported only for vSZ-E and vSZ-H platforms.

Complete the following steps to create a DP zone affinity profile.

1. Select **System > Cluster > DP Zone Affinity**.

2. Click **Create**.

The **Create DP Zone Affinity Profile** form is displayed.

3. Enter a **Name** and **Description** for the zone affinity.

4. Click **Add**.

The **Add DP** page is displayed. Profiles with only one or two data planes are listed in it.

5. Select a data plane from the list and click **OK**.

NOTE

- Only one DP can be assigned to one profile.
- While SZ is upgrading from an older version to a newer version, the system validates whether any DP is assigned a duplicate. If a duplicate is encountered, the following warning message is displayed:

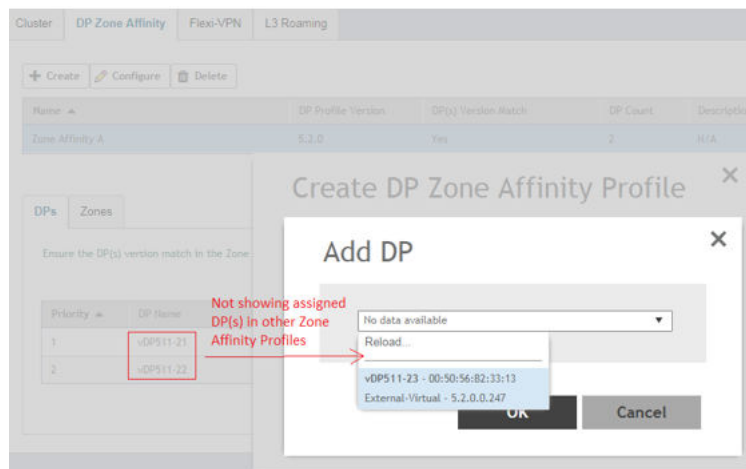
There is an over-assigned DP in the DP Zone Affinity Profile. Please go to the DP Zone Affinity page to edit and make sure only one DP profile is assigned at the same time.

Once the over-assigned DPs are removed, SZ upgrades the system.

- After the configuration that included the over-assigned profiles has been restored, the following message notifies you to correct the configuration:

The overlapping DP Zone Affinity Profile has been detected. There is the over-assigned DP in DP Zone Affinity Profile. Please go to DP Zone Affinity page to edit and make sure the DP only one profile assigned at the same time.

FIGURE 68 Creating a DP Zone Affinity Profile



6. Click **OK**.

NOTE

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

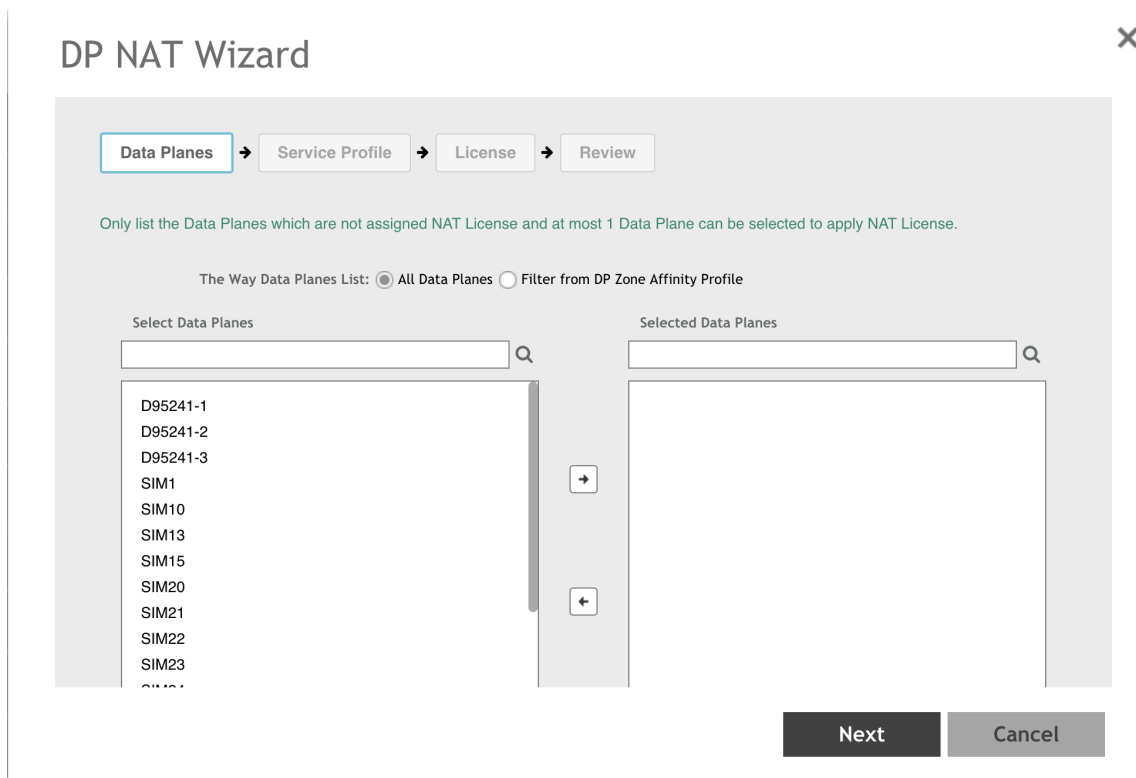
Verifying DP and Profile Version Match

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 different versions. You can click the **DP(s)** tab to verify the version of the DP.

DP NAT License Assignment

1. Select the data plane.
2. Option 1 let the user select filter to apply.
3. The "Select Data Planes" is listing DP(s) filtering by option 1.
4. In "Select Data Planes" area, only list DP(s) which has not assigned NAT license.

FIGURE 69 DP NAT WIZARD



1. Select the NAT service profile.
2. In NAT service profile option, only list the profile which has not assigned to DP.
3. The existed service profile on DP will be replaced after the wizard completed.

Allocate the sufficient license for DP NAT.

FIGURE 70 DP NAT WIZARD License

DP NAT Wizard

Data Planes → Service Profile → License → Review

Setup NAT License Count for Selected Data Plane.

License Usage: Total: 101 / Consumed: 0 / Available: 101

* [?] License Count: 1 x 100000 Sessions/Flows

NAT Sessions/Flows: 100000

Description:

Back Next Cancel

Review all DP NAT configuration before applying.

FIGURE 71 DP NAT WIZARD Review

DP NAT Wizard

Data Planes → Service Profile → License → Review

Data Plane: D95241-3

NAT Profile: NAT-Profile2

License Count: 1

NAT Sessions/Flows: 100000

Back OK Cancel

Enabling Flexi VPN

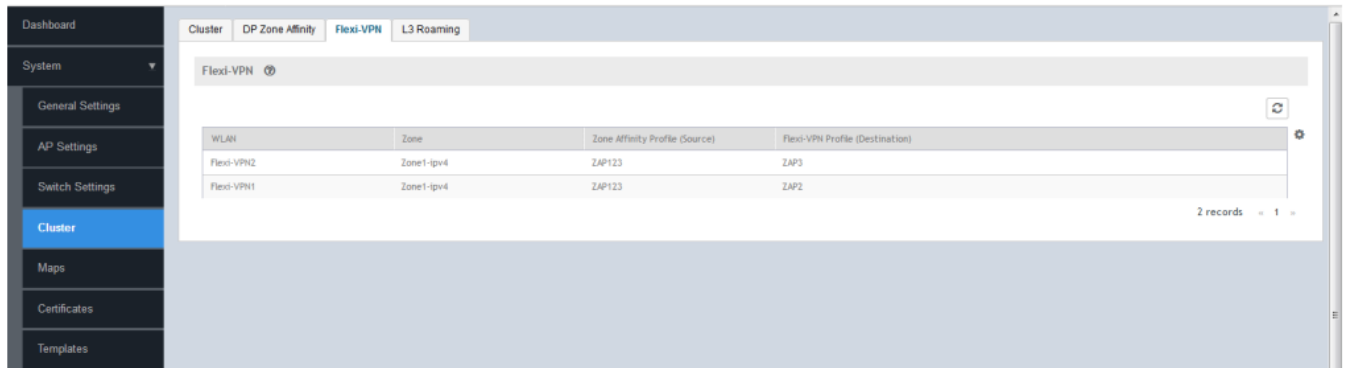
You can enable Flexi-VPN and limit the network resources that a UE can access. Flexi-VPN allows an administrator to customize the network topology, and is thereby able to control the network resources accessible to the end-user. This feature is only supported on vSZ-E and vSZ-H, and is enabled by purchasing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

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

2. Select **Flexi-VPN**.

The **Flexi-VPN** status page is displayed.

FIGURE 72 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

Flexi-VPN is activated when a Flexi-VPN profile is assigned to a WLAN.

NOTE

A maximum of 1024 WLAN IDs can be applied to a Flexi-VPN profile.

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

The following record table indicates that the Flexi-VPN profile is successfully applied to the WLAN:

- 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

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

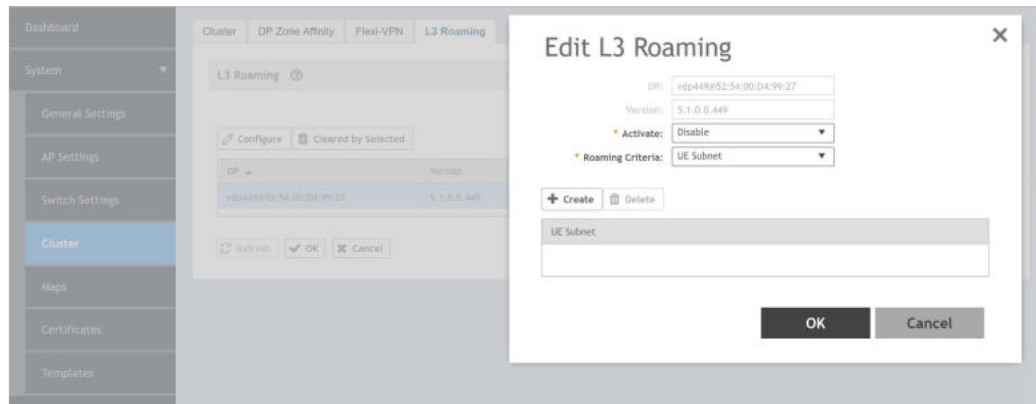
L3 roaming is only supported on vSZ-H and vSZ-E.

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 **L3 Roaming**.
The **Enabling L3 Roaming** page is displayed.

FIGURE 73 Enabling L3 Roaming



3. Click **Configure** to edit the L3 roaming settings.
The **Edit L3 Roaming** page is displayed.
4. From **Activate**, you can enable the feature for the DP by selecting Enable or Disable from the drop-down menu.
5. From the **Roaming Criteria** list, select one of the following options to define the data format to establish connection between DPs: UE Subnet or WLAN VLAN.
6. 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.

Powering Cluster Back

SmartZone cluster nodes may need to be shut down for physical migration/maintenance purpose.

To avoid SmartZone enter crash mode, the cluster needs to form back in time (within Two-and-Half hours). To power up the nodes, perform the following:

1. Power up all nodes at the same time period.
2. All nodes are connected by network.
3. During the setup, it is strongly recommended to configure static IP address to SmartZone interface, if the node's interface IP address settings is configured to DHCP. Make sure the DHCP server assigns a fixed IP address to the interfaces.

Certificates

- Importing New Certificates..... 171
- Assigning Certificates to Services..... 172
- Generating Certificate Signing Request (CSR).....172
- SZ as a Server Certificate..... 173
- SZ as Client Certificate..... 175
- Managing AP Certificates..... 178
- Importing Trusted CA Certificates.....180

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.

Certificates

Assigning Certificates to Services

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.

NOTE

only CRT or PEM format is supported for the CA certificate.

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.

SZ as a Server Certificate

SZ as Server Certificate is used for following purpose

1. AP – SZ Communication.
2. DP – SZ Communication
3. All Portal Redirection (Captive Portal, Web Authentication, WISPr and Guest Access)
4. ZD Style authentication of UE in WISPr

Upload Server Certificate and Map it using 'Certificate to Service Mapping' Tab in Certificates.

Certificates

SZ as a Server Certificate

Import Certificate

Name:

Description:

Server Certificate

Server Certificate: server.cert.pem

Intermediate CA certificate:

Root CA certificate:

Private Key: Upload Using CSR

server.key.pem

No data available

Key Passphrase:

Dashboard

System

General Settings

AP Settings

Switch Settings

Cluster

Maps

Certificates

Certificate to Service Mapping | CSR | SZ as a Server Certificate | SZ

Use this configuration to map various SmartZone services to the certificates already

Service Certificate

Management Web:

AP Portal:

Hotspot (WISPr):

* Ruckus Intra-device Communication:

NOTE

Upload Server Certificate and Map it using 'Certificate to Service Mapping' Tab in Certificates is not a mandatory practice. User should have the knowledge of the usage of third party server certificate and map it to the service.

1. From the application select, **System > Certificates > SZ as a Server Certificate**.
2. Click **Import**.

3. Enter **Name**.
4. Browse **Server Certificate**.
5. Enter **Intermediate CA certificate** - After uploading the Server Certificate.
6. If the certificate is used for Hotspot 2.0 upload the **Root CA certificate**.
7. Click **Validate**.

SZ as Client Certificate

SZ as Client Certificate is used for following purpose:

1. IPSec
 2. RADSec
 3. TLS based AD/LDAP
1. From the application select, **System > Certificates > SZ as Client Certificate**.
 2. Click **Import**.

The screenshot shows the RUCKUS Virtual SmartZone High Scale administrator interface. The left sidebar contains a navigation menu with options like Dashboard, System, General Settings, AP Settings, Switch Settings, Cluster, Maps, Certificates, Templates, Access Points, Switches, Wireless LANs, Clients, Firewall, and Services & Profiles. The main content area shows the 'SZ as Client Certificate' configuration page. A modal dialog titled 'Import CA Certs (Chain)' is open, featuring a 'Name' field with the value 'rootCA_Cert#', a 'Description' field, and two sections for certificate selection. The 'Intermediate CA Certificates' section has a checked checkbox and a list with one entry 'intermediate.cert.p' and 'Browse' and 'Clear' buttons. The 'Root CA Certificate' section has a checked checkbox and a list with one entry 'ca.cert.pem' and 'Browse' and 'Clear' buttons. At the bottom of the dialog are 'Validate', 'OK', and 'Cancel' buttons.

3. Enter **Name**.
4. Upload **Client Certificate**.

Edit Client Certificate: SZ_Clinet_Cert



Name:

Description:

Client Certificate ▼

```
-----BEGIN CERTIFICATE-----
[
[
Version: V3
Subject: CN=ClientCertificate, OU=FTQA Team, O=Commscope Ltd, ST=Karnataka,
C=IN
Signature Algorithm: SHA256withRSA, OID = 1.2.840.113549.1.1.11

Key: Sun RSA public key, 2048 bits
modulus:
23078411678952534998450979686864522029833766184989991636900881339555438
78428231099887832684068536492491037081922528172340873653613614175068597942
7035867566027031850373875740964577782038233975364795952204533928028353460
74638647436116670564521340505732060177937969573434370656191405014437777176
37749076259581636638504845488257063479201320680616351896956503015108852032
91447735136735103288189610195135133396169204312779149898125638511947361974
89457038638012080950846486203990459425597839590592398311963649295790889121
91078217135238157065113109598019393709626625188894455854974358962452176087
2914561478913026786384531
```

Client Certificate:

Private Key:

5. Map in the RAD Sec/ IP Sec Profiles.

The screenshot displays the RUCKUS Virtual SmartZone High Scale administrator interface. On the left is a dark sidebar menu with the following items: Dashboard, System (highlighted), General Settings, AP Settings, Switch Settings, Cluster, Maps, Certificates, Templates, Access Points, Switches, Wireless LANs, Clients, and Firewall. The main content area has a top navigation bar with tabs: About, System IPsec (active), Time, Syslog, Cloud Services, and Northbound Data Streaming. Below the tabs, there is a section for 'Enable IPsec' with a toggle switch set to 'ON'. The configuration fields include: Security Gateway (empty), Subnet (empty), Type (radio buttons for Preshared Key and Certificate, with Certificate selected), Remote ID (empty), Certificate (dropdown menu showing 'SZ_Clinet_Cert'), and OSCP (toggle switch set to 'OFF'). Below this are three sections: 'IKE' with Encryption Algorithm (AES128), Integrity Algorithm (SHA1), and Rekey Time (checked 'Disable'); 'ESP' with Encryption Algorithm (AES128), Integrity Algorithm (SHA1), and Rekey Time (checked 'Disable'); and 'Tunnel State' with a label 'Tunnel State:'.

6. Create Authentication Service

Certificates

Managing AP Certificates

COMMSCOPE
RUCKUS[®] Virtual SmartZone High Scale

Dashboard System Access Points Switches Wireless LANs Clients Firewall Services & Profiles Hotspots & Portals Access Control Wi-Fi Calling Authentication Accounting WIPS Bonjour

Non-Proxy (AP Authenticator) Proxy (SZ Authenticator) Realm Based Proxy EAP-SIM EAP-AKA

Create Authentication Service

* Name:

Friendly Name:

Description:

* Service Protocol: RADIUS Active Directory LDAP

RADIUS Service Options

Encryption: ON TLS

* CN/SAN Identity:

OCSP Validation: OFF * OCSP URL:

Client Certificate:

RFC 5580 Out of Band Location Delivery: OFF Enable for Ruckus AP Only

Primary Server

* IP Address:

* Port:

* Shared Secret:

* Confirm Secret:

Secondary Server

Health Check Policy

7. Click **Validate**.

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 it's 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.

NOTE

The controller does not support the CA certificate with p7b (windows format), only CRT or PEM format is supported. If the Certificates signed by CA chain has more than 5 chain length then you can upload only the Root CA of the certificate.

Configuring Templates

- [Working with Zone Templates.....](#) 181
- [Working with WLAN Templates.....](#) 188

Working with Zone Templates

You can create, configure, and clone zone templates.

To view details about a zone template, select **System > Templates > Zone Templates** and click a zone. The respective contextual tabs are displayed at the bottom of the page.

TABLE 51 Zone Templates: Contextual Tabs

| Tab | Description |
|--------------------------------------|--|
| Zone Configuration | Displays details of the respective zone template. |
| AP Group | Displays details of the respective AP group. You can create or configure an AP group. Refer to <i>Creating an AP Group</i> . |
| WLAN | Displays details of the respective WLAN and WLAN group. You can create or configure a WLAN and a WLAN group. Refer to <i>Working with WLANs and WLAN Groups</i> . |
| Hotspots and Portals | Displays details of the respective hotspots and portals. Refer to <i>Working with Hotspots and Portals</i> . |
| Access Control | Displays details of the respective access control. Refer to <i>Configuring Access Control</i> . |
| Authentication and Accounting | Displays details of the respective authentication and accounting servers. Refer to <i>Authentication and Accounting</i> respectively. |
| Bonjour | Displays details of the respective Bonjour services. Refer to <i>Bonjour</i> . |
| Tunnels & Ports | Displays details of the respective tunnels and ports. Refer to <i>Working with Tunnels and Ports</i> . |
| WIPS | Displays details of the respective WIPS policies. Refer to <i>Classifying Rogue Policies</i> . |
| Radius | Displays details of the respective VSA profiles. You can create or configure a VSA profile. Refer to Creating a Vendor-Specific Attribute Profile on page 473. |

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.

TABLE 52 Zone Template Details

| Field | Description | Your Action |
|------------------------|---|---------------------------|
| General Options | | |
| Zone Name | Indicates a name for the Zone. | Enter a name. |
| Description | Indicates a short description. | Enter a brief description |
| AP Firmware | Indicates the firmware to which it applies. | Select the firmware. |
| Country Code | Indicates the country code to ensure that this zone uses authorized radio channels. | Select the country code. |

TABLE 52 Zone Template Details (continued)

| Field | Description | Your Action |
|--|---|--|
| Location | Indicates generic location. | Enter the location. |
| Location Additional Information | Indicates detailed location. | Enter additional location information. |
| GPS Coordinates | Indicates the geographical location. | Enter the following coordinates in meters or floor: <ul style="list-style-type: none"> • Longitude • Latitude • Altitude |
| AP Admin Logon | Indicates the admin logon credentials. For the Default Zone, the SZ cluster name is used as the default login ID and password. | Enter the Logon ID and Password . |
| Time Zone | Indicates the time zone that applies. | Select the option: <ul style="list-style-type: none"> • System Defined: Select the time zone. • User defined: <ol style="list-style-type: none"> Enter the Time Zone Abbreviation. Choose the GMT Offset time. Select Daylight Saving Time. |
| AP IP Mode | Indicates the IP version that applies. | Select the option: <ul style="list-style-type: none"> • IPv4 only • IPv6 only • Dual |
| Historical Connection Failures | 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. |
| DP Zone Affinity Profile | Specifies the DP affinity profile for the zone. NOTE This option is supported only on vSZ-H. | Select the zone affinity profile from the list. |
| SSH Tunnel Encryption | Specifies the encryption that reduces the load on control of SSH traffic. | Select the required option: <ul style="list-style-type: none"> • AES 128 • AES 256 |
| Cluster Redundancy | Provides cluster redundancy option for the zone. NOTE Cluster redundancy is supported only on SZ300 and vSZ-H. | Select the required option: <ul style="list-style-type: none"> • Zone Enable • Zone Disable |
| Radio Options | | |
| Channel Range | Indicates that you want to override the 2.4GHz channel range that has been configured for the zone. | Select Select Channel Range (2.4G) 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. |
| DFS Channels | Allows ZoneFlex APs to use DFS channels. | Click to enable the option. |

TABLE 52 Zone Template Details (continued)

| Field | Description | Your Action |
|--------------------------------------|--|---|
| Channel 144 | <p>Provides channel 140 and 144 support for 11ac and 11ax APs. Enabling this option supports 20 MHz, 40 MHz, or 80 MHz channel modes. The 80+80 MHz and 160 MHz modes are supported if the AP supports these modes. Disabling this option provides Channel 140 support only to 20 MHz mode.</p> <p>NOTE This option is available for selection only if you enable the DFS Channels option.</p> <p>NOTE This feature is currently supported only in the United States.</p> | Click to enable the option. |
| Channel Range (5G) Indoor | Indicates for what channels want the 5GHz radios to operate. | Select the check boxes. |
| Channel Range (5G) Outdoor | Indicates for what channels want the 5GHz radios to operate. | Select the check boxes. |
| Radio Options b/g/n (2.4 GHz) | Indicates the radio option 2.4 GHz configurations. | <p>Select the following options:</p> <ul style="list-style-type: none"> • Channelization—Set the channel width used during transmission to either 20 or 40 (MHz), or select Auto to set it automatic. • Channel—Select the channel to use for the b/g/n (2.4GHz) radio, or select Auto to set it automatic. • TX Power Adjustment—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 Full/Auto on the 2.4GHz radio. <p>NOTE 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> |

TABLE 52 Zone Template Details (continued)

| Field | Description | Your Action |
|--|---|--|
| Radio Options a/n/ac (5 GHz) | Indicates the radio option 5 GHz configurations. | <p>Select the following options:</p> <ul style="list-style-type: none"> • Channelization—Set the channel width used during transmission to either 20, 40, 80, 80+80 or select Auto. • Channel—For Indoor and Outdoor, select the channel to use for the a/n/c (5GHz) radio, or select Auto. • TX Power Adjustment—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 Full/Auto on the 5GHz radio. <p>NOTE 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> |
| AP GRE Tunnel Options | | |
| Ruckus GRE Profile | Indicates the GRE tunnel profile. | Choose the GRE tunnel profile from the drop-down. |
| Ruckus GRE Forwarding Broadcast | Forwards the broadcast traffic from network to tunnel. | Click the option to enable forwarding broadcast. |
| Soft GRE Profiles | Indicates the SoftGRE profiles that you want to apply to the zone. | <p>a. Click the Select checkbox, a form is displayed.</p> <p>b. From the Available Profiles, select the profile and click the -> icon to choose it.</p> <p>You can also click the + icon to create a new SoftGRE profile.</p> <p>c. Click OK.</p> |
| IPsec Tunnel Mode | Indicated the tunnel mode for the Ruckus GRE and SoftGRE profile. | <p>Select an option:</p> <ul style="list-style-type: none"> • Disable • SoftGRE • Ruckus GRE |
| IPsec Tunnel Profile | <p>Indicates the tunnel profile for SoftGRE.</p> <p>NOTE Select the same tunnel type for IPsec tunnel profile in WLAN configuration.</p> | Choose the option from the drop-down. |
| Syslog Options | | |

TABLE 52 Zone Template Details (continued)

| Field | Description | Your Action |
|--|--|---|
| Enable external syslog server for Aps | 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 server. If the primary server goes down, the AP send syslog messages to the secondary server as backup: <ul style="list-style-type: none"> • Primary Server Address • Secondary Server Address • Port for the respective servers • Portocol: select between UDP and TCP protocols • Event Facility • Priority • Send Logs: you can choose to send the General Logs, Client Logs or All Logs |
| AP SNMP Options | | |
| Enable AP SNMP | Indicates if the AP SNMP option is enabled. | Select the check box. |
| SNMPv2 Agent | Indicates SNMPv2 Agent is applied. | <ol style="list-style-type: none"> Click Create and enter Community. Select the required Privilege: Read or Write. Click OK. |
| SNMPv3 Agent | Indicates SNMPv3 Agent is applied. | <ol style="list-style-type: none"> Click Create and enter User. Select the required Authentication: <ul style="list-style-type: none"> • None • SHA <ol style="list-style-type: none"> Enter the Auth Pass Phrase Select the Privacy option. For DES and AES options, Enter the Privacy Phrase. • MDS <ol style="list-style-type: none"> Enter the Auth Pass Phrase Select the Privacy option. For DES and AES options, Enter the Privacy Phrase. Select the required Privilege: Read or Write. Click OK. |
| Advanced Options | | |
| Channel Mode | Indicates if location-based service is enabled. | Select the check box and choose the option. |
| Auto Channel Selection | Indicates auto-channel settings. | Select the required check boxes and choose the option. |
| Background Scan | Runs a background scan. | Select the respective check boxes and enter the duration in seconds. |
| Smart Monitor | Indicates AP interval check and retry threshold settings. | Select the check box and enter the duration and threshold. |
| AP Ping Latency Interval | 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. |
| AP Management VLAN | Indicates the AP management VLAN settings. | Choose the option. If you select VLAN ID , enter 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>ATTENTION For standalone APs, set the AP ethernet port to trunk before changing the AP Management VLAN settings.</p> |

TABLE 52 Zone Template Details (continued)

| Field | Description | Your Action |
|------------------------------------|--|---|
| Rogue AP Detection | Indicates rogue AP settings. | Enable the option. |
| Rogue Classification Policy | Indicates the parameters used to classify rogue APs. This option is available only if you enable the Rogue AP Detection option. | <p>Select the options for rogue classification policy:</p> <ul style="list-style-type: none"> • – Enable events and alarms for all rogue devices – Enable events and alarms for malicious rogues only • Report RSSI Threshold - enter the threshold. Range: 0 through 100. • Protect the network from malicious rogue access points - Enable the option and choose one of the following: <ul style="list-style-type: none"> – Aggressive – Auto – Conservative • Radio Jamming Detection - enable the option and enter the Jamming Threshold in percentage. |
| DoS Protection | Indicates settings for blocking a client. | <p>Select the check box and enter the:</p> <ul style="list-style-type: none"> • duration in seconds to Block a client for • number of repeat authentication failures • duration in seconds to be blocked for every repeat authentication failures. |
| Load Balancing | Balances the number of clients across APs. | <p>Select one of the following options and enter the threshold:</p> <ul style="list-style-type: none"> • Based on Client Count • Based on Capacity • Disabled <p>NOTE If Based on Capacity is selected, Band Balancing is disabled.</p> |
| Band Balancing | Balances the bandwidth of the clients. | Select the check box and enter the percentage. |
| Location Based Service | 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. |
| Client Admission Control | <p>Indicates the load thresholds on the AP at which it will stop accepting new clients.</p> <p>NOTE Client admission cannot be enabled when client load balancing or band balancing is enabled.</p> | <p>Select the Enable check box 2.4 GHz Radio or 5GHz Radio and update the following details:</p> <ul style="list-style-type: none"> • Min Client Count • Max Radio Load • Min Client Throughput |
| AP Reboot Timeout | Indicates AP reboot settings. | <p>Choose the required option for:</p> <ul style="list-style-type: none"> • Reboot AP if it cannot reach default gateway after • Reboot AP if it cannot reach the controller after |
| Recovery SSID | Allows you to enable or disable the Recovery(Island) SSID broadcast on the controller. | Enable Recovery SSID Broadcast |

TABLE 52 Zone Template Details (continued)

| Field | Description | Your Action |
|-------------------------|---|---|
| Direct Multicast | 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"> • Multicast Traffic from Wired Client • Multicast Traffic from Wireless Client • Multicast Traffic from Network |

4. Click **OK**.

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.

To view details about a WLAN template, select **System > Templates > WLAN Templates** and click a zone. The respective contextual tabs are displayed at the bottom of the page.

TABLE 53 WLAN Templates: Contextual Tabs

| Tab | Description |
|--------------------------------------|--|
| General | Displays details of the respective WLAN template. |
| WLAN | Displays details of the respective WLAN. You can create or configure a WLAN. Refer to <i>Creating a WLAN Configuration</i> . |
| Hotspots and Portals | Displays details of the respective hotspots and portals. Refer to <i>Working with Hotspots and Portals</i> . |
| Access Control | Displays details of the respective access control. Refer to <i>Configuring Access Control</i> . |
| Authentication and Accounting | Displays details of the respective authentication and accounting servers. Refer to <i>Authentication and Accounting</i> respectively. |
| Tunnels & Ports | Displays details of the respective tunnels and ports. Refer to <i>Working with Tunnels and Ports</i> . |
| Radius | Displays details of the respective VSA profiles. You can create or configure a VSA profile. Refer to Creating a Vendor-Specific Attribute Profile on page 473. |

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 from SmartZone

- ICX-Management Feature Support Matrix..... 191
- Overview of ICX Switch Management..... 193
- ICX Switch Behavior with SmartZone..... 194
- Enabling an ICX Device to Be Managed by SmartZone..... 195
- Configuring the ICX Source Address to Be Used by SmartZone..... 195
- Setting up Switch Registrar Discovery..... 196
- Preparing Stacking Devices to Connect to SmartZone..... 198
- Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch..... 198
- Manually Configuring the SmartZone IP Address on an ICX Switch..... 199
- Displaying the SmartZone Connection Status..... 199
- Disconnecting the Switch Connection with SmartZone..... 200
- Disabling SmartZone Management on the ICX Switch..... 200

ICX-Management Feature Support Matrix

Supported ICX Models

The following ICX switch models that can be managed from SmartZone:

- ICX 7150
- ICX 7250
- ICX 7450
- ICX 7650
- ICX 7750
- ICX 7850

The following table defines ICX and SmartZone release compatibility.

TABLE 54 ICX and SmartZone Release Compatibility Matrix

| | SZ 5.0 ¹ | SZ 5.1 ¹ | SZ 5.1.1 | SZ 5.1.2 | SZ 5.2 | SZ 5.2.1 |
|-------------------|---------------------|---------------------|------------------|----------|--------|----------|
| FastIron 08.0.80 | Yes | Yes | Yes ¹ | No | No | No |
| FastIron 08.0.90a | No | No | Yes | Yes | Yes | Yes |
| FastIron 08.0.91 | No | No | Yes | Yes | Yes | Yes |
| FastIron 08.0.92 | No | No | No | Yes | Yes | Yes |

¹ Does not support ICX configuration.

TABLE 54 ICX and SmartZone Release Compatibility Matrix (continued)

| | SZ 5.0 ¹ | SZ 5.1 ¹ | SZ 5.1.1 | SZ 5.1.2 | SZ 5.2 | SZ 5.2.1 |
|---|---------------------|---------------------|----------|----------|--------|----------|
| FastIron 08.0.95 | No | No | No | No | No | Yes |
| NOTE FastIron 08.0.95 is scheduled for release by the end of August 2020. | | | | | | |

The following table provides details on switch management feature compatibility between ICX and SmartZone releases.

TABLE 55 Switch Management Feature Compatibility Matrix

| Feature | SZ Release | ICX FastIron Release |
|---|-----------------|----------------------|
| Switch Registration | 5.0 and later | 08.0.80 and later |
| Switch Inventory | 5.0 and later | 08.0.80 and later |
| Switch Health and Performance Monitoring | 5.0 and later | 08.0.80 and later |
| Switch Firmware Upgrade | 5.0 and later | 08.0.80 and later |
| Switch Configuration File Backup and Restore | 5.0 and later | 08.0.80 and later |
| Client Troubleshooting: Search by Client MAC Address | 5.1 and later | 08.0.80 and later |
| Remote Ping and Traceroute | 5.1 and later | 08.0.80 and later |
| Switch Custom Events | 5.1 and later | 08.0.80 and later |
| Switch Configuration: Zero-touch Provisioning | 5.1.1 and later | 08.0.90a and later |
| Switch-specific Settings: Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server | 5.1.1 and later | 08.0.90a and later |
| Switch Port Configuration | 5.1.1 and later | 08.0.90a and later |
| Switch AAA Configuration | 5.1.1 and later | 08.0.90a and later |
| Switch Client Visibility | 5.1.2 and later | 08.0.90a and later |
| Manage switches from default group in SZ-100/vSZ-E | 5.1.2 and later | 08.0.90a and later |
| Switch Topology | 5.2 and later | 08.0.92 and later |
| Designate a VLAN as Management VLAN | 5.2.1 and later | 08.0.95 and later |
| Change default VLAN | 5.2.1 and later | 08.0.95 and later |
| Configuring the PoE budget per port on ICX through the Controller GUI with 1W granularity | 5.2.1 and later | 08.0.95 and later |
| Configuring Protected Ports | 5.2.1 and later | 08.0.95 and later |
| Configuring QoS | 5.2.1 and later | 08.0.95 and later |
| Configuring Syslog | 5.2.1 and later | 08.0.95 and later |
| Download syslogs for a selected switch | 5.2.1 and later | 08.0.91 and later |

¹ Does not support ICX configuration.

TABLE 55 Switch Management Feature Compatibility Matrix (continued)

| Feature | SZ Release | ICX FastIron Release |
|------------|-----------------|----------------------|
| Remote CLI | 5.2.1 and later | 08.0.95 and later |

Overview of ICX Switch Management

Beginning with SmartZone release 5.0, the SmartZone administrator can monitor and manage switches and routers in the ICX 7000 series. SmartZone release 5.1.1 introduced the capability to configure switches.

SmartZone ICX-Management supports the following ICX switch activities:

- Registration and authentication
- Switch inventory (for example, model, firmware version, and last backup)
- Health and performance monitoring (for example, status, traffic statistics, errors, and clients) with alarms
- Zero-touch provisioning
- Configuration changes
- Port settings
- Configuration copy
- Configuration file backup and restore
- Firmware upgrade
- Client troubleshooting
- Remote Ping and Traceroute

NOTE

Refer [ICX-Management Feature Support Matrix](#) on page 191 for more details.

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:

- Refer to the [ICX-Management Feature Support Matrix](#) on page 191 for detailed information on software compatibility requirements and feature availability.
- The Smartzone IP address must be reachable by the ICX device through the Management interface or through switch or router interfaces.
- The ICX device must be made aware of the configured SmartZone IP address in one of two ways:
 - Configure the DHCP server to use DHCP option 43.
 - Issue the following command at the global configuration level:

```
ICX(conf)# manager 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 **non-tpm-switch-cert-validate** command is entered on the SmartZone console as shown in the following example.

FIGURE 74 Command Required to Disable Certificate Check

```
SZ# conf
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 platform requirements for supporting ICX devices.

NOTE

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

TABLE 56 Virtual Platform Requirements for Supporting ICX Devices

| Platform | Maximum Number of Switches Per Node | RAM | vCPU | Disk Storage |
|----------|-------------------------------------|-------|------|--------------|
| vSZ-E | 200 | 18 GB | 4 | 100 GB |
| vSZ-H | 2000 | 30 GB | 12 | 300 GB |

The scaling limits in the table apply to switch-only deployments. For a mix of APs and switches, the scaling limits vary accordingly. SmartZone supports a 5-to-1 AP-to-switch ratio.

Example 1: vSZ-E supports up to 1,000 APs on a single node. If 200 APs are currently managed by SmartZone, there is room for 800 more APs or 160 ICX switches (800 divided by 5).

Example 2: vSZ-H supports up to 2,000 ICX switches on a single node. If 500 switches are currently managed, there is room for 1,500 more switches, or 7500 APs (1500 multiplied by 5).

ICX Switch Behavior with SmartZone

NOTE

The full range of ICX-Management capabilities (including configuration support in SmartZone 5.1.1 or later) is available only when ICX devices have been upgraded to FastIron release 08.0.90a or later using a Unified Forwarding Image (UFI). Starting from FastIron release 08.0.90, Ruckus ICX devices support unified images that require custom upgrades from prior releases. Any ICX switch that is running a FastIron release 08.0.80 non-UFI image on the ICX switch must follow a two-step image upgrade process to FastIron 08.0.90a through SmartZone controller image updates. If an ICX switch from the factory has a FastIron 08.0.80 non-UFI image, it must first be upgraded with a FastIron 08.0.90 UFI, followed by a FastIron 08.0.90a UFI to avoid any boot configuration issues. Refer to the *Ruckus FastIron Software Upgrade Guide* for more information.

NOTE

Campus Fabric (SPX) is not compatible with SmartZone. When SPX is enabled using the **spx cb-enable** command, SmartZone is disabled automatically. The following messages and syslog entry are displayed.

```
Console message
=====
Disabling SZ since SPX is enabled...
SZ Disable Initiated...
SZ Connection would be disconnected now if connected...

Syslog
=====
Aug  4 00:57:14:W:SZ:Disabling SZ, because SZ is not supported in SPX
```

If SPX is enabled on an ICX device and you try to enable SmartZone using the **no manager disable** command, the following warning message is displayed.

```
ICX(config)# no manager disable
SZ configuration is not allowed in SPX enabled setup. Please disable SPX to enable SZ
When ICX is managed through SZ, if 'spx cb-enable' is configured, SZ will be disconnected from ICX.
```

When an ICX switch is managed by SmartZone, the following considerations 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, or the web.
- It is recommended that the ICX 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 switch initiates a connection with SmartZone.

Enabling an ICX Device to Be Managed by SmartZone

There are several ways to make an ICX device aware of the SmartZone IP address:

- Use switch registrar discovery.
- Use DHCP option 43.
- Configure the ICX device manually using FastIron commands.

All of these methods are supported for new ICX switches with no configuration as well as for ICX switches with existing configuration.

Configuring the ICX Source Address to Be Used by SmartZone

By default, the IP address of the management port is included in the manager query as the ICX source address for an ICX-Management connection. Use the **manager source-interface** command to specify a different ICX source address.

NOTE

Only ICX devices with a router image support the **manager source-interface** command.

The **manager source-interface** command can specify an Ethernet, LAG, loopback, or virtual Ethernet (VE) interface. The IP address with the lowest number for the specified interface is used for the connection.

Managing ICX Switches from SmartZone

Setting up Switch Registrar Discovery

The following example configures an Ethernet port as the ICX source address for an ICX-Management connection.

```
ICX# configure terminal
ICX(config)# manager source-interface Ethernet 1/1/3
```

Refer to the *Ruckus FastIron Command Reference* for more information.

Setting up Switch Registrar Discovery

The switch registrar is a Ruckus-hosted cloud service that enables SmartZone discovery from ICX devices.

You can configure the ICX device to retrieve the correct SmartZone management IP address, IP address set, or fully qualified domain name (FQDN) from the switch registrar. The switch registrar must be set up in advance through Managed Service Provider (MSP) with SmartZone IP addresses or an FQDN and the ICX serial numbers they can manage.

NOTE

If SmartZone management is not enabled on the ICX device, switch registrar discovery does not occur.

How Switch Registrar Discovery Works

The ICX device sends an HTTP GET message to a default server host, `sw-registrar.ruckuswireless.com`, for the list of SmartZone management IP addresses or an FQDN, unless the system administrator configures an alternate host. The SmartZone IP address or FQDN obtained in response to the GET message is used to query the SmartZone device to set up a connection. If the ICX device receives a set of IP addresses from the switch registrar, it stores the information and tries the addresses in turn until a successful connection is established with the SmartZone device. The IP address, set of IP addresses, or FQDN obtained through the switch registrar is given priority above all other addresses in the list of SmartZone IP addresses, including addresses received from other sources such as the DHCP list, the active list, and the passive list. Once the ICX device has obtained a SmartZone IP address from the switch registrar, it no longer attempts switch registrar discovery.

This query is performed only for greenfield deployments and when the ICX device boots up with no startup configuration. ICX switches being upgraded from older releases that already have a configuration in place will not have the registrar-based SmartZone discovery turned on. The HTTPS session used for the database query uses the device certificate installed on the switch for SSL session establishment. For the initial release of the switch registrar, no server certificate validation will be performed.

Disabling or Enabling Switch Registrar Discovery

The system administrator can disable or enable switch registrar discovery from the command line.

NOTE

The registrar IP list is removed when you disable the switch registrar.

To disable switch registrar discovery, enter the **no manager registrar** command in global configuration mode, and use the **write memory** command to save the change as shown in the following example.

```
ICX# configure terminal
ICX(config)# no manager registrar
ICX(config)# write memory
```

To restart the switch registrar discovery process, use one of the following commands at the Privileged EXEC level:

- **manager registrar-query-restart**
- **manager reset**

To enable switch registrar discovery on an alternate registrar host server and save the entry to the startup configuration, enter the following commands.

```
ICX# configure terminal
ICX(config)# manager registrar sw-alternate.ruckuswireless.com
ICX(config)# write memory
```

NOTE

The **manager registrar hostname** command is for test purposes only. The **manager registrar-query-restart** command by itself is sufficient to initiate registrar-based SmartZone discovery.

Confirming Successful Switch Registrar Discovery

To display log entries specific to registrar queries, use the **show manager log** command.

When the switch registrar database has been successfully queried, a syslog message similar to the following is displayed.

```
Aug 8 21:47:17:I:MGMT Agent: SZ Switch Registrar Query to 54.186.143.194 Success
```

When the ICX device requires a restart to connect to the SmartZone address because a new registrar list has been received, a syslog message similar to the following is displayed.

```
Aug 8 21:47:17:I:MGMT Agent: Disconnect to SZ: 54.16.143.194, Got SZ ip via registrar
```

You can use the **show running-config** command to check for the name of the registrar host and the registrar list of SmartZone IP addresses.

The following example indicates that the ICX device uses the default switch registrar host and has obtained one SmartZone IP address (of a possible set of two addresses).

```
ICX# show running-config
!
!
manager registrar
manager registrar-list 23.251.150.119
!
!
```

You can also enter the **show manager status** command to obtain information on the switch registrar as shown in the following example.

```
ICX# show manager status

===== SZ Agent State Info =====
Config Status: None Operation Status: Enabled
State: SZ SSH CONNECTING Prev State: INIT Event: NONE
SWR List : 23.251.150.119
Active List : None
DHCP Option 43 : No
DHCP Opt 43 List : None
Passive List : None
Merged List : 23.251.150.119
Merged Idx: 0 IP : 23.251.150.119
Switch registrar host : sw-registrar.ruckuswireless.com
```

Troubleshooting Switch Registrar Discovery

In the event that switch registrar discovery fails, check for the following conditions:

- The running configuration contains "manager disable".
- The switch registrar is not configured on the ICX device.
- The DNS configuration needed to resolve the switch registrar address is not present on the ICX device.

- The ICX device could not reach the switch registrar due to routing issues.

NOTE

If the switch registrar is enabled and you enter the **no manager disable** command, switch registrar discovery is still started when the registrar IP list is empty.

NOTE

The switch registrar discovery process continues to run until the configuration issues are fixed, a successful query result is obtained, or you enter a command to disable the switch registrar.

Preparing Stacking Devices to Connect to SmartZone

Consider the following guidelines when preparing ICX stacking devices to be discovered and managed by SmartZone:

- Define the stack configuration on the SmartZone before connecting cables between the SmartZone and ICX devices.
- The devices to be managed in the stack must be part of a "firmware version" switch group configured on the SmartZone device.

If only the ICX device intended to be the stack active controller is an active switch under SmartZone control and is part of a configured "firmware version" switch group, do the following to establish a stack:

- Connect all cables between ICX devices to form the desired stack configuration.
- On the active controller, enter the following commands in Privileged EXEC mode:
 - **stack enable** (enables stacking on the active controller)
 - **stack zero-touch-enable** (triggers automatic discovery of the stack units and connections)
 - **write memory** (saves the running configuration to startup flash)

No commands need to be entered on the other stack units in this case.

If all switches intended to be members of a stack have already joined and have been approved by SmartZone and are already part of a "firmware version" switch group, enter the following commands on the ICX devices to form a stack:

- On the active controller, enter the following commands in Privileged EXEC mode:
 - **stack enable** (enables stacking on the active controller)
 - **stack zero-touch-enable** (triggers automatic discovery of the stack units and connections)
 - **write memory** (saves the running configuration to startup flash)
- On all other prospective stack members, configure the following commands in global configuration mode:
 - **stack suggested-id**
 - **stack ztp-force**
 - **write memory**

Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch

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";
  }
}
```

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.

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

IP addresses listed are examples only.

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

Displaying the SmartZone Connection Status

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

```
ICX# show manager 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 **manager disconnect** command can be used to disconnect the ICX switch from SmartZone and initiate a new connection based on the currently available list of SmartZone IP addresses.

Enter the **manager disconnect** command as shown.

This command can be executed on the local terminal.

```
ICX# manager 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 **manager disable** command to disable SmartZone management on the ICX switch.

```
ICX(config)# manager disable
```

SmartZone Switch Management

| | |
|--|-----|
| • Using Controller Settings to Manage Switch Groups..... | 201 |
| • Creating Switch Groups..... | 201 |
| • Creating Switch Registration Rules..... | 202 |
| • Moving the Switches between Groups..... | 204 |
| • Deleting Switches..... | 205 |
| • Backing up and Restoring Switch Configuration..... | 205 |
| • Scheduling a Firmware Upgrade for Switch Group..... | 206 |
| • Scheduling a Firmware Upgrade..... | 208 |
| • Viewing Switch Information..... | 210 |
| • Configuring the Switch..... | 212 |
| • Switch Level Configuration..... | 225 |
| • Port Settings..... | 234 |
| • Creating Routing Configurations..... | 241 |
| • Managing Link Aggregation Groups (LAGs)..... | 244 |
| • Creating a Switch Stack..... | 245 |
| • Viewing Port Details..... | 246 |
| • Viewing Switch Health..... | 249 |
| • Viewing Alarms..... | 252 |
| • Viewing Events..... | 254 |
| • Viewing LLDP Neighbor Information..... | 255 |
| • Viewing Traffic Trends in the Switch..... | 255 |
| • Viewing Firmware History of the Switch..... | 258 |
| • Configuring the Group Firmware Settings..... | 258 |
| • Accessing the switch CLI through SmartZone (Remote CLI)..... | 260 |
| • Viewing PoE Utilization and Health Status of the Switch..... | 263 |

Using Controller Settings to Manage Switch Groups

Controller allows you to create switch groups, similar to AP zones. Switches connecting to controller can be placed in one of these logical groups for better manageability. A Staging or Default Group is created by the controller automatically. All switches are placed in this group when they initially joining the controller. You have the option to create additional groups.

NOTE

In SZ300 and vSZ-H platforms, a warning message is displayed to move the switches from the Staging Group to another group for controller to monitor.

Using registration rules, you can specify which group the switch should be placed into. Refer to [Creating Switch Groups](#) on page 201 and [Creating Switch Registration Rules](#) on page 202 for additional information.

Creating 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.

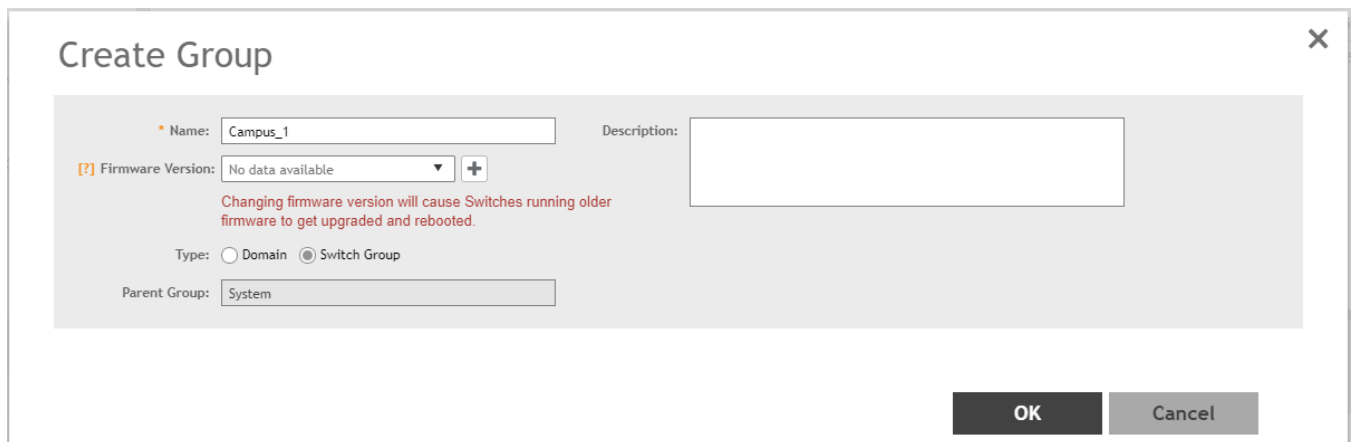
After the switch is registered with the controller interface, you can monitor, view status or usage, and perform some basic management, including configuration backups and firmware management. However, you cannot configure the switch from the controller web user interface.

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

2. Click .

The **Create Group** page appears.

FIGURE 75 Creating switch groups



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
 - Firmware Version: Select the Firmware version (optional) which will automatically upgrade the switches (running an older version) joining the group.
 - 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 76 Creating registration rules

Switch Registration Rule

Rule Description:

* Group Name:

Rule Type: IP Address Range Subnet Model Number

IP Address Range

* From IP:

* To IP:

OK **Cancel**

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 Switches

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

- Switches that do not match any registration rule are automatically placed under the Default group.
- At this point, the switch is not managed and the status is shown as offline.

- In order to actively manage this switch, you need to move it from the Staging Group to any other switch group or Domain in SZ300 and vSZH platforms. In SZ100 and vSZE platforms, the Default Group behavior is like any other group. Refer to [Moving the Switches between Groups](#) on page 204 for more information.

NOTE

A switch capacity license (CAPACITY-SWITCH-DEFAULT) is available for controllers and 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. For the controllers (SZ100 or SZ300), trial license will allow adding the maximum number of switches supported. In the case of vSZ-E or vSZ-H, trial license will allow addition of 5 switches.

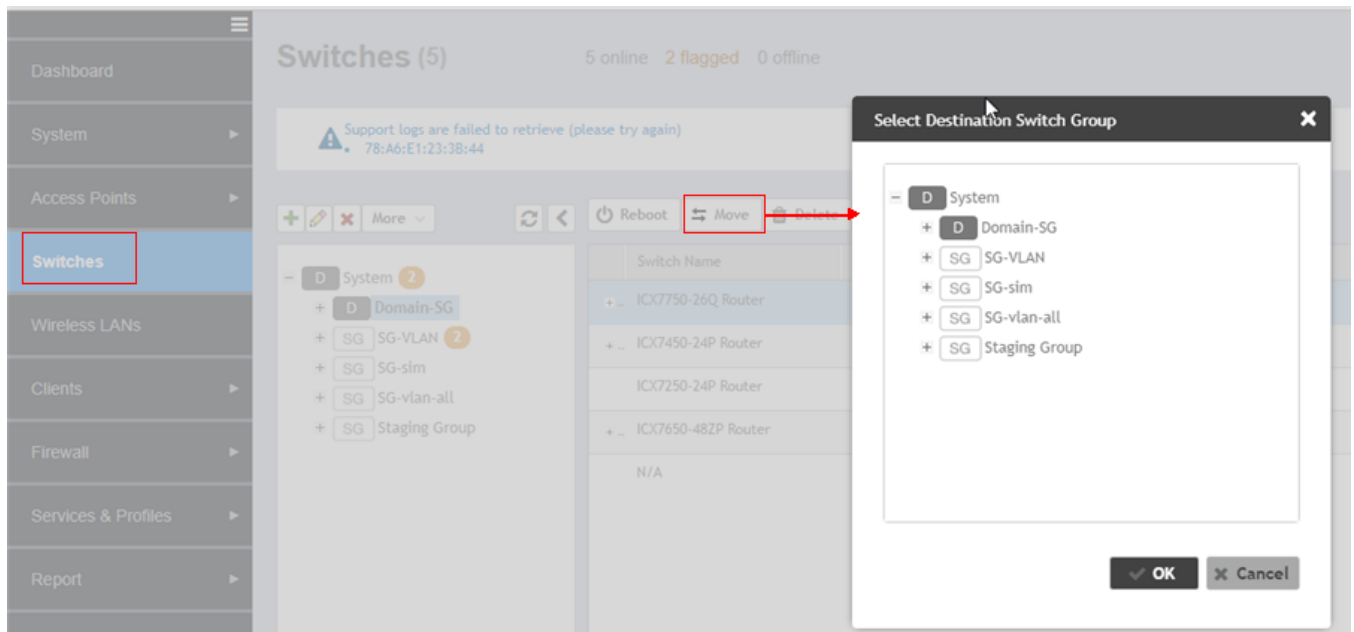
The recommendation is to always use switch registration rules so that they are placed in the correct switch group and avoid manual intervention.

Moving the Switches between Groups

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

1. From the left pane, select **Switches**.
The **Switches** page appears.
2. From the **Switches** page, select the switch that you want to move and click **Move**.

FIGURE 77 Moving the switch



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.

Deleting Switches

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

1. From the left pane, select **Switches**.
The **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 controller interface.

Backing up and Restoring Switch Configuration

The controller can back up the switch's running configuration. By default, controller makes a backup of switch configuration on a daily basis. The configuration is only stored if there is a change between the last configuration backup and the current backup. Otherwise, it is discarded. Controller saves the last seven configuration backups. 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.

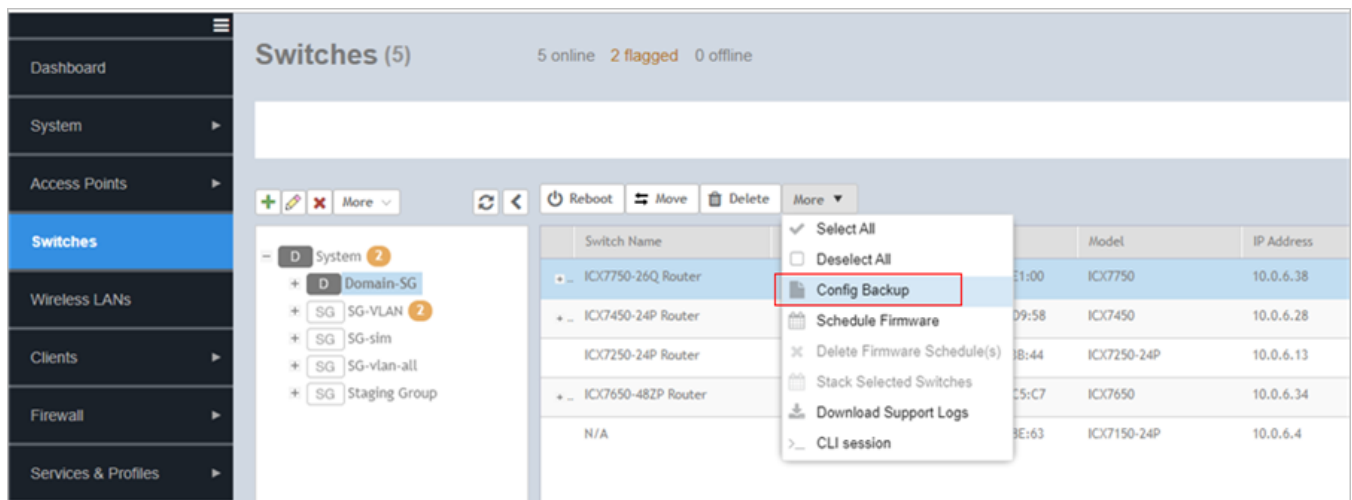
Perform the following steps to configure switch backups.

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 **Switches** page is displayed.
2. From the **Switches** page, select the switch for which you want to backup the configuration and click **More**.

FIGURE 78 Configuring Backup



3. From the drop-down menu, select **Config Backup**.
A confirmation message is displayed asking whether to continue with the backup.

4. 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 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 for Switch Group

You can upgrade a switch group on a Level 1 group that has no default firmware setting. The forced upgrade allows the device to remain in the same firmware type (Layer 2 still Layer 2, Layer 3 still Layer 3) with only a change to the version type.

NOTE

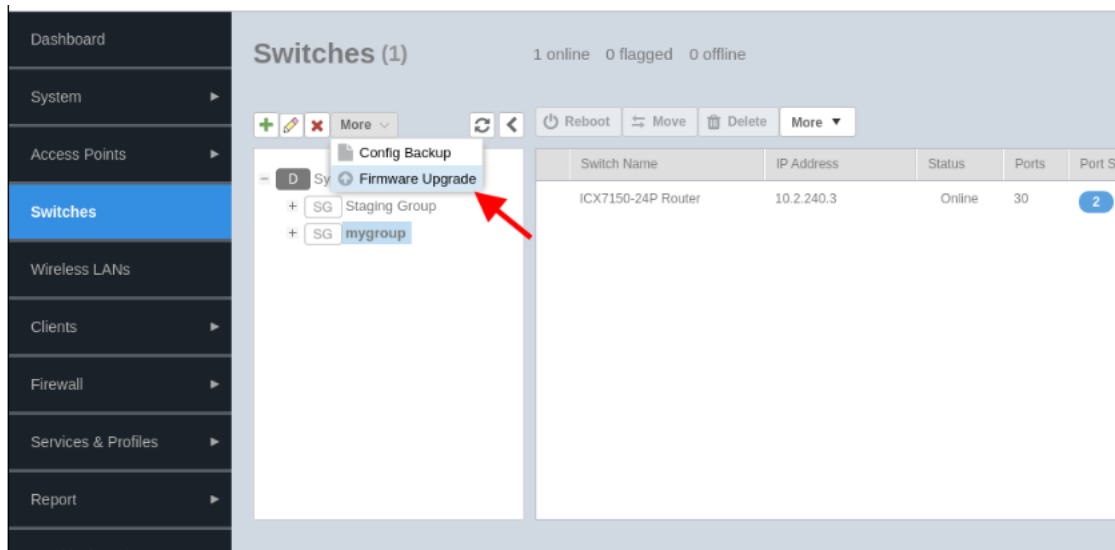
If the switch group has a default firmware selected the **Firmware Upgrade** option is unavailable.

Complete the following steps to perform a firmware upgrade on the switch group.

1. On the Controller web interface, select **Switches** from the left navigation pane.
The **Switches** page is displayed.
2. From the **Switches** page, select the switch group.

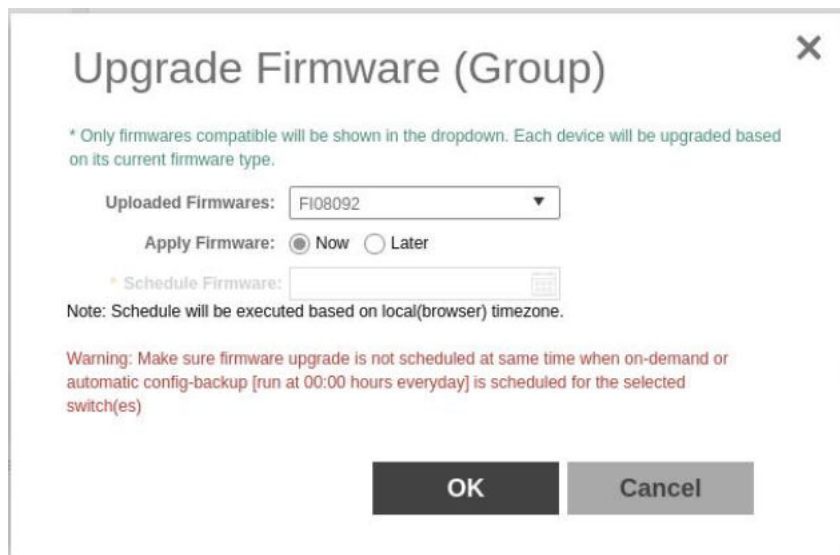
3. Click **More**, and select Firmware Upgrade.

FIGURE 79 Selecting Firmware Upgrade for a Switch Group



The **Upgrade Firmware (Group)** page is displayed.

FIGURE 80 Scheduling the Upgrade for a Switch Group



4. Configure the following options.
 - a. **Uploaded Firmwares:** Select firmware from the list.
 - b. **Apply Firmware:** Select Now or Later to set the new firmware version to the switch group.
 - c. **Schedule Firmware:** If you select Later for **Apply Firmware**, you must select the date to schedule the upload.
5. Click **OK**.

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 switches.

Upload a valid 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 558

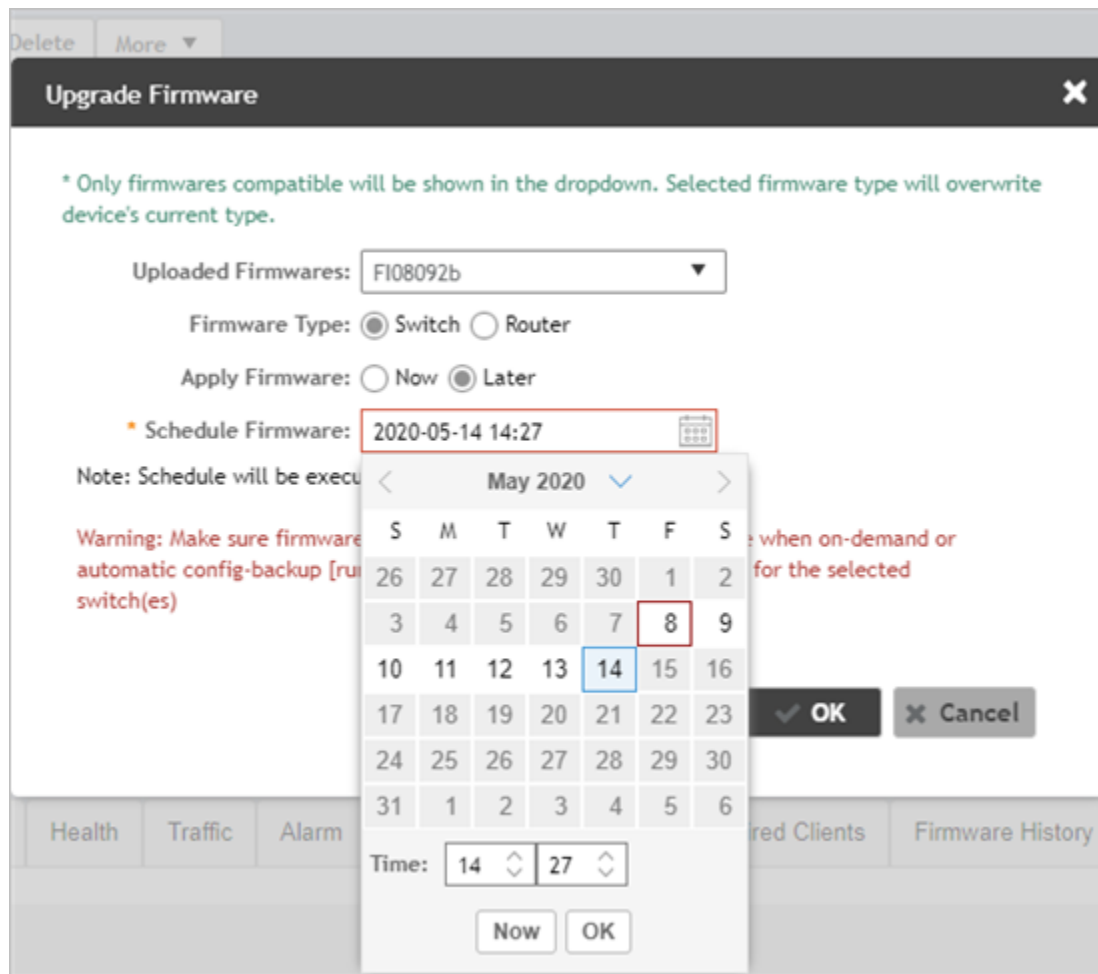
NOTE

Only firmware versions later than ICX 8.0.80 are supported.

1. From the left pane, select **Switches**.
The **Switches** page appears.
2. From the **Switches** page, select the switch that you want to upgrade and click **More**.

- From the drop-down menu, select **Schedule Firmware**.
The **Upgrade Firmware** page appears.

FIGURE 81 Scheduling Firmware Upgrade



- From **Uploaded Firmwares**, select the firmware version that you want the switch to be upgraded to
- In **Firmware Type**, select type of firmware you want to upload to the switch. Options include Switch and Router images.
- 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.
- 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 **Switches** page is displayed as shown in the following example.

FIGURE 82 Switches Page

The screenshot shows the 'Switches (5)' page in the SmartZone management interface. The page header indicates '5 online', '2 flagged', and '0 offline' switches. A left-hand navigation pane is visible with 'Switches' selected. The main content area features a toolbar with icons for adding, deleting, and refreshing, along with buttons for 'Reboot', 'Move', 'Delete', and 'More'. Below the toolbar is a table listing the switches with columns for Switch Name, Switch Group, MAC Address, Model, and IP Address.

| Switch Name | Switch Group | MAC Address | Model | IP Address |
|-------------------------|--------------|-------------------|-------------|------------|
| +.. ICX7750-26Q Router | SG-VLAN | 60:9C:9F:D7:E1:00 | ICX7750 | 10.0.6.38 |
| +.. ICX7450-24P Router | SG-VLAN | D4:C1:9E:2B:D9:58 | ICX7450 | 10.0.6.28 |
| ICX7250-24P Router | SG-VLAN | 78:A6:E1:23:3B:44 | ICX7250-24P | 10.0.6.13 |
| +.. ICX7650-48ZP Router | SG-VLAN | D4:C1:9E:14:C5:C7 | ICX7650 | 10.0.6.34 |
| N/A | SG-VLAN | D4:C1:9E:22:8E:63 | ICX7150-24P | 10.0.6.4 |

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

FIGURE 83 Switch Stack and General Information

The screenshot shows the SmartZone Switch Management interface. On the left is a dark sidebar with navigation options: Administration, Events & Alarms, Diagnostics, and System Info. The System Info section is expanded, showing Hostname: vSZH-...csm-1 and Version: 5.2.1.0.323. The main content area has a light blue header with tabs: General (selected), Configuration, Backup & Restore, Ports, Routing, Health, Traffic, Alarm, and Event. Below the tabs, there are two sections: 'Info' and 'Status Summary'. The 'Info' section contains a table of system details, and the 'Status Summary' section contains a table of operational status.

| Info | |
|------------------------|--------------------|
| Switch Name | ICX7750-26Q Router |
| MAC Address | 60:9C:9F:D7:E1:00 |
| Serial Number | CRK3308N02F |
| IP Address | 10.0.6.38 |
| Gateway | 10.0.0.254 |
| Model | ICX7750-20QXG |
| Switch/Stack | Stack |
| Number of Switch Units | 2 |
| Firmware Version | SWR08090f |

| Status Summary | |
|---------------------------|----------------------|
| Status | Online |
| Registration State | Approved |
| # of Alarms | 0 |
| Uptime | 14 days, 13:04:23.00 |
| Last Configuration Backup | 2020/05/11 09:05:03 |
| Switch Group | SG-VLAN |

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

NOTE

Flagged status indicates that one or more switches have an outstanding alarms and/or Port errors are seen on the switch ports. Click **Flagged** to view the flagged switches.

- **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.

Configuring the Switch

SmartZone 5.1.1 introduces switch configuration capabilities. The following features are added:

- **Zero Touch Provisioning:** Greatly simplifies initial deployment of switches. Users can define switch configuration at a switch group level. Any new switch joining the group automatically gets provisioned.
- **Ongoing Configuration Changes:** Users can further modify the switch configuration as a part of network maintenance. This includes modifying switch group level settings, port settings, and routing interfaces.
- **Stack formation:** Users can configure individual switches to be formed into a stack directly from the controller.
- **Configuration copy:** Users can copy configuration from a working switch to one or multiple new switches seamlessly.

You can view and modify various configuration parameters of switches from the controller web interface. You can create switch configuration profiles at the group level, individual switch level and at the port level.

The **Configuration** page displays common configurations based on DNS, allows setting configuration values for a family of switches and also provides a summary of the switch configuration history.

You can update the configuration profile for new and existing switches, switches that join the controller after being offline, switches that may or may not have local feature changes via CLI/Telnet/SSH/other web interfaces.

After the switch configuration is updated successfully, you can continue to monitor the configuration deployed on the switch. If the switch configuration is not updated successfully, a message is displayed on the controller interface.

Zero Touch Provisioning using Group level Configuration

You can create and view configurations that are defined at the switch group level. Within the switch group, there is an option to define common configuration that is applicable to all the switch models in the group and another option to select configuration based on switch family, for example ICX 7150, ICX 7250, and so on. When a new switch without any existing configuration running FastIron version 8.0.90a or later version joins the controller, the group level configuration is automatically applied to the switch. This includes the global AAA settings, common configuration, and model-specific settings. If the switch joining the group already has an existing configuration, then the group level configuration is not applied during the initial join. Only the subsequent changes done at the group level are applied.

NOTE

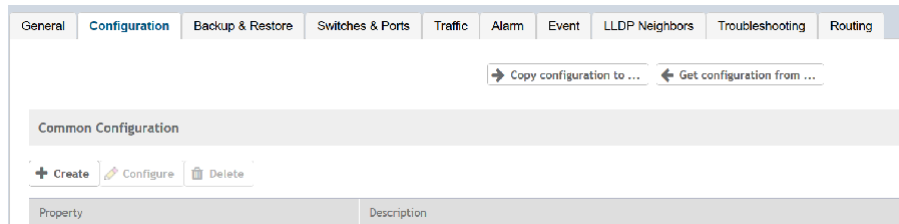
ICX switches must run 08.0.90a or later version to take advantage of the switch configuration capabilities of the controller.

Creating Common Configuration

You can create, view, and edit the configuration settings for a group of switches.

1. Select **Switches** from the navigation bar.
The **Switches** page is displayed.
2. Select the switch and click the **Configuration** tab.

FIGURE 84 Switch Configuration Tab



- Under **Common Configuration**, click **Create**.

The **Common Configuration** page is displayed.

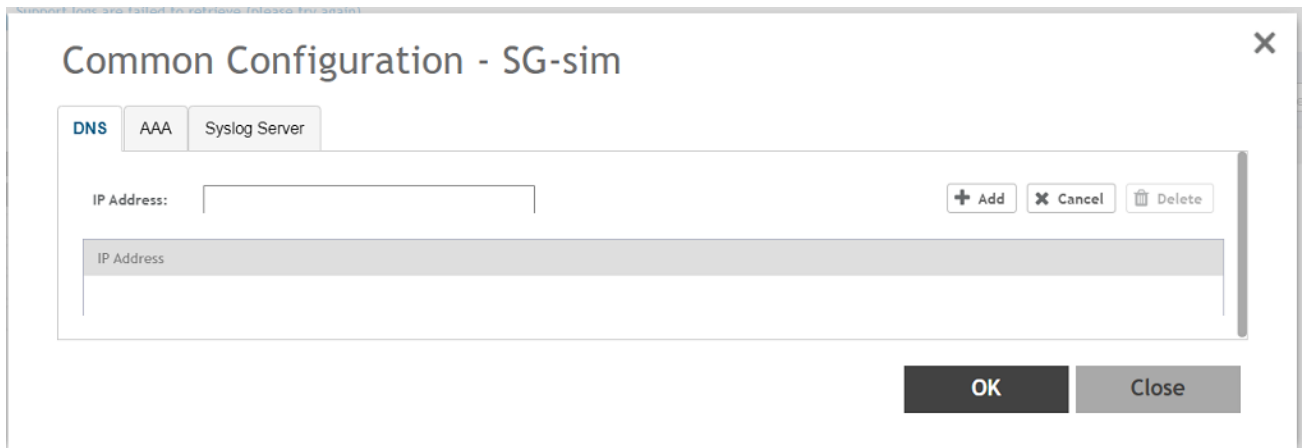
NOTE

In the following example, the Switch Group is the Default Group.

- Click the **DNS** tab.
The **DNS** tab is displayed.
- Enter the IP address and click **Add**.
- Click **OK**.

The IP address is added to the **Common Configuration** page under **Property** and any new (factory default) switch joining this group will have the DNS configuration applied. If you want to edit the configuration, select it and click **Configure** to edit the settings.

FIGURE 85 DNS Settings



- Click **AAA** tab.
The **AAA** page is displayed.

FIGURE 86 AAA Settings

The screenshot shows the AAA Settings configuration window. At the top, there are three tabs: 'DNS', 'AAA' (which is selected and highlighted in blue), and 'Syslog Server'. The main content area is divided into two sections: 'Authorization' and 'Accounting'.
Authorization Section:
- 'Command Authorization' is set to 'OFF'.
- 'Exec Authorization' is set to 'OFF'.
- 'Level' is set to 'Read Write'.
- 'Server 1' is set to 'RADIUS'.
- 'Server 2' is set to 'Please select data'.
Accounting Section:
- 'Command Accounting' is set to 'OFF'.
- 'Exec Accounting' is set to 'OFF'.
- 'Level' is set to 'Read Write'.
- 'Server 1' is set to 'RADIUS'.
- 'Server 2' is set to 'Please select data'.
At the bottom right of the window, there are two buttons: 'OK' and 'Cancel'.

e) Configure the AAA settings for the switches.

A Switch AAA server can be a RADIUS server, a TACACS+ server, or a local server with user name password. Switch AAA settings include enabling or disabling of SSH or Telnet Authentication, Authorization and Accounting, including selecting the order of preference for the AAA servers.

f) Click **OK**.

g) Click the **Syslog Server** tab.

FIGURE 87 Syslog Server Settings

The screenshot shows a web interface titled "Common Configuration - SG-sim" with a close button (X) in the top right corner. It features three tabs: "DNS", "AAA", and "Syslog Server". The "Syslog Server" tab is active. Below the tabs, there are two input fields: "IP Address" and "Port" (with the value "514" entered). To the right of these fields are three buttons: "+ Add", "X Cancel", and a trash icon labeled "Delete". Below the input fields is a table with two columns: "IP Address" and "Port". The table is currently empty. At the bottom right of the configuration area is a "Close" button.

NOTE

This feature is supported on the switch firmware version 08.0.95.

- h) In the **IP Address** field, enter the IP address of the external syslog server. Click **Cancel** to erase the entry in the field.
- i) Enter the port number in the **Ports** field.

NOTE

The default port is 514, but the user can change it as per the requirements.

- j) Click **Add** to add the entries.

NOTE

The maximum of four IP addresses can be added.

- k) Click **Delete** to delete the syslog server.
- l) Click **OK**.

Creating Switch Model-Based Configurations

You can create and edit ACL, Layer 2, and Layer 3 configuration settings for a family of switches. You can also create or update the ACL to configure QoS profiles that prioritize VOIP and VIDEO VLAN traffic.

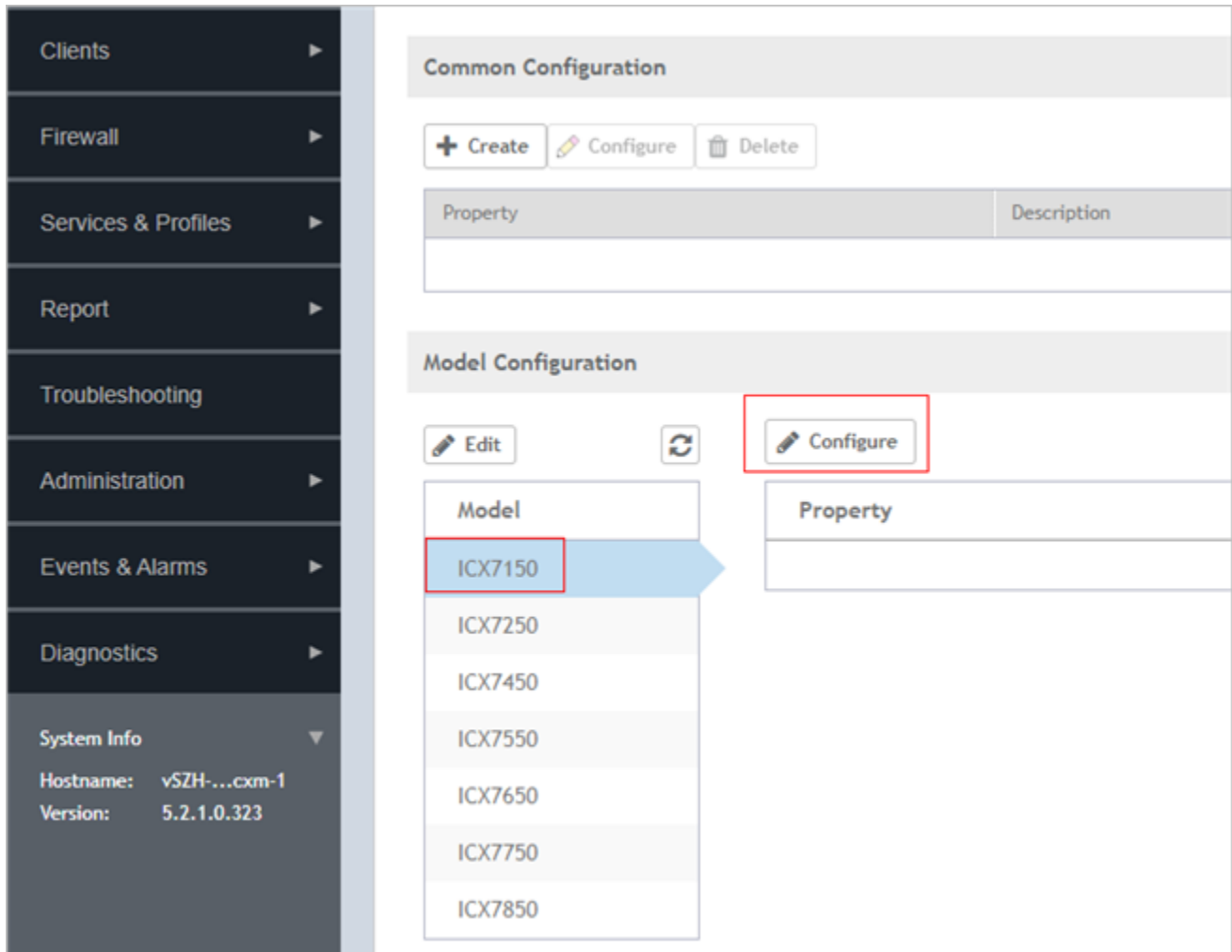
NOTE

Configuring the QoS Profiles requires ICX Firmware version 08.0.95.

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

2. Select the switch group and click the **Configuration** tab.

FIGURE 88 Switch Configuration Tab



3. In **Model Configuration**, select the switch model from the list and click **Configure**.

The **Feature Configuration** page displays details about the ACL, VLAN, and static route. You can create, edit, and delete these configurations as necessary.

FIGURE 89 ACL Configuration

Feature Configuration -

ACL VLAN Static Route

+ Create Configure Delete

| ACL Names / ID | ACL Type | Push ACL Config |
|----------------|----------|-----------------|
|----------------|----------|-----------------|

No data << 1 >>

* ACL Name / ID:

* ACL Type: Standard

* Rules: + Create Delete

| Seq # | Action | Source Network |
|---------|--------|----------------|
| 1.. 100 | Permit | 1.1.1.0/24 |
| 2 65000 | Permit | any |

* Apply ACL Config: Now Schedule Later

OK Cancel

FIGURE 90 ACL Configuration with ICX Firmware version 08.0.95

Switch **ACL** VLAN

+ Create Configure Delete

| ACL Names / ID | ACL Type | Push ACL Config |
|----------------|----------|-----------------|
| No data 1 | | |

ACL Name / ID:

ACL Type: **Extended**

Rules: + Create Delete

| Action | Source Network | Source Port | Destination Network | Destination Port | (1) DSCP Matching | (2) DSCP Marking | (3) Internal Priority Marking |
|--------|----------------|-------------|---------------------|------------------|-------------------|------------------|-------------------------------|
| | N/A | N/A | | | N/A | N/A | N/A |

Apply ACL Config: Now Schedule Later

OK Cancel

Close

Configure the following ACL details:

- **ACL Name/ID:** Enter the name of the access control list or provide the list identifier.
- **ACL Type:** Select Standard and Extended from the list.
- **Rules:** Click **Create** to create an ACL rule. You must provide the list sequence (**Seq#**), **Action** (Permit or Deny) and **Source Network** information to create the rule.

NOTE

Controller supports the "equal to" operator only.

NOTE

The Controller release 5.2.1 adds three new fields (**DSCP Matching**, **DSCP Marking** and **Internal Priority Marking**) to configure QoS. After creating or updating the three fields, apply the ACL on a port or a VE to prioritize/de-prioritize traffic.

- From **Apply ACL Config**, you can either select Now or Schedule Later. If you choose to schedule the configuration deployment later, provide the time and date.
- Click **OK** to add the newly created ACL configuration to the **ACL** page. You can edit the configuration by selecting **Configure**.

FIGURE 91 VLAN Configuration

Feature Configuration

ACL VLAN Static Route

No data « 1 »

VLAN #: 2 VLAN Name:

As Default VLAN: OFF Management VLAN: OFF

IPv4 DHCP Snooping: OFF DHCP Snooping Trust Port:

ARP Inspection: OFF ARP Inspection Trust Port:

IGMP Snooping: None Multicast Version: Version 2

Spanning Tree: None Spanning Tree Priority: 0-65535

Ports:

| Switch Model | Untagged Ports | Tagged Ports |
|--------------|----------------|--------------|
| 1.. | 1/2/1,2/3/2 | 1/1/5,1/1/12 |

Apply VLAN Config: Now Schedule Later

Configure the following VLAN details:

- **VLAN #:** Enter the number of the VLAN.
- **VLAN Name:** Enter the name of the Layer 2 VLAN.
- **As Default VLAN:** If you enable the **As Default VLAN** the **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.
- **Management VLAN:** By enabling this, you can configure Management VLAN for the switches or switch groups. To configure Management VLAN for switches or switch groups refer the topic [Creating Switch Level Configuration](#) on page 225.
- **IPv4 DHCP Snooping:** Enable or disable IPv4 DHCP Snooping. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **DHCP Snooping Trust Port** field.

- **APR Inspection:** enable or disable ARP Inspection. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **ARP Inspection Trust Port** field.
- **IGMP Snooping:** Select **None**, **Active**, or **Passive** from the list. The Internet Group Management Protocol (IGMP) allows the switch to track the communication between hosts and routers based on which the switch maintains a map of which links need which IP multicast streams. If you select **Active** or **Passive**, you are required to select the **Multicast Version** as well.
- **Spanning Tree:** Select **None**, **STP (802.1d)**, or **RSTP (802.1w)** from the list. Both Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) prevent creation of bridge loops when you have redundant paths in your network, and the broadcast radiation that results from them. If you select **STP 802.1d** or **RSTP 802.1w**, you are required to select the **Spanning Tree Priority** as well.
- **Ports:** Click **Create** to assign the ports to the switch model. For desired switch models, enter values for **Untagged Ports**, and **Tagged Ports** and click **Update**. Different set of ports can be entered for each switch model.
- **Apply VLAN Config:** Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
- Click **OK** to add the newly created VLAN configuration to the **VLAN** page. You can edit the configuration by selecting **Configure**.

FIGURE 92 Static Route Configuration

The screenshot shows the 'Feature Configuration' interface for 'Static Route'. It includes a table with the following headers: Destination IP, Next Hop, Admin Distance, and Apply Static Route Config. Below the table, there is a form with the following fields:

- Destination IP: [Text Input]
- Next Hop: [Text Input]
- Admin Distance: [Text Input]
- Apply Static Route Config: Now Schedule Later [Calendar Icon]

Buttons for 'OK', 'Cancel', and 'Close' are visible at the bottom of the configuration area.

Configure the following static route details:

- **Destination IP:** Enter the destination IP address.
- **Next Hop:** Enter the next-hop IP address. Multicast and broadcast IP addresses are not allowed.

- **Admin Distance:** Enter a value from 1 through 255.
 - **Apply Static Route Config:** Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
 - Click **OK** to add the newly created static route configuration to the **Static Route** page. You can edit the configuration by selecting **Configure**.
4. Click **Close**.

The IP address is added to the **Model Configuration** page under **Property**. If you want to edit the configuration, select it and click **Edit** to edit the settings.

NOTE

Any changes made to the group level configuration including common configuration and switch model-based configuration will be applied to all the switches belonging to the group.

Configuration defined at group level can be chosen to be applied instantaneously by selecting the **Now** option or schedule for a later time using **Schedule later** option. The scheduling option is only applicable if you are trying to make changes to existing switches in the group. For any new switches that are joining the group, this configuration gets applied instantaneously.

Copying Switch Group Configuration

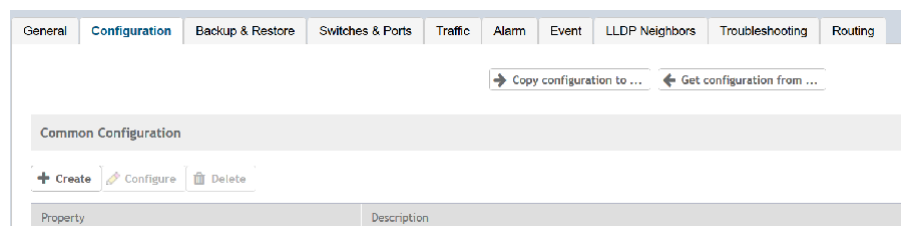
You can copy the configuration settings from a working switch to one or multiple new switches.

NOTE

It is recommended to exercise caution when using the copy configuration option as it replaces the entire configuration of the destination switch.

1. From the left pane, select **Switches**.
The **Switches** page appears.
2. Select the switch group and then the **Configuration** tab.

FIGURE 93 Switch Group Configuration Tab



3. Click **Copy Configuration To** and select the switch or group to which you want to copy the configuration profile, and click **OK**.
4. Click **Get Configuration From** and select the switch or group from which you want to get the configuration profile, and click **OK**.

Accessing AAA Settings for Switch Configuration

You can create, view, and edit the configuration settings for a group of ICX switches.

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

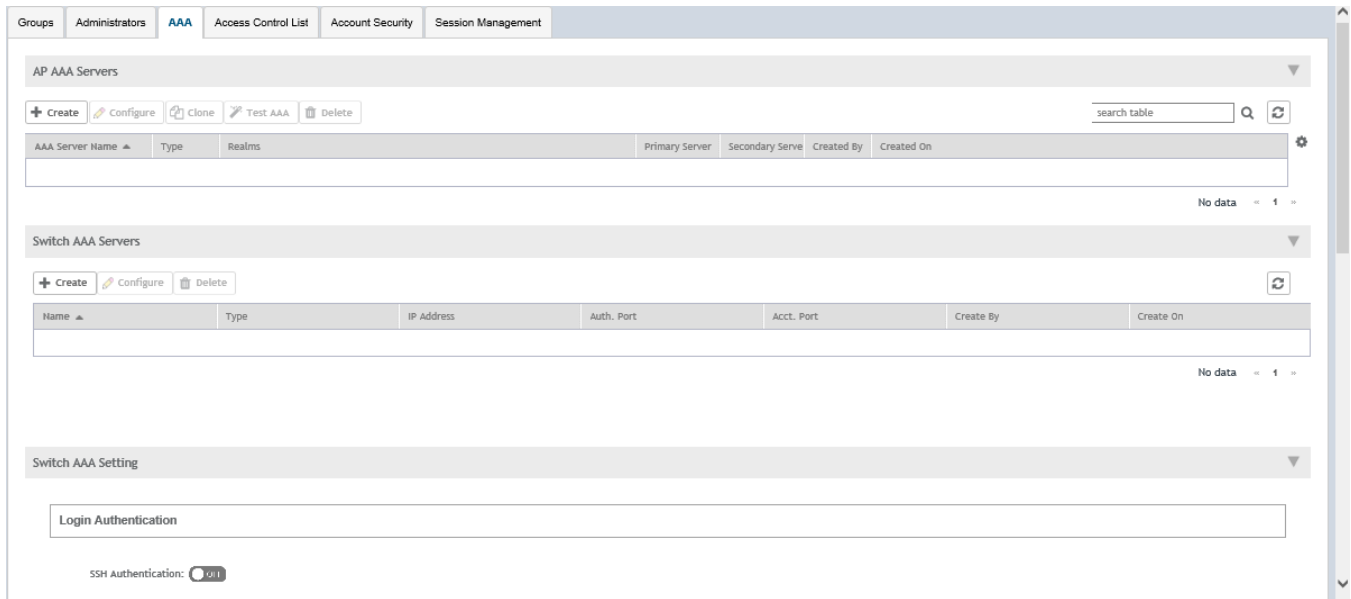
2. Select the switch and click the **Configuration** tab.

FIGURE 94 ICX Switch Configuration Tab

The screenshot displays the configuration interface for an ICX switch. At the top, a navigation bar includes tabs for General, Configuration (selected), Backup & Restore, Switches & Ports, Routing, Traffic, Alarm, Event, LLDP Neighbors, and Troubleshooting. Below the navigation bar are two buttons: 'Copy configuration to ...' and 'Get configuration from ...'. The main content area is divided into two sections: 'Common Configuration' and 'Model Configuration'. The 'Common Configuration' section features a '+ Create' button, a 'Configure' button with a pencil icon, and a 'Delete' button with a trash icon. Below these buttons is a table with two columns: 'Property' and 'Description'. The 'Model Configuration' section includes an 'Edit' button with a pencil icon, a refresh icon, and a 'Configure' button with a pencil icon. To the left of the 'Property' and 'Description' table is a list of switch models: 'ICX7150', 'ICX7250', and 'ICX7450'. The 'ICX7250' model is currently selected. At the bottom right of the 'Common Configuration' section, the text 'No data << 1 >>' is visible.

3. Click **Switch AAA settings** to access the global AAA configuration settings for switches.
The **AAA** page appears.

FIGURE 95 AAA Page



You can configure the AAA settings for the switches.

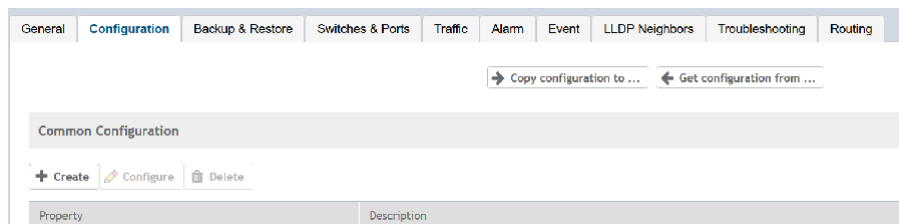
Switch AAA servers can be a RADIUS server, TACACS+, or a local username password. Switch AAA settings include enabling or disabling SSH or Telnet Authentication, Authorization, and Accounting including selecting the order of preference for the AAA servers.

Viewing the Configuration History of Switches

You can view the configuration details of switches from the **Configuration History** tab.

1. From the left pane, select **Switches**.
The **ICX Switches** page appears.
2. Select the switch and then the **Configuration** tab.

FIGURE 96 ICX Switch Configuration Tab



- You can view the following configuration information:

FIGURE 97 Configuration history

The screenshot shows the 'Configuration History' interface. At the top, there is a search bar and a refresh icon. Below it is a table with columns: Date & Time, Type, Model Family, Status, and Message. The table contains 13 records, with the fourth record highlighted in blue. Below the table, there is a 'Configuration Details' section with 'All' and 'Failure' buttons. A table below these buttons shows details for the selected record, including Switch Name, Serial Number, Start Time, End Time, Message, CLI, Failed Line Number, and Failed Message. A tooltip is visible over the CLI field.

| Date & Time | Type | Model Family | Status | Message |
|---------------------|--------------------|--------------|---------|--|
| 2019-04-25 10:01:41 | VE_PORTS | ICX7650 | SUCCESS | Success (1) / Failed (0) / Failed No Response (0) / Failed Save... |
| 2019-04-25 10:00:53 | PORT_CONFIGURATION | ICX7650 | SUCCESS | Success (1) / Failed (0) / Failed No Response (0) / Failed Save... |
| 2019-04-25 10:00:15 | LAG_SETTINGS | ICX7650 | SUCCESS | Success (1) / Failed (0) / Failed No Response (0) / Failed Save... |
| 2019-04-25 09:57:26 | MODEL | ICX7650 | SUCCESS | Success (1) / Failed (0) / Failed No Response (0) / Failed Save... |
| 2019-04-25 09:57:11 | SWITCH_SETTINGS | ICX7650 | SUCCESS | Success (1) / Failed (0) / Failed No Response (0) / Failed Save... |
| 2019-04-25 09:56:48 | MODEL | ICX7650 | SUCCESS | Success (1) / Failed (0) / Failed No Response (0) / Failed Save... |
| 2019-04-25 09:55:05 | MODEL | ICX7650 | SUCCESS | Success (1) / Failed (0) / Failed No Response (0) / Failed Save... |
| 2019-04-25 09:54:53 | MODEL | ICX7650 | SUCCESS | Success (1) / Failed (0) / Failed No Response (0) / Failed Save... |

| Switch Name | Serial Number | Start Time | End Time | Message | CLI | Failed Line Number | Failed Message |
|--------------|---------------|---------------------|---------------------|---------|-------------------------------------|--------------------|----------------|
| ICX7650-48P_ | EZD3350N036 | 2019-04-25 09:57:26 | 2019-04-25 09:58:02 | SUCCESS | ip access-list STANDARD 50 seque... | N/A | N/A |

ip access-list STANDARD 50 sequence 65000 PERMIT any

Information about the date and time at which the configuration profile was created, type of configuration, switch model or switch family that its created for, configuration status and a message confirming the configuration implementation on the switch/switch group is displayed.

Clicking the switch displays more information about the **Configuration Details** as shown.

Switch Level Configuration

In addition to the group level configuration, individual switch-level configuration can be edited by selecting the switch from the Switch table.

Switch-specific settings include **Hostname**, **Jumbo Mode**, **IGMP Snooping**, and **DHCP Server**. In addition, the switch configuration defined at the group level is available for editing at the switch level.

Creating Switch Level Configuration

You can configure switch, ACL, VLAN, and static route settings for each switch.

- From the left pane, select **Switches**.
The **Switches** page is displayed.
- Select a switch and click the **Configuration** tab.

3. Click **Configure** and select the **Switch** tab.

FIGURE 98 Switch Configuration

Feature Configuration -

Switch ACL VLAN

Name: 10.1.200.85

IGMP Snooping: None

Jumbo Mode: OFF

DHCP Server: ON

DHCP Server

+ Create Edit Delete

| Pool Name | Network / Mask | Excluded Range | Lease Time | Default Router IP |
|-----------|----------------|----------------|------------|-------------------|
| fdsd | 198.232.1.2/25 | | 1 0 0 | 1.2.2.1 |

Options: + Create Delete

| Option # | Type | Value |
|----------|-------|-------|
| 2 | ASCII | |

OK Close

4. Configure the following switch details:

- **Name:** Enter the name of the switch.
- **IGMP Snooping:** Select the profile from the list.
- **Jumbo Mode:** Enable this option to reboot the switch.
- **DHCP Server:** Enable this option and click **Create** to configure the following DHCP server settings:

NOTE

You must disable the DHCP client before enabling the DHCP server.

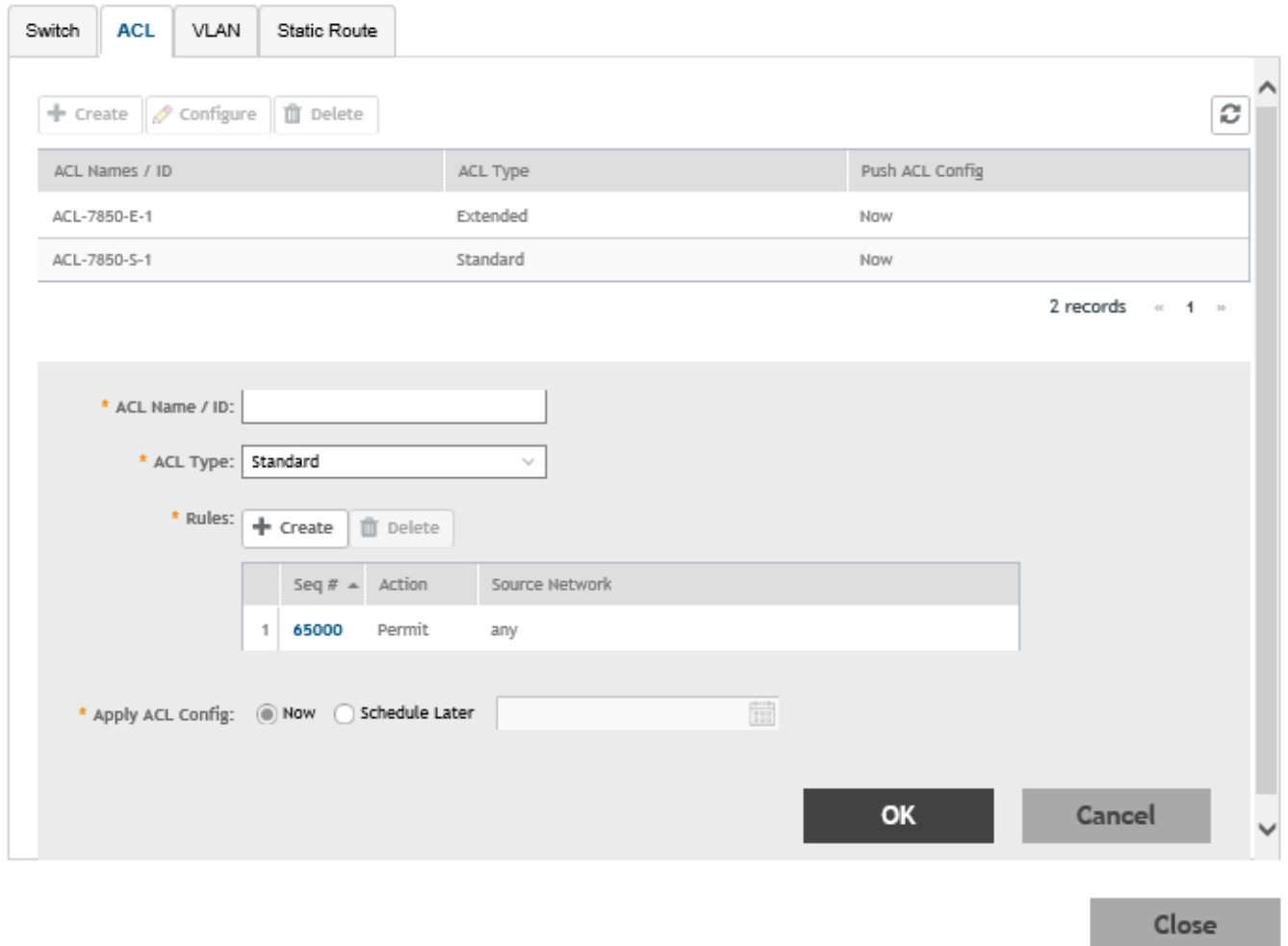
- **Pool Name:** Enter a name.
- **Network/Mask:** Enter the network address and network mask.
- **Excluded Range:** Enter the network range to be excluded.
- **Lease Time:** Enter the lease time duration.
- **Default Router IP:** Enter the default router IP address.
- **Options:** Click **Create** and enter the option number, , select a type, and enter a value for the option.

Click **Update** to apply the option.

Click **OK** to add the newly created switch configuration to the **Switch** tab page. You can edit or delete the configuration by selecting **Edit** or **Delete**, respectively.

5. Select the **ACL** tab.

FIGURE 99 ACL Configuration



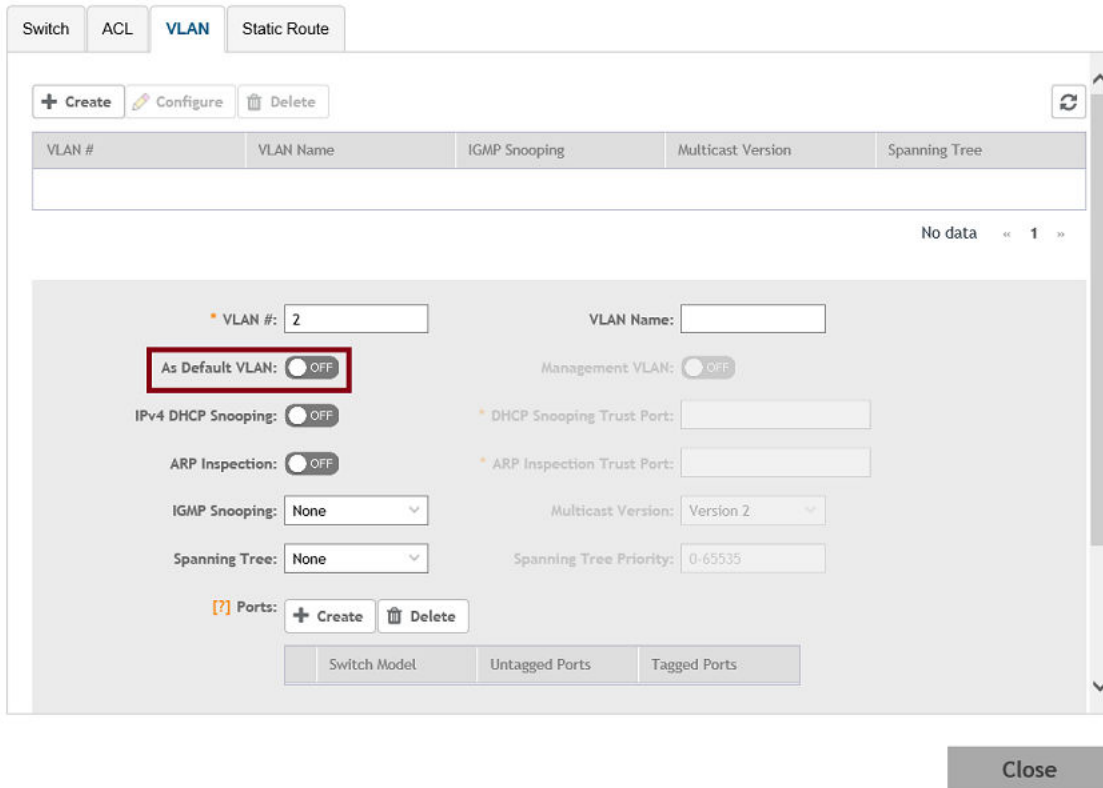
6. Click **Create** and configure the following ACL details:
 - **ACL Name/ID:** Enter the name of the access control list or provide the ACL ID.
 - **ACL Type:** Select **Standard** or **Extended** from the list.
 - **Rules:** Click **Create** to create an ACL rule. You must provide the list sequence number, action (Permit or Deny), and **Source Network** information to create the rule.
 - **Apply ACL Config:** Select **Now** or **Schedule Later**. If you choose to schedule the configuration deployment for later, provide the time and date.

Click **OK** to add the newly created ACL configuration to the **ACL** page. You can edit or delete the configuration by selecting **Configure** or **Delete**, respectively.

7. Select the **VLAN** tab.

You can create a new VLAN and set it as the default VLAN.

FIGURE 100 VLAN Configuration



8. Click **Create** and configure the following VLAN details:

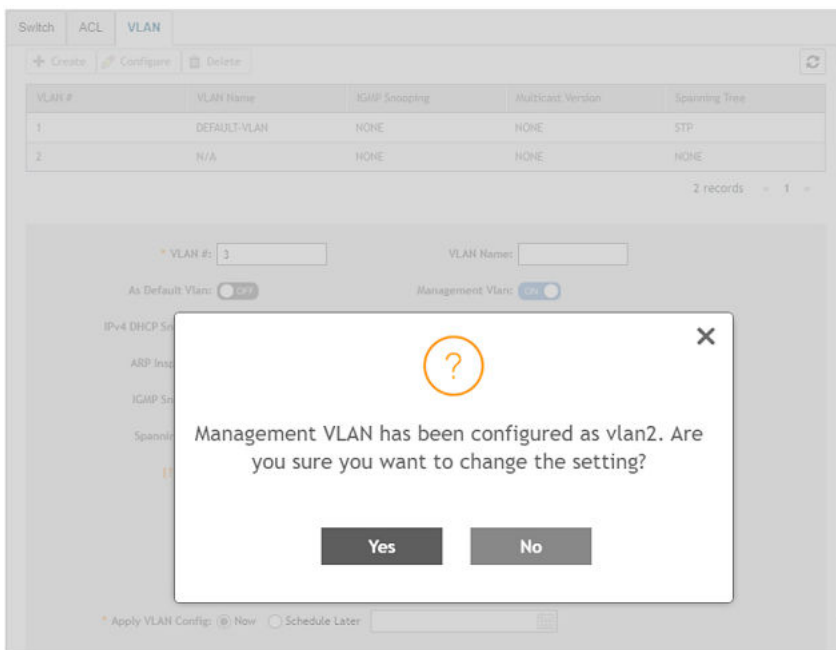
- **VLAN #:** Enter a unique number for VLAN.
- **VLAN Name:** Enter the name of the Layer 2 VLAN.

NOTE

If you enable the **As Default VLAN**, the **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.

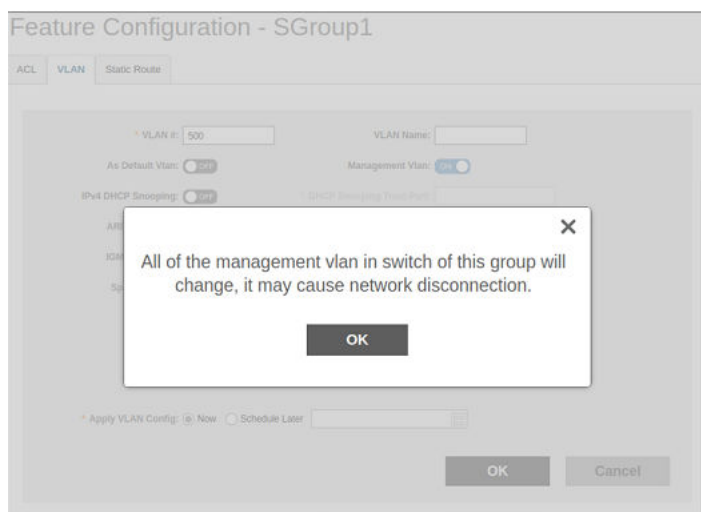
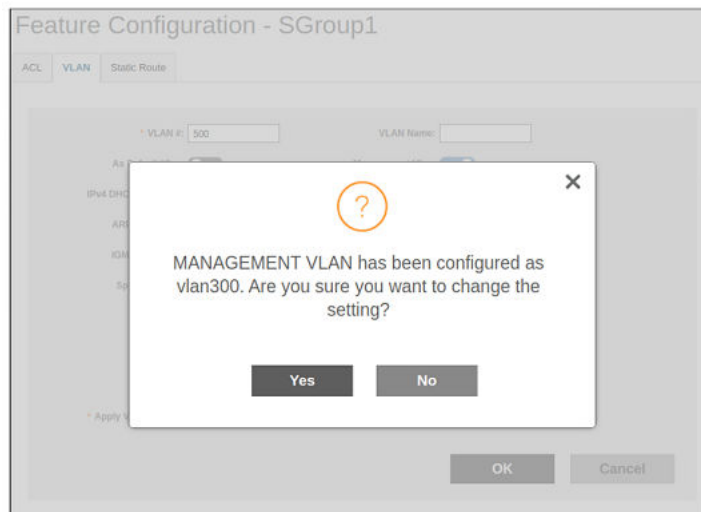
- **Management VLAN:** You can configure the Management VLAN for the switches or switch groups in the following ways:
 - Enable **Management VLAN**, and click **OK**.

If the VLAN is configured as the default VLAN, enable or disable **Management VLAN** on the default VLAN, and click **OK**. A dialogue box is displayed, as shown in the following.



If **Management VLAN** is enabled on a VLAN and you try to enable it on another VLAN, the controller displays a dialogue box showing the VLAN ID that has been configured as the Management VLAN. If you click **Yes**, the controller overwrites the settings.

- For a switch group, the controller displays a dialogue box, as shown in the following figure.



- **IPv4 DHCP Snooping:** Enable or disable IPv4 DHCP Snooping. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **DHCP Snooping Trust Port** field.
- **APR Inspection:** enable or disable ARP Inspection. Enabling this option allows the controller to send the ACL-per-port-per-vlan message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **ARP Inspection Trust Port** field.
- **IGMP Snooping:** Select **None**, **Active**, or **Passive** from the list. The Internet Group Management Protocol (IGMP) allows the switch to track the communication between hosts and routers based on which the switch maintains a map of which links need which IP multicast streams. If you select **Active** or **Passive**, you are required to select the **Multicast Version** as well.
- **Spanning Tree:** Select **None**, **STP (802.1d)**, or **RSTP (802.1w)** from the list. Both Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) prevent creation of bridge loops when you have redundant paths in your network, and the broadcast radiation that results from them. If you select **STP** or **RSTP**, you are required to select the **Spanning Tree Priority** as well.
- **Ports:** Click **Create** to assign the ports to the switch model. Enter values for **Switch Model**, **Untagged Ports**, and **Tagged Ports** and click **Update**.
- **Apply VLAN Config:** Select **Now** or **Schedule Later**. If you choose to schedule the configuration deployment for later, provide the time and date.

Click **OK** to add the newly created VLAN configuration to the **VLAN** tab. You can edit or delete the configuration by selecting **Configure** or **Delete**, respectively.

9. Select the **Static Route** tab.

FIGURE 101 Static Route Configuration

| Destination IP | Next Hop | Admin Distance | Apply Static Route Config |
|------------------|-----------------|----------------|---------------------------|
| 192.168.220.0/24 | 192.168.250.254 | 200 | Now |

1 records << 1 >>

* Destination IP:

* Next Hop:

Admin Distance:

* Apply Static Route Config: Now Schedule Later

OK Cancel

Close

Click **Create** and configure the following static route details:

- **Destination IP:** Enter the destination IP address.
- **Next Hop:** Enter the next hop IP address. Multicast and broadcast IP addresses are not allowed.
- **Admin Distance:** Enter a value from 1 through 255.
- **Apply Static Route Config:** Select **Now** or **Schedule Later**. If you choose to schedule the configuration deployment for later, provide the time and date.

Click **OK** to add the newly created static route configuration to the **Static Route** tab. You can edit or delete the configuration by selecting **Configure** or **Delete**, respectively

10. Click **Close**.

The configurations are updated under **Property**. If you want to edit the configuration, select it and click **Edit** to edit the settings.

NOTE

Use the switch-level option to add additional ACLs, VLANs, or static routes other than those already defined at the switch group level. Use the group-level configuration to make changes to existing settings at the group level.

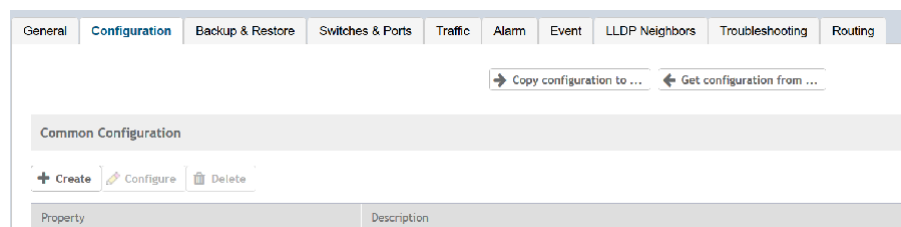
Copying Configuration

If you already have a switch with the desired set of features configured, controller provides an option to load the current configuration of the switch, remove unique settings like hostname, IP addresses, and so on, and copy it to one or more target switches. This procedure is applicable only if the target switches have no existing configuration.

Complete the following steps to copy configuration to one or more target switches.

1. From the left pane, select **Switches**.
The **Switches** page appears.
2. Select the switch and then the **Configuration** tab.

FIGURE 102 Switch Group Configuration Tab



3. Click **Copy Configuration To**. This option lets you replace the entire configuration (startup-config) of the selected switch with that of a source switch.
4. Click **Get Configuration From** and select the switch or group from which you want to get the configuration profile, and click **OK**. This option lets you replace the entire configuration of destination switches (one or more) with the configuration of the selected switch.

- Select the switch group and click the **Ports** tab.
The **Switch Port** page is displayed.

FIGURE 104 Switch Port Page

The screenshot shows the SmartZone Switch Management interface. The left sidebar contains navigation options: System, Access Points, Switches (selected), Wireless LANs, Clients, Applications, Services & Profiles, Report, Troubleshooting, Administration, Events & Alarms, and Diagnostics. The main content area is titled 'Switches (6)' and shows a list of switches. The 'Ports' tab is selected, displaying 'Port Details' for the selected switch (ICX7850-48FS Router) and port (10GigabitEthernet1/1/1). The port status is 'Down'.

| Switch Name | Switch Group | MAC Address | Model | Port Status | Status | IP Address | Last Backup | Registration State | Firmware | Serial Number |
|---------------------|--------------|-------------------|---------------|-------------|--------|------------|-------------|--------------------|-----------|---------------|
| ICX7750-48C Router | ICX-M-Demo | D4-C1-9E-3C-02:00 | ICX7750-48XGC | 0 / 0 / 54 | Online | 10.0.0.136 | 2019/04/12 | Approved | SW808090a | OUJ315P01P |
| ICX7450-48 Router | ICX-M-Demo | 78-A6-E1-3A-73:C0 | ICX7450-48G | 0 / 0 / 57 | Online | 10.0.1.176 | 2019/04/12 | Approved | SP808090a | CYQ2351N00D |
| ICX7250-24G Switch | ICX-M-Demo | CC-4E-24-9C-02:00 | ICX7250-24G | 0 / 0 / 28 | Online | 10.0.2.42 | 2019/04/12 | Approved | SP508090a | DUG3824N0EC |
| ICX7650-48ZP Router | ICX-M-Demo | D4-C1-9E-14-C5:C7 | ICX7650-48ZP | 0 / 0 / 50 | Online | 10.0.2.54 | 2019/04/12 | Approved | TN808090a | EZC3307P01T |
| ICX7150-C12 Switch | ICX-M-Demo | 60-9C-9F-E5-E0:0E | ICX7150-C12P | 0 / 0 / 15 | Online | 10.0.1.31 | 2019/04/12 | Approved | SP508090a | FEK3236N02D |
| ICX7850-48FS Router | ICX-M-Demo | D4-C1-9E-18-76:79 | ICX7850 | 0 / 1 / 110 | Online | 10.0.0.248 | Failed | Approved | TN808090a | FLV3333P001 |

| Port Name | Port Number | Status | Admin Status | Speed | PoE Devi | PoE Usage (s) | VLANs | Bandwidth IN (s) | Bandwidth OUT (s) | Neighbor Name | LAG Name (Type) | Optics | Incoming Mbit | Outgoing Mbit | Incoming Bps | Outgoing Bps | In Errors | Out Errors | CRC Errors | In B |
|------------------------|-------------|--------|--------------|-----------|----------|---------------|-------|------------------|-------------------|---------------|-----------------|----------|---------------|---------------|--------------|--------------|-----------|------------|------------|------|
| 10GigabitEthernet1/1/1 | 1/1/1 | Down | Up | 10 Gb/sec | | | 211 | 0.00 | 0.00 | | | 10 GbitL | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

- Under **Port Details**, select the port that must be updated and click **Configure**.
The **Port Settings** page is displayed.

FIGURE 105 Port Settings Page

Port Settings

Selected Port(s): 1/1/1

Port Name:

Port Enabled: ON

Port Protected: OFF

Tagged VLANs:

Untagged VLAN:

POE Enable: ON

POE Priority:

POE Class:

POE Budget:

Ingress ACL: +

Egress ACL: +

Port Speed:

RSTP Admin Edge Port: OFF

STP BPDU Guard: OFF

STP Root Guard: OFF

DHCP Snooping Trust Port: OFF

IPSG: OFF

OK **Cancel**

FIGURE 106 Port Settings for QoS

Port Settings

QoS Budget:

Ingress ACL: +

Egress ACL: +

Port Speed:

RSTP Admin Edge Port:

STP BPDU Guard:

STP Root Guard:

DHCP Snooping Trust Port:

IPSG:

LLDP:

(1) Voice VLAN:

LLDP QoS:

| Application type | VLAN type | VLAN ID | Priority | DSCP |
|------------------|-----------|---------|----------|------|
| GUEST_VOICE | TAGGED | 100 | 0 | 0 |

(7) DSCP remark:

4. Configure the following port settings:

- **Port Name:** Enter the port name.
- **Port Enabled:** Click to enable the port.
- **Port Protected:** Click to enable the protected port.

NOTE

Port Protected field is displayed only for the switches using SmartZone 5.2.1 and above.

- **Tagged VLANs:** Enter the tagged VLAN ID or VLAN ID range.
- **Untagged VLAN:** Enter an untagged VLAN ID.
- **POE Enable:** Click to enable PoE.
- **POE Class:** Select the PoE class. You can configure the PoE budget on ports by setting the PoE class to 0 through 4.
- **POE Priority:** Enter the PoE priority.
- **POE Budget:** Allows users to manually set the PoE power limit.
- **Ingress ACL:** Select the ingress ACL from the list.
- **Egress ACL:** Select the egress ACL from the list.
- **Port Speed:** Select the required port speed from the list.
- **RSTP Admin Edge Port:** Click to enable the RSTP Admin Edge Port.
- **STP BPDU Guard:** Click to enable the STP BPDU Guard.
- **STP Root Guard:** Click to enable the STP Root Guard.
- **DHCP Snooping Trust Port:** Click to enable the DHCP Snooping Trust Port.
- **IPSG:** Click to enable IPSG.
- **ILLDP:** Click to enable ILLDP.
- **Voice VLAN:** Select the VLAN (tagged or untagged).
- **LLDP QoS:** Click to enable LLDP-MED settings.
- **Application type:** Enter one of the application types : **Guest_Voice**, **Guest_Voice_Signaling**, **Softphone_Voice**, **Streaming_Video**, **Video_Conferencing**, **Video_Signaling**, **Voice**, and **Voice_Signaling**.
- **VLAN type:** The VLAN type can be priority-tagged, tagged, or untagged.
- **VLAN ID:** Enter the **VLAN ID** of the VLAN type.
- **Priority:** Enter the priority for the QoS setting.
- **DSCP:** Enter the DSCP value for the LLDP setting.
- **DSCP remark:** Enter the DSCP remarking value for the interface.

5. Click **OK**.

Editing Ports Across Multiple Switches

Before 5.2.1 release, the user could edit multiple ports for an individual switch. But after 5.2.1 release, the controller allows the user to edit the ports across multiple switches within the same Switch Group.

For example, if you want to disable port 1/1/11 and 1/1/12 across multiple switches, the controller provides an option to filter the ports list by typing the search criteria.

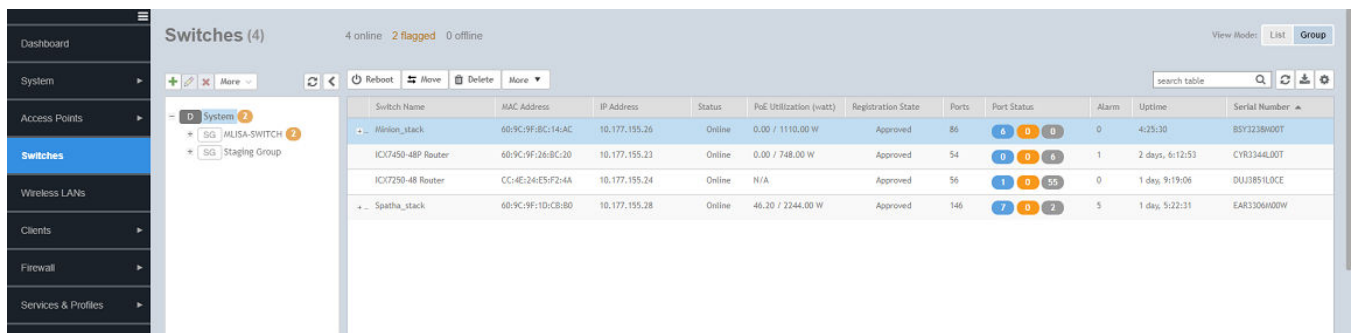
The search criteria is based on the following.

- Switch Name
- Port numbers - comma separated values (1/1/1,1/1/11,1/1/24), (or) Range of ports (1/1/1 to 1/1/20)
- VLAN membership
- PoE detected ports
- Port Status
- Admin Status

You must complete the following steps to edit ports across multiple switches.

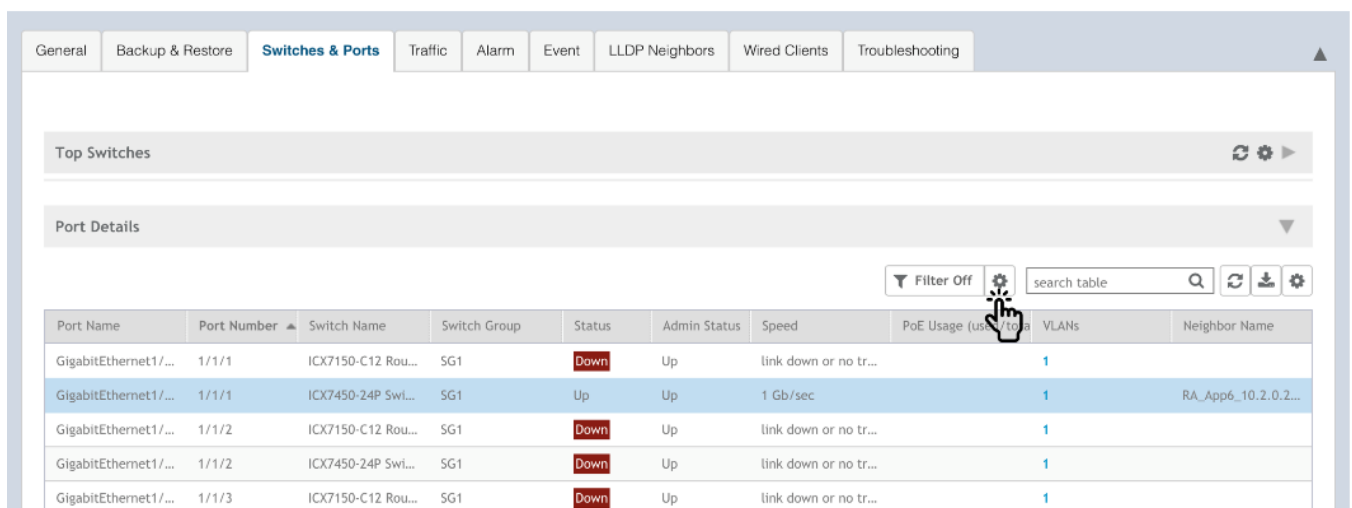
1. From the controller web interface, select **Switches** from the left navigation pane.
The **Switches** page is displayed.
2. Select a **Switch Group**.


FIGURE 107 Selecting a Switch Group



3. Click the **Switches and Ports** tab.

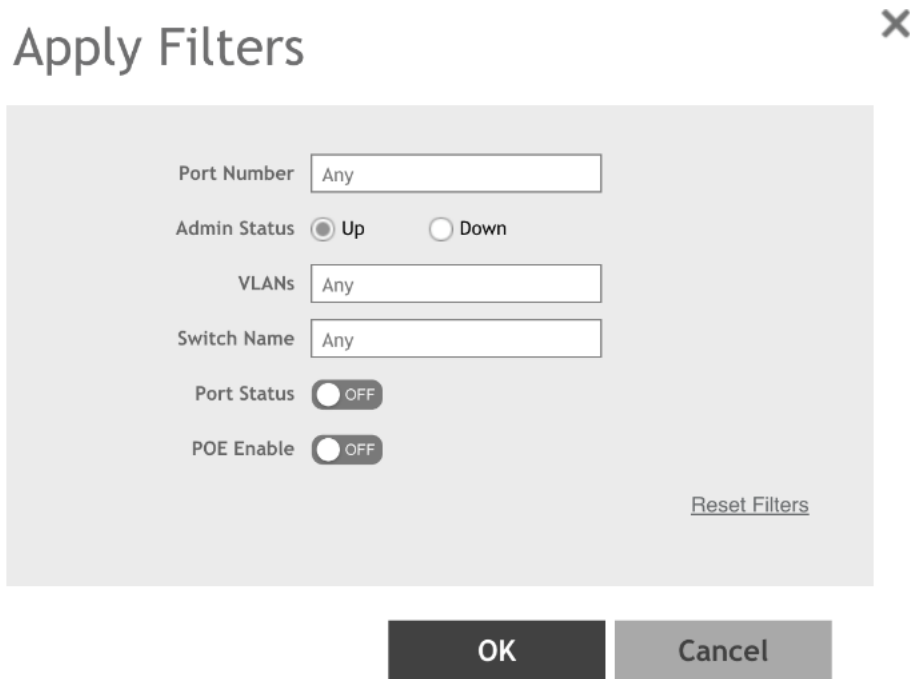
FIGURE 108 Viewing the Switches and Ports Page



4. Click the  icon.

A dialogue box is displayed. The controller provides the following filters to combine several query conditions to filter-out the ports which you want to edit.

FIGURE 109 Applying Filter to Edit the Ports



Apply Filters ✕

Port Number

Admin Status Up Down

VLANs

Switch Name

Port Status OFF

POE Enable OFF

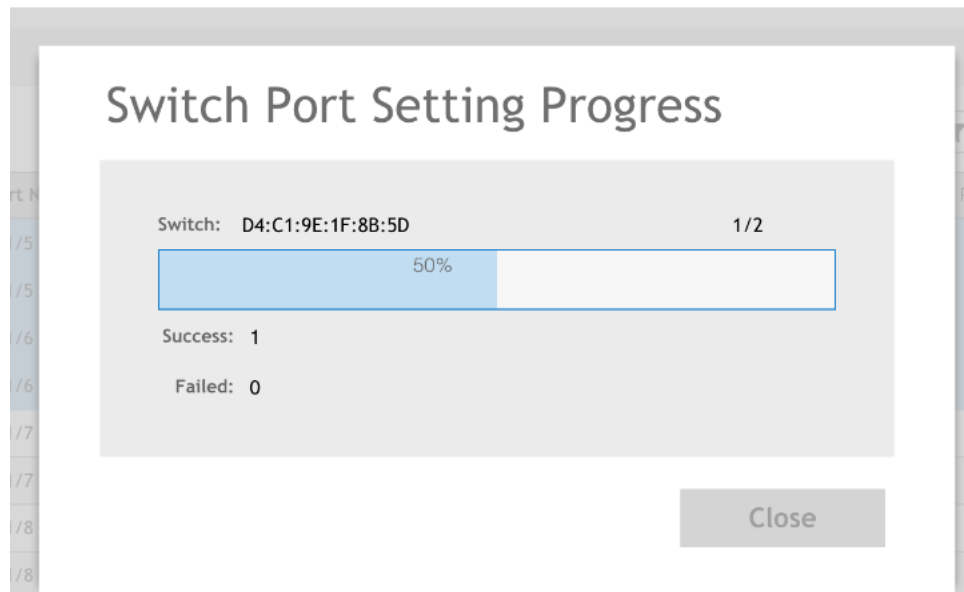
[Reset Filters](#)

OK **Cancel**

5. Click **OK**.

The controller applies the above filters to return ports that meet the search criteria.

FIGURE 110 Showing the Progress of Switches Fulfilling the Search Criteria



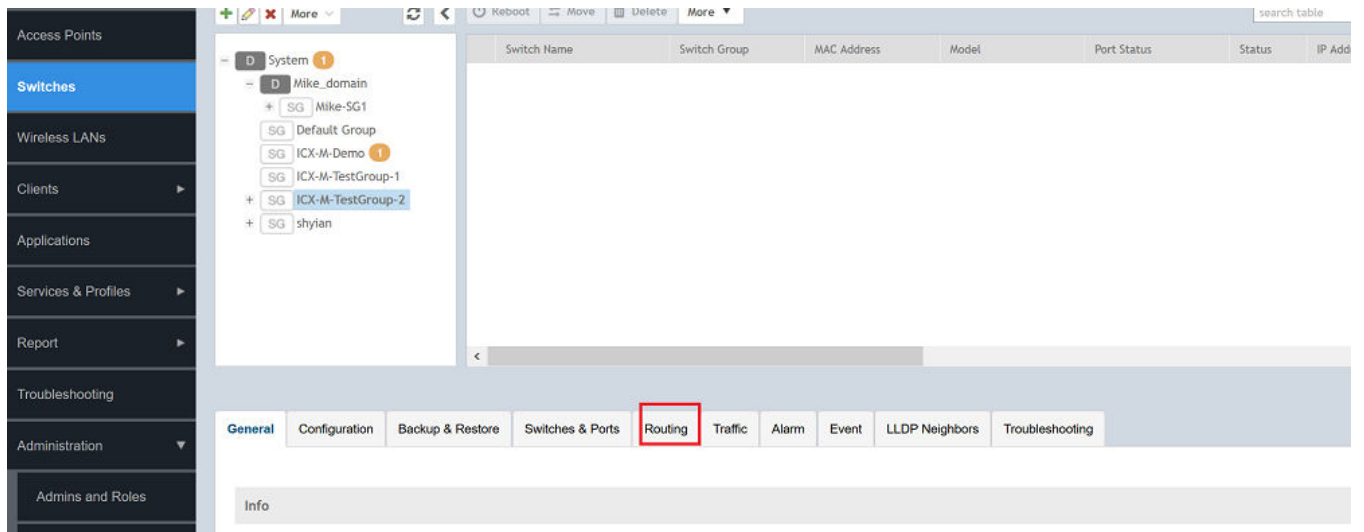
Creating Routing Configurations

You can create, edit, and delete routing configurations for an switch.

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

2. Select the switch group or switch and click the **Routing** tab.

FIGURE 111 Switch Routing Tab



3. In **IP Ports**, click **Create**.

The **IP Ports** page is displayed.

FIGURE 112 IP Ports Page

The screenshot displays the 'IP Ports' management interface. At the top, there are three buttons: '+ Create', 'Configure', and 'Delete'. Below these is a table with the following headers: Switch, Name, Port, DHCP Relay Agent, IP Address, OSPF Area, Ingress ACL, and Egress ACL. The table is currently empty, showing 'No data' and a page indicator '« 1 »'. Below the table is a configuration form with the following fields:

- Switch:** A dropdown menu with the text 'Please select data'.
- Name:** A text input field.
- Port:** A dropdown menu with the text 'Please select data'.
- IP Address:** A text input field.
- OSPF Area:** A text input field.
- DHCP Relay Agent:** A text input field.
- IP Subnet Mask:** A text input field.
- Ingress ACL:** A dropdown menu with the text 'Please select data'.
- Egress ACL:** A dropdown menu with the text 'Please select data'.

At the bottom right of the form are two buttons: 'OK' and 'Cancel'.

Configure the following IP port information:

- **Switch:** Select the switch from the list,
- **Name:** Enter a name.
- **OSPF Area:** Enter the OSPF area IPv4 address.
- **Port:** Select the port number from the list.
- **DHCP Relay Agent:** Enter the DHCP relay agent IP address.
- **IP Address:** Enter a unicast IP address.
- **IP Subnet Mask:** Enter an IP subnet mask.
- **Ingress ACL:** Select the ACL for the ingress network interface.
- **Egress ACL:** Select the ACL for the egress network interface.

4. Click **OK**.

5. In **VE Ports**, click **Create**.

The **VE Ports** page is displayed.

FIGURE 113 VE Ports Page

The screenshot shows the 'VE Ports' management interface. At the top, there are buttons for '+ Create', 'Configure', and 'Delete'. Below this is a table with the following columns: Switch, VLAN#, Name, IP Address, IP Subnet Mask, Ingress ACL, and Egress ACL. The table is currently empty, with a 'No data' message and a page indicator '« 1 »'. Below the table is a configuration form with the following fields:

- Switch: Please select data (dropdown)
- Name: (text input)
- VLAN#: Please select data (dropdown)
- IP Address: (text input)
- Ingress ACL: Please select data (dropdown)
- VE#: 1 (text input)
- OSPF Area: (text input)
- DHCP Relay Agent: (text input)
- IP Subnet Mask: (text input)
- Egress ACL: Please select data (dropdown)

At the bottom right of the form are 'OK' and 'Cancel' buttons.

Configure the following VE port information:

- **Switch:** Select the switch from the list.
- **VE#:** Enter the VE number. Range: 1 through 4095.
- **Name:** Enter a name.
- **OSPF Area:** Enter the OSPF area IPv4 address.
- **VLAN#:** Select the VLAN from the list.
- **DHCP Relay Agent:** Enter the DHCP relay agent IP address.
- **IP Address:** Enter a unicast IP address.
- **IP Subnet Mask:** Enter an IP subnet mask.
- **Ingress ACL:** Select the ACL for the ingress network interface.
- **Egress ACL:** Select the ACL for the egress network interface.

6. Click **OK**.

Managing Link Aggregation Groups (LAGs)

Controller provides an option to define LAGs at an individual switch level.

1. From the **LAG Setting**, click **Create** to view the LAG settings.

The **Create LAG** page is displayed.

- Enter the following settings:
 - LAG Name:** Enter a name.
 - Type:** Select either **Static** or **Dynamic** from the list.
 - Selected Port:** You can select multiple port numbers from the list.
- Click **OK** to apply the LAG configuration onto the selected switch.

Creating a Switch Stack

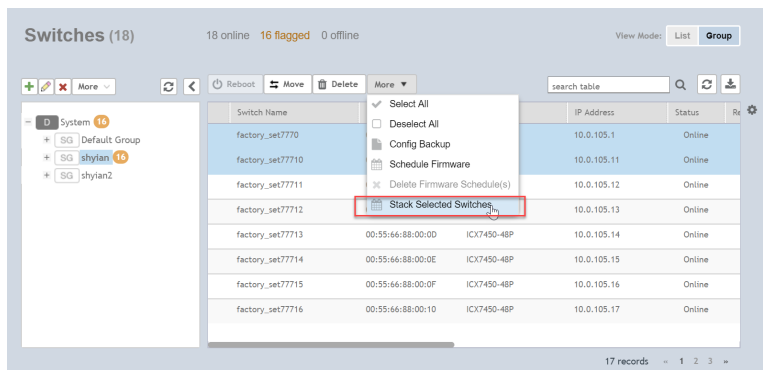
You can create a stack by selecting individual switches that are connected to the controller.

As a pre-requisite, you must configure switch stacking from controller before connecting the switch cables.

Complete the following steps to create a stack of switches.

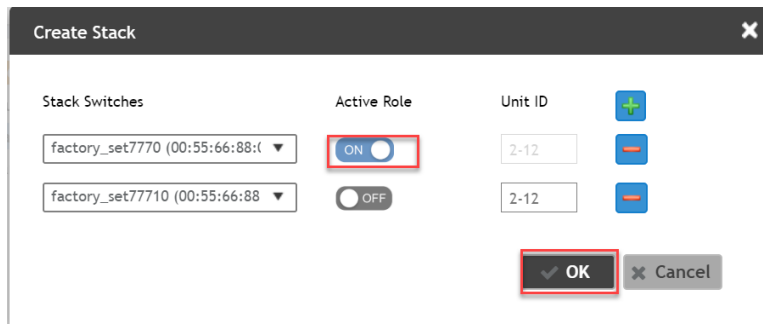
- From the left pane, click **Switches** and then select the switch group.

FIGURE 114 Switches Page



- Select the switches that has to be stacked and click **More > Stack Selected Switches**.
The **Create Stack** page is displayed.

FIGURE 115 Creating a Stack



- Under **Active Role**, select **ON** for the selected switches and click **OK** to create the stack.

The created switch stack is reflected in the Switches page within a switch group.

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.

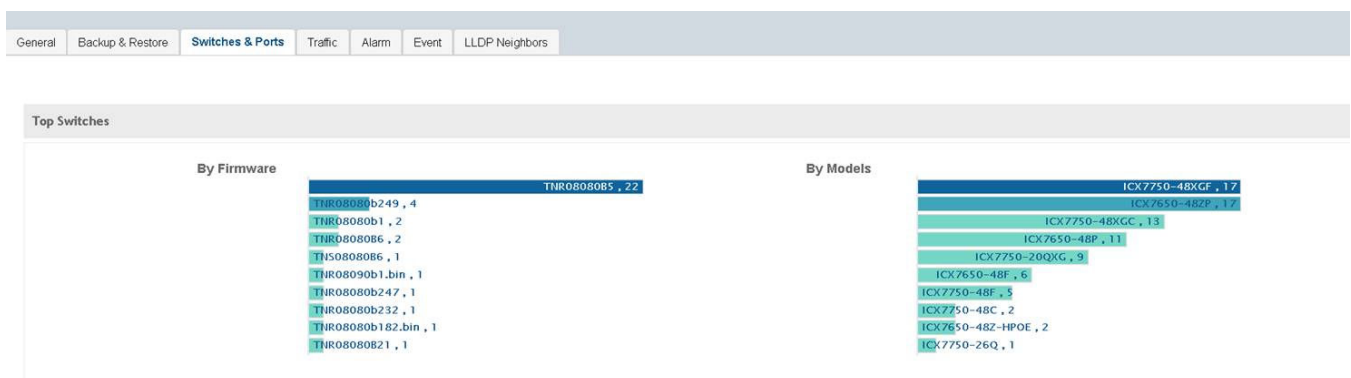
1. From the left pane, select **Switches**.

The **Switches** page is displayed.

2. Select the switch or group and click the **Ports** tab.

For a switch group, a **Top Switches** page similar to the following figure is displayed. The graphs provide information on top switches based on firmware and model.

FIGURE 116 Top Switches Page



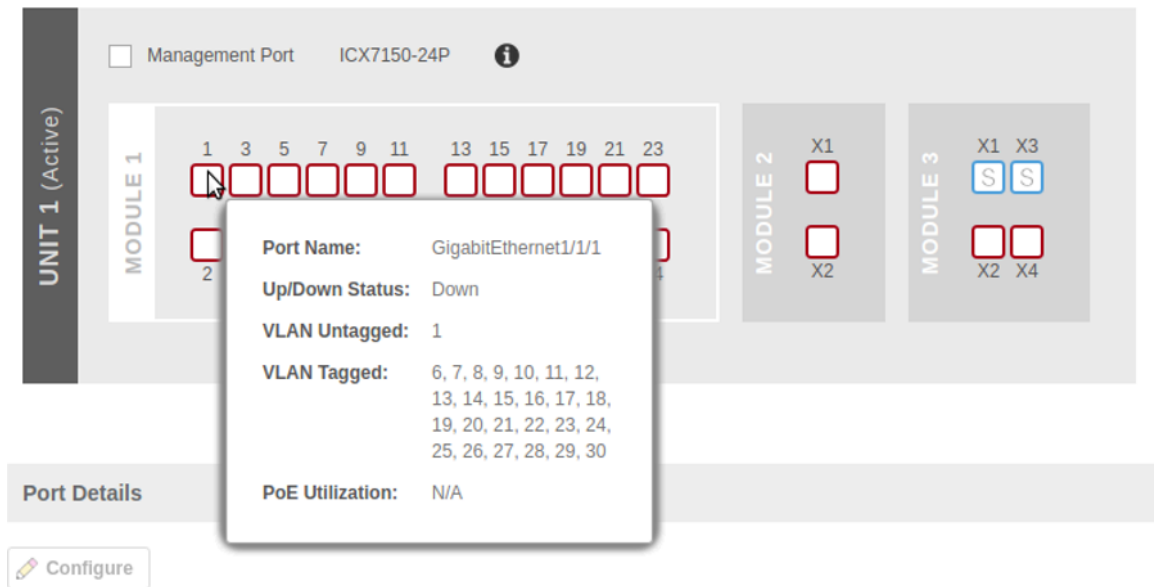
For standalone switches, the **Ports Summary** page is displayed in the **Ports** tab as shown in the following figure. The **Ports Summary** page provides information on the ports for the selected switch or group, including the total number of ports connected to the switch or stack, the number of ports 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 117 Ports Summary

| Switch Name | MAC Address | Model | IP Address | Status | Ports | Alarm | Uptime | Firmware | Serial Number | Last Firmware Update |
|--------------------|-------------------|-------------|----------------|---------|-------|-------|---------------------|------------------|---------------|----------------------|
| ICX7150-48P Router | 60:9C:9F:B8:84:EC | ICX7150-48P | 10.176.187.208 | Online | 54 | 0 | 18 days, 7:00:13.00 | SPR08090a | BTC3243M00J | N/A |
| ICX7250-48 Router | 78:A6:E1:01:FC:5C | ICX7250-48 | 10.176.187.235 | Offline | 56 | 1 | 22:13:08.00 | SPR08090a.bin | DUJ3848N017 | N/A |
| N/A | CC:4E:24:B4:8E:74 | ICX7250-24 | 26.1.1.26 | Offline | 0 | 1 | N/A | SPR08090a_b34... | DUN3204L008 | N/A |
| cloud-switch | CC:4E:24:DE:16:BE | ICX7250 | 10.176.187.210 | Offline | 64 | 1 | 7 days, 0:42:02.00 | SPR08092dev.bin | DUN3245K012 | N/A |
| N/A | CC:4E:24:B4:24:9C | ICX7250-48 | 10.176.189.23 | Offline | 0 | 1 | N/A | SPR08090a.bin | DUP3245K01F | 2019/03/07 |
| ICX7250-48P Router | CC:4E:24:B4:2D:C0 | ICX7250-48P | 10.176.187.201 | Offline | 56 | 1 | 5:20:02.00 | SPR08090dev.bin | DUQ3245K00X | N/A |
| ICX7150-24 Router | 60:9C:9F:F4:F4:D4 | ICX7150-24 | 10.176.155.13 | Offline | 30 | 1 | 2 days, 0:46:25.00 | SPR08090 | FEG321P01X | 2019/03/01 |

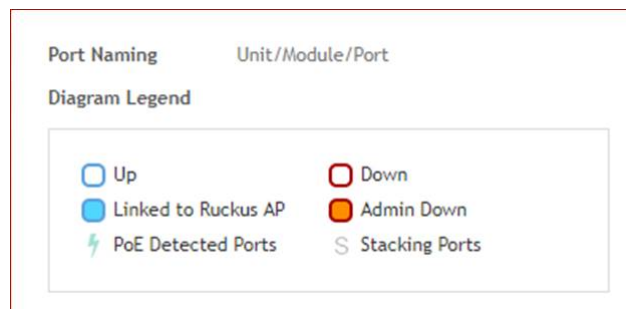
- Click the switch name to view the **Front Panel View** page for additional port information as shown in the following figure. The **Front Panel View** page provides information on the state of all ports in each switch module, for example port Up, Down, or Administratively Down. Additional port details can be seen by hovering the mouse over the port.

FIGURE 118 Front Panel View



The following figure shows the diagram legend used in the Front Panel View page.

FIGURE 119 Diagram Legend



The following list further describes items in the Front Panel 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 name to view the **Port Details** page as shown in the following figure.

FIGURE 120 Port Details

| 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 Gb... | | | 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:

NOTE

Ports for switch stacks are not configurable from the **Port Details** page.

- **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 VLANs 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 (Type):** 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 the received side. A CRC error usually indicates network transmission problems.

- **In Discard:** The number of inbound packets that were chosen to be discarded (even though no errors are detected) to prevent their being deliverable to a higher-layer protocol. One reason 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.

NOTE

In this release only forming a LAG through the controller web user interface is supported. The system does not support configuring LAG interface detail through the controller web user interface. To configure detail settings for LAG after form it, you need to configure it through Switch console directly.

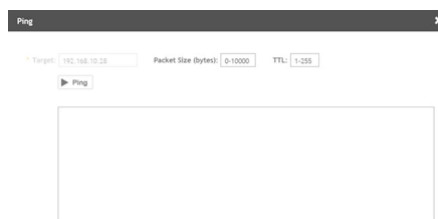
Viewing Switch Health

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 **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 121 Pinging the switch



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

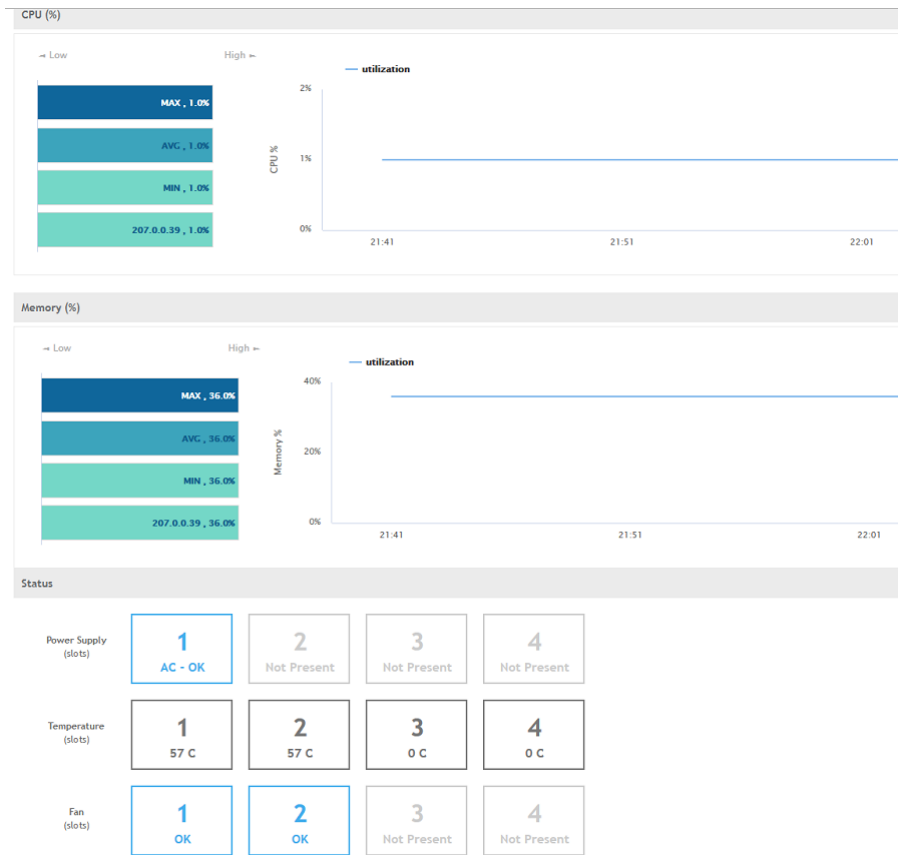
6. On the **Trace Route** page, enter the TTL (Time to Live) value after which the packet is discarded from the network.
As shown in the following example, the page displays the IP address of the hops the packet takes as it traverses the network between the switch and the controller.

FIGURE 122 Tracing the packet route through the network




7. 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 123 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 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 **Switches** page appears.

- Select the switch or group. Then select the **Alarms** tab.


FIGURE 124 Switches 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 **Switches** page appears.
2. Select the switch or group. Then select the **Events** tab.


FIGURE 125 Switches 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 **Switches** page appears.
2. Select the switch or group. Then select the **LLDP Neighbors** tab.

FIGURE 126 LLDP Neighbors Connected to the Switch

| Device Name | Remote MAC | Device Type | Remote Port | Local Port | Local IPAC | Remote Device Description |
|-------------|-------------------|---------------------|-------------|----------------------|---------------------|--|
| RuckusAP | 48:1d:8c:1a:61:40 | Bridge, 802.11ac... | 4818 | GigabitEthernet2/1/6 | 10.0.0.11:10.0.0.23 | Ruckus 802.11ac Media Networks Wireless AP7500 Version: 1.6.R.0.09 |
| RuckusAP | 48:1d:8c:1a:61:40 | Bridge, 802.11ac... | 4818 | GigabitEthernet2/1/4 | 10.0.0.11:10.0.0.30 | Ruckus 802.11ac Media Networks Wireless AP7500 Version: 1.6.R.0.09 |
| RuckusAP | 48:1d:8c:1a:61:40 | Bridge, 802.11ac... | 4818 | GigabitEthernet2/1/7 | 10.0.0.11:10.0.0.38 | Ruckus 802.11ac Media Networks Wireless AP7500 Version: 1.6.R.0.09,1944201 |
| RuckusAP | 48:1d:8c:1a:61:40 | Bridge, 802.11ac... | 4818 | GigabitEthernet2/1/5 | 10.0.0.11:10.0.0.34 | Ruckus 802.11ac Media Networks Wireless AP7500 Version: 1.6.R.0.09 |

| Device Name | Remote MAC | Device Type | Remote Port | Local Port | Local IPAC | Remote Device Description |
|-----------------|-------------------|---------------------|------------------------|----------------------|---------------------|--|
| SR02-C08E | 40:1c:9f:c3:6a:10 | Bridge, Router | 40gigabitEthernet1/1/2 | GigabitEthernet2/1/8 | 10.0.0.11:10.0.0.4 | 802 |
| POE1 | 00:3c:12:1f:6c:05 | Bridge, Router | FastEthernet2/1/1 | GigabitEthernet2/1/8 | 10.0.0.11:10.0.0.30 | OS9722P 24 Port Gigabit Layer 2 PoE Managed Switch with Static Routing |
| sub-vlan84@core | 18:03:79:a6:76:18 | Bridge, 802.11ac... | sws84 | GigabitEthernet2/1/8 | 10.0.0.11:10.0.0.30 | Ubiquiti 16.04.2 LTS Linux 4.4.0-28-generic #99-Ubuntu SMP Thu Apr 27 10:28:09 UTC 2017 x86_64 |
| sub-vlan84@core | 18:03:79:a6:76:18 | Bridge, 802.11ac... | sws84 | GigabitEthernet2/1/8 | 10.0.0.11:10.0.0.30 | Ubiquiti 16.04.2 LTS Linux 4.4.0-28-generic #99-Ubuntu SMP Thu Apr 27 10:28:09 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 **Switches** page appears.

2. Select the switch or group. Then select the **Traffic** tab.

FIGURE 127 Traffic Trend for a Switch

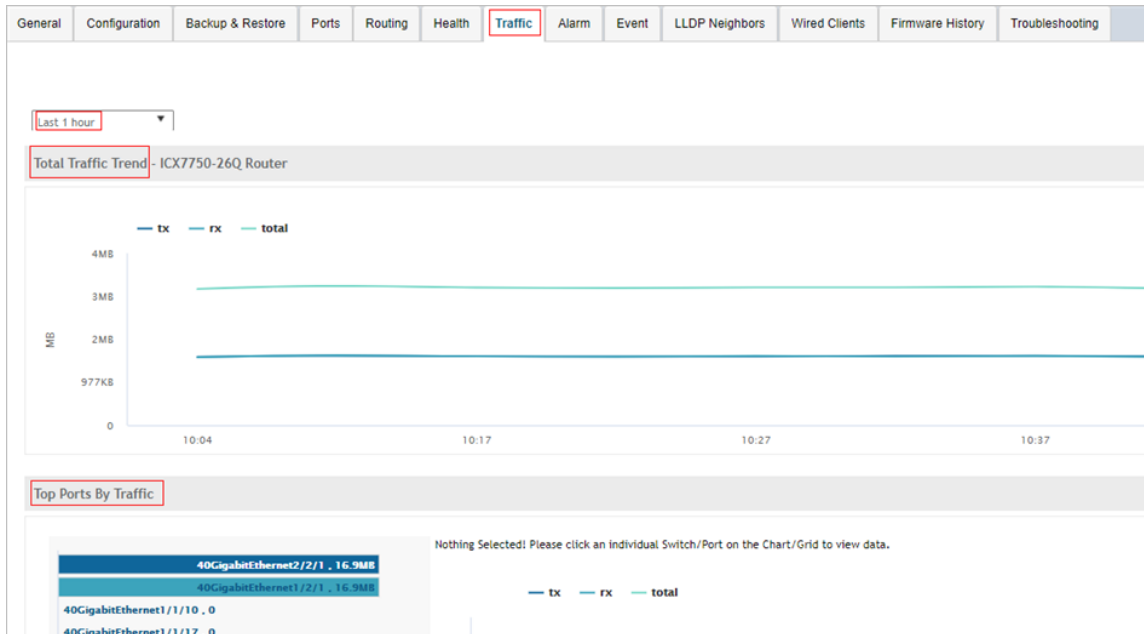


FIGURE 128 Showing Total Multicast Traffic Trend

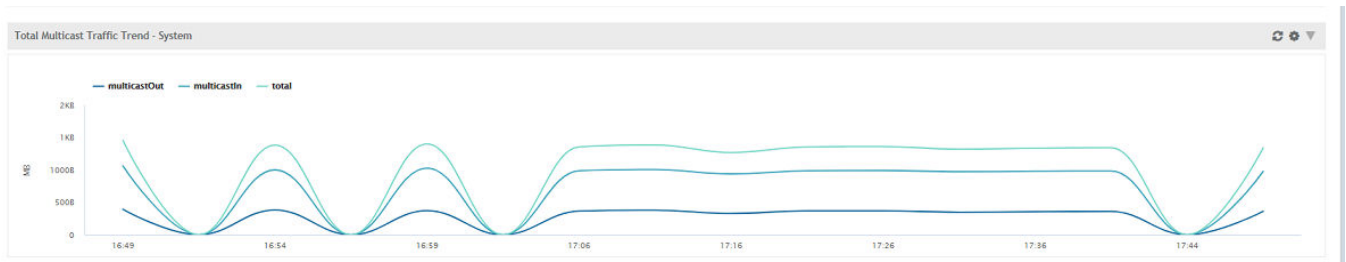
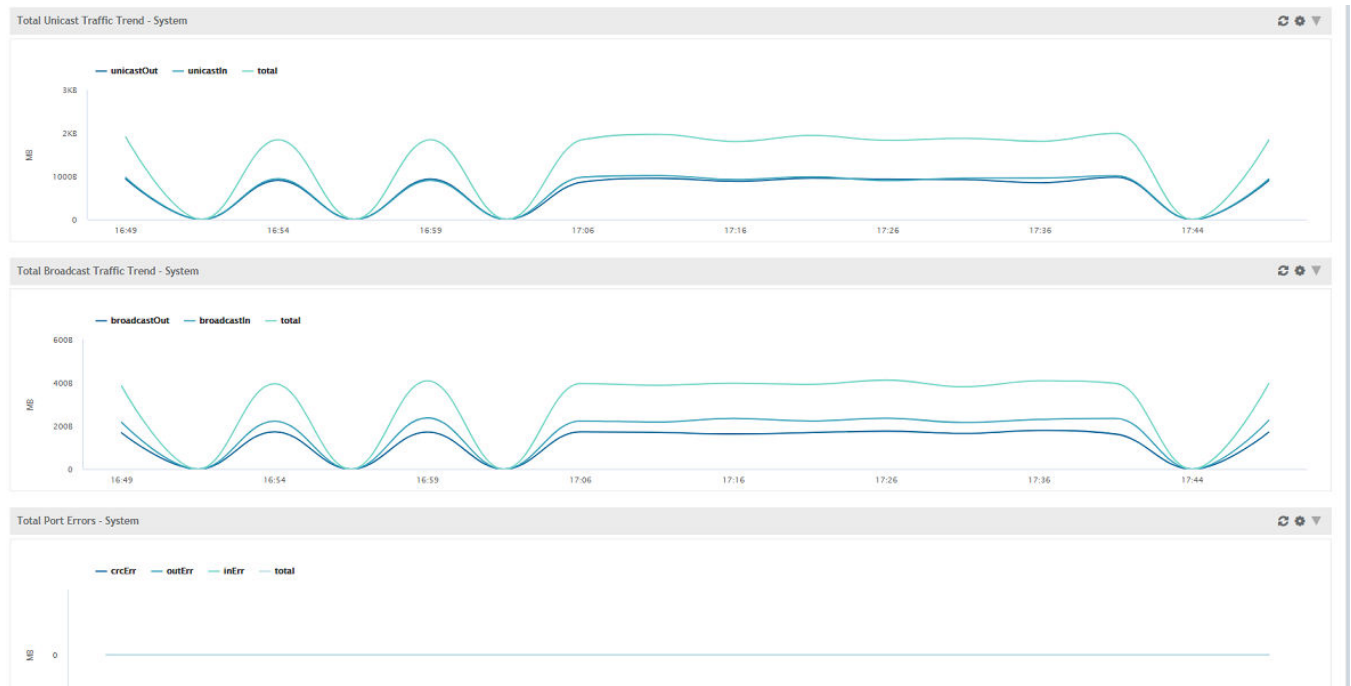


FIGURE 129 Showing Unicast, Broadcast and Port Errors Traffic Trends



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.
- **Total Multicast Traffic Trend:** Provides a graphical representation of the multicast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming multicast data packets (multicastIn) and total number of outgoing multicast packets (multicastOut) by the group in MB, at a certain time and date.
- **Total Unicast Traffic Trend:** Provides a graphical representation of the unicast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming unicast data packet (unicastIn) and total number of outgoing unicast packet (unicastOut) by the group in MB, at a certain time and date.
- **Total Broadcast Traffic Trend:** Provides a graphical representation of the broadcast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming broadcast data packets (broadcastIn) and total number of outgoing broadcast packets (broadcastOut) by the group in MB, at a certain time and date.
- **Total Port Errors:** Provides a graphical representation of the port errors over a period of time in the switch or switch group. It also indicates the total number of inbound packets that contained errors (inErr) and total number of outbound packets that could not be transmitted because of errors (outErr) by the group in MB, at a certain time and date.

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 208

1. From the left pane, select **Switches**.
The **Switches** page appears.
2. Select the switch or group. Then select the **Firmware History** tab.
The **Firmware History** tab is displayed.

FIGURE 130 Viewing Firmware History

| Time | Switch ID | Firmware Version | Image Name | Status | Failure Reason |
|---------------------|---------------|------------------|---------------|-----------|----------------|
| 2018/05/04 14:08:58 | CC4E24A77478D | 8307 | SPR08000207u6 | Completed | N/A |
| 2018/05/04 21:03:20 | CC4E24A77478D | 8302 | SPR08000202u6 | Completed | N/A |

| Time | Firmware Version |
|---------------------|---------------------------|
| 2018/05/04 14:08:58 | SPR08000202 → SPR08000207 |
| 2018/05/04 21:03:20 | SPR08000111 → SPR08000202 |

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 previous upgrade operations, and firmware versions to which the upgrade was done.

Configuring the Group Firmware Settings

The Group Firmware Settings allows the user to select default firmware for the switch group. The newly joined switch is upgraded to the selected firmware in the switch group.

NOTE

The default firmware selection at group level does not trigger upgrade for the existing switches in the switch group, it only triggers upgrade for newly joined switch(es)

Complete the following steps to perform the firmware upgrade of newly added switch in the switch group to the default firmware version.

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


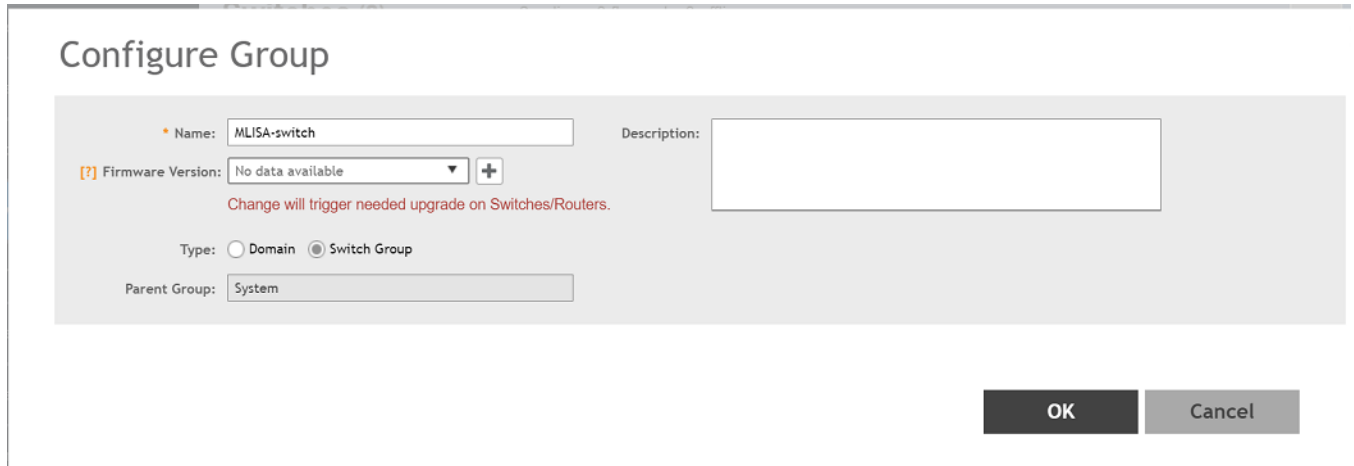
2. From the **Switches** page, select the switch group that you want to configure, and click 
The **Configure Group** page appears.

FIGURE 131 Configuring the Switch with Default Version

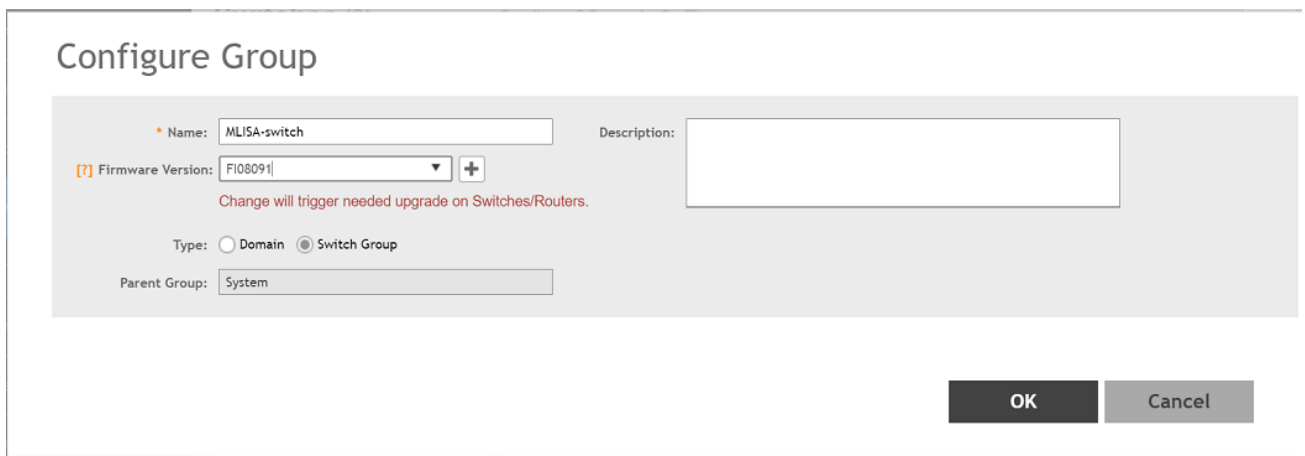


The screenshot shows the 'Configure Group' page with the following fields and options:

- Name:** MLISA-switch
- Description:** (empty text box)
- Firmware Version:** No data available (dropdown menu with a plus icon)
- Change will trigger needed upgrade on Switches/Routers.** (red text)
- Type:** Domain Switch Group
- Parent Group:** System
- Buttons:** OK and Cancel

3. In the **Configure Group** page, configure the following.
 - a) **Name:** Type the name of the switch group that you want to create.
 - b) **Description:** Enter a brief description for the switch group
 - c) **Firmware version:** Select firmware version from the list or retain the default firmware version.

FIGURE 132 Configuring the switch with Firmware version



The screenshot shows the 'Configure Group' page with the following fields and options:

- Name:** MLISA-switch
- Description:** (empty text box)
- Firmware Version:** F108091 (dropdown menu with a plus icon)
- Change will trigger needed upgrade on Switches/Routers.** (red text)
- Type:** Domain Switch Group
- Parent Group:** System
- Buttons:** OK and Cancel

NOTE

The group firmware settings requires switches to be running SmartZone 5.2.1 or later.

- d) **Parent Group:** Displays the parent group under which the switch group resides
4. Click **OK**.

Accessing the switch CLI through SmartZone (Remote CLI)

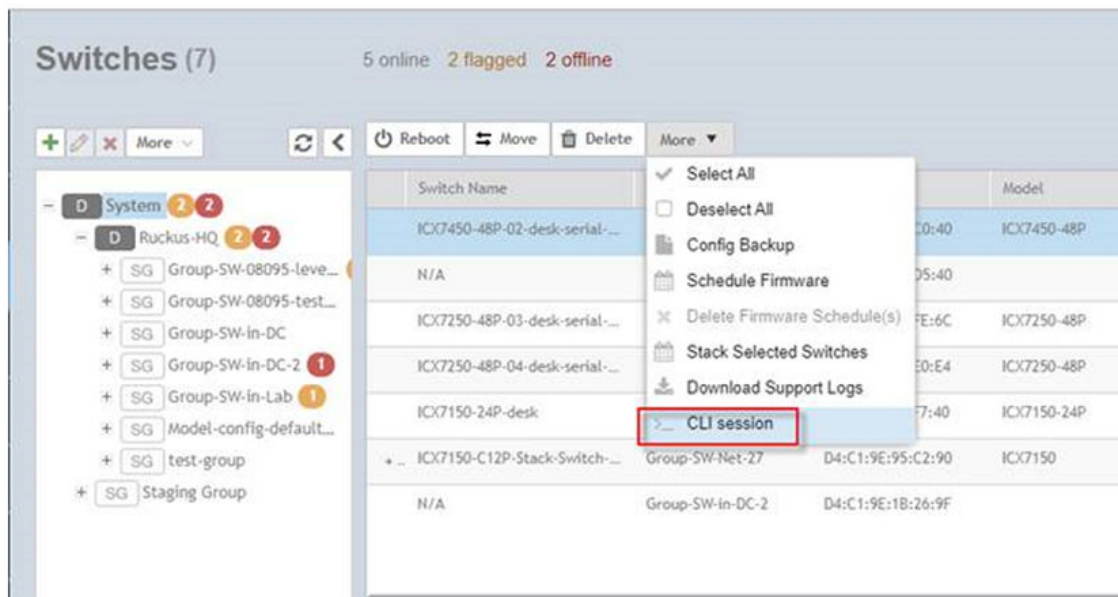
SmartZone 5.2.1 introduces this essential feature that allows you to directly access the Switch CLI prompt from within SmartZone Web Interface. The Remote CLI allows you to establish a secure connection between SmartZone and ICX that can span over Internet, and eliminate the need to open VPN connection to switch's network when trying to access CLI through SSH or Telnet.

The SmartZone administrator must complete the following steps to access a CLI session.

1. From the controller web interface, select **Switches** from the left navigation pane.
The **Switches** page is displayed.
2. From the **Switches** page, select a switch.

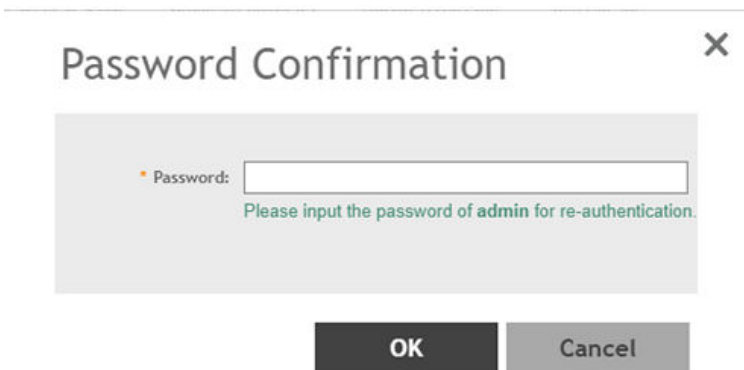
3. Click **More**, and select **CLI session**.

FIGURE 133 Selecting CLI Session



The **Password Confirmation** dialog box is displayed.

FIGURE 134 Logging into the CLI Session



SmartZone Switch Management

Accessing the switch CLI through SmartZone (Remote CLI)

4. Enter the administrator password.

After login, it takes approximately five seconds to set up a secure session within the secure tunnel established between switch and controller to access switch.

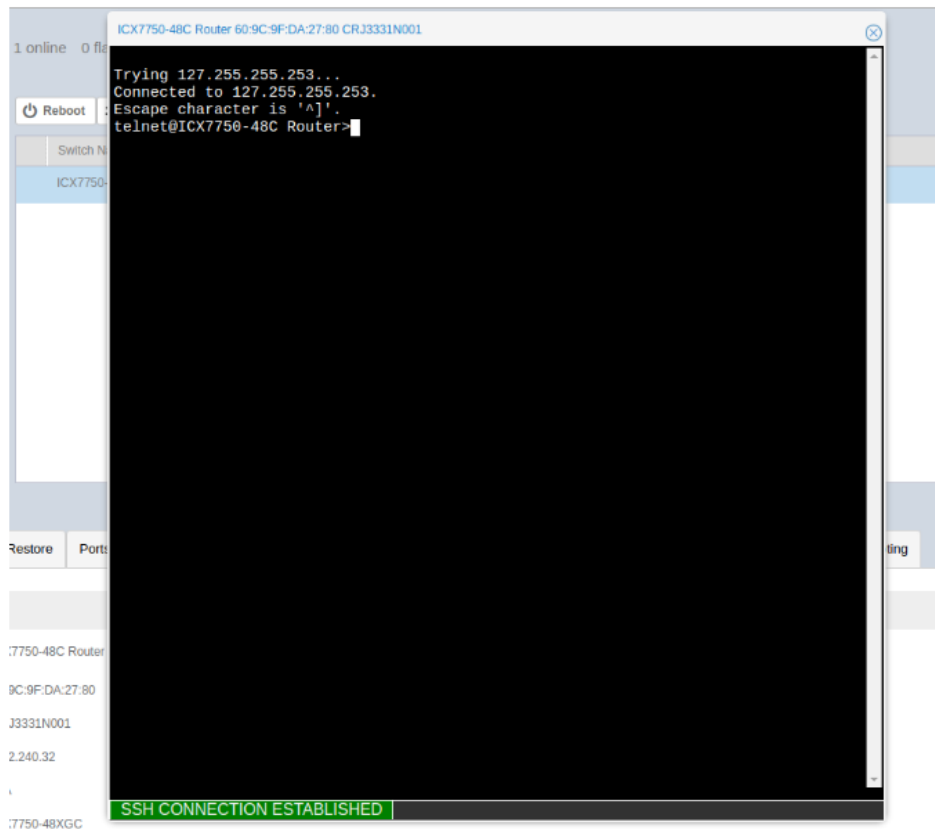
A CLI Window is displayed.

NOTE

You do not need to enable telnet server on ICX switches to use Remote CLI.

However, if telnet authentication is enabled on the switch, you will be prompted to enter the credentials when opening CLI session via SmartZone. The credentials depend on the type of authentication defined on the switch (local user, RADIUS etc.).

FIGURE 135 Accessing Switch Through the CLI Sesion



SmartZone Switch Management

Viewing PoE Utilization and Health Status of the Switch

2. Select a stack switch.

FIGURE 137 Selecting a Stack Switch

| Switch Name | MAC Address | IP Address | Status | PoE Utilization (watt) | Registration State | Ports | Port Status | Alarm | Uptime | Serial Number |
|--------------------|-------------------|---------------|--------|------------------------|--------------------|-------|-------------|-------|-----------------|---------------|
| Allwise_stack | 60:9C:9F:8C:14:AC | 10.177.155.26 | Online | 0.00 / 1110.00 W | Approved | 86 | 6 0 0 | 0 | 4:25:30 | BSY2258M00T |
| ICX7450-48P Router | 60:9C:9F:26:8C:20 | 10.177.155.23 | Online | 0.00 / 748.00 W | Approved | 54 | 0 0 0 | 1 | 2 days, 6:12:53 | CYR3344L00T |
| ICX7250-48 Router | CC:4E:24:E5:F2:4A | 10.177.155.24 | Online | N/A | Approved | 56 | 1 0 55 | 0 | 1 day, 9:19:06 | DUJ3851L0CE |
| Spatha_stack | 60:9C:9F:1D:C8:80 | 10.177.155.28 | Online | 46.20 / 2244.00 W | Approved | 146 | 7 0 2 | 5 | 1 day, 5:22:31 | EAR3306M00W |

3. Click the **Health** tab to view the health status such as the power supply status, temperature, and fan status, of the stack switch.

FIGURE 138 Viewing the Health Status of Stack Switch

| Category | 1 | 2 | 3 | 4 |
|----------------------|--------------|------------------|------------------|------------------|
| Power Supply (Watts) | 1 AC - OK | 2 Not Present | 3 Not Present | 4 Not Present |
| Temperature (Watts) | 1 46 °C | 2 34 °C | 3 Not Present | 4 Not Present |
| Fan (Watts) | 1 OK | 2 OK | 3 Not Present | 4 Not Present |


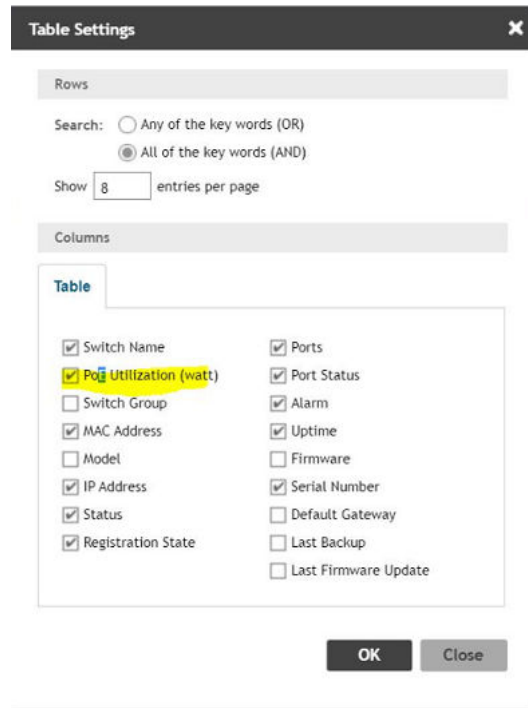
- To enable the PoE Utilization, click  .
The **Table Settings** page is displayed.

FIGURE 139 Enabling the PoE Utilization



- Select a **Stack Switch**, to view the details in the **PoE Utilization (watt)** field.

FIGURE 140 Viewing the PoE Utilization Field

| Switch Name | MAC Address | IP Address | Status | PoE Utilization (watt) | Registration State | Ports | Port Status | Alarm | Uptime | Serial Number |
|--------------------|-------------------|---------------|--------|------------------------|--------------------|-------|-------------|-------|-----------------|---------------|
| Alinlon_stack | 60:9C:9F:8C:14:AC | 10.177.155.26 | Online | 0.00 / 1110.00 W | Approved | 86 | 6 0 0 | 0 | 4:25:30 | BSY3238M00T |
| IC17450-48P Router | 60:9C:9F:26:8C:20 | 10.177.155.23 | Online | 0.00 / 748.00 W | Approved | 54 | 0 0 6 | 1 | 2 days, 6:12:53 | CYR3344L00T |
| IC17250-48 Router | CC:4E:24:E5:F2:4A | 10.177.155.24 | Online | N/A | Approved | 56 | 1 0 55 | 0 | 1 day, 9:19:06 | D113851L0CE |
| Spatha_stack | 60:9C:9F:1D:C8:80 | 10.177.155.28 | Online | 46.20 / 2244.00 W | Approved | 146 | 7 0 2 | 5 | 1 day, 5:22:31 | EAR3306M00W |

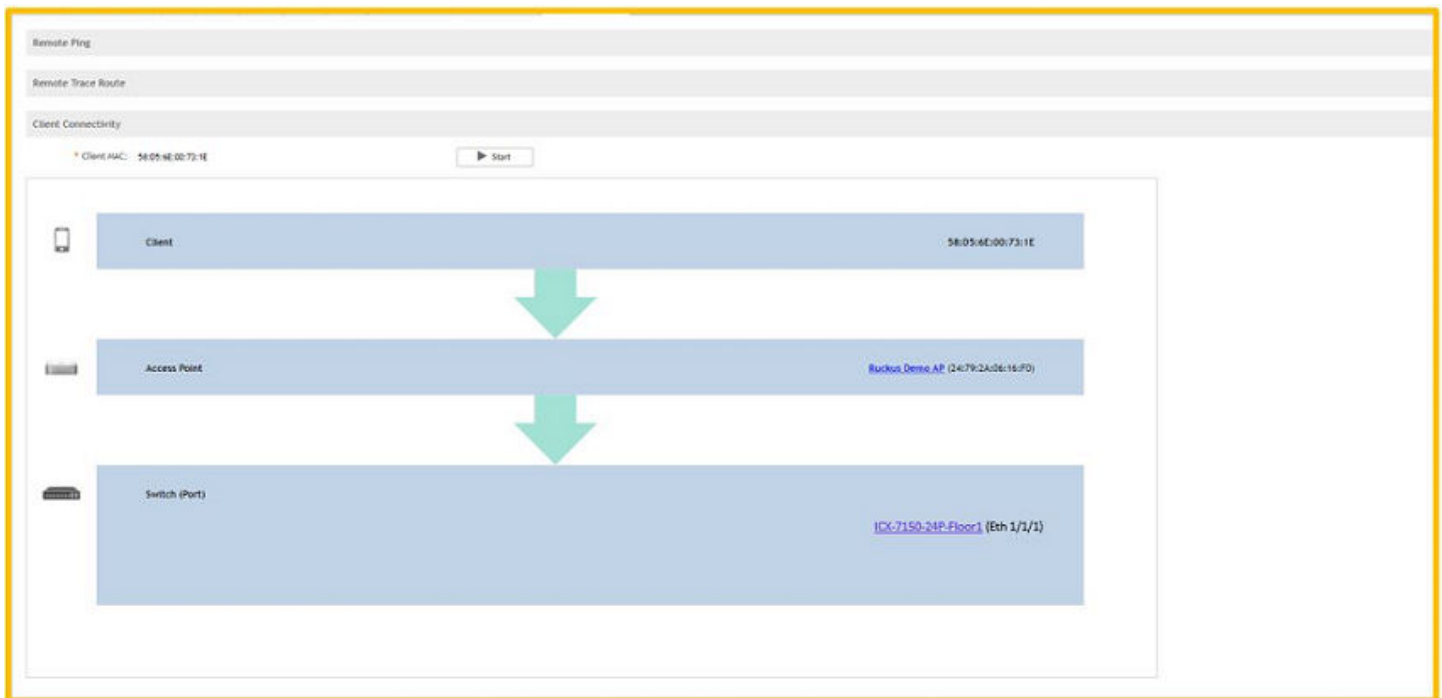
Troubleshooting Switch Issues

- [Troubleshooting Using Custom Events.....](#) 268
- [Troubleshooting Using Remote Operations.....](#) 269

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 141 Client MAC Search

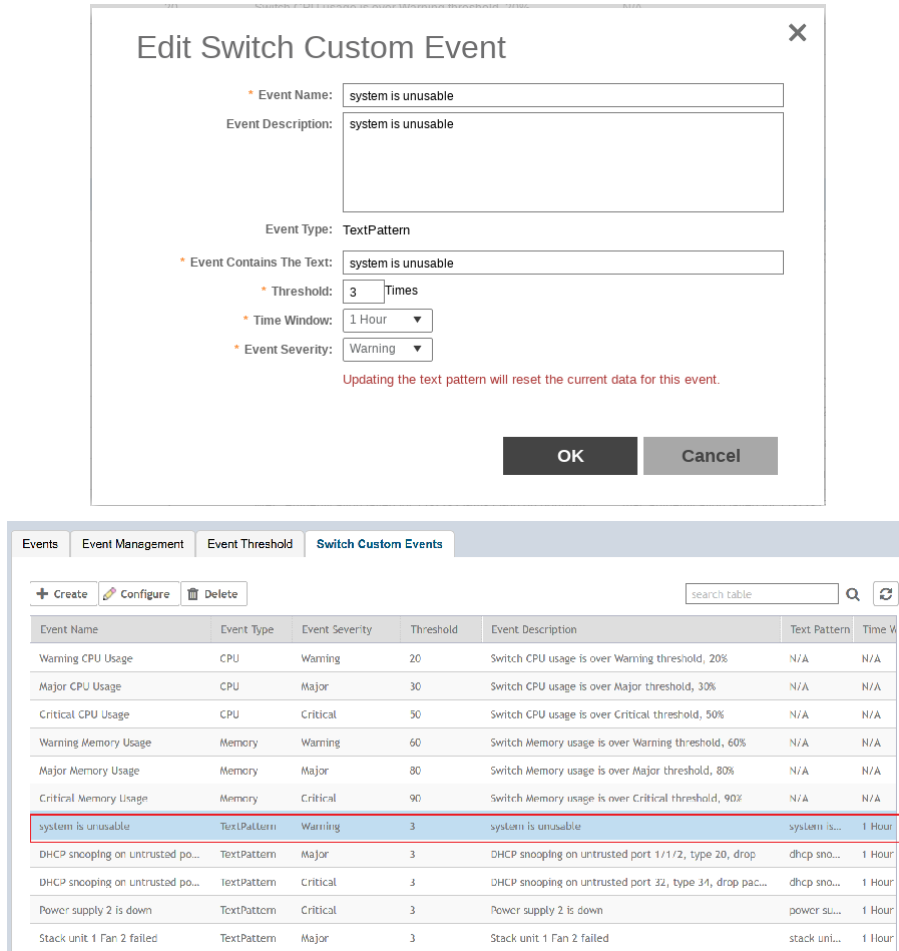


Troubleshooting Using Custom Events

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 497

FIGURE 142 Troubleshooting switch issues through custom events



NOTE

It is quite common that entry level switches like ICX 7150 use up 70-80% of the available memory. You can modify the thresholds for memory usage custom events to a higher limit in such cases.

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.

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

The **Switches** page is displayed.

2. Select a switch.

3. Click the **Troubleshooting** tab.

4. Click **Remote Ping**.

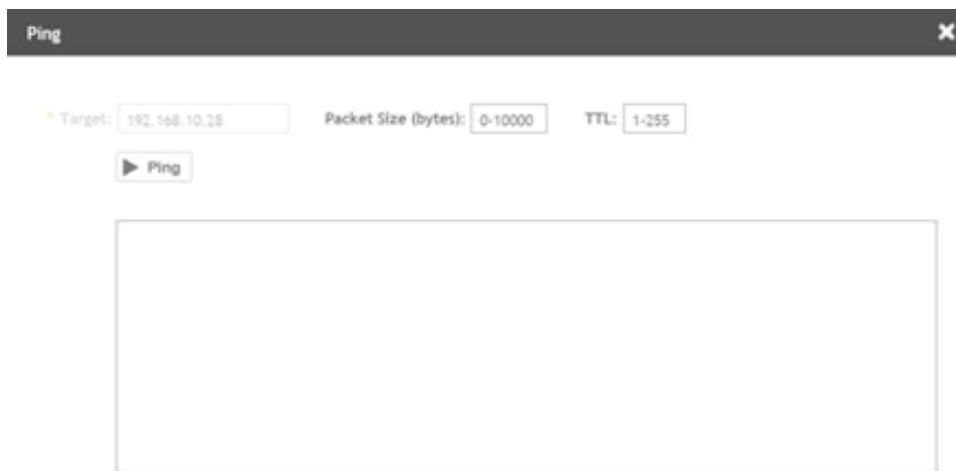
The **Ping** page is displayed.

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 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 143 Pinging the switch



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 144 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 displays charts illustrating traffic trends.

1. From the SmartZone interface, click **Dashboard** in the navigation pane.

The **Dashboard** page is displayed.

2. Click **Wired**.

The **Wired** page is displayed.

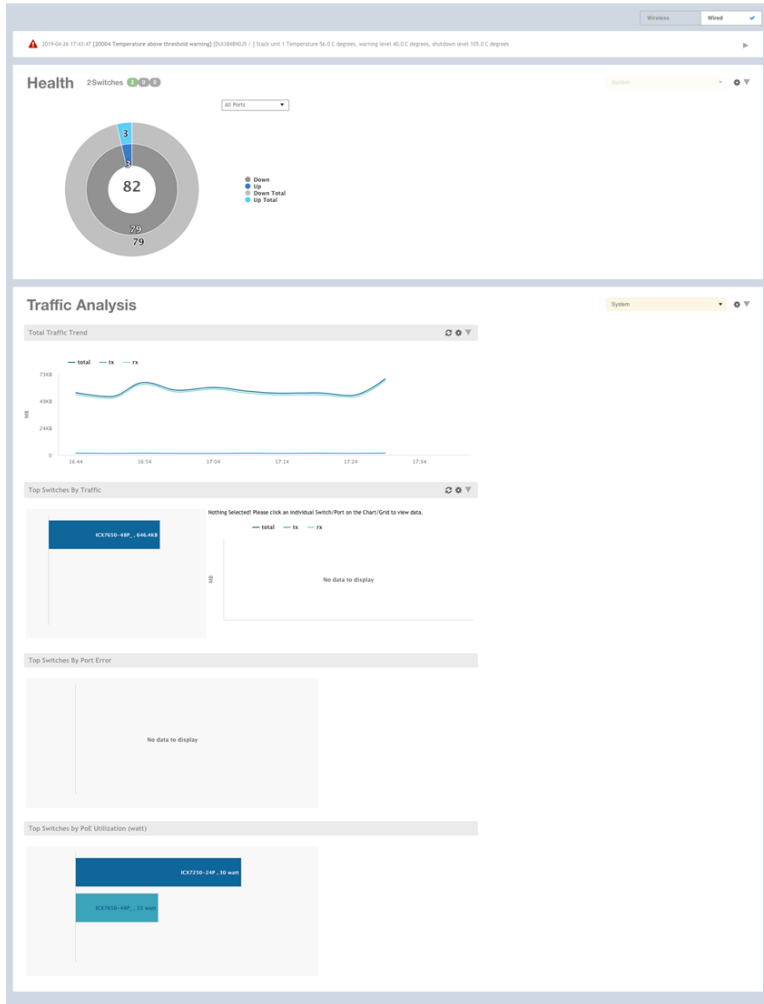
3. Click the Gear icon on the **Health** dashboard.

The **Settings-Health Dashboard** page is displayed.

4. Click the **Display** tab.

- From the **View Mode** , select either **Topology** or **Port** view to be displayed on the dashboard.

FIGURE 145 Showing Wired Devices Using Port View Mode



In the port view mode, the **Health** pane displays the number of switches that are online, offline, and flagged.

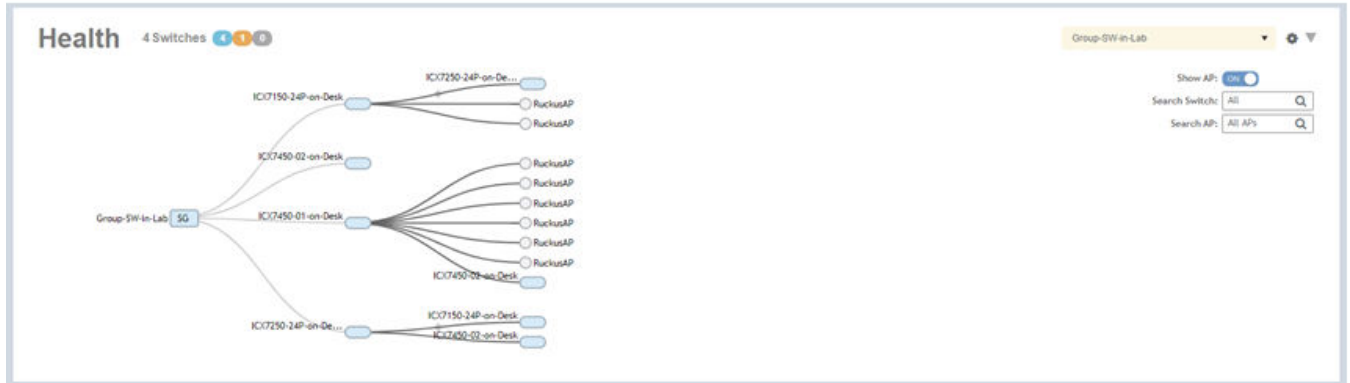
The **Health** pane also displays the number of ports for each port speed (1 Gbps, 2.5 Gbps, 10 Gbps, and so on) or all the ports, and indicates the status of the ports (Up, Down, Down by Admin, Down Total, and Up Total).

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

- Total Traffic Trend
- Top Switches By Traffic
- Top Switches By Port Error

- Top Switches by PoE Utilization (watt)

FIGURE 146 Showing Wired Devices Using Topology View Mode

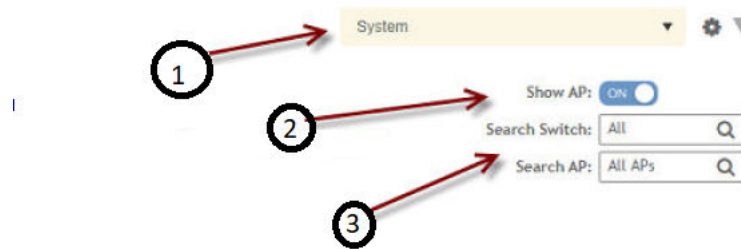


In the topology view mode, the **Health** pane consists of a filter combo box to display domain, sub-domain and switch group in the topology view. The **Show AP** button can be turned on or off to view either the switch or a combination of switch and AP, and **Search** box to search AP or switch based on the device name and MAC address. If you pause the pointer on a link in the topology view, the highlighted link shows the port and LAG information. If you pause the pointer on a device, the highlighted device shows device information such as name, model, MAC address, and IP address (for the switch only).

NOTE

The **Health** dashboard refreshes automatically every 15 minutes to show the latest topology view.

FIGURE 147 Showing Elements on the Health Dashboard



- 1 - Filter
- 2 - Topology Type Switch Button
- 3 - Search Bar

Working with WLANs and WLAN Groups

- Domains, Zones, AP Groups, and WLANs..... 275
- Viewing Modes..... 275
- Creating a WLAN Domain for an MSP..... 276
- WLAN Groups..... 276
- Creating a WLAN Configuration..... 277
- Managing WLANs..... 301

Domains, 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:

- Domains—Geographical grouping for regulatory operation.
- Zones—Comprises of multiple WLAN groups
- WLAN Groups—Comprises of multiple WLANs
- WLANs—Wireless network service

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**

Creating a WLAN Domain for an MSP

A Managed Services Provider (MSP) manages and assumes a defined set of responsibility. You can create an MSP managed domain, to manage all their settings within that domain. You can also limit the number of APs per zone. Refer, [Limiting the Number of APs in a Domain or Zone on page 70](#).

To create a WLAN Domain for an MSP:

1. From the Wireless LANs Page, select **System** from the tree hierarchy.
2. Click the **Create**  button, the Create Group form appears.
3. Configure the following details:
 - a. Enter a **Name** for the domain.
 - b. Enter a **Description** about the domain.
 - c. By default, the **Type** selected is **Domain**.
 - d. The **Parent Group** displays the group to which this domain will be tagged.
 - e. In **Managed by Partner**, select the **Enable** check box.
4. Click **OK**. You have created a new WLAN domain. In the left pane, the new   MSP domain appears.

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 277.

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

Complete the following steps to create a WLAN configuration.

Allows

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

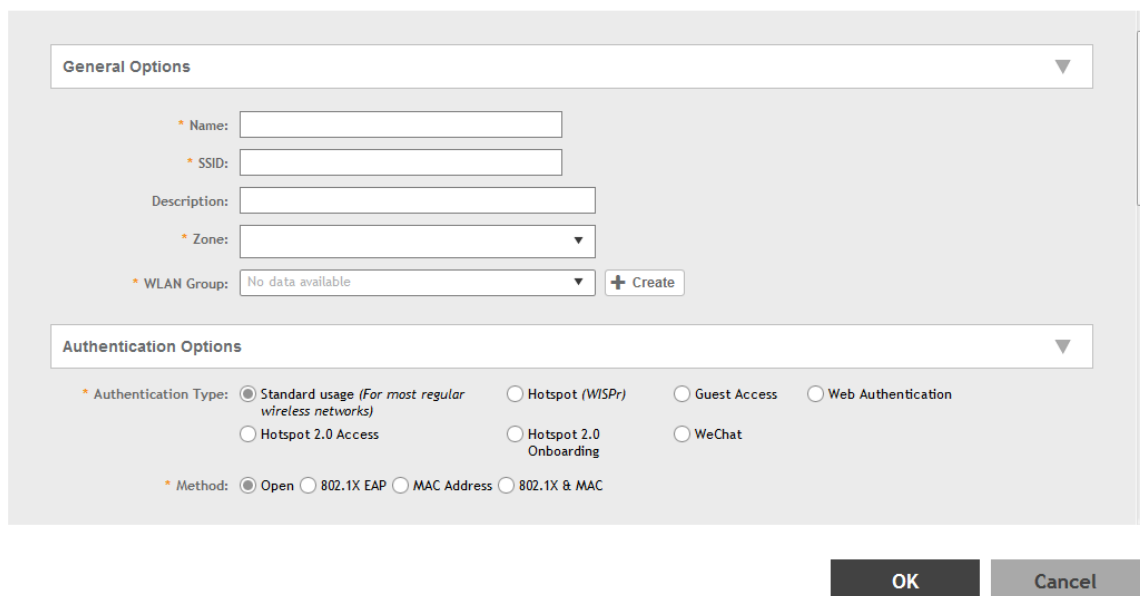
FIGURE 148 Wireless LANs



2. Click **Create** and the **Create WLAN Configuration** page is displayed.

FIGURE 149 Create WLAN Configuration

Create WLAN Configuration



3. Set the required configurations as explained in the following table.

TABLE 57 WLAN Configurations

| Field | Description | Your Action |
|-------------------------------|--|---|
| General Options | | |
| Name | Indicates the user-friendly administrative name for the WLAN. | Enter a name. |
| SSID | Indicates the SSID for the WLAN. | Enter the SSID. |
| Description | Indicates a user-friendly description of the WLAN's settings or function. | Enter a short description. |
| Zone | Indicates the zone to which the WLAN configuration applies. | Select the zone to which the WLAN settings apply. |
| WLAN Groups | Indicates the WLAN groups to which the WLAN applies. | Select the WLAN groups to which the WLAN configuration applies. |
| Authentication Options | | |
| Authentication Type | <p>Defines the type of authentication flow for the WLAN.</p> <p>NOTE 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"> • Standard Usage—This is a regular WLAN suitable for most wireless networks. • Hotspot (WISPr)—Click this option if want to use a hotspot service (use this type for external captive portal workflows) or WISPr. <ul style="list-style-type: none"> NOTE Hotspot (WISPr) applies to WLAN traffic that is tunneled and not tunneled. • Guest Access—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. For more information about Hotspot 2.0 online signup, see the Hotspot 2.0 Reference Guide for this release. • Web Authentication—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. • Hotspot 2.0 Access—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. • Hotspot 2.0 Onboarding—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. • WeChat—Click this option if you want the WLAN usage through WeChat. |
| Authentication Options | | |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|---------------------------|---|--|
| Method | Specifies the authentication mechanism. | <p>Select the following option:</p> <ul style="list-style-type: none"> • Open (Default)—No authentication mechanism is applied to connections. If WPA or WPA2 encryption is used, this implies WPA-PSK authentication. If you clicked Web Authentication in Authentication Type, Open is the only available authentication option, even though PSK-based encryption can be supported. • 802.1X EAP—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 Enable RFC Location Delivery Support for Authentication & Accounting Server, enter the Operator Realm. 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. • MAC Address—Authenticate clients by MAC address. <ul style="list-style-type: none"> – MAC Authentication—Requires a RADIUS server and uses the MAC address as the user logon name and password. <ul style="list-style-type: none"> › Select Use user defined text as authentication password (default is device MAC address) and enter the format. – MAC Address Format—Choose the MAC address format from the drop-down menu. • 802.1X EAP & MAC—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 the two authentication methods succeed, the user equipment gains access to the WLAN. Authentication is handled by a back-end RADIUS server. When this authentication method is selected, the MAC Authentication and MAC Address Format fields will be shown within the Authentication Options section. |
| Encryption Options | | |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|---------------|--|--|
| Method | <p>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> | <p>Select the option:</p> <ul style="list-style-type: none"> • WPA2—Enhanced WPA encryption using AES encryption algorithm. <ul style="list-style-type: none"> a. Choose Algorithm: <ul style="list-style-type: none"> – AES: <ol style="list-style-type: none"> 1. Enter Passphrase. 2. Select or clear Show. 3. Select <ul style="list-style-type: none"> › the Enable 802.11 Fast BSS Transition check box and enter the Mobility Domain ID. › the required 802.11w MFP option. 4. Dynamic PSK <ul style="list-style-type: none"> › Disable › Internal <ol style="list-style-type: none"> a. Enter DPSK Length b. Choose DPSK Type c. Select DPSK Expiration › External—Enables Authentication Service – AUTO: <ol style="list-style-type: none"> 1. Enter Passphrase. 2. Select or clear Show. • WPA3—Enhanced WPA3 encryption using AES encryption algorithm. <ul style="list-style-type: none"> a. Choose Algorithm: <ul style="list-style-type: none"> – AES: <ol style="list-style-type: none"> 1. Enter Passphrase. 2. Select or clear Show. 3. In the 802.11w MFP field, " Required" is the default selected option. – AES-GCMP-256: <ul style="list-style-type: none"> › NOTE WPA3-Enterprise cannot be supported by the 802.11ac Wave-1 AP models. • WPA2/WPA3-Mixed Encryption - Allows mixed networks of WPA2- and WPA3-compliant devices using AES algorithm. <ul style="list-style-type: none"> a. 1. Choose Algorithm: <ul style="list-style-type: none"> – AES: <ol style="list-style-type: none"> a. Enter Passphrase. b. Enter SAE Passphrase c. Select or clear Show. d. In the 802.11w MFP field, " Capable" is the default selected option b. Choose Algorithm: <ul style="list-style-type: none"> – AES: <ol style="list-style-type: none"> 1. Enter Passphrase. 2. Enter SAE Passphrase 3. Select or clear Show. • Opportunistic Wireless Encryption Encryption (OWE) - Allows the encryption without the manual input the passphrase using AES algorithm. <ul style="list-style-type: none"> a. Choose Algorithm <ul style="list-style-type: none"> – AES: In the 802.11w MFP field, " Required" is the default selected option. |

TABLE 57 WLAN Configurations (continued)



| Field | Description | Your Action |
|--|---|--|
| Data Plane Options | | |
| Access Network | Defines the data plane tunneling behavior. | Enable Tunnel WLAN traffic through Ruckus GRE . Configure the following options as appropriate: <ul style="list-style-type: none"> • GRE Tunnel Profile: Manages AP traffic. Select the profile from the list. • Split Tunnel Profile: 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. |
| Core Network | Defines the network mode. | Select the option: <ul style="list-style-type: none"> • Bridge • L2oGRE • TTG+PDG |
| vSZ-D DHCP/NAT | Enables tunneling option for DHCP/NAT. | Select the required check boxes: <ul style="list-style-type: none"> • Enable Tunnel NAT • Enable Tunnel DHCP |
| RADIUS based DHCP/NAT | Enables RADIUS-based DHCP/NAT settings. The DHCP server authorizes remote clients and allocates addresses based on replies from a RADIUS server. | Select the required check boxes: <ul style="list-style-type: none"> • Enable RADIUS based NAT • Enable RADIUS based DHCP |
| Flexi-VPN Profile | Enables forwarding of tunneled traffic to another remote DP instance through inter-DP RuckusGRE Tunnel (Flexi). | Select the profile from the list. |
| Authentication & Accounting Server (for WLAN Authentication Type: Standard usage) | | |
| Authentication Server | 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. | a. Select the Use controller as proxy check box. b. Select the server from the menu. c. Select Enable RFC Location Delivery Support . |
| Accounting Server | 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. | a. Select the Use controller as proxy check box. b. Select the server from the menu. |
| Hotspot Portal (for WLAN Authentication Type: Hotspot (WisPr)) | | |
| Hotspot (WISPr) Portal | Defines hotspot behavior such as redirects, session timers, and location information among others. | Select the hotspot portal profile that you want this WLAN to use. |
| Bypass CNA | Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN. | Select the Enable check box. |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|---|---|---|
| Authentication Service | Indicates the authentication server that you want to use for this WLAN. | <p>Choose the option. Options include Local DB, Always Accept, and any AAA servers that you previously added. Select:</p> <ul style="list-style-type: none"> • Use Controller as Proxy for the controller to proxy authentication messages to the AAA server • Use Realm-based profile to list contents the realm-based profile <p>When the SSH tunnel between the AP and the controller is down, you can enable Backup Authentication Service to back up the AP's authentication services to a secondary device.</p> <p>NOTE The customer portal must use AP WISPr ZD-Style API/ Backup AAA to continue to provide the WISPr service for WISPr survivability.</p> |
| Accounting Service | 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.</p> <p>Additionally, if you want the controller to proxy accounting messages to the AAA server, select the Use the Controller as Proxy check box.</p> <p>Select:</p> <ul style="list-style-type: none"> • Use Controller as Proxy for the controller to proxy authentication messages to the AAA server • Use Realm-based profile to list contents the realm-based profile <p>When the SSH tunnel between the AP and the controller is down, you can enable Backup Accounting Service to back up the AP's accounting services to a secondary device.</p> <p>NOTE The customer portal must use AP WISPr ZD-Style API/ Backup AAA to continue to provide the WISPr service for WISPr survivability.</p> |
| Guest Access Portal (for WLAN Authentication Type: Guest Access) | | |
| Guest Access Service | Indicates the guest access portal to be used on this WLAN. | Choose the guest portal service. |
| Bypass CNA | Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN. | Select the Enable check box. |
| Guest Authentication | Manages guest authentication. | <p>Select:</p> <ul style="list-style-type: none"> • Guest to require users to enter their guest pass credentials. Guest passes are managed directly on the controller. • Always Accept to allow users without guest credentials to receive authentication. |
| Guest Accounting | 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 Use the Controller as Proxy check box. |
| Authentication & Accounting Service (for WLAN Authentication Type: Web Authentication) | | |
| Web Authentication Portal | Indicates the web authentication portal to use for this WLAN. | Choose the web authentication portal from the list. |
| Bypass CNA | Bypasses the Apple CNA feature on iOS and OS X devices that connect to this WLAN. | Select the Enable check box. |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|---|---|---|
| Authentication Service | Indicates the authentication server that you want to use for this WLAN. | Choose the option. Options include Local DB , Always Accept , and any AAA servers that you previously added. Additionally, if you want the controller to proxy authentication messages to the AAA server, select the Use the Controller as Proxy check box. |
| Accounting Service | 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 Use the Controller as Proxy check box. |
| Hotspot 2.0 Profile (for WLAN Authentication Type: Hotspot 2.0 Access) | | |
| Hotspot 2.0 Profile | Indicates the profile, which includes the operator and identifies provider profiles. | Choose the profile. |
| Accounting Service (RFC 5580) | Supports RFC 5580 location delivery on the WLAN, which carries location information in RADIUS exchanges. | Select the check box. |
| Accounting Service (Updates) | Indicates the frequency to send interim updates. Configures the account update interval for accounting servers defined in the Hotspot 2.0 Identity Provider profile. | Enter the duration in minutes. Range: 0 through 1440. |
| WeChat Portal (for WLAN Authentication Type: WeChat) | | |
| WeChat Portal | Defines the WeChat authentication URL, DNAT destination, and other information. | Select a WeChat portal service. |
| Accounting Server | 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 Use the Controller as Proxy check box. |
| Forwarding Profile (for WLAN Usage > Access Network) | | |
| Forwarding Policy | Defines special data packet handling to be taken by the data plane when the traffic is tunneled. | Forwarding Profile is Factory Default . It is disabled. |
| Options | | |
| Wireless Client Isolation | Prevents wireless clients from communicating with each other. | <p>Enable Isolate wireless client traffic from all hosts on the same VLAN/subnet.</p> <p>Enable the following required options as appropriate:</p> <ul style="list-style-type: none"> • Isolate unicast packets: Isolates only unicast packets between a client isolation-enabled client and other clients of the AP. By default, the option is enabled. • Isolate multicast packets: Isolates only multicast packets between a client isolation-enabled client and other clients of the AP. By default, the option is disabled. • Automatic support for VRRP: Isolates packets in VRRP deployment. By default, the option is disabled indicating that the AP is not in a VRRP deployment. |
| Isolation Whitelist | Defines wired destinations on the local subnet that can be reached, even if client isolation is enabled. This option is available only if you enable Wireless Client Isolation . | <p>Select the option.</p> <p>NOTE Isolation Whitelist is not applicable for tunneled WLANs except in the vSZ-D platform.</p> |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|-------------------------------------|---|--|
| Priority | Determines high versus low transmit preference of one WLAN compared to another. Traffic for high priority WLANs is always sent before low priority WLANs in the same QoS category (background, best effort, video, voice). | Choose the priority: <ul style="list-style-type: none"> • High • Low |
| RADIUS Option | | |
| NAS ID | Defines the ID sent to the RADIUS server, which will identify the AP. | Choose the option: <ul style="list-style-type: none"> • WLAN BSSID • AP MAC • User-defined |
| NAS Request Timeout | Indicates the duration after which an expected RADIUS response message is considered to have failed. | Enter the timeout period (in seconds). <p>NOTE It is recommended to configure the same values for NAS Request Timeout, NAS Max Number of Retries, and NAS Reconnect Primary.</p> |
| NAS Max Number of Retries | Indicates the maximum number of failed connection attempts after which the controller will fail over to the backup RADIUS server. | Enter the maximum number of failed connection attempts. <p>NOTE It is recommended to configure the same values for NAS Request Timeout, NAS Max Number of Retries, and NAS Reconnect Primary.</p> |
| NAS Reconnect Primary | 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. | Enter the duration in minutes. Range: 1 through 60 minutes. The default interval is 5 minutes. <p>NOTE It is recommended to configure the same values for NAS Request Timeout, NAS Max Number of Retries, and NAS Reconnect Primary.</p> |
| Called Station ID | Indicates the format for the called station ID, which is sent to the RADIUS server as an attribute, and can be used in policy decisions. | Select a format: <ul style="list-style-type: none"> • WLAN BSSID • AP MAC • AP GROUP • NONE |
| Single Session ID Accounting | Allows the APs to maintain one accounting session for a client roaming between APs. If the client roams from one AP to another, the accounting session ID and statistics will be carried while roaming from one AP to the other. If the feature is not enabled, the accounting session ID is regenerated and the statistics are also reset, essentially resetting the accounting session. | Select the Enable check box. |
| NAS IP | Indicates the NAS IP address. | Select the option: <ul style="list-style-type: none"> • Disabled • SZ Control IP • SZ Management IP • User-defined |

TABLE 57 WLAN Configurations (continued)







| Field | Description | Your Action |
|--|--|---|
| Vendor Specific Attribute Profile | Indicates the VSA profile | Select from the following options: <ul style="list-style-type: none"> VSA profiles <p>NOTE VSA profiles are configured at the zone level.</p> Disabled (default) <p>NOTE Click  to edit the VSA profile.</p> |
| Firewall Options | | |
| Firewall Profile | Indicates the zone for which the firewall profile applies. | Select the option. |
| Enable WLAN specific | Applies the firewall profile to the WLAN. | Select the option and update the following: <ol style="list-style-type: none"> In the Rate Limiting field, select the Uplink and Downlink option to specify and apply rate limit values for the device policy to control the data rate. Select the L3 Access Control Policy from the drop-down list or click  to create a new policy. Refer Creating an L3 Access Control Policy on page 346 for more information. Select the L2 Access Control Policy from the drop-down list or click  to create a new policy. Refer Creating an L2 Access Control Service on page 349 for more information. Select the Application Policy from the drop-down list or click  to create a new policy. Refer Creating an Application Control Policy on page 352 for more information. Select the URL Filtering Profile from the drop-down list or click  to create a new profile. Refer Creating a URL Filtering Policy on page 360 for more information. Select the Device Policy from the drop-down list or click  to create a new policy. Refer Creating a Device Policy on page 366 for more information. |
| Application Recognition and Control | Enables DPI-based Layer 7 application recognition, and if enabled, an application control policy. Recognition and control are performed on the AP. | Select the option. |
| URL Filtering | Enables URL filtering on the WLAN controller to block or allow access to specific websites or web pages. | Select the option. |
| Advanced Options | | |
| Client Fingerprinting | Enables the AP to attempt to utilize DHCP fingerprinting to identify client devices by their operating system, device type, and host name. | Select the check box. |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|-------------------------------|--|--|
| Access VLAN | Tags the WLAN traffic with a VLAN ID from 2 through 4094. By default, all client traffic will be assigned to the native (untagged) VLAN on the AP's Ethernet port, which is represented as VLAN ID 1. | Select the check box and enter the VLAN ID . |
| Hotspot 2.0 Onboarding | Allows devices to connect to a Wi-Fi network automatically, wherein the service providers engage in roaming partnerships to provide seamless access to Wi-Fi networks. The devices are authenticated using credentials or certificates. | Select the check box to allow Hotspot 2.0 Onboarding for the WISPr WLAN. |
| Hide SSID | Removes the SSID from beacon frames. By removing the SSID, in most cases, clients will not show this SSID in their scan list unless the device is already configured to connect. This can simplify the network decision for an end user. | Select the check box. |
| Client Load Balancing | Disables client load balancing on this WLAN if the option is selected. | Select the check box to disable client load balancing on this WLAN. |
| Proxy ARP | Enables proxy ARP. When proxy ARP is enabled on a WLAN, the AP provides ARP response service for stations. When the AP receives an ARP request for a known host, it replies with an ARP response on behalf of the host. If the AP receives a request for an unknown host, it forwards the request. | Select the check box. |
| ND Proxy | Enables Neighbor Discovery proxy. When ND proxy is enabled on a WLAN, the AP provides Neighbor Advertisement service for stations. When the AP receives a Neighbor solicitation request for a known host, it replies with a Neighbor Advertisement on behalf of the host. If the AP receives a request for an unknown host, it forwards the request. NOTE This feature is available only on IPv6 and Dual zone and is enabled by default. | Enable the option. |
| Suppress NS | Suppress Network Solicitation (NS) on a wireless medium when there is no Station entry available in the cache. This feature can be configured only when the ND Proxy option is enabled. NOTE This feature is available only on IPv6 and Dual zone and is disabled by default. | Enable the option. |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|----------------------|--|--|
| RA Proxy | <p>Enables Router Advertisement proxy. When RA proxy is enabled on a WLAN, the AP provides Router Advertisement service for wireless stations. When the AP receives a Router solicitation request on a WLAN, it replies with a Router Advertisement on behalf of the routers available on the network learned by the AP. If the router entries are not found in the cache, the AP forwards the request.</p> <p>NOTE This feature is available only on IPv6 and Dual zone and is enabled by default.</p> | Enable the option. |
| RS/RA Guard | <p>Prevents Router Solicitation (RS) from the wired side of the network to a wireless side. Also prevents Router Advertisement (RA) from a wireless side of the network to the wired side. This feature can be configured only when the RA Proxy option is enabled.</p> <p>NOTE This feature is available only on IPv6 and Dual zone and is disabled by default.</p> | Enable the option. |
| RA Throttling | <p>Regulates the multicast Router Advertisement (RA) from a wired medium to a wireless medium based on the configured Max Allowed RA and Interval. This feature can be configured only when RA Proxy is enabled.</p> <p>NOTE This feature is available only on IPv6 and Dual zone and is disabled by default.</p> | <ul style="list-style-type: none"> • Max Allowed RA: Enter the maximum number of Router Advertisements (RAs) allowed per minute. Range: 1 through 1440, default 10 • Interval: Enter the regulating frequency in minutes. Range: 1 through 256, default 10 |
| MAX Clients | <p>Limits the number of clients that can associate with this WLAN per AP radio (default is 100). Every connection attempt after this maximum value will not be permitted to connect.</p> | Enter the number of clients allowed. |
| 802.11d | <p>Adds additional regulatory information to AP beacons and probe responses. This compliance information provides country-specific guidance such as 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.</p> | Enable the option. |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|--------------------------------|--|--|
| 802.11k Neighbor Report | 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. | Enable the option. |
| 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. | <p>Enable the option. By default, the following options are also enabled:</p> <ul style="list-style-type: none"> • ARP request rate limit: Enter the packets to be reviewed for Address Resolution Protocol (ARP) attacks, per minute. In ARP attacks a rouge client sends messages to a genuine client to establish connection over the network. • DHCP request rate limit: Enter 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 may miss out on obtaining the IP addresses. <p>NOTE When you enable anti-spoofing, an ARP request and DHCP request rate limiter is automatically enabled with default values (in packets per minute, or ppm) 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.</p> <p>NOTE The Force-DHCP option will be enabled by default when anti-spoofing is enabled, and it cannot be changed after anti-spoofing is enabled.</p> |
| Force DHCP | 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. |
| DHCP Option 82 | Enables an AP to encapsulate additional information (such as VLAN ID, AP name, SSID, and MAC address) into DHCP request packets before forwarding them to the DHCP server. The DHCP server uses this information to allocate an IP address to the client from a particular DHCP pool based on these parameters. | <p>Enable the On/Off button.</p> <p>NOTE The options are displayed only if the On is enabled.</p> |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|---------------------------------|--|---|
| DHCP Option 82 Format | Enables an AP to encapsulate additional information into DHCP request packets before forwarding them to the DHCP server. The DHCP server uses this information to allocate an IP address to the client from a particular DHCP pool based on these parameters. | Enable the required format: <ul style="list-style-type: none"> • Subopt-1 with format and select the option. The options are : <ul style="list-style-type: none"> – AP-MAC – AP-MAC ESSID – AP-NAME ESSID • Subopt-2 with format and select the option. The options are: <ul style="list-style-type: none"> – Client-MAC – AP-MAC – AP-MAC ESSID – AP-NAME • Subopt-150 with VLAN-ID. • Subopt-151 with format and select the option. • Mac format delimiter, choose the MAC format from the drop-down list. |
| DTIM Interval | Indicates the frequency at which the Delivery Traffic Indication Message (DTIM) will be included in Beacon frames. | Enter the frequency number. Range: 1 through 255. |
| Directed MC/BC Threshold | 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 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, and 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. | Enter the client count number. Range: 0 through 128. |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|--------------------------------|---|--|
| Client Tx/Rx Statistics | Stops the controller from monitoring traffic statistics for unauthorized clients. | Select the check box. |
| Inactivity Timeout | Indicates the duration after which idle clients will be disconnected. | Enter the duration. Range: 60-864000 seconds |
| WiFi 6 | Allows legacy Wi-Fi 5 clients with outdated drivers to interoperate with a Wi-Fi 6 AP. Use this option to disable Wi-Fi 6 if the client drivers on the network are not the latest or are free of bugs. Wi-Fi 6 clients connecting to a WLAN with Wi-Fi 6 disabled on a Wi-Fi 6 AP will not be able to use Wi-Fi 6 features such as the OFDMA and TWT. | Select the option. |
| OFDM Only | Disconnects 802.11b devices from the WLAN and all devices are forced to use higher data rates for more efficient airtime usage. This setting only affects the 2.4-GHz radio. OFDM is used by 802.11a, g, n, and ac, but is not supported by 802.11b. | Select the check box. |
| BSS Min Rate | Forces client devices to be both closer to the AP and to use higher, more efficient rates when you increase the BSS minimum 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 minimum rate settings. | Select the option. |
| Mgmt Tx Rate | Sets the transmit rate for management frame types such as beacon and probes. | Select the value. |
| Service Schedule | Controls when the WLAN service is active. The purpose of this setting is to automatically enable or disable a WLAN based on a predetermined schedule. By default, the service is Always On . Always Off can be selected 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. NOTE When a service schedule is created, it is saved by the SZ and AP using the time zone of the browser. When it is enforced by the AP, the AP will enforce it according to the time zone of the browser when it was configured. | Choose the option: <ul style="list-style-type: none"> • Always On • Always Off • Specific and select a schedule profile from the drop-down list. |
| Band Balancing | Disables band balancing only for this WLAN, if you select the check box. | Select the Disable band balancing for this WLAN service check box. |

TABLE 57 WLAN Configurations (continued)



| Field | Description | Your Action |
|--------------------------------|--|---|
| Qos Map Set | <p>Reprioritizes downlink packets based on the configured mappings. When an AP receives a downlink packet, it checks the existing DSCP (Layer 3 QoS) marking, compares it to this map set, and then changes the user priority (Layer 2 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 and honored 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>Select Enable QOS Map Set.</p> |
| Multicast Filter | Drops the broadcast and multicast from the associated wireless clients. | Click to enable this option. |
| SSID Rate Limiting | 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 the Uplink and Downlink check boxes and enter the limiting rates in mbps, respectively. Range: 1 through 200 Mbps. |
| Multicast Rate Limiting | <p>Multicast rate limit can be configured at WLAN level. The Uplink Downlink values are displayed only if the multicast rate limit is enabled.</p> <p>The Downlink traffic is limited to 50% of the configured multicast rate limiting. For example, if multicast rate limiting downlink traffic is set to 6Mbps, only ~50%, .i.e. 3.00Mbps to 4.00Mbps max per second traffic passes. This limit is only for downlink and shall not be affected by BSS Min Rate setting.</p> <p>NOTE SSID Rate Limit always take precedence, if, Mutlicast Rate Limit is also configured.</p> | <p>Select the Uplink and Downlink check boxes and enter the limiting rates in Mbps, respectively. Range: 1 through 100 Mbps.</p> <p>NOTE Multicast Rate Limit value cannot exceed SSID Rate Limit values for respective Uplink and Downlink direction.</p> |
| DNS Server Profile | Allows the AP to inspect DHCP messages and overwrite the DNS servers with the DNS server configured in this profile. This allows for policy-based DNS application in which unique users/roles should use a different DNS server than others. | <p>Select a profile from the menu. Select Disable from the menu if you want to disable the DNS Server profile for the WLAN service. Click  to add a new profile or click  to edit a profile.</p> |

TABLE 57 WLAN Configurations (continued)





| Field | Description | Your Action |
|--|--|--|
| DNS Spoofing Profile | <p>When an AP receives a DNS packet, all the fields in the packet are validated.</p> <p>NOTE Only A/AAA server DNS query packets are considered. When same domain name is present in both DNS spoofing profile and walled garden table in the WISPr WLAN, then the AP DNS cache is updated with the IP address present in the DNS spoofing profile.</p> <p>If DNS spoofing and URL filtering with safe search is enabled, URLfiltering (safe search) takes precedence for the Google, YouTube, and Bing domain names. If safe search is not enabled, DNS spoofing takes the precedence. If safe search is not enabled and URL filtering is enabled also DNS-Spoof takes the precedence.</p> | <p>Select a profile from the menu. Select Disable from the menu if you want to disable the DNS Spoofing profile for the WLAN service. Click  to add a new profile or click  to edit a profile</p> |
| Precedence Profile | <p>Defines the relative policy assignment priority for some specific settings. For example, if a WLAN is configured to use VLAN 10, and an 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.</p> | <p>Select the option. Click  to add a new profile or click  to edit a profile.</p> |
| CALEA (This feature is supported only for SZ300 controllers.) | <p>Intercepts traffic, a requirement enforced on some networks by government agencies. To utilize CALEA, you must support a vSZ-D and configure the CALEA settings in the Services & Profiles > Tunnels & Ports menu.</p> | <p>Select the check box.</p> |
| Client Flow Data Logging | <p>Sends a log message with the source MAC address, destination MAC address, source IP address, destination IP address, source port, destination port, Layer 4 protocol, and AP MAC address of each packet session to the external syslog server. This function is provided by the AP syslog client (not the SZ syslog client), which must be enabled at the zone level in order to support this client flow logging.</p> | <p>Select the check box to log the client-flow data to the external syslog server. Then enable AP syslog functionality from the Zone settings.</p> |
| Airtime Decongestion | <p>Mitigates airtime congestion caused by management frames in high-density deployments.</p> | <p>Select the check box.</p> |

TABLE 57 WLAN Configurations (continued)

| Field | Description | Your Action |
|--|--|--|
| Join RSSI threshold | Indicates the signal threshold that could connect to the Wi-Fi. If Airtime Decongestion is enabled, Join RSSI threshold is automatically disabled. | Enter the Client RSSI threshold to allow joining. Range: -60 through -90 dBm. |
| Transient Client Management | Discourages transient clients from joining the network. | Select enable Transient Client Management and set the following parameters: <ul style="list-style-type: none"> • Join wait time—Enter the wait time before a client can be permitted to join. Range: 1 through 60 secs. • Join expire time—Enter the time during which a rejoin request is accepted without delay. Range: 1 through 300 secs. • Join wait threshold—Enter the number of join attempts after which a client is permitted to join even before the join wait time expires. |
| Optimized Connectivity Experience (OCE) | 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 Optimized Connectivity Experience (OCE) and set the following parameters: <ul style="list-style-type: none"> • Broadcast Probe Response Delay: Indicates the time delay to transmit probe response frames in milliseconds. • RSSI-based Association Rejection Threshold: 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. |

4. Click **OK**.

For SZ300 and vSZ-H, you can also migrate the WLAN configuration from a regular Domain to a Partner Domain. For more information, see <https://support.ruckuswireless.com/answers/000006414>.

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.

Channel Mode

Channel mode is a method of statistically picking the most potent channel for an AP.

Some countries restrict certain 5GHz channels to indoor use only. For instance, Germany restricts channels in the 5.15GHz to 5.25GHz band to indoor use. When ZoneFlex Outdoor APs and Bridges with 5GHz radios (ZoneFlex 7762, 7762-S, 7762-T, 7761-CM and 7731) are set to a country code where these restrictions apply, the AP or Bridge can no longer be set to an indoor-only channel and will no longer select from amongst a channel set that includes these indoor-only channels when SmartSelect or Auto Channel selection is used, unless the administrator configures the AP to allow use of these channels.

For instance, if the AP is installed in a challenging indoor environment (such as a warehouse), the administrator may want to allow the AP to use an indoor-only channel. These channels can be enabled for use through the AP CLI or the controller web interface.

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 - 0 - 100. To set minimum client control to 0, select Client Admission Control threshold.
- Maximum radio load (%) - 50 - 100
- Minimum client throughput (Mbps) - 0 -100

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

NOTE

Client admission control cannot be enabled if client load balancing/band balancing (or both) is enabled.

NOTE

If you are trying to steer clients to the appropriate band (band steering), please refer [Band Balancing](#) on page 295 section.

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.

NOTE

Adaptive Client Load Balancing (ACLB) is not supported on AP R730 in this release. AP R730 supports only legacy Client Load Balancing (CLB). ACLB is disabled by default if *capacity mode* is configured on the controller and if *station mode* is configured, then ACLB acts as legacy CLB on the AP.

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 58 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

Multicast Rate Filter

All SZ Managed APs will support this feature. The GUI for rate limit control is designed as:

- **FIGURE 150** Multicast Rate Limiting



Configuring Multicast rate limit

- Multicast Downlink/Uplink Rate Limit should be configured at WLAN level.
- Multicast Rate Limit and Drop Multicast/Broadcast Traffic from Associated Wireless Clients are mutually exclusive feature.
- Multicast UL/DL values should be shown only if Multicast Rate limit is enabled.
- Downlink value default is up to 6 mbps. The range of multicast values depends on the BSS minimum rate selection in the wlan and a maximum of half of the BSS minimum rate.
- SSID Rate Limit will always take precedence if Multicast Rate Limit is also configured.

Add multicast rate limiting uplink and downlink fields in advanced option of wlan

FIGURE 151 Configuring Multicast Rate Limit

| Advanced Options | | | |
|-----------------------------------|----------------|--|----------------|
| User Traffic Profile | System Default | Inactivity Timeout | 120 seconds |
| L2 Access Control | Disabled | Client Fingerprinting | Enabled |
| OS Policy | Disabled | OFDM Only | Disabled |
| Application Recognition & Control | Disabled | BSS Min Rate | Default |
| URL Filtering Profile | Disabled | Mgmt Tx Rate | 2mbps |
| Access VLAN | 1 | Time Schedule | Always On |
| Hide SSID | Disabled | Band Balancing | Enabled |
| Client Load Balancing | Enabled | QoS Map Set | Enabled |
| Proxy ARP | Disabled | Precedence Profile | System Default |
| ND Proxy | Disabled | DNS Server Profile | Disabled |
| RA Proxy | Disabled | DNS Spoofing Profile | Disabled |
| Uplink Limit (mbps) | 0 | Multicast Uplink Limit (mbps) | 20 |
| Downlink Limit (mbps) | 0 | Multicast Downlink Limit (mbps) | 50 |
| Max Clients | 100 | Wi-Fi Calling profile | Disabled |
| 802.11d | Enabled | CALEA | Disabled |
| 802.11k Neighbor Report | Enabled | Venue Code | Disabled |
| Force DHCP | Disabled | Client Flow Data Logging | Disabled |
| DHCP Option 82 | Disabled | Airtime Decongestion | Disabled |
| DTIM Interval | 1 | Transient Client Management | Disabled |
| Directed MC/BC Threshold | 5 | Optimized Connectivity Experience(OCE) | Disabled |
| Client TX/RX Statistics | Disabled | | |

User can check multicast uplink and downlink fields in WLAN preview

FIGURE 152 WLAN Preview

The screenshot displays a configuration page for a WLAN. At the top, there are several toggle switches: 'OFDM Only' (OFF), 'BSS Min Rate' (24 mbps), 'Mgmt Tx Rate' (24 mbps), 'Time Schedule' (Always On), 'Band Balancing' (Disable band balancing for this WLAN service), 'QoS Map Set' (OFF), and 'Multicast Filter' (OFF). Below these are sections for 'SSID Rate Limiting' and 'Multicast Rate Limiting', each with uplink and downlink rate limiters. The 'Join RSSI threshold' is set to 0 dBm. At the bottom, there are more toggle switches for 'CALEA', 'Venue Code', 'Client Flow Data Logging', 'Airtime Decongestion', 'Transient Client Management', and 'Optimized Connectivity Experience(OCE)'. The interface includes dropdown menus for 'DNS Server Profile', 'DNS Spoofing Profile', and 'Precedence Profile'. Red text warnings are present regarding rate limiting and multicast filter exclusivity.

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 59 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 47.

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, Domain, Zone, or WLAN Group from the hierarchy tree, respective contextual tabs appear at the bottom of the page.

TABLE 60 System/Domain/Zone/WLAN Groups Monitoring Tabs

| Tabs | Description | System | Domain | Zone | WLAN Groups |
|-----------------------|--|--------|--------|------|-------------|
| Configuration | Displays the respective configuration information. | Yes | Yes | Yes | Yes |
| Traffic | Displays the respective historical traffic information. | Yes | Yes | Yes | Yes |
| Alarm | Displays the respective alarms information. | Yes | Yes | Yes | Yes |
| Event | Displays the respective event information. | Yes | Yes | Yes | Yes |
| APs | Displays the respective AP information. | Yes | Yes | Yes | NA |
| Clients | Displays the respective client information. | Yes | Yes | Yes | NA |
| Services | Displays the respective Services information. | Yes | Yes | Yes | NA |
| Administrators | Displays the respective administrator account information. | Yes | NA | NA | NA |

When you can select a Zone and click **More** you can perform the following operations:

- **Move**
- **Extract WLAN Template**
- **Apply WLAN Template**
- **Change AP Firmware**
- **Switchover Cluster**
- **Trigger Preferred Node**

Moving a Single WLAN to a Different WLAN Zone

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

NOTE

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

- From the Wireless LANs page, locate the WLAN zone that you want to move to a different WLAN zone.
- Click **More** and select **Move**, the **Select Destination Management Domain** dialog box appears.
- Select the destination WLAN zone.
- Click **OK**, a confirmation message appears.
- Click **Yes**. The WLAN zone is moved to the destination location.

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.

Triggering a Preferred Node

You can trigger an AP that belongs to the current zone to force go to their preferred node. For this, you must enable Node affinity, which gives AP the priority of preferred nodes.

Follow these steps to trigger a node:

NOTE

You must enable node affinity before triggering nodes.

1. From the Wireless LANs page, locate the zone.
2. Click **More** and select **Trigger Preferred Node**, a confirmation dialog box appears.
3. Click **OK**. You have triggered the nodes in the AP zone.

How Dynamic VLAN Works

Dynamic VLAN can be used to automatically and dynamically assign wireless clients to different VLANs based on RADIUS attributes.

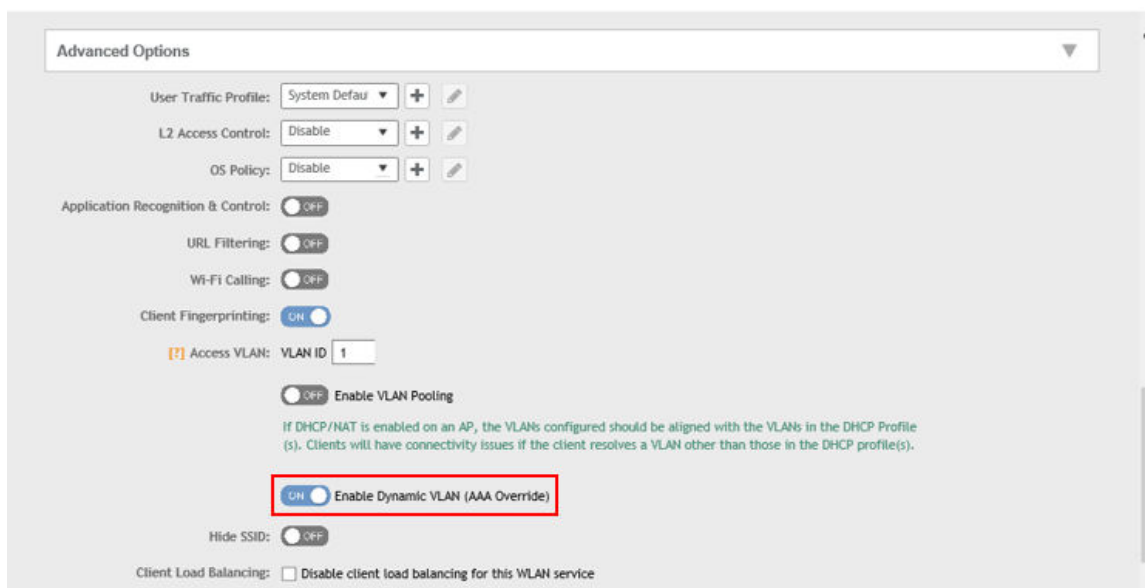
Dynamic VLAN Requirements:

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

FIGURE 153 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 61 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..... 305
- Working with Wired Clients..... 308
- Working with Users and Roles..... 309
- Working with Guest Passes..... 322
- Working with Dynamic PSKs..... 335

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 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 62 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 62 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 |
| CPE MAC | Displays the WLAN MAC address of the CPE |
| User Name | Displays the name of the user logged on to the wireless client |
| MCS Rate (Tx) (Rx) | Displays the median of MCS rate Tx/Rx for both client and AP in there respective pages. These values are updated every 180 seconds (Highscale) and 90 seeconds (Essentials). |
| 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 63 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 444.

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 154 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 an L3 Access Control Policy](#) on page 346.
 - 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 391.
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 64 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 65 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 66 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 | |

Managing Clients

Working with Users and Roles

TABLE 66 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)

| Resource | Operation | Resource Group | Permission Levels |
|--|--|----------------|-------------------|
| 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"> System Time Syslog Server SCI northbound portal | View configuration content | SZ Management | Read |
| <ul style="list-style-type: none"> SMTP FTP server for upload stats Critical AP rules Q-in-Q Ether Type Gateway Advanced Options Certificate Store | Modify configuration content | SZ Management | Modify |
| <ul style="list-style-type: none"> Cluster Redundancy(3.6) SNMP Agent Event Management Event Threshold Management Interface ACL Hosted AAA services (EAP-SIM, EAP-AKA) MNC-NDC Mappings FTP SMS Server Approval (System > AP Settings > Approval) AP Switchover EPVOT (Ethernet Port Validate On Trunk) Gateway advanced ZeroIT lwapp2scg | Create new configuration entity Event Management : Disable/Enable Cluster Redundancy - Rehome Per cluster, Restore Config, Switchover | SZ Management | Full Access |

TABLE 66 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)

| Resource | Operation | Resource Group | Permission Levels |
|---------------------|--|---|-------------------|
| 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 |
| | 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 |

Managing Clients

Working with Users and Roles

TABLE 66 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)

| Resource | Operation | Resource Group | Permission Levels | |
|--|--|---|-------------------|--|
| Zone related service/profile <ul style="list-style-type: none"> • Node affinity • Ruckus GRE Tunnel • SoftGRE Tunnel • IPsec Tunnel • LBS • Hotspot 2.0 Venue Profile • Ethernet Port Profile | 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"> • AAA • Hotspot • WeChat • Guest Access | Modify Test AAA | WLAN Management | Modify | |
| | | | | |
| | | | | |
| | | | | |
| <ul style="list-style-type: none"> • Web Auth • Hotspot 2.0 WLAN Profile • WLAN scheduler • Device Policy | Create/Delete | WLAN Management | Full Access | |
| | | | | |
| | | | | |
| | | | | |
| <ul style="list-style-type: none"> • L2 Access Control • DiffServ • VLAN Pooling | View configuration content | WLAN Management | Read | |
| | | | | |
| | | | | |
| | | | | |

TABLE 66 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"> • Authentication/Accounting Profile • AAA (authentication/accounting services) • Hotspot 2.0 Wi-Fi Operator • Hotspot 2.0 Wi-Fi Provider • Online Signup Portal • User Traffic Profile • Forwarding Profile (all types, e.g. Bridge,L2oGRE...) • Application Control (AVC) • DNS server services • URL Filtering | 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"> • Lock • Unlock • Import Batch Provisioning APs • Import Swapping APs • Trigger Preferred Node • Restart Cable Modem • Reset Cable Modem • Swap • Approve | AP Management | Full Access |
| | AP Table: <ul style="list-style-type: none"> • Export All Batch Provisioning APs • Export All Swapping APs • Download Support Log • Trigger AP Binary Log • Download CM Support Log | AP Management | Read |
| | Untag Critical APs | AP Management | Modify |
| | Get All APs Firmware | AP Management | Read |
| | Get AP Binary Log | AP Management | Read |
| | | | |

Managing Clients

Working with Users and Roles

TABLE 66 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)

| Resource | Operation | Resource Group | Permission Levels |
|--|---|------------------------------------|-------------------|
| 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"> Bonjour Gateway WIPS (Rogue AP Policy) | 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 | | |
| View, print, text guest pass | User/Device/Application Management | | |
| 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 | User/Device/Application Management | Read |
| | Disconnect | | |
| | View client or managed devices | | |
| 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 | User/Device/Application Management | Modify |
| | Modify user name | | |
| Export CSV | User/Device/Application Management | | |
| Rogue Device | | AP Management | Read |
| Admin Activity Log | | Administrator Management | Read |

TABLE 66 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)

| Resource | Operation | Resource Group | Permission Levels |
|---|--|---|-------------------|
| 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 |
| Diagnosics > Scripts > Patch Scripts Diagnosics > Scripts > Diagnostics Scripts | | Super Admin only | Full Access |
| Diagnosics > Scripts > AP CLI Scripts | | AP Management | Full Access |
| Diagnosics > Scripts > Applications Logs | Download log | SZ Management | Read |
| | Set log level | SZ Management | Modify |
| Diagnosics > Others | | SZ Management | Read |
| Historical Client Statistics | View | User/Device/Application Management AP management | Read |
| Core Tunnel Statistic (generated By DP) <ul style="list-style-type: none"> Core Network Tunnel Stats > SoftGRE Core Network Tunnel Stats > GRE Core Network Tunnel Stats > GTP Core Network Tunnel Stats > PMIPv6 | | SZ Management | Read |
| Access Tunnel Statistics (generated By DP) | | SZ Management | Read |
| Access Tunnel Statistics (generated by AP) <ul style="list-style-type: none"> Ruckus AP Tunnel Stats > Ruckus GRE Ruckus AP Tunnel Stats > SOFT GRE Ruckus AP Tunnel Stats > SoftGRE + IPsec | | 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 |

TABLE 66 Relationship between Resource, Operation -Resource Group and Permission Levels (continued)

| Resource | Operation | Resource Group | Permission Levels |
|---|---|--|-------------------|
| | 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) DHCP Pools (AP) | AP Management, WLAN Management and SZ Management | Full Access |
| 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 |
| | 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 an L3 Access Control Policy](#) on page 346.
2. Create a role, refer [Creating a User Role](#) on page 309.

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 414.

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 419.

5. Create a web authentication portal WLAN configuration and assign the Non-proxy AD server to it. Refer [Creating a WLAN Configuration](#) on page 277.

- 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 an L3 Access Control Policy](#) on page 346 .
2. Create a role, refer [Creating a User Role](#) on page 309.
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 414.

4. Perform an authentication test to ensure that the user gets assigned the correct Role. Refer [Testing AAA Servers](#) on page 419.
5. Create a web authentication portal WLAN configuration and assign the Non-proxy RADIUS server to it. Refer [Creating a WLAN Configuration](#) on page 277.
 - 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.

- Role-based policies are only supported in proxy-mode AAA WLANs, where proxy AAA method is used for authentication. If the authentication method is non-proxy AAA, where the AP authenticates the user, the user equipment (UE) cannot be determined and therefore, user-role policies are not supported on non-proxy mode AAA WLANs.
- Typically, the RADIUS/AAA servers return a user attribute to the controller, and the controller assigns it to an UE. However, you must establish a mapping between the user attribute and the user role, so that the user role policy can be applied to the UE. The attribute-role mapping is configured within the AAA policy.
- User Traffic Profiles are configured with various policies such as rate limiting so when a profile is applied to a WLAN, the policies in the profile are applied to all the UEs in the WLAN. The policies can also be applied to a user role in a WLAN, but not all the policies defined in the profile are applied to the role.

If a role-based VLAN policy is defined in the profile, it cannot be applied to the WLAN if its authenticated based on a L7 method (WebAuth or Hotspot/WISPr). This is because when a VLAN is applied on a per-role basis for a L7 authentication method, the user receives an IP address via DHCP before the UE is authenticated - this happens at layer 3 or 4, and you cannot authenticate the UE and assign a role to it till layer 7 is reached. This results in a mismatch between the VLAN IDs set within the roles, and could possibly lead to service disruptions.

- Precedence profiles are configured at the WLAN level, but impact the manner in which roles are assigned. The manner in which the profile is defined, indicates the order in which policies defined within the profile are assigned. The order of priorities can be customized. For example, if you have WLAN5 configured with VLAN ID 5, An OS policy configured with an iOS VALN ID 10, and a role policy assigned to a student with VALN ID 40, then there are multiple orders one can set when a *student user with iOS connects to WLAN 5*.
- You can assign a UE to a role through RADIUS, or you can use RADIUS attributes to apply policies. However, using RADIUS attributes take precedence over assigning UEs to a role (though it is easy to configure, as the only element required to authenticate the UE is the role information).

In the RADIUS attributes method, each policy, such a rate limiting or user traffic profile has a unique RADIUS attribute. Therefore, specifying the RADIUS attribute for a policy will override all other forms of the controller policy. For example, if a UE is already

assigned to VLAN 7 through RADIUS, setting a RADIUS attribute for VLAN IDs to 9 will override all VLAN=7 configurations in say WLANs, OS policies, role policies etc.

Creating a Local User

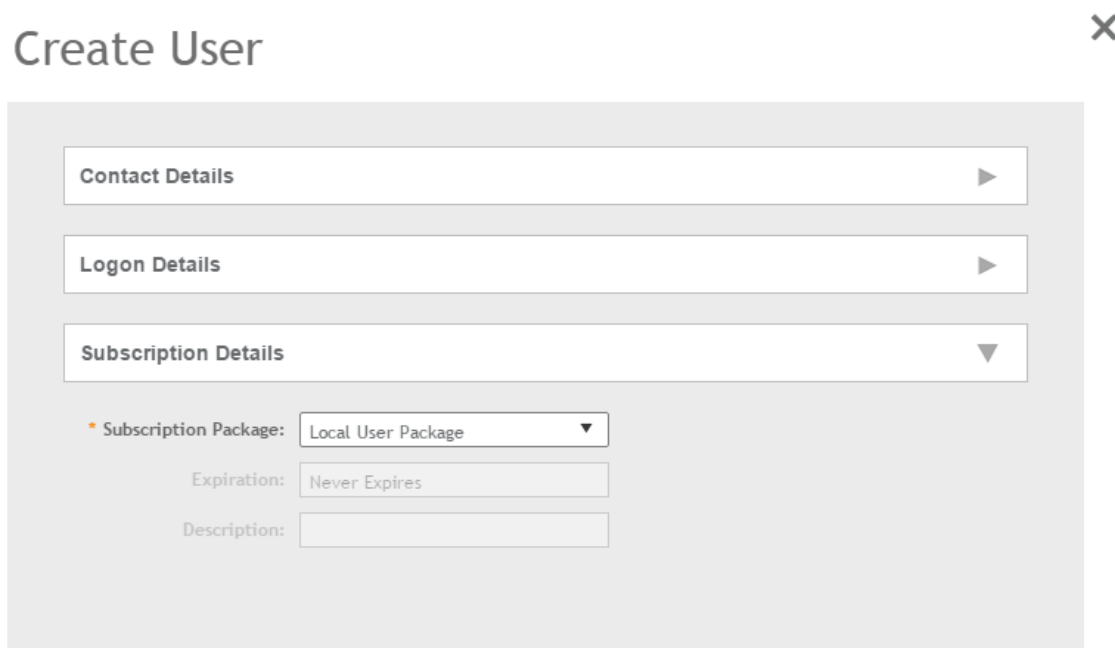
A local user in the controller refers to a registered user who may be given access to the controller hotspot. A user account contains a user's personal information, logon information, and the subscription package that he or she has been assigned. The controller's local user database can include 802.1X, 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 391 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 155 Create User



Create User ✕

Contact Details ▶

Logon Details ▶

Subscription Details ▼

* Subscription Package: Local User Package ▼


Expiration: Never Expires

Description:


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 321, 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 156 Create Subscription Package

The screenshot shows a web form titled "Create Subscription Package". The form contains the following fields and controls:

- * Name:** A text input field.
- Description:** A text input field.
- * Expiration Interval:** A dropdown menu currently showing "No data available".
- * Expiration Value:** A text input field.

At the bottom of the form, there are two buttons: "OK" and "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 323

[Step 2: Create a Guest Access WLAN](#) on page 323

[Step 3: Generate a Guest Pass](#) on page 324

[Step 4: Send Guest Passes to Guest Users](#) on page 326

Step 1: Create a Guest Access Service

1. Follow the instructions in [Creating a Guest Access Portal](#) on page 371 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.

Managing Clients

Working with Guest Passes

- When you finish creating a guest access WLAN, continue to the next step.

FIGURE 157 Creating a WLAN for guest access only

The screenshot shows a configuration page with two main sections. The first section, 'Encryption Options', has a dropdown menu and a 'Method' field with radio buttons for WPA2, WPA-Mixed, WEP-64 (40 bits), WEP-128 (104 bits), and None (selected). The second section, 'Guest Access Portal', has a dropdown menu and several fields: 'Guest Portal Service' (dropdown with '+ Create' button), 'Bypass CNA' (checkbox checked, 'Enable' selected), 'Guest Authentication' (dropdown with 'Select an authentication se'), and 'Guest Accounting' (checkbox checked, 'Use the Controller as Proxy' selected, 'KIKK-ACCT' dropdown, '+ Create' button, and 'Send interim update every' field set to '1' minutes).

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 323.
- 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 326 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 158 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:

NOTE

We can generate maximum 40000 guest passes.

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 159 Options for delivering guest passes to guest users

Here are the generated guest passes

Enable
 Disable

| 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 160 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.

Managing Clients

Working with Guest Passes

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.

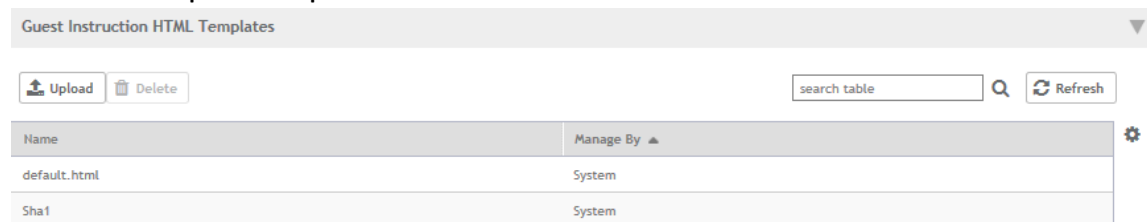
10. Configure the **Upload a Template File** options:
 - **Template Name**: Type a name for the template that you are uploading.
 - **Template File**: Click **Browse**, and select the template file you created.
11. Click **Upload**.

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 161 The **Upload a Template File** form



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.

- 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 162 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.

- 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.

- Save the file.

- 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.

- 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.

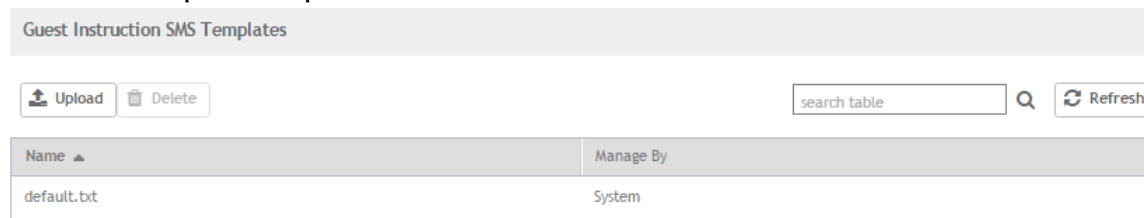
- Click **Upload**.

An information message box appears and informs you that the template file has been uploaded successfully.

- Click **OK**.

The template file you uploaded now appears in the list of templates.

FIGURE 163 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.

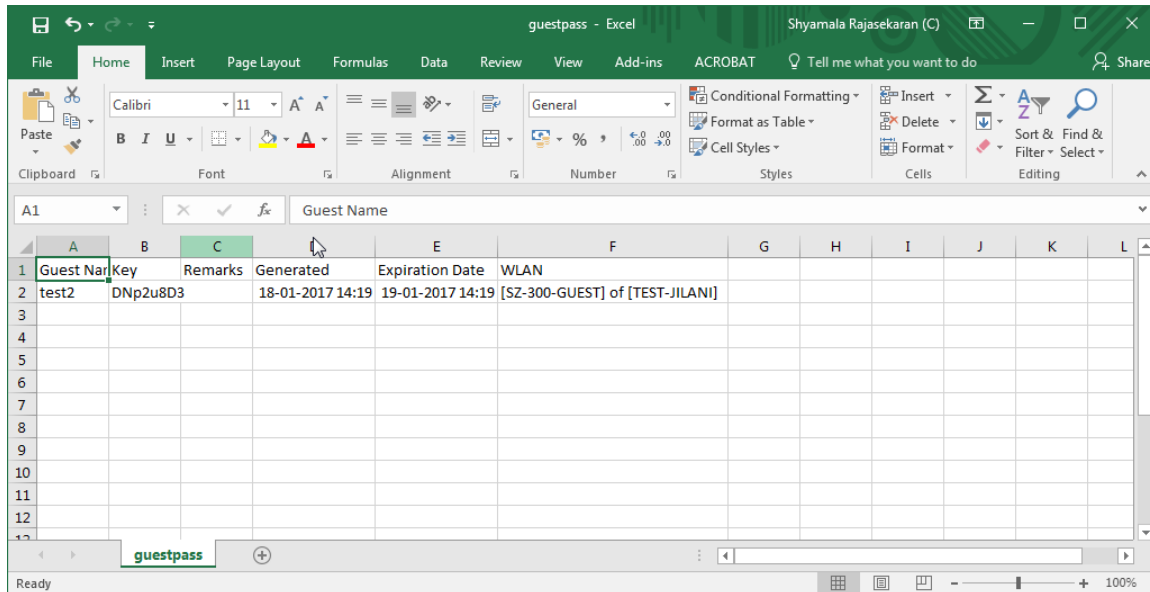
1. From the generate guest pass list, select the guest passes that you want to export to CSV.
2. Click **Export Selected**.

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 164 A sample CSV of generated guest passes when opened in Excel



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.

- Click **Import Guest Pass**,

The **Import Guest Pass** form appears.

- Look for the following text under Browse:

To download a sample guest pass, click here.

- Click the **here** link to download the sample CSV file.
- Using Microsoft Excel or a similar application, open the CSV file.
- 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 165 The sample CSV file when opened in Excel

| | A | B | C |
|----|--------------------|------------------|--------------------------------|
| 1 | #Guest Name (Must) | Remarks | Key (Empty Implies random key) |
| 2 | Batch-Guest-1 | Batch generation | AAAAAAA |
| 3 | Batch-Guest-2 | Batch generation | |
| 4 | Batch-Guest-3 | | |
| 5 | | | |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |
| 11 | | | |
| 12 | | | |
| 13 | | | |
| 14 | | | |

- Save the CSV file.
- 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 323.
 - 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.

Managing Clients

Working with Guest Passes

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-login 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 326 for information.

FIGURE 166 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 | DNp2u803 | 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.

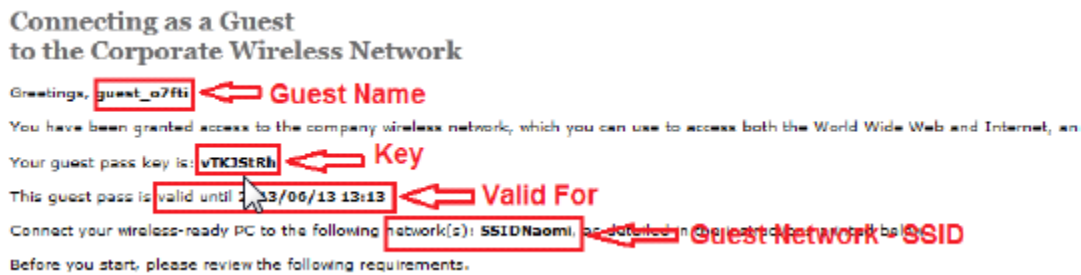
Follow these steps to print a guest pass.

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 327), 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 167 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 168](#)).
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.

Managing Clients

Working with Guest Passes

FIGURE 168 Use the Recipient Email form to specify who will receive the guest passes via email

Here are the generated guest passes

Print Selected Export Selected Email SMS Delete Enable Disable More

| 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 |

Recipient Email Add New
sama@yahoo.co Remove
Send Email

3 total records < 1 >

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.

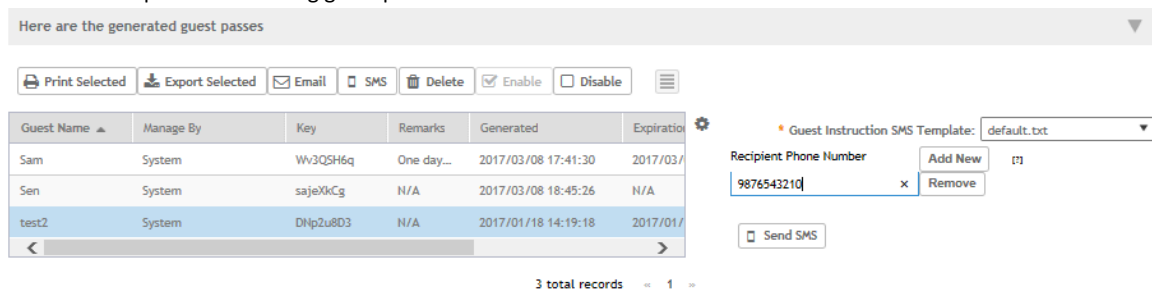
1. From the generated guest passes list, select the guest pass that you want to send via SMS.
2. Click **SMS**.
3. In Guest Instruction SMS Template, select the SMS template that you want to use.
4. Click **Add New**.
5. In the box that appears below, type the phone number to which you want to send the 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 169 Options for sending guest passes via 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 DPSK. 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.

Managing Clients

Working with Dynamic PSKs

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 SZ300/vSZ-H platform, the maximum number of DPSKs is 25,000 per zone or domain and 50,000 for the 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):

Managing Clients

Working with Dynamic PSKs

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 170 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 171 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 411.
2. Create an Accounting Service. Refer, [Creating Proxy Accounting AAA Servers for Standby Cluster](#) on page 428.
3. Create Zone Configuration. Refer, [Creating an AP Zone](#) on page 80.

4. Create a WLAN Configuration for DPSK. Refer, [Creating a WLAN Configuration](#) on page 277.

FIGURE 172 External DPSK Configuration

The screenshot shows the 'Create WLAN Configuration' dialog box with the following settings:

- 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 Select an authentication service
 - Accounting Service: Use the controller as proxy

Buttons: 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: $Key = PBKDF2(\text{passphrase}, \text{ssid}, 4096, 256)$. (Here, we can also have reference to RFC2898).
- Pre-pend 0x00 to the calculated value of the key.

Application Recognition and Control

- [Monitoring Applications.....](#) 341

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 351.

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.

- 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 173 Top Applications - Chart View

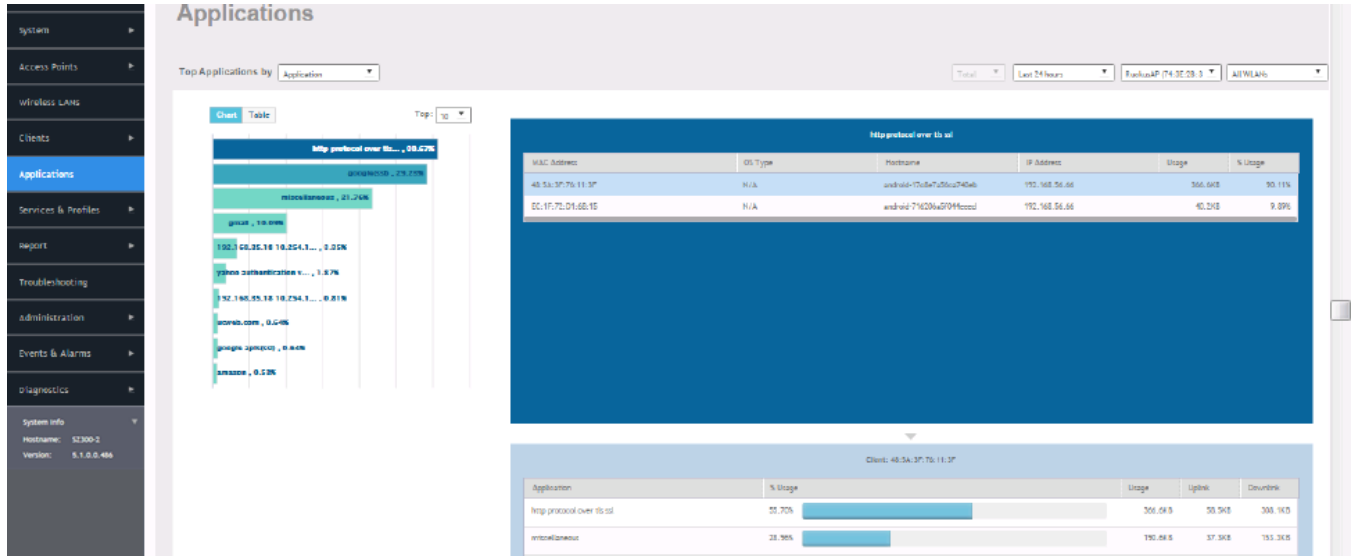
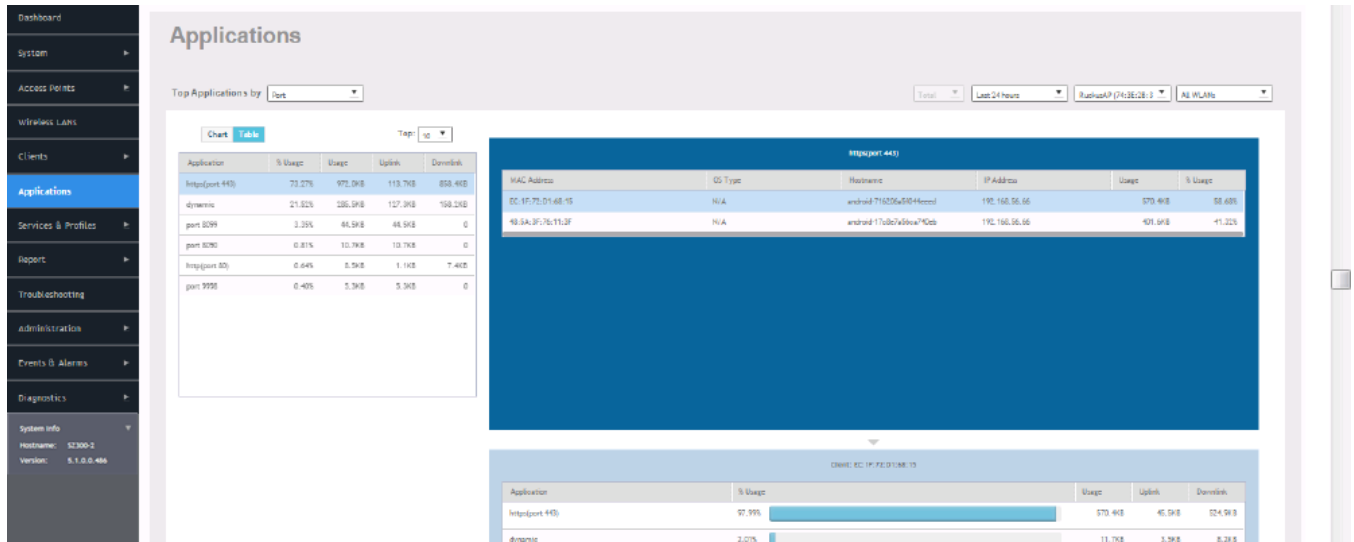
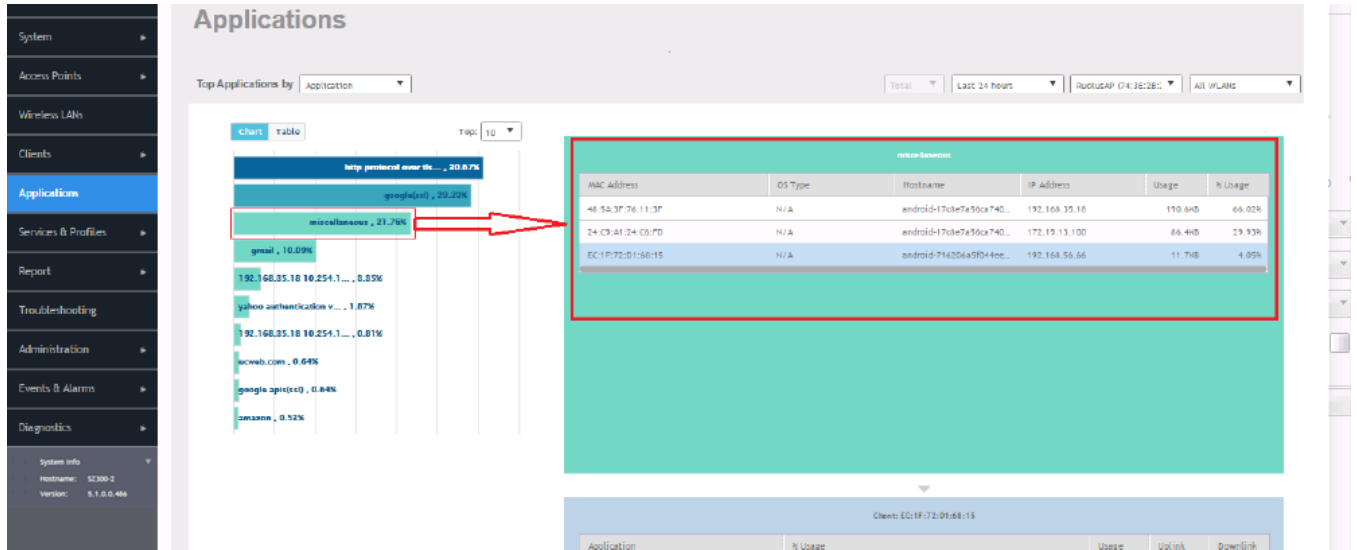


FIGURE 174 Top Applications by Port - Table View



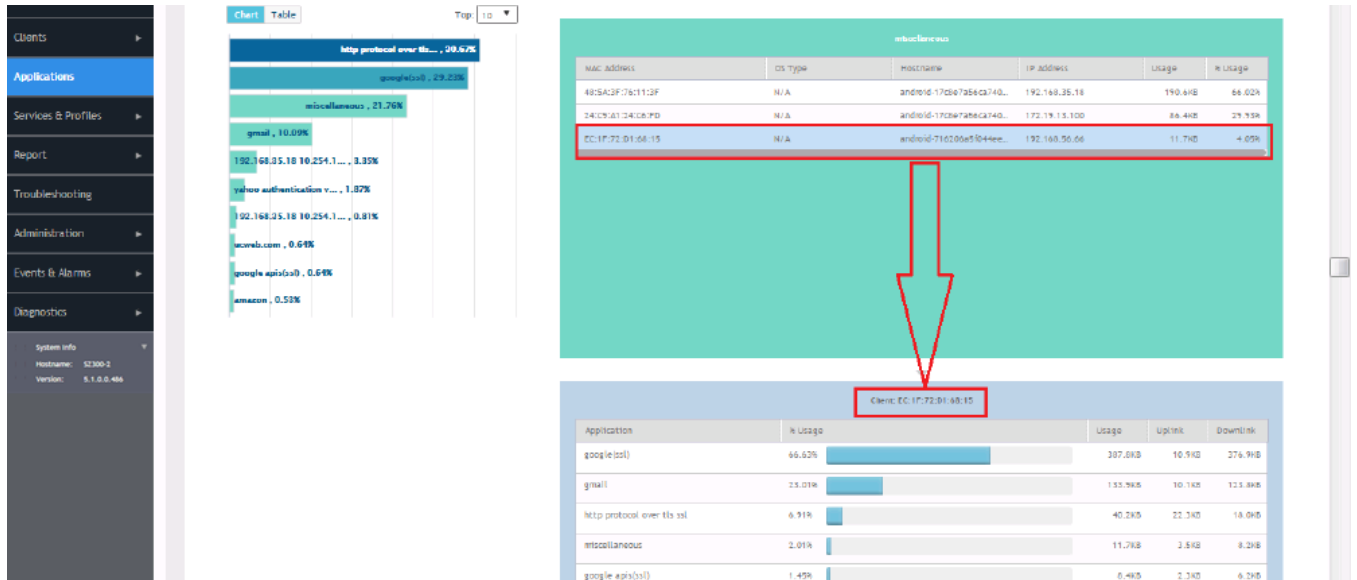
- Click on an application from the list on the left (either Chart or Table view) to view a list of the top clients using the selected application in the list on the right. The client list displays the client's MAC address, OS, hostname, IP address (IPv4 and IPv6), and application usage volume and percent 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 175 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 176 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 351.

Managing a Firewall Profile

- [Creating an L3 Access Control Policy.....](#) 346
- [Creating an L2 Access Control Policy.....](#) 349
- [Configuring Application Controls.....](#) 351
- [URL Filtering.....](#) 360
- [Creating a Device Policy.....](#) 366

To create a firewall profile, perform the following steps:

1. Select **Firewall**, the **Firewall Profiles** page is displayed.

The **Summary** tab displays the firewall profiles in chart and graph format. You can filter the profiles based on duration and zone.

2. Select **Profiles** tab and click **Create**.

This displays the **Create Firewall Profile** page.

FIGURE 177 Creating a Firewall Profile

Create Firewall Profile ✕

Name:

Description:

Rate Limiting: **Uplink** OFF Mbps (0.1~200)

Downlink OFF Mbps (0.1~200)

L3 Access Control Policy:

L2 Access Control Policy:

Application Policy:

URL Filtering Profile:






Device Policy:

3. In the **Name** field, enter a name for this profile.
4. In the **Description** field, enter a short description for this profile.
5. In the **Rate Limiting** field, select the **Uplink** and **Downlink** options to specify and apply rate limit values for the device policy to control the data rate.

Managing a Firewall Profile

Creating an L3 Access Control Policy

6. Configure the following policies:

- a. Select the **L3 Access Control Policy** from the drop-down list or click  to create a new policy. Refer to [Creating an L3 Access Control Policy](#) on page 346 for more information.
- b. Select the **L2 Access Control Policy** from the drop-down list or click  to create a new policy. Refer to [Creating an L2 Access Control Service](#) on page 349 for more information.
- c. Select the **Application Policy** from the drop-down list or click  to create a new policy. Refer to [Creating an Application Control Policy](#) on page 352 for more information.
- d. Select the **URL Filtering Profile** from the drop-down list or click  to create a new profile. Refer to [Creating a URL Filtering Policy](#) on page 360 for more information.
- e. Select the **Device Policy** from the drop-down list or click  to create a new policy. Refer to [Creating a Device Policy](#) on page 366 for more information.

7. Click **OK**.

NOTE

You can also edit, clone and delete a firewall profile by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Firewall Profiles** page.

Creating an L3 Access Control Policy

An L3 Access Control Policy 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, an L3 Access Control Policy can be created to shape traffic according to a configurable Application Control Policy.

After L3 Access Control Policy is created, it can be applied to any WLAN from the **Wireless LANs** page.

1. Select **Firewall > L3 Access Control**. The **L3 Access Control** page is displayed.

2. Click **Create**.

This displays the **L3 Access Control Policy** page.

FIGURE 178 Creating an L3 Access Control Policy

Create L3 Access Control Policy

Name:

Description:

Default Access: Default access if no rule is matched: Allow Block

+ Create Configure Delete Up Down

| Priority | Description | Matching Criteria | Type | Access |
|----------|-------------|--|------|--------|
| 1 | Allow DNS | Direction:Inbound Destination Port:53 | IPv4 | Allow |
| 2 | Allow DHCP | Direction:Inbound Destination Port:67 | IPv4 | Allow |

OK Cancel

3. In the **Name** field, enter a policy name.
4. In the **Description** field, enter a short description for the policy.
5. In **Default Access**, select **Allow** or **Block** if no rule is matched.
6. To assign rules for the policy, click **Create**. The **L3 Access Control** page is displayed.

Refer to [Creating an L3 Access Control Policy Rule](#) on page 347 for more information.

NOTE

You can set a priority to the policy by selecting the policy and click **Up** or **Down** to set the desired order.

NOTE

You can edit or delete a policy rule by selecting the options **Configure** or **Delete** respectively.

7. Click **OK** to save the policy.

After the L3 access control policy is created, it can be applied to any WLAN from the Wireless LANs page.

NOTE

You can edit, clone, or delete a policy by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the L3 Access Control page.

Creating an L3 Access Control Policy Rule

An L3 Access Control Policy of multiple traffic control rules, which can be enforced in any order you prefer.

To create an L3 access control policy rule:

1. From the **L3 Access Control Policy** page, click **Create**. The **L3 Access Control Policy Rule** page is displayed.

FIGURE 179 Creating an L3 Access Control Policy Rule

Create L3 Access Control Policy Rule

The screenshot shows a configuration form for creating an L3 Access Control Policy Rule. The form is titled "Create L3 Access Control Policy Rule" and has a close button (X) in the top right corner. The form fields are as follows:

- Description: [Text input field]
- Access: [Dropdown menu, set to "Allow"]
- Protocol: [Dropdown menu, set to "No data available"]
- Type: [Radio buttons for "IPv4" (selected) and "IPv6"]
- Source IP: [ON] [Radio button] Subnet Network Address: [Text input field] Subnet Mask: [Text input field]
- Source Port: [ON] [Radio button] Range: [Text input field] - [Text input field]
- Destination IP: [ON] [Radio button] Subnet Network Address: [Text input field] Subnet Mask: [Text input field]
- Destination Port: [ON] [Radio button] Range: [Text input field] - [Text input field]
- Direction: [Dropdown menu, set to "Inbound"]

At the bottom right of the form, there are two buttons: "OK" and "Cancel".

2. Configure the following:

- **Description:** Type a short description for the access control policy rule.
- **Access:** Select Allow or Block depending on whether you want to set this rule as the default rule.

NOTE

All unicast, multicast and broadcast traffic, except the ACL rules will be allowed or dropped depending on the option selected. Add the appropriate rules.

- **Protocol:** Select the network protocol to which this rule will apply. Supported protocols include TCP, UDP, UDPLITE, ICMP (ICMPv4), ICMPv6, IGMP, ESP, AH, SCTP.
- **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.
- **Direction:** Select Inbound, Outbound or Dual indicating the direction of the traffic.

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

NOTE

Alternatively, in **Wireless LANs** configuration under **Firewall Options**, select the **Enable WLAN specific** option or map the firewall profile from the firewall drop-down list which has the L3 access control policy mapped to it.

Creating an L2 Access Control Policy

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 based on the MAC addresses that are configured. Further, L2 ACLs can also be used to allow-only or deny-only clients based on the ether types of the packet where EtherTypes is a field present in the ethernet header of a packet.

NOTE

If a tagged packet with Tag Protocol Identifier (TPID) value of 0x8100, 0x9100, or 0x88A8 is received, then instead of the TPID, the actual Ether-Type of the packet will be used for making the allow or block decision against the configured Ether-Types. If the mentioned TPID values need to be treated as Ether-Type to make the allow or block decision, configure the required TPID values in the custom Ether-Type list.

1. Select **Firewall > L2 Access Control**.

2. Click **Create**.

The **Create L2 Access Control Service** is displayed.

FIGURE 180 Creating an L2 Access Control Service

Create L2 Access Control Service

General Options

Name:

Description:

Rules

Restriction: Allow only the stations listed below Block only the stations listed below

MAC + Add Import CSV Cancel Delete

MAC

EtherTypes

Restriction: Allow only the EtherTypes listed below Block only the EtherTypes listed below

Standard EtherTypes

Protocol IPv4 (0x0800) + Add Cancel Delete

Protocol

If a tagged packet with TPID(Tag Protocol Identifier) value of 0x8100 or 0x9100 or 0x88A8 is received, then instead of the TPID, the actual Ether-Type of the packet will be used for making the allow/block decision(s) against configured Standard EtherType(s). If the mentioned TPID value(s) need to be treated as Ether-Type(s) to make allow/block decision(s), please configure the required TPID value(s) in the Use Defined EtherTypes list explicitly.

User Defined EtherTypes

Protocol name EtherType value + Add Cancel Delete

Protocol name EtherType value

OK **Cancel**

3. Configure the following options:
 - a. **General Options**
 - **Name:** Enter a name for this policy.
 - **Description:** Enter a short description for this policy.
 - b. **Rules**
 - **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**.
 - **MAC Address:** Enter the MAC address to which this L2 access policy applies and click **Add** or click **Import CSV** to import the MAC address.
 - c. **EtherTypes**
 - **Restriction:** The EtherType in the L2 ACL profile allows or blocks the specified EtherType traffic from the clients toward the network. Available options include **Allow only the EtherTypes listed below** or **Block only the EtherTypes listed below**.
 - **Standard Ether Types:** Select a protocol from the **Protocol** list to which this L2 access policy applies and click **Add**.
 - **User Defined Ether Types:** Enter a protocol name and EtherType value in hexadecimal format and click **Add**. A maximum of ten custom EtherTypes can be configured to be allowed or blocked.
4. Click **OK**.

NOTE

Alternatively, in the **Wireless LANs** configuration under **Firewall Options**, select the **Enable WLAN specific** option or map the firewall profile from the firewall list which has the L2 access control policy mapped to it.

NOTE

You can also edit, clone, or delete a policy by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **L2 Access Control** page.

Configuring Application Controls

Using the **Application Control** screen, you can identify, control, and monitor applications that are running on wireless and wired 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.

Viewing Application Control Summary

You can view application-wise or port-wise summary in a chart or table format.

To view the application control summary:

1. Select **Firewall > Application Control**. This displays the **Summary** page.
2. You can filter **Summary** with the following options:
 - **Count:** Select 10 or 25.
 - **Radio option:** Select Total, 2.4 GHz or 5GHz.
 - **Duration:** Select Last 1 hour, Last 24 hours, Last 7 days or 14 days.
 - **APs:** Select All APs or a specific AP.
 - **All Clients:** Displays all wired and wireless clients.

Creating an Application Control Policy

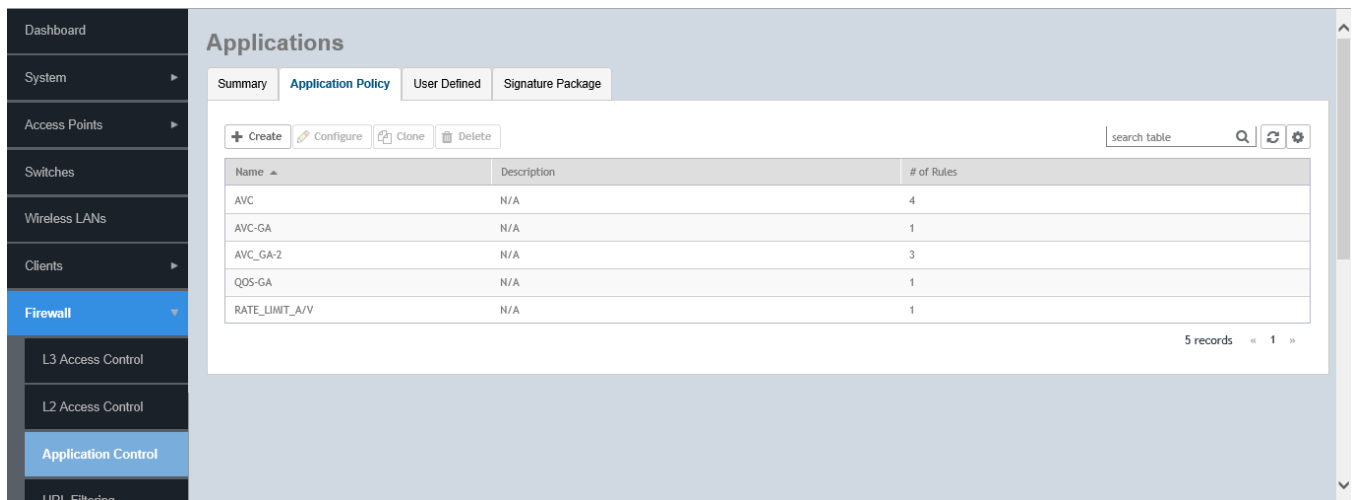
You must create an application policy to limit traffic by application, to classify traffic into priority queues using QoS traffic shaping rules, or to completely block access to an application.

Complete the following steps to create an application control policy:

1. Select **Firewall > Application Control**.
2. Click the **Application Policy** tab.

The **Application Policy** page is displayed.

FIGURE 181 Viewing Application Policy



The screenshot shows the 'Applications' page in a management console. The left sidebar contains a navigation menu with 'Firewall' selected, and 'Application Control' highlighted. The main content area has tabs for 'Summary', 'Application Policy', 'User Defined', and 'Signature Package'. The 'Application Policy' tab is active, displaying a table with columns 'Name', 'Description', and '# of Rules'. The table contains five rows of application policies. Below the table, it indicates '5 records' and a page navigation control showing '1'.

| Name | Description | # of Rules |
|----------------|-------------|------------|
| AVC | N/A | 4 |
| AVC-GA | N/A | 1 |
| AVC_GA-2 | N/A | 3 |
| QOS-GA | N/A | 1 |
| RATE_LIMIT_A/V | N/A | 1 |

3. Click **Create**.

The **Create Application Policy** page is displayed.

FIGURE 182 Creating an Application Policy

Create Application Policy

General Options

Name:

Description:

Rules

+ Create Configure Delete

| # | Rule Type | Content |
|---|-----------|---------|
| | | |

Logging

[?] Send App Logs to SZ: OFF Allow the AP to log every application event and send the events to SmartZone

[?] Enable Remote Syslog: OFF Allow the AP to log every application event and send the events to external syslog

OK Cancel

4. Under **General Options**, enter a policy name and description.

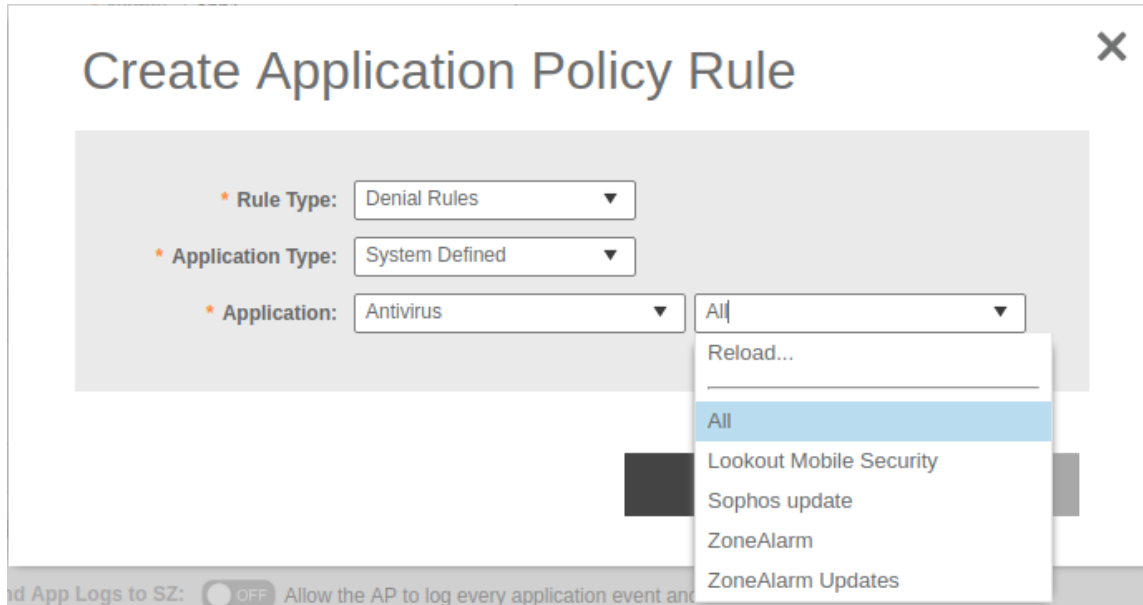
- Under **Rules**, click **Create** to create a new rule.

NOTE

Each application policy can contain up to 128 rules.

The **Create Application Policy Rule** page appears.

FIGURE 183 Creating an Application Policy Rule



- In the **Rule Type** field, select one of the following options:

- **Denial Rules**
- **QoS**
- **Rate Limiting**

- In **Application Type** field, select application type.

- In **Application** field, select the application for which you want to create a policy rule.

For example, if you select **All** in application category and save the application rule, the application rule list reflects all Anti-virus 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 send the events to SmartZone**
- **Allow the AP to log every application event and send 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 355.

Implementing an Application Control Policy

Deploying an application control policy involves configuring a Firewall Profile with the policy, and then applying that profile to a WLAN.

To implement an Application Control Policy:

1. Go to **Firewall > Application Control**.
Refer to [Creating an Application Control Policy](#) on page 352 for more information.
2. Go to **Wireless LANs**.
3. Locate the WLAN for which you want to apply the application policy, and select it from the list.
4. Click **Configure**. The **Edit WLAN [WLAN Name]** page appears.
5. Under **Firewall Options**, select the **Enable WLAN specific** option.
6. From **Application Control**, select an application control policy you created from the drop-down list. Alternatively, click **Create** to create a new application control policy.

7. Click **OK** to save your WLAN changes.

FIGURE 184 Select an Application Policy to apply to the Firewall Profile

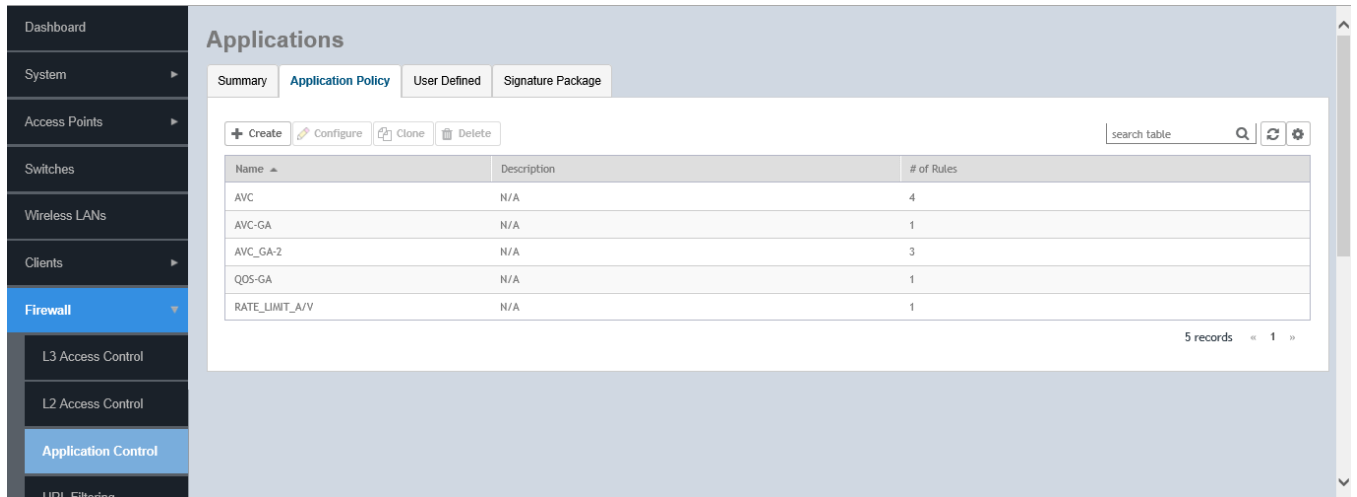


FIGURE 185 Apply the Application Control Policy to a WLAN



Creating an 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 **Firewall > Application Control**.
2. Select the **User Defined** tab.
3. Click **Create**.

The **Create User Defined Application** page appears.

FIGURE 186 Creating an User Defined Application

Create User Defined Application

* Name:

* Type: Default Port Mapping

* 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

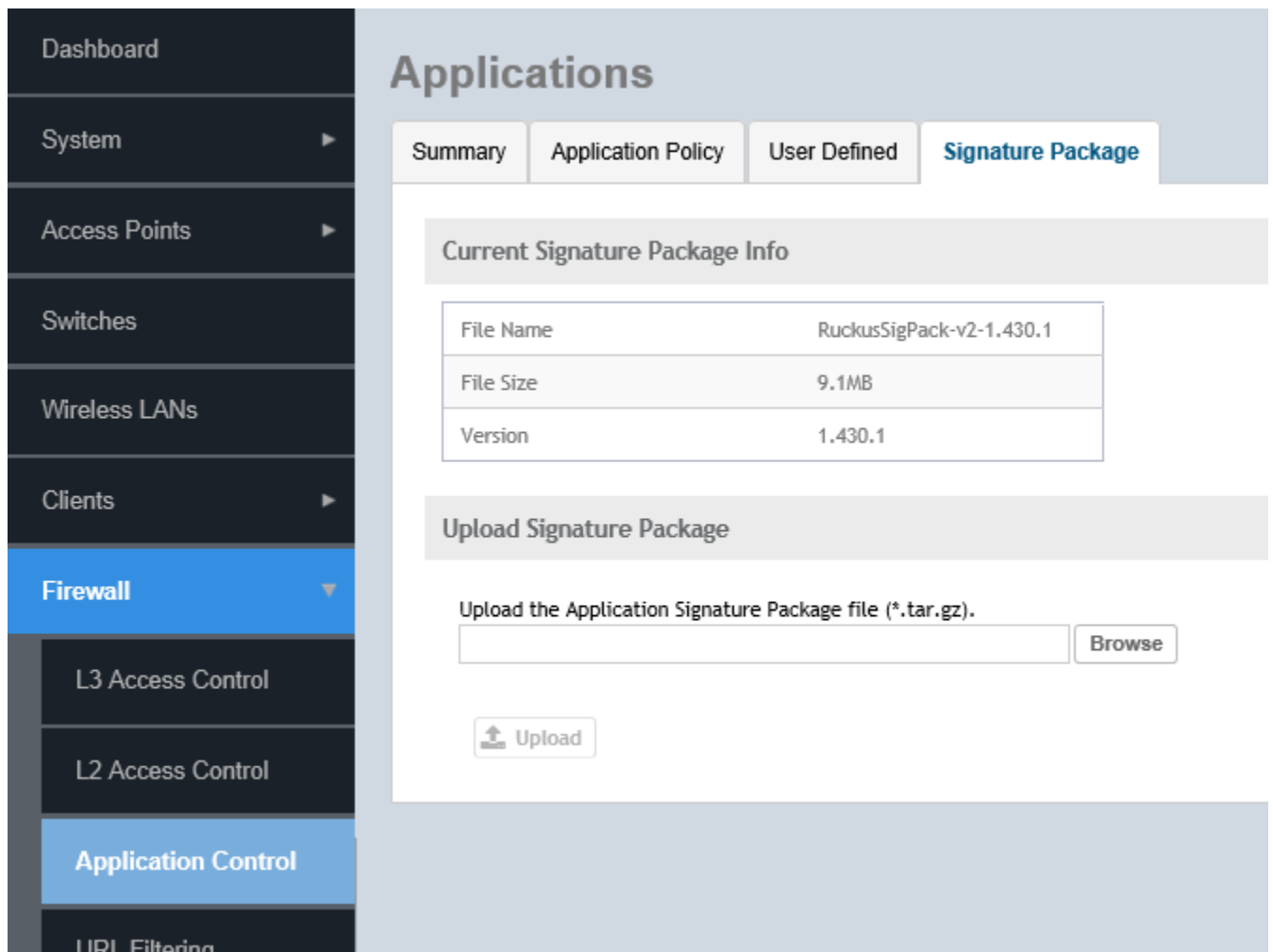
Ruckus will periodically release and make new application signature packages available for download.

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 **Firewall > Application Control**.
2. Select the **Signature Package** tab.

FIGURE 187 Viewing and Uploading Signature Package File Information



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.

```
get qmdpi-version : get qmdpi-version
                  == get version details of DPI

rkscli: get qmdpi-version
DPI Signature Version : RuckusSigPack-v2-1.430.1
DPI Engine Version   : 5.4.0-68.052 (build date Jun  3 2019)
DPI Bundle Version   : 1.430.0-20 (build date Apr 15 2019)

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 L3 Access Control Policy:

1. Go to **Firewall > L3 Access Control**.
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 profile and click **Delete**.

Step 2: Delete the Application Control Policy:

1. Go to **Firewall > 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 **Firewall > 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 L3 Access Control Policy with the details of the policy 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 **Firewall > URL Filtering**.

2. Select the **Profiles** tab, and then click **Create**.
The **Create URL Filtering Policy** page is displayed.

FIGURE 188 Creating a URL Filtering Policy

Create URL Filtering Policy

General Options

Blocked Categories

No adult content No adult content or nudity
 Clean and safe No adult content plus, no malware, spyware, phishing, botnet or spamware
 Child and student friendly Clean and safe plus no alcohol, intimate apparel, dating, or weapons
 Strict Child and student friendly plus no streaming media, personal storage and, games
 Custom 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 **+ Add** **✕ Cancel** **🗑 Delete**

Domain Name

Whitelist: * Domain Name **+ Add** **✕ Cancel** **🗑 Delete**

Domain Name

Safe Search

Google Safe Search: OFF

YouTube Safe Search: OFF

Bing Safe Search: OFF

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 Whitelist
- 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**.

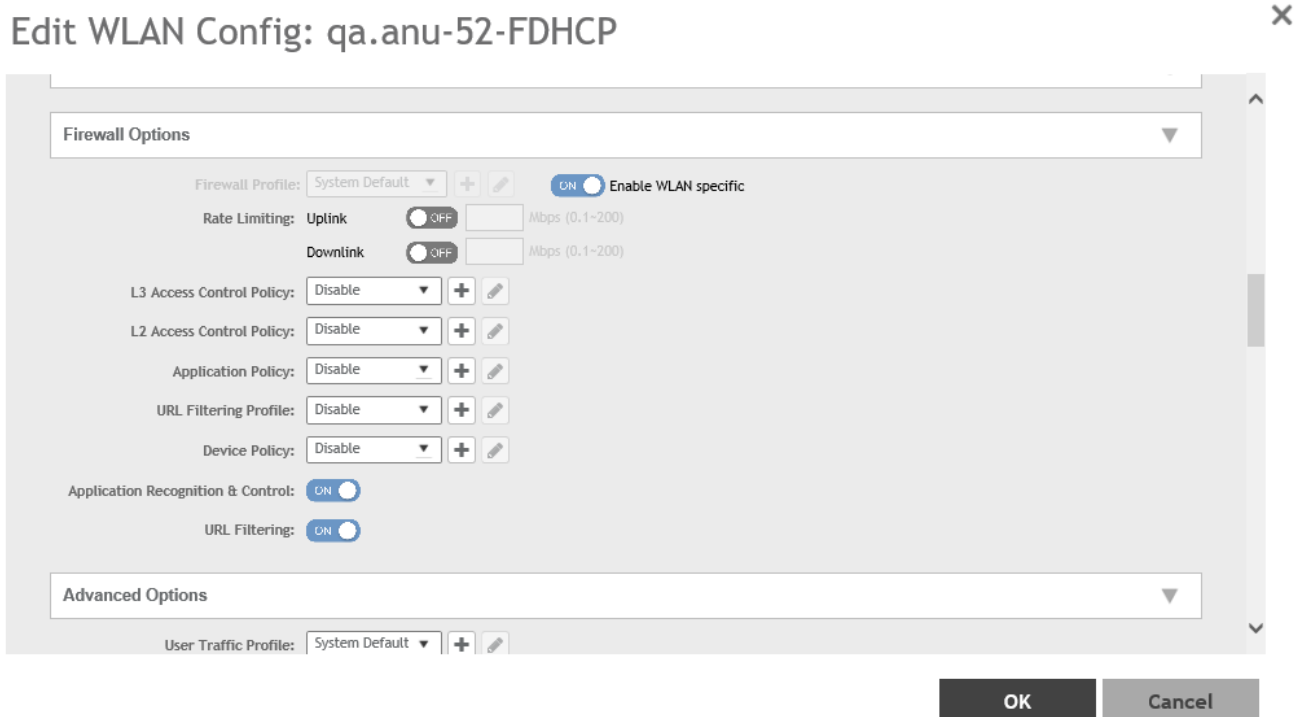
The **Wireless LANs** page appears.

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 360.

FIGURE 189 Enabling URL Filtering



NOTE

Application rules are applied based on the following priority, and user defined rules take precedence over URL filtering.

- a. User defined Access Control Profile
- b. URL Filtering
- c. Application Control Policy

You have enabled URL filtering on the controller.

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 67 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 | |

Creating a Device Policy

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 device policy service, the system can identify the type of client attempting to connect, and perform control actions such as allowing or blocking access, rate limiting, and VLAN tagging based on the OS rule.

To create a device policy:

1. Select **Firewall > Device Policy**. The **Device Policy Service** page is displayed.
The **Summary** tab displays the device policy services in chart and graph format. You can filter the profiles based on frequency, duration, APs and zone.
2. Select the **> Device Policy** tab, and then select the one for which you want to create the policy
3. Click **Create**.

The **Create Device Policy Service** page is displayed.

FIGURE 190 Creating a Device Policy Service

| Description | Device Type | OS Vendor | Access | Uplink Rate Limit | Downlink Rate Limit | VLAN |
|-------------|-------------|-----------|--------|-------------------|---------------------|------|
|-------------|-------------|-----------|--------|-------------------|---------------------|------|

4. Configure the following policy service details:
 - a. **Name:** Enter a name for the device policy.
 - b. **Description:** Enter a short description for this device 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. Under Rules, define the device policy rules. For more information Refer to [Creating Device Policy Rules](#) on page 367
 - e. Click **OK**.

NOTE

You can also edit, clone, and delete a service by selecting the options Configure, Clone, and Delete respectively, from the Device Policy tab.

Creating Device Policy Rules

You can create rules for every device policy service that you create.

1. Select Go to **Firewall > Device policy**. The **Device Policy Service** page is displayed.
2. Click **Create**. The **Create Device Policy Service** page appears
3. In **Rules**, click **Create**. The **Create Device Policy Rule** page is displayed.

FIGURE 191 Creating a Device Policy Rule

Create Device Policy Rule

* Description:

* Action:

* Device Type:

* OS Vendor:

Rate Limiting: Uplink Mbps (0.1~200)

Downlink Mbps (0.1~200)

VLAN:

OK Cancel

4. Configure the following policy rule details:
 - a. **Description:** Enter a short description for this device policy.
 - b. **Action:** Select Allow or Block. This is the action that the system will take if the client matches any of the attributes in the rule.
 - c. **Device Type:** Select from any of the supported device types. This feature is also supported on 11ax APs.
 - d. **OS Vendor:** Select from any of the supported OS types.
 - e. **Rate Limiting:** Enable the uplink and downlink rate limiting, and enter a rate limit value for each.
 - f. **VLAN:** Enter the number of the VLAN in which to segment the client type. The value ranges from 1 through 4094; if no value is entered, this policy does not impact device VLAN assignment.
 - g. Click **OK**.

Enabling the Device Policy Service

1. Select **Wireless LANs**

Managing a Firewall Profile
 Creating a Device Policy

2. Select the **Create/Configure** tab
3. Select **Firewall Options** to edit the required firewall profile

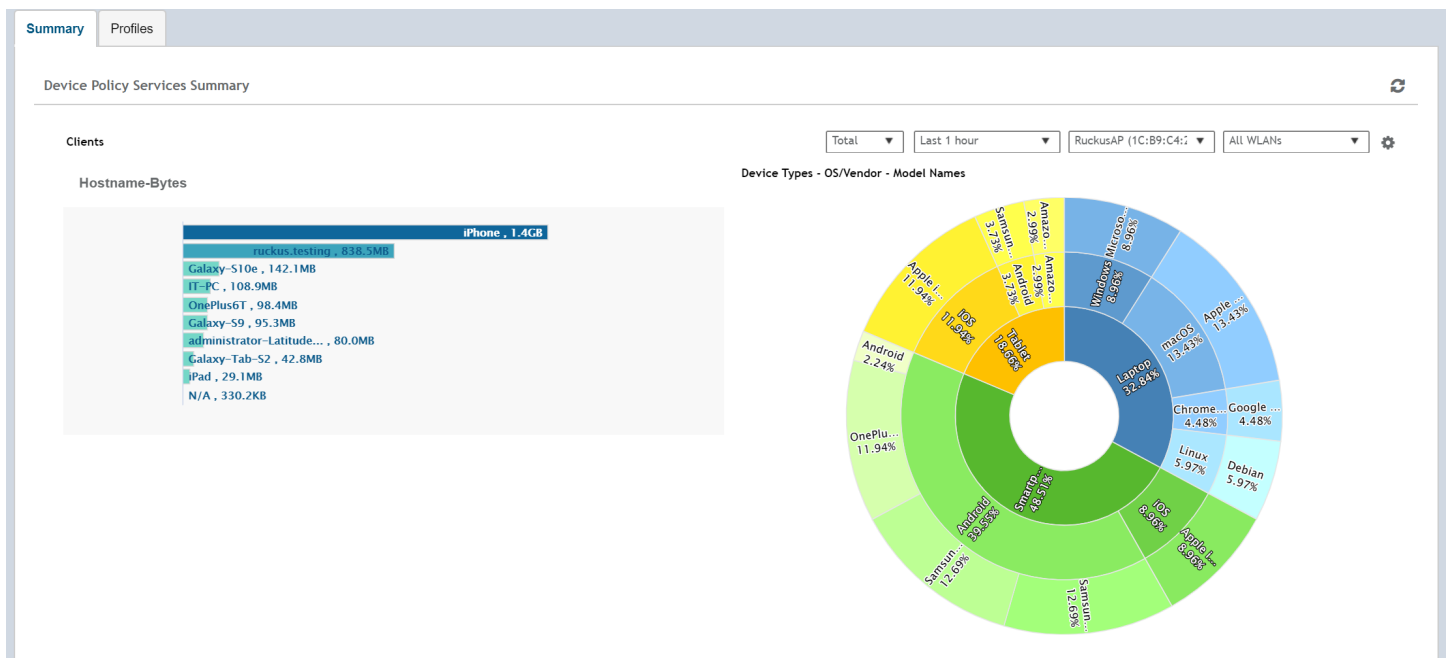
Summary

The summary tab displays device hardware and software attributes as charts.

To view wireless client attributes:

1. Click **Firewall**.
2. Select **Device Policy**. This displays the **Summary** page.

FIGURE 192 List of Devices



The graph has 3 zones -

- Outer zone - Displays the model names of device types.
- Central zone - Displays information of the operating system used by the device type or the vendor name.
- Inner Zone - Displays the device type.
- Core - Displays the number of clients connected. (Hover the mouse to view the information).

The **Device Policy Services Summary** screen has the following set of filters to view the graph:

TABLE 68 Filters

| Filter Name | Description |
|-------------------|---|
| Total/2.4GHz/5GHz | User can select the radio options from the drop down menu to generate the report. |

TABLE 68 Filters (continued)

| Filter Name | Description |
|---------------------------------------|--|
| Last report/Last 1 hour/Last 24 hours | User can select the options from the drop down menu generate the report. Last report - Accumlates stats of 180 seconds from the Access Point. Last 1 hour - Accumlates stats of 60 minutes from the Access Point. Last 24 hours - Accumlates stats of 24 hours from the Access Point. |
| All APs | By default displays details of the Access Point selected from Access Points tab. User can select the option from drop down menu to view a particular AP or all APs. |
| All WLANs | Displays the WLANs associated with each AP. User can select the option from drop down menu to view a particular WLAN or all WLANs. |
| Settings - Clients | User can set the preferred display settings. <p style="text-align: center;">NOTE The maximum clients displayed is 20.</p> |
| Host name - Bytes | This displays traffic consumed per client. |

Services and Profiles

- Working with Hotspots and Portals..... 371
- Configuring Access Control..... 391
- Understanding WiFi Calling..... 407
- Authentication..... 411
- Accounting..... 426
- Wireless Intrusion Detection and Prevention Services..... 430
- Bonjour..... 431
- Working with Tunnels and Ports..... 438
- Managing Core Network Tunnels..... 451
- DHCP/NAT..... 458
- 3rd Party Service..... 472
- Vendor-Specific Attribute (VSA) Profile..... 473

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 193 Creating a Guest Access Portal

Create Guest Access 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:

*

Guest Access

* Guest Pass SMS Gateway: Disabled

Terms and Conditions: Off

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:

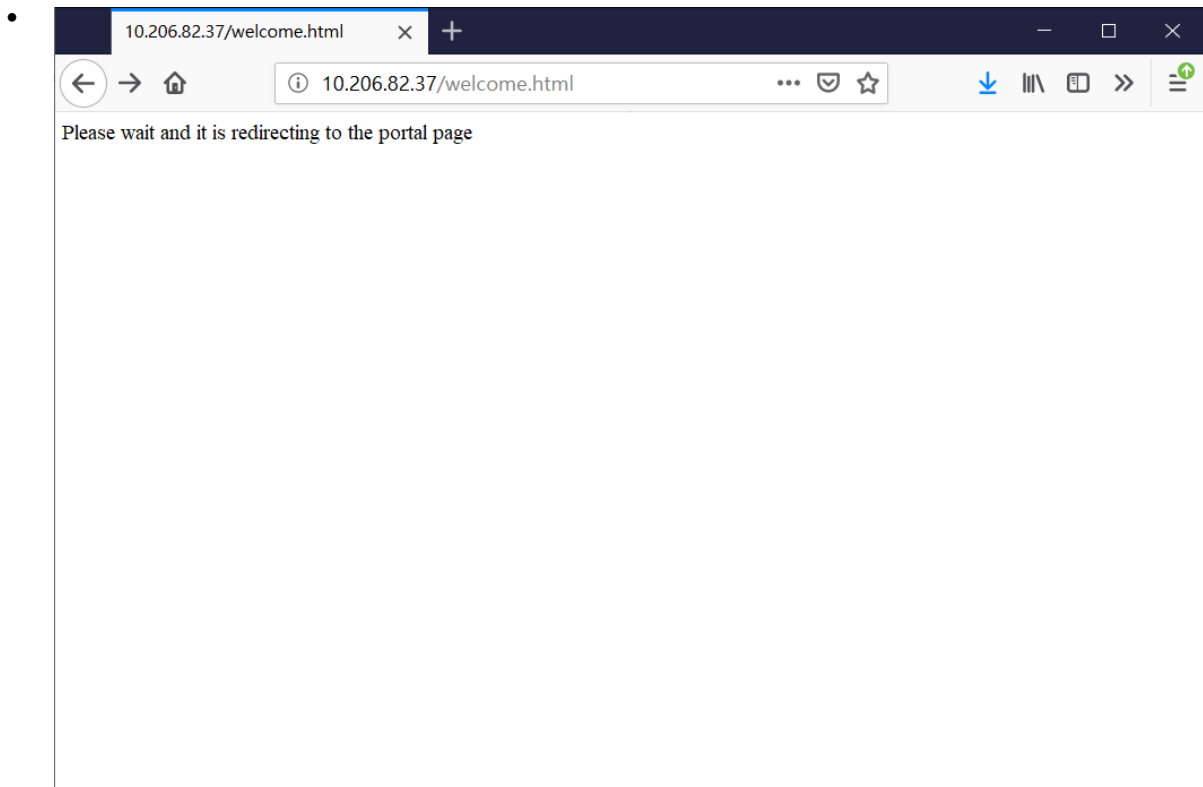
4. Configure the following:

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.
- "When the Guest Access Portal's Guest Authentication is "Always Accept" and the Guest Access doesn't enable the "Terms and Conditions", the client will be redirected to this page for 3 seconds and then go to the start URL or the original URL the browser opens".



After 3 seconds redirect to the Start Page.

Enter a domain name or IP address to which 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**.

Services and Profiles

Working with Hotspots and Portals

- 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.

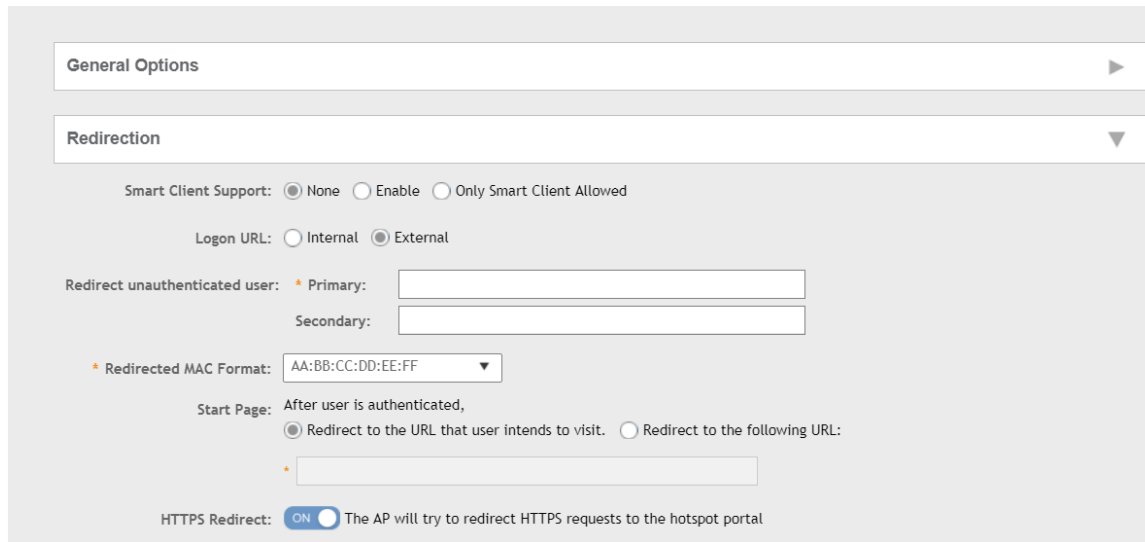
1. Go to **Services & Profiles > Hotspots & Portals**.
2. Select the **Hotspot (WISPr)** tab, and then select the zone for which you want to create the portal.

3. Click **Create**.

The **Create Hotspot (WISPr) Portal** page appears.

FIGURE 194 Creating a Hotspot (WISPr) Portal

Create Hotspot Portal



General Options ▶

Redirection ▼

Smart Client Support: None Enable Only Smart Client Allowed

Logon URL: Internal External

Redirect unauthenticated user: * Primary:
Secondary:

* Redirected MAC Format: AA:BB:CC:DD:EE:FF ▼

Start Page: After user is authenticated,
 Redirect to the URL that user intends to visit. Redirect to the following URL:
*

HTTPS Redirect: ON 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

The AP uses the secondary portal when the AP cannot 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 login web page the first time they connect to this WLAN, and requires them to log in 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 is displayed.

FIGURE 195 Creating a Web Authentication Portal

Create Web Authentication 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:

*

Web Authentication

[?] Web Portal Logo:

Web Portal Title:

User Session

* Session Timeout: Minutes (2-14400)

* Grace Period: Minutes (1-14399)

4. Configure the following options:

- 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.
- Redirection (Select where to redirect the user after successfully completing authentication.)
 - Redirect to the URL that user intends to visit: Allows the guest user to continue to destination URL without redirection.
 - Redirect to the following URL: Redirect the user to a specified web page (entered into the text box) prior to forwarding to the destination URL. When a guest user lands on this page, the guest pass expiration time is displayed.

Enter a domain name or IP address to which to be redirected.
- Web Authentication
 - Web Portal Logo: By default, the web portal page displays the Ruckus logo. To use your own logo, click the **Browse** button, select your web portal logo (recommended size is 138 x 40 pixels, maximum file size is 20 KB), and then click **Open**.
 - Web Portal Title: Type your own web portal title text or accept the default portal title text (Welcome to the Web Authentication login page).
- 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 in again.
 - Grace Period: Set the time period (in minutes) during which disconnected users are allowed access to the hotspot service without having to log in again.

5. Click **OK**.

You have completed creating a Web Authentication.

NOTE

You can also edit, clone,, and delete a Web Authentication 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.

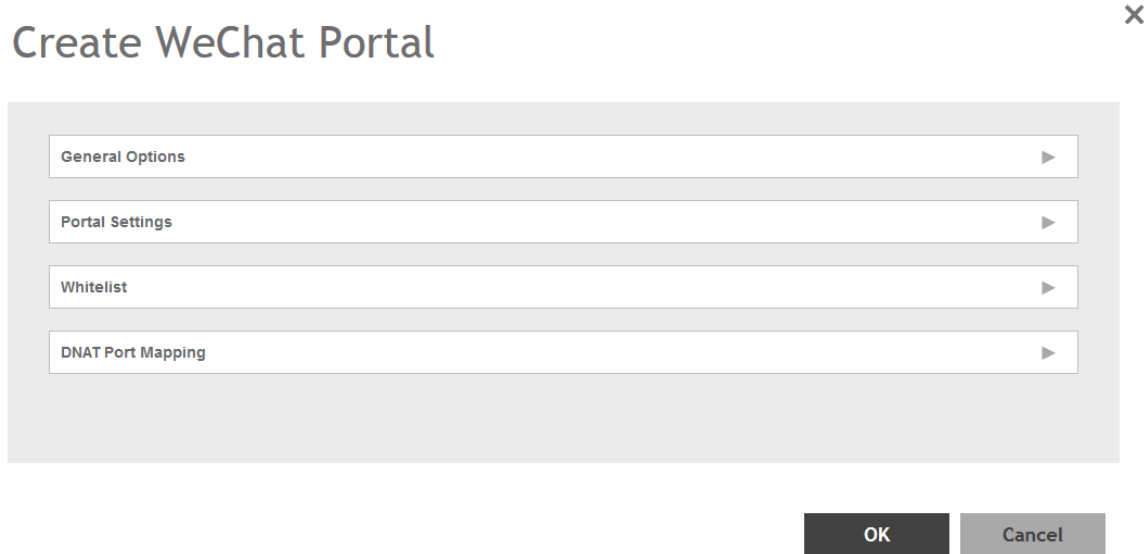
A WeChat portal defines the third party authentication server, also known as the equipment service provider (ESP) server, to which the controller will forward all WeChat authentication requests from wireless devices that are associated with controller-managed APs. In turn, the third party authentication 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 196 Creating a WeChat Portal



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.

Services and Profiles

Working with Hotspots and Portals

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 197 Creating a Hotspot 2.0 WLAN Profile

Create Hotspot 2.0 WLAN Profile

* Name:

Description:

* Operator: No data available

* Identity Providers: * Identity Provider No data available

| 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

OK

Cancel

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 383 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 384 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 198 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 text input field.
- Description:** A text input field.
- Domain Names:** A section with a "Domain Name" input field, an "+ Add" button, an "x Cancel" button, and a "Delete" button. Below this is a table with a "Domain Name" header and one empty row.
- 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 "Language" dropdown (set to "English"), a "Name" input field, an "+ Add" button, an "x Cancel" button, and a "Delete" button. Below this is a table with "Language" and "Name" headers and one empty row.

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.

Services and Profiles

Working with Hotspots and Portals

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 199 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 with 'Venue' selected.
- Venue Names:** A table with two columns: 'Language' and 'Name'. The 'Language' column has a dropdown menu with 'English' selected. The 'Name' column has a text input field. To the right of the table are three buttons: '+ Add', 'x Cancel', and a trash icon '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:

- a. **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.
- b. **Description:** Enter a description for the venue profile.
- c. **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

Services and Profiles

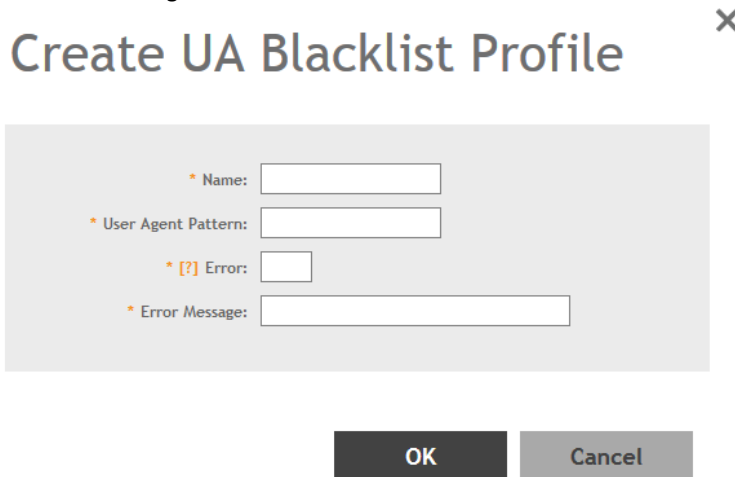
Working with Hotspots and Portals

- 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 200 Creating a UA Blacklist Profile



Create UA Blacklist Profile

* Name:

* User Agent Pattern:

* [?] Error:

* Error Message:

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 201 Creating Portal Detection Profile

Create Portal Detection Profile [X]

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.

5. Under **Portal Detection Patterns**, click **Create** to create a portal detection pattern.

The **Create a Portal Detection Pattern** page is displayed.

FIGURE 202 Creating Portal Detection Pattern

The screenshot shows a dialog box titled "Create Portal Detection Pattern" with a close button (X) in the top right corner. The dialog contains four input fields, each with a red asterisk indicating it is required: "Name", "User Agent Pattern" (with a help icon [?]), "HTTP Code", and "HTTP Response Body". Below the input fields are two buttons: "OK" and "Cancel".

6. In the **Name** field, enter the name of the portal detection pattern.
7. 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.

8. In the **HTTP Code** field, enter the code.

NOTE

The HTTP code range must be from 100 through 599.

9. In the **HTTP Response Body** field, enter the HTML string.
10. 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.

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.

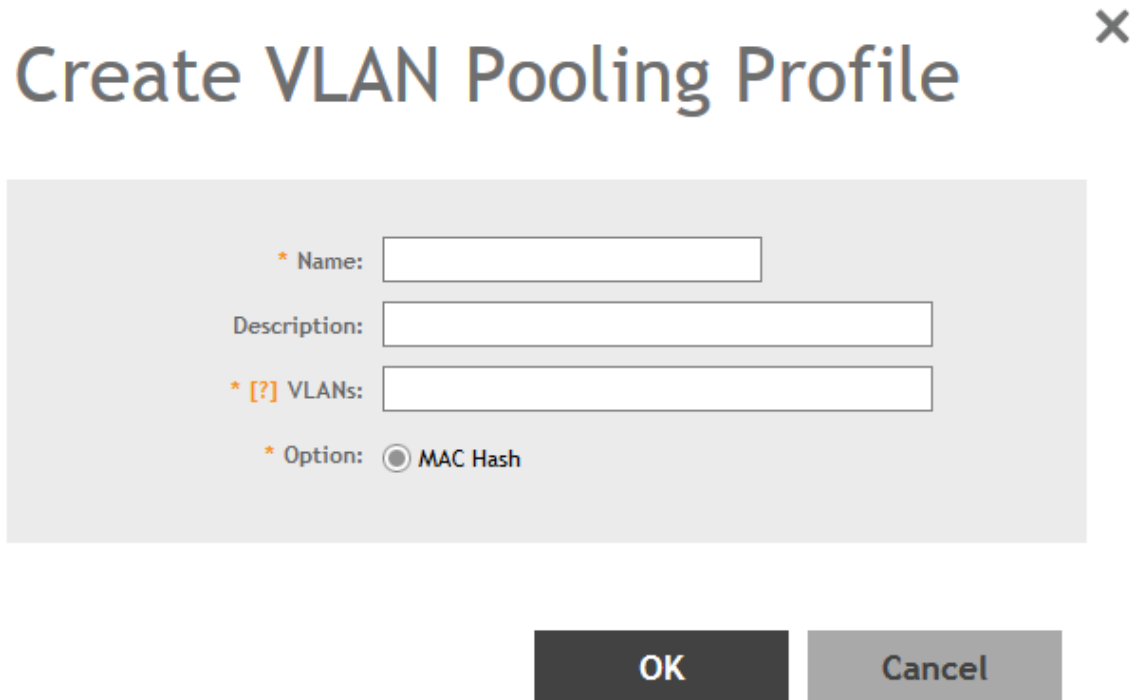
Creating a VLAN Pooling Profile

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 203 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 204 Creating a Create Precedence Profile

Create Precedence Profile

* Name:

VLAN Precedence ▼

↑ Up ↓ Down

| Priority | Description |
|----------|-------------|
| 1 | AAA |
| 2 | DEVICE |
| 3 | WLAN |

OK Cancel

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.

Restricted Access

The Restricted Access profile can be created without having any blocked ports or enabling well known and any entries in the whitelist ports.

Restricted Access Point(AP) profile can be configured multiple ways through SmartZone user interface.

The access point node on the network can be vulnerable to malicious attacks. Access Point(AP) is a critical node on the network and therefore such an attack can expose the whole network. The restricted access profile provides a mechanism to restrict unauthorized access to the AP and allows access only to authorized users thereby increasing the AP's inherent security.

NOTE

Maximum of 5 Restricted AP Access profiles can be created per zone.

The AP currently has the following categories of open ports:

TABLE 69 Well Known Ports on Access Points

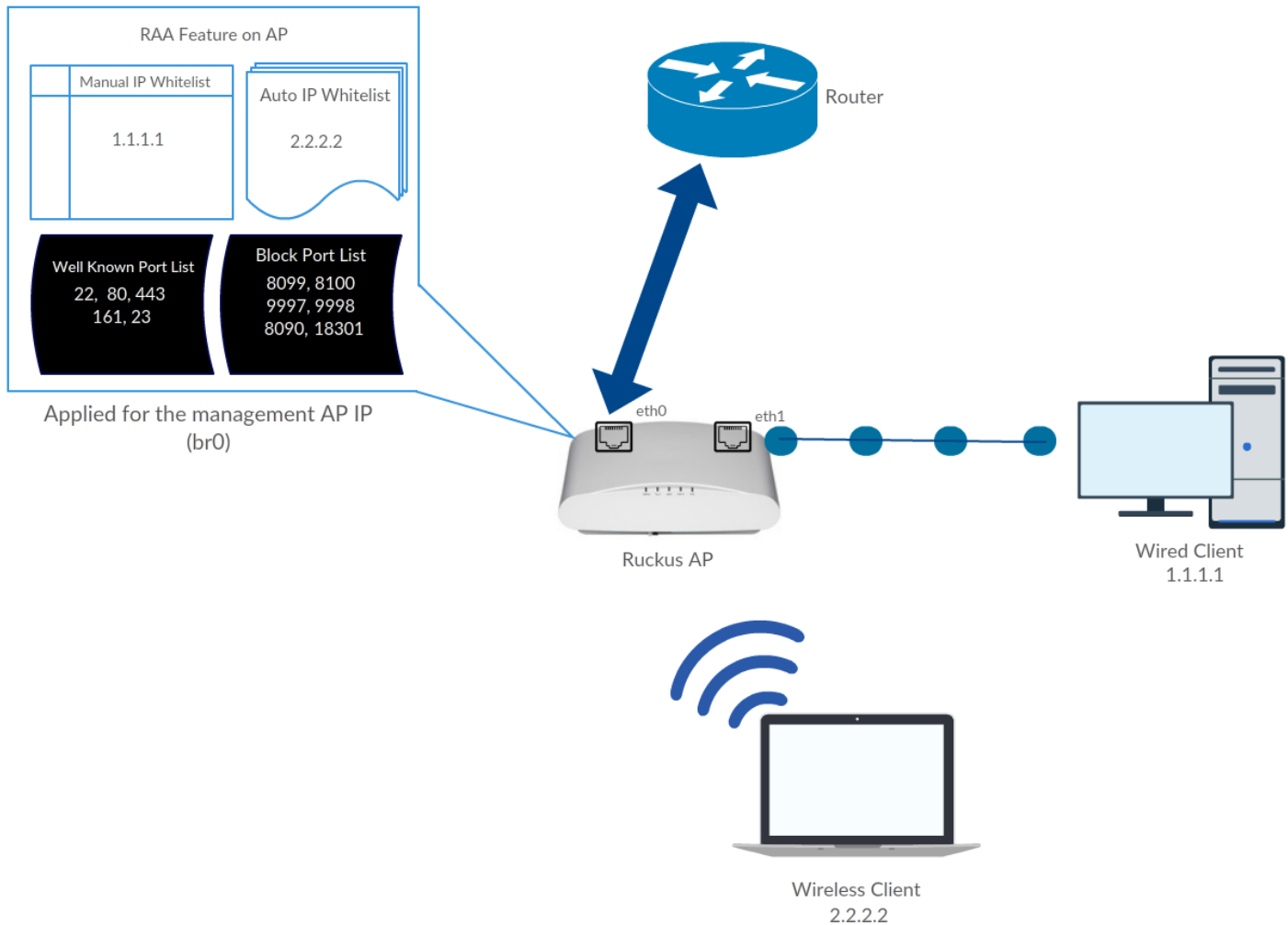
| Sl. No. | Port | Use | Protocol |
|---------|------|--------|-------------------|
| 1 | 80 | HTTP | TCP - IPv4 & IPv6 |
| 2 | 22 | SSH | TCP - IPv4 & IPv6 |
| 3 | 443 | HTTPS | TCP - IPv4 & IPv6 |
| 4 | 161 | SNMP | UDP - IPv4 & IPv6 |
| 5 | 23 | TELNET | TCP - IPv4 & IPv6 |

Overview

The Well known Port List includes the ports that are most likely to be exploited, with restricted access enabled, any node on the network trying to access the AP using these ports is blocked. This blocking functionality is configurable from the user interface by an administrator. The administrator can perform the following functions:

- The administrator can allow temporary or permanent access to these ports for an IP or a list of IPs (IP and Subnet). These IP(s) when configured are added to the Manual White List (Max 10) and these IP(s) are given unrestricted access to the AP.
- The administrator can add ports or a range of ports to the Port Black List (Max 10) as well. These ports will be inaccessible for any node on the network that is not part of the Manual White List as configured by the administrator.

FIGURE 205 Restricted Access Overview



Creating Restricted AP Access Profile

The Access Point (AP) is a critical node in the network that can be at risk of the malicious attacks as some of its ports are open. The Restricted AP Access Profile addresses this kind of risk and enhances AP's security.

Restricted AP Access protects the AP in the following ways.

1. By blocking access to the AP's standard well know open ports such as:
 - Port- 22 (TCP -IPv4 & IPv6) - For SSH Operation
 - Port- 23 (TCP - IPv4 & IPv6) - For Telnet Operation
 - Port- 80 (TCP - IPv4 & IPv6) - For HTTP Operation
 - Port- 443 (TCP - IPv4 & IPv6) - For HTTPs Operation
 - Port- 161 (UDP -IPv4 & IPv6) - For SNMP Operation

Services and Profiles

Configuring Access Control

2. By blocking access to AP's Internal ports (used mainly for Ruckus internal communication) such as:
 - Wisper internal ports
 - Port 9997 (http) : [Subscriber portal]
 - Port 9998 (https): [Subscriber portal]
 - Port 1997 (http): [Captive Portal Listening Server]
 - Port 1998 (https): [Captive Portal Listening Server]
 - Walled Garden internal Ports
 - Port 8090 (http) : [Subscriber portal]
 - Port 8099 (https) : [Subscriber portal]
 - Port 18090 (http) : Captive Portal Listening Server /Redirect server listen port]
 - Port 18099 (https): Captive Portal Listening Server/Redirect server listen port]
 - Speedflex Port 18301
 - Proxy Web server for Unauthorized UEs 8100
 - DNSMASQ 53
3. By providing a mechanism to block any ports or port range to restrict access.
4. By allowing AP to be accessed by authorized users.

To create a Restricted AP Access profile perform the following steps.

1. On the Controller web interface, Go to **Services & Profiles > Access Control**.
2. Select the **Restricted AP Access** tab, and then select the zone for which you want to create the policy.

3. Click **Create**.

The **Create Restricted AP Access Profile** page appears.

FIGURE 206 Creating Restricted AP Access Profile

Create Restricted AP Access Profile

Name:

Description:

Blocked Port List:

Protocol: Port:

+ Add X Cancel Delete

| Protocol | Port |
|----------|------|
| | |

OFF Block well known ports

List of well known ports

SSH: 22

TELNET: 23

HTTP: 80

HTTPS: 443

SNMP: 161

IP Address Whitelist:

IP:

+ Add X Cancel Delete

| IP |
|----|
| |

The SCG IP (10.1.13.64 / 2005::64) and the DP IP (10.148.124.64 / 2148::71e2:a8a3:5c8a:7fa5, 10.148.124.65 / ::) are whitelisted by default.

OK Cancel

4. Configure the following:
 - a. Name: Type the name of the profile.
 - b. Description: Type the description of the profile.
 - c. Blocked Port List: Select the protocol (TCP, UDP or Both) from the **Protocol** drop-down, and enter the port number in the **Port** field. You can click **Cancel** to re-type the entry or you can click **Add** to add the entries. The protocol and the port get listed in the table below the Blocked Port List. Click **Delete** to delete the values in the table.
 - d. Block well known ports: Enable the sidebar to block the well known ports.
 - e. IP Address Whitelist: When Restricted AP Access is enabled, network devices may use non-whitelisted IPv6 IP address for Restricted AP Access related operations, which may cause unexpected result. So, it is recommended to add ipv6 IP addresses manually.
5. Click **OK**.

You have created the Restricted AP Access profile.

Configuring Restricted Access via Services & Profiles

This topic describes configuring Restricted Access via Services & Profile tab.

1. Go to **Services & Profiles > Access Control**.
2. Click **Restricted Access** tab.
3. Select a **Zone** and click **Create**.

This displays **Create Restricted AP Access Profile** screen.

4. Enter the values in the fields and click **Ok**.

| Fields | Description |
|------------------------|--|
| Name | Restricted Access Profile name. |
| Description | Enter a description to identify the Restricted Access Profile. |
| Blocked Port List | <p>*Protocol - Choose the protocol for communicating from the drop down list (Both, TCP, UDP)</p> <p>*Port - Enter the port numbers. These port numbers will be added to the Blocked Port list.</p> <p>The port numbers can be deleted by selecting the same from the table.</p> |
| Block well known ports | To add all well know ports to the Blocked Port List, click the On/Off switch. The Block well known ports, by default is Off . |
| IP Address Whitelist | <p>*IP - Enter the IP addresses to allow the communication. These IP addresses will be part of the IP Address Whitelist.</p> <p>The IP Address can be deleted by selecting the same from the table.</p> |

5. The new Restricted AP Access profile is displayed in the **Restricted AP Access** drop-down list.

To enable the Restricted AP Access profile, refer [Enabling Restricted Access](#) on page 399 topic.

Configuring Restricted Access via Access Point

This topic describes the steps to configure Restricted AP Access Profile through Access Point tab.

1. Go to **Access Points > Access Points**.
2. Select a Zone from the left column and click **Configure selected Domain/Zone/Group**  icon.

This displays **Configure Group** screen.

3. In the **Configure Group** screen, navigate to **Advanced Options**. Locate **Restricted AP Access Profile** field.

To create a Restricted AP Access Profile, click **On/Off** button to **On**.

NOTE

By default the **On/Off** button is in the **Off** mode.

4. Click + to **Create Restricted AP Access Profile**.
This displays **Create Restricted AP Access Profile** screen.
5. Enter the details as provided in the [Configuring Restricted Access via Services & Profiles](#) on page 398 topic.
6. The new Restricted AP Access profile is displayed in the **Restricted AP Access** drop-down list.
7. Select the Restricted AP Access profile from the drop-down list to map the RA profile to a particular zone.

Configuring Restricted Access via Templates

This topic describes the steps to configure Restricted AP Access Profile through Templates tab.

1. Go to **System > Templates**.

This displays **Zone Templates** screen.

NOTE

To create a Restricted AP Access Profile via Templates, user has to create a new zone and map the zone to a group. To create a new zone, refer to the [Configuring Templates](#) on page 181 chapter.

2. After creating a new Zone Template, select the new zone and click **Configure**.

This displays **Edit Zone Template** screen.

3. Navigate to **Advanced Options** and click on **On/Off** button to **On**.

This highlights the greyed out **Restricted Access Profile**.


NOTE

By default the **Restricted Access Profile** is set to **Off** mode.

4. Click **+** to create a new **Restricted AP Access profile**.
5. Enter the details as provided in the [Configuring Restricted Access via Services & Profiles](#) on page 398 topic.
The new Restricted AP Access profile is displayed in the **Restricted AP Access** drop-down list.
6. Select the Restricted AP Access profile from the drop-down list to map the RA profile to a particular zone.

Enabling Restricted Access

To enable the Restricted Access, perform the following:

1. Go to **Access Points > Access Points**.
2. Select a Zone from the left column and click **Configure selected Domain/Zone/Group**  icon.
This displays **Configure selected Domain/Zone/Group**
3. Navigate to **Advanced Options**.
4. Click **On/Off** button to **On** mode.

NOTE

By default the **On/Off** button is in the **Off** mode.

This highlights the greyed out **Restricted AP Access Profile**. Select the RA profile from the drop-down list to enable the restricted access for the selected zone.

The selected **Restricted AP Access Profile** can be edited by clicking .

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 207 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 208 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 ▼

| MAC | IP Address | Description |
|-----|------------|-------------|
| | | |

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 209 Creating a Time Schedule Table
Create Time Schedules Table

Screenshot of the 'Create Time Schedules Table' form. The form includes two input fields: 'Schedule Name' (with a red asterisk) and 'Schedule Description'. Below these is a grid for defining the schedule. The grid has columns for hours (1-11 AM and 1-11 PM) and rows for days (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 210 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.

NOTE

This feature supports IPv4 format.

- d. Secondary DNS IP: Type the secondary DNS IP address.

NOTE

This feature supports IPv4 format.

- 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.

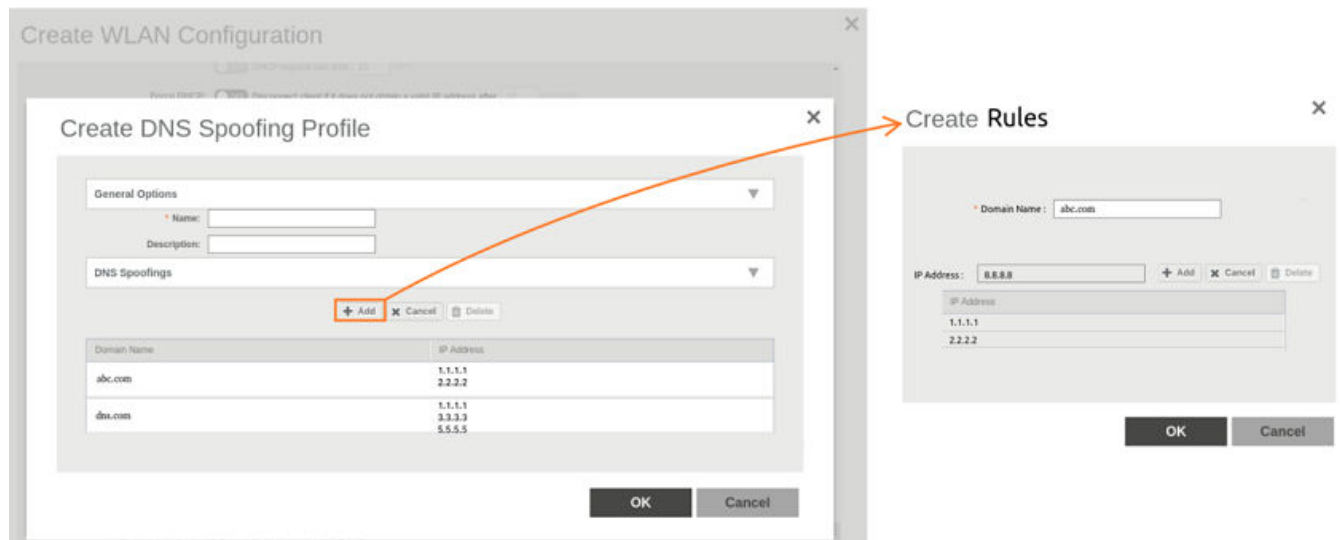
Creating a DNS Spoofing Profile

By creating a DNS spoofing profile, you can specify the IPv4 or IPv6 address of the DNS server. The AP then transmits the data packets to the DNS server.

1. Go to **Services and Profiles > Access Control**
2. Select the **DNS Spoofing** tab, and then select the zone for which you want to create profile.
3. Click **Create**.

The **Create DNS Spoofing Profile** page is displayed.

FIGURE 211 Creating DNS Spoofing Profile



4. Configure the following:
 - a) **Name**: Enter a name for the DNS spoofing profile.
 - b) **Description**: Enter a short description for the profile.
 - c) Click **Add**, and the **Create Rules** dialog box is displayed.
 - d) In the **Domain Name** field, enter the domain name of the DNS server, and in the **IP Address** field, enter the IPv4 or IPv6 of the DNS server. If the user sends DNS request with the domain name configured in the DNS Spoofing profile, then the AP responds with the IP address configured in the DNS Spoofing profile for the requested domain name. Click **OK** to confirm the rules.
 - e) Click **OK** to confirm the creation of DNS spoofing profile.

NOTE

You can also edit, clone or delete the profile by selecting the options **Configure**, **Clone** or **Delete** respectively, from the **DNS Spoofing** 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 212 Creating a Traffic Class Profile

Create Traffic Class Profile

General Options

* Name:

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 213 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.

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

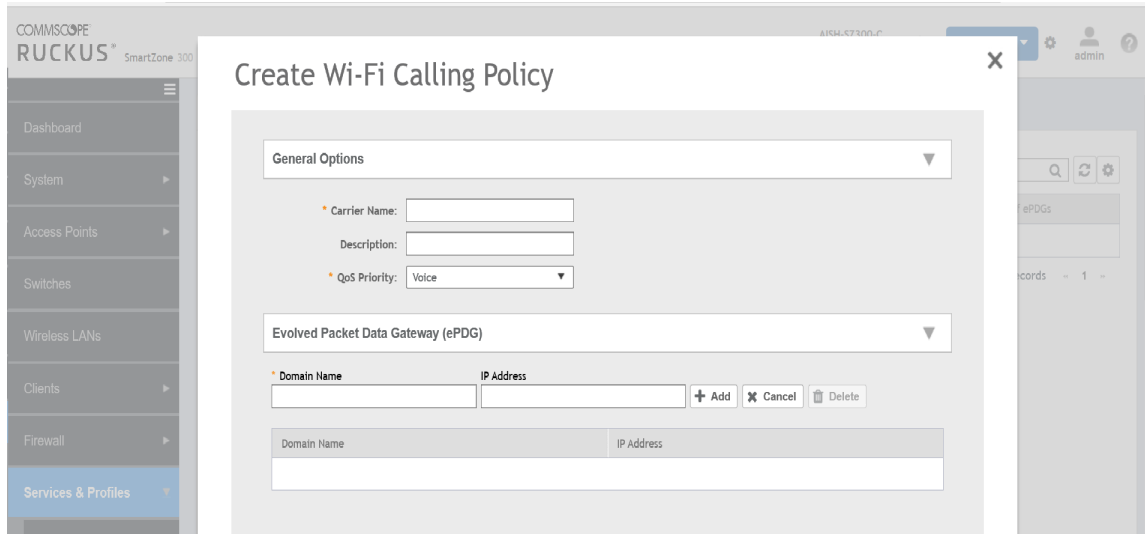
You can classify the voice packets in a WiFi call based on the carrier, by creating a WiFi calling profile.

1. Go to **Services & Profiles > WiFi Calling > Profiles**.

2. Click **Create**.

The **WiFi Calling Profile** page appears.

FIGURE 214 Creating a WiFi Calling Profile



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

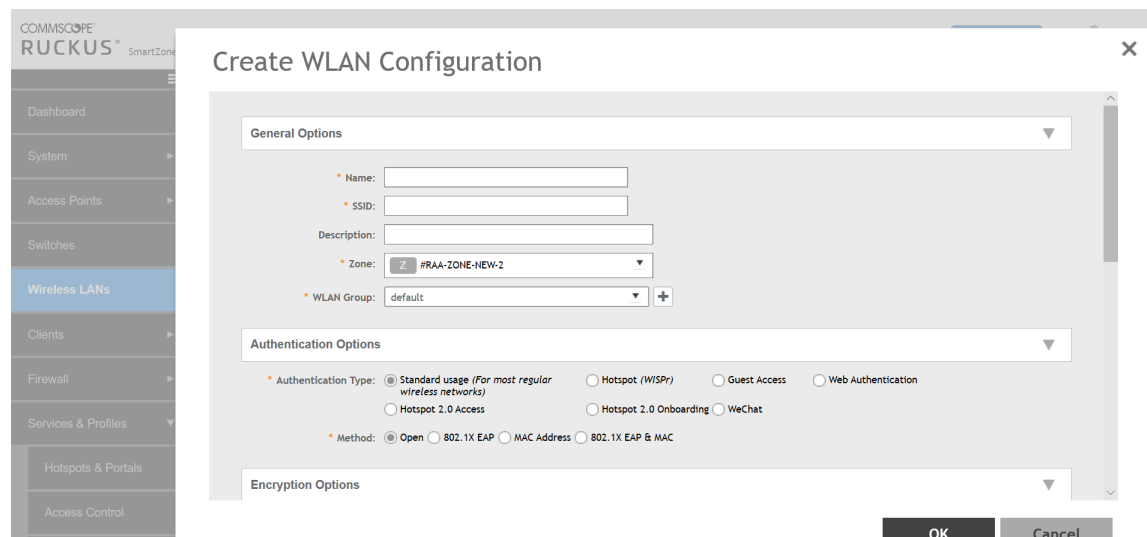
You can also edit the WLAN configuration to select a WiFi calling profile.

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 215 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 Wi-Fi Calling Statistics

You can view a summary of the Wi-Fi calling traffic by the top ten SSIDs by traffic and ePDGs by traffic. The trends provide information about the Wi-Fi usage, and uplink and downlink speeds.

Go to **Services & Profiles > WiFi Calling > Summary**.

The **WiFi Calling Clients** area provides the following information about clients using Wi-Fi Calling feature, such as:

- **Hostname:** The name of the user equipment or device that is connected to the Wi-Fi
- **MAC Address:** The MAC address of the user equipment
- **Carrier Name:** The name of the carrier network or service provider used by the user equipment, such as AT&T, Sprint, T-Mobile, and so on.
- **Priority:** The priority set for the Wi-Fi call through this device, such as voice, video, best effort, and background
- **Traffic Session:** The amount of data that is transmitted during the Wi-Fi call

- Traffic (uplink/downlink): The speed with which data is transmitted during the Wi-Fi call

FIGURE 216 Analyzing Wi-Fi Calling Traffic



The Clients detail section provides the following information about the client involved in the Wi-Fi call:

- AP MAC: The MAC address of the AP
- Client IP: The IP address of the client
- Carrier Name: The name of the carrier, for example, epdg.epc.att.net
- Start Time: The time when the client initiated the Wi-Fi call
- End Time: The time when the client completed the Wi-Fi call
- Traffic (uplink/downlink): The speed with which the data is transmitted during the Wi-Fi call session

FIGURE 217 Wi-Fi Calling Client Details

Wi-Fi Calling Clients

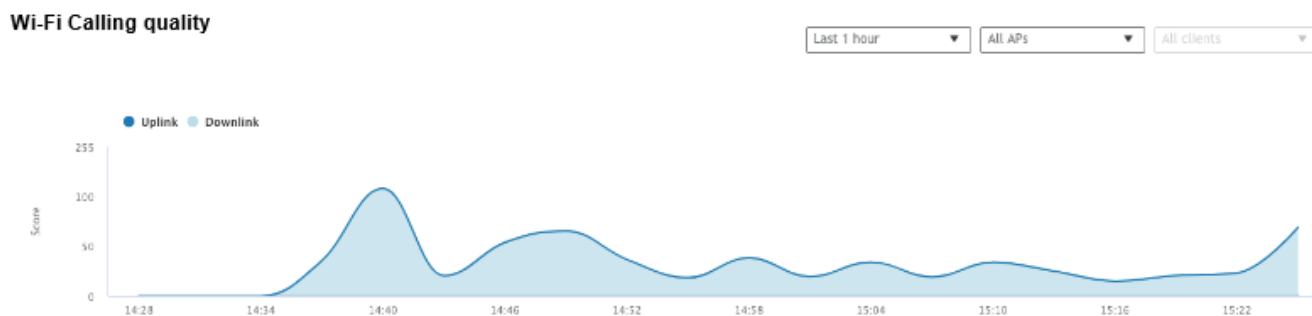
| Hostname | MAC Address | Carrier Name | Priority | Traffic (session) | Traffic (uplink) | Traffic (downlink) |
|------------------------|--------------------|--------------|----------|-------------------|------------------|--------------------|
| RovikIranAoltspart | 24:F3:94:96:25:c37 | att | Voice | 3.6MB | 2.0MB | 1.6MB |
| Samsung Galaxy S7 edge | 2C:9E:3D:39:BF:BD | tnoblic | Voice | 2.5MB | 1.2MB | 1.3MB |

Client Detail:

| AP MAC | Client IP | Carrier Name | Start Time | End Time | Traffic (uplink) | Traffic (downlink) |
|----------------------|--------------|------------------|---------------------|----------|------------------|--------------------|
| 1C:85:1C:45:2A:8F:50 | 10.150.5.155 | epdg.epc.att.net | 19/AU/1/18 19:12:24 | N/A | 1.1MB | 842.3KB |

The **Wi-Fi Calling quality** chart displays the uplink and downlink Wi-Fi calling quality. Call quality can be filtered based on Time, the AP list, and the client MAC address list.

FIGURE 218 Wi-Fi Call Quality Chart



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 219 Creating an AAA Server

Create AAA Server [Close]

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 417 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)

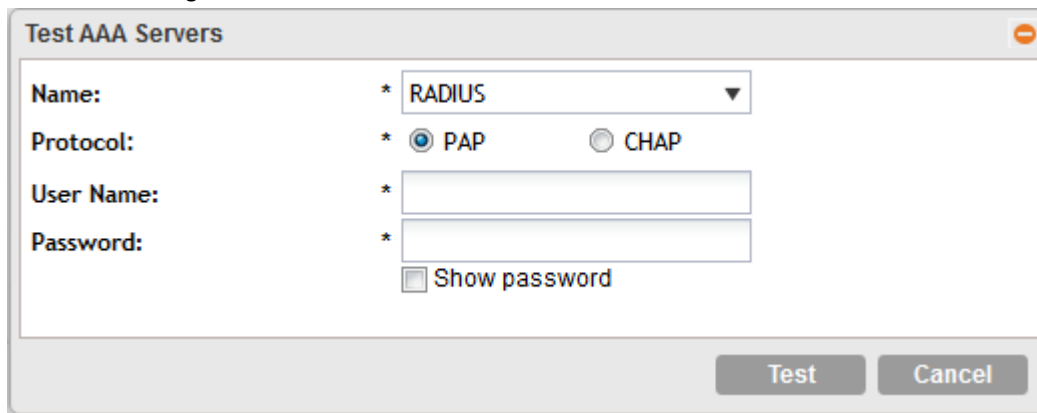
To ensure that the controller administrators will be able to authenticate successfully with the RADIUS server type that you selected, Ruckus strongly recommends testing the AAA server after you set it up.

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.

FIGURE 220 Testing an AAA Server



4. Configure the following:
 - a. Name: Select one of the AAA servers that you previous created.
 - b. Protocol: Select the Password Authentication Protocol (PAP), or the Challenge Handshake Authentication Protocol (CHAP) to authenticate the AAA server.
 - c. User Name: Type an existing user name on the AAA server that you selected.
 - d. 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 221 Creating an Authentication Service

Create Authentication Service ✕

Name:

Friendly Name:

Description:

Service Protocol: RADIUS Active Directory LDAP

ClusterRedundancy: OFF Enable Service for Standby Cluster

RADIUS Service Options

RFC 5580 Out of Band Location Delivery: OFF Enable for Ruckus AP Only

Primary Server

IP Address:

Port:

Shared Secret:

Confirm Secret:

Primary Server (Standby Cluster)

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 417 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 70 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 71 Secondary Server Options

| Option | Description |
|----------------|--|
| Backup RADIUS | Select Enable Secondary Server . 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 Automatic Fallback Disable 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 72 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>NOTE The zombie period is not started immediately after the Response Window expires, but after the configured Response Window plus $\frac{1}{4}$ 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 Yes to respond with a reject message to the NAS if no response is received from the RADIUS server. Click No 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 73 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> |
| Sanity Timer | <p>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.</p> |

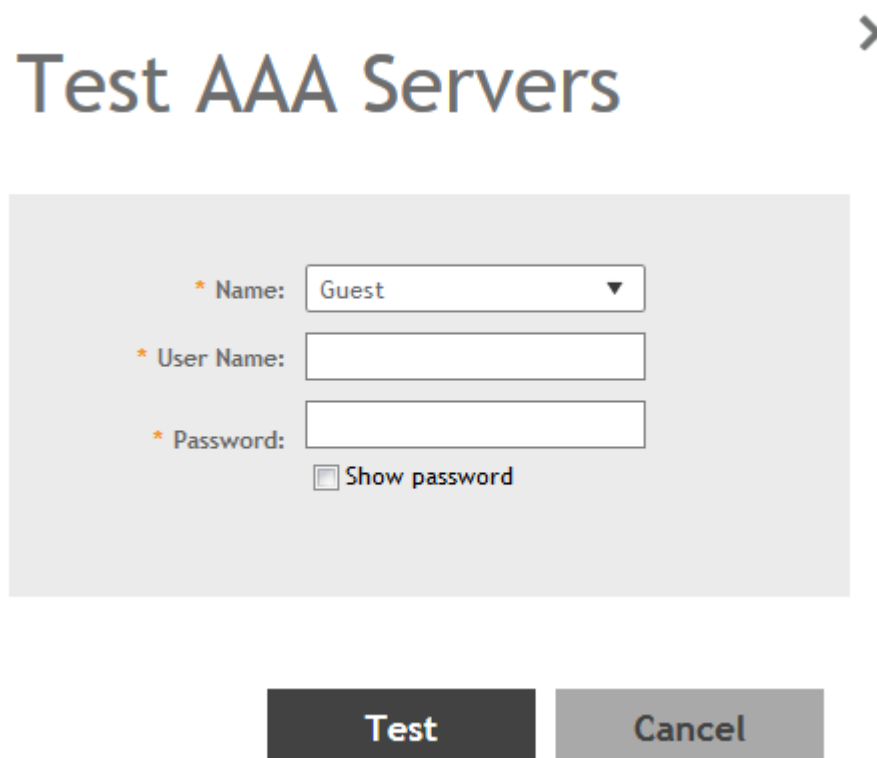
Testing AAA Servers

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 222 Testing an AAA Server



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 74 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 75 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 76 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 |

TABLE 76 Profile Configuration (continued)

| Feature | SZ100 | vSZ-E | vSZ-H | Description |
|--------------------------------|-------|-------|-------|---|
| 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 77 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 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. |

Services and Profiles

Authentication

TABLE 77 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 |
|--------------------|--------|-----------------|----------------|---------------|----------|---------------|----------|---|
| 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 78 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. NOTE From SmartZone release 3.4, UTP contains ACL and rate limit. |
| Dynamic ACL | | | | Ability to assign a specific ACL to a user through an attribute from the authentication source. NOTE ACLs are a part of a UTP. If you configure a UTP without a rate limit, you effectively only have an ACL. |
| Dynamic Rate Limit | | | | Ability to assign a specific Rate Limit to a user through an attribute from the authentication source. NOTE Rate limiting is also a part of a UTP. If you configure a UTP without ACL, you effectively only have a rate limiting policy. |

Other Authentication Features

The following table details authentication support for various authentication features.

TABLE 79 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 | Ability to test a specific username/password against a configured LDAP serve. NOTE Only Non-Proxy LDAP is supported at the Zone Level. |
| 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 80 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. |

TABLE 80 PAP/CHAP Support (continued)

| Feature | 802.1X | Web Auth | Hotspot/ WISPr | MAC Auth | Notes |
|------------------------|--------|----------|----------------|----------|--|
| 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.

Creating Realm Based Authentication Profile

An authentication profile defines the authentication policy when the controller is used as a Radius proxy service for WLANs.

1. Go to **Services & Profiles > Authentication**.
2. Select the **Realm Based Proxy** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

The **Create Authentication Profile** page appears.

FIGURE 223 Creating a Realm Based Proxy Authentication Profile

Create Authentication Profile

Name:

Description:

OFF Enable Hosted AAA Support OFF Configure PLMN identifier

Realm Based Authentication Service

+ Create

| Realm | Protocol | Auth Service | Auth Method | Dynamic VLAN ID |
|-------------|----------|--------------|----------------|-----------------|
| No Match | NA | NA-Disabled | NonGPPCallFlow | N/A |
| Unspecified | NA | NA-Disabled | NonGPPCallFlow | N/A |

Note: If device onboarding was done with credential type 'remote', then map your 'realm' value to its respective authentication service PLUS define 'Unspecified' realm & map it to corresponding authentication service to properly handle legacy (non-Hotspot 2.0) devices.

OK **Cancel**

4. Configure the following:
 - a. Name: Type a name for the authentication service profile that you are creating.
 - b. Description: Type a short description of the authentication service profile.
 - c. To enable hosted AAA support, select the **Enable Hosted AAA Support** check box, and then configure these options:
 1. Interim Accounting Interval (secs): Set the interim time interval for RADIUS clients to send accounting updates. Default is 0, which indicates that the accounting interval is disabled.
 2. Sessions Timeout (secs): Set a time limit after which users will be disconnected and required to log on again.
 3. Session Idle Timeout (secs): Set a value in seconds (60 to 600) after which idle clients will be disconnected.
 - d. Select the **Configure PLMN Identifier** check-box, and set the following options:
 1. Mobile Country Code: Set the correct country code for the geographical location.
 2. Mobile Network Code: Set the mobile network code based on the geographical location.

NOTE

Enable this option if you want to configure the authentication service profile for TTG WLANs.

- e. Realm-Based Authentication Service
 - Realm: Type where the realm is No Match or Unspecified.
 - Auth Service: Select a default authentication service for the realm.
 - Auth Method: Select an authorization method as 3GPP or Non-3GPP call flow.
 - Dynamic VLAN ID: Type the vlan ID.
 - f.
 - 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.
5. Click **OK**.

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 224 Creating an AAA Server

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 419

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 225 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 417.
 - 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 419

NOTE

You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Proxy** tab.

Creating Realm Based Proxy

An accounting profile defines the accounting policy when the controller is used as a RADIUS proxy for WLAN services.

1. Go to **Services & Profiles > Accounting**.
2. Select the **Realm Based Proxy** tab, and then select the zone for which you want to create the AAA server.
3. Click **Create**.

The **Create Accounting Profile** page appears.

FIGURE 226 Creating an Accounting Profile

Create Accounting Profile

The screenshot shows the 'Create Accounting Profile' configuration page. At the top, there are two input fields: 'Name' and 'Description'. Below them is a dropdown menu labeled 'Accounting Service Per Realm'. Underneath is a table with two columns: 'Realm' and 'Accounting Service'. The table has two rows: 'No Match' and 'Unspecified', both with 'NA-Disabled' as the Accounting Service. There are '+ Add', 'x Cancel', and 'Delete' buttons for the table. At the bottom right, there are 'OK' and 'Cancel' buttons.

| Realm | Accounting Service |
|-------------|--------------------|
| No Match | NA-Disabled |
| Unspecified | NA-Disabled |

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. Accounting Service per Realm: Specify the accounting service for each of the realms specified in this table. If you set the accounting service for a particular realm to NA-Disabled, then the accounting request is rejected. To create a new service click, **Create** and then configure **Realm** and **Accounting Service**.
5. Click **OK**.

Services and Profiles

Wireless Intrusion Detection and Prevention Services

You have completed creating a Realm-based proxy Accounting AAA server.

NOTE

You can also edit, clone and delete an AAA server by selecting the options **Configure**, **Clone** and **Delete** respectively, from the **Realm Based Proxy** tab.

Wireless Intrusion Detection and Prevention Services

Wireless Intrusion Detection and Prevention Services (WIDS/WIPS) is a security system that monitors a WLAN for any threats from rogue devices.

Classifying a Rogue Policy

You can create rogue classification policy with rules at the zone and monitoring group level. This helps in automatic classification behavior when a specific-rogue detection criteria are met.

Complete the following steps to create a rogue classification policy.

1. Select **Services & Profiles > WIPS**.
2. Under **Policy**, select the zone for which you want to create the policy and click **Create**.

FIGURE 227 Creating a Rogue Classification Policy

Create Rogue Classification Policy

Name:

Description:

Rogue Classification Rules

+ Create Configure Delete Up Down search table

| Priority | Name | Type and Criteria | Classification |
|----------|------|-------------------|----------------|
|----------|------|-------------------|----------------|

OK Cancel

3. Enter the policy name and description.

4. Under **Rogue Classification Rules**, click **Create** and complete the following steps to create a rogue classification rule.
 - a) In the **Name** field, enter the rule name.
 - b) Under **Rule Type**, select one from the following rule type for classification:
 - **Ad Hoc**: The monitoring AP is able to detect the ad hoc network as a rogue.
 - **Clear to Send (CTS) Abuse**: Reported when the number of CTS frames per second to a specific receiver MAC address exceeds the specific threshold. The default number of frames per second is 50.
 - **Deauth Flood**: Reported when the number of deauthentication frames per second exceeds the specific threshold from a specific transmitter. The default number of frames per second is 50.
 - **Disassoc Flood**: Reported when the number of disassociation frames per second exceeds the specific threshold from specific transmitter. The default number of frames per second is 50.
 - **Excessive Power**
 - **Low RSSI**: In the **Signal Threshold** field, enter the RSSI threshold in dBm.
 - **MAC OUI**: In the **MAC OUI** field, enter the first three octets of the MAC address. For example, for a MAC address 11:22:33:44:55:66, the MAC OUI is 11:22:33.
 - **MAC (BSSID) Spoofing**
 - **Request to Send (RTS) Abuse**: Reported when the number of RTS frames per second to a specific receiver MAC address exceeds the specific threshold. The default number of frames per second is 50.
 - **Same Network**
 - **SSID**: Enter the partial or complete SSID string regardless of the zone being configured with the specific SSID.
 - **NULL SSID**
 - **SSID Spoofing**: Enter the SSID that is configured in a specific zone from a non-managed AP.
 - c) Under **Classification**, select one of the following actions to be taken for the selected rule type:
 - **Ignore**
 - **Know**
 - **Malicious**
 - **Rogue**
 - d) Click **OK** to save the changes.
5. Click **OK**.

NOTE

Click **Configure** or **Delete** to edit or delete a rogue classification policy respectively. To prioritize a 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.

Services and Profiles

Bonjour

SmartZone provides two features for controlling how and where Bonjour services are available to clients:

- [Bonjour Gateway](#) on page 432: Bridge Bonjour services from one VLAN to another.
- [Bonjour Fencing](#) on page 433: 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 228 Creating a Bonjour Gateway Policy

Create Bonjour Policy

* Name:

Description:

Rules

| Priority | Bridge Service | From VLAN | To VLAN | Notes |
|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

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 433.

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.

Services and Profiles

Bonjour

- 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)

NOTE

If hop 0 and hop 1 service records come in the same packet from a Bonjour server, AP will always give priority to hop 1 service record. Since tagging happens for hop1 service, hop 0 service can also be discovered by Bonjour clients.

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.

NOTE

Bonjour Fencing for a particular service does not work if another service from same server which is not fenced is enabled simultaneously.

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 229 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 230 Fencing Rule

The screenshot shows a configuration window titled "Fencing Rule" with a close button in the top right corner. The window contains the following fields and controls:

- Device Type:** A dropdown menu set to "Wired".
- Closest AP:** A dropdown menu set to "No data available".
- Service:** A dropdown menu set to "Other".
- Custom Service Name:** An empty text input field.
- Fencing Range:** A dropdown menu set to "Same AP".
- Description:** An empty text input field.
- Device MAC:** A label "Device MAC:" followed by a "MAC" label and an empty text input field. To the right of this field are three buttons: "+ Add", "X Cancel", and a trash icon labeled "Delete".

At the bottom of the dialog, there are two large buttons: "OK" and "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 231 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 232 Creating a Ruckus GRE Profile

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 233 Creating a Soft GRE Profile

3. Enter profile name and description.
4. Under **Gateway IP Mode**, select **IPv4** or **IPv6** 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

This feature is supported on both 11ac and 11ax APs.

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 234 Creating an IPsec Profile

Create IPsec profile

General Options

Name:

Description:

Security Gateway:

Tunnel Mode: SoftGRE RuckusGRE

Authentication

Type: Preshared Key Certificate

Security Association

IKE Proposal Type: Default Specific

ESP Proposal Type: Default Specific

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.

NOTE

This option appears only when SoftGRE Tunnel Mode option is selected.

- d. IP Mode: Select IPv4 or IPv6 addressing modes
- 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.

NOTE

For the RuckusGRE Tunnel mode option the following IKE and ESP proposals are supported:

- AES128-SHA1-MODP2048
- AES256-SHA384-ECP384

IKE encryption proposals should be greater than or equal to ESP encryption proposal. RuckusGRE over IPsec supports IKEv2 authentication by X.509 certificate only.

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 trying 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. Select **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 is displayed.

FIGURE 235 Creating an Ethernet Port Profile

Create Ethernet Port ✕

General Options ▶

Ethernet Port Usage ▼

• Access Network: Default WAN
 Local Subnet(LAN)
 Tunnel Ethernet Port traffic

Anti-spoofing: OFF
 OFF ARP request rate limit ppm
 OFF DHCP request rate limit ppm

• User Side Port: OFF Number of clients allowed to be connected

Authentication Options ▶

VLAN Options ▶

Firewall Options ▼

Firewall Profile: + ✎

Rate Limiting and Device policy features are not supported with wired clients.
Firewall Profile is only functional when User Side Port is enabled.

Application Recognition & Control: OFF

URL Filtering Policy: OFF

L2 Access Control Policy: + ✎

OK **Cancel**

4. Configure the following options:

a. General Options

1. **Name:** Enter a name for the Ethernet port profile that you are creating.
2. **Description:** Enter 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, you can configure the Ethernet ports to be used for the wired client. If you select a non-user port, there is no restriction on the number of clients supported. If the User Side Port is selected, the maximum number of supported clients is 32 and this number is configurable.

b. Ethernet Port Usage

1. **Access Network:** Select this check box to enable tunneling on the Ethernet port.
2. **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:** The ARP request rate limits the number of ARP requests from the connected clients to prevent ARP flooding. Enter the number of packets to be reviewed for Address Resolution Protocol (ARP) attacks per minute. In ARP attacks, a rogue client sends messages to a genuine client to establish connection over the network.
 - **DHCP request rate limit:** The DHCP request rate limits the number of DHCP requests from the connected clients to prevent DHCP flooding. Enter the number of packets to be reviewed for DHCP pool exhaustion, per minute. When rogue 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 may miss out on obtaining the IP addresses.

NOTE

When you enable anti-spoofing, an ARP request rate limiter and a DHCP request rate limiter are automatically enabled with default values (in 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 and DHCP request packets per minute (ppm). The "X" value is configured on the interface to which the client is connected.

NOTE

Force-DHCP will be enabled by default when anti-spoofing is enabled, and it cannot be changed after anti-spoofing is enabled.

3. **User Side Port:** The Ethernet port must be configured as a User Side Port for QinQ to work.
 - **Number of clients allowed to be connected:** Enter the number of clients that can be connected to the User Side Port. The maximum number of clients that can be connected is 32.

c. Authentication Options

1. **802.1X:** Select this check box to enable 802.1X authentication.
2. **Enable client visibility regardless of 802.1X authentication:** If client visibility is enabled, you can view connected wired client information. The client visibility check box is enabled by default if the 802.1x authentication method is selected. For the open authentication method, you must enable client visibility based on your requirements.

NOTE

You can view statistical information about wired clients without enabling 802.1X authentication.

3. **802.1X Role:** Select the authenticator role from the menu. Options include Supplicant, MAC-based Authenticator, and Port-based Authenticator. When you select Supplicant, you can customize the user name 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 address 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.

d. VLAN Options

1. **VLAN Untag ID:** Enter 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 VLAN Untag ID of the AP Trunk port with the native VLAN used throughout your network.
2. **VLAN Members:** Enter the VLAN IDs that you want to use to tag WLAN traffic that will use this profile. You can enter a single VLAN ID or a VLAN ID range (or a combination of both). The valid VLAN ID range is from 1 through 4094.
3. **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 must define on the RADIUS server the VLAN IDs that you want to assign to users.

NOTE

The Enable Dynamic 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.

4. **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.
5. **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

NOTE

For QinQ VLAN to work, the User Side Port and Enable Dynamic VLAN must be enabled.

e. Authentication and Accounting Services

1. **Authentication Server:** Select the check box and a controller from the menu to use the controller as a proxy authentication server.
2. **Accounting Server:** Select the check box and a controller from the 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 (user name and password).

f. 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.



g. Firewall Options

NOTE

The User Side Port must be enabled to configure the Firewall Profile, Application Recognition and Control, and URL Filtering Policy.

Services and Profiles

Working with Tunnels and Ports

1. Firewall Profile: Select the firewall profile for wired ports.
 2. Application Recognition and Control: Enable the option for the wired clients.
 3. URL Filtering Policy: Enable the option for the wired clients.
 4. L2 Access Control Policy: Select the Layer 2 policy for wired ports. When user-port is not enabled L2 AC wired support policy can be mapped directly to the wired port. When the User Side Port is not enabled, an L2 AC wired support policy can be mapped directly to the wired port. If the User Side Port is enabled, the L2 AC wired support policy can be mapped to the wired port by way of the firewall profile. Click  to create a new policy. Refer to [Creating an L2 Access Control Service](#) on page 349.
 5. Click  to create a new firewall profile.
- h. Click **OK**.

NOTE

You can edit, clone, or delete the profile by selecting the options **Configure**, **Clone**, and **Delete** respectively, from the **Ethernet Port** tab.

Creating a Tunnel DiffServ Profile

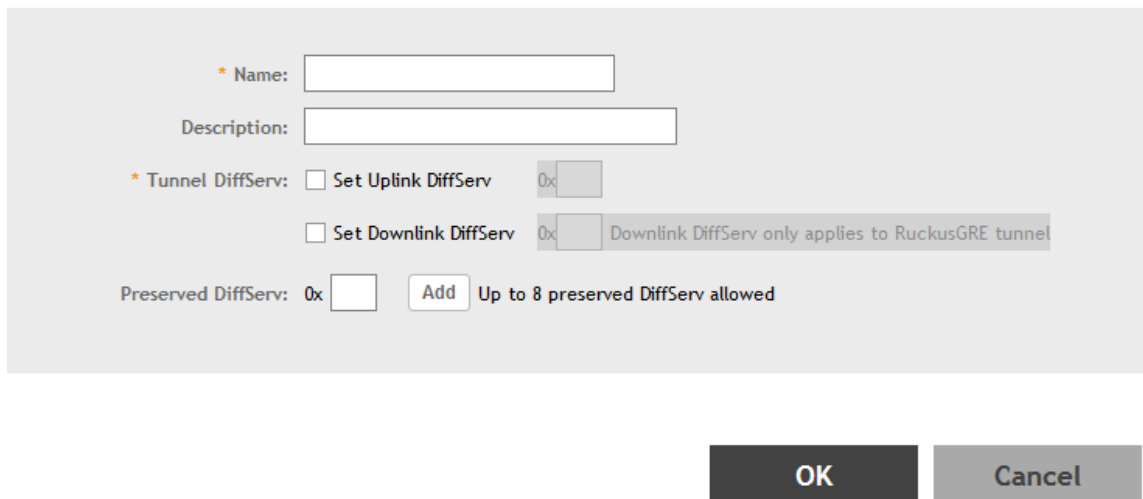
If you need to configure the type of traffic (ToS) bit settings for the access side traffic from Ruckus APs, follow these steps to create a Differentiated Services (DiffServ) profile. This profile can only be applied to Ruckus GRE and SoftGRE traffic.

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 236 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

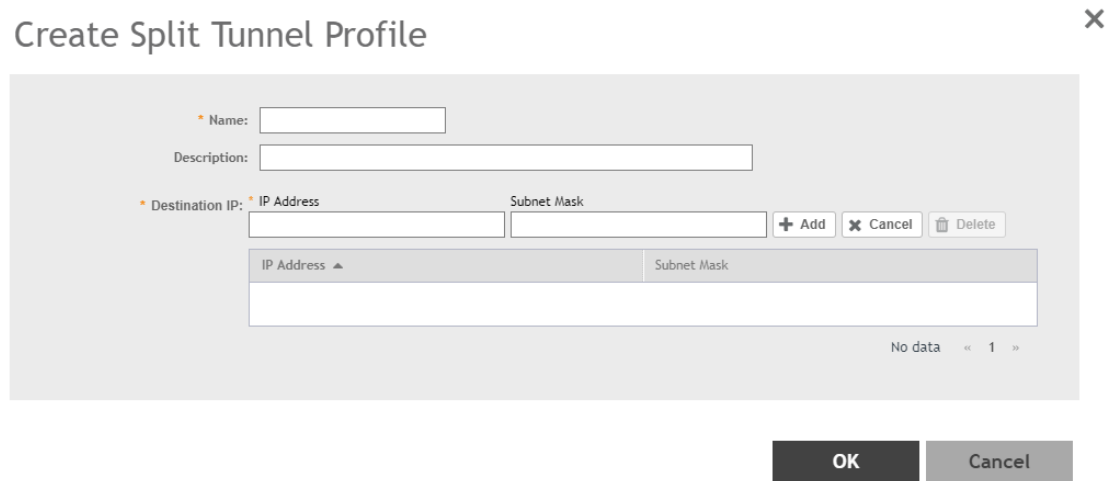
Complete the following steps to configure a split tunnel profile:

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 237 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.

Communications Assistance for Law Enforcement Act (CALEA)

The Communications Assistance for Law Enforcement Act is a law passed by the United States to enhance the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment to modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.

NOTE

This feature only applies to the SmartZone 300 (SZ300) controller.

1. Go to **Services & Profiles > Tunnels and Ports**.
2. Select the **CALEA** tab.
3. Server IP: Type the CALEA server IP address.

4. Click **Create**.

The **Create UE MAC** page appears.

NOTE

The list of client health will only list top 100 clients.

5. **MAC Address:** Type the MAC address of the client/user equipment for which CALEA mirroring is required. The MAC address is sent by the SZ controller to the vSZ-D.

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.

The **Tunnel Encryption (DP)** page appears.

FIGURE 238 Tunnel Encryption (DP)



3. Select the **Enable Tunnel Encryption** check-box.
4. Click **OK**.

You have successfully enabled tunnel encryption.

Managing Core Network Tunnels

Tunneling protocols allows a user to access or provide a network service that the network does not support or provide directly.

Creating Bridge Forwarding Profiles

An Bridge forwarding profile defines the DHCP configuration for the core network.

NOTE

This feature is available only on vSZ-H platform.

1. Go to **Services & Profiles > Core Network Tunnel**.
2. Select the **Bridge** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

The **Create Bridge Forwarding Profile** page appears.

FIGURE 239 Creating a Bridge Forwarding Profile

Create Bridge Forwarding Profile

The screenshot shows the 'Create Bridge Forwarding Profile' configuration page. It includes the following elements:

- Name:** A text input field.
- Description:** A text input field.
- DHCP Relay:** A dropdown menu currently set to 'DHCP Relay'.
- Enabled DHCP Relay:** A checked checkbox.
- DHCP Server 1:** A text input field.
- DHCP Server 2:** A text input field.
- Send DHCP requests to both servers simultaneously:** An unchecked checkbox.
- DHCP Option 82:** A checked checkbox.
- Subopt-1 with format:** A checked checkbox with a dropdown menu showing 'IF-Name:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC'.
- Subopt-2 with format:** An unchecked checkbox with a dropdown menu showing 'Client-MAC-hex'.
- Subopt-150 with VLAN-ID:** An unchecked checkbox.
- Subopt-151 with format:** An unchecked checkbox with a dropdown menu showing 'Area-Name' and an adjacent text input field.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right.

4. Configure the following:

- a. **Name:** Type a name for the profile that you are creating.
- b. **Description:** Type a brief description for the profile.
- c. **DHCP Relay:** Select the **Enable DHCP Relay** check-box and configure the DHCP server IP address and DHCP option 82 settings.
 1. **DHCP Server 1:** Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
 2. **DHCP Server 2:** If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
 3. **DHCP Option 82:** Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 sub-options by selecting the corresponding check boxes:
 - **Subopt-1 with format:** You can customize sub-option 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.
 - **Subopt 2 with format:** You can customize sub-option 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
 - **Subopt-150 with VLAN ID:** This sub-option encapsulates the VLAN ID.
 - **Subopt-151 with format:** This sub-option can encapsulate either the ESSID or a configurable Area Name.
 -
- d. Click **OK**.

You have created the Bridge forwarding profile.

NOTE

You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **Bridge** tab.

Creating L2oGRE Forwarding Profiles

An L2oGRE forwarding profile defines the gateway and tunnel configuration for the core network of L2oGRE tunnels.

1. Go to **Services & Profiles > Core Network Tunnel**.
2. Select the **L2oGRE** tab, and then select the zone for which you want to create the profile.
3. Click **Create**.

The **Create L2oGRE Forwarding Profile** page appears.

FIGURE 240 Creating a L2oGRE Forwarding Profile

Create L2oGRE Forwarding Profile

• Name:

Description:

Core Network Gateway Settings

• Primary Gateway IP:

Secondary Gateway IP:

Gateway Path MTU: Auto Manual bytes (850-1500)

• ICMP Keep-Alive Period (secs):

• ICMP Keep-Alive Retry:

DHCP Relay

OK Cancel

4. Configure the following:
 - a. Name: Type a name for the profile that you are creating.
 - b. Description: Type a brief description for the profile.
 - c. Core Network Gateway Settings
 1. Primary Gateway IP: Type the IP address of the primary gateway for the L2oGRE tunnel.
 2. Secondary Gateway IP: Type the IP address of the secondary gateway for the L2oGRE tunnel. If the primary gateway is unreachable, this gateway will be used for the L2oGRE tunnel.
 3. Gateway Path MTU: Set it the MTU manually or use Auto (default). MTU is the size of the largest protocol data unit (in bytes) that can be passed on the controller network.
 4. ICMP Keep-Alive Period (secs): Set the time in seconds between sending retry messages to the keepalive IP address. Enter an integer between 2 and 255. The default is 10 seconds.
 5. ICMP Keep-Alive Retry: Set the retry period to send messages to the keepalive IP address. The default value is 3 retries.
 - d. DHCP Relay: Select the **Enable DHCP Relay** check-box and configure the DHCP server IP address and DHCP option 82 settings.
 1. DHCP Server 1: Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
 2. DHCP Server 2: If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
 3. DHCP Option 82: Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled DHCP Option 82, you can configure the following Option 82 sub-options by selecting the corresponding check boxes:
 - Subopt-1 with format: You can customize sub-option 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.
 - Subopt 2 with format: You can customize sub-option 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
 - Subopt-150 with VLAN ID: This sub-option encapsulates the VLAN ID.
 - Subopt-151 with format: This sub-option can encapsulate either the ESSID or a configurable Area Name.
 -
 - e. Click **OK**.

You have created the L2oGRE forwarding profile.

NOTE

You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **L2oGRE** tab.

Creating TTG+PDG Forwarding Profiles

A TTG+PDG forwarding profile defines the gateway and tunnel configurations for core network GTP tunnels and LBO configurations.

Follow these steps to add a TTG+PDG profile:

1. Go to **Services & Profiles > Core Network Tunnel**.
2. Select the **TTG+PDG** tab, and then select the zone for which you want to create the profile.

3. Click **Create**.

The **Create TTG+PDG Forwarding Profile** page appears.

FIGURE 241 Creating a TTG+PDG Forwarding Profile

Create TTG+PDG Forwarding Profile

Name:

Description:

Common Settings

APN Format to GGSN:

Use APN-OI for DNS Resolution: Yes No

of Accounting Retry:

Accounting Retry Timeout (secs):

PDG UE Session Idle Timeout (secs):

DHCP Relay

Enabled DHCP Relay

DHCP Server 1:

DHCP Server 2: Send DHCP requests to both servers simultaneously

DHCP Option 82:

Subopt-1 with format

Subopt-2 with format

Subopt-150 with VLAN-ID

OK **Cancel**

4. Configure the following:
 - a. **Name:** Type a name for the profile that you are creating.
 - b. **Description:** Type a brief description for the profile.
 - c. **Common Settings**
 1. **APN Format to GSN:** Select either **DNS** or **String** from the drop-down list.
 2. **APN-OI for DNS Resolution:** Specify if the APN-OI is required.
 3. **# of Accounting Retry:** Specify the interval (in minutes) at which the controller will recheck the primary TTG+PDG RADIUS profile, if it is available. The default interval is 5 minutes.
 4. **Accounting Retry Timeout (secs):** Type the timeout period (in seconds) after which an expected response message is considered to have failed.
 5. **PDG UE Session Idle Timeout (secs):** Type the timeout period (in seconds) after which an expected response message is considered to have failed.
 - d. **DHCP Relay:** Select the **Enabled DHCP Relay** button to enable the DHCP relay agent in the controller and configure the DHCP server IP address and DHCP option 82 settings.
 1. **DHCP Server 1:** Type the IPv4 address of the DHCP server that will allocate IP addresses to DHCP clients.
 2. **DHCP Server 2:** If a secondary DHCP server exists on the network, type the IPv4 address of the secondary server.
 3. **DHCP Option 82:** Select this check box if you want the DHCP relay agent (in this case, the controller) to insert specific identification information into requests that are forwarded to the DHCP server. If you enabled **DHCP Option 82**, you can configure the following Option 82 sub-options by selecting the corresponding check boxes:
 - **Subopt-1 with format:** You can customize sub-option 1 (Circuit ID) to send only the AP's MAC address in hexadecimal format or the MAC address and ESSID. The default format is: IFName:VLAN-ID:ESSID:AP-Model:AP-Name:AP-MAC.
 - **Subopt 2 with format:** You can customize sub-option 2 (Remote ID), which sends the client's MAC address by default, to send the AP's MAC address, or the client MAC plus ESSID or AP MAC plus ESSID.
 - **Subopt-150 with VLAN ID:** This sub-option encapsulates the VLAN ID.
 - **Subopt-151 with format:** This sub-option can encapsulate either the ESSID or a configurable Area Name.
 -
 - e. **Forwarding Policy per Realm**, specify the forwarding policy for each realm in the table.
Configure the following:
 - **APN**
 - **APN Type**
 - **Route Type**
 - **Profile Name**
 - f. In **Default APN Settings**, configure the following:
 - **No Matching Realm Found**
 - **No Realm Specified**
 - g. In **Default APN per Realm**, configure the following:
 - **Realm**
 - **Default APN**
 - h. Click **OK**.

You have created the TTG+PDG forwarding profile.

NOTE

You can also edit and delete the profile by selecting the options **Configure** and **Delete** respectively, from the **TTG+PDG** tab.

Configuring the GGSN/PGW Service

The controller has 3GPP-defined Tunnel Terminating Gateway (TTG) functionality, which enables it to act as a gateway between the UE (southbound) and the telecom core (northbound) to tunnel traffic between the UE (User Equipment, such as mobile phones) and controller gateway terminates the tunnel and then transfers the data over to GGSN (Gateway GPRS Serving Node) implementing the Gn interface via GTPv1 (Release 6). The Gn interface is used in controlling the signal between controller and GGSN as well as for tunneling end user data payload within the backbone network between both the nodes.

GPRS Tunneling Protocol (GTP) transmits user data packets and signaling between controller and GGSN. GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels for transmission of packet data between controller and GGSN. A GTP tunnel is established between controller and GGSN for a data session initiated from UE.

A GTP tunnel is identified by a pair of IP addresses and a pair of GTP Tunnel End Point Identifiers (TEIDs), where one IP address and TEID is for the SGSN and the other is for GGSN. TEID is a session identifier used by GTP protocol entities in SGSN and GGSN.

GTP separates signaling from payload. Traffic is sorted onto a control plane (GTP-C) for signaling and a user plane (GTP-U) for user data. GTP-C is a tunnel control and management protocol and is used to create, modify and delete tunnels. GTP-U is a tunneling mechanism that provides a service for carrying user data packets.

To configuring the GGSN/PGW Service:

1. Go to **Services & Profiles > Core Network Tunnel**.
2. Select the **GGSN/PGW** tab.

The **GGSN/PGW** page appears.

FIGURE 242 GGSN/PGW

The screenshot shows the configuration interface for the GGSN/PGW service. It features several sections:

- GTP Common Configuration:** Contains five dropdown menus for:
 - Response Timer (2-5 Seconds): 3
 - Number of Retries (N3 3-6): 5
 - Echo Request Timer (60-300 Seconds): 60
 - DNS Response Timeout (secs): 3
 - DNS # of Retry: 3
- DNS Servers:** Includes an IP input field and an "Add Server" button.
- APN Resolution:** Includes a table with the following data:

| Domain Name | IP |
|--------------------|------------|
| ruckuswireless.com | 10.0.0.254 |

At the bottom of the configuration area, there are buttons for "Refresh", "OK", and "Cancel".

3. Configure the following:
 - a. **GTP Common Configuration**
 1. **Response Timer:** Define the response expected from GGN server from the drop down list, which ranges from 2 to 5 seconds. The controller will attempt to contact the GGSN during call establishment.
 2. **Number of Retries:** Define the number of times that controller will attempt to contact the GGSN. If all attempts fail, the relevant alarm is raised to confirm the failure of the GGSN path. For example, if the response timer is 3 and the number of retries is 5, it means that for each retry, controller will for 3 seconds.
 3. **Echo Request Timer:** Define number of seconds that the GGSN waits before sending an echo-request message to check for GTP path failure.
 4. **DNS Response Timeout:** Specify the maximum time that DNS waits for a response from a signaling request message.
 5. **DNS # Retry:** specify the maximum number of times that the DNS attempts to send a signaling request.
 - b. **DNS Servers:** Click **Add Server** to add a DNS IP address. If you're adding multiple DNS IP addresses, you can set their priority by clicking the **Move Up** and **Move Down** buttons. DNS servers that are higher up on the list of servers are given higher priority.
 - c. **APN Resolution:** Type the GGSN **Domain Name** and **IP** address and click **Add**.
4. Click **OK**.

You have configuring the GGSN/PGW Service

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 2 million 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.

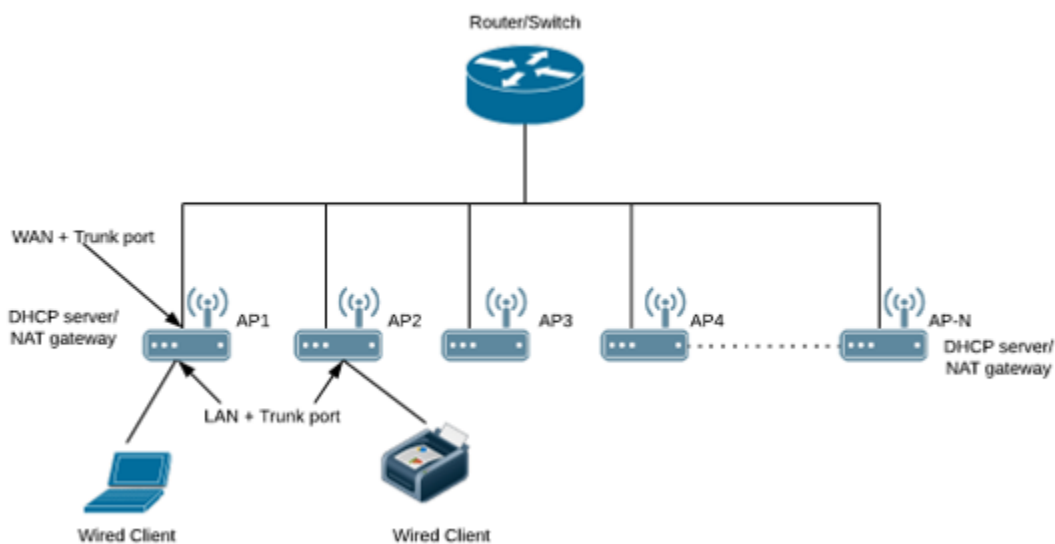
Network Topology

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.

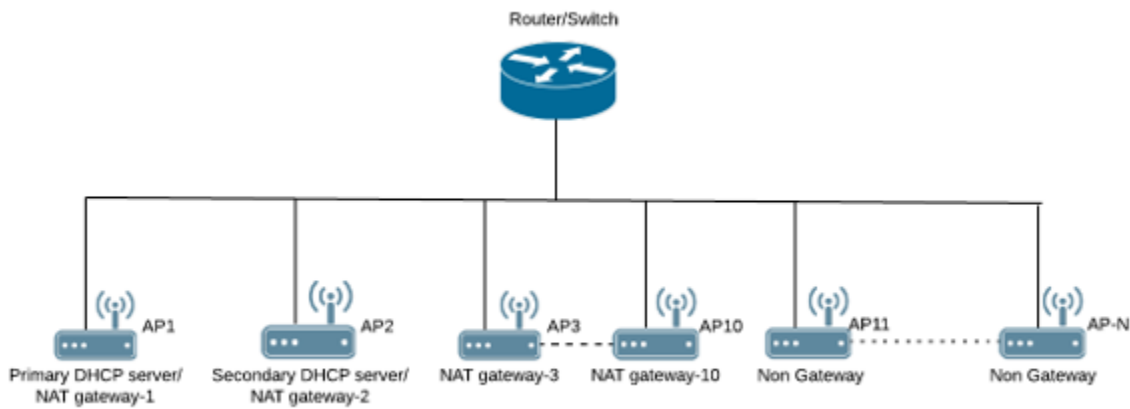
FIGURE 243 Single AP Topology



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.

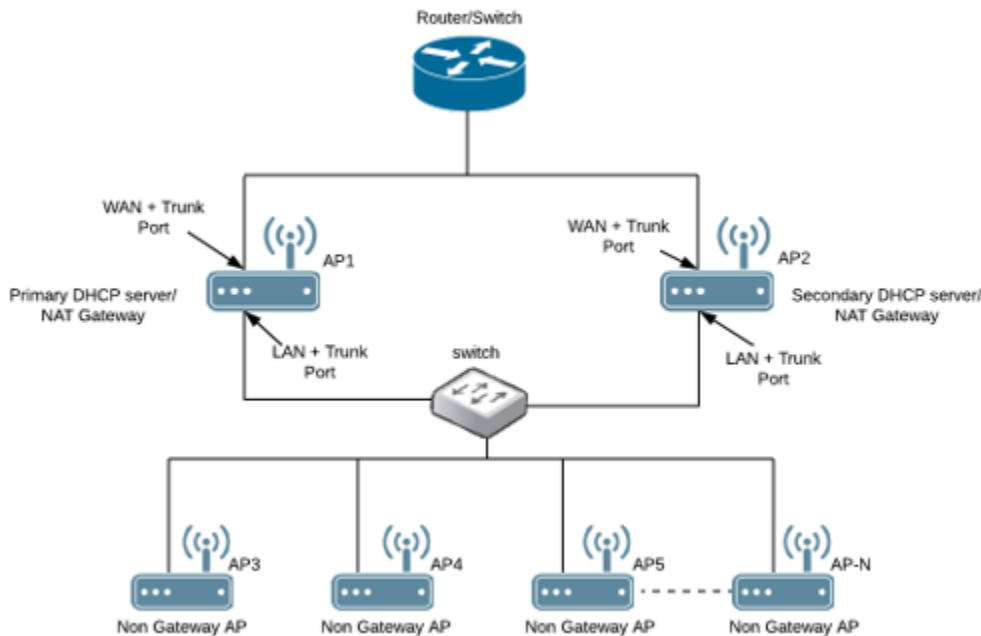
FIGURE 244 Multiple AP (Flat Network) Topology



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 245 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 WAN. LAN port selection is based on the availability of wired port with tunnel enabled. All other wired ports on the AP 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.

While using DHCP NAT-HN with DWPD, the AP will ignore the eth port configuration which is pushed from the interface. The AP will select the WAN and LAN ports dynamically. After successful detection of the WAN port, it marks the other port as LAN port. When it marks an eth port as LAN, DWPD chooses untagged VLAN ID as 1 by default. This configuration for LAN port is not changeable. Hence, wired client can get the IP address from DHCP Pool VLAN ID 1. If you want to configure eth port VLAN ID to 100 through the interface, manually select WAN port and apply appropriate eth port profile to the eth0 and eth1 ports of AP.

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:

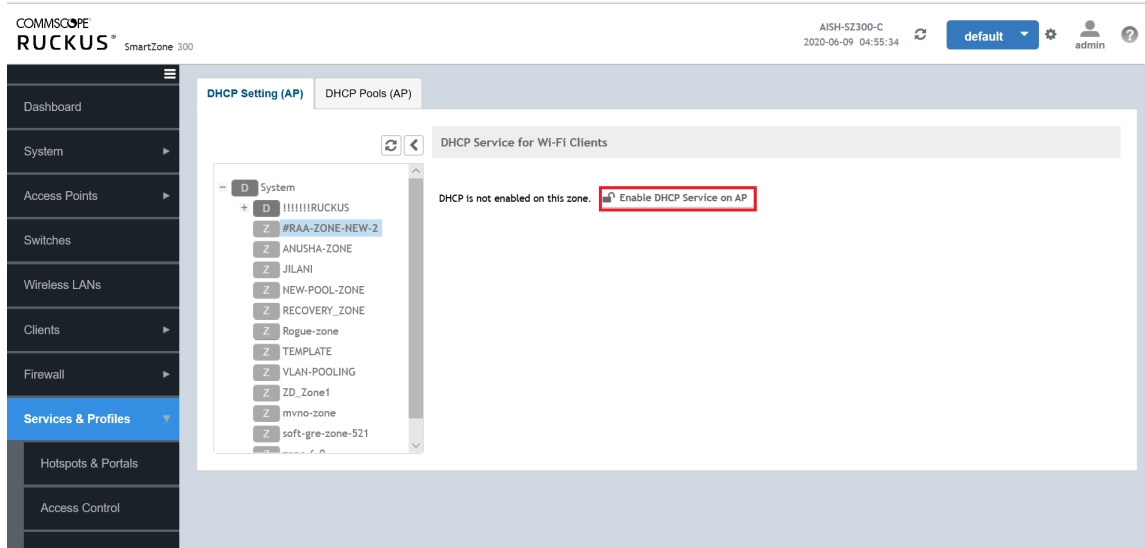
- There must be minimum one and maximum two APs acting as Gateway AP (GAP). There is no count in the number of APs acting as Non-Gateway APs (NGAP).
- For a single non-Gateway AP (NGAP) you can connect eth0 of NGAP to LAN port (usually eth1) of GAP.
- For more than one NGAP you need a minimum L2 switch 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.

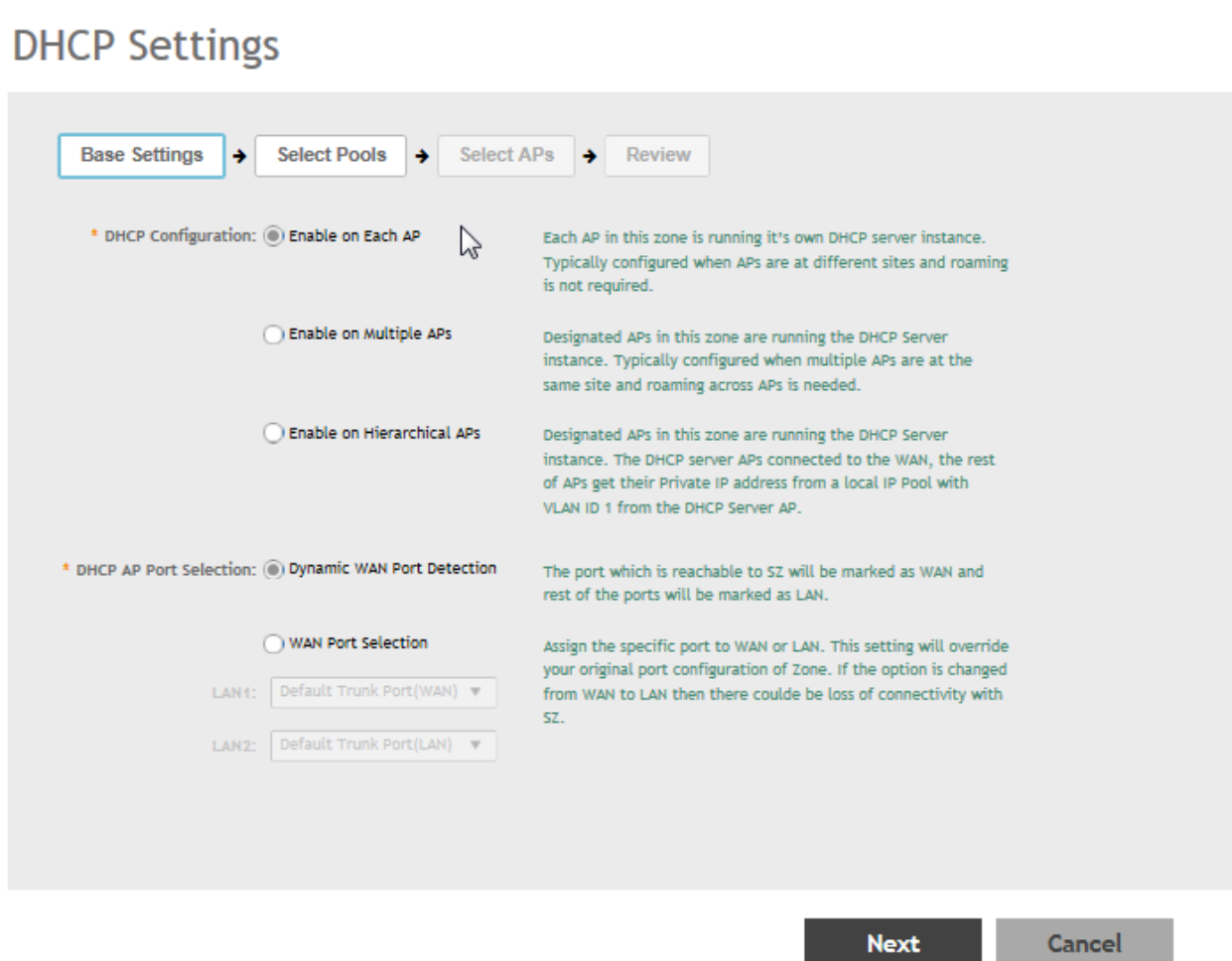
3. Select a Zone from the zone list on the left side of the screen, and click **Enable DHCP Service on AP**.

FIGURE 246 Enabling DHCP Service



4. Click **Edit DHCP Service on AP**. The **DHCP Settings** wizard appears.

FIGURE 247 DHCP Settings wizard

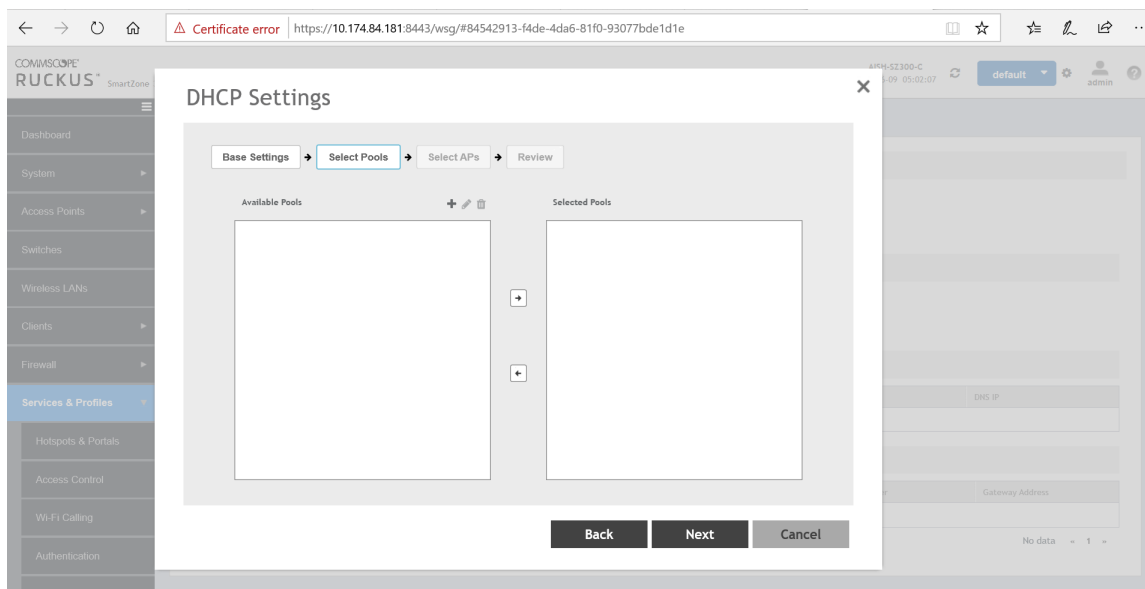


- On the first page of the wizard (**Base Settings**), configure the **DHCP Configuration** as follows:
 - Enable on Each AP:** Each AP in this zone runs its own DHCP server instance. This option is typically used when APs are at different sites and roaming is not required. Now configure the **DHCP AP 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 Hierarchical APs** DHCP configuration, one of the pools must be VLAN ID 1.

FIGURE 248 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 466.

- 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.

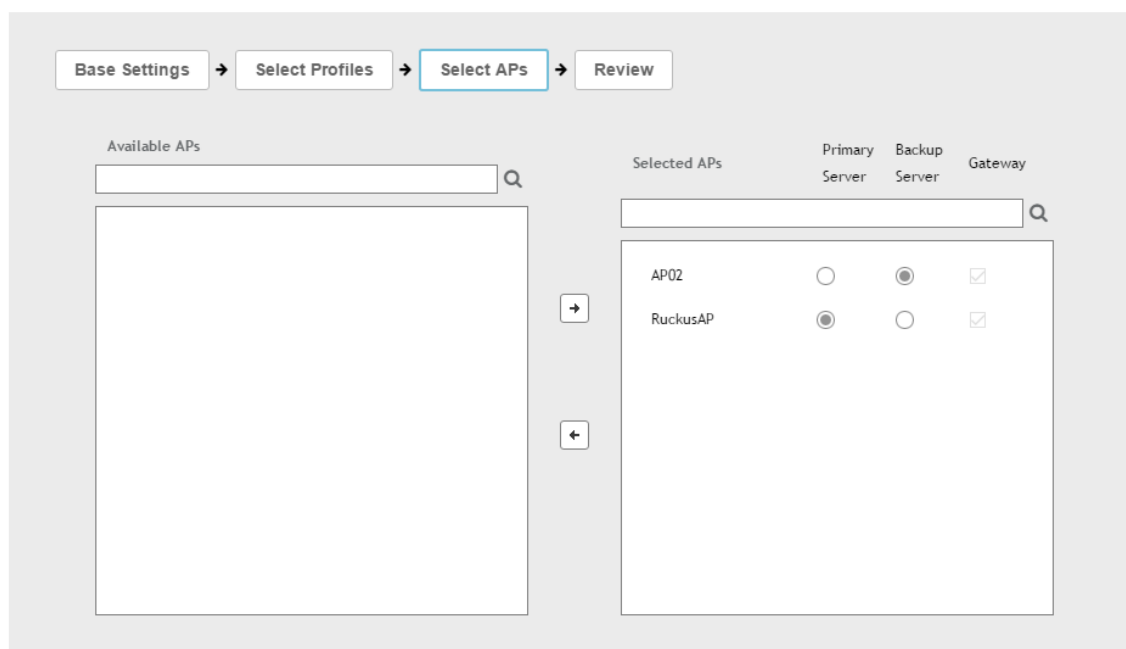
- On the **Select APs** wizard screen, select the AP(s) that you want to set as the primary and secondary DHCP servers (if you previously selected **Enable on Multiple APs**).

NOTE

For the **Enable on Hierarchial APs** DHCP configuration, you can select only two APs.

FIGURE 249 Selecting APs

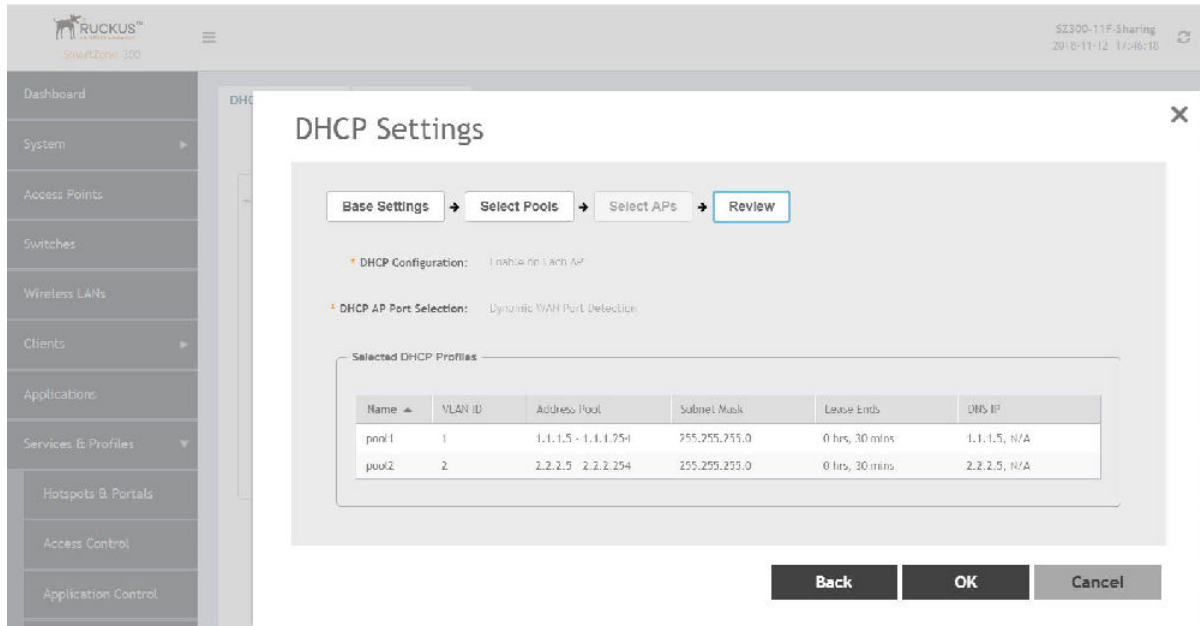
DHCP Settings



- 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 250 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 251 Creating a DHCP Pool

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

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 461.

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 vSZ-D and the vSZ-D 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 468
- [Configuring DHCP Pool Settings](#) on page 469

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:

NOTE

This feature is supported only in vSZ-H platform.

- › **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 vSZ-D. 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 471
- [Configuring NAT Pool Setting](#) on page 471

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.

NOTE

This feature is supported only in vSZ-H platform.

- **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 80.
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 466.
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 461.

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 252 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**.

Vendor-Specific Attribute (VSA) Profile

The SmartZone UI provides the VSA profile, where the user can define VSAs to be included in authentication and accounting messages. The AP receives the configuration from the Change and Configuration Management (CCM) and appends the VSAs to each user equipment (UE) authentication and accounting request and forwards the requests to the AAA server.

For HotSpot WISPr, the UE authentication is handled by the northbound Interface (NBI) where Real Application Clusters (RAC) appends the VSAs to the authentication messages and the AP appends the VSAs to the accounting messages.

Creating a Vendor-Specific Attribute Profile

Perform the following procedure to add the VSAs in the RADIUS authentication and accounting messages.

1. Select **Services and Profiles > Vendor Specific Attributes > Vendor Specific Attributes Profile**.
2. Select the zone for which you want to create a VSA profile.
3. Click **Create**.

The **Create Vendor Specific Attribute Profile** page is displayed.

FIGURE 253 Creating a Vendor-Specific Attribute Profile

Create Vendor Specific Attribute Profile

Name:

Description:

Attributes:

| Vendor ID | Key ID | Value | Type | Radius Message |
|----------------------|----------------------|----------------------|--------|----------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | String | Both |

No data « 1 »

+ Add Import CSV Cancel Delete

OK Cancel

4. Enter the profile name and description.

Services and Profiles

Vendor-Specific Attribute (VSA) Profile

5. Under **Attributes**, define the VSA profile by completing the following steps:

- a) In the **Vendor ID** field, enter an integer from 1 through 65536.

NOTE

Do not configure the vendor IDs 25053 (Ruckus) and 14122 (WISPr) because they are reserved for internal use only. If you try to configure these vendor IDs, the system throws an error message.

- b) In the **Key ID** field, enter an integer from 0 through 255.

- c) In the **Type** list, select from the following options:

- **Integer**
- **String**

- d) In the **Value** field, enter an integer or string depending on the **Type** selected.

NOTE

The integer range is from 0 through 2147483647. The maximum length of a string is 247 characters.

- e) In the **Radius Message** list, select from the following options:

- **Accounting:** The attributes defined in the VSA profile are included in the accounting messages.
- **Authentication:** The attributes defined in the VSA profile are included in the authentication messages.
- **Both:** The attributes defined in the VSA profile are included in both the accounting and authentication messages.

6. Click **Add** to add the VSA profile or click **Import CSV** to upload a CSV file containing multiple VSA profiles.

NOTE

To download a CSV template, click the **Import CSV** arrow and select **Download a CSV Sample**.

The VSA profiles are added to the **Attributes** table. Check the VSA information in the **Attributes** table for any modifications.

NOTE

You can edit the VSAs by clicking the **Vendor ID** in the **Attributes** table.

NOTE

A maximum of 32 VSAs can be added to a VSA profile. A maximum of 4 VSA profiles can be configured for a zone.

7. Click **OK** to update the VSA profile to the database.

NOTE

To edit a VSA profile, select a VSA profile and click **Configure** in the **Vendor Specific Attribute Profile** page.

NOTE

To associate a VSA profile to a WLAN, refer to [Associating a VSA Profile to a WLAN Configuration](#) on page 475.

NOTE

You can also configure a VSA profile in the zone and WLAN templates. For more information, refer to *Working with Zone Templates* and *Working with WLAN Templates* respectively .

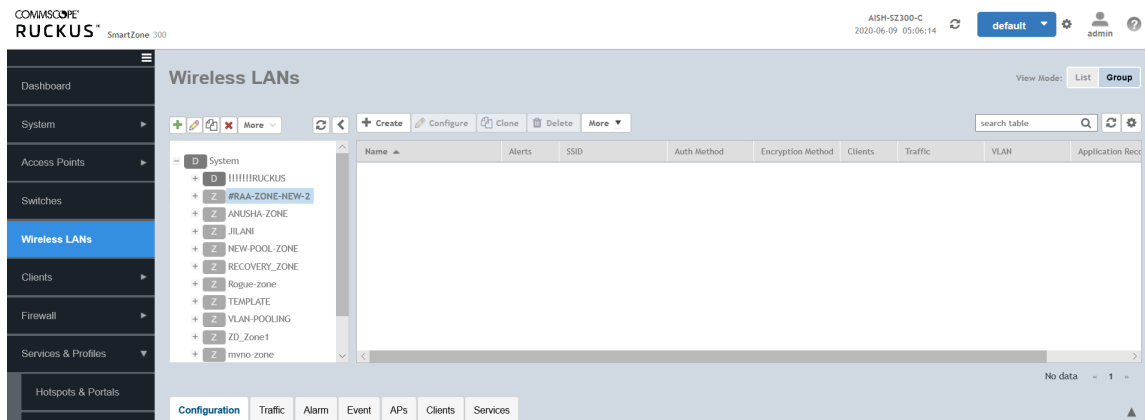
Associating a VSA Profile to a WLAN Configuration

Perform the following procedure to associate a VSA profile to a WLAN configuration.

1. On the main menu, click **Wireless LANs** and select the zone where the VSA profiles are created.

The **Wireless LANs** page is displayed.

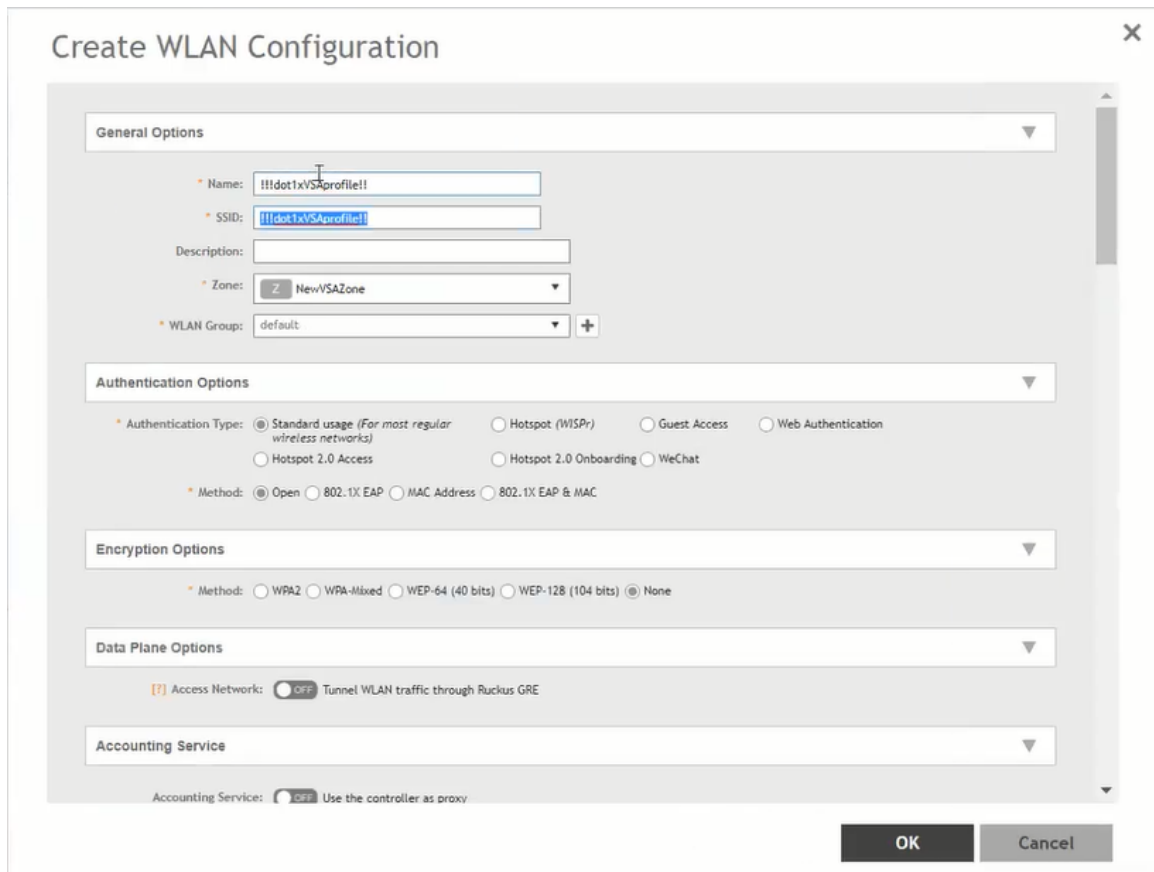
FIGURE 254 Viewing the Wireless LANs



2. Click **Create**.

The **Create WLAN Configuration** page is displayed.

FIGURE 255 Creating a WLAN Configuration




3. Under **General Options**, enter the WLAN name and SSID.
4. Under **Authentication and Accounting Service**, complete the following steps:
 - a) Under **Authentication Service**, click **Use the controller as proxy** and select the authentication service profile.
 - b) Under **Accounting Service**, click **Use the controller as proxy** and select the accounting service profile.
5. Under **Radius Options**, click **Vendor Specific Attribute Profile** and select a VSA profile.

NOTE

By default, **Vendor Specific Attribute Profile** is disabled.

NOTE

Click  to configure the VSA profile.

6. Under **Advanced Options**, enter the VLAN ID.

NOTE

Enter an integer from 2 through 4094 for **VLAN ID**.

NOTE

The WLAN configuration is shown in the **Access Points** page for the zone where VSA profiles are created.

Working with Reports

- Types of Reports..... 479
- Managing Report Generation..... 480
- Rogue Devices..... 482
- Historical Client Stats..... 484
- Ruckus AP Tunnel Stats..... 485
- Core Network Tunnel Stats..... 488

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.

Continuously Disconnected APs Report

The Continuously Disconnected APs report shows a list of access points disconnected within the specified time range.

Switch Traffic Statistics

The Switch Traffic Statistics report displays information about each port and line associated with the selected switches. The report includes information about port number, total incoming and outgoing frames, total incoming and outgoing multicast packets, total incoming and outgoing broadcast packets, and total errors.

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.

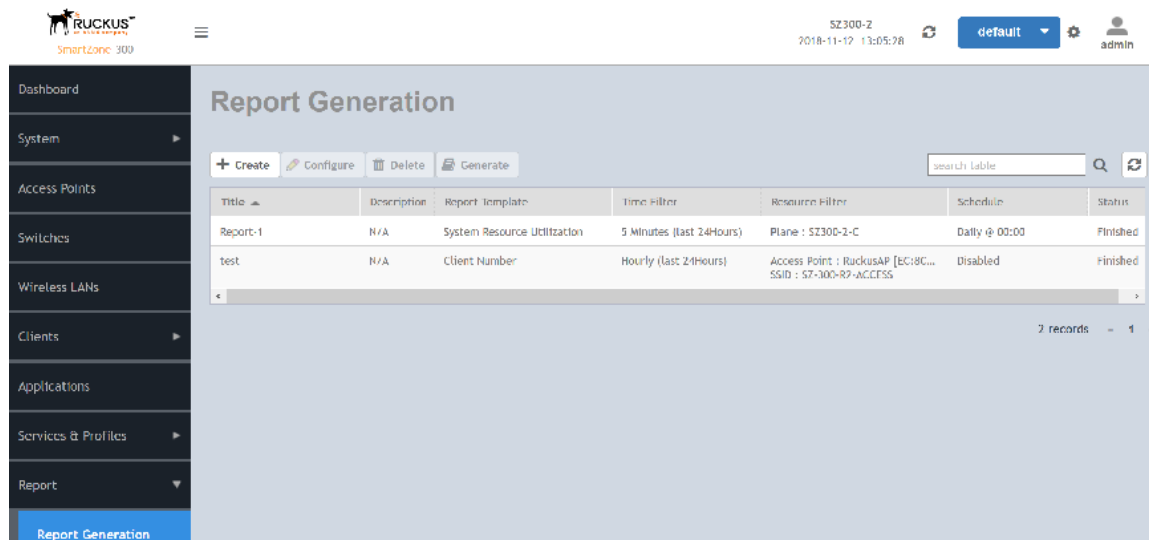
Creating Reports

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 256](#) appears.

FIGURE 256 Report Generation Screen



2. Click **Create**, [Figure 257](#) appears.

FIGURE 257 Create Reports Screen
Create Report

3. Enter the required parameters as explained in [Table 81](#).
4. Click **OK**.

TABLE 81 Report Parameters

| Field | Description | Your Action |
|---------------------------------|---|--|
| General Information | | |
| Title | Indicates the report name. | Enter a title for the report. |
| Description | Describes the report type. | Enter a short description. |
| Report Category | Provides an option to generate reports for System or Switch devices in the network. | Select System or Switch as appropriate. |
| Report Type | Specifies the report type | Select the required report. |
| Output Format | Specifies the report output format. | Select the required report output format. |
| Resource Filter Criteria | | |
| Device | 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. |
| SSID | 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 All SSIDs to generate reports for all the SSIDs available. This option is convenient as you do not have to update the resource filter criteria periodically. |
| Radio | 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"> • 2.4G • 5G |
| Time Filter | | |
| Time Interval | Defines the time interval at which to generate the report. | Select the required time interval. |
| Time Filter | Defines the time duration for which to generate the report. | Select the required time filter. |
| Schedules | | |

TABLE 81 Report Parameters (continued)

| Field | Description | Your Action |
|--|---|---|
| Enable/Disable | 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 Enable and select the Interval , Hour and Minute . You can add multiple schedules. You can also click Add New to include more schedules. |
| Email Notification | | |
| Enable/Disable | Triggers an email notification when the report is generated. | By default the option is disabled. Select Enable and click the Add New and enter the email address. You can add multiple email addresses. |
| Export Report Results | | |
| Export Report Results, Enable/Disable | Uploads the report results to an FTP server. | By default the option is disabled. Select Enable and select the FTP Server . Click Test 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 256](#) on page 480 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 Devices

Rogue (or unauthorized) APs and rogue clients pose problems for a wireless network in terms of airtime contention and security.

Usually, a rogue AP or a rogue client appears when an employee obtains another manufacturer's AP and connects it to the LAN to gain wireless access to other LAN resources. This connection potentially allows more unauthorized users to access the corporate LAN, posing a security risk. Rogue APs and rogue clients also interfere with nearby Ruckus APs, thus degrading overall wireless network coverage and performance.

The SZ controller's rogue AP detection options include identifying the presence of a rogue AP or rogue client, and categorizing it as either a known neighbor AP or as a malicious rogue.

Viewing Rogue Devices

To view the rogue APs or rogue clients, select **Access Point** or **Client** from the **Device Type** list.

If you enabled rogue AP or rogue client detection when you configured the common AP settings (refer to [Configuring APs](#)), click **Report > Rogue Devices**. Under **Device Type**, select **Access Point** or **Client**. The **Rogue Devices** page displays all the rogue APs or rogue clients that the controller has detected on the network, including the following information:

- **Rogue MAC:** The MAC address of the rogue AP.
- **Type:** The client has a different set of rogue types (for example, rogue, normal rogue AP, not yet categorized as malicious or non-malicious).

- **Classification Policy:** The rogue classification policy associated with the rogue AP.
- **Channel:** The radio channel used by the rogue AP.
- **Radio:** The WLAN standards with which the rogue AP complies.
- **SSID:** The WLAN name that the rogue AP is broadcasting.
- **Detecting AP Name:** The name of the AP.
- **Zone:** The zone to which the AP belongs.
- **RSSI:** The radio signal strength.
- **Encryption:** Indicates whether the wireless signal is encrypted.
- **Detected Time:** The date and time that the rogue AP was last detected by the controller.

Filtering Rogue Devices

From the list of rogue APs or rogue clients, you can filter the required rogue AP or rogue client based on rogue MAC address, type, or SSID.

Perform the following procedure to filter the rogue devices.

1. Select **Report > Rogue Devices**.
2. In the **Rogue Devices** page, select **Access Point** from the **Device Type** list and click **Settings** (⚙️).
3. In the **Apply Filters** page, enter the rogue MAC address for **Rogue MAC**.
4. Select **Type** from the list.

If **Device Type** is **Access Point**, select **Ignore**, **Known**, **Rogue**, or **Malicious**.

If **Device Type** is client, select **Active Probing**, **CTS Abuse**, **Data Encrypted**, **Deauth Flood**, **Disassoc Flood**, **Excessive Power**, **Known**, **Rogue Client**, and **RTS Abuse**.

5. Enter **SSID**.
6. Click **OK**.

NOTE

You can click **Filter On** or **Filter Off** to add or remove the filters.

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 > Rogue Devices**. The **Rogue Devices** page is displayed.
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 Device

You can identify the estimated location area of a rogue AP or rogue client on a map. Managed APs that detect the rogue APs and rogue clients are also visible on the map.

Perform the following procedure to locate a rogue AP or rogue client.

1. From the left pane, select **Report > Rogue Devices**.
2. In the **Rogue Devices** page, select **Rogue AP** or **Client** from the **Device** list.
3. Click **Locate Rogue**.

The **Rogue AP Location** page appears locating the rogue AP or rogue client. You can select from the following options:

- **Map**: View the location in street view.
- **Satellite**: View the location as satellite imagery.
- **+**: Zoom in on the location.
- **-**: Zoom out of the location.

You can find the following information about rogue and detecting APs:

- Rogue APs: MAC address, type, and SSID
 - Detecting APs: MAC address, name, and RSSI
4. 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 82](#).
3. Click:
 - **Load Data**— To view the report in the workspace.
 - **Export CSV**—To open or save the report in CSV file format.

TABLE 82 AP Client Statistics Report Parameters

| Field | Description | Your Action |
|--------------------|---|---|
| Time Period | Indicate the time period for which you want to view the report. | Move the slider to set the duration. |
| Zone Name | Specifies the zone for which you want to view the report. | Enter the zone name or choose the zone from the list. |
| Client MAC | Specifies the MAC. | Enter the client MAC. |
| Client IP | Indicates the client IP. | Enter the client IP address. |

TABLE 82 AP Client Statistics Report Parameters (continued)

| Field | Description | Your Action |
|------------------|---|------------------|
| MVNO Name | Indicates the mobile virtual network operator name. | Choose the MVNO. |

Table 83 contains historical client statistics report based on the UE session statistics.

TABLE 83 AP Client Statistics Report Attributes

| Attribute | Type | Description |
|------------------------------------|--------|---|
| Start | Long | Indicates the session creation time. |
| End | Long | Indicates the session end time. |
| Client MAC | String | Indicates the Mac address of the client. |
| Client IP Address | String | Indicates the IP address of the client. |
| Core Type | String | Indicates the core network tunnel type. |
| MVNO Name | String | Indicates the mobile virtual network operator name. |
| AP MAC | String | Indicates the Client AP MAC. |
| SSID | String | Indicates the SSID |
| Bytes from Client | Long | Indicates the number of bytes received from the client. |
| Bytes to Client | Long | Indicates the number of bytes sent to the client. |
| Packets from Client | Long | Indicates the number of packets received from the client. |
| Packets to Client | Long | Indicates the number of packets sent to the client. |
| Dropped Packets from Client | Long | Indicates the number of packets dropped from the client. |
| Dropped Packets to Client | 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 84](#).
3. Click:
 - **Load Data**— To view the report in the workspace.
 - **Export CSV**—To open or save the report in CSV file format.

TABLE 84 Ruckus GRE Report Parameters

| Field | Description | Your Action |
|-----------------------------|---|---|
| Time Period | Indicate the time period for which you want to view the report. | Move the slider to set the duration. |
| Data Plane | Indicates the Data Plane. | Select the Data Plane. |
| AP MAC or IP Address | Indicates the MAC of the Access Point or IP Address. | Enter the AP MAC or IP address. |
| Zone Name | Specifies the zone for which you want to view the report. | Enter the zone name or select the zone from the list. |

Table 85 contains the report based on the statistics for Ruckus GRE. Each entry contains the 15 minutes cumulative data.

TABLE 85 Ruckus GRE report attributes

| Attribute | Type | Description |
|------------------------|------|--|
| Time | Long | Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15. |
| TXBytes | Long | Indicates the number of bytes sent. |
| RXBytes | Long | Indicates the number of bytes received. |
| TXPkts | Long | Indicates the number of packets sent. |
| RXPkts | Long | Indicates the number of packets received. |
| Dropped Packets | 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:

- From the left pane, select **Report > Ruckus AP Tunnel Stats**. The Ruckus GRE tab appears by default.
- Select **SoftGRE**. Update the parameters as explained in Table 86.
- Click:
 - Load Data**— To view the report in the workspace.
 - Export CSV**—To open or save the report in CSV file format.

TABLE 86 SoftGRE Report Parameters

| Field | Description | Your Action |
|-----------------------------|---|--------------------------------------|
| Time Period | Indicate the time period for which you want to view the report. | Move the slider to set the duration. |
| Zone Name | Specifies the zone for which you want to view the report. | Select the required zone. |
| Gateway Address | Specifies the gateway address | Enter the gateway address. |
| AP MAC or IP Address | Indicates the MAC of the Access Point or IP Address. | Enter the AP MAC or IP address. |

Table 87 contains the report based on the statistics for SoftGRE. Each entry contains the 15 minutes cumulative data.

TABLE 87 SoftGRE Report Attributes

| Attribute | Type | Description |
|---------------------------|------|--|
| Time | Long | Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15. |
| TXBytes | Long | Indicates the number of bytes sent. |
| RXBytes | Long | Indicates the number of bytes received. |
| TXPkts | Long | Indicates the number of packets sent. |
| RXPkts | Long | Indicates the number of packets received. |
| RX Dropped Packets | Long | Indicates the number of packets dropped. |
| TX Dropped Packets | Long | Indicates the number of packets dropped. |
| TX Error Packets | Long | Indicates the number of packets with a header error. |
| RX Error Packets | 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 88](#).
3. Click:
 - **Load Data**— To view the report in the workspace.
 - **Export CSV**—To open or save the report in CSV file format.

TABLE 88 SoftGRE + IPsec Report Parameters

| Field | Description | Your Action |
|-----------------------------|---|--------------------------------------|
| Time Period | Indicate the time period for which you want to view the report. | Move the slider to set the duration. |
| Zone Name | Specifies the zone for which you want to view the report. | Select the required zone. |
| Gateway Address | Specifies the gateway address | Enter the gateway address. |
| AP MAC or IP Address | Indicates the MAC of the Access Point or IP Address. | Enter the AP MAC or IP address. |

[Table 89](#) contains the report based on the statistics for access point IPsec. Each entry contains the 15 minutes cumulative data.

TABLE 89 SoftGRE + IPsecReport Attributes

| Attribute | Type | Description |
|---------------------------|------|--|
| Time | Long | Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15. |
| TXBytes | Long | Indicates the number of bytes sent. |
| RXBytes | Long | Indicates the number of bytes received. |
| TXPkts | Long | Indicates the number of packets sent. |
| RXPkts | Long | Indicates the number of packets received. |
| TX Dropped Packets | Long | Indicates the number of packets dropped. |

TABLE 89 SoftGRE + IPsecReport Attributes (continued)

| Attribute | Type | Description |
|---------------------------|------|--|
| RX Dropped Packets | Long | Indicates the number of packets dropped. |

Core Network Tunnel Stats

Viewing Statistics for L2oGRE Core Network Tunnel

To view Stats for L2oGRE Core Network Tunnel:

1. From the left pane, select **Report > Core Network Tunnel Stats**. The L2oGRE page appears.
2. Update the parameters as explained in [Table 90](#).
3. Click:
 - **Load Data**— To view the report in the workspace.
 - **Export CSV**—To open or save the report in CSV file format.

TABLE 90 L2oGRE Core Network Tunnel Parameters

| Field | Description | Your Action |
|---------------------------|---|--------------------------------------|
| Time Period | Indicate the time period for which you want to view the report. | Move the slider to set the duration. |
| Data Plane | Indicates the Data Plane. | Select the Data Plane. |
| Gateway IP Address | Indicates the gateway IP Address. | Enter the gateway IP address. |
| MVNO Name | Indicates teh mobile virtual network operator name. | Choose the MVNO name. |

[Table 91](#) contains the report based on the statistics for L2oGRE core network tunnel.

TABLE 91 L2oGRE Core Network Tunnel Attributes

| Attribute | Type | Description |
|------------------------|------|--|
| Time | Long | Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15. |
| TX Bytes | Long | Indicates the number of bytes sent. |
| RX Bytes | Long | Indicates the number of bytes received. |
| TX Packets | Long | Indicates the number of packets sent. |
| RX Packets | Long | Indicates the number of packets received. |
| Dropped Packets | Long | Indicates the number of packets dropped. |

Viewing Statistics for GTP Core Network Tunnel

You can view historical traffic statistics and trends of th core GTP tunnels.

GPRS Tunneling Protocol (GTP) transmits user data packets and signaling between controller and GGSN. GTP encapsulates traffic and creates GTP tunnels, which act as virtual data channels for transmission of packet data between the controller and GGSN. A GTP tunnel is established between the controller and GGSN for a data session initiated from UE.

To view Stats for GTP Core Network Tunnel:

1. From the left pane, select **Report > Core Network Tunnel Stats**. The SoftGRE page appears.
2. Select **GTP** and update the parameters as explained in [Table 92](#).
3. Click:
 - **Load Data**— To view the report in the workspace.
 - **Export CSV**—To open or save the report in CSV file format.

TABLE 92 GTP Core Network Tunnel Parameters

| Field | Description | Your Action |
|-----------------------------|---|--------------------------------------|
| Time Period | Indicate the time period for which you want to view the report. | Move the slider to set the duration. |
| Zone Name | Indicates the zone. | Select the Zone name. |
| Gateway Address | Indicates the gateway address. | Enter the gateway address. |
| AP MAC or IP Address | Indicates the MAC of the Access Point or IP Address. | Enter the AP MAC or the IP address. |

[Table 93](#) contains the report based on the statistics for GTP. Each entry contains the 15 minutes cumulative data.

TABLE 93 GTP Report Attributes

| Field | Type | Description |
|---------------------------|------|---|
| Time | Long | Bin ID, which is stamped at a 15 minute interval. For example, 10:00, 10:15. |
| TX Bytes | Long | Indicates the number of bytes sent. |
| RX Bytes | Long | Indicates the number of bytes received. |
| TX Packets | Long | Indicates the number of packets sent. |
| RX Packets | Long | Indicates the number of packets received. |
| Tx Dropped Packets | Long | Indicates the number of packets dropped while sending. |
| Rx Dropped Packets | Long | Indicates the number of packets dropped while receiving. |
| Bad GTPU | Long | Indicates a tunneling mechanism that provides a service for carrying user data packets dropped. |
| RX TEID Invalid | Long | Indicates the number of invalid packets received by Tunnel End Point Identifiers. |
| TX TEID Invalid | Long | Indicates the number of invalid packets sent by Tunnel End Point Identifiers. |
| Echo RX | Long | Indicates the echo message received. |
| Last Echo RX Time | Long | Indicates the time when the last echo message was received. |

Troubleshooting

- Troubleshooting Client Connections..... 491
- Troubleshooting through Spectrum Analysis..... 493

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 258 Troubleshooting - Client Connections

The screenshot displays the 'Troubleshooting' interface. At the top, there are two main sections: '1' with a 'Type' dropdown menu set to 'Client Connection' and '2' with a 'Client MAC' field containing '18:AF:61:60:49:0F'. Below these, there is a '3' section with 'Select APs' and 'Total APs: 1', and a '4' section with 'Connectivity Trace' and buttons for 'Start', 'Stop', and 'Clear'. The main content area shows 'Access Points hearing client's probe requests:' with a table listing 'RuckusAP (e0:10:7f:23:da:b0)' with details like '5GHz (149)', '42' SNR, '8192' latency, '0' failure rate, and '45' utilization. Below the table is a connectivity trace diagram for AP 'RuckusAP (e0:10:7f:23:da:b0)' at 10:15:29, showing a sequence of frames: 802.11 Authentication Request/Response, 802.11 Association Request/Response, 4-Way Handshake (Frames 1-4), and DHCP Discover. The diagram uses vertical bars to represent the Client Device and Access Point, and horizontal arrows to show the flow of frames through various network layers: Data Plane, Control Plane (co-v699), DHCP, AAA Server, Captive Portal, and Broadcast.

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.

Troubleshooting

Troubleshooting Client Connections

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 259 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.

Troubleshooting

Troubleshooting through Spectrum Analysis

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..... 495
- Sending SNMP Traps and Email Notifications for Events..... 495
- Configuring Event Threshold..... 496
- Creating Custom Events for ICX Switches..... 497
- Configuring Alarms..... 499


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 260 Types of custom events available

The screenshot shows the 'Switch Custom Events' configuration page. At the top, there are tabs for 'Events', 'Event Management', 'Event Threshold', and 'Switch Custom Events'. Below the tabs are buttons for '+ Create', 'Configure', and 'Delete'. A red arrow points to the 'Event Type' column header with the text 'Types of switch custom events'. A search bar is located on the right side of the table. The table lists various event types with their respective severities, thresholds, descriptions, text patterns, and time windows.

| 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 261 Creating custom events for switches - TextPattern type

Event Name:

Event Description:

Event Type: TextPattern

Event Contains The Text:

Threshold: Times

Time Window: 1 Hour

Event Severity: Warning

OK Cancel

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 262 Editing custom events for switches - CPU/Memory type

Event Name: Warning CPU Usage

Event Description: Switch CPU usage is over Warning threshold, 20%

Event Type: CPU

Threshold: 20 %

Event Severity: Warning

OK Cancel

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:

Managing Events and Alarms

Configuring Alarms

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.

Statistics Files the Controller Exports to an FTP Server

If you added an FTP server to the controller, the controller will export statistics files to that FTP server, either on demand or based on a schedule. This is however only applicable for SZ300 and vSZ-H.

NOTE

The feature to export CSV files is only supported in SZ300 and vSZ-H platforms.

To enable this feature, go to the controller web UI and select the **Enable uploading statistical data to the FTP server** check-box from **System > General Settings > FTP**.

After the feature is enabled, each controller node sends a zip file to the FTP server via FTP or SFTP, on an hourly basis. The zip file is named as: `<directory_name> + '_' + <controller_node_identifier> + ".zip"`.

Here, `directory_name` is named as `yyyymmddhh` (indicating the beginning of the hour that the data was received). For example, the directory name for the data that comes between 10 and 11 AM of May 26, 2016, is **"2016052610"**.

The zip file contains all the reported data collected within the hour.

The data is divided into tables, and each data table is associated with files. The files are named as follows: `<Table Name> + '_' + <Thread_ID> + '_' + <Sequence_No>.csv`.

Here, `Table Name` is as described in [Table 94](#). `Thread_ID` is an integer, and `Sequence_No` is from 1 to N to limit each file to be capped around 1G bytes.

Each AP sends its statistic counters to the controller, every 180 seconds. The controller stores the data, and exports them as CSV files to the external FTP server, every hour. The controller stores the data for up to 6 hours; if the FTP server is down, the controller resends data for up to 6 hours.

TABLE 94 Exported CSV file table

| Table Name | Table Description |
|--------------------|---|
| APStatus | Root for all Status: Cluster, Domain, Zone info |
| APStatusSystem | AP Level Info |
| APStatusRadio | AP Radio Info |
| APStatusWlan | AP Wlan Info |
| APStatusTunnel | AP Tunnel Info |
| APStatusIPSec | AP IPSec Info |
| APStatusIPSecStats | AP IPSec stats |
| LanPortStatus | AP Lan Port Status |
| CertificateReload | AP Certificate Reload Info |
| CableModemInfo | Cable Modem inside AP |
| APStatusLBS | Location-Based Service |
| APStatusBrownout | AP Voltage Brownout Event |
| APReportStats | Root for all ReportCluster, Domain, Zone Info |
| APReportBin | Little Bin info |
| APReportBinRadio | Radio Stats |
| APReportBinWlan | Wlan Stats |

TABLE 94 Exported CSV file table (continued)

| Table Name | Table Description |
|-------------------|---------------------|
| APReportBinClient | Client Stats |
| APReportBinTunnel | Tunnel Stats |
| APReportBinIPSec | IPSec Stats |
| APClientStats | Root for all Client |
| APClientInfo | Client Stats |
| APClientRadio | Radio Static Info |
| APClientWlan | Wlan Static Info |
| APMeshStats | Root for all Mesh |
| APMeshDownlink | Mesh Downlink AP |
| APMeshUplink | Mesh Uplink AP |
| APMeshNeighbor | AP Mesh Neighbor |
| ArcMessage | Root for all AVC |
| FlowMessage | AVC Flow |
| RogueAPStats | Root for all Rogue |
| ReportType | Rogue Devices |

Administering the Controller

- [Managing Administrator and Roles.....](#) 503
- [Managing Licenses.....](#) 526
- [ZoneDirector to SmartZone Migration.....](#) 534
- [Monitoring Administrator Activities.....](#) 535
- [Managing Mobile Virtual Network Operator \(MVNO\) Accounts.....](#) 536
- [Terminating Administrator Sessions.....](#) 537

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 505.

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. Domain: Select the domain from the list of domains to which this user group will be associated. From **Select Domains**, choose the domains you want to assign to this user group. Click the  icon and they appear under **Selected Domains** now. Use the  icon to deselect the domains assigned to the group.
 - e. Click **Next**.
 - f. 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.
 - g. Click **Next**.
 - h. Review: Verify the configuration of the user group. Click **Back** to make modifications to the configuration settings.
 - i. 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 95 Resource Group Table

| Resource Category | Resources |
|-------------------|--|
| SZ | <ul style="list-style-type: none"> System Settings Cluster Settings and Cluster Redundancy Control Planes and Data Planes Firmware and Patches Cluster and Configuration Backups Licensing Cluster Stats and Health System Events and Alarms System Certificates Northbound Interface SCI Integration |
| AP | <ul style="list-style-type: none"> Zones and Zone Templates AP groups AP Settings AP Stats and Health Maps AP Events and Alarms Bonjour Policies Location Services Ethernet Port Profiles Tunneling Profiles and Settings AP Zone Registration |
| WLAN | <ul style="list-style-type: none"> WLANs WLAN Groups and Templates AAA Services L2-7 Policies Rate Limiting Application Policies Device OS Policies QoS Controls Hotspots and Portals Hotspot 2.0 Service Schedules VLAN Pools |

TABLE 95 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 263 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 264 Configuring an Administrator Account

Edit Administrator Account: admin [Close]

* Account Name:

Real Name:

* New Password:

* Confirm New Password:

Phone:

Email:

Job Title:

Account Lockout: Lock account for (1-1440) minutes after (1-100) authentic attempt

Session Idle Timeout: (1-1440) minutes

Password Expiration: Require password change every (1-365) days

Password Reuse: Passwords cannot be the same as the last (1-6) times

Minimum Password Length: Password must be at least (8-64) characters
When minimum password length is changed, admin should change password well. Minimum password length changes apply for all future passwords on

Password Complexity: Password must be fulfilled as below:
- At least one upper-case character
- At least one lower-case character
- At least one numeric character
- At least one special character
- At least 8-chars within the old password should be changed

Minimum Password Lifetime: Password should not be changed twice within the 24 hours.

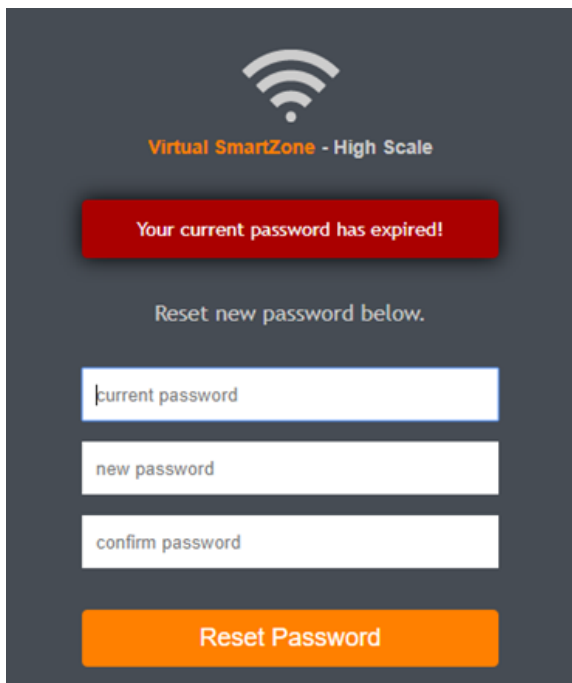
OK **Cancel**

4. Configure the following:

- Real Name: Type the name of the administrator.
- Phone: Type the phone number.
- Email: Type the email address.
- Job Title: Enter the role.
- 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.
- Session Idle Timeout: Click the button and enter the timeout duration in minutes.
- 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 265 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).
- Minimum Password Length: Indicates the minimum number of characters required for a password. If there is a change in the number of characters, the Admin must manually change the passwords for all users. Enter the minimum number of characters required for a password.
- Password Complexity: Ensures that the password applies the following rules:
 - At least one upper-case character
 - At least one lower-case character

- At least one numeric character
- At least one special character
- At least eight characters from the previous password is changed

Select the option.

- Minimum Password Lifetime: Ensures that the password is not changed twice within a period of 24 hours. Select the option.

5. Click **OK**.

The **Password Confirmation** page is displayed.

6. Enter the **Password**.

7. Click **OK** to apply the new configuration.

You have configured an administrator account.

Working with AAA Servers

You can configure the controller to use external AAA servers to authenticate users.

Configuring SZ Admin AAA Servers

To add and manage AAA servers that the controller can use to authenticate users, complete the following steps.

1. Select **Administration > Admins and Roles > AAA**.

2. From **AP AAA Servers**, click **Create**.

The **Create Administrator AAA Server** page is displayed.

FIGURE 266 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:

Administrators:

Backup RADIUS: ON Enable Secondary Server

Primary Server

* IP Address:

* Port:

* Protocol: PAP CHAP PEAP

* Shared Secret:

* Confirm Secrets:

Secondary Server

* IP Address:

* Port:

* Protocol: PAP CHAP PEAP

* Shared Secret:

* Confirm Secrets:

Failover Policy at NAS

* Request Timeout: Seconds

* Max Number of Retries: Times

* Reconnect Primary: Minute (1-60)

3. Enter the AAA server name.

4. For **Type**, select the type of AAA server to authenticate users:

- **RADIUS**
- **TACACS+**
- **Active Directory**
- **LDAP**

5. For **Realm**, enter the realm or service.

Multiple realms or services are supported. Separate multiple realms or services with a comma.

NOTE

Because the user login format (User Account + @ + Realm) includes a special character, the at symbol (@), the user account must not include the at symbol (@) separately on the AAA server.

6. Enable **Default Role Mapping**.

You can select **auto-mapping** for the system to automatically map between the AAA and SZ accounts.

If **Default Role Mapping** is disabled, the AAA administrator must be mapped to a local SZ Admin user with matching AAA attributes for the RADIUS, TACACS+, Active Directory, or LDAP servers.

- 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**, **user2**, or **user3** value depending on the SZ users or permissions you want the TACACS+ user to map.
- On an Active Directory or LDAP server, the user data can belong to the group **cn=Ruckus-WSG-User-SZAdminName** (for example, **cn=Ruckus-WSG-User-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 **Default Role Mapping** at the same time, but the mapping attributes override **Default Role Mapping**.

7. For **Backup RADIUS**, select **Enable Secondary Server** if a secondary RADIUS server exists on the network. Refer to step 9 for configuration settings.

8. Under **Primary Server**, configure the settings of the primary AAA server.
 - **IP Address:** Enter the IP address of the AAA server.
 - **Port:** Enter the UDP port that the RADIUS server is using. The default port is 1812.
 - **Protocol:** Select the **PAP** or **CHAP** or **PEAP** protocol.

NOTE

For the protocol PEAP and PAP, you must configure the Trusted CA certificate to support PEAP and EAP connection respectively.

- **Shared Secret:** Enter the shared secret.
- **Confirm Secret:** Re-enter the shared secret to confirm.
- **Windows Domain name:** Enter the domain name for the Windows server.
- **Base Domain Name:** Enter the name of the base domain.
- **Admin Domain Name:** Enter the domain name for the administrator.
- **Admin Password:** Enter the administrator password.
- **Confirm New Password:** Re-enter the password to confirm.
- **Key Attribute:** Enter the key attribute, such as UID.
- **Search Filter:** Enter a filter by which you want to search, such as objectClass=*

For **Active Directory**, configure the settings for the **Proxy Agent**.

- **User Principal Name:** Enter the Windows domain Administrator name
- **Password:** Enter the administrator password.
- **Confirm Password:** Re-enter the password to confirm.

9. Under **Secondary Server**, configure the settings of the secondary RADIUS server.
 - **IP Address:** Enter the IP address of the AAA server.
 - **Port:** Enter the UDP port that the RADIUS server is using. The default port is 1812.
 - **Protocol:** Select the **PAP** or **CHAP** or **PEAP** protocol.

NOTE

For the protocol PEAP and PAP, you must configure the Trusted CA certificate to support PEAP and EAP connection respectively.

- **Shared Secret:** Enter the shared secret.
- **Confirm Secret:** Re-enter the shared secret to confirm.

10. Under **Failover Policy at NAS**, configure the settings of the secondary RADIUS server.
 - **Request Timeout:** Enter the timeout period in seconds. After the timeout period, an expected RADIUS response message is considered to have failed.
 - **Max Number of Retries:** Enter the number of failed connection attempts. After the maximum number of attempts, the controller tries to connect to the backup RADIUS server.
 - **Reconnect Primary:** Enter the time in minutes, after that the controller connects to the primary server.

11. 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.

Testing SZ Admin AAA Servers

To ensure that the controller administrators are 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. Select **Administration > Admins & Roles > AAA**.
2. Select the created AAA server and click **Test AAA**.

An example for testing a RADIUS server is shown.

FIGURE 267 Testing an AAA Server: RADIUS

The screenshot shows a dialog box titled "Test AAA Servers" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Name:** A dropdown menu with "peapiPv6" selected.
- Protocol:** Labeled "PEAP".
- User Name:** A text input field containing "ramu". Below it is the text "(Test with username ONLY.)".
- Password:** A masked text input field containing ".....". Below it is a checkbox labeled "Show password".

Below the input fields, a green message reads: "AAA testing : Success! Associated with Auto Mapping [CACDEV]". At the bottom of the dialog are two buttons: "Test" and "Cancel".

The **Protocol** field is displayed only for RADIUS server that depends on the SZ AAA server configuration.

3. In the **Name** field, select the AAA server that you created.
4. In the **User Name** field, enter an existing user name that is associated to a user group.

NOTE

For TACACS+ server, test with username and realm.

5. In the **Password** field, enter password for the user name you specified.
6. Click **Test**.

If the username is associated with an user group, the following message is displayed: "AAA testing: Success! Associated with Auto Mapping". If the username is not associated with any user group, the following message is displayed: "AAA testing: Success! No SZ User or Default role mapping associated".

Configuring Switch AAA Servers

To add and manage AAA servers that the controller can use to authenticate users, complete the following steps.

1. Select **Administration > Admins and Roles > AAA**.
2. From **Switch AAA Servers**, click **Create**.

The **Create AAA Server** page is displayed.

FIGURE 268 Creating a Switch AAA Server

The screenshot shows a web form titled "Create AAA Server". The form includes the following fields and options:

- Name:** A text input field with an asterisk indicating it is required.
- Type:** Radio button options for "Radius" (selected), "TACACS+", and "Local User".
- IP Address:** A text input field with an asterisk indicating it is required.
- Auth. Port:** A text input field containing the value "1812".
- Acct. Port:** A text input field containing the value "1813".
- Shared Secret:** A text input field with an asterisk indicating it is required.
- Confirm Shared Secret:** A text input field with an asterisk indicating it is required.

At the bottom of the form are two buttons: "OK" and "Cancel".

3. Enter the AAA server name.
4. For **Type**, select the type of AAA server to authenticate users:
 - **RADIUS**
 - **TACACS+**
 - **Local User**
5. Enter the following information:
 - **IP Address:** Enter the IP address of the AAA server.
 - **Auth Port:** Enter the authentication port that the server is using.
 - **Acct Port:** Enter the accounting port that the server is using.
 - **Shared Secret:** Enter the shared secret.
 - **Confirm Shared Secret:** Re-enter the shared secret to confirm.
6. Click **OK**.

NOTE

You can also edit or delete the server by selecting the options **Configure** or **Delete** from the **Administrator** tab.

NOTE

ICX switch fails to delete the TACACS+ and Radius AAA servers when pushed from the SZ or vSZ if SNMP query is disabled in the switch or if this is a pre-configured switch before joining SZ or vSZ.

Configuring Switch AAA Server Settings

To configure and manage AAA servers, complete the following steps.

1. Select **Administration > Admins and Roles > AAA**.
2. From **Switch AAA Setting** configure the following.

Login Authentication

- **SSH Authentication:** Enable the option for secure authentication.
- **Telnet Authentication:** Enable the option to set Telnet authentication. This option requires SSH authentication to be enabled.
- **First Pref:** Select the first preferred authentication system.
- **Second Pref:** Select the second preferred authentication system.
- **Third Pref:** Select the third preferred authentication system.

Authorization

- **Command Authorization:** Enable this option to assign the following authorization services:
 - **Level:** Select the required privilege: **Port Config, Read Only, or Read Write.**
 - **Server 1:** Select the authorization method for the first server.
 - **Server 2:** Select the authorization method for the second server.
- **Exec Authorization:** Enable this option to authorize the user to access the privilege mode.
 - **Server 1:** Select the authorization method for the first server.
 - **Server 2:** Select the authorization method for the second server.

Accounting

- **Command Accounting:** Enable this option to track the following accounting services:
 - **Level:** Select the required privilege: **Port Config, Read Only, or Read Write.**
 - **Server 1:** Select the tracking method for the first server.
 - **Server 2:** Select the tracking method for the second server.
- **Exec Accounting:** Enable this option to track the services in the privilege mode.
 - **Server 1:** Select the tracking method for the first server.
 - **Server 2:** Select the tracking method for the second server.

3. Click **OK**.

AAA Server Authentication

Complete AAA-based authentication for the AAA server by performing one of the following steps.

1. Enable **Default Role Mapping** to map the external AAA users to a single SZ local admin user.

2. Apply the permissions of AAA users on SZ using the corresponding AAA server attributes.

Following is an example:

- a. Create three user groups with the following access permissions in SZ:
 - Group1 with SZ super permission
 - Group2 with SZ AP admin permission
 - Group3 with SZ read-only permission
- b. Create three SZ local users corresponding to the user groups as follows:
 - Bind User1 with Group1
 - Bind User2 with Group2
 - Bind User3 with Group3

NOTE

Following are the attribute values on AAA servers:

- RADIUS: **Ruckus-WSG-User=User1 or User2 or User3.**
 - TACACS+: **user-name=User1 or User2 or User3.**
 - Active Directory and LDAP: **Group cn=Ruckus-WSG-User-User1 or Ruckus-WSG-User-User2 or cn=Ruckus-WSG-User-User3.**
- c. Select **Administrator > Admins and Roles > AAA** and click **Create** to create an Admin AAA profile.
Refer to [Configuring SZ Admin AAA Servers](#) on page 511.

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 506. 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 503.

4. When adding a server type for administrators, select RADIUS as the authentication server type.

NOTE

Refer to [Configuring SZ Admin AAA Servers](#) on page 511.

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 506.

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 506.

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 503.

4. When adding a server type for administrators, select TACACS+ as the authentication server type.

NOTE

Refer to [Configuring SZ Admin AAA Servers](#) on page 511.

5. Test the TACACS+ server using the account **username@super-login**.

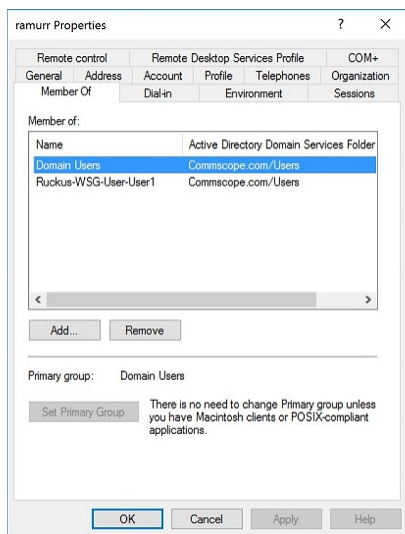
About Active Directory (AD) Support

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 506. 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 503 .

4. When you add an AAA server for administrators, select **Active Directory** as the authentication server type.

NOTE

Refer to [Configuring SZ Admin AAA Servers](#) on page 511.

5. 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 506.

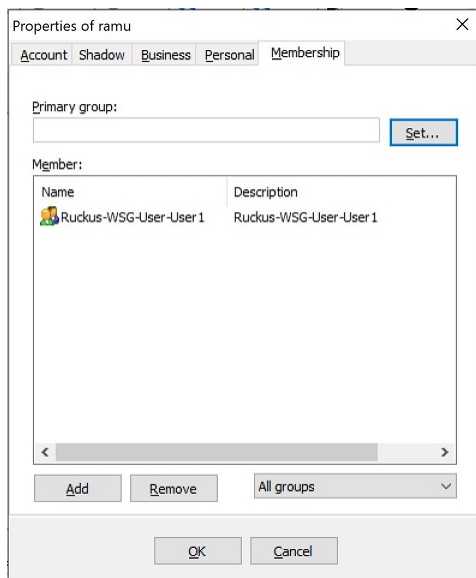
About LDAP Support

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.

1. Edit the LDAP configuration file on the LDAP 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 506. 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 503.

4. When you add an AAA server for administrators, select **LDAP** as the authentication server type.

NOTE

Refer to [Configuring SZ Admin AAA Servers](#) on page 511.

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 506.

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 269 Management Interface Access Control Rule

Management Interface Access Control Rule

The screenshot shows a configuration form for a Management Interface Access Control Rule. It includes the following fields and options:

- Name:** A text input field with an asterisk indicating it is required.
- Description:** A text input field.
- Type:** Radio button options for **Single IP** (selected), **IP Range**, and **Subnet**.
- Single IP:** A sub-section containing an **IP Address:** text input field with an asterisk.
- Buttons:** **OK** and **Cancel** buttons at the bottom right.

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

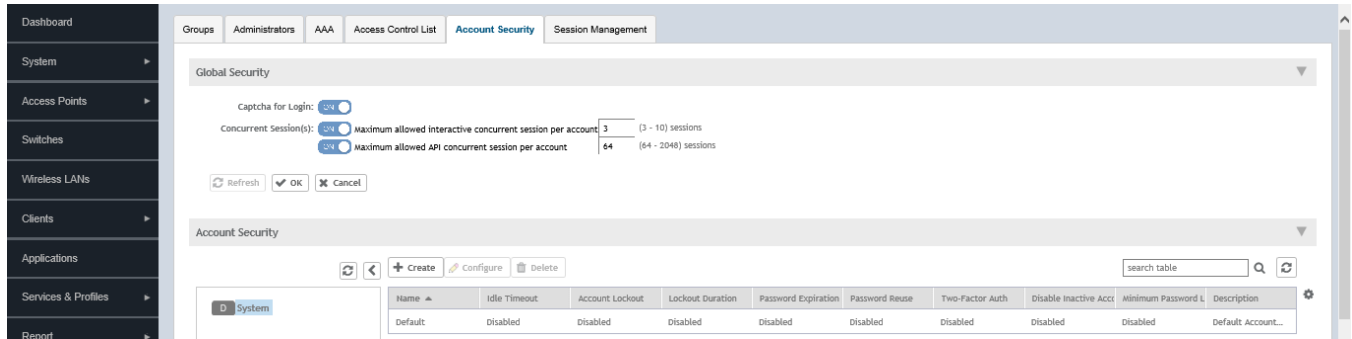
Creating an account security profile enables end-users to control administrative accounts to better manage admin accounts, passwords, login, and DoS prevention.

1. Go to **Administration > Admins and Roles**.

2. Select the **Account Security** tab.

The **Global Security** section and **Account Security** section is displayed.

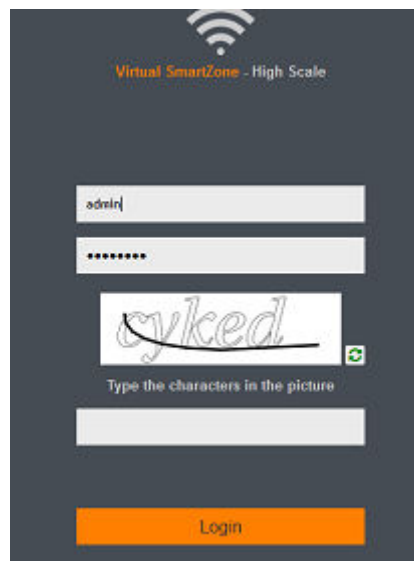
FIGURE 270 Account Security page



3. From Global Security, configure the following:

- a. **Captcha for Login:** select the option 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 271 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.

- b. **Concurrent sessions:** Click the required options and enter the number of sessions allowed:
 - **Maximum allowed interactive concurrent session per account**
 - **Maximum allowed API concurrent sessions per account**
- c. Click **OK**.

4. From **Account Security**, click **Create**.

The **Create Account Security** page appears.

FIGURE 272 Creating Account Security

Create Account Security

Name:

Description:

Session Idle Timeout: ON 15 (1-1440) minutes

Account Lockout: OFF Lock account for 30 (1-1440) minutes after 6 (1-100) failed authentication attempts

ON Lock account forever after 3 (1-100) failed attempts during 15 (1-1440) minute time period.
This option does not apply to AAA Admin Users.

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

Disable Inactive Accounts: ON Lock admin accounts if they have not been used in the last 90 (1-1000) days

Minimum Password Length: ON Password must be at least 8 (8-64) characters
When minimum password length is changed, admin should change passwords for all users manually as well. Minimum password length changes apply for all future passwords only

Password Complexity: OFF Password must be fulfilled as below:
When the password complexity is turned from off to on, admin should change all users' passwords manually. The password complexity rule will only be applied to the upcoming password changes.

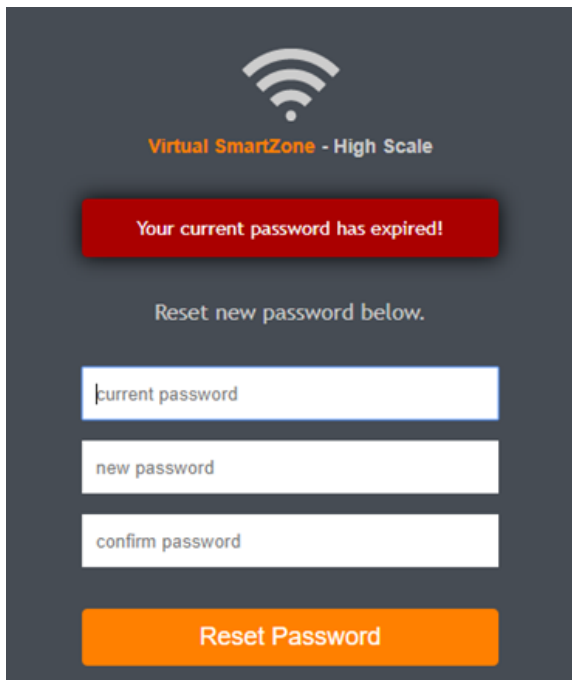
- At least one upper-case character
- At least one lower-case character

5. 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. Enable and configure one of the following:
 - Enter the account lockout time and number of failed authentication attempts.
 - Enter the number of failed attempts after which the account is locked and the corresponding time period. After three unsuccessful login attempts in a time interval of 15 minutes, the account is locked and must be released by an Administrator.
- 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 273 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).
- 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.
- Minimum Password Length: Indicates the minimum number of characters required for a password. If there is a change in the number of characters, the Admin must manually change the passwords for all users. Enter the minimum number of characters required for a password.

- **Password Complexity:** Ensures that the password applies the following rules:
 - At least one upper-case character
 - At least one lower-case character
 - At least one numeric character
 - At least one special character
 - At least eight characters from the previous password is changedSelect the option.
- **Minimum Password Lifetime:** Ensures that the password is not changed twice within a period of 24 hours. Select the option.

6. 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 SCI.
- 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 SCI 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>).

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 274 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:

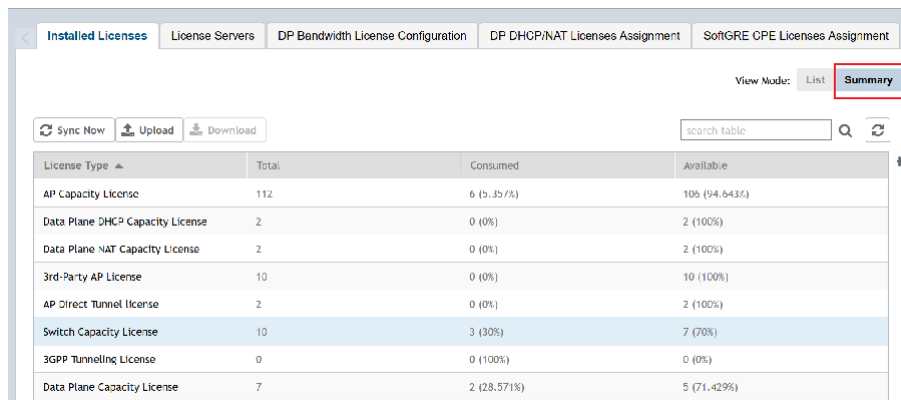
- **Name:** The name of the node to which the license was uploaded
- **Node:** The name of the controller node
- **Start Date:** The date when the license file was activated
- **Expiration Date:** For time-bound licenses, the date when the license file expires
- **Capacity:** The number of units or license 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 275 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 manages the licenses that you have purchased for the controller - Cloud License Server.

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.
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 276 License Bandwidth Configuration

| vSZ-D | Bandwidth |
|----------|-----------|
| 8799-vDP | 1Gbps |

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.



Assigning DP DHCP License Using the Wizard

The wizard is used to collect each DHCP setup component including service profile, licenses assignment and profile assignment by a group. The wizard does not change the DHCP license, profile assignment, limitation or rule.

To assign the DP DHCP License using the wizard:

1. Go to **Administration > Licenses**.
2. Select the **DP DHCP/NAT License Assignment** tab.
3. From the **DHCP License** area, click **Wizard**.

The **DP DHCP Wizard** form appears.

4. From the Data Planes tab, select a maximum of two DPs by zone affinity profile from the **Select Data Planes** list and click  to move it to the **Selected Data Planes** list.
5. Click **Next**, the **Service Profile** tab is displayed.
6. Select the **DHCP Profile** from the drop-down list or click  to create a new DHCP Profile.
 - For DHCP Profile Configuration, DHCP Option43 Space, and Host Configuration, refer [Configuring Global Settings](#) on page 468.
 - For DHCP Pools Configuration, refer [Configuring DHCP Pool Settings](#) on page 469.
7. Click **Next**, the **License** tab is displayed.

License Usage information displays the total number of licenses, number of licenses used, and the number of licenses available.
8. **License Count:** enter the number of licenses to be assigned for the DP not exceeding 101. Each count is multiplied into 1000 IP leases.
9. **Description:** enter a short description about the license assignment.
10. Click **Next**, the **Review** tab is displayed.
11. Review your settings to make sure everything is correct. Once you are satisfied with your settings, click **OK** to confirm.

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.



Assigning DP NAT License Using the Wizard

The wizard is used to collect NAT setup component by a group.

To assign the DP NAT License using the wizard:

1. Go to **Administration > Licenses**.
2. Select the **DP DHCP/NAT License Assignment** tab.
3. From the **NAT License** area, click **Wizard**.

The **DP NAT Wizard** form appears.

4. From the Data Planes tab, select a maximum of two DPs by zone affinity profile from the **Select Data Planes** list and click  to move it to the **Selected Data Planes** list.
5. Click **Next**, the **Service Profile** tab is displayed.
6. Select the **NAT Profile** from the drop-down list or click  to create a new NAT Profile.
 - For NAT Profile configuration, refer [Configuring NAT Global Settings](#) on page 471.
 - For NAT Pools configuration, refer [Configuring NAT Pool Setting](#) on page 471.
7. Click **Next**, the **License** tab is displayed.

License Usage information displays the total number of licenses, number of licenses used, and the number of licenses available.
8. **License Count:** enter the number of licenses to be assigned for the DP not exceeding 20 licenses. Each count is multiplied into 100000 sessions/flows.
9. **Description:** enter a short description about the license assignment.
10. Click **Next**, the **Review** tab is displayed.
11. Review your settings to make sure everything is correct. Once you are satisfied with your settings, click **OK** to confirm.

Configuring URL Filtering Licenses

You can configure the number of URL filtering licenses on an AP within a 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 a URL filtering license enabled, 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 must enable URL filtering on the zone or WLAN.

If the license limited to the zone is specified, 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 SZ300 and vSZ-H controllers is 10,000 licenses.

1. Select **Administration > Licenses**.
2. Select the **URL Filtering Licenses** tab.

FIGURE 277 URL Filtering Licenses

| Zone Name | Number of Licenses | License Limit | WLANs with URL Filtering ON | Ethernet Port Profiles with URL Filtering ON |
|-----------|--------------------|---------------|-----------------------------|--|
| 11ax-Zone | 1 | Unlimited | 11R730-WLAN-DVC | Eth |

The **URL Filtering Licenses** tab displays the following information:

- **Zone Name:** The name of the zone within which APs are present.
- **Number of Licenses:** Displays the total number of licenses allocated to the zone.
- **License Limit:** Displays the number of APs (with URL filtering enabled) that can be accommodated within the zone. Can be set to a specific value or Unlimited.
- **WLANs with URL Filtering ON:** Displays all the WLANs within the zone that have the URL filtering service enabled.
- **Ethernet Port Profiles with URL Filtering ON:** Displays the Ethernet port profiles 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**.

Support AP Licensing for the Controller

In the previous SmartZone releases, users were unable to view the AP support license information until the controller displayed a warning message during system upgrade.

From the current release, users can view the AP support license information on the controller web user interface by navigating to **Administration > Licenses > Installed License** retrieved from the license server at any given point of time. To view the AP license status and validity click **View > Summary** tab.

The screenshot shows the 'Installed Licenses' page. At the top, there are tabs for 'Installed Licenses', 'License Servers', and 'URL Filtering Licenses'. Below the tabs, there are buttons for 'Sync Now', 'Upload', and 'Download'. A 'View Mode' dropdown is set to 'Summary'. There are search and refresh icons for both tables. The first table has 5 records, and the second table has 1 record.

| License Type | Total | Consumed | Available |
|----------------------------------|-------|----------|--------------|
| AP Capacity License | 100 | 3 (3%) | 97 (97%) |
| AP Direct Tunnel license | 100 | 0 (0%) | 100 (100%) |
| AP Split Tunnel Capacity License | 10000 | 0 (0%) | 10000 (100%) |
| Switch Capacity License | 2000 | 0 (0%) | 2000 (100%) |
| URL Filtering Capacity License | 10000 | 0 (0%) | 10000 (100%) |

| License Type | Status | Expiration Date |
|--------------------|--------|-----------------|
| AP Support License | Valid | 2029/03/08 |

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.

TABLE 96 Migration Support Matrix

| SmartZone Version | ZoneDirector Version |
|-------------------|------------------------|
| 3.5.x | 9.13x |
| 3.5.x | 9.13.x, 10.0.x, 10.1.x |
| 3.5.x | 9.13.x, 10.0.x, 10.1.x |
| 3.5.x | 9.13.x, 10.0.x, 10.1.x |



CAUTION

Do not power off the AP during the migration process.

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.

NOTE

To migrate ZoneDirector Mesh APs to SmartZone, upgrade ZoneDirector to its supported version. For information on the supported versions, refer 5.2.1 release notes.

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
- Managed By: Displays the system that manages the admin activities.
- Source IP: Displays the IP address of the device form 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.

Managing Mobile Virtual Network Operator (MVNO) Accounts

A Mobile Virtual Network Operator (MVNO) uses a host carrier network to service its mobile users. An MVNO account is created for each operator and the MVNO page lists the accounts that are created.

1. Go to **Administration > MVNO**.

The **MVNO** page appears displaying information about MVNO accounts created.

2. Click **Create** to create an MVNO account.

The **The Mobile Virtual Network Operator** page appears.

3. Configure the following:

- a. The Mobile Virtual Network Operator Summary

1. **Domain Name:** Type a domain name to which this account will be assigned
2. **Description:** Type a brief description about this domain name.

- b. **AP Zones of Mobile Virtual Network Operator:** Displays the AP zones that are allocated to this MVNO account

1. Click **Add AP Zone**. The **Add AP Zone** page appears.
2. **AP Zone:** Select the AP zone you want to add to the MVNO account from the drop-down menu.
3. Click **OK**.

NOTE

You can only select a single AP zone at a time. If you want to grant the MVNO account management privileges to multiple AP zones, select them one at a time.

- c. **WLAN Services:** Configure the WLAN services to which the MVNO account that you are creating will have management privileges.

1. Click **Add WLAN**. The **Add WLAN** page appears.
2. **SSID:** Select the WLAN to which the MVNO account will have management privileges.

NOTE

You can only select one WLAN service at a time. If you want to grant the MVNO account management privileges to multiple WLAN service zones, select them one at a time.

3. Click **OK**.

- d. **Super Administrator:** Configure and define the logon details and management capabilities that will be assigned to the account.

1. **Account Name:** Type the name that this MVNO will use to log on to the controller.
2. **Real Name:** Type the actual name (for example, John Smith) of the MVNO.
3. **Password:** Type the password that this MVNO will use (in conjunction with the Account Name) to log on to the controller.
4. **Confirm Password:** Type the same password as above. f) **In Phone,** type the phone number of this MVNO.
5. **Phone:** Type the phone number of the administrator.
6. **Email:** Type the email address of this MVNO.
7. **Job Title:** Type the job title or position of this MVNO in his organization.

- e. **RADIUS Server for Administrator Authorization and Authentication:** See [Configuring SZ Admin AAA Servers](#) on page 511 for more information.

4. Click **OK**.

You have created an MVNO account.

NOTE

You can also edit and delete the account by selecting the options **Configure**, and **Delete** respectively, from the **MVNO** page.

Terminating Administrator Sessions

From the **Session Management** tab, you can view and also terminate the administrator's sessions that are currently sunning.

1. From the controller web interface, go to **Administration > Admin and Roles > Session Management**
2. Select the administrator session you want to discontinue and click **Terminate**.
The **Password Confirmation** page appears.
3. Type the password and click **OK**. The session ends.

You can terminate all CLI and UI sessions that you were logged into.

FIGURE 278 Sample Session Termination for UI session.

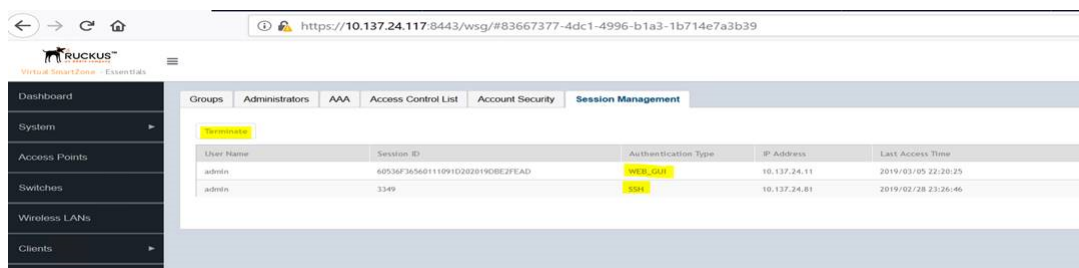


FIGURE 279 Sample Session Termination for CLI session.

```
[root@IRAWAT ~]# ssh admin@10.1.200.102
The authenticity of host '10.1.200.102 (10.1.200.102)' can't be established.
RSA key fingerprint is 03:f8:c0:07:99:1f:cd:d7:83:22:9f:81:17:5e:b5:97.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.1.200.102' (RSA) to the list of known hosts.
Access to this system is reserved only for authorized administrators.
This is a default login banner and can be configured by authorized administrators of the system
admin@10.1.200.102's password:
Last login: Fri Jan 11 05:26:59 2019

en
Please wait. CLI initializing...

Welcome to the Ruckus SmartZone 300 Command Line Interface
Version: 5.1.1.0.242

VSZ100>
VSZ100>
VSZ100> en
Password: *****

VSZ100# Connection to 10.1.200.102 closed by remote host.
Connection to 10.1.200.102 closed.
```


Administrating the Cluster

- SmartZone Cluster Mode..... 539
- Powering Cluster Back..... 541
- Backing Up and Restoring Clusters..... 541
- Replacing a Controller Node..... 552
- Upgrading the Controller..... 553
- Cautions & Limitations of Administrating a Cluster 558

SmartZone Cluster Mode

SmartZone system state has two cluster modes.

The two cluster modes are -

- Crash mode
- Suspend mode

Crash mode

The system cluster enters this mode when system meets unexpected error during fresh install or reboot flow. The system runs into ir-recoverable error and should be set to reset-factory settings.

System enters into *Crash mode* in any one of the below conditions:

1. System reboot with environment inconsistency.
 - a. Model
 - b. Port group (SZ 100)
 - c. Firmware Version
2. Fresh install fail.
3. Join cluster fail.

Suspend mode

The system enters this mode if there is an environment error during reboot flow. The configurer sets up suspend flag and stops all applications. The system can be recovered by rebooting as it is a temporary fail.

System enters into *Suspend mode* in any one of the below conditions:

1. Platform applications cannot be launched successfully.
2. Failed on membership authentication in cluster .

To check status of the cluster state, use **show cluster state** command.

FIGURE 280 Crash and Suspended modes

```
dean300-3# show cluster-state
Current Management Service Status : Out of service
Current Node Status : Out of service
Cluster Status : In service
Cluster Operation : None
System Mode : Suspend
```

```
dean100521-3# show cluster-state
Current Management Service Status : Out of service
Current Node Status : Out of service
Cluster Status : In service
Cluster Operation : None
System Mode : Crash
```

To recover system in case of *Suspend mode*, use **reload** command. System automatically detects suspend flag and clears before launching applications.

FIGURE 281 reload

```
login as: admin
#####
# Welcome to vSZ #
#####
admin@10.206.20.243's password: *****
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface
Version: 5.2.1.0.145
% System is in Suspend Mode. Please reboot system to recover.

deanvszh521-3> en
Password: *****

deanvszh521-3# reload
Do you want to gracefully reboot system after 30 seconds (or input 'no' to cancel)? [yes/no] yes
Server would be rebooted in 30 seconds
```

To reset system to factory settings in case of *Crash mode*, use **set-factory** command.

FIGURE 282 set-factory

```
#####  
#       Welcome to vSZ       #  
#####  
admin@10.206.20.244's password: *****  
Please wait. CLI initializing...  
  
Welcome to the Ruckus Virtual SmartZone - High Scale Command Line Interface  
Version: 5.2.1.0.171  
* System is in Crash Mode. Please set-factory system to recover.  
  
deanvszh52geocrash> en  
Password: *****  
  
deanvszh52geocrash# set-factory
```

Powering Cluster Back

SmartZone cluster nodes may need to be shut down for physical migration/maintenance purpose.

To avoid SmartZone enter crash mode, the cluster needs to form back in time (within Two-and-Half hours). To power up the nodes, perform the following:

1. Power up all nodes at the same time period.
2. All nodes are connected by network.
3. During the setup, it is strongly recommended to configure static IP address to SmartZone interface, if the node's interface IP address settings is configured to DHCP. Make sure the DHCP server assigns a fixed IP address to the interfaces.

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.

Disaster Recovery

Creating cluster backup and restoring cluster configurations periodically helps manage disaster recovery.

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 97 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.

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 98 Information that is backed up to the FTP server

| Control Plane | Data Plane |
|--|--|
| <ul style="list-style-type: none"> Control interface Cluster interface Management interface Static routes User-defined interfaces | <ul style="list-style-type: none"> Primary interface Static routes Internal subnet prefix |

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 283 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 284 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 285 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 286 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.

- 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 287 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:AAAAaa123@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
```

- 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.

- 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 288 Enable privileged mode

```
cb172651> en
Password: *****
```

3. 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 289 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 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`
5. 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
6. Enter `show backup-network` to verify that the backup file was copied back to the controller successfully.

FIGURE 290 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
```

7. 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 291 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 292 The controller performs several steps to restore the backup file

```

cal12651# 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
07:20:24.342 [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, 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 (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 293 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.

Replacing a Controller Node

Replacing a Controller Node in Multi-Node Cluster

This section describes how to replace a controller node in a multi-node cluster. Removing a node and joining a new node is the standard process to replace a node.

Step 1: Wipe-out Upgrade Controller Node

If the Controller node does not match with the existing cluster version, prepare a new Controller and wipe-out upgrade to the same version of the running cluster. See [Performing a Wipe-out Upgrade for Controller Node](#) on page 553.

Step 2: Remove RMA Controller Node

Choose a controller that will remain in the cluster and follow the steps:

1. Log on to the web interface of the chosen controller using administrator credentials.
2. Go to **System > Cluster** and locate the node that you want to replace in the cluster planes.
3. Click **Delete** to remove the node from the cluster.

Step 3: Join the New Controller Node

To join the new controller into the running cluster:

1. Prepare a proper version of the controller by wipe-out upgrade. See [Performing a Wipe-out Upgrade for Controller Node](#) on page 553.
2. Set up the node as a new controller, and then join the existing cluster. For step by step instructions, refer to the *Getting Started Guide*.

Replacing a Controller Node in Single Node Cluster

This section describes how to replace a controller node in single node cluster. Original configuration backup and a new node are required.

Step 1: Wipe-out Upgrade Controller Node

If the Controller node does not match with the existing cluster version, prepare a new Controller and wipe-out upgrade to the same version of the running cluster. See [Performing a Wipe-out Upgrade for Controller Node](#) on page 553.

Step 2: Join New Controller Node

Set up the node as a new controller. For step by step instructions, see the *Getting Started Guide*.

Step 3: Configuration Restore

With original configuration backup follow the steps to restore the configuration in cluster:

1. Prepare the new controller to which you will restore the cluster backup.
 - a. Either obtain a new controller or factory reset an existing controller.
 - b. Log on to the controller as a system administrator.
 - c. Run the setup command to configure the controller's network settings.
 - d. Complete the controller setup process from the **CLI**.
2. After you complete the controller setup, log on to the controller web interface as a system administrator.
3. Go to **Administration > Backup and Restore**.
4. Select the **Configuration** tab.
5. Click **Upload**. After the configuration file is uploaded successfully, it appears in the Configuration section.
6. Restore the configuration backup to the node either using the web interface or the **CLI**.
 - To use the web interface:
 - a. Go to **Administration > Backup and Restore** page.
 - b. In the **Configuration** tab, locate the configuration backup file that you want to restore.
 - c. Click **Restore**.
 - d. Follow the prompts (if any) to complete the restore process.
 - To use the **CLI**:
 - a. Log on to the **CLI** of the node as a system administrator.
 - b. Run the **restore config** command.

Performing a Wipe-out Upgrade for Controller Node

If the firmware version on this controller (shown in the Cluster Information page) does not match the firmware version for new cluster setup or join an existing, a message appears and prompts you to upgrade the controller's firmware. Click **Upgrade**, and then follow the prompts to perform the upgrade.

NOTE

Refer [Cautions & Limitations of Administrating a Cluster](#) on page 558 for more information.

- For controller running firmware version 5.1 or later can do wipe-out upgrade successfully to greater than 5.1.
- For controller running firmware version earlier than 5.1, apply a KSP patch to make wipe-out upgrade successful Contact Ruckus support to receive a KSP patch to apply the patch from CLI.

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.

If you are managing a vSZ-H controller, you can also perform system configuration backup, restore, and upgrade from the controller command line interface.

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 command. If you have a two nodes controller cluster, run the restore command on one of the nodes to restore them to the previous software before attempting to upgrade them again. The restore command will trigger restore action on all nodes of the cluster if all nodes could be connected to each other. Confirm if each node can be restored

back to the previous version. If any node does not roll back to the previous version, execute the restore command again on the failure node.

- 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 544 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 544.
- 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 545 for remote backup instructions and [Restoring from an FTP Server](#) on page 547 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 SZ100-D

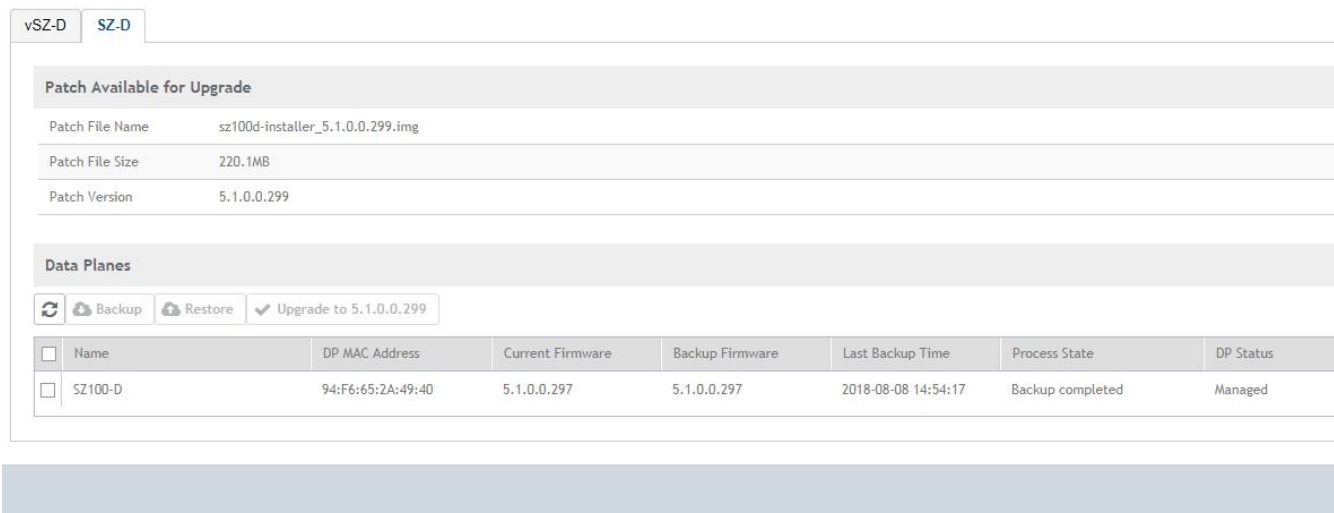
SZ100-D is shipped with 3.6.1 release version and you must upgrade it to 5.1 release version. As vSZ manages SZ100-D, ensure that vSZ has the same or later version than SZ100-D. Otherwise, upgrade vSZ before upgrading SZ100-D. SmartZone release 5.1.1 supports SZ100-D. For more information, refer to the *Ruckus SmartZone100-D Quick Setup Guide*.

To Upgrade the Data Plane:

1. Go to **Administration > Upgrade**.

2. Select the **DP Patch** tab.
The **DP Patch** page appears.

FIGURE 294 DP Patch - Data Plane Upgrade



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

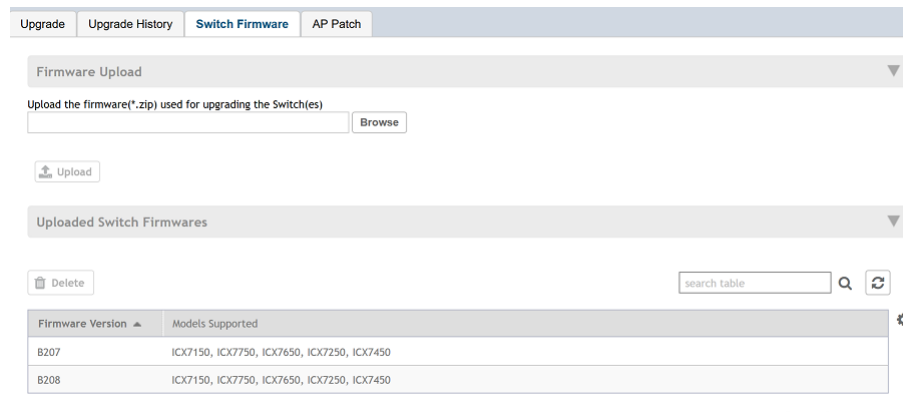
To have a copy of the data plane firmware or move back to the older version, you can select the data plane from the list and click **Backup** or **Restore** respectively.

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 295 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.

Cautions & Limitations of Administrating a Cluster

Wipeout Upgrade

Wipe-out upgrade can be done to a controller firmware running

- a version later than 5.1 to a version later than 5.1
- a version earlier than 5.1 by applying a KSP patch to make the wipe-out upgrade successful.

Contact Ruckus support to receive a KSP patch file to patch from CLI.

Cluster Upgrade

For issues during software upgrade, you can only perform the software rollback from the CLI using the restore command. If you have a two nodes controller cluster, run the restore command on one of the nodes to restore them to the previous software before attempting to upgrade them again. The restore command will trigger restore action on all nodes of the cluster if all nodes could be connected to each other. Confirm if each node could be restored back to the previous version. If any node does not roll back to previous version, execute the restore command again on the failure node. Refer [Rolling Back to a Previous Software Version](#) on page 555.

Cluster Restore

The cluster Restore feature is designed for disaster recovery when the cluster upgrade fails and the user need rollback the cluster to its previous version.

NOTE

Do not restore the cluster to future version. Go to future version is an upgrade activity, not a restore activity.

When the cluster upgrade fails, the cluster needs restore by the cluster backup files. The restore function is designed to rollback to previous version. The restore to future version is not supported. The upgrade requirement need go through upgrade function. If you are trying to replace a controller node, please refer to section [Replacing a Controller Node in Multi-Node Cluster](#) on page 552. Do not perform restore action for the replace node action.

If you try to restore the cluster to a future version, you will encounter a fatal error. For example, restoring 5.1.x → 5.2 will trigger a fatal brick issue especially on SZ100, SZ300.

Diagnostics

- Applying Scripts..... 561
- Uploading AP CLI Scripts..... 561
- Viewing and Downloading Logs..... 566
- Viewing DHCP and NAT Information..... 567
- GGSN..... 569
- RADIUS..... 570

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.

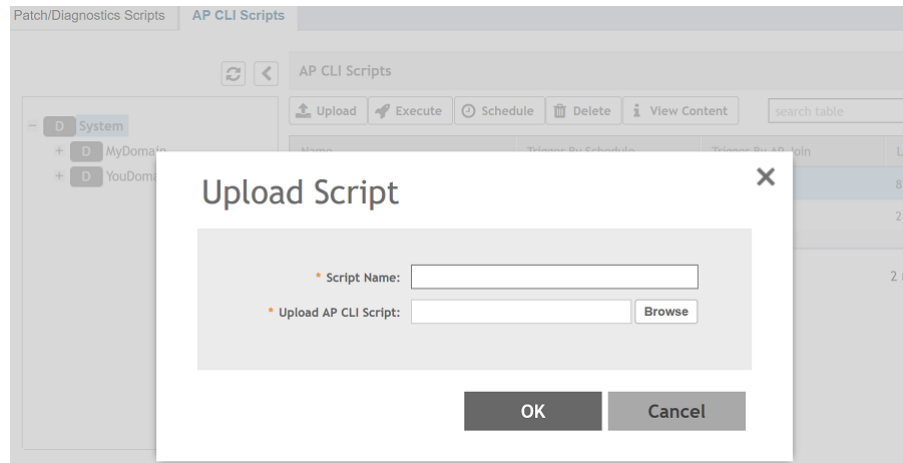
Diagnostics

Uploading AP CLI Scripts

4. Click **Upload**.

The Upload page appears.

FIGURE 296 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.

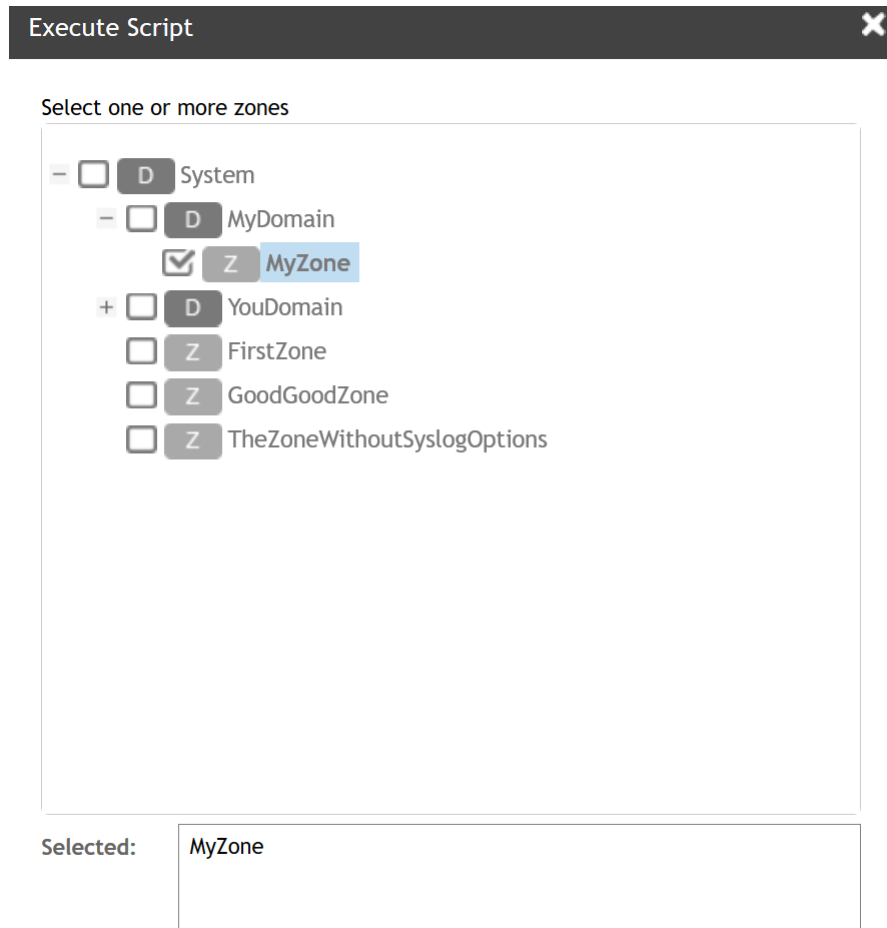
Executing AP CLI Scripts

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.

5. Click **Execute**.
The **Execute Script** page appears.

FIGURE 297 Executing script



6. Select one or more zones from the domain tree.
7. 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.

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.

5. Click **Schedule**.

The **Schedule Script** page appears.

FIGURE 298 Scheduling scripts

Schedule Script [X]

Execute on a Schedule: ON

Current System Time Zone is (GMT+8:00) Asia/Taipei.

* Interval: Daily

* Time: 00 00

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.

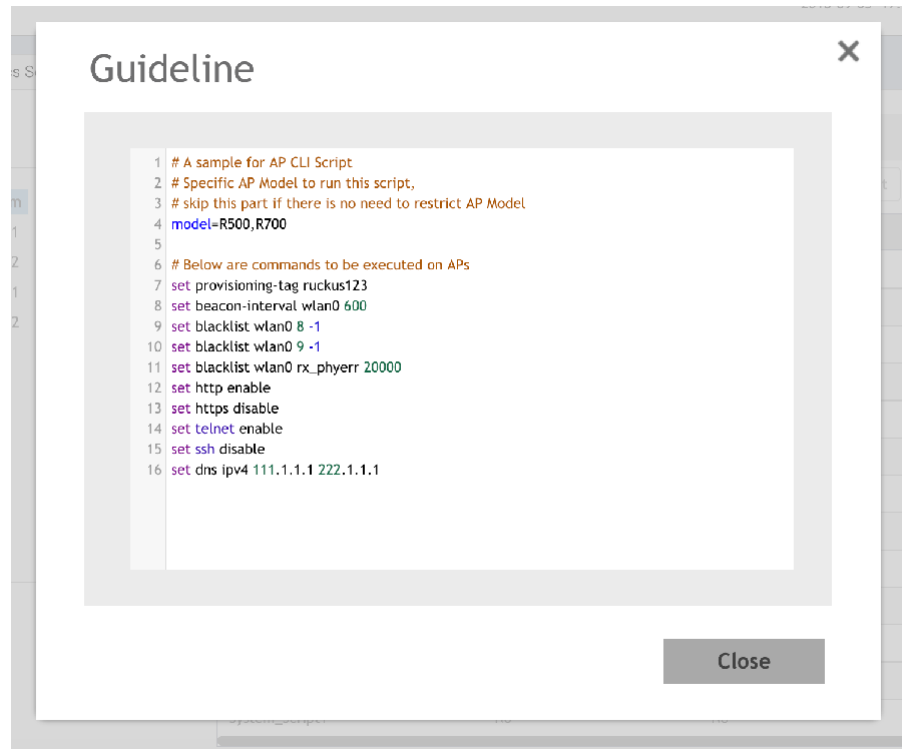
Viewing Scripts

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.

5. Click **View Content**.
The script page appears.

FIGURE 299 Viewing script details



6. 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.

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.
5. In the History tab below, you will see the list of scripts that were executed.

Diagnostics

Viewing and Downloading Logs

- 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 300 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 Logs To download all available logs from the controller.

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 99 Controller applications and log types for vSZ-H and SZ300

| Application | Description |
|----------------------|---|
| 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 |
| Communicator | Communicates with access points and retrieves statuses, statistics, and configuration updates |
| Configurer | Performs configuration synchronization and cluster operations (for example, join, remove, upgrade, backup, and restore) |
| Diagnostics | An interface that can be use to upload Ruckus scripts (.ksp files) for troubleshooting or applying software patches. This interface displays the diagnostic scripts and system patch scripts that are uploaded to a node. |
| EAut | Manages the sessions on the controller TTG module |
| EventReader | Receives event messages from access points and saves the information into the database |
| Greyhound | The interface between the controller TTG module and the AP interface, used to send and receive proprietary messages for AP association and disassociation |
| LogMgr | Organizes the Application Logs into a common format, segregates them, and copies them into the respective Application log file |
| MdProxy | MdProxy on AP and controller connect to AP-MD and controller-MD respectively. MdProxy on controller receives messages and retrieves the message header. It also forwards the response to controller-MD. This message is sent to the MdProxy on AP through AP-MD. MdProxy on the AP removes the MSL header and responds to the connection on which the request was received. |
| 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 |
| MsgDist | The Message distributor (MD) maintains a list of communication points for both local applications and remote MDs to perform local and remote routing |
| NC | The Node Controller, which monitors all controller TTG processes |
| NginX | Is a web server that is used as a reserve proxy server or a HTTP cache |
| Northbound | As an interface between SP and AAA, it 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 |
| Scheduler | Performs task scheduling and aggregates statistical data |
| SNMP | Provides a framework for the monitoring devices on a network. The SNMP manager is the system is used to control and monitor the activities of network hosts using SNMP. As an agent that responds to queries from the SNMP Manager, SNMP Traps with relevant details are sent to the SNMP Manager when configured. |
| SubscriberManagement | Maintains 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 management web server |

Viewing DHCP and NAT Information

You must be aware of the DHCP and NAT information of the controller to monitor the health of the controller.

1. Go to **Diagnostics > DHCP & NAT** .

2. Select the following tabs to monitor:

- **DHCP Relay (DP):** To monitor the DHCP relay information of the Data Planes. Displays information the of DHCP relay packets when DHCP relay is enabled in **Core Network Tunnel > Bridge or L2oGRE**.

FIGURE 301 Diagnostics - DHCP Relay

| Data Plane | DHCP Server IP | DISCOVER | OFFER | REQUEST | ACK | DHCP Option 82 | DHCP Packets Dropped |
|---------------|----------------|----------|-------|---------|-----|----------------|----------------------|
| No data - 1 - | | | | | | | |

- **TTG (DHCP Proxy):** To monitor TTG (DHCP Proxy) information of the Data Planes. Displays information on the TTG packets of DHCP relay when DHCP relay is enabled in **Core Network Tunnel > TTG+PDG**.

FIGURE 302 Diagnostics - TTG (DHCP Proxy)

| Data Plane | OFFER | REQUEST | NAK | ACK | DISCOVER | RELEASE | DECLINE | DROP | INFORM | OTHERS |
|------------|-------|---------|-----|-----|----------|---------|---------|------|--------|--------|
| Demo-D-2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Demo-D-1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

2 records - 1 -

- **DHCP (DP):** To monitor the DHCP DP information of the Data Planes. Display information of the DP DHCP server packets and the number of IPs assigned .

FIGURE 303 Diagnostics - DHCP DP

| Data Plane | Status | DISCOVER | OFFER | REQUEST | NAK | ACK | RELEASE | INFORM | DECLINE | DROP | ERROR | OTHERS |
|------------|---------|----------|-------|---------|-----|-----|---------|--------|---------|------|-------|--------|
| Demo-D-1 | Enabled | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

1 records - 1 -

- **NAT (DP):** To monitor the NAT DP information of the Data Planes. Displays information of the DP NAT server packets and the number of used ports.

FIGURE 304 Diagnostics - NAT DP

| Data Plane | Status | Public VLAN | Num of Pools | Up Stream(bps) | Down Stream(bps) |
|---------------|--------|-------------|--------------|----------------|------------------|
| No data - 1 - | | | | | |

GGSN

Viewing GGSN Connection Settings

You must be aware of the GGSN connection settings on the controller to monitor the health of the controller.

To view the GGSN connection settings:

1. Go to **Diagnostics > GGSN**.
2. Select the **GGSN Connection** tab.

The **GGSN Connection** page appears displaying the settings.

FIGURE 305 Diagnostics - GGSN connection

| Control Plane | GGSN IP | Echo Req Sent | Echo Rsp Rcvd | Echo Req Rcvd | Echo Rsp Sent | PathFailure | Created On | Last Modified On |
|---------------|------------|---------------|---------------|---------------|---------------|-------------|---------------------|---------------------|
| setup-1-C | 10.1.13.43 | 2 | 2 | N/A | N/A | N/A | 2017/02/24 16:09:45 | 2017/03/01 12:48:25 |

1 total records « 1 »

Viewing GGSN/PGW GTP-C Session Settings

You must be aware of the GGSN session settings on the controller to monitor the health of the controller.

To view the GGSN/PGW GTP-C session settings:

1. Go to **Diagnostics > GGSN**.
2. Select the **GGSN/PGW GTP-C Session** tab.

The **GGSN/PGW GTP-C Session** page appears displaying the settings.

FIGURE 306 Diagnostics - GGSN/PGW GTP-C Session

| MVNO Account | Control Plane | GGSN IP | Created On | Last Modified On | PDP Context | GGSN Init Updat | Controller Init U | Controller Init U | Cont |
|--------------|---------------|------------|---------------------|---------------------|-------------|-----------------|-------------------|-------------------|------|
| Super | setup-1-C | 10.1.13.43 | 2017/02/24 16:09:45 | 2017/03/01 13:00:55 | 0/2/0 | 0/0 | 0/0 | 0/0 | 0/0 |

1 total records « 1 »

RADIUS

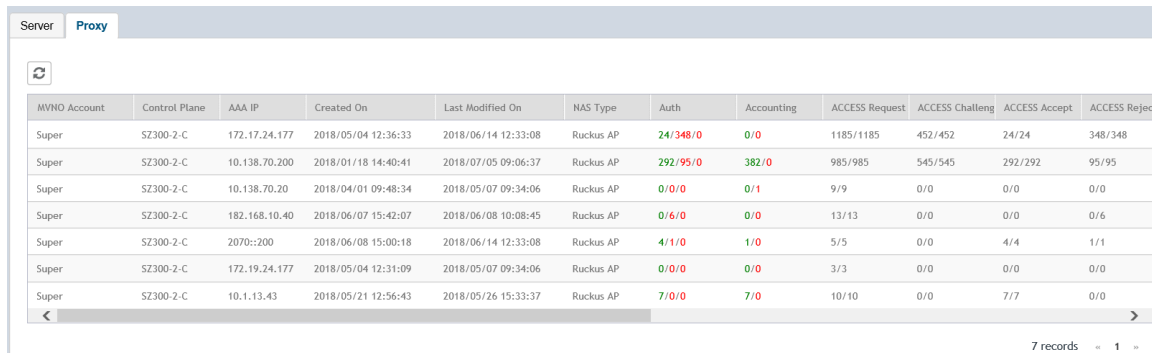
Viewing RADIUS Proxy Settings

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 307 Diagnostics - RADIUS Proxy



The screenshot shows the 'Proxy' tab in the RADIUS settings. It features a table with 12 columns: MVNO Account, Control Plane, AAA IP, Created On, Last Modified On, NAS Type, Auth, Accounting, ACCESS Request, ACCESS Challeng, ACCESS Accept, and ACCESS Rejec. There are 7 rows of data. Below the table, it indicates '7 records' and navigation arrows.

| MVNO Account | Control Plane | AAA IP | Created On | Last Modified On | NAS Type | Auth | Accounting | ACCESS Request | ACCESS Challeng | ACCESS Accept | ACCESS Rejec |
|--------------|---------------|---------------|---------------------|---------------------|-----------|----------|------------|----------------|-----------------|---------------|--------------|
| Super | SZ300-2-C | 172.17.24.177 | 2018/05/04 12:36:33 | 2018/06/14 12:33:08 | Ruckus AP | 24/348/0 | 0/0 | 1185/1185 | 452/452 | 24/24 | 348/348 |
| Super | SZ300-2-C | 10.138.70.200 | 2018/01/18 14:40:41 | 2018/07/05 09:06:37 | Ruckus AP | 292/95/0 | 382/0 | 985/985 | 545/545 | 292/292 | 95/95 |
| Super | SZ300-2-C | 10.138.70.20 | 2018/04/01 09:48:34 | 2018/05/07 09:34:06 | Ruckus AP | 0/0/0 | 0/1 | 9/9 | 0/0 | 0/0 | 0/0 |
| Super | SZ300-2-C | 182.168.10.40 | 2018/06/07 15:42:07 | 2018/06/08 10:08:45 | Ruckus AP | 0/6/0 | 0/0 | 13/13 | 0/0 | 0/0 | 0/6 |
| Super | SZ300-2-C | 2070::200 | 2018/06/08 15:00:18 | 2018/06/14 12:33:08 | Ruckus AP | 4/1/0 | 1/0 | 5/5 | 0/0 | 4/4 | 1/1 |
| Super | SZ300-2-C | 172.19.24.177 | 2018/05/04 12:31:09 | 2018/05/07 09:34:06 | Ruckus AP | 0/0/0 | 0/0 | 3/3 | 0/0 | 0/0 | 0/0 |
| Super | SZ300-2-C | 10.1.13.43 | 2018/05/21 12:56:43 | 2018/05/26 15:33:37 | Ruckus AP | 7/0/0 | 7/0 | 10/10 | 0/0 | 7/7 | 0/0 |

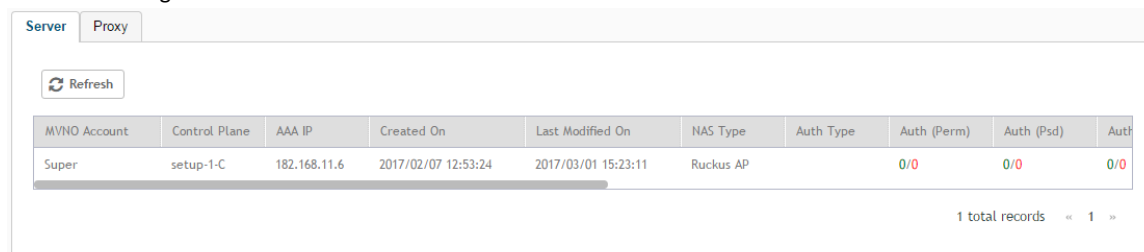
Viewing RADIUS Server Settings

You must be aware of the RADIUS server settings on the controller to monitor the health of the controller.

Go to **Administration > RADIUS**.

The **Server** page appears displaying the RADIUS settings.

FIGURE 308 Diagnostics - RADIUS Server



The screenshot shows the 'Server' tab in the RADIUS settings. It features a table with 10 columns: MVNO Account, Control Plane, AAA IP, Created On, Last Modified On, NAS Type, Auth Type, Auth (Perm), Auth (Psd), and Auth. There is 1 row of data. Below the table, it indicates '1 total records' and navigation arrows.

| MVNO Account | Control Plane | AAA IP | Created On | Last Modified On | NAS Type | Auth Type | Auth (Perm) | Auth (Psd) | Auth |
|--------------|---------------|--------------|---------------------|---------------------|-----------|-----------|-------------|------------|------|
| Super | setup-1-C | 182.168.11.6 | 2017/02/07 12:53:24 | 2017/03/01 15:23:11 | Ruckus AP | | 0/0 | 0/0 | 0/0 |

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 100 Ports to open for AP-Controller Communication Table

| Port Number | Layer 4 Protocol | From (Sender) | To (Listener) | Interface | Configurable from Web Interface? | Purpose |
|-------------|------------------|---|--|------------------------------|----------------------------------|--|
| 21 | TCP | AP | Control plane of <ul style="list-style-type: none"> • SZ100 • SZ300 • SCG200 • vSZ | Control | No | ZD/Solo APs can download SZ AP firmware and converting themselves to SZ APs. |
| 20-21 | TCP | SZ | External FTP server | Control, Cluster, Management | No | Transfer data to external FTP servers |
| 22 | TCP | <ul style="list-style-type: none"> • AP • vSZ-D | vSZ control plane | Control, Cluster, Management | No | SSH tunnel |
| 49 | TCP | TACACS+ Server | TACACS+ Server | Management, Cluster, Control | No | TACACS_Plus |
| 53 | TCP/UDP | DNS Server | DNS | Management, Cluster, Control | No | DNS |
| 67,68 | UDP | DHCP Server | SZ | Control, Cluster, Management | No | DHCP Protocol |
| 69 | UDP | ZD AP | SZ | Control | No | ZD Migration |
| 80 | TCP | Walled-Garden Web Server | CaptivePortal with HTTP Proxy | Management, Cluster, Control | No | WISPr_WalledGarden |

Ports to Open for AP-Controller Communication

TABLE 100 Ports to open for AP-Controller Communication Table (continued)

| Port Number | Layer 4 Protocol | From (Sender) | To (Listener) | Interface | Configurable from Web Interface? | Purpose |
|--|------------------|---|--------------------------------|------------------------------|----------------------------------|---|
| 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 | Control | 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>NOTE 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> |
| 123 | UDP | Follower SZ nodes | Master SZ node | Cluster | No | Sync system time among SZ nodes |
| 161 | UDP | SNMP Client | SZ | Management | No | Simple Network Management Protocol (SNMP) |
| 389 | TCP/UDP | LDAP Server | RAC | Management, Cluster, Control | Yes | SZ to LDAP |
| 443 | TCP | <ul style="list-style-type: none"> • AP • vSZ-D | vSZ control plane | Control | No | Access to the vSZ/SZ control plane over secure HTTPS |
| 443 | HTTPS | Controller | License server | Control | No | Cloud license server |
| 514 | TCP/UDP | | rsyslog | Management, Cluster, Control | No | Remote Syslog |
| 636 | TCP | LDAPS Server | RAC | Management, Cluster, Control | Yes | SZ to LDAPS Server |
| 546,547 | UDP | DHCP v6 Server | SZ | Control, Cluster, Management | No | DHCP v6 Protocol |
| 1812 | UDP | SZ-RAC | External AAA | Control, Cluster, Management | Yes | To Support Radius Proxy Authentication |
| 1813 | UDP | AP | RAC (Radius Access Controller) | Management, Cluster, Control | No | Radius_Auth profile defines both inbound and outbound traffic. lo specified here is for inbound traffic only. |
| 2083 (Radsec) | TCP | AAA server | SZ | Control, Cluster, Management | No | The default destination port number for RADIUS over TLS is TCP/2083 (As per RFC-6614) |

TABLE 100 Ports to open for AP-Controller Communication Table (continued)

| Port Number | Layer 4 Protocol | From (Sender) | To (Listener) | Interface | Configurable from Web Interface? | Purpose |
|-------------|------------------|-----------------------------------|-----------------------------|------------------------------|----------------------------------|--|
| 3268 | TCP | AD Server (MSTF-GC) | RAC | Management, Cluster, Control | Yes | SZ to AD (MSTF-GC) |
| 3799 | UDP | External AAA Server (free Radius) | SZ-RAC (vSZ control plane) | Control, Cluster, Management | 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. |
| 4443 | TCP | JITC CAC | SZ | Control | No | Since R5.1.2, mainly for JITC CAC login support. This port is opened for NGINX to configure for client cert authentication. |
| 5353 | UDP | AP | SZ | Control | No | Resolves hostnames to IP addresses |
| 6379,6380 | TCP | SZ | SZ | Cluster | No | Internal communication among SZ nodes |
| 7000 | TCP/UDP | SZ | SZ | Cluster | No | Cassandra (database) cluster communication and data replication |
| 7443 | TCP | Legacy Public API Client | SZ | Management | No | Deprecated Public API |
| 7500 | UDP | SZ | SZ | Cluster | No | SZ Clustering Operation |
| 7800 | TCP/UDP | SZ | SZ | Cluster | No | Cluster node communication for cluster's operations |
| 7801 | TCP | SZ | SZ | Cluster | No | A protocol stack using TCP on JGroups library for node to node communication on SZ |
| 7800-7805 | TCP | SZ | SZ | Cluster | No | A protocol stack using TCP on JGroups library for node to node communication |
| 7810 | TCP | SZ | SZ | Cluster | No | A protocol stack using FD_SOCKET on JGroups library for node to node communication |
| 7811 | TCP | SZ | SZ | Cluster | No | A protocol stack using FD_SOCKET on JGroups library for node to node communication |
| 7812 | TCP | SZ | SZ | Cluster | No | A protocol stack using FD_SOCKET on JGroups library for node to node communication |
| 8022 | No (SSH) | Any | Management interface | Management | 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 | Control | No | Allows unauthorized UEs to browse to an HTTP website |
| 8099 | TCP | Any | vSZ control plane | Control | No | Allows unauthorized UEs to browse to an HTTPS website |
| 8100 | TCP | Any | vSZ control plane | Control | No | Allows unauthorized UEs to browse using a proxy UE |

Ports to Open for AP-Controller Communication

TABLE 100 Ports to open for AP-Controller Communication Table (continued)

| Port Number | Layer 4 Protocol | From (Sender) | To (Listener) | Interface | Configurable from Web Interface? | Purpose |
|---------------|------------------|---|----------------------|------------------------------|----------------------------------|--|
| 8200 | TCP | <ul style="list-style-type: none"> • AP • DP | SZ | Control | No | Captive Portal OAuth service port for HTTP |
| 8222 | TCP | <ul style="list-style-type: none"> • AP • DP | SZ | Control | No | Captive Portal OAuth service port for HTTPS |
| 8280 | TCP | <ul style="list-style-type: none"> • AP • DP | SZ | Control | No | Captive Portal Web Proxy service port for HTTPS |
| 8443 | TCP | Any | vSZ management plane | Management | No | Access to the controller web interface via HTTPS |
| | | <p>NOTE The Public API port has changed from 7443 to 8443.</p> | | | | |
| 8883 | TCP | SZ | SPoT | Management, Cluster, Control | No | Communication between SZ and SPoT |
| 9080 | HTTP | Any | vSZ control plane | Management, Control | No | Northbound Portal Interface for hotspots |
| 9191 | TCP | AP-MD | SZ-MD | Cluster | No | Communication between AP-MD and SZ-MD |
| 9300-9400 | TCP | SZ | SZ | Cluster | No | Internal communication between nodes within the cluster (ElasticSearch database) |
| 9300 - 9311 | TCP | SZ | SZ | Cluster | No | Internal communication between nodes within the cluster (ElasticSearch database) |
| 9443 | HTTPS | Any | vSZ control plane | Management, Control | No | Northbound Portal Interface for hotspots. |
| 9997 | TCP | Client Device | SZ control Plane | Control | No | Internal Subscriber Portal in HTTP protocol |
| 9998 | TCP | Any | vSZ control plane | Control | No | Hotspot WISPr subscriber portal login/logout over HTTPS |
| 11211 | TCP | SZ Local Modules | SZ memproxy | Cluster | No | Internal proxy for saving in-memory data to memcached |
| 11311 | TCP | SZ | SZ | Cluster | No | Memory cache server |
| 12223 | UDP | AP | vSZ control plane | Control | No | LWAPP discovery, send image upgrade request to ZD-APs via LWAPP (rfc5412). |
| | | | | | | NOTE |
| 18301 | UDP | <ul style="list-style-type: none"> • AP • UE | SZ | Management, Cluster, Control | No | SpeedFlex tests the network performance between AP, UE, and SZ |
| 33434 - 33534 | UDP | SZ | SZ | Management, Cluster, Control | No | ICX Trouble Shooting (traceroute) |
| 65534, 65535 | TCP | SZ CS | DP | Management | No | DP Debug |

TABLE 100 Ports to open for AP-Controller Communication Table (continued)

| Port Number | Layer 4 Protocol | From (Sender) | To (Listener) | Interface | Configurable from Web Interface? | Purpose |
|-------------|------------------|---------------|---------------|-----------|----------------------------------|---------|
| | | | | | | |

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.

SoftGRE Support

- Overview of SoftGRE Support.....577
- Configuring And Monitoring AP Zones..... 579
- SoftGRE SNMP MIBs..... 580
- SoftGRE Events and Alarms..... 581

This appendix describes the SoftGRE support that the controller provides and the supported deployment topology.

Overview of SoftGRE Support

There are numerous equipment vendors serving the service provider market today. Among these vendors, the more prominent ones include Alcatel-Lucent (ALU), Ericsson, NSN, Huawei and Cisco. Most of these vendors support different tunneling and mobility management protocols at their packet gateways.

Since most (if not all) of these equipment vendors do not develop access points themselves, they are publishing SoftGRE specifications to enable access point vendors (such as Ruckus) to support SoftGRE on their devices.

Supported Deployment Scenario

The controller supports SoftGRE in the deployment scenario wherein the controller functions purely as an AP controller. In this deployment topology, the controller only manages the Ruckus APs and does not perform other functions. All control paths (RADIUS Authentication/Accounting) and data paths (SoftGRE tunnel) terminate on the third party WLAN gateway.

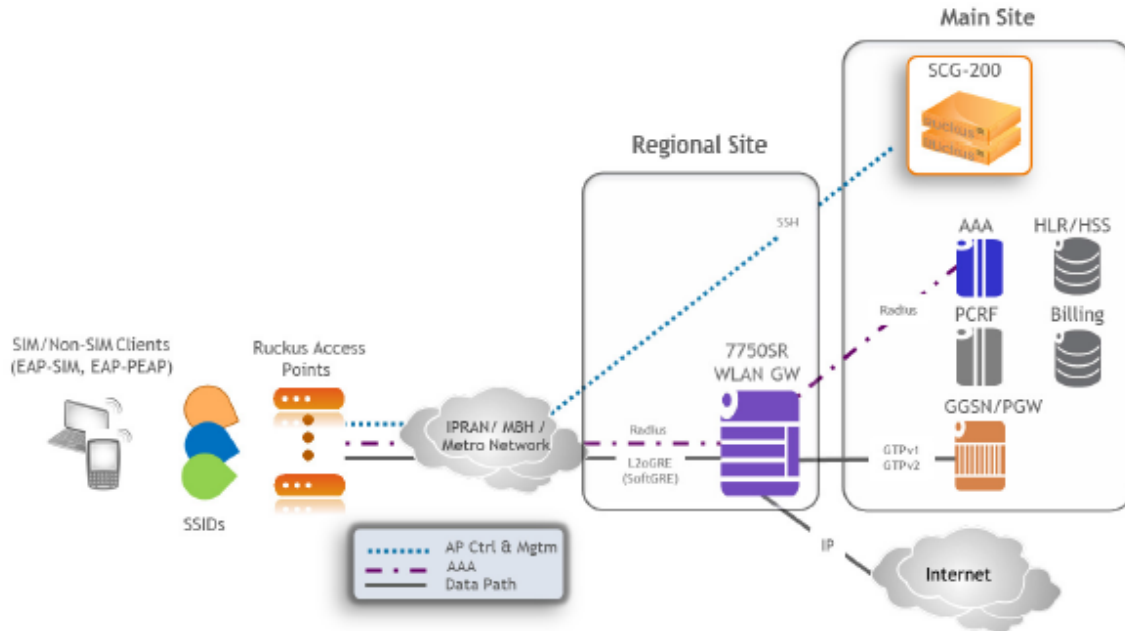
If 802.1x authentication is used, the RADIUS server will be outside of the SoftGRE tunnel. If open, WISPr-based authentication is used, the portal or redirect function will be on the edge router or northbound of the edge router. The controller does not play any role in the control and data path functions.

FIGURE 309 The controller as a pure AP controller

Direct AP to GW Tunnel Solution

Distributed WAG & Centralized WAC

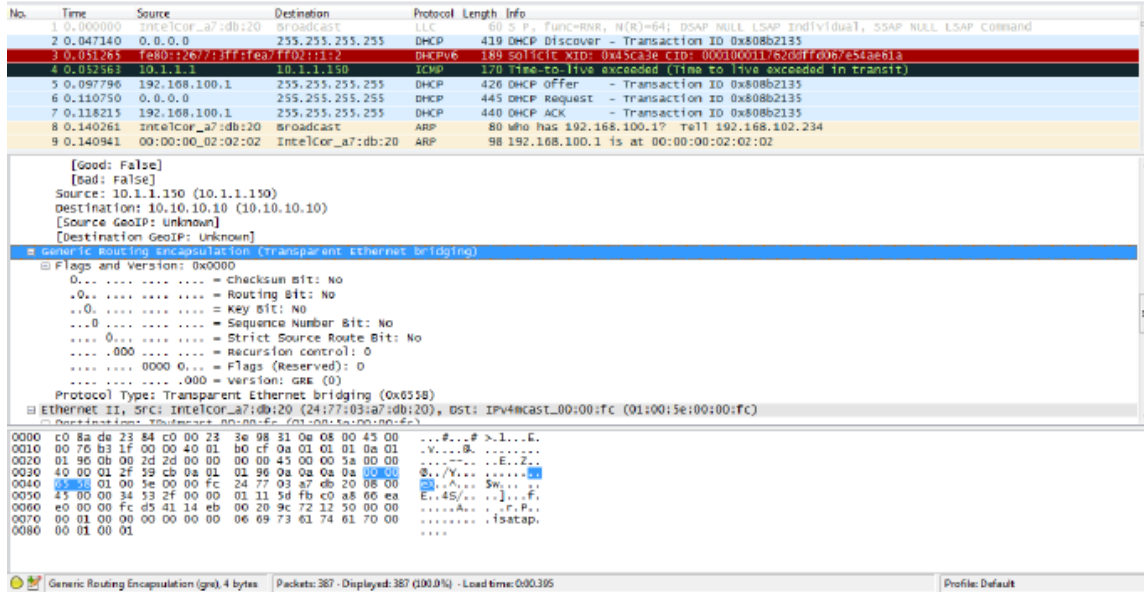
SCG-200 <-> AP Mgmt & 7750 <-> WAG Authentication & Data Plane AP



SoftGRE Packet Format

The following figure displays a screen shot of SoftGRE packet capture data.

FIGURE 310 Example of SoftGRE packet format



Configuring And Monitoring AP Zones

If no tunneled WLANs exist in the zone, you can change the tunnel type from SoftGRE to GRE or GRE + UDP.

MVNO accounts are currently unsupported by SoftGRE tunnels. If you create an MVNO account and assign an AP zone that is using a SoftGRE tunnel, an error message appears.

1. Follow the steps as described in [Monitoring WLAN Services](#) on page 105 to change the tunnel type from SoftGRE.
2. Scroll down to the **AP GRE Tunnel Option** section.
3. In **AP Tunnel Type**, select the tunnel type to which you want to change from SoftGRE.

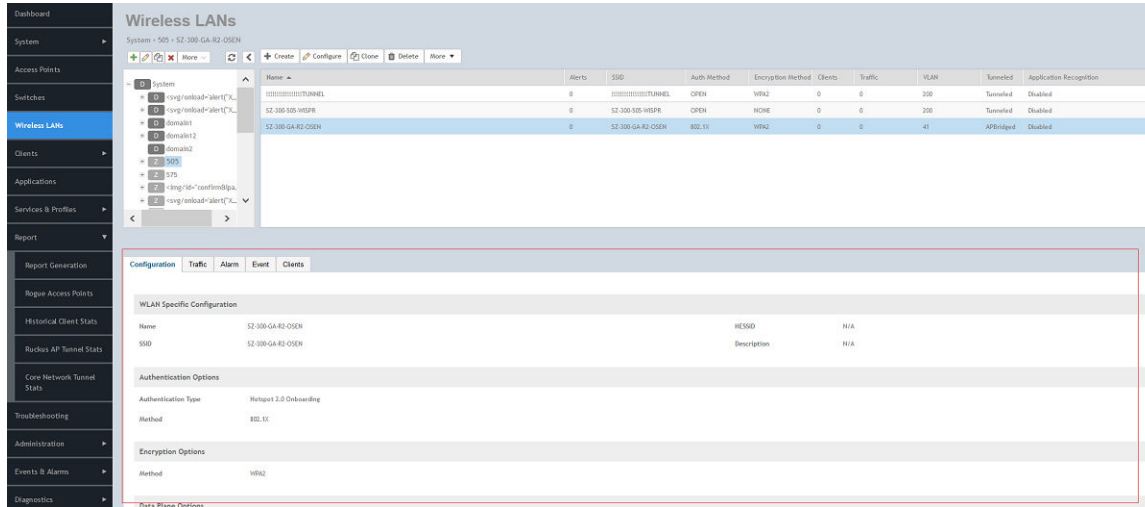
If you attempt to change the tunnel type when a tunneled WLAN exists within the zone, the following error message appears:

Unable to update the configuration of the AP zone. Reason: It is disallowed to change the tunnel type, because it has tunneled WLAN.

4. Click **OK**.

The zone configuration information is displayed.

FIGURE 311 Monitoring Zone Configuration



SoftGRE SNMP MIBs

The following table lists the SoftGRE OIDs.

TABLE 101 OIDs related to SoftGRE

| Parent Node | Node Name | OID |
|------------------|-------------------------------------|--------------------------------------|
| ruckusWLANAPInfo | ruckusSCGWLANAPMacAddr | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.1 |
| | ruckusSCGWLANAPSoftGREServer | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.2 |
| | ruckusSCGWLANAPSoftGREGWAddr | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.3 |
| | ruckusSCGWLANAPSoftGREActive | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.4 |
| | ruckusSCGWLANAPSoftGRETxBkts | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.5 |
| | ruckusSCGWLANAPSoftGRETxBkts | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.6 |
| | ruckusSCGWLANAPSoftGRERxPkts | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.7 |
| | ruckusSCGWLANAPSoftGRERxBytes | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.8 |
| | ruckusSCGWLANAPSoftGRETxBktsErr | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.9 |
| | ruckusSCGWLANAPSoftGRERxPktsErr | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.10 |
| | ruckusSCGWLANAPSoftGRETxBktsDropped | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.11 |
| | ruckusSCGWLANAPSoftGRERxPktsDropped | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.12 |
| | ruckusSCGWLANAPSoftGRETxBktsFrag | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.13 |
| | ruckusSCGWLANAPSoftGREICMPTotal | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.14 |
| | ruckusSCGWLANAPSoftGREICMPNoReply | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.15 |
| | ruckusSCGWLANAPSoftGREDisconnect | 1.3.6.1.4.1.25053.1.3.2.1.1.2.3.1.16 |

SoftGRE Events and Alarms

If there is no downstream traffic in the tunnel, APs that belong to the zone configured for SoftGRE send out-of-band ICMP keep-alive messages (interval is configurable) to the active third party WLAN gateway. If an AP does not receive a response from the active WLAN gateway, it triggers an alarm and it automatically creates a SoftGRE tunnel to the standby WLAN gateway.

If the AP does not receive a response from the standby WLAN gateway either, the AP disconnects all tunneled WLAN services. It continues to send keep-alive messages to both the active WLAN gateway (primary GRE remote peer) and standby WLAN gateway (secondary GRE remote peer). If it receives a response from either WLAN gateway, the AP restores all tunneled WLAN services automatically.

There are four types of events that APs send to the controller:

- Failover from primary GRE remote peer to secondary GRE remote peer
- Failover from secondary GRE remote peer to primary GRE remote peer.
- Tunnel disconnected because both primary and secondary GRE remote peers are unreachable
- Tunnel restored because either primary or secondary GRE remote peer is reachable

For the list of alarms and events related to SoftGRE that APs generate, refer to [SoftGRE Events](#) on page 581 and [SoftGRE Alarms](#) on page 582.

SoftGRE Events

SoftGRE related events that APs send to the controller.

Following are the events related to SoftGRE that AP generates.

apSoftGRE Tunnel Fail over PtoS AP [{apname@apMac}] fails over from primaryGRE [{address}] to secondaryGRE [{address}].

Code: 611

Severity:

Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "primaryGRE"="xxx.xxx.xxx.xxx"
- "secondaryGRE"="xxx.xxx.xxx.xxx"

apSoftGRE Tunnel Fail over StoP AP [{apname@apMac}] fails over from secondaryGRE [{address}] to primaryGRE [{address}].

Code: 612

Severity: Warning

Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "secondaryGRE"="xxx.xxx.xxx.xxx"
- "primaryGRE"="xxx.xxx.xxx.xxx"

apSoftGRE Gateway Reachable AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully.

Code: 613

Severity: Informational

Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "softgreGW"="primaryGRE"
- "softgreGWAddress"="xxx.xxx.xxx.xxx"

apSoftGRE Gateway Not Reachable AP [{apname@apMac}] is able to reach [{softgreGW}] [{softgreGWAddress}] successfully.

Code: 614

Severity: Critical

Attributes:

- apMac="xx:xx:xx:xx:xx:xx"
- "softGREGatewayList"="xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy"

SoftGRE Alarms

SoftGRE related alarms that APs send to the controller.

Following are the SoftGRE related alarms:

apSoftGRE Tunnel Fail AP[apname@apMac] fails over from primaryGRE[address] to secondaryGRE[address]

overPtoS

Code: 611

Default to Trap: true

Severity: major

Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "primaryGRE"="xxx.xxx.xxx.xxx"
- "secondaryGRE"="xxx.xxx.xxx.xxx"

apSoftGRE Tunnel Fail AP[apname@apMac] fails over from secondaryGRE[address] to primaryGRE[address]

overStoP

Code: 612

Default to Trap: true

Severity: major

Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "secondaryGRE"="xxx.xxx.xxx.xxx"
- "primaryGRE"="xxx.xxx.xxx.xxx"

apSoftGRE Gateway R AP [apname@apMac] is able to reach [softgreGW] [softgreGWAddress] successfully

eachable

Code: 613

Default to Trap: true

Severity: informational

Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "softgreGW"="primaryGRE"
- "softgreGWAddress"="xxx.xxx.xxx.xxx"

apSoftGRE Gateway N AP [apname@apMac] is unable to reach the following gateways: [gateway list]

otReachable

Code: 614

Default to Trap: true

Severity: major

Attributes:

- "apMac"="xx:xx:xx:xx:xx:xx"
- "softGREGatewayList"="xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy"

Replacing Hardware Components

- [Installing or Replacing Hard Disk Drives.....](#) 583

This appendix describes how to replace hardware components (including hard disk drives, power supply units, and system fans) on the controller.

Installing or Replacing Hard Disk Drives

You can install up to six hot-swappable SAS or SATA hard disk drives on the controller. The drives go into carriers that connect to the SAS/SATA backplane board once the carriers with drives attached are inserted back into the drive bays. The controller ships with six drive carriers.



CAUTION

If you install fewer than six hard disk drives, the unused drive bays must contain the empty carriers that ship with the server to maintain proper cooling.

Ordering a Replacement Hard Disk

To order a replacement hard disk for the controller, contact your Ruckus sales representative and place an order for FRU part number 902-0188-0000 (Hard Drive, 600GB, 10K RPM, 64MB Cache 2.5 SAS 6Gb/s, Internal).



CAUTION

Use only FRU part number 902-0188-0000 as replacement hard disk for the controller. Using other unsupported hard disks will render the controller hardware warranty void.

Removing the Front Bezel

You must remove the front bezel to add or replace a hard drive in one of the drive bays. It is not necessary to remove the front chassis cover or to power down the system. The hard drives are hot-swappable.

Follow these steps to remove the front bezel of the controller.

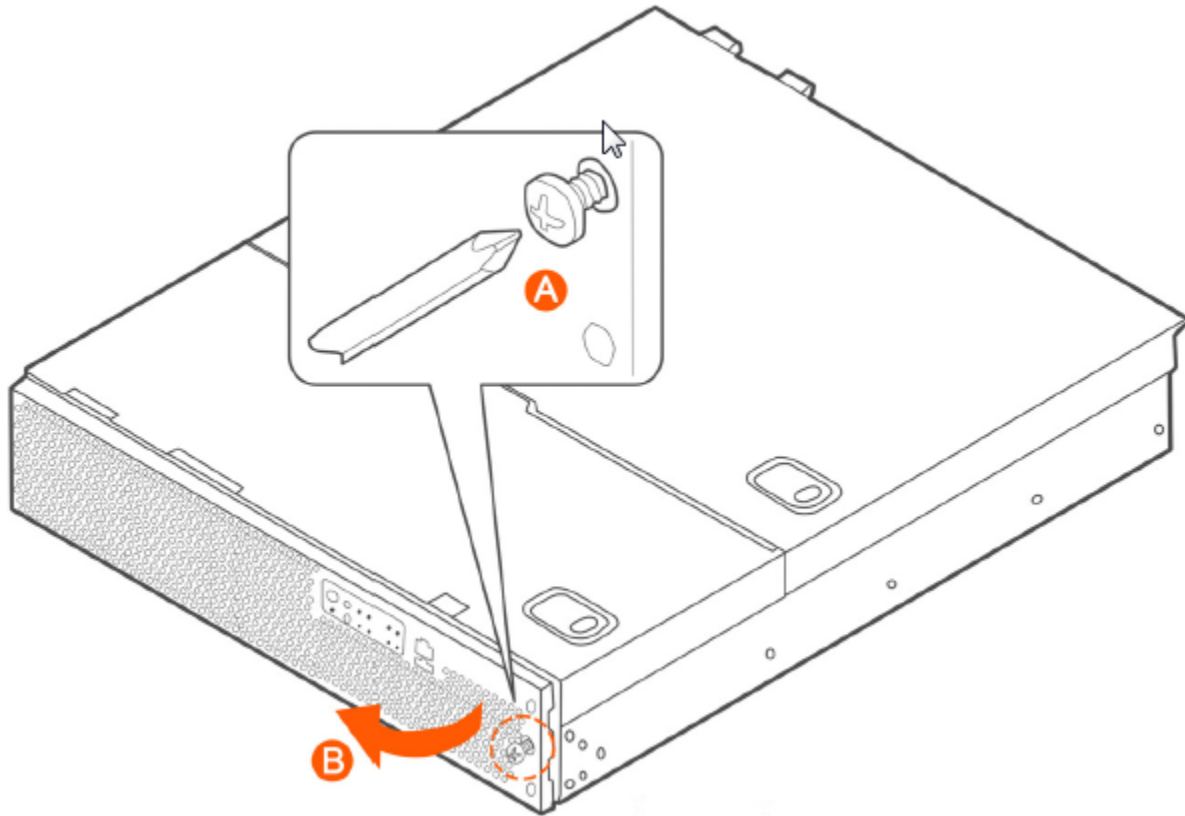
You need to remove the front bezel for tasks such as:

- Installing or removing hard disk drives or an SD flash card
- Observing the individual hard disk drive activity/fault indicators
- Replacing the control panel LED/switch board

The server does not have to be powered down just to remove the front bezel.

1. Loosen the captive bezel retention screw on the right side of the bezel (see A in [Figure 312](#)).
2. Rotate the bezel to the left to free it from the pins on the front panel (see B in [Figure 312](#)), and then remove it.

FIGURE 312 Removing the front bezel



Removing an HDD Carrier from the Chassis

Follow these steps to remove a hard disk drive carrier from the chassis.

1. Remove the front bezel (see [Removing the Front Bezel](#) on page 583).

2. Select the drive bay where you want to install or replace the drive.

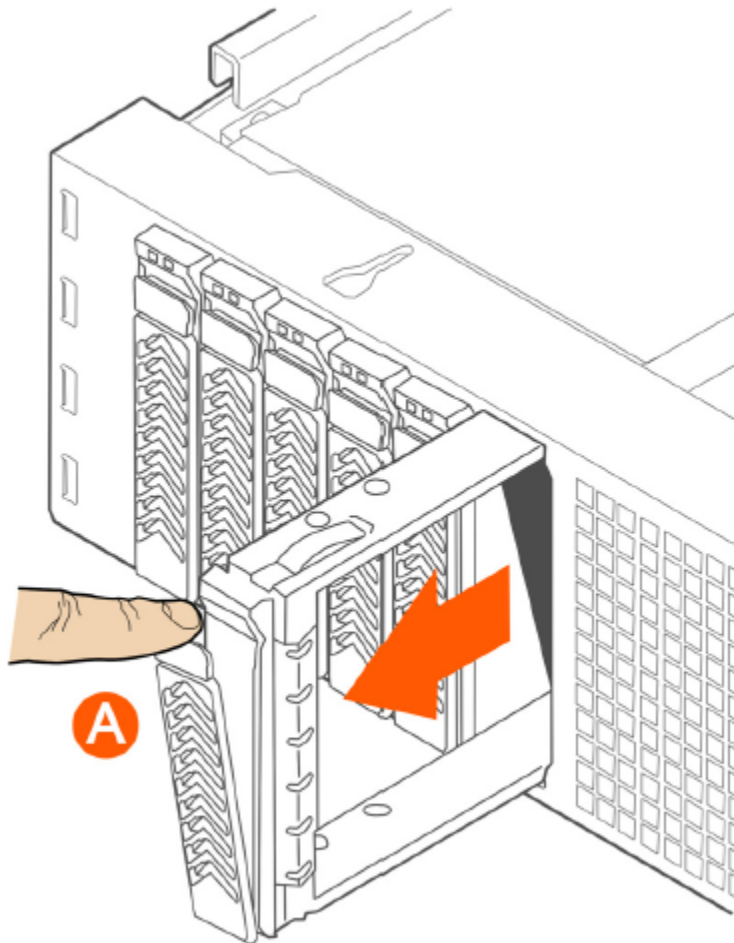
Drive bay 0 must be used first, then drive bay 1 and so on. The drive bay numbers are printed on the front panel below the drive bays.

3. Remove the drive carrier by pressing the green button to open the lever.

(See A in [Figure 313](#)).

4. Pull the drive carrier out of the chassis.

FIGURE 313 Removing the drive carrier



Installing a Hard Drive in a Carrier

Follow these steps to install a hard drive in a drive carrier.

1. If a drive is already installed (that is, if you are replacing the drive), remove it by unfastening the four screws that attach the drive to the drive carrier (see A in [Figure 314](#)). Set the screws aside for use with the new drive.

2. Lift the drive out of the carrier (see B in [Figure 314](#)).

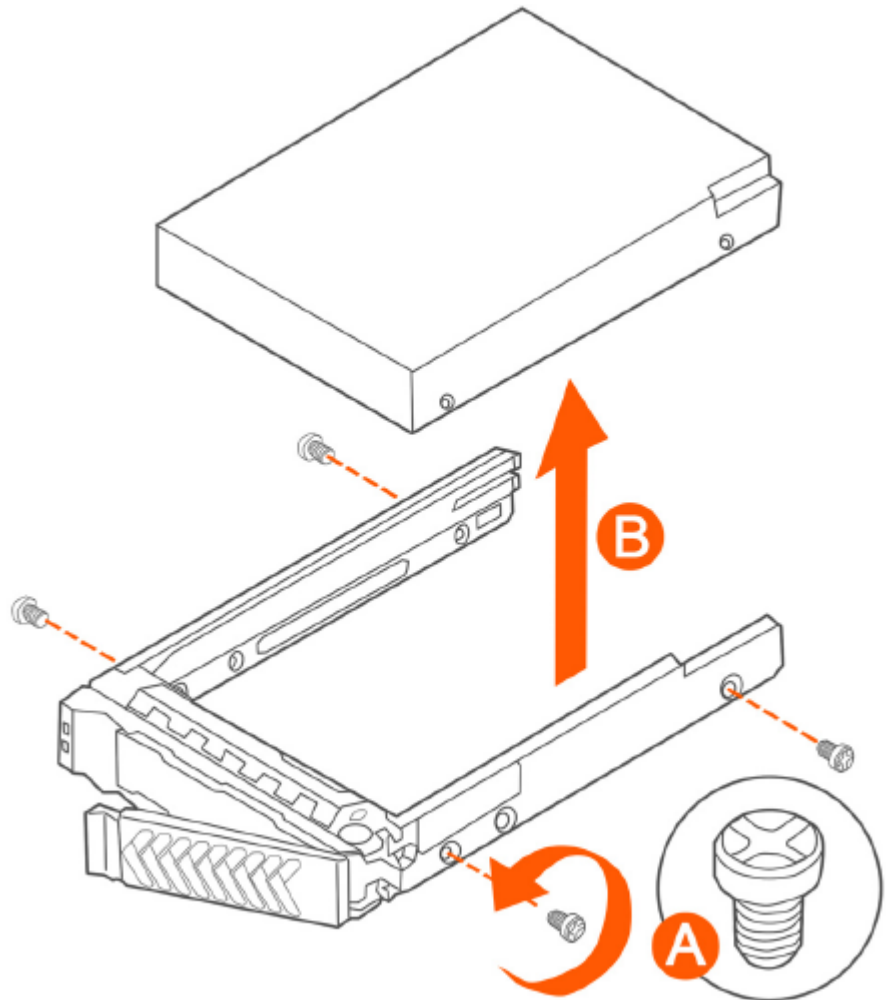


FIGURE 314 Removing the hard drive

3. Install the new drive in the drive carrier (see A in Figure 315), and then secure the drive with the four screws that come with the carrier (see B).

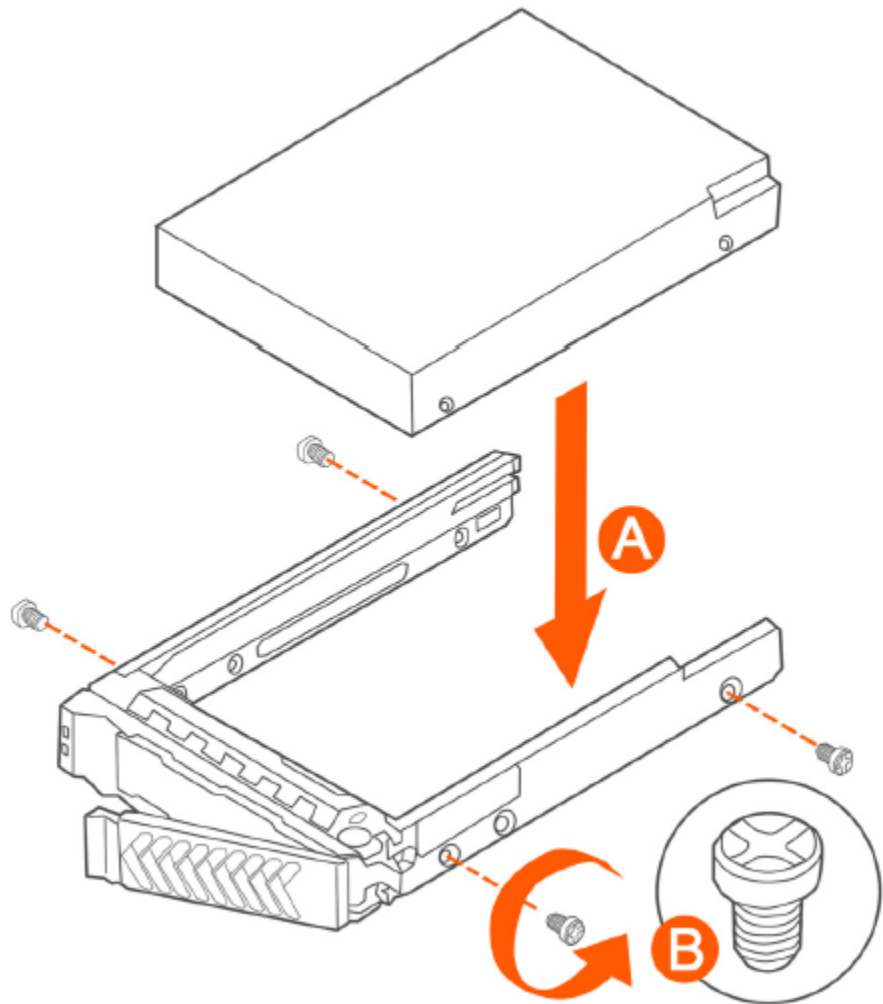


FIGURE 315 Installing the hard drive

4. With the drive carrier locking lever fully open, push the hard drive carrier into the drive bay in the chassis until it stops (see A in [Figure 316](#)).

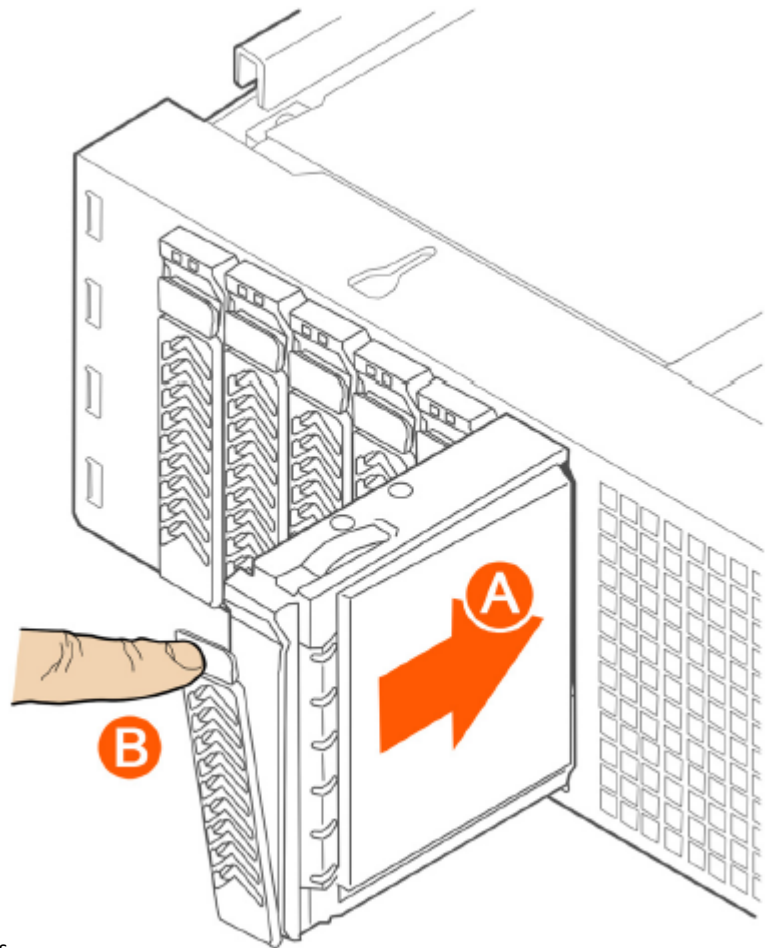


FIGURE 316 Inserting the carrier back into the chassis

5. Press the locking lever until it snaps shut and secures the drive in the bay.

You have completed installing or replacing the hard drive onto the controller.

NOTE

The new hard drive will synchronize automatically with the existing RAID array. During the synchronization process, the HDD LED on the controller will blink amber and green alternately. When the process is complete, the HDD LED will turn off.

Reinstalling the Front Bezel

Follow these steps to reinstall the front bezel on the controller.

1. Insert the tabs on the left side of the bezel into the slots on the front panel of the chassis.
2. Move the bezel toward the right of the front panel and align it on the front panel pins.
3. Snap the bezel into place and tighten the retention screw to secure it.

Replacing PSUs

The controller includes two redundant, hot-swappable power supply units (2 AC PSUs or 2 DC PSUs). No chassis components need to be removed to add or replace a PSU.

Follow these steps to remove and replace a PSU.

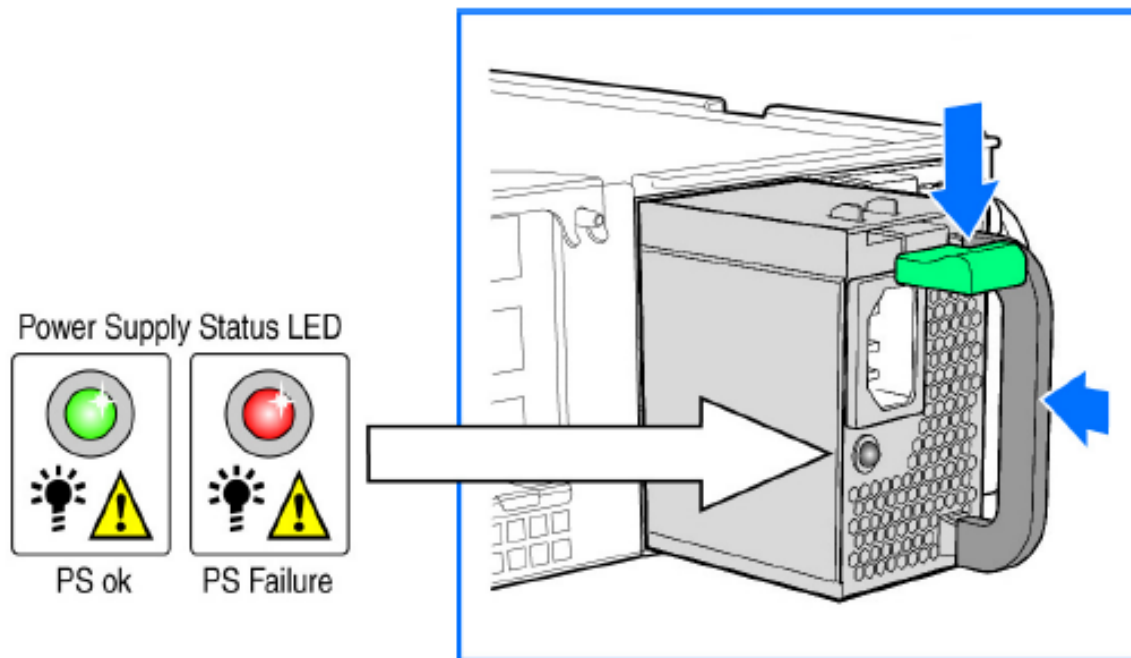
1. Identify the faulty PSU by looking at the PSU status LED (red indicates PSU failure, green indicates normal operation).
2. Press and hold the green safety lock downward while grasping the PSU handle.
3. Pull outward on the handle, sliding the PSU all the way out of the rear of the machine.
4. Insert the new PSU into the slot and, while holding the green safety lock, slide the PSU into the slot until it locks in place.

The PSU status LED turns green, indicating that the PSU is operating normally.

NOTE

If you are installing a DC power supply, there are two threaded studs for chassis enclosure grounding. A 90° standard barrel, two-hole, compression terminal lug with 5/8-inch pitch suitable for a #14-10 AWG conductor must be used for proper safety grounding. A crimping tool may be needed to secure the terminal lug to the grounding cable.

FIGURE 317 Replacing a PSU



Replacing System Fans

The controller includes six redundant, hot-swappable system fans (four 80mm fans and two 60mm fans). There are also two fans located inside the power supply units. Redundancy for the two PSU fans is only achieved when both PSUs are installed.

If any of the system fans requires replacement, the replacement procedure is identical.

Electrostatic discharge (ESD) can damage internal components such as printed circuit boards and other parts. Ruckus recommends that you only perform this procedure with adequate ESD protection. At a minimum, wear an anti-static wrist strap attached to the ESD ground strap attachment on the front panel of the chassis.

Replacing Hardware Components

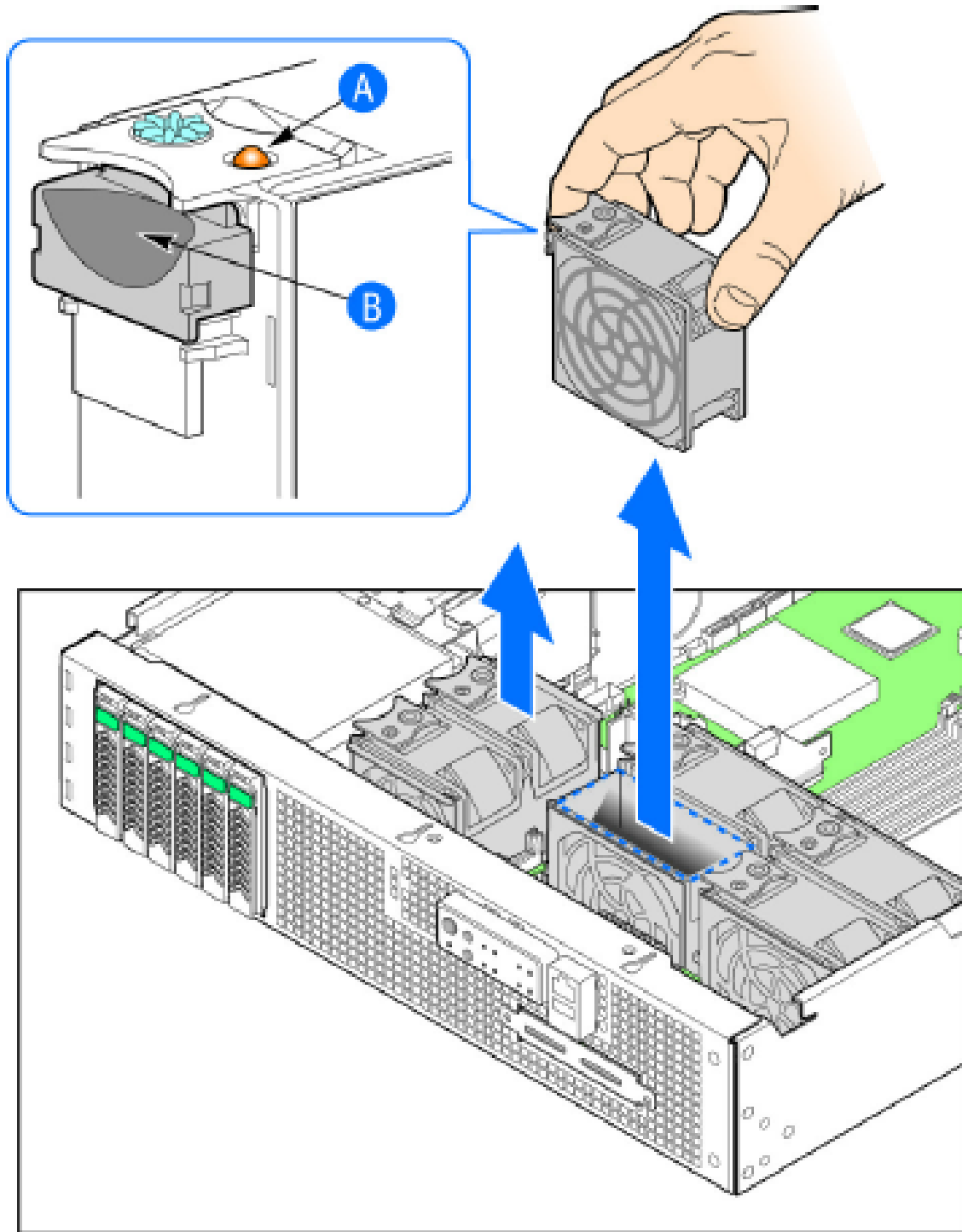
Installing or Replacing Hard Disk Drives

Follow these steps to replace a system fan.

1. Open the front chassis cover of the controller. It may be necessary to extend the controller into a maintenance position.
2. Identify the faulty fan. Each fan has a "service required" LED that turns amber when the fan is malfunctioning.
3. Remove the faulty fan by grasping both sides of the fan assembly, using the plastic finger guard on the left side and pulling the fan out of the metal fan enclosure.
4. Slide the replacement fan into the same metal fan enclosure. Use the edges of the metal enclosure to align the fan properly and ensure the power connector is seated properly in the header on the side of the enclosure.
5. Apply firm pressure to fully seat the fan.
6. Verify that the (service required) LED on the top of the fan is not lit.

7. Close the front chassis cover and return the controller to its normal position in the rack, if necessary.

FIGURE 318 Replacing a system fan



vSZ-H SSID Syntax

- [SSIDs Supported in Release 1.1.x](#)..... 593
- [SSIDs Supported in Release 2.1.x](#)..... 593
- [SSIDs Supported in Release 2.5.x](#)..... 594
- [SSIDs Supported in Release 3.0 and Above](#)..... 594
- [ZoneDirector SSID Syntax](#)..... 595
- [ZoneFlex AP SSID Syntax](#)..... 596

The following sections describe the supported SSID syntax in the following vSZ-H release versions:

SSIDs Supported in Release 1.1.x

Release 1.1.x supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

The following table describes the SSID syntaxes that are supported in release 1.1.x.

TABLE 102 Supported SSID syntaxes in 1.1.x

| | | |
|---------------|----------------------|---|
| Web Interface | Length | Between 1 and 32 characters, including characters from printable characters (ASCII characters space (32) to ~ (126)) |
| | Supported Characters | <ul style="list-style-type: none"> • A-Z • a-z • 0-9 • _space_!#\$%&'()*+,-./ • ;<=?@ • [\]^_` • {} |
| CLI | Length | Unsupported |
| | Supported Characters | Unsupported |

SSIDs Supported in Release 2.1.x

Release 2.1.x supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

The following table describes the SSID syntaxes that are supported in release 2.1.x.

TABLE 103 Supported SSID syntaxes in 2.1.x

| | | |
|---------------|----------------------|---|
| Web Interface | Length | Between 1 and 32 characters, including characters from printable characters (ASCII characters space (32) to ~(126)) |
| | Supported Characters | <ul style="list-style-type: none"> • A-Z • a-z • 0-9 • _space_!#\$%&'()*+,-./ • ;<=?@ • [\]^_` • {} |

TABLE 103 Supported SSID syntaxes in 2.1.x (continued)

| | | |
|-----|----------------------|---|
| CLI | Length | Between 2 and 32 characters |
| | Supported Characters | All characters, but the space character cannot be the first or last character in the SSID |

SSIDs Supported in Release 2.5.x

Release 2.5.x supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

The following table describes the SSID syntaxes that are supported in release 2.5.x.

TABLE 104 Supported SSID syntax in 2.5.x

| | | |
|---------------|----------------------|--|
| Web Interface | Length | Between 1 and 32 characters, including characters from printable characters (ASCII characters space (32) to ~ (126)) |
| | Supported Characters | <ul style="list-style-type: none"> • A-Z • a-z • 0-9 • _space_!"#\$%&'()*+,-./ • ;<=?@ • [\]^_` • {} |
| CLI | Length | Between 2 and 32 characters |
| | Supported Characters | All characters |

SSIDs Supported in Release 3.0 and Above

Release 3.0 and above supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

The following table describes the SSID syntaxes that are supported in release 3.0 and above.

TABLE 105 Supported SSID syntax in 3.0 and above

| | | |
|-----------------------|------------|---|
| Web Interface and CLI | Length | Between 2 to 32 characters are supported |
| | Characters | <p>Unsupported: ` and \$(Space is allowed, but it must include at least one non-space character (" abc" is valid, however only space such as " " is invalid).</p> <p>NOTE One Chinese word is regarded as three special characters.</p> |

ZoneDirector SSID Syntax

The following sections describe the supported SSID syntax in the following vSZ-H release version:

SSIDs Supported in Releases 9.8 and 9.7

ZoneFlex releases 9.8 and 9.7 support a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

TABLE 106 Supported SSID syntaxes in ZoneFlex 9.8 and 9.7

| | | |
|---------------|----------------------|--|
| Web Interface | Length | Between one and 32 characters |
| | Supported Characters | All printable ASCII characters from space (32) to ~(126) |
| | Exceptions | The space character (32) cannot be the first or last character in the SSID. Otherwise, the following error message appears: can only contain between 1 and 32 characters, including characters from ! (char 33) to ~ (char 126) . |
| CLI | Length | Between one and 32 characters |
| | Supported Characters | All printable ASCII characters from space (32) to ~(126) |
| | Exceptions | The space character (32) can be placed anywhere in the SSID (including the beginning or end) provided that it enclosed by a double quotation mark. |

Supported SSIDs in ZoneFlex Release 9.6

ZoneFlex release 9.6 supports a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

TABLE 107 Supported SSID syntaxes in ZoneFlex 9.6

| | | |
|---------------|----------------------|--|
| Web Interface | Length | Between two and 32 characters |
| | Supported Characters | All printable ASCII characters from space (32) to ~(126) |
| | Exceptions | The space character (32) cannot be the first or last character in the SSID. Otherwise, the following error message appears: can only contain between 1 and 32 characters, including characters from ! (char 33) to ~ (char 126) . |
| CLI | Length | Between two and 32 characters |
| | Supported Characters | All printable ASCII characters from space (32) to ~ (126) |
| | Exceptions | The space character (32) can be placed anywhere in the SSID (including the beginning or end) provided that it enclosed in a double quotation mark (for example, "Ruckus SSID"). |

ZoneFlex AP SSID Syntax

The following sections describe the supported SSID syntax in the following ZoneFlex AP release versions:

Supported SSIDs in Releases 9.8, 9.7, and 9.6

ZoneFlex release 9.8, 9.7, and 9.6 support a specific set of SSID syntaxes, which may be different from the syntaxes supported in other releases.

TABLE 108 Supported SSID syntaxes in ZoneFlex AP 9.8, 9.7, and 9.6

| | | |
|---------------|----------------------|--|
| Web Interface | Length | Between one and 32 characters |
| | Supported Characters | All printable ASCII characters from space (32) to ~ (126) |
| CLI | Length | Between one and 32 characters |
| | Supported Characters | All printable ASCII characters from space (32) to ~ (126) |
| | Exceptions | The space character (32) can be placed anywhere in the SSID (including the beginning or end) provided that it is enclosed in a double quotation mark (for example, "Ruckus SSID"). If the space character is not enclosed in a double quotation mark, the space character and any characters after that will be ignored. For example, if you run the command " set ssid wlan0 ruckus-ap 123 ", the controller CLI will run the command as " set ssid wlan0 ruckus-ap 123 ". |

Web Server Support

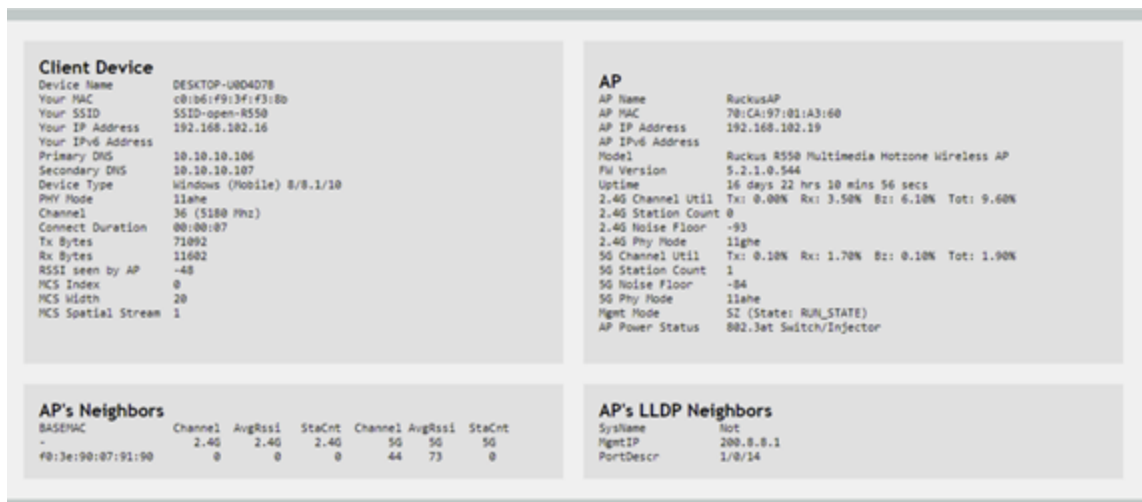
The <https://my.ruckus> web page is a supplementary tool for reporting a problem without much understanding of the infrastructure.

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 319 Viewing Diagnostic Information in WPA2 WLAN



On entering <https://my.ruckus> when connected over an Open or WEP WLAN, the diagnostic information is restricted for security reasons.

FIGURE 320 Viewing Diagnostic Information in Open WLAN

| Client Device | | | | | | |
|--------------------|---------------------------|--|--|--|--|--|
| Device Name | DESKTOP-U0D4D7B | | | | | |
| Your MAC | c0:b6:f9:3f:f3:8b | | | | | |
| Your SSID | SSID-open-R550 | | | | | |
| Your IP Address | 192.168.102.16 | | | | | |
| Your IPv6 Address | | | | | | |
| Primary DNS | 10.10.10.106 | | | | | |
| Secondary DNS | 10.10.10.107 | | | | | |
| Device Type | Windows (Mobile) 8/8.1/10 | | | | | |
| PHY Mode | 11ahe | | | | | |
| Channel | 36 (5180 Mhz) | | | | | |
| Connect Duration | 00:00:07 | | | | | |
| Tx Bytes | 71092 | | | | | |
| Rx Bytes | 11602 | | | | | |
| RSSI seen by AP | -48 | | | | | |
| MCS Index | 0 | | | | | |
| MCS Width | 20 | | | | | |
| MCS Spatial Stream | 1 | | | | | |

| AP | | | | | | |
|--------------------|--|--|--|--|--|--|
| AP Name | RuckusAP | | | | | |
| AP MAC | 70:CA:97:01:A3:60 | | | | | |
| AP IP Address | 192.168.102.19 | | | | | |
| AP IPv6 Address | | | | | | |
| Model | Ruckus R550 Multimedia Hotzone Wireless AP | | | | | |
| FW Version | 5.2.1.0.544 | | | | | |
| Uptime | 16 days 22 hrs 10 mins 56 secs | | | | | |
| 2.4G Channel Util | Tx: 0.00% Rx: 3.50% Bz: 6.10% Tot: 9.60% | | | | | |
| 2.4G Station Count | 0 | | | | | |
| 2.4G Noise Floor | -93 | | | | | |
| 2.4G Phy Mode | 11ghe | | | | | |
| 5G Channel Util | Tx: 0.10% Rx: 1.70% Bz: 0.10% Tot: 1.90% | | | | | |
| 5G Station Count | 1 | | | | | |
| 5G Noise Floor | -84 | | | | | |
| 5G Phy Mode | 11ahe | | | | | |
| 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 |
| F0:3e:90:07:91:90 | 0 | 0 | 0 | 44 | 73 | 0 |

| AP's LLDP Neighbors | |
|---------------------|-----------|
| SysName | Not |
| MgmtIP | 200.8.8.1 |
| PortDescr | 1/0/14 |

Appendix

- Copyright..... 599

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.

