Deployment Guide

RUCKUS WAN Gateway – Portals

July 2023

Rev. 0

Table of Contents

Changes

- No changes. This is the initial document version.

Intended Audience

The audience for this document is customers and operators deploying RWG solutions using captive portals. It is expected that the reader already possesses a working knowledge on the RUCKUS WAN Gateway.

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/

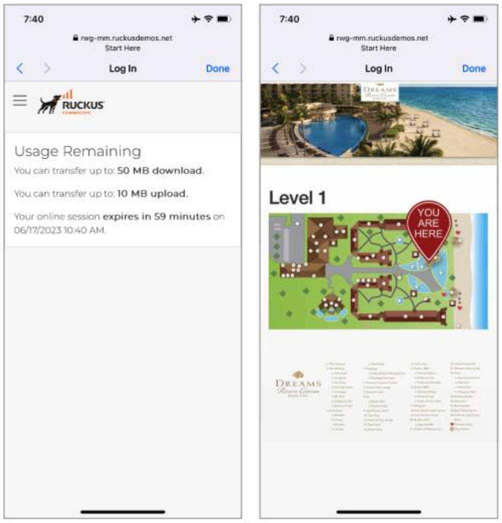
The RWG documentation is embedded into the product.
You can access the embedded documentation at https://{your RWG_IP_address}/admin/manual/help_online

Benefits and Concepts

By using portals and plans, RWG can incorporate lots of features to the user experience:

- Control of upload and download speeds.
- Traffic quota
- Expiration time
- Interstitial redirection
- Location-based services
- Message campaigns

For the network operators, billing is a key component for the business models offered by RWG. RWG enables the operators to generate profit through business models that leverage automation, microtransactions and subscriptions.



Usage Remaining

You can transfer up to: **50 MB download.**

You can transfer up to: **10 MB upload.**

Your online session **expires in 59 minutes** on 06/17/2023 10:40 AM.

Figure 1 – Portal Examples

Portals, Plans and Billing Concepts

Microsegmentation and DPSK are two of the main technologies used by RWG.

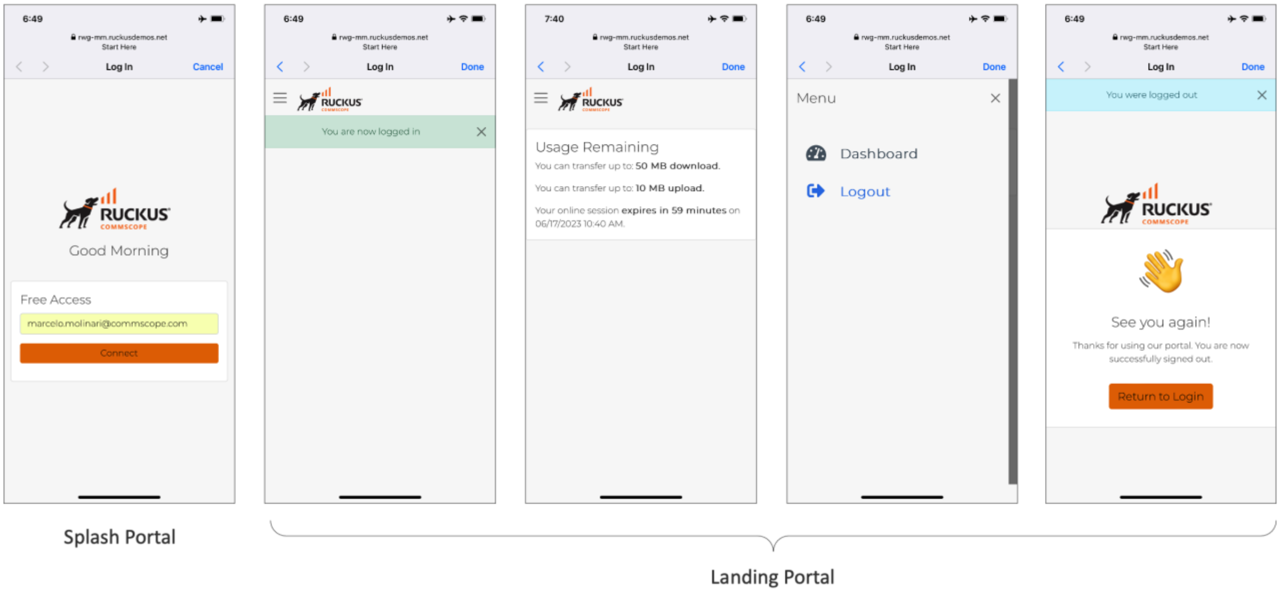
Along with that, portals, plans, and billing are used to identify and control the user experience, defining the traffic quotas, service duration and billing for different verticals and use cases.

Everything starts with a **Captive Portal** (also named **Splash Portals** in RWG). The captive portal is shown to the users right after they connect to the SSID.

By default, the captive portal does not allow access to any network resource, or to the Internet. Instead, the user needs to be authenticated first by entering his email, credentials, or other personal data.

He may also be presented options to select plans with different speeds, traffic quotas, or expiration times. Some of those plans might be free, and others might be charged. The user may need provide to provide a credit card number or other method for payment.

After authentication, the client is directed to a **Landing Portal**.



You are now logged in

Usage Remaining

You can transfer up to: **50 MB download.**

You can transfer up to: **10 MB upload.**

Your online session **expires in 59 minutes** on 06/17/2023 10:40 AM.

You were logged out

See you again!

Thanks for using our portal. You are now successfully signed out.

FIGURE 2 – USER EXPERIENCE USING FREE SERVICES

Detailed Traffic Flow

RWG is inline with the traffic. When a HTTP request comes for a policy that includes a splash portal, RWG forces a browser redirection to the captive portal. After the user logs in, it gets to the landing page.

To implement free services, the operator needs to create a shared credential for user login. This document will show the details later.

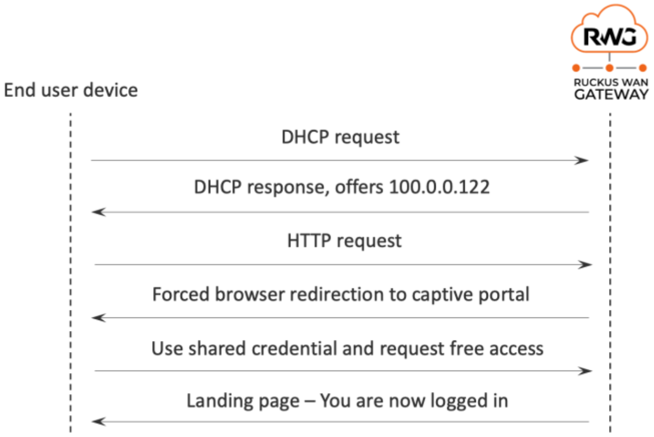
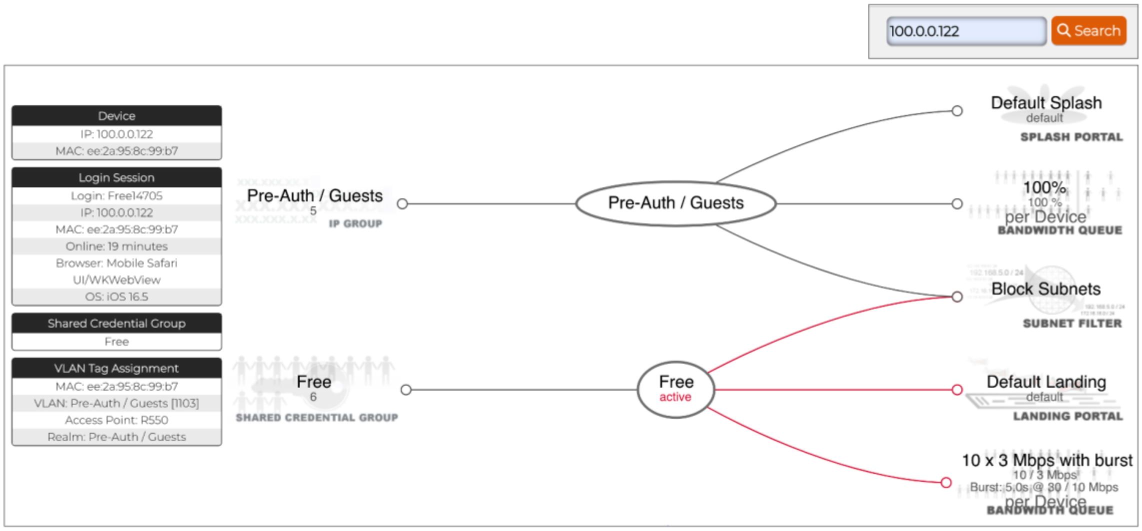

End user device
RWG
RUCKUS WAN GATEWAY
DHCP request
DHCP response, offers 100.0.0.122
HTTP request
Forced browser redirection to captive portal
Use shared credential and request free access
Landing page – You are now logged in

FIGURE 3 – TRAFFIC FLOW USING PORTALS

The Operator View – Policies with Portals

Use the **Search** button at the top right corner to get the session details. Device **100.0.0.122** started at the **Pre-Auth/Guests** IP group and got redirected to the **Default Splash** portal. After login, the device moved to the **Free** shared credential group and got redirected to the **Default Landing** portal.



Device
IP: 100.0.0.122
MAC: ee:2a:95:8c:99:b7

Login Session
Login: Free14705
IP: 100.0.0.122
MAC: ee:2a:95:8c:99:b7
Online: 19 minutes
Browser: Mobile Safari UI/WKWebView
OS: iOS 16.5

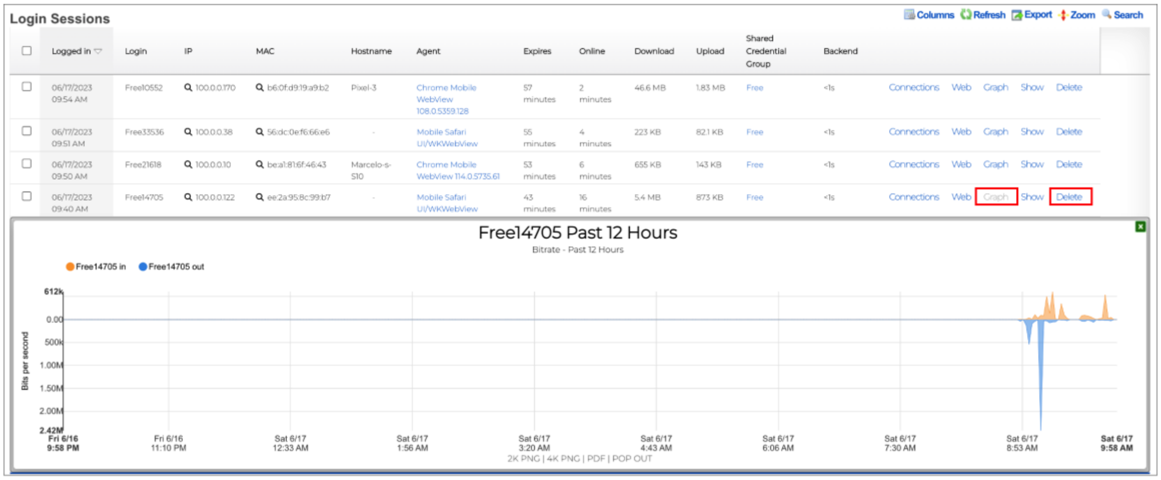
Shared Credential Group
Free

VLAN Tag Assignment
MAC: ee:2a:95:8c:99:b7
VLAN: Pre-Auth / Guests [1103]
Access Point: R550
Realm: Pre-Auth / Guests

Figure 4 – Policies with Portals

The Operator View – Login Sessions

A **Login Session** is created when the client is authenticated via the captive portal. The operator can see the current sessions at **Instruments/Device Sessions**. Click on **Graph** to plot the upload and download traffic. Click on **Delete** to terminate the device sessions.



Login Sessions

□	Logged in	Login	IP	MAC	Hostname	Agent	Expires	Online	Download	Upload	Shared Credential Group	Backend					
□	06/17/2023 09:54 AM	Free10552	100.0.0.170	b6:0f:d9:19:a9:b2	Pixel-3	Chrome Mobile WebView 108.0.5359.128	57 minutes	2 minutes	46.6 MB	1.83 MB	Free	<1s	Connections	Web	Graph	Show	Delete
□	06/17/2023 09:51 AM	Free33536	100.0.0.38	56:dc:0e:f6:66:e6	-	Mobile Safari UI/WKWebView	55 minutes	4 minutes	223 KB	82.1 KB	Free	<1s	Connections	Web	Graph	Show	Delete
□	06/17/2023 09:50 AM	Free21618	100.0.0.10	be:a1:81:6f:46:43	Marcelo-s-S10	Chrome Mobile WebView 114.0.5735.61	53 minutes	6 minutes	655 KB	143 KB	Free	<1s	Connections	Web	Graph	Show	Delete
□	06/17/2023 09:40 AM	Free14705	100.0.0.122	ee:2a:95:8c:99:b7	-	Mobile Safari UI/WKWebView	43 minutes	16 minutes	5.4 MB	873 KB	Free	<1s	Connections	Web	Graph	Show	Delete

Figure 5 – Login Sessions

Microsegmentation Setup

We will use a network topology that is like what we employed in **DPSK Using a VLAN Pool**, included in the document **RWG DPSK Step-by-Step Configuration**. Instead of using a WLAN with eDPSK, we will configure a MAC Bypass WLAN, and the users will login with a shared credential.

This topology requires only one RADIUS realm, one policy, one IP group, one VLAN pool and one network address. To save VLAN IDs, the ratio between IP subnets and VLANs will be 8:1.

This section assumes you have a SmartZone controller and an ICX switch already onboarded and in sync with RWG. You can load a config template to setup this topology with just a few clicks, or you can follow the step-by-step configuration in the next sections.

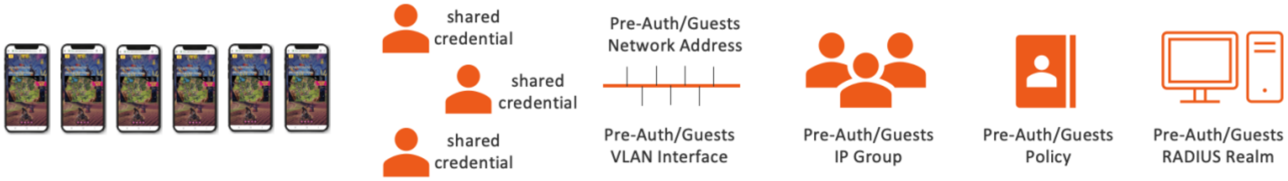


FIGURE 6 – MICROSEGMENTATION USING VLAN POOL

Using the Config Template

Download the config template from the following URL:

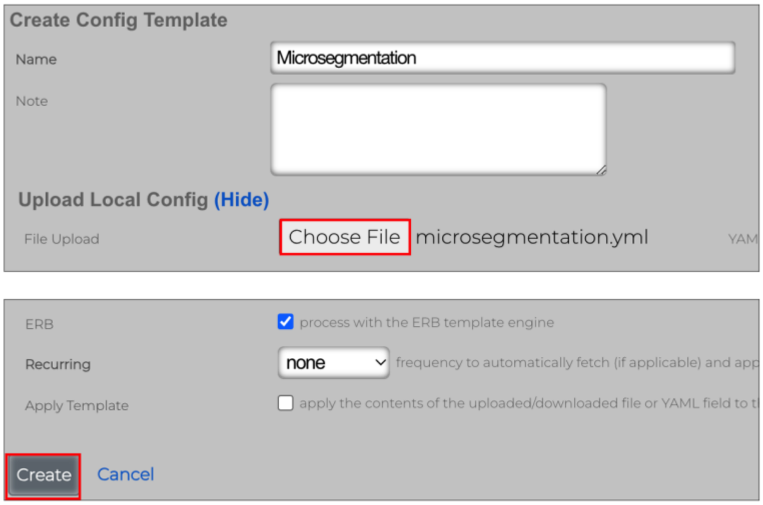
https://github.com/commscope-ruckus/RUCKUS-RWG-Templates/blob/main/microsegmentation.yml

Edit the template to match the following parameters in your environment:

- **interface**: change to match the LAN interface on your RWG.
- **cidr**: make sure the subnet does not conflict with your network.
- **switch_ports**: follow the instructions at the **Troubleshooting** section.
- **infrastructure_device**: change to match your SmartZone name.
- **access_point_zone**: change to match your zone.

Navigate to System/Backup and click Create New in the section Config Templates. Enter the following information:

- **Name**: Enter a name for the template.
- **File Upload**: Select the file with the edited config template.
- Scroll down and click **Create** to finish.



Create Config Template

Name: Microsegmentation

Note:

Upload Local Config (Hide)

File Upload: Choose File microsegmentation.yml YAM

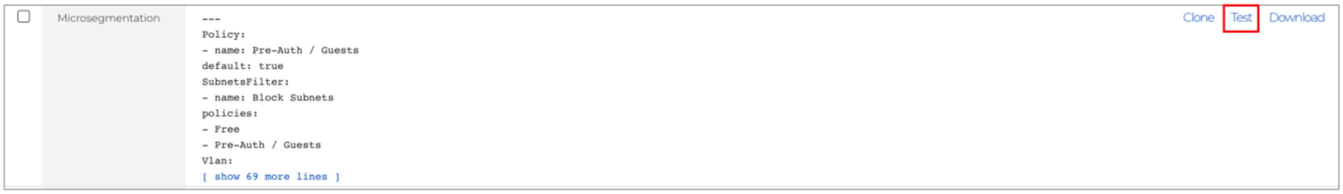
ERB: ☑ process with the ERB template engine

Recurring: none — frequency to automatically fetch (if applicable) and app

Apply Template: □ apply the contents of the uploaded/downloaded file or YAML field to t

FIGURE 7 – CREATE CONFIG TEMPLATE

Click **Test** to verify the template syntax and conflicts. That will not apply the template to RWG.

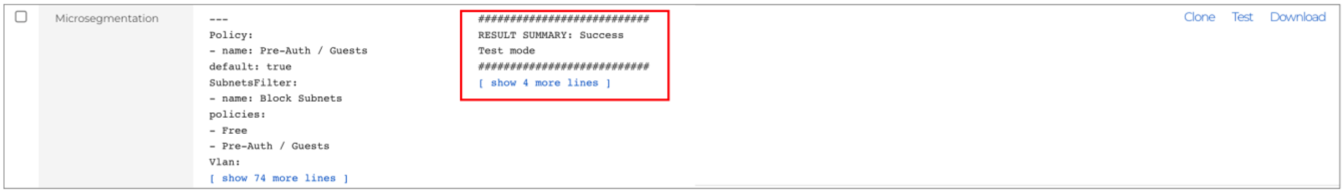


□ Microsegmentation

```
---
Policy:
- name: Pre-Auth / Guests
default: true
SubnetsFilter:
- name: Block Subnets
policies:
- Free
- Pre-Auth / Guests
Vlan:
[ show 69 more lines ]
```

FIGURE 8 – TEST THE CONFIG TEMPLATE

If all is good, the test will succeed. Otherwise, edit the template and fix the error.



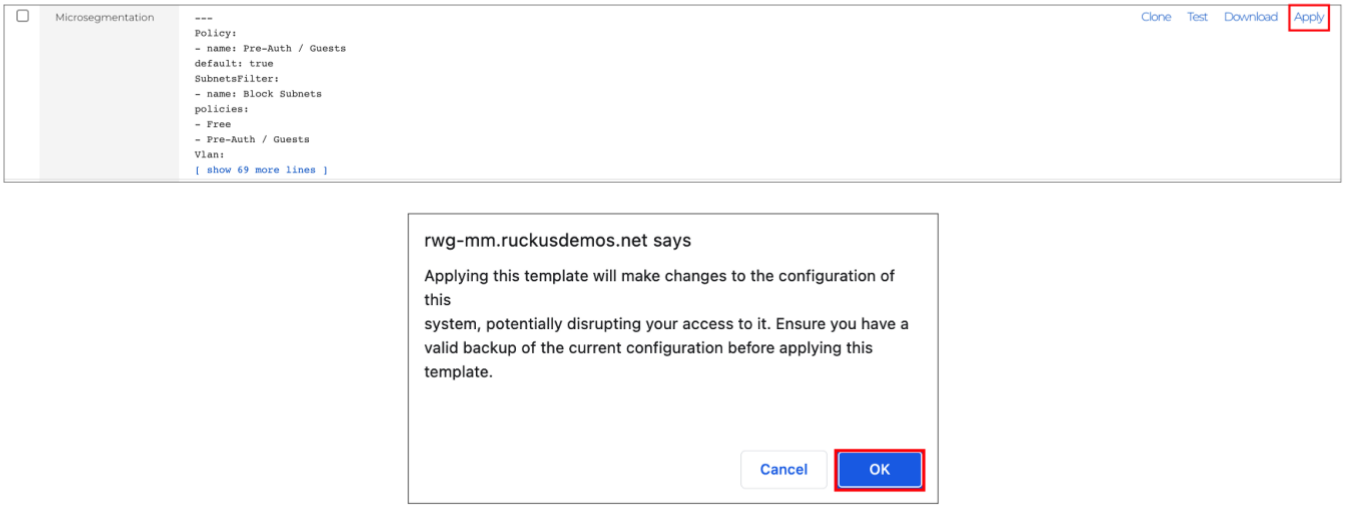
□ Microsegmentation

```
---
Policy:
- name: Pre-Auth / Guests
default: true
SubnetsFilter:
- name: Block Subnets
policies:
- Free
- Pre-Auth / Guests
Vlan:
[ show 74 more lines ]
```

```
###########################
RESULT SUMMARY: Success
Test mode
###########################
[ show 4 more lines ]
```

FIGURE 9 – SUCCESS – TEST MODE

Click **Apply**, then click **OK** in the confirmation window that follows.



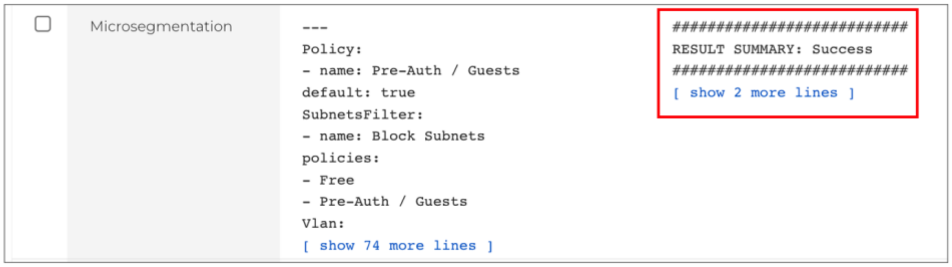
```
---
Policy:
- name: Pre-Auth / Guests
default: true
SubnetsFilter:
- name: Block Subnets
policies:
- Free
- Pre-Auth / Guests
Vlan:
[ show 69 more lines ]
```

rwg-mm.ruckusdemos.net says

Applying this template will make changes to the configuration of this
system, potentially disrupting your access to it. Ensure you have a valid backup of the current configuration before applying this template.

FIGURE 10 – APPLY THE TEMPLATE

If all goes well, you will receive a success message.



```
---
Policy:
- name: Pre-Auth / Guests
default: true
SubnetsFilter:
- name: Block Subnets
policies:
- Free
- Pre-Auth / Guests
Vlan:
[ show 74 more lines ]
```

```
###########################
RESULT SUMMARY: Success
###########################
[ show 2 more lines ]
```

FIGURE 11 – SUCCESS

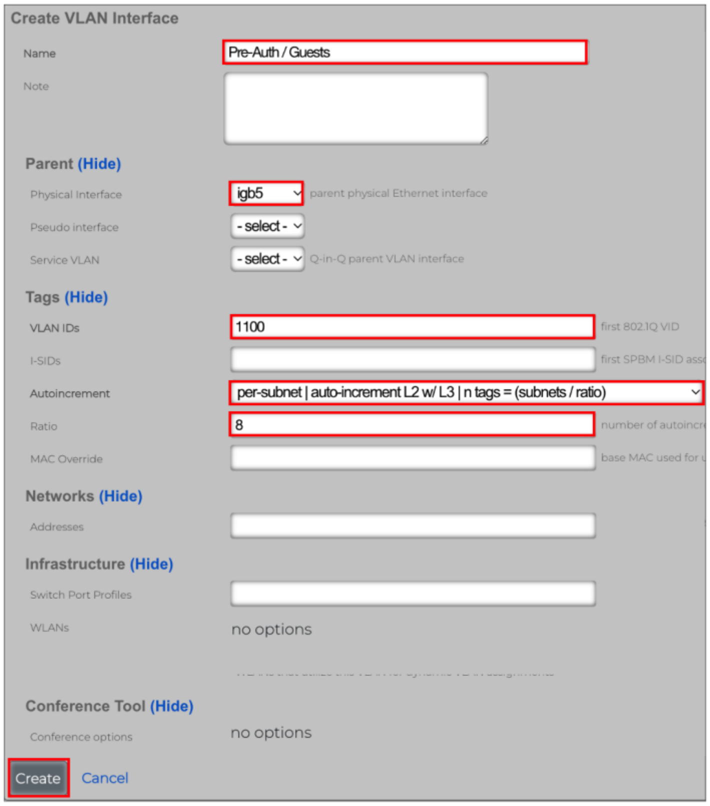
Skip steps 1 to 7 that come next, then test the configuration.

Step 1 - Create the VLAN Pool

Note: Only follow these steps if you did not use the config template.

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 **Pre-Auth/Guests.**
- **Physical Interface**: Select the RWG's physical interface that is connected to the LAN side.
- **VLAN IDs**: Enter **110.**
- **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 **8**.



Create VLAN Interface

Name: Pre-Auth / Guests

Note:

Parent (Hide)

Physical Interface: igb5 — parent physical Ethernet interface

Pseudo interface: - select -

Service VLAN: - select - — Q-in-Q parent VLAN interface

Tags (Hide)

VLAN IDs: 1100 — first 802.1Q VID

I-SIDs: — first SPBM I-SID ass

Autoincrement: per-subnet | auto-increment L2 w/ L3 | n tags = (subnets / ratio)

Ratio: 8 — number of autoincr

MAC Override: — base MAC used for

Networks (Hide)

Addresses:

Infrastructure (Hide)

Switch Port Profiles:

WLANs: no options

Conference Tool (Hide)

Conference options: no options

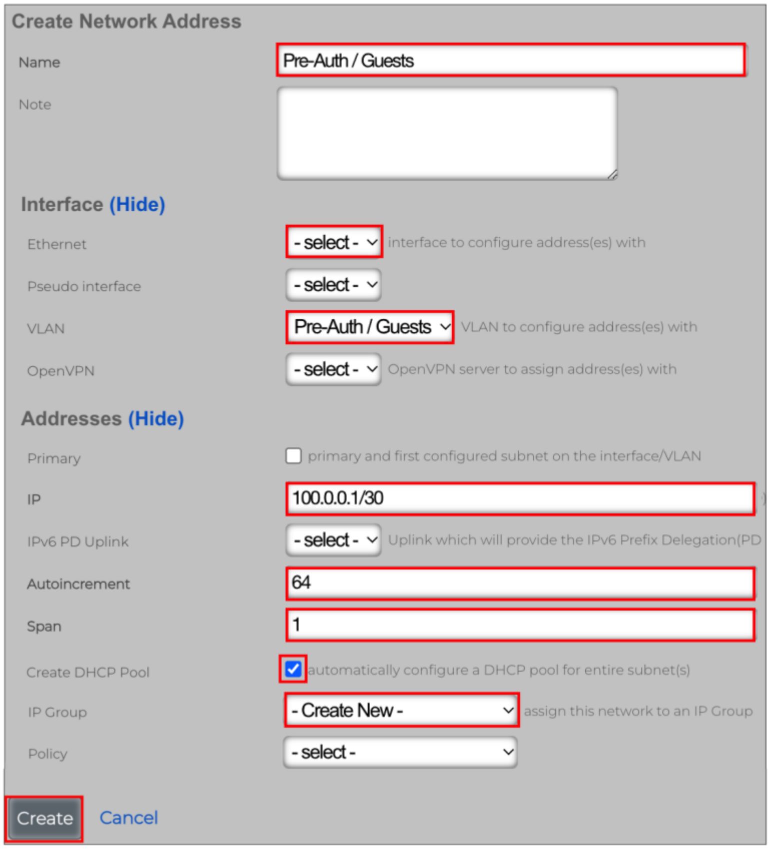
FIGURE 12 – CREATE VLAN INTERFACE

Click **Create** to finish.

Step 2 – Create the Network Address

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

- **Name:** Enter the name for the subnet. Here we used subnet **Pre-Auth/Guests.**
- **Ethernet**: Do not select any physical interface. Select the option **- select -.**
- **VLAN**: Select **Pre-Auth/Guests.**
- **IP**: Enter 100.0.0.1/30.
- **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.
- **IP Group**: Select **- Create New –**



Create Network Address

Name	Pre-Auth / Guests
Note	

Interface (Hide)

Ethernet	- select - interface to configure address(es) with
Pseudo interface	- select -
VLAN	Pre-Auth / Guests 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	100.0.0.1/30
IPv6 PD Uplink	- select - Uplink which will provide the IPv6 Prefix Delegation(PD
Autoincrement	64
Span	1
Create DHCP Pool	☑ automatically configure a DHCP pool for entire subnet(s)
IP Group	- Create New - assign this network to an IP Group
Policy	- select -

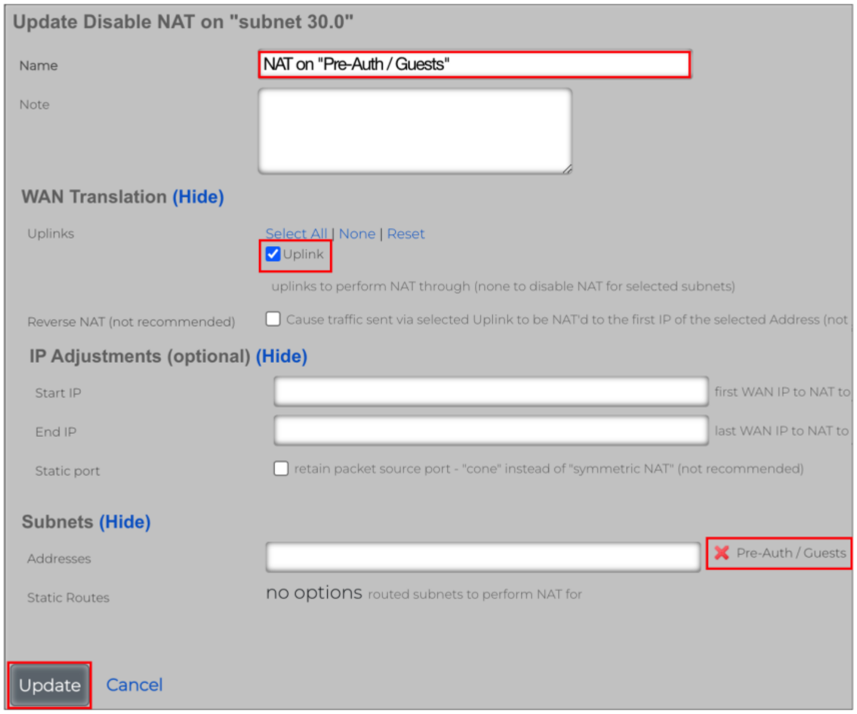
FIGURE 13 – CREATE NETWORK ADDRESS

Click **Create** to finish.

Step 3 – Enable NAT for the New Subnet

Navigate to **Network/NAT** and click **Edit** on the entry for **Pre-Auth/Guests.** Enter the following information:

- **Name**: Change the name to **NAT on "Pre-Auth/Guests".**
- **Uplinks**: Mark the **Uplink** checkbox.
- **Addresses**: Make sure subnet **Pre-Auth/Guests** is selected.



Update Disable NAT on "subnet 30.0"

Name: NAT on "Pre-Auth / Guests"

Note:

WAN Translation (Hide)

Uplinks: Select All | None | Reset

☑ Uplink

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 Address (not

IP Adjustments (optional) (Hide)

Start IP: first WAN IP to NAT to

End IP: last WAN IP to NAT to

Static port: □ retain packet source port - "cone" instead of "symmetric NAT" (not recommended)

Subnets (Hide)

Addresses: ✕ Pre-Auth / Guests

Static Routes: no options routed subnets to perform NAT for

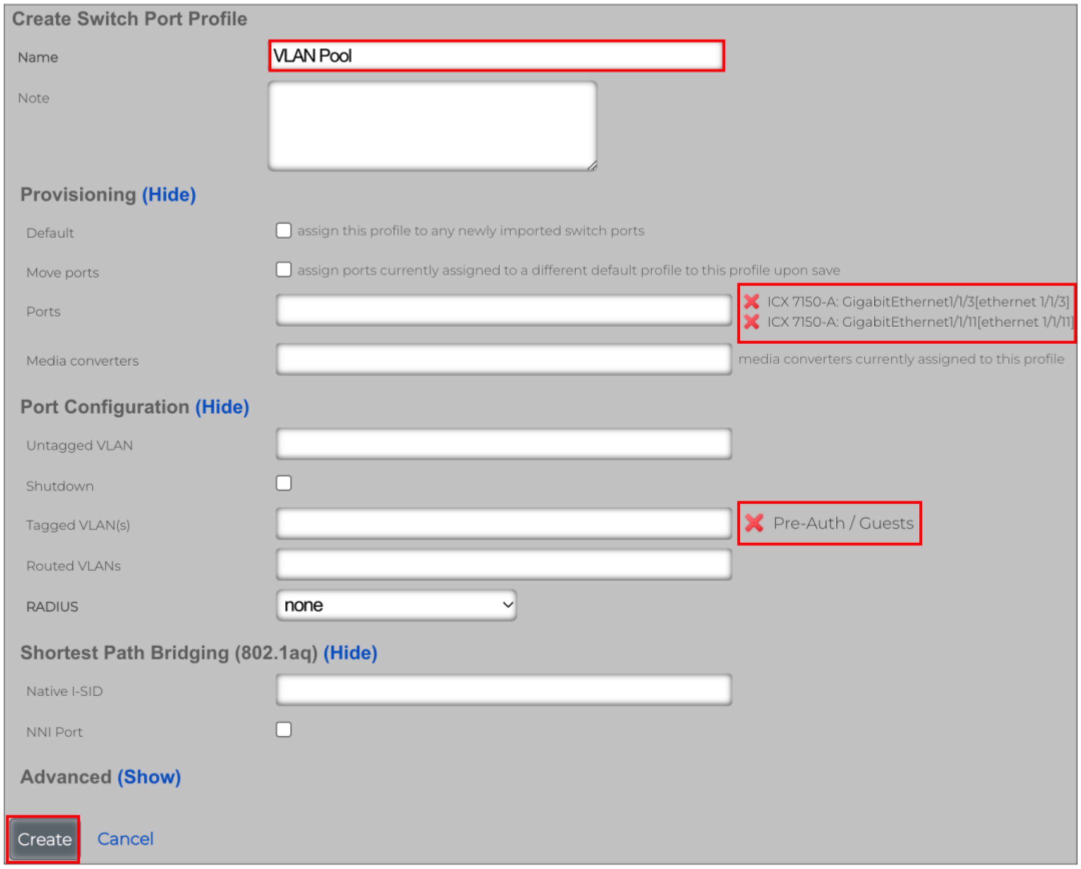
FIGURE 14 – UPDATE THE NAT ENTRY

Click **Update** to finish.

Step 4 – Create the Switch Port Profile

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

- **Name**: Enter **VLAN Pool.**
- **Ports**: Select the ports that are connected to RWG and to the access point. It's **1/1/3** and **1/1/11** in this lab.
- **Tagged VLANs**: Select **Pre-Auth/Guests**.



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: ✗ ICX 7150-A: GigabitEthernet1/1/3[ethernet 1/1/3]
✗ ICX 7150-A: GigabitEthernet1/1/11[ethernet 1/1/11]

Media converters: media converters currently assigned to this profile

Port Configuration (Hide)

Untagged VLAN:

Shutdown: □

Tagged VLAN(s): ✗ Pre-Auth / Guests

Routed VLANs:

RADIUS: none

Shortest Path Bridging (802.1aq) (Hide)

Native I-SID:

NNI Port: □

Advanced (Show)

Create Cancel

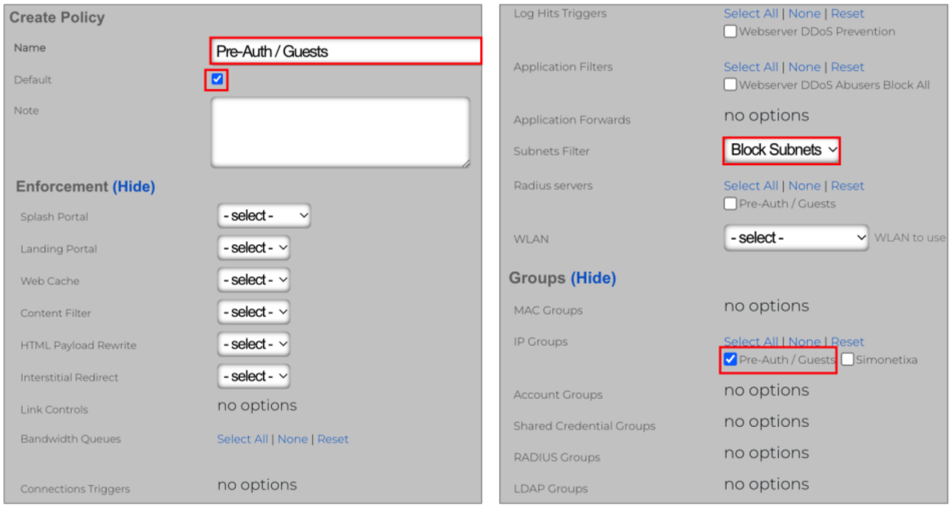
Figure 15 – Create Switch Port Profile

Click **Create** to finish.

Step 5 – Create the Policy

The policy will tie the IP group with a bandwidth queue and a subnet filter. Later it will also be tied to splash portal. Click **Policies** at the top menu, scroll down and click **Create New** in the **Policies** section. Enter the following information:

- **Name**: Enter **Pre-Auth/Guests.**
- **Default**: Mark the checkbox.
- **Subnets Filter**: Select **Block Subnets**.
- **IP Groups**: Select **Pre-Auth/Guests.**



Create Policy

Name	Pre-Auth / Guests
Default	☑
Note	

Enforcement (Hide)

Splash Portal	- select -
Landing Portal	- select -
Web Cache	- select -
Content Filter	- select -
HTML Payload Rewrite	- select -
Interstitial Redirect	- select -
Link Controls	no options
Bandwidth Queues	Select All | None | Reset
Connections Triggers	no options
Log Hits Triggers	Select All | None | Reset ☐ Webserver DDoS Prevention
Application Filters	Select All | None | Reset ☐ Webserver DDoS Abusers Block All
Application Forwards	no options
Subnets Filter	Block Subnets
Radius servers	Select All | None | Reset ☐ Pre-Auth / Guests
WLAN	- select - WLAN to use

Groups (Hide)

MAC Groups	no options
IP Groups	Select All | None | Reset ☑ Pre-Auth / Guests ☐ Simonetixa
Account Groups	no options
Shared Credential Groups	no options
RADIUS Groups	no options
LDAP Groups	no options

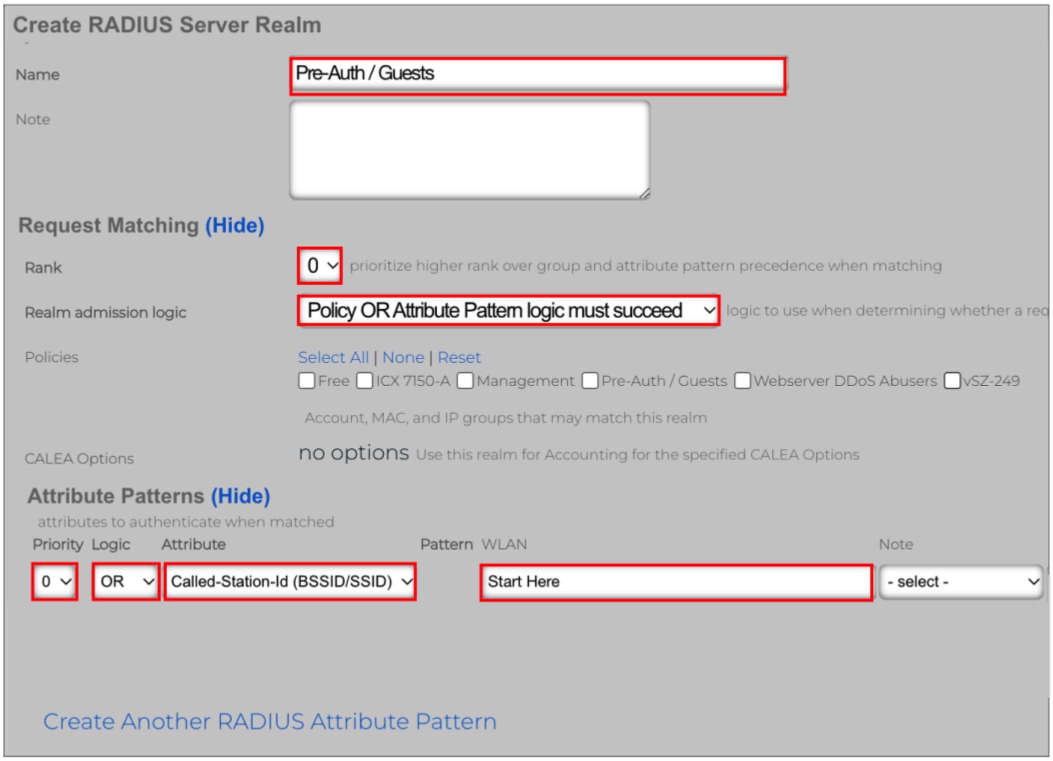
FIGURE 16 – CREATE POLICY

Click **Create** to finish.

Step 6 – Create the RADIUS Realm

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

- **Name**: Enter **Pre-Auth/Guests.**
- **Rank**: Select **0.**
- **Real admission logic**: Select **Policy OR Attribute Pattern logic must succeed.**
- **Priority**: Select **0.**
- **Logic**: Select **OR.**
- **Attribute**: Select **Called-Station-Id (BSSID/SSID).**
- **Pattern**: Enter **Start Here**. That will be the SSID for the WLAN we will create soon.



Create RADIUS Server Realm

Name: Pre-Auth / Guests

Note:

Request Matching (Hide)

Rank: 0 prioritize higher rank over group and attribute pattern precedence when matching

Realm admission logic: Policy OR Attribute Pattern logic must succeed logic to use when determining whether a req

Policies: Select All | None | Reset

□Free □ICX 7150-A □Management □Pre-Auth / Guests □Webserver DDoS Abusers □vSZ-249

Account, MAC, and IP groups that may match this 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	OR	Called-Station-Id (BSSID/SSID)	Start Here	- select -

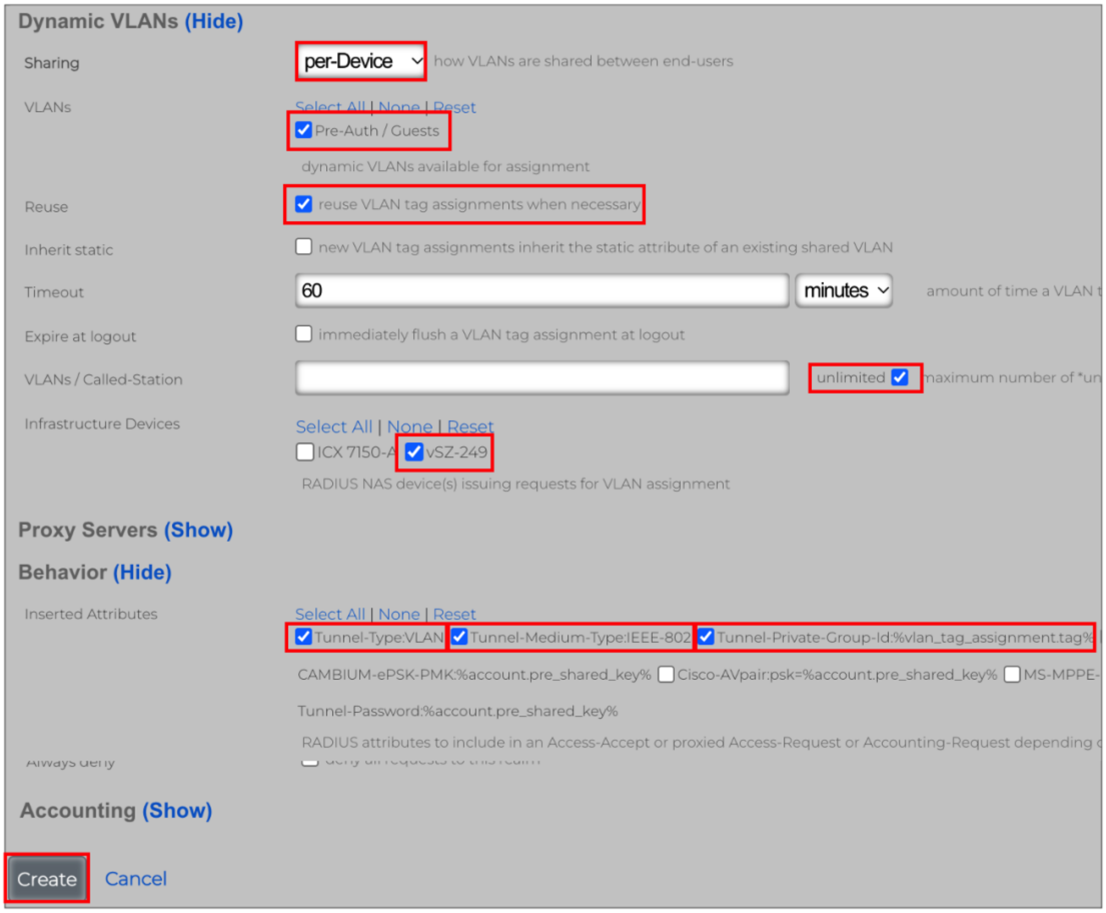
Create Another RADIUS Attribute Pattern

Figure 17 – Create RADIUS Server Realm

Scroll down to continue.

Enter the following information:

- **Sharing**: Select **per-Device**.
- **VLANs**: Check **Pre-Auth/Guests**.
- **Reuse**: Check **reuse VLAN tag assignments when necessary**.
- **VLANs/Called-Station**: Check **unlimited**.
- **Infrastructure Devices**: Check the name of your SmartZone controller. This whitelists the controller to send requests to the realm).
- **Inserted Attributes**: Check the following attributes:
  - Tunnel-Type:VLAN.
  - Tunnel-Medium-Type-IEEE-802.
  - Tunnel-Private-Group-Id:%vlan_tag_assignment.tag%.



Dynamic VLANs (Hide)

Sharing: per-Device — how VLANs are shared between end-users

VLANs: Select All | None | Reset
☑ Pre-Auth / Guests
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 VLAN t

Expire at logout: □ immediately flush a VLAN tag assignment at logout

VLANs / Called-Station: unlimited ☑ maximum number of "un

Infrastructure Devices: Select All | None | Reset
□ ICX 7150-A ☑ 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-802 ☑ Tunnel-Private-Group-Id:%vlan_tag_assignment.tag%
CAMBIUM-ePSK-PMK:%account.pre_shared_key% □ Cisco-AVpair:psk=%account.pre_shared_key% □ MS-MPPE-
Tunnel-Password:%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)

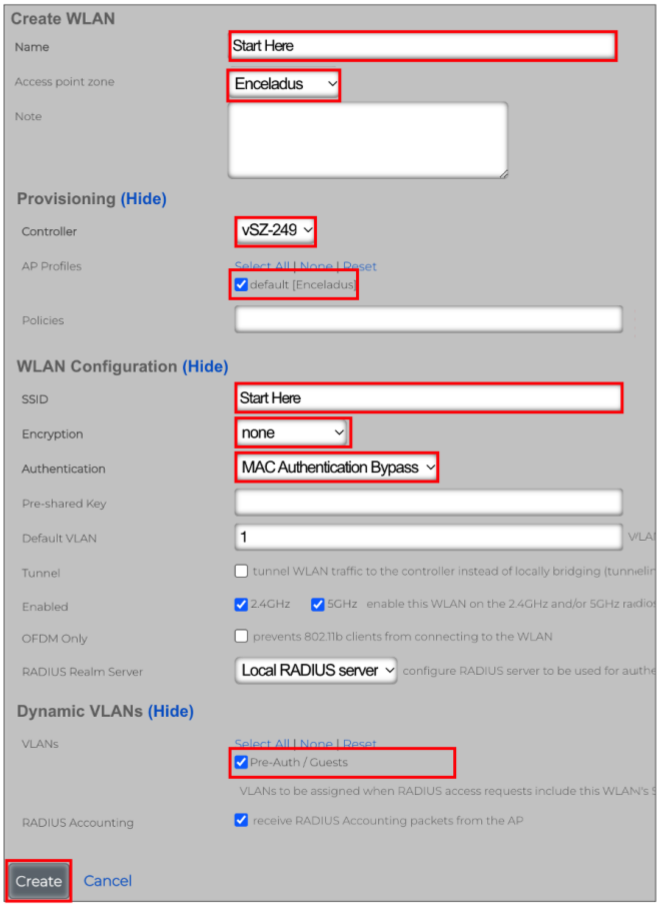
Figure 18 – Create RADIUS Server Realm

Click **Create** to finish.

Step 7 – Create the WLAN

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

- **Name**: Enter **Start Here**.
- **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 **Start Here**.
- **Encryption**: Select **none**.
- **Authentication**: Select **MAC Authentication Bypass**.
- **VLANs**: Check **Pre-Auth/Guests**.



Create WLAN

Name	Start Here
Access point zone	Enceladus
Note	

Provisioning (Hide)

Controller	vSZ-249
AP Profiles	Select All | None | Reset ☑ default [Enceladus]
Policies	

WLAN Configuration (Hide)

SSID	Start Here
Encryption	none
Authentication	MAC Authentication Bypass
Pre-shared Key	
Default VLAN	1 VLAI
Tunnel	☐ tunnel WLAN traffic to the controller instead of locally bridging (tunnelir
Enabled	☑ 2.4GHz ☑ 5GHz enable this WLAN on the 2.4GHz and/or 5GHz radios
OFDM Only	☐ prevents 802.11b clients from connecting to the WLAN
RADIUS Realm Server	Local RADIUS server configure RADIUS server to be used for authe

Dynamic VLANs (Hide)

VLANs	Select All | None | Reset ☑ Pre-Auth / Guests VLANs to be assigned when RADIUS access requests include this WLAN's S
RADIUS Accounting	☑ receive RADIUS Accounting packets from the AP

FIGURE 19 – CREATE WLAN

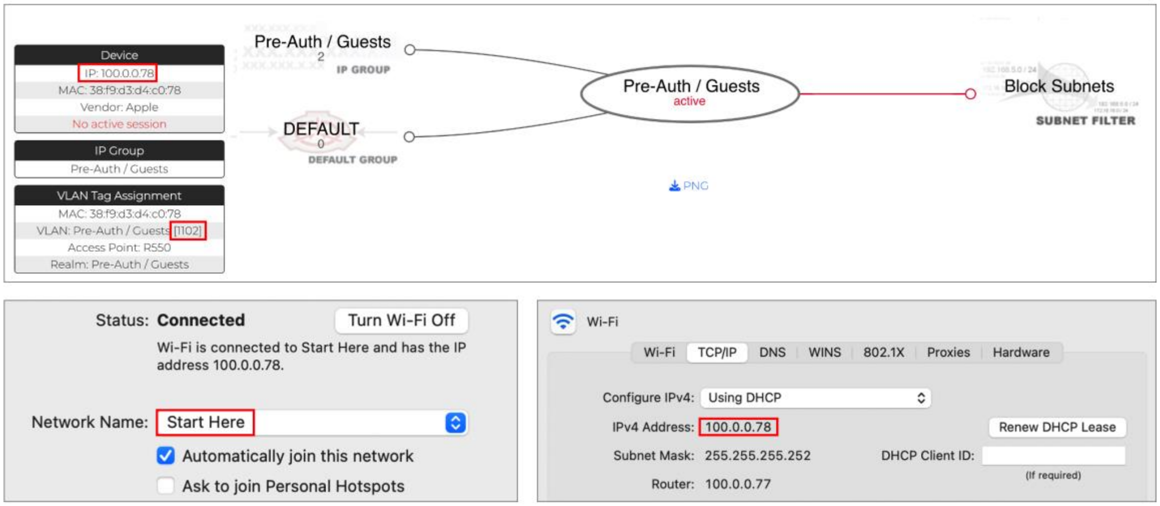
Click **Create** to finish.

Test the Configuration

Test the configuration before continuing.

You should be able to connect to the **Start Here** SSID without a password, get a VLAN from the pool and an IP address from the 100.0.0.x /30 subnet. At this moment, we don't have any portals configured.

We used a MacBook to connect. As expected, it got associated to VLAN 1102 and received an IP address in the subnet 100.0.0.76/30.



Device
IP: 100.0.0.78
MAC: 38:f9:d3:d4:c0:78
Vendor: Apple
No active session

IP Group
Pre-Auth / Guests

VLAN Tag Assignment
MAC: 38:f9:d3:d4:c0:78
VLAN: Pre-Auth / Guests [1102]
Access Point: R550
Realm: Pre-Auth / Guests

Status: **Connected**

Wi-Fi is connected to Start Here and has the IP address 100.0.0.78.

Network Name: Start Here

☑ Automatically join this network

□ Ask to join Personal Hotspots

Configure IPv4: Using DHCP

IPv4 Address: 100.0.0.78

Subnet Mask: 255.255.255.252

DHCP Client ID: (If required)

Router: 100.0.0.77

Figure 20 – Testing the Configuration

Portals Setup

In this section we will create a splash portal which will be used as an enforcement rule to the **Pre-Auth/Guests** policy. A splash portal is a captive portal, and it prevents the user to access the network until he logs in.

For this exercise, we will use a **Shared Credential Group** for the user login in the splash portal. A shared credential group can be used to define the traffic quotas and time expiration for the session. Our shared credential will be tied to a new policy.

The new policy will have the following enforcement rules:

- A bandwidth queue with less speed.
- A landing portal.
- The Block Subnets filter.

How It Works

The client device is assigned a VLAN from the VLAN pool and an IP address from the Pre-Auth/Guests DHCP scope. Because of that, the device is identified by RWG as a member of the **Pre-Auth/Guests IP group**.

That group uses the **Pre-Auth/Guests Policy**, which has a splash portal as an enforcement rule.

The splash portal is configured to use the shared credential. When the user enters the required data and logs in the splash portal, his identity changes. He is now a member of the **Shared Credential Group**.

The shared credential group uses the **Free Policy**, which has a landing portal as an enforcement rule.

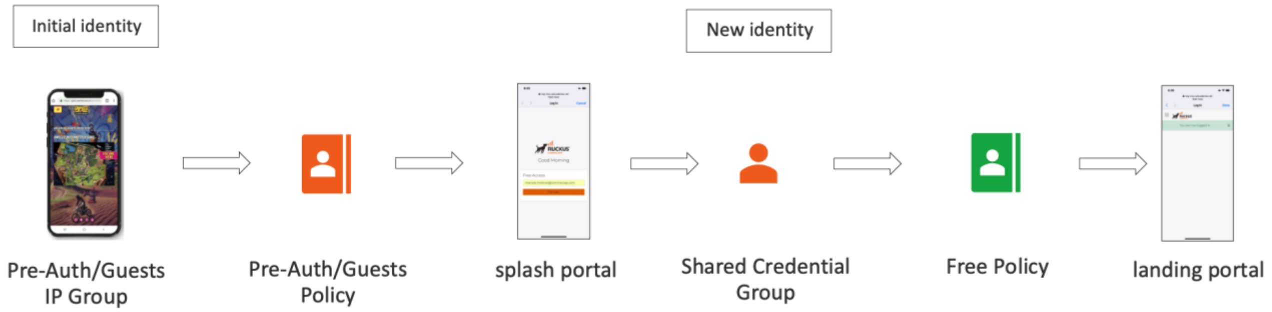
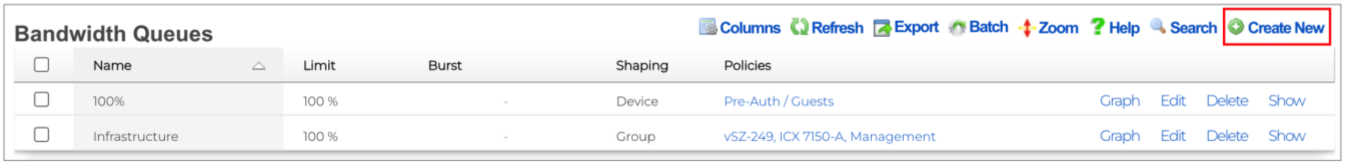


FIGURE 21 – FLOW TOWARDS THE LANDING PORTAL

Step 1 – Create a Bandwidth Queue

We want the **Free Policy** to use less speed. For that, we need to create a new bandwidth queue. Navigate to **Policies/Traffic Shaping**, scroll down, and click **Create New** in the **Bandwidth Queues** section:



☐	Name	Limit	Burst	Shaping	Policies				
☐	100%	100 %	-	Device	Pre-Auth / Guests	Graph	Edit	Delete	Show
☐	Infrastructure	100 %	-	Group	vSZ-249, ICX 7150-A, Management	Graph	Edit	Delete	Show

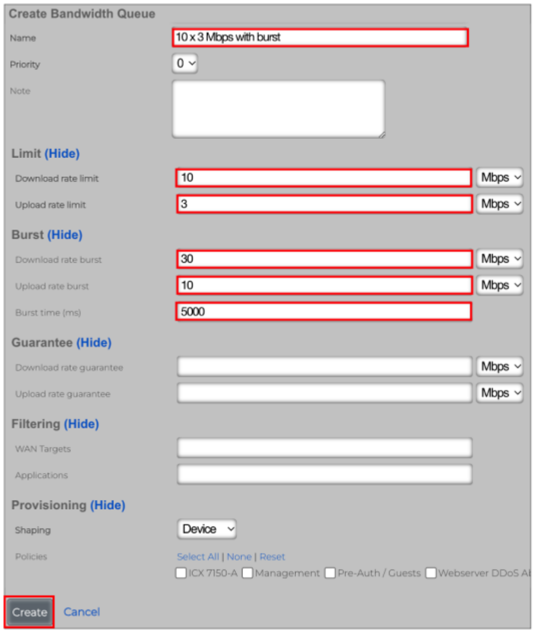
FIGURE 22 – BANDWIDTH QUEUES

Enter the following information:

Name: Enter **10 x 3 Mbps with burst**

- **Download rate limit**: Enter 10.
- **Upload rate limit**: Enter 3.
- **Download rate burst**: Enter 30.
- **Upload rate burst**: Enter 10.
- **Burst time (ms):** Enter 5000.

Click **Create** to finish.



Create Bandwidth Queue

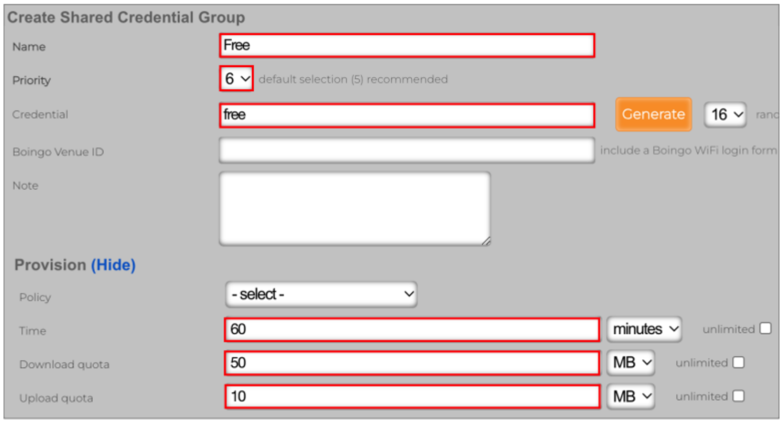
Name	10 x 3 Mbps with burst	
Priority	0	
Note		
Limit (Hide)		
Download rate limit	10	Mbps
Upload rate limit	3	Mbps
Burst (Hide)		
Download rate burst	30	Mbps
Upload rate burst	10	Mbps
Burst time (ms)	5000	
Guarantee (Hide)		
Download rate guarantee		Mbps
Upload rate guarantee		Mbps
Filtering (Hide)		
WAN Targets		
Applications		
Provisioning (Hide)		
Shaping	Device	
Policies	Select All | None | Reset ☐ ICX 7150-A ☐ Management ☐ Pre-Auth / Guests ☐ Webserver DDoS A	

FIGURE 23 – CREATE BANDWIDTH QUEUE

Step 2 – Create Shared Credential Group

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

- **Name**: Enter **Free**.
- **Priority**: Select 6 (it needs to be higher than the priority for the **Pre/Auth/Guests IP Group**).
- **Credential**: Enter **free**. This is a special credential to allow the user to login without an access code.
- **Time**: 60.
- **Download quota**: 50.
- **Upload quota**: 10.



Create Shared Credential Group

Name	Free		
Priority	6	default selection (5) recommended	
Credential	free	Generate	16 ranc
Boingo Venue ID		include a Boingo WiFi login form	
Note			

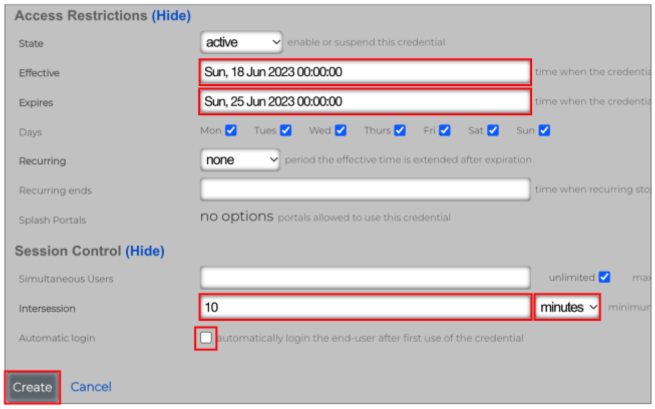
Provision (Hide)

Policy	- select -		
Time	60	minutes	unlimited □
Download quota	50	MB	unlimited □
Upload quota	10	MB	unlimited □

FIGURE 24 – CREATE SHARED CREDENTIAL GROUP

Scroll down to continue. Enter the following information:

- **Effective**: Date and time when the credential starts to be valid. Use the current date and time.
- **Expires**: Date and time when the credential expires. The default is one week after **Effective**.
- **Intersession**: Enter 10 minutes. This is the time to wait between new logins from the same client.
- **Automatic login**: Unmark the checkbox.



Access Restrictions (Hide)

State	active	enable or suspend this credential
Effective	Sun, 18 Jun 2023 00:00:00	time when the credentia
Expires	Sun, 25 Jun 2023 00:00:00	time when the credentia
Days	Mon ☑ Tues ☑ Wed ☑ Thurs ☑ Fri ☑ Sat ☑ Sun ☑	
Recurring	none	period the effective time is extended after expiration
Recurring ends		time when recurring sto
Splash Portals	no options	portals allowed to use this credential

Session Control (Hide)

Simultaneous Users		unlimited ☑	ma
Intersession	10	minutes	minimur
Automatic login	□ automatically login the end-user after first use of the credential		

FIGURE 25 – ACCESS RESTRICTIONS

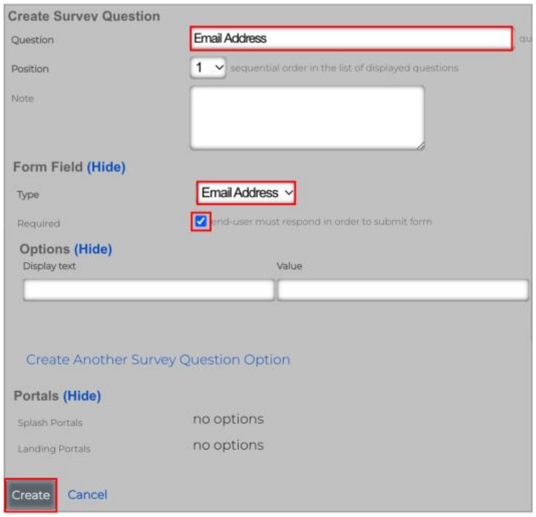
Click **Create** to finish.

Step 3 – Create Survey Question

Survey Questions enable the operator to build a form that collects data before allowing a user to login. Navigate to **Identity/Shared Credentials**, then click **Create New** in the section **Survey Questions**. Enter the following information:

- **Question**: Enter **Email Address.**
- **Type**: Select **Email Address**.
- **Required**: Mark the checkbox.

Click **Create** to finish.



Create Survey Question

Question: Email Address

Position: 1 sequential order in the list of displayed questions

Note:

Form Field (Hide)

Type: Email Address

Required: ☑ end-user must respond in order to submit form

Options (Hide)

Display text	Value

Create Another Survey Question Option

Portals (Hide)

Splash Portals: no options

Landing Portals: no options

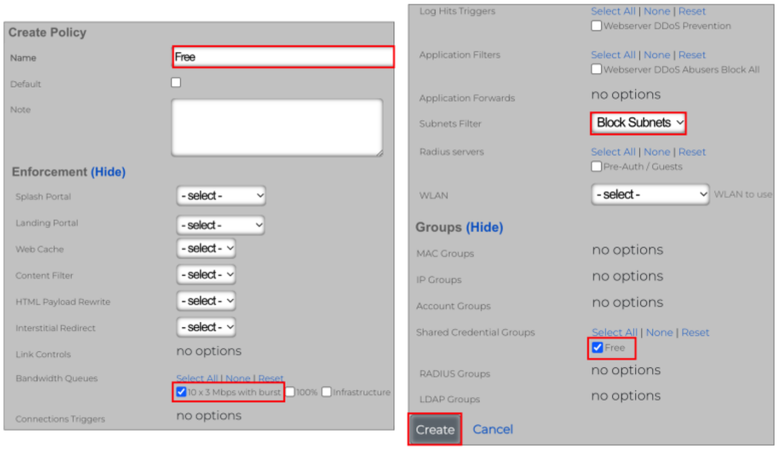
Create Cancel

FIGURE 26 – CREATE SURVEY QUESTION

Step 4 – Create the Free Policy

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

- **Name**: Enter **Free.**
- **Bandwidth Queues**: Check **10 x 3 Mbps with burst.**
- **Subnets Filter**: Select **Block Subnets.**
- **Shared Credential Groups**: Select **Free.**



Create Policy

Name: Free

Default: □

Note:

Enforcement (Hide)

Splash Portal: - select -

Landing Portal: - select -

Web Cache: - select -

Content Filter: - select -

HTML Payload Rewrite: - select -

Interstitial Redirect: - select -

Link Controls: no options

Bandwidth Queues: Select All | None | Reset
☑ 10 x 3 Mbps with burst □ 100% □ Infrastructure

Connections Triggers: no options

Log Hits Triggers: Select All | None | Reset
□ Webserver DDoS Prevention

Application Filters: Select All | None | Reset
□ Webserver DDoS Abusers Block All

Application Forwards: no options

Subnets Filter: Block Subnets

Radius servers: Select All | None | Reset
□ Pre-Auth / Guests

WLAN: - select - WLAN to use

Groups (Hide)

MAC Groups: no options

IP Groups: no options

Account Groups: no options

Shared Credential Groups: Select All | None | Reset
☑ Free

RADIUS Groups: no options

LDAP Groups: no options

Create Cancel

FIGURE 27 – CREATE POLICY

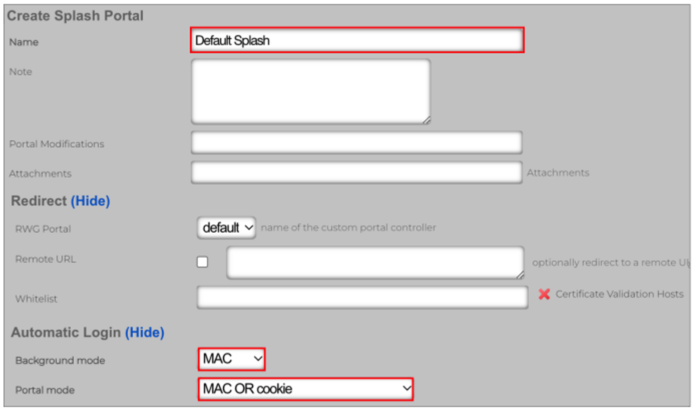
Click **Create** to finish.

Step 5 – Create the Splash Portal

Navigate to **Policies/Captive Portal**, then click **Create New** in the **Splash Portals** section. Enter the following information:

- **Name**: Enter **Default Splash**.
- **Background mode**: Select **MAC.**
- **Portal mode**: Select **MAC OR cookie**.

Scroll down to continue.



Create Splash Portal

Name: Default Splash

Note:

Portal Modifications:

Attachments: Attachments

Redirect (Hide)

RWG Portal: default — name of the custom portal controller

Remote URL: □ — optionally redirect to a remote U

Whitelist: ✗ Certificate Validation Hosts

Automatic Login (Hide)

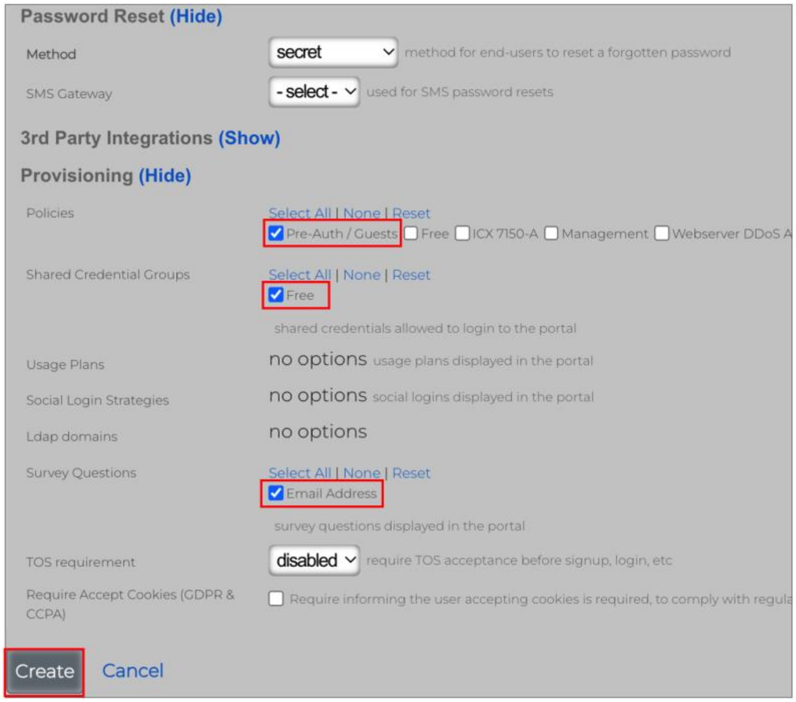
Background mode: MAC

Portal mode: MAC OR cookie

FIGURE 28 – CREATE SPLASH PORTAL

Enter the following information:

- **Policies**: Mark **Pre-Auth/Guests**.
- **Shared Credential Groups**: Mark **Free**.
- **Survey Questions**: Mark **Email Address**.



Password Reset (Hide)

Method: secret — method for end-users to reset a forgotten password

SMS Gateway: - select - — used for SMS password resets

3rd Party Integrations (Show)

Provisioning (Hide)

Policies: Select All | None | Reset
☑ Pre-Auth / Guests □ Free □ ICX 7150-A □ Management □ Webserver DDoS A

Shared Credential Groups: Select All | None | Reset
☑ Free
shared credentials allowed to login to the portal

Usage Plans: no options — usage plans displayed in the portal

Social Login Strategies: no options — social logins displayed in the portal

Ldap domains: no options

Survey Questions: Select All | None | Reset
☑ Email Address
survey questions displayed in the portal

TOS requirement: disabled — require TOS acceptance before signup, login, etc

Require Accept Cookies (GDPR & CCPA): □ Require informing the user accepting cookies is required, to comply with regula

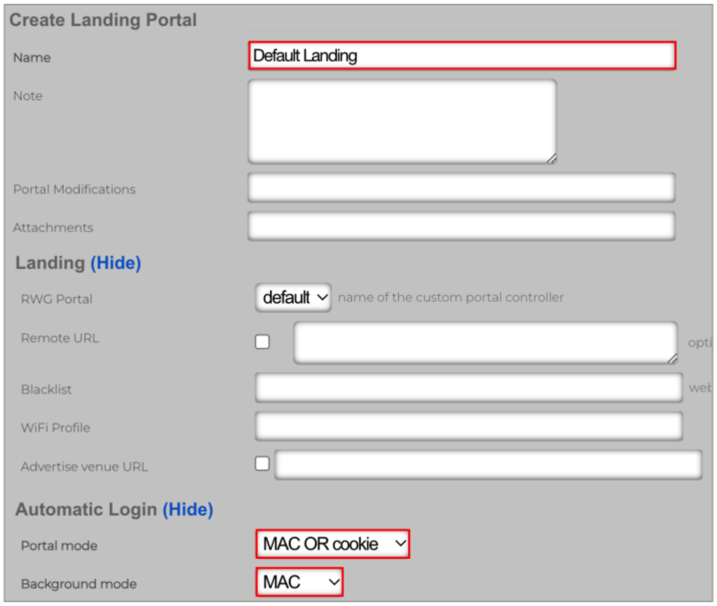
FIGURE 29 – CREATE SPLASH PORTAL

Click **Create** to finish.

Step 6 – Create Landing Portal

Navigate to **Policies/Captive Portal**, then click **Create New** in the **Landing Portals** section. Enter the following information:

- **Name**: Enter **Default Landing**.
- **Portal mode**: Select **MAC OR cookie**.
- **Background mode:** Select **MAC**.



Create Landing Portal

Name	Default Landing
Note	
Portal Modifications	
Attachments	

Landing (Hide)

RWG Portal	default name of the custom portal controller
Remote URL	□ opti
Blacklist	wet
WiFi Profile	
Advertise venue URL	□

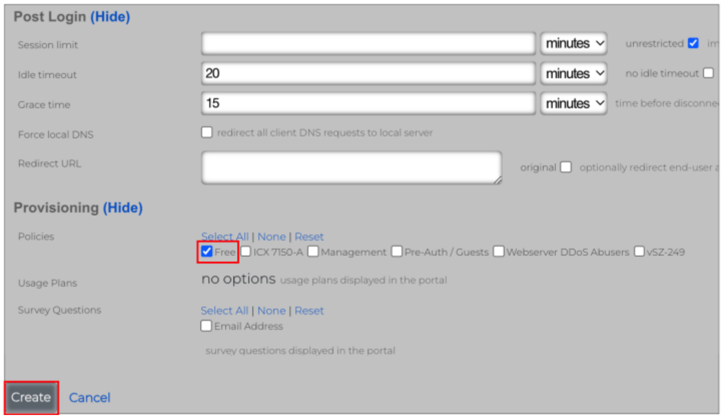
Automatic Login (Hide)

Portal mode	MAC OR cookie
Background mode	MAC

FIGURE 30 – CREATE LANDING PORTAL

Scroll down to continue. Enter the following information:

- **Policies**: Mark **Free.**



Post Login (Hide)

Session limit	minutes unrestricted ☑ im
Idle timeout	20 minutes no idle timeout □
Grace time	15 minutes time before disconne
Force local DNS	□ redirect all client DNS requests to local server
Redirect URL	original □ optionally redirect end-user a

Provisioning (Hide)

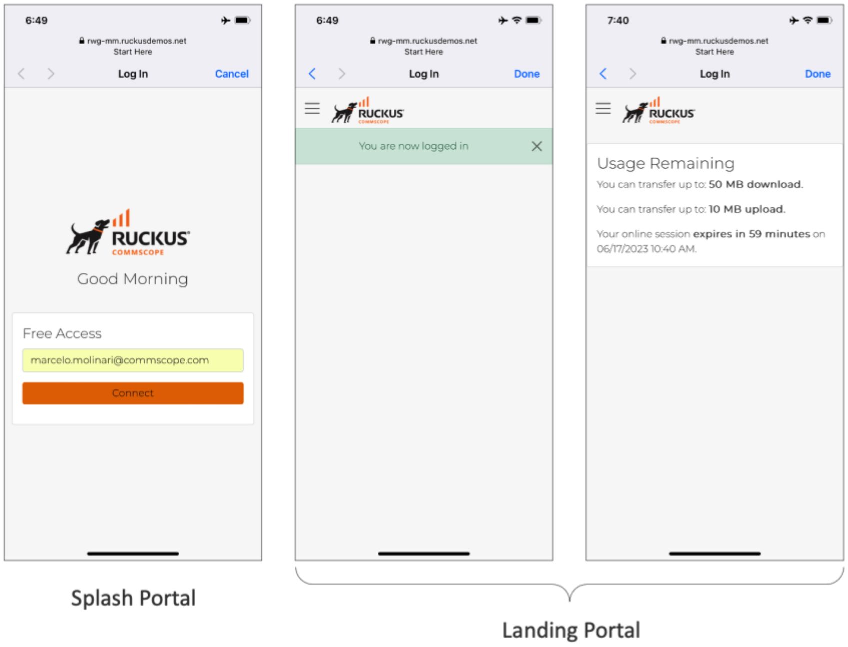
Policies	Select All | None | Reset ☑ Free □ ICX 7150-A □ Management □ Pre-Auth / Guests □ Webserver DDoS Abusers □ vSZ-249
Usage Plans	no options usage plans displayed in the portal
Survey Questions	Select All | None | Reset □ Email Address survey questions displayed in the portal

FIGURE 31 – CREATE LANDING PORTAL

Click **Create** to finish.

Testing the Portals

The configuration is complete. After connecting to the SSID, the client device should redirect to the captive portal automatically. Enter your email and click **Connect**. You should be redirected to the landing portal.



Good Morning

Free Access

marcelo.molinari@commscope.com

Connect

You are now logged in

Usage Remaining

You can transfer up to: 50 MB download.

You can transfer up to: 10 MB upload.

Your online session expires in 59 minutes on 06/17/2023 10:40 AM.

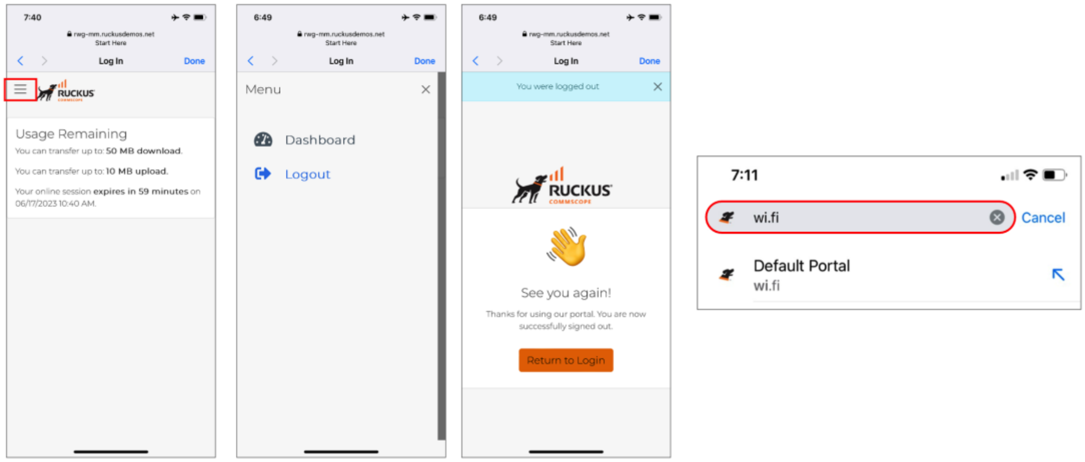
Splash Portal

Landing Portal

FIGURE 32 – TESTING THE PORTALS

Portal Navigation

The basic portal includes a menu function. Click the menu icon ☰ to access the menu. When no plans are being used, only the options **Dashboard** and **Logout** show. **Dashboard** returns to the landing portal page showing **Usage Remaining**. At any moment, you can invoke the landing portal by entering **wi.fi** in your browser:



Usage Remaining

You can transfer up to: 50 MB download.

You can transfer up to: 10 MB upload.

Your online session expires in 59 minutes on 06/17/2023 10:40 AM.

You were logged out

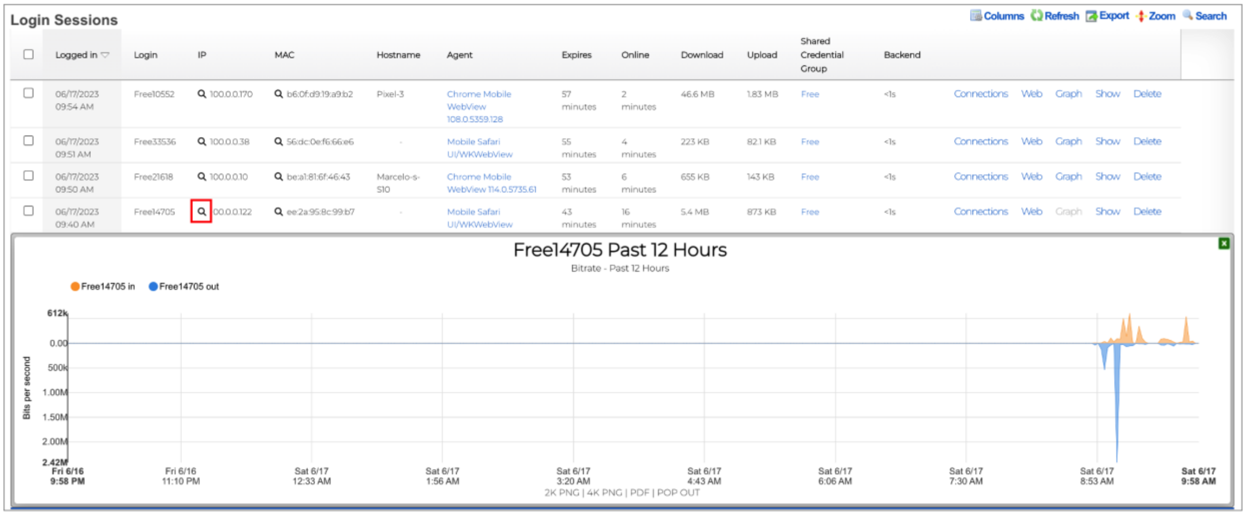
See you again!

Thanks for using our portal. You are now successfully signed out.

FIGURE 33 – PORTAL NAVIGATIONS AND USE OF WI.FI

Viewing Login Sessions

The operator can see the current login sessions at **Instruments/Device Sessions**. Click the lens 🔍 icon to see the policies for the device. Click on **Delete** to terminate any device sessions. Click on **Graph** to plot the upload and download traffic for the selected device.



Login Sessions

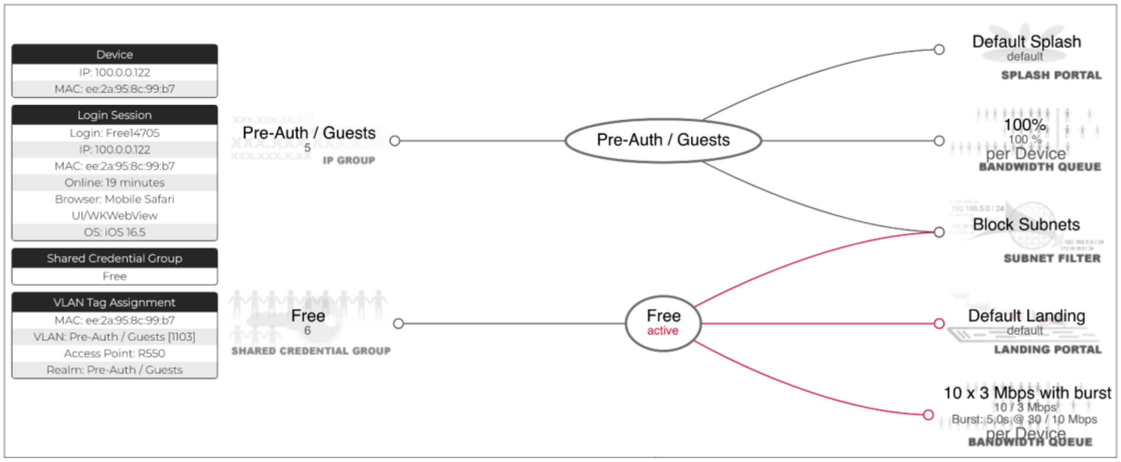
□	Logged in ▽	Login	IP	MAC	Hostname	Agent	Expires	Online	Download	Upload	Shared Credential Group	Backend					
□	06/17/2023 09:54 AM	Free10552	🔍 100.0.0.170	🔍 b6:0f:d9:19:a9:b2	Pixel-3	Chrome Mobile WebView 108.0.5359.128	57 minutes	2 minutes	46.6 MB	1.83 MB	Free	<1s	Connections	Web	Graph	Show	Delete
□	06/17/2023 09:51 AM	Free33536	🔍 100.0.0.38	🔍 56:dc:0e:f6:66:e6	-	Mobile Safari UI/WKWebView	55 minutes	4 minutes	223 KB	82.1 KB	Free	<1s	Connections	Web	Graph	Show	Delete
□	06/17/2023 09:50 AM	Free21618	🔍 100.0.0.10	🔍 be:a1:81:6f:46:43	Marcelo-s-S10	Chrome Mobile WebView 114.0.5735.61	53 minutes	6 minutes	655 KB	143 KB	Free	<1s	Connections	Web	Graph	Show	Delete
□	06/17/2023 09:40 AM	Free14705	🔍 00.0.0.122	🔍 ee:2a:95:8c:99:b7	-	Mobile Safari UI/WKWebView	43 minutes	16 minutes	5.4 MB	873 KB	Free	<1s	Connections	Web	Graph	Show	Delete

FIGURE 34 – LOGIN SESSIONS

View Session Details

By clicking the lens icon, you see the session details for the device.

Device 100.0.0.122 started at the **Pre-Auth/Guests** IP group and got to the **Default Splash** portal. After login, the device moved to the **Free** shared credential group and got to the **Default Landing** portal. The section in red indicates the profile and enforcements that are currently in use by the client device.



Device
IP: 100.0.0.122
MAC: ee:2a:95:8c:99:b7

Login Session
Login: Free14705
IP: 100.0.0.122
MAC: ee:2a:95:8c:99:b7
Online: 19 minutes
Browser: Mobile Safari UI/WKWebView
OS: iOS 16.5

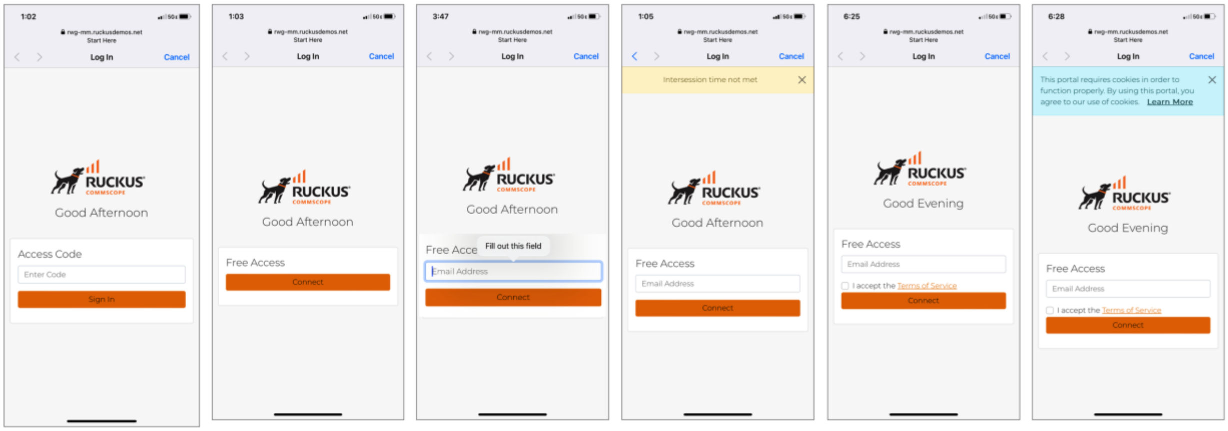
Shared Credential Group
Free

VLAN Tag Assignment
MAC: ee:2a:95:8c:99:b7
VLAN: Pre-Auth / Guests [1103]
Access Point: R550
Realm: Pre-Auth / Guests

FIGURE 35 – SESSION DETAILS AND POLICY

Splash Portal Variations

Here are some captive portal variations obtained by changing the splash portal settings:


rwg-mm.ruckusdemos.net
Start Here
Log In
Cancel
RUCKUS
COMMSCOPE
Good Afternoon
Access Code
Enter Code
Sign In
Free Access
Connect
Fill out this field
Email Address
Intersession time not met
Good Evening
I accept the Terms of Service
This portal requires cookies in order to function properly. By using this portal, you agree to our use of cookies. Learn More

The shared credential is not 'free'

No survey question

The survey question response is required

The survey question response is optional. The intersession time has not elapsed

Including Terms of Service

Including GDPR & CCPA

FIGURE 36 – SPLASH PORTAL VARIATIONS

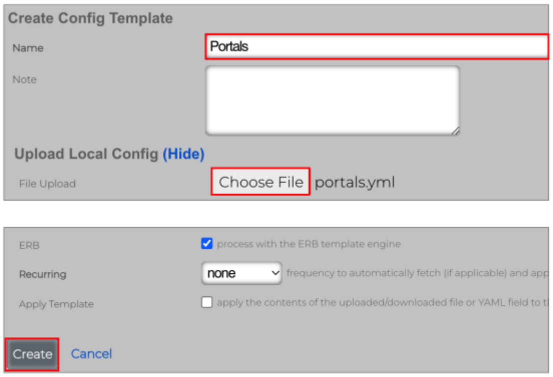
Using a Config Template to Create the Portals

Download the config template at the URL below to configure the bandwidth queue, shared credential, policy, and portals with just four clicks:

https://github.com/commscope-ruckus/RUCKUS-RWG-Templates/blob/main/portals.yml

Navigate to **System/Backup** and click **Create New** in the section **Config Templates**. Enter the following information:

- **Name**: Enter a name for the template.
- **File Upload**: Select the file with config template.



Create Config Template

Name: Portals

Note:

Upload Local Config (Hide)

File Upload: Choose File portals.yml

ERB: ☑ process with the ERB template engine

Recurring: none frequency to automatically fetch (if applicable) and app

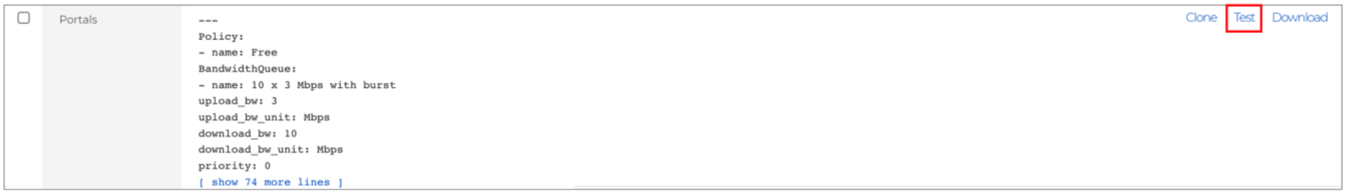
Apply Template: □ apply the contents of the uploaded/downloaded file or YAML field to t

Create Cancel

FIGURE 37 – CREATE CONFIG TEMPLATE

Scroll down and click **Create** to finish.

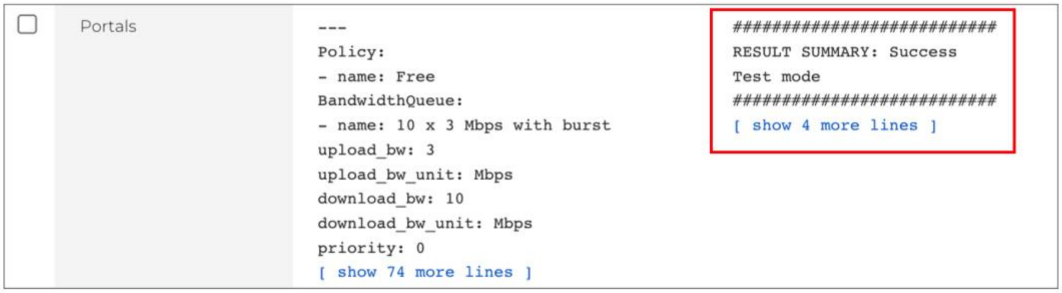
Click **Test** to verify the template syntax and conflicts. That will not apply the template to RWG.



```
---
Policy:
- name: Free
BandwidthQueue:
- name: 10 x 3 Mbps with burst
upload_bw: 3
upload_bw_unit: Mbps
download_bw: 10
download_bw_unit: Mbps
priority: 0
[ show 74 more lines ]
```

FIGURE 38 – TEST THE TEMPLATE

If all is good, the test will succeed. Otherwise, edit the template and fix the error.

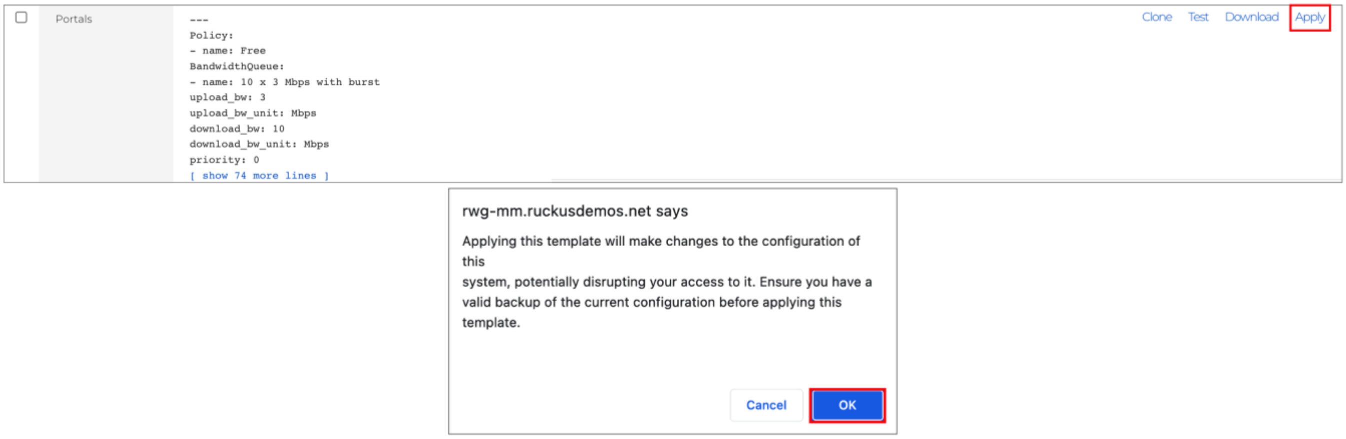


```
---
Policy:
- name: Free
BandwidthQueue:
- name: 10 x 3 Mbps with burst
upload_bw: 3
upload_bw_unit: Mbps
download_bw: 10
download_bw_unit: Mbps
priority: 0
[ show 74 more lines ]
```

```
##########################
RESULT SUMMARY: Success
Test mode
##########################
[ show 4 more lines ]
```

FIGURE 39 – SUCCESS – TEST MODE

Click **Apply**, then click **OK** in the confirmation window that follows.



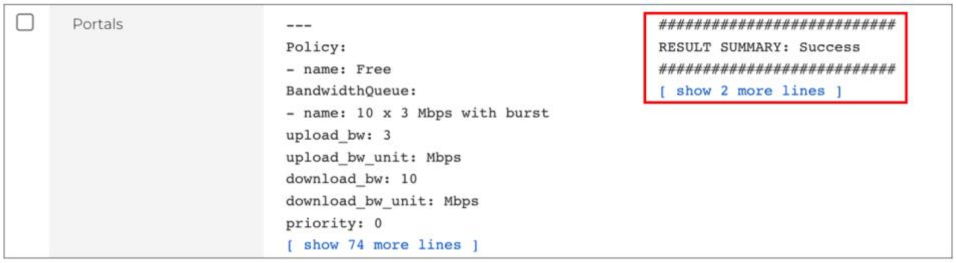
```
---
Policy:
- name: Free
BandwidthQueue:
- name: 10 x 3 Mbps with burst
upload_bw: 3
upload_bw_unit: Mbps
download_bw: 10
download_bw_unit: Mbps
priority: 0
[ show 74 more lines ]
```

rwg-mm.ruckusdemos.net says

Applying this template will make changes to the configuration of this
system, potentially disrupting your access to it. Ensure you have a valid backup of the current configuration before applying this template.

FIGURE 40 – APPLY THE TEMPLATE

If all goes well, you will receive a success message.



```
---
Policy:
- name: Free
BandwidthQueue:
- name: 10 x 3 Mbps with burst
upload_bw: 3
upload_bw_unit: Mbps
download_bw: 10
download_bw_unit: Mbps
priority: 0
[ show 74 more lines ]
```

```
##########################
RESULT SUMMARY: Success
##########################
[ show 2 more lines ]
```

FIGURE 41 – SUCCESS

Portal Modifications

The captive portal is the initial destination for web requests originating from unauthenticated devices. End users navigate and utilize the functionality in the captive portal web application to obtain access to the network. Given that, the RWG captive portal represents most of the end-user experience, and customization of the captive portal is an integral facet of the operator marketing strategy.

The default captive portal contains functions that are fully integrated into RWG's packet management capabilities. The operator may choose to deploy a fully operational network by using the default captive portal as is.

Alternatively, the operator may choose to customize the captive portal in several ways, ranging from changing the artwork and layout to implementing entirely new functionality through the underlying the **Ruby on Rails** infrastructure.

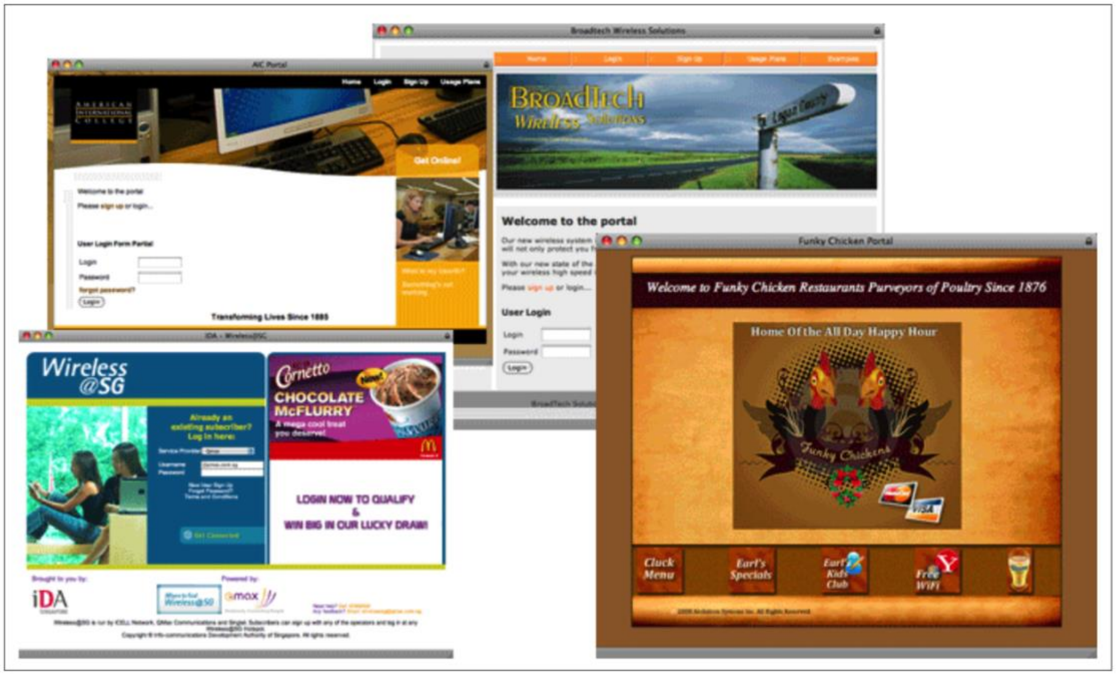

Broadtech Wireless Solutions
AIC Portal
Get Online!
Welcome to the portal
User Login
Transforming Lives Since 1885
Wireless @SG
Cornetto
CHOCOLATE McFLURRY
LOGIN NOW TO QUALIFY & WIN BIG IN OUR LUCKY DRAW!
iDA
Funky Chicken Portal
Welcome to Funky Chicken Restaurants Purveyors of Poultry Since 1876
Home Of the All Day Happy Hour
Funky Chickens
Cluck Menu
Earl's Specials
Earl's Kids Club
Free WiFi

FIGURE 42 – SPLASH PORTAL CUSTOMIZATION

Modifying the artwork and layout of the default captive portal is easily accomplished. RWG uses standard CSS and HTML to control the presentation of the captive portal.

Ruby on Rails is the infrastructure used to implement the RWG captive portal. When customizing the captive portal, the operator has complete access to the underlying Ruby on Rails infrastructure.

In this section we will show simple modifications using **Partial override**, **Image override** and **Variable customization**.

For more information, please access the section **Portal Customization** at the RWG's embedded help on-line documentation.

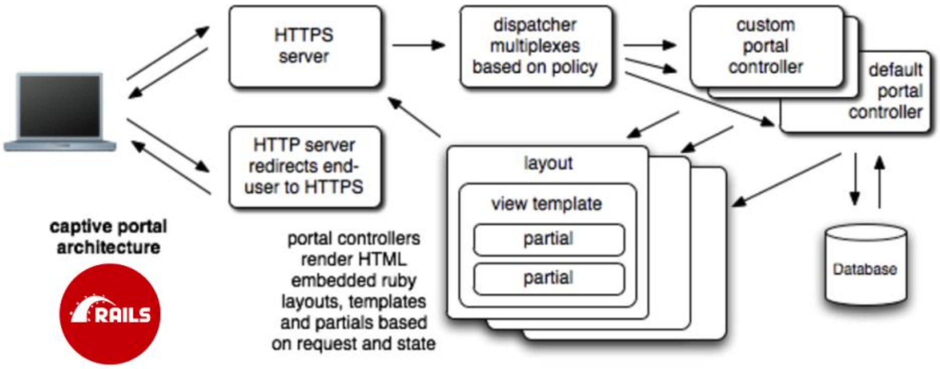
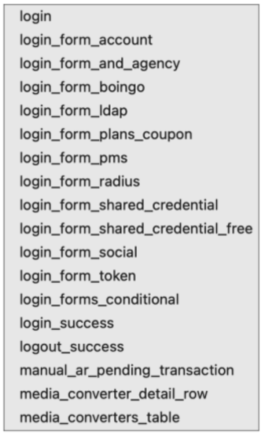

HTTPS server
dispatcher multiplexes based on policy
custom portal controller
default portal controller
HTTP server redirects end-user to HTTPS
layout
view template
partial
partial
Database
captive portal architecture
RAILS
portal controllers render HTML embedded ruby layouts, templates and partials based on request and state

FIGURE 43 – RUBY ON RAILS PORTALS ARCHITECTURE

Partial Override

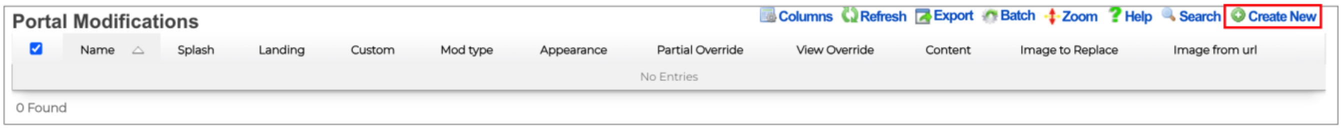
A **Partial Override** allows the operator to change only one part of a portal. There are partial overrides for every part of the portals. The diagram to the right shows some examples.



login
login_form_account
login_form_and_agency
login_form_boingo
login_form_ldap
login_form_plans_coupon
login_form_pms
login_form_radius
login_form_shared_credential
login_form_shared_credential_free
login_form_social
login_form_token
login_forms_conditional
login_success
logout_success
manual_ar_pending_transaction
media_converter_detail_row
media_converters_table

FIGURE 44 – EXAMPLES OF MODIFIABLE SECTIONS

Navigate to **System/Portals**, scroll down to **Portal Modifications,** and click **Create New**:



Portal Modifications

☑	Name	Splash	Landing	Custom	Mod type	Appearance	Partial Override	View Override	Content	Image to Replace	Image from url
							No Entries				

0 Found

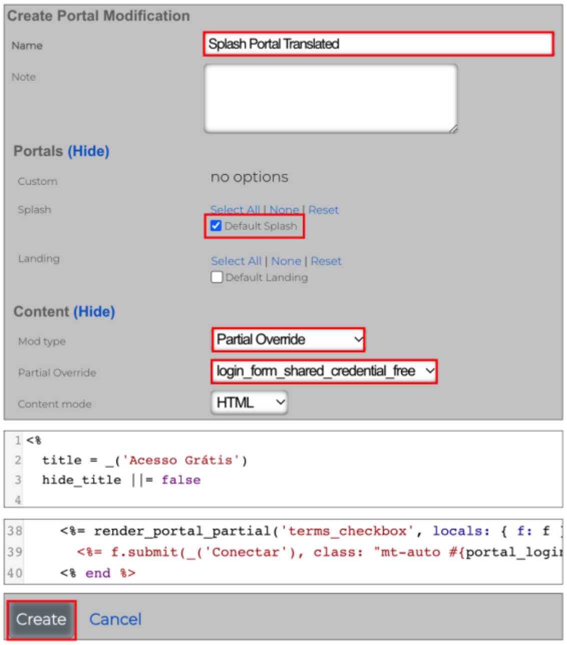
FIGURE 45 – PORTAL MODIFICATIONS

Enter the following information:

- **Name**: Enter a name for the modification.
- **Splash**: Mark the portals where the modification will be applied.
- **Landing**: Mark the portals where the modification will be applied.
- **Mod type**: Select **Partial Override**.
- **Partial Override**: Select **login_form_shared_credential_free.**

Scroll down and edit the template:

- **Line 2**: Remove the **||** before the equal sign and change the text.
- **Line 39**: Change the button text.



Create Portal Modification

Name: Splash Portal Translated

Note:

Portals (Hide)

Custom: no options

Splash: Select All | None | Reset
☑ Default Splash

Landing: Select All | None | Reset
□ Default Landing

Content (Hide)

Mod type: Partial Override

Partial Override: login_form_shared_credential_free

Content mode: HTML

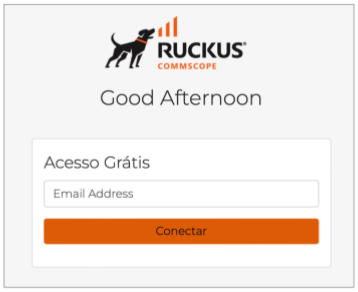
```
1 <%
2   title = _('Acesso Grátis')
3   hide_title ||= false
4
```

```
38     <%= render_portal_partial('terms_checkbox', locals: { f: f 
39       <%= f.submit(_('Conectar'), class: "mt-auto #{portal_logi
40     <% end %>
```

FIGURE 46 – PARTIAL OVERRIDE

Scroll down and click **Create**.

Here is the resulting splash portal:

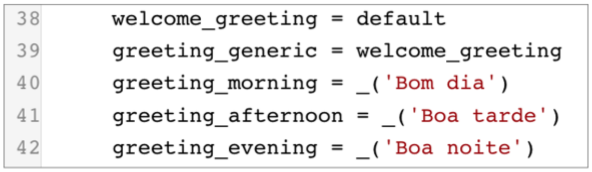


Good Afternoon

Acesso Grátis

FIGURE 47 – RESULTING PORTAL

If you want to change the greeting messages too, edit lines 40 – 42 in the partial **welcome_message**:



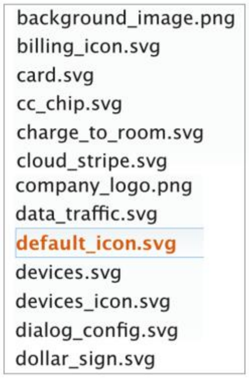
```
38      welcome_greeting = default
39      greeting_generic = welcome_greeting
40      greeting_morning = _('Bom dia')
41      greeting_afternoon = _('Boa tarde')
42      greeting_evening = _('Boa noite')
```

FIGURE 48 – CHANGE THE GREETING MESSAGES

If you wish to translate every text in all forms, please consult the **Internationalization** section under **Portal Customization** in the online help.

Image Override

Image overrides are used to change the background image or other image elements in the portal. A sample of the images that can be replaced is shown at the right.

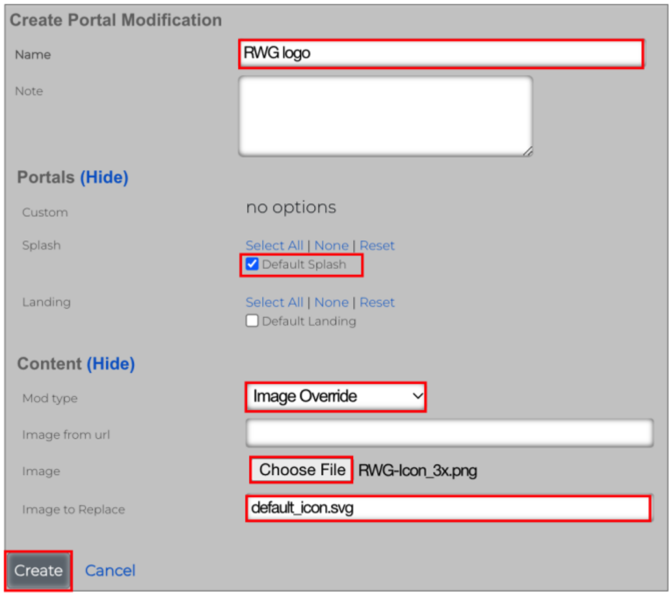


background_image.png
billing_icon.svg
card.svg
cc_chip.svg
charge_to_room.svg
cloud_stripe.svg
company_logo.png
data_traffic.svg
default_icon.svg
devices.svg
devices_icon.svg
dialog_config.svg
dollar_sign.svg

FIGURE 49 – EXAMPLES OF MODIFIABLE IMAGES

Navigate to **System/Portals**, scroll down to **Portal Modifications,** and click Create **New**. Enter the following information:

- **Name**: Enter a name for the modification
- **Splash**: Mark the portals where the modification will be applied.
- **Landing**: Mark the portals where the modification will be applied.
- **Mod type:** Select **Image Override**.
- **Image**: Select the file with the new image.
- **Image to Replace**: Select the image to replace. Here, we will change the logo that shows in the splash page.



Create Portal Modification

Name: RWG logo

Note:

Portals (Hide)

Custom: no options

Splash: Select All | None | Reset
☑ Default Splash

Landing: Select All | None | Reset
☐ Default Landing

Content (Hide)

Mod type: Image Override

Image from url:

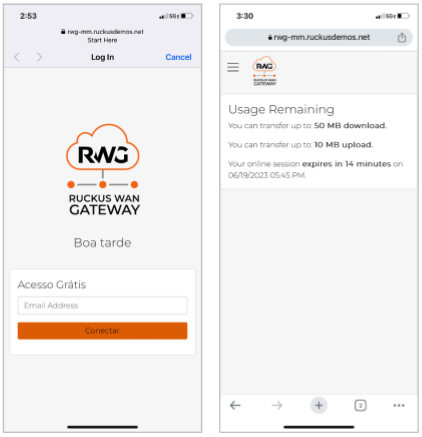
Image: Choose File RWG-Icon_3x.png

Image to Replace: default_icon.svg

FIGURE 50 – IMAGE OVERRIDE

Click **Create** to finish.

Here is the resulting portal:



Usage Remaining

You can transfer up to: **50 MB download.**

You can transfer up to: **10 MB upload.**

Your online session **expires in 14 minutes** on 06/19/2023 05:45 PM.

FIGURE 51 – PORTAL WITH NEW LOGO

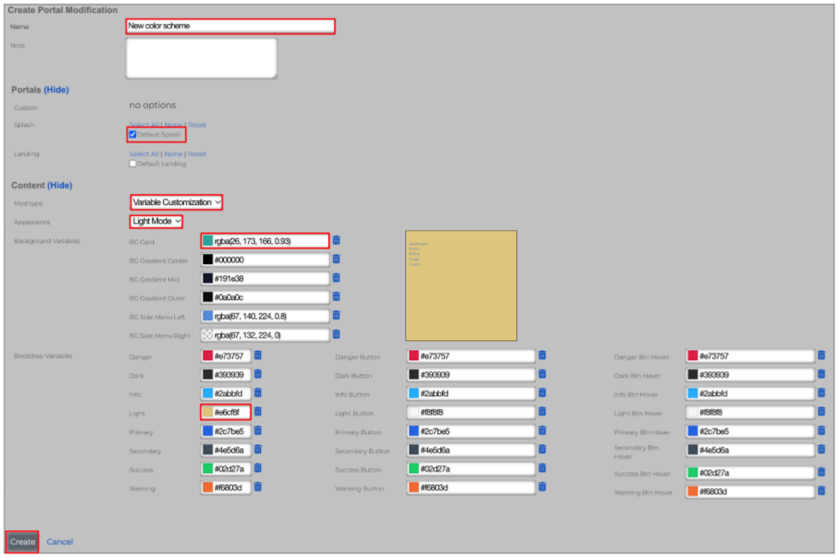
If you want to add a background image, select **background_image** at **Image to Replace**.

Variable Customization

Variable Customization allows the operator to change the color of any portal element or region. Enter the following information:

- **Name**: Enter a name for the modification.
- **Splash & Landing**: Mark the portals where the modification will be applied.
- **Mod type**: Select **Variable Customization**.
- **Appearance**: Select **Light Mode.**

In our example we changed the highlighted colors.



Create Portal Modification

Name: New color scheme

Note:

Portals (Hide)

Custom: no options

Splash: Select All | None | Reset
☑ Default Splash

Landing: Select All | None | Reset
☐ Default Landing

Content (Hide)

Mod type: Variable Customization

Appearance: Light Mode

Background Variables

BG Card	rgba(26, 173, 166, 0.93)
BG Gradient Center	#000000
BG Gradient Mid	#191e38
BG Gradient Outer	#0a0a0c
BG Side Menu Left	rgba(67, 140, 224, 0.8)
BG Side Menu Right	rgba(67, 132, 224, 0)

Bootstrap Variables

Danger	#e73757	Danger Button	#e73757	Danger Btn Hover	#e73757
Dark	#393939	Dark Button	#393939	Dark Btn Hover	#393939
Info	#2abbfd	Info Button	#2abbfd	Info Btn Hover	#2abbfd
Light	#e6cf8f	Light Button	#f8f8f8	Light Btn Hover	#f8f8f8
Primary	#2c7be5	Primary Button	#2c7be5	Primary Btn Hover	#2c7be5
Secondary	#4e5d6a	Secondary Button	#4e5d6a	Secondary Btn Hover	#4e5d6a
Success	#02d27a	Success Button	#02d27a	Success Btn Hover	#02d27a
Warning	#f6803d	Warning Button	#f6803d	Warning Btn Hover	#f6803d

FIGURE 52 – VARIABLE CUSTOMIZATION

Click **Create** to finish.

Here is the resulting splash portal:

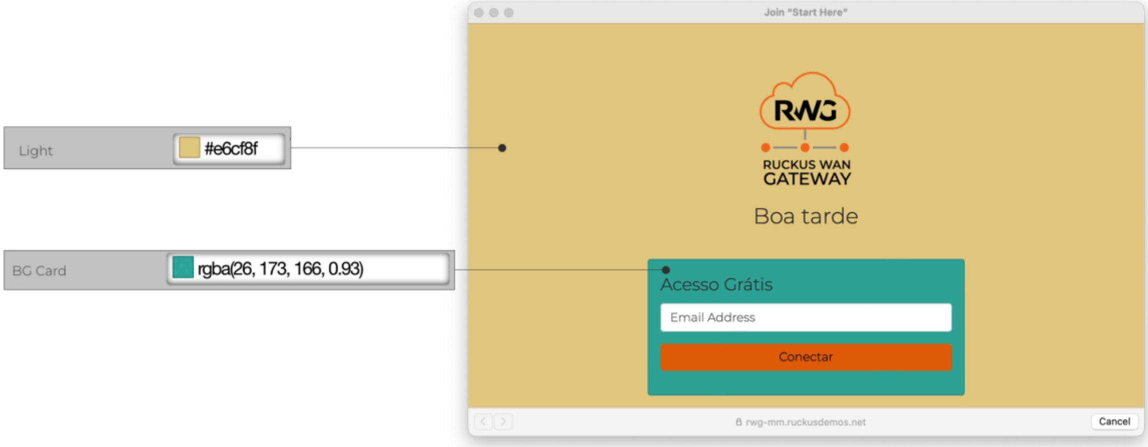


FIGURE 53 – SPLASH PORTAL WITH NEW COLORS

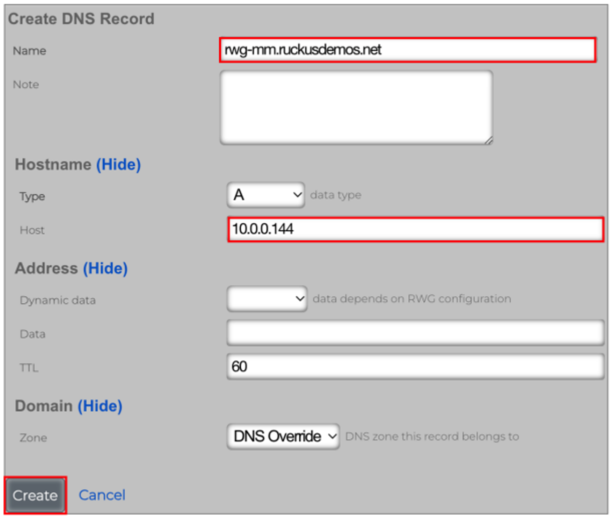
Troubleshooting

The Captive Portal Never Shows

If the client device associated to the WLAN, gets the correct VLAN and IP address, but it is never redirected to the captive portal, check the following:

- Is the RWG FQDN advertised in a public DNS? If not, navigate to **Services/DNS** and click **Create New** under **DNS Records** to add a DNS record for your RWG. You can use the WAN or LAN IP address for your RWG.
- Check if the splash portal is associated to the Pre-Auth/Guests policy.

You can use the command **tfpro | grep Redirecting** to see the redirections at the RWG console.



Create DNS Record

Name	rwg-mm.ruckusdemos.net
Note	

Hostname (Hide)

Type	A data type
Host	10.0.0.144

Address (Hide)

Dynamic data	data depends on RWG configuration
Data	
TTL	60

Domain (Hide)

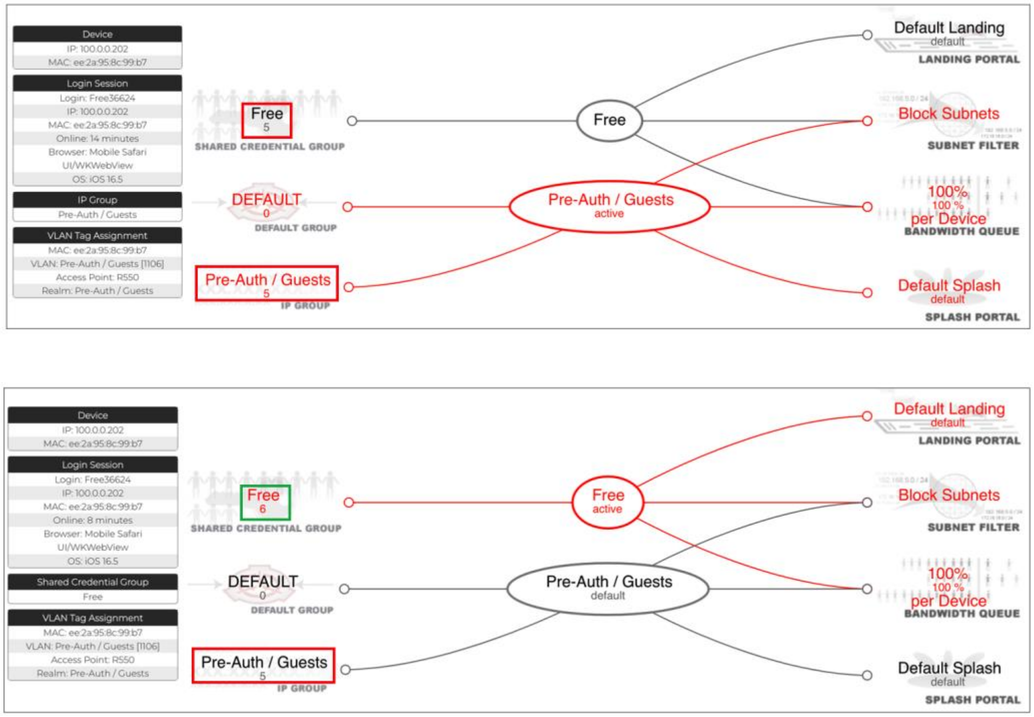
Zone	DNS Override DNS zone this record belongs to

FIGURE 54 – CREATE A DNS RECORD

No Internet Access

The device leaves the splash portal, but there is no internet access. Check the policies for the device:

- The top diagram shows a device without internet access. Notice that the priorities for the shared credential group and the IP group are the same (5). The device is stuck at the splash portal without network access.
- The bottom diagram shows a device with internet access. Notice that the priorities for the shared credential group is higher (6). The device has fully moved to the landing portal.



Device
IP: 100.0.0.202
MAC: ee:2a:95:8c:99:b7

Login Session
Login: Free36624
IP: 100.0.0.202
MAC: ee:2a:95:8c:99:b7
Online: 14 minutes
Browser: Mobile Safari UI/WKWebView
OS: iOS 16.5

IP Group
Pre-Auth / Guests

VLAN Tag Assignment
MAC: ee:2a:95:8c:99:b7
VLAN: Pre-Auth / Guests [1106]
Access Point: R550
Realm: Pre-Auth / Guests

Device
IP: 100.0.0.202
MAC: ee:2a:95:8c:99:b7

Login Session
Login: Free36624
IP: 100.0.0.202
MAC: ee:2a:95:8c:99:b7
Online: 8 minutes
Browser: Mobile Safari UI/WKWebView
OS: iOS 16.5

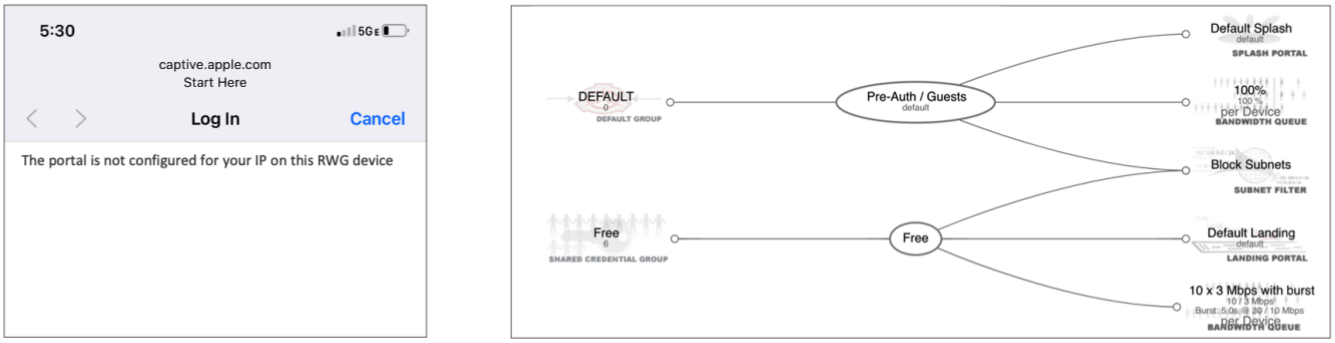
Shared Credential Group
Free

VLAN Tag Assignment
MAC: ee:2a:95:8c:99:b7
VLAN: Pre-Auth / Guests [1106]
Access Point: R550
Realm: Pre-Auth / Guests

FIGURE 55 – NO INTERNET ACCESS (TOP) AND GOOD INTERNET ACCESS (BOTTOM)

The Portal is not Configured for your IP on this RWG

The policy **Pre-Auth / Guests** is not using the IP group **Pre-Auth / Guests**.



The portal is not configured for your IP on this RWG device

FIGURE 56 – MISSING IP GROUP

Add the IP group **Pre-Auth / Guests** to the policy.

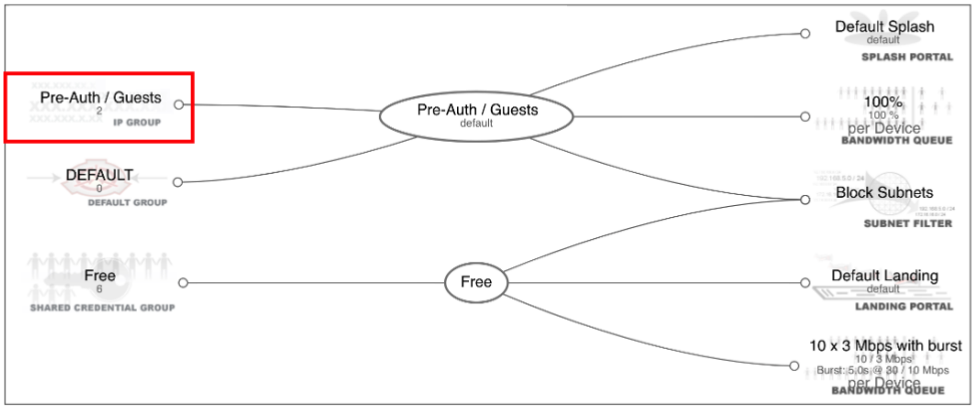
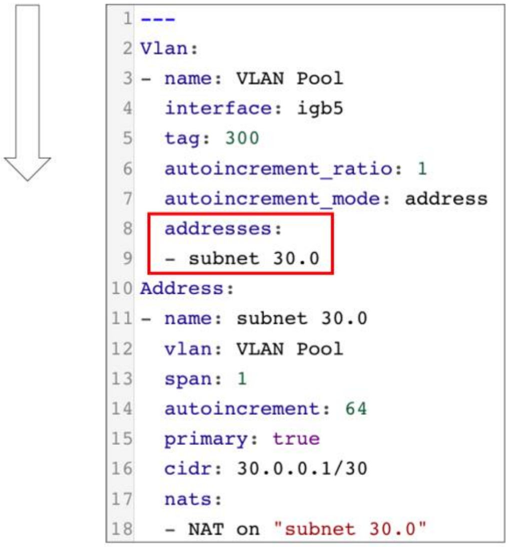


FIGURE 57 – IP GROUP IS ADDED

Common Config Template Error

A common error in a config template is to reference an object that is not created yet. The config template lines are executed in sequence, from top to bottom.

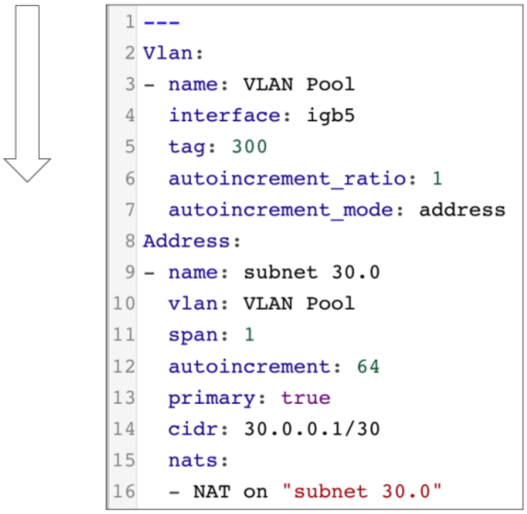
This template will fail, because **subnet 30.0** is being referenced by the VLAN section, but it was not created yet:



```
---
Vlan:
- name: VLAN Pool
  interface: igb5
  tag: 300
  autoincrement_ratio: 1
  autoincrement_mode: address
  addresses:
  - subnet 30.0
Address:
- name: subnet 30.0
  vlan: VLAN Pool
  span: 1
  autoincrement: 64
  primary: true
  cidr: 30.0.0.1/30
  nats:
  - NAT on "subnet 30.0"
```

FIGURE 58 – THIS TEMPLATE FAILS

This template will work:

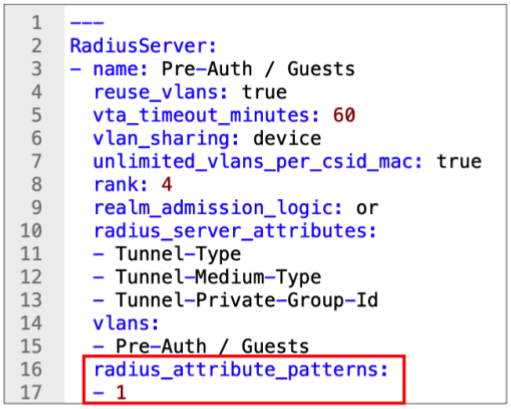


```
---
Vlan:
- name: VLAN Pool
  interface: igb5
  tag: 300
  autoincrement_ratio: 1
  autoincrement_mode: address
Address:
- name: subnet 30.0
  vlan: VLAN Pool
  span: 1
  autoincrement: 64
  primary: true
  cidr: 30.0.0.1/30
  nats:
  - NAT on "subnet 30.0"
```

FIGURE 59 – THIS TEMPLATE WORKS

RadiusServer Config Template Error

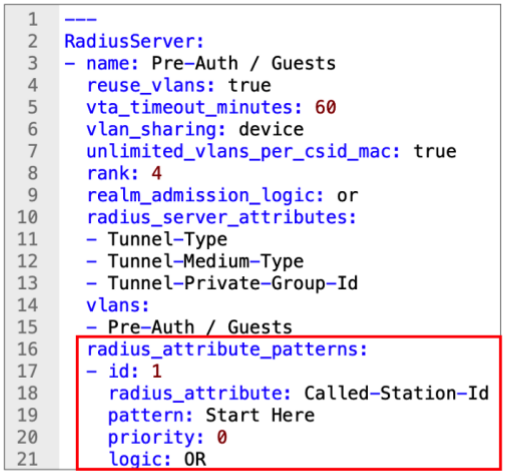
The template for the **Radius Server Realms** scaffold is exported using a child ID for the attribute patterns. It will fail if you try to apply this template back to RWG:



```
---
RadiusServer:
- name: Pre-Auth / Guests
  reuse_vlans: true
  vta_timeout_minutes: 60
  vlan_sharing: device
  unlimited_vlans_per_csid_mac: true
  rank: 4
  realm_admission_logic: or
  radius_server_attributes:
  - Tunnel-Type
  - Tunnel-Medium-Type
  - Tunnel-Private-Group-Id
  vlans:
  - Pre-Auth / Guests
  radius_attribute_patterns:
  - 1
```

Figure 60 – This Template Fails

Change the attribute patterns section like in this example:

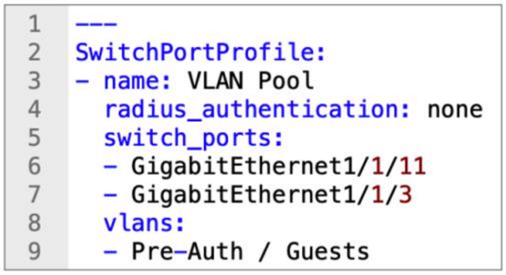


```
---
RadiusServer:
- name: Pre-Auth / Guests
  reuse_vlans: true
  vta_timeout_minutes: 60
  vlan_sharing: device
  unlimited_vlans_per_csid_mac: true
  rank: 4
  realm_admission_logic: or
  radius_server_attributes:
  - Tunnel-Type
  - Tunnel-Medium-Type
  - Tunnel-Private-Group-Id
  vlans:
  - Pre-Auth / Guests
  radius_attribute_patterns:
  - id: 1
    radius_attribute: Called-Station-Id
    pattern: Start Here
    priority: 0
    logic: OR
```

Figure 61 – This Template Works

SwitchPortProfile Template Error

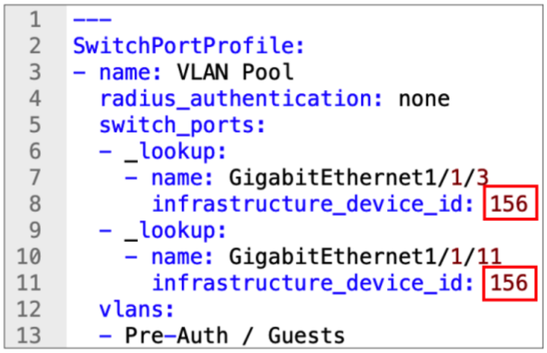
The template for the **Switch Port Profiles** scaffold is exported without the switch name. It will fail if you try to apply this template back to RWG when there are multiple ICX switches configured:



```
---
SwitchPortProfile:
- name: VLAN Pool
  radius_authentication: none
  switch_ports:
  - GigabitEthernet1/1/11
  - GigabitEthernet1/1/3
  vlans:
  - Pre-Auth / Guests
```

FIGURE 62 – THIS TEMPLATE FAILS

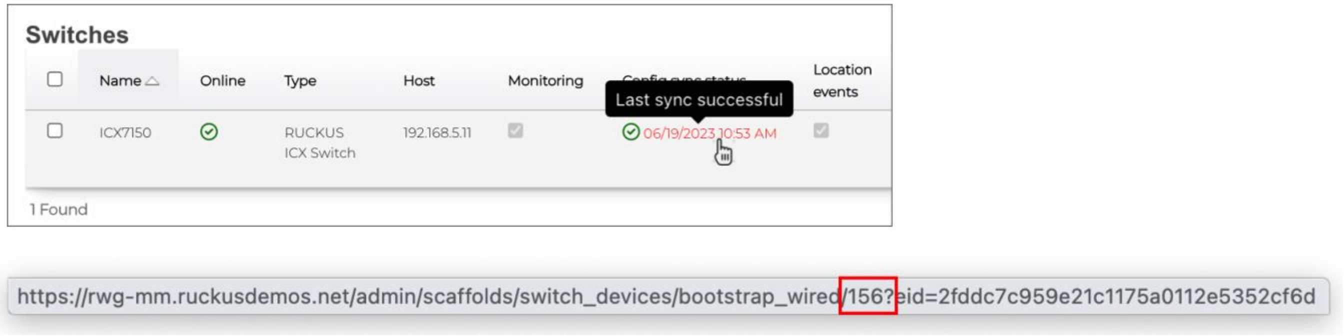
Change the template like in example below, where 156 is your **switch ID**:



```
---
SwitchPortProfile:
- name: VLAN Pool
  radius_authentication: none
  switch_ports:
  - _lookup:
    - name: GigabitEthernet1/1/3
      infrastructure_device_id: 156
  - _lookup:
    - name: GigabitEthernet1/1/11
      infrastructure_device_id: 156
  vlans:
  - Pre-Auth / Guests
```

FIGURE 63 – THIS TEMPLATE FAILS

To get your switch ID, hover your mouse over the sync message at the switch entry in the **Switches** scaffold. Get the ID from the URL at the bottom of the page:



Switches

□	Name △	Online	Type	Host	Monitoring	Config sync status	Location events
□	ICX7150	✓	RUCKUS ICX Switch	192.168.5.11	☑	✓ 06/19/2023 10:53 AM	☑

Last sync successful

1 Found

https://rwg-mm.ruckusdemos.net/admin/scaffolds/switch_devices/bootstrap_wired/156?eid=2fddc7c959e21c1175a0112e5352cf6d

FIGURE 64 – OBTAINING THE SWITCH ID

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.

RUCKUS®
COMMSCOPE