
Deploy a Cloudpath ES Workflow on a Ruckus SmartZone

Cloudpath as RADIUS server and as a Hotspot (WISPr) Portal

Best Practices and Deployment Guide

Table of Contents

This table of contents can be used as a checklist

Intent of this Document

Cloudpath Best Practices and Deployment Guides are meant to address specific subjects in Ruckus Cloudpath deployments and to tackle those subjects in bite sized chunks. Although Cloudpath is simpler and more user-friendly than competitors, there are many options within Cloudpath and network administrators will benefit from a series of targeted Best Practices and Deployment Guides.

The configuration steps and illustrations in this Guide are based on Cloudpath v5.2 and SmartZone v5.1. Additionally, this configuration document is built on an existing Cloudpath workflow configuration which was covered in a separate Best Practices and Deployment Guides called Basic Cloudpath Workflow - secure users and MAC auth guests.

What is Ruckus Cloudpath? Cloudpath is a self-service onboarding portal for secure networks. We are all familiar with captive portals for public access/hotspot networks. Unlike those systems, Cloudpath can support self-service secure registration for networks, combining everything necessary for:

- *Policy Management* - Is the user a student or a teacher? Is the device a phone or a laptop?
- *Device Enablement* - Is the anti-virus up-to-date? Is the firewall running and the OS patched?
- *Certificate Deployment and Management* – Certificates are deployed automatically, uniquely identifying all devices

IT gets more control and more information, while spending less time on password problems and basic access issues.

This document walks through the deployment of a Cloudpath workflow (or registration portal), on a Ruckus SmartZone WLAN controller. It supports the typical case of two WLANs (SSIDs) – one for the onboarding portal, one for secure users. The secure SSID is 802.1X certificate secured for users and is accessible only after they have registered their devices at the onboarding portal. The open SSID can serve double duty as both the secure user onboarding portal, and also as the guest WLAN with automatic MAC registration of guest devices. Configuration of both options is described below.

This document is not an installation guide for Cloudpath or for Ruckus SmartZones.

Cloudpath ES server should already be fully deployed and accessible, locally or as a cloud system. An external database of users should be available. A workflow should already be configured on Cloudpath ES. If necessary, consult the Cloudpath Best Practices and Deployment Guide "Basic Cloudpath Workflow - secure users and MAC auth guests".

Similarly, a Ruckus SmartZone controller should be deployed and ready, with at least one AP connected to it. To test, Wi-Fi client devices such as tablets, smart phones, or laptops will be needed.

*There is a limited onboard database in Cloudpath that can be used in a lab environment, but it is not recommended for a production environment

Cloudpath Workflow Overview

A workflow is a tree of network access policy/classification steps contained in a series of web pages. A policy is built in a series of steps, and then published as an onboarding portal (web pages) on the Cloudpath web server. Adding a step usually involves adding a web page, but it could be a filter or other classification step that automatically flows through to the next step/page. A workflow generally ends in downloading a *Device Configuration* onto a secure client. A Cloudpath *Device Configuration* is typically a WLAN/SSID profile, including security settings and an 802.1X certificate. However, it may end in some alternative grant of network access, such as a PSK, a Ruckus Dynamic PSK, or display of a voucher code for a guest user.

Hotspot Portal SSID and RADIUS Secured SSID

This document describes deployment of a Cloudpath workflow for an environment with two WLANs/SSIDs. The first WLAN is a secure/employee SSID that uses 802.1X certificate authentication (supported by the Cloudpath RADIUS server). Take special note – the Cloudpath ES RADIUS server authenticates the certificates for access to the secure network. At registration, there will need to be an authentication server (database) of employees (secure users) that Cloudpath can check before distributing profiles and certificates.

The second SSID is an open WLAN redirected as a Hotspot/WISPr portal. It serves both as employee registration and as a guest access portal. Secure users (e.g. employees) initially register their devices and download a certificate using the open SSID. This is a one-time process for each employee device. Once a device is registered and has a unique certificate, it will automatically and securely connect whenever it detects the secure network.

Guest users can connect to the open SSID, choose to register as a guest, and their device will be uniquely registered by its MAC address. The portal/walled garden will open up and the guest will be granted Internet access.

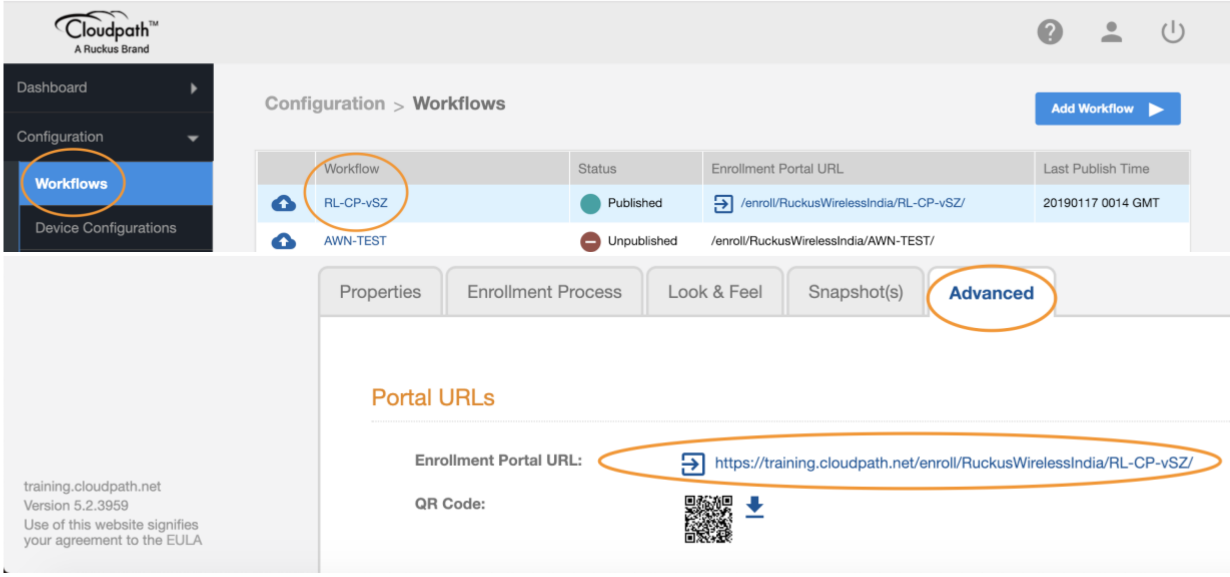
This is designed to be a simple but effective workflow that can be built on, and necessary configuration of Cloudpath is described in the Cloudpath Best Practices and Deployment Guide "Basic Cloudpath Workflow - Secure Users and MAC-auth Guests".

Onboarding and Secure WLANs on Ruckus SmartZone Controllers

1) Get the enrollment URL and the RADIUS shared secret from Cloudpath ES

Configuration of a basic workflow in Cloudpath ES should have been completed. However, before moving on to a WLAN controller, there are two pieces of information that will be needed.

- The Enrollment Portal URL
- The Cloudpath ES RADIUS settings



	Workflow	Status	Enrollment Portal URL	Last Publish Time
	RL-CP-vSZ	Published	/enroll/RuckusWirelessIndia/RL-CP-vSZ/	20190117 0014 GMT
	AWN-TEST	Unpublished	/enroll/RuckusWirelessIndia/AWN-TEST/	

Portal URLs

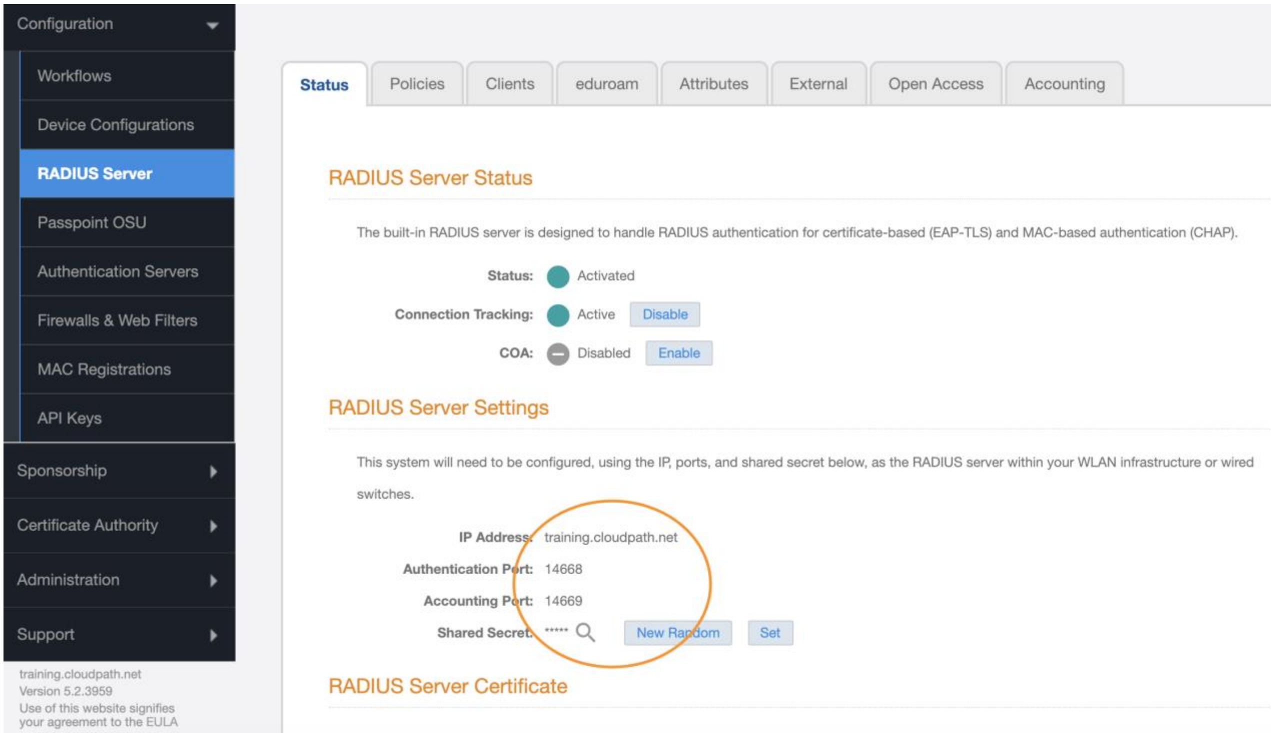
Enrollment Portal URL: https://training.cloudpath.net/enroll/RuckusWirelessIndia/RL-CP-vSZ/

QR Code:

Login to Cloudpath ES and navigate to:
Configuration > Workflow
Click on the workflow to be deployed
Click on the workflow's **Advanced** tab
Go to the Enrollment Portal URL.
Copy this URL to a text editor for later (or be prepare to return to this window).
This URL will be added to the SmartZone as a WISPr or external portal

NB: If you performed "Copy Link Address" by right clicking the link, make sure you remove the tail end "/reset" before pasting into the SmartZone controller configuration.

i.e. https://training.cloudpath.net/enroll/RuckusWirelessIndia/RL-CP-vSZ/reset



RADIUS Server Status

The built-in RADIUS server is designed to handle RADIUS authentication for certificate-based (EAP-TLS) and MAC-based authentication (CHAP).

Status: Activated
Connection Tracking: Active
COA: Disabled

RADIUS Server Settings

This system will need to be configured, using the IP, ports, and shared secret below, as the RADIUS server within your WLAN infrastructure or wired switches.

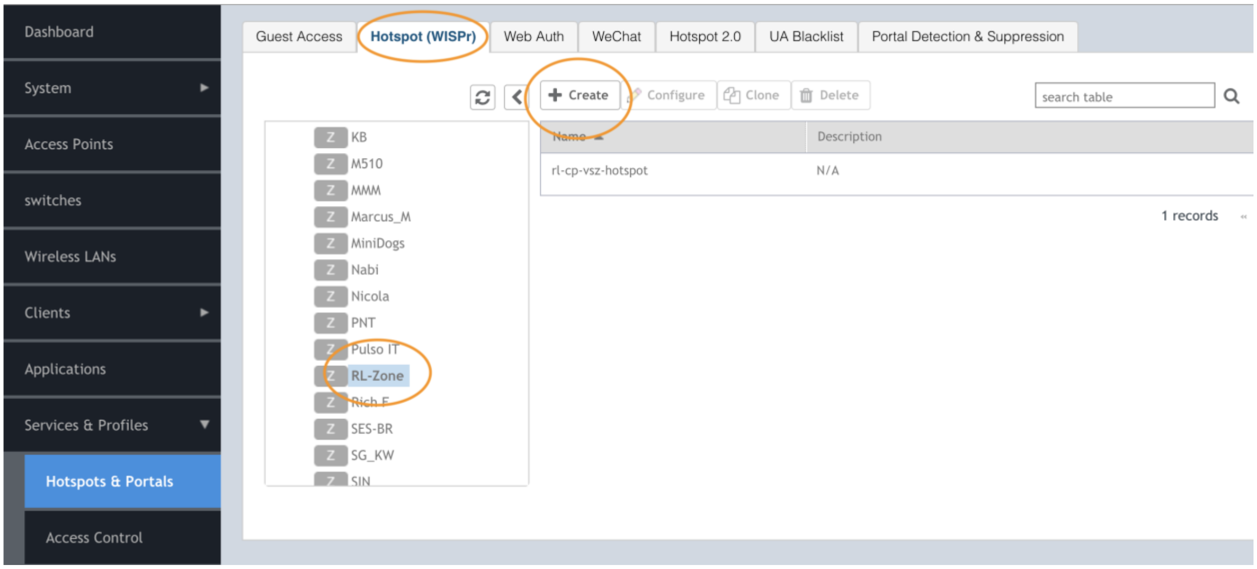
IP Address: training.cloudpath.net
Authentication Port: 14668
Accounting Port: 14669
Shared Secret: *****

RADIUS Server Certificate

The SmartZone will need the RADIUS server settings. On the main menu bar, navigate to **Configuration -> RADIUS Server.** Copy the following information for later

- The IP address - must be an IP address. If necessary, a CLI ping will determine the IP from the FQDN
- Authentication port
- The Accounting port (optional)
- The Shared Secret - which can be revealed by clicking on the magnifying glass

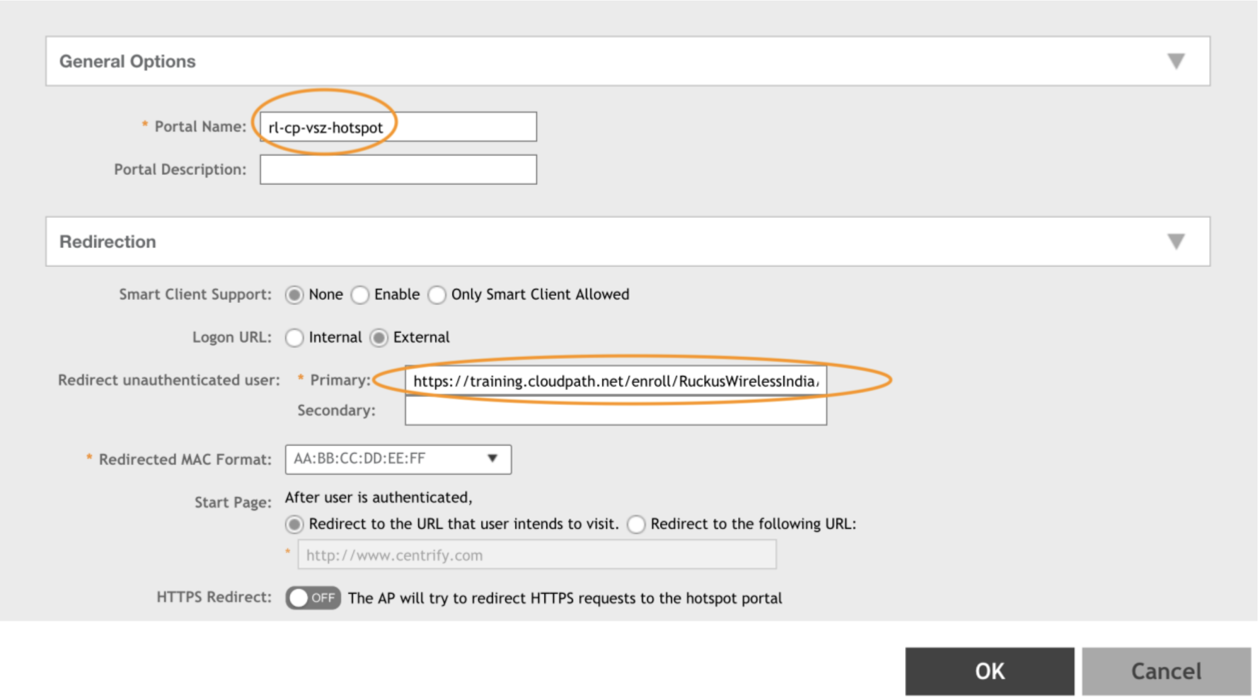
2) Define a Hotspot (WISPr) service on the SmartZone



Name	Description
rl-cp-vsz-hotspot	N/A

1 records

Login to the SmartZone controller and navigate to
Services & Profiles
Hotspots & Portals
Hotspot (WISPr) tab
The domain and **zone** for deployment
Click on **+ *Create***



General Options

* Portal Name: rl-cp-vsz-hotspot

Portal Description:

Redirection

Smart Client Support: ● None ○ Enable ○ Only Smart Client Allowed

Logon URL: ○ Internal ● External

Redirect unauthenticated user: * Primary: https://training.cloudpath.net/enroll/RuckusWirelessIndia/

Secondary:

* Redirected MAC Format: AA:BB:CC:DD:EE:FF

Start Page: After user is authenticated,
● Redirect to the URL that user intends to visit. ○ Redirect to the following URL:
* http://www.centrify.com

HTTPS Redirect: OFF The AP will try to redirect HTTPS requests to the hotspot portal

In the Create Hotspot Portal screen
Name the portal
Smart Client Support: accept **None**
Logon URL: **External**
Paste the URL of Cloudpath Enablement Portal (see above) into the redirect box
Start Page: Choose how to redirect an authenticated user

NB: If you performed "Copy Link Address" by right clicking the link, make sure you remove the tail end "/reset" before pasting into the SmartZone controller configuration.

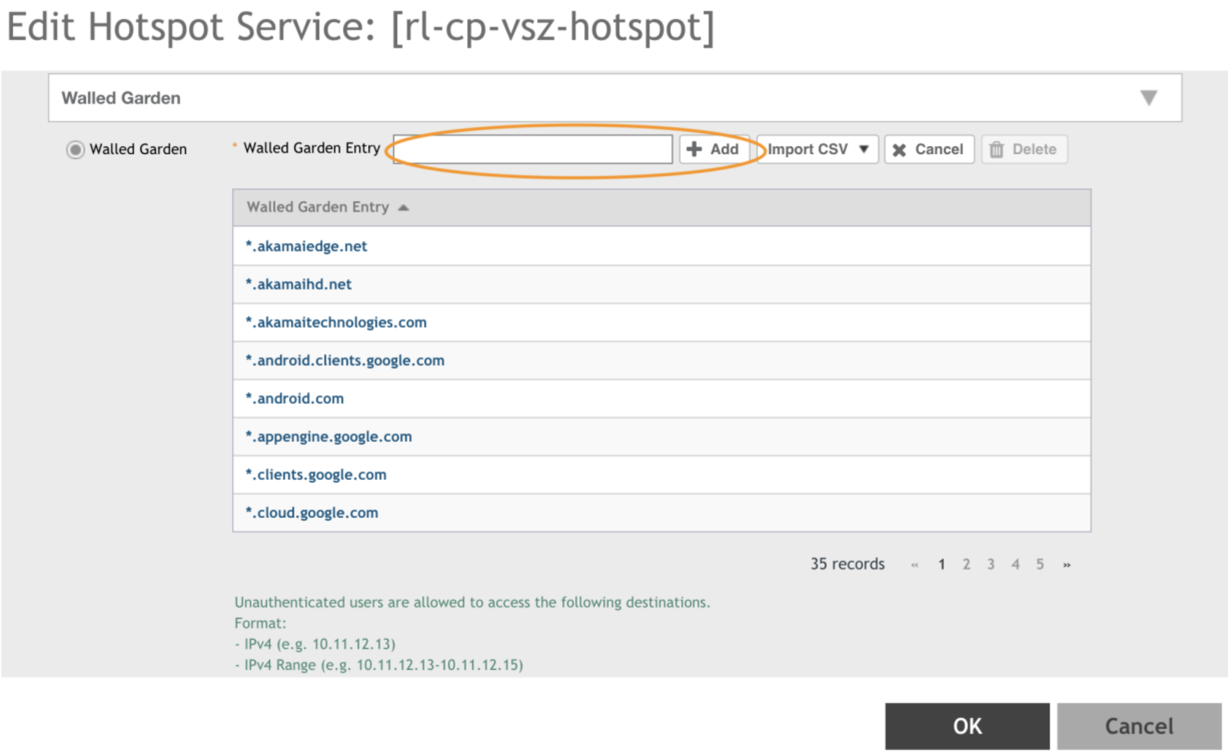
i.e. https://training.cloudpath.net/enroll/RuckusWirelessIndia/RL-CP-vSZ/reset

You may have to scroll down for the Walled Garden settings

Configuring the Walled Garden Whitelist

Walled Garden: In order to support the authentication process, specific internet traffic must be allowed before the user can be authenticated.

You would need different sets of Walled Garden URL entries for Apple, Windows, Android devices or CNA for downloading Apps from the Google Play, Apple Store and Amazon Market.



Edit Hotspot Service: [rl-cp-vsz-hotspot]

Walled Garden

● Walled Garden

* Walled Garden Entry

Walled Garden Entry ▲
*.akamaiedge.net
*.akamaihd.net
*.akamaitechnologies.com
*.android.clients.google.com
*.android.com
*.appengine.google.com
*.clients.google.com
*.cloud.google.com

35 records « 1 2 3 4 5 »

Unauthenticated users are allowed to access the following destinations.
Format:
- IPv4 (e.g. 10.11.12.13)
- IPv4 Range (e.g. 10.11.12.13-10.11.12.15)

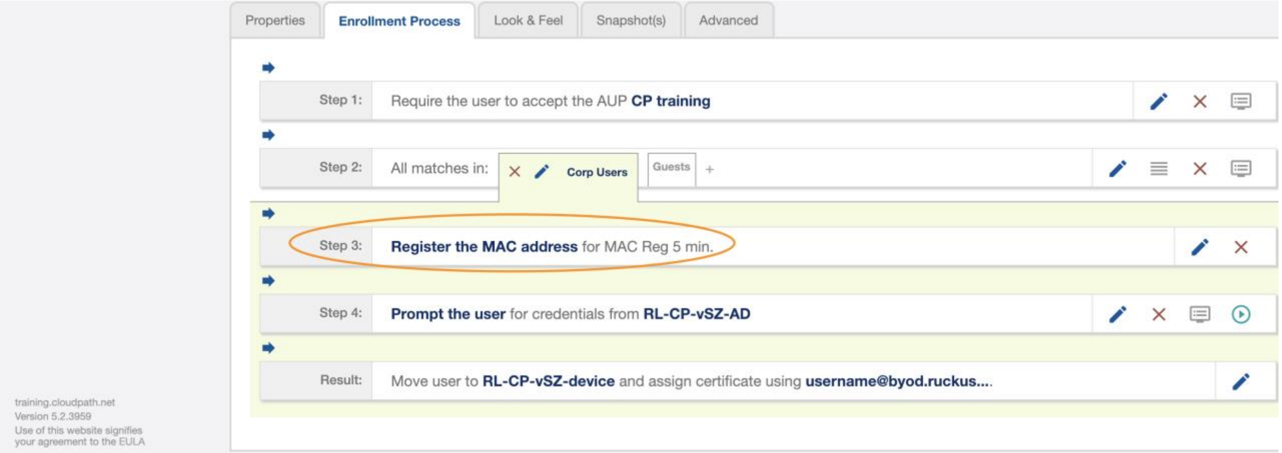
Depending on your local network setup, you may additionally need to add the gateway, DNS and DHCP server addresses as well.
Click OK to save the portal

If you want to restrict internet access only to the required App Stores, you would need to fully configure the Walled Garden with all the required URLs. For details about the latest Whitelist URLs, go to the following site to download the Walled Garden document.

https://support.ruckuswireless.com/articles/000005988

Alternate Option to Walled Garden

Instead of allowing internet access through the Walled Garden, you could simply choose to configure an extra Workflow step with MAC authentication (before the 802.1X EAP steps) to open up the internet connection for a short (e.g. 5 minutes) window to allow access to the App Stores, such that it saves you efforts of setting up the Walled Garden with the required Whitelist URLs.



Step 1: Require the user to accept the AUP **CP training**

Step 2: All matches in: **Corp Users** Guests +

Step 3: **Register the MAC address** for MAC Reg 5 min.

Step 4: **Prompt the user** for credentials from **RL-CP-vSZ-AD**

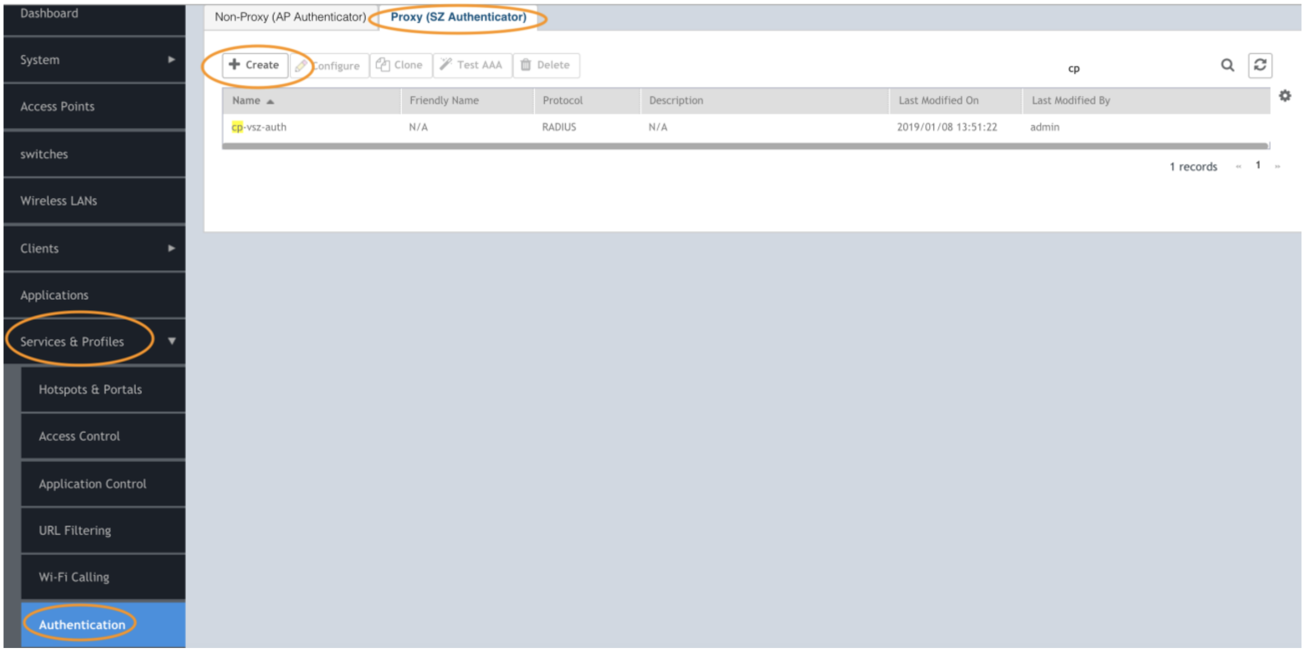
Result: Move user to **RL-CP-vSZ-device** and assign certificate using **username@byod.ruckus....**

training.cloudpath.net
Version 5.2.3959
Use of this website signifies
your agreement to the EULA

You should be aware of the pros and cons of taking this option, while this would save you efforts and details of administering the Walled Garden, however you should note that all users would have unrestricted access to the internet during the 5 minutes window. Hence, it is advised to check this against your own company polices before deciding your option.

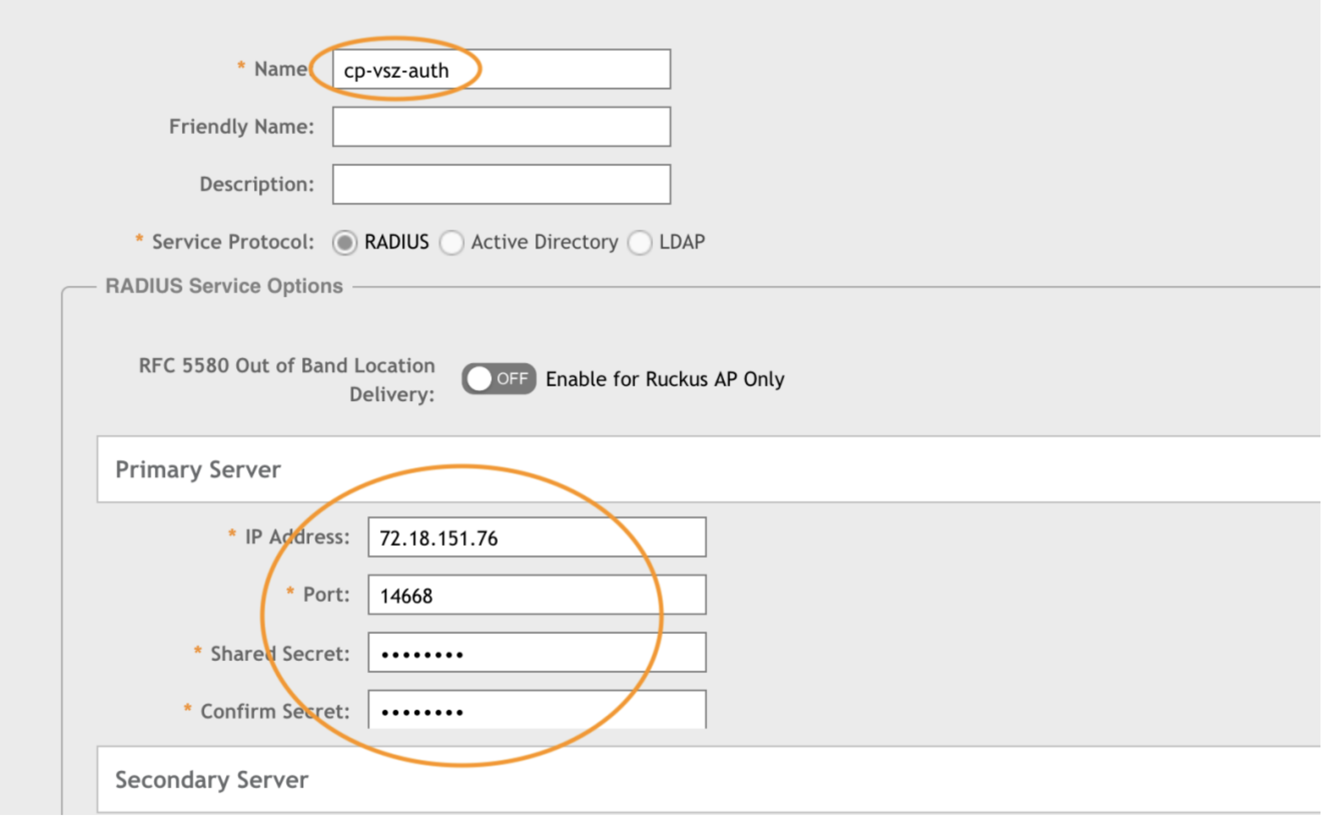
3) Add Cloudpath ES as a AAA server on the SmartZone

Add Cloudpath as a RADIUS server, with the SmartZone as proxy. In this case, the AP will ask the SmartZone to authenticate the client, and the SmartZone will connect to Cloudpath. In the Non-Proxy option, each AP connects directly to Cloudpath.



Name	Friendly Name	Protocol	Description	Last Modified On	Last Modified By
cp-vsz-auth	N/A	RADIUS	N/A	2019/01/08 13:51:22	admin

Navigate to:
Services & Profiles
Authentication
Proxy (SZ Authenticator) tab
If configuring non-Proxy, the correct **Zone** must be selected. Proxy is system wide, while Non-Proxy is zone specific
Click on **+ *Create***



* Name: cp-vsz-auth
Friendly Name:
Description:
* Service Protocol: ● RADIUS ○ Active Directory ○ LDAP

RADIUS Service Options

RFC 5580 Out of Band Location Delivery: OFF Enable for Ruckus AP Only

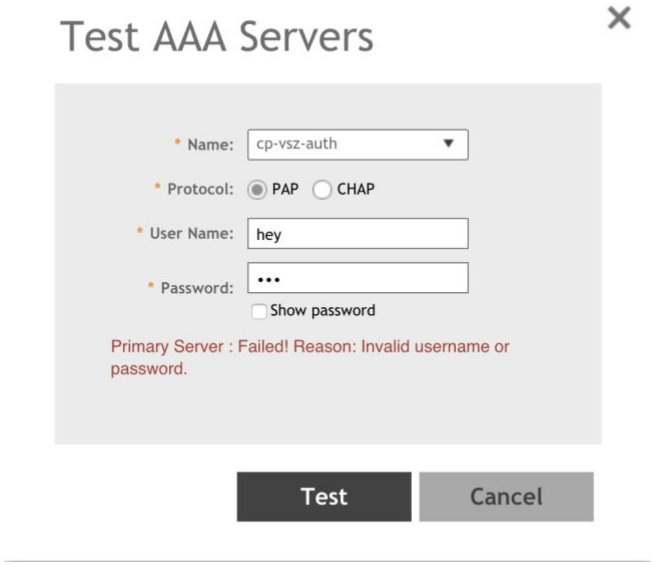
Primary Server

* IP Address: 72.18.151.76
* Port: 14668
* Shared Secret: ••••••••
* Confirm Secret: ••••••••

Secondary Server

In the Create Authentication Service screen
Name the Service
Service Protocol: choose **RADIUS**
Primary Server
IP address - must be a dotted decimal IP address
Enter the **port number** configured at the RADIUS server (1812 is standard)
Enter the **Shared Secret** in Shared Secret and Confirm Shared Secret
Click **OK**

4) Test the AAA connection



Test AAA Servers

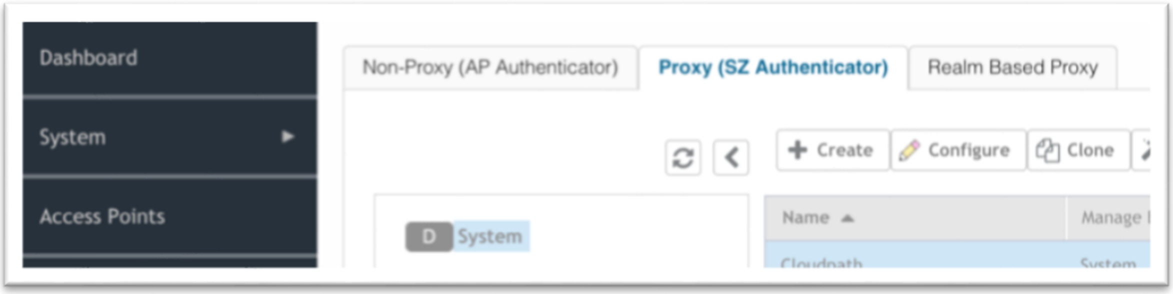
* Name: cp-vsz-auth
* Protocol: ● PAP ○ CHAP
* User Name: hey
* Password: •••

□ Show password

Primary Server : Failed! Reason: Invalid username or password.

Test the AAA server for connectivity.
The Cloudpath ES RADIUS server will not authenticate a user name and password, only a certificate. However, this test still confirms connectivity.
Enter anything in the user name and password, and if the fail message is quick with reason "Invalid username or password" then the SmartZone and Cloudpath are communicating. A timeout indicates they are not connecting.

5) Differences between Proxy, Non-Proxy, and Realm Based Proxy Authentication



A Proxy AAA server is used when the APs send authentication/accounting messages to the SmartZone and the SmartZone forwards those messages to the AAA server. It centralizes authentication and the RADIUS server needs to allow only one RADIUS client, the SmartZone.

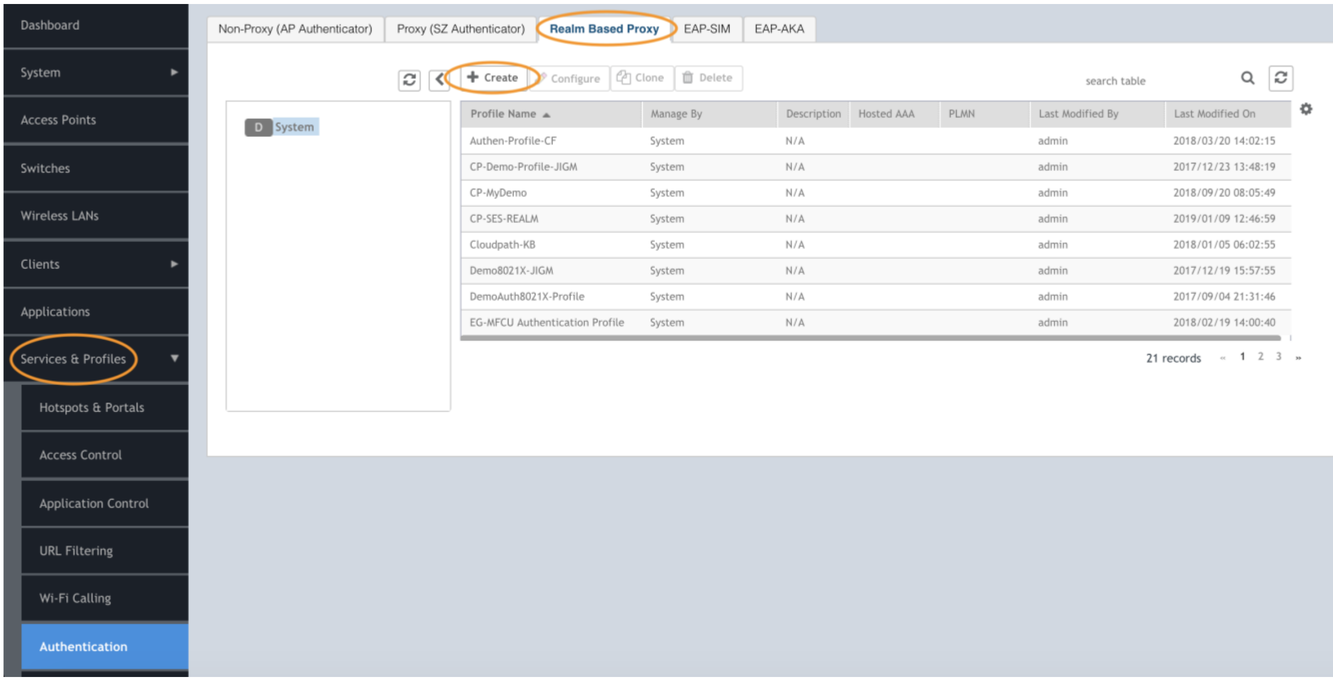
A Non-Proxy AAA server is used when the APs send authentication/accounting messages directly to the AAA server. The RADIUS server needs to allow multiple RADIUS clients (all the APs). Non-Proxy AAA is a per-Zone configuration

A Realm Based Proxy AAA Profile is needed when using Proxy AAA on the vSZ-H or the SZ-300. It is architecturally necessary for large service providers, but in the overwhelming majority of enterprise and K-12 deployments it is merely a slightly annoying additional configuration detail. If multiple realm based AAA servers are required, please contact your Ruckus SE. Otherwise, follow the next section to enable Proxy AAA on vSZ-H

6) vSZ-H + Proxy AAA only: Create a Realm Based Authentication Profile

This step is not necessary on the vSZ-E or the SZ-100 platforms, and is not necessary on any platform when configuring a Non-Proxy AAA server. For 90% of vSZ-H users, this is the exact configuration.

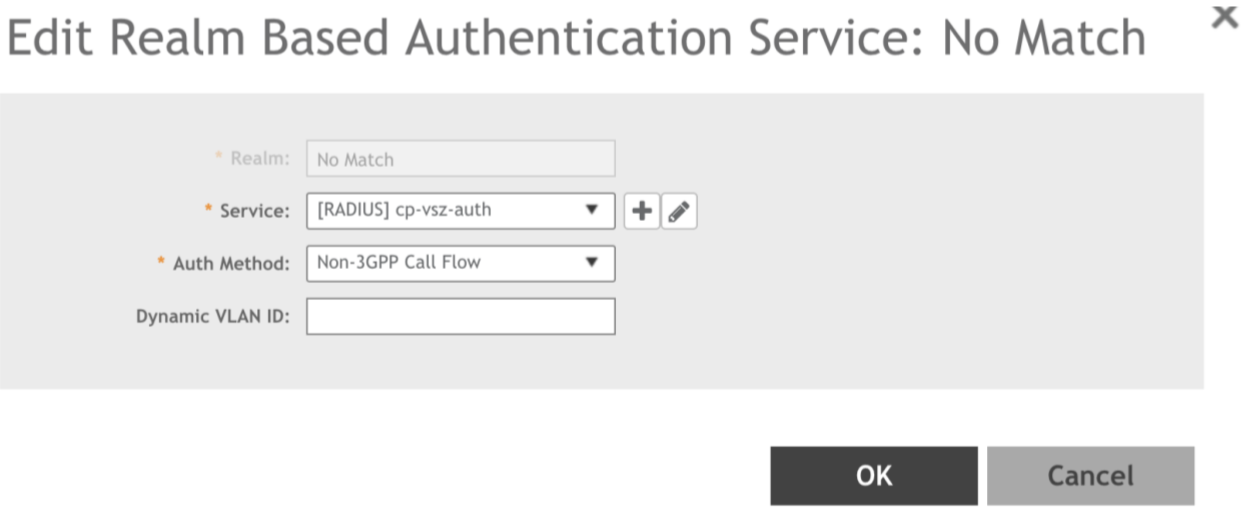
On the left menu, navigate to:
Services & Profiles
Authentication
Go to the Realm Based Proxy tab
Click on + Create



Profile Name ▲	Manage By	Description	Hosted AAA	PLMN	Last Modified By	Last Modified On
Authen-Profile-CF	System	N/A			admin	2018/03/20 14:02:15
CP-Demo-Profile-JIGM	System	N/A			admin	2017/12/23 13:48:19
CP-MyDemo	System	N/A			admin	2018/09/20 08:05:49
CP-SES-REALM	System	N/A			admin	2019/01/09 12:46:59
Cloudpath-KB	System	N/A			admin	2018/01/05 06:02:55
Demo8021X-JIGM	System	N/A			admin	2017/12/19 15:57:55
DemoAuth8021X-Profile	System	N/A			admin	2017/09/04 21:31:46
EG-MFCU Authentication Profile	System	N/A			admin	2018/02/19 14:00:40

21 records « 1 2 3 »

The Create Authentication Profile window appears
Name the profile
Do not check the check boxes
Click on **No match Realm** to highlight it
Click on **Configure**



Edit Realm Based Authentication Service: No Match

* Realm: No Match
* Service: [RADIUS] cp-vsz-auth
* Auth Method: Non-3GPP Call Flow
Dynamic VLAN ID:

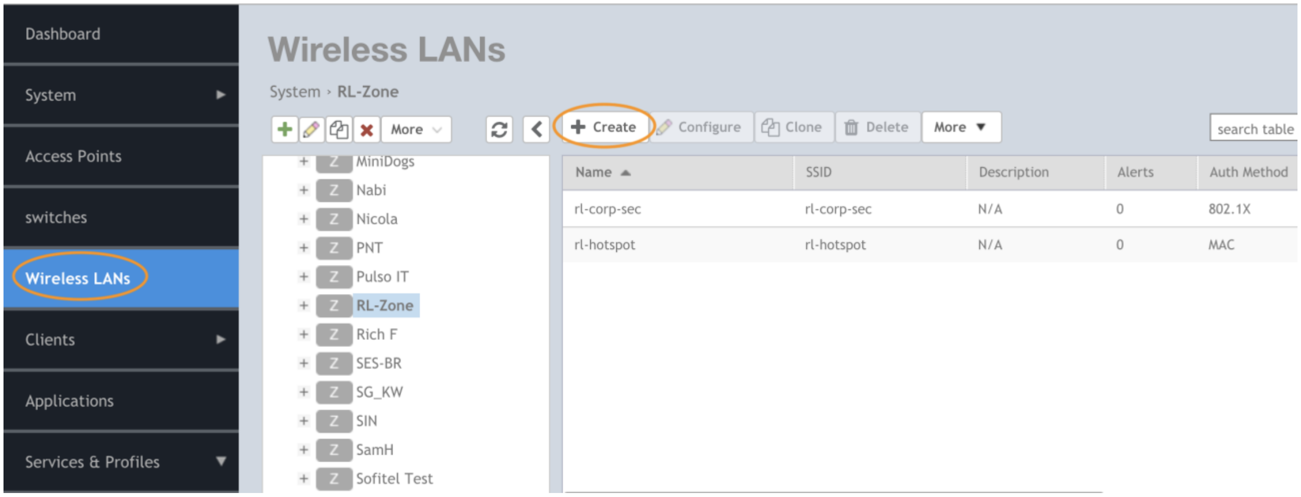
In the Edit Realm Based Authentication Service Window
From the **Service** drop down, Choose the previously created Authentication Server
From the Auth Method drop down, choose Non-3GPP Call Flow
Leave **Dynamic VLAN ID blank** – Dynamic VLANs can be enabled elsewhere
Click **OK**

Repeat for the Unspecified Realm
The Create Authentication Profile window returns
Click on **Unspecified** to highlight it
Click on **Configure**

In the Edit Realm Based Authentication Service Window
From the **Service** drop down, Choose the previously created Authentication Server
From the Auth Method drop down, choose Non-3GPP Call Flow
Leave **Dynamic VLAN ID blank** – Dynamic VLANs can be enabled elsewhere
Click **OK**

The Create Authentication Profile window returns

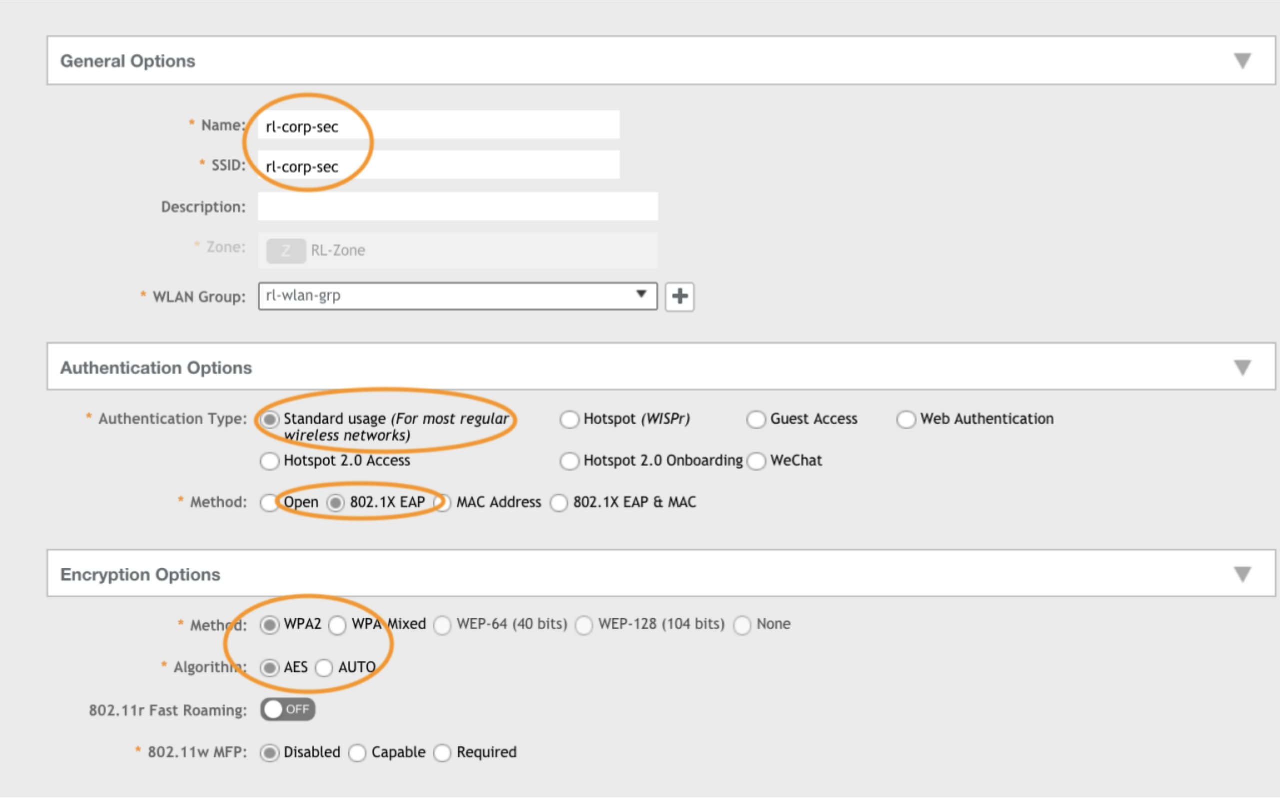
Click **OK** to save



Name	SSID	Description	Alerts	Auth Method
rl-corp-sec	rl-corp-sec	N/A	0	802.1X
rl-hotspot	rl-hotspot	N/A	0	MAC

7) Create the Secure WLAN

On the menu bar, go to **Wireless LANs**
Click on **+Create**



General Options

* Name:	rl-corp-sec
* SSID:	rl-corp-sec
Description:	
* Zone:	RL-Zone
* WLAN Group:	rl-wlan-grp

Authentication Options

* Authentication Type: ● Standard usage *(For most regular wireless networks)* ○ Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat

* Method: ○ Open ● 802.1X EAP ○ MAC Address ○ 802.1X EAP & MAC

Encryption Options

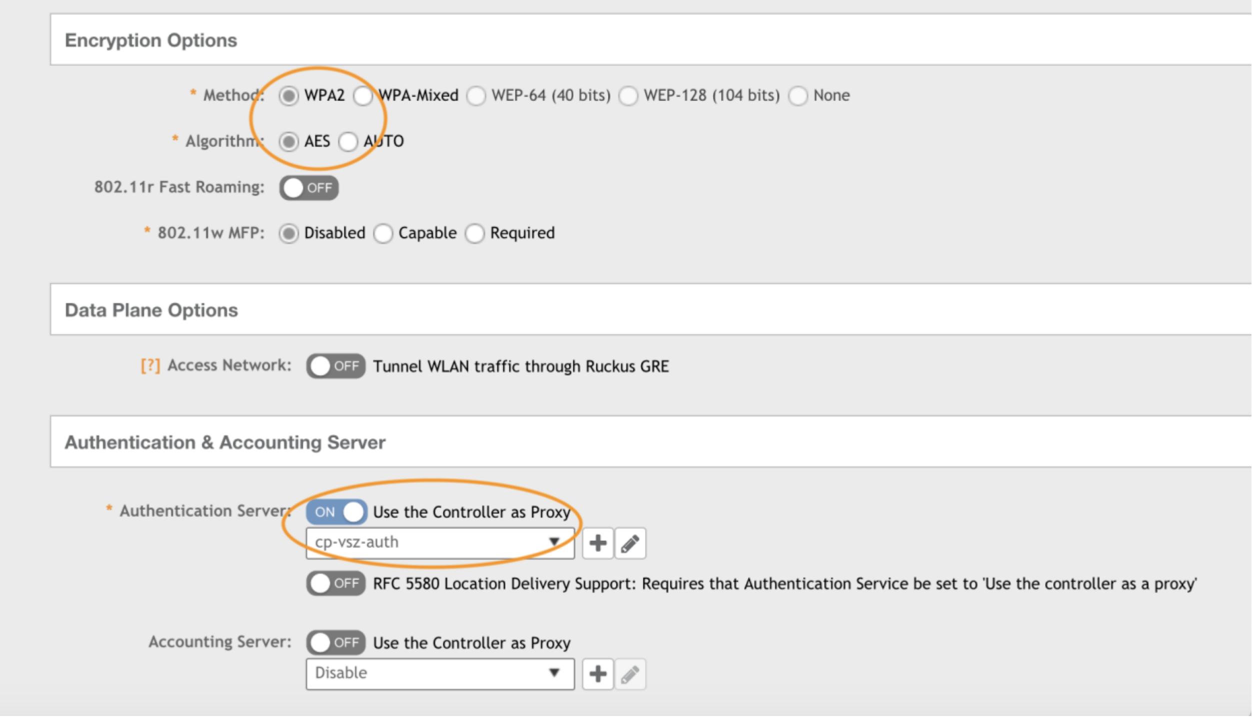
* Method: ● WPA2 ○ WPA Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

* Algorithm: ● AES ○ AUTO

802.11r Fast Roaming: OFF

* 802.11w MFP: ● Disabled ○ Capable ○ Required

In the Create WLAN Configuration screen
Fill in the General Options
Name the WLAN SSID
Choose the **Zone**
Choose the **WLAN group** (the default group is fine)
Under WLAN Usage, choose **Standard Usage**
Authentication options, choose **802.1X EAP**



Encryption Options

* Method: ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ○ None

* Algorithm: ● AES ○ AUTO

802.11r Fast Roaming: OFF

* 802.11w MFP: ● Disabled ○ Capable ○ Required

Data Plane Options

[?] Access Network: OFF Tunnel WLAN traffic through Ruckus GRE

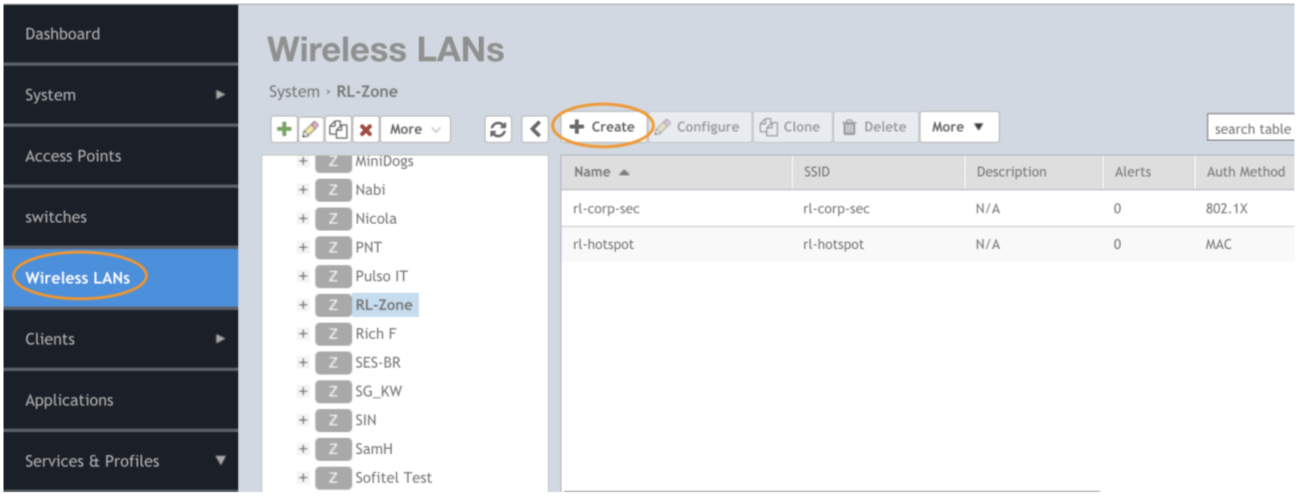
Authentication & Accounting Server

* Authentication Server: ON Use the Controller as Proxy
cp-vsz-auth
OFF RFC 5580 Location Delivery Support: Requires that Authentication Service be set to 'Use the controller as a proxy'

Accounting Server: OFF Use the Controller as Proxy
Disable

Encryption Options
Method - choose **WPA2**
Algorithm – choose **AES**
Authentication and Accounting
Choose Use the controller as proxy
From the drop down, **Choose the proxy** previously defined
Click **OK** to save the WLAN

8) Create the Portal WLAN and allow Guest MAC-authentication pass through

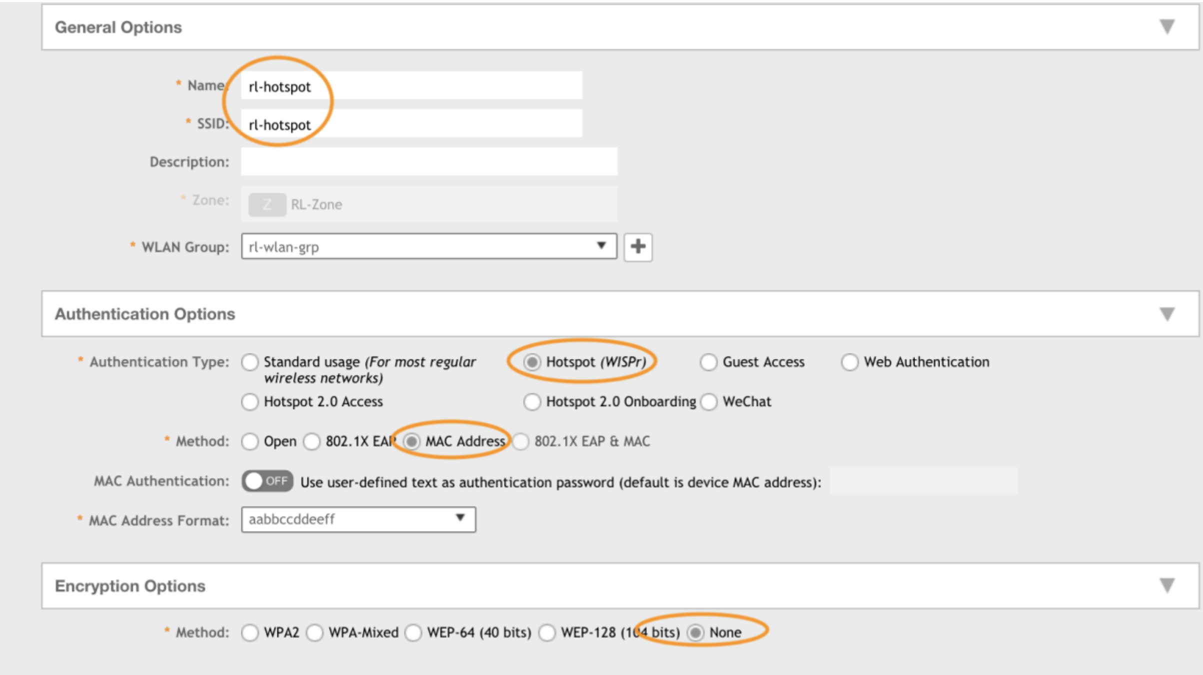


Wireless LANs

System › RL-Zone

Name	SSID	Description	Alerts	Auth Method
rl-corp-sec	rl-corp-sec	N/A	0	802.1X
rl-hotspot	rl-hotspot	N/A	0	MAC

Create another WLAN



General Options

- * Name: rl-hotspot
- * SSID: rl-hotspot
- Description:
- * Zone: RL-Zone
- * WLAN Group: rl-wlan-grp

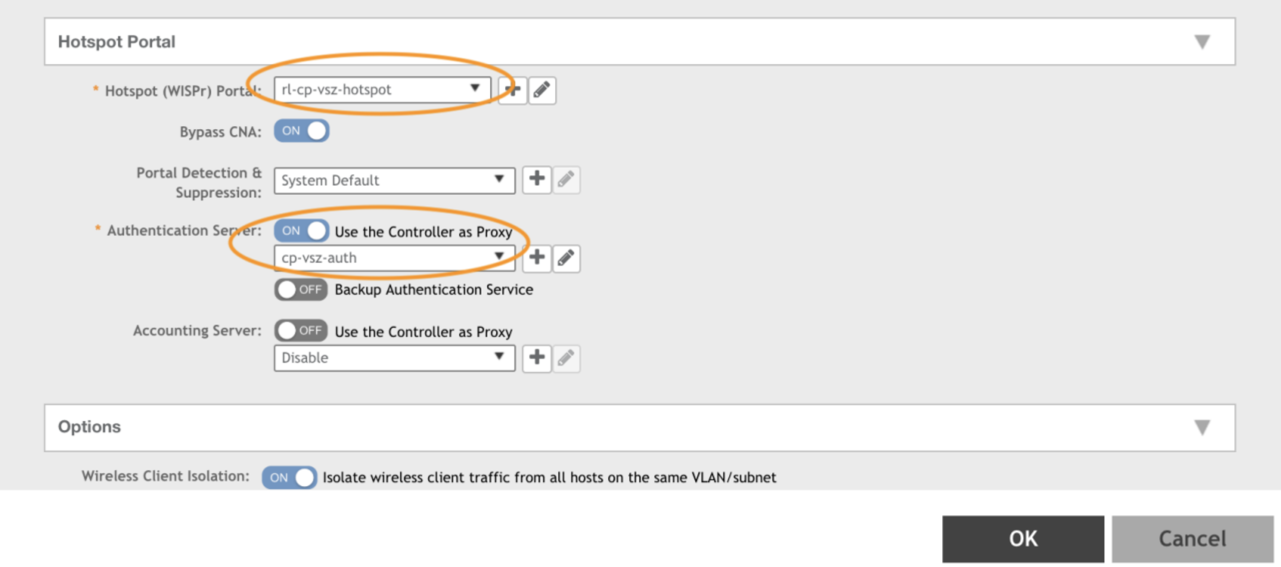
Authentication Options

- * Authentication Type: ○ Standard usage *(For most regular wireless networks)* ● Hotspot *(WISPr)* ○ Guest Access ○ Web Authentication ○ Hotspot 2.0 Access ○ Hotspot 2.0 Onboarding ○ WeChat
- * Method: ○ Open ○ 802.1X EAP ● MAC Address ○ 802.1X EAP & MAC
- MAC Authentication: OFF Use user-defined text as authentication password (default is device MAC address):
- * MAC Address Format: aabbccddeeff

Encryption Options

- * Method: ○ WPA2 ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ● None

Fill in the General Options
Name the WLAN
Give it an SSID
Choose the **Zone**
Choose the **WLAN group** (the default group is fine)
Under Authentication Type, choose **Hotspot (WISPr)**
Authentication Method, choose **MAC Address,** accept the default format
If MAC Authentication pass through for guests is NOT part of the workflow, Open will enable a registration-only portal.



Hotspot Portal

* Hotspot (WISPr) Portal: rl-cp-vsz-hotspot

Bypass CNA: ON

Portal Detection & Suppression: System Default

* Authentication Server: ON Use the Controller as Proxy
cp-vsz-auth
OFF Backup Authentication Service

Accounting Server: OFF Use the Controller as Proxy
Disable

Options

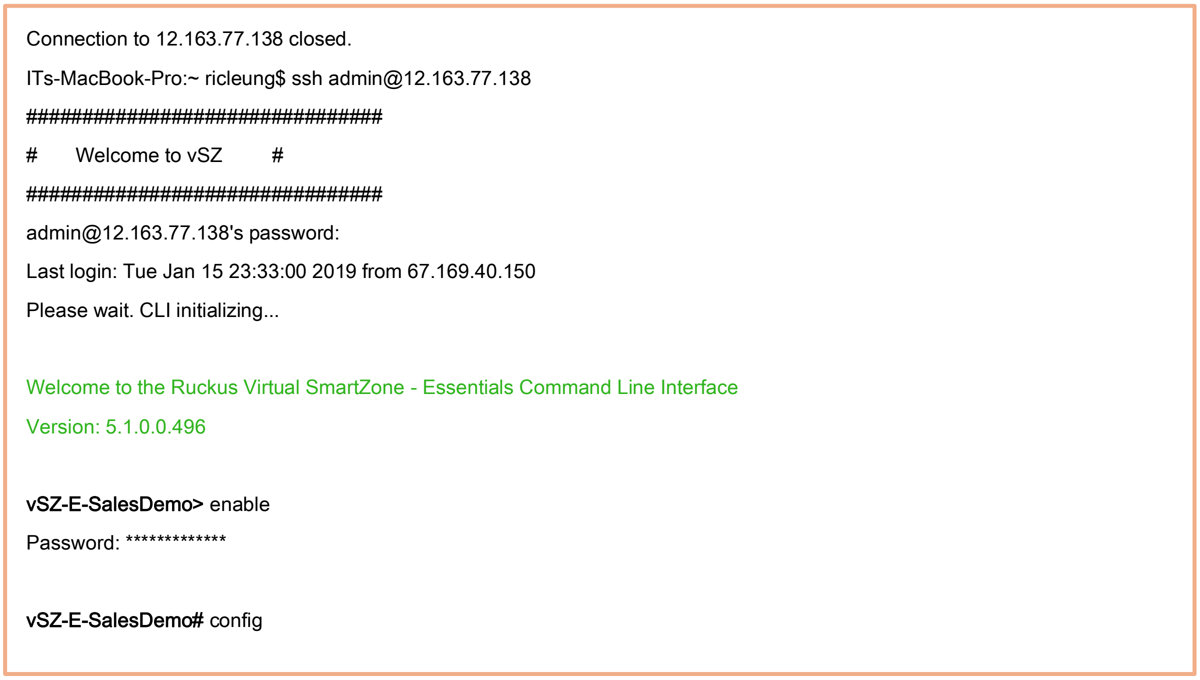
Wireless Client Isolation: ON Isolate wireless client traffic from all hosts on the same VLAN/subnet

Hotspot Portal
Hotspot (WISPr) Portal - In the drop-down, choose the previously created hotspot service
Authentication service
 Check Use the controller as proxy
From the drop down, Choose the proxy previously defined
vSZ-H will require you to choose a Realm Based Proxy
Click **OK** to save the WLAN

9) Disable MAC Encryption on SmartZone

SmartZones encrypt MAC addresses by default. MAC address encryption must be disabled to allow the MAC address to be sent to the Cloudpath ES. This is a command line function.

Open an **SSH** connection to the SmartZone and login
On Windows, use a tool like Putty
Enter privileged mode with the command **enable**
Enter the enable password
Type **config** to enter config mode
Enter the command **no encrypt-mac-ip**
Confirm by typing **yes**



```
Connection to 12.163.77.138 closed.
ITs-MacBook-Pro:~ ricleung$ ssh admin@12.163.77.138
################################
#      Welcome to vSZ          #
################################
admin@12.163.77.138's password:
Last login: Tue Jan 15 23:33:00 2019 from 67.169.40.150
Please wait. CLI initializing...

Welcome to the Ruckus Virtual SmartZone - Essentials Command Line Interface
Version: 5.1.0.0.496

vSZ-E-SalesDemo> enable
Password: *************

vSZ-E-SalesDemo# config
```

Cloudpath On SmartZone

Deploying a Cloudpath Workflow on a Ruckus SmartZone Controller

January 2019

About Ruckus Networks

Ruckus Networks enables organizations of all sizes to deliver great connectivity experiences. Ruckus delivers secure access networks to delight users while easing the IT burden, affordably. Organizations turn to Ruckus to make their networks simpler to manage and to better meet their users' expectations. For more information, visit www.ruckuswireless.com.

Ruckus Networks | 350 West Java Drive | Sunnyvale, CA 94089 USA | T: (650) 265-4200 | F: (408) 738-2065 ruckuswireless.com

About ARRIS

ARRIS International plc (NASDAQ: ARRS) is powering a smart, connected world. The company's leading hardware, software and services transform the way that people and businesses stay informed, entertained and connected. For more information, visit www.arris.com.

For the latest ARRIS news:

Check out our blog: ARRIS EVERYWHERE

Follow us on Twitter: @ARRIS