



# **Deployment Guide**

RUCKUS & Mobimesh August 2021



### **Table of Contents**

TABLE OF CONTENTS	2
INTENDED AUDIENCE	3
OVERVIEW	4
Assumptions	4
SmartZone version number	5
RADIUS services	5
WISPr/Hotspot settings	8
Wireless LANs	10
MobiMESH inPiazza Captive Portal	15
Add new Location	16
Add new Access Point	18
SUMMARY	20

### **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.

COMMSCOPE" RUCKUS <sup>®</sup> Virtual SmartZ	one High Scal	le							2	vSZ-H-v 021-08-03	POC-4 16:20:32	lefault 🔻 🔅	rucku	15 0
E Dashboard	About	Time	Syslog	Cloud Services	Northbound Data Streaming	WISPr Northbound Interface	SNMP Agent	SMTP	FTP	SMS	Gateway Advanced	Location Servic	e	
System 🔻	Syste	em Info												V
General Settings	Contro	oller Versi ol Plane So	on: oftware Vers	5.2.2.0.317 sion: 5.2.2.0.126										
AP Settings	[?] AP	P Firmware	Version:	5.2.2.0.301										
Switch Settings	Syste	em Summ	ary											V
Cluster	Cluste # of P	er Name: lanes (Cor	itrol/Data):	vSZ-H-vPOC	-4									
Maps	System	m Name:		vSZ-H-vPOC	-4									
Certificates	Syster Serial	m Uptime: Number:		102d 20h 43	im in the second se									
Templates	Syster	m Capacity	of Cluster:	Total Capac Connected	tity: 100 APs AP: 1 APs	( 20 Switches )								
Access Points				Connected	Switch: 0 Switch	nes								
Switches				Remaining. Remaining	AP: 99 APs Switch: 19 Switc	ches								

### 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.

COMMSCOPE" RUCKUS <sup>*</sup> Virtual SmartZo	one High Scale										vSZ-H-vPOC-4 2021-08-03 16:39:20	default 🔻	¢	15
=	Non-Proxy (AP Authenticator)	Proxy (SZ A	(uthenticator)	Realm Ba	ised Proxy	EAP-SIM	FAP-AKA							
Dashboard	, (		,		,									
System ►		2 <	🕂 Create 🖉	Configure	Clone	🎢 Test AAA	Delete				se	arch table	Q 2	٥
	D System		Name 🔺		Mai	nage By	Frier	idly Name	Protocol	Description	Last Modified On	Last Modified B	ý.	
Access Points			DEVCP-AAA		Syst	tem	N/A		RADIUS	N/A	2021/07/12 16:23:55	ruckus		
Switches			Guest		Syst	tem	N/A		GUEST	N/A	2020/06/05 20:42:55	N/A		
			Local Database		Syst	tem	N/A		LOCAL_DB	N/A	2020/06/05 20:42:55	N/A		
Wireless LANs												3 recor	ds « 1	2
Clients ►			Protocol	RA	DIUS									
Firewall			Name	DE	EVCP-AAA									
Filewali F			Manage By	Sy	stem									
Services & Profiles 🔹 🔻			Description IP Address	N/ 15	'A 9.69.216.20	1								
			Port	18	12									
Hotspots & Portals			Secondary IP	Address N/	A									
Access Control			Port	N/	A									
			Last Modified	d By rus	ckus									
Wi-Fi Calling			Last Modified	d On 20	21/07/12 16	5:23:55								
Authentication														
Accounting														



### **Mobimesh Deployment Guide**



- 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.

COMMSCOPE RUCKUS <sup>*</sup> Virtual SmartZone High Scale					vSZ-H-vPOC-4 2021-08-03 17:00:00	C default 🔹 🌣 🔔 📀
Dashboard Non-Proxy Proxy Realm Based Proxy						
System ►	🕂 Create 🖉 Configure	🖆 Clone 🎢 Test AAA 📋	Delete			search table Q
D System	Name 🔺	Manage By	Protocol	Description	Last Modified On	Last Modified By
Access Points	DEVCP-ACT	System	RADIUS	N/A	2021/06/09 16:14:15	ruckus
Switches						1 records « 1 »
Wireless LANs	Name	DEVCP-ACT				
Cliente	Manage By	System				
	Description	N/A				
Firewall	IP Address	159.69.216.201				
	Port	1813				
	Enable Secondary Server	No				
Hotspots & Portais	Secondary IP Address	N/A				
	Port	N/A ruckus				
Access Control	Last Modified On	2021/06/09 16:14:15				
Wi-Fi Calling						
Authentication						
Accounting						

#### FIGURE 3: ACCOUNTING

- *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.

COMMSCOPE" RUCKUS <sup>®</sup> Virtual SmartZone High Scale		vSZ-H-vPOC-4 2021-08-03 17:06:56 2 default 🔹 🌣 🔔 🕜
Guest Access Hotspot (WISPr) Web /	uth WeChat Hotspot 2.0 UA Blacklist Portal Detection & Suppression	
System	+ Create 2 Configure 2 Clone 1 Delete	search table Q 2 4
Access Points	Name ▲         Description           DEVCP.WEB         N/A	
Switches		1 records « 1 »
Wireless LANs		
Clients ►		
Firewall ►		
Services & Profiles 🛛 🔻		
Hotspots & Portais		
Access Control Description N/A		
Wi-Fi Calling Portal Logo N/A		
Authentication Last Modified By ruckus Last Modified On 2021-07-12 16:27:16		
Accounting		

#### FIGURE 4: WISPR CONFIGURATION

- 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

### Edit Hotspot Portal: DEVCP-WEB

General Options		
* Portal Name:	DEVCP-WEB	
Portal Description:		
Redirection		
Smart Client Suppor	t:   None  Enable  Only Smart Client Allowed	
Logon UR	.: 🕐 Internal 🛞 External	
Redirect unauthenticated us	er: * Primary: https://devcp.mobimesh.eu/start?vendor=ruckus Secondary:	
* Redirected MAC Forma	t: aa:bb:cc:dd:ee:ff 🔹	
Start Pag	e:       After user is authenticated,         O       Redirect to the URL that user intends to visit. (a) Redirect to the following URL:         *       https://devcp.mobimesh.eu/outcome	
HTTPS Redired	t: ON O The AP will try to redirect HTTPS requests to the hotspot portal	
User Session		►
Location Information		
		_

FIGURE 5: ADDING EXTERNAL PORTAL





### Wireless LANs

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

	tZone High Scale										v <b>SZ-H-vP</b> 2021-08-04	0C-4 17:54:41	default 🔻 🔅 📕	kus 🕜
E Dashboard	Wireless	LANs											View Mode: List	Group
System ►	+ 🖉 🖓 🗙 M	ore 🗸 📿	< + Create	🖉 Configur	e 🖓 Clone	1 Delete Ma	re 🔻						search table Q	2 ¢
A	- D System		Name 🔺		Ale	erts SSID		Auth Method	Encryption Method	Clients	Traffic	VLAN	Application Recognition	Tunneler
Access Points	E D Mobi/	AESH	Test-WISP	R	0	Test-WIS	PR	OPEN	NONE	0	0	11	Disabled	APBridge
Switches			Test-WPA		0	Test-WP/		OPEN	WPA2/WPA3-Mixed	0	0	1	Disabled	APBridge
Wireless LANs														
Clients ►														
Firewall ►														
Services & Profiles														_
Report ►													2 records «	1 »
Troubleshooting	Configuration	Traffic Alarm	Event AP	s Clients	Services	Administrators								
	Group Specif	ic Configuration											Configure	
Administration	AP GRE Tunnel	UDP Port 23	233										oomigae	
Events & Alarms														
Diagnostics														

#### FIGURE 6: CONFIGURING WLAN

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

### Edit WLAN Config: Test-WISPR

		▼
* Name:	Test-WISPR	
* SSID:	Test-WISPR	
Description:		
* Zone:	Z Milano	
* WLAN Group:	default 🔻 🕇	
	·, ·	
Authentication Option	5	▼
* Authentication Type:	Standard usage (For most regular  Hotspot (WISPr) Guest Access Web Authentication wireless networks)	
	O Hotspot 2.0 Access O Hotspot 2.0 Onboarding O WeChat	
	Open O 802.1X EAP MAC Address 802.1X EAP & MAC	
* Method:		
* Method:		
* Method: Encryption Options	○ WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits) ◎ None	▼
* Method: Encryption Options * Method:	○ WPA2 ○ WPA3 ○ WPA2/WPA3-Mixed ○ OWE ○ WPA-Mixed ○ WEP-64 (40 bits) ○ WEP-128 (104 bits)	

### 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

×

### **COMMSCOPE**<sup>®</sup>

### Mobimesh Deployment Guide

Hotspot Portal	▼
* Hotspot (WISPr) Portal: DEVCP-WEB	
Bypass CNA: OFF	
(?) Authentication Service:     (ov ) Use the controller as proxy OFF Use Realm-based profile     [DEVCP-AAA      ]      [OFF] Backup Authentication Service	
Accounting Service: ON Use the controller as proxy OFF Use Realm-based profile DEVCP-ACT	ate every 1 Minutes (0-1440)
Options	•
RADIUS Options	▼
NAS ID: O WLAN BSSID AP MAC User-defined: Crespi57	
* NAS Request Timeout: 3 Seconds	
* NAS Max Number of Retries: 2 Times	
* NAS Reconnect Primary: 5 Minute (1-300)	
* [?] Called Station ID: WLAN BSSID  AP MAC  None  AP GROUP	
NAS IP: O Disabled O SZ Control IP O SZ Management IP () User-def	ined: 134.242.138.24
Single Session ID Accounting: ON O APs will maintain one accounting session for client roan	ning.
* Vender Serville Attribute Deviller District and a	

#### 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.

RUCKUS®

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:

dit L3 A	ccess Contr	ol Policy: WebO	nly_L3ACL			×
D. * Defa	Name: WebOnly_L3ACL escription: ult Access: Default access if	no rule is matched: O Allow () Block				
🕂 Create 💋	<sup>9</sup> Configure Delete	🕇 Up 🚽 Down				
Priority 🔺	Description	Matching Criteria		Туре	Access	
1	Allow DNS	Direction:Inbound Destination Port:53		IPv4	Allow	
2	Allow DHCP	Direction:Inbound Destination Port:67		IPv4	Allow	
3	НТТР	Direction:Dual Inbound: Destination Port:80 Outbound: Source Port:80 Protocol:TCP		IPv4	Allow	
4	нттря	Direction:Dual Inbound: Destination Port:443 Outbound: Source Port:443		IPv4	Allow	
				ОК	Cancel	

FIGURE 9: ADDING L3 ACL

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

Name: WebOnly_FwProf   Description:	
Description:       Image: Construction of the second	
Rate Limiting:       Uplink       OFF       Mbps (0.1-200)         Downlink       OFF       Mbps (0.1-200)         L3 Access Control Policy:       WebOnly_L3ACL       Image: Control Policy         L2 Access Control Policy:       Disable       Image: Control Policy         Application Policy:       Disable       Image: Control Policy         URL Filtering Policy:       Disable       Image: Control Policy         Device Policy:       Disable       Image: Control Policy	
Downlink       OFF       Mbps (0.1-200)         L3 Access Control Policy:       WebOnly_L3ACL       Image: Control Policy:         L2 Access Control Policy:       Disable       Image: Control Policy:         Application Policy:       Disable       Image: Control Policy:         URL Filtering Policy:       Disable       Image: Control Policy:         Device Policy:       Disable       Image: Control Policy:	
L3 Access Control Policy: WebOnly_L3ACL	
L2 Access Control Policy: Disable   Application Policy: Disable   URL Filtering Policy: Disable   Device Policy: Disable    Disable	
Application Policy:       Disable       Image: Constraint of the second	
URL Filtering Policy: Disable   Disable  Disable  Disable  Disable  Disable  Disable  Disable  Disable  Disable  Disable  Disable  Disable  Disable  Disable D	
Device Policy: Disable   Disable	
OK Cancel	

### 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:

## Edit User Role: WebOnly\_Role

* Role Name: WebOnly_Role	
Description: Only web browsing (http/https)	
* User Traffic Profile: System Default 🔹 🕂 🖉	
* Firewall Profile: WebOnly_FwProf	
Access VLAN: VLAN ID	
OFF Enable VLAN Pooling	
OK Cance	

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 <u>Authentication</u> 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.

🕇 Create 🔗 Configure 📋 Delete	2			
Group Attribute Value 🔺	User Role	User Traffic Profile	Firewall Profile	
LB-Prof	LB-Prof	System Default	P-2Mbps_fw	
WebOnly	WebOnly_Role	System Default	WebOnly_FwProf	



### 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.

Helpdesk					Hotspot	Authenticator	Export	System
inPiazza	• Service p	profiles						
<ul> <li>Manage tenants</li> <li>Manage my tenants</li> <li>NAS finder</li> <li>Access point finder</li> <li>All sessions</li> <li>Tenants sessions</li> <li>NAS sessions</li> </ul> MacroMali <ul> <li>System</li> <li>Service profile</li> <li>Location</li> <li>Access Point</li> <li>Data &amp; status</li> <li>Authorization</li> <li>Other</li> </ul>	# 76 77 78 79	Name Common_HotSpot Food_Court_WiFi McRoman's_WiFi Paulmart_WiFi						
	Add new	Edit Delete					Total prof	iles: 4

FIGURE 13: NEW SERVICE PROFILE

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



### RUCKUS®

### **Mobimesh Deployment Guide**

Service profile					×
Name: *					
Business logic:	[DEFAULT]				~
Search locatio	in(s)				
Available location	15		Selected locations	5	
Underground Outdoor Parki Ground Floor First Floor Second Floor Paulmart Entr Paulmart Entr Paulmart Offic Food Court GF Food Court 1F McRomans Ins McRomans Out	Parking ing ance way tes tes side utside	<ul> <li>×</li> <li>×</li> <li>×</li> </ul>			*
				ОК	Cancel

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.

	ocati	ons						
IPIAZZA Se	rvice pr	ofile:		Search:				
V4.2.2			~					
age tenants age my tenants	#	Name	NAS Id	Client IP network	Client IP netmask	NAS type	Last connection	Service profile
înder	100	Underground Parking	Mall-01	10.1.0.0	255.255.255.0	MobiMESH	-	
ss point finder	101	Outdoor Parking	Mall-02	10.1.0.0	255.255.255.0	MobiMESH	-	
ssions	102	Ground Floor	Mall-03	10.2.0.0	255.255.0.0	MobiMESH	-	
essions	103	First Floor	Mall-04	10.2.0.0	255.255.0.0	MobiMESH	-	
	104	Second Floor	Mall-05	10.2.0.0	255.255.0.0	MobiMESH	-	
<b>`</b>	105	Paulmart Entrance	PM001	172.16.100.0	255.255.255.0	MobiMESH	-	
n rice profile	106	Paulmart Hallway	PM002	172.16.101.0	255.255.255.0	MobiMESH	-	
tion	107	Paulmart Offices	PM003	172.16.103.0	255.255.255.0	MobiMESH		
ss Point	108	Food Court GF	Mall-20	192.168.2.0	255.255.255.0	MobiMESH	-	
status	109	Food Court 1F	Mall-21	192.168.2.0	255.255.255.0	MobiMESH	-	
Ization	110	McRomans Inside	MR-001	172.16.20.0	255.255.255.0	MobiMESH	-	
	111	McDomans Outsido	MP 002	172 16 20 0	255 255 255 0	MobiMESH		

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)

NAS type:	Ruckus	Service profile:	Food_Court_W 🗸
Name: *		CoA: *	<ul> <li>Supported</li> <li>Not supported</li> </ul>
NAS id: *		CoA IP/host:	
Client IP netwo	ork: *	CoA port:	
Client IP netm	ask: *		
NAS IP list: *	Comma separated netwo	orks or IP list	
Secret: *	Shared secret for messa	ges sent from NAS IPs	
Notes:			

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.

Helpdesk				Hotspot	Authenticator	Export	Systen
	Access Point						
<b>InPlazza</b>	Location(s):		Search:				
v4.2.2		~					
Manage tenants							
Manage my tenants	#	Name	Location	MAC	Essid		
Q NAS finder							
▼ Access point finder							
All sessions							
Tenants sessions							
NAS sessions							
MacroMall 🗸							
🗸 System							
Service profile							
Location							
🛜 Access Point							
Data & status							
Authorization							
> Other							
	Add new Ec	lit Delete Duplicate		Т	otal access point: 0	1	*

FIGURE 17: ADDING ACCESS POINT

- 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)

### **COMMSCOPE**°

### **Mobimesh Deployment Guide**

Access Point		$\times$
Location: *		
MAC Address: *		
Name: *		
Essid:		
Description:		
	ОК	Cancel



# RUCKUS®



### **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



# RUCKUS®

#### commscope.com

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

© 2021 CommScope, Inc. All rights reserved.

Unless otherwise noted, all trademarks identified by <sup>®</sup> or <sup>™</sup> are registered trademarks, respectively, of CommScope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to CommScope products or services. CommScope is committed to the highest standards of business integrity and environmental sustainability with a number of CommScope's facilities across the globe certified in accordance with international standards, including ISO9001, TL9000, ISO14001 and ISO45001. Further information regarding CommScope's commitment can be found at www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability.