Deployment Guide

RUCKUS WAN Gateway - DPSK Step-by-Step Configuration

June 2023

Rev. 1

Table of Contents

© 2023 CommScope Inc. All rights reserved.

© 2023 CommScope Inc. All rights reserved.

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 https://support.ruckuswireless.com/

The RWG documentation is embedded into the product.
You can access the embedded documentation at https://{your RWG_IP_address}/admin/manual/help_online

© 2023 CommScope Inc. All rights reserved.

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.

© 2023 CommScope Inc. All rights reserved.

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.

© 2023 CommScope Inc. All rights reserved.

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.

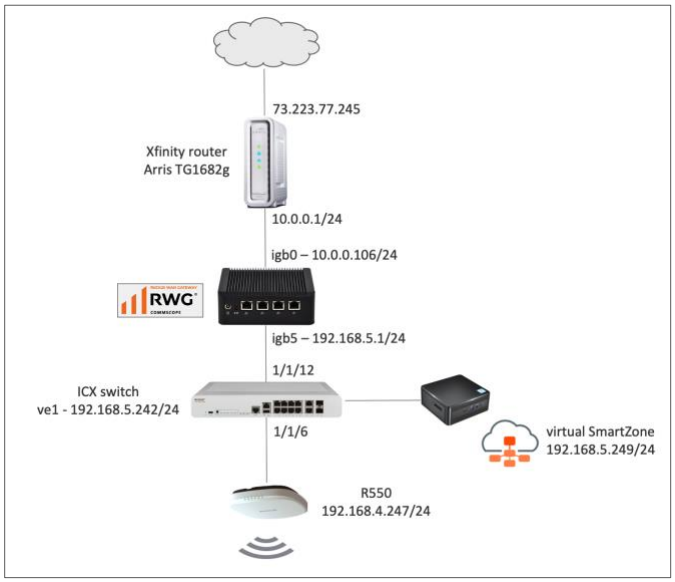
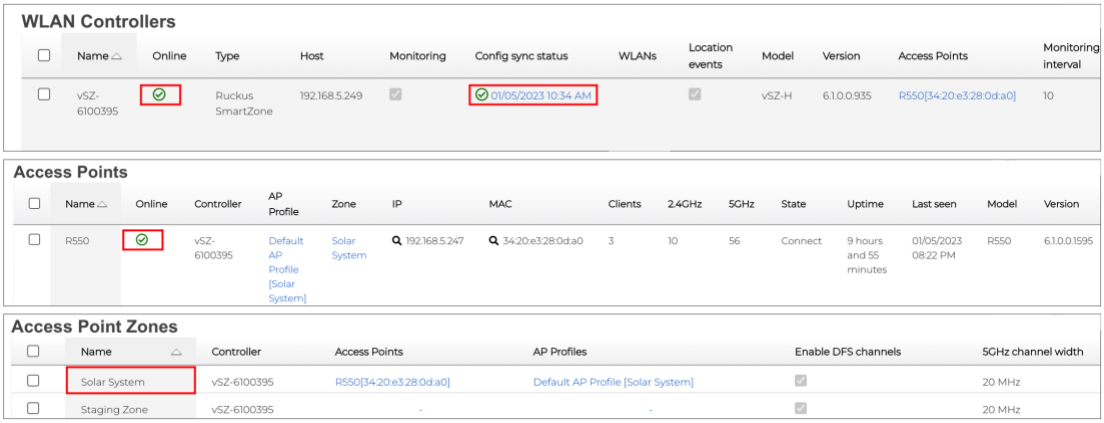


FIGURE 1 – TEST TOPOLOGY

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.



WLAN Controllers

Name	Online	Type	Host	Monitoring	Config sync status	WLANs	Location events	Model	Version	Access Points	Monitoring interval
vSZ-6100395	✓	Ruckus SmartZone	192.168.5.249	✓	01/05/2023 10:34 AM		✓	vSZ-H	6.1.0.0.935	R550[34:20:e3:28:0d:a0]	10

Access Points

Name	Online	Controller	AP Profile	Zone	IP	MAC	Clients	2.4GHz	5GHz	State	Uptime	Last seen	Model	Version
R550	✓	vSZ-6100395	Default AP Profile [Solar System]	Solar System	192.168.5.247	34:20:e3:28:0d:a0	3	10	56	Connect	9 hours and 55 minutes	01/05/2023 08:22 PM	R550	6.1.0.0.1595

Access Point Zones

Name	Controller	Access Points	AP Profiles	Enable DFS channels	5GHz channel width
Solar System	vSZ-6100395	R550[34:20:e3:28:0d:a0]	Default AP Profile [Solar System]	✓	20 MHz
Staging Zone	vSZ-6100395	-	-	✓	20 MHz

FIGURE 2 – SMARTZONE IS ONLINE AND IN SYNC

© 2023 CommScope Inc. All rights reserved.

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.

Switches

Name	Online	Type	Host	Monitoring	Config sync status	Location events	Model	Version	Ports	Pms rooms	Monitoring interval
ICX 7150-B	✓	Ruckus ICX Switch	192.168.5.242	✓	✓ 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**.

© 2023 CommScope Inc. All rights reserved.

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.

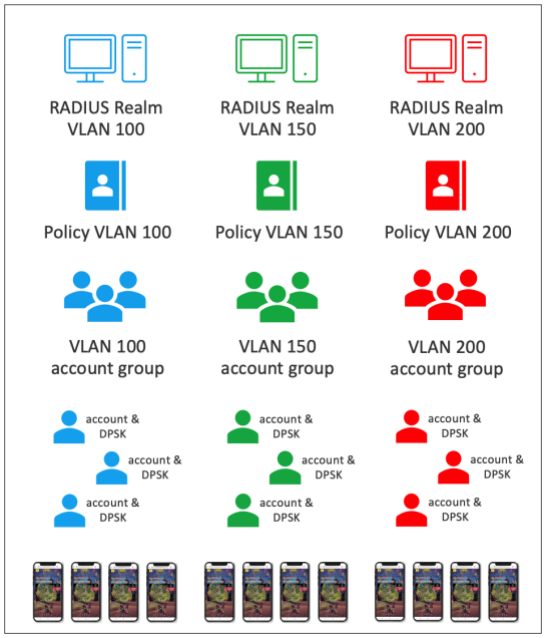


FIGURE 4 – EACH VLAN NEEDS A SEPARATE RADIUS REALM, POLICY, AND ACCOUNT GROUP

© 2023 CommScope Inc. All rights reserved.

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.

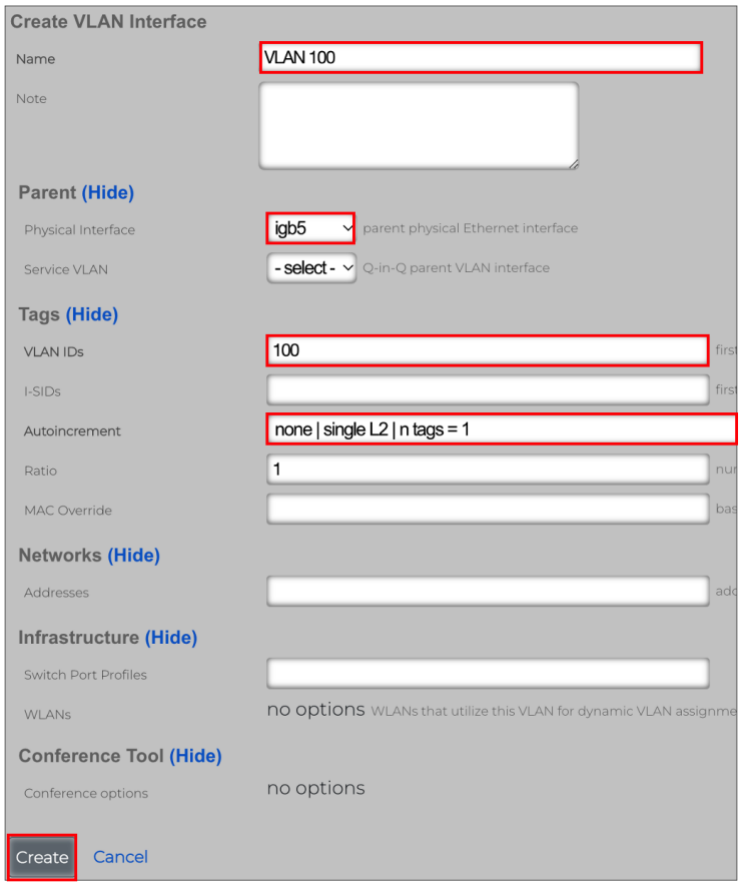


FIGURE 5 – CREATE VLAN INTERFACE

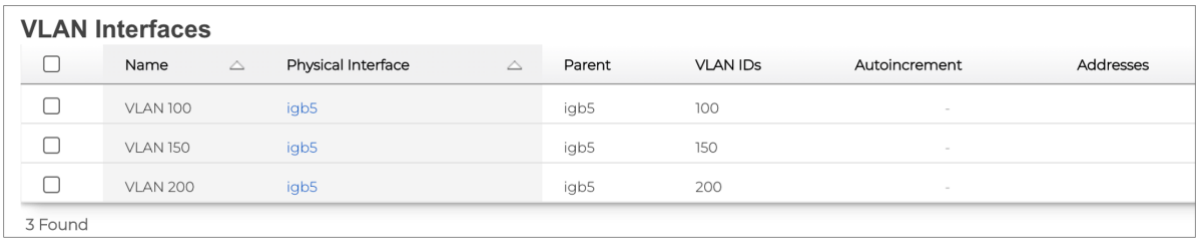
Click **Create** to finish.

Use the same procedure to create VLANs 150 and 200.

© 2023 CommScope Inc. All rights reserved.

Step 1a – Check the VLANs

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



VLAN Interfaces

Name	Physical Interface	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.

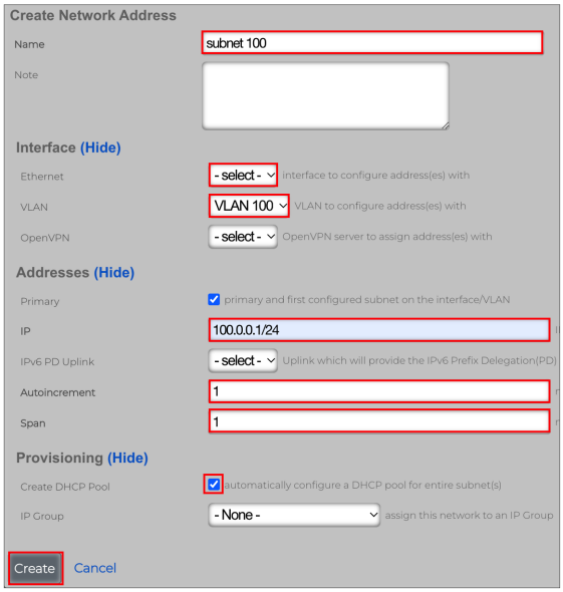


FIGURE 7 – CREATE NETWORK ADDRESS

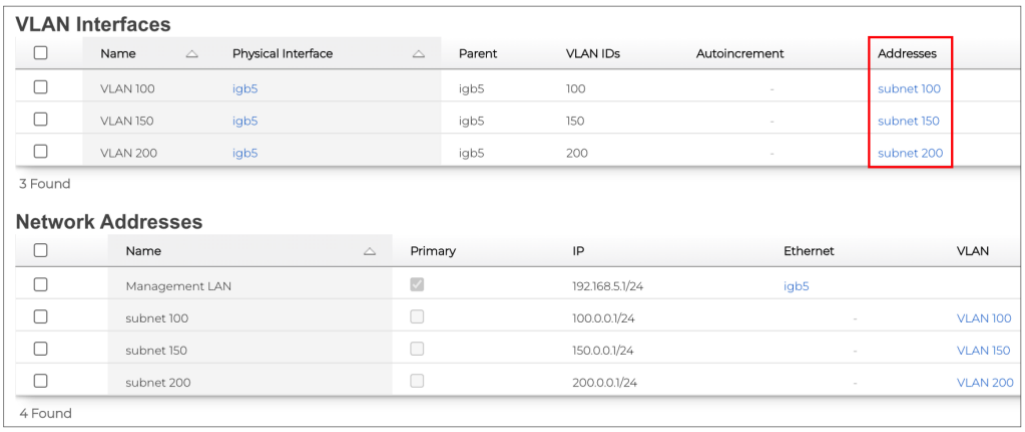
Click **Create** to finish.

Use the same procedure to create subnets 150 and 200.

© 2023 CommScope Inc. All rights reserved.

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 Interfaces

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

Network Addresses

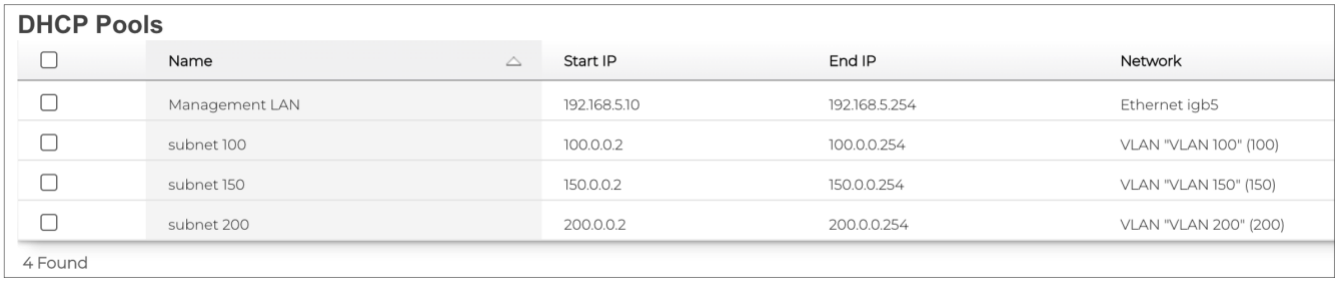
Name	Primary	IP	Ethernet	VLAN
Management LAN	☑	192.168.5.1/24	igb5	
subnet 100	☐	100.0.0.1/24	-	VLAN 100
subnet 150	☐	150.0.0.1/24	-	VLAN 150
subnet 200	☐	200.0.0.1/24	-	VLAN 200

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	100.0.0.254	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

© 2023 CommScope Inc. All rights reserved.

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.

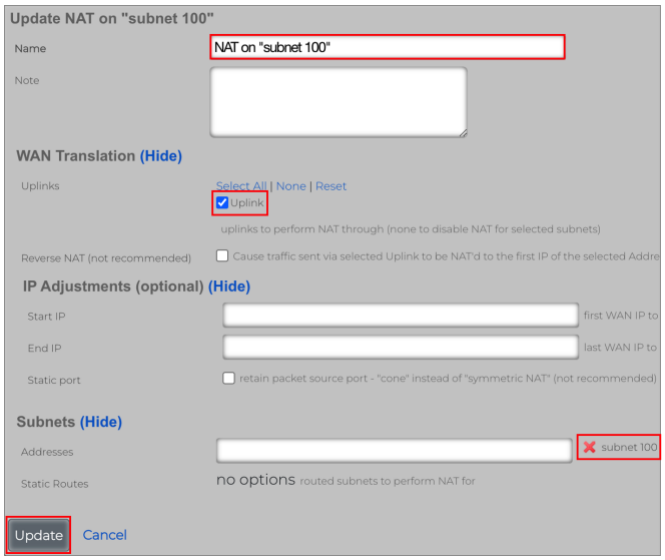


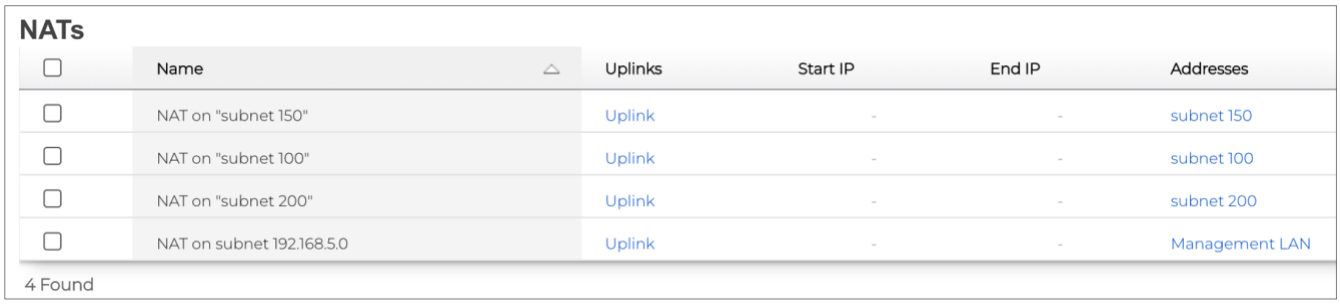
FIGURE 10 – ENABLE THE NAT ENTRY

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

FIGURE 11 – THREE NEW NAT ENTRIES

© 2023 CommScope Inc. All rights reserved.

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.

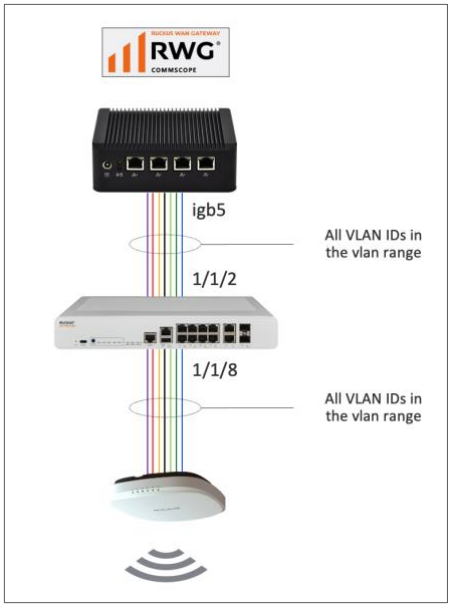


FIGURE 12 – VLANS WITH TAGGED INTERFACES

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.

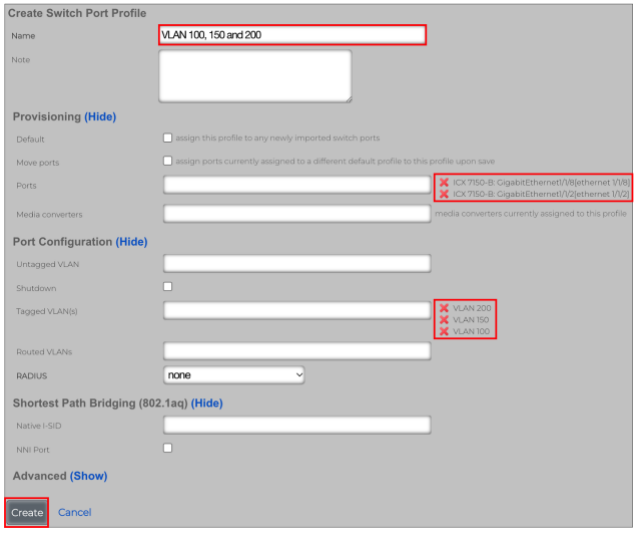


FIGURE 13 – CREATE SWITCH PORT PROFILE

Click **Create** to finish.

© 2023 CommScope Inc. All rights reserved.

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**.


```
SSH@ICX 7150-B(config)#sh ru vlan
vlan 1 name DEFAULT-VLAN by port
!
vlan 100 by port
 tagged ethe 1/1/2 ethe 1/1/8
!
vlan 150 by port
 tagged ethe 1/1/2 ethe 1/1/8
!
vlan 200 by port
 tagged ethe 1/1/2 ethe 1/1/8
!
vlan 999 name Auth-Default by port
!
```

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**.

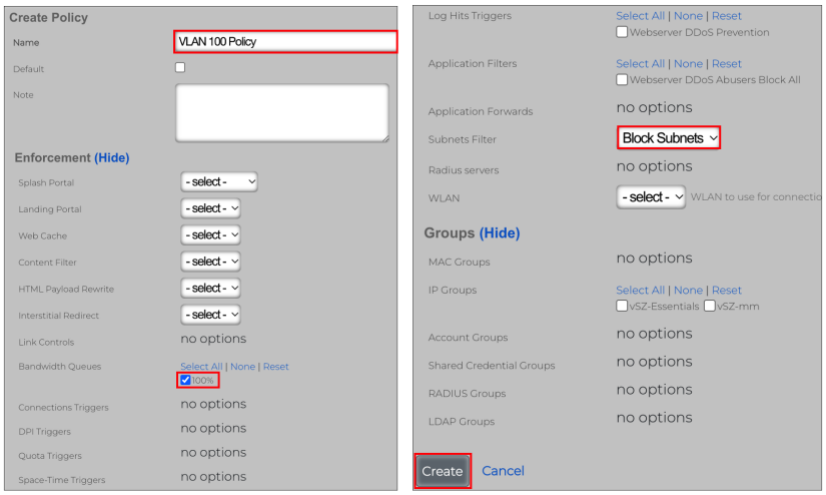


FIGURE 15 – CREATE POLICY

Click **Create** to finish.

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

© 2023 CommScope Inc. All rights reserved.

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.

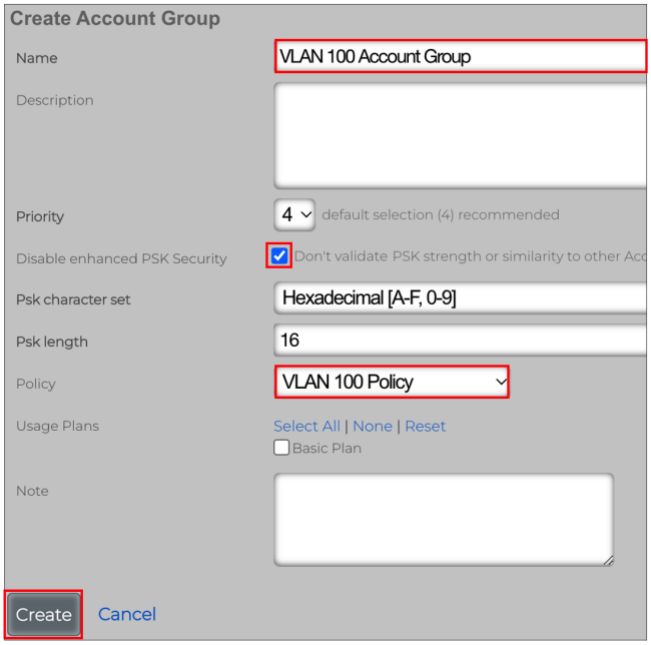


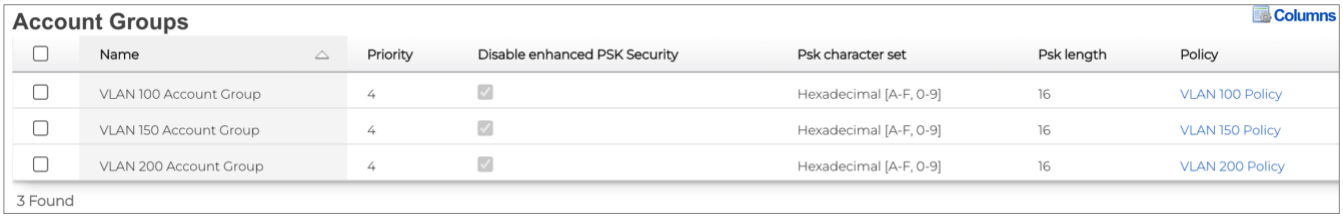
FIGURE 16 – CREATE ACCOUNT GROUP

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.



Account Groups

Columns

Name	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

FIGURE 17 – THREE NEW ACCOUNT GROUPS

© 2023 CommScope Inc. All rights reserved.

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.

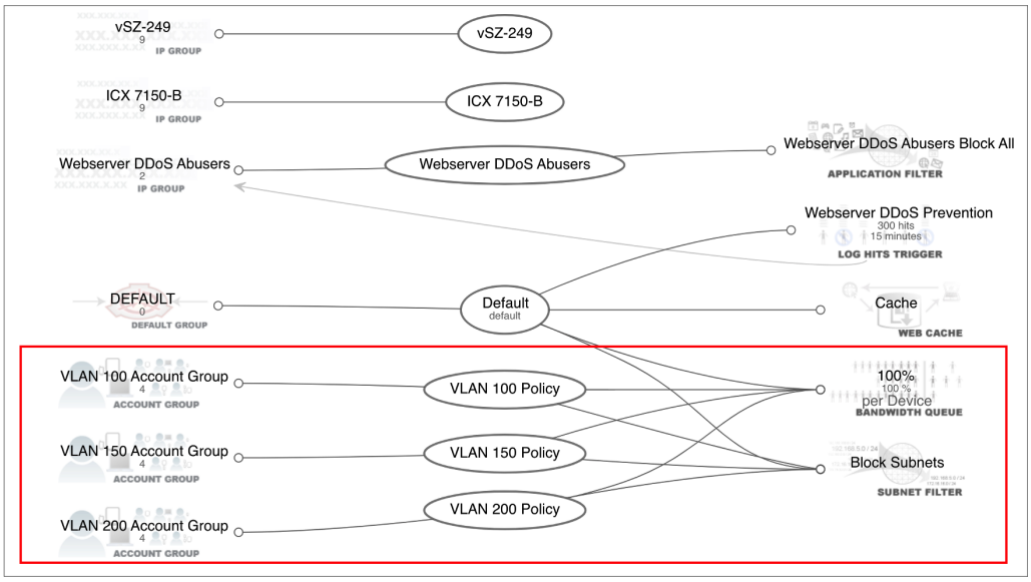


FIGURE 18 – POLICY ASSOCIATIONS

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.

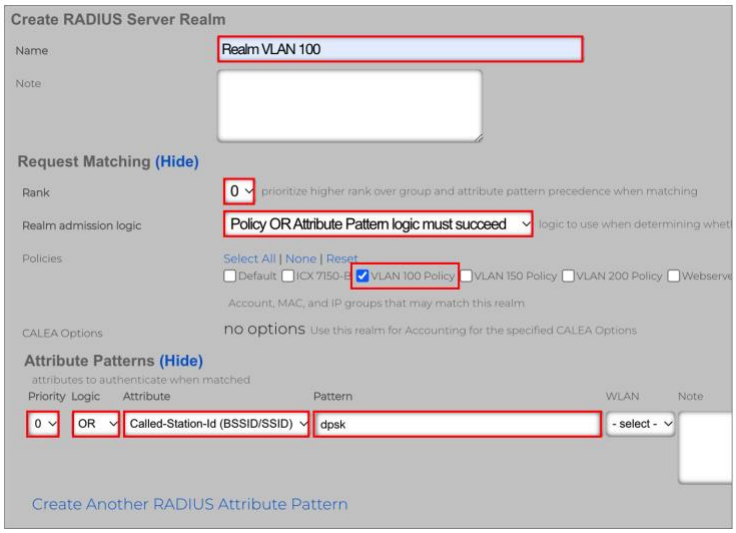


FIGURE 19 – CREATE RADIUS SERVER REALM

© 2023 CommScope Inc. All rights reserved.

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%

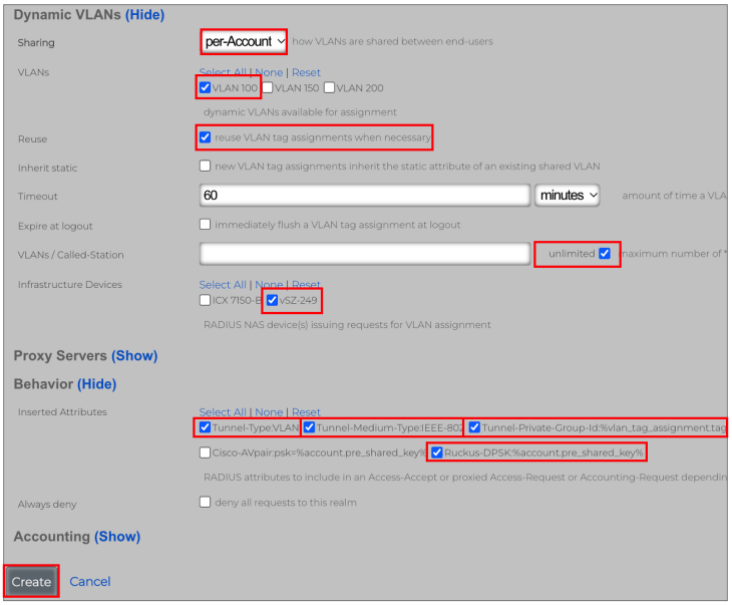
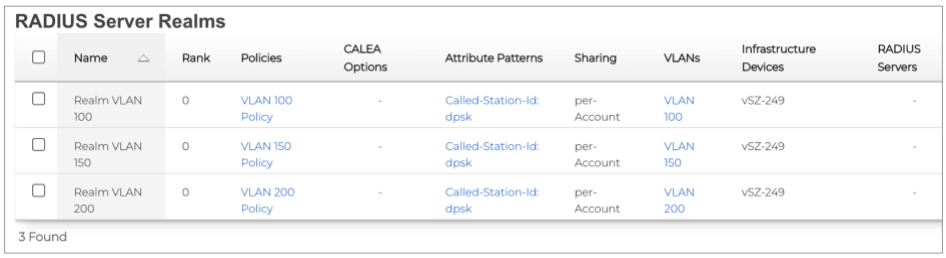


FIGURE 20 – CREATE RADIUS SERVER REALM (CONT'D)

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:



RADIUS 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	-

3 Found

FIGURE 21 – THREE NEW RADIUS SERVER REALMS

© 2023 CommScope Inc. All rights reserved.

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**

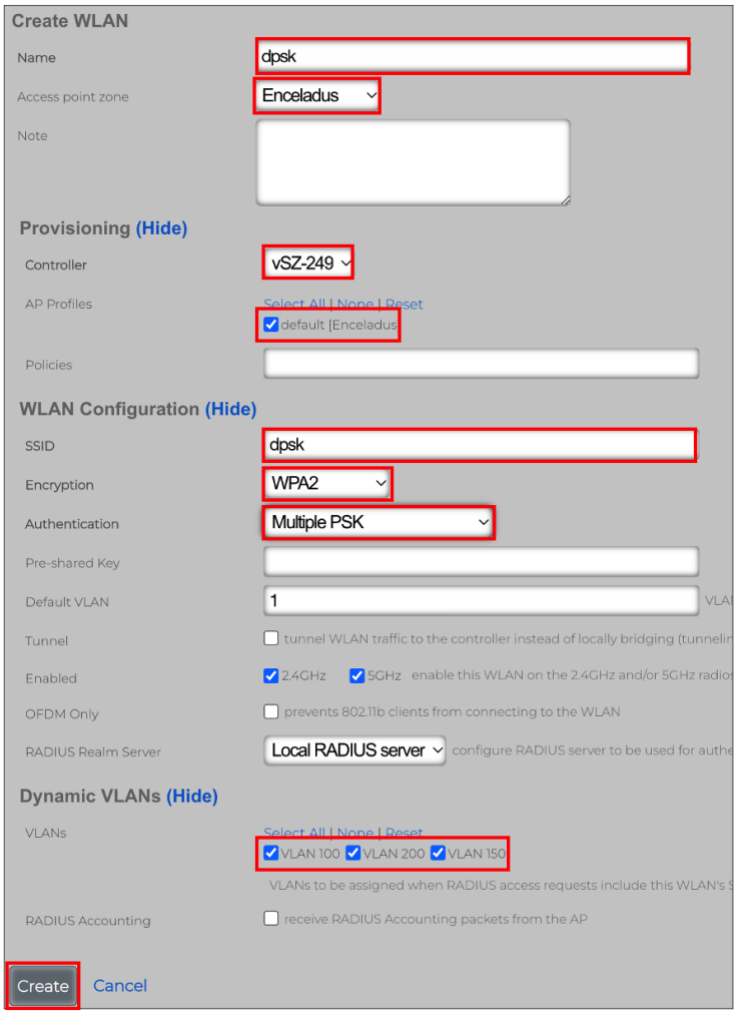


FIGURE 22 – CREATE WLAN

Click **Create** to finish.

© 2023 CommScope Inc. All rights reserved.

Step 8a – Check the WLAN

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

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**

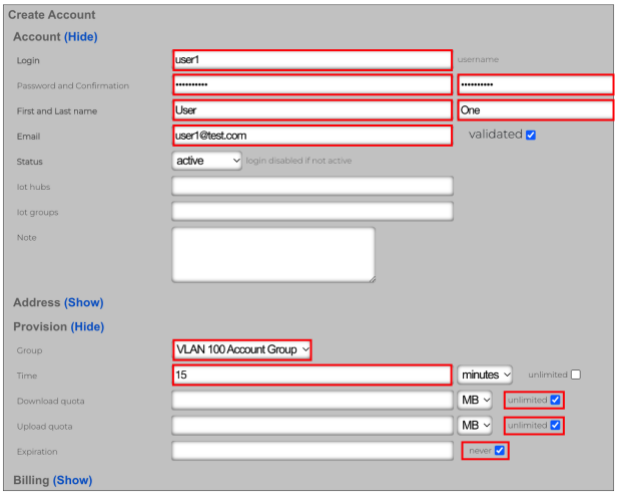


FIGURE 25 – CREATE ACCOUNT

Scroll down to continue.

© 2023 CommScope Inc. All rights reserved.

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)

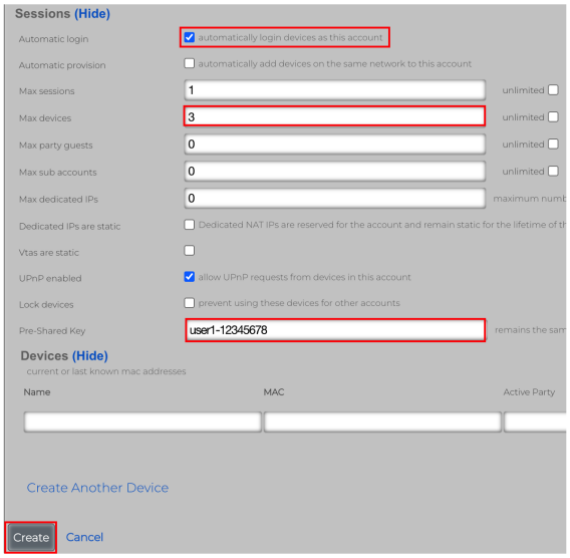
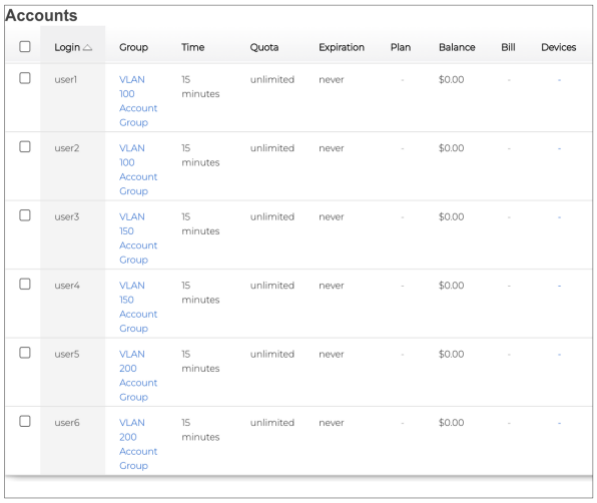


FIGURE 26 – CREATE ACCOUNT (CONT'D)

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.



Accounts

Login	Group	Time	Quota	Expiration	Plan	Balance	Bill	Devices
user1	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

© 2023 CommScope Inc. All rights reserved.

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.

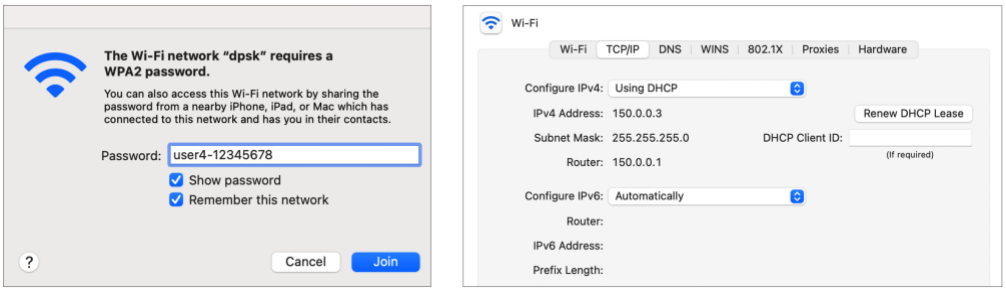
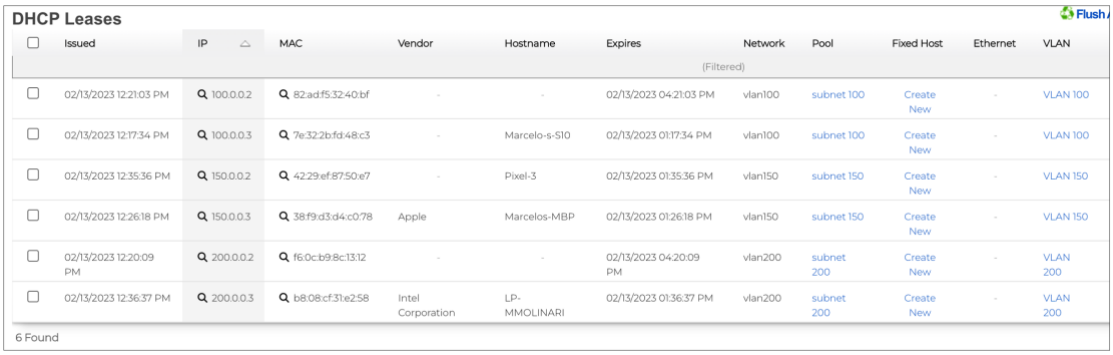


FIGURE 28 – USER4 IS CONNECTED

As expected, it got associated to VLAN 150 and received an IP address from the DHCP scope **150.0.0.2 – 150.0.0.254**.

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.



DHCP Leases

Issued	IP	MAC	Vendor	Hostname	Expires	Network	Pool	Fixed Host	Ethernet	VLAN
02/13/2023 12:21:03 PM	100.0.0.2	82:adf5:32:40:bf	-	-	02/13/2023 04:21:03 PM	vlan100	subnet 100	Create New	-	VLAN 100
02/13/2023 12:17:34 PM	100.0.0.3	7e:32:2b:fd:48:c3	-	Marcelo-s-S10	02/13/2023 01:17:34 PM	vlan100	subnet 100	Create New	-	VLAN 100
02/13/2023 12:35:36 PM	150.0.0.2	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	150.0.0.3	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	200.0.0.2	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	200.0.0.3	b8:08:cf:31:e2:58	Intel Corporation	LP-MMOLINARI	02/13/2023 01:36:37 PM	vlan200	subnet 200	Create New	-	VLAN 200

6 Found

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.

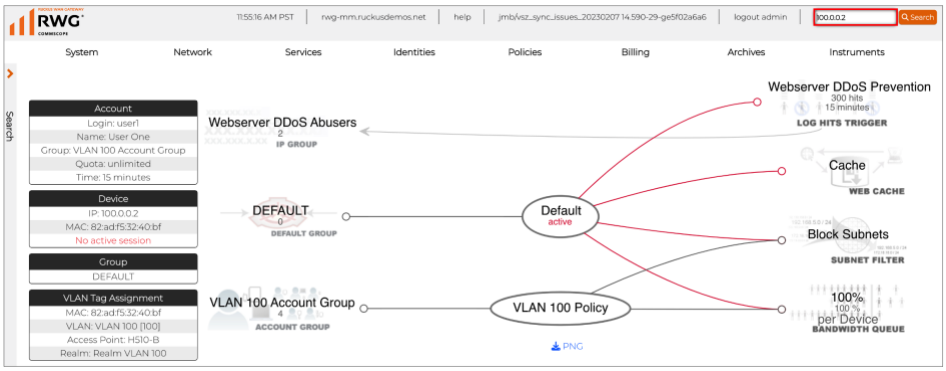


FIGURE 30 – USING THE SEARCH TOOL

© 2023 CommScope Inc. All rights reserved.

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.

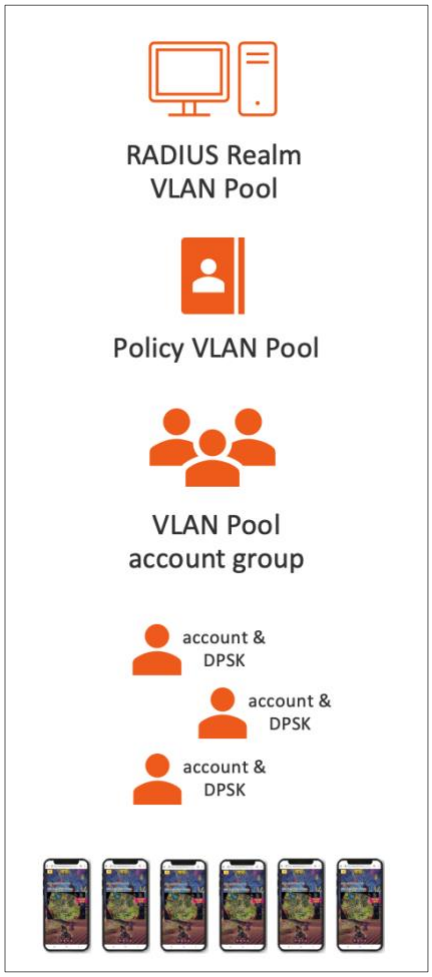


FIGURE 31 – ONE RADIUS REALM, ONE POLICY, ONE ACCOUNT GROUP AND ONE VLAN POOL

© 2023 CommScope Inc. All rights reserved.

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**

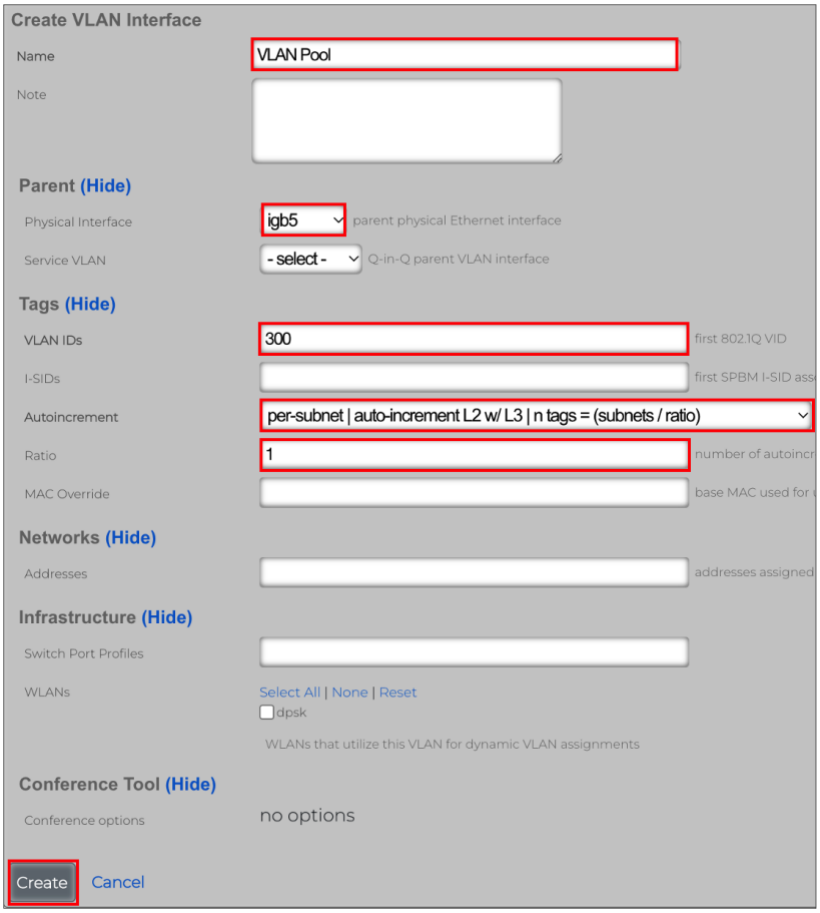


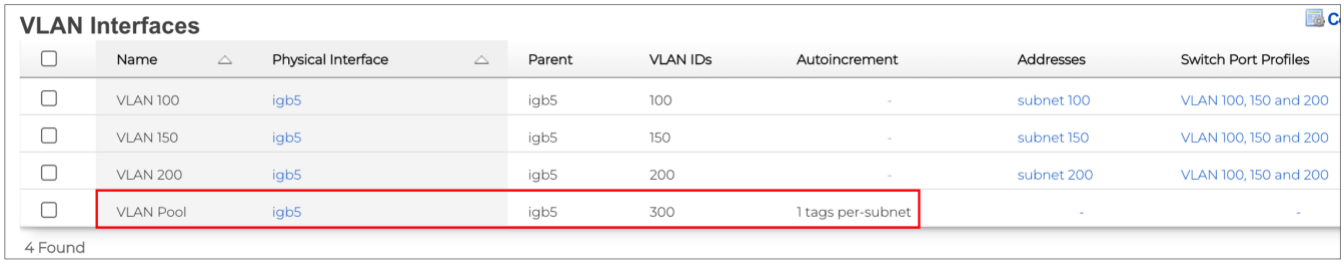
FIGURE 32 – CREATE VLAN INTERFACE

Click **Create** to finish.

© 2023 CommScope Inc. All rights reserved.

Step 1a – Check the VLANs

The **VLAN Interfaces** section shows the new VLAN.



VLAN Interfaces

Name	Physical Interface	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	1 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.

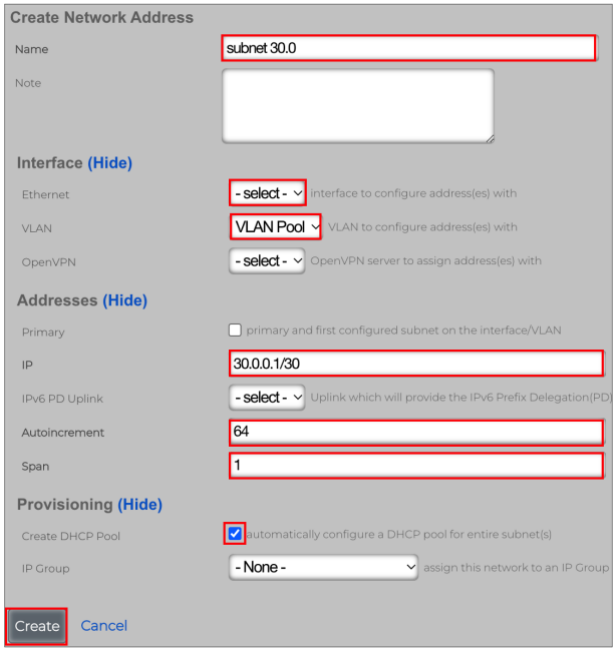


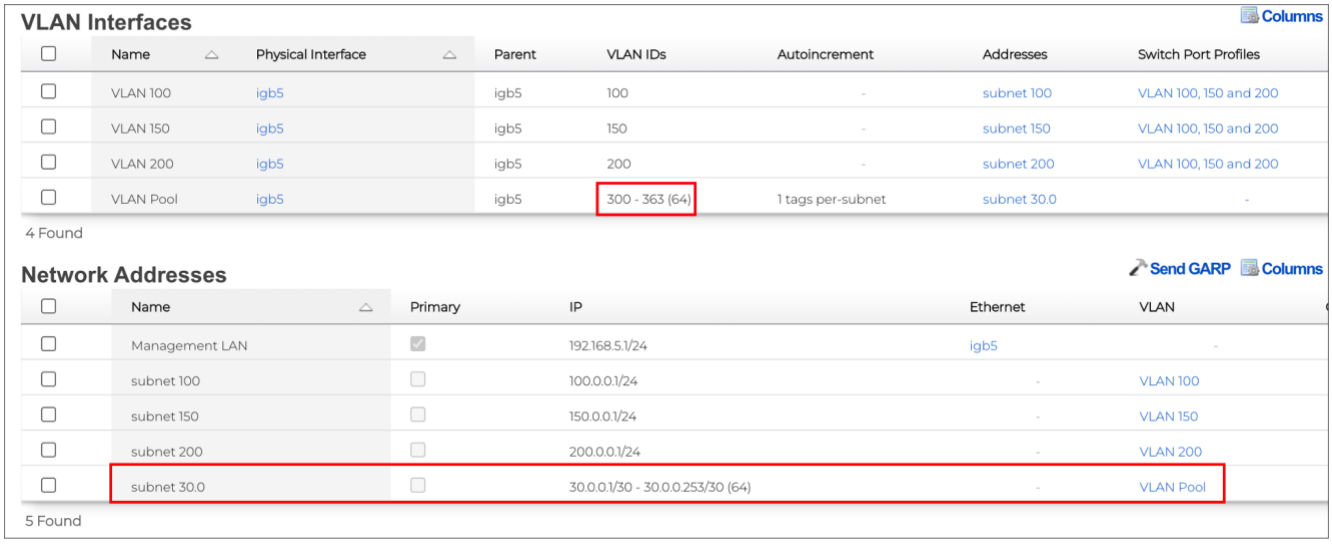
FIGURE 34 – CREATE NETWORK ADDRESS

- Click **Create** to finish.

© 2023 CommScope Inc. All rights reserved.

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 Interfaces

Name	Physical Interface	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

Network Addresses

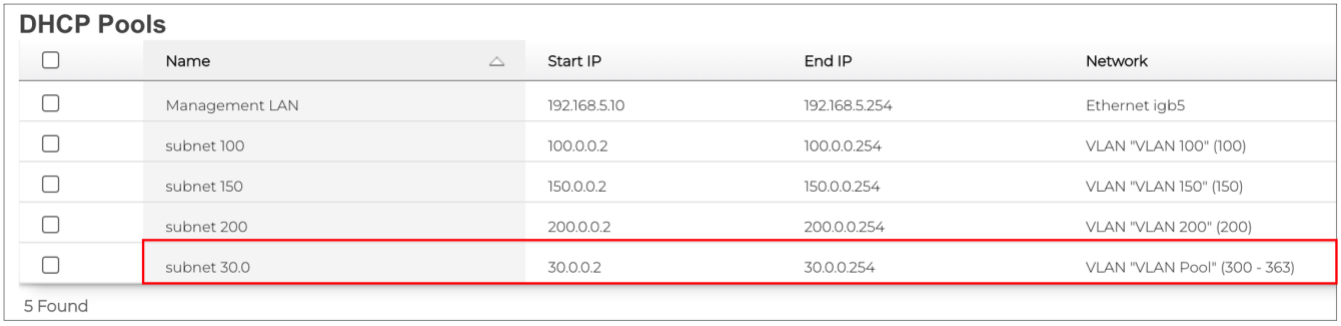
Name	Primary	IP	Ethernet	VLAN
Management LAN	☑	192.168.5.1/24	igb5	-
subnet 100	☐	100.0.0.1/24	-	VLAN 100
subnet 150	☐	150.0.0.1/24	-	VLAN 150
subnet 200	☐	200.0.0.1/24	-	VLAN 200
subnet 30.0	☐	30.0.0.1/30 - 30.0.0.253/30 (64)	-	VLAN Pool

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 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	100.0.0.254	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)
subnet 30.0	30.0.0.2	30.0.0.254	VLAN "VLAN Pool" (300 - 363)

5 Found

FIGURE 36 – DHCP POOL FOR SUBNET 30.0

© 2023 CommScope Inc. All rights reserved.

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.

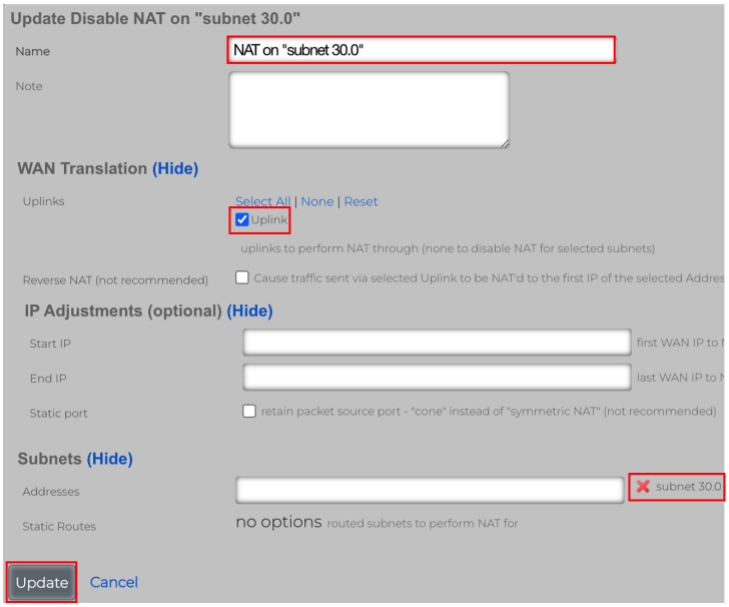
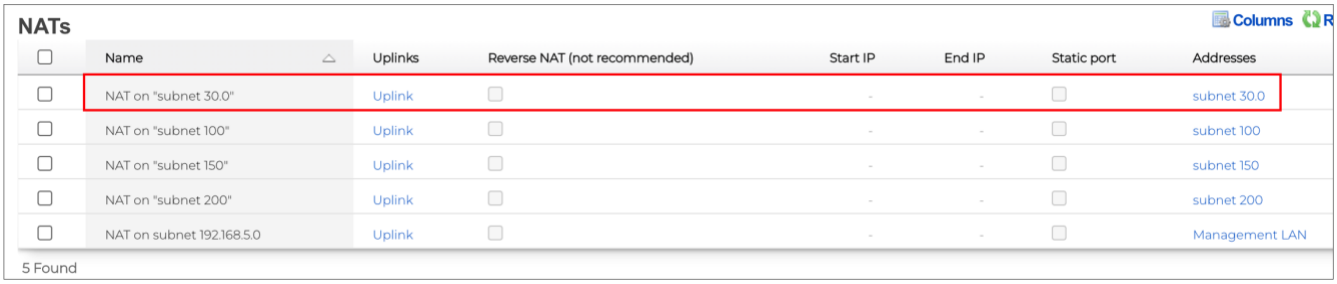


FIGURE 37 – ENABLE NAT FOR SUBNET 30.0

Click **Update** to finish.

Step 3a – Check the NAT Configuration

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



NATs

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.

© 2023 CommScope Inc. All rights reserved.

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 pre-configured 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.

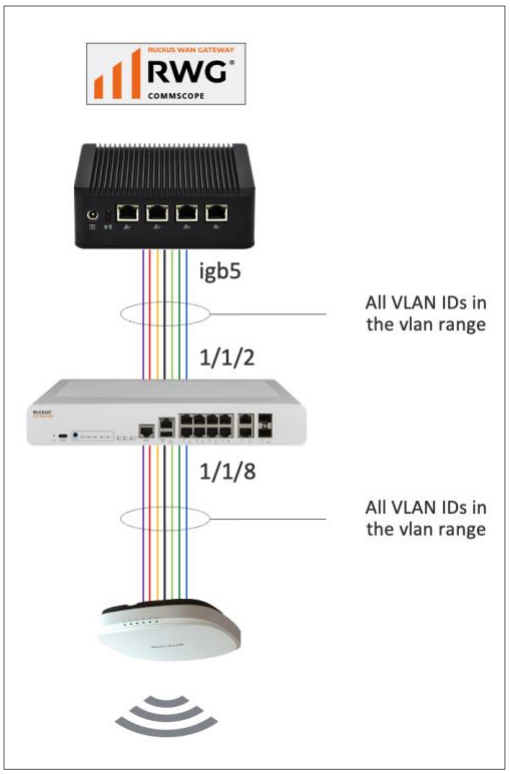


FIGURE 39 – VLANS WITH TAGGED INTERFACES IN THE ICX SWITCH

© 2023 CommScope Inc. All rights reserved.

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**

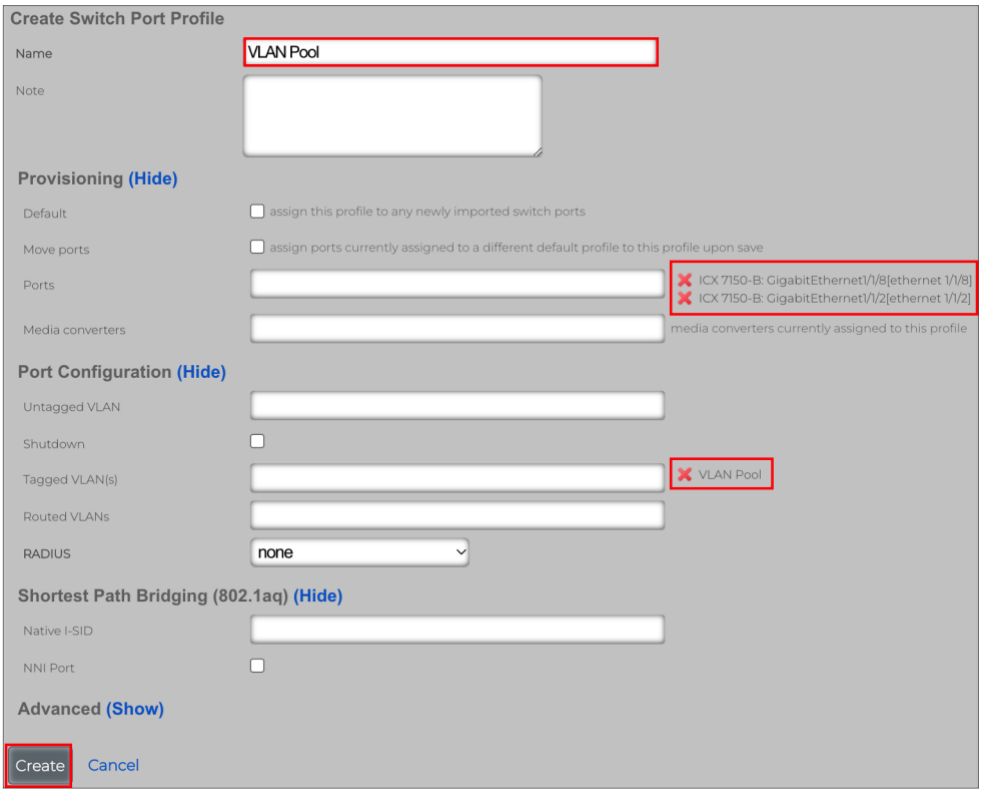


FIGURE 40 – CREATE SWITCH PORT PROFILE

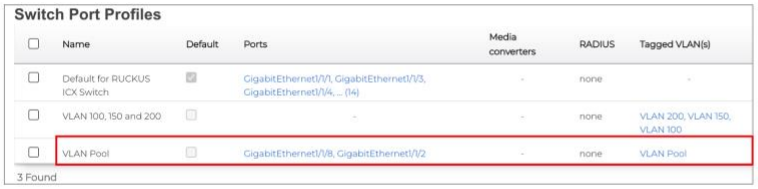
Click **Create** to finish.

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.

© 2023 CommScope Inc. All rights reserved.

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**.




```
SSH@ICX 7150-B#sh ru vlan
vlan 1 name DEFAULT-VLAN by port
!
vlan 300 by port
 tagged ethe 1/1/2 ethe 1/1/8
!
vlan 301 by port
 tagged ethe 1/1/2 ethe 1/1/8
!
vlan 302 by port
 tagged ethe 1/1/2 ethe 1/1/8
!
vlan 303 by port
 tagged ethe 1/1/2 ethe 1/1/8
!
vlan 304 by port
 tagged ethe 1/1/2 ethe 1/1/8
!
vlan 305 by port
 tagged ethe 1/1/2 ethe 1/1/8
!
vlan 306 by port
 tagged ethe 1/1/2 ethe 1/1/8
```

... etc.

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**

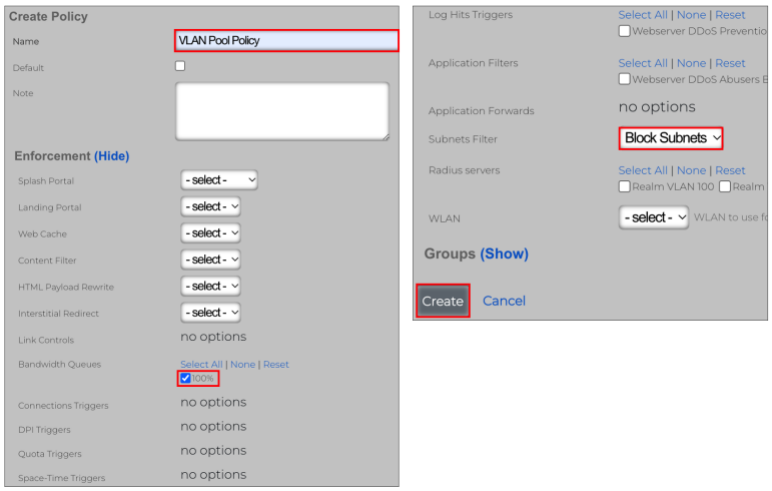


FIGURE 42 – CREATE POLICY

Click **Create** to finish.

© 2023 CommScope Inc. All rights reserved.

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.

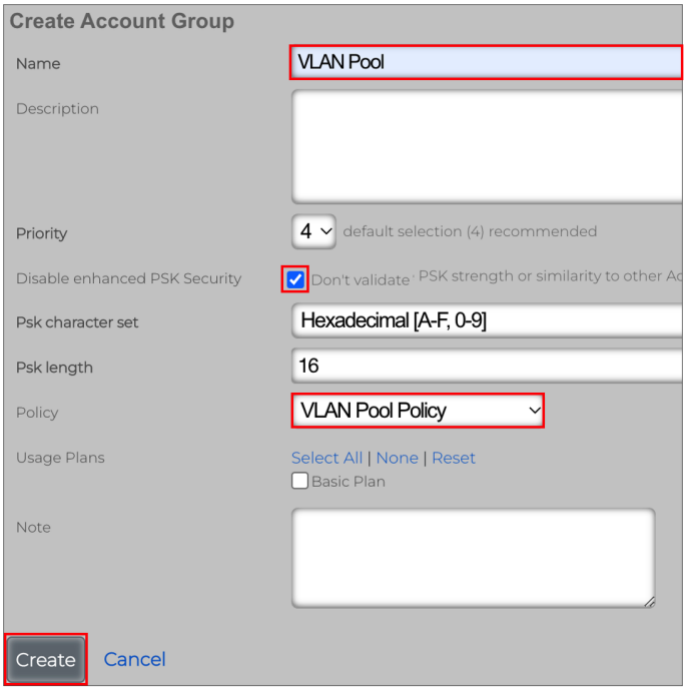


FIGURE 43 – CREATE ACCOUNT GROUP

Click **Create** to finish.

Step 6a – Check the Account Groups

VLAN Pool now shows in the account groups list.

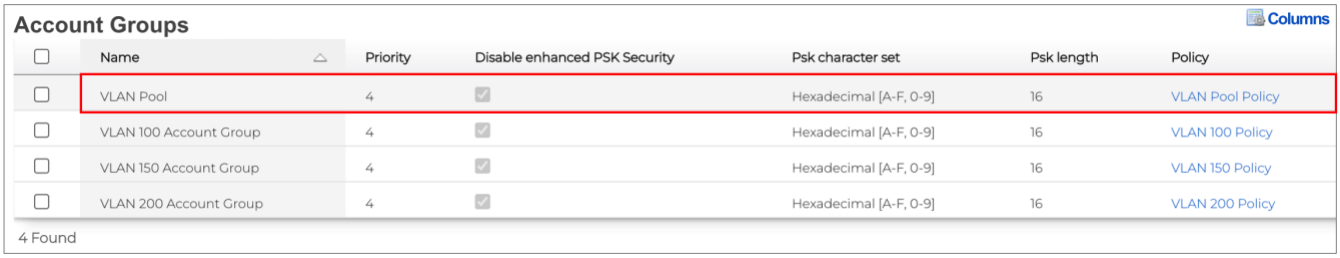


FIGURE 44 – NEW ACCOUNT GROUP

© 2023 CommScope Inc. All rights reserved.

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

© 2023 CommScope Inc. All rights reserved.

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.

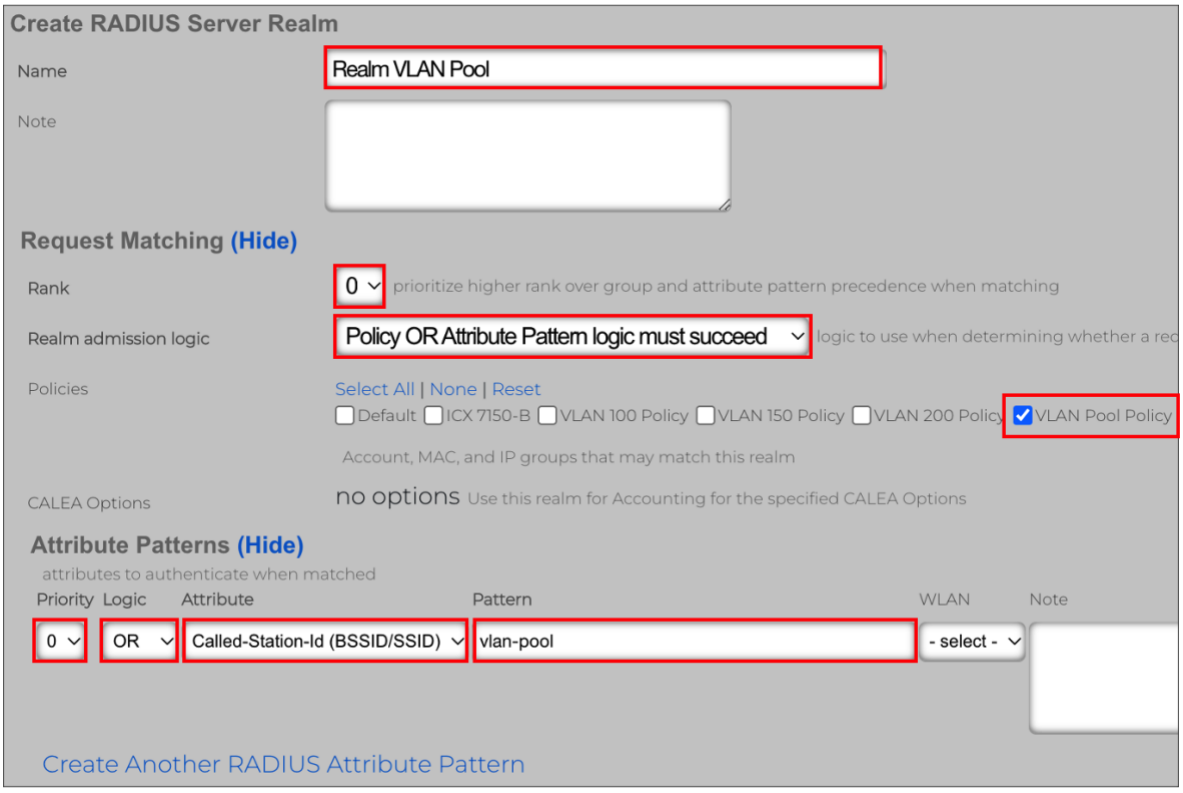


FIGURE 46 – CREATE RADIUS SERVER REALM

Scroll down to continue.

© 2023 CommScope Inc. All rights reserved.

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%

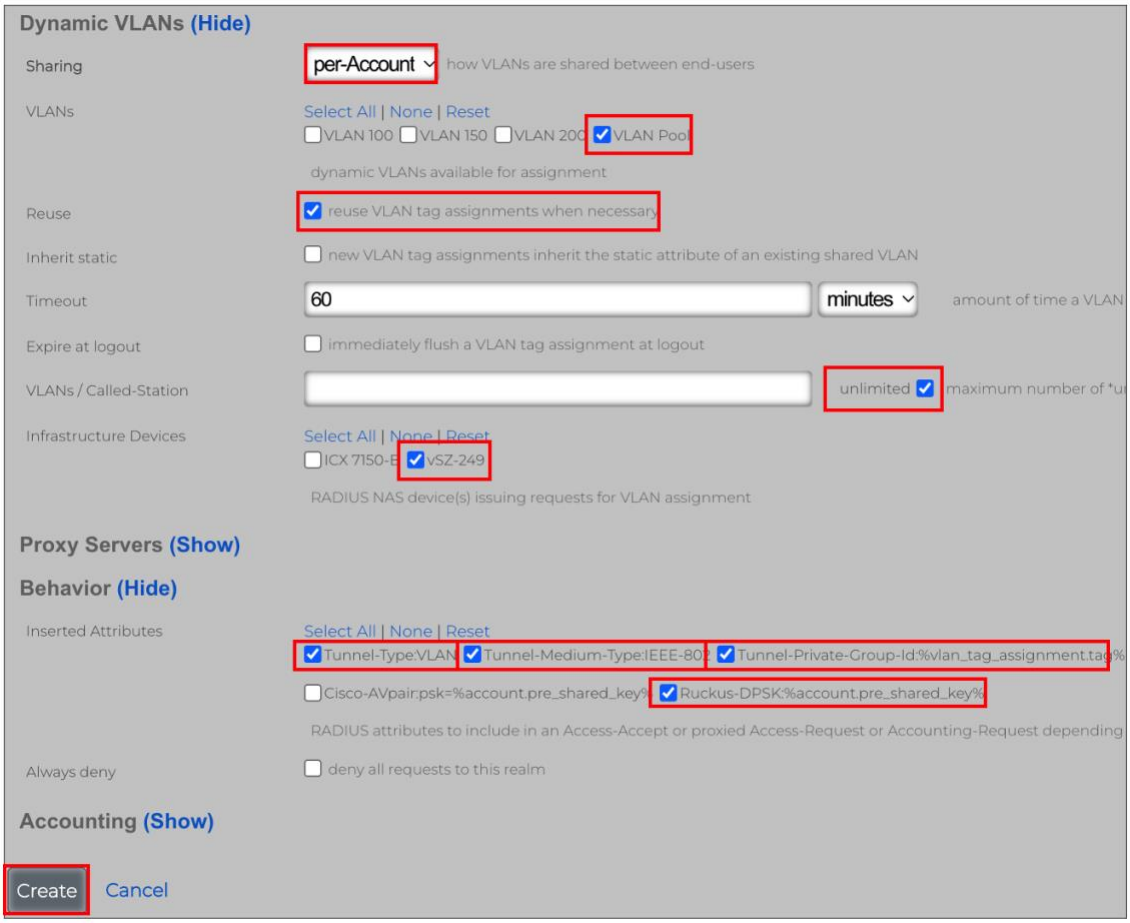


FIGURE 47 – CREATE RADIUS SERVER REALM (CONT'D)

Click **Create** to finish.

© 2023 CommScope Inc. All rights reserved.

Step 7a – Check the New RADIUS Realms

The section **RADIUS Server Realms** shows the new realm.

RADIUS Server 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 Found

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.

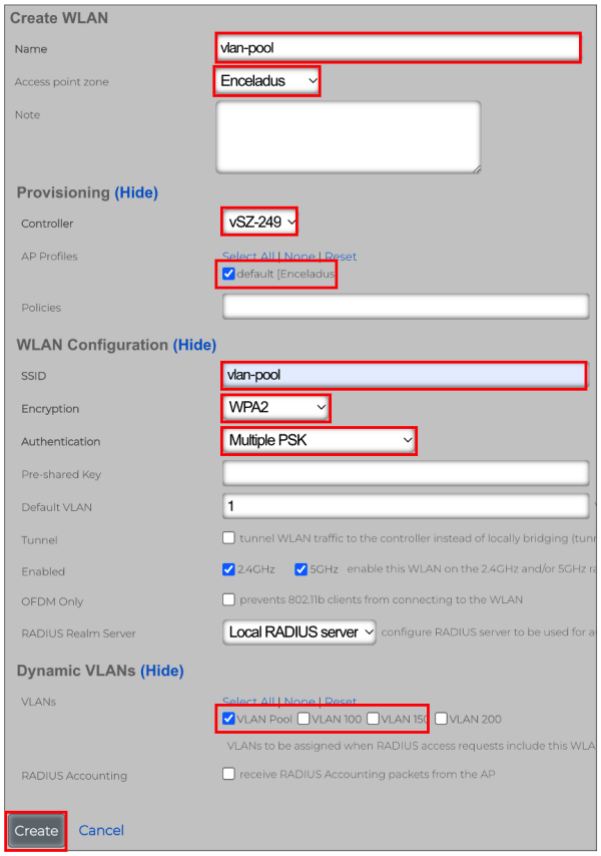


FIGURE 49 – CREATE WLAN

© 2023 CommScope Inc. All rights reserved.

Step 8a – Check the New WLAN

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

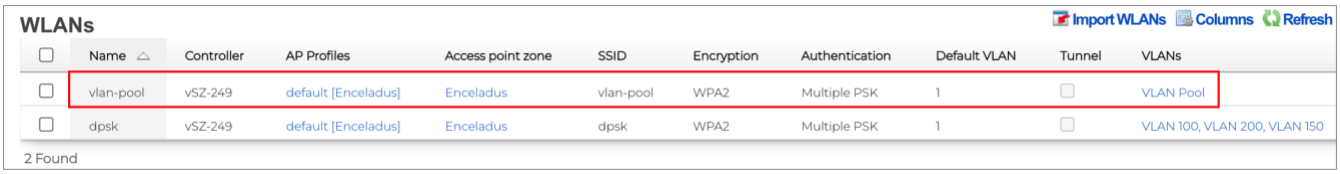


FIGURE 50 – WLAN VLAN-POOL IS CREATED

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.

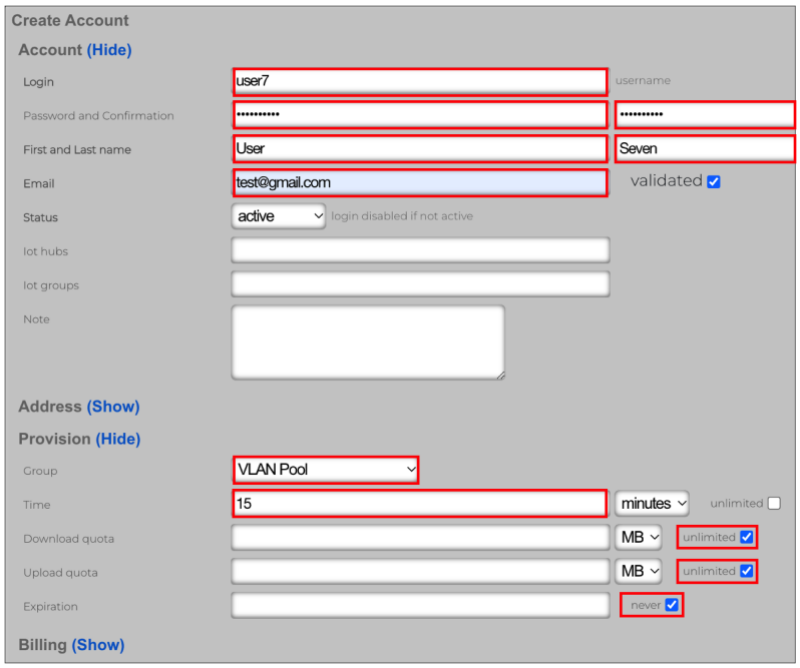


FIGURE 52– CREATE ACCOUNT

© 2023 CommScope Inc. All rights reserved.

Enter the following information:

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

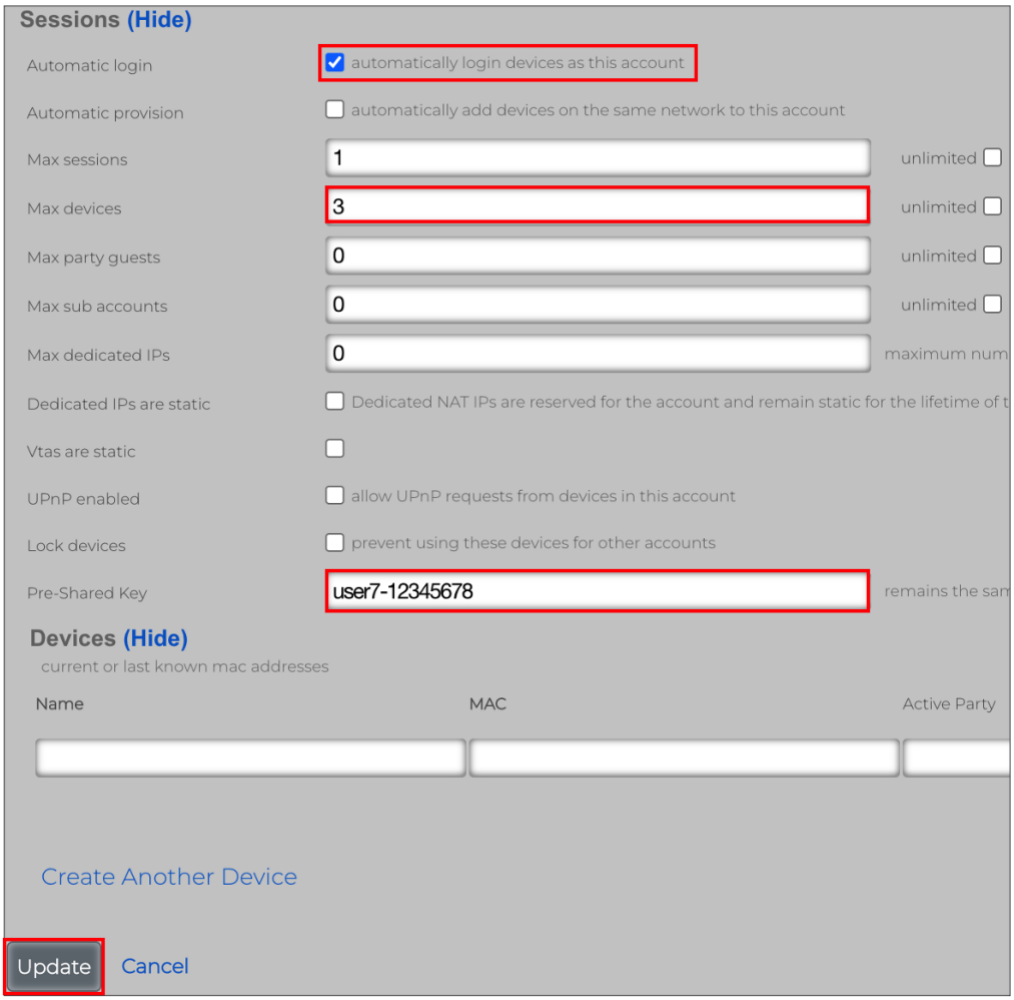


FIGURE 53 – CREATE ACCOUNT (CONT'D)

Click **Create** to finish.

Repeat the process to create the other account.

© 2023 CommScope Inc. All rights reserved.

Step 9a – Check the New Accounts

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

Accounts

Login	Group	Time	Quota	Expiration	Plan	Balance	Bill	Devices
user8	VLAN Pool	15 minutes	unlimited	never	-	$0.00	-	-
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 **30.0.0.13 – 30.0.0.14**

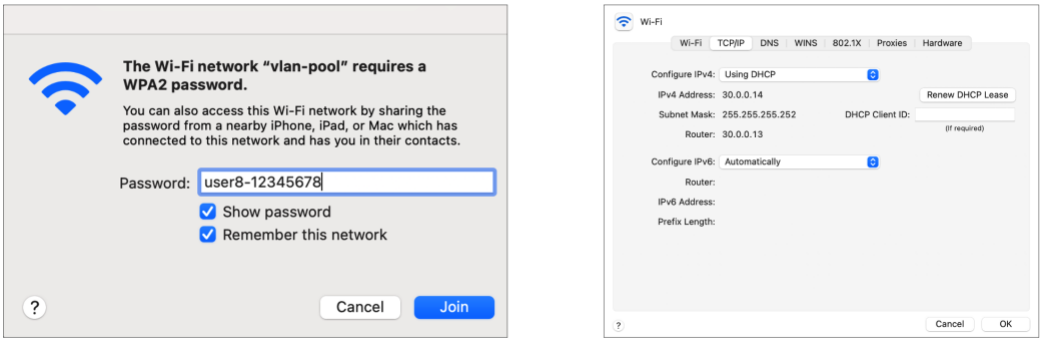


FIGURE 55 – TEST USING A MACBOOK USING USER8

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

FIGURE 56 – USER7 AND USER8 ARE CONNECTED

© 2023 CommScope Inc. All rights reserved.

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

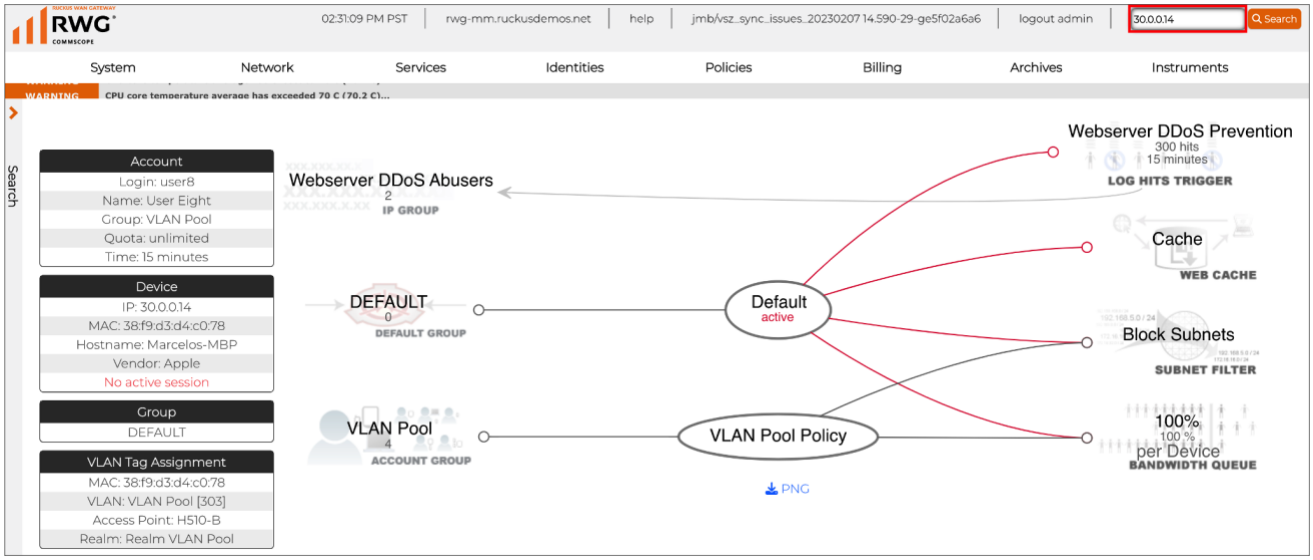


FIGURE 57 – SEARCHING A DEVICE

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** ②in the device entry. Do not click **Delete** at the top right, otherwise you will delete the entire account.

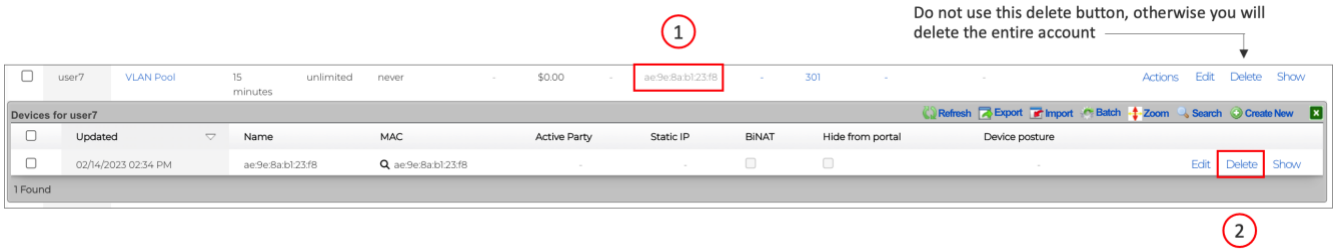


FIGURE 58 – DELETE A DEVICE

© 2023 CommScope Inc. All rights reserved.

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.

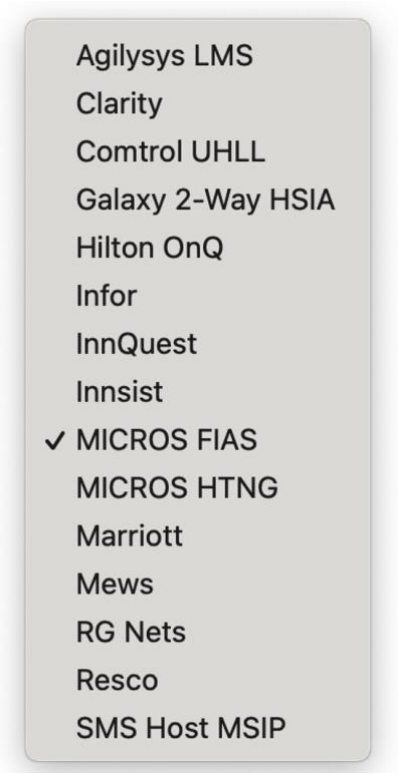


FIGURE 59 – SUPPORTED PMS PLATFORMS

© 2023 CommScope Inc. All rights reserved.

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.

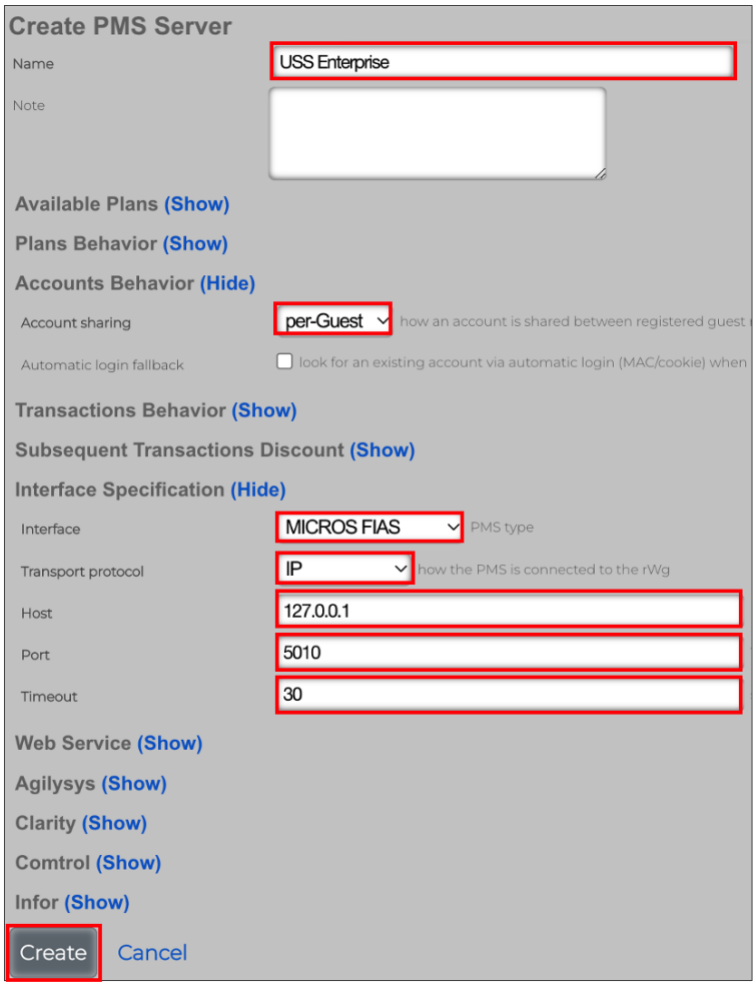


FIGURE 60 – CREATE PMS SERVER

Click **Create** to finish.

© 2023 CommScope Inc. All rights reserved.

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.

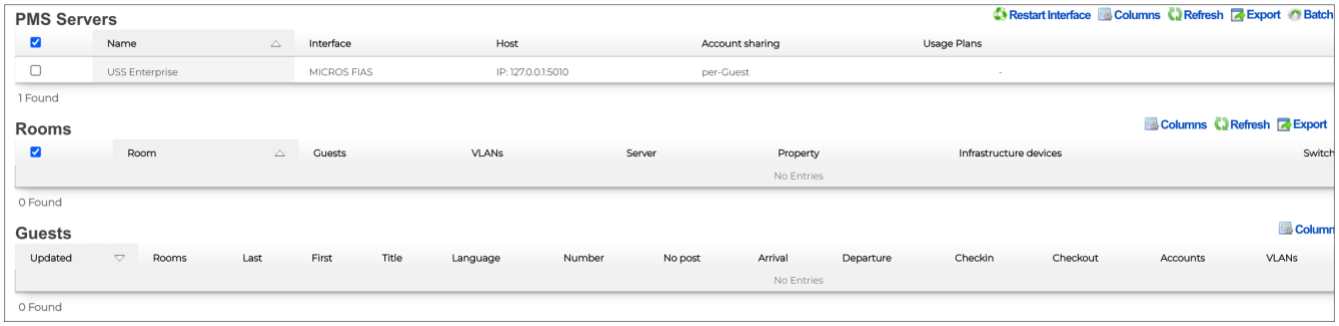


FIGURE 61 – NEW PMS SERVER

Step 2 – Activate the RWG FIAS Server

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

```
[marcelo@rwg-home ~]$ iui

ANNMTSGHDQVIAXMLXPJBDCFF
HCPTFFGWQCPOGGMWZFSGOJUS

4 3000 8192 214 ANNMTSGHDQVIAXMLXPJBDCFF HCPTFFGWQCPOGGMWZFSGOJUS
```

this is the su password

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

© 2023 CommScope Inc. All rights reserved.

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 &
```

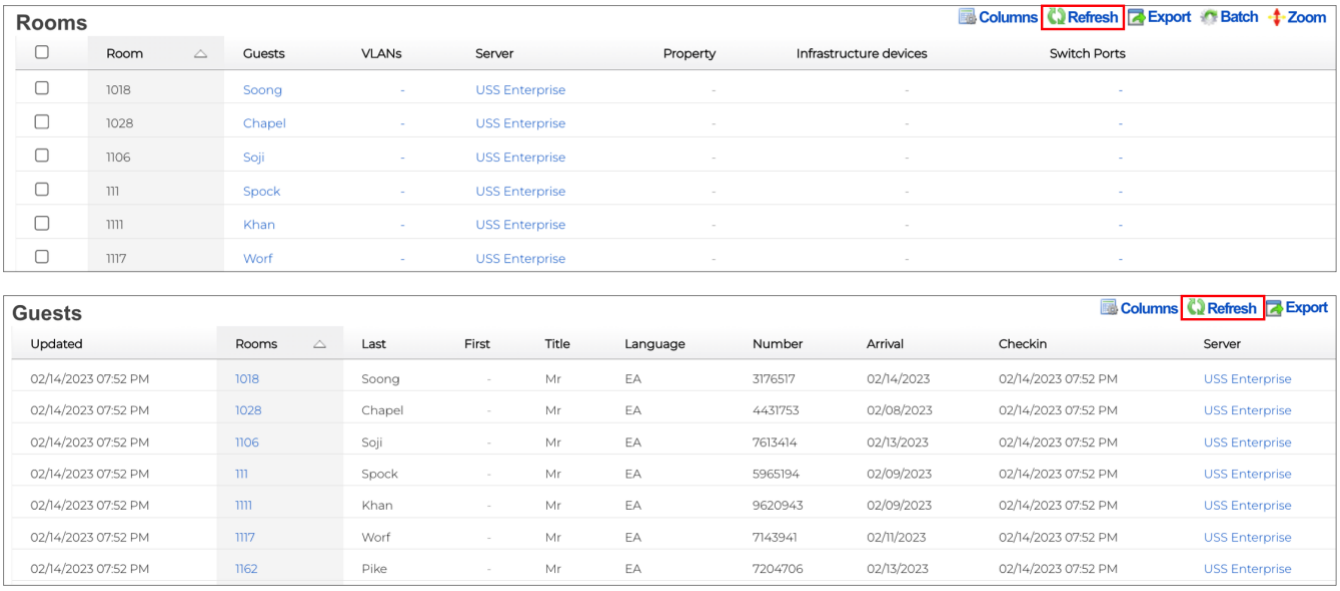
The first line opens the file named **rc.local.hook**, next you add three lines, and the **CTRL-D** writes the file and closes it. After that, enter the following command to make the file executable:

```
[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

Columns | Refresh | Export

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	111	Spock	-	Mr	EA	5965194	02/09/2023	02/14/2023 07:52 PM	USS Enterprise
02/14/2023 07:52 PM	1111	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

© 2023 CommScope Inc. All rights reserved.

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.

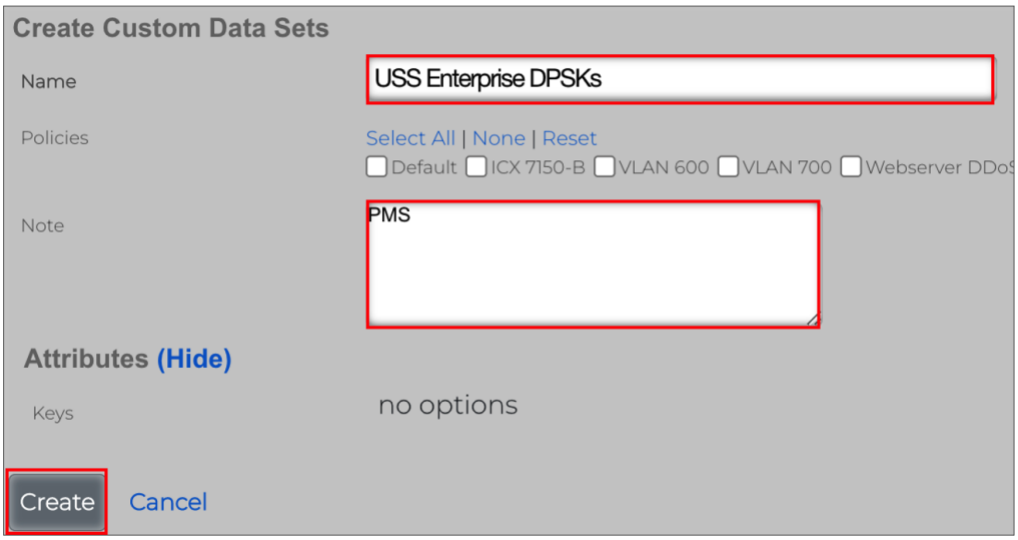


FIGURE 65 – CREATE CUSTOM DATA SETS

Click **Create** to finish.

© 2023 CommScope Inc. All rights reserved.

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.

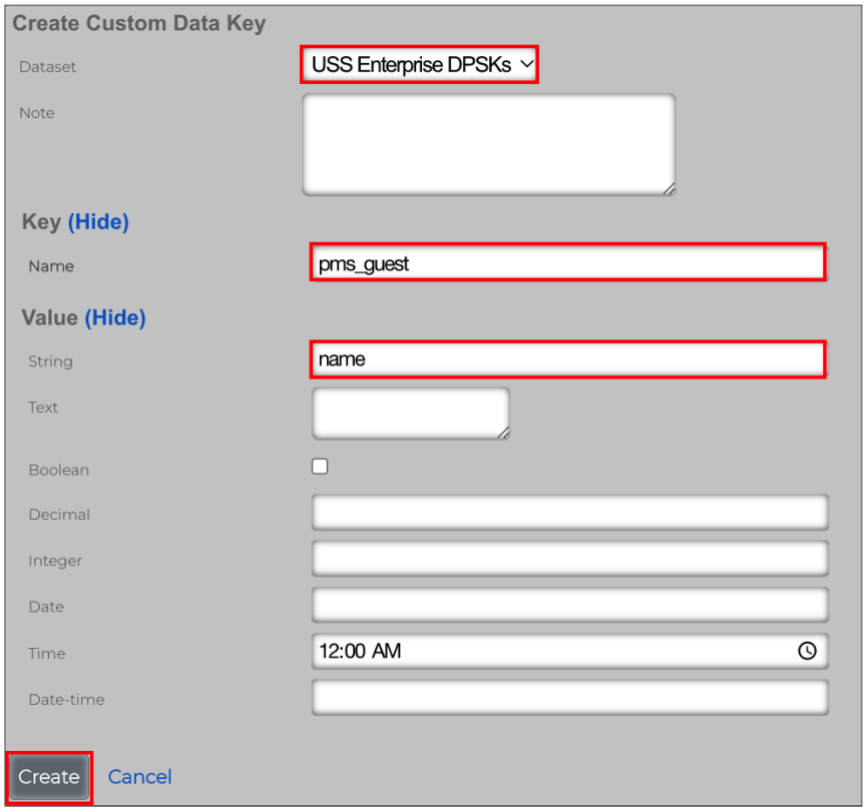


FIGURE 66 – CREATE FIRST CUSTOM DATA KEY

Click **Create** to finish.

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

© 2023 CommScope Inc. All rights reserved.

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.

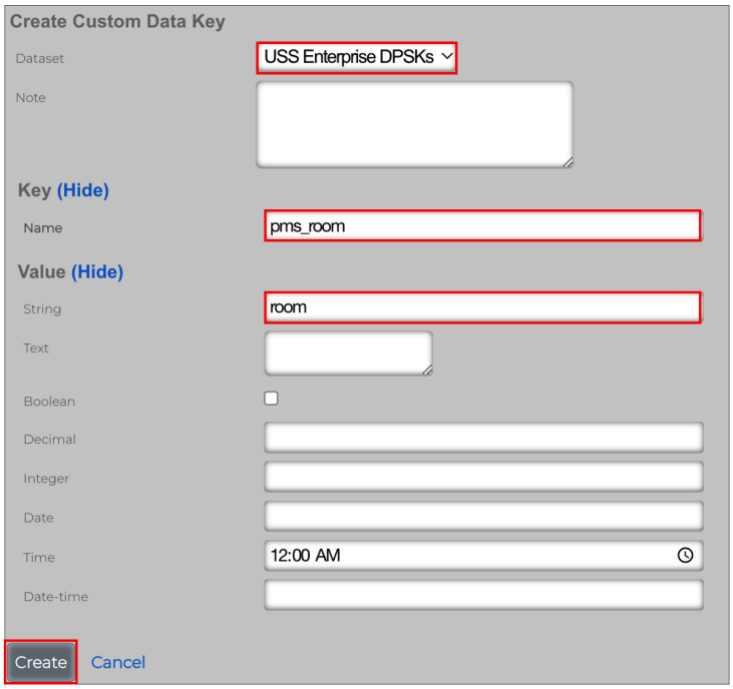
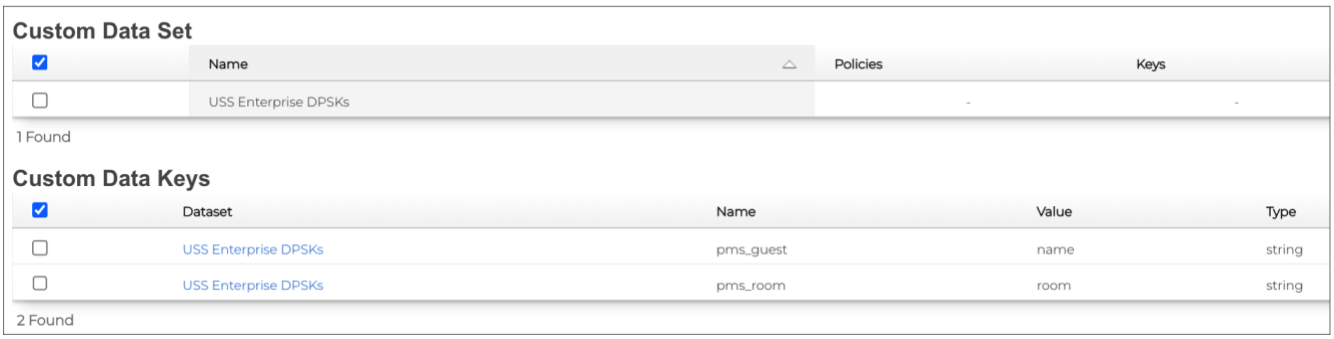


FIGURE 67 – CREATE SECOND CUSTOM DATA KEY

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	Policies	Keys
☐	USS Enterprise DPSKs	-	-

1 Found

Custom Data Keys

	Dataset	Name	Value	Type
☐	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

© 2023 CommScope Inc. All rights reserved.

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

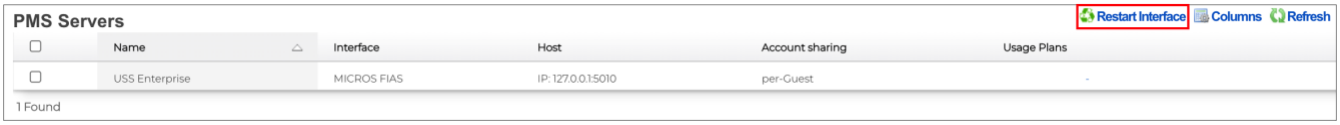


FIGURE 69 – RESTARTING THE PMS INTERFACE

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.

```
[2] pry(main)> PairwiseMasterKey.all

#<PairwiseMasterKey:0x000000080b805c88
 id: 1048577,
 ssid: "vlan-pool",
 psk: "111Spock",
 account_id: nil,
 pms_room_id: 1,
 pms_guest_id: 1,
 wlan_id: 486,
 created_by: "pmsdemuxd",
 updated_by: "pmsdemuxd",
 created_at: Tue, 14 Feb 2023 21:04:13.927410000 PST -08:00,
 updated_at: Tue, 14 Feb 2023 21:04:13.927410000 PST -08:00,
 pmk: "uTTubCO2DyVZwqzwGFOlWDe+xyIR1NnE8gqdfTU7jfg=">,
#<PairwiseMasterKey:0x000000080b805bc0
 id: 1048578,
 ssid: "vlan-pool",
 psk: "Spock 111",
 account_id: nil,
 pms_room_id: 1,
 pms_guest_id: 1,
 wlan_id: 486,
 created_by: "pmsdemuxd",
 updated_by: "pmsdemuxd",
 created_at: Tue, 14 Feb 2023 21:04:13.945530000 PST -08:00,
 updated_at: Tue, 14 Feb 2023 21:04:13.945530000 PST -08:00,
 pmk: "acaqN1aIRTg/OWyE+yQquWtoubsosbCZdWFa+mG5Kw4=">,
```

```
#<PairwiseMasterKey:0x000000080b805af8
 id: 1048579,
 ssid: "vlan-pool",
 psk: "111 Spock",
 account_id: nil,
 pms_room_id: 1,
 pms_guest_id: 1,
 wlan_id: 486,
 created_by: "pmsdemuxd",
 updated_by: "pmsdemuxd",
 created_at: Tue, 14 Feb 2023 21:04:13.963360000 PST -08:00,
 updated_at: Tue, 14 Feb 2023 21:04:13.963360000 PST -08:00,
 pmk: "VdTZTdYqFkTNzcKiY9a4S1OkLjTtszcN3Rdh1aMn3tM=">,
#<PairwiseMasterKey:0x000000080b805a30
 id: 1048580,
 ssid: "vlan-pool",
 psk: "Spock111",
 account_id: nil,
```

FIGURE 72 – LISTING THE DPSKS

© 2023 CommScope Inc. All rights reserved.

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:

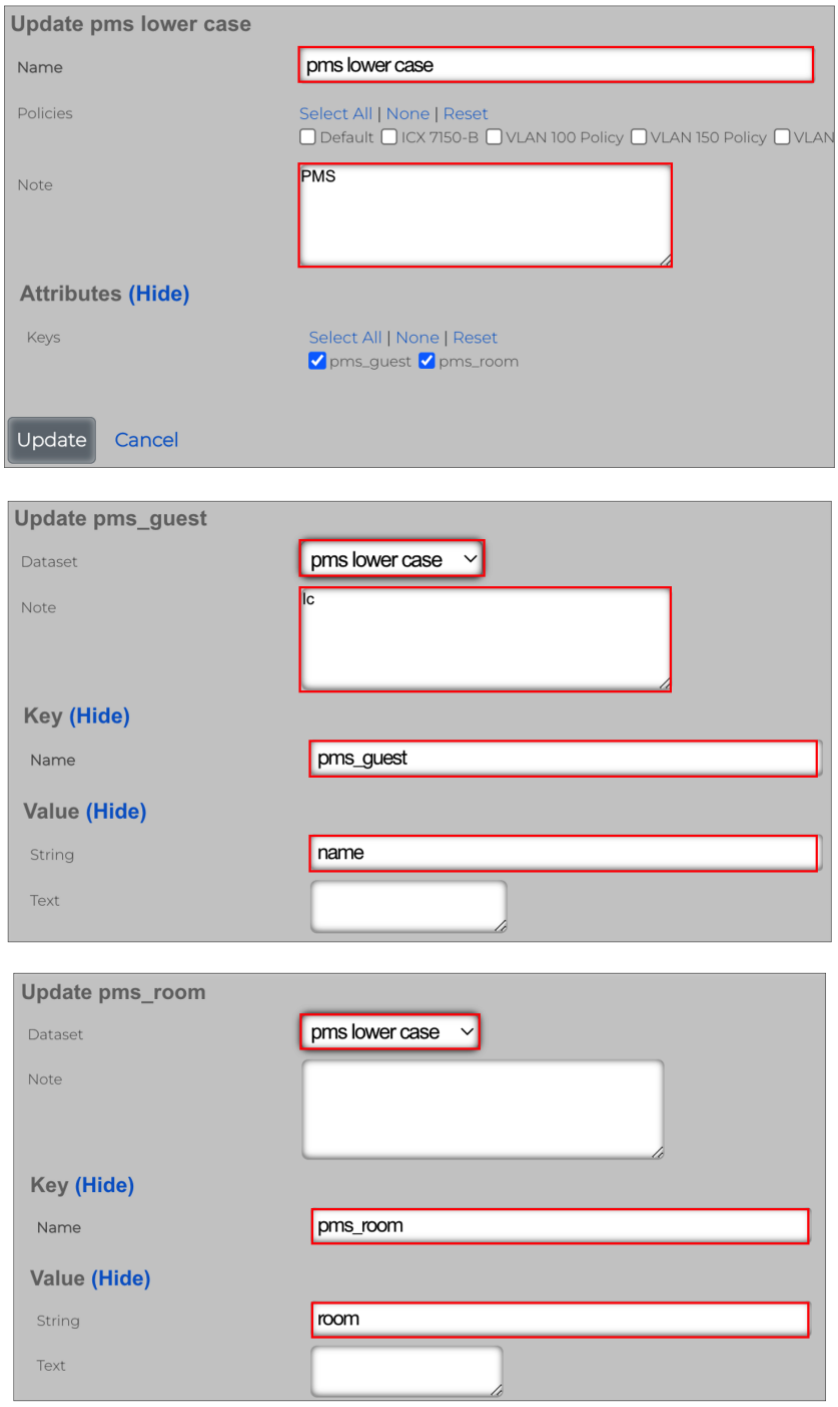


FIGURE 73 – DATA SET AND DATA KEYS TO GENERATE DPSKS WITH LAST NAME IN LOWERCASE

© 2023 CommScope Inc. All rights reserved.

lc 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**.

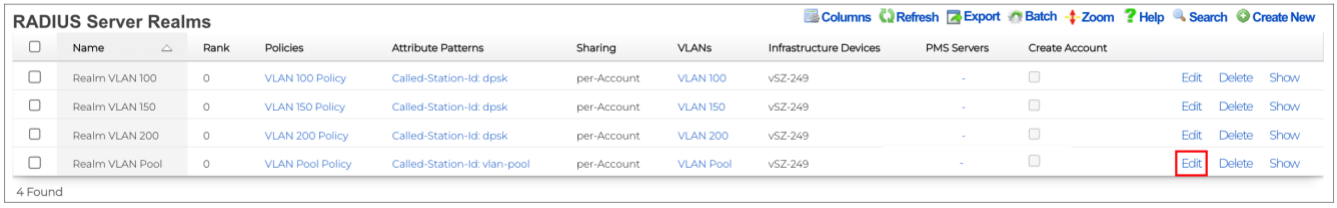


FIGURE 74 – EDITING THE RADIUS REALM

Scroll down, then enter the following information:

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

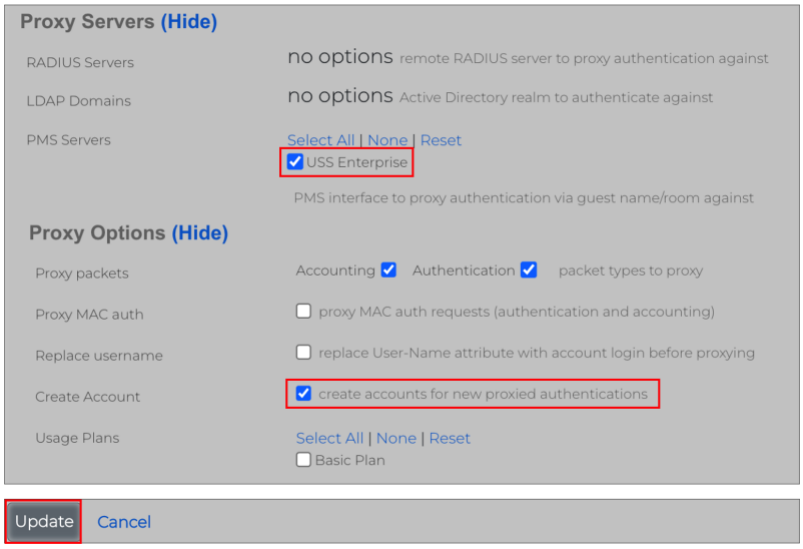


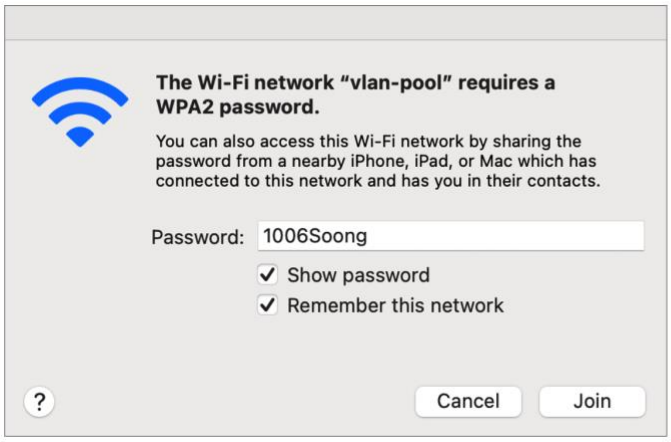
FIGURE 75 – ADDING THE PMS SERVER TO THE REALM

Click **Update** to finish.

© 2023 CommScope Inc. All rights reserved.

Test Results

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




```
#<PairwiseMasterKey:0x0000000812c34a28
 id: 1052403,
 ssid: "vlan-pool",
 psk: "1006Soong",
 account_id: nil,
 pms_room_id: 149,
 pms_guest_id: 156,
 wlan_id: 136,
```

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.

© 2023 CommScope Inc. All rights reserved.

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 ™ or ® 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.

RUCKUS®
COMMSCOPE