

Ruckus 9.6 or 9.7 (ZD managed)

Modified on: Tue, 27 Jan, 2015 at 11:17 AM

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

NB: Support for ZoneDirector 9.6 and 9.7 is limited by restrictions in the Ruckus captive portal settings, and user experience may be varied. We strongly recommend using 9.8 or above.

Open a web browser and log in to your Ruckus ZoneDirector

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



The screenshot shows the Ruckus ZoneDirector web interface. The top navigation bar includes "Dashboard", "Monitor", "Configure", and "Administer". The left sidebar menu lists various system components, with "AAA Servers" selected. The main content area is titled "Authentication/Accounting Servers" and contains a table for listing authentication mechanisms, a "Create New" link, and a "Test Authentication Settings" section with input fields for "Test Against", "User Name", and "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 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	<input type="text" value="Guest WiFi"/>
Type	<input type="radio"/> Active Directory <input type="radio"/> LDAP <input checked="" type="radio"/> RADIUS <input type="radio"/> RADIUS Accounting <input type="radio"/> TACACS+
Auth Method	<input checked="" type="radio"/> PAP <input type="radio"/> CHAP
Backup RADIUS	<input checked="" type="checkbox"/> Enable Backup RADIUS support
First Server	
IP Address*	<input type="text" value="192.168.1.12"/>
Port*	<input type="text" value="1812"/>
Shared Secret*	<input type="password" value="....."/>
Confirm Secret*	<input type="password" value="....."/>
Second Server	
IP Address*	<input type="text" value="192.168.1.12"/>
Port*	<input type="text" value="1812"/>
Shared Secret*	<input type="password" value="....."/>
Confirm Secret*	<input type="password" value="....."/>
Retry Policy	
Request Timeout*	<input type="text" value="3"/> seconds
Max Number of Retries*	<input type="text" value="2"/> times
Reconnect Primary*	<input type="text" value="5"/> minutes
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

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	<input type="text" value="Guest WiFi Acct"/>
Type	<input type="radio"/> Active Directory <input type="radio"/> LDAP <input type="radio"/> RADIUS <input checked="" type="radio"/> RADIUS Accounting <input type="radio"/> TACACS+
Backup RADIUS	<input checked="" type="checkbox"/> Enable Backup RADIUS Accounting support
First Server	
IP Address*	<input type="text" value=""/>
Port*	<input type="text" value="1813"/>
Shared Secret*	<input type="password" value=""/>
Confirm Secret*	<input type="password" value=""/>
Second Server	
IP Address*	<input type="text" value=""/>
Port*	<input type="text" value="1813"/>
Shared Secret*	<input type="password" value=""/>
Confirm Secret*	<input type="password" value=""/>
Retry Policy	
Request Timeout*	<input type="text" value="3"/> seconds
Max Number of Retries*	<input type="text" value="2"/> times
Reconnect Primary*	<input type="text" value="5"/> minutes
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

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



ZoneDirector

Dashboard Monitor **Configure** Administer

- System
- WLANS
- Access Points
- Access Control
- Maps
- Roles
- Users
- Guest Access
- Hotspot Services**

Hotspot Services

Hotspot Services

<input type="checkbox"/>	Name	Login Page	Start Page	WISPr Smart Client Support	Actions
	Create New				Delete 0-0 (0)
Search terms <input type="text"/> <input checked="" type="radio"/> Include all terms <input type="radio"/> 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 Close

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

OK Cancel

- **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 domain: *insert access_domain here*

Press "OK" to Save

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



- System
- WLANs**
- Access Points
- Access Control

WLANs

WLANs

This table lists your current WLANs and provides basic details about them. Click [Create New](#)

<input type="checkbox"/>	Name	ESSID	Description	Authentication	Encryption	Actions
Create New						Delete 0-0 (0)

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* ESSID

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

Priority High Low

Advanced Options

Access Control L2/MAC Device Policy Precedence Policy
 Enable Role based Access Control Policy

Call Admission Control Enforce CAC on this WLAN when CAC is enabled on the radio

Rate Limiting Uplink Downlink
(Per Station Traffic Rate)

Multicast Filter Drop multicast packets from associated clients

Access VLAN VLAN ID 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 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 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 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.