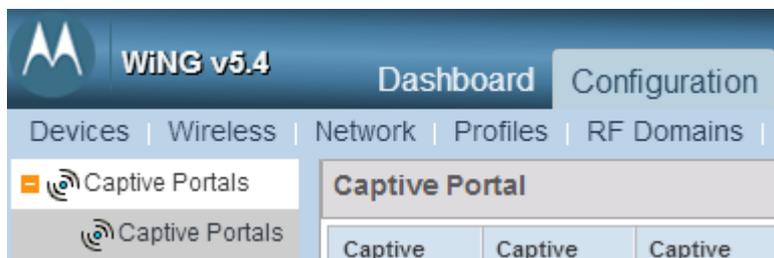


Motorola / Zebra (RFS based)

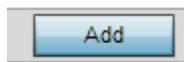
Modified on: Sun, 20 Sep, 2015 at 10:20 PM

NOTE: Before you begin, please ensure you have added your AP's Radio MAC's (as well as the normal AP MAC) to the portal "Hardware" screen, as these are required for authentication to work correctly.

Login to your RFS controller and click on **Configuration** at the top



On the left, click **Captive Portals** and choose **Add**



Configure with the below settings:

- **Captive Portal Server Mode:** Internal (Self)
- **Connection Mode:** HTTP
- **AAA Policy:** Click the **Add** icon and enter the name of **guestwifi** before clicking **Continue**

Next, on the RADIUS Authentication tab, click on **Add** and configure with:

- **Host:** *insert radius_server here*
- **Port:** 1812

- **Server Type:** Host
- **Secret:** *insert radius_secret here*

Click **OK** to Add

Settings

Host  rad1.venuewifi.net Hostname ▾

Port  1812 (1 to 65,535)

Server Type  Host ▾

Secret  Show

Request Proxy Mode  None ▾

Request Attempts  3 (1 to 10)

Request Timeout  3 Seconds ▾ (1 to 60)

Retry Timeout Factor  100 (50 to 200)

DSCP  46 (0 to 63)

Network Access Identifier Routing

NAI Routing Enable 

Realm 

Realm Type  Prefix Suffix

Strip Realm 

Next, on the RADIUS Accounting tab, click on **Add** and configure with:

- **Host:** *insert radius_server here*
- **Port:** 1813
- **Server Type:** Host
- **Secret:** *insert radius_secret here*

Click **OK** to Add

Next, on the **Settings** tab, configure with:

- **Protocol:** PAP
- **Accounting Packet Type:** Start/Stop
- **Request Interval:** 3 Minutes
- **Accounting Server Preference:** Prefer Same Authentication Server Host
- **Format:** Dash Delimiter
- **Case:** Uppercase

- **Attributes:** All

AAA Policy default-external ?

RADIUS Authentication
RADIUS Accounting
Settings

RADIUS Authentication

Protocol for MAC, Captive-Portal Authentication i
 PAP
 CHAP
 MS-CHAP
 MS-CHAPv2

RADIUS Accounting

Accounting Packet Type i Start/Stop ▼

Request Interval i (1 to 60)

Accounting Server Preference i Prefer Same Authentication Server Host ▼

RADIUS Address Format

Format i Dash Delimiter (aa-bb-cc-dd-ee-ff) ▼

Case i Uppercase ▼

Attributes i All ▼

Server Pooling

Server Pooling Mode i
 Failover
 Load Balanced

EAP Wireless Client Settings

Client Attempts i (1 to 10)

Request Timeout i (1 to 60 seconds)

ID Request Timeout i (1 to 60 seconds)

Retransmission Scale Factor i (50 to 200)

- **Access Type:** RADIUS Authentication
- **Client Access Time:** 1440
- **Inactivity Timeout:** 30
- **DNS Whitelist:** Click on the **Add** icon and enter a name of **guestwifi**

You will now need to add each of the below domains by clicking in to the DNS Entry column and typing in each domain, clicking **Add Row** after each one. E.g:

- **DNS Entry:** *insert access_domain here*

- **Type:** Hostname
- **Match Suffix:** Yes

Please add all the domains below in the same way:

www.google.com

www.google.co.uk

google-analytics.com

venuewifi.com

openweathermap.org

cloudfront.net

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

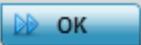
Facebook	Twitter	LinkedIn	Google	Instagram
facebook.com			googleusercontent.com	
fbcdn.net	twitter.com	linkedin.com	googleapis.com	
akamaihd.net	twimg.com	licdn.net	accounts.google.com	instagram.com
connect.facebook.net		licdn.com	gstatic.com	

Name 

DNS Entries

DNS Entry	Match Suffix	
 <input type="text" value="..."/> Hostname 	Yes 	

 Add Row

 OK

Click **OK** when finished adding all the domains.

- **Enable RADIUS Accounting:** Ticked

Settings

Captive Portal Server Mode  Internal (Self) Centralized Centralized Controller

Hosting VLAN Interface    (0 to 4,096)

Captive Portal Server  

Connection Mode  HTTP HTTPS

Simultaneous Users    (1 to 8,192)

Security

AAA Policy   

Access

Access Type No authentication required  Generate Logging Record and Allow Access Custom User Information for RADIUS Authentication RADIUS Authentication

RADIUS Lookup Information 

Terms and Conditions page 

Client Settings

Client Access Time    (30 to 10,080 minutes)

Inactivity Timeout   (5 to 1,440)

DNS Whitelist

DNS Whitelist   

Accounting

Enable RADIUS Accounting 

Enable Syslog Accounting 

Syslog Host  

Syslog Port   

Data Limit

Limit    (1 to 102,400 MegaBytes)

 OK

Press **OK** to Save

Next, click on the **Web Page** tab and configure with the following:

Web Page Source: Externally Hosted

Login URL: *insert access_url

here*?login_ip=WING_TAG_CP_SERVER&motoapmac=WING_TAG_AP_MAC&client_mac=WING_TAG_CLIENT_MAC&random=

Welcome URL: *insert redirect_url here*&random=

Fail URL: *insert access_url here*?res=failed&random=

Captive Portal Policy guest-wifi

Basic Configuration Web Page

Web Page Source Internal Advanced Externally Hosted

Login URL	*_TAG_CLIENT_MAC&random=
Agreement URL	
Welcome URL	s/?res=success&random=
Fail URL	:t/access/?res=failed&random=

A set of pre-existing web pages outside of the Controller are specified by the provided URLs. Four separate URLs point to external web pages for: Logging the user in, Welcoming the user after logging in successfully and Informing the user of a failed login attempt.

Click **OK** to Save

Next, click on **Configuration** at the top and choose the **Wireless** sub-tab underneath.

Click on **Add** and configure with the following:

Basic Configuration

- **SSID:** Guest WiFi (or whatever you wish)
- **WLAN Status:** Enabled
- **Broadcast SSID:** Ticked

WLAN  Guest WiFi

Basic Configuration

Security

Firewall

Client Settings

Accounting

Client Load Balancing

Advanced

Auto Shutdown

WLAN Configuration

SSID  Guest WiFi

Description 

WLAN Status  Disabled Enabled

QoS Policy  default  

Bridging Mode  Local

Other Settings

Broadcast SSID 

Answer Broadcast Probes 

VLAN Assignment

Single VLAN VLAN Pool

 VLAN

RADIUS VLAN Assignment

Allow RADIUS Override 

Security:

- **Authentication:** PSK / None
- **Captive Portal Enforcement:** Captive Portal Enable (Ticked)
- **Captive Portal Policy:** guestwifi
- **Select Encryption:** Open

Select Authentication

EAP EAP-PSK EAP-MAC MAC Kerberos PSK / None

Kerberos Configuration Settings

AAA Policy i <none> ▼

Reauthentication i 30 (30 to 86,400)

Captive Portal

Enforcement i Captive Portal Enable Captive Portal if Primary Authentication Fails

Captive Portal Policy ✎ guestwifi ▼ + ⚙

MAC Registration

Enable i

Radius Group Name i

Expiry Time i 1500 (1 to 1,500 days)

External Controller

Enable i

Host i Hostname ▼

Proxy Mode i None ▼

Select Encryption

i WPA/WPA2-TKIP WEP 128 WEP 64 Open
 WPA2-CCMP KeyGuard

Click **OK** to Save

At the top right, click on **Commit** and **Save**