COMMSCOPE®

RUCKUS®

Deployment Guide

RUCKUS & Mobimesh

August 2021

Table of Contents

5

Intended Audience

This document provides an overview of how to configure Ruckus products to support an WiSPr and RADIUS with Mobimesh. Step-by-step procedures for configuration and testing are demonstrated. Some knowledge of the SmartZone, RADIUS and 802.1X is recommended.

This document is written for and intended for use by technical engineers with background in Wi-Fi design and 802.11/wireless engineering principles.

For more information on how to configure CommScope products, please refer to the appropriate CommScope user guide available on the CommScope support site. https://www.commscope.com/SupportCenter/.

Overview

This document is a step by step guide to configure a CommScope Ruckus SmartZone network and make it interact correctly with MobiMESH inPiazza.

Assumptions

This guide applies to versions 5.2.x of the SmartZone Ruckus Controller and while performing the following steps, it is important to keep in mind the following basic points:

- an administrator account is needed on both SmartZone and inPiazza platforms.
- CommScope Ruckus APs must support Hotspot WISPr authentication method and they must be registered to the SmartZone controller.
- The SmartZone controller should be reachable at its public IP.
- The inPiazza dashboard should be reachable at its public URL.

SmartZone version number

You can get the firmware version of your controller by going to System - General Settings - About tab.

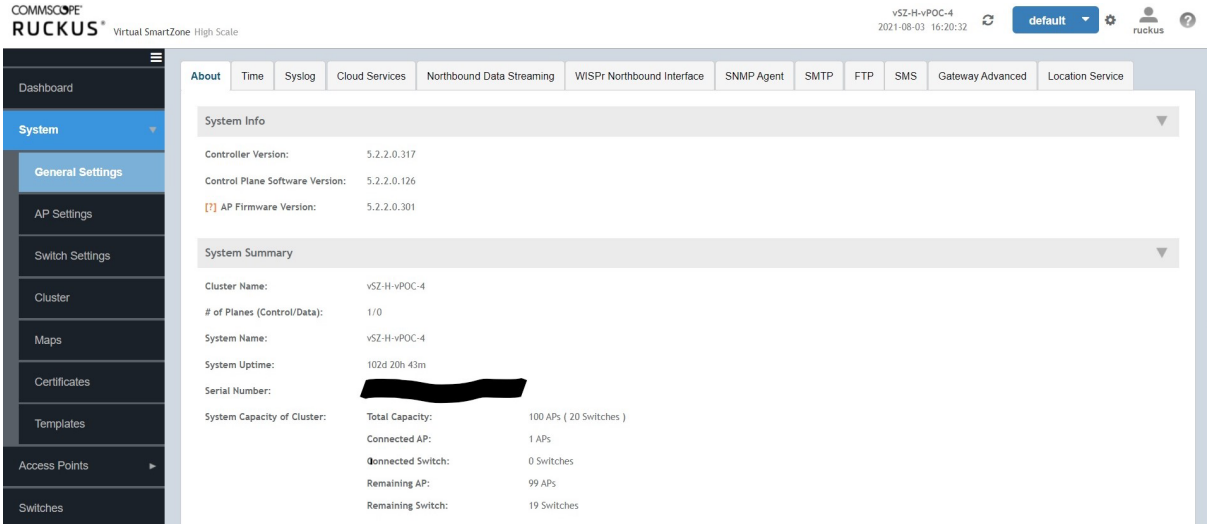

FIGURE 1: CONTROLLER VERSION

RADIUS services

Authentication

Services & profiles - Authentication - Proxy (SZ Authenticator) tab. You can create a new service by clicking the Create button.

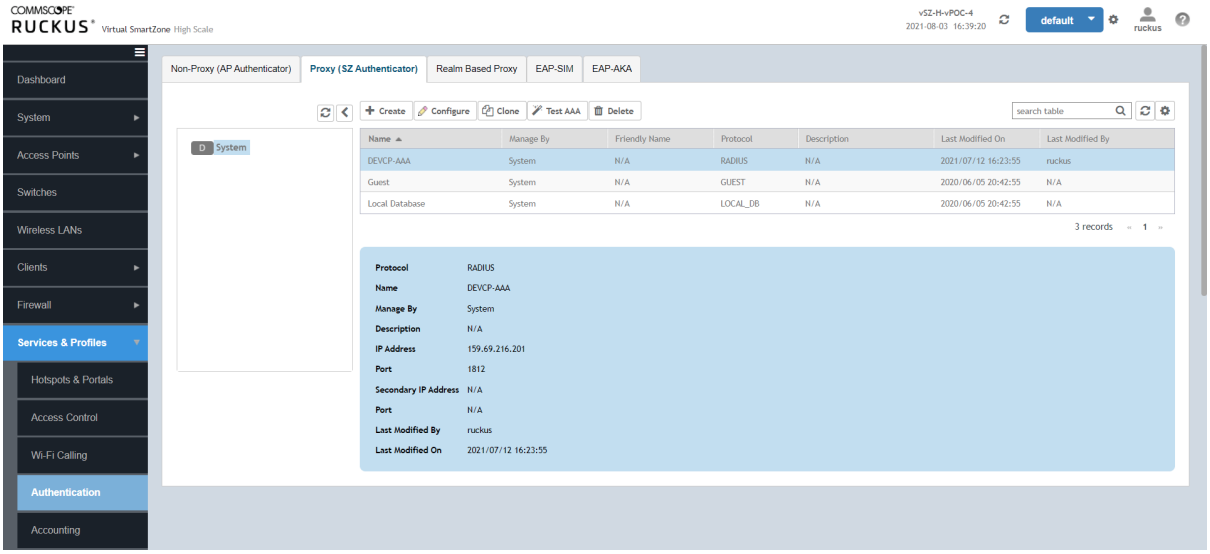

FIGURE 2: SZ AUTHENTICATOR

On the configuration page, enter the following data:

- Portal Name: (any name you wish)
- Service Protocol: RADIUS
- RFC 5580 Out of Band Location Delivery: OFF
- Primary Server:
- IP Address: 159.69.216.201
- Port: 1812
- Shared Secret: privately shared by MobiMESH
- Confirm Secret: privately shared by MobiMESH
- Health Check Policy:
- Response window: 20 sec
- Zombie period: 40 sec
- Revive Interval: 120 sec
- No Response Fail: No
- Rate limiting:
- Maximum Outstanding Request: 0
- Threshold: 0
- Sanity Timer: 10

Accounting

Go to *Services & profiles - Accounting - Proxy* tab. You can create a new service by clicking the *Create* button.

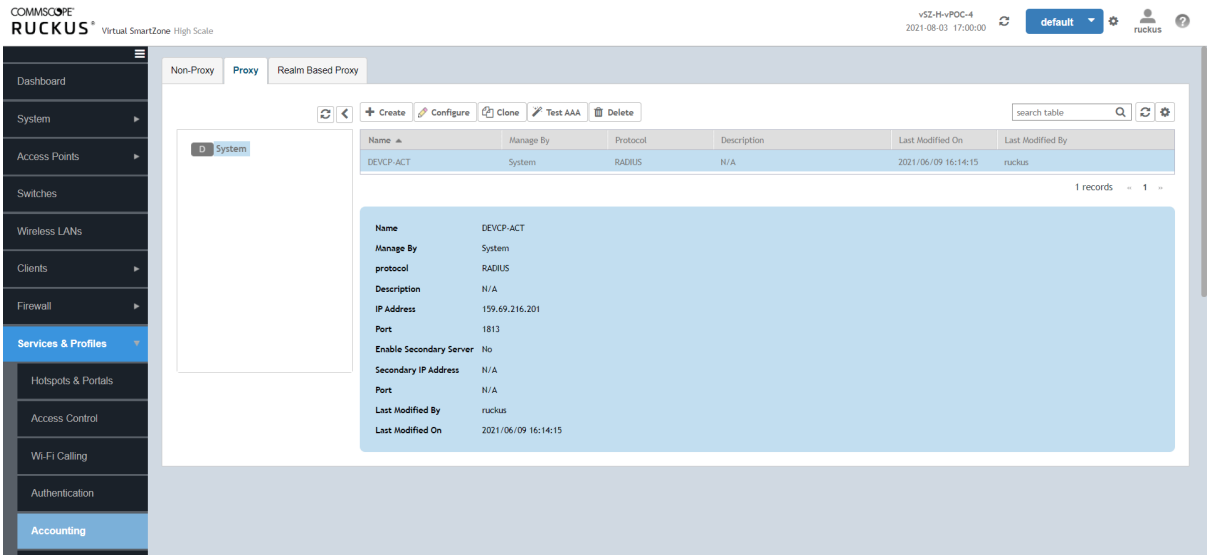

FIGURE 3: ACCOUNTING

On the configuration page, enter the following data:

- *Portal Name*: (any name)
- *Service Protocol*: RADIUS Accounting
- RFC 5580 Out of Band Location Delivery: OFF
- Primary Server:
- IP Address: 159.69.216.201
- Port: 1813
- Shared Secret: privately shared by MobiMESH
- Confirm Secret: privately shared by MobiMESH
- Health Check Policy:
- Response window: 20 sec
- Zombie period: 40 sec
- Revive Interval: 120 sec
- No Response Fail: No
- Rate limiting:
- Maximum Outstanding Request: 0
- Threshold: 0
- Sanity Timer: 10

WISPr/Hotspot settings

Go to Services & profiles - Hotspots & Portals - Hotspot (WISPr) tab. You can create a new service by clicking the Create button.

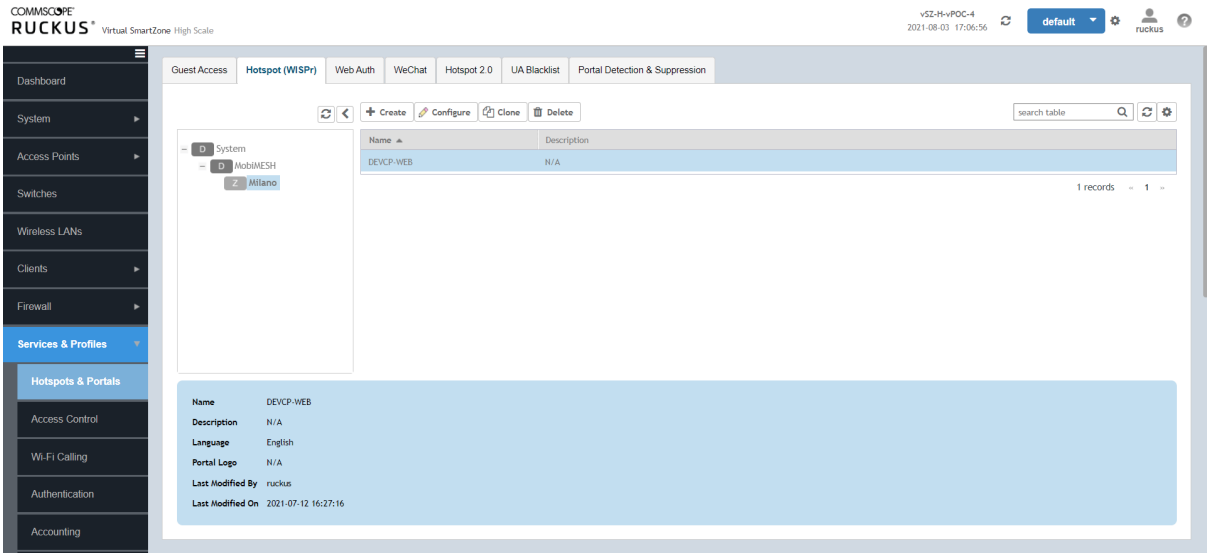

FIGURE 4: WISPR CONFIGURATION

On the configuration page, enter the following data:

- General Options
- Portal Name: (any name)
- Portal Description: optional
- Redirection
- Smart Client Support: None
- Logon URL: External
- Redirect unauthenticated user: Primary https://devcp.mobimesh.eu/start?vendor=ruckus
- Redirected MAC Format: aa:bb:cc:dd:ee:ff
- Start page: Redirect to the following URL: https://devcp.mobimesh.eu/outcome
- HTTPS Redirect: ON
- User Session:
- Session Timeout: 28800
- Grace Period: 1800
- Walled Garden: based on login authentication you have to insert some domains

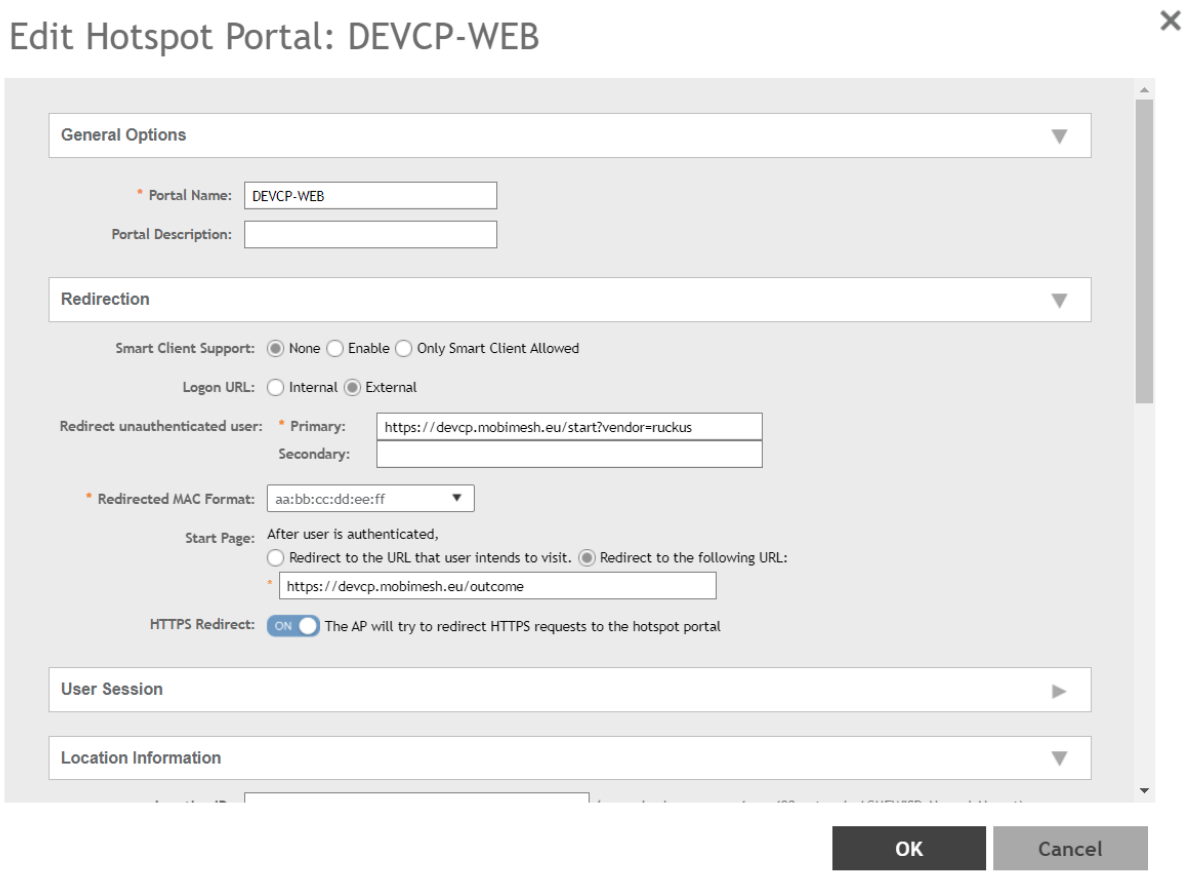

FIGURE 5: ADDING EXTERNAL PORTAL

Wireless LANs

Go to *Wireless LANs* - You can create a new wireless lan by clicking the *Create button.*

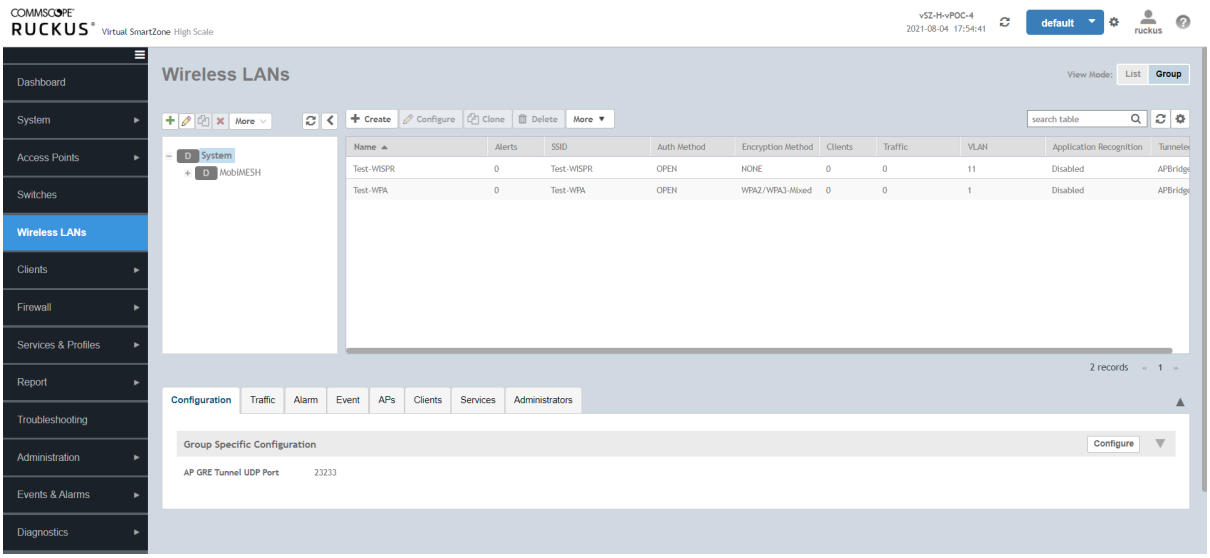

FIGURE 6: CONFIGURING WLAN

On the configuration page, enter the following data:

- Name: (any name)
- SSID: (any name)
- Authentication type: Hotspot(WISPr)
- Method: Open
- Encryption Options: None

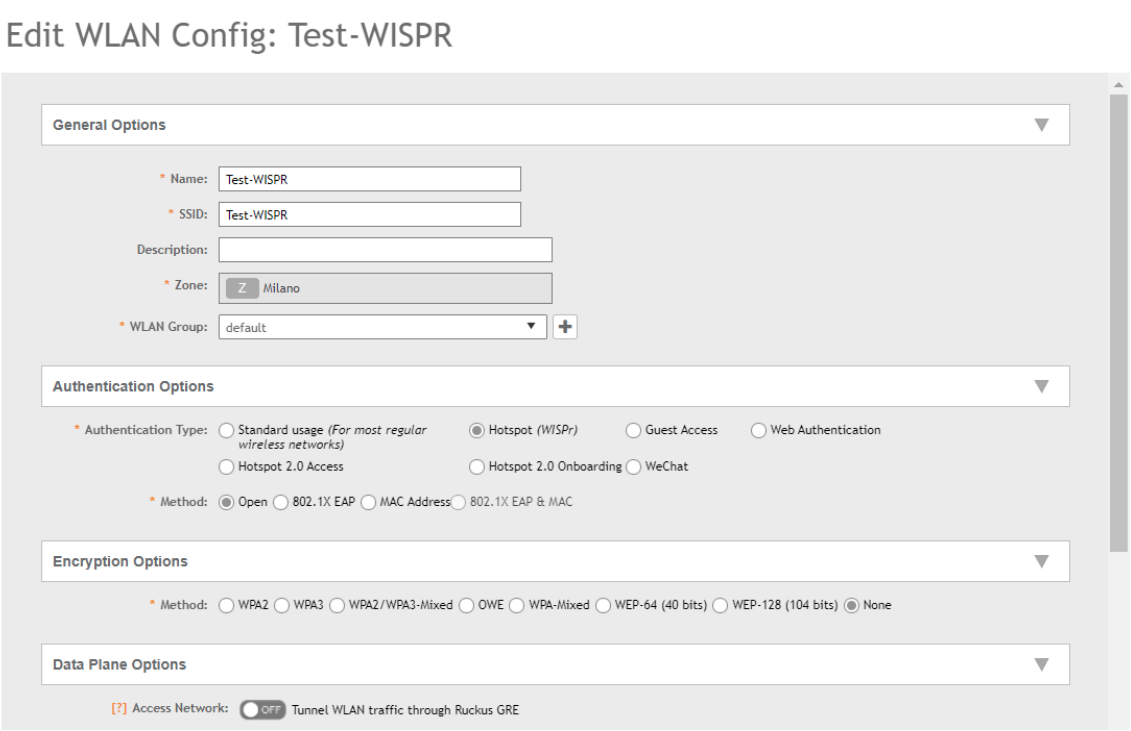

FIGURE 7: CREATING A WISPR WLAN

- Hotspot (WISPr) Portal: portal created in the “WISPr/Hotspot settings” section
- Bypass CNA: OFF
- Authentication Service: Use the controller as proxy & Authentication service created in” Authentication” section
- Accounting Service: Use the controller as proxy & Accounting service created in ”Accounting” section
- NAS ID: User-defined (any name)
- NAS Request Timeout: 3
- NAS MAx Number of Retries: 2
- NAS Reconnect Primary: 5
- Called Station ID: AP MAC
- NAS IP: User-defined *132.242.138.24*
- Single Session ID Accounting: ON
- Vendor Specific Attribute Profile: Disable

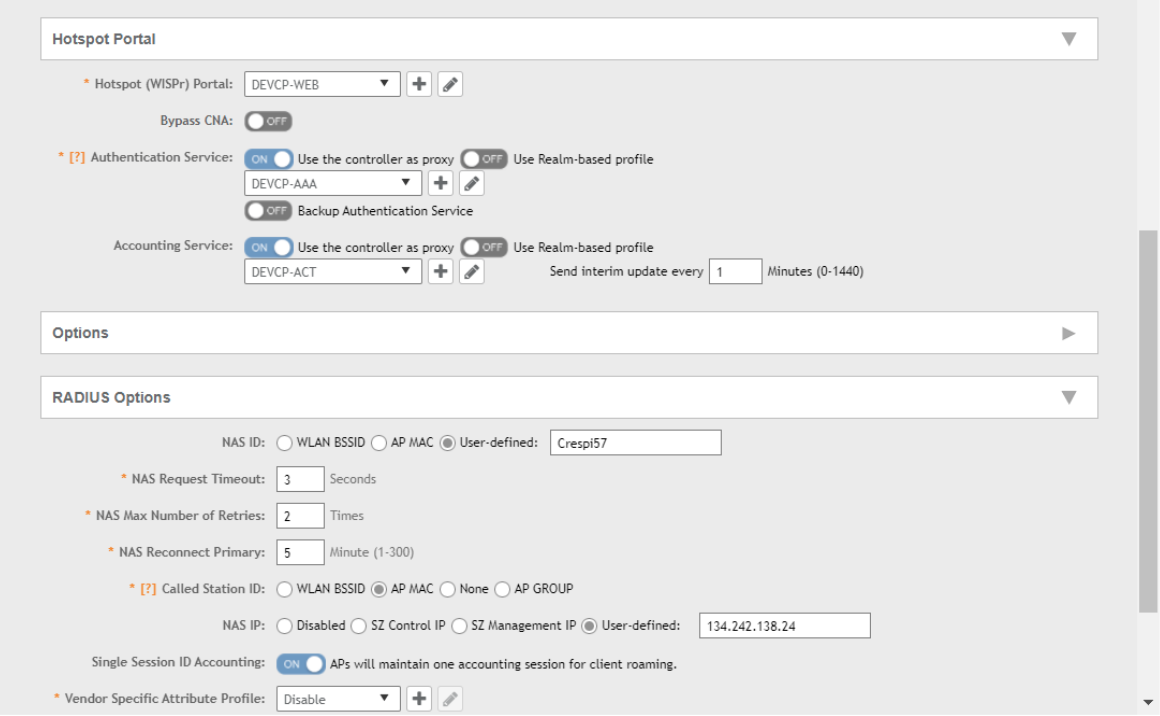

FIGURE 8: ACTIVATING AAA

User Roles

If you want to assign a specific user profile via RADIUS, for example you want to define an ad hoc ACL to surf the net, you can create different profiles for different use cases.

If you use “click&surf” login you will have only web browsing (http/https) instead if you use “user&password” login every type of traffic will be permitted.

In this case we will create an ACL “WebOnly” where it permits only TCP/80, TCP/443 and DNS traffic.

In order to create this profile you have to do:

- Go to *Firewall - L3 Access Control* and create an L3 Access Control Policy with these parameters:

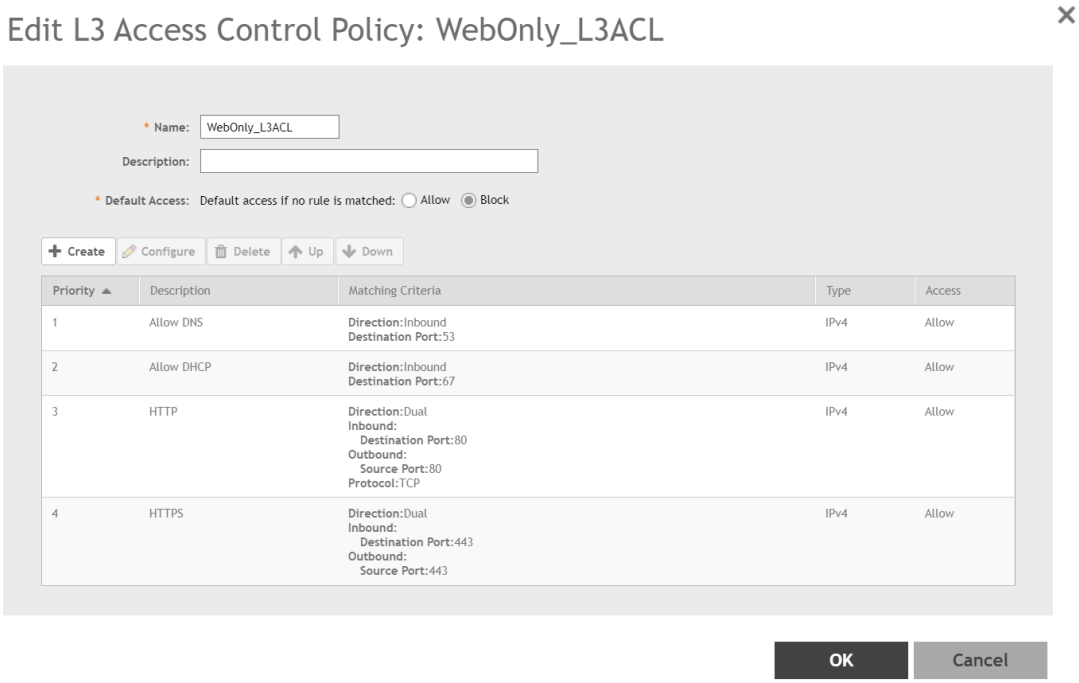

FIGURE 9: ADDING L3 ACL

Go to *Firewall - profile tab* and create a new firewall profile with these parameters:

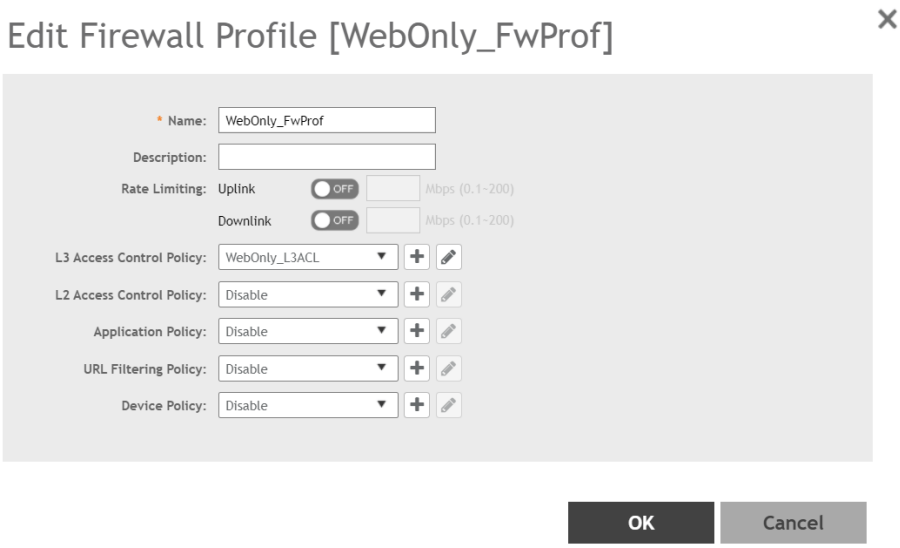

FIGURE 10: WLAN PROFILE

In L3 Access Control Policy chose the “L3 Access Control Policy” created in the previous point.

Go to *Clients - User roles* and create a new User role with these parameters:

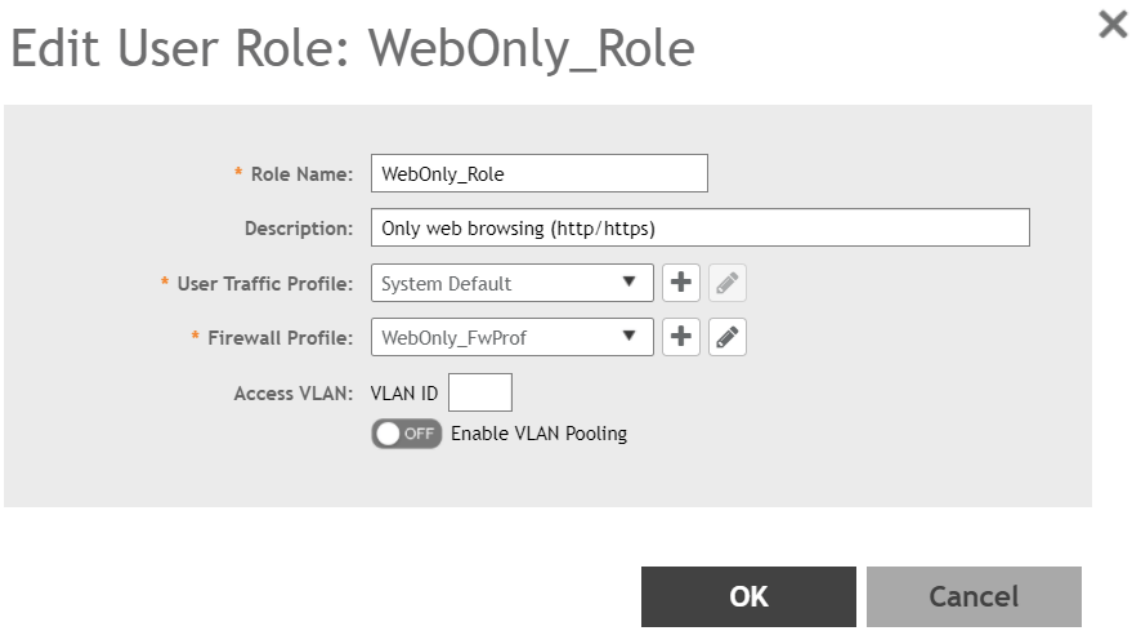

FIGURE 11: WLAN USER ROLE PROFILE

In Firewall Profile chose the “Firewall profile” created in the previous point.

Then you can use this user role in Authentication process in the “User Role Mapping” section. For example, “WebOnly” is the value of attribute “Filter-Id” returned by the RADIUS server in the auth-reply response.

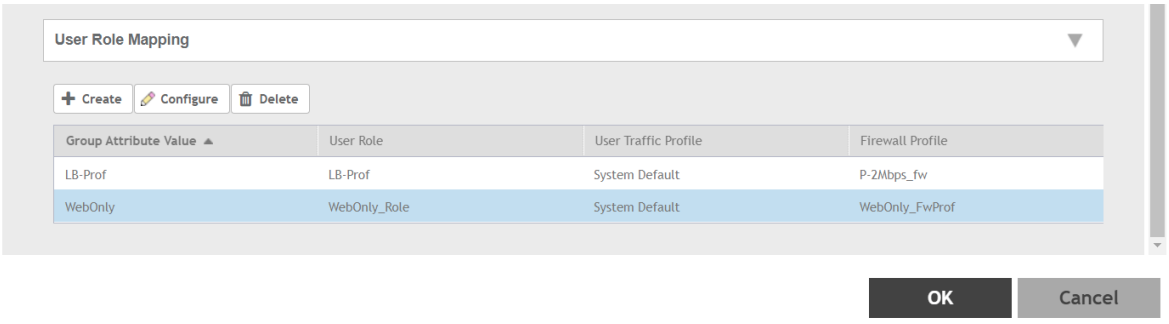

FIGURE 12: USER ROLE MAPPING

MobiMESH inPiazza Captive Portal

Go to Authenticator: https://devcp.mobimesh.eu:8443/aaa-ui/

Add new Service Profile

Go to System - Service profile. You can create a new service profile by clicking the Add new button.

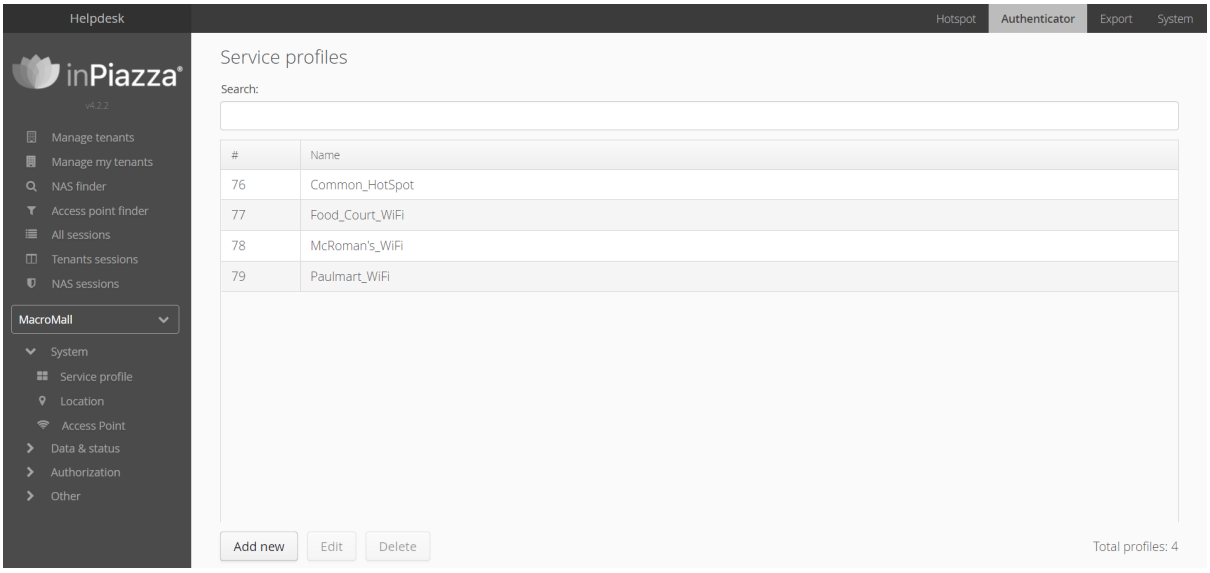

FIGURE 13: NEW SERVICE PROFILE

On the configuration page, enter the following data:

- Name: (any name)
- Business logic: (StaticLimits | DailyLimits)
- Selected location: None

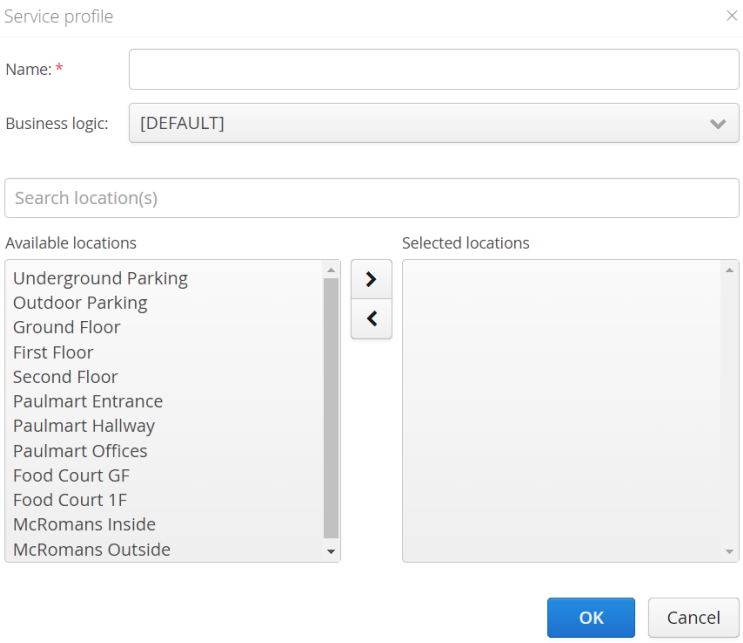

FIGURE 14: ADDING SERVICE PROFILE

Add new Location

Go to *System - Location.* You can create a new service profile by clicking the *Add new button.*

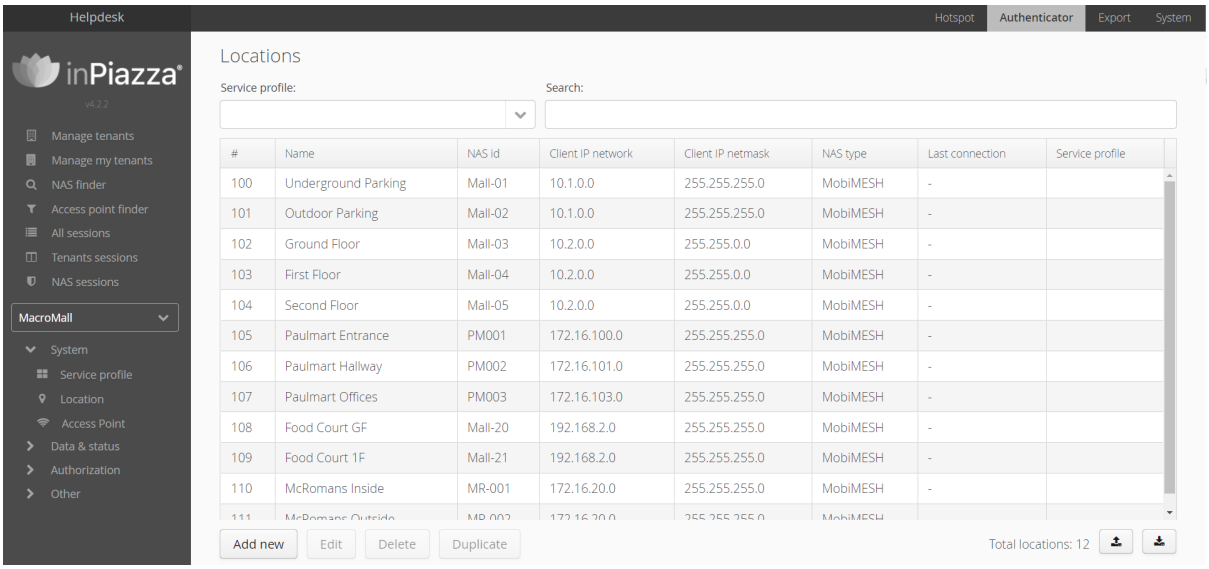

FIGURE 15: ADDING LOCATION

On the configuration page, enter the following data:

- Nas type: Ruckus
- Service profile: Service Profile name created in the previous point
- Name: (any name)
- CoA:
- Nas id: (selected name in Wireless LANs section)
- Client IP network: (selected ipin Wireless LANs section)
- Client IP netmask: (selected maskin Wireless LANs section)
- NAS IP list:
- Secret: (Shared secret messages sent from NAS IPs)

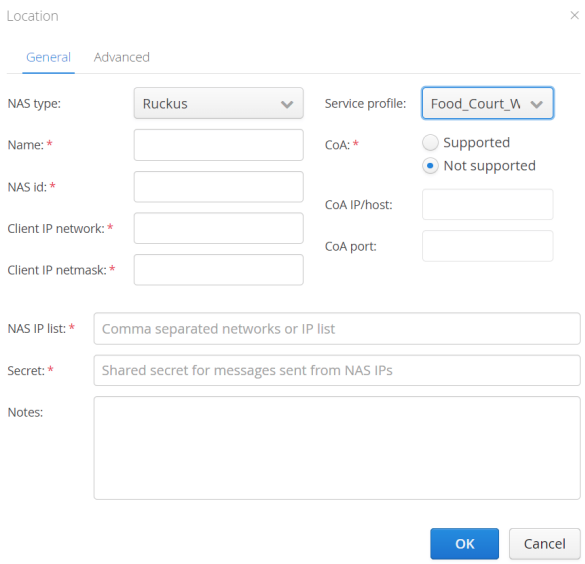

FIGURE 16: MODIFYING LOCATION INFORMATION

This information depends on the specific configuration of the MobiMESH inPiazza Captive Portal; different operators host the platform in different clouds; therefore the parameters depend on the specific instance. Please ask such information to the operator/reseller/distributor that is providing the MobiMESH inPiazza solution.

Add new Access Point

Go to *System - Access point.* You can create a new service profile by clicking the *Add new button.*

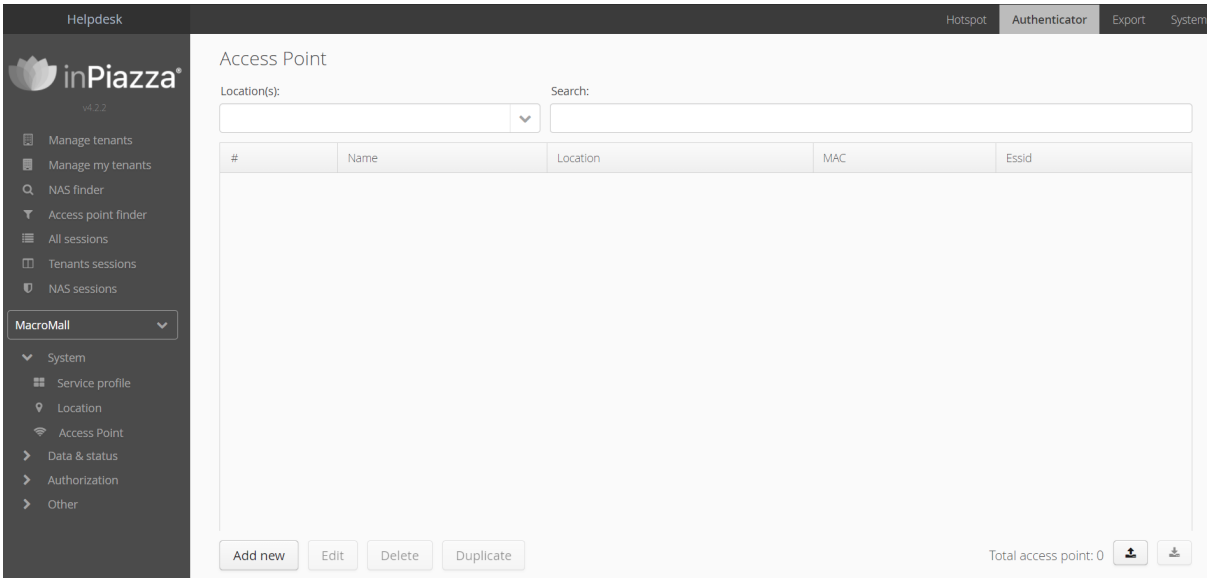

FIGURE 17: ADDING ACCESS POINT

On the configuration page, enter the following data:

- Location: Location name created in the previous point
- MAC Address: (aa:bb:cc:dd:ee:ff)
- Name: (any name)
- Essid: (selected name in Wireless LANs section)
- Description: (any description)

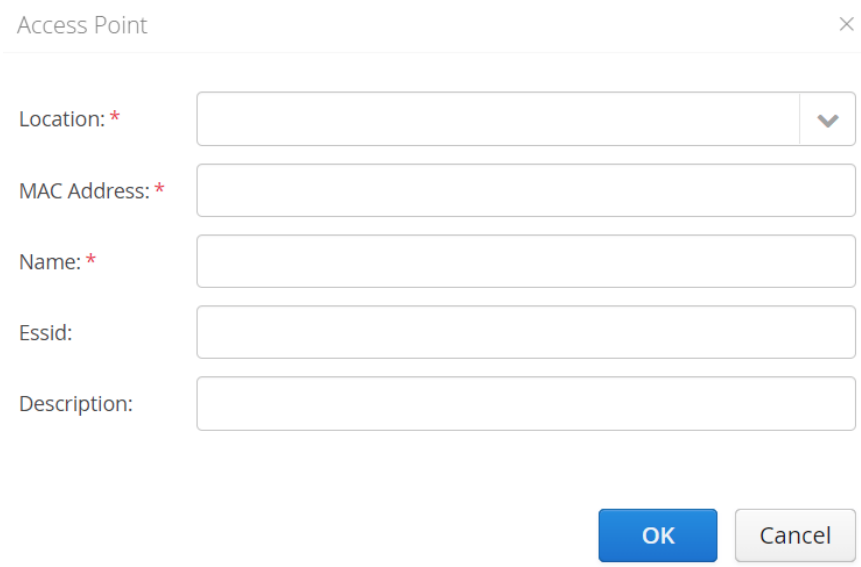

FIGURE 18: MODIFYING ACCESS POINT

Summary

The following document demonstrated how configuring SmartZone and Mobimesh. For further or complex configurations, please contact #ProductSolutions-TechMarketing@commscope.com

Ruckus solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- Ruckus Wi-Fi Access Points
- Ruckus ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

COMMSCOPE®

RUCKUS®

commscope.com

Visit our website or contact your local CommScope representative for more information.