


Deploy a Cloudpath ES Workflow on a Ruckus SmartZone

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

Best Practices and Deployment Guide

Cloudpath On SmartZone

Deploying a Cloudpath Workflow on a Ruckus SmartZone Controller

August 2017

Table of Contents

This table of contents can be used as a checklist

Cloudpath On SmartZone

Deploying a Cloudpath Workflow on a Ruckus SmartZone Controller

August 2017

Intent of this Document

Cloudpath Best Practices and Deloyment 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.

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 On SmartZone

Deploying a Cloudpath Workflow on a Ruckus SmartZone Controller

August 2017

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.

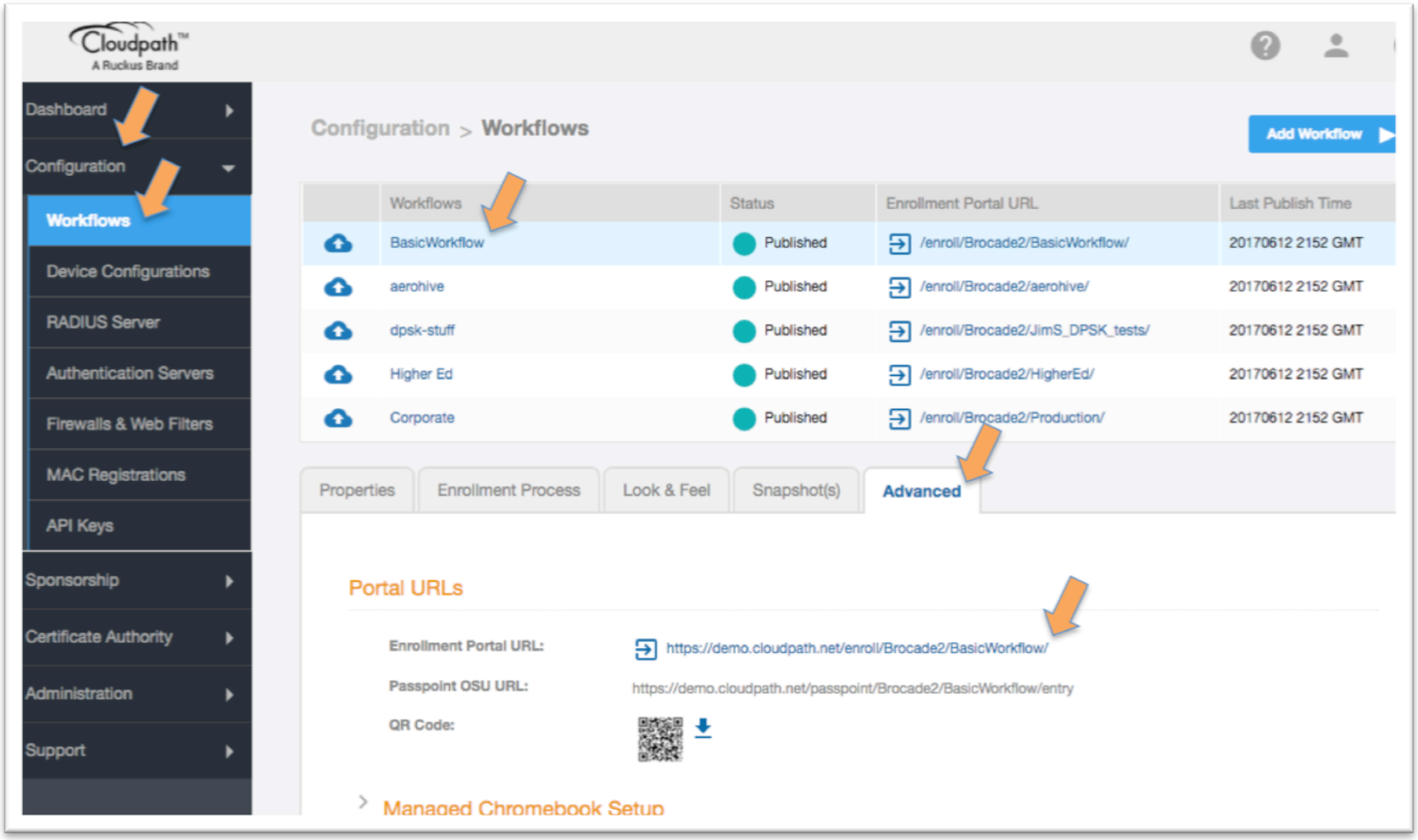
Guest users can connect to the open SSID, choose to register as a guest, and their device will be uniquely registered by its MAC address. The portal/walled garden will open up and the guest will be granted Internet access.

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”.

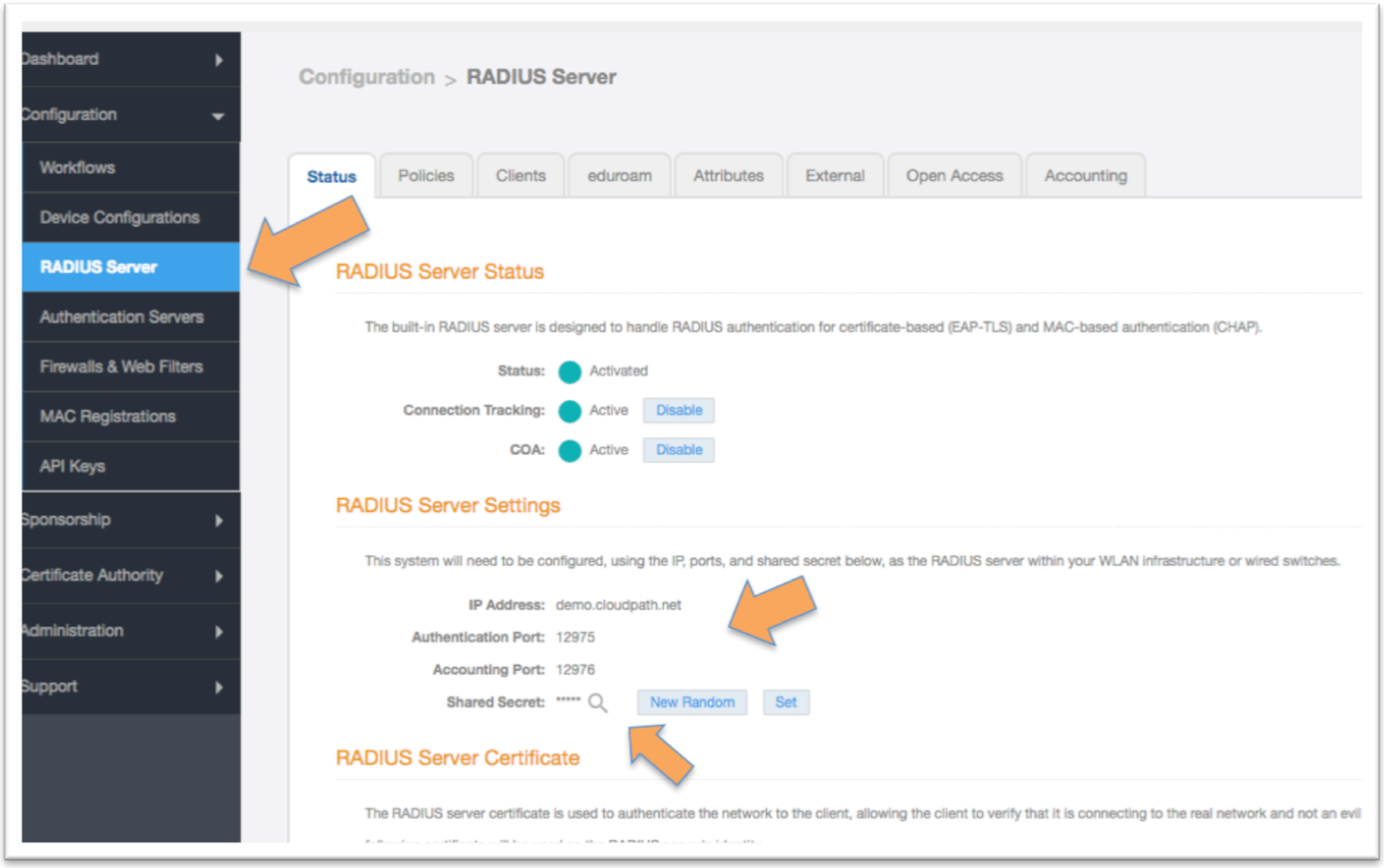
Onboarding and Secure WLANs on Ruckus SmartZone Controllers

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

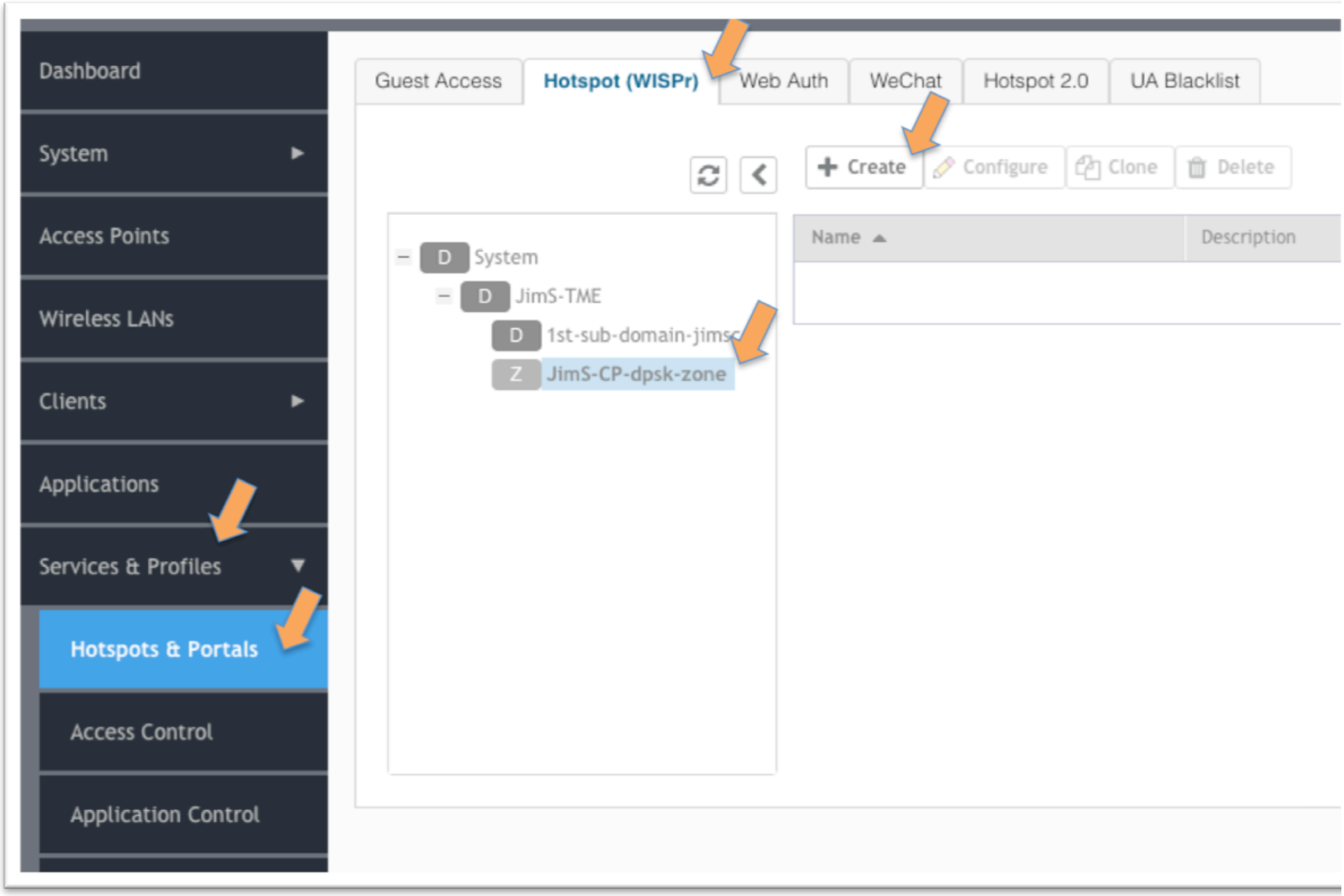


- Login to Cloudpath ES and navigate to:
  - **Configuration**
  - **Workflow**
  - Click on the workflow to be deployed
  - Click on the workflow's **Advanced** tab
  - Go to the **Enrollment Portal URL.**
  - Copy this URL to a text editor for later (or be prepare to return to this window).
    - This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

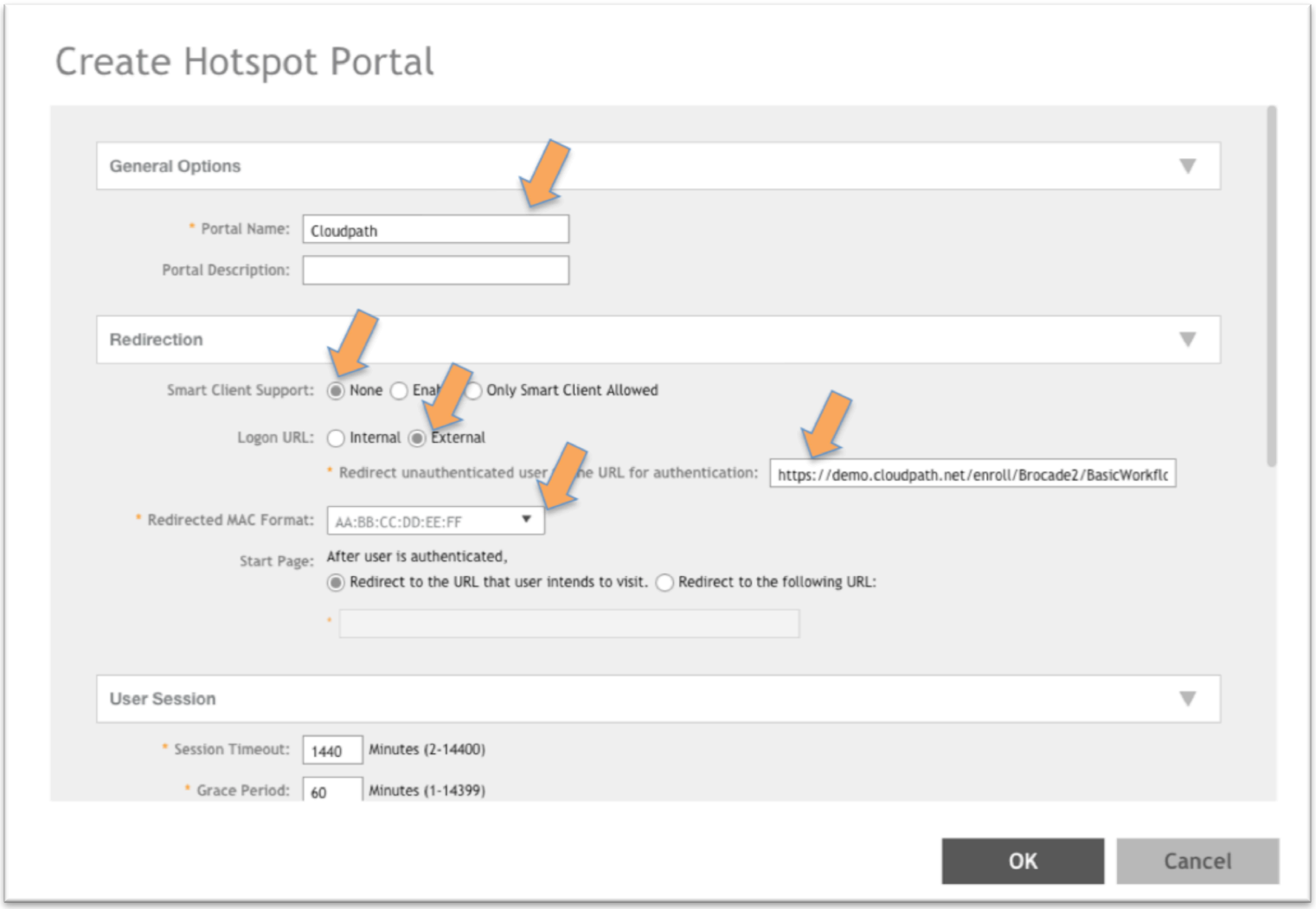


- The SmartZone will need the RADIUS server settings. On the main menu bar, navigate to **Configuration -> RADIUS Server**. Copy the following information for later
  - The **IP address**
    - *NB - must be an IP address. If necessary, a CLI ping will determine the IP from the FQDN*
  - **Authentication port**
  - The Accounting port (optional)
  - The **Shared Secret**
    - which can be revealed by clicking on the magnifying glass

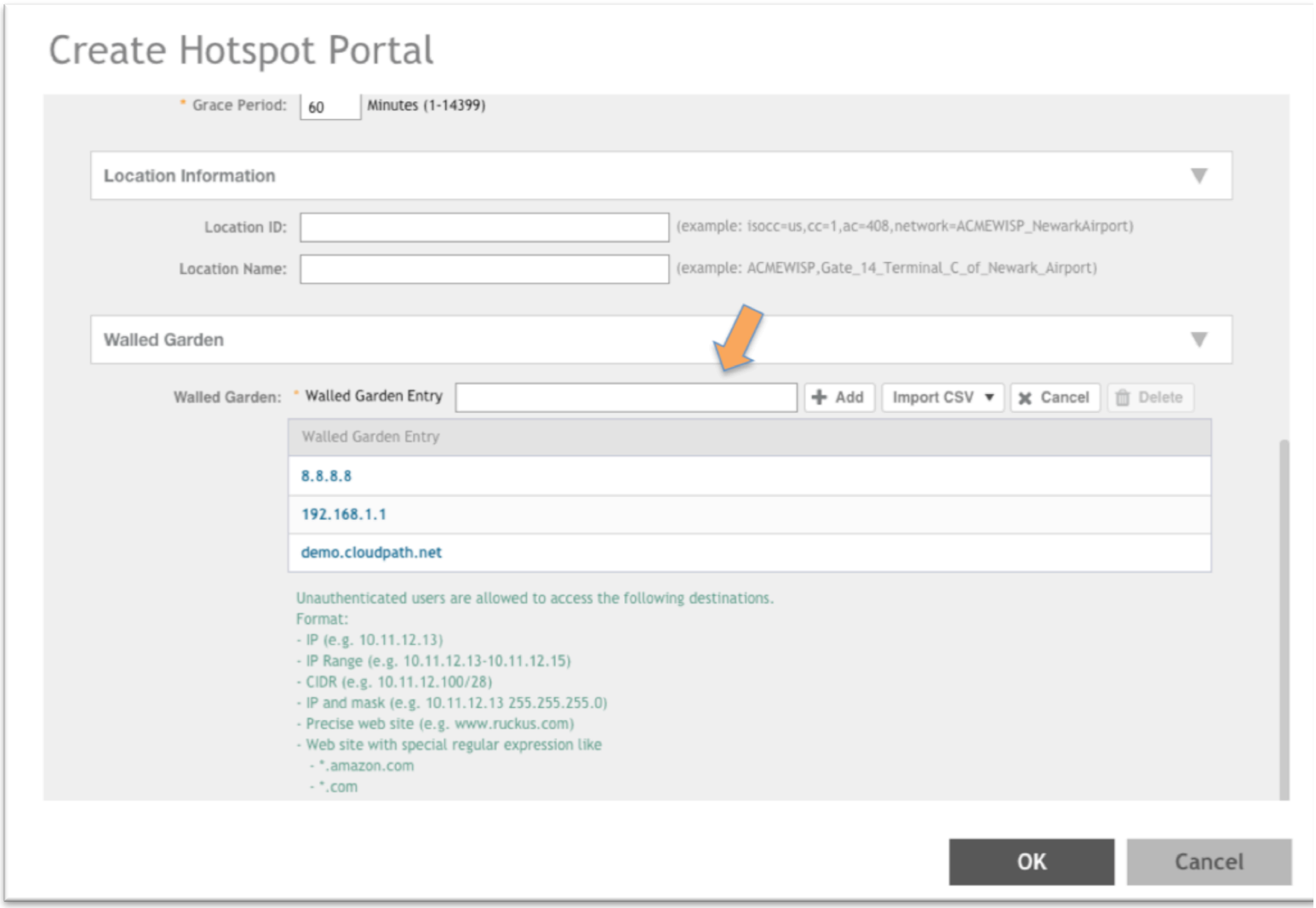
2) Define a Hotspot (WISPr) service on the SmartZone



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



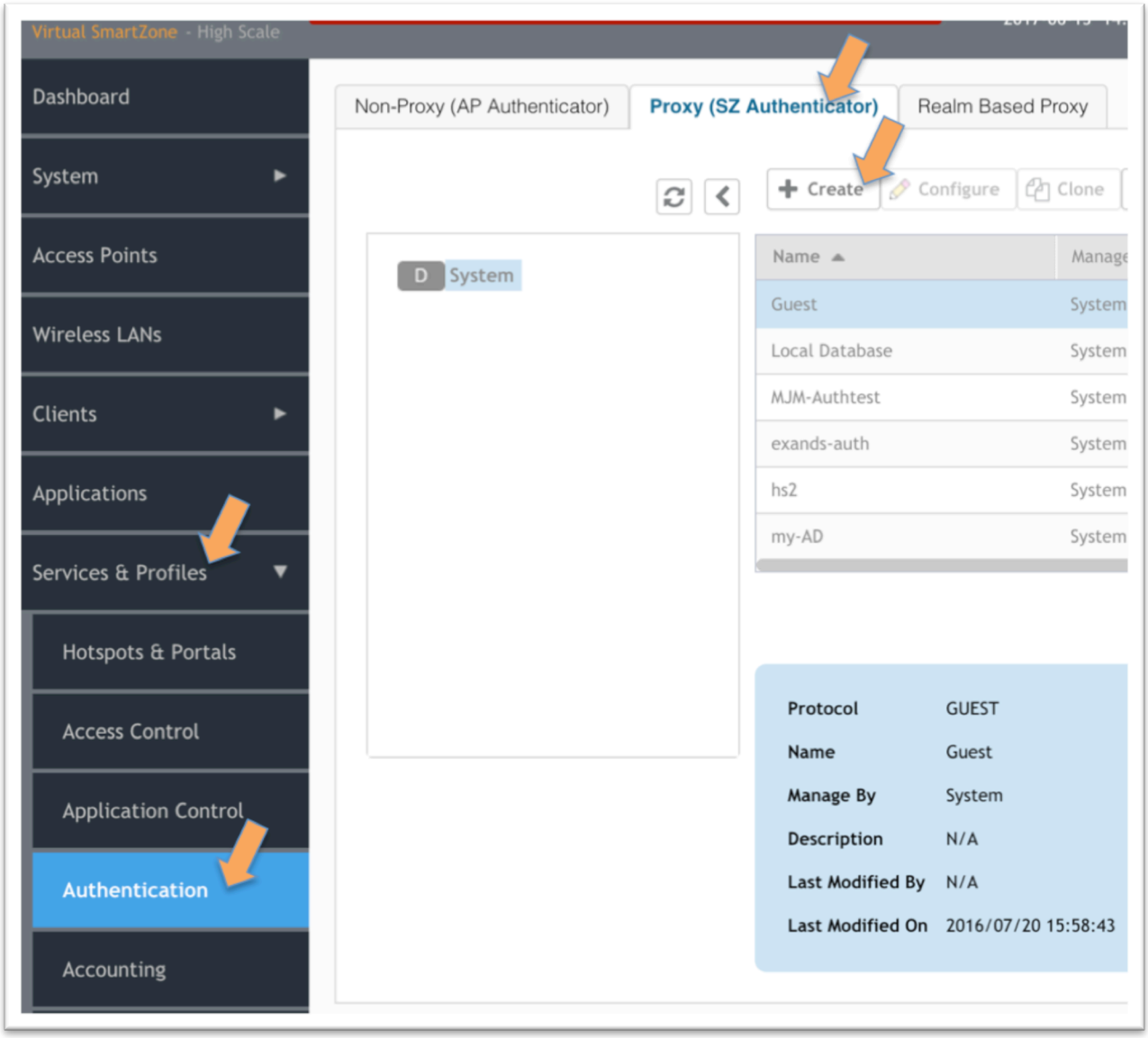
- In the **Create Hotspot Portal** screen
  - **Name** the portal
  - Smart Client Support: accept **None**
  - Logon URL: **External**
  - **Paste the URL** of Cloudpath Enablement Portal (see above) into the redirect box
  - Start Page: Choose how to redirect an authenticated user
- You may have to scroll down for the Walled Garden settings



- **Walled Garden**: In order to function, specific network traffic must be allowed before the user is authenticated in order to support the authentication process. The exact entries depend on the local network. The following are generally required
    - DHCP server – the client generally needs an IP address
    - DNS server
    - Gateway (in many case, all three are the same)
    - Cloudpath server, including subdomains of the enrollment URL
    - Click *OK* to save the portal

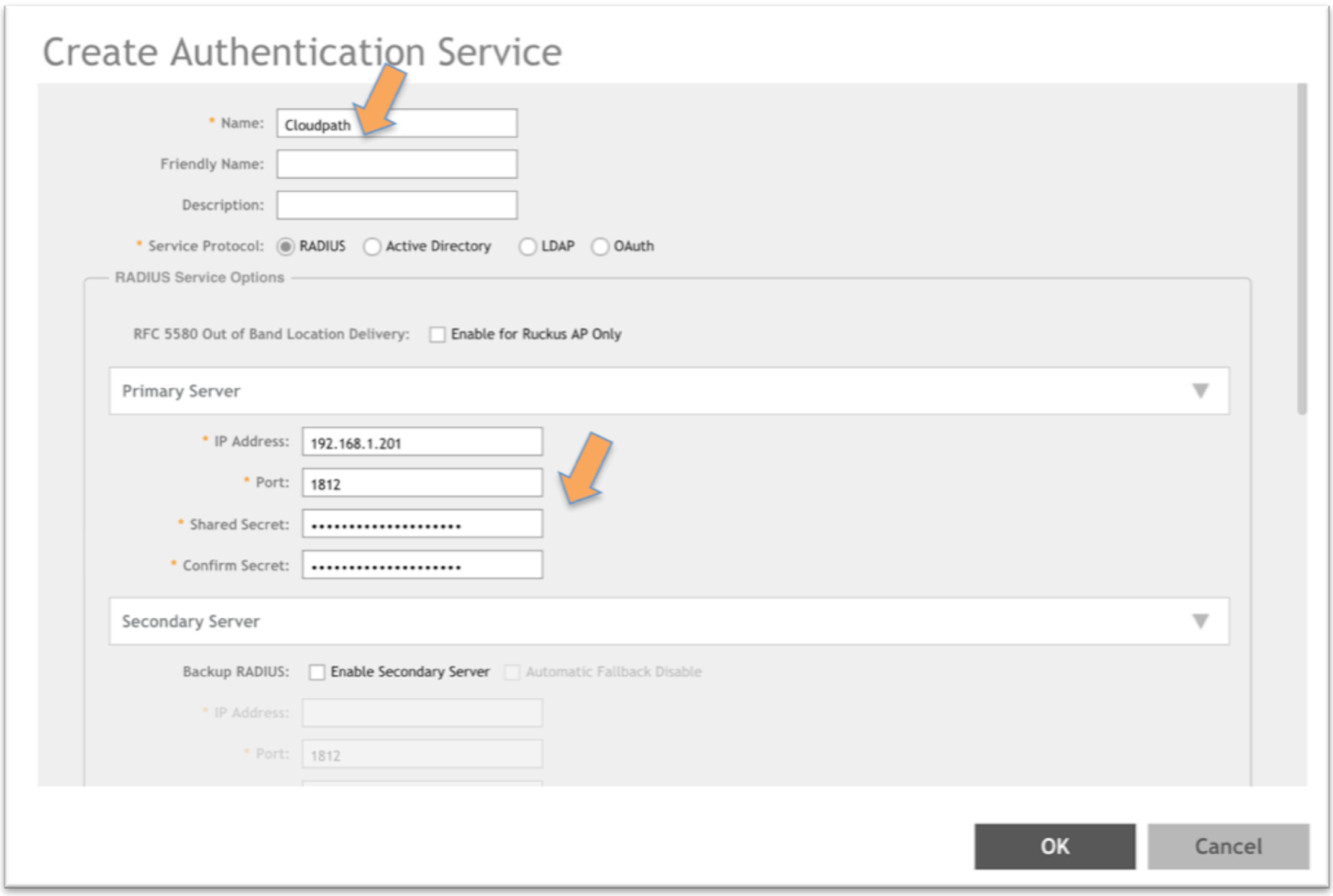
3) Add Cloudpath ES as a AAA server on the SmartZone

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.



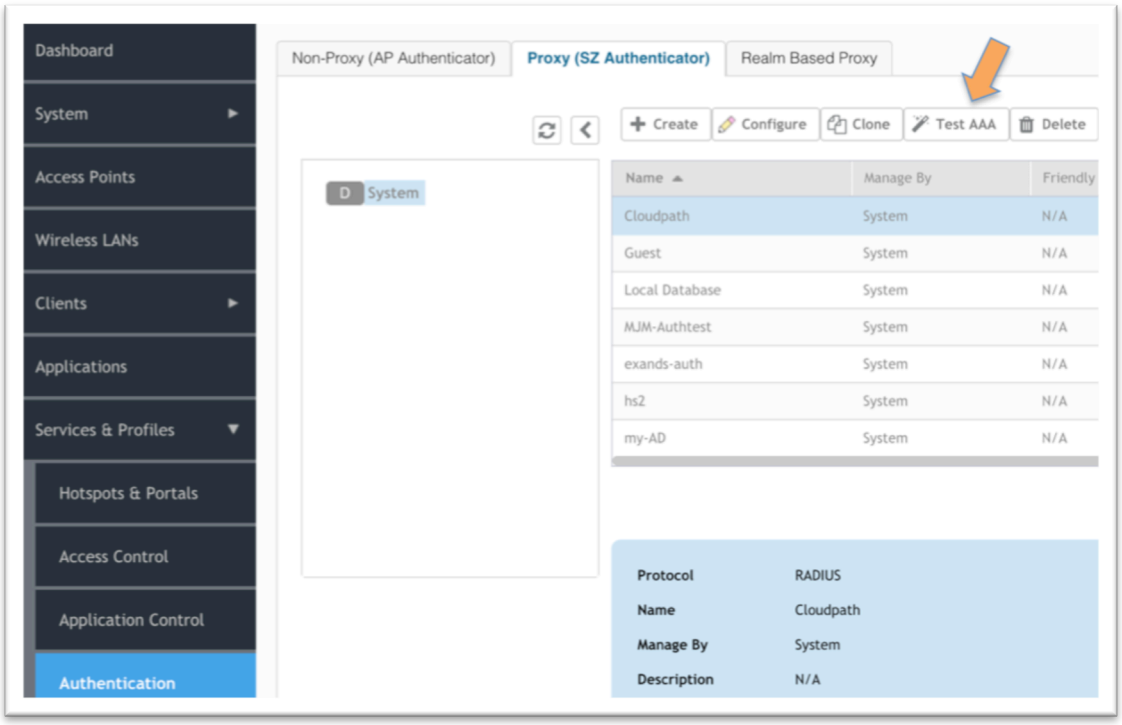
- Navigate to:
  - **Services & Profiles**
  - **Authentication**
  - **Proxy (SZ Authenticator)** tab

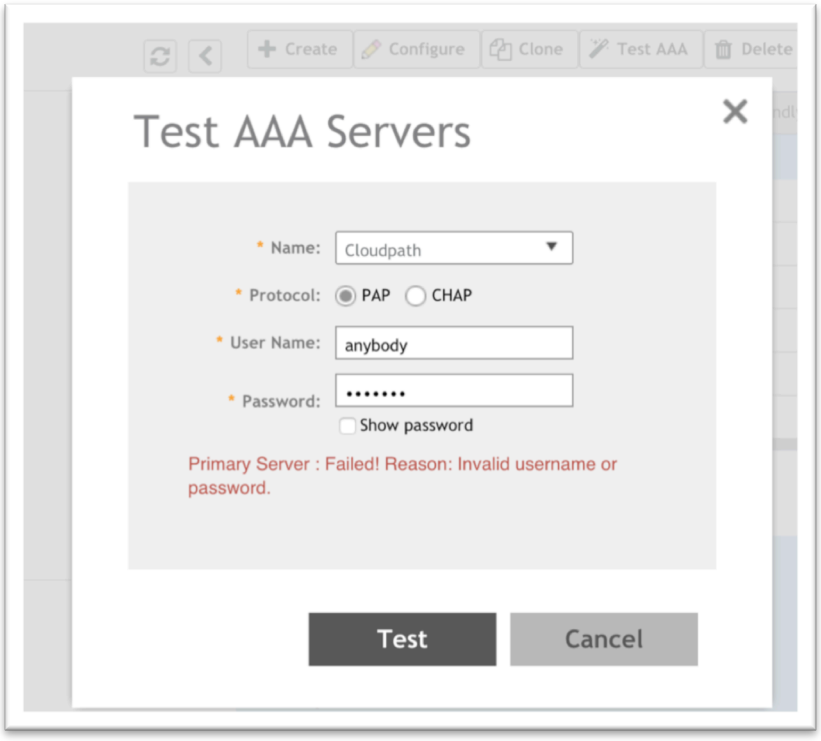
- If configuring non-Proxy, the correct **Zone** must be selected. Proxy is system wide, while Non-Proxy is zone specific
- Click on ***+ Create***



- 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** (1812 is standard)
    - Enter the **Shared Secret** in Shared Secret and Confirm Shared Secret
  - Click **OK**

4) Test the AAA connection





- 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

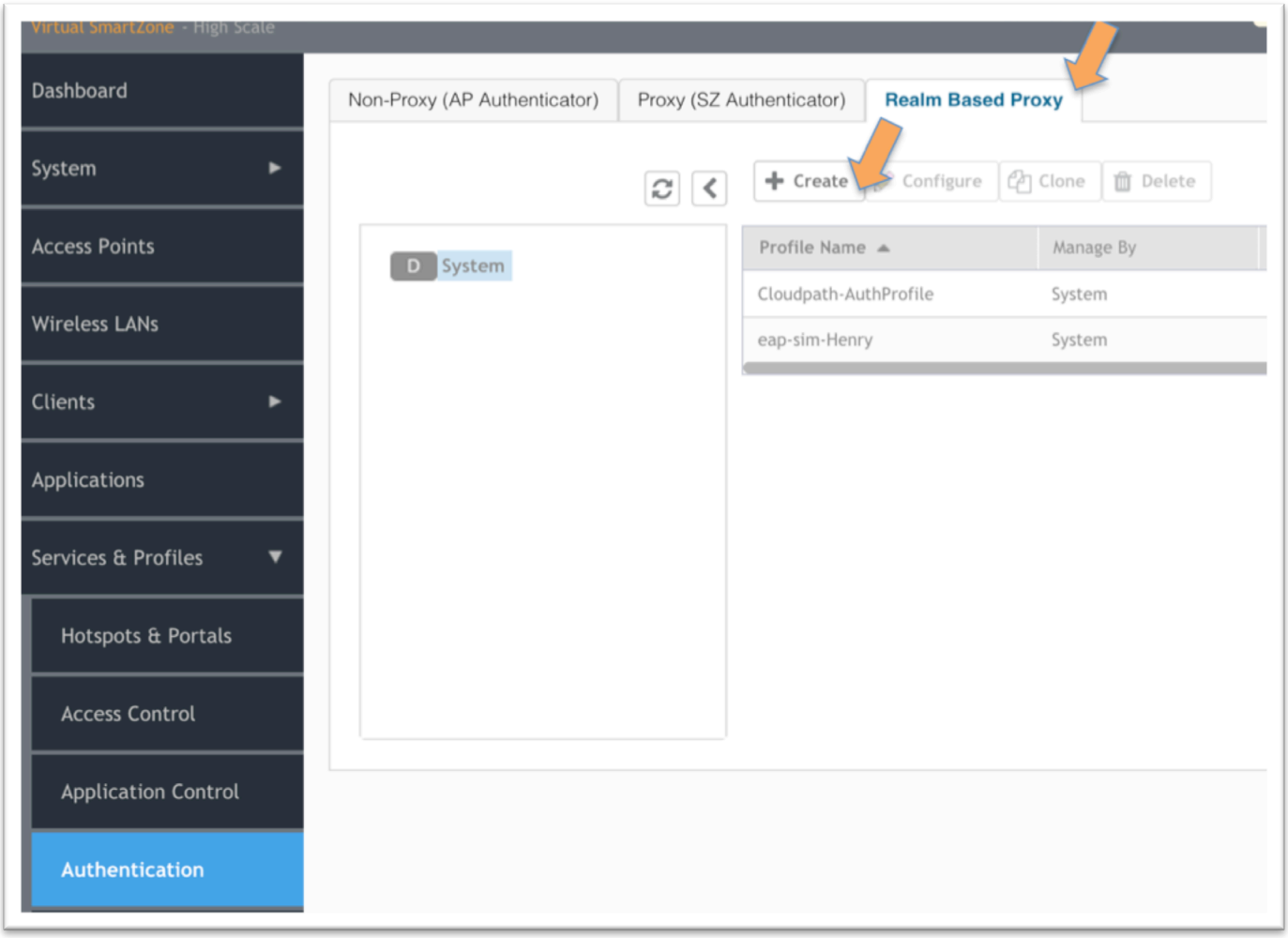
A Proxy AAA server is used when the APs send authentication/accounting messages to the SmartZone and the SmartZone forwards those messages to the AAA server. It centralizes authentication and the RADIUS server needs to allow only one RADIUS client, the SmartZone.

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

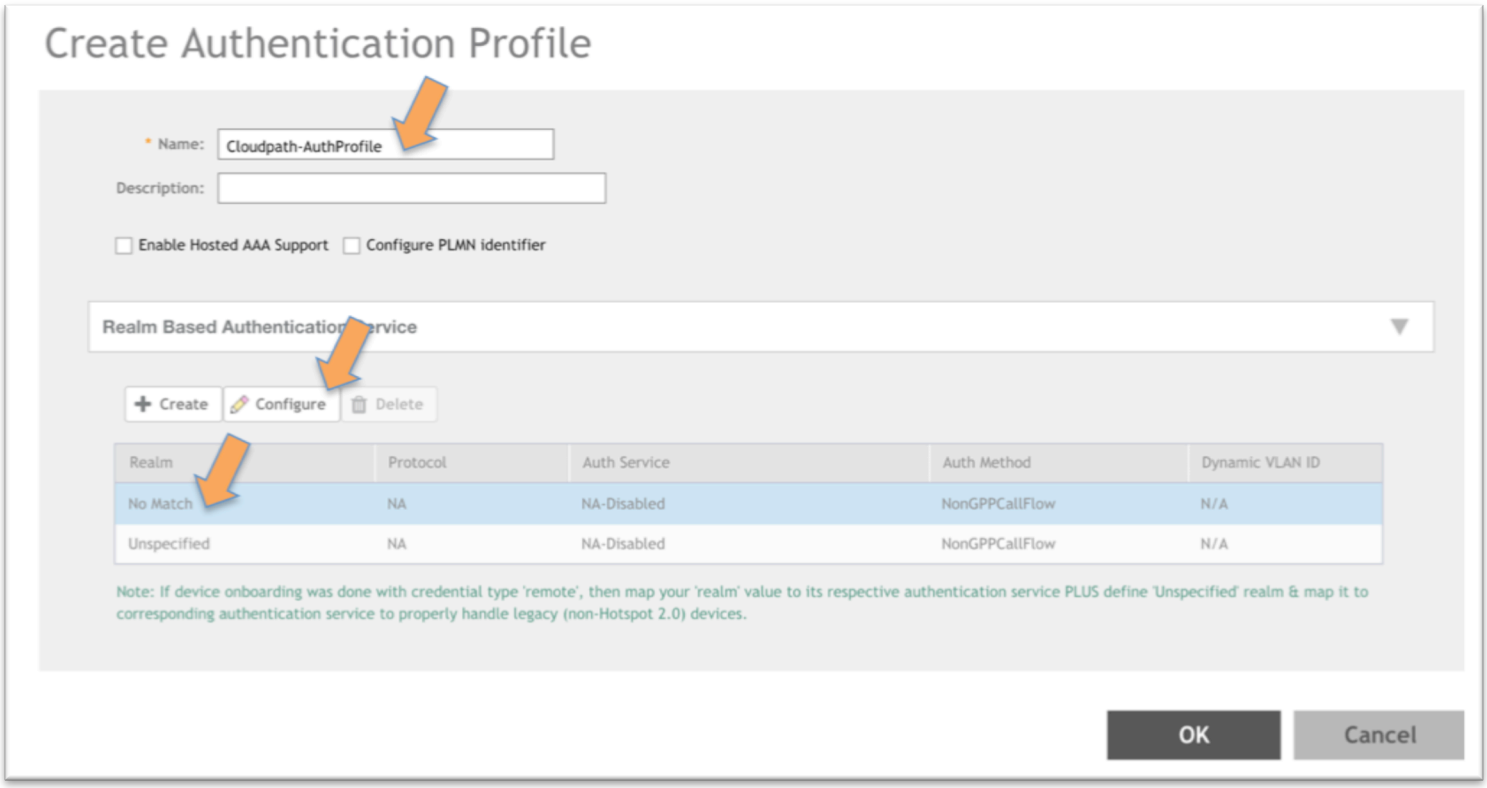
A Realm Based Proxy AAA Profile is needed when using Proxy AAA on the vSZ-H or the SZ-300. It is architecturally necessary for large service providers, but in the overwhelming majority of enterprise and K-12 deployments it is merely a slightly annoying additonal configuration detail. If multiple realm 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

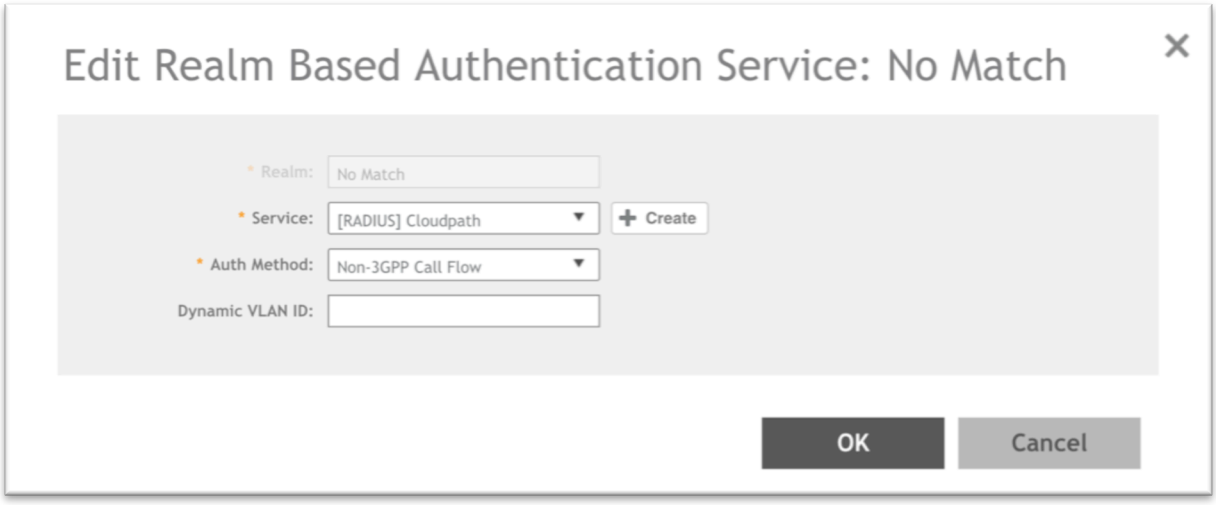
This step is not necessary on the vSZ-E or the SZ-100 platforms, and is not necessary on any platform when configuring a Non-Proxy AAA server. For 90% of vSZ-H users, this is the exact configuration.



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



- 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**



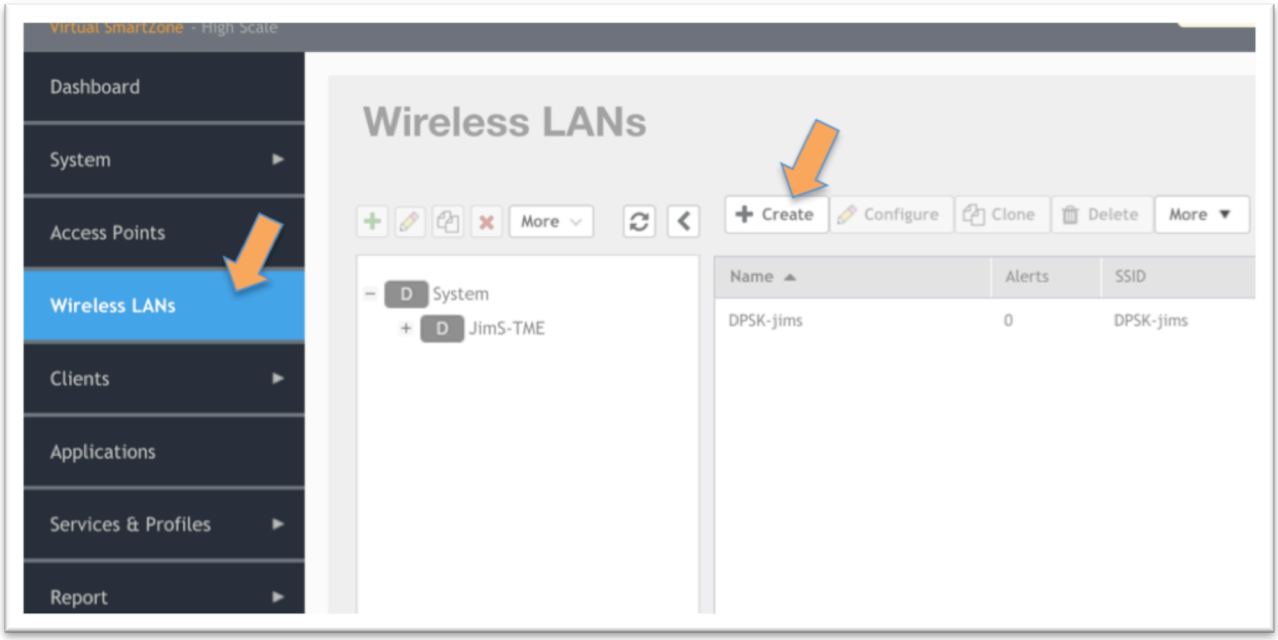
- In the Edit Realm Based Authentication Service Window
  - From the **Service** drop down, Choose the previously created Authentication Server
  - From the **Auth Method** drop down, choose **Non-3GPP Call Flow**
  - Leave **Dynamic VLAN ID blank** – Dynamic VLANs can be enabled elsewhere
  - Click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

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

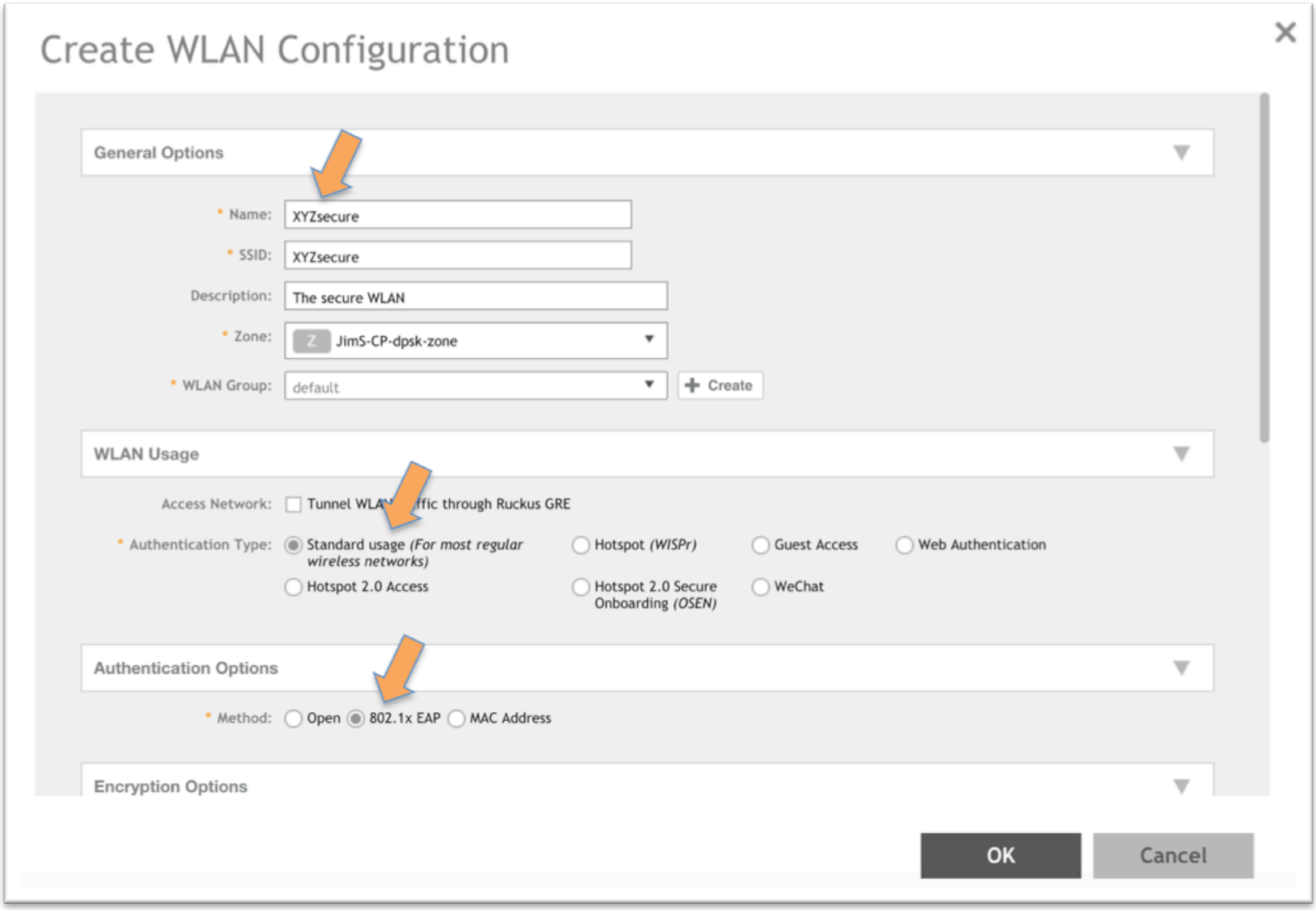
- In the Edit Realm Based Authentication Service Window
  - From the **Service** drop down, Choose the previously created Authentication Server
  - From the **Auth Method** drop down, choose **Non-3GPP Call Flow**
  - Leave **Dynamic VLAN ID blank** – Dynamic VLANs can be enabled elsewhere
  - Click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

- The Create Authentication Profile window returns
- Click **OK** to save

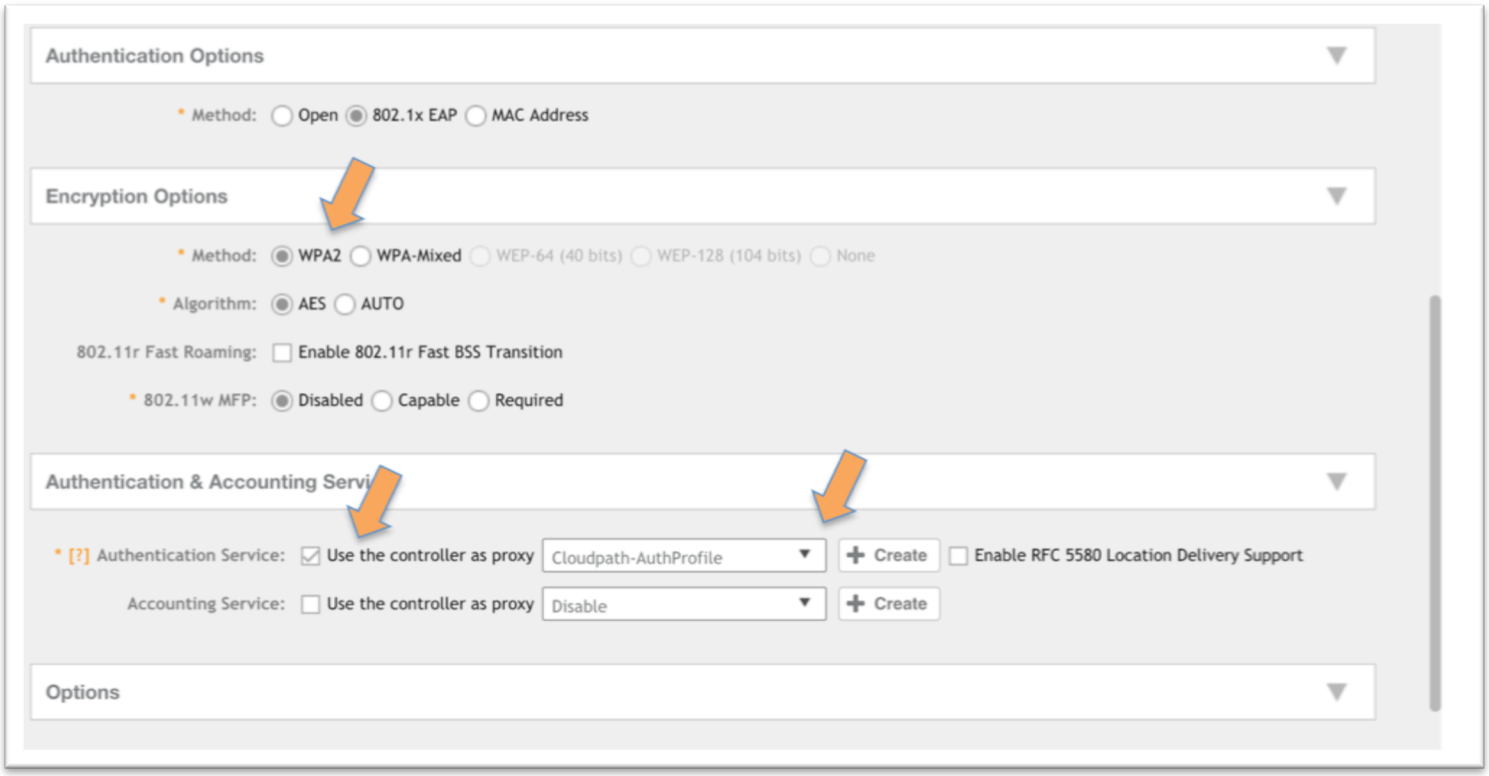
7) Create the Secure WLAN



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

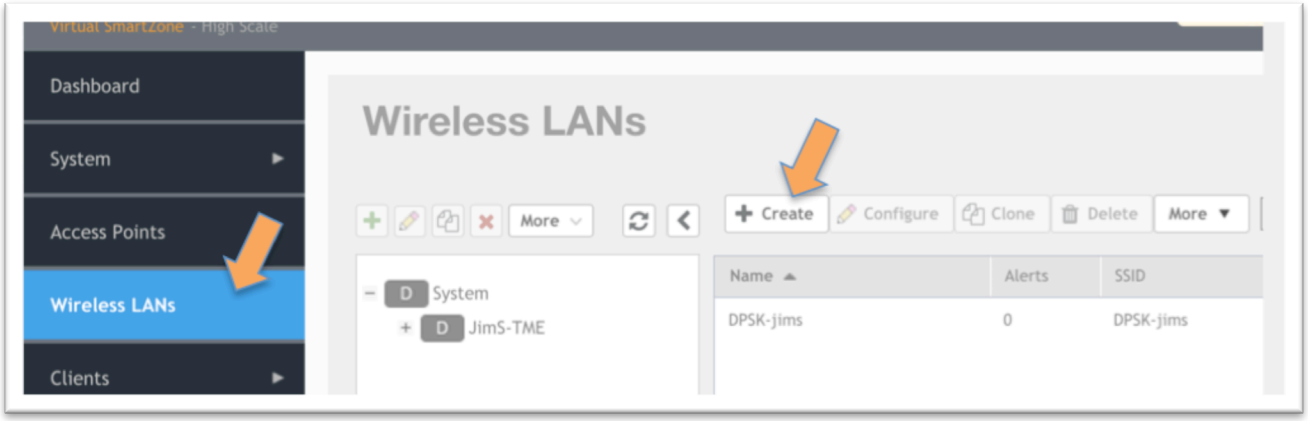


- In the **Create WLAN Configuration screen**
  - Fill in the **General Options**
    - **Name** the WLAN
    - **SSID**
    - Choose the **Zone**
    - Choose the **WLAN group** (the default group is fine)
  - Under WLAN Usage, choose **Standard Usage**
  - Authentication options, choose **802.1X EAP**

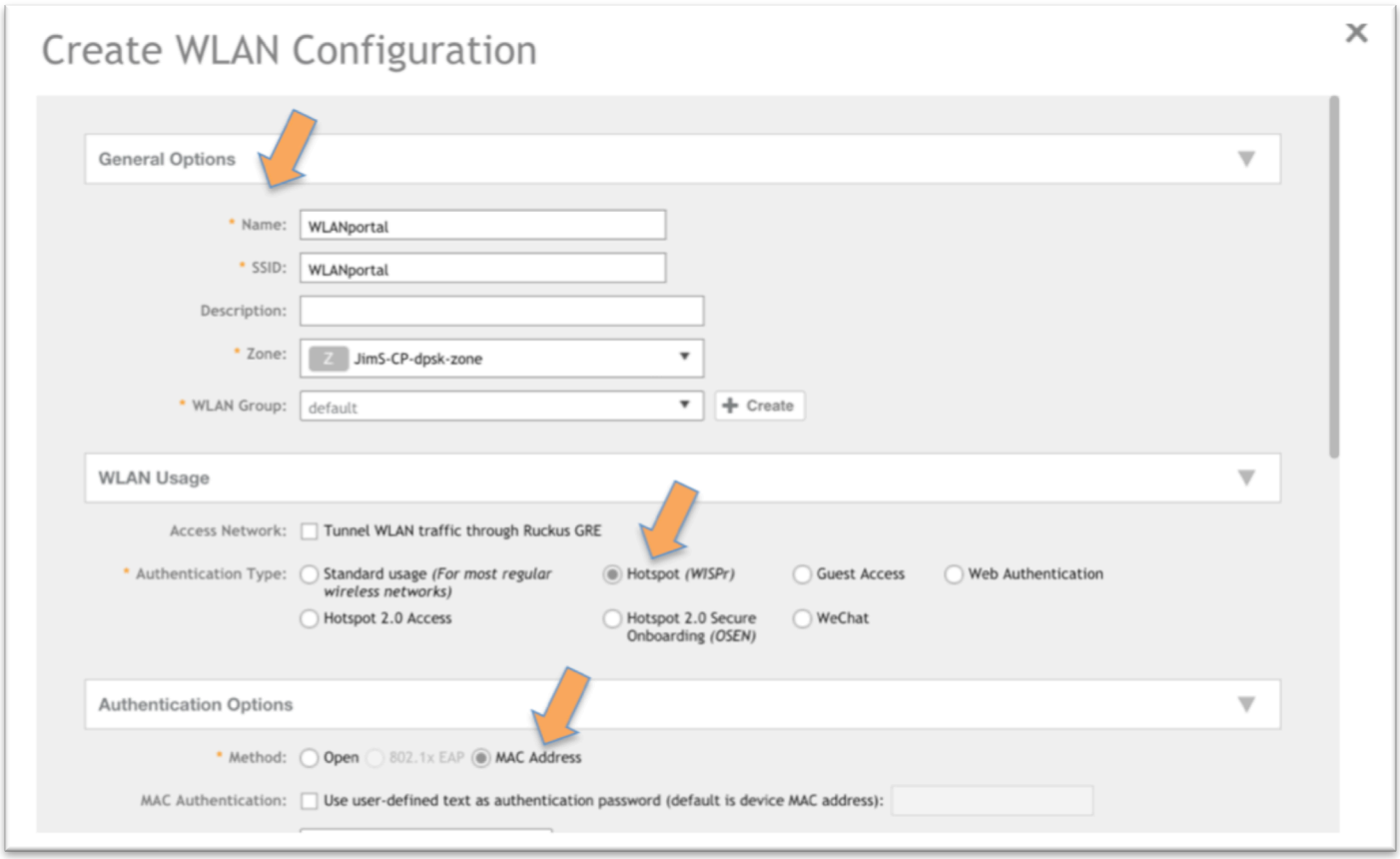


- Encryption Options
  - Method - choose **WPA2**
  - Algorithm – choose **AES**
- Authentication and Accounting
  - Choose **Use the controller as proxy**
  - From the drop down, **Choose the proxy** previously defined
- Click **OK** to save the WLAN

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



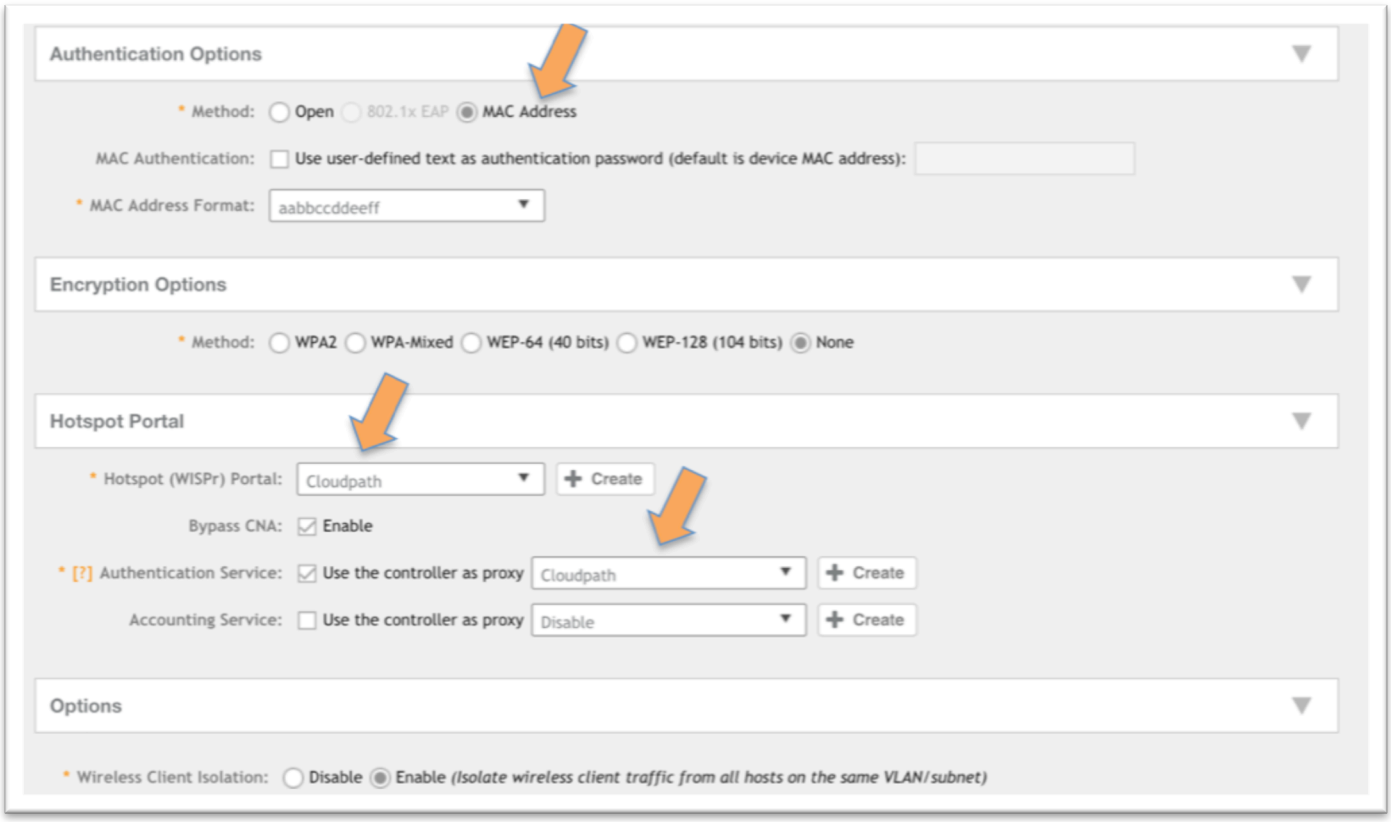
- Create another WLAN



- 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 WLAN Usage, choose **Hotspot (WISPr)**
- Authentication options, 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** - 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

```
its-MacBook-Pro-10:~ jim.stewart$ ssh admin@12.33.223.81
################################
#    Welcome to vSZ     #
################################
admin@12.33.223.81's password:
Last login: Mon Apr 24 19:00:30 2017
Please wait. CLI initializing...
Welcome to the Ruckus Virtual SmartZone - Essentials Command Line Interface
Version: 3.5.0.0.808
vSZ-E-SKO-1>
vSZ-E-SKO-1> config
% Privileged command. Please enable privileged mode first, run enable
command
vSZ-E-SKO-1> enable
Password: **************
vSZ-E-SKO-1# config
vSZ-E-SKO-1(config)# no encrypt-mac-ip
Do you want to continue to disable (or input 'no' to cancel)? [yes/no] yes
```

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**

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.

Cloudpath On SmartZone

Deploying a Cloudpath Workflow on a Ruckus SmartZone Controller

August 2017