

# **Deployment Guide**

# **RUCKUS WAN Gateway - DPSK Step-by-Step Configuration**

June 2023

Rev. 1



## **Table of Contents**

Changes in Revision 1
INTENDED AUDIENCE
INTRODUCTION
TEST ENVIRONMENT
Test Components
Test Topology
Verify that the vSZ Instance is Adopted and in Sync
Verify that the ICX Switch is Adopted and in Sync
DPSK USING THE SAME VLANS
Clients Using DPSKs Associates to the Same VLAN
Step 1 – Create VLANs
Step 2 – Create IP Subnets
Step 3 – Enable NAT for the New Subnet
Architecture Recap
Step 4 – Configure the Switch Port Profile
Step 5 – Create the Policies
Step 6 – Create the Account Groups
Step 7 – Create RADIUS Realms
Step 8 – Create the DPSK WLAN
Step 9 – Create Accounts in RWG
Test Results
DPSK USING A VLAN POOL
Clients Using DPSKs Are Assigned to Dedicated VLANs
Step 1 – Create the VLAN Pool
Step 2 – Create the IP Subnets
Step 3 – Enable NAT for the New Subnet
Architecture Recap
Step 4 – Create the Switch Port Profile
Step 5 – Create the Policy
Step 6 – Create the Account Group
Step 7 – Create the RADIUS Realm
Step 8 – Create the WLAN
Step 9 – Create the Accounts
Delete an Existing Device



40
41
42
44
44
45
46
46
47
48
49
50



### **Changes in Revision 1**

- Minor corrections.
- Added note about NAT using the private networks defined by RFC 1918.

## **Intended Audience**

This document is a step-by-step guide on how to configure RWG solutions using DPSK.

The audience for this document is System Engineers who want to deploy the RUCKUS WAN Gateway (RWG) for L2/L3 microsegmentation using regular VLANs configured in the ICX switches, SmartZone controllers and access points. It is expected that the reader possesses a working knowledge on ICX switches and SmartZone, RADIUS, routing, and security concepts.

For more information on how to configure RUCKUS products, please refer to the appropriate RUCKUS user guide available on the RUCKUS support site at <a href="https://support.ruckuswireless.com/">https://support.ruckuswireless.com/</a>

The RWG documentation is embedded into the product. You can access the embedded documentation at <u>https://{your RWG\_IP\_address}/admin/manual/help\_online</u>



## Introduction

RWG supports DPSKs for WLAN authorization in several ways. The DPSKs are associated to accounts created in the RWG account database. They can be auto generated, or entered manually, and the clients that are authorized clients can change their own DPSK if desired.

RWG can also be integrated with an external PMS, and DPSKs can be created automatically for the imported accounts using mangling – for example, different combinations of a guest's last name and room number can be used as the DPSK.

DPSK also supports microsegmentation. After authorization, the client device can be placed in a dedicated VLAN and subnet, or in a shared subnet.

This guide will cover the step-by-step configuration of the following use cases:

- Clients using DPSK are associated to the same VLAN and subnet.
- Each client using DPSK are associated to a dedicated VLAN and subnet.
- PMS integration using DPSK mangling.



## **Test Environment**

#### **Test Components**

The following components were used for the examples and tests described in this document:

#### Virtual SmartZone High-Scale (sw version 6.1.0.0.935)

- VM running in an Intel NUC mini-PC, using only one interface.
- Besides the Staging Zone, only one zone is configured (named Solar System)
- One R550 is onboarded and online in zone Solar System (fw version 6.1.0.0.1595)
- No wlans are configured.

#### ICX 7150C12-POE (sw version 9.0.10d, routing code)

- Before adoption by RWG, the only configurations were:
- The interface ve1 was created.
- DHCP-client was enabled for virtual interfaces (using ip dhcp-client ve default)
- A read-only SNMP community string was added (using snmp-community public ro)

#### RWG (build 14.065)

- Bare-metal installation in a Qotom 4-LAN mini-PC with 8GB RAM and 128GB SSD (Q190G4U-S02)
- Installed a non-wildcard SSL certificate from Let's Encrypt US
- The vSZ instance and the ICX switch are adopted and in sync.



### **Test Topology**

In this test topology, the Qotom mini server running RWG uses interface **igb0** to connect to a Xfinity router. By default, igb0 is pre-configured as a DHCP client, and igb3 is pre-configured as a DHCP server.

Note that this is a test scenario - igb0 is using a private IP address. In production networks, the server running RWG is generally connected to an ISP that provides a public IP address directly to the igb0 interface.

**igb3** comes pre-configured with the IP address 192.168.5.1/24. The ICX switch, the vSZ instance and the R500 received their IP addresses from the DHCP server configured at igb3 in RWG.



FIGURE 1 - TEST TOPOLOGY

### Verify that the vSZ Instance is Adopted and in Sync

Navigate to **Network/Wireless** and to check the status of the vSZ instance. It should be online and in sync. Scroll down to see the discovered access point and zones. The access point should also be online.

WL/	AN Cont	rollers													
	Name 🛆	Online	Туре	Hos	it	Monitoring	Config sync status	WLANs	Locati events	on S	Model	Version	Access Points		Monitoring interval
	vSZ- 6100395	$\oslash$	Ruckus SmartZo	192. ne	168.5.249		Ø 01/05/2023 10:34 AM				vSZ-H	6.1.0.0.935	R550[34:20:e3:	28:0d:a0]	10
Acce	ss Points	5													
	Name 🛆	Online	Controller	AP Profile	Zone	IP	MAC	Clients	2.4GHz	5GHz	State	Uptime	Last seen	Model	Version
	R550	0	vSZ- 6100395	Default AP Profile [Solar System]	Solar System	<b>Q</b> 192.168.5.247	<b>Q</b> 34:20:e3:28:0d:a0	3	10	56	Connec	t 9 hours and 55 minutes	01/05/2023 08:22 PM	R550	6.1.0.0.1595
Acce	ss Point	Zones													
	Name	$\bigtriangleup$	Controller		Access Po	pints	AP Profiles				Enab	ble DFS channe	els	5GHz cha	nnel width
	Solar Sys	stem	√SZ-61003	95	R550[34:2	(0:e3:28:0d:a0]	Default AP Pr	ofile (Solar Sy	/stem]					20 MHz	
	Staging	Zone	√SZ-61003	95							<b>V</b>			20 MHz	

FIGURE 2 – SMARTZONE IS ONLINE AND IN SYNC



### Verify that the ICX Switch is Adopted and in Sync

Navigate to **Network/Wired** to check the status of the ICX switch. It should be online and in sync.

Swit	ches											
	Name $ riangleq$	Online	Туре	Host	Monitoring	Config sync status	Location events	Model	Version	Ports	Pms rooms	Monitoring interval
	ICX 7150- B	$\oslash$	Ruckus ICX Switch	192.168.5.242		Ø 01/05/2023 10:47 AM		Stackable ICX7150- C12-POE	Version 09.0.10dT213	GigabitEthernet1/1/2, GigabitEthernet1/1/3, GigabitEthernet1/1/4, (16)	-	10

#### FIGURE 3 – ICX IS ONLINE AND IN SYNC

For details on how to adopt devices, please refer to the document **RUCKUS WAN Gateway - Adoption of Devices**.



## **DPSK Using the Same VLANs**

#### **Clients Using DPSKs Associates to the Same VLAN**

In this solution, the wireless clients use a DPSK to authenticate and get associated to the same VLAN and subnet. If several VLANs are required, each VLAN needs one account group, one policy and one RADIUS Realm at RWG.

Each guest or tenant has an account with its own DPSK. This solution is useful for situations where we need to define the VLANs in advance, and a group of users need to work in the same VLAN – maybe different departments in an enterprise network.

This solution is harder to configure if many VLANs are required – every VLAN needs an account group, policy, and RADIUS realm.



FIGURE 4 – EACH VLAN NEEDS A SEPARATE RADIUS REALM, POLICY, AND ACCOUNT GROUP



#### Step 1 – Create VLANs

Navigate to Network/LAN and click Create New in the VLAN Interfaces section. Enter the following information:

- Name: Enter a name for the VLAN.
- **Physical Interface**: Select the RWG's physical interface that is connected to the LAN side.
- VLAN IDs: Enter 100
- Autoincrement: Select none | single L2 | n tags = 1. Using that setting only one VLAN will be created.

Create VLAN Interface		
Name	VLAN 100	
Note		
Parent (Hide)		
Physical Interface	igb5 varent physical Ethernet interface	
Service VLAN	- select - Q-in-Q parent VLAN interface	
Tags (Hide)		
VLAN IDs	100	first
I-SIDs		first
Autoincrement	none   single L2   n tags = 1	
Ratio	1	nur
MAC Override		bas
Networks (Hide)		
Addresses		add
Infrastructure (Hide)		
Switch Port Profiles		
WLANs	no options WLANs that utilize this VLAN for dynamic VLAN assign	nme
Conference Tool (Hide)		
Conference options	no options	
Create Cancel		

FIGURE 5 – CREATE VLAN INTERFACE

Click Create to finish.

Use the same procedure to create VLANs 150 and 200.



### Step 1a – Check the VLANs

The VLAN Interfaces section shows VLAN 100, 150 and 200.

VLAN I	nterfaces						
	Name 🛆	Physical Interface	<u>~</u>	Parent	VLAN IDs	Autoincrement	Addresses
	VLAN 100	igb5		igb5	100		
	VLAN 150	igb5		igb5	150		
	VLAN 200	igb5		igb5	200		
3 Found							

#### FIGURE 6 – THREE NEW VLAN INTERFACES

#### Step 2 – Create IP Subnets

Navigate to **Network/LAN** and click **Create New** in the **Network Addresses** section. Enter the following information:

- Name: Enter a name for the subnet.
- Ethernet: Do not select any physical interface. Use the option -select-
- VLAN: Select VLAN 100
- IP: Enter 100.0.0.1/24
- Autoincrement: Enter 1
- Span: Enter 1
- Create DHCP Pool: Make sure to mark the checkbox.

Create Network Address	
Name	subnet 100
Note	
Interface (Hide)	
Ethernet	- select - v interface to configure address(es) with
VLAN	VLAN 100 VLAN to configure address(es) with
OpenVPN	- select -  OpenVPN server to assign address(es) with
Addresses (Hide)	
Primary	✓ primary and first configured subnet on the interface/VLAN
IP	100.0.0.1/24
IPv6 PD Uplink	- select - V Uplink which will provide the IPv6 Prefix Delegation(PD)
Autoincrement	1
Span	1
Provisioning (Hide)	
Create DHCP Pool	automatically configure a DHCP pool for entire subnet(s)
IP Group	- None - v assign this network to an IP Group
Create Cancel	

FIGURE 7 – CREATE NETWORK ADDRESS

Click Create to finish.

Use the same procedure to create subnets 150 and 200.



### Step 2a – Check the Network Addresses

The **Network Addresses** section shows subnet 100, 150 and 200. The **VLAN Interfaces** section now shows the subnets in the **Address** column.

VLAN I	nterfaces							_
	Name 🛆	Physical Interface		△ Parent	VLAN IDs	Autoincrement	Addresses	
	VLAN 100	igb5		igb5	100		subnet 100	
	VLAN 150	igb5		igb5	150		subnet 150	
	VLAN 200	igb5		igb5	200		subnet 200	
3 Found								
Networ	k Addresses	5						
	Name		$\bigtriangleup$	Primary	IP	Ethernet		VLAN
	Managemen	it LAN		¥	192.168.5.1/24	igb5		
	subnet 100				100.0.0.1/24			VLAN 100
	subnet 150				150.0.0.1/24			VLAN 150
	subnet 200				200.0.0.1/24			VLAN 200
4 Found								

#### FIGURE 8 – THREE NEW NETWORK ADDRESS

#### Step 2b – Check the DHCP Pools

Navigate to **Services/DHCP** to see the DHCP pools that were created along with the subnets.

DHCP Pools								
	Name	Start IP	End IP	Network				
	Management LAN	192.168.5.10	192.168.5.254	Ethernet igb5				
	subnet 100	100.0.0.2	100.0.254	VLAN "VLAN 100" (100)				
	subnet 150	150.0.0.2	150.0.0.254	VLAN "VLAN 150" (150)				
	subnet 200	200.0.0.2	200.0.0.254	VLAN "VLAN 200" (200)				
4 Found								

FIGURE 9 – THREE NEW DHCP POOLS



#### Step 3 – Enable NAT for the New Subnet

Navigate to Network/NAT, and click Edit on the entry for subnet 100. Enter the following information:

- Name: Change the name to NAT on "subnet 100"
- Uplinks: Mark the Uplink checkbox.
- Addresses: Make sure subnet 100 is selected.

Update NAT on "subnet 100"	•
Name	NAT on "subnet 100"
Note	
WAN Translation (Hide)	
Uplinks	Select All   None   Reset
	uplinks to perform NAT through (none to disable NAT for selected subnets)
Reverse NAT (not recommended)	Cause traffic sent via selected Uplink to be NAT'd to the first IP of the selected Addre
IP Adjustments (optional)	(Hide)
Start IP	first WAN IP to
End IP	last WAN IP to
Static port	retain packet source port - "cone" instead of "symmetric NAT" (not recommended)
Subnets (Hide)	
Addresses	X subnet 100
Static Routes	no options routed subnets to perform NAT for
Update Cancel	

FIGURE 10 - ENABLE THE NAT ENTRY

Click **Update** to finish. Repeat the process for subnets 150 and 200.

**Note**: A NAT entry will not be created for the private subnets defined by RFC 1918 (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16). RWG will automatically enable NAT for those subnets, even without a NAT entry showing in the NAT scaffold.

#### Step 3a – Check the NAT Configuration

The NATs section now shows subnets 100, 150 and 200 associated with the RWG uplink.

NATs					
	Name	Uplinks	Start IP	End IP	Addresses
	NAT on "subnet 150"	Uplink		-	subnet 150
	NAT on "subnet 100"	Uplink	-	-	subnet 100
	NAT on "subnet 200"	Uplink	-		subnet 200
	NAT on subnet 192.168.5.0	Uplink	-	-	Management LAN
4 Found					





### **Architecture Recap**

When a wireless client associates to the WLAN configured with DPSK, the access point sends an authorization request to the RADIUS server running in RWG. The RADIUS server responds with a message that contains the VLAN tag that will be used for the wireless client traffic when that traffic is forwarded across the switch ports. The VLAN tag will the determined by the RADIUS realms.

In our topology, the switch ports used to forward the traffic are 1/1/2 and 1/1/8. They need to be pre-configured as tagged interfaces with the VLAN IDs defined in the RADIUS realms. No configuration is required in the access point's ethernet interface, because by default, all RUCKUS access points come with the ethernet interface already configured as tagged ports for all VLAN IDs.





### Step 4 – Configure the Switch Port Profile

Navigate to **Network/Wired** and click **Create New** in the **Switch Port Profiles** section. Enter the following information:

- Name: Enter VLAN 100, 150 and 200
- Ports: Select ports 1/1/2 and 1/1/8
- Tagged VLANs: Select VLANs 100, 150 and 200.

Create Switch Port Profile		
Name	VLAN 100, 150 and 200	
Note		
Provisioning (Hide)		
Default	assign this profile to any newly imported switch ports	
Move ports	assign ports currently assigned to a different default profile to this	profile upon save
Ports		X ICX 7150-B: GigabitEthernet1/1/8[ethernet 1/1/8] ICX 7150-B: GigabitEthernet1/1/2[ethernet 1/1/2]
Media converters		media converters currently assigned to this profile
Port Configuration (Hide)		
Untagged VLAN		
Shutdown		
Tagged VLAN(s)		X VLAN 200 X VLAN 150 X VLAN 100
Routed VLANs		)
RADIUS	none ~	
Shortest Path Bridging (80	2.1aq) (Hide)	
Native I-SID		
NNI Port		
Advanced (Show)		
Create Cancel		

FIGURE 13 - CREATE SWITCH PORT PROFILE

Click Create to finish.



#### Step 4a – Check the Results

VLANs 100, 150 and 200 using tagged ports 1/1/2 and 1/1/8 are created in the ICX switch, and a new entry shows in the section **Switch Port Profiles**.

Swite	h Port Profiles			
0	Name	Default	Ports	Tagged VLAN(s)
	Default for RUCKUS ICX Switch	10	GigabitEthemetIVVI, GigabitEthemetIVV3, GigabitEthemetIVV4, (14)	-2
	VLAN 100, 150 and 200		GigabitEthernetI/l/2, GigabitEthernetI/l/8	VLAN 200, VLAN 150, VLAN 100
Found	ł			

FIGURE 14 – THREE VLANS CREATED IN THE ICX SWITCH

#### **Step 5 – Create the Policies**

The policies will tie together the account groups and the RADIUS realms at RWG. Click **Policies** at the top menu, scroll down and click **Create New** in the **Policies** section. Enter the following information:

- Name: Enter VLAN 100 Policy
- Bandwidth Queues: Check 100%
- Subnets Filter: Select Block Subnets.

Create Policy		Log Hits Triggers	Select All   None   Reset
Name	VLAN 100 Policy		Webserver DDoS Prevention
Default		Application Filters	Select All   None   Reset
Note		Application Forwards	no options
		Subnets Filter	Block Subnets 🗸
Enforcement (Hide)		Radius servers	no options
Splash Portal	- select - V	WLAN	- select - 🗸 WLAN to use for connectio
Web Cache	- select - ~	Groups (Hide)	
Content Filter	- select - ~	MAC Groups	no options
HTML Payload Rewrite	- select - v	IP Groups	Select All   None   Reset
Link Controls	no options	Account Groups	no options
Bandwidth Queues	Select All   None   Reset	Shared Credential Groups	no options
	<b>2</b> 100%	RADIUS Groups	no options
Connections Triggers	no options	LDAP Groups	no options
DPI Triggers	no options		
Quota Triggers Space-Time Triggers	no options	Create Cancel	

FIGURE 15 - CREATE POLICY

Click Create to finish.

Repeat the process to create the policies for VLAN 150 and 200.



### Step 6 – Create the Account Groups

Navigate to **Identities/Groups**, then click **Create New** under the **Account Groups** section. Enter the following information:

- Name: Enter a name for the account group
- Policy: Select VLAN 100 Policy
- Disable enhanced PSK Security: Mark the Don't validate checkbox. This way we can create DPSKs that are like each other.

Create Account Group	
Name	VLAN 100 Account Group
Description	
Priority	4 v default selection (4) recommended
Disable enhanced PSK Security	Oon't validate PSK strength or similarity to other Acc
Psk character set	Hexadecimal [A-F, 0-9]
Psk length	16
Policy	VLAN 100 Policy ~
Usage Plans	Select All   None   Reset Basic Plan
Note	
Create Cancel	

#### FIGURE 16 - CREATE ACCOUNT GROUP

Click Create to finish.

Repeat the process to create the account groups for VLANs 150 and 200.

#### Step 6a – Check the Account Groups

The section Account Groups shows three new account groups.

Accou	Account Groups										
	Name	$\bigtriangleup$	Priority	Disable enhanced PSK Security	Psk character set	Psk length	Policy				
	VLAN 100 Account Group		4		Hexadecimal [A-F, 0-9]	16	VLAN 100 Policy				
	VLAN 150 Account Group		4		Hexadecimal [A-F, 0-9]	16	VLAN 150 Policy				
	VLAN 200 Account Group		4		Hexadecimal [A-F, 0-9]	16	VLAN 200 Policy				
3 Found											





### Step 6b – Check the Policies

Click **Policies** at the top menu. The policies for VLAN 100, 150 and 200 will show. Make sure the associations between the account groups, policies and enforcement rules are correct.



FIGURE 18 – POLICY ASSOCIATIONS

### Step 7 – Create RADIUS Realms

Navigate to **Services/RADIUS** and click **Create New** in the section **RADIUS Server Realms**. Enter the following information:

- Name: Enter a name for the realm.
- Rank: Select 0
- Real admission logic: Select Policy OR Attribute Pattern logic must succeed.
- Policies: Select VLAN 100 Policy
- Priority: Select 0
- Logic: Select OR
- Attribute: Select Called-Station-Id (BSSID/SSID)
- **Pattern**: Enter **dpsk**. That will be the SSID for the WLAN we will create later.

Create RADIUS Server Re	alm	
Name	Realm VLAN 100	
Note		
Request Matching (Hide)		
Rank	0 y prioritize higher rank over group and attrit	oute pattern precedence when matching
Realm admission logic	Policy OR Attribute Pattern logic must succ	xeed 🖂 logic to use when determining w
Policies	Select All   None   Reset □ Default □ ICX 7150-E VLAN 100 Policy □ V	LAN 150 Policy OVLAN 200 Policy OWebse
	Account, MAC, and IP groups that may match th	iis realm
CALEA Options	no options Use this realm for Accounting for	the specified CALEA Options
Attribute Patterns (Hide attributes to authenticate when	) matched	
Priority Logic Attribute	Pattern	WLAN Note
0 V OR V Called-Statio	n-ld (BSSID/SSID) 🗸 dpsk	- select - V
Create Another RADI	JS Attribute Pattern	

FIGURE 19 – CREATE RADIUS SERVER REALM



Scroll down to continue. Enter the following information:

- Sharing: Select per-Account
- VLANs: Check VLAN 100
- Reuse: Check reuse VLAN tag assignments when necessary
- VLANs/Called-Station: Check unlimited.
- Infrastructure Devices: Check vSZ-249 (the name of your SmartZone controller)
- Inserted Attributes: Check the following attributes:
  - Tunnel-Type:VLAN
  - Tunnel-Medium-Type-IEEE-802
  - Tunnel-Private-Group-Id:%vlan\_tag\_assignment.tag%
  - Ruckus-DPSK:%account.pre\_shared\_key%

Dynamic VLANs (Hide)	
Sharing	per-Account  v how VLANs are shared between end-users
VLANS	Select All I None   Reset
	dynamic VLANs available for assignment
Reuse	reuse VLAN tag assignments when necessary
Inherit static	new VLAN tag assignments inherit the static attribute of an existing shared VLAN
Timeout	60 minutes ~ amount of time a VLA
Expire at logout	immediately flush a VLAN tag assignment at logout
VLANs / Called-Station	unlimited 🗹 naximum number of *
Infrastructure Devices	Select All   None   Deset □ ICX 7150-E 2V52-249
	RADIUS NAS device(s) issuing requests for VLAN assignment
Proxy Servers (Show)	
Behavior (Hide)	
Inserted Attributes	Select All   None   Reset
	Cisco-AVpair:psk=%account.pre_shared_key%
	RADIUS attributes to include in an Access-Accept or proxied Access-Request or Accounting-Request dependin
Always deny	deny all requests to this realm
Accounting (Show)	
Create Cancel	

FIGURE 20 - CREATE RADIUS SERVER REALM (CONT'D)

Click Create to finish. Repeat the process to create RADIUS realms for VLANs 150 and 200.

#### Step 7a – Check the New RADIUS Server Realms

The RADIUS Server Realms section shows three new realms:

RADI	ADIUS Server Realms										
	Name 🛆	Rank	Policies	CALEA Options	Attribute Patterns	Sharing	VLANs	Infrastructure Devices	RADIUS Servers		
	Realm VLAN 100	0	VLAN 100 Policy	-	Called-Station-Id: dpsk	per- Account	VLAN 100	vSZ-249	-		
	Realm VLAN 150	0	VLAN 150 Policy		Called-Station-Id: dpsk	per- Account	VLAN 150	vSZ-249	-		
	Realm VLAN 200	0	VLAN 200 Policy	-	Called-Station-Id: dpsk	per- Account	VLAN 200	vSZ-249	-		

FIGURE 21 – THREE NEW RADIUS SERVER REALMS



#### Step 8 – Create the DPSK WLAN

Navigate to Network/Wireless, then click New in the WLANs section. Enter the following information:

- Name: Enter dpsk
- Access point zone: Select the zone where the WLAN will be created. Here, we used Enceladus.
- **Controller**: Select the SmartZone controller where the WLAN will be created.
- **AP Profiles**: Select the AP profile for the zone.
- SSID: Enter dpsk.
- Encryption: Select WPA2
- Authentication: Select Multiple PSK
- VLANs: Check VLAN 100, VLAN 200 and VLAN 150

Create WLAN	
Name	dpsk
Access point zone	Enceladus ~
Note	
Provisioning (Hide)	
Controller	vSZ-249 ~
AP Profiles	Select All LNone L Reset
Policies	
WLAN Configuration (Hide	)
SSID	dpsk
Encryption	WPA2 ~
Authentication	Multiple PSK ~
Pre-shared Key	
Default VLAN	[1 VLA
Tunnel	tunnel WLAN traffic to the controller instead of locally bridging (tunnelin
Enabled	✓ 2.4GHz
OFDM Only	prevents 802.11b clients from connecting to the WLAN
RADIUS Realm Server	Local RADIUS server
Dynamic VLANs (Hide)	
VLANS	Select All I None   Beset
	VLANs to be assigned when RADIUS access requests include this WLAN's S
RADIUS Accounting	receive RADIUS Accounting packets from the AP
Create Cancel	

#### FIGURE 22 - CREATE WLAN

Click Create to finish.



### Step 8a – Check the WLAN

The section **WLANs** shows the new WLAN.

WLANs									t WLANs 🐻 Columns  🏹 Refresh	
	Name 🛆	Controller	AP Profiles	Access point zone	SSID	Encryption	Authentication	Default VLAN	Tunnel	VLANs
	dpsk	vSZ-249	default [Enceladus]	Enceladus	dpsk	WPA2	Multiple PSK	1		VLAN 100, VLAN 200, VLAN 150
1 Found										

#### FIGURE 23 – CREATE WLAN

#### Step 9 – Create Accounts in RWG

Using the table below, create six accounts, including the DPSK, distributed among the three account groups:

Account	Account Group	DSPK
user1	VLAN 100 Account Group	user1-12345678
user2	VLAN 100 Account Group	user2-12345678
user3	VLAN 150 Account Group	user3-12345678
user4	VLAN 150 Account Group	user4-12345678
user5	VLAN 200 Account Group	user5-12345678
user6	VLAN 200 Account Group	user6-12345678

FIGURE 24 - CREATE SIX ACCOUNTS

Navigate to **Identities/Accounts** and click **Create New** in the **Accounts** section. Enter the following information:

- Login: Enter user1
- **Password and Confirmation**: Enter the password in the two fields.
- First and Last name: Enter a first and last name.
- Email: Enter an email for the account
- Group: Select VLAN 100 Account Group
- Time: Enter 15
- Download quota: Check unlimited.
- Upload quota: Check unlimited.
- Expiration: Check never





Scroll down to continue.



Enter the following information:

- Automatic login: Check automatically login devices at this account
- Max devices: Enter 3
- Pre-Shared Key: Enter user1-12345678 (use the DPSKs in the table in the last page)

Sessions (Hide)		
Automatic login	automatically login devices as this account	
Automatic provision	automatically add devices on the same network to this account	
Max sessions	1	unlimited 🗌
Max devices	3	unlimited 🗌
Max party guests	0	unlimited 🗌
Max sub accounts	0	unlimited 🗌
Max dedicated IPs	0	maximum numb
Dedicated IPs are static	Dedicated NAT IPs are reserved for the account and remain static f	or the lifetime of th
Vtas are static		
UPnP enabled	allow UPnP requests from devices in this account	
Lock devices	prevent using these devices for other accounts	
Pre-Shared Key	user1-12345678	remains the sam
Devices (Hide) current or last known mac address	ies	
Name	MAC	Active Party
Create Another Device		
Create Cancel		

#### FIGURE 26 – CREATE ACCOUNT (CONT'D)

Click **Create** to finish. Repeat the process to create the other five accounts.

### Step 9a – Check the New Accounts

The section **Accounts** shows the six new accounts.

Acco	Accounts										
	Login $ riangle$	Group	Time	Quota	Expiration	Plan	Balance	Bill	Devices		
	userl	VLAN 100 Account Group	15 minutes	unlimited	never		\$0.00				
	user2	VLAN 100 Account Group	15 minutes	unlimited	never		\$0.00				
	user3	VLAN 150 Account Group	15 minutes	unlimited	never		\$0.00				
	user4	VLAN 150 Account Group	15 minutes	unlimited	never		\$0.00				
	user5	VLAN 200 Account Group	15 minutes	unlimited	never		\$0.00				
	user6	VLAN 200 Account Group	15 minutes	unlimited	never	-	\$0.00		-		

FIGURE 27 – SIX NEW ACCOUNTS



### **Test Results**

In the example, we used a MacBook with account **user4** to connect. Notice that the DPSK for user4 was entered in the **Password** field.

<b>?</b>	The Wi-Fi WPA2 pas You can also	network "dpsk" requires a sword. access this Wi-Fi network by sharing the	Wi-Fi Configure IPv4:	TCP/IP DNS W	INS 802.1X Proxies	Hardware
	password fro connected to	om a nearby iPhone, iPad, or Mac which has this network and has you in their contacts.	IPv4 Address:	150.0.0.3	DHCP Client ID:	Renew DHCP Lease
	Password:	user4-12345678	Router:	150.0.0.1	Drice client ib.	(If required)
		<ul> <li>Show password</li> <li>Remember this network</li> </ul>	Configure IPv6:	Automatically	٢	
			Router: IPv6 Address:			
?		Cancel Join	Prefix Length:			

FIGURE 28 – USER4 IS CONNECTED

As expected, it got associated to VLAN 150 and received an IP address from the DHCP scope **150.0.02** – **150.0.0254**.

In the diagram below we see six different devices connected using one account each. As expected, they are using VLAN 100, VLAN 150 and VLAN 200 and their corresponding IP subnets.

HCI	P Leases										4 Flus
	Issued	IP 🛆	MAC	Vendor	Hostname	Expires	Network	Pool	Fixed Host	Ethernet	VLAN
						(Filter	red)				
	02/13/2023 12:21:03 PM	<b>Q</b> 100.0.0.2	<b>Q</b> 82:ad:f5:32:40:bf			02/13/2023 04:21:03 PM	vlan100	subnet 100	Create New		VLAN 100
	02/13/2023 12:17:34 PM	<b>Q</b> 100.0.0.3	<b>Q</b> 7e:32:2b:fd:48:c3		Marcelo-s-S10	02/13/2023 01:17:34 PM	vlan100	subnet 100	Create New		<b>VLAN 100</b>
	02/13/2023 12:35:36 PM	<b>Q</b> 150.0.0.2	<b>Q</b> 42:29:ef:87:50:e7		Pixel-3	02/13/2023 01:35:36 PM	vlan150	subnet 150	Create New		VLAN 150
	02/13/2023 12:26:18 PM	<b>Q</b> 150.0.0.3	<b>Q</b> 38:f9:d3:d4:c0:78	Apple	Marcelos-MBP	02/13/2023 01:26:18 PM	vlan150	subnet 150	Create New		VLAN 150
	02/13/2023 12:20:09 PM	<b>Q</b> 200.0.0.2	<b>Q</b> f6:0c:b9:8c:13:12			02/13/2023 04:20:09 PM	vlan200	subnet 200	Create New		VLAN 200
	02/13/2023 12:36:37 PM	<b>Q</b> 200.0.0.3	<b>Q</b> b8:08:cf:31:e2:58	Intel Corporation	LP- MMOLINARI	02/13/2023 01:36:37 PM	vlan200	subnet 200	Create New		VLAN 200

FIGURE 29 – SIX DEVICES CONNECTED, TWO IN EACH VLAN

Enter the client IP address and click **Search** at the top right menu to see details and the policy for the authenticated client.

RWG	T	55.16 AM PST nwg-mm.	ruckusdemos.net he	lp jmb/vsz_sync_issues_202	230207 14.590-29-ge5f02	a6a6 logout admin	000.0.2 Q Searc
System	Network	Services	Identities	Policies	Billing	Archives	Instruments
Account Login: user1 Name: User One	Webs	erver DDoS Abusers				Webs	and the second s
Group: VLAN 100 Account G Quota: unlimited Time: 15 minutes Device	roup	IP GROUP				0	Cache web cache
IP: 100.0.0.2 MAC: 82:ad:f5:32:40:bf No active session Croup		DEFAULT GROUP		Default		0	Block Subnets
DEFAULT VLAN Tag Assignment MAC: 82:ad:f5:32:40:bf VLAN: VLAN 100 [100]	VLAN	100 Account Group	0	VLAN 100 Pol	cy	0	100% 100% per Device BANDWIDTH QUEUE
Realm: Realm VLAN 100				🛓 PNG			





## **DPSK Using a VLAN Pool**

### **Clients Using DPSKs Are Assigned to Dedicated VLANs**

In this solution, the wireless clients use a DPSK to authenticate and each of them gets associated to a different, dedicated VLAN and subnet. The VLANs comes from a single VLAN pool.

This use case requires only RADIUS realm, one policy and one account group. This solution is easier to configure than the previous one.



FIGURE 31 - ONE RADIUS REALM, ONE POLICY, ONE ACCOUNT GROUP AND ONE VLAN POOL



### Step 1 – Create the VLAN Pool

Navigate to Network/LAN and click Create New in the VLAN Interfaces section. Enter the following information:

- Name: Enter a name for the VLAN. Here we used VLAN Pool
- **Physical Interface**: Select the RWG's physical interface that is connected to the LAN side.
- VLAN IDs: Enter 300
- Autoincrement: Select per-subnet | auto-increment L2 w/L3 | n tags = (subnets/ratio). Using this option RWG will create a VLAN range starting at the VLAN ID defined above.
- Ratio: Enter 1

Create VLAN Interface		
Name	VLAN Pool	]
Note		-
Parent (Hide)		
Physical Interface	igb5 -> parent physical Ethernet interface	
Service VLAN	- select - VLAN interface	
Tags (Hide)		
VLAN IDs	300	first 802.1Q VID
I-SIDs		first SPBM I-SID ass
Autoincrement	per-subnet   auto-increment L2 w/ L3   n tags = (subnets / n	atio) ~
Ratio	1	number of autoincr
MAC Override		base MAC used for
Networks (Hide)		
Addresses		addresses assigned
Infrastructure (Hide)		
Switch Port Profiles		
WLANS	Select All   None   Reset	
	WLANs that utilize this VLAN for dynamic VLAN assignments	
Conference Tool (Hide)		
Conference options	no options	
Create Cancel		

FIGURE 32 – CREATE VLAN INTERFACE

Click **Create** to finish.



### Step 1a – Check the VLANs

The VLAN Interfaces section shows the new VLAN.

VLAN	Interfaces	;							<b>B</b> C
	Name	$\bigtriangleup$	Physical Interface	$\bigtriangleup$	Parent	VLAN IDs	Autoincrement	Addresses	Switch Port Profiles
	VLAN 100		igb5		igb5	100		subnet 100	VLAN 100, 150 and 200
	VLAN 150		igb5		igb5	150		subnet 150	VLAN 100, 150 and 200
	VLAN 200		igb5		igb5	200	-	subnet 200	VLAN 100, 150 and 200
	VLAN Pool		igb5		igb5	300	l tags per-subnet		
4 Found									

#### FIGURE 33 - THE VLAN POOL IS CREATED

#### Step 2 – Create the IP Subnets

Navigate to **Network/LAN** and click **Create New** in the **Network Addresses** section. Enter the following information:

- Name: Enter a name for the subnet. Here we used subnet 30.0.
- Ethernet: Do not select any physical interface. Use the option -select-
- VLAN: Select VLAN Pool
- IP: Enter 30.0.0.1/30
- Autoincrement: Enter 64. RWG will create 64 subnets starting at the address defined above.
- Span: Enter 1
- Create DHCP Pool: Make sure to mark the checkbox.



FIGURE 34 – CREATE NETWORK ADDRESS

• Click **Create** to finish.



### Step 2a – Check the Network Addresses

The **Network Addresses** section now shows **subnet 30.0**. The **VLAN Interfaces** section now shows the range of VLANs in pool in the VLAN IDs column.

VLAN I	nterfaces							Columns
	Name 🛆	Physical Interface	$\bigtriangleup$	Parent	VLAN IDs	Autoincrement	Addresses	Switch Port Profiles
	VLAN 100	igb5		igb5	100		subnet 100	VLAN 100, 150 and 200
	VLAN 150	igb5		igb5	150		subnet 150	VLAN 100, 150 and 200
	VLAN 200	igb5		igb5	200		subnet 200	VLAN 100, 150 and 200
	VLAN Pool	igb5		igb5	300 - 363 (64)	1 tags per-subnet	subnet 30.0	
4 Found								
Networ	rk Addresses	;						ntering Send GARP 🐻 Columns
	Name	$\triangle$	Primary		IP		Ethernet	VLAN
	Management	LAN	1		192.168.5.1/24		igb5	
	subnet 100				100.0.0.1/24			VLAN 100
	subnet 150				150.0.0.1/24			VLAN 150
	subnet 200				200.0.0.1/24		-	VLAN 200
	subnet 30.0				30.0.0.1/30 - 30.0.0.253/30	(64)	-	VLAN Pool
5 Found								

#### FIGURE 35 – VLAN POOL AND SUBNET 30.0 ARE ASSOCIATED

### Step 2b – Check the DHCP Pools

Navigate to **Services/DHCP** to see the new DHCP pool for subnet 30.0.

DHCP Poo	DHCP Pools								
	Name $ riangleq$	Sta	art IP	End IP	Network				
	Management LAN	192	2.168.5.10	192.168.5.254	Ethernet igb5				
	subnet 100	100	0.0.0.2	100.0.0.254	VLAN "VLAN 100" (100)				
	subnet 150	150	0.0.0.2	150.0.0.254	VLAN "VLAN 150" (150)				
	subnet 200	20	0.0.0.2	200.0.0.254	VLAN "VLAN 200" (200)				
	subnet 30.0	30	0.0.0.2	30.0.0.254	VLAN "VLAN Pool" (300 - 363)				
5 Found									

FIGURE 36 – DHCP POOL FOR SUBNET 30.0



#### Step 3 – Enable NAT for the New Subnet

Navigate to **Network/NAT**, and click **Edit** on the entry for subnet 30.0. Enter the following information:

- Name: Change the name to NAT on "subnet 30.0"
- Uplinks: Mark the Uplink checkbox.
- Addresses: Make sure subnet 30.0 is selected.

Update Disable NAT on "su	bnet 30.0"	
Name	NAT on "subnet 30.0"	
Note		
WAN Translation (Hide)		
Uplinks	Select All   None   Reset	
	uplinks to perform NAT through (none to disable NAT for selected subnets)	
Reverse NAT (not recommended)	Cause traffic sent via selected Uplink to be NAT'd to the first IP of the selected Ad	ddres
IP Adjustments (optional)	(Hide)	
Start IP	first WAN I	IP to I
End IP	last WAN II	P to I
Static port	retain packet source port - "cone" instead of "symmetric NAT" (not recommend	ded)
Subnets (Hide)		
Addresses	Subnet	30.0
Static Routes	<b>NO Options</b> routed subnets to perform NAT for	
Update Cancel		

FIGURE 37 – ENABLE NAT FOR SUBNET 30.0

Click Update to finish.

### Step 3a – Check the NAT Configuration

The **NATs** section now shows the new subnet associated with the RWG uplink.

NATs							🐻 Columns  议 R
	Name 🛆	Uplinks	Reverse NAT (not recommended)	Start IP	End IP	Static port	Addresses
	NAT on "subnet 30.0"	Uplink		-	-		subnet 30.0
	NAT on "subnet 100"	Uplink					subnet 100
	NAT on "subnet 150"	Uplink					subnet 150
	NAT on "subnet 200"	Uplink					subnet 200
	NAT on subnet 192.168.5.0	Uplink					Management LAN
5 Found							

#### FIGURE 38 - NAT IS ENABLED FOR SUBNET 30.0

**Note**: A NAT entry will not be created for the private subnets defined by RFC 1918 (10.0.0.0/8, 172.16.0.0/12 and 192.168.0.0/16). RWG will automatically enable NAT for those subnets, even without a NAT entry showing in the NAT scaffold.



### **Architecture Recap**

When a wireless client associates to the WLAN, the access point sends an authorization request to the RADIUS server running in RWG. The RADIUS server responds with a message that contains the VLAN tag that will be used for the wireless client traffic, when that traffic is forwarded across the switch ports. The VLAN tag will the chosen from the vlan pool configured at the RADIUS realm.

In our topology, the switch ports used to forward the traffic are 1/1/2 and 1/1/8. They need to be preconfigured as tagged interfaces with all VLAN IDs defined in the vlan pool that will be used in the RADIUS realm.

No configuration is required in the access point's ethernet interface, because by default, all RUCKUS access points come with the ethernet interface already configured as tagged ports for all VLAN IDs.



FIGURE 39 – VLANS WITH TAGGED INTERFACES IN THE ICX SWITCH



### Step 4 – Create the Switch Port Profile

Navigate to **Network/Wired** and click **Create New** in the **Switch Port Profiles** section. Enter the following information:

- Name: Enter VLAN Pool
- Ports: Select ports 1/1/2 and 1/1/8
- Tagged VLANs: Select VLAN Pool

Create Switch Port Profile	
Name	VLAN Pool
Note	
Provisioning (Hide)	
Default	assign this profile to any newly imported switch ports
Move ports	assign ports currently assigned to a different default profile to this profile upon save
Ports	X       ICX 7/50-B: GigabitEthernet1/1/8[ethernet 1/1/8]         X       ICX 7/50-B: GigabitEthernet1/1/2[ethernet 1/1/2]
Media converters	media converters currently assigned to this profile
Port Configuration (Hide)	
Untagged VLAN	
Shutdown	
Tagged VLAN(s)	X VLAN Pool
Routed VLANs	
RADIUS	none
Shortest Path Bridging (80	2.1aq) (Hide)
Native I-SID	
NNI Port	D
Advanced (Show)	
Create Cancel	

#### FIGURE 40 – CREATE SWITCH PORT PROFILE

Click Create to finish.

**Note**: If you want to maintain the ICX VLANs created in the previous use case, add VLAN 100, 150 and 200 to **Tagged VLANs**, otherwise they will be replaced by the VLANs in the VLAN pool.



#### Step 4a – Check the Results

The VLANs 300 to 363 using tagged ports 1/1/2 and 1/1/8 are created in the ICX switch, and a new entry shows in the section **Switch Port Profiles**.



FIGURE 41 – NEW SWITCH PORT PROFILE AND VLANS IN THE ICX SWITCH

#### Step 5 – Create the Policy

Click **Policies** at the top menu, scroll down and click **Create New** in the **Policies** section. Enter the following information:

- Name: Enter VLAN Pool Policy
- Bandwidth Queues: Mark the checkbox 100%
- Subnets Filter: Select Block Subnets

Create Policy		Log Hits Triggers	Select All   None   Reset
Name	VLAN Pool Policy		Uwebserver DDoS Preventio
Default		Application Filters	Select All   None   Reset
Note		Application Converde	no options
		Application Forwards	
Enforcement (Llide)		Subnets Filter	Block Subnets ~
Splash Portal	- select - V	Radius servers	Select All   None   Reset
Landing Portal	- select - ~	W/ AN	
Web Cache	- select - ~	WLDAN	- Solder - Martin asen
Content Filter	- select - ~	Groups (Show)	
HTML Payload Rewrite	- select - ~	Crossia Consol	
Interstitial Redirect	- select - ~	Create	
Link Controls	no options		
Bandwidth Queues	Select All   None   Reset		
Connections Triggers	no options		
DPI Triggers	no options		
Quota Triggers	no options		
	no options		

#### FIGURE 42 – CREATE POLICY

Click **Create** to finish.



### Step 6 – Create the Account Group

Navigate to **Identities/Groups**, then click **Create New** under the **Account Groups** section. Enter the following information:

- Name: Enter a name for the account group.
- Policy: Select VLAN Pool Policy
- Disable enhanced PSK Security: Mark the Don't validate checkbox. That way we can create DPSKs that are like each other.

Create Account Group	
Name	VLAN Pool
Description	
Priority	4 v default selection (4) recommended
Disable enhanced PSK Security	Oon't validate <sup>, PSK</sup> strength or similarity to other Ac
Psk character set	Hexadecimal [A-F, 0-9]
Psk length	16
Policy	VLAN Pool Policy
Usage Plans	Select All   None   Reset Basic Plan
Note	
Create Cancel	

#### FIGURE 43 – CREATE ACCOUNT GROUP

Click Create to finish.

### Step 6a – Check the Account Groups

VLAN Pool now shows in the account groups list.

Accou	nt Groups						Columns		
	Name	e 🛆 Prioriț		Disable enhanced PSK Security	Psk character set	Psk length	Policy		
	VLAN Pool		4	V	Hexadecimal [A-F, 0-9]	16	VLAN Pool Policy		
	VLAN 100 Account Group		4	V.	Hexadecimal [A-F, 0-9]	16	VLAN 100 Policy		
	VLAN 150 Account Group		4	v.	Hexadecimal [A-F, 0-9]	16	VLAN 150 Policy		
	VLAN 200 Account Group		4	v.	Hexadecimal [A-F, 0-9]	16	VLAN 200 Policy		
4 Found									

#### FIGURE 44 - NEW ACCOUNT GROUP



### **Step 6b – Check the Policies**

Click **Policies** at the top menu. The **VLAN Pool Policy** now shows in the policies panel.



FIGURE 45 - THE VLAN POOL POLICY



### Step 7 – Create the RADIUS Realm

Navigate to **Services/RADIUS** and click **Create New** under **RADIUS Server Realms**. Enter the following information:

- Name: Enter a name for the realm. Here we entered Realm VLAN Pool.
- Rank: Select 0
- Real admission logic: Select Policy OR Attribute Pattern logic must succeed.
- Policies: Select VLAN Pool Policy
- Priority: Select 0
- Logic: Select OR
- Attribute: Select Called-Station-Id (BSSID/SSID)
- **Pattern**: Enter **vlan-pool**. That will be the SSID for the WLAN we will create later.

Create RADIUS Server Real	m								
Name	Realm VLAN Pool								
Note									
Request Matching (Hide)									
Rank	<b>0</b> v prioritize higher rank over group and attribute pattern preceden	ce when mate	ching						
Realm admission logic	Policy OR Attribute Pattern logic must succeed v logic to use	when determ	nining whether a rec						
Policies	Select All   None   Reset								
	Account, MAC, and IP groups that may match this realm								
CALEA Options	<b>no options</b> Use this realm for Accounting for the specified CALEA (	Options							
Attribute Patterns (Hide) attributes to authenticate when m	atched								
Priority Logic Attribute	Pattern	WLAN	Note						
0 V OR V Called-Station-Ic	I (BSSID/SSID) V vlan-pool	- select - 🗸							
Create Another RADIUS	Attribute Pattern								

FIGURE 46 - CREATE RADIUS SERVER REALM

Scroll down to continue.



Enter the following information:

- Sharing: Select per-Account
- VLANs: Check VLAN Pool
- Reuse: Check reuse VLAN tag assignments when necessary
- VLANs/Called-Station: Check unlimited.
- Infrastructure Devices: Check vSZ-249 (the name of your SmartZone controller)
- Inserted Attributes: Mark the checkbox for the following attributes:
  - Tunnel-Type:VLAN
  - Tunnel-Medium-Type-IEEE-802
  - Tunnel-Private-Group-Id:%vlan\_tag\_assignment.tag%
  - Ruckus-DPSK:%account.pre\_shared\_key%

Dynamic VLANs (Hide)	
Sharing	per-Account V how VLANs are shared between end-users
VLANs	Select All   None   Reset
	dynamic VLANs available for assignment
Reuse	reuse VLAN tag assignments when necessary
Inherit static	new VLAN tag assignments inherit the static attribute of an existing shared VLAN
Timeout	60 minutes VLAN
Expire at logout	immediately flush a VLAN tag assignment at logout
VLANs / Called-Station	unlimited 🗹 maximum number of *u
Infrastructure Devices	Select All   None   Reset □ICX 7150-E ♥ vsZ-249
	RADIUS NAS device(s) issuing requests for VLAN assignment
Proxy Servers (Show)	
Behavior (Hide)	
Inserted Attributes	Select All   None   Reset
	✓ Tunnel-Type:VLAN ✓ Tunnel-Medium-Type:IEEE-801 ✓ Tunnel-Private-Group-Id:%vlan_tag_assignment.tag%
	Cisco-AVpair.psk=%account.pre_shared_key%
	RADIUS attributes to include in an Access-Accept or proxied Access-Request or Accounting-Request depending
Always deny	deny all requests to this realm
Accounting (Show)	
Create Cancel	

FIGURE 47 - CREATE RADIUS SERVER REALM (CONT'D)

Click Create to finish.



### Step 7a – Check the New RADIUS Realms

RAD	IUS Server F	Realms						
	Name 🛆	Rank	Policies	CALEA Options	Attribute Patterns	Sharing	VLANs	Infrastructure Devices
	Realm VLAN Pool	0	VLAN Pool Policy	-	Called-Station-Id: vlan-pool	per- Account	VLAN Pool	vSZ-249
	Realm VLAN 100	0	VLAN 100 Policy	-	Called-Station-Id: dpsk	per- Account	VLAN 100	vSZ-249
	Realm VLAN 150	0	VLAN 150 Policy	-	Called-Station-Id: dpsk	per- Account	VLAN 150	vSZ-249
	Realm VLAN 200	0	VLAN 200 Policy	-	Called-Station-Id: dpsk	per- Account	VLAN 200	vSZ-249
4 Four	nd							

The section RADIUS Server Realms shows the new realm.

#### FIGURE 48 – REALM VLAN POOL IS CREATED

#### Step 8 – Create the WLAN

Enter the following information:

- Name: Enter vlan-pool
- Access point zone: Select the zone where the WLAN will be created.
- **Controller**: Select the SmartZone controller where the WLAN will be created.
- **AP Profiles**: Select the AP profile for the zone.
- SSID: Enter vlan-pool.
- Encryption: Select WPA2
- Authentication: Select Multiple PSK
- VLANs: Check VLAN Pool

Click Create to finish.

Create WLAN	
Name	vlan-pool
Access point zone	Enceladus ~
Note	
Provisioning (Hide)	
Controller	vSZ-249 ~
AP Profiles	Select All I None   Reset
Policies	
WLAN Configuration (Hide	)
SSID	vlan-pool
Encryption	WPA2 ~
Authentication	Multiple PSK ~
Pre-shared Key	
Default VLAN	1
Tunnel	tunnel WLAN traffic to the controller instead of locally bridging (tun
Enabled	☑ 2.4GHz ☑ 5GHz enable this WLAN on the 2.4GHz and/or 5GHz in
OFDM Only	prevents 802.11b clients from connecting to the WLAN
RADIUS Realm Server	Local RADIUS server - configure RADIUS server to be used for a
Dynamic VLANs (Hide)	
VLANS	Celect all I None   Deset
RADIUS Accounting	receive RADIUS Accounting packets from the AP
Create Cancel	

FIGURE 49 - CREATE WLAN



### Step 8a – Check the New WLAN

The section **WLANs** shows the new WLAN.

WLA	Ns								💽 Import V	WLANs 📓 Columns 🖏 Refresh
	Name 🛆	Controller	AP Profiles	Access point zone	SSID	Encryption	Authentication	Default VLAN	Tunnel	VLANs
	vlan-pool	vSZ-249	default [Enceladus]	Enceladus	vlan-pool	WPA2	Multiple PSK	1		VLAN Pool
	dpsk	vSZ-249	default [Enceladus]	Enceladus	dpsk	WPA2	Multiple PSK	1		VLAN 100, VLAN 200, VLAN 150
2 Foun	d									

#### FIGURE 50 – WLAN VLAN-POOL IS CREATED

#### Step 9 – Create the Accounts

Using this table, create two accounts, including the DPSK, in the same account group:

Account	Account Group	DSPK
user7	VLAN Pool Account Group	user7-12345678
user8	VLAN Pool Account Group	user8-12345678

FIGURE 51 – ACCOUNTS IN THE SAME ACCOUNT GROUP

Navigate to Identities/Accounts and click Create New in the Accounts section. Enter the following information:

- Login: Enter user7
- **Password and Confirmation**: Enter the password in the two fields.
- First and Last name: Enter the first and last name.
- Email: Enter an email for the account
- Group: Select VLAN Pool
- Time: Enter 15
- Download quota: Check unlimited.
- Upload quota: Check unlimited.
- Expiration: Check never

Scroll down to continue.

Create Account		
Account (Hide)		
Login	user7	username
Password and Confirmation		
First and Last name	User	Seven
Email	test@gmail.com	validated 🔽
Status	active V login disabled if not active	
lot hubs		
lot groups		
Note		
Address (Show)		
Provision (Hide)		
Group	VLAN Pool Y	
Time	15	minutes  unlimited
Download quota		MB 🗸 unlimited 🗹
Upload quota		MB ~ unlimited V
Expiration		never 🗹
Billing (Show)		

#### FIGURE 52- CREATE ACCOUNT



Enter the following information:

- Automatic login: Check automatically login devices at this account
- Max devices: Enter 3
- Pre-Shared Key: Enter user7-12345678

Sessions (Hide)		
Automatic login	automatically login devices as this account	
Automatic provision	automatically add devices on the same network to this account	
Max sessions	1	unlimited 🗌
Max devices	3	unlimited 🗌
Max party guests	0	unlimited 🗌
Max sub accounts	0	unlimited 🗌
Max dedicated IPs	0	maximum num
Dedicated IPs are static	Dedicated NAT IPs are reserved for the account and remain static	for the lifetime of t
Vtas are static		
UPnP enabled	allow UPnP requests from devices in this account	
Lock devices	prevent using these devices for other accounts	
Pre-Shared Key	user7-12345678	remains the sam
Devices (Hide)	565	
Name	MAC	Active Party
	1	
Create Another Device		
Update Cancel		

#### FIGURE 53 - CREATE ACCOUNT (CONT'D)

Click **Create** to finish.

Repeat the process to create the other account.



### Step 9a – Check the New Accounts

The section **Accounts** shows the two new accounts.

Acco	ounts								
	Login 🗢	Group	Time	Quota	Expiration	Plan	Balance	Bill	Devices
	user8	VLAN Pool	15 minutes	unlimited	never	-	\$0.00	-	7
	user7	VLAN Pool	15 minutes	unlimited	never		\$0.00	-	-

#### FIGURE 54 – TWO NEW ACCOUNTS

#### **Test Results**

In the example, we used MacBook with account **user8** to connect to WLAN vlan-pool. After authentication, it got associated to VLAN 303, which is included in the VLAN pool, and received an IP address from the DHCP scope **30.0.13 – 30.0.14** 



FIGURE 55 – TEST USING A MACBOOK USING USER8

In the diagram below, two different devices connected using different accounts. As expected, they were associated to VLAN 301 and VLAN 303 from the VLAN pool and received addresses from dedicated IP subnets.

Accounts												
Login 🛆	Group	Time	Quota	Expiration	Plan	Balance	Bill	Devices	Parties	VLANs		
user7	VLAN Pool	15 minutes	unlimited	never	-	\$0.00	-	ae:9e:8a:b1:23:f8	-	301		
user8	VLAN Pool	15 minutes	unlimited	never	-	\$0.00		Marcelos-MBP	-	303		





Enter the client IP address and click **Search** at the top right menu to see details for the authenticated client.



#### FIGURE 57 – SEARCHING A DEVICE

#### **Delete an Existing Device**

If you try to authenticate with a device that is already associated to a different DPSK, the new authentication will fail. To delete an existing device association, navigate to **Identities/Accounts**, look for the account with the device in use, then click the device ① to bring up the list of devices for that account. Click **Delete** ② in the device entry. Do not click **Delete** at the top right, otherwise you will delete the entire account.

								1		Do not use this delete button, delete the entire account —				otherwise you will		
	user7	VLAN Pool		15 minutes	unlimited	never	\$0.00	ae:9e:8a:b1:23:f8		301			Actions	Edit	Delete	Show
Devices for user7										🖏 Refresh 🔀 Export 🕝 Import 🔗 Batch	🛟 Zoom 🔇	Search	O Creat	e New 🛛 🗙		
	Update	d	$\bigtriangledown$	Name		MAC	Active Party	Static IP	BINAT	Hide from	portal	Device posture				
	02/14/20	023 02:34 PM		ae:9e:8a:bl	:23:f8	<b>Q</b> ae:9e:8a:b1:23:f8								Edit	Delete	Show
1 Found																
														(	2	





## **DPSK Using PMS Integration**

RWG can be integrated with the Property Management System (PMS) guest databases of many large hotel chains, like Marriot, Hilton, and Clarion. The table at the right shows all PMS platforms supported by RWG.

A **PMS Server** entry needs to be created in RWG. Some of RWG's PMS integrations import all the guests, while others act as proxy, populating the RWG database with a new entry when a guest tries to authenticate. For the integrations where all guests are imported, RWG can create DPSKs automatically, using a combination of the guest's last name, room number, email, or any other field from the guest database.

**MICROS FIAS** is a PMS used by several hotel chains, and it is one of the PMS's that supports importation of all guests. FIAS stands for **Fidelio Interface Application Specification**. It is a hospitality standard developed by MICROS and Oracle, which can be used by different kinds of PMSs to exchange data.

The next sections will describe how to use MICROS FIAS with a simulated PMS and database included with RWG, to create DPSKs and test guest authentication.

Agilysys LMS Clarity Comtrol UHLL Galaxy 2-Way HSIA Hilton OnQ Infor InnQuest Innsist ✓ MICROS FIAS MICROS HTNG

Marriott

Mews

- RG Nets
- Resco
- SMS Host MSIP

#### FIGURE 59 – SUPPORTED PMS PLATFORMS



#### Step 1 – Create a PMS Server

Navigate to **Billing/Gateways** and click **Create New** under the section **PMS Servers**. Enter the following information:

- Name: Enter the name for the PMS entry. Here, we used USS Enterprise
- Account sharing: Select per-Guest
- Interface: Select MICROS FIAS
- Transport protocol: Select IP
- Host: Enter 127.0.0.1
- Port: Enter 5010
- Timeout: Enter 30

You can keep the defaults for all other parameters.

Create PMS Server	
Name	USS Enterprise
Note	
Available Plans (Show)	
Plans Behavior (Show)	
Accounts Behavior (Hide)	
Account sharing	per-Guest v how an account is shared between registered guest
Automatic login fallback	look for an existing account via automatic login (MAC/cookie) when
Transactions Behavior (Sh	ow)
Subsequent Transactions I	Discount (Show)
Interface Specification (Hid	le)
Interface	MICROS FIAS Y PMS type
Transport protocol	▶ w how the PMS is connected to the rWg
Host	127.0.0.1
Port	5010
Timeout	30
Web Service (Show)	
Agilysys (Show)	
Clarity (Show)	
Comtrol (Show)	
Infor (Show)	
Create Cancel	



Click **Create** to finish.



### **Step 1a – Check the Results**

The new PMS server entry is created, but the RWG database has not imported the guests yet, because the MICROS FIAS server in RWG is not active yet.

PMS Serv	ers								43	Restart Interface	Columns 🕻 Refresh	🛃 Export 🐇	Batch
	Name	$\triangle$	Interface	Host		Ac	count sharing	l	Usage Plans				
	USS Enterprise		MICROS FIAS	IP: 127.0	0.0.1:5010	pe	r-Guest						
1 Found													
Rooms											🐻 Columns 🐧	Refresh 🛃	Export
	Room	$\triangle$	Guests	VLANs		Server	Property		Infrastruct	ture devices			Switch
							No Entries						
0 Found													
Guests													Column
Updated	▽ Rooms	Last	First	litle Language	Number	No post	Arrival	Departure	Checkin	Checkout	Accounts	VLANS	5
							No Entries						
0 Found													

#### FIGURE 61 – NEW PMS SERVER

#### Step 2 – Activate the RWG FIAS Server

Start a SSH session to RWG, then enter the following command:

[marcelo@rwg-home ~]\$ iui
ANNMTSGHDQVIAXMLXPJBDCFF < this is the su password HCPTFFGWQCPOGGMWZFSGOJUS
4 3000 8192 214 ANNMTSGHDQVIAXMLXPJBDCFF HCPTFFGWQCPOGGMWZFSGOJUS

#### FIGURE 62 – COPY THE SU PASSWORD

The first line of characters is the **su** password. Elevate the session to **su** level using the following command, plus the password obtained above:

[marcelo@rwg-home	~]\$ su -
Password:	
rwg-home#	

FIGURE 63 – MOVE TO SU LEVEL



Enter the following commands, followed by CTRL-D:

```
[marcelo@rwg-mm ~]$ cat > /etc/rc.local.hook
#!/bin/sh
/space/rxg/rxgd/debug/gen_fias_guest_list > /space/guest_list.csv
nohup /space/rxg/rxgd/debug/fias_server.py -g /space/guest_list.csv &
```

The first line opens the file named **rc.local.hook**, next you add three lines, and the **CTRL-D** writes the file and closes it. After that, enter the following command to make the file executable:

[marcelo@rwg-mm ~]\$ chmod +x /etc/rc.local.hook

Finally, enter the following command to create the database:

[marcelo@rwg-mm ~]\$ sh /etc/rc.local.hook

[marcelo@rwg-mm ~]\$ appending output to nohup.out

Return to the RWG UI and click **Refresh** in the sections **Rooms** and **Guests**. You should see 79 entries for rooms and 82 entries for guests.

Rooms							🗟 Columns 🚺 Refresh 🛃 Export 🛷 Batch 💠 Zoom
	Room 🛆	Guests	VLANs	Server	Property	Infrastructure devices	Switch Ports
	1018	Soong	-	USS Enterprise			-
	1028	Chapel	-	USS Enterprise			
	1106	Soji	-	USS Enterprise			
	111	Spock	-	USS Enterprise			
	1111	Khan	-	USS Enterprise			
	1117	Worf	-	USS Enterprise			-

Guests	uests								
Updated	Rooms	Last	First	Title	Language	Number	Arrival	Checkin	Server
02/14/2023 07:52 PM	1018	Soong		Mr	EA	3176517	02/14/2023	02/14/2023 07:52 PM	USS Enterprise
02/14/2023 07:52 PM	1028	Chapel		Mr	EA	4431753	02/08/2023	02/14/2023 07:52 PM	USS Enterprise
02/14/2023 07:52 PM	1106	Soji		Mr	EA	7613414	02/13/2023	02/14/2023 07:52 PM	USS Enterprise
02/14/2023 07:52 PM	m	Spock		Mr	EA	5965194	02/09/2023	02/14/2023 07:52 PM	USS Enterprise
02/14/2023 07:52 PM	m	Khan		Mr	EA	9620943	02/09/2023	02/14/2023 07:52 PM	USS Enterprise
02/14/2023 07:52 PM	1117	Worf		Mr	EA	7143941	02/11/2023	02/14/2023 07:52 PM	USS Enterprise
02/14/2023 07:52 PM	1162	Pike		Mr	EA	7204706	02/13/2023	02/14/2023 07:52 PM	USS Enterprise

FIGURE 64 - NEW ROOMS AND GUESTS



### **Generate PMS DPSKs**

Now let's create DPSKs that combine the guest's last name and room number in any order, with or without a space between them. For example, user **Spock** in room **111** will generate four DPSKs:

- Spock111
- 111Spock
- Spock 111
- 111 Spock

We will use the **Custom Data Set** and **Custom Data Keys** scaffolds to create the rules to generate the DPSKs.

**Note**: For the DPSKs generation to work, it is mandatory that a WLAN using **Multiple PSK** is already configured in RWG. If you followed the two initial use cases in this slide deck, you already have the WLANs **dpsk** and **vlan-pool** configured.

#### Step 3 – Create the Custom Data Set

Navigate to **System/Portals** and click **Create New** in the section **Custom Data Set**. Enter the following information:

- Name: Enter a name for the custom data set.
- Note: Enter PMS in capital letters. This is not an optional entry.

Create Custom Data Sets	
Name	USS Enterprise DPSKs
Policies	Select All   None   Reset
Note	PMS
Attributes (Hide)	
Keys	no options
Create Cancel	



Click **Create** to finish.



### Step 4 – Create the First Custom Data Key

Navigate to **System/Portals** and click **Create New** in the section **Custom Data Key**. Enter the following information:

- Dataset: Make sure USS Enterprise DPSKs is selected.
- Name: Enter pms\_guest in lowercase.
- String: Enter name in lowercase.

Create Custom Data Key	
Dataset	USS Enterprise DPSKs ~
Note	
Key (Hide)	
Name	pms_guest
Value (Hide)	
String	name
Text	
Boolean	
Decimal	
Integer	
Date	
Time	12:00 AM O
Date-time	
Create Cancel	

#### FIGURE 66 – CREATE FIRST CUSTOM DATA KEY

Click **Create** to finish.

**Note**: The values entered at the string field can be found at the following URL: <u>https://{rwg-ip-address}/rdoc/PmsGuest.html</u>



### Step 4a – Create the Second Custom Data Key

Navigate to **System/Portals** and click **Create New** in the section **Custom Data Key**. Enter the following information:

- Dataset: Make sure USS Enterprise DPSKs is selected.
- Name: Enter pms\_room in lowercase.
- String: Enter room in lowercase.

Create Custom Data Key	
Dataset	USS Enterprise DPSKs ~
Note	
Key (Hide)	
Name	pms_room
Value (Hide)	
String	room
Text	
Boolean	
Decimal	
Integer	
Date	
Time	12:00 AM 🛇
Date-time	
Create Cancel	

#### FIGURE 67 – CREATE SECOND CUSTOM DATA KEY

Click Create to finish.

#### Step 5 – Check the Results and Restart the Interface

You should see one entry for **Custom Data Set** and two entries for **Custom Data Keys**.

Custom Data Set						
	Name	$\bigtriangleup$	Policies	Keys		
	USS Enterprise DPSKs		-		-	
1 Found	1 Found					
Custom Data Ke	eys					
	Dataset	Name		Value	Туре	
	USS Enterprise DPSKs	pms_guest		name	string	
	USS Enterprise DPSKs	pms_room		room	string	
2 Found						

#### FIGURE 68 – ONE DATA SET AND TWO DATA KEYS



To generate the DPSKs based on the custom data set and data keys, you need to restart the PMS interface. Click **Restart Interface**.

PMS Servers									ıs 🖏 Refresh
		Name	$\bigtriangleup$	Interface	Host	Account sharing	Usage Plans		
		USS Enterprise		MICROS FIAS	IP: 127.0.0.1:5010	per-Guest			
	l Found								



#### Step 6 – Check the DPSKs

Open a SSH session to your RWG instance and enter the following command:

```
[marcelo@rwg-home ~]$ console
Loading development environment (Rails 7.0.4)
[1] pry(main)>
```

FIGURE 70 – ENTERING THE RUBY ON RAILS CONSOLE

After a few moments, you will enter the **Ruby on Rails** console. Enter the following command to see the number of DPSK entries created:

[3] pry(main)> PairwiseMasterKey.count => 339 [4] pry(main)>

FIGURE 71 – NUMBER OF DPSKS CREATED

Enter the following command to see the DPSKs, then hit the space bar until you start to see the DPSKs from the PMS guest database. Enter **q** to stop the listing and **exit** to quit the Ruby on Rails console.



FIGURE 72 – LISTING THE DPSKS



### **Optional Step**

You can create additional custom data sets and data keys to generate DPSKs using different patterns. The following configurations show a new data set and two new data keys to generate DPSKs with the last name in lowercase:

Update pms lower case	
Name	pms lower case
Policies	Select All   None   Reset Default ICX 7150-B VLAN 100 Policy VLAN 150 Policy VLAN
Note	PMS
Attributes (Hide)	
Keys	Select All   None   Reset
Update Cancel	
Undate nms_quest	
Dataset	pms lower case V
Note	lc
Key (Hide)	
Name	pms_guest
Value (Hide)	
String	name
Text	
Undete nuce veen	
Dataset	nms lower case
Note	
Kov (Hido)	1
Name	pms room
Value (Ulde)	
value (Hide)	(room)
String	
rext	

FIGURE 73 – DATA SET AND DATA KEYS TO GENERATE DPSKS WITH LAST NAME IN LOWERCASE



**Ic** is a function to generate a lower-case string. The other available functions are: **uc** (uppercase) and **ucfirst** (first letter only is uppercase).

You need to restart the PMS interface after the new data set and data keys are created.

Using that configuration, the user Spock in room 111 will generate the following DPSKs: **spock111**, **111spock**, **spock 111** and **111 spock**.

#### Step 7 – Edit the RADIUS Realm

We will use the RADIUS realm for vlan-pool that we created in the section DPSK Using a VLAN Pool.

Navigate to Services/RADIUS, then click Edit in the entry Realm VLAN Pool.

RADIUS Server Realms							🗟 Columns 🚺 Refresh 🛃 Export 🛷 Batch 💠 Zoom			? Help 🔍 Search 🔇 Create New		
	Name 🛆	Rank	Policies	Attribute Patterns	Sharing	VLANs	Infrastructure Devices	PMS Servers	Create Account			
	Realm VLAN 100	0	VLAN 100 Policy	Called-Station-Id: dpsk	per-Account	VLAN 100	√SZ-249			Edit (	Selete	Show
	Realm VLAN 150	0	VLAN 150 Policy	Called-Station-Id: dpsk	per-Account	VLAN 150	vSZ-249			Edit (	Delete	Show
	Realm VLAN 200	0	VLAN 200 Policy	Called-Station-Id: dpsk	per-Account	VLAN 200	vSZ-249			Edit [	Delete	Show
	Realm VLAN Pool	0	VLAN Pool Policy	Called-Station-Id: vlan-pool	per-Account	VLAN Pool	vSZ-249	-		Edit	Delete	Show
4 Found	i											

#### FIGURE 74 – EDITING THE RADIUS REALM

Scroll down, then enter the following information:

- PMS Servers: check USS Enterprise.
- Create Account: check create accounts for new proxied authentications.

Proxy Servers (Hide)					
RADIUS Servers	no options remote RADIUS server to proxy authentication against				
LDAP Domains	<b>no options</b> Active Directory realm to authenticate against				
PMS Servers	Select All None Reset				
Proxy Options (Hide)					
Proxy packets	Accounting 🗹 Authentication 🗹 packet types to proxy				
Proxy MAC auth	proxy MAC auth requests (authentication and accounting)				
Replace username	replace User-Name attribute with account login before proxying				
Create Account	create accounts for new proxied authentications				
Usage Plans	Select All   None   Reset				
Underson Connect					
Update Cancel					



Click Update to finish.



### **Test Results**

In this example, we used a MacBook with the DPSK 1006Soong to connect:

Ŷ	The Wi-Fi WPA2 pase You can also password fr connected t	network "vlan-pool" requires a sword. o access this Wi-Fi network by sharing the om a nearby iPhone, iPad, or Mac which has o this network and has you in their contacts.	<pre>#<pairwisemasterkey:0x0000000812c34a28 "1006soong",="" "vlan-pool",="" 1052403,="" <="" id:="" pre="" psk:="" ssid:=""></pairwisemasterkey:0x0000000812c34a28></pre>
	Password:	1006Soong ✓ Show password	pms_room_id: 149,
		<ul> <li>Remember this network</li> </ul>	pms_guest_1d: 156, wlan_id: 136,
?		Cancel Join	

FIGURE 76 – CONNECTING USING A DPSK GENERATED FROM THE PMS GUEST DATABASE

Navigate to **Identities/Accounts** to see the authenticated users. You should see a new account created automatically for any user authenticated with the DPSK generated from the PMS server guest database.

**Note**: When using DPSKs from a PMS server, the devices used by the account will only show if a billing plan is added to the RADIUS realm. RWG's billing plans will be covered in another document.

# 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

#### www.ruckusnetworks.com

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

© 2023 CommScope, Inc. All rights reserved.

All trademarks identified by  $^{\rm TM}$  or  $^{\otimes}$  are trademarks or registered trademarks in the US and may be registered in other countries. All product names, trademarks and registered trademarks are property of their respective owners.

