APPLICATION NOTE

Enabling WISPr (Hotspot Services) in the ZoneDirector

Introduction

This document describes the WISPr support (hotspot service) for ZoneDirector.

WISPr (pronounced "whisper", stands for Wireless Internet Service Provider Roaming, is a draft protocol submitted to the Wi-Fi Alliance allowing for hotspot service.

The ZoneDirector delivers several WISPr-based features: universal authentication method or UAM (browser-based login at a captive portal), walled garden, time-based user session control, and additional RADIUS attributes for some hotspot service settings.

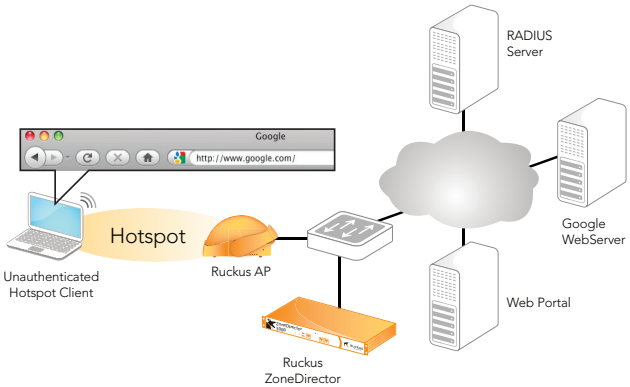
Terminology

- **Hotsp ot client:** A wireless client (device) associating with 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 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.
- **UAM login URL:** The URL that is served (handled) by Zone Director for user login.
- **UAM logout URL:** The URL that is served (handled) by Zone Director for user logout.
- **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.

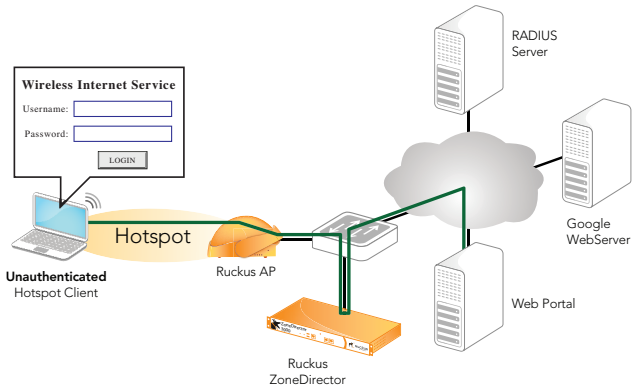
How WISPr Works

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

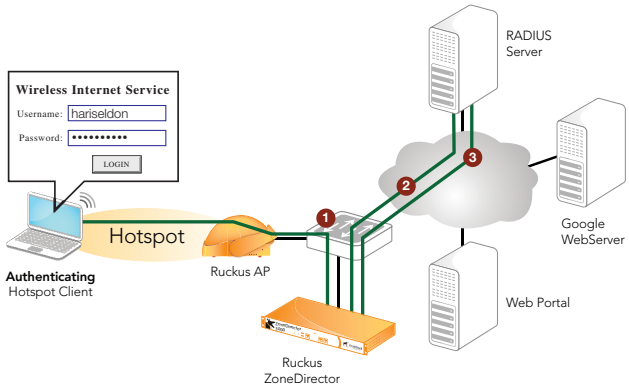
2. The hotspot user tries to browse the web on the hotspot client by going to www.google.com



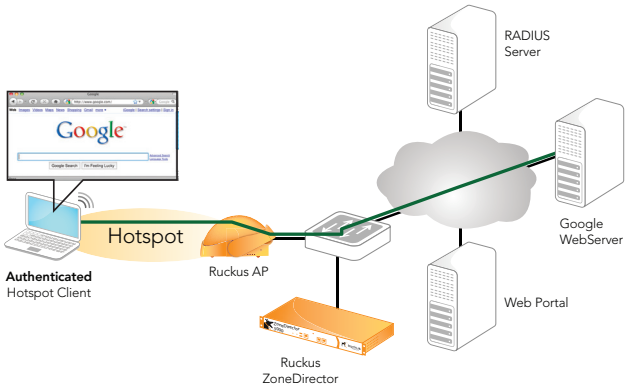
3. The hotspot user is re-directed to the Web Portal server by the Ruckus ZoneDirector



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 (2), the RADIUS server 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).



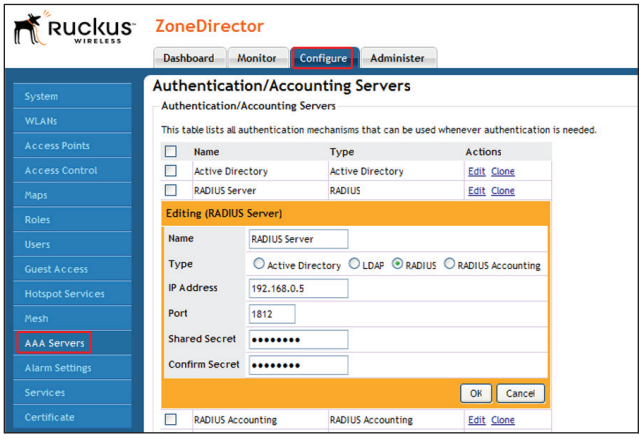
ZoneDirector Setup

4.1 Requirements

- External Web Server (Apache, IIS or equivalent) with a properly configured login portal page. *(See Section 5 for web page setup information)*
- Local Directory, Active Directory, LDAP or RADIUS authentication server (RADIUS is recommended)
- RADIUS accounting server (optional)

4.2 Configure AAA server on the ZoneDirector

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

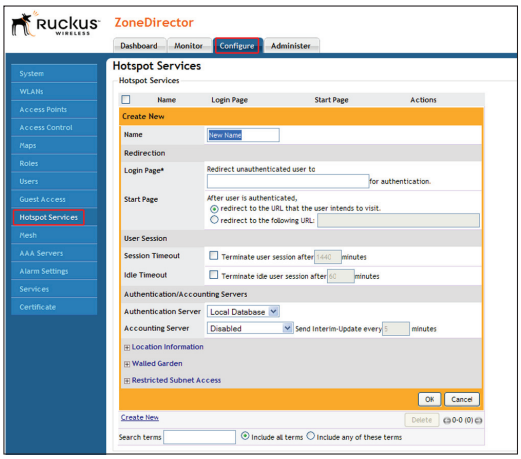


4.3 (Optional) Configure RADIUS accounting server on the ZoneDirector

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

4.4 Create a hotspot service

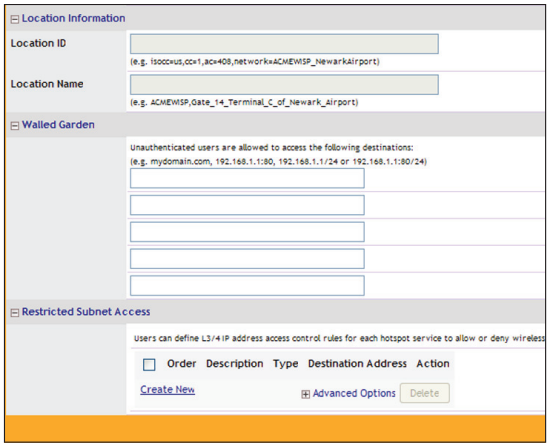
- Under the Configure ---> Hotspot services section, enter appropriate settings to create the new hotspot service.



- **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 (optional):** 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

4.4.1 Advanced hotspot settings

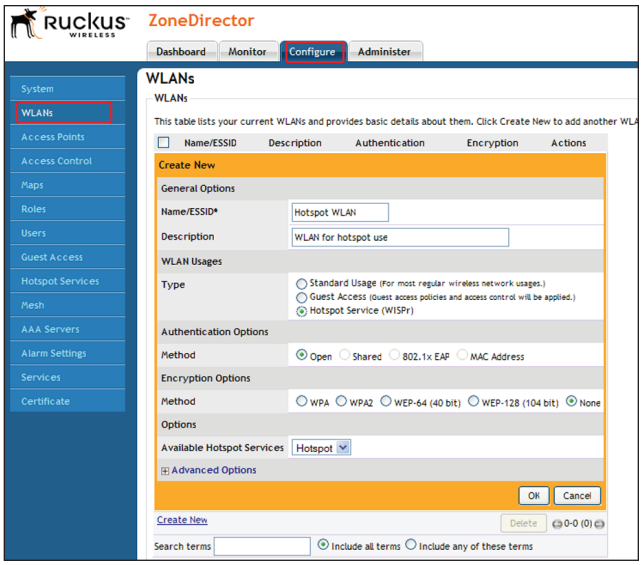
- By clicking on "Location Information", "Walled Garden", or "Restricted Subnet Access" additional settings can be accessed.



- Enter optional attributes for Location ID and Location Name which will be sent to RADIUS accounting server. Administrators can use these additional fields to provide vendor and location-specific information to the RADIUS accounting server.
- **Walled Garden:** Enter destinations that unauthenticated hotspot users are allowed to access to. The walled garden is only effective for unauthenticated users. Entries can be in domain name, IP address, or subnet format. *(e.g., mydomain.com, mydomain.com:80, mydomain.com/24, mydomain.com:80/24, 192.168.0.100, 192.168.0.100:80, 192.168.0.100/24 or 192.168.0.100:80/24)*
- **Restricted Subnet Access:** Enter subnets that hotspot users are not allowed to access. This feature is only effective for authenticated users. A valid subnet entry is in the format *192.168.0.0/16*

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.

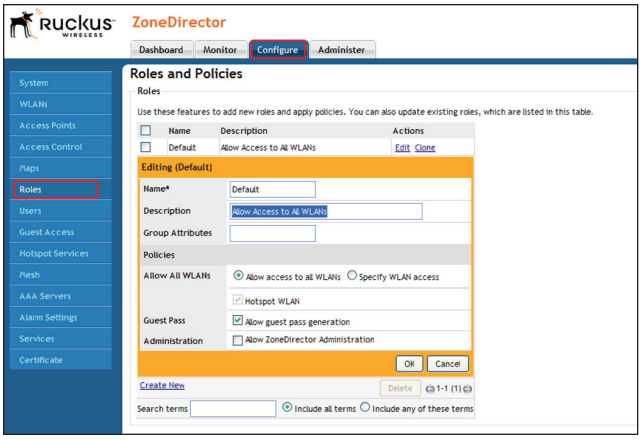


- **Encryption method:** "None" is the default setting and is recommended for most hotspot networks for ease of use. For hotspot networks where encryption is required, WPA/ WPA2 and WEP are supported. Keep in mind the hotspot user will need to enter a valid encryption key first before they can associate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



Web Page Setup

5.1 URL parameters

The following URL parameters are provided. These parameters have no effect on the operation of wireless network:

- sip is the IP address of the Zone Director.
- mac is the MAC address of the access point.
- lid (location id) is the Location Id of the hotspot service. This value can be edited in the hotspot service configuration.
- uip is the client's real IP address. *In L3 local bridge environment, if the gateway for the client NAT the client's traffic, when logging to the hotspot service, the client's IP address will be NAT to the gateway's. In this case, the login request has to include the client's real IP address to be handled properly.*
- dn is the domain name of the ZoneDirector. The domain name is obtained from the certificate of the ZoneDirector when importing the certificate.

  If a start page is specified, 3 URL parameters, uid, mac and url, will be provided:

- mac is the MAC address of the access point.
- uid is the user's login id. (passed in the UAM login form's username parameter)
- url is the user's original requested URL.

5.2 UAM login URL

Zone Director provides the following URL for user login:

- http://director_IP_address:9997/login
- https://director_IP_address:9998/login

The method of HTTP request can be GET or POST. POST is recommended in order to keep the username and password from appearing in the web browser address bar.

Zone Director redirects the user to login page if the authentication is failed.

Zone Director redirects the user to start page if the authentication is successful.

NOTE: Layer 3 AP with NAT
When the AP is in Layer 3 local bridge mode and the client traffic is NATed by a gateway, the ip URL parameter is required. The value of ip is the IP address of the client.

For example:

- http://director_IP_address:9997/login?ip=<client's IP address>
- https://director_IP_address:9998/login?ip=<client's IP address>

5.3 User Login page

A hotspot user uses the login page to login to the hotspot service. The Login page is provided by the Hotspot Service Provider and is hosted on an HTTP server. A typical login page contains a form for username and password. The hotspot user submits the form data to the UAM Login URL for authentication.

5.3.1 Form inputs

Two form inputs, username and password, are required.

The maximum length of username or password is 31 characters.

Basic example for login page:

```
<html>
<head><title>Wireless Internet
Service</title></head>
<body>
<br/><center><h2>Wireless Internet
Service</h2>
<br/><form method=POST action="http://19
2.168.0.76:9997/login">
Username:<input type="text"
name="username">
Password:<input type="password"
name="password">
<input type="submit" value="Login"></
form>
</center>
</body>
</html>
```

In the above example, the system presents the user with a simple form to enter a username and password. Note the example UAM Login URL in this example, http://192.168.0.76:9997/login. The IP address is simply the IP address of the Zone Director. In case you want to use https instead of http take care to change the port number as well. The URL in that case would be: https://192.168.0.76:9998/login

Advanced example for login page:

```
<html>
<head>
<title>Wireless Internet Service</
title>
<script type="text/javascript">
function get_param(name)
{
    if (location.href.indexOf("?") >= 0)
{
        var query=location.href.
        split("?")[1];
        var params=query.split("&");
        for (var i = 0; i < params.
        length; i ++) {
            value_pair=params[i].
            split("=");
            if (value_pair[0] == name)
                return
                unescape(value_pair[1]);
        }
    }
    return "";
}
</script>
</head>
<body>
<center>
<h2>Wireless Internet Service</h2>
<script type="text/javascript">
document.write('<form method=POST
action="http://' + get_param("sip") +
':9997/login">');
</script>
Username:<input type="text"
name="username">
Password:<input type="password"
name="password" >
<input type="submit" value="Login">
</form>
</center>
</body>
</html>
```

In the above example, the system presents the user with a simple form to enter a username and password. Note the example UAM Login URL in this example, http://192.168.0.76:9997/login. The IP address is simply the IP address of the Zone Director. In case you want to use https instead of http take care to change the port number as well. The URL in that case would be: https://192.168.0.76:9998/login

5.4 Start page

After user is authenticated, the user can be redirected to the start page if setup in the hotspot service configuration (See 4.3)

The administrator can use the supplied URL parameters to provide some advanced features within this start page:

Advanced example for start page:

```
<html>
<head>
<title>Redirect</title>
<script type="text/javascript">
function get_param(name)
{
    if (location.href.indexOf("?") >= 0)
{
        var query=location.href.
        split("?")[1];
        var params=query.split("&");
        for (var i = 0; i < params.
        length; i ++) {
            value_pair=params[i].
            split("=");
            if (value_pair[0] == name)
                return
                unescape(value_pair[1]);
        }
    }
    return "";
}

var location_content={"001f41eacbc9":
"http://www.flysfo.com"};

function redirect(){
    var mac=get_param("mac");
    if (mac in location_content)
        window.location.href=
        location_content[mac];
    else
        window.location.href="http://www.
        google.com";
}
</script>
</head>
<body onLoad="setTimeout(redirect,
500);">
</body>
</html>
```

The above example illustrates how to use one of the parameters (in this case the "mac" parameter) to customize where the hotspot user is forwarded to. If the MAC address of the hotspot client is 001f41eacbc9, then they are sent to http://www.flysfo.com, otherwise, they are sent to http://www.google.com.

5.4.1 HTTPS redirection

Due to the nature of HTTPS traffic, there might be confusion over the redirection of HTTPS. The ZoneDirector attempts to redirect possible HTTP traffic while in restricted mode by redirecting traffic destined not only to port 80, but also to ports 443, 3128 and 8080.

It is important to be aware that if an unauthenticated user tries to first go to a secure website (such as https://www.hsbc.com) and is then redirected to the UAM server, the subsequent redirection to the originally requested secure website will fail with a browser message similar to "Secure Connection Failed".

Suggested workaround: Redirect users to a non-secure website (such as a hotel front-page), from there, the user can manually go to the secure website of their choice.

5.5 User Logout Page

Hotspot users can logout of the hotspot service via a logout page. A typical logout page contains a link to the UAM logout URL. The user clicks the link to logout of the hotspot service. After the user is logged out, the browser is redirected to the login page.

Zone Director provides the following URLs for user logout:

- http://director_IP_address:9997/logout
- https://director_IP_address:9998/logout

Example for logout page:

```
<html>
<head><title>Wireless Internet
Service</title></ head>
<body>
<a href="http://192.168.0.76:9997/
logout">Logout Hotspot</a>
</body>
</html>
```

NOTE: Layer 3 AP with NAT
When the AP is in Layer 3 local bridge mode and the client traffic is NATed by the gateway, the ip URL parameter is required. The value of ip is the IP address of the client.

For example:

- http://director_IP_address:9997/logout?ip=<client's IP address>
- https://director_IP_address:9998/logout?ip=<client's IP address>

RADIUS Accounting Reference

6.1 User Logout Page

In ZD-managed network, ZD plays the role of RADIUS client, which is responsible for sending Accounting Request. The events to trigger Accounting Request with different Acct-Status-Type are listed as follows.

- ZD sends Accounting-On to external RADIUS server when an AP joins.
- ZD sends Accounting-Off when an AP leaves. Thus the AP restart operation triggers Accounting-Off and then Accounting-On.
- ZD sends Accounting-Start and Accounting-Stop when a client associates and disassociates respectively.
- ZD periodically sends Interim-Update for an associated client.

6.1.1 Attributes Description

Most attributes valid in RADIUS Access-Request or Access-Accept packet are also valid in RADIUS Accounting-Request packet. These attributes used in our RADIUS Accounting-Request packet are listed as follows. To know attribute definition more detailed, please refer to RFC 2866 [2].

Attribute	Description
Mandatory Attributes	
Acct-Status-Type	This attribute indicates Accounting-Start, Accounting-Stop, Interim-Update, Accounting-On, or Accounting-Off.
Acct-Session-Id	This is a unique Accounting ID to match Accounting-Start and Accounting-Stop records.
Acct-Authentic	This attribute indicates how the STA was authenticated. In our system, its value is always RADIUS.
Optional Attributes	
NAS-IP-Address	This attribute indicates the ZD's IP address.
NAS-Identifier	This attribute indicates BSSID, that is to say, the WLAN's MAC address.
Location-ID	See section 4.4.1
Location-name	See section 4.4.1
Calling-Station-Id	This attribute indicates the STA's MAC address.
Attributes only included in Accounting-Stop	
Acct-Input-Octets	This attribute indicates how many octets the STA has received.
Acct-Input-Packets	This attribute indicates how many packets the STA has received.
Acct-Output-Octets	This attribute indicates how many octets the STA has transmitted.
Acct-Output-Packets	This attribute indicates how many packets the STA has transmitted.
Acct-Session-Time	This attribute indicates how many seconds the STA has associated to Ruckus ZD-managed network.

Ruckus Wireless, Inc.
880 West Maude Avenue, Suite 101, Sunnyvale, CA 94085 USA (650) 265-4200 Ph \ (408) 738-2065 Fx