VIEW Certified Configuration Guide

Ruckus® Wireless

ZoneDirector 1100, 3000, 5000
with ZoneFlex™ 7363, 7982

1725-86983-000 Rev: B
May 2013

Copyright Notice

© 2012-2013 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink's products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

Contact Information

US Location
800-775-5330

Spectralink Corporation
1765 W. 121st Avenue
Westminster, CO 80234

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Langmarksvej 34
8700 Horsens

infodk@spectralink.com

Contents

Chapter 1: Introduction 4

Certified Product Summary 4
Known Limitations 5
Spectralink References 5
Product Support 6

Chapter 2: Overview 7

Network Topology 7

Chapter 3: Getting Started 8

Out of the Box Configuration of ZoneDirector 8
Connecting with the ZD through the Browser 8
Software Upgrade 9
View/Configure System Settings 10

Chapter 4: General Settings 11

RADIUS Server Definition 11
Configure Background Scanning 12
Configure Admission Control 12
QoS Configuration 13

Chapter 5: WLAN Configuration 17

Configure Security Settings 17
Security: Open 17
Security: WPA-PSK 18
Security: WPA2-PSK 19
Security: WPA2-Enterprise 20
Advanced Options on the WLAN 21
WLAN Settings from the CLI 23

Chapter 6: AP Configuration 24

AP Group Setup 24
Individual AP Configuration 25

Chapter 1: Introduction

Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between Spectralink Wireless Telephones and wireless LAN (WLAN) infrastructure products.

The products listed below have been thoroughly tested in Spectralink's lab and have passed VIEW Certification. This document details how to configure Ruckus controllers ZD 1100/3000/5000 and Ruckus Access Points ZF 7363/7982 with Spectralink Wireless Telephones.

Certified Product Summary

Manufacturer:	Ruckus Wireless; www.ruckuswireless.com			
Certified products:	Controllers: ZD1100 ZD3000 ZD5000	APs: ZF 7363 ZF 7982		
AP radio:	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n)			
Security :	None, WEP, WPA-PSK, WPA2-PSK, and WPA2-Enterprise (EAP-FAST and PEAPv0/MSCHAPv2) with OKC			
QoS:	Wi-Fi Standard for Spectralink 8440/8441 and 8450/8452/8453 and 8020/8030			
AP and ZD software version tested:	9.5.0.99.124			
Network topology:	Switched Ethernet (recommended)			
Handset models tested:	Spectralink 8440/8441 and 8450/8452/8453 Wireless Telephone			
Handset radio mode:	802.11b	802.11b/g	802.11b/g/n	802.11 a & a/n
Meets VIEW minimum call capacity per AP:	8 calls	8 calls	8 calls	10 calls
Handset* models tested:	Spectralink 8020/8030*** Spectralink 8440/8441 and 8450/8452/8453			
Handset radio mode:	802.11b/g		802.11a/n	
Meets VIEW minimum call capacity per AP:**	8 with Wi-Fi Std QoS		8 with Wi-Fi Std QoS	

*****Spectralink handset models and their OEM derivatives are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as "Spectralink Wireless Telephones", "phones" or "handsets".

** Maximum calls tested per the VIEW Certification Test Plan. The certified product may actually support a higher number of maximum calls

***WPA2-Enterprise and Wi-Fi Standard QoS are not available for Spectralink 8020/8030 handsets connecting to PBXs using the TDM protocol through a Spectralink Telephony Gateway (phone type 30 on the 8020/8030).

Known Limitations

- Background scanning must have a time setting for seamless roaming. This means that ChannelFly should be disabled with Spectralink. When settings are changed on an AP, the AP should be power cycled so that the neighbor lists are updated. In addition, all handsets associated with the AP at any time in the last 24 hours should be power cycled no sooner than 10 minutes after the AP is power cycled.
- 40 MHz paired channels are not recommended on the 2.4 GHz radio.
- 8020/8030 handsets are not compatible with the N-Only AP mode. 8400 series handsets may be used with the N-Only AP mode.

Spectralink References

All documents are available at http://support.spectralink.com. Use the Documents and Downloads pane and select Voice as the Product Type and then for Product select Spectralink 8400 Series Wireless Telephone from the dropdown list. For other documents, use the navigation pane on the left to locate the product and open the page.

For the Spectralink 8020/8030 Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 8020/8030 Wireless Telephones.* This white paper covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

For the Spectralink 8400 Series Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 8400 Series Wireless Telephones* for detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets.

These two white papers identify issues and solutions based on Spectralink's extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with Spectralink Wireless Telephones.

The *Spectralink 8400 Series Wireless Telephone Administration Guide* provides a comprehensive list of every parameter available on Spectralink 8400 Series Wireless Telephones.

The *Spectralink 8400 Series Deployment Guide* is your essential reference for provisioning and deploying Spectralink 8400 handsets in any environment.

The *Web Configuration Utility User Guide* explains how to use a web browser to configure the Spectralink 8400 Series handsets on a per handset basis.

The *Spectralink 8020/8030 Wireless Telephone Handset Administration Tool* document explains how to use a software interface to configure the handsets.

Product Support

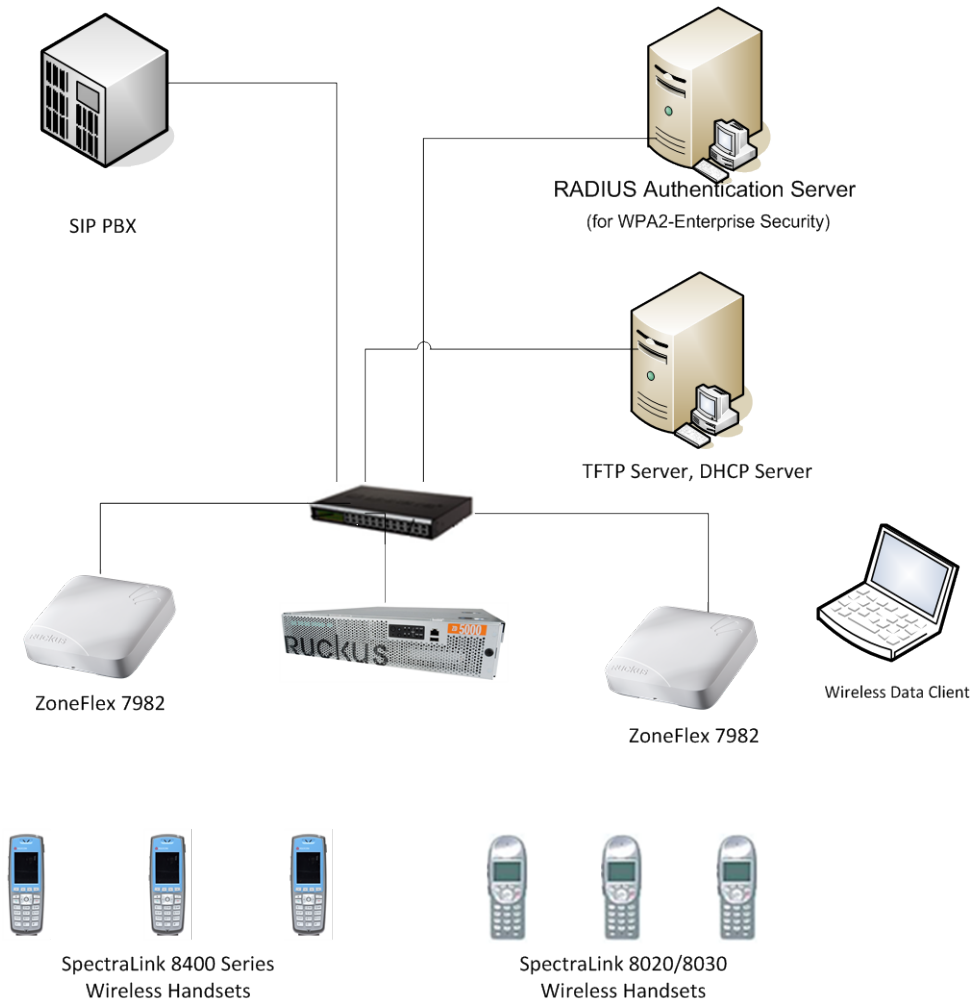
If you encounter difficulties or have questions regarding the configuration process, please contact Ruckus Wireless at support@ruckuswireless.com or Spectralink at support.spectralink.com.

Chapter 2: Overview

Spectralink 8020/8030 handsets can be configured with Wi-Fi Standard QoS. On the Admin menu navigate to **Network Config > WLAN settings > Custom > QoS >** .

Spectralink 8400 handsets only support Wi-Fi Standard QoS. Refer to the *Spectralink 8400 Series Deployment Guide* for complete information on how to provision the handsets.

Network Topology



Note: Example configuration shown

This configuration is not applicable to all customer environments.

Chapter 3: Getting Started

Out of the Box Configuration of ZoneDirector

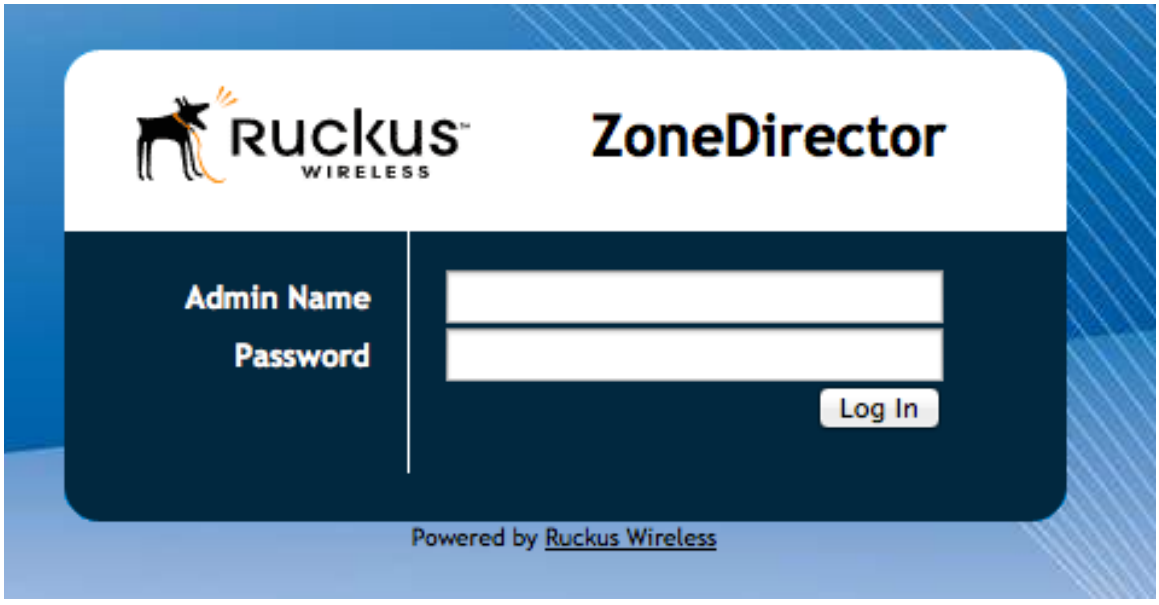
When Ruckus Wireless gear is unpacked, the first piece of equipment that needs to be configured is the ZoneDirector. The goal of the initial setup is to give the ZoneDirector a name and to assign an IP address or tell it to use DHCP. Upon completion of the initial setup, the ZoneDirector can be managed from any computer on the network by browsing to the device's IP address.

1. Unpack and plug in the ZoneDirector.
2. Cable the ZD to the Ethernet.
3. Using a PC on the same LAN, open a browser and connect to the ZD using IP address 192.168.0.2 (default IP address of the Zone Director).
4. Run the ZD's setup wizard.

Connecting with the ZD through the Browser

After initial configuration, browse to the ZD by entering its IP address into the browser.

You will be prompted for user credentials:



The default Admin name is **admin**.

The default Password is **admin**.

Tthe dashboard screen appears. Use the menu bar at the top of the screen to navigate to the three options: Monitor, Configure and Administer.

Software Upgrade

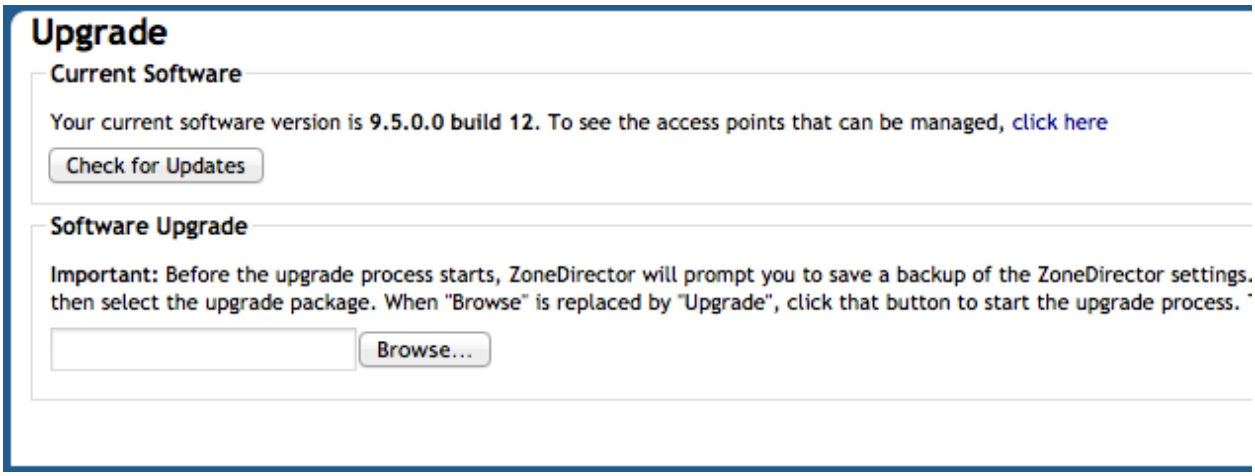
Perform the software upgrade in the following order:

1. Versions earlier than 9.1.2.x.x, first upgrade to 9.1.2.0.8
2. Upgrade to 9.3.2.0.3
3. Upgrade to 9.4.0.0.110
4. Upgrade to 9.5.0.99.124.

Web: Upgrade path support

Contact support@ruckuswireless.com if the software version of the AP/ZD is other than the ones listed above.

To upgrade, go to **Administer > Upgrade > Software Upgrade.**



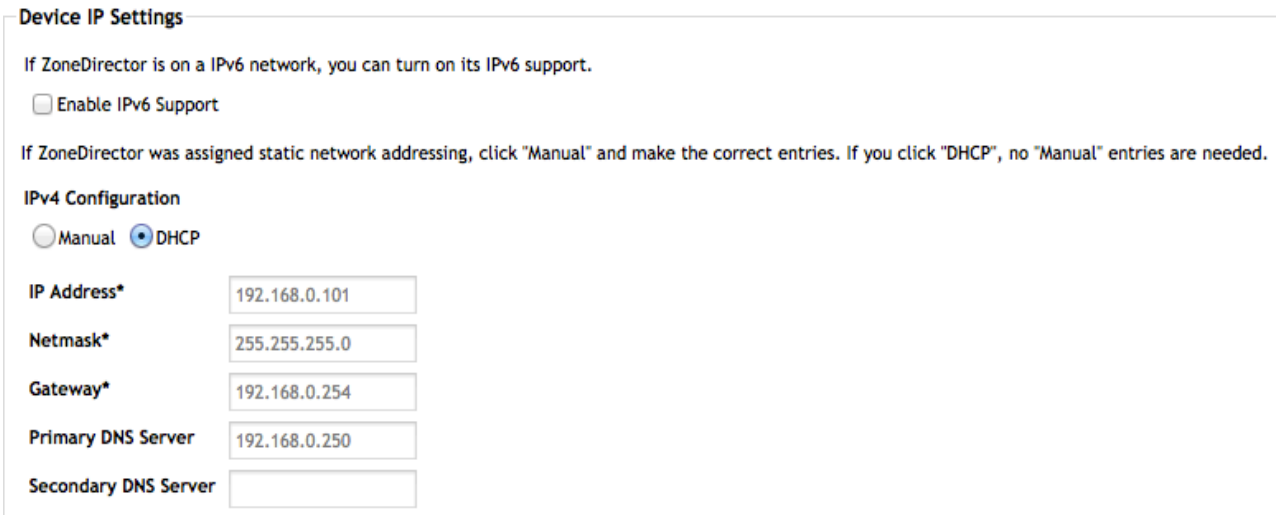
The upgrade procedure starts with backing up your current configuration.

Browse to the location where you will save your backup files.

Follow the prompts to save the current configuration and then click **Upgrade** to start the upgrade procedure.

View/Configure System Settings

Navigate to **Configure > System**. System is where basic information about the ZD can be entered.

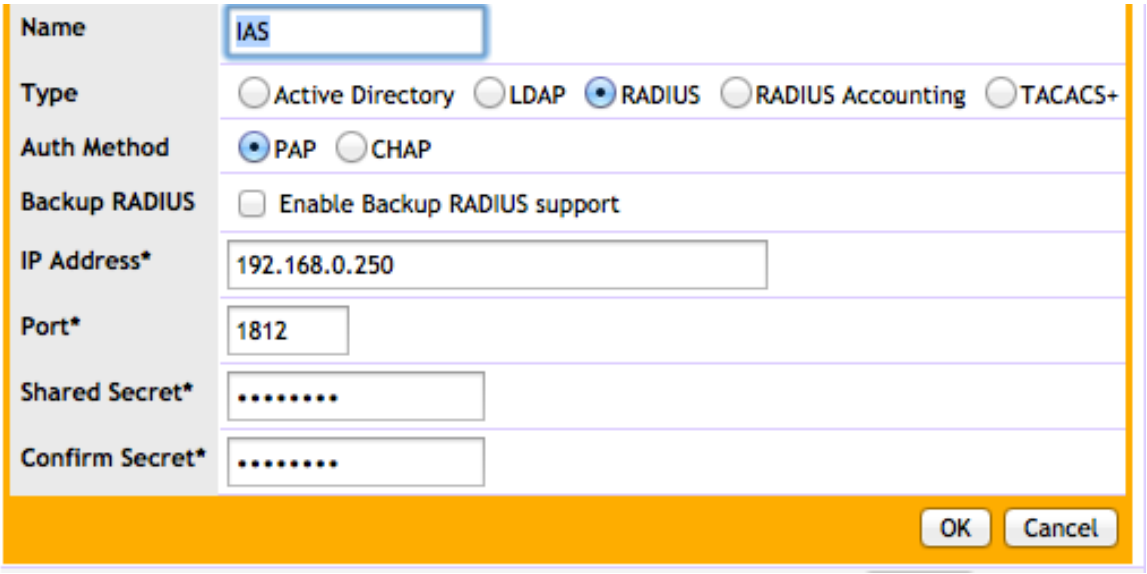


Chapter 4: General Settings

RADIUS Server Definition

Configuring a WLAN with WPA2-Enterprise scheme requires configuration of a RADIUS server. How to setup and configure an external radius server is not discussed in this document. However, configure a radius server details within ZD so that ZD can communication with external server as follows

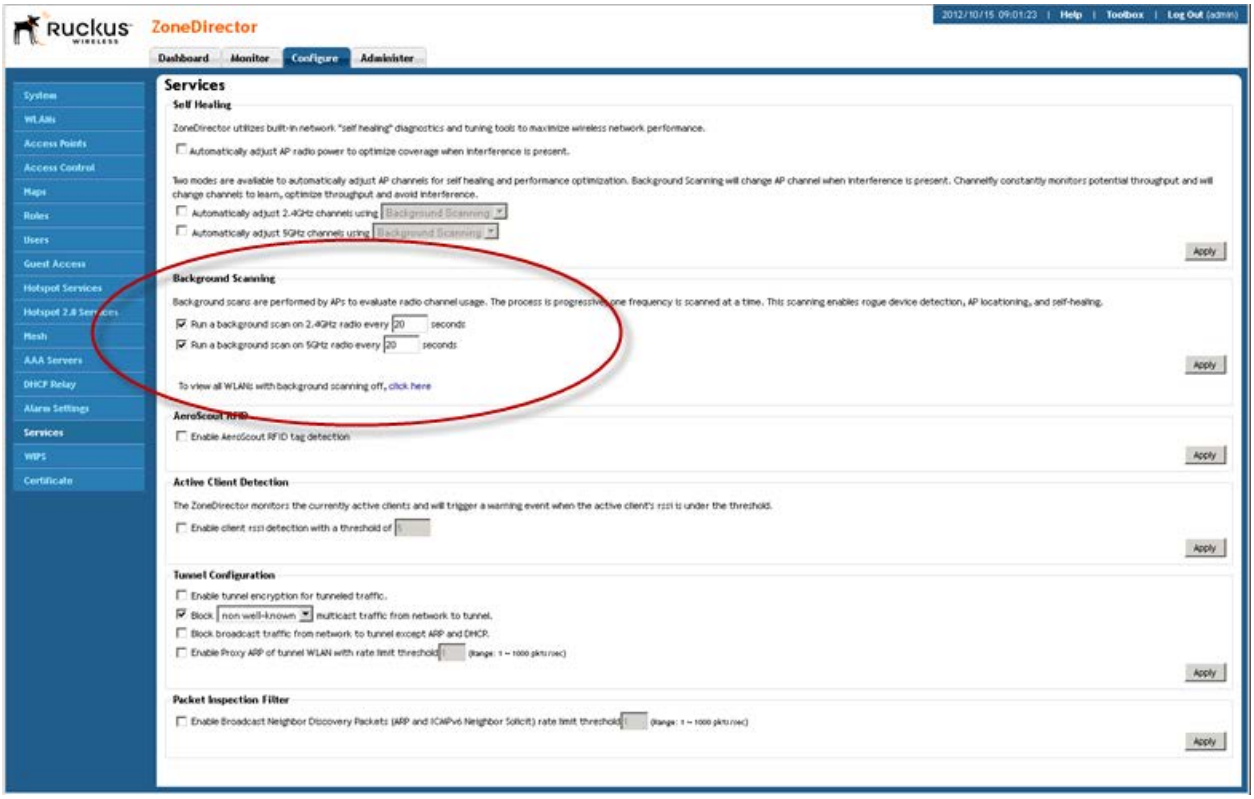
1. Navigate to Configure > AAA servers.
2. Click **Create New**.
3. Enter required details such as Name, IP, Port and Shared Secret.
4. Select **RADIUS** for Type.
5. Select Auth Method as **PAP**.
6. Click **OK** to save and create a RADIUS server.



Configure Background Scanning

Background scanning must be set to allow the AP's to find the neighboring AP's for effective roaming. The handsets are not compatible with the automatic channel optimization provided by the ChannelFly Self Healing method.

Navigate to **Configure > Services** and check the two Background Scanning checkboxes.



Configure Admission Control

Call admission control can be configured at different places in a ZD depending on what level of call admission control is required. The various places where it can be configured are listed below.

- Per WLAN - > Denotes if CAC is enabled for this WLAN. This option is only available if CAC and usage limits are defined in the AP config
- Per AP - > Bandwidth limits for the whole of the AP are defined here. This applies to all WLANs configured in the AP for which CAC is enforced
- Per AP group - > Denotes CAC for member APs defined in a AP group and all WLANs configured in the AP. Per AP level configuration overrides group configuration

The specifics will be shown in the sections below in WLAN Configuration and AP Configuration.

QoS Configuration

The network devices must be configured to prioritize the traffic between the wireless and wired networks. Below is a table showing the relationship between DSCP tags – the prioritization method used by the Spectralink handsets – and the ToS identification system used by the Ruckus infrastructure.

DSCP Class	DSCP (hex)	DSCP (dec)	ToS (hex)	ToS Prec. (dec)	ToS Delay Flag	ToS Throghput Flag	ToS Reliability Flag	TOS String Format
none	0×00	0	0×00	0	0	0	0	Routine
cs1	0×08	8	0×20	1	0	0	0	Priority
af11	0×0A	10	0×28	1	0	1	0	Priority
af12	0×0C	12	0×30	1	1	0	0	Priority
af13	0×0E	14	0×38	1	1	1	0	Priority
cs2	0×10	16	0×40	2	0	0	0	Immediate
af21	0×12	18	0×48	2	0	1	0	Immediate
af22	0×14	20	0×50	2	1	0	0	Immediate
af23	0×16	22	0×58	2	1	1	0	Immediate
cs3	0×18	24	0×60	3	0	0	0	Flash
af31	0×1A	26	0×68	3	0	1	0	Flash
af32	0×1C	28	0×70	3	1	0	0	Flash
af33	0×1E	30	0×78	3	1	1	0	Flash
cs4	0×20	32	0×80	4	0	0	0	FlashOverride
af41	0×22	34	0×88	4	0	1	0	FlashOverride
af42	0×34	36	0×90	4	1	0	0	FlashOverride
af43	0×26	38	0×98	4	1	1	0	FlashOverride
cs5	0×28	40	0xA0	5	0	0	0	Critical
ef	0×2E	46	0xB8	5	1	1	0	Critical
cs6	0×30	48	0xC0	6	0	0	0	Internetworkcontrol
cs7	0×38	56	0xE0	7	0	0	0	Networkcontrol

The default values in the Ruckus system are:

Default voice settings:

- 0xE0 = 1110 0000 which will map to DSCP = 56 **(Network Control)**
- 0xC0 = 1100 0000 which will map to DSCP =48 (**Internetwork Control)**
- 0xB8 = 1011 1000 which will map to DSCP= 46 (**Expedited Forwarding**)

Default video settings:

- 0xA0 = 1010 0000 which will map to DSCP = 40**(Critical)**
- 0x80 = 1000 0000 which will map to DSCP= 32 **(Flash Override)**

The default values in the handsets are:

Default voice settings:

- 8400 Series voice DSCP =46
- 8020/8030 DSCP=46

Default video settings:

- 8400 Series DSCP = 44 (4.2 versions and before. Maps to best effort. Must be changed)
- 8020/8030 DSCP = 26 or 40(depending on branding)

The settings must be reconciled between the handsets and the infrastructure. The settings on other devices such as a PBX or SIP server and network routers, must be taken into consideration.

To change the settings in the Ruckus controller, use the CLI interface by using the ssh protocol with the IP address of the controller and using the administrative login.

```
ruckus#
ruckus# config
ruckus(config)# system
ruckus(config-sys)# qos
ruckus(config-sys-qos)# show
System QoS:
ToS Classification-Voice = 0xE0 0xC0 0xB8
ToS Classification-Video = 0xA0 0x80
ToS Classification-Data = 0
ToS Classification-Background = 0
Tx fail threshold = 50
heuristics inter-packet-gap Video = 0  65
heuristics inter-packet-gap Voice = 15 275
```

```
heuristics packet-length Video = 2200 2201
heuristics packet-length Voice = 70 400
heuristics classification Video = 50000
heuristics classification Voice = 600
heuristics no classification Video = 500000
heuristics no classification Voice = 10000
```

To change default ToS classification, you can use following command:

```
ruckus(config-sys-qos)# tos classification voice 0xb8
ruckus(config-sys-qos)# tos classification video 0x68
```

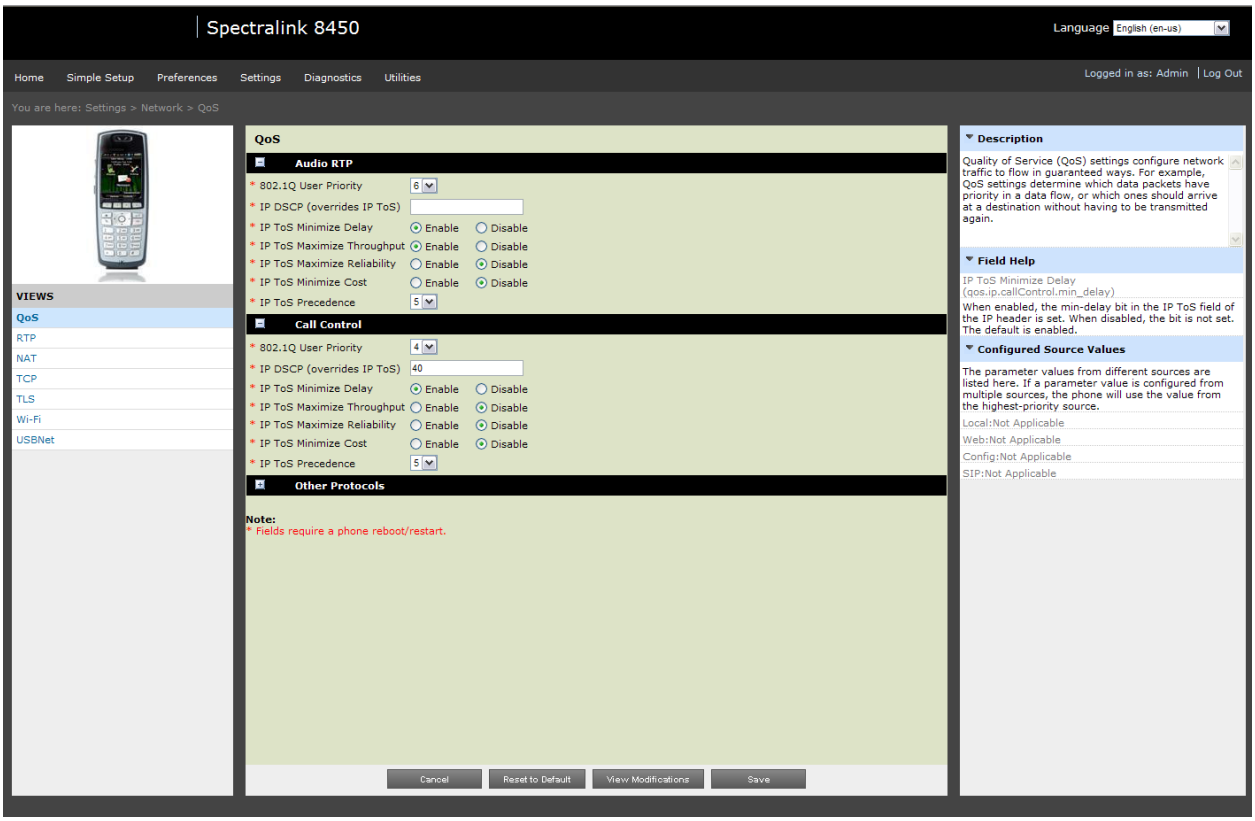
To change the settings in the 8020/8030 handsets:

1. Hold down the End Call and Start Call buttons with the handset powered off.
2. Let go of the End Call button while continuing to hold the Start Call button until the Admin Menu is displayed.
3. Navigate to **Network Config > WLAN Settings > Custom > QoS > Wi-Fi Standard > DSCP tags**.
4. Highlight Voice, press **OK**.
5. Enter the desired DSCP tag value in decimal.
6. Press **OK**.
7. Highlight Control, press **OK**.
8. Enter the desired DSCP tag value in decimal.
9. Press **OK**.

To change settings in the 8400 handsets, there are two methods:

Method 1: Use the Web Configuration Utility on a handset-by-handset basis.

1. Open the Web Configuration Utility and navigate to Settings > Network > QoS.
2. Edit the parameters as shown on the example screen:



Method 2: For broad deployment, use the provisioning .cfg files as described in the Spectralink 8400 Series Deployment Guide.

The setting for the video tag is:

```
< qos.ip.callControl.dscp=”26” >
```

The setting for the voice tag is:

```
< qos.ip.rtp.dscp=”46” >
```

These parameters may be added to the configuration files on the provisioning server for the handset to change the DSCP tag. QoS tags are usually added to the wireless.cfg file.

Chapter 5: WLAN Configuration

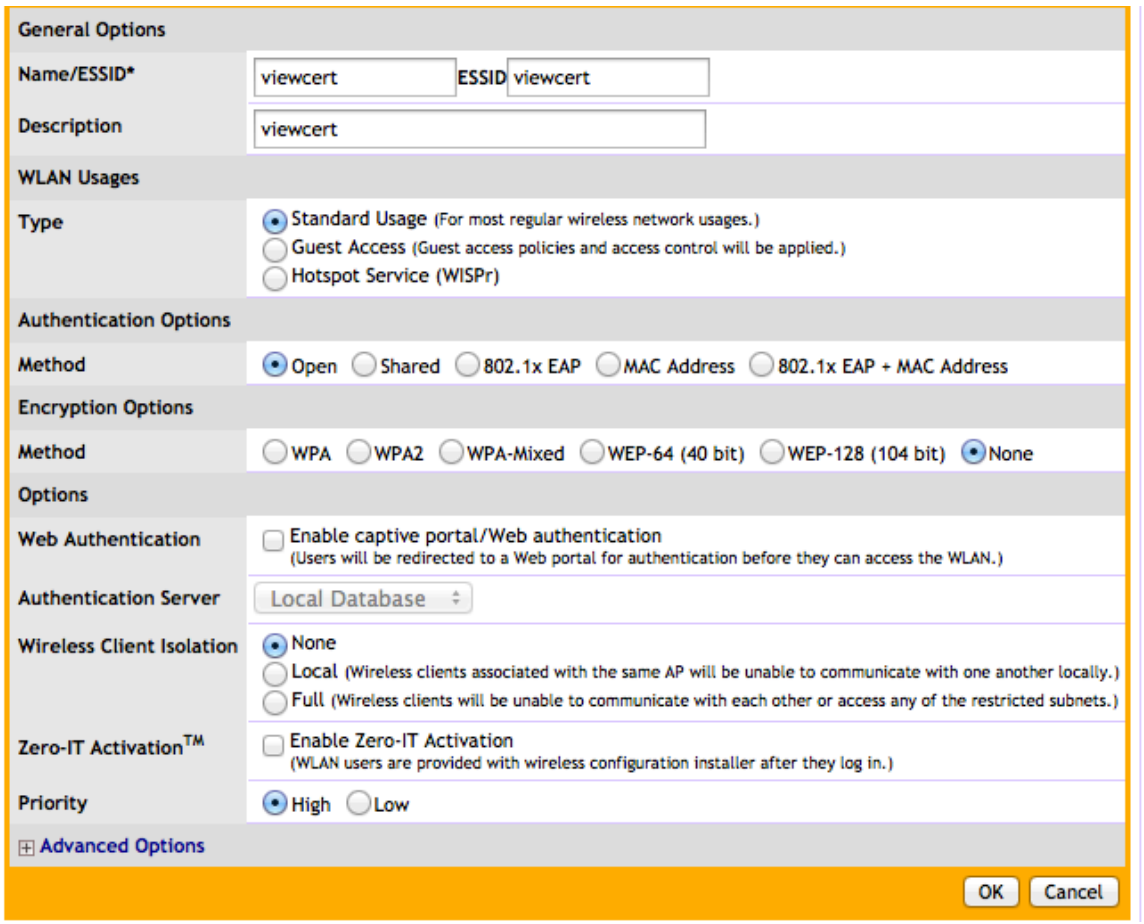
This section describes how various WLANs can be configured.

Configure Security Settings

For any security option, you will first name and describe the configuration. Then you will select the security type and complete the required information for that type.

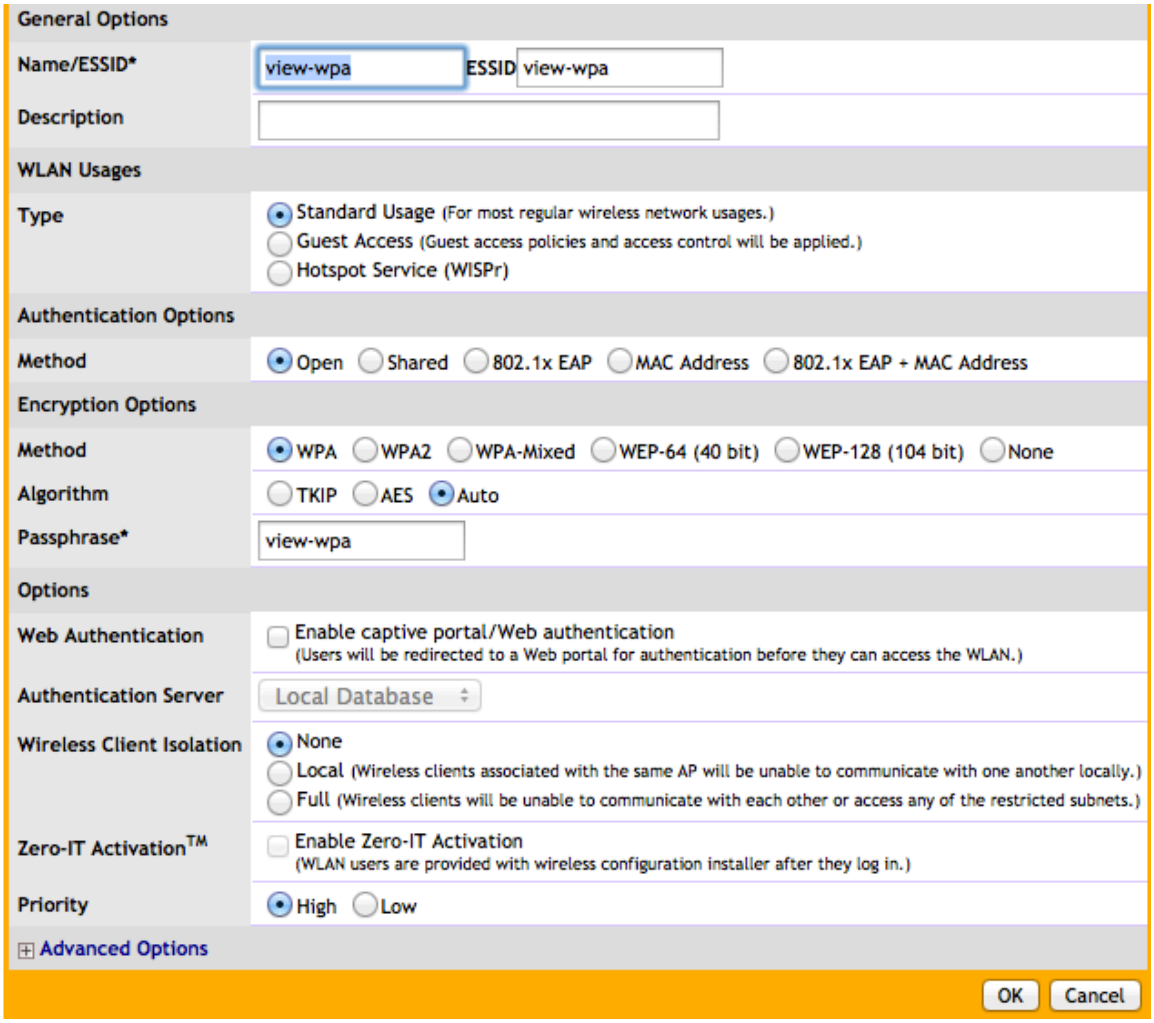
Security: Open

1. Navigate to **Configure > WLAN > Create New**.
2. Enter the values for Name, ESSID, Description and Type.
3. Select **Open** under Authentication Options Method.
4. Select **None** for Encryption Options Method.



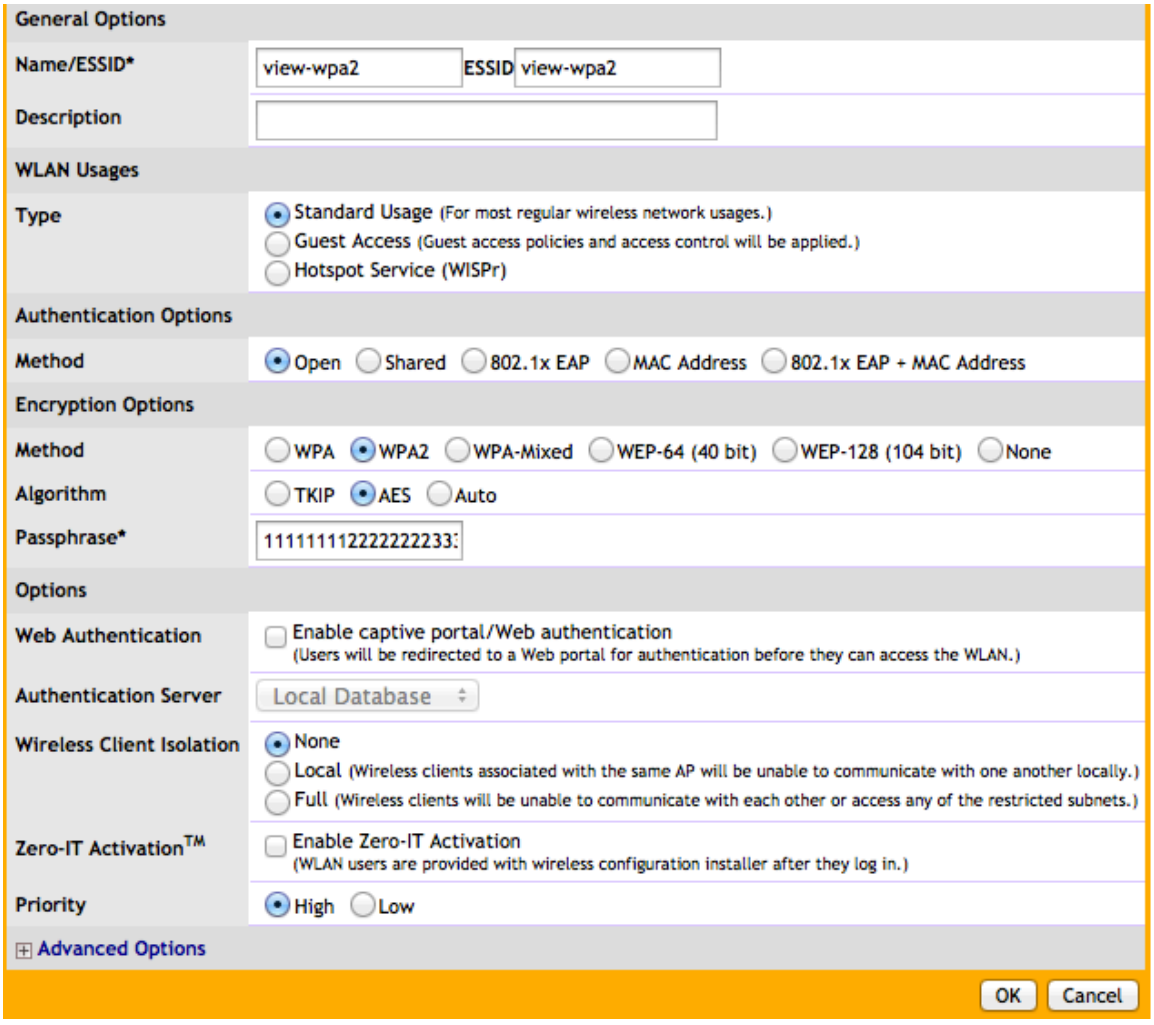
Security: WPA-PSK

1. Navigate to **Configure > WLAN > Create New**.
2. Enter the required values for Name, ESSID, Description and Type.
3. Select **Open** under Authentication Options Method.
4. Select **WPA** for Encryption Options Method.
5. Choose **Auto** for Encryption Options Algorithm.
6. Enter [your passphrase] in the Passphrase text box.



Security: WPA2-PSK

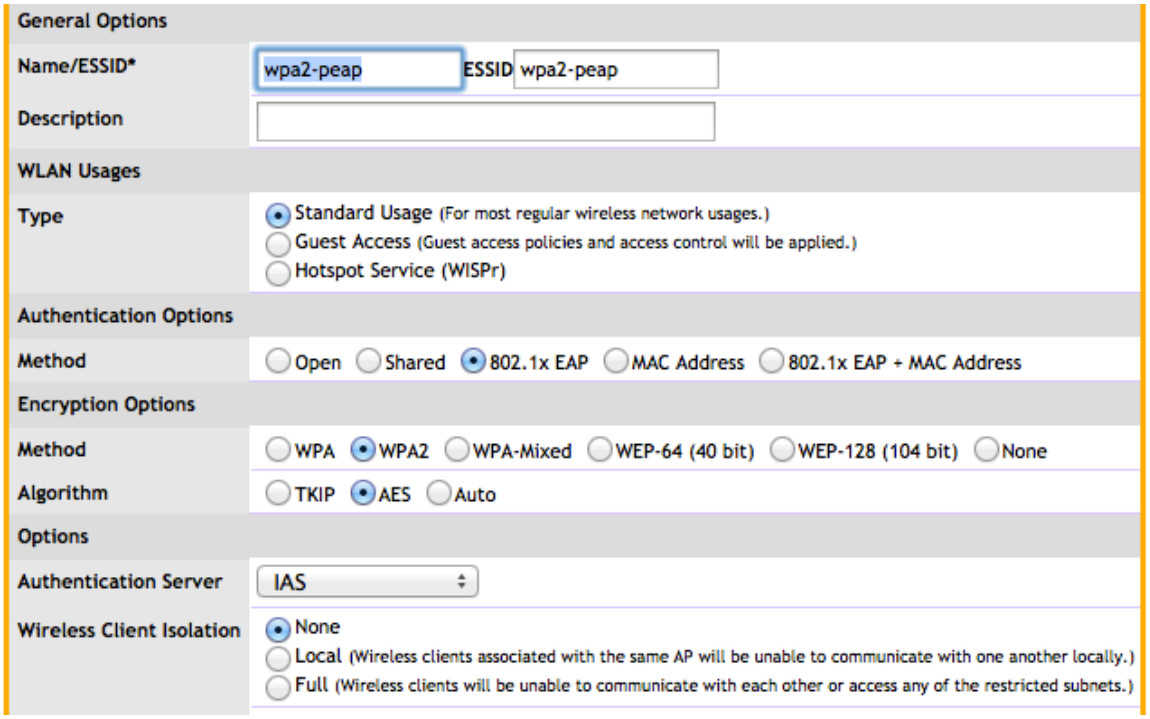
1. Navigate to **Configure > WLAN > Create New**.
2. Enter the Name, ESSID, Description and Type.
3. Select **Open** under Authentication Options Method.
4. Select **WPA** for Encryption Options Method.
5. Select **AES** for Encryption Options Algorithm.
6. Enter [your passphrase] in the Passphrase text box.



Security: WPA2-Enterprise

After defininining a RADIUS server as described in RADIUS Server Definition, follow the steps below to create a WLAN with WPA2-Enterprise scheme

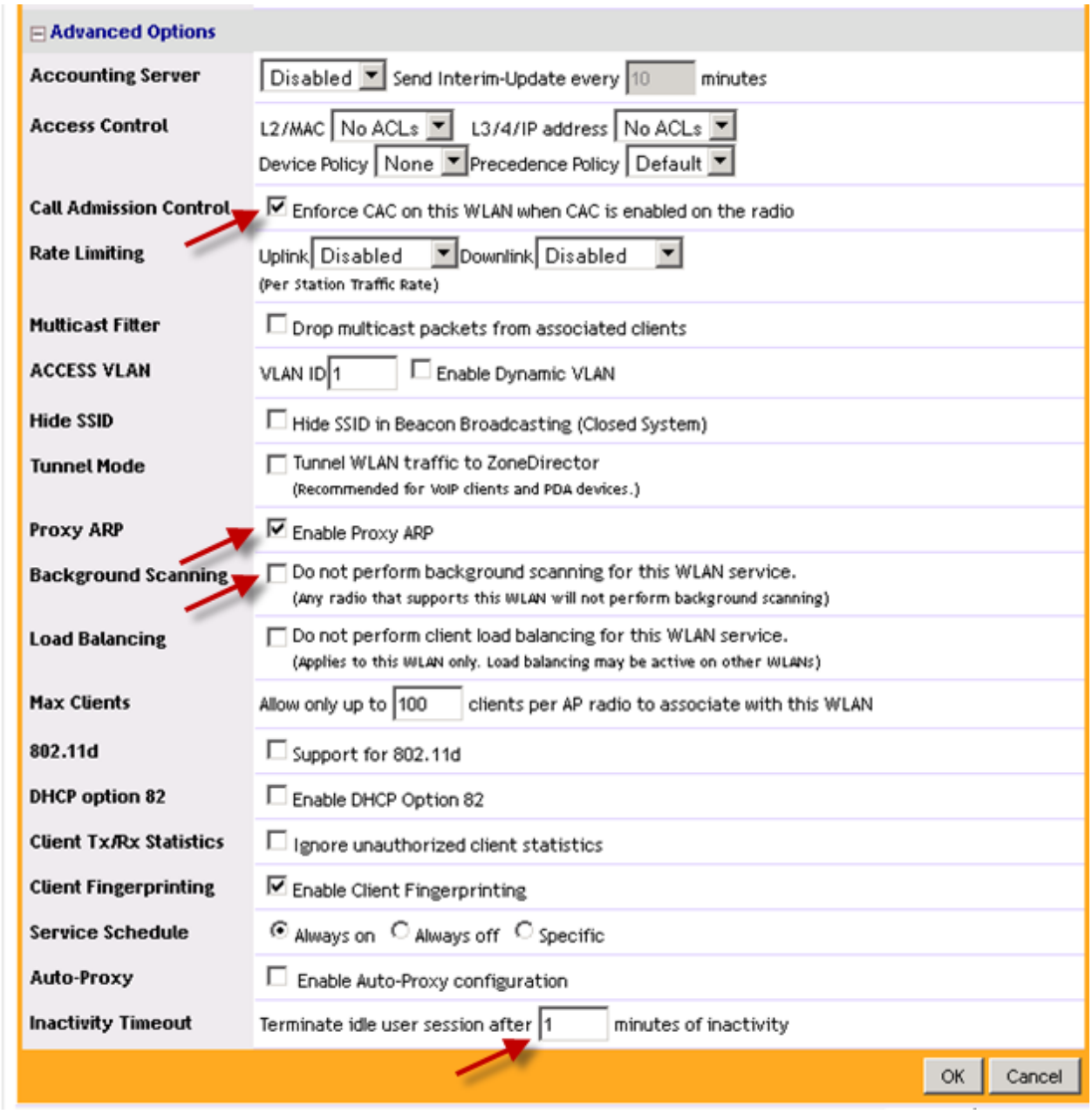
1. Navigate to **Configure** > **WLAN** > **Create New**.
2. Enter the values for Name, ESSID, Description and Type.
3. Select **802.1x EAP** under Authentication Options Method.
4. Select **WPA2** for Encryption Options Method.
5. Select **AES** for Encryption Options Algorithm.
6. Select the already-created RADIUS server from the Authentication Server drop down box.



Advanced Options on the WLAN

After setting the Security option, additional WLAN options can be configured.

1. At the bottom of the Security window is the **Advanced Options** hyperlink. Click it to open the Advanced Options window.
2. For Call Admission Control, click the checkbox for **Enforce CAC** on this WLAN when CAC is enabled on the radio.
3. For Proxy AP, click the checkbox for **Enable Proxy ARP**
4. For Background Scanning, ensure that Do not perform background scanning for this WLAN service is unchecked. This enables background scanning which is essential for fast roaming on the WLAN carrying the voice service.
5. Set Inactivity Timeout to **1 minute**.
6. Click **OK** to save changes made to this WLAN


Advanced Options
Accounting Server
Disabled
Send Interim-Update every
10
minutes
Access Control
L2/MAC
No ACLs
L3/4/IP address
No ACLs
Device Policy
None
Precedence Policy
Default
Call Admission Control
Enforce CAC on this WLAN when CAC is enabled on the radio
Rate Limiting
Uplink
Disabled
Downlink
Disabled
(Per Station Traffic Rate)
Multicast Filter
Drop multicast packets from associated clients
ACCESS VLAN
VLAN ID
1
Enable Dynamic VLAN
Hide SSID
Hide SSID in Beacon Broadcasting (Closed System)
Tunnel Mode
Tunnel WLAN traffic to ZoneDirector
(Recommended for VoIP clients and PDA devices.)
Proxy ARP
Enable Proxy ARP
Background Scanning
Do not perform background scanning for this WLAN service.
(Any radio that supports this WLAN will not perform background scanning)
Load Balancing
Do not perform client load balancing for this WLAN service.
(Applies to this WLAN only. Load balancing may be active on other WLANs)
Max Clients
Allow only up to
100
clients per AP radio to associate with this WLAN
802.11d
Support for 802.11d
DHCP option 82
Enable DHCP Option 82
Client Tx/Rx Statistics
Ignore unauthorized client statistics
Client Fingerprinting
Enable Client Fingerprinting
Service Schedule
Always on
Always off
Specific
Auto-Proxy
Enable Auto-Proxy configuration
Inactivity Timeout
Terminate idle user session after
1
minutes of inactivity
OK
Cancel

WLAN Settings from the CLI

The minimum data rate for BSS is done through CLI by the following commands. This reduces range from an AP slightly but improves throughput.

In addition, pmk caching must be disabled to enable the OKC algorithm expected for fast roaming.

```
ruckus> enable
ruckus# config
ruckus(config)# wlan <wlan name>
(The WLAN service <wlan name> has been loaded. To save the WLAN
service, type 'end' or 'exit'.)
ruckus(config-wlan)# bss-minrate 5.5
ruckus(config-wlan)# no pmk-cache-for-reconnect
ruckus(config-wlan)# end
(message saying values were saved)
```

The DTIM must be set to 2 for good PTT (“walkie-talkie”) performance. These commands are executed through a special debug interface which sends the setting out to all AP’s currently attached.



AdminTip: Repeat when new APs added

These commands must be re-issued when a new AP is powered up and added to the network.

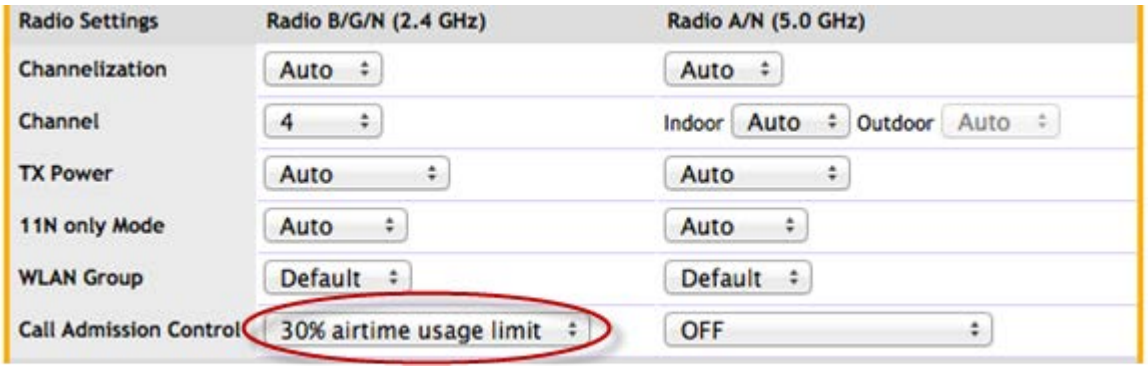
```
Welcome to the Ruckus Wireless ZoneDirector 1100 Command Line
Interface
ruckus> enable
ruckus# debug
ruckus(debug)# rksap_cli -A "set dtim-period wlan0 2”
ruckus(debug)# rksap_cli -A "set dtim-period wlan1 2”
…
ruckus(debug)# rksap_cli -A "set dtim-period wlan14 2”
ruckus(debug)# rksap_cli -A "set dtim-period wlan15 2”
ruckus(debug)# quit
```

Chapter 6: AP Configuration

AP Group Setup

Call Admission Control (CAC) can be configured for an AP group instead of configuring at individual AP. However, configuration at individual AP radio supersedes the configuration at AP group. This configuration ensures all configured APs in the AP group to have same CAC setting instead of configuring CAC for individual APs.

1. Navigate to **Configure > Access Points**.
2. In the main screen, go to Access Point Groups.
3. Click **Edit** for the AP group where CAC is required.
4. Under Radio Settings, go to Call Admission Control and choose the required **CAC** % limit per radio. Use **10%** for the 8020/8030 handsets and **20%** for the 8400 handsets. If both types of handsets are present, use the smaller number.
5. Click **OK** to save the changes



AdminTip: 8020/8030 handsets are not 802.11n devices

8020/8030 handsets will not be admitted to a network with 11N only Mode set to N-only.

Individual AP Configuration

At the AP level, CAC is configured per radio. The airtime % denotes the percentage of total available BW that shall be reserved for voice/video class. This reservation ensures voice bandwidth for handsets and prevents VoIP handsets using up all the available bandwidth.

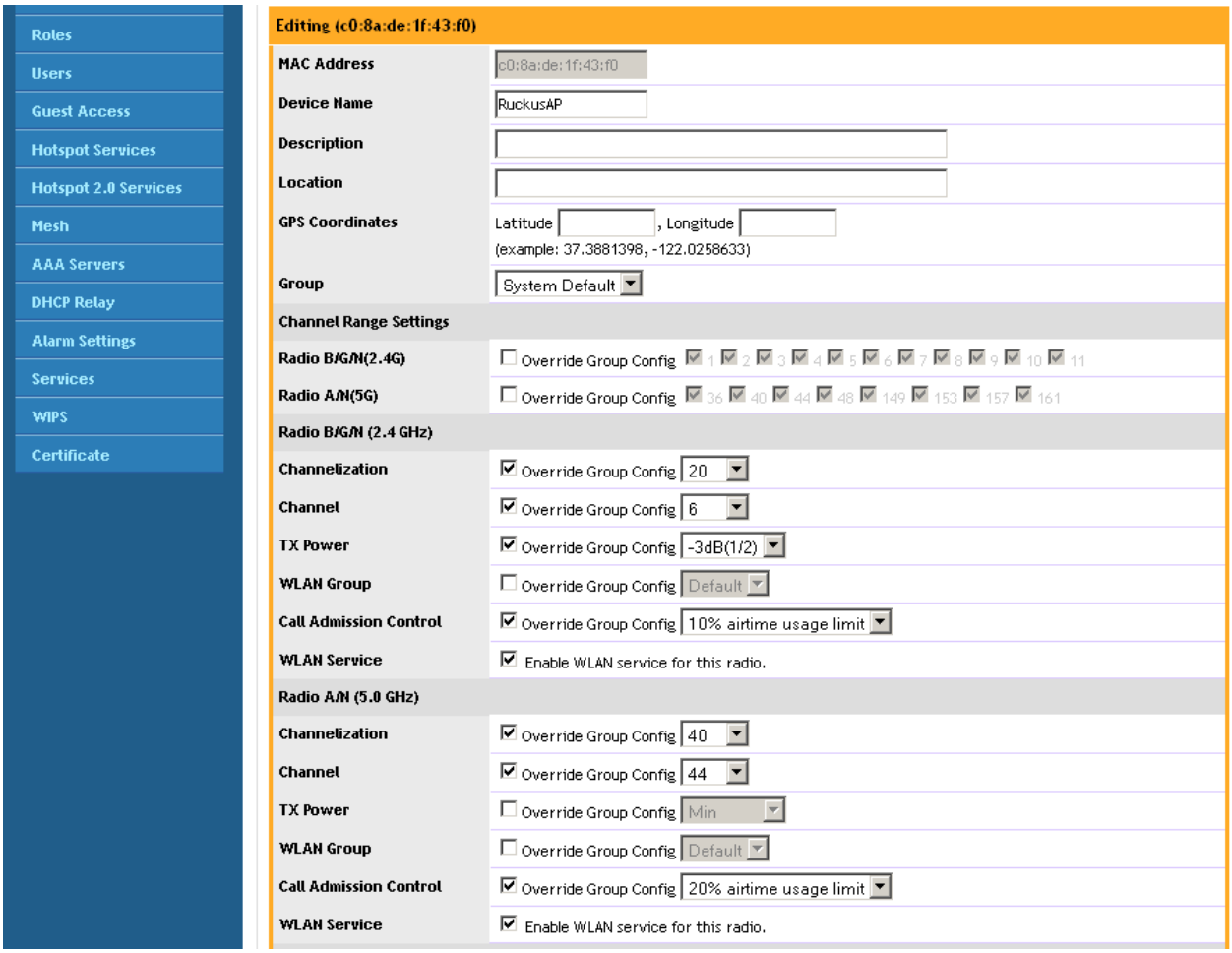
1. Click **Configure > Access Points** and click **Edit** for the AP where CAC is required.
2. Under each of the radios B/G/N 2.4 GHz or A/N 5.0 GHz Call Admission Control check **Override Group Config** and select the % of airtime usage limit.

   Select **10%** for the 8020/8030 handsets and select **20%** for the 8400 handsets. If both types of handsets are present, use the smaller number.
3. Change the Tx Power if necessary for each radio.

   Please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all expected data rates.

   The handset requires the following minimum dBm reading – determined by the AP Tx power setting and the plan architecture - to support the corresponding data rate in the access point.

802.11 Radio Standard	*Minimum Available Signal Strength (RSSI)*	*Maximum "Mandatory" Data Rate*
802.11b	-70 dBm	1 Mb/s
	-60 dBm	11 Mb/s
802.11g	-63 dBm	6 Mb/s
	-47 dBm	54 Mb/s
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s



AdminTip: Don’t overpower handset radio chip

Received power at the handsets needs to be less than -30 dB for best operation.

AdminTip: OKC Roaming data base refresh

When the channel is changed on an AP, it must be power cycled for the change to propagate to the neighbor lists in the other APs. No sooner than 10 minutes later, all the handsets that have been associated with the AP in the last 24 hours must be power cycled. Please advise your handset users to power cycle their handsets.