



Introduction

This document describes how ZoneDirector support Wi-Fi hotspot service with Radio Jungle AAA through WISPr based features: universal authentication method or UAM (browser based login at a captive portal).

RadioJungle AAA appliance is a highly flexible and configurable RADIUS server based on FreeRADIUS v2.x with web-based management GUI developed by 3TSolutions s.r.l.

RadioJungle AAA provides the professional and easy to use solution to control your network access and track the activities of users in the network.

Terminology

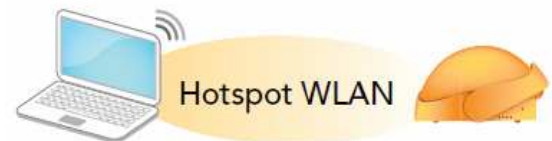
- **Hotspot client:** A wireless client (device) associating with (which is typically encrypted) hotspot service.
- **Hotspot user:** A human being using the hotspot service on the hotspot client.
- **Login page:** The web page which is hosted on an external Hotspot WLAN HTTP server for user login.
- **Logout page:** The web page which is hosted on an external HTTP server for user logout.
- **WISP:** Wireless Internet Service Provider.
- **UAM (Universal Authentication Method):** The UAM allows a subscriber to access and login to WISP services with just a Wi-Fi network interface and Internet browser on the user's device.
- **Authenticated users:** The users who pass the authentication.
- **Unauthenticated users:** The users who have not passed authentication or have failed authentication.

- **Walled garden:** The purpose of the walled garden is to let unauthenticated users access online registration, payment services, or other websites (such as a hotel reservation page) without needing to login first. All other sites are off limits.

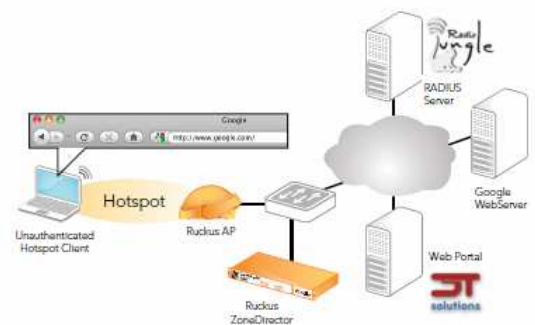
- **WISPr and Hotspot Service:** For our implementation of hotspot service is based on WISPr. In this document, WISPr Service and Hotspot Service are interchangeable. In some sense, hotspot is generic while WISPr is technically defined.

How a Wi-Fi Hotspot Works

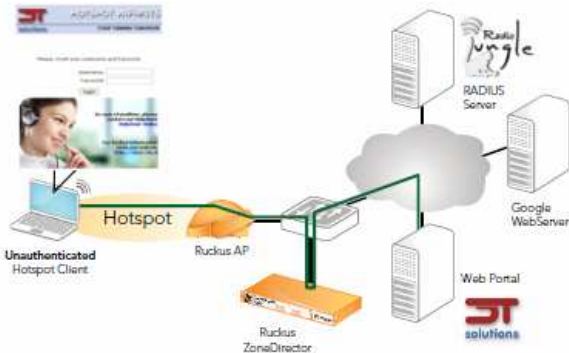
1. Hotspot client associates with the hotspot WLAN (which is typically open).



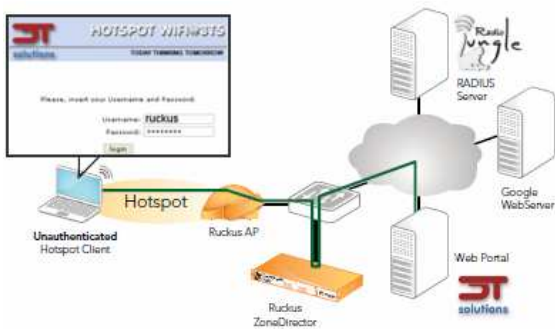
2. The hotspot user tries to browse the web on the hotspot client by going to www.google.com



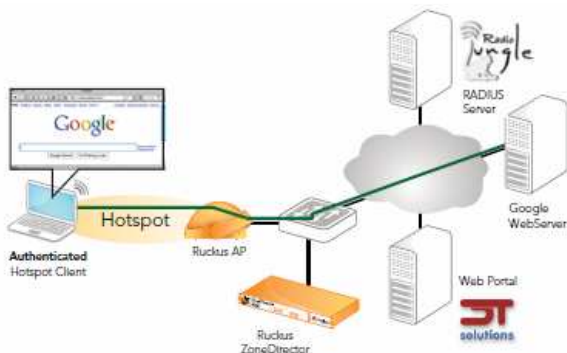
3. The hotspot user is re-directed to the [3TSolutions](http://3TSolutions.com) Web Portal server by the Ruckus ZoneDirector.



4. After the hotspot user types in authentication information, the information is sent to the UAM server on the Ruckus ZoneDirector (1), the ZoneDirector then sends the access request to the RADIUS server [RJAAA](http://RadioJungle.com) (2), the RADIUS server RJAAA then responds back to the ZoneDirector with an accept/reject message (3).



5. After the user is authenticated, they will be redirected to their original web page they requested. Optionally, administrators can redirect them to another appropriate web page (such as an airport homepage for example).



ZoneDirector Setup

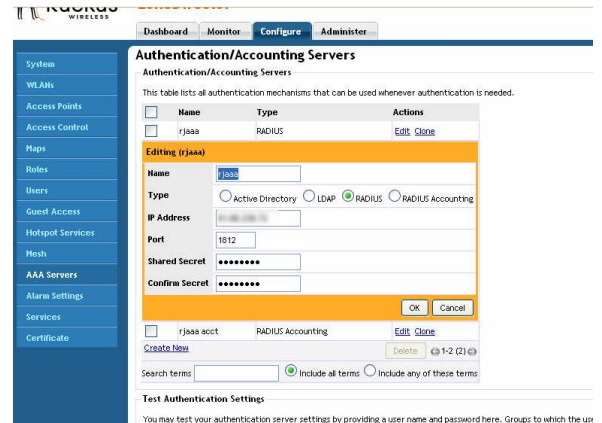
4.1 Requirements

- External Web Server (Apache, IIS or equivalent) with a properly configured login portal page (if interested in 3TSolutions Captive Portal please contact us by [email](mailto:info@3tsolutions.com)).

- RADIUS authentication and accounting server (RADIUS RJAAA is recommended).

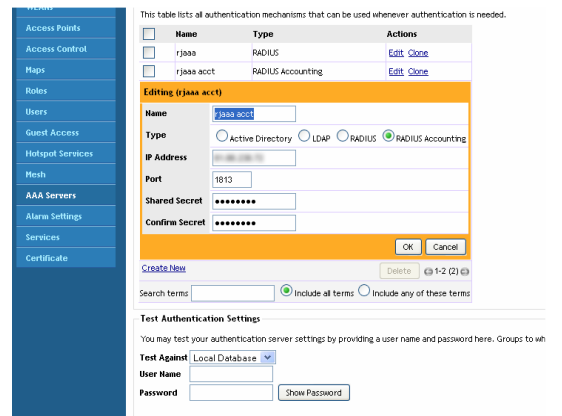
4.2 Configure AAA server on the ZoneDirector

- Under the Configure ---> AAA server sections, enter appropriate settings for your AAA server and for your RADIUS Accounting server. [RJAAA](http://RadioJungle.com) is also available as Remote RADIUS server.



4.3 Configure RADIUS accounting server on the ZoneDirector

- Under the Configure ---> AAA server sections, enter appropriate settings for your RADIUS accounting server.



4.4 Create a hotspot service

- Under the Configure ---> Hotspot services section, enter appropriate settings to create the new hotspot service.

An example of [Captive portal](#) is available at 3TSolutions Web site

- **Name:** Enter a descriptive name for the hotspot service here.
- **Login Page:** Unauthenticated users are redirected to this login page. It must be a valid URL. The ZoneDirector will redirect HTTP requests from all unauthenticated users to this login page. This URL will be added to the walled garden by the ZoneDirector automatically.
- **Start page:** The administrator has the option to allow, after authentication, the hotspot client to be redirected to the original URL that the user intended to visit or to another URL. For example: The user originally requested www.google.com, and was redirected to the login page because they were unauthenticated. After successful authentication if “redirect to the URL that the user intends to visit” is selected that user will be redirected to www.google.com. If “redirect to the following URL” is selected then the user will be redirected to URL specified in the field (a hotel homepage for example).
- **Session timeout:** If selected, the user is automatically disconnected after session time is elapsed. Re-authentication is required after session timeout. If RADIUS session timeout attribute is included in RADIUS Access Accept for specific user, the user’s maximum session time shall be the value of the attribute.

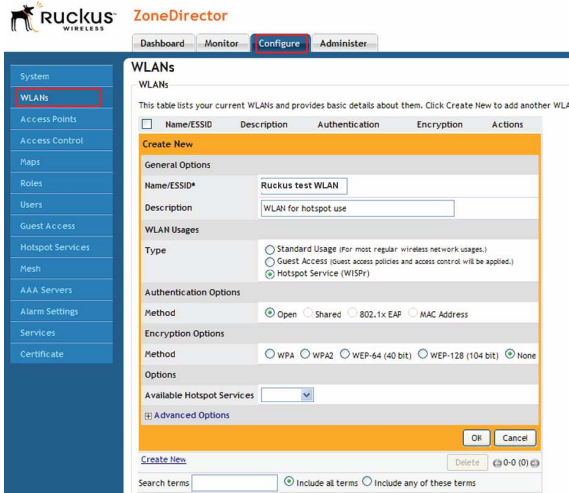
- **Idle timeout:** If selected, the user is automatically disconnected if there is no traffic between the client and AP for specified amount of time. Re-authentication is required after idle timeout. The idle timeout period is implemented at 10-minute intervals. If you set idle timeout to 12 minutes, ZoneDirector will terminate sessions that are idle for 20 minutes. Likewise, if you set idle timeout to 5 minutes, ZoneDirector will terminate sessions that are idle for 10 minutes. If RADIUS idle timeout attribute is included in RADIUS Access Accept, the user’s maximum idle time shall be the value of the attribute.

- **Authentication server:** Choose the AAA server you configured earlier.

- **Accounting server:** Choose the RADIUS accounting server you configured earlier. Choose an interim-update interval between 2-120 minutes. The interim-update interval determines how often the ZoneDirector sends updates to the RADIUS accounting server. If using a RADIUS accounting server, note that the following information is tracked: Login/logout timestamp, Total session time, Bytes sent/received, Packets sent/received.

4.5 Create hotspot WLAN

- Under the Configure ---> WLAN section, enter appropriate settings to create a WLAN that uses the hotspot service.
- **Name/ESSID:** Enter the desired wireless network name. This is how a hotspot user will identify your network when connecting wirelessly.
- **Description:** Enter a descriptive name for your convenience. Type: Choose “Hotspot service” to enable the WLAN for hotspot use.
- **Authentication:** “Open” is the only available option. Authentication will automatically be handled through the UAM and AAA server.

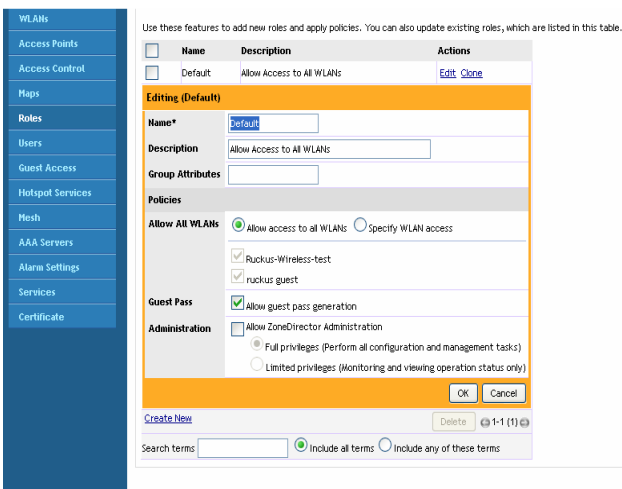


- **Encryption method:** "None" is the default setting and is recommended for most hotspot networks for ease of use. For hotspot networks where encryption is required, WPA/ WPA2 and WEP are supported. Keep in mind the hotspot user will need to enter a valid encryption key first before they can associate to the network, and additionally will need to login to the hotspot service after association.

- **Available Hotspot Service:** Select the Hotspot Service you created earlier.

4.6 Configure Group Roles

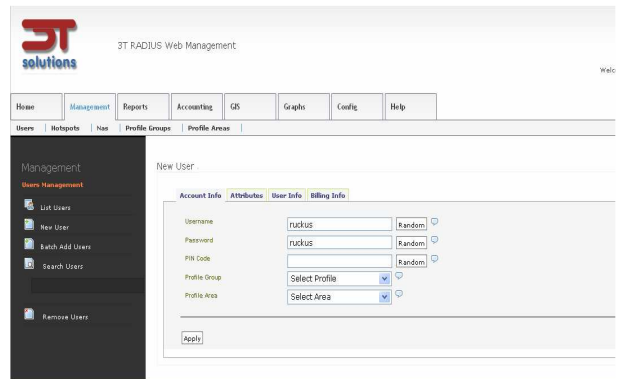
- Under the Configure ---> Roles, make sure that the role that your users belong to are allowed access either to all WLANs, or at least to the specific hotspot WLAN you just created.



RadioJungle AAA RADIUS Setup example

5.1 User creation

Opening the management in RadioJungle AAA interface, you can create a new account with user/password and specifying WISPr attributes.



5.1 User Accounting

Accounting menu shows on the top a summary of all user's sessions and in the bottom a detailed row of each session for selected user.

