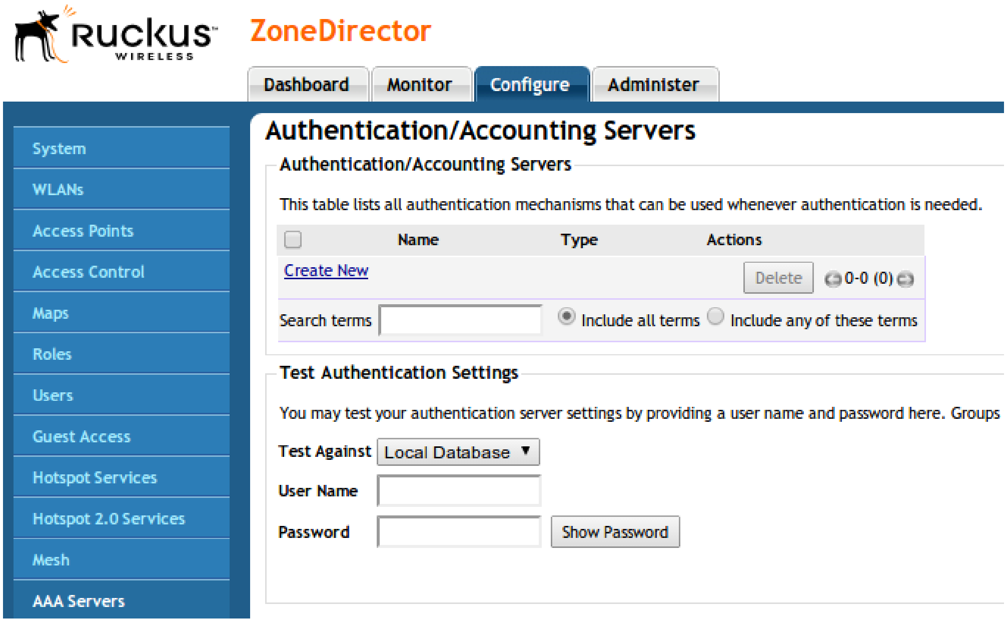
Ruckus 9.8 or above (ZD managed)

Modified on: Fri, 20 Feb, 2015 at 10:37 AM

IMPORTANT: This guide is for the Ruckus ZoneDirector release 9.8 or above. If you are using release 9.6 or 9.7 please select **Ruckus AP (ZD v9.7 or below)** in your portal and use that guide instead.

Open a web browser and log in to your Ruckus ZoneDirector

Click on **"Configure"** on the top menu



Authentication/Accounting Servers

Authentication/Accounting Servers

This table lists all authentication mechanisms that can be used whenever authentication is needed.

□	Name	Type	Actions

Search terms ● Include all terms ○ Include any of these terms

Test Authentication Settings

You may test your authentication server settings by providing a user name and password here. Groups

Test Against: Local Database

User Name

Password

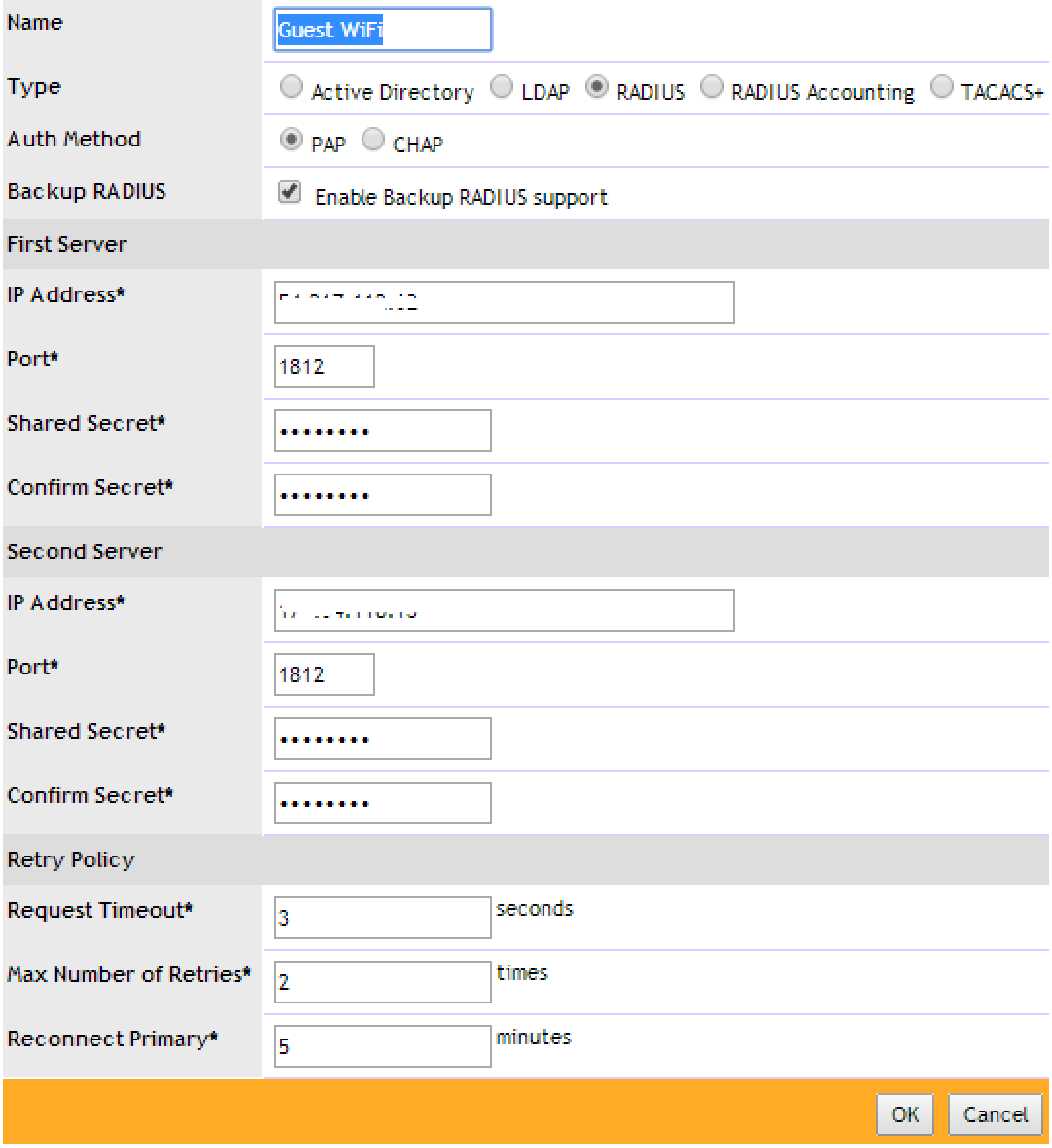
Click on **"AAA Servers"** on the left menu and then **"Create New"**. Configure with the below settings:

- **Name**: Guest WiFi
- **Type**: RADIUS
- **Auth Method**: PAP
- **Backup Backup RADIUS support**: Ticked

- **First Server IP Address**: *insert radius_server_ip here*
- **Port**: 1812
- **Shared Secret**: *insert radius_secret here*
- **Confirm Secret**: as above

- **Second Server IP Address:** *insert radius_server2_ip here*
- **Port:** 1812
- **Shared Secret:** *insert radius_secret here*
- **Confirm Secret:** as above

- Press **OK** to save



Name	Guest WiFi
Type	○ Active Directory ○ LDAP ● RADIUS ○ RADIUS Accounting ○ TACACS+
Auth Method	● PAP ○ CHAP
Backup RADIUS	☑ Enable Backup RADIUS support
First Server	
IP Address*	[illegible]
Port*	1812
Shared Secret*	••••••••
Confirm Secret*	••••••••
Second Server	
IP Address*	[illegible]
Port*	1812
Shared Secret*	••••••••
Confirm Secret*	••••••••
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times
Reconnect Primary*	5 minutes

Click **"Create New"** again and configure with the below settings:

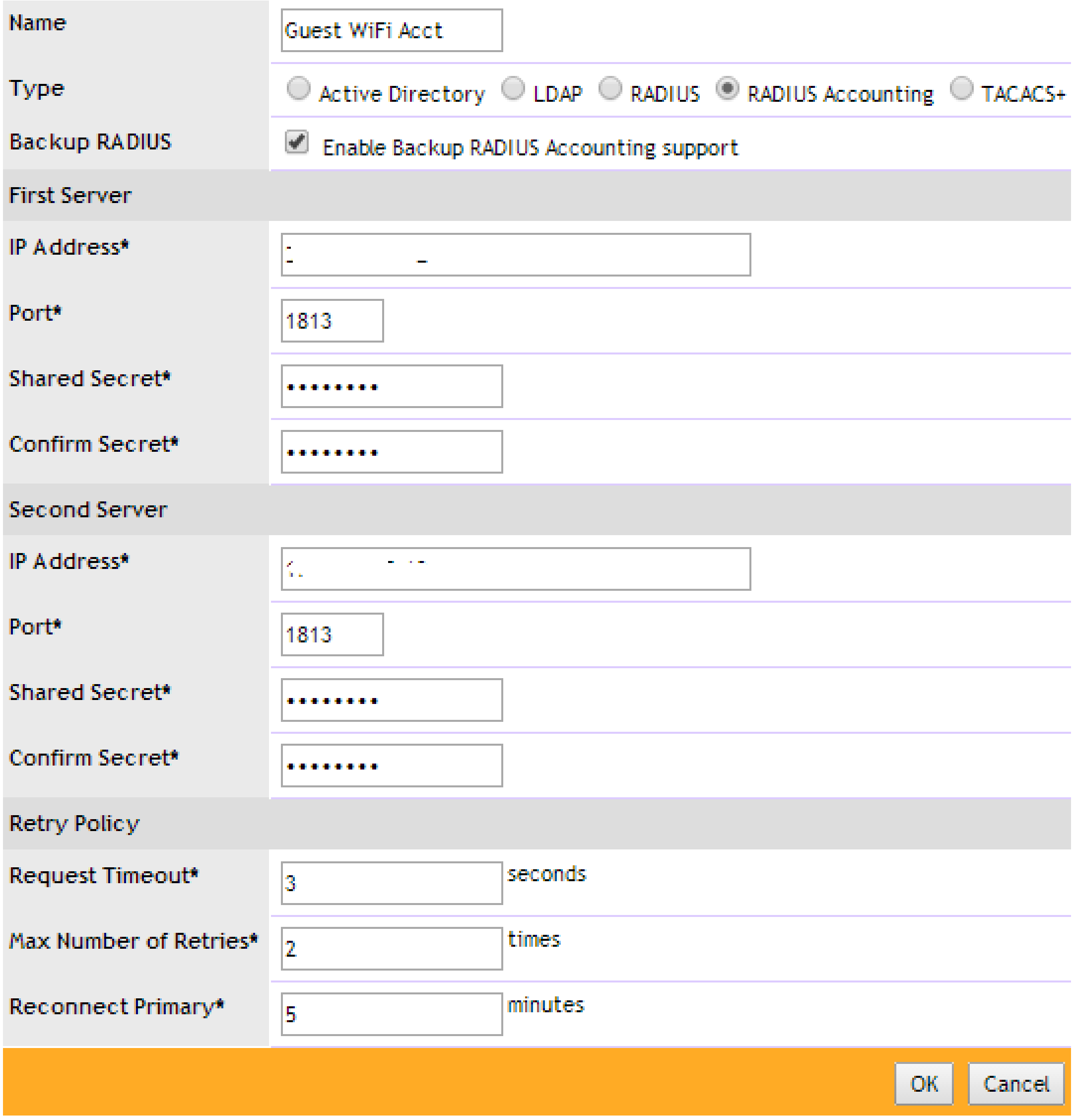
- **Name:** Guest WiFi Acct
- **Type:** RADIUS Accounting
- **Backup RADIUS Support:** Ticked

- **First Server IP Address:** *insert radius_server_ip here*

- **Port:** 1813
- **Shared Secret:** *insert radius_secret here*
- **Confirm Secret:** as above

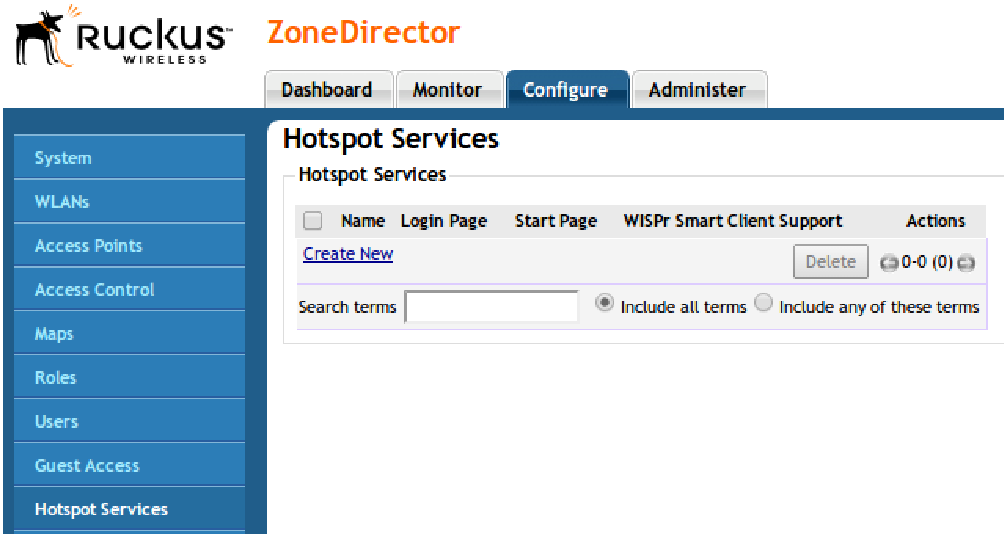
- **Second Server IP Address:** *insert radius_server2_ip here*
- **Port:** 1813
- **Shared Secret:** *insert radius_secret here*
- **Confirm Secret:** as above

Press **OK** to save



Name	Guest WiFi Acct
Type	○ Active Directory ○ LDAP ○ RADIUS ● RADIUS Accounting ○ TACACS+
Backup RADIUS	☑ Enable Backup RADIUS Accounting support
First Server	
IP Address*	
Port*	1813
Shared Secret*	••••••••
Confirm Secret*	••••••••
Second Server	
IP Address*	
Port*	1813
Shared Secret*	••••••••
Confirm Secret*	••••••••
Retry Policy	
Request Timeout*	3 seconds
Max Number of Retries*	2 times
Reconnect Primary*	5 minutes

Click on "**Hotspot Services**" on the left menu and then "**Create New**".

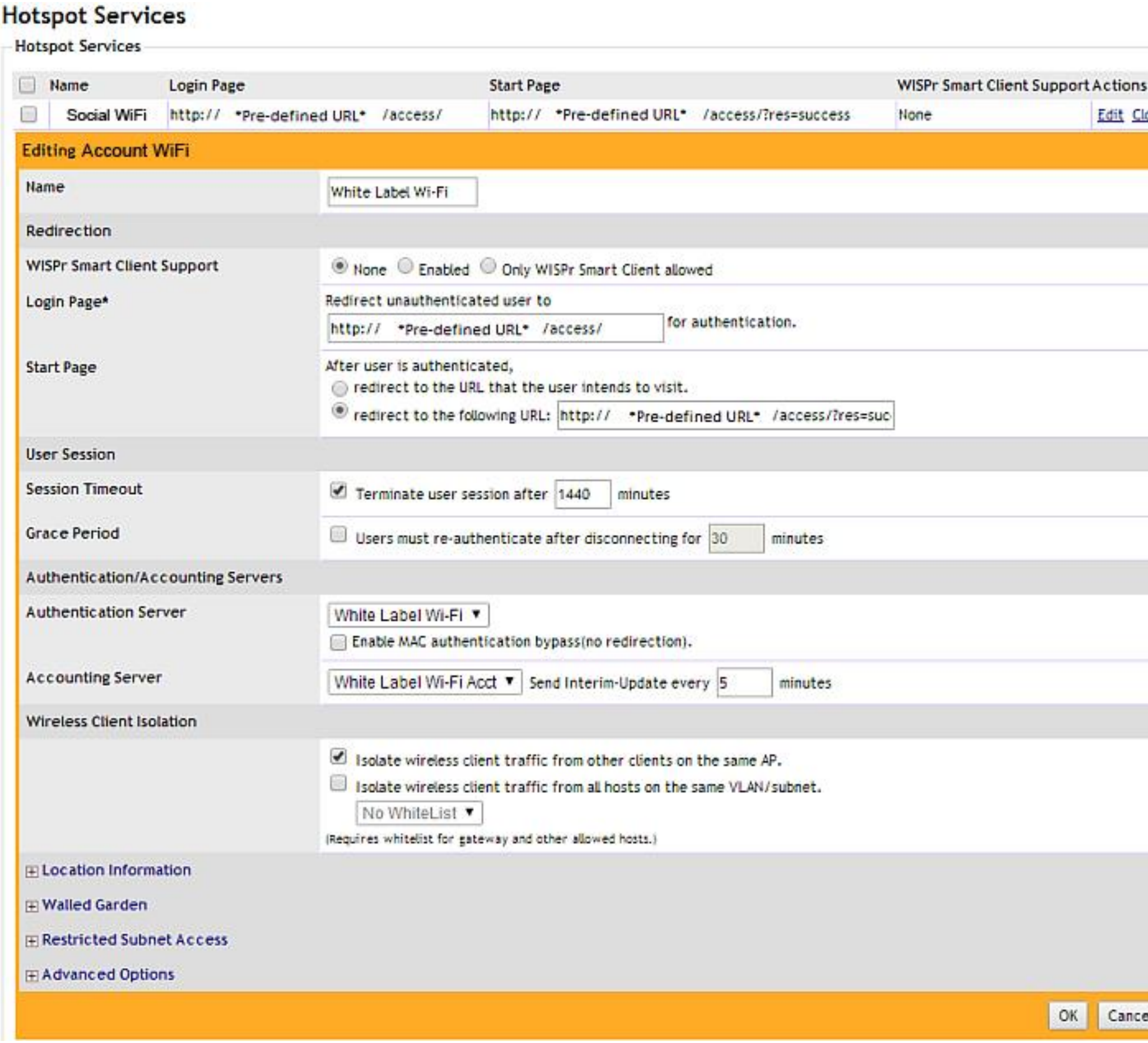


Hotspot Services

Hotspot Services

□	Name	Login Page	Start Page	WISPr Smart Client Support	Actions

Search terms ☐ ● Include all terms ○ Include any of these terms



Hotspot Services

Hotspot Services

□	Name	Login Page	Start Page	WISPr Smart Client Support	Actions
□	Social WiFi	http:// *Pre-defined URL* /access/	http:// *Pre-defined URL* /access/?res=success	None	Edit Cl

Editing Account WiFi

Name	White Label Wi-Fi
Redirection	
WISPr Smart Client Support	● None ○ Enabled ○ Only WISPr Smart Client allowed
Login Page*	Redirect unauthenticated user to http:// *Pre-defined URL* /access/ for authentication.
Start Page	After user is authenticated, ○ redirect to the URL that the user intends to visit. ● redirect to the following URL: http:// *Pre-defined URL* /access/?res=suc
User Session	
Session Timeout	☑ Terminate user session after 1440 minutes
Grace Period	☐ Users must re-authenticate after disconnecting for 30 minutes
Authentication/Accounting Servers	
Authentication Server	White Label Wi-Fi ▼ ☐ Enable MAC authentication bypass(no redirection).
Accounting Server	White Label Wi-Fi Acct ▼ Send Interim-Update every 5 minutes
Wireless Client Isolation	
	☑ Isolate wireless client traffic from other clients on the same AP. ☐ Isolate wireless client traffic from all hosts on the same VLAN/subnet. No WhiteList ▼ (Requires whitelist for gateway and other allowed hosts.)

⊞ Location Information

⊞ Walled Garden

⊞ Restricted Subnet Access

⊞ Advanced Options

- **Name:** Guest Wi-Fi
- **Login Page:** *insert access_url here*
- **Redirect to the following URL:** *insert redirect_url here*
- **Authentication Server:** Guest Wi-Fi
- **Accounting Server:** Guest Wi-Fi Acct
- **Wireless Client Isolation:** Full

Walled Garden: Add the following domains one by one:

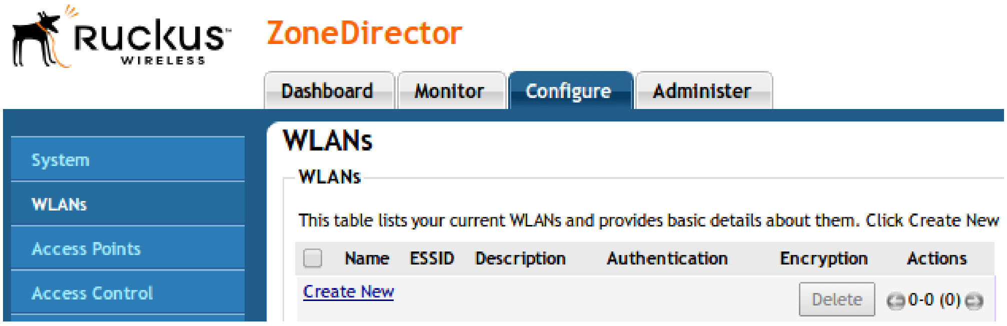
*.*insert access_domain here*
www.google.com
www.google.co.uk
*.google-analytics.com
*.openweathermap.org
*.cloudfront.net
*.venuewifi.com

If you wish to support social network logins, you also need to add the domains below for each network you plan to support

Facebook	**Twitter**	**LinkedIn**	**Google**	**Instagram**
*.facebook.com *.fbcdn.net *.akamaihd.net *.connect.facebook.net	*.twitter.com *.twimg.com	*.linkedin.com *.licdn.net *.licdn.com	*.googleusercontent.com *.googleapis.com *.accounts.google.com *.gstatic.com	*.instagram.com

Press "**OK**" to Save

Click on **"WLANs"** on the left menu and then **"Create New"**.



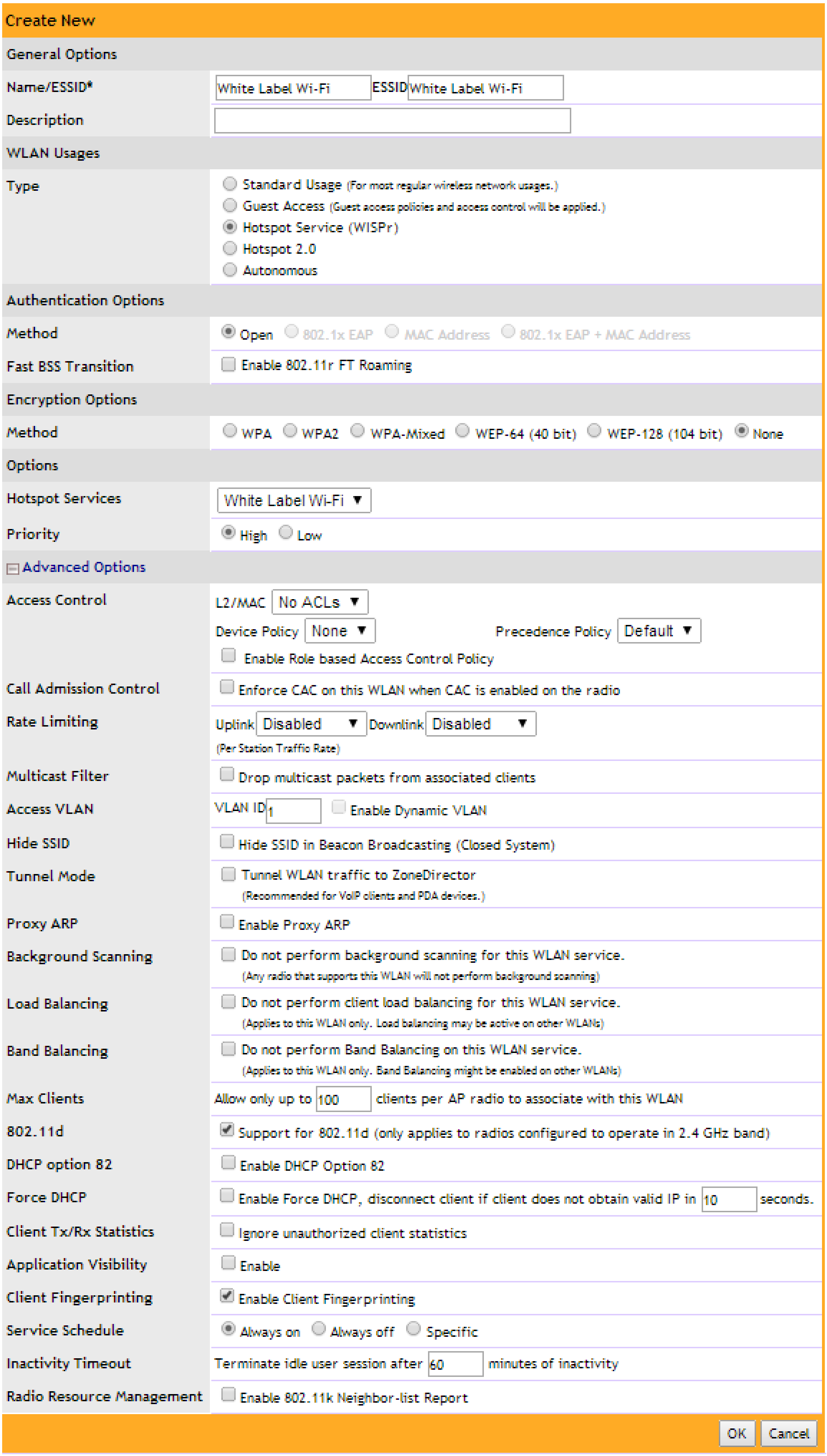
This table lists your current WLANs and provides basic details about them. Click Create New

Configure with the below settings:

- **Name**: Guest Wi-Fi

- **ESSID**: Whatever you want to broadcast as your wireless network name (SSID)
- **Type**: Hotspot Service (WISPr)
- **Authentication Method**: Open
- **Encryption Method**: Open
- **Hotspot Service**: Guest Wi-Fi
- **Priority**: High
- **Inactivity Timeout**: 60

Click on **"OK"**



Create New

General Options	
Name/ESSID*	White Label Wi-Fi ESSID White Label Wi-Fi
Description	
WLAN Usages	
Type	○ Standard Usage (For most regular wireless network usages.) ○ Guest Access (Guest access policies and access control will be applied.) ● Hotspot Service (WISPr) ○ Hotspot 2.0 ○ Autonomous
Authentication Options	
Method	● Open ○ 802.1x EAP ○ MAC Address ○ 802.1x EAP + MAC Address
Fast BSS Transition	□ Enable 802.11r FT Roaming
Encryption Options	
Method	○ WPA ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bit) ○ WEP-128 (104 bit) ● None
Options	
Hotspot Services	White Label Wi-Fi ▼
Priority	● High ○ Low
⊟ Advanced Options	
Access Control	L2/MAC No ACLs ▼ Device Policy None ▼ Precedence Policy Default ▼ □ Enable Role based Access Control Policy
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)
Band Balancing	□ Do not perform Band Balancing on this WLAN service. (Applies to this WLAN only. Band Balancing might be enabled 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 (only applies to radios configured to operate in 2.4 GHz band)
DHCP option 82	□ Enable DHCP Option 82
Force DHCP	□ Enable Force DHCP, disconnect client if client does not obtain valid IP in 10 seconds.
Client Tx/Rx Statistics	□ Ignore unauthorized client statistics
Application Visibility	□ Enable
Client Fingerprinting	☑ Enable Client Fingerprinting
Service Schedule	● Always on ○ Always off ○ Specific
Inactivity Timeout	Terminate idle user session after 60 minutes of inactivity
Radio Resource Management	□ Enable 802.11k Neighbor-list Report

To complete the set up you will need to SSH in to the Ruckus ZoneDirector and type the commands below, one line at a time.

```
enable
config
wlan "Guest Wi-Fi"
called-station-id-type ap-mac
end
```

This will set the correct parameter we require for the MAC of the AP to be sent in the RADIUS request.