



## How to Configure a SmartZone WLAN for Cloudpath

Technical Note

## Copyright Notice and Proprietary Information

Copyright 2017 Ruckus Wireless, Inc. All rights reserved.

No part of this documentation may be reproduced, transmitted, or translated, in any form or by any means, electronic, mechanical, manual, optical, or otherwise, without prior written permission of Ruckus Wireless, Inc. ("Ruckus"), or as expressly provided by under license from Ruckus.

### Destination Control Statement

Technical data contained in this publication may be subject to the export control laws of the United States of America. Disclosure to nationals of other countries contrary to United States law is prohibited. It is the reader's responsibility to determine the applicable regulations and to comply with them.

### Disclaimer

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN ("MATERIAL") IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

### Limitation of Liability

IN NO EVENT, SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIAL.

### Trademarks

Ruckus Wireless is a trademark of Ruckus Wireless, Inc. in the United States and other countries. All other product or company names may be trademarks of their respective owners.

### Table of Contents

<b>Overview .....</b>	<b>5</b>
<b>Cloudpath Context .....</b>	<b>5</b>
<b>Requirements for this Document.....</b>	<b>5</b>
<b>Summary of Steps .....</b>	<b>5</b>
<b>Ruckus Cloudpath Configuration Settings .....</b>	<b>6</b>
<b>Step 1: Obtain the FQDN/IP Address.....</b>	<b>6</b>
<b>Step 2: Obtain the RADIUS Shared Secret.....</b>	<b>7</b>
<b>Step 3: Obtain the WLAN Redirect URL .....</b>	<b>8</b>
<b>Ruckus vSZ-E/SmartZone 100 Configuration Settings.....</b>	<b>9</b>
<b>Step 4a: Configure the Authentication Server.....</b>	<b>9</b>
<b>Step 5a: Create a Hotspot (WISPr) Service .....</b>	<b>10</b>
<b>Step 6a: Create a Walled Garden .....</b>	<b>10</b>
<b>Step 7a: Create an Open SSID (for Onboarding) .....</b>	<b>11</b>
<b>Step 8a: Create a Secure SSID .....</b>	<b>12</b>
<b>Ruckus vSZ-H/SCG 200 Configuration Settings.....</b>	<b>13</b>
<b>Step 4b: Configure the Authentication Server.....</b>	<b>13</b>
<b>Step 5b: Configure the Authentication Profile.....</b>	<b>14</b>
<b>Step 6b: Create a Hotspot (WISPr) Service .....</b>	<b>15</b>
<b>Step 7b: Create a Walled Garden .....</b>	<b>16</b>
<b>Step 8b: Create an Open SSID (for Onboarding).....</b>	<b>17</b>
<b>Step 9b: Create a Secure SSID.....</b>	<b>18</b>
<b>Summary .....</b>	<b>19</b>
<b>About Ruckus .....</b>	<b>20</b>
<b>Copyright 2017 Ruckus Wireless, Inc. All Rights Reserved. ....</b>	<b>20</b>

## Intended Audience

This document provides an overview of how to configure the Ruckus SmartZone controller with a WLAN that supports Cloudpath. Some knowledge of Wi-Fi and SmartZone and Cloudpath configuration is recommended.

## Overview

This document provides a step-by-step guide to configuring a WLAN in the Ruckus SmartZone controllers for the Cloudpath Enrollment System. The reader is expected to be reasonably familiar with the Ruckus SmartZone platform as well as the Cloudpath ES.

There are four manifestations of the Ruckus SmartZone controller platform:

- Appliances: SmartZone SZ100, Smart Cell Gateway SCG 200
- Virtual: SmartZone – Essentials (vSZ-E), SmartZone – High Scale (vSZ-H)

The vSZ-E and the SZ100 are similar in their GUI. Likewise with the SCG 200 and vSZ-H. This guide therefore has two sets of instructions: one for each of these like GUI groups.

All of the steps and screenshots in this document are for SmartZone version 3.4.1.208.

## Cloudpath Context

The Cloudpath client onboarding platform calls for two WLANs (SSIDs): Onboarding and Production. The first one is used for onboarding the clients. This is a Hotspot (WISPr) type SSID and it redirects clients to the Cloudpath Enrollment System (ES). After the client is authenticated, a certificate is downloaded and installed on the client. This certificate provides the client with access to the second secure SSID.

## Requirements for this Document

In order to successfully follow the steps in this document, the following equipment (at a minimum) is required and assumed:

- Admin access to the SmartZone controller
- FQDN/IP Address of the Cloudpath Enrollment System
- RADIUS Shared Secret on Cloudpath
- WLAN Redirect URL on Cloudpath

## Summary of Steps

The steps involved in configuring a WLAN for Cloudpath can be summarized as follows:

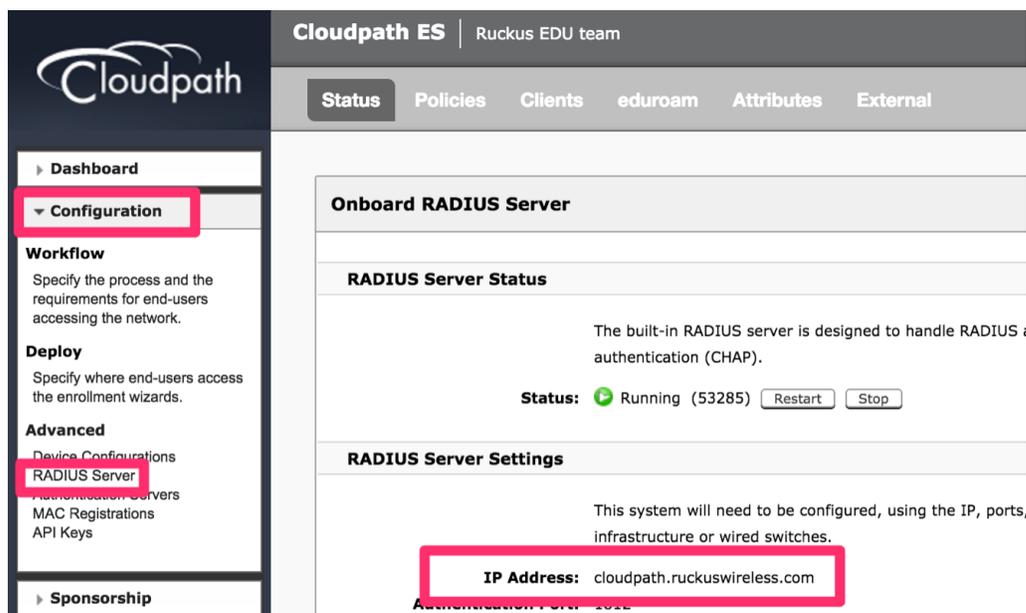
1. Obtain the FQDN/IP address
2. Obtain the RADIUS shared secret
3. Obtain the WLAN Redirect URL
4. Configure AAA Authentication Server
5. Create HotSpot service
6. Set up Walled Garden
7. Create Onboarding SSID
8. Create Secure, Production SSID

## Ruckus Cloudpath Configuration Settings

In the Ruckus Cloudpath Enrollment System, login and make note of the following settings. You will need these parameter values when configuring any of the SmartZone controller platforms.

### Step 1: Obtain the FQDN/IP Address

1. In Cloudpath ES, navigate to the Configuration menu.
2. Under Advanced, select RADIUS Server and record the FQDN or IP in the IP Address field.



The screenshot displays the Ruckus Cloudpath ES web interface. The top navigation bar includes 'Cloudpath ES' and 'Ruckus EDU team'. Below this is a menu with 'Status', 'Policies', 'Clients', 'eduroam', 'Attributes', and 'External'. The left sidebar contains a navigation menu with 'Dashboard', 'Configuration' (highlighted), 'Workflow', 'Deploy', 'Advanced', and 'Sponsorship'. Under 'Advanced', 'RADIUS Server' is highlighted. The main content area is titled 'Onboard RADIUS Server' and contains the following information:

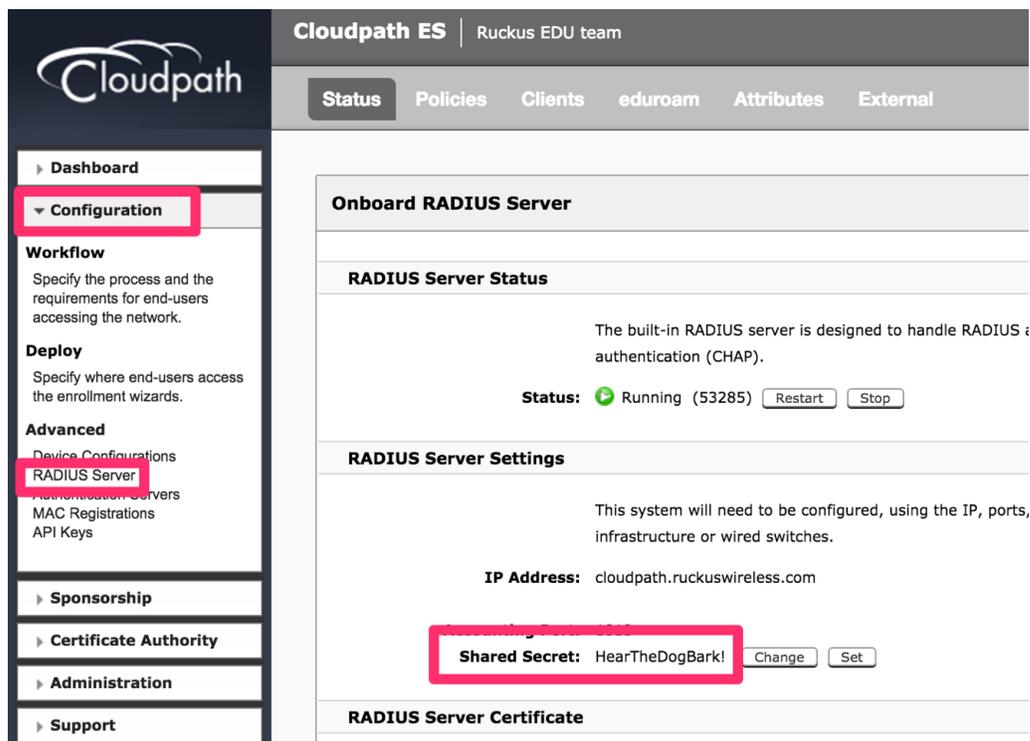
- RADIUS Server Status:** The built-in RADIUS server is designed to handle RADIUS authentication (CHAP). Status: ● Running (53285) [Restart] [Stop]
- RADIUS Server Settings:** This system will need to be configured, using the IP, ports, infrastructure or wired switches.
- IP Address:** cloudpath.ruckuswireless.com

FIGURE 1: RADIUS FQDN/IP ADDRESS

February 2017

### Step 2: Obtain the RADIUS Shared Secret

1. In Cloudpath ES, navigate to the Configuration menu.
2. Under Advanced, select RADIUS Server and record the Shared Secret.



The screenshot displays the Cloudpath ES web interface. The left sidebar shows the navigation menu with 'Configuration' selected. Under 'Advanced', 'RADIUS Server' is highlighted. The main content area is titled 'Onboard RADIUS Server' and includes the following sections:

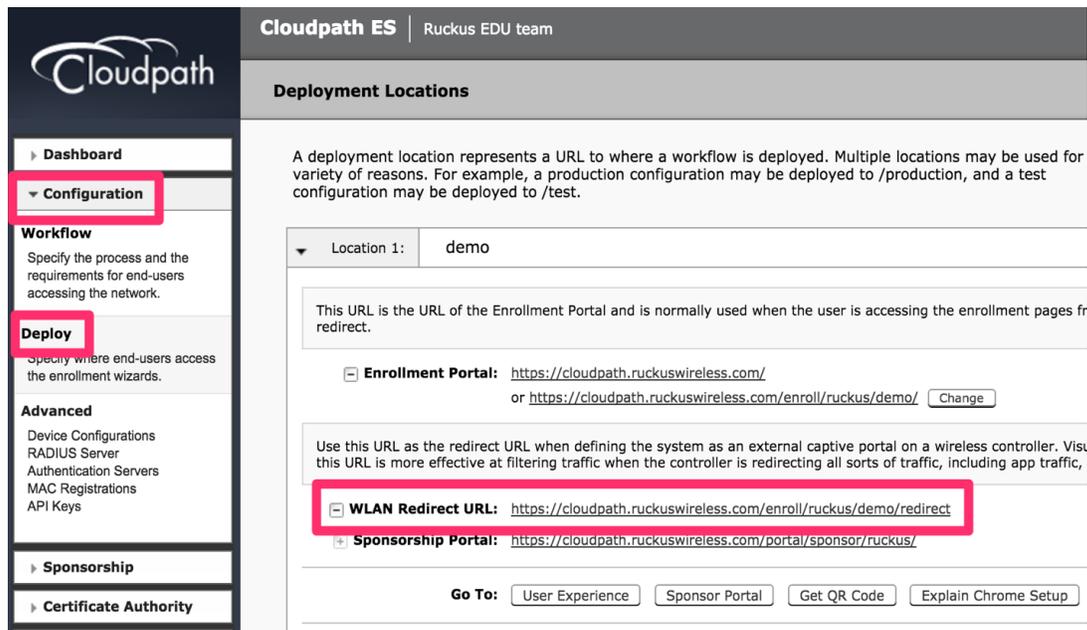
- RADIUS Server Status:** The built-in RADIUS server is designed to handle RADIUS authentication (CHAP). Status: ● Running (53285) with 'Restart' and 'Stop' buttons.
- RADIUS Server Settings:** This system will need to be configured, using the IP, ports, infrastructure or wired switches. IP Address: cloudpath.ruckuswireless.com. Shared Secret: HearTheDogBark! with 'Change' and 'Set' buttons.
- RADIUS Server Certificate:** (Section header only)

FIGURE 2: RADIUS SHARED SECRET

### Step 3: Obtain the WLAN Redirect URL

1. In Cloudpath ES, navigate to the Configuration menu.
2. Under Deploy, record the WLAN Redirect URL.

HotSpot Redirect URL: Obtained from Cloudpath: Configure->Deploy on the Cloudpath Admin UI. See below



The screenshot shows the Cloudpath ES admin interface. The left sidebar contains a navigation menu with items: Dashboard, Configuration (highlighted with a red box), Workflow, Deploy (highlighted with a red box), Advanced, Sponsorship, and Certificate Authority. The main content area is titled 'Deployment Locations' and includes a description of deployment locations. Below this, there is a section for 'Location 1: demo'. It contains two text boxes: one for the Enrollment Portal URL and another for the WLAN Redirect URL. The 'WLAN Redirect URL' field is highlighted with a red box and contains the value: `https://cloudpath.ruckuswireless.com/enroll/ruckus/demo/redirect`. At the bottom, there are 'Go To' buttons for 'User Experience', 'Sponsor Portal', 'Get QR Code', and 'Explain Chrome Setup'.

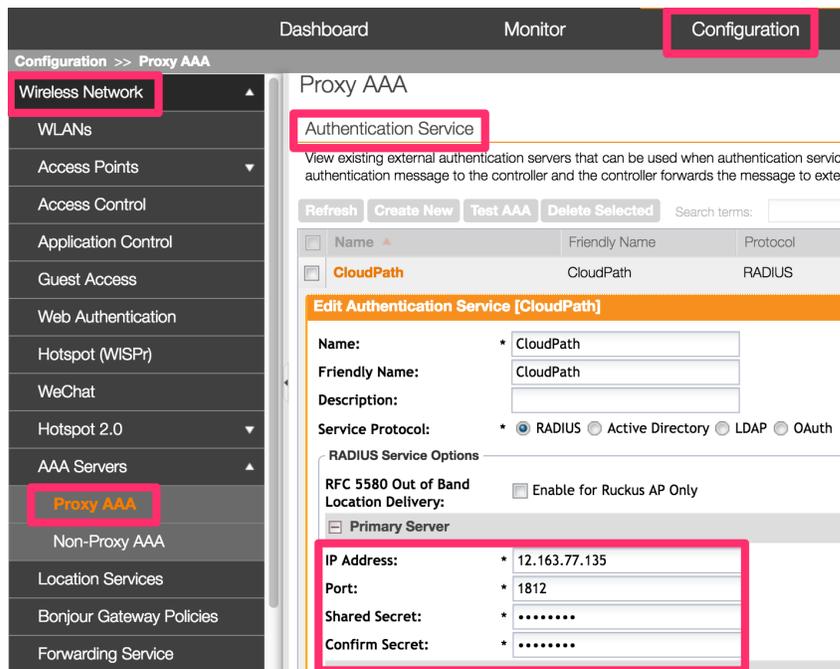
FIGURE 3: WLAN REDIRECT URL

## Ruckus vSZ-E/SmartZone 100 Configuration Settings

For the vSZ-E or SmartZone 100 controller types, use steps 4a through 8a to finish the configuration.

### Step 4a: Configure the Authentication Server

1. Login to the vSZ-E or SmartZone 100 interface with the admin account.
2. Navigate to the Configuration tab.
3. Select Wireless Network.
4. Under AAA Servers, select Proxy AAA.
5. Under Authentication Service, select Create New. Note that you will need the Shared Secret that was obtained from the Cloudpath Enrollment System.



The screenshot displays the Ruckus configuration interface. At the top, there are tabs for 'Dashboard', 'Monitor', and 'Configuration', with 'Configuration' being the active tab. Below the tabs, the breadcrumb path is 'Configuration >> Proxy AAA'. The left sidebar contains a menu with 'Wireless Network' and 'Proxy AAA' highlighted. The main content area is titled 'Proxy AAA' and contains an 'Authentication Service' section. This section includes a table with one entry: 'CloudPath' with a 'RADIUS' protocol. Below the table is an 'Edit Authentication Service [CloudPath]' form. The form fields are: Name (CloudPath), Friendly Name (CloudPath), Description (empty), Service Protocol (RADIUS selected), RADIUS Service Options (RFC 5580 Out of Band Location Delivery: Enable for Ruckus AP Only), Primary Server (checked), IP Address (12.163.77.135), Port (1812), Shared Secret (masked with dots), and Confirm Secret (masked with dots).

FIGURE 4: AUTHENTICATION SERVICE

### Step 5a: Create a Hotspot (WISPr) Service

1. While still in the Configuration tab and the Wireless Network menu, select Hotspot (WISPr).
2. Click Create New. Note that you will need the Redirect URL that was obtained from the Cloudpath Enrollment System.

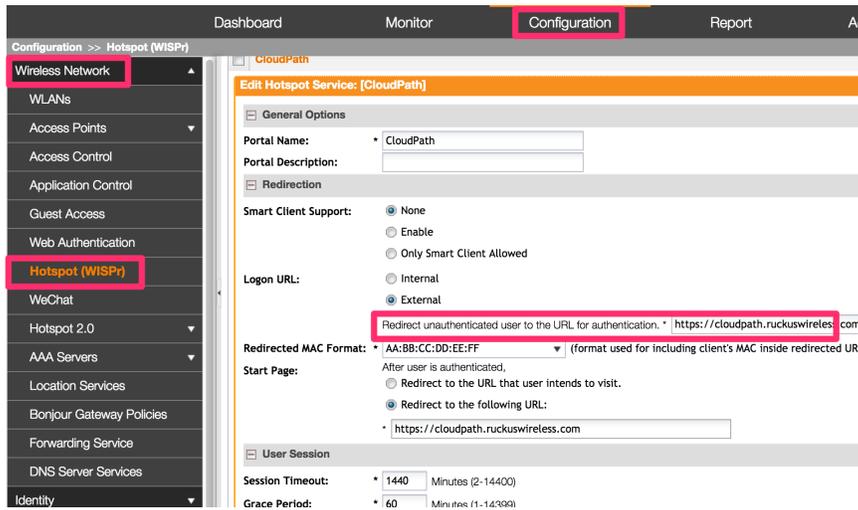


FIGURE 5: HOTSPOT (WISPR) SERVICE

### Step 6a: Create a Walled Garden

1. While still in the Configuration > Hotspot (WISPr) menu, select Walled Garden.
2. For the above-created Hotspot service, include the FQDN/IP address of the Cloudpath ES in the Walled Garden.
3. If OAuth is going to be used for Authentication, then allow access to Google, Facebook and LinkedIn as well.

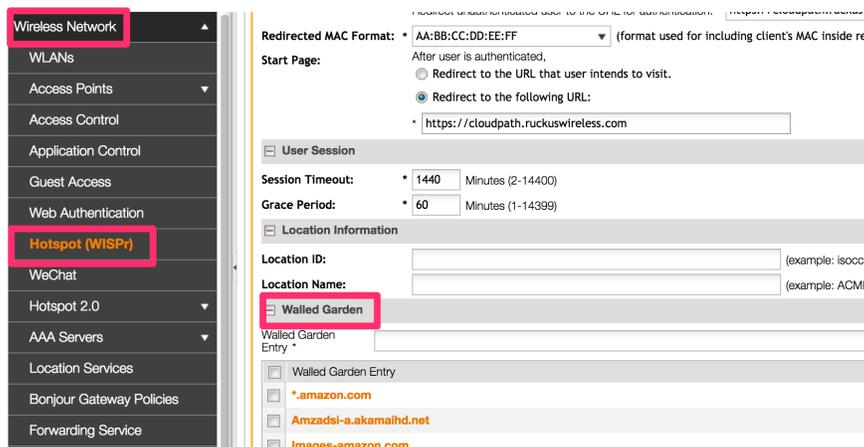


FIGURE 6: WALLED GARDEN CONFIGURATION

### Step 7a: Create an Open SSID (for Onboarding)

1. Under the Configuration > Wireless Network menu, select WLANs.
2. Click Create New.
3. Create a WLAN with the following parameters:
  - o Authentication Type: Hotspot (WISPr)
  - o Authentication Option: Open
  - o Encryption Option: Open
  - o Hotspot (WISPr) Portal: Hotspot service created earlier
  - o Authentication Server: Radius Server created earlier.

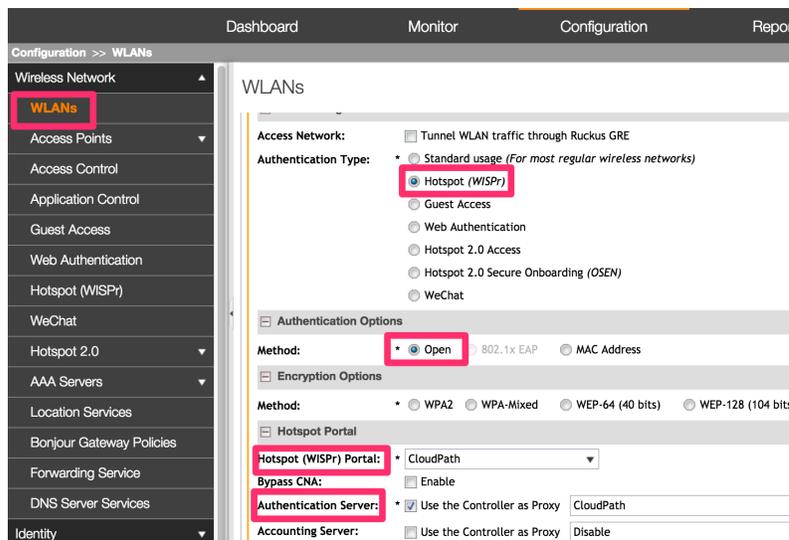


FIGURE 7: OPEN SSID CONFIGURATION

### Step 8a: Create a Secure SSID

1. While still in the Configuration > Wireless Network> WLANs menu, click Create New.
2. Create a WLAN with following parameters:
  - o Authentication Type: Standard Usage
  - o Authentication Option: 802.1x EAP
  - o Encryption Method: WPA2
  - o Algorithm: AES
  - o Authentication Server: Radius Server created earlier.

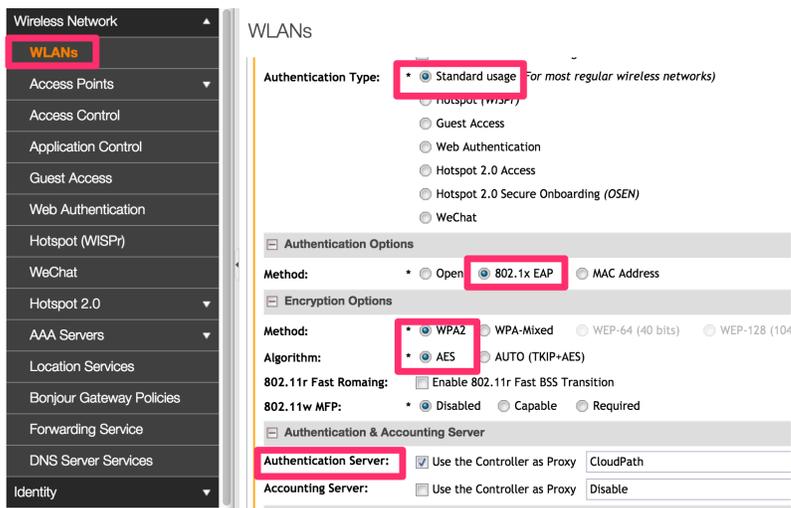


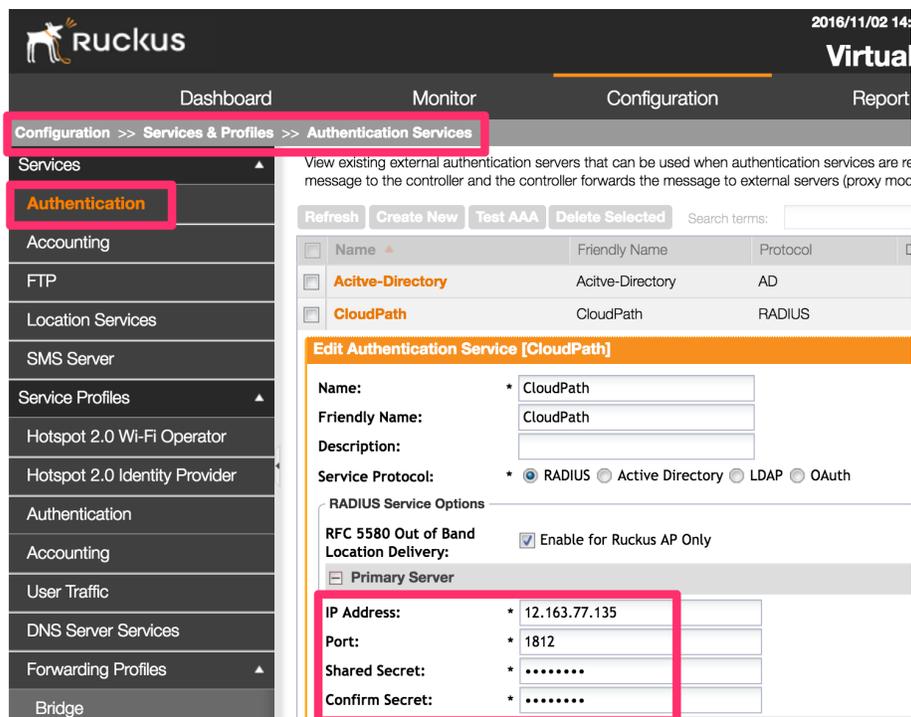
FIGURE 8: SECURE SSID CONFIGURATION

## Ruckus vSZ-H/SCG 200 Configuration Settings

For the vSZ-H or SCG 200 controller types, use steps 4b through 9b to finish the configuration.

### Step 4b: Configure the Authentication Server

1. Login to the vSZ-H or SCG 200 interface with the admin account.
2. Navigate to the Configuration tab.
3. Select Services & Profiles.
4. Under Services, select Authentication.
5. Under Authentication Services, select Create New. Note that you will need the FDCN/IP Address and Shared Secret that was obtained from the Cloudpath Enrollment System.



The screenshot shows the Ruckus configuration interface. The top navigation bar includes 'Dashboard', 'Monitor', 'Configuration', and 'Report'. The 'Configuration' tab is active, and the breadcrumb path is 'Configuration >> Services & Profiles >> Authentication Services'. The left sidebar shows a menu with 'Authentication' highlighted. The main content area displays a table of existing authentication services:

Name	Friendly Name	Protocol
Active-Directory	Active-Directory	AD
CloudPath	CloudPath	RADIUS

Below the table is the 'Edit Authentication Service [CloudPath]' form. The 'Name' field is set to 'CloudPath'. The 'Service Protocol' is set to 'RADIUS'. Under 'RADIUS Service Options', the 'Enable for Ruckus AP Only' checkbox is checked. The 'Primary Server' section is expanded, showing the following fields:

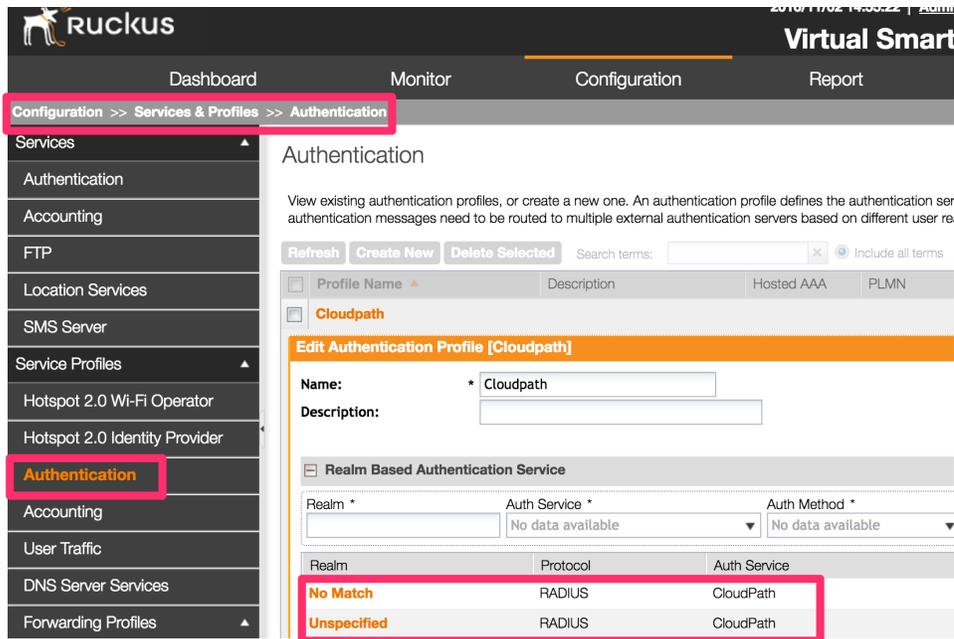
IP Address:	12.163.77.135
Port:	1812
Shared Secret:	.....
Confirm Secret:	.....

FIGURE 9: AUTHENTICATION SERVICE

February 2017

### Step 5b: Configure the Authentication Profile

1. While still in the Configuration tab and the Services & Profiles menu, select Service Profiles.
2. Under Service Profiles, select Authentication.
3. Specify the RADIUS AAA server created in step 5a.



The screenshot shows the Ruckus Virtual SmartZone configuration interface. The navigation menu on the left includes 'Authentication' which is highlighted. The main content area is titled 'Authentication' and shows a table of existing profiles. The 'Cloudpath' profile is selected and its configuration is displayed below. The 'Realm Based Authentication Service' section contains a table with the following data:

Realm	Protocol	Auth Service
No Match	RADIUS	CloudPath
Unspecified	RADIUS	CloudPath

FIGURE 10: AUTHENTICATION PROFILE

February 2017

### Step 6b: Create a Hotspot (WISPr) Service

This is to be done for the AP Zone of interest. Configuration->AP Zones->Select Your Zone-> Hotspot (WISPr) service. The

1. Under the Configuration tab, select the appropriate AP Zone for your configuration.
2. Within your AP Zone, select the Hotspot (WISPr) menu.
3. Click Create New. Note that you will need the Redirect URL that was obtained from the Cloudpath Enrollment System.

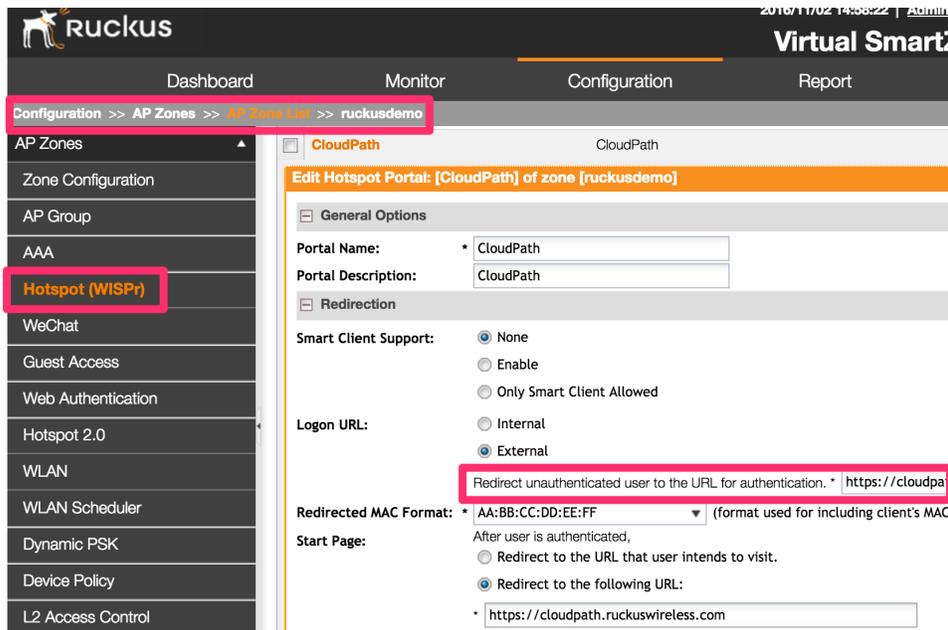
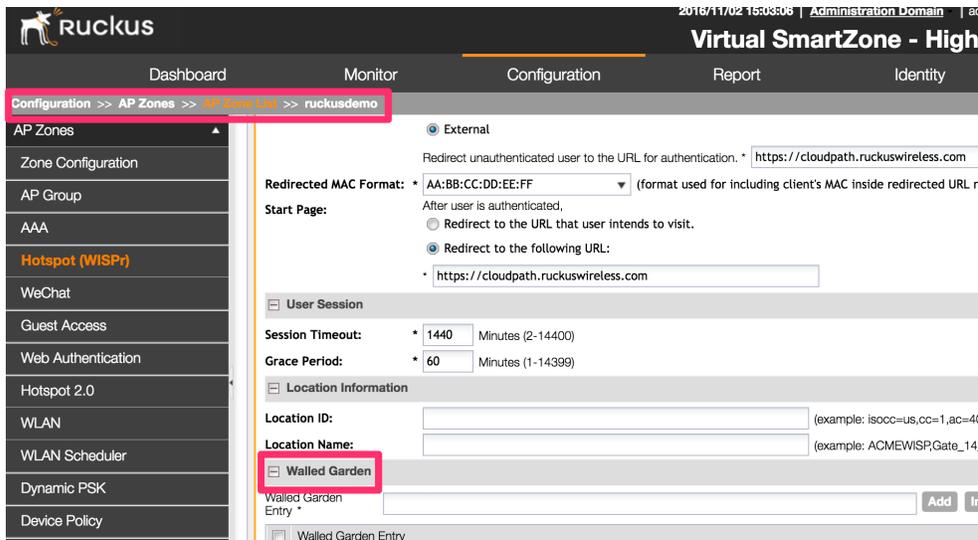


FIGURE 11: HOTSPOT (WISPr) SERVICE

February 2017

### Step 7b: Create a Walled Garden

1. While still in your AP Zone and the Hotspot (WISPr) menu, select Walled Garden.
2. For the above-created Hotspot service, include the FQDN/IP address of the Cloudpath ES in the Walled Garden.
3. If OAuth is going to be used for Authentication, then allow access to Google, Facebook and LinkedIn as well.



The screenshot shows the Ruckus Virtual SmartZone configuration interface. The breadcrumb trail is Configuration >> AP Zones >> AP Zone List >> ruckusdemo. The left sidebar lists various configuration options, with 'Hotspot (WISPr)' selected. The main content area is titled 'Virtual SmartZone - High' and shows the configuration for a Walled Garden. The 'Walled Garden' section is highlighted with a red box. The configuration includes:

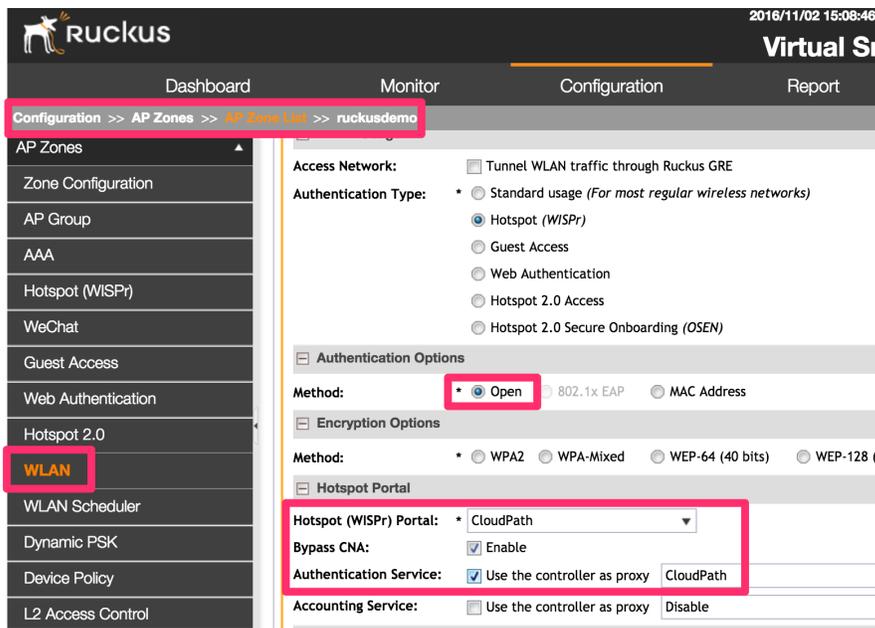
- External** (selected): Redirect unauthenticated user to the URL for authentication:
- Redirected MAC Format**:  (format used for including client's MAC inside redirected URL)
- Start Page**: After user is authenticated,  Redirect to the following URL:
- User Session**:
  - Session Timeout**:  Minutes (2-14400)
  - Grace Period**:  Minutes (1-14399)
- Location Information**:
  - Location ID**:
  - Location Name**:
- Walled Garden** (highlighted):
  - Walled Garden Entry**:
  - Walled Garden Entry

FIGURE 12: WALLED GARDEN CONFIGURATION

February 2017

### Step 8b: Create an Open SSID (for Onboarding)

1. While still in your AP Zone under the Configuration tab, select WLAN.
2. Click Create New.
3. Create a WLAN with the following parameters:
  - o Authentication Type: Hotspot (WISPr)
  - o Authentication Option: Open
  - o Encryption Option: Open
  - o Hotspot (WISPr) Portal: Hotspot service created earlier
  - o Authentication Server: Radius Server created earlier.



The screenshot shows the Ruckus Virtual SmartZone configuration interface. The breadcrumb navigation at the top reads: Configuration >> AP Zones >> AP Zone List >> ruckusdemo. The left sidebar menu has 'WLAN' highlighted. The main configuration area is titled 'Hotspot (WISPr)' and includes the following settings:

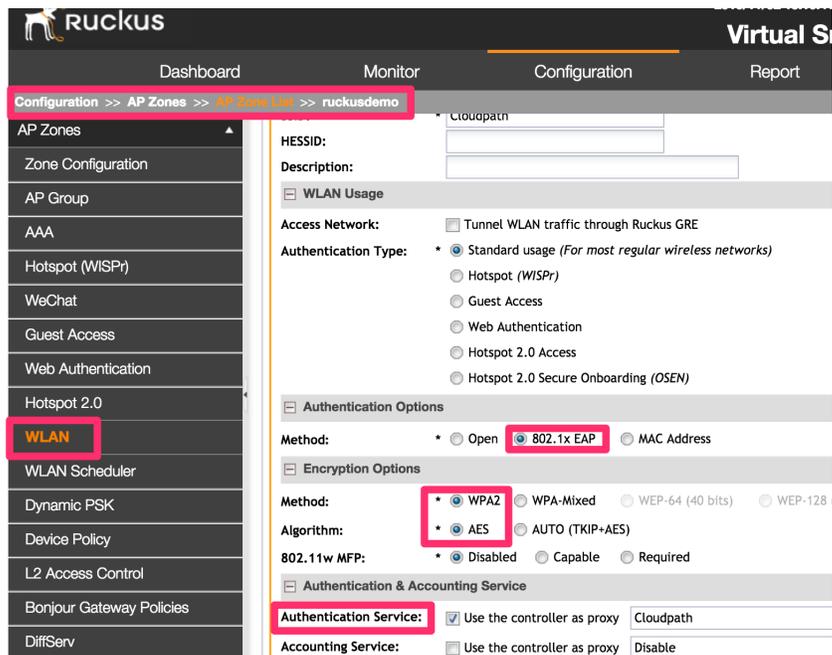
- Access Network:**  Tunnel WLAN traffic through Ruckus GRE
- Authentication Type:**  Standard usage (For most regular wireless networks),  Hotspot (WISPr),  Guest Access,  Web Authentication,  Hotspot 2.0 Access,  Hotspot 2.0 Secure Onboarding (OSEN)
- Authentication Options:**
  - Method:**  Open,  802.1x EAP,  MAC Address
- Encryption Options:**
  - Method:**  WPA2,  WPA-Mixed,  WEP-64 (40 bits),  WEP-128 (40 bits)
- Hotspot Portal:**
  - Hotspot (WISPr) Portal:** CloudPath
  - Bypass CNA:**  Enable
  - Authentication Service:**  Use the controller as proxy, CloudPath
  - Accounting Service:**  Use the controller as proxy, Disable

FIGURE 13: OPEN SSID CONFIGURATION

February 2017

### Step 9b: Create a Secure SSID

1. While still in the Configuration > Wireless Network> WLANs menu, click Create New.
2. Create a WLAN with following parameters:
  - o Authentication Type: Standard Usage
  - o Authentication Option: 802.1x EAP
  - o Encryption Method: WPA2
  - o Algorithm: AES
  - o Authentication Server: Radius Server created earlier.



The screenshot displays the Ruckus Virtual SmartZone configuration interface. The left sidebar shows the navigation menu with 'WLAN' highlighted. The main content area shows the configuration for a WLAN named 'Cloudpath'. The 'WLAN Usage' section is expanded, showing the following settings:

- Access Network:**  Tunnel WLAN traffic through Ruckus GRE
- Authentication Type:**  Standard usage (For most regular wireless networks)
  - Hotspot (WISPr)
  - Guest Access
  - Web Authentication
  - Hotspot 2.0 Access
  - Hotspot 2.0 Secure Onboarding (OSEN)
- Authentication Options:**
  - Method:**  Open  802.1x EAP  MAC Address
- Encryption Options:**
  - Method:**  WPA2  WPA-Mixed  WEP-64 (40 bits)  WEP-128
  - Algorithm:**  AES  AUTO (TKIP+AES)
  - 802.11w MFP:**  Disabled  Capable  Required
- Authentication & Accounting Service:**
  - Authentication Service:**  Use the controller as proxy  Cloudpath
  - Accounting Service:**  Use the controller as proxy  Disable

FIGURE 14: SECURE SSID CONFIGURATION

## Summary

This document provided a step-by-step guide to configuring a WLAN in the Ruckus SmartZone controllers for the Cloudpath Enrollment System. The Cloudpath client onboarding platform calls for two WLANs (SSIDs): Onboarding and Production. The first one is used for onboarding the clients. This is a Hotspot (WISPr) type SSID and it redirects clients to the Cloudpath Enrollment System (ES). After the client is authenticated, a certificate is downloaded and installed on the client. This certificate provides the client with access to the second secure SSID.

## About Ruckus

Headquartered in Sunnyvale, CA, Ruckus Wireless, Inc. is a global supplier of advanced wireless systems for the rapidly expanding mobile Internet infrastructure market. The company offers a wide range of indoor and outdoor “Smart Wi-Fi” products to mobile carriers, broadband service providers, and corporate enterprises, and has over 36,000 end-customers worldwide. Ruckus technology addresses Wi-Fi capacity and coverage challenges caused by the ever-increasing amount of traffic on wireless networks due to accelerated adoption of mobile devices such as smartphones and tablets. Ruckus invented and has patented state-of-the-art wireless voice, video, and data technology innovations, such as adaptive antenna arrays that extend signal range, increase client data rates, and avoid interference, providing consistent and reliable distribution of delay-sensitive multimedia content and services over standard 802.11 Wi-Fi. For more information, visit <http://www.ruckuswireless.com>.

Ruckus and Ruckus Wireless are trademarks of Ruckus Wireless, Inc. in the United States and other countries.

## Copyright 2017 Ruckus Wireless, Inc. All Rights Reserved.

Copyright Notice and Proprietary Information No part of this documentation may be reproduced, transmitted, or translated, in any form or by any means without prior written permission of Ruckus Wireless, Inc. (“Ruckus”), or as expressly provided by under license from Ruckus

### **Destination Control Statement**

Technical data contained in this publication may be subject to the export control laws of States law is prohibited. It is the reader’s responsibility to determine the applicable regulations and to comply with them.

### **Disclaimer**

THIS DOCUMENTATION AND ALL INFORMATION CONTAINED HEREIN (“MATERIAL”) IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. RUCKUS AND ITS LICENSORS MAKE NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, WITH REGARD TO THE MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE, OR THAT THE MATERIAL IS ERROR-FREE, ACCURATE OR RELIABLE. RUCKUS RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES TO THE MATERIAL AT ANY TIME.

### **Limitation of Liability**

IN NO EVENT SHALL RUCKUS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR USE,