



# Deployment Guide

## **RUCKUS WAN Gateway – Basic Setup**

June 2023

Rev. 1

## Table of Contents

Changes in Revision 1 .....	3
<b>INTENDED AUDIENCE .....</b>	<b>3</b>
<b>OVERVIEW .....</b>	<b>4</b>
<b>SUPPORTED TOPOLOGIES.....</b>	<b>5</b>
Local RWG and SmartZone.....	5
Local RWG and Remote SmartZone .....	6
Local RWG and Remote SmartZone .....	7
Default Security Rules.....	8
<b>BASIC UI NAVIGATION.....</b>	<b>9</b>
Login and Logout .....	9
The RWG User Interface.....	10
RWG Shutdown .....	11
<b>SSH ACCESS .....</b>	<b>12</b>
Create a SSH Key Pair Using MacOS .....	13
Create a SSH Key Pair Using Termius .....	16
Create a SSH Key Pair Using PuTTYgen .....	19
<b>SSL CERTIFICATES .....</b>	<b>24</b>
<b>NETWORK TOPOLOGY DIAGRAMS.....</b>	<b>29</b>
<b>RWG SOFTWARE UPGRADE .....</b>	<b>32</b>
<b>RWG BACKUP AND RESTORE .....</b>	<b>35</b>
Backup .....	35
Restore .....	37
<b>CONFIG TEMPLATES .....</b>	<b>38</b>
Generate a Config Template for a Scaffold .....	38
Generate a Config Template for the Entire RWG .....	39
Upload, Test and Apply a Config Template.....	40
<b>BASIC TROUBLESHOOTING .....</b>	<b>43</b>
Instruments.....	43
Logs .....	44
Search Tool .....	46

## Changes in Revision 1

- Minor corrections and text changes.
- Added new location for RWG .ISO files.
- Added section on Config Templates.

## Intended Audience

This document shows supported topologies, basic navigation and step-by-step procedures to manage and configure the basic functions in RWG.

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

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 in the product.

You can access it by navigating to [https://{your RWG IP address}/admin/manual/help\\_online](https://{your RWG IP address}/admin/manual/help_online)

## Overview

This document includes the following sections:

- Supported Topologies
- Basic UI Navigation
- SSH Keys and SSH Access
- SSL Certificates
- Network Topology Diagrams
- RWG Software Upgrade
- RWG Backup and Restore
- Config Templates
- Basic Troubleshooting

## Supported Topologies

RWG stands for RUCKUS Wireless Gateway, and as such, it is a router running NAT and DHCP, plus a RADIUS server, NAC and many other services.

Its main usage is at the edge of an enterprise network, branch office, hotel property or MDU/MTU, where it can control the incoming and outgoing traffic, using packet filters and rate limiting, act as SD-WAN/VPN endpoint, and apply policies to the wireless and wired devices in the internal network.

Therefore, in most environments, RWG is installed locally, even though it is also possible to install it remotely for specific use cases. The SmartZone controller installation can be local or remote.

The next section shows the details for the supported topologies.

### Local RWG and SmartZone

In this topology RWG and SmartZone are local to the hotel property, MDU, enterprise network, etc.

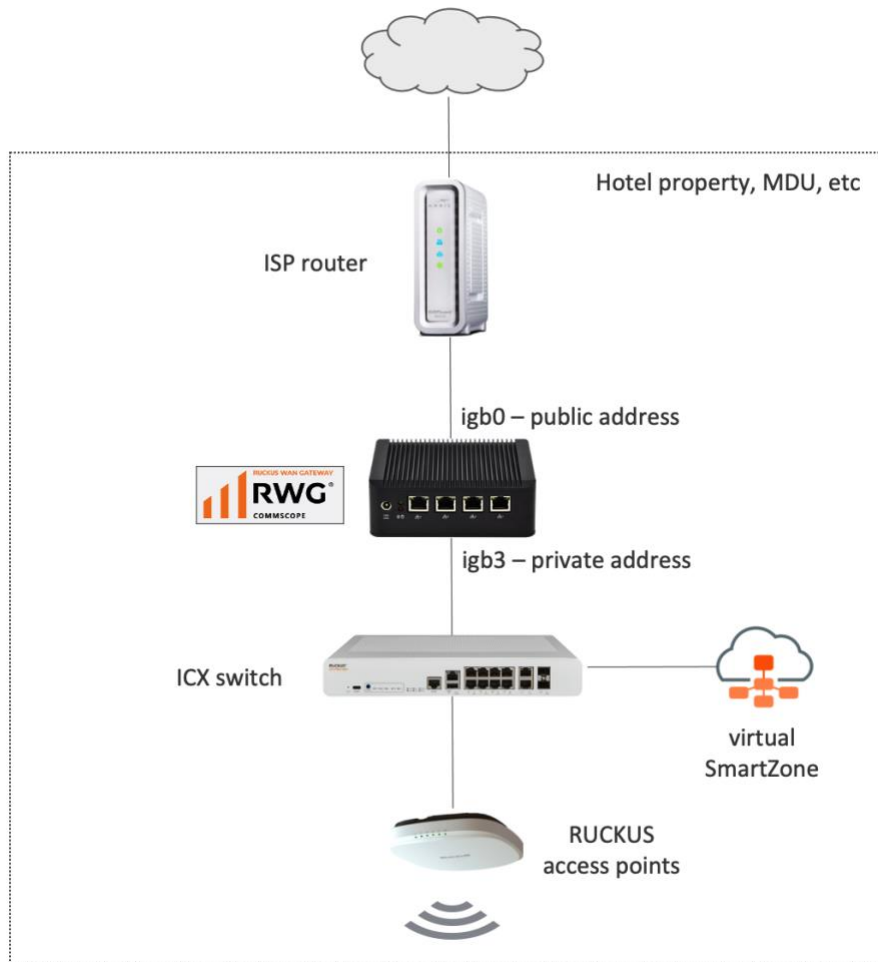


FIGURE 1 – LOCAL RWG AND SMARTZONE

RWG acquires a public IP address from the ISP router and provides private IP address to the devices and clients connected at the LAN side. Microsegmentation is fully supported, and its configuration is automated by RWG. The ICX switch and the SmartZone controller are configured by RWG automatically. SmartZone acts as a proxy authenticator, and RWG is the RADIUS/NAC server.

**Note:** It is possible to use a private IP address in the RWG WAN interface, but in that case SD-WAN features like IPsec VPNs may not work.

## Local RWG and Remote SmartZone

In this topology RWG is local and SmartZone is installed in a remote location.

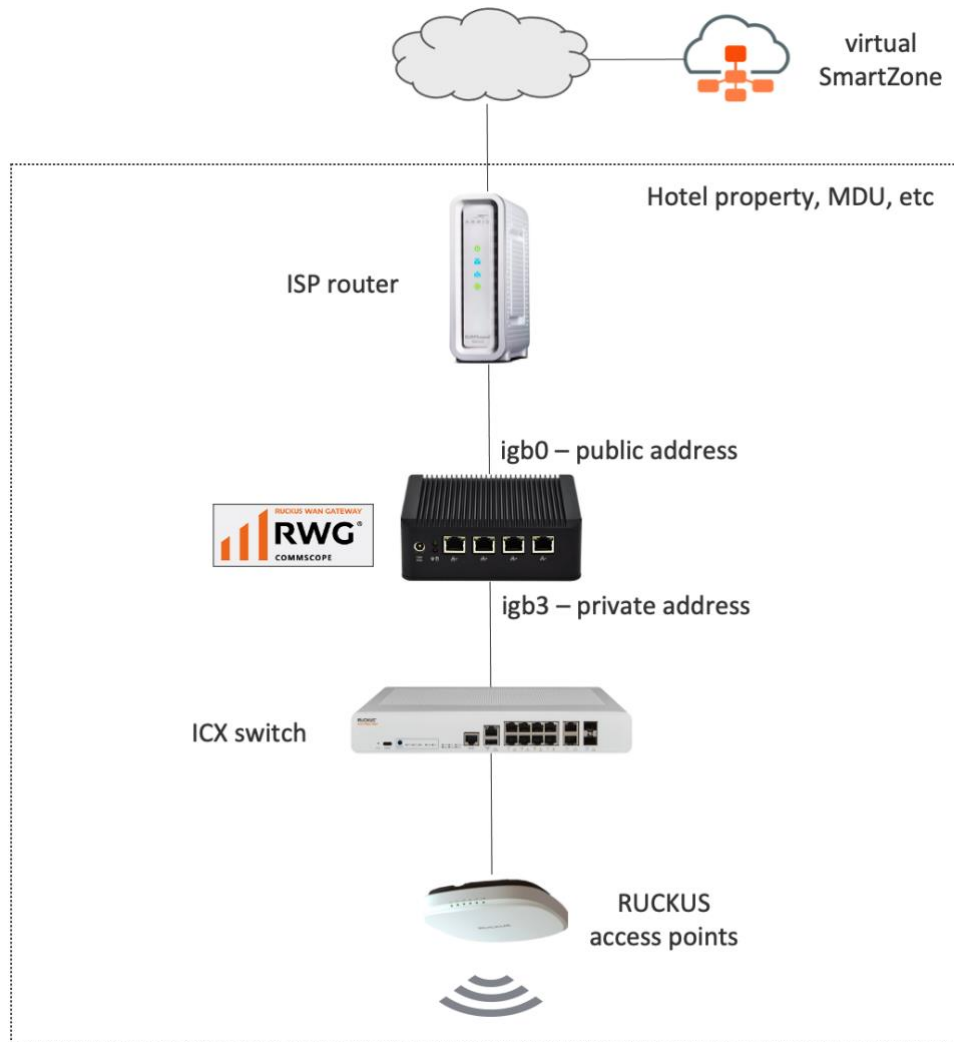


FIGURE 2 – LOCAL RWG AND REMOTE SMARTZONE

As with the previous topology, RWG acquires a public IP address from the ISP router and provides private IP address to the devices and clients connected at the LAN side. Microsegmentation is also fully supported, and its

configuration is fully automated by RWG. The ICX switch and the SmartZone controller are configured by RWG automatically. But in this topology, SmartZone acts as a non-proxy authenticator.

This topology will work equally well as the topology where RWG and SmartZone are local to the network.

## Local RWG and Remote SmartZone

In this topology both RWG and SmartZone are installed in a remote location.

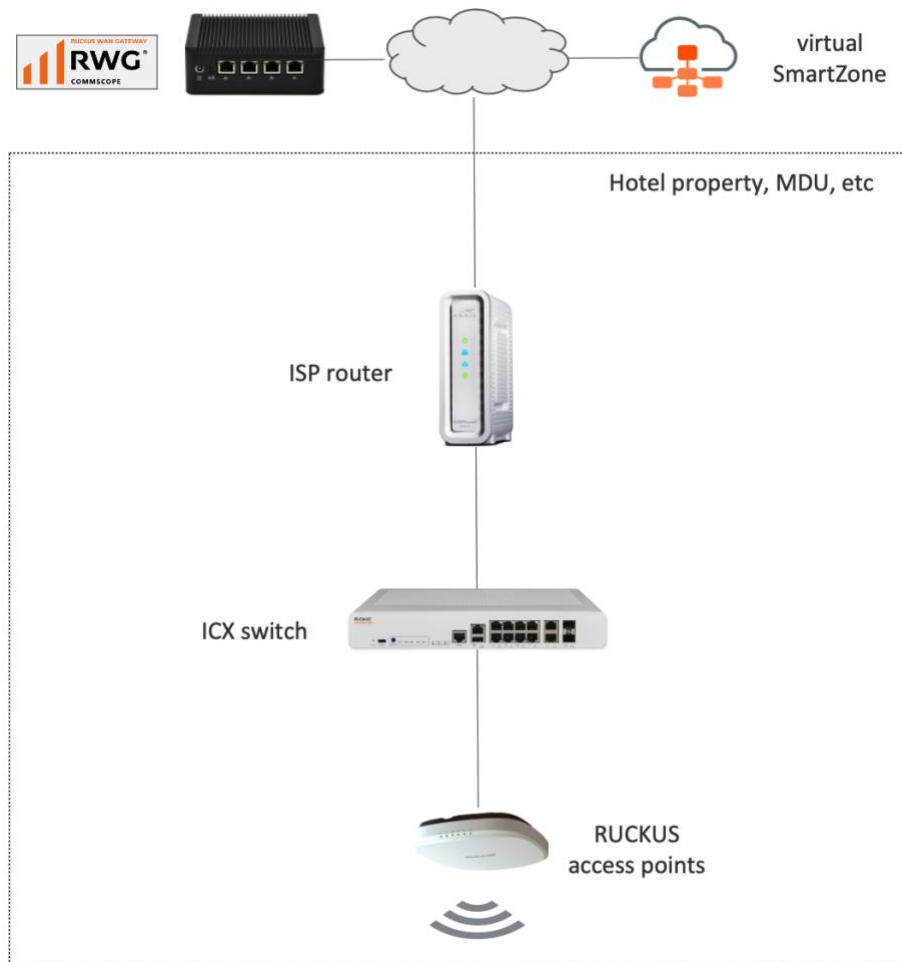


FIGURE 3 – REMOTE RWG AND REMOTE SMARTZONE

Microsegmentation is not supported when RWG is installed remotely. For every microsegmentation use case, RWG defines the VLAN assignments and the DHCP scopes used by the clients. The RADIUS response from RWG with the VLAN assignment will reach the wireless clients, but the client's DHCP request will fail, because there is a router between RWG and the client network. RWG does not have control on that router. The router would

need to be manually configured with DHCP helper services for all scopes provided by RWG, and that may not be feasible in many cases.

Apart from that, there are specific use cases that do not require microsegmentation – like providing simple WiFi access to the wireless clients using authentication portals and billing – and that is fully supported in this topology. Because SmartZone is also remote, it is configured as a non-proxy authenticator.

## Default Security Rules

A fresh installed RWG has a WAN and a LAN subnet, a NAT entry configured for the WAN uplink, a DHCP scope enabled for a LAN interface using the network 192.168.5.0/24, and a **Block Subnets** policy applied to all local subnets by default.

All traffic initiated from clients at the LAN side is allowed to go to the Internet, but if different subnets and DHCP scopes are created at the LAN side, the client traffic between any local subnets will be isolated.

If required, the block subnets policy can be disabled, or specific hosts can be whitelisted.

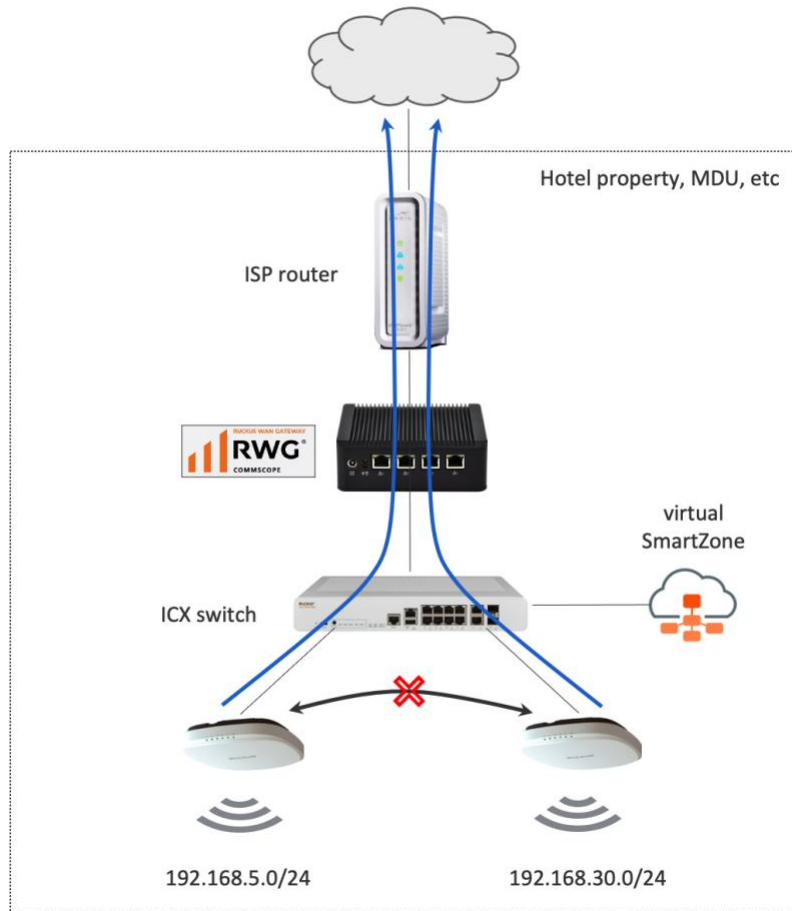


FIGURE 4 – DEFAULT SECURITY RULES



## Basic UI Navigation

### Login and Logout

To login to RWG, type [https://{RWG\\_ip\\_address}/admin](https://rwg-mm.ruckusdemos.net/admin) in your browser.

RWG does not have a default administrator account. One or more accounts should have been created during the RWG installation process. Enter the credentials and click **Authenticate** to login.

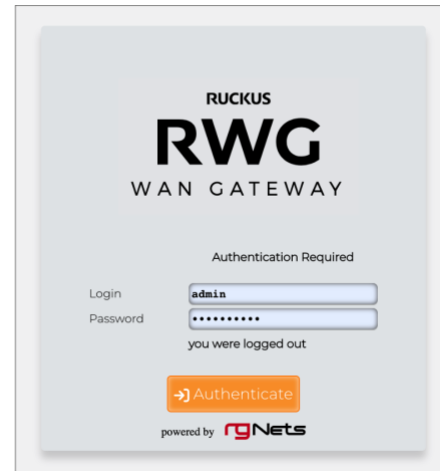
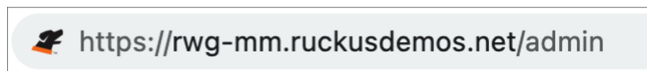


FIGURE 5 – RWG LOGIN

Right after login, the **Instruments** panel is shown. To logout, click **logout admin**.

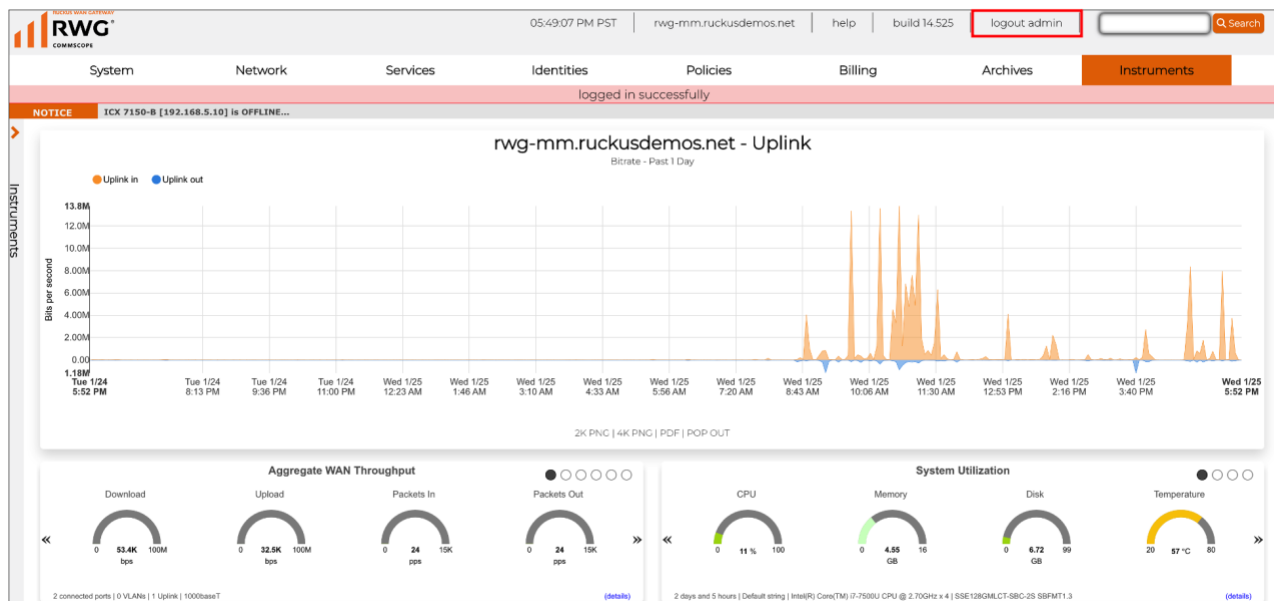


FIGURE 6 – LOGOUT

## The RWG User Interface

Navigation in the RWG UI starts at the top menu. The diagram below shows all menu options displayed at the same time.

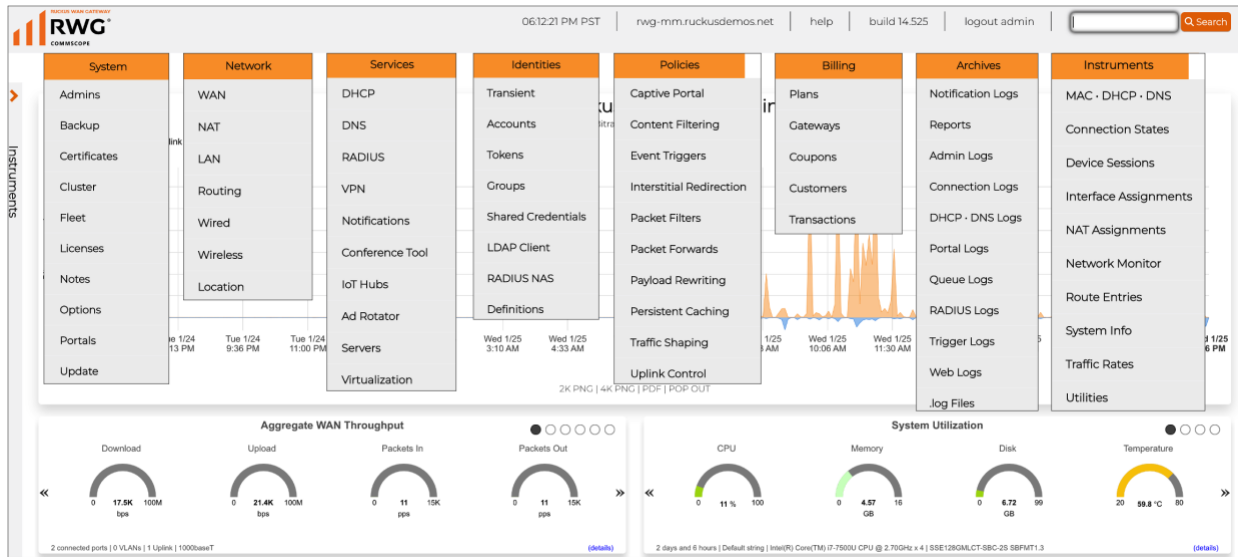


FIGURE 7 – RWG USER INTERFACE

RWG uses **scaffolds**. Scaffolds are the forms and tables used throughout the RWG user interface.

In the example below, we navigated to **Network/Wired**, and we see scaffolds for **Switches**, **Switch Fabrics**, **Switch Port Profiles** and **Switch Ports**.

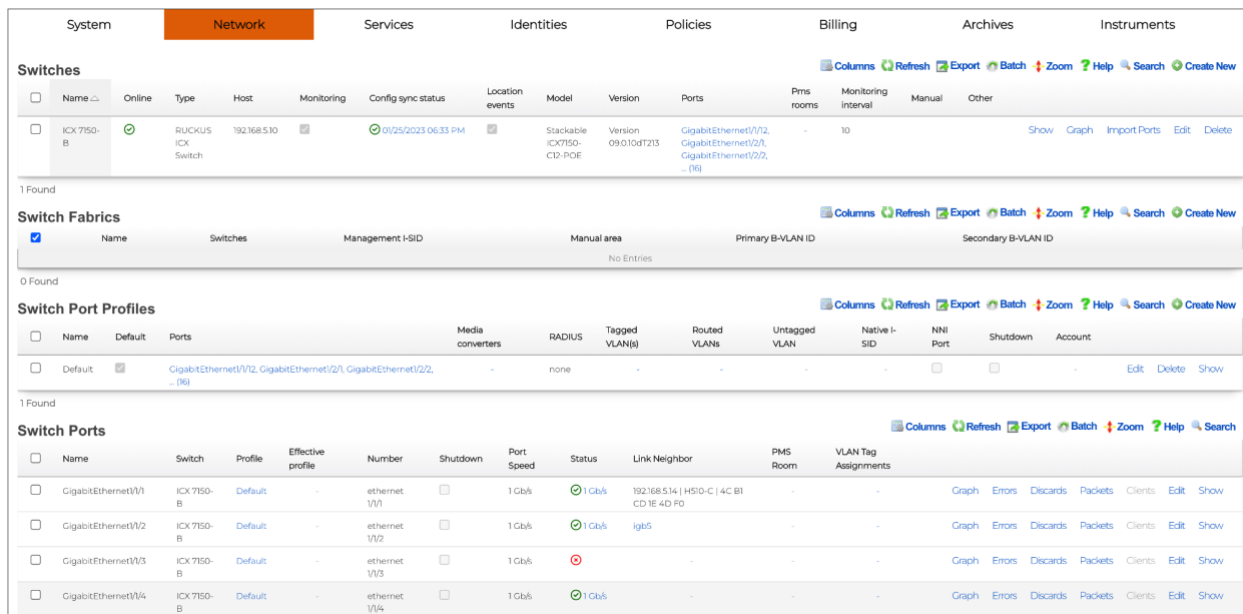


FIGURE 8 – RWG SCAFFOLDS

The most common scaffold options appear in this example:

VLAN Interfaces											Columns	Refresh	Export	Batch	Zoom	Help	Search	Create New
<input type="checkbox"/>	Name	Physical Interface	Service VLAN	Parent	VLAN IDs	I-SIDs	Autoincrement	Addresses	Switch Port Profiles	WLANs								
<input type="checkbox"/>	Client VLANs	igb3	-	igb3	400 - 463 (64)	-	1 tags per-subnet	Client Subnets	Client VLANs	micro, microseg		Graph	Edit	Delete	Show			
<input type="checkbox"/>	VLAN 200	igb3	-	igb3	200	-	-	Onboard Addresses	-	-		Graph	Edit	Delete	Show			
<input type="checkbox"/>	VLAN 500	igb3	-	igb3	500	-	-	VLAN 500 subnet	Client VLANs	-		Graph	Edit	Delete	Show			
<input type="checkbox"/>	VLAN 600	igb3	-	igb3	600	-	-	VLAN 600 subnet	Client VLANs	microseg, microDPSK		Graph	Edit	Delete	Show			
<input type="checkbox"/>	VLAN 700	igb3	-	igb3	700	-	-	VLAN 700 subnet	Client VLANs	microseg, microDPSK		Graph	Edit	Delete	Show			
<input type="checkbox"/>	VLAN 800	igb3	-	igb3	800	-	-	VLAN 800 subnet	-	-		Graph	Edit	Delete	Show			

6 Found

FIGURE 9 – THE VLAN INTERFACES SCAFFOLD

- **Columns:** Allows you to select which columns will be displayed in the table.
- **Refresh:** Click to refresh the items in the table.
- **Export:** Allows you to export the items in the table using .CSV, .XLSX or create config templates using YAML.
- **Batch:** Used to delete table items. Hover over **Destroy** to see **listed** or **marked**, to delete all items in the table or only the checked items.
- **Zoom:** Opens a new window to display the table only.
- **Help:** Shows a context-based help for the scaffold.
- **Search:** Allows you to filter items in the table. Only the items that match will show.
- **Create New:** Allows you to create a new item in the table.

## RWG Shutdown

If RWG is installed in bare metal, you can shutdown RWG by simply pressing the power on/power off button in the server, provided that this starts a graceful shutdown (i.e., the services and OS stops, the disks are unmounted, etc). Do not use the power on/power off button if it powers off the server immediately.

A safer way to do a shutdown is to click **System** at the top menu, then scroll down and click **Shutdown**.

### Backup History

Backup	Time	Size	Download
Daily Backup	3 hours ago	10.4 MB	<a href="#">download</a>
Daily Backup	01/24/2023 08...	12 MB	<a href="#">download</a>
Daily Backup	01/22/2023 04...	12.3 MB	<a href="#">download</a>

### System Switches

↻ Reboot

🗑 Factory Reset

🔌 Shutdown

FIGURE 10 – SHUTDOWN

## SSH Access

You need to install a public SSH key in RWG's administrator accounts in order to access the RWG console via SSH. Let's start by creating a new administrator. Navigate to **System/Administrator** and click **Create New**.

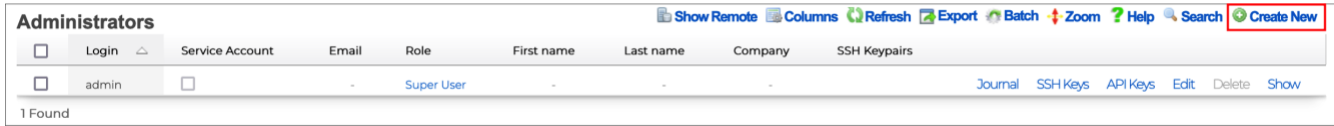


FIGURE 11 – CREATE A NEW ADMINISTRATOR ACCOUNT

The **Create Administrator** form will show:

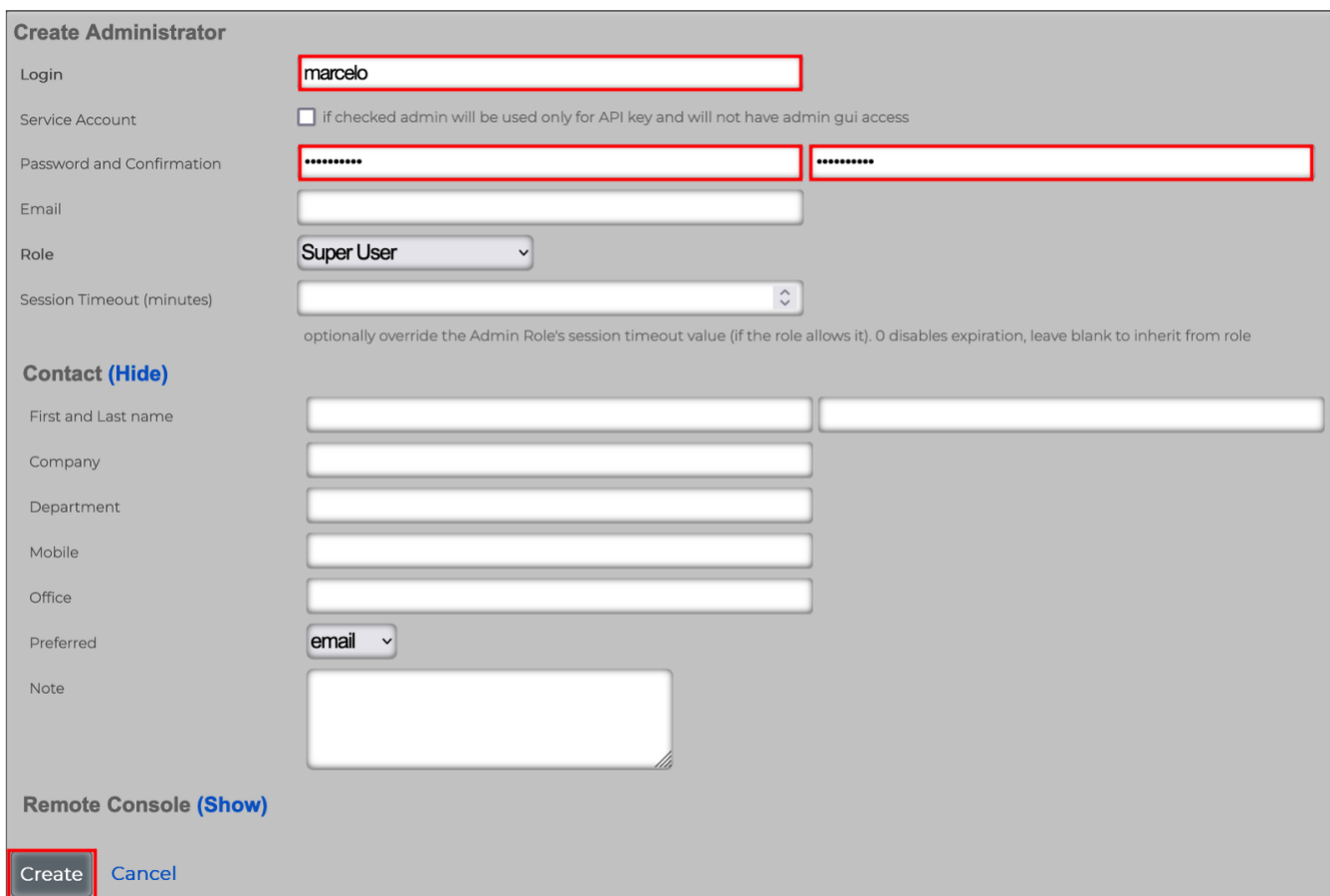


FIGURE 12 – CREATE ADMINISTRATOR

Enter the following information:

- **Login:** Enter a username
- **Password and Confirmation:** Enter the password.

Click **Create** to finish.

Let's now see three methods to create a SSH key pair:

- Using MacOS in a Mac computer
- Using Termius in a Mac computer
- Using PuTTYgen in Windows

## Create a SSH Key Pair Using MacOS

Open a terminal in your Mac computer and enter the command `ssh-keygen -b 4096 -t rsa`, then follow the instructions.

You can keep the proposed filename (`id_rsa`) and the passphrase (empty).

```

Marcelos-MacBook-Pro:home marcelo$ ssh-keygen -b 4096 -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/marcelo/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/marcelo/.ssh/id_rsa
Your public key has been saved in /Users/marcelo/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:FYtaYJnF46fMcvQz1z2Qovg2XUNbMfLixsYPHao112s marcelo@Marcelos-MacBook-Pro.local
The key's randomart image is:
+---[RSA 4096]-----+
|
|  o=. .
|  .o+.oo
|  .o=oo
|  . .o*. =
|  o o.OS% o
|  . o + ^ *
|  . o @ * o
|  + + E
|  .
+-----[SHA256]-----+
Marcelos-MacBook-Pro:home marcelo$
    
```

FIGURE 13 – CREATE THE SSH KEY PAIR

Use the command `cat /Users/marcelo/.ssh/id_rsa.pub` to see the public key and copy the entire string. Change the path to match your environment.

```

Marcelos-MacBook-Pro:home marcelo$ cat /Users/marcelo/.ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDW8BMidgspiF+B07WMfRrN16sMaPu1DIaro/IIk112AQ2H33J5EKI4WKUSxgWc6+VNVNXsg1Gp
75j14zuZNHK775qUkWkyP02yusiLh0RI2hfP0zWU1TdyvC31ZPkVHMor4KagC5qno+W2WE68WxVtrY0B7wiDs2JCeqGkFsK030KwZdCvc0brxgP6
0LT0tEHE5J26UjB1w8496baXXRtBCRXmbXHWufxRmv3ISaq+DsSrYNai6isnkspxGQVcCBf+tcfvfLNey+EwJvTPv4TLt1QtCIZQHvH8LNFXCcPy
/IeDHivJ6/q5Evr1kZqTMwHaHx+ApxMw6bqYKN//2nxK40kk9uzKcEAWzX6776HP8pxf/Y51RuXjjomYBvtk6AM84QRuyX0QfxLMyuV2U7IP1CT2
aLRUHIsluUZAGjVyiMiGDvzNlriBM0nDlxXUTUN0r+GxhO+P8kN+jURmpdeK7mATjdDubZTyHMv5fMwwICyf3W7Vdhga8I4cf19zNpMwnJq+jDN
XJmeSwBdHGF/SXRFpOTg1RYzNkGGmB+WVyjgeOHOUUSifyIamLzB50od6i1Mgs3a/VuoTERcqqps4L5BPd0vUqhY93gALsMK2dp4UtHpIpEgLN32
kCZY/8h7u05Zt1BNBqwnWYHOkcT8pdfS0den8tRSpGAFggcEjQ== marcelo@Marcelos-MacBook-Pro.local
    
```

FIGURE 14 – COPY THE PUBLIC KEY

Now, navigate to **System/Administrators** and click **Edit** on the entry where you wish to add the public key.

Administrators							Show Remote	Columns	Refresh	Export	Batch	Zoom	Help	Search	Create New
<input type="checkbox"/>	Login	Service Account	Role	First name	Last name	SSH Keypairs									
<input type="checkbox"/>	admin	<input type="checkbox"/>	Super User	-	-	admin key	Journal	SSH Keys	API Keys	Edit	Delete	Show			
<input type="checkbox"/>	marcelo	<input type="checkbox"/>	Super User	-	-		Journal	SSH Keys	Edit	Delete	Show				

FIGURE 15 – EDIT THE ADMINISTRATOR ACCOUNT

The update account form will show. Enter the following information:

- **Name:** Enter a name for the key
- **Public key:** Paste the public key you copied from the MacOS terminal.
- **Authorized for Admin login:** Make sure the checkbox is marked.

**Update marcelo**

Login:

Password and Confirmation:

Email:

Role:

Session Timeout (minutes):  optionally override the Admin Role's session timeout value (if the

**Contact (Hide)**

First and Last name:

Company:

Department:

Mobile:

Office:

Preferred:

Note:

**Remote Console (Hide)**

**SSH Keypairs (Hide)**

Name	Public key	Authorized for Admin login
<input type="text" value="RWG"/>	ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDW8BMIdgspIF+BO7WMfRrN16sMaP u1Dlaro/lk12AQ2H33J5EkI4WKUSxgWc6+VNVNXsglGp75j4zuZNHK775qUKWk yP02yusiLhORl2hFPOzWU1TdyvC31ZPkvhMor4KagC5qno+W2WE68WxvTrY0B7 wiDs2JCeQGkFsK03OKwZdCvcObrxgP60LT0tEHE5J26UJb1w84966baXXRtBCRX mbXHWufxRmV3lSaq+DsSrYNai6isnkspxGXQVcCBf+tcvfl_Ney+EwJvTPv4TLlQlCI ZQHvH8LNFxCCPy/lDHLvJ6/q5EvrlkZqTMwHaHx+ApxMW6bqYKN //2nxK4Okk9uzKcEAWzX6776HP8pxf /Y51RuXjomYBvtk6AM84QRuyXOQfxLMyuV2U7IPICT2aLRUHISLuUZAGjVyIMIG DvzNLrIBM0nDlxXUTUNOr+GxhO+P8kn+jURmpdeK7mATjdDubZTyHMv5fMwwj	<input checked="" type="checkbox"/>

Allow this key to log in as the admin via SSH

FIGURE 16 – UPDATE THE ACCOUNT

Click **Update** to finish.

Using the account where you copied the public key, connect from a MacOS terminal using the command  
`ssh username@FQDN-or-IP-address`

```
Marcelos-MacBook-Pro:~ marcelo$ ssh marcelo@10.0.0.144
The authenticity of host '10.0.0.144 (10.0.0.144)' can't be established.
ED25519 key fingerprint is SHA256:YdrzGctyybNeDSvhprgqJR909c0mxuVSHFFCxPSH7hA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.144' (ED25519) to the list of known hosts.

WARNING
-----
YOU CAN EASILY BREAK THINGS HERE

*****

CLI access is for troubleshooting and advanced integration only.
Please use the web GUI for all normal administrative operations.
https://rwg-mm.ruckusdemos.net/admin

*****
```

FIGURE 17 – SSH CONNECTION TO RWG

## Create a SSH Key Pair Using Termius

Termius is a popular SSH client for Mac computers.

At the Mac's top menu, select **Termius/Settings/Keychain**, then click **NEW/Generate new key**:

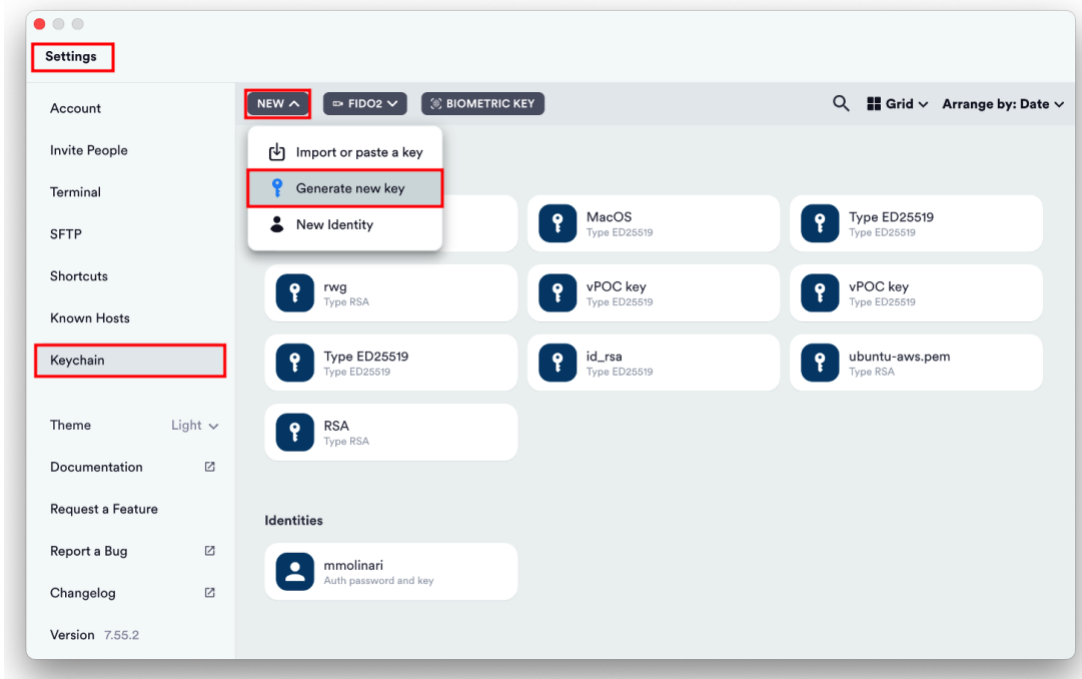


FIGURE 18 – GENERATE SSH KEYS USING TERMIUS

Enter the following information:

- **Label:** Enter a name for the key
- **Key type:** Select **RSA**
- **Key size (bits):** Select **4096**

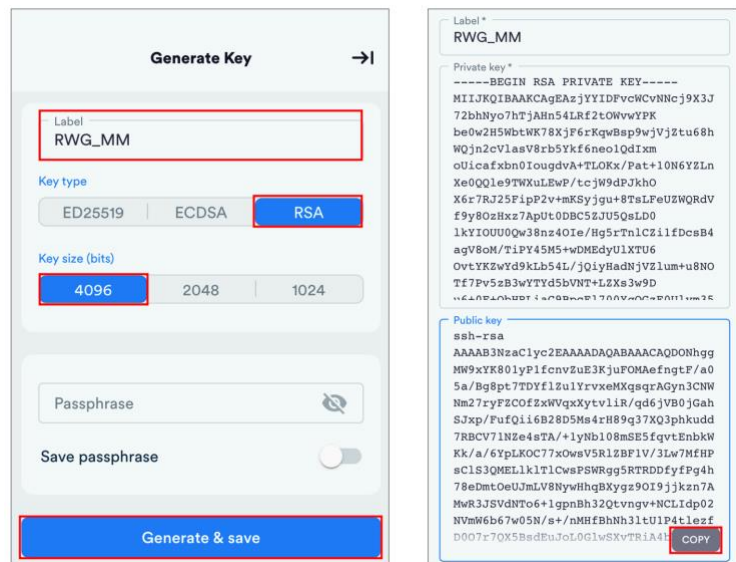


FIGURE 19 – GENERATE KEY AND COPY THE PUBLIC KEY

Click **Generate & save** to finish, then copy the public key using the **COPY** button.



Now, navigate to **System/Administrators** and click **Edit** on the entry where you wish to add the public key.

Administrators										
<input type="checkbox"/> Select All   <input type="checkbox"/> Select None										
<input checked="" type="checkbox"/> Login <input checked="" type="checkbox"/> Service Account <input type="checkbox"/> Email <input checked="" type="checkbox"/> Admin Role <input type="checkbox"/> First Name <input type="checkbox"/> Last Name <input type="checkbox"/> Company <input checked="" type="checkbox"/> Ssh Keypairs										
<input type="checkbox"/>	Login	Service Account	Role	SSH Keypairs						
<input type="checkbox"/>	admin	<input type="checkbox"/>	Super User	admin key	Journal	SSH Keys	API Keys	Edit	Delete	Show
<input type="checkbox"/>	marcelo	<input type="checkbox"/>	Super User	RWG	Journal	SSH Keys		Edit	Delete	Show
<input type="checkbox"/>	sheldon	<input type="checkbox"/>	Super User		Journal	SSH Keys		<b>Edit</b>	Delete	Show

FIGURE 20 – EDIT THE ADMINISTRATOR ACCOUNT

The update account form will show. Enter the following information:

- **Name:** Enter a name for the key
- **Public key:** Paste the public key you copied from Termius.
- **Authorized for Admin login:** Make sure the checkbox is marked.

### Update sheldon

Login:

Password and Confirmation:

Email:

Role:

Session Timeout (minutes):  optionally override the Admin Role's session timeout value (if the

**Contact (Hide)**

First and Last name:

Company:

Department:

Mobile:

Office:

Preferred:

Note:

**Remote Console (Hide)**

**SSH Keypairs (Hide)**

Name	Public key	Authorized for Admin login
<input type="text" value="RWG-Termius"/>	<pre>39fnBza95dpHFtJi69COV1cY2LxPIXJglu7jkSxvPJ0y0cHaJCJ0gU24nHdUE5C K1Fbt8aqsZRuElmDbzvVNV4vdOIOY91efLwAt8reju6q9oNKabo4p2EAd8YKyqHb Qlhk0X38BBJGjasbxOspjrpeMYPsLwU+7jsKyhZYAv605C4mi8rYZOHCsKuUQI45 /F9b79jNIEJ+ShUyVAk+ns1P/5k9Vwu+VUCBn+JXhIY29bL:ECwFjPYTzJPw8 8PT+EEUpUTel8rHL+EnR1jqUVxZiAZhS3u3TB6bit74l9ds2pqCRw5zQC3f7xg KZ0gmCSkeYHXDFnL++d kAPgU40C6Z1tEbx54kJO8wqVZNaNpHddjCujlb9okadqhAD9ASbABlxEGmRzKB nscb+9xB0wcTopJOLMTyNqzJ1kQHT7ZdCLIBQP3vk8CVjk8PTQ== Generated By Termius</pre>	<input checked="" type="checkbox"/>

Allow this key to log in as the admin via SSH

Create Another SSH Keypair

FIGURE 21 – UPDATE THE ACCOUNT

Click **Update** to finish.

On Termius, click **Hosts/Add/New Host**, then enter the following information:

- **Label:** Enter a name for the host
  - **Address:** Enter the IP address or FQDN
  - **SSH:** Make sure SSH is on
  - **Username:** Enter the account in RWG where the public key was copied
  - **Set a Key:** Click and select the SSH key pair you created earlier.
- The host profile will be saved automatically.

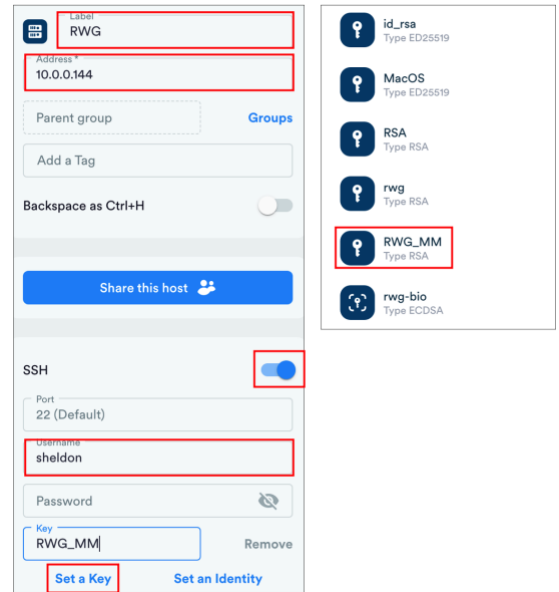


FIGURE 22 – CREATE A NEW HOST IN TERMIUS

Click on the host profile at the Termius main panel to connect to RWG:

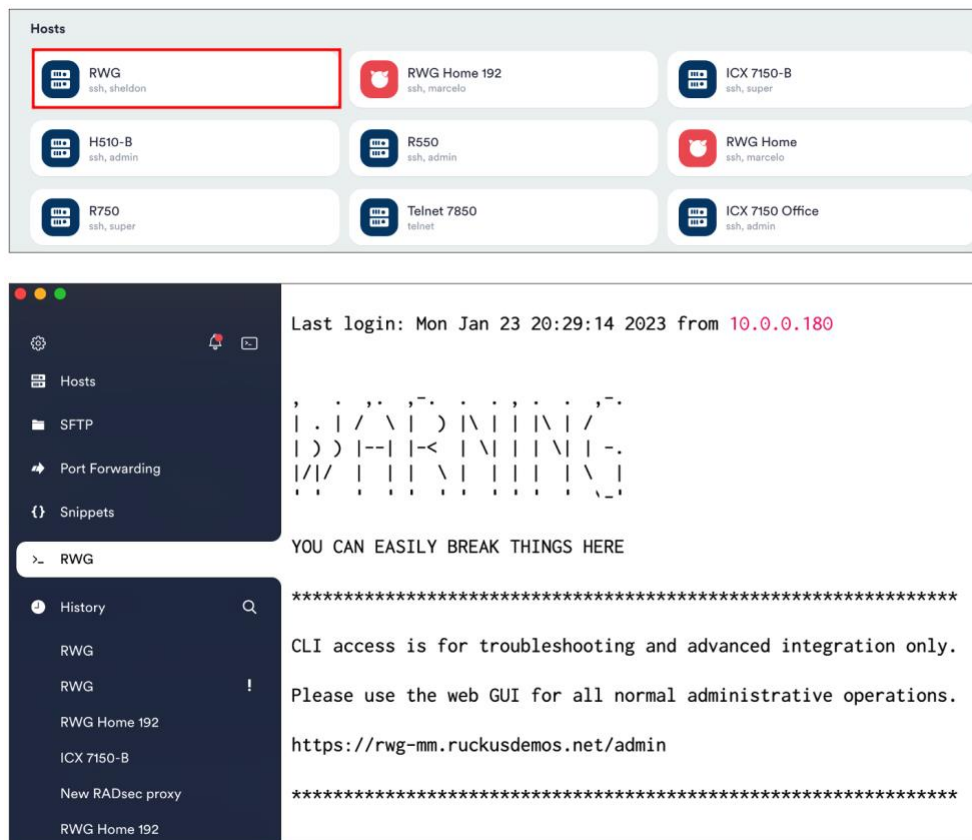


FIGURE 23 – SSH CONNECTION TO RWG

### Create a SSH Key Pair Using PuTTYgen

PuTTY and PuTTYgen are popular SSH tools used in Windows computers. Type `puttygen` in the search field at the Windows bar to invoke PuTTYgen.

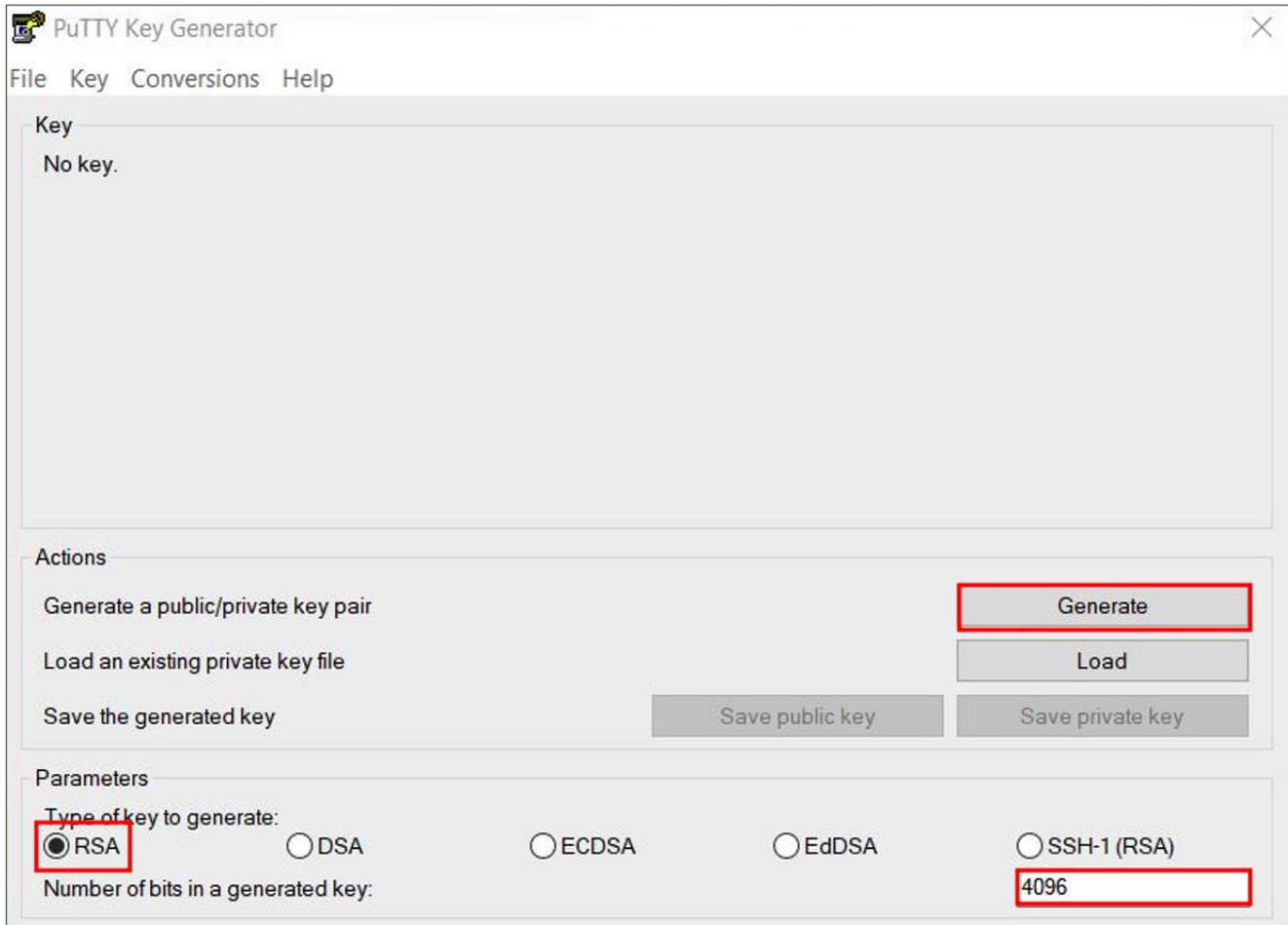


FIGURE 24 – CREATE A SSH KEY USING PUTTYGEN

Select **RSA** and enter **4096**, then click **Generate**.

Move your mouse over the blank area to randomize the creation of the key pair.

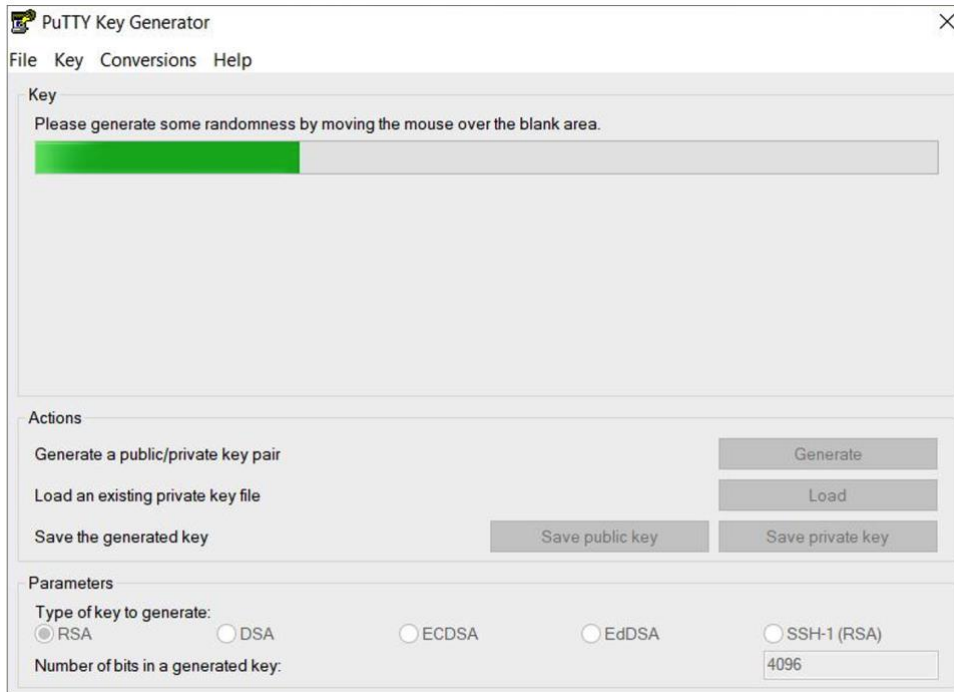


FIGURE 25— CREATE SOME RANDOMNESS

After the key pair is created, click **Save public key** and **Save private key** to save them in your computer.

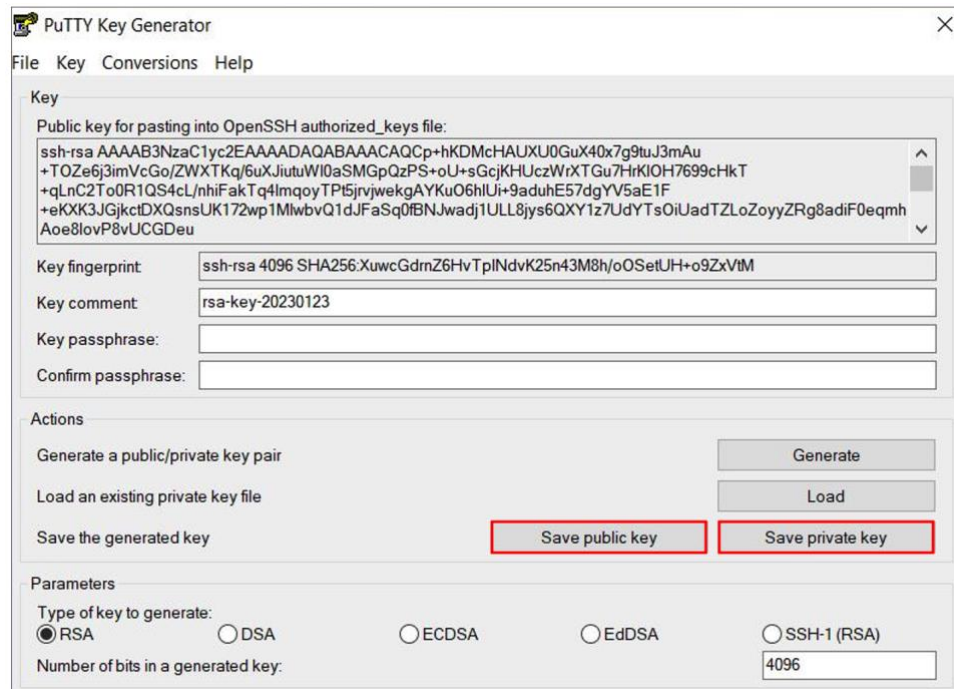


FIGURE 26 – SAVE BOTH KEYS

Open the file for the public key and copy its entire content.

Navigate to **System/Administrators** and click **Edit** on the entry where you wish to add the public key.

Administrators							<a href="#">Show Remote</a>	<a href="#">Columns</a>	<a href="#">Refresh</a>	<a href="#">Export</a>	<a href="#">Batch</a>	<a href="#">Zoom</a>	<a href="#">Help</a>	<a href="#">Search</a>	<a href="#">Create New</a>
<input type="checkbox"/>	Login	Email	Role	First name	Last name	SSH Keypairs									
<input type="checkbox"/>	admin	-	Super User	-	-	admin key	Journal	SSH Keys	API Keys	Edit	Delete	Show			
<input type="checkbox"/>	marcelo	-	Super User	-	-	RWG	Journal	SSH Keys		Edit	Delete	Show			
<input type="checkbox"/>	sheldon	-	Super User	-	-	RWG-Termius	Journal	SSH Keys		Edit	Delete	Show			
<input type="checkbox"/>	simone	-	Super User	-	-		Journal	SSH Keys		<b>Edit</b>	Delete	Show			

4 Found

FIGURE 27 – EDIT THE ADMINISTRATOR ACCOUNT

Enter the following information:

- **Name:** Enter a name for the key
- **Public key:** Paste the public key you copied from the file.
- **Authorized for Admin login:** Make sure the checkbox is marked.

### Update simone

Login:

Password and Confirmation:

Email:

Role:

Session Timeout (minutes):  optionally override the Admin Role's session timeout value (if the

**Contact (Hide)**

First and Last name:

Company:

Department:

Mobile:

Office:

Preferred:

Note:

**Remote Console (Hide)**

**SSH Keypairs (Hide)**

Name	Public key	Authorized for Admin login
<input type="text" value="RWG-Putty"/>	<pre> ----- BEGIN SSH2 PUBLIC KEY ----- Comment: "rsa-key-20230123" AAAAB3NzaC1yc2EAAAADAQABAAQCAQCp+hKDMcHAUXU0GuX40x7g9tuJ3m Au+TOZ e6j3mVcGo/ZWXTKg /buXJiutuWi0aSMGpQzPS+oU+sGcjKHUczWXTGu7HrKIOH 7699cHKT+qLnC2ToR1QS4cL/nhIFakTq4ImqoyTPf5jrvjwekAYKuO6hUI+9a duhE57dgYV5aE1F+eKXK3JGjktDXQsnsUK172wp1MlwvQ1dJFaSq0fBNJwadj1 ULL8jys6QXY1z7UdYTsOIUadTZLoZoyyZRg8adiF0eqmhAoe8lovP8vUCGDeu+FK VIU76mZoCzC5586L/Gp6O9L1FDiFeSpmPc0ncFEPwNRptaPyM3Og9w5+pRNjL                     </pre>	<input checked="" type="checkbox"/>

Allow this key to log in as the admin via SSH

[Create Another SSH Keypair](#)

FIGURE 28 – UPDATE ACCOUNT

Click **Update** to finish.

Type **putty** in the search field at the Windows bar to invoke PuTTY.

Click **Session** and enter the FQDN or IP address for your RWG instance.

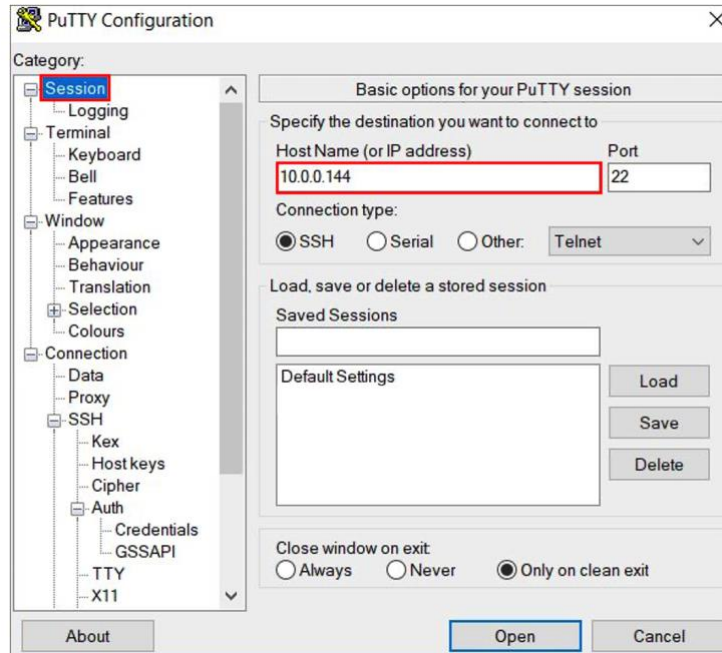


FIGURE 29 – PUTTY CONFIGURATION

Click **Data** and enter the account name in RWG where the public key was copied.

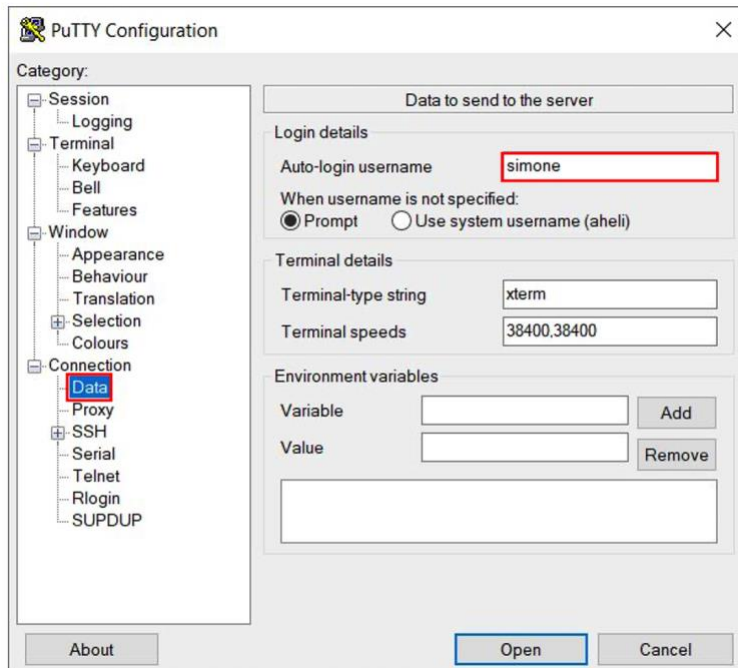


FIGURE 30 – ENTER THE ACCOUNT NAME

Click **Credentials** then click **Browse...** and select the file you saved earlier with the private key.

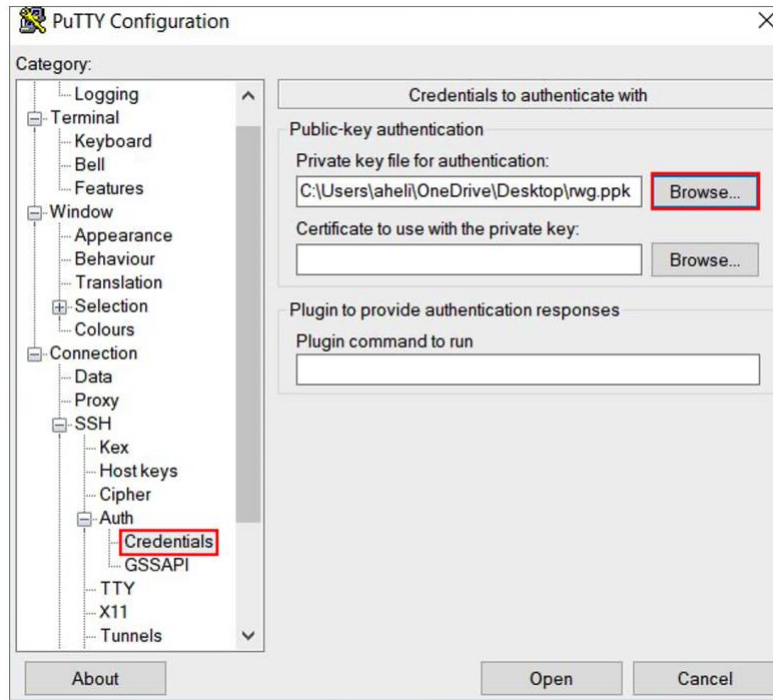


FIGURE 31 – ADD THE PRIVATE KEY

Go back to **Session**, then enter a name for the session and click **Save** to save the configuration.

Finally, click **Open** to connect to RWG. Click **Accept** to continue.

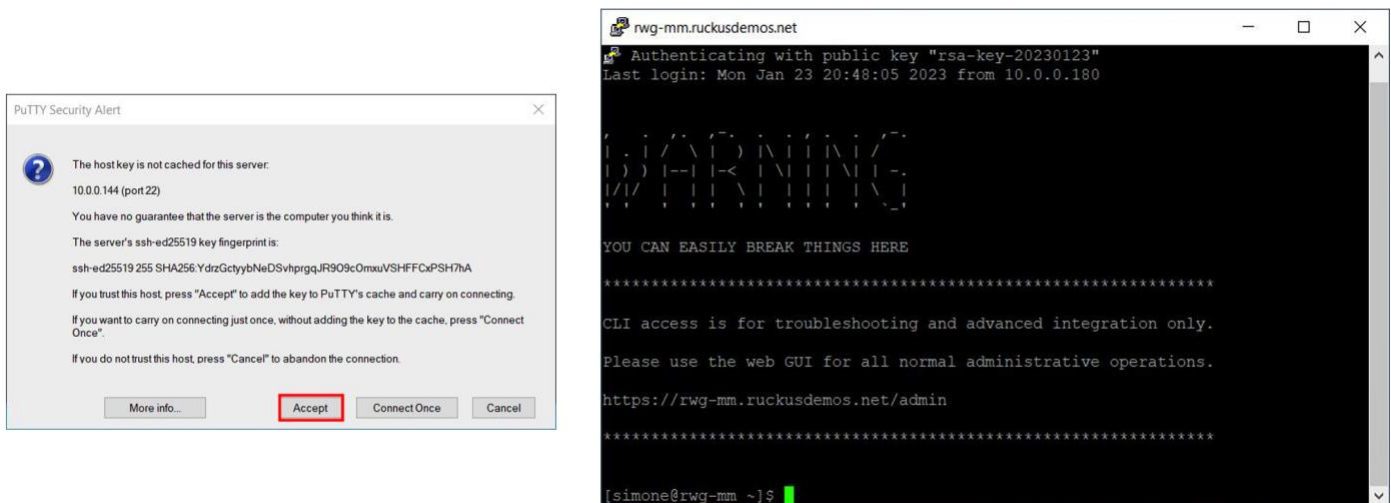


FIGURE 32 – SSH CONNECTION TO RWG

## SSL Certificates

RWG comes with a self-signed SSL certificate. For production networks you will need a valid certificate. It's recommended that a non-wildcard certificate be used. Some Windows computers might not work correctly when using 802.1X-EAP, if RWG is configured with a wildcard certificate.

You can generate a CSR request from RWG directly. Your RWG instance needs to have a public DNS entry before you start the CSR request.

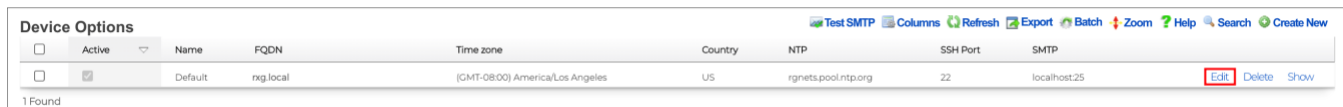
In our example RWG will send the CSR to **Let's Encrypt**. Let's Encrypt offers free SSL certificates with the following limitations:

- The certificate expires after 3 months (but it is renewed by RWG automatically).
- Let's Encrypt rate-limits the certificate renewals. Large service providers with hundreds of SSL certificates will not be able to use Let's Encrypt.
- The security level of the Let's Encrypt certificates is not adequate for PCI transactions.

For large deployments, or for use cases not covered by Let's Encrypt, simply generate the CSR in RWG, then download the CSR and send it to your preferred certificate issuer.

After you have a public DNS entry set and published for your RWG, you need to change the RWG FQDN. By default, RWG's FQDN is **rxg.local**.

Navigate to **System/Options**, then click **Edit** in the **Default** entry at the section **Device Options**.

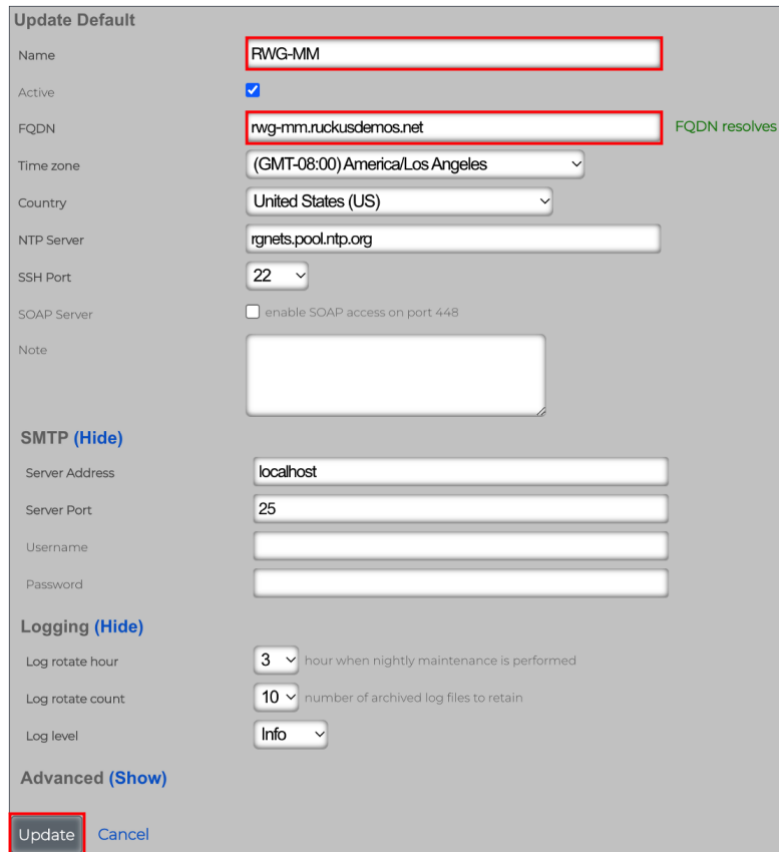


Active	Name	FQDN	Time zone	Country	NTP	SSH Port	SMTP
<input checked="" type="checkbox"/>	Default	rxg.local	(GMT-08:00) America/Los Angeles	US	rgnets.pool.ntp.org	22	localhost:25

FIGURE 33 – DEVICE OPTIONS



Enter a new name and the FQDN for your instance:



**Update Default**

Name:

Active:

FQDN:  FQDN resolves

Time zone: (GMT-08:00) America/Los Angeles

Country: United States (US)

NTP Server: rgnets.pool.ntp.org

SSH Port: 22

SOAP Server:  enable SOAP access on port 448

Note:

**SMTP (Hide)**

Server Address: localhost

Server Port: 25

Username:

Password:

**Logging (Hide)**

Log rotate hour: 3 hour when nightly maintenance is performed

Log rotate count: 10 number of archived log files to retain

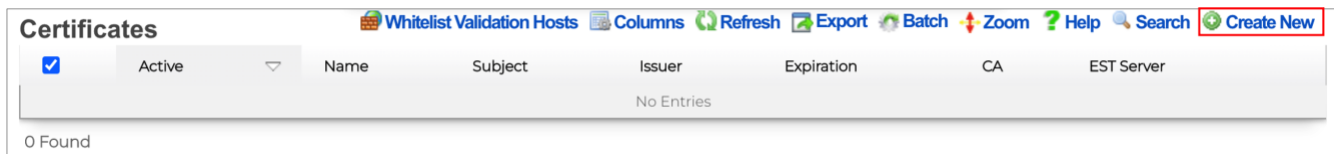
Log level: Info

**Advanced (Show)**

FIGURE 34 – UPDATE DEFAULT

Click **Update** to finish. RWG's web service will reinitialize automatically.

Next, navigate to **System/Certificates**, scroll down and click **Create New** in the section **Certificates**.



**Certificates**

Whitelist Validation Hosts Columns Refresh Export Batch Zoom Help Search

<input checked="" type="checkbox"/>	Active	Name	Subject	Issuer	Expiration	CA	EST Server
No Entries							

0 Found

FIGURE 35 – CERTIFICATES

The **Create Certificate** form shows. Enter the following information:

- **Name:** Enter the name for the certificate. Here, we used the FQDN for RWG.
- **CA:** Select **Trusted third-party**
- **Sign mode:** Select **Generate CSR and obtain certificate from Let's Encrypt**

**Create Certificate**

Active

Name

Key 

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQE339nIJ4Eq190MzE7A4U83R5Elodr3qy96H251/po+HnuLfjS
poTW94VWICyE3iBgxGxcxFkbLyHgSBO3qDsCCw1KD6jhgdiInA5EVPYfquR0AaG
ZXvENRazaNd6xBU+VX352/rs7pFNVsy4hdq7XiUPVI9zYmGVzfbeJjbpAKqwh0N1
NsGOWqboJ5MeHUG200zf1B5/S2joOpf/ossv4xJJABhbfnrcN4j8FFSAFe6r3DPD
ZWVdjPiLOHKsoKHK0ik1Oz8Q9MEXQ405z+Kq1TOEu2EQu3dyTgVH9Yt2ZaL46dSH
CKKOIhb2+nZMGdBZIE9pBkAnIKzMQxNuUsaQIDAQABoIBAGjh3eCFp0TYxKwd
Z0dQqG5P/PnzFSELSZeoIId8oPQyLB7wzNIONt8zeGZi3ftrkF29SI9wDXzBlgGd
FyvvgfSX2twXASAtnKFkrRk/A/DD9jNDlrV5C5aHQRGNN85m/KmBuXOnpyHRwRa39
Jn7SVe1sYbfaFdjOWMGuHzNminOfxxZNLWvKRXqoiDCTbjv7mqvSMYngdtRW9hQC
```

Intermediate

Certificate

CA  local issuer (optional)

EST Server  EST server to request a certificate from via RFC 7030

**Certificate signing request (Hide)**

Name

Usage

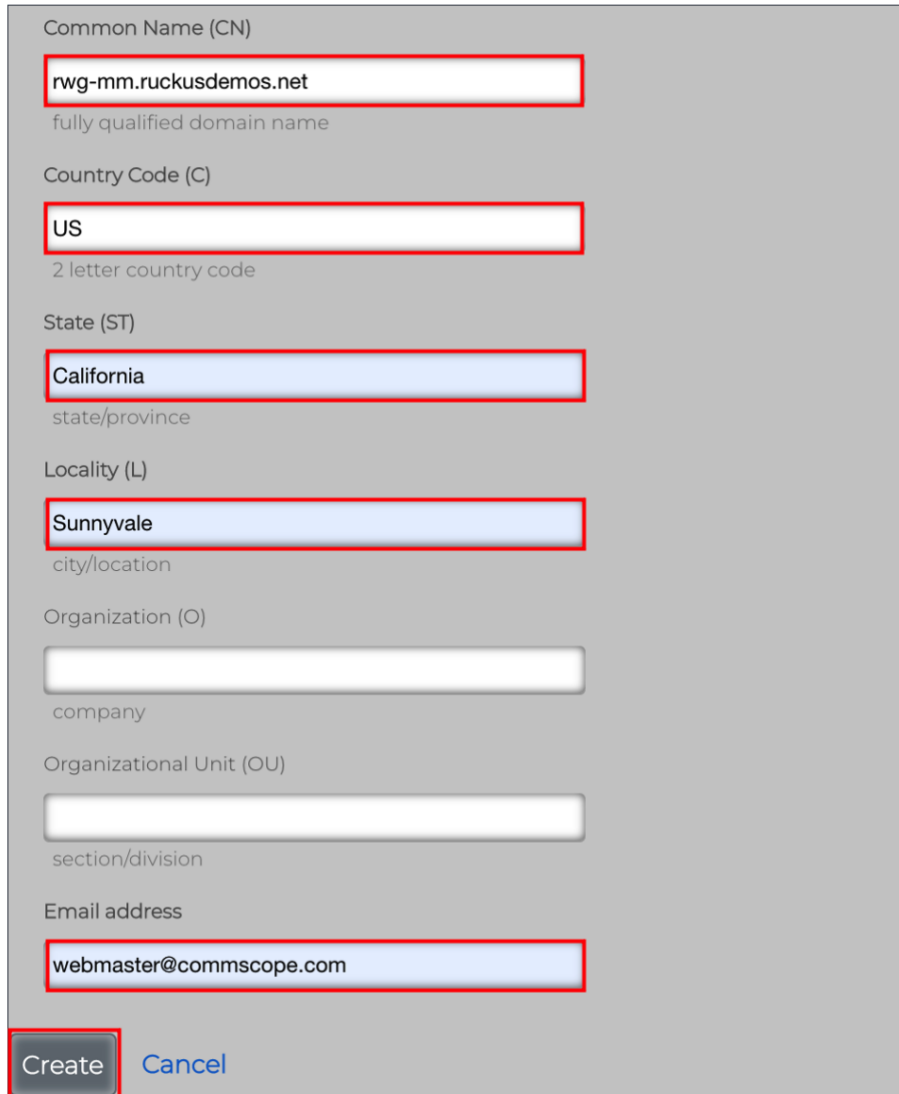
ExtendedKeyUsage (EKU) extension

Sign mode

FIGURE 36 – CREATE CERTIFICATE

Scroll down and enter the following information:

- **Common Name (CN):** Enter the FQDN for RWG.
- **Country Code (C):** Enter the 2-letter country code for where RWG is installed.
- **State (ST):** Enter the state. Do not use initials.
- **Locality (L):** Enter the city.
- **Email address:** Enter an email for contact. Do not use your personal email.



Common Name (CN)  
  
fully qualified domain name

Country Code (C)  
  
2 letter country code

State (ST)  
  
state/province

Locality (L)  
  
city/location

Organization (O)  
  
company

Organizational Unit (OU)  
  
section/division

Email address

FIGURE 37 – CREATE CERTIFICATE (CONT'D)

Click **Create** to finish.

RWG will contact Let's Encrypt and send the CSR. If all is right, a new certificate entry will show in the **Certificates** section.

Click **Edit** in the certificate entry, then mark the **Active** checkbox. Scroll down and click **Update** to finish.

Active	Name	Subject	Issuer	Expiration	CA	EST Server	
<input checked="" type="checkbox"/>	rwg-mm.ruckusdemos.net	rwg-mm.ruckusdemos.net	R3 Let's Encrypt US	3 months and 22 hours			Renew Download DER Download PKCS#12 Download PEM <b>Edit</b> Delete Show

1 Found

### Update rwg-mm.ruckusdemos.net

Active

Name

Key 

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA339nIj4Eq190MzE7A4U83R5E1odr3qy96H251/po+HnuLfjs
poTW94VWICyE3iBgxGxcxPkbLyHgSB03qDsCCw1KD6jhgdiInA5EEVPYfqr0AaG
ZXvENRazaNd6xBU+VX352/rs7pFNvSy4hdq7XiuPVI9zYmGvzFbeJbPAKqwh0N1
NsGOWQboJ5MeHUG200zf1B5/S2joOpf/ossv4xJABhbfnrcN4j8FFSAFe6r3DPD
ZWVdjP1LOHKsoKHk0ik1Oz8Q9MEXQ4O5z+Kq1TOEu2EQu3dyTgVH9Yt2ZaL46dSH
CKK0hb2+nZMGd8ZIE9pBkAnIKzMQXNuWusaQIDAQABAOIBAGjh3eCFp0TYxKwd
Z0dQqG5P/PnzFSELSZeoIId8oPQyLB7wzNIONT8zeGZi3ftrkF29SI9wDXzB1gGd
FyvgfSX2twASAtnKFkrrK/A/DD9jND1rv5C5aHQRGNn85m/KmBuXONpyHRwRa39
Jn7SVe1sYbfaFdjOWMGUhzNminOfxxZNLWvKRKqoiDCTbjv7mqvSMYngdtRW9hQC

```

 private key

Intermediate 

```
-----BEGIN CERTIFICATE-----
MIIFFFjCCAv6gAwIBAgIRAJErCErPDBinU/bWLiWnX1owDQYJKoZIhvcNAQELBQAw
TzELMAkGA1UEBhMCVVMxKTAnBgNVBAoTIEludGVybWV0IFN1Y3VyaXR5IFJlc2Vh
cmNoIEYdyb3VwMRUwEwYDVQQDEwJULJHIFJvY3QgWDEwHhcNMjAwOTA0MDAwMDAw
WheNMjUwOTE1MTYwMDAwWjAyMjAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAw
RW5jcnlwdDELMAkGA1UEAxMjMwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC7AhUozPaglNMPeuyNVZLD+ILxma26QoinXSagtSu5xUyxr45r+XXI09cP
R5QUVTVXjJ6oojk29YI8Qq1ObvU7wy7b2jCwXPNZOOftz2nWwgsbvsCUJCWH+jdx
sxPnHKzhm+/b5DtFukWwqCFTzjTIIUu61ru2P3mBw4qVUq7ZtDpe1QDRrK908Zutm
NHZ6a4uPVymZ+DAXXbpyb/uBxa3Sh1g9F8fnCbvxk/eG3MHacV3URuPMrSXBilXg

```

 issuer certificate (optional)

Certificate 

```
-----BEGIN CERTIFICATE-----
MIIFMDCBBigAwIBAgISB07KiaFw9xHGrFNSiUDvKZUvMA0GCSqGSIb3DQEBCwUA
MDIxCzAJBgNVBAYTAlVTMRwFAyQVQKQEWIMZQncybFbmlNyeXBOMQMsCQYDVQQD
EwJSMzAeFw0yMzAxMjQxOTUxMDhaFw0yMzA0MjQxOTUxMDhaMCEwH2AdBgNVBAMT
FnJ3Zy1tbS5ydWNRdXNkZW1vcy5uZXQvvgEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCdf2cgngSqX3QzMTSDhtzdhKSWH2verL3ofbmX+mj4ee4t+nKmhnb3
hVYgLIteIGDEBfzEWRsvIEIE7eoOwILCUoPqOGB0gicDKQRU9h+q5HQBoz1e8Q1
FrNo13rEFT5VfFnb+uzukU1WzLiF2rteK49Uj3NiYZXN9t4klukAqrCHQ3U2w7B
Bugnk4dQbbTTN/UHn9LaOg61/+iyy/jEkkAGft82tw3iPwUVIAV7qvcM8N1ZV2M
+K04cqygoeTSKSU7PxD0wRdDg7n4qrVM4S7YRC7d3JOBuFi13Z1ovjp1IcIqQ4g

```

 host certificate

CA  local issuer (optional)

EST Server  EST server to request a certificate from via RFC 7030

FIGURE 38 – MAKING THE CERTIFICATE ACTIVE

Now, if you close and restart your browser, the URL will show a secure SSL connection.

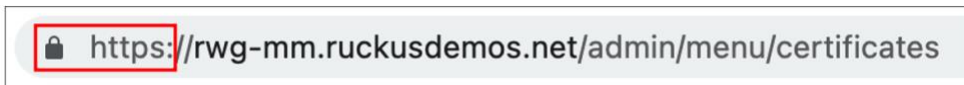


FIGURE 39 – A SECURE CONNECTION

## Network Topology Diagrams

RWG uses discovery protocols like LLDP or CDP to learn about infrastructure devices and to create topology diagrams including adopted devices.

By default, all discovery protocols are disabled.

Click **Network** at the top menu to see the basic diagram created by RWG, showing its physical interfaces only.

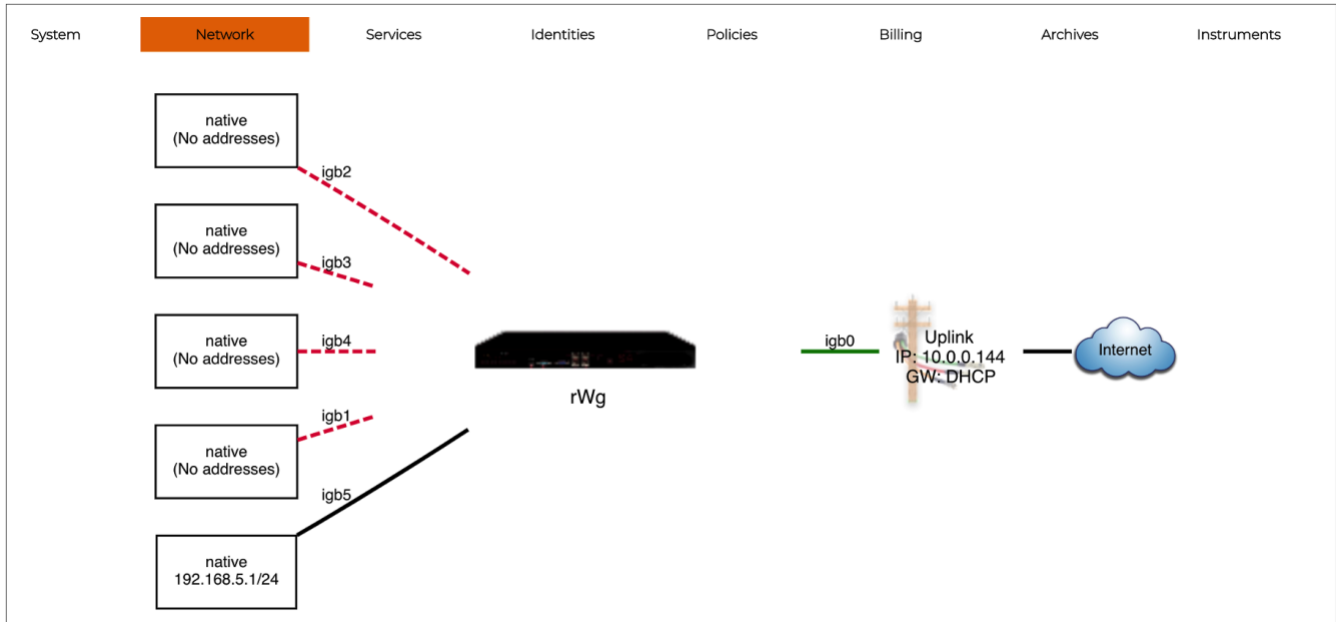


FIGURE 40 – DEFAULT TOPOLOGY DIAGRAM

Navigate to **Services/Server**, then click **Create New** in the LLDP Servers section.

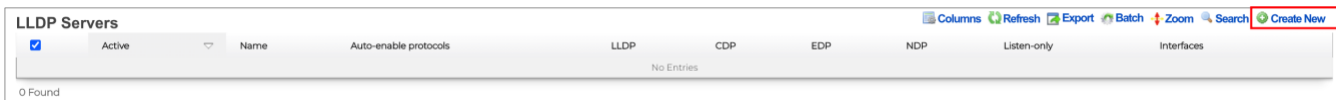
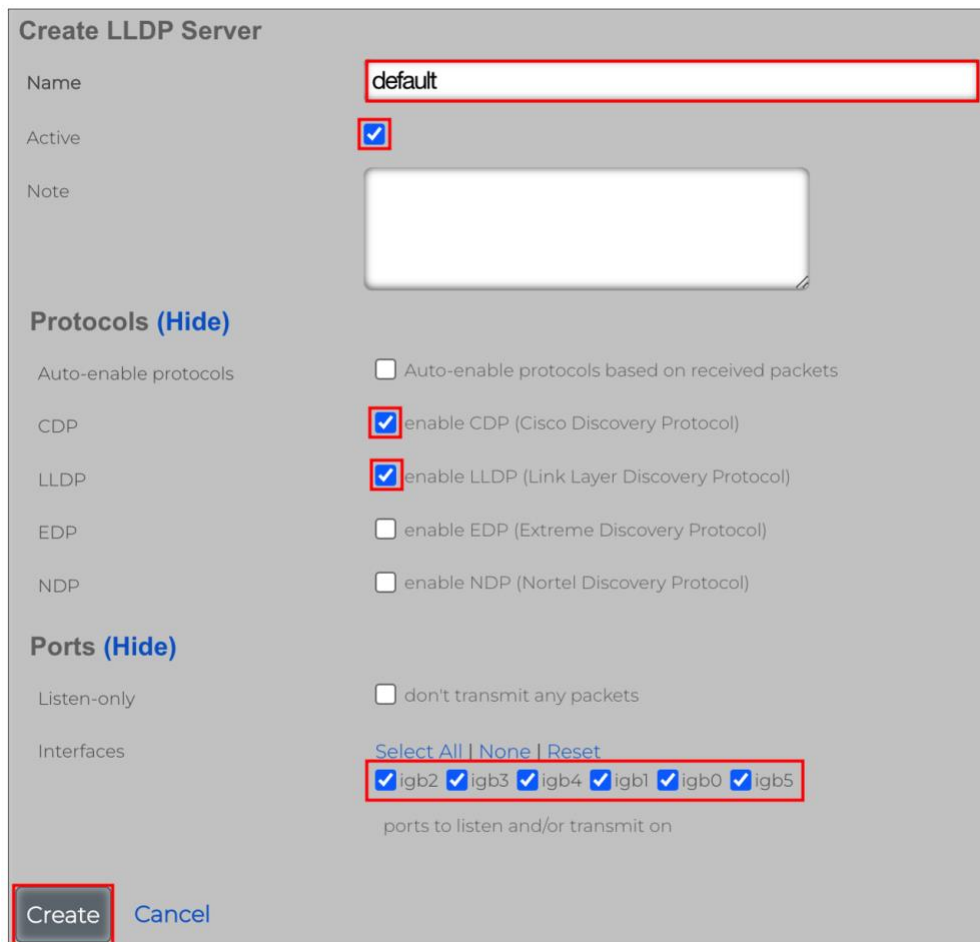


FIGURE 41 – LLDP SERVERS

Enter the following information:

- **Name:** Enter a name for the server. Here, we kept the default name.
- **Active:** Make sure the checkbox is marked.
- **Auto-enable protocols:** You can unmark the checkbox if you define the protocols manually.
- **CDP, LLDP, EDP and NDP:** Mark the checkbox for the protocols you want to use.
- **Listen-only:** Unmark the checkbox, so RWG will be discovered by the infrastructure devices.
- **Interfaces:** Mark all interfaces that needs to use the discovery protocols.



**Create LLDP Server**

Name: default

Active:

Note: [Empty text area]

**Protocols (Hide)**

Auto-enable protocols:  Auto-enable protocols based on received packets

CDP:  enable CDP (Cisco Discovery Protocol)

LLDP:  enable LLDP (Link Layer Discovery Protocol)

EDP:  enable EDP (Extreme Discovery Protocol)

NDP:  enable NDP (Nortel Discovery Protocol)

**Ports (Hide)**

Listen-only:  don't transmit any packets

Interfaces: [Select All](#) | [None](#) | [Reset](#)

igb2  igb3  igb4  igb1  igb0  igb5

ports to listen and/or transmit on

**Create** Cancel

FIGURE 42 – CREATE LLDP SERVER

After the infrastructure devices are adopted and discovered, you will see new topology diagrams in **Networks**.

Here we show an example after an ICX switch is adopted.

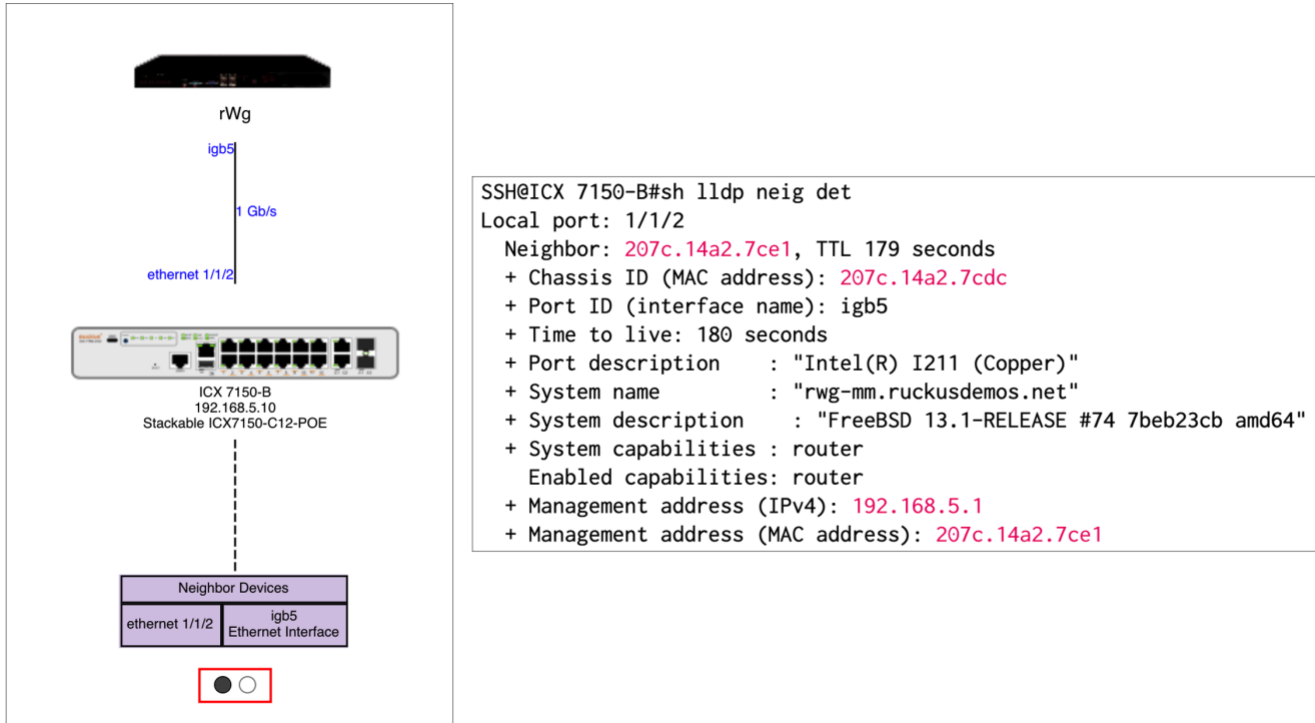


FIGURE 43 – NEW TOPOLOGY DIAGRAM AND ICX NEIGHBORS LIST

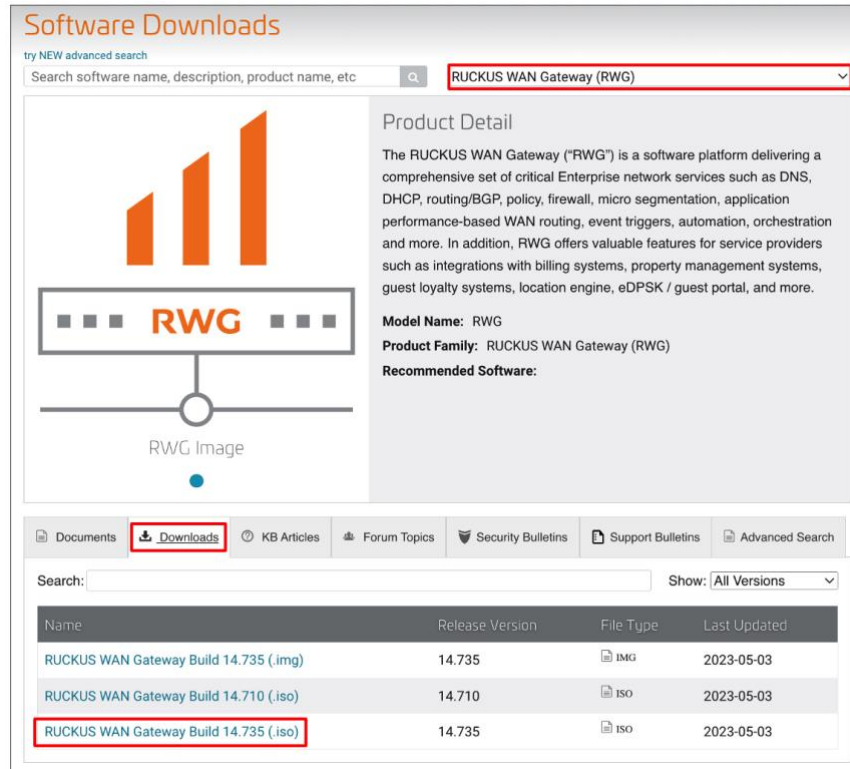
You can use the dots at the bottom of the diagram to navigate between the discovered topology and the original one showing the RWG interfaces.

The ICX switch also discovers RWG, including information of its hardware and software releases.

## RWG Software Upgrade

RWG can download new software automatically, or you can download a .ISO file manually from the RUCKUS support site. Navigate to the RUCKUS support site at <https://support.ruckuswireless.com/software>, and select RUCKUS WAN Gateway (RWG) in the dropdown list.

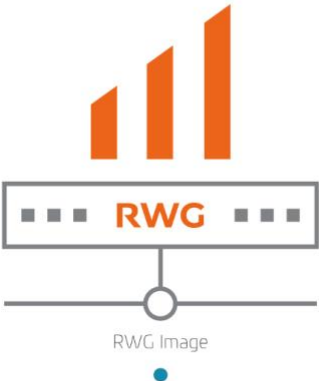
The **Downloads** tab will show the recommended ISO images. Download the latest recommended image to your computer.



**Software Downloads**

try NEW advanced search

Search software name, description, product name, etc



RWG Image

**Product Detail**

The RUCKUS WAN Gateway ("RWG") is a software platform delivering a comprehensive set of critical Enterprise network services such as DNS, DHCP, routing/BGP, policy, firewall, micro segmentation, application performance-based WAN routing, event triggers, automation, orchestration and more. In addition, RWG offers valuable features for service providers such as integrations with billing systems, property management systems, guest loyalty systems, location engine, eDPSK / guest portal, and more.

**Model Name:** RWG  
**Product Family:** RUCKUS WAN Gateway (RWG)  
**Recommended Software:**

Documents **Downloads** KB Articles Forum Topics Security Bulletins Support Bulletins Advanced Search

Search:  Show: All Versions

Name	Release Version	File Type	Last Updated
<a href="#">RUCKUS WAN Gateway Build 14.735 (.img)</a>	14.735	IMG	2023-05-03
<a href="#">RUCKUS WAN Gateway Build 14.710 (.iso)</a>	14.710	ISO	2023-05-03
<a href="#">RUCKUS WAN Gateway Build 14.735 (.iso)</a>	14.735	ISO	2023-05-03

FIGURE 44 – IMAGE DOWNLOAD FROM THE RUCKUS SUPPORT SITE

You can upgrade only the RWG software, or the RWG software and OS. Before upgrading, it is recommended that you perform a configuration backup of your system.

The upgrade process might take several minutes depending on your link speed, and RWG will be unavailable during the process.

Navigate to **System/Update** and click **Download Backup** to backup your system. A .tgz file will be downloaded to your computer.



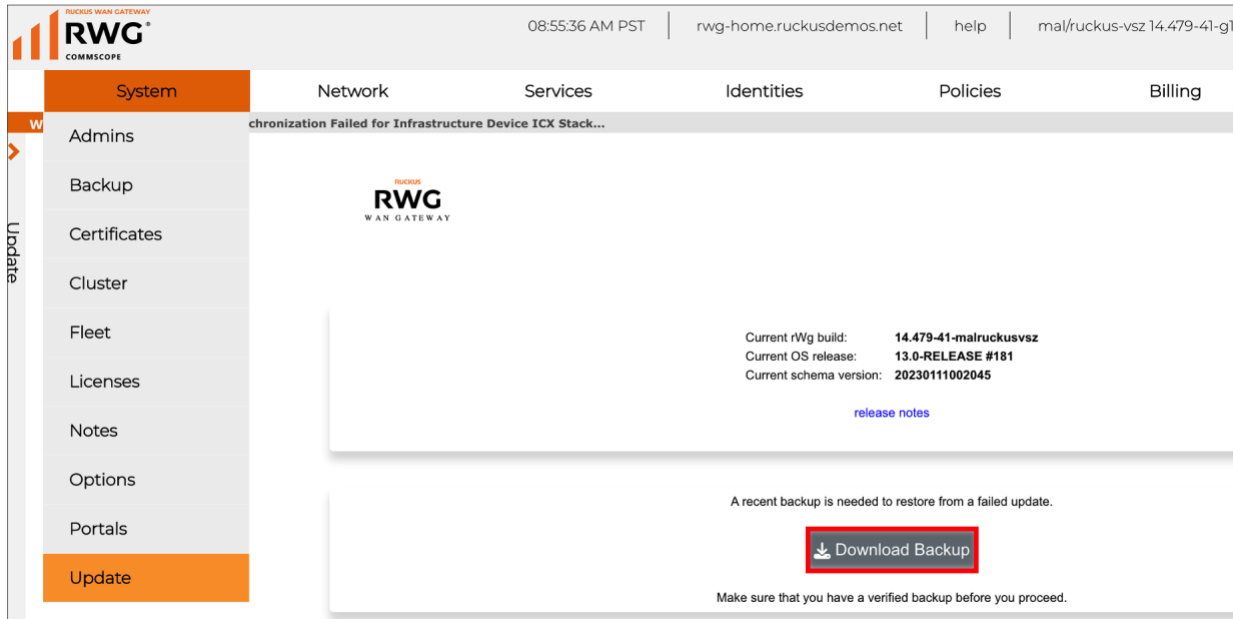


FIGURE 45 – DOWNLOAD BACKUP

Scroll down to see the upgrade options. You can perform three types of upgrades:

- OS and RWG software
- Only RWG software
- Using a local file

If you choose the options that fetch the software automatically, you need to enter your RUCKUS support credentials. In our example we see that both the RWG software and the OS need to be upgraded. Click **Update RWG + OS**.

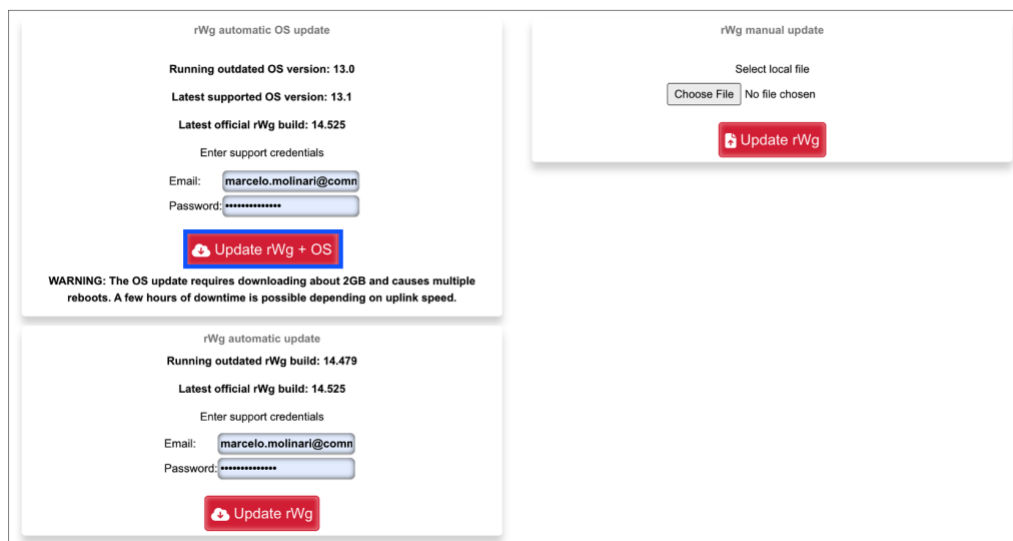


FIGURE 46 – UPGRADE RWG + OS

Click **OK** to proceed. The **Upgrade Log** panel shows the upgrade progress. After the first reboot, you can follow the upgrade process using the **tfuf** command in a SSH session to RWG.

rwg-home.ruckusdemos.net says

Click OK to update the rWg software AND operating system on [rwg-home.ruckusdemos.net](http://rwg-home.ruckusdemos.net) (10.0.0.106) by fetching the latest version from Ruckus over the Internet. This process requires downloading about 3GB and causes multiple reboots. A few hours of downtime is possible depending on uplink speed. Download a full backup before continuing if not done so already.

The upgrade is in progress. Please wait on this page until the upgrade is complete. The contents of this page should change throughout the upgrade process and notify you when the upgrade is finished. Please be patient as this process can take up to a few hours depending on Internet connection speed and hardware performance.

The system will reboot three times and be inaccessible via the web admin console for the later part of the update. Do not manually power off, reboot, or disconnect the rWg device from the Internet. For detailed progress after the first reboot, open an SSH terminal connection to the rWg and run:

```
tfuf
```

Upgrade Log

Enable auto scroll down

< 1 2 3 >

```

140200K ..... 43% 56.1M 5s
140250K ..... 43% 67.7M 5s
140300K ..... 43% 93.2M 5s
140350K ..... 43% 93.1M 5s
140400K ..... 43% 97.8M 5s
140450K ..... 43% 96.8M 5s
140500K ..... 43% 96.2M 5s
140550K ..... 43% 80.8M 5s
140600K ..... 44% 95.0M 5s
140650K ..... 44% 102M 5s
    
```

FIGURE 47 – UPGRADE IN PROGRESS

The upgrade process completes after the 3rd reboot. The new build shows at the top menu.

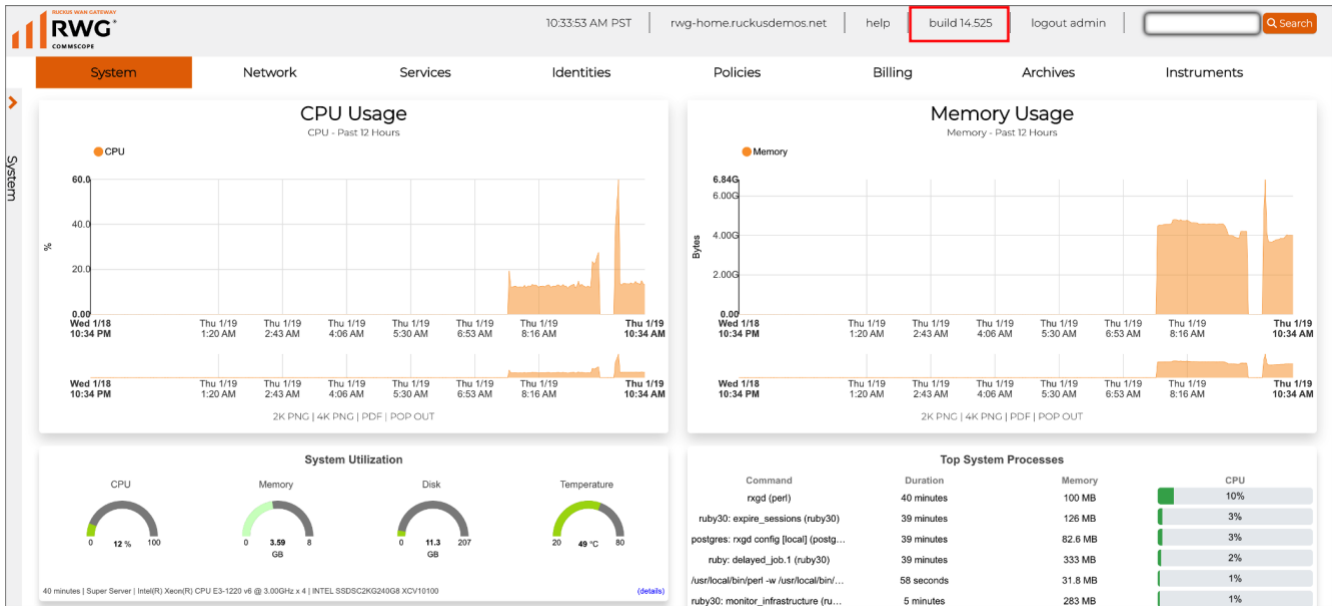


FIGURE 48 – UPGRADE COMPLETED

## RWG Backup and Restore

You can perform a RWG configuration backup at any moment.

Also, RWG comes with a pre-configured backup routine to perform backups daily. You can change that routine according to your needs. The backup files can be manually downloaded to your computer, or you can define a backup server running FTP, SFTP or HTTPS, to send the backup files to an external repository automatically.

Normally, the backup files will be restored to the same RWG. It is possible to restore the backup onto a different RWG. The destination RWG needs to run the same software version or superior, and it does not need to have the same number or interfaces. If the number of interfaces in the destination RWG is different, a dialogue form will propose the necessary changes in the configuration. After the restore process is completed, the destination RWG will use the IP addresses that exist in the backup file – the ones used by the source RWG.

### Backup

Navigate to **System/Backup** to see the backup and restore dialogue form.

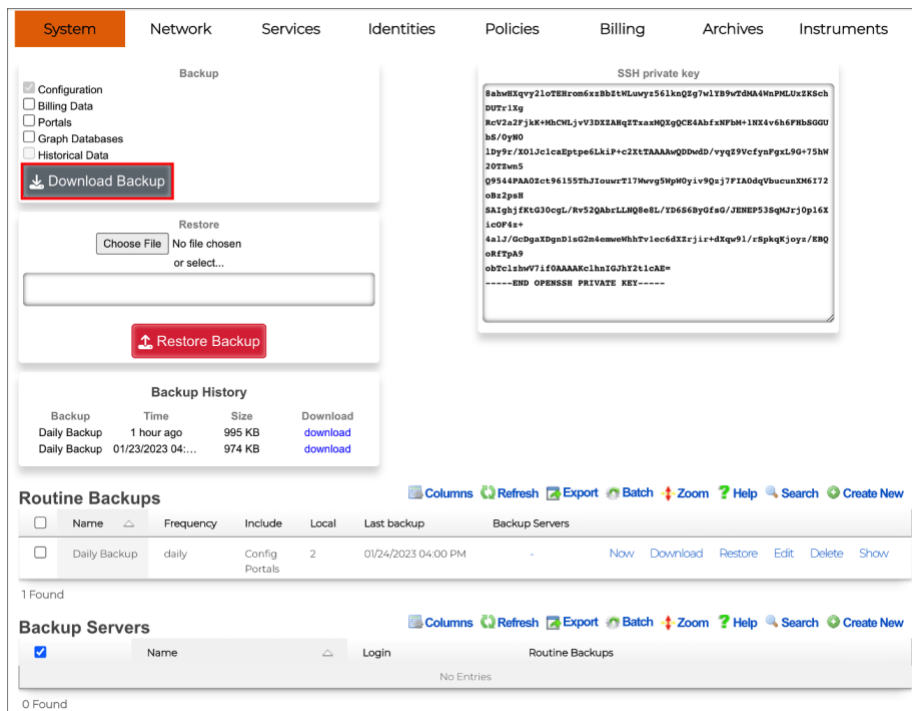


FIGURE 49 – BACKUP AND RESTORE

At the top left, you can perform a manual backup and select what type of information will be included in the backup files:

- Configuration (always checked by default)
- Billing Data
- Portals
- Graph Databases
- Historical Data

Click **Download Backup** to perform a manual backup. That will download a timestamped compressed .tgz file directly to your computer.

**Routine Backups** are used to schedule automatic backups. Multiple routines can be created. You can define hourly, daily, weekly and monthly backups. By default, RWG runs a daily backup routine.

The RWG configuration data is always included in the backup. As with manual backups, you can define what additional data will be backed up. The backup files will be stored inside RWG, up to a defined number. Click download to download a backup to your computer.

You can also define external **Backup Servers**, where the backup files will be sent to automatically. Backup servers can use SFTP, FTP and HTTPS. If required, multiple backup servers can be created.

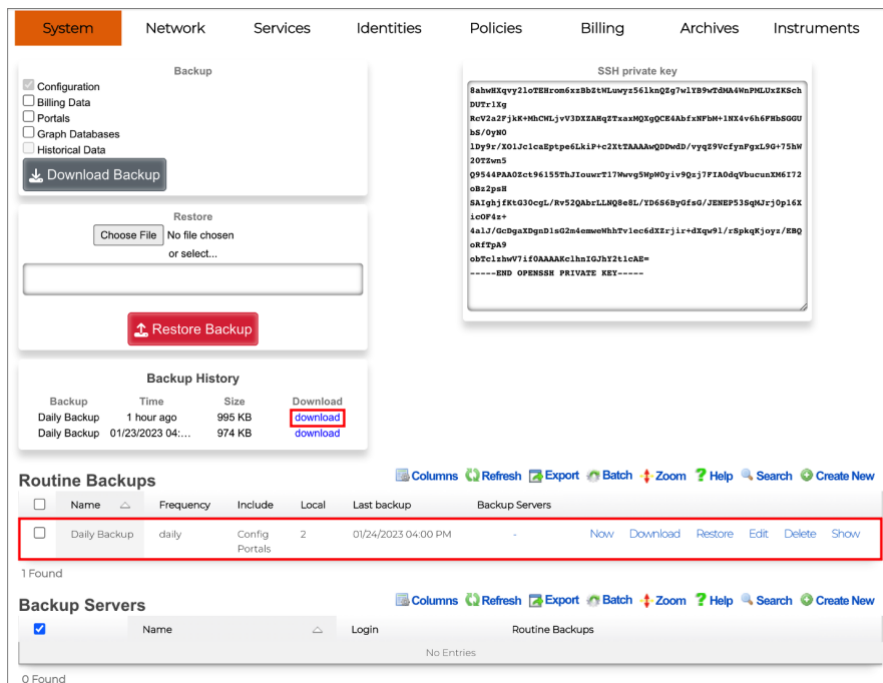


FIGURE 50 – ROUTINE BACKUPS

## Restore

You can choose an external file to restore (that needs to be the compressed .tgz file), or you can select a backup file from the list of backups stored in RWG. Click **Restore Backup** to execute the restore.

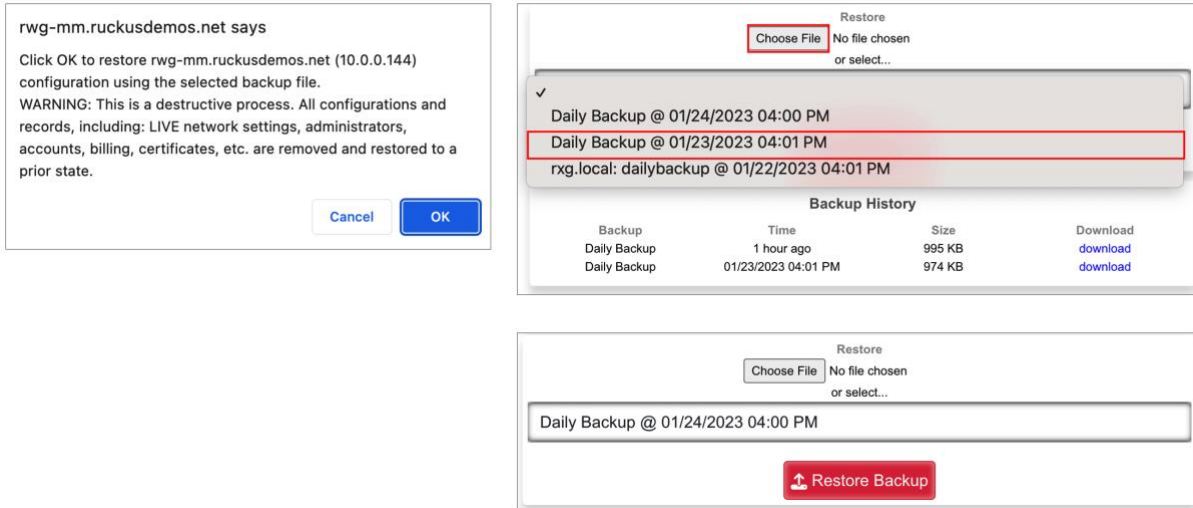


FIGURE 51 – SELECT THE BACKUP TO RESTORE

Right after the restore process starts, a **Restore Log** is shown. If required, you can download a log file to see all the steps in the restore process.

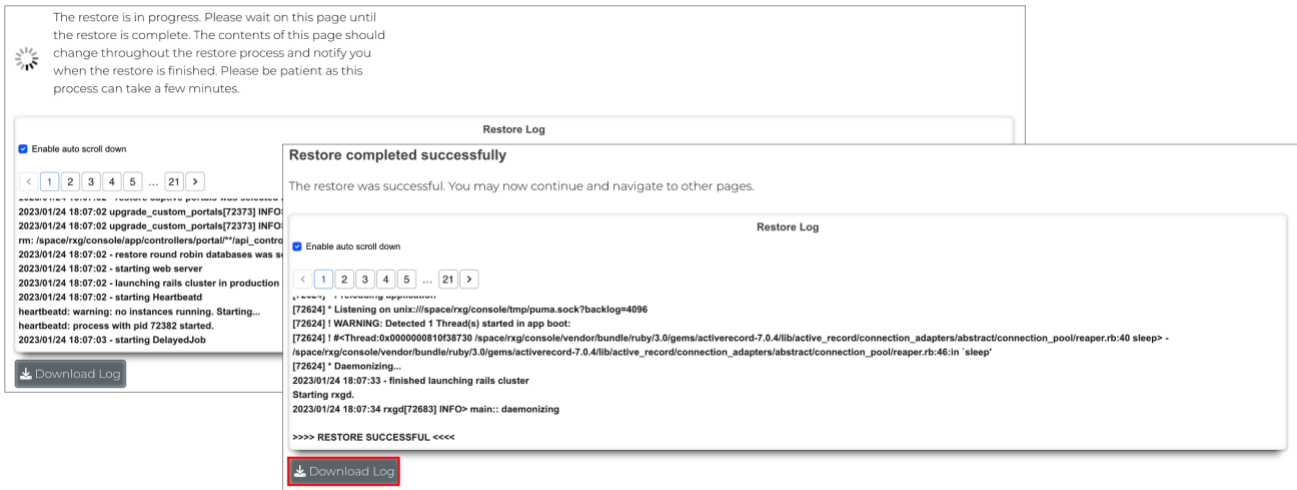


FIGURE 52 – THE RESTORE LOG

## Config Templates

Configuration templates are YAML definitions used to bootstrap a new RWG node, or change the configuration of existing RWGs. The templates can be created manually, or generated automatically for any RWG scaffold, or for the entire RWG configuration. Using config templates makes it very easy to share the entire configuration for a complete MDU or HSP solution. The example below shows the YAML file for the **VLAN Interfaces** scaffold:

```

Vlan:
- name: VLAN 100
  interface: igb5
  tag: 100
  autoincrement_mode: none
- name: VLAN 200
  interface: igb5
  tag: 200
  autoincrement_mode: none
  addresses:
  - subnet 200
- name: VLAN 150
  interface: igb5
  tag: 150
  autoincrement_mode: none
  addresses:
  - subnet 150
    
```

FIGURE 53 – CONFIG TEMPLATE FOR VLAN INTERFACES

### Generate a Config Template for a Scaffold

To generate a config template, navigate to the desired scaffold, then click **Export/rWg Config Template**:

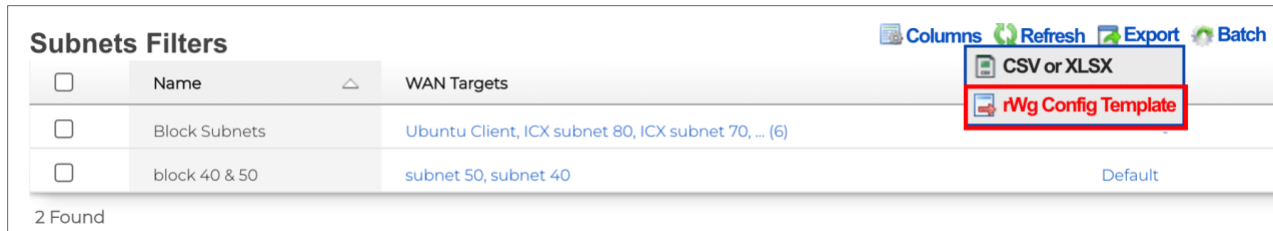


FIGURE 54 – GENERATE THE TEMPLATE FOR SUBNETS FILTERS

Accept the defaults and click **Export**. The YAML file will be downloaded to your computer.



FIGURE 55 – EXPORT THE CONFIG TEMPLATE

```

---
SubnetsFilter:
- name: Block Subnets
  wan_targets:
  - ICX subnet 90
  - ICX subnet 80
  - ICX subnet 70
  - ICX subnet 60
  - Ubuntu Client
  - ISP 1
- name: block 40 & 50
  wan_targets:
  - subnet 50
  - subnet 40
  policies:
  - Default
    
```

FIGURE 56 – TEMPLATE FOR SUBNET FILTERS

## Generate a Config Template for the Entire RWG

It is also possible to generate a config template for the entire RWG. Navigate to **System/Backup**, then click **Generate Template** at the **Config Templates** section:

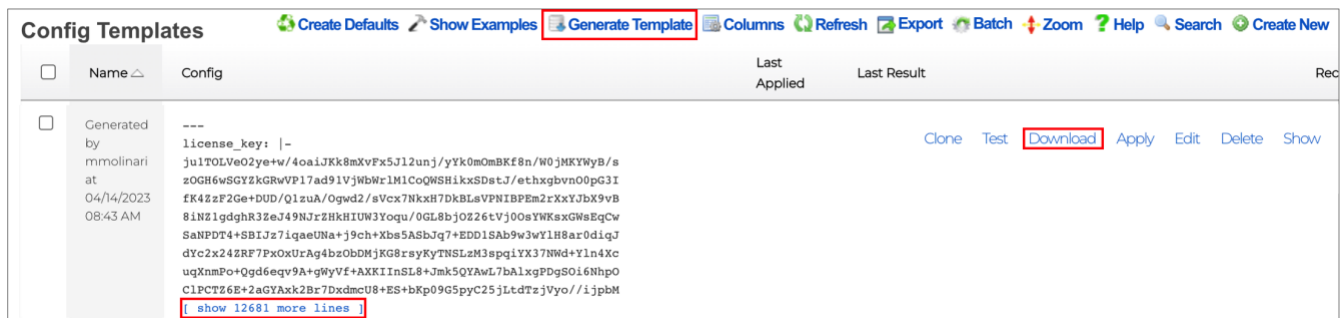


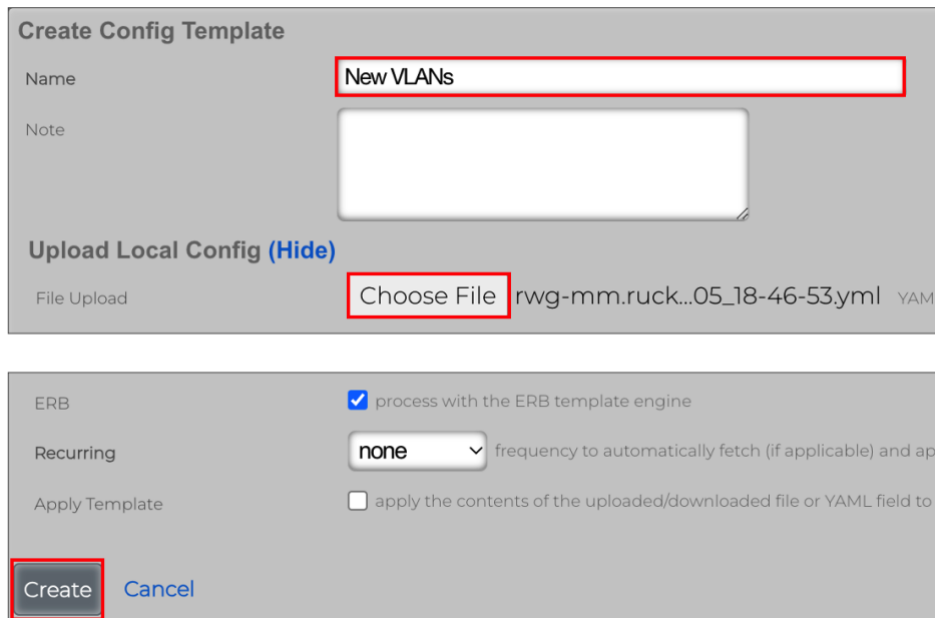
FIGURE 57 – GENERATE TEMPLATE FOR THE ENTIRE SMARTZONE

After a few seconds, a new template entry will show under the Config Templates section. You can click **show more lines** to see details or **Download** to get the YAML file.

## Upload, Test and Apply a Config Template

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 YAML file with the configuration that you want to apply to RWG.



**Create Config Template**

Name:

Note:

**Upload Local Config (Hide)**

File Upload:  rwg-mm.ruck...05\_18-46-53.yml YAML

ERB:  process with the ERB template engine

Recurring:  frequency to automatically fetch (if applicable) and apply

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

FIGURE 58 – UPLOAD THE TEMPLATE FILE

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

It is possible to create recurrent templates, which will execute every hour, day, week, etc. If you mark the **Apply Template** checkbox, the template will be applied to RWG as soon as it is created. Leave the checkbox unmarked for now.

To edit an existing template, click **Edit** on the new entry.



**Config Templates**

<input type="checkbox"/>	Name	Config	Last Result	
<input type="checkbox"/>	New VLANs	<pre> --- Vlan: - name: VLAN 100   interface: igb5   tag: 100   autoincrement_mode: none - name: VLAN 200   interface: igb5   tag: 200   autoincrement_mode: none [ show 8 more lines ]                     </pre>		<input type="button" value="none"/> <input type="button" value="Clone"/> <input type="button" value="Test"/> <input type="button" value="Download"/> <input type="button" value="Apply"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Show"/>

FIGURE 59 – EDIT THE TEMPLATE FILE



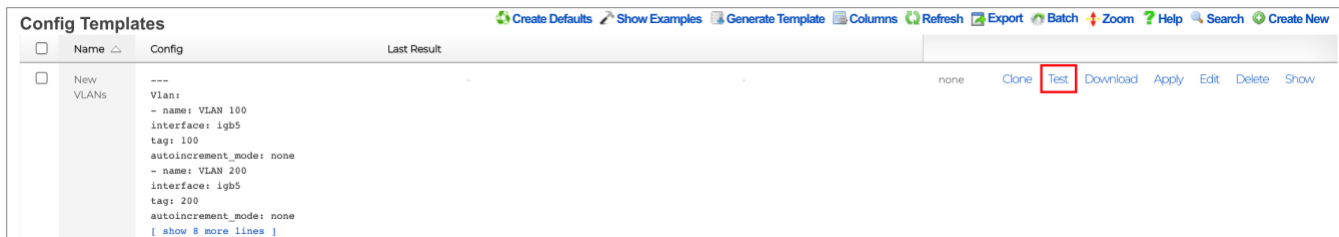
If required, you can edit the template lines directly inside the **Config** form.

```

Template (Hide)
Config
1 ---
2 Vlan:
3 - name: VLAN 100
4   interface: igb5
5   tag: 100
6   autoincrement_mode: none
7 - name: VLAN 200
8   interface: igb5
9   tag: 200
10  autoincrement_mode: none
11  addresses:
12  - subnet 200
13 - name: VLAN 150
14   interface: igb5
15   tag: 150
16   autoincrement_mode: none
17   addresses:
18   - subnet 150
19
    
```

FIGURE 60 – EDIT THE TEMPLATE LINES

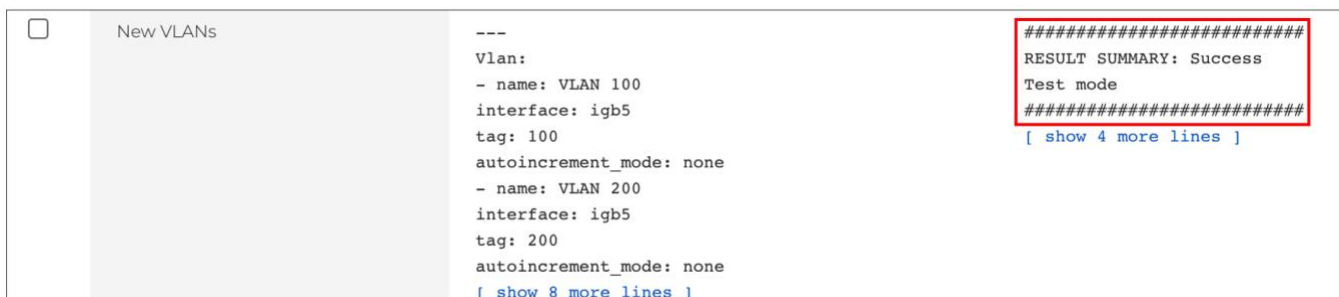
Click **Test** to verify the template syntax. That does not apply the template to RWG.



The screenshot shows the 'Config Templates' interface. At the top, there are several utility buttons: 'Create Defaults', 'Show Examples', 'Generate Template', 'Columns', 'Refresh', 'Export', 'Batch', 'Zoom', 'Help', 'Search', and 'Create New'. Below this is a table with columns for 'Name', 'Config', and 'Last Result'. The first row is 'New VLANs' with a checkbox. The 'Config' column contains the same template code as in Figure 60. The 'Last Result' column is empty. To the right of the table, there are several action buttons: 'none', 'Clone', 'Test' (highlighted with a red box), 'Download', 'Apply', 'Edit', 'Delete', and 'Show'.

FIGURE 61 – TEST THE TEMPLATE

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



The screenshot shows the 'Config Templates' interface with the 'New VLANs' template selected. The 'Last Result' column now contains the following text:
 

```

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

 A red box highlights the success message. The 'Config' column still shows the template code. Below the 'Last Result' column, there is a link '[ show 8 more lines ]'.

FIGURE 62 – TEST SUCCEED

To apply the template to RWG, click **Apply**:



FIGURE 63 – APPLY THE TEMPLATE

Click **OK** to confirm. If all goes well, you will receive a success message:



FIGURE 64 – SUCCESS

## Basic Troubleshooting

RWG includes several tools to manage the solutions and to troubleshoot the network or client access problems. This document covers the following tools:

- Instruments: Ping, Traceroute and DHCP Leases
- Logs: Notification logs, RADIUS logs, etc
- Search Tool

### Instruments

Click **Instruments** at the top menu to see a graph for uplink traffic, and several gauges and tables to monitor your RWG. You can rotate among different gauges by clicking the dots.

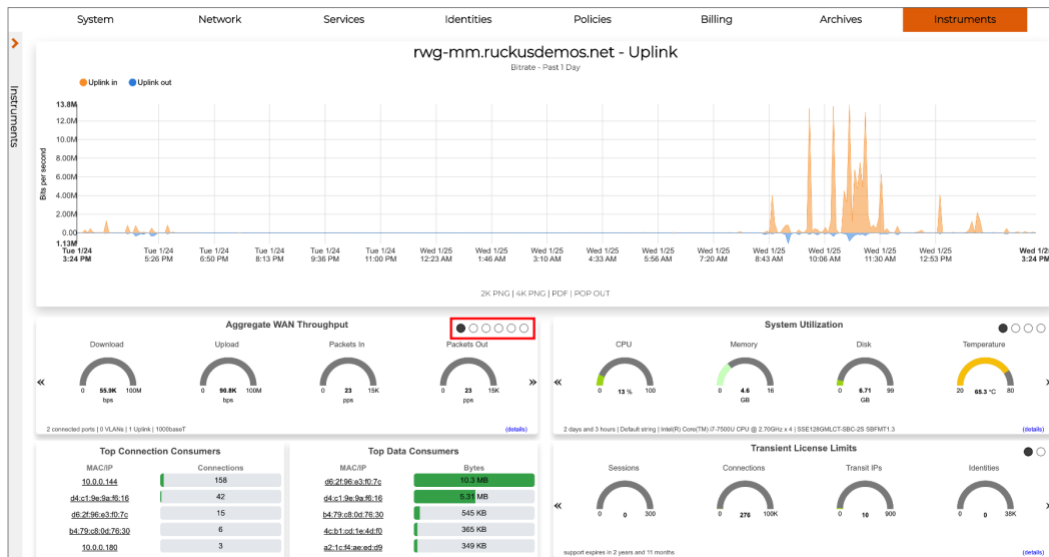


FIGURE 52 – INSTRUMENTS

The **Instruments** menu has a variety of tools to help you manage and troubleshoot your network.

Here are some of the most useful tools:

- **MAC • DHCP • DNS:** Here you can find the MAC addresses and DHCP leases for all infrastructure devices and client devices. You can see the VLAN assignment in the DHCP leased, and you can also convert a leased entry to a fixed IP address directly from the list of devices.
- **NAT Assignments:** Useful to make sure a local subnet is being NAT'ed correctly by RWG.
- **Route Entries:** Shows the RWG routing table.
- **Utilities:** Includes a ping and a traceroute tool.

Instruments
MAC • DHCP • DNS
Connection States
Device Sessions
Interface Assignments
NAT Assignments
Network Monitor
Route Entries
System Info
Traffic Rates
Utilities

DHCP Leases												
<input type="checkbox"/>	Issued	IP	MAC	Vendor	Hostname	Expires	Network	Pool	Fixed Host	Ethernet	VLAN	
<input type="checkbox"/>	01/25/2023 03:40:35 PM	192.168.5.253	b4:79:c8:0d:76:30	Ruckus Wireless	-	01/25/2023 04:40:35 PM	igb5	Management LAN	Create New	igb5	-	
<input type="checkbox"/>	01/25/2023 03:40:11 PM	192.168.5.10	d4:c1:9e:9a:f6:16	Ruckus Wireless	-	01/25/2023 04:40:11 PM	igb5	Management LAN	ICX 7150-B	igb5	-	
<input type="checkbox"/>	01/25/2023 03:40:09 PM	192.168.5.250	da:79:93:60:18:6a	-	Marcelo-s-S10	01/25/2023 04:40:09 PM	igb5	Management LAN	Create New	igb5	VLAN600	

FIGURE 53 – CONVERTING A DHCP LEASE TO A FIXED HOST ADDRESS

## Logs

The Archives menu include logs for most of the RWG services. Here are the most useful ones:

- **Notification Logs:** Here are the warning messages shown at top of the RWG UI are stored.
- **RADIUS Logs:** Useful to check VLAN tag assignments.
- **.log Files:** Includes complete log files for all RWG services. Very useful to check detailed RADIUS responses with VLAN assignments or DHCP messages.

Let’s see some examples.

Archives
Notification Logs
Reports
Admin Logs
Connection Logs
DHCP - DNS Logs
Portal Logs
Queue Logs
RADIUS Logs
Trigger Logs
Web Logs
.log Files

## Notification Logs

The Notification Logs show the warning messages that show at the top of the RWG UI:

System	Network	Services	Identities	Policies	Billing	Archives	Instruments																																																						
<b>WARNING</b> NTP is not synchronized...																																																													
<div style="display: flex; justify-content: space-between; align-items: center;"> <span>Cure All</span> <span>Columns</span> <span>Refresh</span> </div> <table border="1"> <thead> <tr> <th>Created</th> <th>Name</th> <th>Message</th> <th>Severity</th> <th>Cured</th> <th>Reason</th> </tr> </thead> <tbody> <tr> <td>01/23/2023 11:14 AM</td> <td>My Ip Conflict</td> <td>another device is using my IP address!</td> <td>Critical</td> <td>01/25/2023 04:10 PM</td> <td>I had two RWGs with the same address</td> </tr> <tr> <td>01/23/2023 11:22 AM</td> <td>Monitor Infrastructure Device 62</td> <td>Unreachable: vSZ-249 - Failed to open TCP connection to 192.168.5.249:8443 [Connection refused - connect(2) for 192.168.5.249:8443]</td> <td>Warning</td> <td>-</td> <td>-</td> </tr> <tr> <td>01/24/2023 08:55 AM</td> <td>Infrastructure Device 62 Monitor</td> <td>vSZ-249 [192.168.5.249] is OFFLINE</td> <td>Notice</td> <td>-</td> <td>-</td> </tr> <tr> <td>01/24/2023 12:36 PM</td> <td>Ping Target 1 Monitor</td> <td>Google Public DNS 1 [8.8.8.8] is OFFLINE</td> <td>Notice</td> <td>-</td> <td>-</td> </tr> <tr> <td>01/24/2023 12:37 PM</td> <td>Ping Target 2 Monitor</td> <td>Google Public DNS 2 [8.8.4.4] is OFFLINE</td> <td>Notice</td> <td>-</td> <td>-</td> </tr> <tr> <td>01/24/2023 12:37 PM</td> <td>Monitor Infrastructure Device 61</td> <td>Unreachable: vSZ-MM - Failed to open TCP connection to vszh-mm.ruckusdemos.net:8443 [getaddrinfo: Name does not resolve]</td> <td>Warning</td> <td>-</td> <td>-</td> </tr> <tr style="border: 2px solid red;"> <td>01/25/2023 04:04 PM</td> <td>Ntp Server</td> <td>NTP is not synchronized</td> <td>Warning</td> <td>-</td> <td>-</td> </tr> <tr> <td>01/22/2023 04:58 PM</td> <td>Infrastructure Device 53 Monitor</td> <td>ICX 7150-B [192.168.5.242] is OFFLINE</td> <td>Notice</td> <td>01/25/2023 04:06 PM</td> <td>ICX 7150-B [192.168.5.242] is ONLINE</td> </tr> </tbody> </table>								Created	Name	Message	Severity	Cured	Reason	01/23/2023 11:14 AM	My Ip Conflict	another device is using my IP address!	Critical	01/25/2023 04:10 PM	I had two RWGs with the same address	01/23/2023 11:22 AM	Monitor Infrastructure Device 62	Unreachable: vSZ-249 - Failed to open TCP connection to 192.168.5.249:8443 [Connection refused - connect(2) for 192.168.5.249:8443]	Warning	-	-	01/24/2023 08:55 AM	Infrastructure Device 62 Monitor	vSZ-249 [192.168.5.249] is OFFLINE	Notice	-	-	01/24/2023 12:36 PM	Ping Target 1 Monitor	Google Public DNS 1 [8.8.8.8] is OFFLINE	Notice	-	-	01/24/2023 12:37 PM	Ping Target 2 Monitor	Google Public DNS 2 [8.8.4.4] is OFFLINE	Notice	-	-	01/24/2023 12:37 PM	Monitor Infrastructure Device 61	Unreachable: vSZ-MM - Failed to open TCP connection to vszh-mm.ruckusdemos.net:8443 [getaddrinfo: Name does not resolve]	Warning	-	-	01/25/2023 04:04 PM	Ntp Server	NTP is not synchronized	Warning	-	-	01/22/2023 04:58 PM	Infrastructure Device 53 Monitor	ICX 7150-B [192.168.5.242] is OFFLINE	Notice	01/25/2023 04:06 PM	ICX 7150-B [192.168.5.242] is ONLINE
Created	Name	Message	Severity	Cured	Reason																																																								
01/23/2023 11:14 AM	My Ip Conflict	another device is using my IP address!	Critical	01/25/2023 04:10 PM	I had two RWGs with the same address																																																								
01/23/2023 11:22 AM	Monitor Infrastructure Device 62	Unreachable: vSZ-249 - Failed to open TCP connection to 192.168.5.249:8443 [Connection refused - connect(2) for 192.168.5.249:8443]	Warning	-	-																																																								
01/24/2023 08:55 AM	Infrastructure Device 62 Monitor	vSZ-249 [192.168.5.249] is OFFLINE	Notice	-	-																																																								
01/24/2023 12:36 PM	Ping Target 1 Monitor	Google Public DNS 1 [8.8.8.8] is OFFLINE	Notice	-	-																																																								
01/24/2023 12:37 PM	Ping Target 2 Monitor	Google Public DNS 2 [8.8.4.4] is OFFLINE	Notice	-	-																																																								
01/24/2023 12:37 PM	Monitor Infrastructure Device 61	Unreachable: vSZ-MM - Failed to open TCP connection to vszh-mm.ruckusdemos.net:8443 [getaddrinfo: Name does not resolve]	Warning	-	-																																																								
01/25/2023 04:04 PM	Ntp Server	NTP is not synchronized	Warning	-	-																																																								
01/22/2023 04:58 PM	Infrastructure Device 53 Monitor	ICX 7150-B [192.168.5.242] is OFFLINE	Notice	01/25/2023 04:06 PM	ICX 7150-B [192.168.5.242] is ONLINE																																																								

FIGURE 54 – NOTIFICATION LOGS/HEALTH NOTICE

## RADIUS Logs

The RADIUS Logs show the expired VLAN Tag Assignments:

Expired VLAN Tag Assignments									
Assigned	Expired	MAC	VLAN	Tag	Account	Group	Duration	RADIUS Server Realm	Called-Station MAC
01/22/2023 07:30 AM	01/22/2023 04:58 PM	Q 38f9:d3d4:c0:78	Client VLANs	405	-	-	9 hours and 28 minutes	Microsegmentation Realm	b4:79:c8:0d:76:30
01/21/2023 05:28 PM	01/21/2023 06:29 PM	Q 6e9b:45:33:32:a0	Client VLANs	404	simone	VLAN 700	1 hour	Microsegmentation Realm	b4:79:c8:0d:76:30
01/21/2023 05:28 PM	01/21/2023 10:58 PM	Q 38f9:d3d4:c0:78	Client VLANs	402	-	-	5 hours and 30 minutes	Microsegmentation Realm	b4:79:c8:0d:76:30
01/21/2023 03:06 PM	01/21/2023 04:59 PM	Q 7a8f:7a:1c:84:63	Client VLANs	400	-	-	less than 1 second	-	b4:79:c8:0d:76:30
01/21/2023 07:11 AM	01/21/2023 05:19 PM	Q ae:e5:cb:69:08:2a	VLAN 700	700	simone	VLAN 700	less than 1 second	VLAN 700 Realm	b4:79:c8:0d:76:30
01/21/2023 07:11 AM	01/21/2023 01:43 PM	Q 6e9b:45:33:32:a0	VLAN 700	700	simone	VLAN 700	6 hours and 32 minutes	VLAN 700 Realm	b4:79:c8:0d:76:30
01/21/2023 07:10 AM	01/21/2023 07:11 AM	Q 6e9b:45:33:32:a0	VLAN 600	600	marcelo	VLAN 600	less than 1 second	VLAN 600 Realm	b4:79:c8:0d:76:30
01/21/2023 07:03 AM	01/21/2023 07:09 AM	Q ae:e5:cb:69:08:2a	VLAN 600	600	marcelo	VLAN 600	less than 1 second	VLAN 600 Realm	b4:79:c8:0d:76:30
01/21/2023 06:52 AM	01/21/2023 07:02 AM	Q ae:e5:cb:69:08:2a	VLAN 700	700	simone	VLAN 700	less than 1 second	VLAN 700 Realm	b4:79:c8:0d:76:30
01/21/2023 06:49 AM	01/21/2023 07:08 AM	Q 6e9b:45:33:32:a0	VLAN 600	600	marcelo	VLAN 600	less than 1 second	VLAN 600 Realm	b4:79:c8:0d:76:30

FIGURE 55 – RADIUS LOGS/EXPIRED VLAN TAG ASSIGNMENTS

## .log Files

Here you can see all details for the RADIUS and DHCP handshake:

```

280]: Signalled to terminate
280]: (42) Login OK: [368c2e7655a7] (from client 192.168.5.249/32 port 0 cli 36-8C-2E-76-55-A7) User-Name:
  > main::post_auth - performing post_auth
  > main::log_request_to_database - logging Access-Accept for username 368c2e7655a7
  > main::append_attributes - reply AVP: Tunnel-Private-Group-Id => %vlan_tag_assignment.tag% (301)
  > main::append_attributes - reply AVP: Tunnel-Medium-Type => IEEE-802
  > main::append_attributes - reply AVP: Tunnel-Type => VLAN
  > main::append_attributes - appending RadiusServer "Onboarding Realm" Attributes to the reply
  > main::perform_vta - assigning MAC 36:8c:2e:76:55:a7 to new VTA on Vlan "Onboard VLANs" with tag 301
  > Rng:Util::seedRNG - seeding rand using /dev/random
  > main::perform_vta - selected Vlan "Onboard VLANs" for tag pool of size 16
  > main::perform_vta - MAC 36:8c:2e:76:55:a7 does not have an existing VTA to use
  > main::perform_vta - trying to assign a Vlan tag
  > main::perform_vta - using Calling-Station-Id as the end-user's MAC: 36:8c:2e:76:55:a7
  > main::find_radius_server - found configured RadiusServer "Onboarding Realm" for the request
  > main::realm_matches_request - selected highest priority(0) matching RadiusAttributePattern "Titan" for t
  > main::realm_matches_request - request matches pattern set in RadiusServer "Onboarding Realm" rank(t
  > main::find_match_attributes - AVP Called-Station-Id => 34-20-E3-A8-0D-A3: Titan matches RadiusAttribute
  > main::find_match_attributes - trying to find a RadiusAttributePattern set matching the request
  > main::find_match_attributes - trying to find a RadiusAttributePattern set matching the request
                
```

```

ig-home.ruckusdemos.net dhcpd[60944]: DHCPREQUEST for 192.168.5.245 from 54:ec:2f:04:59:30 via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPACK on 192.168.5.252 to 94:c6:91:15:80:87 via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPREQUEST for 192.168.5.252 from 94:c6:91:15:80:87 via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPACK on 192.168.5.249 to 00:0c:29:84:07:bb via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPREQUEST for 192.168.5.249 from 00:0c:29:84:07:bb via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPACK on 192.168.5.253 to b4:79:c8:0d:76:30 via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPREQUEST for 192.168.5.253 from b4:79:c8:0d:76:30 via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPACK on 70.0.0.2 to 6e:9b:45:33:32:a0 via vlan700
ig-home.ruckusdemos.net dhcpd[60944]: DHCPREQUEST for 70.0.0.2 from 6e:9b:45:33:32:a0 via vlan700
ig-home.ruckusdemos.net dhcpd[60944]: DHCPACK on 60.0.0.3 to ae:e5:cb:69:08:2a via vlan600
ig-home.ruckusdemos.net dhcpd[60944]: Wrote 2 leases to leases file.
ig-home.ruckusdemos.net dhcpd[60944]: Wrote 0 new dynamic host decls to leases file.
ig-home.ruckusdemos.net dhcpd[60944]: Wrote 0 class decls to leases file.
ig-home.ruckusdemos.net dhcpd[60944]: Wrote 0 class decls to leases file.
ig-home.ruckusdemos.net dhcpd[60944]: DHCPREQUEST for 60.0.0.3 from ae:e5:cb:69:08:2a via vlan600
ig-home.ruckusdemos.net dhcpd[60944]: DHCPACK on 192.168.5.247 to 34:20:e3:28:0d:a0 via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPREQUEST for 192.168.5.247 from 34:20:e3:28:0d:a0 via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPACK on 192.168.5.242 to d4:c1:9e:9a:f6:16 via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPREQUEST for 192.168.5.242 from d4:c1:9e:9a:f6:16 via igb3
ig-home.ruckusdemos.net dhcpd[60944]: DHCPACK on 192.168.5.245 to 54:ec:2f:04:59:30 via igb3
                
```

FIGURE 56 – RADIUS SERVER AND DHCP SERVER LOGS

## Search Tool

The **Search** button at the top right corner is not for searching documents. It's for searching devices (either infrastructure devices or client devices). You will see the identity groups, sessions in use, and policies applied to the device. In the example we entered the IP address for an adopted ICX switch. The policy that is in use by the device is marked **active**.

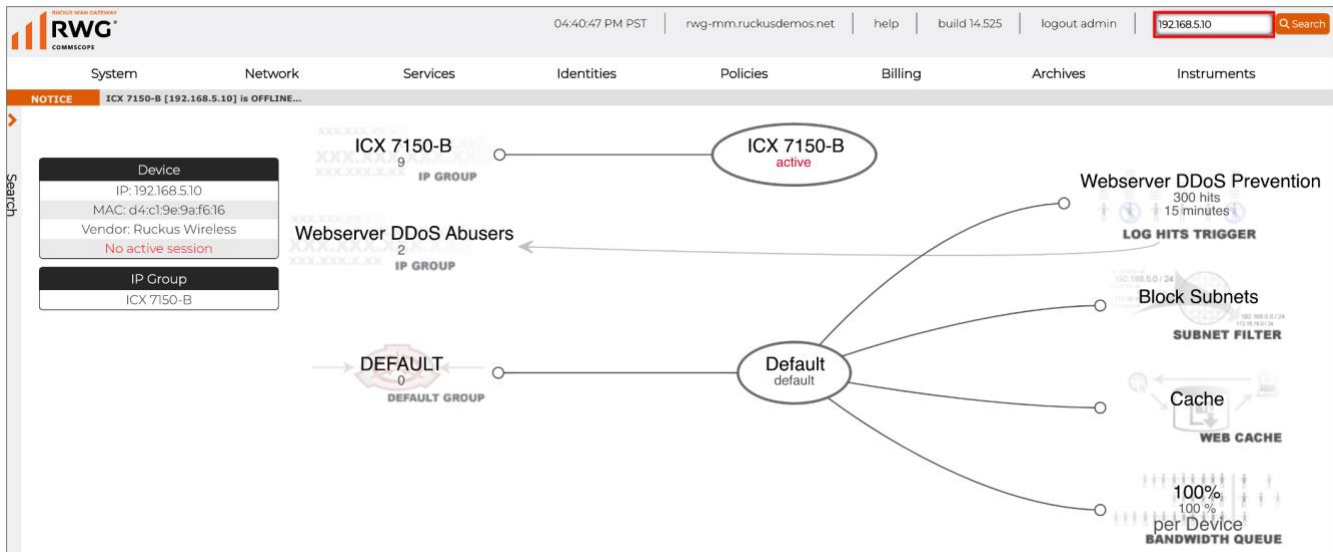


FIGURE 57 – THE SEARCH TOOL

You can also search devices by MAC address, client last name or room number.

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

We encourage you to visit [commscope.com](https://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](https://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**<sup>®</sup>  
COMMSCOPE