



# Optimizer

ADVANCED USER GUIDE  
FOR WXA-223

**Revision History**

| Doc Rev | Date      | Name             | Changes Made             |
|---------|-----------|------------------|--------------------------|
| 1.0.0.  | 16FEB2022 | Bethany Headrick | Issued as version 1.0.0. |

## Table of Contents

|  |           |
|--|-----------|
| REVISION HISTORY .....   | 1         |
| <b>1. ABOUT THIS GUIDE.....</b>  | <b>4</b>  |
| <b>2. INTRODUCTION TO THE REDPORT OPTIMIZER.....</b>                                     | <b>4</b>  |
| 2.1. OPTIMIZER KEY FEATURES.....   | 5         |
| 2.2. SERVICES INCLUDED.....  | 6         |
| 2.3. PREMIUM SERVICES AVAILABLE .....  | 7         |
| <b>3. SAFETY .....</b>   | <b>8</b>  |
| <b>4. THINGS TO KNOW BEFORE GETTING STARTED.....</b>                                     | <b>9</b>  |
| 4.1. MORE THAN JUST A ROUTER .....   | 9         |
| 4.2. HOW IT WORKS OUT OF THE BOX .....   | 10        |
| <b>5. GETTING STARTED – USER INTERFACE (UI) ACCESS.....</b>                              | <b>11</b> |
| 5.1. ACCESS THE PORTAL DASHBOARD .....   | 12        |
| 5.1.1. THE DASHBOARD AND WIDGETS.....  | 14        |
| <b>6. ROUTER SECURITY.....</b>   | <b>16</b> |
| 6.1. FIREWALL SETTINGS .....   | 16        |
| 6.2. ADVANCED FIREWALL SETTINGS .....  | 17        |
| 6.2.1. <i>General Settings</i> .....   | 17        |
| <b>7. SERVICES.....</b>  | <b>19</b> |
| 7.1. REDPORT PBX.....  | 19        |
| 7.1.2. <i>Voice PBX Settings</i> .....   | 21        |
| 7.1.3. <i>SIP Extensions</i> .....   | 23        |
| 7.2. REDPORT VOIP .....  | 24        |
| 7.2.1. <i>How to Make and Receive Voice Calls</i> .....                                  | 26        |
| 7.3. SMS MESSAGING.....  | 27        |
| 7.3.1. <i>How to Send SMS Messages through the User Interface</i> .....                  | 29        |
| 7.3.2. <i>Received Messages</i> .....  | 30        |
| 7.3.3. <i>Sent Messages</i> .....  | 31        |
| 7.3.4. <i>Sending SMS Messages through the XGate Phone Application</i> .....             | 32        |
| 7.4. EMAIL AND WEB BROWSING.....   | 33        |
| 7.5.0. WEB COMPRESSION AND FILTERING.....  | 34        |
| 7.5.1. <i>Setting Up Satellite Web Compression</i> .....                                 | 34        |
| 7.5.3. <i>Advanced Settings</i> .....  | 40        |
| 7.5.4. <i>Filters</i> .....  | 41        |
| 7.6. FLEETBROADBAND MONITOR (FBB) .....  | 42        |
| 7.7. HALO WI-FI EXTENDER .....   | 45        |
| 7.7.1. <i>Configure Optimizer for use with the Halo Single Band Wi-Fi Extender</i> ..... | 45        |
| 7.7.2. <i>Configure Optimizer for use with the Halo Pro Wi-Fi Extender</i> .....         | 47        |
| 7.7.3. <i>Disconnect from the Halo Wi-Fi</i> .....                                       | 48        |
| 7.8. GPS TRACKING.....   | 49        |
| 7.8.1. <i>Tracking powered by RedPort</i> .....  | 49        |
| 7.8.2. <i>SMS Tracking</i> .....   | 49        |
| 7.9. GPS/NMEA REPEATER .....   | 50        |
| 7.9.1. <i>GPS/NMEA Repeater Equipment Setup</i> .....                                    | 50        |
| <b>8. STATUS UNDER SYSTEM SETTINGS.....</b>  | <b>56</b> |

- 8.1. ACCESS SYSTEM LOG..... 56
- 8. SYSTEM SETTINGS..... 57
  - 8.1. UPDATE FIRMWARE ..... 57
  - 8.2. PROFILE MANAGER ..... 57
  - 8.3. REBOOT THE OPTIMIZER ROUTER..... 58
- 9. WI-FI..... 59
  - 9.1. RESTRICT WIRELESS NETWORK ACCESS (ADD OR CHANGE NETWORK PASSWORD) ..... 59
  - 9.2. RENAME THE WIRELESS NETWORK (CHANGE SSID NAME) ..... 61
- 10. PRODUCT WARRANTY AND SUPPORT INFORMATION ..... 62
  - 10.1. PRODUCT WARRANTY INFORMATION ..... 62
  - 10.2. PRODUCT SUPPORT INFORMATION ..... 63

## 1. About this Guide

This guide is intended for users of the RedPort Optimizer wXa-223 router. It features only those sections of the user interface that require configuration for a specific service or feature that may need to be accessed by the average user.

## 2. Introduction to the RedPort Optimizer

RedPort, the leader in advancing satellite data speeds and services, helps Fixed and Mobile Satellite Services providers and their customers by offering the industry's fastest and most reliable, email, web, VoIP and other hardware and software services to maritime, oil and gas, first responder, and business continuity users.

Ship to shore network management solutions are sold by Pivotal under the RedPort brand name at [redportglobal.com](http://redportglobal.com), and as white-label solutions for the world's premier satellite data service providers.

Optimizer is a satellite Wi-Fi router that combines a powerful satellite data router with voice capabilities, including a full PBX. It is more than just a voice device. It gives you everything you need to create a local voice and data network with your satellite device. You can protect against accidental airtime usage, accelerate your data speeds, enable web compression, track your location via GPS, and provide routing, filtering, and local network security.

## 2.1. Optimizer Key Features

Designed specifically for use with satellite phones and satellite terminals:

- Replaces a standard unconfigured router that is typically added to any satellite broadband installation.
- Powerful firewall accommodates any common installation scenario, with features including blocking or allowing of any range of port, IP address and protocols.
- Proxy Server enables HTTP filtering: whitelist/blacklist of URLs, domains, and rudimentary content filtering.
- Logging/Reporting to keep track of usage.
- Wi-Fi hotspot makes setup and use easy for end users. Access satellite devices via Optimizer's Wi-Fi hotspot with computers, smartphones, and tablets you already own.
- Supports Shared Web Compression.
- GSM Compatibility - bring your own GSM modem and own SIM card.
- GPS NMEA Repeater reads the built-in GPS in any satellite broadband terminal and rebroadcasts via Wi-Fi.
- Supports voice calling and SMS messages using smartphones connected to the local network.
- Compatible with any IP-based satellite phone and satellite broadband terminal.
- Powerful firewall stops all unwanted data traffic. Optimizer blocks all traffic except XGate-compressed email, web, and weather data.
- Works with XGate for email, web, weather, and social media services.
- GSM support to switch between satellite and GSM when available.
- Track GPS locations from compatible GPS-enabled devices.
- Compatible with optional RedPort Halo Wi-Fi Extender and/or RedPort Halo Pro Wi-Fi Extender for access to external Wi-Fi networks, when available.

*NOTE: XGate and Tracking services are premium services. Premium services are not included with the Optimizer and must be purchased separately. Contact your satellite service provider for details.*

## 2.2. Services Included

**Halo Wi-Fi Extender** - The Halo Long Range Wi-Fi Extender allows users to connect to remote Wi-Fi signal (e.g. at a marina, truck stop, or basecamp) and repeats that signal through the RedPort Optimizer Wi-Fi hotspot. Requires a RedPort Halo Long Range Wi-Fi Extender or Halo Pro Long Range Wi-Fi Extender.

**PBX** - Voice PBX allows smartphones to send/receive calls to others on the local area network for free, or over the satellite link at standard satellite airtime rates. Requires a supported satellite terminal.

**SMS Messaging** - SMS Messaging allows smartphones to send SMS messages to others on the local area network for free, or over the satellite link at standard satellite airtime rates. Requires a supported satellite terminal.

**GPS NMEA Repeater** – GPS NMEA Repeater allows other devices onboard/on-site to read your GPS location. For example, a navigation program running on an iPad could be used on your boat, or you could get weather information tailored to your location. Requires a connected GPS NMEA device.

**Fleet Broadband Monitor** - Fleet Broadband Monitor provides vessel side users with visual indications of the Cobham Fleet Broadband terminal status by augmenting the blink patterns of the RedPort Optimizer. The service also restricts access to the Optimzier devices to all users except the admin. This service requires a Cobham Fleet Broadband satellite terminal.

**Support Remote Access** - Support Remote Access provides remote access and control capabilities. While remote access service is included with the purchase of RedPort hardware any airtime used and charges incurred providing connection for the remote user is the responsibility of the customer. Requires a connection source (e.g. satellite terminal with active airtime.)

**NAS Server** - Allows the sharing of files among Windows and Mac computers via Wi-Fi, without the requirement of a wired local network of computers.

### 2.3. Premium Services Available

The following additional services are available for purchase. Contact your RedPort dealer to purchase.

**XGate Local Mail Server** - XGate Local Mail Server is an onboard mail server running on your Optimizer router. This mail server can be connected to over your local network with an email client, and will transmit email using XGate compression over your upstream connection. XGate service subscription required.

**PredictWind Weather Services** - PredictWind provides the top ranked forecast models globally. These leading models are only available through PredictWind, giving unparalleled weather data. For High Resolution coastal forecasts the PWG & PWE proprietary models offer unparalleled forecast accuracy, complemented by the regional NAM, HRRR, and AROME models. Requires service subscription.

**GPS Tracking** - Reliably tracks personnel, equipment, vessels, or vehicles anywhere in the world. Using a connected GPS-enabled device, submit position reports to a central database for reporting or viewing on a tracking website. Requires service subscription.

**RedPort VoIP Service** - RedPort VoIP service transforms your satellite device into a multi-user unit. Up to four users can send/receive phone calls and/or SMS (text) messages simultaneously. Experience significant price reduction in outbound calls when using VoIP in lieu of standard satellite airtime rates. Requires a supported satellite terminal. Requires service subscription. Multi-VoIP codec powered by Vobal.

**RedPort Shared Web Compression** - RedPort Shared Web Compression routes all web traffic through a proxy service that works with an onshore server to deliver 3-5 times average web compression, along with virus detection and ad blocking. Requires service subscription.



### 3. Safety



#### **Shock Hazard**

The Optimizer is a sealed device and is not meant to be opened for repair in the field by operators or technicians. The enclosure must always remain in place on the router to maintain the warranty terms. Make sure the system is correctly grounded and power is off when installing, configuring, and connecting components.



#### **Passive POE Port(s)**

The Optimizer has a SAT (WAN) and LAN port that are Passive POE. Connecting any device such as a laptop or switch with a Gigabit ethernet, 1000Mbps speed NIC will potentially put your device or port at risk of damage or burn out. RedPort does not provide coverage or warranty for this damage. Connect any device of this nature at your own risk.



#### **Proposition 65**

This product can expose you to Acrylonitrile, which is known to the State of California to cause cancer. For more information go to [www.P65Warnings.ca.gov](http://www.P65Warnings.ca.gov).

## 4. Things to Know Before Getting Started

As the onboard/onsite administrator, under normal operating conditions, you will seldom have a need to interact with the user interface of the router. However, should you find yourself in a position that requires you to login to the router, this Advanced User Guide is designed to help you.

### 4.1. More Than Just a Router

The Optimizer is more than just a router. It has some enhanced proxy services in addition to basic routing capabilities.

**Proxy Server(s)** - With transparent proxy enabled, all HTTP traffic is redirected through the proxy without the need to reconfigure the client. The proxy server allows automatic URL filtering and logging, and content filtering (e.g., strip flash video from pages). Logging will also allow auditing of high usage sites that generate traffic.

**NOTE:** If enabling the transparent proxy, make sure there is an exception for the Router's IP (usually 192.168.10.1). Otherwise, the Router UI will be inaccessible.

**Firewall** - A full-featured firewall is included. Block or allow IP address/ranges, port ranges, and/or different protocols. Rules can be applied to any path in and out of the router.

## 4.2. How It Works Out of the Box

We ship the router ready for use with a RedPort-certified compression email and/or web browsing account (which must be purchased separately).

This default setup allows anyone with an XGate or RedPort-Certified email account or web service to use the router to send and receive email and to browse the Internet.

This out-of-the-box configuration works well for both single and multi-user environments.

This configuration is also suitable for an environment where each person has a separate primary email and/or web browsing account.

If you are in a multi-user environment, we recommend enabling Transparent proxy for use with web compression. With Transparent Proxy enabled, all HTTP traffic is redirected through the internal proxy server. This allows URL and DNS filtering (whitelist and blacklist sites), some content filtering (i.e., removing flash video), and http logging to see what URLs are being accessed by the users. You also have the option to communicate upstream to a compression proxy server. For savings on voice calls consider RedPort VoIP service. You may realize further savings by enabling satellite web compression (see Section 6.5.0.).

Best Practice is to have a knowledgeable technician (someone who knows about proxy servers and routers) go through and generate a custom configuration. In a fleet environment, this custom configuration can be recorded and used on other Optimizer routers within the organization.

## 5. Getting Started – User Interface (UI) Access

The Optimizer router arrives to you with a Closed Firewall allowing email and web access via RedPort-certified services only.

There are also services available that are disabled:

- Internal Transparent Proxy for Web Filtering.
- SMS for compatible satellite devices.
- Voice Capability for compatible satellite devices.
- Web Compression\*
- GPS Tracking\*
- RedPort VoIP for multi-user calls and SMS\*
- GPS/NMEA Repeater.

\*Premium services – additional fees apply. Contact Pivotel or your RedPort authorized dealer for details.

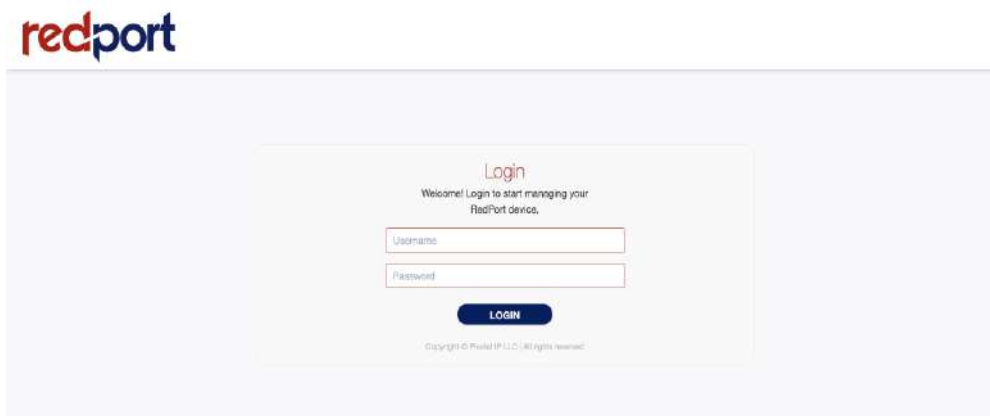
## 5.1. Access the Portal Dashboard

Access the UI by logging in using the superadmin login.

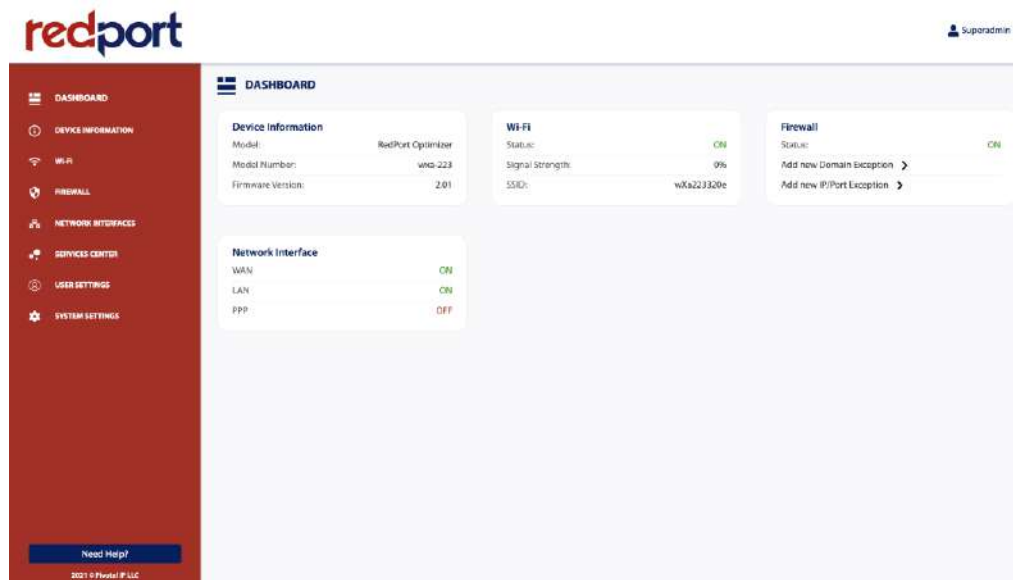
1. To access the User Interface, first ensure that your computer is connected to the Optimizer router Wi-Fi, which will show up in your Wi-Fi preferences as “wxa-223-XXXX,” where “XXXX” matches the last four characters of the MAC address for that specific device.



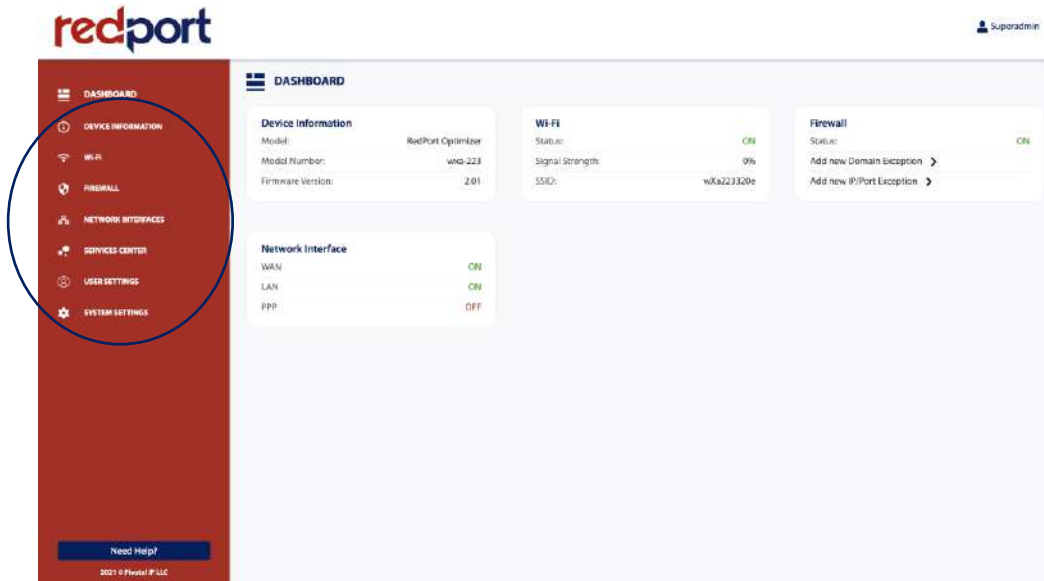
2. Connect your device to this Wi-Fi source and use the login:  
Username: superadmin  
Password: webxaccess



You will see the Dashboard page upon login.



The tabs on the side of the Dashboard page are used to navigate the features and services activated on the router.

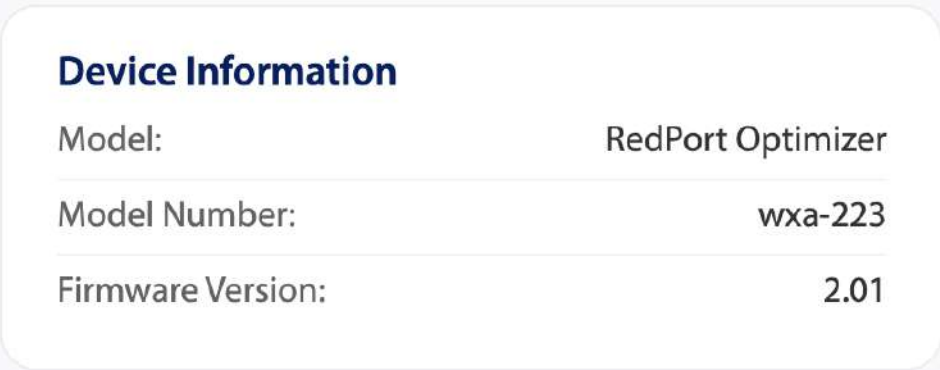


NOTE: The Wi-Fi Extender Setup section only displays when the Wi-Fi Extender is plugged into the Optimizer and “ACTIVATED” in the Services Center. See section 7.7 for details on how to use the Extender with the Optimizer.

### 5.1.1. The Dashboard and Widgets

The Dashboard is the onsite administrator's gateway to the most used features. On the Dashboard are the four main widgets that you see upon login: "Device Information," "Wi-Fi," "Firewall," and "Network Interface."

#### Device Information Widget



| Device Information |                   |
|--------------------|-------------------|
| Model:             | RedPort Optimizer |
| Model Number:      | wxa-223           |
| Firmware Version:  | 2.01              |

The Device Information widget shows basic information about the Optimizer device, such as the model, model number, and firmware version. This information is helpful when troubleshooting problems with the router as it gives the user the basic overview of the device at an immediate glance.

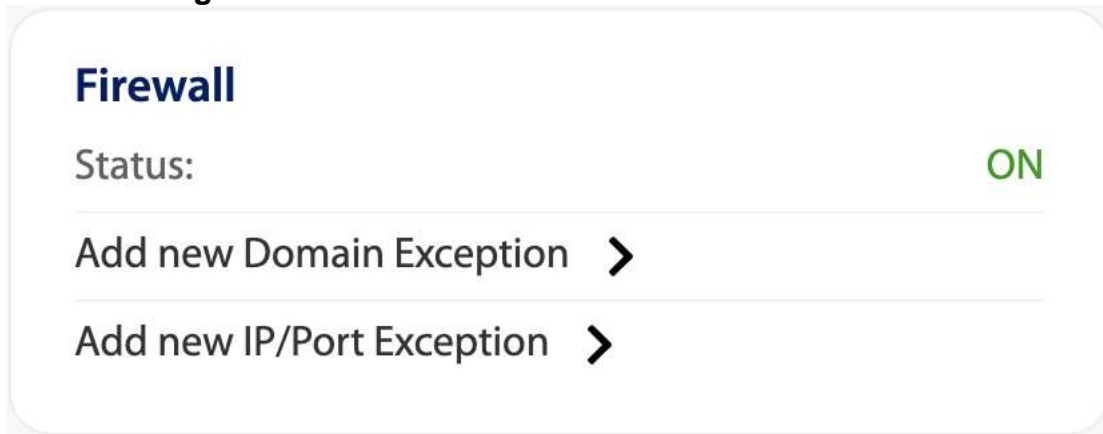
#### Wi-Fi Widget



| Wi-Fi            |            |
|------------------|------------|
| Status:          | ON         |
| Signal Strength: | 0%         |
| SSID:            | wXa223320e |

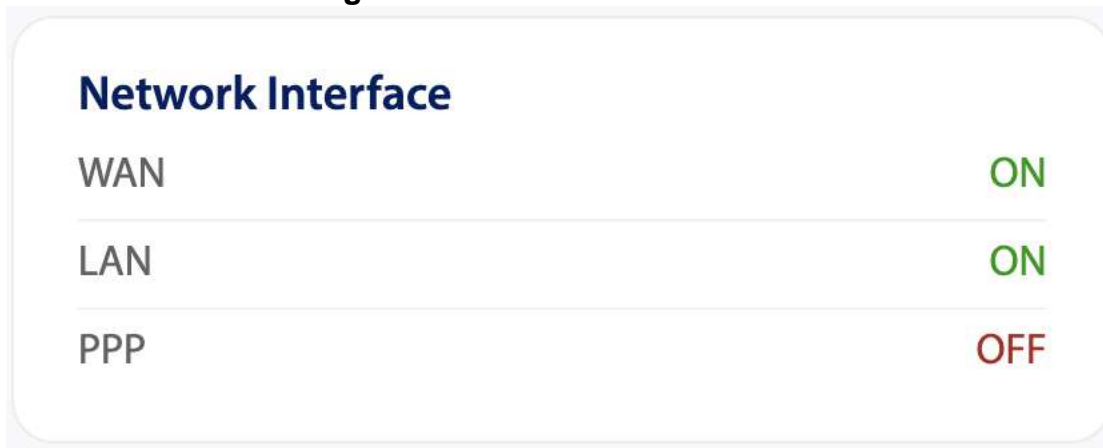
The Wi-Fi Widget shows the Status of the Wi-Fi network coming off the Optimizer (OFF or ON), the Signal Strength shows the strength of the Optimizer Wi-Fi network, and the SSID shows the name of the Optimizer Wi-Fi network as it will show in the Wi-Fi settings on your computer, tablet, or phone.

## Firewall Widget



The Firewall Widget shows the Status of the Firewall (OFF or ON) and allows the user to add a new Domain Exception or new IP/Port Exception to the Firewall Rules. Clicking into the Firewall widget takes the user to the Firewall tab, where the user can click on “Advanced Firewall Configuration” to access advanced settings where the user can further edit the Firewall.

## Network Interface Widget



The Network Interface Widget shows an overlook of the WAN, LAN, and PPP interfaces. This widget shows whether each interface is ON or OFF. To edit these interfaces, hover over the widget and click anywhere within it to access Network Interface settings.



## 6. Router Security

If you modify the default settings of the firewall you may have WAN ports open. RedPort is not responsible for any overages incurred due to unrecommended changes in Firewall rules.

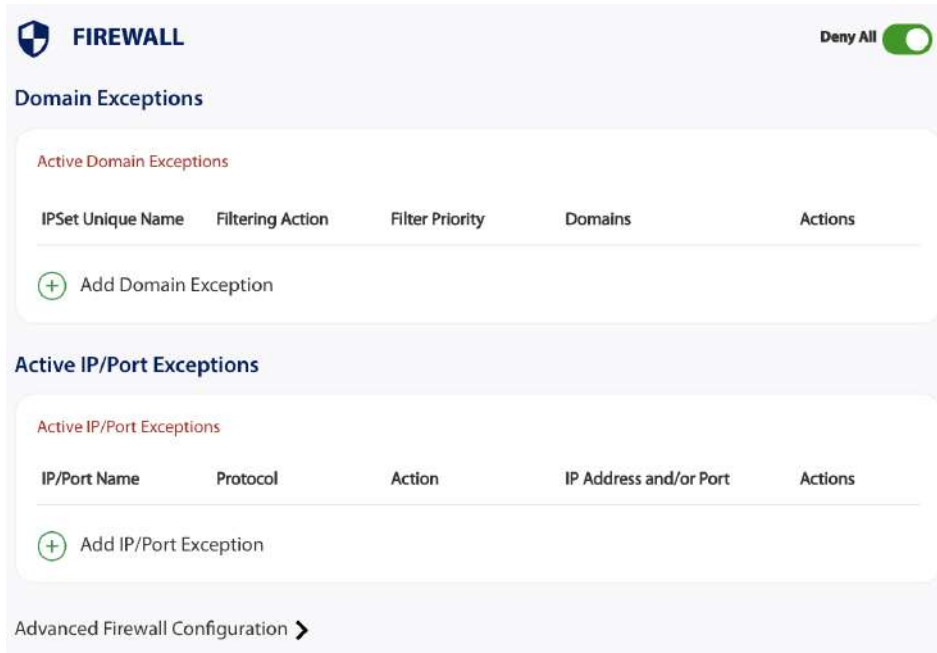
Any firewall changes could leave you vulnerable to unwanted traffic. Note that ports open to the Internet on satellite systems that have public IP addresses are vulnerable to attackers that run dictionaries trying to guess usernames and passwords on the router. These dictionary attacks, at best, can result in large amounts of accounted traffic; and, at worst, they are a security breach that could endanger communications on the vessel. Systems open to public Internet must take special precautions to secure the router from intrusion.

Web Proxy is not a problem, by default, unless you make changes since the software, by default, only listens to traffic on the LAN.

### 6.1. Firewall Settings

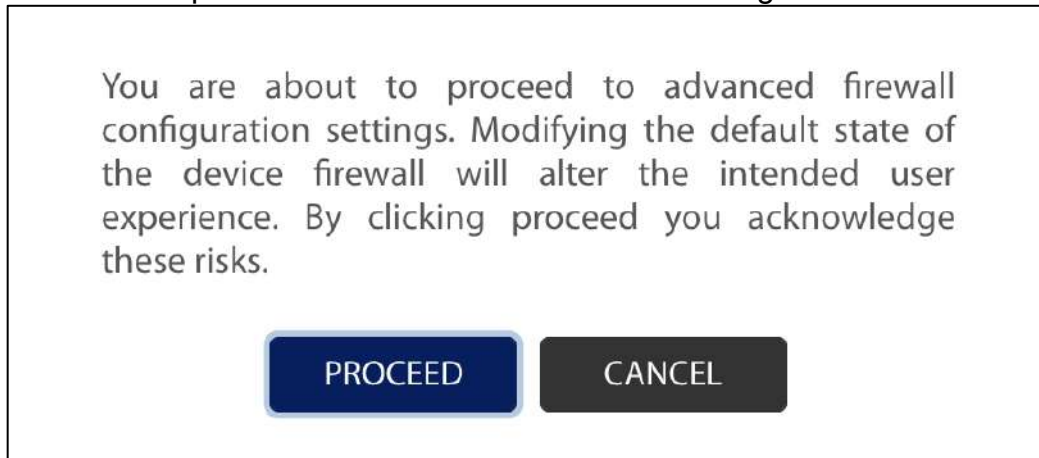
To navigate to the Firewall page, click on the “Firewall” module on the Dashboard.





## 6.2. Advanced Firewall Settings

Click on “Advanced Firewall Configuration” and a window will pop up asking if you would like to proceed to the Advanced Firewall Settings. Click “Proceed.”



### 6.2.1. General Settings

Use this section to create and edit general Firewall rules.

**General Settings**

|                             |                                     |
|-----------------------------|-------------------------------------|
| Enable SYN-flood protection | <input checked="" type="checkbox"/> |
| Drop invalid packets        | <input type="checkbox"/>            |
| Input                       | reject ▾                            |
| Output                      | accept ▾                            |
| Forward                     | reject ▾                            |

**Enable SYN-flood protection:** SYN-flood protection protects against Distributed Denial of Service attacks that would hinder the use of the Optimizer. Best Practice is to leave this box ticked.

**Input:** access to the router itself.

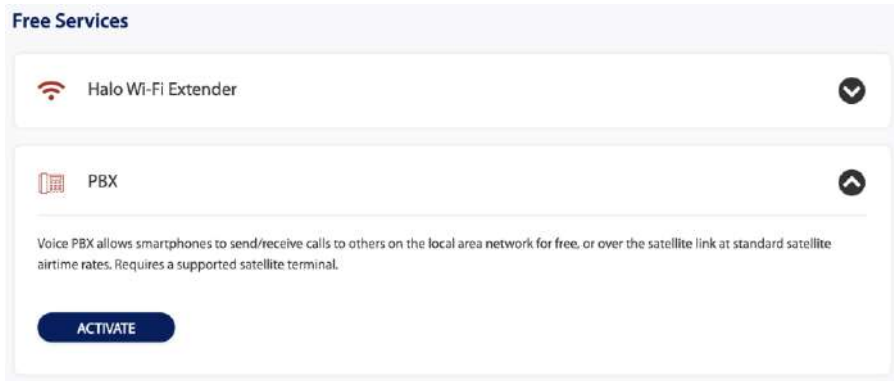
**Output:** access to the "lan". DO NOT MODIFY.

**Forward:** pass traffic thru the router via an interface and out of the router. If Forward is allowed you must configure the Inter-Zone Forwarding.

## 7. Services

### 7.1. RedPort PBX

1. To enable Voice PBX, navigate to the Services Center and expand the Voice PBX tab under “Free Services.”



2. Click “ACTIVATE” then when the confirmation window pops up, choose “ACTIVATE” to confirm your choice.



3. Navigate to the side menu and choose “PBX” to access the PBX Settings page.



4. On the PBX page, tick the box for “Enable/Disable PBX” and click “Save Changes” to apply the change.

 **PBX**

|                   |  |
|-------------------|--|
| Enable/Disable    | <input checked="" type="checkbox"/> Enable/Disable PBX   |
| Listen Port       | <input type="text" value="5060"/><br><small>Port used by the PBX to listen for SIP traffic. Leave blank for default port 5060.</small> |
| Listen Interfaces | <input type="text" value="ALL - 0.0.0.0"/> <small>Bind proxy to the following interfaces.</small>                                      |

**SAVE CHANGES**

## 7.1.2. Voice PBX Settings

The Optimizer allows unlimited SIP extensions with free local calling and text messaging within your local area network using the XGate Phone app.\*

\*XGate Phone app is available for free in the Apple iTunes App Store and in the Google PlayStore.

When the PBX is enabled, it is listening on the interface you specify. This may leave you vulnerable to unwanted traffic if you expose it to the internet. We recommend configuring it to use the LAN interface for this reason.

The screenshot displays the RedPort PBX configuration interface. On the left is a navigation menu with options like DASHBOARD, DEVICE INFORMATION, WI-FI, FIREWALL, NETWORK INTERFACES, HALO WI-FI EXTENDER, PBX, SMS MESSAGING, XGATE, RedPort VoIP, SERVICES CENTER, USER SETTINGS, and SYSTEM SETTINGS. The main content area is titled 'PBX' and includes the following settings:

- Enable/Disable:** A checkbox labeled 'Enable/Disable PBX' is checked.
- Listen Port:** A text input field contains '5060'. Below it, a note states: 'Port used by the PBX to listen for SIP traffic. Leave blank for default port 5060.'
- Listen Interfaces:** A dropdown menu is set to 'ALL - 0.0.0.0'. Below it, a note states: 'Bind proxy to the following interfaces.'
- A 'SAVE CHANGES' button is located below the settings.

Below the settings is a section titled 'SIP Extensions' containing a table:

| Extension | Password | Caller ID | Description  | Ring                                | SMS                                 |  |
|-----------|----------|-----------|--------------|-------------------------------------|-------------------------------------|--|
| 201       | 1234     | 201       | Captain line | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |
| 202       | 1234     | 202       | Crew line 1  | <input type="checkbox"/>            | <input type="checkbox"/>            |  |
| 203       | 1234     | 203       | Crew line 2  | <input type="checkbox"/>            | <input type="checkbox"/>            |  |
| 204       | 1234     | 204       | Crew line 3  | <input type="checkbox"/>            | <input type="checkbox"/>            |  |

At the bottom of the table is a '+ Add SIP Extension' button.

Users with smartphones can send and receive voice calls and SMS messages over the following satellite communication setups:

- Sailor FBB terminal - requires XGate Phone app.\*
- Any satellite terminal with an RJ-11 port requires a soft phone app or XGate Phone app.\*

This configuration allows one voice call or one SMS message at a time and standard satellite voice airtime rates apply.

Multi-VoIP capability is available with the optional RedPort VoIP service on virtually any satellite terminal. This VoIP service allows you to make calls for considerably less than standard satellite voice airtime costs and allows up to four users sending/receiving phone calls and/or SMS messages simultaneously. As of this writing, Multi-VoIP is compatible with the following:

- FBB/GX
- BGAN
- VSAT
- RedPort Aurora and Glow
- Iridium Pilot/Certus
- Thuraya MarineStar

The Optimizer allows unlimited SIP extensions with free local calling and text messaging within your local area network using the XGate Phone app.\*

\*XGate Phone app is available for free in the Apple iTunes App Store and in the Google PlayStore.







**CAUTION:** Before enabling the PBX service, read section titled, “Router Security.” When you enable the SMS service, it is listening on all ports. Without further configuration, this could leave you vulnerable to unwanted traffic.


### 7.1.3. SIP Extensions

By default, there are 4 extensions enabled. Extension 201 is enabled for inbound and outbound calling. The remaining extensions are enabled but are configured for outbound calling only.

Incoming calls will ring only on those extensions with Ring enabled.

**SIP Extensions**

| Extension | Password | Caller ID | Description  | Ring                                | SMS                                 |   |
|-----------|----------|-----------|--------------|-------------------------------------|-------------------------------------|---|
| 201       | 1234     | 201       | Captain line | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |
| 202       | 1234     | 202       | Crew line 1  | <input type="checkbox"/>            | <input type="checkbox"/>            |  |
| 203       | 1234     | 203       | Crew line 2  | <input type="checkbox"/>            | <input type="checkbox"/>            |  |
| 204       | 1234     | 204       | Crew line 3  | <input type="checkbox"/>            | <input type="checkbox"/>            |  |

 Add SIP Extension

To enable Ring or SMS on an extension, simply check the box for the service you want enabled.

When Ring is checked, the smartphone configured with the corresponding Extension will Ring with every incoming call.

When SMS is checked that smartphone will receive every incoming SMS message.

To use a smartphone to send and/or receive phone calls requires a soft phone or XGate Phone app installed on the smartphone. The XGate Phone app can be found in Apple iTunes App Store for iOS devices and the Google Playstore for Android devices.

The smartphone user configures the XGate Phone app with their corresponding SIP Extension.

On this page, you can also:

- Change the SIP extension password
- Change the outgoing CallerID display
- Enter a description for your reference



## 7.2. RedPort VoIP

Voice is disabled by default but can be enabled for use with compatible satellite devices using standard satellite airtime.

1. To utilize the RedPort VoIP services, first activate PBX Services under the Services Center.
2. You will be navigated to the PBX Services tab. Tick the box for “Enable/Disable PBX” and click “Save Changes” to apply the change.



### PBX

Enable/Disable



Enable/Disable PBX

Listen Port

Port used by the PBX to listen for SIP traffic. Leave blank for default port 5060.

Listen Interfaces

Bind proxy to the following interfaces.

SAVE CHANGES

3. Under the Services Center, Activate “RedPort VoIP Services.”



RedPort VoIP



RedPort VoIP service transforms your satellite device into a multi-user unit. Up to four users can send/receive phone calls and/or SMS (text) messages simultaneously. Experience significant price reduction in outbound calls when using VoIP in lieu of standard satellite airtime rates. Requires a supported satellite terminal. Requires service subscription. Multi-VoIP codec powered by Vobal.

ACTIVATE

- a. When the window pops up asking if you would like to proceed, click “Proceed.”

Are you sure you want to activate RedPort VoIP?

ACTIVATE

CANCEL

4. In the “VOIP” tab, fill out the form with information provided to you by your RedPort dealer or reseller.
  - a. MAC Address: Check the bottom of the Optimizer unit to see the MAC Address, and enter it in this box,
  - b. Mode: This dropdown should be left to IAX
  - c. Activation Key: Paste the Activation Key here, provided by your RedPort dealer.
  - d. Hit “Save & Apply” at the bottom to save your changes.
5. On your iPhone or Android, download the XGate Phone app, or any other soft phone app.
6. Connect your device to the wXa-223 Wi-Fi from the Optimizer.
7. Open the XGate Phone app and wait until the top left of the screen shows a green dot and says Connected.
  - a. If you see a red dot that says: Connection failure, then you are most likely not connected to the Optimizer Wi-Fi on your iPhone or Android.

NOTE: When you enable the PBX you will be presented with a choice as to which interface you wish the PBX service to listen on. Listening on the LAN interface will prevent internet traffic from connecting to your PBX and is recommended.

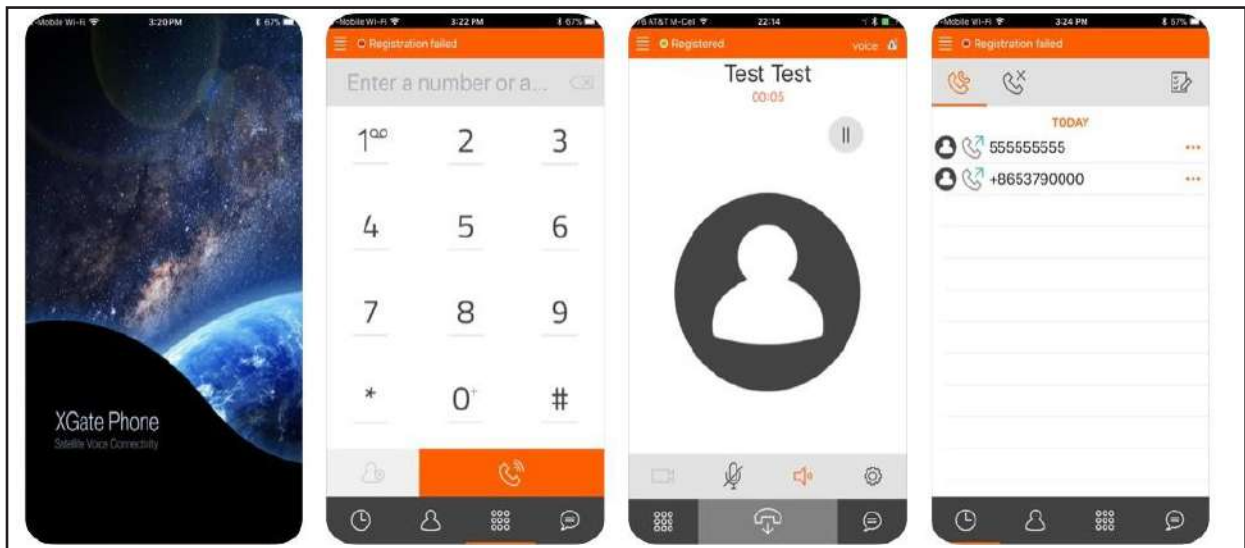
### 7.2.1. How to Make and Receive Voice Calls

Using your smartphone or tablet Wi-Fi network settings, connect to the Optimizer wireless network “wXa-223-xxxx.”

Open the XGate Phone App to make and receive calls.

Note: Standard voice calling rates apply.

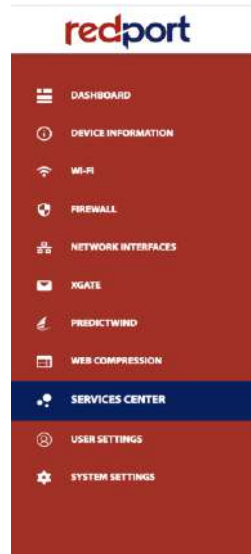
Only one phone call can be active at a time. Multi-user Voice and SMS is possible -- up to four consecutive sessions -- with the optional RedPort VoIP service. Contact your service provider for details.



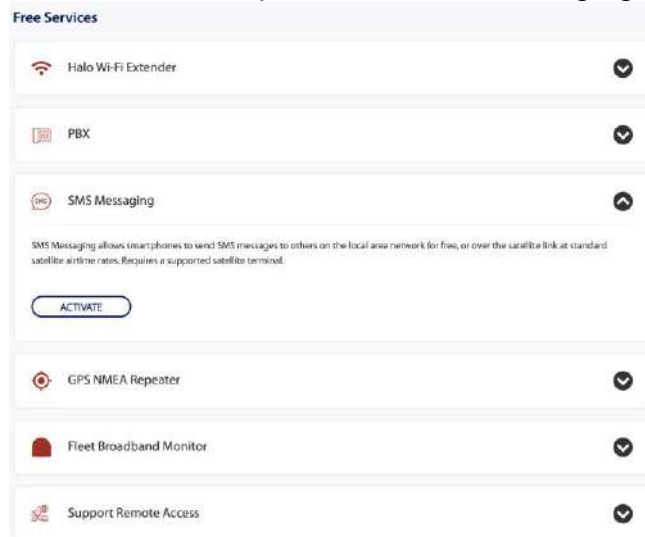
### 7.3. SMS Messaging

SMS Messaging via the Optimizer is disabled by default but can be enabled for use with compatible satellite devices.

1. To enable SMS Messaging, navigate to the Services Center tab on the side menu of the dashboard page.



2. Then, under “Free Services,” expand the “SMS Messaging” tab.



3. Click “ACTIVATE” to activate the service. A second window will pop up, asking if you are sure you want to activate SMS Messaging. Confirm by choosing “ACTIVATE.” After the service is activated, it will appear as a tab on the side menu.



- Click on “SMS Messaging” on the side menu to navigate to the SMS Messaging page. Once that is open, click on the “Settings” tab.

**SMS Messaging**

Create Message Received Messages Sent Messages Settings

Enable/Disable

Interval in SECONDS between LOCAL send attempts 240

Number of Days that Messages stays in Queue when Receiving Messages 3

Satellite Device Iridium

Check for Received Messages (in seconds) 360

Configure Extensions to Receive SMS Redirect >

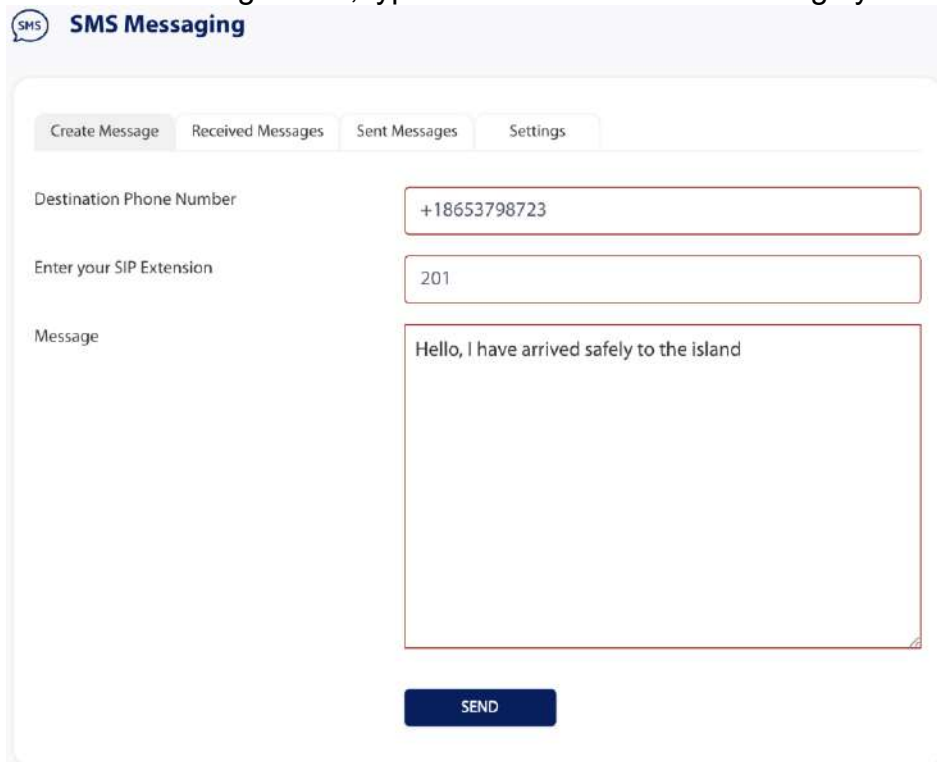
SAVE CHANGES

- Once you have accessed the settings tab, tick the checkbox beside “Enable/Disable” to **enable** SMS Messaging. Note that when the box is NOT ticked, that SMS messaging is disabled. Once you have ticked the box, click on “SAVE CHANGES” to apply the change and ensure that SMS Messaging is fully enabled.

### 7.3.1. How to Send SMS Messages through the User Interface

Once SMS Messaging is enabled following the instructions in section 5.2.3., the user can send and receive messages through the Optimizer device.

1. Navigate to the SMS Messaging page in the User Interface by either clicking on the SMS Messaging tab on the side menu, or by clicking on the SMS Messaging Widget on the Dashboard.
2. In the “Create Message” tab, fill in the fields to send a text message.
  - a. When filling out the “Destination Phone Number,” be sure that there is a ‘+’ sign before the country code. Without this, SMS Messages will not go through the system.
  - b. The “Enter your SIP Extension” is automatically set to extension 201. To change it, click in the box and type in the correct extension.
  - c. In the “Message” field, type in the content of the message you want to send.



The screenshot shows the 'SMS Messaging' interface. At the top, there is a header with an 'SMS' icon and the text 'SMS Messaging'. Below this is a navigation bar with four tabs: 'Create Message', 'Received Messages', 'Sent Messages', and 'Settings'. The 'Create Message' tab is active. The form contains three input fields: 'Destination Phone Number' with the value '+18653798723', 'Enter your SIP Extension' with the value '201', and a larger 'Message' text area containing the text 'Hello, I have arrived safely to the island'. At the bottom of the form is a blue 'SEND' button.

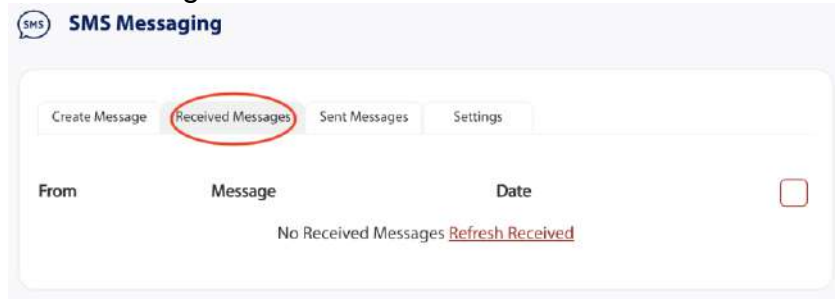
3. Click “SEND” to send your SMS Message through to the Destination Phone Number via your SIP extension. Another window will pop up, asking you to confirm sending the SMS. Click “SEND” to send the message through.



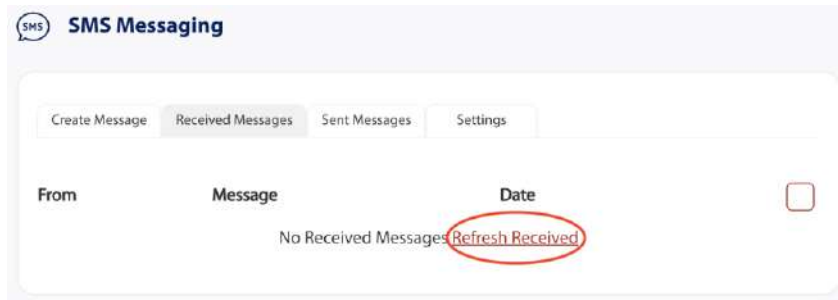
The screenshot shows a confirmation dialog box with the text 'Are you sure you want to send SMS?'. Below the text are two buttons: a blue 'SEND' button and a dark grey 'CANCEL' button.

### 7.3.2. Received Messages

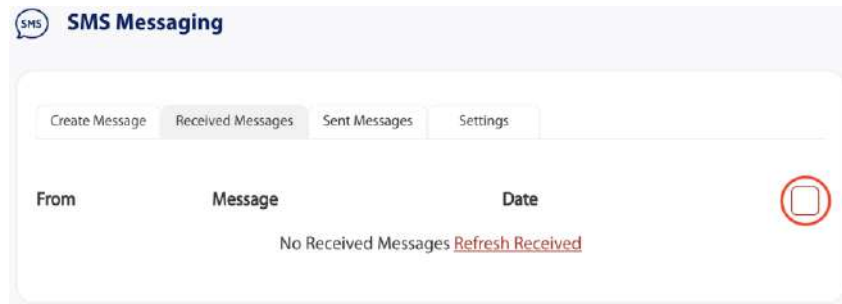
1. Click into the “Received Messages” tab on the SMS Messaging page to view and edit received messages.



2. To view the most updated list of received messages, click on the “Refresh Received Messages,” and the most recently received messages will be added to the list.

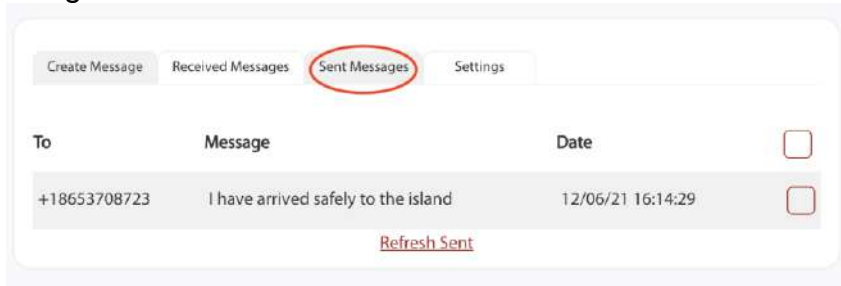


3. To delete a message from the list, tick the box to the right of the message. Then click “Delete” to confirm.

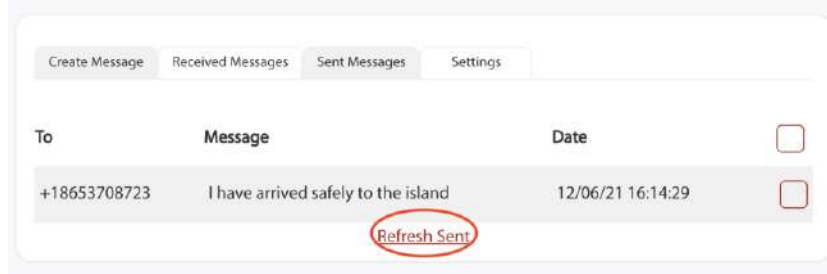


### 7.3.3. Sent Messages

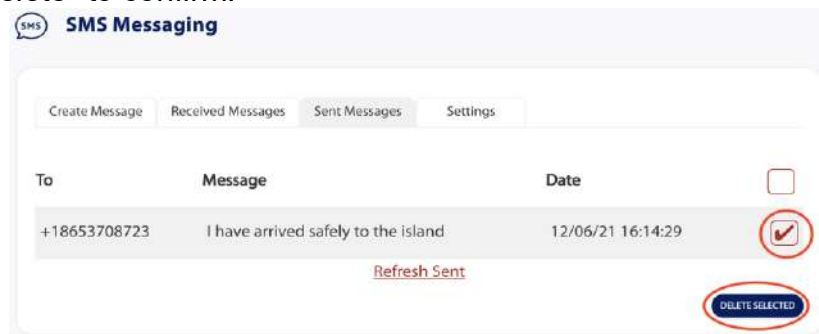
1. Click into the “Sent Messages” tab on the SMS Messaging page to edit and view sent messages.



2. To view the most updated list of sent messages, click on the “Refresh Sent Messages” and the most recently sent messages will be added to the list.



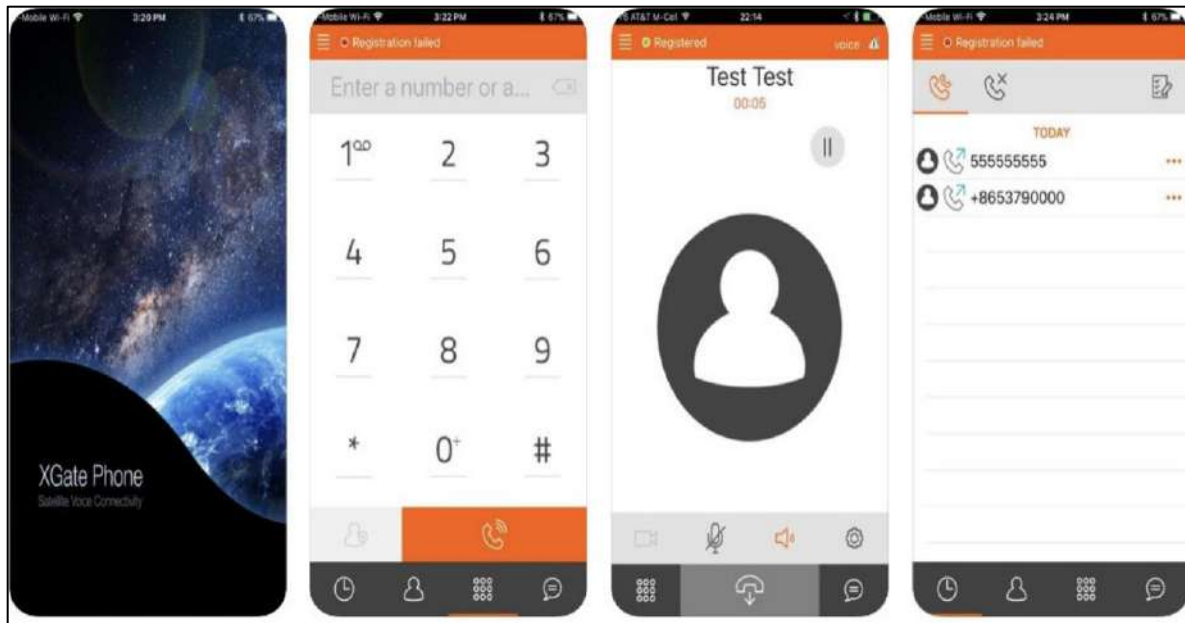
3. To delete a message from the list, tick the box to the right of the message. Then click “Delete” to confirm.





### 7.3.4. Sending SMS Messages through the XGate Phone Application

To use a smartphone or tablet to send/receive SMS messages requires XGate Phone App installed on the smartphone or tablet. The XGate Phone App can be found in Apple iTunes App Store for iOS devices and the Google Playstore for Android devices. Using the smartphone or tablet Settings, connect to the Optimizer wireless network “wXa-223-xxxx.” Open the XGate Phone App. Click <Chat> to send an SMS message or to view an SMS message received.



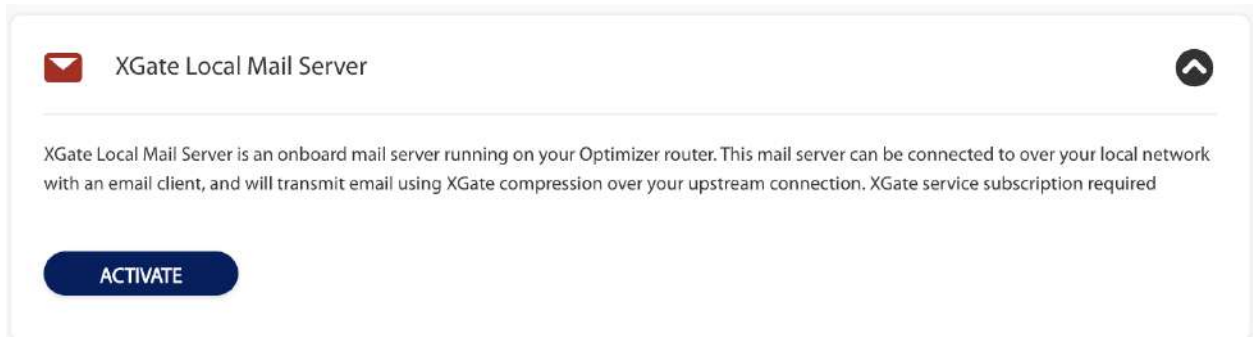
NOTE: Only one SMS message can be sent at a time. Standard SMS message rates apply. Multi-user Voice and SMS is possible with the optional RedPort VoIP service. Contact your service provider for details.

#### 7.4. Email and Web Browsing

This default setup allows anyone with a RedPort-certified email account (such as XGate) or web account (such as XWeb), with a Primary Account username and password, to use the router, as is, to send and receive email and to browse the Internet.

Here are the basic instructions:

1. Power the Optimizer ON.
2. Connect to the Optimizer's network, "wXa-223-XXXX."
3. Login to the Optimizer with username: superadmin and password: webxaccess.
4. Navigate to the Services Center on the side of the Dashboard page. Under the "Premium Services" section in the Services Center, expand the "XGate Local Mail Server" widget and click "ACTIVATE" to allow the services to be utilized on the router.



5. Turn your satellite phone ON.
6. Connect the Optimizer to your satphone with the appropriate cable.
7. Open XGate.
8. Wait for a strong satellite signal.
9. Start an email or a web browsing session.

## 7.5.0. Web Compression and Filtering

This section is used to:

- Configure filters for the internal proxy server when compression is not enabled
- Enable compression so that traffic is passed to the upstream proxy server
- Configure filters for the proxy server (internal or upstream)
- View traffic logs

### 7.5.1. Setting Up Satellite Web Compression

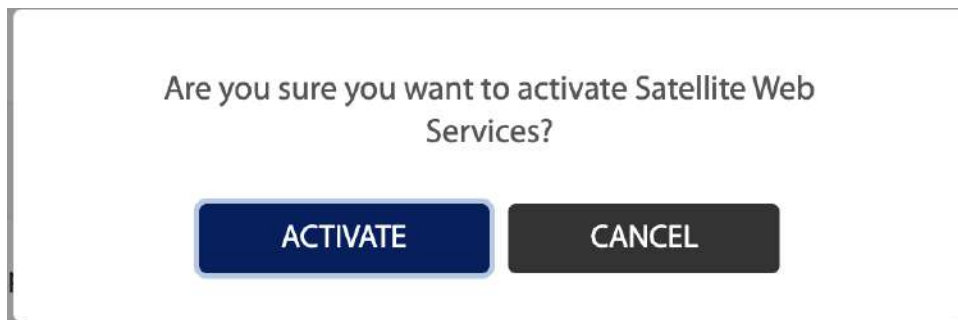
By default, the router is shipped with web compression disabled. Web compression is a premium service that carries an additional charge. Contact your RedPort service provider for pricing.

Enable Compression:

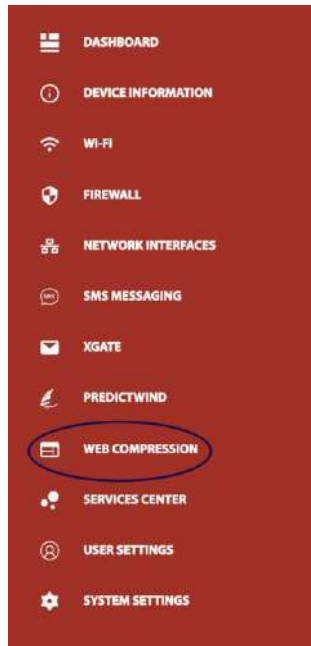
1. If you have purchased Web Compression service, navigate to the Services Center and expand the “RedPort Shared Web Compression” window under Premium Services.



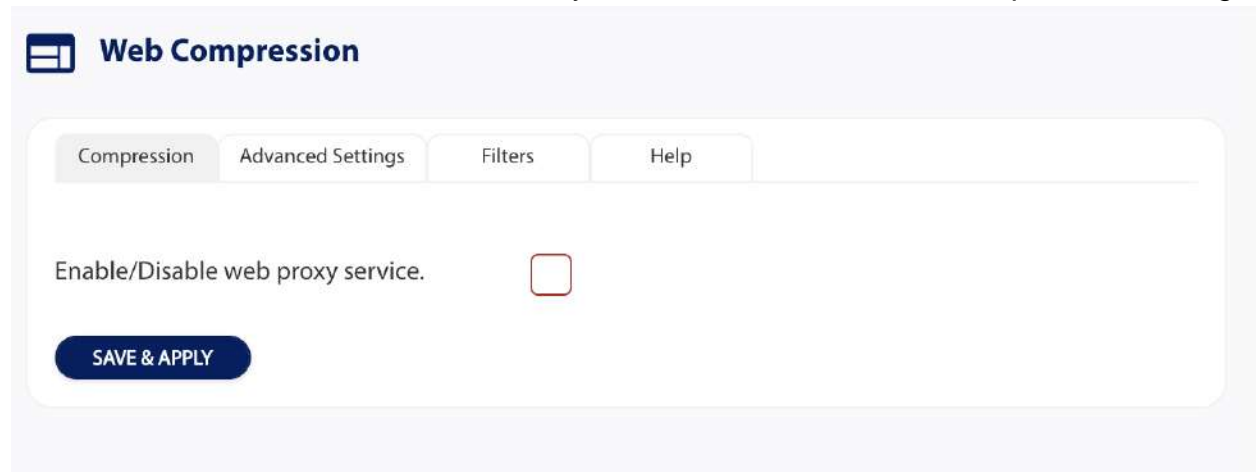
2. Click “ACTIVATE” and another window will pop up asking to confirm you want to activate. Choose “ACTIVATE” to confirm.



3. To navigate to the Web Compression page, choose the “Web Compression” tab on the side menu.



4. Tick the box at the top of the page, under the “Compression” tab. Then hit “Save & Apply” at the bottom of the section to fully enable compression.
  - a. When the box is unticked, you will not be able to alter compression settings.



b. When the box is ticked, you will see the full list of compression settings.

## Web Compression

Compression

Advanced Settings

Filters

Help

Enable/Disable web proxy service.

---

Transparent Proxy

Enable Transparent proxy, i.e. transparently redirect HTTP web traffic to the web proxy for filtering and/or compression without having to modify the end user's browser settings. Caution: Enabling transparent mode requires opening TCP ports 53 (DNS), 80 (HTTP), and 443 (HTTPS) which can (will) result in high traffic usage. Note: This mode is not compatible with the captive portal. The captive portal, if enabled, will disable this feature automatically to prevent conflicts.

---

Enable compression

Web compression will, on average, decrease overall bandwidth usage by a factor of 3-5X while simultaneously increasing overall speed. Don't yet have the incredible airtime savings and optimization of web compression? Contact your dealer for additional information. They can set you up with an account username and password to enable compression for this device.

---

Server

---

Compression Level

---

Bypass Regex Domain

Bypass compression for listed sites. Enter host regular expression to match. e.g. "google.com" to bypass any domain containing .google.com. See "Domain Syntax" under Help tab for additional information.


SAVE & APPLY

**Transparent Proxy:** Enable Transparent proxy. i.e., transparently redirect HTTP web traffic to the web proxy for filtering and/or compression without having to modify the end user's browser settings.



**Caution:** Enabling transparent mode requires opening TCP ports 53 (DNS), 80 (HTTP), and 443 (HTTPS) which will result in high traffic usage. Before enabling Transparent Proxy, refer to section titled Router Security (Section 6.0.).

**Note:** This mode is not compatible with the captive portal. The captive portal, if enabled, will disable this feature automatically to prevent conflicts.

|  |  |
|--|--|
| Enable compression   | <input checked="" type="checkbox"/>  |
| <p>Web compression will, on average, decrease overall bandwidth usage by a factor of 3-5X while simultaneously increasing overall speed. Don't yet have the incredible airtime savings and optimization of web compression? Contact your dealer for additional information. They can set you up with an account username and password to enable compression for this device.</p> |  |
| Proxy Authentication by Client   | <input type="checkbox"/>   |
| <p>Specifies whether upstream proxy authentication requests are passed through to the client browser. If not, authentication (if required) is done by proxy. Note: this feature will not work with transparent proxy. When using transparent proxy you must uncheck this option and enter a valid username and password.</p>   |  |
| Username   | <input type="text"/>   |
| Password   | <input type="password"/>  |

**Enable Compression:** When you tick this box, it enables compression. You can then choose to enable Proxy Authentication by Client and enter your Username and Password.

**Proxy Authentication by Client:** By default, this is unchecked as it does not work with the Captive Portal enabled. In this state, unchecked, the upstream proxy server will login on your behalf. If this is checked, then the authentication happens at the user end, which means that when a user goes to any webpage they will be prompted for a username and password.

☰

Web Compression

Compression

Advanced Settings

Filters

Help

Enable/Disable web proxy service.

---

Transparent Proxy

Enable Transparent proxy, i.e. transparently redirect HTTP web traffic to the web proxy for filtering and/or compression without having to modify the end user's browser settings. Caution: Enabling transparent mode requires opening TCP ports 53 (DNS), 80 (HTTP), and 443 (HTTPS) which can (will) result in high traffic usage. Note: This mode is not compatible with the captive portal. The captive portal, if enabled, will disable this feature automatically to prevent conflicts.

---

Enable compression

Web compression will, on average, decrease overall bandwidth usage by a factor of 3-5X while simultaneously increasing overall speed. Don't yet have the incredible airtime savings and optimization of web compression? Contact your dealer for additional information. They can set you up with an account username and password to enable compression for this device.

---

Server

---

Compression Level

---

Bypass Regex Domain

Bypass compression for listed sites. Enter host regular expression to match. e.g. "google.com" to bypass any domain containing .google.com. See "Domain Syntax" under Help tab for additional information.

SAVE & APPLY

**Server:** Do not change this unless instructed to do so by your service provider.

**Compression Level:** Set the level of compression that meets your needs. Those on entry level plans should click “Maximum.” Those on high data plans may prefer “Standard” or “Minimum.”

**Bypass Regex Domain:** This is the whitelist of sites that should not be compressed. To add a site, type it into the text box. Proper syntax must be used to successfully bypass compression. See the Help tab for guidance and examples of using regular expressions.

With Compression Enabled, the page expands to reveal Proxy Authentication by Client, Server, and Compression Level.





### 7.5.3. Advanced Settings

Under normal operating conditions there is little to change here.

Some items of interest include:

- **Default Filtering Scheme:** impacts the amount of content filtering that is applied to a webpage, by removing elements, before presenting it to the end user. It determines the amount of filtering to be done to the page. “Light” has the least impact and is not recommended for those on low data plans. “Aggressive” has the most impact and is suggested for the best bandwidth utilization. This blocks YouTube, flash, etc.
- **Debug Level:** determines what will show on the Web Compression and Filtering ‘Log’ page. Adding the debug level of “1”, all URLs will be logged and will appear on the Log page, one line per URL.



**CAUTION:** Utilization of debug level 1 is not recommended for normal operation. The Log files are kept in RAM and with debug level 1 activated you run the risk of RAM filling up, the Swap Partition filling up and the router might crash.

**BEST PRACTICE:** Activate debug level 1 for testing that your setup is working as you intend, i.e., the proxy server working as expected, and that whitelists and blacklists are working as expected. Deactivate debug level 1 when testing is complete.

#### 7.5.4. Filters

By default, you have control over what sites are ALLOWED (whitelist) and what sites are BLOCKED (blacklist) and some control over content filtering without having to enable compression.

There are three filter categories:

- **Fragile Sites:** list sites that you want the content kept intact without any modification.
- **Sites Blocked:** the blacklist; users are prevented from viewing these sites.
- **Sites Allowed:** the whitelist; these sites are allowed for viewing. This list overrides the blocked list.

Filters respond to POSIX Regular Expressions. Example: If you place a slash ( / ) in Sites Blocked then the entire Internet is blocked (blacklist). Enter the whitelist in the Sites Allowed section. If any of the allowed sites should be accessed without any content filtering, enter that site in the Fragile sites section as well.

## 7.6. FleetBroadband Monitor (FBB)

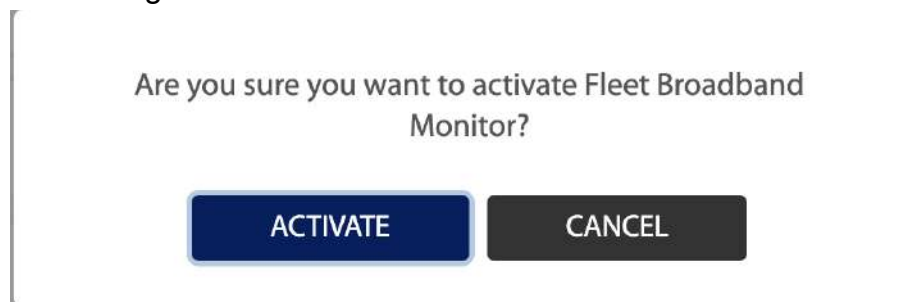


FleetBroadband Monitor requires that the Fleet Broadband be configured to accept AT commands.

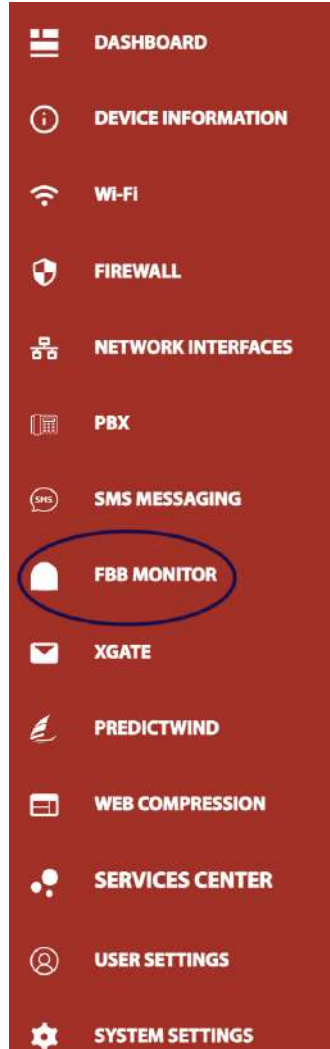
1. To Activate the FleetBroadband Monitor, navigate to the Services Center tab and expand the drop down labelled “FleetBroadband Monitor” underneath the “Free Services”

The screenshot shows a 'Free Services' panel with three service cards. The first card is 'GPS NMEA Repeater' with a downward arrow. The second card is 'Fleet Broadband Monitor' with an upward arrow, indicating it is expanded. Below the title, there is a paragraph of text: 'Fleet Broadband Monitor provides vessel side users with visual indications of the Cobham Fleet Broadband terminal status by augmenting the blink patterns of the RedPort Optimizer. The service also restricts access to the Optimzier devices to all users except the admin. This service requires a Cobham Fleet Broadband satellite terminal.' Below this text is a blue 'ACTIVATE' button. The third card is 'Support Remote Access' with a downward arrow.

2. Click “ACTIVATE” then when the confirmation window pops up, choose “ACTIVATE” again to confirm the choice.



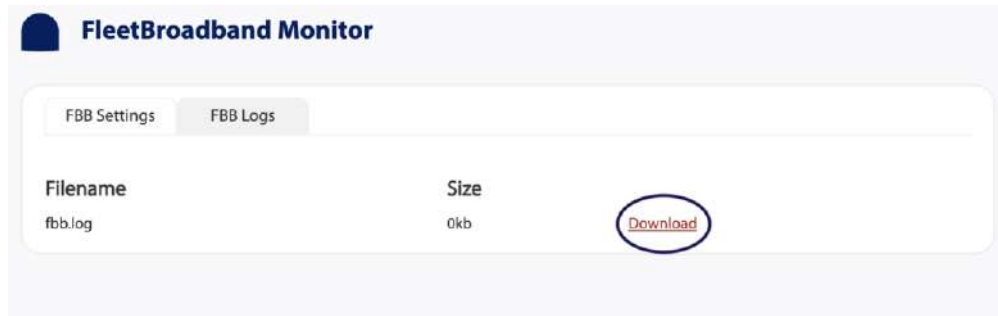
3. Navigate to the side menu and choose “FBB Monitor” to access the FBB Monitor page.



4. To enable the FBB Monitor, tick the checkbox on the FBB Settings tab. Then click “SAVE CHANGES” to apply the changes.



5. To download FBB Logs, click the “Download” link on the FBB Logs tab.



## 7.7. Halo Wi-Fi Extender

Requires a Halo Long Range Wi-Fi Extender for use.

The Halo long-range Wi-Fi extender system takes a weak Wi-Fi signal – at a marina, for example, or truck stop, basecamp, etc. – and amplifies that signal and routes it through the RedPort Optimizer Wi-Fi hotspot. It has a marine enclosure designed for outside installation. Install the Wi-Fi Extender almost anywhere outside.

Please consult the Halo Long Range Wi-Fi Extender Quick Start Guide for initial set up.

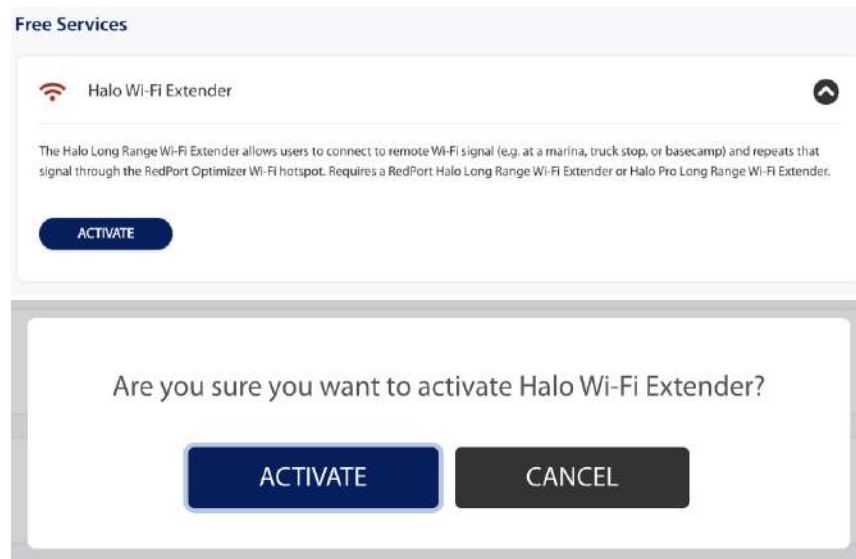


**CAUTION:** Attach the antenna to the Halo SB Extender Base **BEFORE** powering the unit. Powering the Halo without the antenna attached will damage the unit and may render it inoperable.

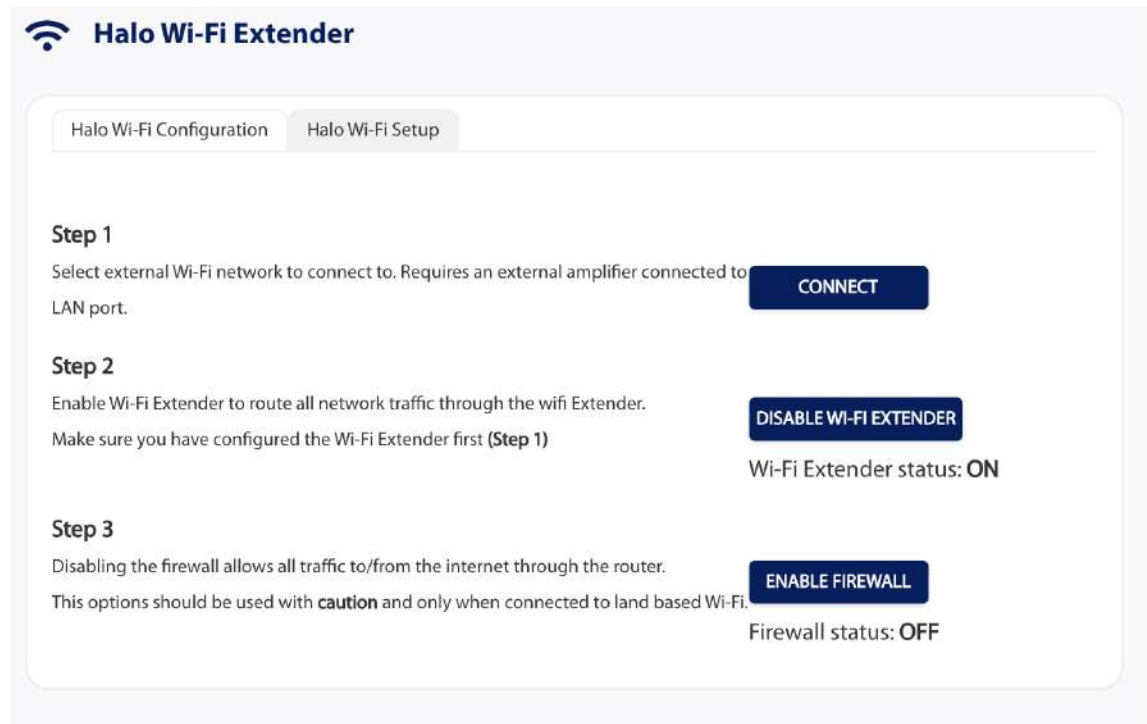
### 7.7.1. Configure Optimizer for use with the Halo Single Band Wi-Fi Extender

With the Halo powered ON and connected to the Optimizer, login to the Optimizer router. Configuration of the Halo Wi-Fi Extender can be accessed through the services center or dashboard. Configuration of the Optimizer for use with your Halo Long Range Wi-Fi Extender is outlined as follows:

1. On the side menu, navigate to the “Services Center.” Once in the “Services Center,” under the “Free Services” list, expand the “Halo Wi-Fi Extender” widget and click “ACTIVATE.” Another window will pop up afterwards that asks you to confirm your choice to activate the service.



2. Once this is activated, the Optimizer will automatically redirect to the Halo Wi-Fi Extender page. You can also reach this page by clicking on the widget on the main page.



3. Click the wireless network you want to connect to and press <Join Network>.

4. If the Wi-Fi source you are connecting to is password protected enter the password to access the external wireless network and click <Submit>.

Notice the signal strength is 0% as you are not yet connected to the wireless network. Click <Save & Apply> to tell the Halo to connect to that network.

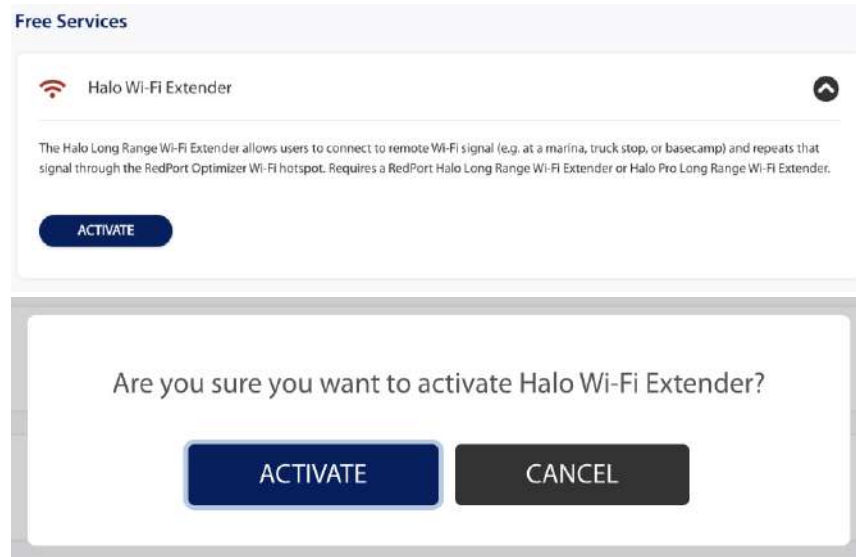
Notice that now the signal strength now registers greater than 0%.

**NOTE:** If the signal status is blinking from 0% to 100% this typically means that the Wi-Fi Network Password/Key was entered incorrectly. Check with the external Wi-Fi Network Administrator to confirm the correct password. Click the Wireless Security tab and enter the correct password in the Key field and <Save & Apply>.

5. Click the <Home> Tab to return to the Welcome screen.

### 7.7.2. Configure Optimizer for use with the Halo Pro Wi-Fi Extender

1. With the Halo powered ON and connected to the Optimizer, login to the Optimizer router. Configuration of the Halo Wi-Fi Extender can be accessed through the services center or dashboard. Configuration of the Optimizer for use with your Halo Long Range Wi-Fi Extender is outlined as follows:



2. On the side menu, navigate to the “Services Center.” Once in the “Services Center,” under the “Free Services” list, expand the “Halo Wi-Fi Extender” widget and click “ACTIVATE.” Another window will pop up afterwards that asks you to confirm your choice to activate the service.
3. Click the wireless network you want to connect to and press <Join Network>.
4. If the Wi-Fi source you are connecting to is password protected enter the password to access the external wireless network and click <Submit>.

Notice the signal strength is 0% as you are not yet connected to the wireless network. Click <Save & Apply> to tell the Halo to connect to that network.

Notice that now the signal strength now registers greater than 0%.

**NOTE:** If the signal status is blinking from 0% to 100% this typically means that the Wi-Fi Network Password/Key was entered incorrectly. Check with the external Wi-Fi Network Administrator to confirm the correct password. Click the Wireless Security tab and enter the correct password in the Key field and <Save & Apply>.

5. Click the <Home> Tab to return to the Welcome screen.



### 7.7.3. Disconnect from the Halo Wi-Fi

To disconnect from the Halo, click <Disable Wi-Fi Extender>.

Notice that the Firewall is turned back on automatically to protect you from runaway airtime charges.

**NOTE:** An alternate method of disconnecting from the Halo is to cycle power to Optimizer or Reboot the Optimizer. This will also restore the Firewall Status to ON.



**CAUTION:** It is important to <Disable Wi-Fi Extender> when the external Wi-Fi network is no longer available, and you want to use your satellite device. Failure to Disable will prevent a successful satellite connection as the Optimizer continues to look for the external Wi-Fi network.

## 7.8. GPS Tracking

GPS Tracking is a premium service with a monthly charge and is not included with the purchase of a RedPort Optimizer. If you wish to have tracking service using your satellite device, the Optimizer works with RedPort Tracking. Contact your RedPort dealer or RedPort directly ([support@redportglobal.com](mailto:support@redportglobal.com)) to enable RedPort Tracking before you set it up on your Optimizer.

### 7.8.1. Tracking powered by RedPort

Using a GPS-enabled satellite device (e.g., Aurora, Glow), the Optimizer can be configured to submit position reports to a central database for viewing on the tracking website.

1. To enable tracking services, go to the Services Center and
2. Enter the Tracking Interval in minutes; the default is set to hourly reporting (60 minutes). This means that every 60 minutes a position report will be transmitted over your satellite link. Keep in mind that standard airtime charges will apply to each position report. Adjust the Tracking Interval to meet your needs.
3. Select the satellite terminal you are using.
4. Click <Save & Apply>.

**NOTE:** A valid NMEA/GPS feed is required when using some satellite devices.

### 7.8.2. SMS Tracking

If using certain satellite devices, GPS information can be sent to an email address using your satellite provider's SMS service. Standard SMS charges may apply; check with your satellite airtime provider for details.

1. Enter the Tracking Interval in minutes; the default is set to hourly reporting (60 minutes). This means that every 60 minutes a position report will be transmitted via the SMS service provided by your satellite provider network. Keep in mind that standard SMS charges may apply to each position report. Adjust the Tracking Interval to meet your needs.
2. Select which satellite device you are using. Currently, tracking via SMS is available with the Inmarsat IsatPhone, Iridium handheld 9575 Extreme, Iridium GO! Or an Iridium terminal such as the Pilot.
3. Enter the recipient's email address. The SMS message with the GPS information will be sent to this email address at the interval entered in Step 1.
4. Click <Save & Apply>.

**NOTE:** A valid NMEA/GPS feed is required when using an Iridium terminal.

## 7.9. GPS/NMEA Repeater

The Optimizer supports USB and RS-232 NMEA devices allowing multiple applications to share the GPS/NMEA data. If you have a NMEA RS-422 device, adding a RS-422 to RS-232 converter to your setup may allow the sharing of data.

The Optimizer does not transmit data but can be configured to receive and repeat GPS/NMEA data from:

- A broadband satellite terminal with integrated GPS when connected to the Optimizer via a standard Ethernet connection. (As of this writing, supported terminals include Iridium Pilot, Inmarsat FBB and Inmarsat BGAN.)
- A handheld satellite phone with integrated GPS when connected to the Optimizer with the satphone's USB- Mini/Micro USB cable. (As of this writing, supported handheld satphones include Iridium 9575 Extreme and Inmarsat IsatPhonePro.)



**CAUTION: IsatPhone users! The phone only transmits GPS coordinates about every 10 minutes. It is NOT recommended for navigation or any application that requires real time data.**

- A USB connected GPS or NMEA device.
- A serial port connected GPS or NMEA device.

**NOTE:** If you are using a satellite phone with a serial port (RS-232) that transmits GPS data (i.e., some fixed phones and fleet phones), it is NOT compatible with the Optimizer. To repeat GPS data, a separate GPS device must be connected.

### 7.9.1. GPS/NMEA Repeater Equipment Setup

A physical connection is required from the source (satellite terminal or satellite phone that transmits GPS coordinates, or another GPS/NMEA device) to the Optimizer.

### **7.9.2. Broadband Satellite Terminal with Integrated GPS**

When using a supported broadband satellite terminal with integrated GPS, connect the terminal to the Optimizer SAT port using a standard Ethernet cable. (OPTIONAL: Use a second Ethernet cable to connect the computer with the destination software, like a navigation program, to the Optimizer LAN port.) The Optimizer will broadcast the GPS signal both over Ethernet and Wi-Fi, so you can connect your computer either way to establish a successful connection with your destination software.

### **7.9.3. USB NMEA Device**

When using a NMEA device that supports a USB connection, connect the GPS/NMEA device to the Optimizer with an appropriate USB to NMEA device cable as indicated by the NMEA device manufacturer.

(OPTIONAL: Use an Ethernet cable to connect the computer with the destination software, like a navigation program, to the Optimizer LAN port.)

The Optimizer will broadcast the GPS signal both over Ethernet and Wi-Fi, so you can connect your computer either way to establish a successful connection with your destination software.

**NOTE:** If your satellite device requires a USB connection to the Optimizer (for example, an Iridium 9555) you can use a 2-port USB hub (either 1.0 or 2.0) plugged into the Optimizer's USB port to accommodate two USB devices.

#### 7.9.4. RS-232 NMEA Device

When using a NMEA device with Serial Port connection, a USB to Serial Adapter (PL-2303HX) is required to connect the device to the Optimizer.



**CAUTION:** The PL-2303 is the only USB to Serial Adapter that is compatible with the Optimizer.

The Optimizer will broadcast the GPS signal both over Ethernet and Wi-Fi, so you can connect your computer either way to establish a successful connection with your destination software.

**NOTE:** If your satellite device requires a USB connection to the Optimizer (for example, an Iridium 9555) you can use a 2-port USB hub (either 1.0 or 2.0) plugged into the Optimizer's USB port to accommodate two USB devices.

#### For those users without a Serial Port Connector

Some NMEA devices do not have a serial port; instead, they have a group of wires extending from the back or bottom of the unit. These devices require proper wiring to a serial port.

As the Optimizer does not transmit, it only repeats the data, you will only need two of the wires. The Receive (RD) wire goes to pin 2 and the Ground (SG) wire goes to pin 5.

A simple solution is to use a terminal block as shown here. Simply connect the RD wire to pin2 and the SG wire to pin 5. Then connect the terminal block to the PL-2302 USB to serial adapter.

### 7.9.5. Connecting Multiple NMEA Devices

It is possible to connect to four NMEA devices if you have the proper hardware. It will require a USB to RS-232 4-port Hub or a RS-232 4-port terminal block that you would simply plug into the Optimizer's USB port.



**NOTE:** The Optimizer supports RS232. If you have a NMEA RS-422 device, adding a properly wired RS-422 to RS-232 converter to your setup may allow the sharing of data.

### 7.9.6. GPS/NMEA Repeater Parameters Configuration

For the destination software to properly route the GPS data you must configure the GPS/NMEA Repeater Parameters in the Optimizer User Interface.

From the Optimizer Home page Click Services > GPS/NMEA Repeater tab.

1. Select the source of the GPS/NMEA information (choose only one):
  - GPS from broadband satellite: Click this if you are using a broadband satellite terminal with integrated GPS.
  - GPS/NMEA feed from USB: Click this when connecting a GPS or NMEA device via USB cable. NMEA Baud Rate - Using the drop-down menu, Click the baud rate required for the destination software. By default, most NMEA 183 devices (GPS) and applications use 4800 baud for this setting.
2. UDP Listener Port - Enter the UDP port number that the GPS is connected to. The default is set to the standard UDP Listener Port for NMEA 183 devices of 10101.
3. UDP Port - Enter the UDP port number to broadcast the GPS data to. The default is set to the standard UDP Port for NMEA 183 devices of 11101.

**NOTE:** Configure the destination software to match this port number; or change this entry to match the requirements of the destination software.

4. TCP Port - Enter the TCP port number to broadcast the GPS data to. The default is set to the standard TCP Port for NMEA 183 devices of 11102.

NOTE: Configure the destination software to match this port number; or change this entry to match the requirements of the destination software. The data will be broadcast to both the UDP Port and the TCP Port. It is important to make sure that these two ports are NOT set to the same port number.

To use the GPS Repeater feature, your computer must be connected to the Optimizer's Wi-Fi network or directly connected to the LAN port of the Optimizer.

## 7.10. Remote Support



**CAUTION:** Remote Support requires an upstream connection source. If using a satellite device with activate satellite airtime, it will require the use of your satellite airtime data.

**NOTE:** Do not set your remote Access Port to the presented port in this document's screen shots. The router will present a port to you. Do not attempt to log in with the example remote login, it is just presented for your knowledge.

Click <Enable remote support> under "Remote Support" section of the <Home> tab.

When remote support is enabled, Remote Access URLs are displayed.

Disabling this Remote Support will not disable the persistent Remote Support. To disable this remote support access, either:

1. Reboot the router.
2. Click <Disable Remote Support>.
3. Persistent Remote Support Access - The second remote support login access is located from the Services tab and permits persistent access. Even if the router is rebooted, this access will remain.

To enable Persistent Remote Support Access - Navigate to <Services> tab, then to <Remote Access>.

Click the "Enable Remote Support" button and then click <Save & Apply>.

When remote support is enabled, Remote Access URLs are displayed.

Disabling this Remote Support will not disable the one-time Remote Support. To disable remote support access:

1. Click <Services> tab, then click "Enable Remote Access".



## 8. Status under System Settings

Use the Status tab to display current information of the router's performance.

Some of the information provided here includes:

- How much memory the router is currently using
- Who is currently connected via Wi-Fi
- Error messages reported in the System Log and can be useful when troubleshooting connection issues
- Realtime Graphs report how much data is being used by the different interfaces

All Status information is READ ONLY

### 8.1. Access System Log

If you are experiencing connection issues your service provider may request that you send them a copy of the Optimizer System Log.

1. Attempt an email connection.
2. Login to the Optimizer Home page.
3. Go to Status > System Log.
4. Copy/paste the entire log into an email and send to your service provider.

**NOTE:** The System Log date will show May 31 unless you have synced the Optimizer Local Time with a browser in System Tab > Local Time > Sync with browser. This is NOT recommended when using a satellite connection and it is not necessary to ever sync the time. If you do sync the time as soon as power is removed from the Optimizer the date will revert to May 31.

## 8. System Settings

### 8.1. Update Firmware

Get the latest Optimizer firmware version from here:

[redportglobal.com/support/technical-downloads/](http://redportglobal.com/support/technical-downloads/)  
Save the .bin file to your computer.

**NOTE:** If you have created any Profiles you may want to Export them before flashing new firmware and import them when done.

Login to the Optimizer and go to: System > Backup/Flash Firmware.

1. Keep Settings: untick the box to uncheck Keep Settings.
2. <Browse> to where you saved the .bin file and click that file.
3. Click <Flash Image>.
4. Wait a few minutes to give the Optimizer time to perform the update.
5. To confirm the firmware upgrade, login to the Optimizer Home Page again.  
Check the Firmware Version in the Status tab under System Settings.

### 8.2. Profile Manager

Profile Manager is designed for users of multiple satellite devices and integrators of custom installations. You can configure the Optimizer for a specific satellite device and save the profile. This is good for failover situations when using multiple devices. An extreme example would be that you might have the firewall wide open on a VSAT device but in an emergency must use an Iridium handheld device where you want the full protection of the Optimizer firewall. Have a profile for each configuration and select the appropriate one for the satellite device being used.

To access Profile Manager, go to System Settings.

To create and use a new Profile:

1. Click <Add>.
2. Enter a Name of the new profile and a description.
3. Click <Install> to add the new profile.
4. Click <Save & Apply>.

To change from using one profile to another, simply Click <Install> for the desired profile, then <Save & Apply>.

### **8.3. Reboot the Optimizer Router**

The easiest way to reboot the Optimizer is to use the reset button on the bottom of the router. Using a pointed instrument, press and hold the red reset button for 20-30 seconds and release. Wait for the Optimizer reboot, this will take several minutes. After this reset, the Optimizer will be configured with its factory defaults. You will need to reenter any modifications you made to the user interface. You can also reboot the router from within the Optimizer user interface:

1. Login to the Optimizer Home page.
2. Click <Reboot Router>.
3. Click <Perform reboot>.

The gray button on top of the Optimizer will flash during the reboot process. When the light stops flashing the reboot is complete. This will take several minutes.

During the reboot process you will lose access to the Optimizer User Interface. You must login again if you want access.

## 9. Wi-Fi

### 9.1. Restrict Wireless Network Access (Add or Change Network Password)

Add/change a password to the Wi-Fi Hotspot (wXa-223-xxxx). This procedure adds/changes the password for the Wi-Fi hotspot only. When connecting your computer, iOS, or Android device to the wireless network, this is the password you will use. This password does not change the router superadmin or admin password when logging in to access the Optimizer user interface.

1. Login to the Optimizer.
2. Click on the Wi-Fi module on the Dashboard page of the Optimizer.
3. At the top of the Wi-Fi page, there is a section called “Device Wi-Fi Information.” Click on the “Advanced Configuration” option at the bottom of the window.

#### Device Wi-Fi Information

SSID: wXa-223-3368

Password Protected: NO

Advanced Configuration >

4. A window will pop up asking if you would like to move forward with Advanced Configuration of Wi-Fi settings. Click “Proceed.”

You are about to proceed to advanced Wi-Fi configuration settings. Modifying the default state of the device Wi-Fi will alter the intended user experience. By clicking proceed you acknowledge these risks.

PROCEED CANCEL

5. At the bottom of the Wireless Network page, there is a section called “Interface Configuration.” Click on the “Wireless Security” tab and choose “WPAPSK/WPA2- PSK Mixed Mode” from the dropdown. Leave the Cipher at “Auto.” Enter the desired password in “Key.”

#### Interface Configuration

General Setup   **Wireless Security**   MAC-Filter

Encryption  
WPA-PSK/WPA2-PSK Mixed Mode

Cipher  
auto

Key  
\*\*\*\*\*

6. Click <Save & Apply> to save the changes.

## 9.2. Rename the Wireless Network (Change SSID Name)

NOTE: Renaming the Wireless Network (SSID Name) will not transfer into a Profile Save as each router needs to have a unique Wireless Network (SSID Name) to avoid network conflict.

It is possible to change the name of your wireless network. This is the name of the wireless network that you connect to using your computer or iOS or Android device. The default name is wXa-223-xxxx where the xxxx represents a unique number specific to your device. There is no default password to connect to the network.

1. Click <Wi-Fi Setup> and go to: Interface Configuration > General Setup.
2. Enter the new wireless network name in ESSID field.
3. Click <Save & Apply>.

This procedure changes the name for the Wi-Fi hotspot only. When connecting your computer, iOS or Android device to the wireless network, this is the network name that will appear in the wireless network list. This name does not change the router superadmin or admin name when logging in to access the Optimizer user interface.

## **10. Product Warranty and Support Information**

### **10.1. Product Warranty Information**

RedPort hardware carries a Limited 1-year manufacturer warranty against defects from the date of sale.

#### **What is covered by this limited hardware warranty?**

This limited hardware warranty covers defects in materials and workmanship in your RedPort-branded hardware products.

#### **What is not covered by this limited hardware warranty?**

This limited hardware warranty does not cover:

- Software, including without limitation, the operating system and software added to the RedPort -branded hardware products through our factory-integration system, third-party software or the reloading of software
- Non-RedPort-branded products and accessories
- Problems that result, directly or indirectly, from:
  - External causes such as accident, abuse, misuse, water ingress, or problems with electrical power.
  - Servicing not authorized by RedPort.
  - Usage that is not in accordance with product instructions.
  - Failure to follow the product instructions or failure to perform preventive maintenance.
  - Using accessories, parts or components not supplied by RedPort.
  - Products with missing or altered service tags or serial numbers
  - Products for which RedPort has not received payment
  - Normal wear and tear

## 10.2. Product Support Information

RedPort agrees to provide initial customer assistance, up to thirty (30) minutes at no charge. It is recommended that a customer has reasonable knowledge of basic computer and software setup procedures for the initial installation.

| Feature                       | Description   | Details For Warranty  |
|-------------------------------|---|---|
| Remote Email Support          | Customer may contact their RedPort dealer or <a href="mailto:support@redportglobal.com">support@redportglobal.com</a> to report an issue. | 1 year included in RedPort hardware purchase  |
| Remote Live Technical Support | Customer may contact their RedPort dealer or <a href="mailto:support@redportglobal.com">support@redportglobal.com</a> to report an issue. | Up to 30 minutes of free phone support included during warranty period. Additional time available for purchase. |

### Company Contact Information

For product orders, support or returns, please contact:

Phone: +1-865-379-8723

Email: [support@pivotel.com](mailto:support@pivotel.com)

Web: [redportglobal.com](http://redportglobal.com)

### Company Address

2 Oakwood Blvd

Suite 200

Hollywood, FL 33020

United States of America