# RedPort®



# **RedPort Optimizer Advanced User's Guide**

RedPort Router: wXa-203

# **Revision History**

Date	Version	Point of Contact
May 12, 2020	Version 1.0	Aaron Dickson

Contents	
1. About This Guide	5
2. Introduction to the RedPort Optimizer	5
2.1. Key Features	5
2.2. Services Included	6
2.3. Premium Services Available	6
3. Important Things to Know Before Getting Started	6
3.1. More Than Just a Router	6
3.2. Designed Use of the Optimizer	7
3.2.1. Single User Environment	7
3.2.2. Multi-User Environment	7
3.3. How It Works At First Launch (Out Of The Box)	7
3.4. Navigating the User Interface (UI)	/
4. Getting Started - User Interface (UI) Access	8
4.1. Access the Home Page	8
4.1.1. Onsite Administrator Login (Admin)	0
4.1.2. Installer/Network Administrator Login (Superadmin)	9
4.2. Now to Use with Deladit Setup	10
4.2.2 Voice Calls	10
4.2.3 SMS Messaging	11
4.3 Bouter Security **IMPORTANT**	11
4.3.1. How to Secure Your Router***IMPORTANT***	11
5. Services	12
5.1. Web Compression and Filtering	12
5.1.1. Settings	12
5.1.1.1. Compression	12
5.1.1.2. General Settings	13
5.1.1.3. Advanced Settings	14
5.1.2. Filters	15
5.2. SMS Messaging	16
5.2.1. SMS Settings	16
5.2.2. Configure SIP Extensions to Receive SMS Messages	16
5.2.3. How to Send/Receive SMS Messages	17
5.2.4. SMS Management	17
5.3. Voice PBX	18
5.3.1. Voice PBX Settings	19
5.3.2. Setup Extensions	19
5.3.3. HOW TO Make/Receive Voice Calls	20
5.3.4. Fleet Broadband Monitoring (FBB)	20
5.4. Halo WI-FI EXTENDER	21
5.4.2. Connect to the External $W_{i-}$ Fi Network	21
5.4.3. Boute Network Traffic through the Halo	23
5.4.4 Manage the Firewall (Optional)	20
5.4.5 Disconnect from the Halo	24
5.5. GPS Tracking	25
5.5.1. Tracking powered by GSatTrack	25
5.5.2. Tracking via SMS	26
5.6. GPS/NMEA Repeater	27
5.6.1. Equipment Setup	27
5.6.1.1. Broadband Satellite Terminal with Integrated GPS	27
5.6.1.2. Handheld Satellite Phone with Integrated GPS	27
5.6.1.3. USB NMEA Device	27
5.6.1.4. RS-232 NMEA Device	28
5.6.1.5. Connecting Multiple NMEA Devices	28
5.6.2. GPS/NMEA Repeater Parameters Configuration	29
5.7. Remote Support	30
6. Status	32
D.I. ACCESS SYSTEM LOG	32

6.2. System Status for Monitoring Usage	33
7. System	33
7.1. Change Superadmin and/or Admin Password	33
7.2. Profiles	35
7.3. Update Optimizer Firmware	36
7.4. Reboot the Optimizer Router	37
8. Network	38
8.1. Signal Monitor	38
8.2. GSM	38
8.2.1. GSM Configuration in Optimizer	39
8.2.2. Using GSM	40
8.2.3. Changing from GSM service to satellite service	41
8.3. Restrict Wireless Network Access (Add or Change Network Password)	41
8.4. Rename the Wireless Network (Change SSID Name)	43
8.5. Firewall	44
8.5.1. General Settings	44
8.5.2. Add a Firewall Zone	46
8.5.3. Port Forwards	47
8.5.4. Firewall Rules	48
8.5.4.1. Create a Custom Firewall Rule	50
8.5.5. IP Sets	51
8.5.5.1. IP Sets Example (WhatsApp Configuration)	52
9. Statistics	55
10. Corporate Contact Information	56

# 1. About This Guide

This guide is intended for users of the RedPort Optimizer wXa-203 routers. It features only those sections of the user interface that require configuration for a specific service or may need to be accessed by the average user. **\*wXa refers to the webXaccelerator by RedPort, a trademark of Global Marine Networks, LLC.** 

The following chapter references will help you in administering the most-used features of the Optimizer:

Chapter 4 Getting Started Chapter 5.4 Halo Wi-Fi Extender Chapter 7.1 Change the Router Admin Password Chapter 7.3 Update Firmware Chapter 7.4 Reboot the Router Chapter 8.3 Restrict Wireless Network (Add or Change Network Password) Chapter 8.4 Rename the Wireless Network (Change SSID Name)

Other useful information can be found in the following chapters: Chapter 5.5 GPS Tracking Service Chapter 5.6 GPS/NMEA Repeater Settings Chapter 5.7 Remote Support Chapter 8.2 GSM Capability Chapter 8.5 Firewall Chapter 10 Corporate Contact Information

# 2. Introduction to the RedPort Optimizer

Global Marine Networks (GMN), the leaders in advancing satellite data speeds and services, helps Fixed and Mobile Satellite Services providers and their customers by offering the industry's fastest, most reliable and easy-to-use 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 GMN under the RedPort Global brand name at <u>redportglobal.com</u> 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 manage your usage, protect against accidental airtime usage, accelerate your data speeds, enable web compression, track your location via GPS, and provide routing, filtering and security.

Web, Weather and Tracking features require compatible service subscriptions.

# 2.1. Key Features

Designed specifically for use with satellite phones and satellite terminals:

- Replaces a standard router that is typically added to any satellite broadband installation.
- Powerful firewall accommodates any common installation scenario, with features including block or allow any range of port, IP address and protocols.
- Proxy Server enables HTTP filtering: whitelist/blacklist of URL's, domains, and rudimentary content filtering.
- Logging/Reporting to keep track of usage.
- Wi-Fi hotspot makes setup and use easy for crew with compatible computers and tablets.
- Supports Shared Web Compression.
- GSM Compatibility with optional GSM modem and your 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.

© 2020 RedPort Global I Powered by Pivotel America Inc.

- 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 for access to external Wi-Fi networks, when available.

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

## 2.2. Services Included

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

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.

GSM Compatibility - allows Internet connectivity via your GSM modem or cell phone with your own SIM card.

File Sharing - Network Shares 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. Contact your RedPort dealer to purchase.

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.

GPS Tracking - Using a GPS-enabled device, submit position reports to a central database for viewing on the tracking website.

RedPort VoIP Service - Transform 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.

# 3. Important 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 Guide is designed to help you.

CAUTION: The Optimizer ships pre-configured for use with the optional RedPort Halo Wi-Fi Extender. Tampering with any settings that are not addressed in this Guide will violate the warranty and may render the Optimizer inoperable.

## 3.1. 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) - when Transparent proxy is enabled, all traffic on port 80 (http port) is redirected through the internal proxy server. This allows URL and DNS filtering (whitelist and blacklist sites), some content filtering (i.e. remove flash video) and you can turn on 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.

Optimizer Advanced User Guide wXa-203

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

# 3.2. Designed Use of the Optimizer

This router is suitable for two distinctly different audiences:

#### 3.2.1. Single User Environment

For the single user that wants the convenience of BYOD (bring your own device) for email, web browsing, SMS and phone calls. All that is required is a RedPort-certified compression email account like XGate and/or compression web-browsing service like XWeb. By adding the XGate Phone app, a smartphone can be used to place and receive voice calls and/or SMS messages over the satellite network. With the optional RedPort VoIP service, the costs of those voice calls can be kept to a minimum.

#### 3.2.2. Multi-User Environment

This is a single-user router that can be configured for use in a multi-user environment. The idea is that you, as the installer or network administrator, will configure the router, using these guidelines, before installing it at its ultimate destination.

Once installed, the onsite administrator will log in and land on the Home page. The Home page has the common tasks that will be used locally just as creating and managing crew accounts.

The onsite administrator does not have access to the full user interface and therefore does not have the ability to re-configure the router. There is a separate user guide for the onsite administrator: Optimizer Onsite Administrator Guide.

# 3.3. How It Works At First Launch (Out Of The Box)

We ship the router ready for use with a RedPort-certified compression email and/or web browsing account.

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

This out-of-the-box configuration works well for single broadband users.

This configuration is also suitable for the multi-user environment where each person has a separate primary email and/or web browsing account. While you have the benefit of email and web compression on each primary account, all users have unlimited access to the Internet.

If you are in a multi-user environment, we recommend enabling Transparent proxy. With Transparent Proxy enabled, all traffic on port 80 (http port) is redirected through the internal proxy server. This allows URL and DNS filtering (whitelist and blacklist sites), some content filtering (i.e. remove flash video) and you can turn on 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 shared web compression (see Section 5.1).

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.

# 3.4. Navigating the User Interface (UI)

Access to the UI depends upon how you login to the router. There are two logins available: admin and superadmin.

The user interface is divided into sections; use the tabs to access the required service or information. On most pages in the user interface you will see three buttons in the lower right corner: **Reset:** Returns the page to its previous saved state.

Save: Saves the changes, but does not yet apply the changes.

**Save & Apply:** Saves the changes and applies them to the router configuration. In some cases, the router must reboot to apply the change. If reboot is required, it will be noted on the page.

# 4. Getting Started - User Interface (UI) Access

In a typical situation, the Optimizer router arrives to you with the following services enabled:

- Closed Firewall allowing email and web access via RedPort-certified services only.
- GPS/NMEA Repeater.

🙆 Reset

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 (additional fees may apply).
- GPS Tracking (additional fees may apply).
- · RedPort VoIP for multi-user calls and SMS (additional fees may apply).

This guide is designed to help you understand the Optimizer to customize the configuration to meet your needs.

For alternative Home Page access methods, see the RedPort Optimizer Installation Guide.

2. Open any web browser on the computer and enter the URL: 192.168.10.1

The Optimizer ships with two existing accounts:

- Admin for normal day-to-day operation.
- Superadmin for configuration and maintenance.

## 4.1. Access the Home Page

To access the router's Home page you must login to the router. This can be accomplished in several ways however the most popular method is to:

1. Connect to the Wi-Fi Hotspot created by the router using a PC. Connect to the Wi-Fi Hotspot just like you would any other Wi-Fi connection: On a Windows PC, go to: Windows Start > Control Panel > Network Connections.

On a MAC, go to: Apple > System Preferences > Network.

The Network Name will look something like: 'wXa-203-XXXX' where 'XXXX' is the last four digits of the Optimizer's Mac address.

For alternative Home Page access methods, see the RedPort Optimizer Installation Guide.

2. Open any web browser on the computer and enter the URL: http://192.168.10.1

The Optimizer ships with two existing accounts:

- Admin for normal day-to-day operation.
- Superadmin for configuration and maintenance.

#### 4.1.1. Onsite Administrator Login (Admin)

Onsite Admin: username=admin, password=webxaccess.

This login gives the user access to portions of the user interface and the ability to perform common tasks such as:

- Monitor the system status.
- Reboot the router, if necessary.
- · Change the router password for the admin account, if necessary.

#### 4.1.2. Installer/Network Administrator Login (Superadmin)

Technician: username=superadmin, password=webxaccess.

This login provides full access to the user interface for configuration and maintenance of the router.

Once logged in, you will see the router's Home page (Super Administrator login shown):

ome Services Status System Netwo	rk Statistics Logout
asks	
elcome	
'iFi Extender Setup	
Step 1	Connect Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
Step 2	Enable WiFi Extender     WiFi Extender Status: OFF
	Enable WiFI Extender to route all network traffic through WiFI Extender. Make sure you have configured the WiFI Extender first (see Step 1).
Step 3 (Automatic)	2 Disable Firewall
	Iterwall Status: ON Disabling the firewall allows all traffic to/from the Internet through the router. This options should be used with caution and only when connected to land based WiFi.
ystem Status	
	System status overview
	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> </ul>
	System status overview  Realtime bandwidth usage over satellite link  Historic bandwidth usage over satellite link
	System status overview Realtime bandwidth usage over satellite link  System message log
	System status overview Realtime bandwidth usage over satellite link SHistoric bandwidth usage over satellite link System message log
ocal WiFi setup	System status overview Realtime bandwidth usage over satellite link SHistoric bandwidth usage over satellite link System message log
ocal WiFi setup SSID and Security	System status overview  Realtime bandwidth usage over satellite link  Historic bandwidth usage over satellite link  System message log  WiFi setup  Change hotspot name and/or add security and set password
ocal WiFi setup SSID and Security	System status overview  Realtime bandwidth usage over satellite link  System message log  WiFi setup  Change hotspot name and/or add security and set password
ocal WiFi setup SSID and Security /stem	System status overview Realtime bandwidth usage over satellite link  Historic bandwidth usage over satellite link  System message log  WiFi setup  Change hotspot name and/or add security and set password
ocal WiFi setup SSID and Security Istem	System status overview  Realtime bandwidth usage over satellite link  System message log  MiFi setup  Change hotspot name and/or add security and set password  Realtime bandword  Rea
ocal WiFi setup SSID and Security /stem	System status overview   Realtime bandwidth usage over satellite link  Historic bandwidth usage over satellite link  System message log   WiFi setup  Change hotspot name and/or add security and set password  Rebot router  Rebot router
scal WiFi setup SSID and Security Istem	System status overview      Realtime bandwidth usage over satellite link      Historic bandwidth usage over satellite link      System message log      WiFi setup     Change hotspot name and/or add security and set password      Router password      Router password      Reboot router

NOTE: The Wi-Fi Extender Setup section only displays when the optional RedPort Halo Wi-Fi Extender is physically connected to the Optimizer and powered ON.

NOTE: An alternate method to access the user interface: With power to the Optimizer, physically connect the Optimizer to your computer using a standard Ethernet cable in the Optimizer's LAN port and follow the directions above, starting with Step 2, entering the URL http:192.168.10.1

This Home Page is the onsite administrator's gateway to the most used features.

From the Home Page you have access to the remaining sections of the user interface.

Services: allows access to all the services available on the router.



Each service is contained in its own tab under the Services section. This is where you will enable/disable the services and configure them for use.

**Status:** displays how much memory the router is using, who is connected via Wi-Fi and other information you may find useful.

Opti	mizer   w	Xa-203 v2.6	51   Load:	1.09 1.03	1.01   Auto	Refresh: or		Changes: 0
	Home	Services	Status	System	Network	Statistics	Logout	
	Overvie	Firewa	all Route	es Syste	m Log K	ernel Log	Realtime Graphs	

The System Log contains detailed information of the router's performance. It will report error messages and can be useful when troubleshooting connection issues. Realtime Graphs report how much data is being using by the different interfaces. All Status information is Read Only.

**System:** contains some of the router's basic settings for you to configure plus a few maintenance functions.

Optin	nizer   w	Xa-203 v2.	58   Load:	: 1.03 1.04	0.70   Auto	o Refresh: or		Changes: 0
	Home	Services	Status	System	Network	Statistics	Logout	
	System	Router F	Password	Profiles	Backup / Fl	lash Firmware	Reboot	

Use this section to set your time zone, change the 'admin' and/or 'superadmin' password, flash new firmware to the router, reboot the router if necessary. Profiles is a way to 'clone' the router configuration for use on another Optimizer router.

Network: contains access to the network interfaces and the firewall.

Opt	mizer   w	Xa-203	v2.6	1   Load:	1.00 1.02	1.00   Auto F	Refresh: on									Chang	es: 0
	Home	Servio	ces	Status	System	Network	Statistics	Logout									
	Interfa	ces	Wifi	DHCP a	nd DNS	Hostnames	Static Routes	Diagnostics	Firewall	PPP	_	_	_		_		

Use this section to configure network interfaces, run diagnostics, or modify the firewall. Statistics: contains information about resource usage.

#### Statistics: contains information about resource usage.



Use the tabs to navigate through the user interface. You will see that the information represented in the user interface can be quite technical. This Guide will cover only those sections of the user interface that require configuration for a specific service or may need to be accessed by the average user.

# 4.2. How to Use with Default Setup

We ship the router ready for use with Voice and SMS ready to be enabled for use with compatible satellite devices using standard satellite airtime.

This out-of-the-box configuration works well for single broadband users. This configuration is also suitable for the multi-user environment where each person has a separate primary email and/or web browsing account.

While you have the benefit of email and web compression on each primary account, all users have unlimited access to the Internet.

BEST PRACTICE: If you are in a multi-user environment, we recommend enabling Transparent proxy. With Transparent Proxy enabled, all traffic on port 80 (http port) is redirected through the internal proxy server. This allows URL and DNS filtering (whitelist and blacklist sites), some content filtering (i.e. remove flash video) and you can turn on 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 shared web compression.

#### 4.2.1. 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. Turn your satellite phone ON.

3. Connect the Optimizer to your satphone with the appropriate cable.

4. On your computer, iOS or Android device, connect to the wireless network created by the Optimizer. The name of the wireless network will be something like: wXa-203-xxxx, where xxxx may represent the last four digits of the Mac address of the Optimizer.

5. Once connected to the wireless network, open the RedPort-certified email program (such as XGate) and go to Settings > Connection > and set the Connection Type to "Optimizer xxxxxx" where xxxxxx represents your satphone connection. Click [OK].

6. Wait for a strong satphone signal.

7. Start an email or a web browsing session.

#### 4.2.2. Voice Calls

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

CAUTION: When you enable the Voice PBX it is listening on all ports. Without further configuration, this could leave you vulnerable to unwanted traffic. Please review Chapter 4.3.1 How to Secure Your Router.

#### 4.2.3. SMS Messaging

SMS is disabled by default but can be enabled for use with compatible satellite devices using standard satellite airtime. See Section 5.3 for details on configuration and use of the SMS Messaging service.

CAUTION: When you enable the SMS service it is listening on all ports. Without further configuration, this could leave you vulnerable to unwanted traffic. Please review Chapter 4.3.1 How to Secure Your Router.

## 4.3. Router Security \*\*IMPORTANT\*\*

If you modify the firewall from its default state you may have WAN ports open.

If you enable the Voice PBX, SMS messaging it is listening on all ports.

Any of these 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 the 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.

CAUTION: Before you block the WAN ports, read the next chapter. **Blocking the WAN ports at this stage may lock you out of the router.** We've built in some measures to help minimize that possibility, but, please pay special attention when making router configuration modifications.

#### 4.3.1. How to Secure Your Router\*\*\*IMPORTANT\*\*\*

First, confirm that the Disable anti-lock rule setting is "Unchecked" in System > System Settings. If it is checked, you want to uncheck it to Enable the anti-lock rule. The anti-lock rule prevents the administrator from inadvertently locking him/herself out of the router when programming firewall rules.

Confirm that in Network > Firewall > Firewall Rules that the first rule "BLOCK WAN" is disabled. If you Enable (check) this rule you will lock yourself OUT of the router, unless the antilock rule is enabled (unchecked). If you lock yourself out of the router you must perform a factory reset.

Confirm that in Services > Web Compression and Filtering > Advanced that Listen Interfaces is set to LAN. Do not change this to WAN unless you desire proxy service through the WAN port. If changing the default configuration to listen on the WAN then firewall rules must be created to allow access to the proxy listen port (port 3128 by default).

Go to System > Router Password and change the router password for both the "superadmin" and the "admin" access.

NOTE: The BLOCK WAN firewall rule, if enabled, will prevent access to these ports.

If Voice PBX is enabled, it is listening on all ports. You can specify the Interface to Listen (such as LAN) in Services > Voice PBX > Settings OR, you can leave it to listening on all interfaces and use a firewall rule to restrict traffic Network > Firewall.

NOTE: The BLOCK WAN firewall rule, if enabled, will prevent access to these ports.

If planning to access the web user interface over the WAN port then create firewall rules with higher precedence than the BLOCK ALL rule that allow traffic from your Internet IP address to the router.

NOTE: Ports 80, 443 and 22 are open, if not disabled.

When you have completed and tested your configuration and are confident that it is working as desired, you can remove the Anti-Lock rule in System > System Settings. Now you can Enable the BLOCK ALL from WAN firewall rule in Network > Firewall > Firewall Rules.

# 5. Services

## 5.1. 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.

#### 5.1.1. Settings

ptimizer   wXa-203 v2.61   Load: 1.00 1.00 1.00	Changes: 0
Home Services Status System Network Statistics Log	gout
Web Compression and Filtering SMS GPS Tracking Remote Acces	ess WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor
Settings Filters Log Help	
Web Filtering and Compression Proxy Settings	
Enable and configure web compression and filtering features.	
Compression General Settings Advanced	
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.
Username	Enter_Compression_User_Name_Here
Password	Compression_Password_Here
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.
(Caracteria)	Save 🗓 Save & Apply
Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Right	ts Reserved)

#### 5.1.1.1. Compression

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

Optimizer Advanced User Guide wXa-203

**Enable Compression:** If you have purchased Web Compression service, click the checkbox to Enable compression. The page will expand; see With Compression Enabled below.

**Username:** Enter the Username given to you by your service provider. This username is specific to the compression service.

**Password:** Enter the Password given to you by your service provider. This password is specific to the compression service.

**Bypass Regex Domain:** This is the 'whitelist' of sites that should not be compressed. To add a site, click the Add icon . 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.

Ontimi	zer   wXa-203 v2 61   load: 1 00 1 00 1 00		Changes: 0
Optim	Inne Carriers Status Custom Naturals Statistics		changes. o
	Tome Services Status System Network Statistics Log	gout	_
12	Web Compression and Filtering SMS GPS Tracking Remote Acce	ss WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor	
11	Settings Filters Log Help		_
w	eb Filtering and Compression Proxy Settings		
Er	able and configure web compression and filtering features		
	Compression General Settings Advanced		
	Enable compression	✓ ② 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.	
	Proxy Authentication by Client	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.	
	Username	Enter_Compression_User_Name_Here	
	Password	Password_Here	
	Server	xweb.gmn-usa.com	
	Compression Level	(Maximum 🛟	
	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.	
(	Reset	Save DSave	e & Apply

**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.

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".

#### 5.1.1.2. General Settings

These are the general settings for the internal proxy service. You can use the internal proxy server and enable transparent proxy to redirect all http traffic for filtering.

Optimizer   wXa-203 v2.61   Load: 1.00 1.00 1.00	Changes: 0
Home Services Status System Network Statistics Log	gout
Web Compression and Filtering SMS GPS Tracking Remote Access	ess WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor
Settings Filters Log Help	
Web Filtering and Compression Proxy Settings	
Enable and configure web compression and filtering features.	
Compression General Settings Advanced	
Enable Web Proxy	🛛 🙆 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.
Reset	Save DSave & Apply

CAUTION: Before enabling Transparent Proxy, refer to Chapter 4.3 Router Security.

## 5.1.1.3. Advanced Settings

Under normal operating conditions there is little to change here.

nizer   wXa-203 v2.61   Load: 1.00 1.00 1.00	Chang
Home Services Status System Network Statistic	s Logout
Web Compression and Filtering SMS GPS Tracking	Remote Access WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor
Settings Filters Log Help	
Web Filtering and Compression Proxy Settings	5
nable and configure web compression and filtering features.	
Compression General Settings Advanced	
Filtering	💟 ③ Enable/Disable content filtering.
Default filtering scheme	Light +
	Filtering makes changes to the webpages to either help with compression or niter content by removing it before loading on the users' page. Filtering schemes are as follows:
	Light - Safe for all sites. Most content will remain on page with little monnication to the original content. Moderate - Safe for most sites. Modereate content filtering with removal of some elements.
	Aggressive - Reasonable privacy protection with best bandwidth utilization but require some exceptions for trusted sites, most likely because of cookies or SSL.
Listen address	3128
	Bind proxy to interface IP address and port number using [ipaddress:port] formatting. Omit IP address to bind to all interfaces.
Listen interfaces	✓ LAN - 192.168.10.1
	Bind proxy to the following interfaces
Enforce Blocks	🕑 🗐 Whether the user is allowed to ignore blocks and can "go there anyway".
Buffer Limit	4096
	Maximum size of the buffer for content filtering.
Forwarded Connect Retries	2 How often the Proxy retries if a forwarded connection request fails.
Keep Alive Timeout	300
	In Number of seconds after which an open connection will no longer be reused.
Socket Timeout	300
Log Rotation	
	<ul> <li>Iconstruction schedule.</li> </ul>
Debug Level	4096
	8192
	through. 4096 = Startup banner and warnings. 8192 = Non-fatal errors.
Reset	Save 🛛 Save & Appl
red by RedPort (Copyright © Global Marine Networks, LLC 20:	15 - All Rights Reserved)

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: determine 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 will 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, whitelists and blacklists are working. Deactivate debug level 1 when testing is complete.

#### 5.1.2. 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.

izer   wXa-203 v2.61   Load: 2.08 1.14 0.45
Home Services Status System Network Statistics Logout
Web Compression and Filtering SMS GPS Tracking Remote Access WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor
Settings Filters Log Help
ilters
et of domains and/or urls which override the default filtering scheme defined in settings i.e. excentions to default filtering scheme
Fragile sites that should not be filtered
List of domains and paths for complex sites that require minimal interference such as ".office.microsoft.com" and "www.apple.com". See Help for "Domain and Path Syntax".
X Clear
Class which should be blocked
Sites which should be blocked List of domains and paths for sites which should be blocked such as ".windowsupdate.microsoft.com" or ".update.". Use "/" to block all sites then white list specific ones below. See Help for "Domain
and Path Syntax".
Y
V Maar
Clear
Sites which are allowed
List of domains and paths for sites which should be allowed. This list overides the block list above. See Help for "Domain and Path Syntax".
X)Clear
Sub
red by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

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 (see section 5.1.4 for details). 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.

# 5.2. SMS Messaging

If using a compatible satellite device, it is possible to send and receive SMS messages directly from the Optimizer and to route incoming SMS messages to one or more smartphones connected to the local wireless network. Access to Services > SMS requires the 'superadmin' login.

#### 5.2.1. SMS Settings

Use Settings to enable and configure the SMS parameters.

timize	er   wXa-203 v2.61   Load: 1.00 1.02 0.70				Chan		
Ho	me Services Status System Network Statistics Log	out					
We	eb Compression and Filtering SMS GPS Tracking Remote Access	WiFi Extender 0	GPS/NMEA Repeater	Voice PBX	FBB Monitor		
Se	ttings Management						
~ m	c paramotors						
sm	s parameters						
conf	igure the parameters for SMS						
·							
E	Enabled						
1	nterval in seconds between LOCAL send attempts	240					
	number of days that messages stay in queue when receiving messages						
-	alliber of days that messages stay in quede when receiving messages						
	satellite device	Iridium	Ţ				
(	Check for received messages (in seconds)	360					
(	Configure extensions to receive SMS	Redirect					
L							

1. Click the checkbox to enable SMS.

Satellite device	V Iridium
Check for received messages (in seconds)	iSavi Sailor FBB
Configure extensions to receive SMS	Redirect

- 2. Select the appropriate Satellite device from the drop down menu.
- 3. Click <Save & Apply>.

#### 5.2.2. Configure SIP Extensions to Receive SMS Messages

With SMS enabled, click <Redirect> (see SMS Settings screen above) to go to the Voice PBX Settings page. Click the Extensions tab to configure which extensions are to receive incoming SMS messages.

Optin	ptimizer   wXa-203 v2.61   Load: 1.00 1.00 0.81 Changes: 0									
	Home	Sei	vices Status	System Network	Statistics Lo	ogout				
	Web C	ompre	ssion and Filtering	SMS GPS Trackin	g Remote Access	WiFi Extender	GPS/NMEA Repeater	Voice PBX	FBB Monitor	
	Setting	gs E	xtensions Logs	Sat SIP Trunk R	edPort VoIP					
	vton	cion								
-	xten	sion								
	SIP	Exter	isions							
	Ring	SMS	Extension	Password	Caller ID			Description		
			Value larger than 200	SIP extension password	d Free text		You may enter a de	escription here fo	r your reference	
		$\checkmark$	201	1234	201	Captain line				× Delete
			202	1234	202	Crew line 1				Delete
			203	1234	203	Crew line 2				× Delete
			204	1234	204	Crew line 3				× Delete
	📋 Ac	ld								
L.										
	🖉 Reset									Save 🛛 Save & Apply

To enable an extension to receive SMS messages, use the checkbox in the SMS column.

#### 5.2.3. How to Send/Receive SMS Messages

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-203-xxxx'. Open the XGate Phone App. Click <Chat> to send an SMS message or to view an SMS message received.



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.)

#### 5.2.4. SMS Management

With SMS enabled you can send SMS messages directly from the Optimizer user interface and you can manage SMS messages that have been sent and received.

1.
Select
ct

Using the <Select> checkbox you can specify which messages to delete or you can delete all messages.

# 5.3. Voice PBX

Requires 'superadmin' login.

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

- Sailor FBB terminal requires XGate Phone app\*.
- · IsatHub iSavi requires IsatHub Control app and either IsatHub Voice app or XGate Phone app.
- Any satellite terminal with a RJ-11 port requires XGate Phone app\* AND an ATA accessory. Contact your satellite service provider for ATA information.

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

Multi-Voice 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
- BGAN
- VSAT
- RedPort Aurora
- Iridium Pilot
- Thuraya IP
- IsatHub iSavi

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 Chapter 4.3 Router Security.

#### 5.3.1. 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.

NOTE: Prior to enabling PBX service, review Chapter 4.3.1 How to Secure Your Router.

Click the checkbox to Enable the PBX.

When the PBX is enabled it is listening on all ports. This may leave you vulnerable to unwanted traffic. See Chapter 4.3.1 How to Secure Your Router.

Optimizer   wXa-203 v2.61   Load: 1.35 1.15 1.05 Changes
Home Services Status System Network Statistics Logout
Web Compression and Filtering SMS GPS Tracking Remote Access WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor
Settings Extensions Logs Sat SIP Trunk RedPort VoIP
PBX Services
Enable PBX I Brable/Disable PBX VOIP service.
Listen port
Port used by the PBX to listen for SIP traffic. Leave blank for default port 5060.
Listen interfaces       ALL - 0.0.0       Bind proxy to the following interfaces
Save Save Save Save Save Save Save Save
Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

#### 5.3.2. Setup 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.

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

Optin	izer   v	vXa-2	03 v2.61   Load: 1.0	5 1.10 1.04						Changes: 0
J	Home	Se	rvices Status S	system Network	Statistics Lo	gout				
H.	Web Co	ompre	ssion and Filtering	SMS GPS Tracking	Remote Access	WiFi Extender	GPS/NMEA Repeater	Voice PBX	FBB Monitor	
	Setting	s I	Extensions Logs	Sat SIP Trunk Re	edPort VoIP					
, I	vten	cion	c .							
	Atens	sions	<b>.</b>							
	SIP	ixter	isions							
	Ring	SMS	Extension	Password	Caller ID			Description		
			Value larger than 200	SIP extension password	Free text		You may enter a de	scription here for	your reference	
		$\checkmark$	201	1234	201	Captain line				× Delete
			202	1234	202	Crew line 1				Delete
			203	1234	203	Crew line 2				Delete
			204	1234	204	Crew line 3				× Delete
	📋 Ade	d								
	👂 Reset									Save 🔝 Save & Apply
Pow	ered by	RedP	ort (Convright © Gld	bal Marine Networks.	LLC 2015 - All Righ	ts Reserved)				

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/receive phone calls requires the 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

#### 5.3.3. How to Make/Receive Voice Calls

Using the smartphone or tablet Settings, connect to the Optimizer wireless network 'wxa-203-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 consective sessions -- with the optional RedPort VoIP service. Contact your service provider for details.



## 5.3.4. Fleet Broadband Monitoring (FBB)

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

Optin	Dptimizer   wXa-203 v2.61   Load: 1.00 1.01 1.00 Changes: 0							
	Home Services Status System Network Statistics Lo	gout						
	Web Compression and Filtering SMS GPS Tracking Remote Access	WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor						
1	Fleet Broadband Monitor							
F	leet Broadband monitoring							
-	eet Broadband Monitoring requires that the Eleet Broadband he configured	d to accent &T commands						
	Elect Broadband Monitoring Settings							
	Enable							
	Configure Port and IP	Is this to configure the IP address and port if different than the default route						
	Debug	🕑 🐵 Enable debug ouput in the system log						
	Threshold	26.5						
		Isignal Levels greater than this produce a constant orange LED If the lower the LED is off						
	Reset 3	Save 💷 Save & Apply						
Pow	ered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Righ	ts Reserved)						

# 5.4. Halo Wi-Fi Extender

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.

For your convenience, the Halo Wi-Fi Extender Quick Start Guide can be found in Appendix B of this document. It includes important information regarding the physical connection setup.

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

5.4.1. Configure Connection to the Halo

With the Halo powered ON and connected to the Optimizer. Login to the Optimizer router with either username = admin or with username = superadmin (see Chapter 4 Getting Started for details). Configuration requires two steps to connect:

#### 5.4.2. Connect to the External Wi-Fi Network.

ptin	nizer   w	Ka-203 v2.61   Load: 1.08 1.02 1.01	Changes: 0
J	Home	Services Status System Network Statistics Logout	
ľ	Tasks		_
ľ	Velcon	ne	
	WiFi Ex	xtender Setup	
	Step 1	Connect Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.	
	Step 2	Enable WiFi Extender     WiFi Extender Status: <b>OFF</b> Enable WiFi Extender Status: <b>OFF</b> Enable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi     Extender first (see Step 1).	
	Step 3	(Automatic)  (Automatic)  (Automatic)  (Automatic)  (Automatic)  (Automatic)  (Automatic)  (Building the firewall allows all traffic to/from the Internet through the router. This options should be used with caution and only when connected to land based WiFi.	1
		<b>6</b>	

1. Click <Connect> button.

Optimizer   wX	ptimizer   wXa-WiFi v2.0   Load: 0.41 0.29 0.20   Auto Refresh: on Changes: 0								
Home	Status Admin								
Wireles	s Overview								
	Generic MAC	80211 802.11bgn (radio0) Wi Hz)   Bitrate: ? Mbit/s	Fi Extender			C Scar	Add		
	<b>SSID:</b> GMN 0% <b>BSSID:</b> 92:3	WiFi   <b>Mode:</b> Client 3B:AD:26:39:A3   <b>Encryption:</b> -				🛿 Disable 🗹 Edit	Remove		
Associa	ted Stations								
	SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate		
			No information a	available					
Powered by R	edPort (Copyright	© Global Marine Networks, LLC 2015	- All Rights Reserved)						

2. Click <Scan> to see what wireless networks may be available.

Optimizer   v	wXa-WiFi v2.0   Load: 0.09 0.22 0.15	Changes: 0
Home	Status Admin	
Join N	Network: Wireless Scan	
100%	GMN WiFi Channel: 8   Mode: Master   BSSID: 92:3B:AD:26:39:A3   Encryption: <u>WPA2 - PSK</u>	Join Network
100%	ATT8qfw8C4 Channel: 4   Mode: Master   BSSID: 14:ED:B8:42:1F:51   Encryption: <u>WPA2 - PSK</u>	Join Network
100%	GMN WiFi Channel: 8   Mode: Master   BSSID: 92:38:AD:26:3A:D4   Encryption: <u>WPA2 - PSK</u>	Join Network
<b>4</b> 61%	CGNM-0408 Channel: 6   Mode: Master   BSSID: 1C:AB:C0:81:04:08   Encryption: mixed WPA/WPA2 - PSK	Join Network
1	NTGR_VMB_1480705304	C lain Maturali

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

Optimizer   wXa-WiFi v2.0   Load: 0.38 0.25 0.17	Changes: 0
Home Status Admin	
Join Network: Settings	
WPA passphrase	Ø           Specify the secret encryption key here.
Name of the new network	wwan \$
	<sup>(2)</sup> Back to scan results <sup>(2)</sup> Submit
Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserve	ad)

4. Enter the password to access the external wireless network, if required. Click <Submit>.

mizer   wXa-WIFi v2.0   Load: 0.08 0.19 0.16   Auto Refresh: on Unsaved	Changes: 10						
Home Status Admin							
Wireless Network: Client "GMN WiFi" (wlan0)							
The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the Interface Configuration.							
Device Configuration							
General Setup							
Status Mode: Client [ SSID: GNN WIFi BSSID: 238:AD 266:39:A3 ] Encryption: WPA2 PSK (CCMP) Channel: 8 (2:447 GHz)   Tx-Power: 27 dBm 100% Signal: -15 dBm   Noise: -84 dBm Bitrate: 72.2 Mbit/s   Country: US							
Operating frequency Mode Channel Width							
Back to Overview @Reset	ve & Apply						
wered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)							

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.

ptimizer   w	imizer   wXa-WiFi v2.0   Load: 0.22 0.21 0.16   Auto Refresh: on Changes: 0						
Home	Status Admin						
Wirele	ss Overview						
<b>@</b>	Generic MAC8 Channel: 8 (2.44	80211 802.11bgn (radio0) 17 GHz)   Bitrate: 72.2 Mbit/s	ViFi Extender				
	ad SSID: GMI 100% BSSID: 92	N WiFi   <b>Mode:</b> Client 1:3B:AD:26:39:A3   <b>Encryption:</b> W	PA2 PSK (CCMP)				Q Scan
Associa	ated Stations						
	SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
	GMN WiFi	92:3B:AD:26:39:A3	?	-15 dBm	-84 dBm	39.0 Mbit/s, MCS 4, 20MHz	72.2 Mbit/s, MCS 7, 20MHz
WiFi E	ktender Statu	IS					
Auth	entication Stat	us					
Authe	nticated						
Inte	rface Live Statu	IS					
		HTTP is active web:direct	WIFI is active IPv4:192.168.51.71	50	DNS is active erver:192.168.51.	1	
Powered by F	RedPort (Copyright	© Global Marine Networks, LLC	2015 - All Rights Reserved)				

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.
- 5.4.3. Route Network Traffic through the Halo

Optimizer   wXa-203 v2.61   Load: 1.11 1.05 1.01	Changes: 0
Home Services Status System Net	ork Statistics Logout
Tasks	
Welcome	
WiFi Extender Setup	
Step 1	Connect Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
Step 2	<ul> <li>Enable WiFi Extender</li> <li>WiFi Extender Status: OFF</li> <li>Enable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi</li> <li>Extender first (see Step 1).</li> </ul>
Step 3 (Automatic)	(@ Disable Firewall) (@) Firewall Status: ON Disabling the firewall allows all traffic to/from the Internet through the router. This options should be used with caution and only when connected to land based WiFi.

1. Click < Enable Wi-Fi Extender>.

Optir	nizer   wXa-203 v2.61   Load: 1.03 1.04 1.00	Changes: 0
	Home Services Status Statistics Logout	
	Tasks	
١,	Velcome	
	WiFi Extender Setup	
	Step 1	Connect Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
	Step 2	Object         Disable WiFi Extender           WiFi Extender Status:         ON           Disable WiFi Extender to route traffic through Satellite Link.         Disable WiFi Extender to route traffic through Satellite Link.
	Step 3 (Automatic)	Enable Firewall     Firewall Status: OFF Enabling the firewall disables all traffic to the Internet except for optimized Email and web browsing.

All traffic is now routed through the Wi-Fi Extender. You can run XGate and XWeb.

To return to routing traffic through your satellite device, simply Click <Disable Wi-Fi Extender>.

5.4.4. Manage the Firewall (Optional)

If the firewall is ENABLED, ALL traffic from your computer is blocked from the Internet with the exception of XGate and XWeb traffic. This setting is recommended when using the Halo in areas where there may be many users competing for the wireless network bandwidth thereby causing slow and painful Internet connections.

If the firewall is DISABLED, ALL traffic is permitted, allowing unfettered access to the Internet as well as XGate and XWeb traffic.

If you want to sync some applications or perform some other function that is currently being blocked, i.e. streaming video, you must Disable the Firewall.

To Enable or Disable the firewall:

Optimi	zer   wXa-203 v2.61   Load: 1.03 1.04 1.00	Changes: 0
	tome Services Status Statistics Logout	
	asks	
w	elcome	
M	/iFi Extender Setup	
	Step 1	Connect Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
	Step 2	Disable WiFi Extender     WiFi Extender Status: ON Disable WiFi Extender to route traffic through Satellite Link.
	Step 3 (Automatic)	Enable Firewall     Firewall Status: OFF Enabling the firewall disables all traffic to the Internet except for optimized Email and web browsing.

To Disable the Firewall, Click <Disable Firewall>. To Enable the Firewall, Click <Enable Firewall>.

NOTE: When the <Disable Firewall> button is presented and the "Status" of the Firewall is: ON, then the Firewall is currently on, and Clicking the button will Disable the Firewall. Otherwise, when the <Enable Firewall> button is presented and the "Status" of the Firewall is: OFF, then the Firewall is currently off.

#### 5.4.5. Disconnect from the Halo

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

Optin	nizer   wXa-203 v2.61   Load: 1.15 1.04 1.01		Changes: 0
	Home Services Status Statistics Logout		
	Tasks		
	Velcome		
	WiFi Extender Setup		
	Step 1	Connect Select external WIFI network to connect to. Requires an external antenna amplifier connected to LAN port.	
	Step 2	Enable WiFi Extender     WiFi Extender Status: OFF     Enable WiFi Extender Status: OFF     Enable WiFi Extender for coute all network traffic through WiFi Extender. Make sure you have configured the WiFi     Extender first (see Step 1).	
	Step 3 (Automatic)	Disable Firewall     Firewall Status: ON     Disabling the firewall allows all traffic to/from the Internet through the router. This options should be used with caution     and only when connected to land based WiFi.	

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.

#### 5.5. GPS Tracking

If you wish to have tracking service using your satellite device, the Optimizer offers GPS Tracking service powered by GSatTrack or Tracking service via SMS message.

#### 5.5.1. Tracking powered by GSatTrack

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

NOTE: This tracking service must be purchased separately. See your satellite service provider for details.

To enable this service, Click Services > GPS Tracking > Tracking.

Item: Services Status System Network Status System   Web Compression and Nileting StS GPS Tacking Rendez Access WH i Letander Caching Tracking Parameters Endelp/disable tracking and set parameters. Status Statu	imizer   wXa-203 v2.61   Load: 1.05 1.03 1.00	Changes:
Web Compression and Filtering       Sty       OPS Tracking       Remode Access       WHI Extender       OPS//MHEA Repeater       Note PEX       File Monitor         Tracking Parameters       Exable/diable tracking and set parameters.       Standard airtime charges apply.         Exable/diable tracking and set parameters.       Exable/diable tracking Parameters         Evolution       Image: Standard airtime charges apply.         Exable/diable tracking parameters.       Evolution         Tracking parameters       Image: Standard airtime charges apply.         Evolution       Image: Standard airtime charges apply.         Tracking powered by RedPort       Image: Standard airtime charges of file tracking interval in minutes.         Tracking powered by RedPort       Image: Standard airtime charges of file tracking interval in minutes.         Indum OpenPort/Pilot       Image: Pass of file tracking interval in minutes.         Taking powered by RedPort       Image: Pass of file tracking interval in minutes.         Indum OpenPort/Pilot       Image: Pass of file tracking interval in minutes.         Val or broadband JP       IP sofrees of file tracking interval in tracking interval in minutes.         Val or broadband stellite       A valid NMEA/CPS feed is required. Tracking IME: 10137602410.         Indum terminal/Aurora/MCG-101       A valid NMEA/CPS feed is required.         Exerc GPS information to enen	Home Services Status System Network Statistics Lo	gout
Tracking         Checked Status         Schedur Handlesse tracking parameters. Standard airtime charges apply.         Schedur Handlesse tracking         Provider         Tracking parameters         Provider         Tracking provider. Please contact provider to setup tracking account.         Tracking powered by RedPort         Preserval         Tracking powered by RedPort         Preserval         Pret Broadband         Pret Broadband and IP         Pret Broadband statellite         I'MARSAT IsetBroadband         I'MARSAT IsetBroadband statellite         I'MARSAT IsetBroadband statellite         I'MARSAT IsetBroadband statellite         I'MARSAT IsetSphone         I'MARSAT Is	Web Compression and Filtering SMS GPS Tracking Remote Access	WIFI Extender GPS/NMEA Repeater Voice PBX FBB Monitor
Tracking Parameters    Enable/Idsoble tracking and set parameters. Standard airlime charges apply.    General Tracking Parameters   Enable Tracking Parameters   Enable Tracking Parameters   Enable Tracking Interval   Provider   Tracking Interval   Specify the tracking interval in minutes.    Tracking Devered by RedPort  Paese visit www.RedPortGlobal.com for registration information  IMARSAT FleetBroadband P P P P P P P P P P P P P P P P P P P	Tracking	
Enable/disable tracking and set parameters. Standard aitime charges apply.	Tracking Parameters	
General Tracking Parameters         Enable Tracking         Provider         State Devider         Tracking Interval         Bit         Specify the tracking interval in minutes.           Tracking powered by RedPort <th>Enable/disable tracking and set parameters. Standard airtime charges apply</th> <th>/.</th>	Enable/disable tracking and set parameters. Standard airtime charges apply	/.
	General Tracking Parameters	
Provider   Select Provider   Tracking provider. Please contact provider to setup tracking account.   Tracking Interval   Specify the tracking interval in minutes.   Tracking powered by RedPort Please visit www. RedPortClicbal.com for registration information   INMARSAT FleetBroadband   Pleet Broadband IP   IP address of Fleetbroadband.   Indium OpenPort/Plot   Indium OpenPort/Plot   Indium OpenPort/Plot   Indium Terminal/Aurora/NCG-101   A valid NMEA/GPS feed is required.   Tracking softs   Send GPS Information to an email address using satellite provider's SMS service   INMARSAT Isatphone   Indium terminal/Aurora/NCG-101   Indium terminal/Aurora/NCG-101   Stattack   Stattack   Send GPS Information to an email address using satellite provider's SMS service   INMARSAT Isatphone   Indium terminal/Aurora/NCG-101   Stattack   Stattack   Stattack   Stattack   Stattack   Stattack   Stattack   Stattack	Enable Tracking	
Tracking Interval       Image: Specify the tracking interval in minutes.         Tracking powered by RedPort         Please visit www.RedPortGlobal.com for registration information         IMMARSAT FleetBroadband         Pleet Broadband IP         IP address of FleetBroadband.         Indum OpenPort/Pilot         Indum OpenPort/Pilot         InMARSAT Istaphone         VSAT or broadband satellite         If vidium OpenPort/Pilot         Indum terminal/Aurora/MCG-101         ImMarSAT Istaphone         Tracking via SMS         Send GPS Information to an email address using satellite provider's SMS service         IMMARSAT Istaphone         Information to an email address using satellite provider's SMS service         IMMARSAT Istaphone         Vessel name         Send GPS Information to an email address using satellite provider's SMS service	Provider	Select Provider : (a) Tracking provider. Please contact provider to setup tracking account.
Tracking powered by RedPort         Please visit www.RedPortGlobal.com for registration information         IMMARSAT FleetBroadband         Fleet Broadband IP         Fleet Broadband IP         Indium OperAr/Pliot         Indium Compart/Pliot         Indium Terminal/Aurora/MCG-101         Indium terminal/Aurora/MCG-101 <th>Tracking Interval</th> <td>60 Specify the tracking interval in minutes.</td>	Tracking Interval	60 Specify the tracking interval in minutes.
INMARSAT FleetBroadband   Fleet Broadband IP   I P address of Fleetbroadband. Leave blank for default gateway.   Thales Certus VesselLink   Indium OpenPort/Pilot   Indium OpenPort/Pilot   INMARSAT Isatphone   VSAT or broadband satellite   Globalstar phone   I indium terminal/Aurora/MCG-101   I A valid NMEA/GPS feed is required.   INMARSAT Isatphone   Indium terminal/Aurora/MCG-101   I racking via SMS   Send GPS information to an email address using satellite provider's SMS service   INMARSAT Isatphone   Indium terminal/Aurora/MCG-101   I A valid NMEA/GPS feed is required.   Recipient Email Address   Sent   Sent	Tracking powered by RedPort Please visit www.RedPortGlobal.com for registration information	
Fleet Broadband IP   I P address of Fleetbroadband. Leave blank for default gateway.   Thales Certus VesselLink   Iridium OpenPort/Pilot   INMARSAT Isatphone   VAT or broadband satellite   Globalstar phone   I obstature   I obs	INMARSAT FleetBroadband	0
Thales Certus VesselLink   Iridium OpenPort/Pilot   INMARSAT Isatphone   VSAT or broadband satellite   Q A valid NMEA/GPS feed is required. Tracking IMEI: 101376092410.   Globalstar phone   Paracking via SMS   Send GPS Information to an email address using satellite provider's SMS service   Indium terminal/Aurora/MCG-101   Paracking via SMS   Send GPS Information to an email address using satellite provider's SMS service   Indium terminal/Aurora/MCG-101   Q A valid NMEA/GPS feed is required.   Recipient Email Address   Q Sate Tracking service or enter a valid email address. Also used for SOS messages. Enter blank to reset defaults.   Vessel name   Q Enter optional vessel name and/or other free text.	Fleet Broadband IP	IP address of Fleetbroadband. Leave blank for default gateway.
Iridium OpenPort/Pilot   INMARSAT Isatphone   VSAT or broadband satellite   Qiabalstar phone   Iridium terminal/Aurora/MCG-101   Iridium terminal/Aurora/MCG-101   Iridium terminal/Aurora/MCG-101   Index SMS   Send GPS information to an email address using satellite provider's SMS service   Indium terminal/Aurora/MCG-101   Indium terminal Address   Indium terminal Address <th>Thales Certus VesselLink</th> <td></td>	Thales Certus VesselLink	
INMARSAT Isatphone         VSAT or broadband satellite         VSAT or broadband satellite         Globalstar phone         Iridium terminal/Aurora/MCG-101         Iridium terminal/Aurora/MCG-101         Iridium terminal/Aurora/MCG-101         Invariant         Invariant         Send GPS information to an email address using satellite provider's SMS service         Invariant         Invariant         Inidium terminal/Aurora/MCG-101         Invariant         I	Iridium OpenPort/Pilot	0
VSAT or broadband satellite	INMARSAT Isatphone	0
Globalstar phone  Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar phone Globalstar glo	VSAT or broadband satellite	Q A valid NMEA/GPS feed is required. Tracking IMEI: 101376092410.
Iridium terminal/Aurora/MCG-101       Image: A valid NMEA/GPS feed is required.         Tracking via SMS         Send GPS information to an email address using satellite provider's SMS service         INMARSAT Isatphone         Iridium terminal/Aurora/MCG-101         Iridium terminal/Aurora/MCG-101         Recipient Email Address         GSatTrack         Image: Image	Globalstar phone	🗌 🙆 A valid NMEA/GPS feed is required. Tracking IMEI: 101376092410.
Tracking via SMS         Send GPS information to an email address using satellite provider's SMS service         INMARSAT Isatphone         Iridium terminal/Aurora/MCG-101         @ A valid NMEA/GPS feed is required.         Recipient Email Address         @ Select SMS tracking service or enter a valid email address. Also used for SOS messages. Enter blank to reset defaults.         Vessel name         @ Enter optional vessel name and/or other free text.	Iridium terminal/Aurora/MCG-101	Q A valid NMEA/GPS feed is required.
INMARSAT Isatphone         Iridium terminal/Aurora/MCG-101         Recipient Email Address         OSatTrack         Select SMS tracking service or enter a valid email address. Also used for SOS messages. Enter blank to reset defaults.         Vessel name         Enter optional vessel name and/or other free text.	Tracking via SMS Send GPS information to an email address using satellite provider's SMS serv	ice
Iridium terminal/Aurora/MCG-101       Image: A valid NMEA/GPS feed is required.         Recipient Email Address       Image: GSatTrack	INMARSAT Isatphone	
Recipient Email Address       GSatTrack         @ Select SMS tracking service or enter a valid email address. Also used for SOS messages. Enter blank to reset defaults.         Vessel name       @ Enter optional vessel name and/or other free text.	Iridium terminal/Aurora/MCG-101	A valid NMEA/GPS feed is required.
Vessel name   Enter optional vessel name and/or other free text.  Reset  Save I Save & Apply	Recipient Email Address	GSatTrack =
Save Save Save Save Save Save Save Save	Vessel name	Enter optional vessel name and/or other free text.
	le Reset	Save Save Save Apply

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 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.

#### 2. Select the satellite terminal you are using.

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

3. Click <Save & Apply>.

#### 5.5.2. Tracking via SMS

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.

me Services Status System Network St	atistics Logout Remote Access WiFi Extender GPS/NMFA Repeater Voice PBX EBB Monitor
acking	
orking Parameters	
ale/dicable tracking and set parameters. Standard aid	ing charges apply
eneral Tracking Parameters	nne charges appry.
Enable Tracking	0
Provider	Select Provider =
Fracking Interval	60 Specify the tracking interval in minutes.
racking powered by RedPort	
ease visit <u>www.RedPortGlobal.com</u> for registration inform	lation
NMARSAT FleetBroadband	0
leet Broadband IP	IP address of Fleetbroadband. Leave blank for default gateway.
Thales Certus VesselLink	0
ridium OpenPort/Pilot	0
NMARSAT Isatphone	
/SAT or broadband satellite	🗌 🗐 A valid NMEA/GPS feed is required. Tracking IMEI: 101376092410.
Globalstar phone	Ø A valid NMEA/GPS feed is required. Tracking IMEI: 101376092410.
ridium terminal/Aurora/MCG-101	A valid NMEA/GPS feed is required.
racking via SMS	
- and GPS information to an email address using satellite p	rovider's SMS service
NMARSAT Isatphone	0
ridium terminal/Aurora/MCG-101	🗌 🕼 A valid NMEA/GPS feed is required.
Recipient Email Address	GSatTrack  GSatTrack  GSelect SMS tracking service or enter a valid email address. Also used for SOS messages. Enter blank to reset defaults.
/essel name	Enter optional vessel name and/or other free text.

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. At this time, tracking via SMS is available with the Inmarsat IsatPhone, Iridium handheld 9575 Extreme, Iridium GO! or an Iridium terminal such as the Pilot.

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

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>.

# 5.6. 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: IsatPhonePro 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. In order to repeat GPS data, a separate GPS device must be connected.

#### 5.6.1. Equipment Setup

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

#### 5.6.1.1. 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 in order to establish a successful connection with your destination software.

#### 5.6.1.2. Handheld Satellite Phone with Integrated GPS

When using a supported USB connected satphone with integrated GPS, connect the satphone to the Optimizer using the Mini-USB (satphone) to USB (Optimizer) cable.

(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 in order to establish a successful connection with your destination software.

#### 5.6.1.3. 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 in order 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.

#### 5.6.1.4. RS-232 NMEA Device

With Serial Port Connector

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-2303HX 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 in order 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.

Without 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-2302HX USB to serial adapter as noted above.



#### 5.6.1.5. Connecting Multiple NMEA Devices

It is possible to connect up 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.

0         0
2 💿 💿 1
4 (сом) (сом)
RL45 RESET RESET RESET RESET RESET RESET RESET RESET RESET RESET RESET RESET

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.

## 5.6.2. GPS/NMEA Repeater Parameters Configuration

In order 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.

ptimizer   wXa-203 v2.61   Load: 1.00 1.00 1.00 Changes:				
Home Services Status System Network Statistics Log	gout			
Web Compression and Filtering SMS GPS Tracking Remote Access	WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor			
GPS/NMEA Repeater				
GPS/NMEA Repeater Settings				
Read GPS/NMEA information from a number of sources and repeat the data	over WiFi and Ethernet.			
Repeater Parameters				
Enable	Brable GPS montioring and repeating.			
Binary Mode	🗌 🍘 Pass raw binary data through without parsing for NMEA-183 sentenses.			
GPS/NMEA feed from USB	We USB connected GPS or NMEA feed as a source.  Note: Not compatible with RS-232 based satellite phones.			
Remote TCP server	Connect to remote TCP NMEA server.			
UDP Listener Port	10101 Sisten on UDP port number and rebroadcast.			
UDP Port	11101 Second and the			
TCP Port	11102  Broadcast to TCP port number.			
(See the set of the se	🧭 Save 💹 Save & Apply			
Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Right	ts Reserved)			

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.

2. 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.

3. 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.

4. 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.

5. 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.

NOTE: 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.

# 5.7. Remote Support

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.

Remote Support Access can be granted from two locations, each with some differences.

• Temporary Remote Support Access - The first remote support login access is located from the homepage and permits a one-time temporary access. Once the router is rebooted, this access will no longer be available.

To enable Temporary Remote Support Access, click <Home> tab, scroll down to the "Remote Access" section.

ter   wXa-203 v2.61   Load: 1.73 1.27 1.13	Chan
Services Status Statistics	ogout
asks	
elcome	
iFi Extender Setup	
Step 1	Connect Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
Step 2	<ul> <li>Disable WiFi Extender</li> <li>WiFi Extender Status: ON</li> <li>Disable WiFi Extender to route traffic through Satellite Link.</li> </ul>
Step 3 (Automatic)	Enable Firewall Firewall Status: OFF Enabling the firewall disables all traffic to the Internet except for optimized Email and web browsing.
rstem Status	
	System status overview
	Realtime bandwidth usage over satellite link
	Historic bandwidth usage over satellite link
	System message log
ocal WiFi setup	
SSID and Security	<ul> <li>WiFi setup</li> <li>Change hotspot name and/or add security and set password</li> </ul>
emote Support	
	Enable remote support Allow remote personal access to your router via a broadband satellite, WiFi, or cell phone link
/stem	
	Router password
	Reboot router

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

When remote support is enabled Remote Access URLs are displayed.

SSID and Security	III WIFF setup Change hotspot name and/or add security and set password	
emote Support		
http://remote.redportglobal.com:5614     schi/(remote.redportglobal.com:5613		
<ul> <li>ssn.//remote.reuportgiobal.com;5615</li> </ul>		
<ul> <li>ssi.//remote.reuporgioudi.com:so13</li> </ul>	Comparing the support     Comparing the support     Comparing the support	

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

- Reboot the router.
- Click < Disable Remote Support>.
- 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>.

ptimizer   wXa-203 v2.61   Load: 1.51 1.38 1.20 Changes:
Home Services Status System Network Statistics Logout
Web Compression and Filtering SMS GPS Tracking Remote Access WiFi Extender GPS/NMEA Repeater Voice PBX FBB Monitor
Remote Access
Options
Remote access uris:
Enable Remote Access Open up a tunnel to remote.redportglobal.com allowing remote access to the router and keep it running.
Save Save Save Save Save Save Save Save
owered by RedPort (Copyright @ Global Marine Networks, LLC 2015 - All Rights Reserved)

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

When remote support is enabled Remote Access URLs are displayed.

mizer   wXa-203 v2.61   Load: 1.66 1.42 1.22 Changes: 0
Home Services Status System Network Statistics Logout
Web Compression and Filtering         SMS         GPS Tracking         Remote Access         WiFi Extender         GPS/NMEA Repeater         Voice PBX         FBB Monitor
Remote Access
Options
Remote access urls: • http://remote.redportglobal.com:5041 • ssh://remote.redportglobal.com:5040
Enable Remote Access 2 Open up a tunnel to remote.redportglobal.com allowing remote access to the router and keep it running.
Access Port 5040
Save Save Save Save Save Save Save Save
vered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)

Disabling this Remote Support will not disable the one-time Remote Support. To disable remote support access: • Click <Services> tab, then click "Enable Remote Access".

# 6. Status

Available to both 'admin' and 'superadmin' login.

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 wifi
- 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

# 6.1. 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.

Step 1. Attempt an email connection. Step 2. Login to the Optimizer Home page.

Step 3. Go to Status > System Log.

Optimizer   wXa-203 v2.61   Load: 1.02 1.03 1.04	Changes: 0
Home Services Status System Network Statistics Logout	
Overview Firewall Routes System Log Realtime Graphs	
System Log	
Wed Mar 25 12:29:51 2020 daemon.info dnsmasq[738]: read /tmp/hosts/dhcp - 2 addresses Wed Mar 25 12:29:51 2020 daemon.info dnsmasq-dhcp[738]: read /etc/ethers - 0 addresses	
Wed Mar 25 12:30:11 2020 deemon.info dnsmaag[866]: started, version 2.80 cachesize 150 Wed Mar 25 12:30:11 2020 daemon.info dnsmaag[866]: scompile time options: IPV6 GNU-getopt no-DBus no-il®n no-IDN DHCP DHCPv6 no-Lua TFTP no-conntrack ipset auth DNSSE Wed Mar 25 12:30:11 2020 daemon.info dnsmaag[866]: DHCP. PT range 192.168.10.00 192.168.10.249. Lease time 12h	C no-I
Wed Mar 25 12:30:11 2020 daemon.info dnsmaaq-tftp[866]: TTTP root is /tftpboot Wed Mar 25 12:30:11 2020 daemon.info dnsmaaq[866]: read /etc/hosts - 1 addresses Wed Mar 25 12:30:11 2020 daemon.info dnsmaaq[866]: read /tmc/hosts/dhcp - 2 addresses	
Wed Mar 25 12:30:11 2020 daemon.info dnsmasq-dhcp[066]: read /etc/ethers - 0 addresses Wed Mar 25 12:30:11 2020 daemon.err uhttpd[1398]: Warning: Section @zone[1] (cap) cannot resolve device of network 'cap'	e

Step 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.

# 6.2. System Status for Monitoring Usage

For those that are interested, you can view the connection status in Status > Realtime Graphs.



# 7. System

# 7.1. Change Superadmin and/or Admin Password

The default password for both the superadmin login and the admin login is set to: webxaccess.

The easiest way to change the login admin password is to modify the XGate Settings. See the XGate Help File > User Interface > Settings > Optimizer, wXa, & Sat-Fi for details. The only way to change the superadmin password is via the Optimizer User Interface.

To change the password(s), login to the Optimizer:

ome Services Status System Netwo	rk Statistics Logout
asks	
elcome	
iFi Extender Setup	
Step 1	Connect Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
Step 2	Enable WiFi Extender
	WiFi Extender Status: OFF Enable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi
	Extender first (see Step 1).
Step 3 (Automatic)	Disable Firewall     Erewall
	Disabling the firewall allows all traffic to/from the Internet through the router. This options should be used with caution
	and only when connected to land based WiFi.
vstem Status	
	D Sustam status sussiliau
	System status overview
	Realtime bandwidth usage over satellite link
	Realtime bandwidth usage over satellite link     Historic bandwidth usage over satellite link
	Realtime bandwidth usage over satellite link      Historic bandwidth usage over satellite link      System message log
	Realtime bandwidth usage over satellite link      Historic bandwidth usage over satellite link      System message log
ocal WiFi setup	Realtime bandwidth usage over satellite link      Historic bandwidth usage over satellite link      System message log
ocal WiFi setup SSID and Security	Change hotspot name and/or add security and set password
ocal WiFi setup SSID and Security	Realtime bandwidth usage over satellite link     Realtime bandwidth usage over satellite link     System message log
ocal WiFi setup SSID and Security /stem	
ocal WiFi setup SSID and Security /stem	Constant status vorteen
ocal WiFi setup SSID and Security Istem	Constant status devices      Realtime bandwidth usage over satellite link      Historic bandwidth usage over satellite link      Historic bandwidth usage over satellite link      System message log      WiFi setup     O     Change hotspot name and/or add security and set password      Router password      Rebot router
scal WiFi setup SSID and Security rstem	Control of the second security and set password      Control of the security and set password      Control of

Click <Router password>.

When logged in as the superadmin, you will see this screen. If logged in as the admin user, you can only change the password for the admin login.

Optim	izer   wXa-203 v2.61   Load:	1.02 1.05 1.06			Changes: 0
	Home Services Status	System Network Statistics	Logout		
	System Router Password	Profiles Backup / Flash Firmware	Reboot		_
R	outer Password				
	Change Password Change password for the supe	radmin user.			
	Password		<i>"</i>	_ #	
	Confirmation		Ø	ø	
	Change Password Change the password for the a	dmin user. This password does not apply	to the superadmin account.		
	Password		2		
	Confirmation		<b>i</b>		
	Reset			Save 2	Save & Apply
Powe	red by RedPort (Copyright ©	Global Marine Networks, LLC 2015 - All	Rights Reserved)		

- 1. Enter the new password in the password text box.
- 2. Enter the same password again in the Confirmation text box.
- 3. Click <Save & Apply>.

This procedure changes the password for the Superadmin or the Admin login only. When connecting your computer, iOS or Android device to the wireless network, you will not use this Admin login password. This

password is used only to access the Optimizer user interface.

## 7.2. Profiles

Profiles 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 > Profiles.

Optim	izer   w>	(a-203 v2.61   Loa	d: 1.37 1.15	1.07											Chan	ges: 0
	Home	Services Status	System	Network Sta	atistics	Logout										
P	System	Router Password	Profiles	Backup / Flash	Firmware	Reboot	_	_	_	_	_	_	_	_	_	-
L.	Profiles	Tools	_				_		_	_		_		_	_	-
Р	rofile	Manager														
т	o create	predefined router	onfigurations	first adjust route	er settings th	nen save then	n by selecti	ing Add, givi	ng the profile	e a name a	and description	, followed by	Save & Apply	. The Ad	d function	
m	emorize	s the current route	r configuratio	n and stores it in	n the named p	profile.										
	Manag	je Profiles														
		Profile						Description								
	ATA		Analog Teleph	ione Adapter and Wi	/iFi-Ethernet Ne	etwork Bridge								Insta	ll 🙁 Delete	
	SatFi		SatFi ATA Pro	file										🕒 Insta	ll 🙁 Delete	
	Factory		Factory defau	lt settings										Insta	ll 🙁 Delete	
	Add															
	Reset													Save 💟	Save & App	y
Powe	red by R	edPort (Copyright	© Global Mar	ine Networks, LL	_C 2015 - All	Rights Reserv	ved)									

There are three default profiles:

ATA: This profile is used to make the Optimizer into an Analog Telephone Adapter when linking an Analog Telephone through Wi-Fi Ethernet Networking Bridge and repeats the satellite terminal's SSID. This profile would be installed automatically as needed when the Optimizer is plugged into a satellite terminal.

SatFi: This profile is used to make the Optimizer into an Analog Telephone Adapter when linking an Analog Telephone through Wi-Fi Ethernet Networking Bridge and repeats the satellite terminal's SSID. This profile would be installed automatically as needed when the Optimizer is plugged into a satellite terminal.

Factory: This profile will reset the Optimizer to factory defaults and all custom configuration will be lost.

To create and use a new Profile:

Opti	mizer   wX	(a-203 v2.61	Load: 1	1.37 1.15 1.	.07				Chang	es: 0
	Home	Services S	Status	System	Network Statistics	Logout				
	System	Router Pas	sword	Profiles	Backup / Flash Firmware	Reboot				
	Profiles	Tools		_		-				
	Profile	Manager								
	To create memorizes	predefined ro s the current	outer conf router co	figurations fi onfiguration	irst adjust router settings t and stores it in the named	hen save the profile.	by selecting Add, giving the profile a	name and description, followed by Save & Appl	y. The Add function	
	Manag	e Profiles								
		Profile					Description			
	ATA		Ar	Analog Telephor	ne Adapter and WiFi-Ethernet N	etwork Bridge			🖸 Install 🙁 Delete	
	SatFi		Sa	GatFi ATA Profile	0				🛛 Install 🙁 Delete	
	Factory		Fa	actory default	settings				🛛 Install 💌 Delete	
	Add									
	🖾 Reset								Save Save & Apply	y.
Pov	ered by R	edPort (Copy	right © (	Global Marin	ne Networks, LLC 2015 - All	Rights Rese	ed)			

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 desire profile, then <Save & Apply>.

# 7.3. Update Optimizer Firmware

Get the latest Optimizer firmware version from here:

redportglobal.com/support/technical-downloads/

Save the .bin file to your computer (pc or mac).

NOTE: If you have created any Profiles you may want to Export them before flashing new firmware and Import them when done. See Chapter 7.2 for Profiles details.

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

ptimizer   wXa-203 v2.61   Load: 1.00 1.03 1.05		C	nanges: 0
Home Services Status System Network Statistics Log	gout		
System Router Password Profiles Backup / Flash Firmware Re	eboot		-
Flash operations			_
Actions Configuration			
Backup / Restore Click "Generate archive" to download a tar archive of the current configurat	ion files. To reset the firmware to its initial	state, click "Perform reset" (only possible with squashfs images).	
Download backup:	Generate archive		
Reset to defaults:	🙆 Perform reset		1
To restore configuration files, you can upload a previously generated backu	p archive here.		
Restore backup:	Choose File No file chosen	Upload archive	1
Upload a sysupgrade-compatible image here to replace the running firmwar usually best to leave "Keep settings" unchecked. Keep settings:	re. Check "Keep settings" to retain the curr	ent configuration (requires an Optimizer compatible firmware image). It is	1
Image:	Choose File No file chosen	Flash image	
			J
WiFi Extender			
Click to peform flash operations such as firmware update or factory default	restore on WiFi Extender.		
Caution: Note that this method is used to update firmware on the WiFi ext you are doing. Loading the incorrect firmware on your device could render	ender and not your Optimizer. Be sure to set t	elect the appropriate firmware for your device. Make certain you know what	
Flash operations:	Backup / Flash Firmware		
Powered by RedPort (Convright © Global Marine Networks, LLC 2015 - All Righ	ts Reserved)		

1. Keep Settings: remove the check in 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 for the gray button on top of the Optimizer to begin flashing. When the button stops flashing, the firmware is done updating. This typically takes several minutes.

To confirm the firmware upgrade, login to the Optimizer Home Page again. The firmware version displays in the top banner of the User Interface.



# 7.4. 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.

ome Services Status System Networ	rk Statistics Logout
asks	
elcome	
iFi Extender Setup	
Step 1	Connect Select external WIFi network to connect to. Requires an external antenna amplifier connected to LAN port.
Step 2	Enable WiFI Extender WiFI Extender Status: OFF Enable WiFI extender to route all network traffic through WiFI Extender. Make sure you have configured the WiFI Extender first (see Step 1).
Step 3 (Automatic)	<ul> <li>Disable Firewall</li> <li>Frewall Status: ON</li> <li>Disabling the firewall allows all traffic to/from the Internet through the router. This options should be used with caution and only when connected to land based WiFi.</li> </ul>
vstem Status	
rstem Status	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> </ul>
rstem Status	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> <li>Historic bandwidth usage over satellite link</li> <li>System message log</li> </ul>
rstem Status	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> <li>Historic bandwidth usage over satellite link</li> <li>System message log</li> </ul>
rstem Status	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> <li>Historic bandwidth usage over satellite link</li> <li>System message log</li> </ul>
rstem Status Dcal WiFi setup SSID and Security	System status overview Realtime bandwidth usage over satellite link Historic bandwidth usage over satellite link System message log WiFi setup Change hotspot name and/or add security and set password
rstem Status Docal WiFi setup SSID and Security rstem	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> <li>Historic bandwidth usage over satellite link</li> <li>System message log</li> <li>WiFi setup</li> <li>Change hotspot name and/or add security and set password</li> </ul>
rstem Status Docal WiFi setup SSID and Security rstem	System status overview Realtime bandwidth usage over satellite link Historic bandwidth usage over satellite link System message log WiFi setup Change hotspot name and/or add security and set password Router password
rstem Status Docal WiFi setup SSID and Security rstem	System status overview Realtime bandwidth usage over satellite link Historic bandwidth usage over satellite link System message log
rstem Status Docal WiFi setup SSID and Security rstem	System status overview  Realtime bandwidth usage over satellite link  Historic bandwidth usage over satellite link  System message log  WiFi setup  Change hotspot name and/or add security and set password  Redout router Reboot router

#### 2. Click <Reboot Router>.

Optimizer   w	vXa-203 v2.61   Load	: 1.00 1.02	1.03		Changes: 0					
Home	Services Status	System	Network Statistics	Logout						
System	Router Password	Profiles	Backup / Flash Firmware	Reboot						
System	n									
Reboot										
Reboots t	Reboots the operating system of your device									
Perform r	reboot									
Powered by	RedPort (Copyright ©	Global Ma	rine Networks, LLC 2015 - A	All Rights Reserv	ed)					

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. (See Chapter 3.0 Getting Started).

# 8. Network

## 8.1. Signal Monitor

Signal monitor queries your satellite device to determine if the signal strength is sufficient to make a successful data connection. Typically, a minimum of 60% signal is required; however, 100% is ideal for the fastest possible data transfer rate.

NOTE: Some of the older satellite phones (for example, the Iridium 9505a) do not support the signal monitor feature. For these older satellite phones, the signal monitor MUST be DISABLED for a successful data connection.

To modify the Signal Monitor, go to: Network > PPP > Settings.

Optimi	zer   wX	(a-203 v2	.61   Load	: 1.00 1.0	00 1.00					C	hanges: 0
F	lome	Services	Status	System	Network	Statistics	Logout				
I	nterface	s Wifi	DHCP a	nd DNS	Hostnames	Static Routes	Diagnostics	Firewall	PPP		-
5	itatus	Settings	Log						_		-
Р	PP and	d Mode	m Settiı	ngs							
Se	ttings w	hich cont	rol the dial	lun hehavi	ior of USB cor	nected satellite	nhones				
	eange n			ap senar			prioricoi				
	Networ	rk PPP	GSM	Signal M	lonitor						
	Enable						🔽 😰	Enable/Disat	ole signa	I monitoring during connections.	
	Level						60		0.014		
							UP AII	ow satellite d	r GSM C	onnections only it signal strength is larger than this value.	
	Reset									Save 🖾 Save &	Apply
Power	ed by R	edPort (C	opyright @	Global M	arine Networl	ks, LLC 2015 - A	II Rights Reser	ved)			

From this screen you can enable/disable signal monitor using the "Enable" checkbox.

You can change the level of the Signal Monitor. Keep in mind that 60% is typically the minimum required for a successful data connection. If you must change the Signal Monitor, we recommend lowering the Level vs. disabling it. Many IsatPhonePro users have had success by lowering the level to 40 or 30.

CAUTION: Reducing the signal strength to less than 60% or disabling it altogether may cause lengthy data connections due to poor signal.

When you are done making changes, click <Save & Apply>.

Signal monitor can also be changed from within the XGate Settings. See the XGate Help File > User Interface > Settings > Optimizer, wXa, & Sat-Fi for details.

## 8.2. GSM

The GSM feature is offered for your convenience but we are not able to support it. The information provided here is general in nature but may not be sufficient to establish a GSM connection. If you run into any difficulties you must contact your GSM network provider for support.

If you have a GSM-based cellular phone, it may be possible to use the GSM network, when available, for XGate and XWeb data over the Optimizer. You will get the benefits of compression and a faster data transfer rate than over a satellite phone which typically equates to cost savings.

Optimizer Advanced User Guide wXa-203

Only GSM-based service is supported. LTE-based and CDMA-based service is NOT supported. If you are unsure of which service you have, contact your cellular provider before attempting to configure for GSM connection.

#### 8.2.1. GSM Configuration in Optimizer

Before you can configure the Optimizer for GSM, you must:

- Obtain a USB data dongle from your cellular provider. Your provider may also require you to purchase a data plan.
- Activate the USB data dongle with your cellular carrier and test it to make sure it works. Typically, testing
  requires only that you plug the USB Data Dongle into your computer and see if you can get on the Internet. If
  testing fails, contact your cellular carrier for support.
- Contact your cellular provider to obtain the information required to connect to their GSM network. The information may include:

Access Point Name (APN). Username required for access to the APN. Password required for access to the APN.

To configure the Optimizer for GSM service.

Login to the Optimizer and go to: Network > PPP > Settings > GSM.

Optimizer   wXa-203 v2.61   Load: 1.04 1.01 1.00	Changes: 0
Home Services Status System Network Statistics Lo	agout
Interfaces Wifi DHCP and DNS Hostnames Static Routes Diag	anostics Firewall PPP
Status Settings Log	
PPP and Modem Settings	
Settings which control the dialup behavior of USB connected satellite phone	is.
Network PPP GSM Signal Monitor	
	APN Wizard     Select APN by Country, Provider, and Plan.
APN	Access Point Name.
APN Delay	7      Ormer moderns (such as the sierra wireless mc7455) require a delay (in seconds) between setting the APN and dialing.
Username	Blank Entry Ø Value set under PPP settings and displayed here for convenience.
Password	Blank Entry Ø Value set under PPP settings and displayed here for convenience.
Pincode	SIM card pin. Leave blank if none required.
(2) Reset	Save 🛽 Save & Apply
Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Righ	ts Reserved)

1. Enter the Access Point Name (APN) as provided to you by your cellular carrier.

2. If you have protected your cellular SIM card with a pincode, enter the pincode here.

3. Click <Save & Apply>.

NOTE: As of this writing, some customers have found the APN Wizard helpful in lieu of entering the information manually; however, it is still under development and may or may not help with your configuration.

Now go to: Network > PPP > Settings > PPP.

Home       Services       Status       Network       Status       Logut         Interfaces       MID       DHCP and DNS       Hostnames       Static Routes       Diagnostics       Firewall       PPP         Status       Settings       Log       Log       Diagnostics       Firewall       PPP         Status       Settings       Log       Diagnostics       Firewall       PPP         Status       Settings       Log       Diagnostics       Firewall       PPP         Status       Settings       Log       Diagnostics       Firewall       PPP         Status       Settings which control the dialup behavior of USB connected satellite phones.       Settings which control the dialup behavior of USB connected satellite phones.       Settings which control the dialup behavior of USB connected satellite phones.         Modem       Spinal Monitor       Interface       Status       Settings which control the dialup behavior of USB connected satellite phones.         Modem Speed       Spinal Monitor       Interface       Settings behavior of USB connection after spinal Monitor       Settings behavior of USB connection after spinal Monitor       Settings behavior of USB connection after spinal Monitor         Phone Number       Interface       Interface       Interface       Settings behavior of USB connected satelits interface.	Optin	nizer   v	vXa-203 v2.	61   Load:	1.04 1.0	L 1.00					Chang	ges: O
Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics Firewall PPP Status Settings Ing PPP and Modern Settings Settings which control the dialup behavior of USB connected satellite phones.  Wetwork PPP CSM Signal Monitor Modern Interface System Default :		Home	Services	Status	System	Network	Statistics	Logout				
Status       Settings         DPD and Modem Settings         Settings which control the dialup behavior of USB connected satellite phones.         Network       PPP         Modem Interface       © steen Default         © Setect COM port assigned to modem.         Modem Speed       © steen Default         © Bud rate for modem serial interface.         Username       © Leave blank if none required.         Phone Number       Phone number to dial. Leave blank if none required.         Phone Number       © Drop connection after X seconds if no network traffic is detected. Note it is not advisable to use this option with the persist option without the demand option. Set to 0 to diable.         Persist       © Enable persistent connections. Rerestent connections forces the modem to reconnect if connection drops.         Ktru Init       © Enable persistent connections. Rerestent connections forces the modem to reconnect if connection drops.         MTU       © Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.	P	Interfa	ces Wifi	DHCP an	d DNS	Hostnames	Static Routes	Diagnostics	Firewall	PP	PP	-
PPP and Modem Settings         Settings which control the dialup behavior of USB connected satellite phones.         Network       PPP         Modem Interface       System Default         Modem Speed       System Default         Password       Leave blank if none required.         Phone Number       Phone number to dial. Leave blank if none required.         Phone Number       Phone number to dial. Leave blank if for system default.         Idle Timeout       So for porconnection after X seconds if no network traffic is detected. Note it is not advisable to use this option with the persist option within the demand option. Set to 0 to disable.         Persist       Extra Init       Extra modem initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modem before dialing.         MTU       Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.	P	Status	Settings	Log	_					-		1
Settings which control the dialup behavior of USB connected satellite phones.         Network       PPP         Modem Interface       System Default         Modem Speed       System Default         Setect COM port assigned to modem.         Modem Speed       System Default         Vsername       Baud rate for modem serial interface.         Username       Leave blank if none required.         Password       Leave blank if none required.         Phone Number       Phone number to dial. Leave blank for system default.         Idle Timeout       So         Or por connection after X seconds if in network traffic is detected. Note it is not advisable to use this option with the persist option with the demand option. Set to 0 to disable.         Persist       Enable persistent connections. Persistent connections forces the modem to reconnect if connection drops.         Extra Init       Extra modem initialization. Leave blank if nor required. Enter full AT command (including AT) to send to the modem before ialing.         MTU       Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.	F	PPP a	nd Moder	n Settin	gs							
Network PP   GSM Signal Monitor   Modem Interface System Default   © Select COM port assigned to modem.   Modem Speed System Default   © Baud rate for modem serial Interface.   Username © Leave blank if none required.   Password © Leave blank if none required.   Phone Number © hone number to dial. Leave blank for system default.   Ide Timeout Some connection after X seconds if no network traffic is detected. Note it is not advisable to use this option with the persist option without the demand option. Set to 0 to disable.   Persist © Enable persistent connections. Persistent connections forces the modem to reconnect if connection drops.   Extra Init © Extra modem initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modem before alion.   MTU © Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.	S	Settings	which contr	ol the dialu	p behavio	or of USB co	nnected satellite	e phones.				
Modem Interface       System Default       •         Wodem Speed       System Default       •         Username       •       •         Password       •       •         Phone Number       •       •         Ide Timeout       •       •         Option       •       •         Persist       •       •         Extra Init       •       •         •       •       •         MTU       •       •		Netw	ork PPP	GSM	Signal Mo	onitor						
Modern Speed       System Default       •         Wearname       •       Baud rate for modern serial interface.         Vasername       •       Leave blank if none required.         Password       •       Leave blank if none required.         Phone Number       •       Phone number to dial. Leave blank for system default.         Idle Timeout       •       •         Persist       •       Phone persist option without the demand option. Set to 0 to disable.         Persist       •       •         Extra Init       •       Extra modern initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modern before dialing.         MTU       •       Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.		Mode	em Interface					Sys	tem Default elect COM po	rt assi	\$jsigned to modem.	
Username       Isave blank if none required.         Password       Isave blank if none required.         Phone Number       Phone number to dial. Leave blank for system default.         Idle Timeout       Iso prop connection after X seconds if no network traffic is detected. Note it is not advisable to use this option with the persist option without the demand option. Set to 0 to disable.         Persist       Image: Design after X seconds if no required. The demand option option option option with the demand option. Set to 0 to disable.         Extra Init       Extra Init         Image: Design after X seconds if no required. Enter full AT command (including AT) to send to the modern before dialing.         MTU       Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.		Mode	em Speed					Sys	tem Default aud rate for r	noden	em serial interface.	
Password       Image: Leave blank if none required.         Phone Number       Image: Phone number to dial. Leave blank for system default.         Idle Timeout       Image: Phone number to dial. Leave blank for system default.         Persist       Image: Persist connection after X seconds if no network traffic is detected. Note it is not advisable to use this option with the persist option without the demand option. Set to 0 to disable.         Persist       Image: Persist connections. Persistent connections forces the modern to reconnect if connection drops.         Extra Init       Image: Extra modern initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modern before dialing.         MTU       Image: Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.		User	name					[ 2 L	eave blank if	none	e required.	
Phone Number       Image: Phone number to dial. Leave blank for system default.         Idle Timeout       Image: Prop connection after X seconds if no network traffic is detected. Note it is not advisable to use this option with the persist option without the demand option. Set to 0 to disable.         Persist       Image: Persist option without the demand option. Set to 0 to disable.         Persist       Image: Persist option without the demand option. Set to 0 to disable.         Persist       Image: Persist option without the demand option. Set to 0 to disable.         Persist       Image: Persist option without the demand option. Set to 0 to disable.         Persist       Image: Persist option without the demand option. Set to 0 to disable.         Persist       Image: Persist option without the demand option. Set to 0 to disable.         Persist       Image: Persist option without the demand option. Set to 0 to disable.         Persist option without the demand option. Set to 0 to disable.       Image: Persist option without the demand option.         Image: Persist option without the demand option. Set to 0 to disable.       Image: Persist option without the demand option.         Image: Persist option without the demand option. Set to 0 to disable.       Image: Persist option without the demand option.         Image: Persist option without the demand option.       Image: Persist option without the demand option.         Image: Persist option without the demand option.       Image: Persist option.      <		Pass	word					() ()	eave blank if	none	e required.	
Idie Timeout       E0         I die Timeout       Image: Comp connection after X seconds if no network traffic is detected. Note it is not advisable to use this option with the persist option without the demand option. Set to 0 to disable.         Persist       Image: Comp connection after X seconds if no network traffic is detected. Note it is not advisable to use this option with the persist option without the demand option. Set to 0 to disable.         Persist       Image: Comp connection after X seconds if no network traffic is detected. Note it is not advisable to use this option with the persist option without the demand option. Set to 0 to disable.         Extra Init       Image: Comp connection after X seconds if not required. Enter full AT command (including AT) to send to the modern before dialing.         MTU       Image: Comp connection after X seconds if not required. Leave blank for system default.		Phon	e Number					2 P	hone number	to dia	lial. Leave blank for system default.	
Persist <ul> <li>Persistent connections. Persistent connections forces the modern to reconnect if connection drops.</li> <li>Extra Init</li> <li>Extra Init</li> <li>Extra modern initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modern before dialing.</li> </ul> MTU     Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.		Idle '	Timeout					60 2 Dependie	rop connection with	on afte	ter X seconds if no network traffic is detected. Note it is not advisable to use this option with the the demand option. Set to 0 to disable.	
Extra Init  Extra Init		Persi	st						Enable pers	istent	nt connections. Persistent connections forces the modem to reconnect if connection drops.	
MTU		Extra	ı Init					E	xtra modem i re dialing.	nitiali:	lization. Leave blank if not required. Enter full AT command (including AT) to send to the modem	
		MTU						2 S	et the MTU [I	Maxim	mum Transmit Unit] value in bytes. Leave blank for system default.	
debug 🗌 🚱 Write PPP connection debugging information to the system log.		debu	g						Write PPP c	onnec	ection debugging information to the system log.	
🕲 Reset		🗵 Reset									Save 🛽 🖾 Save & App	ly

- 4. Enter the username required for access to the APN, if any.
- 5. Enter the password required for access to the APN, if any.
- 6. Click <Save & Apply>

#### 8.2.2. Using GSM

When you want to use GSM service instead of satellite service:

Plug the USB data dongle you obtained from your cellular provider into the Optimizer's USB port.

NOTE: If your satellite terminal is connected to the Optimizer's SAT port, unplug the cable from the SAT port before attempting a GSM connection.

Configure XGate Settings for GSM connection. Open XGate to Settings > Connection

	S	ettings				
Gateway	Profile					
Connection E-Mail Settings	Active Profile:	Default				Delete
Miscellaneous	Save Profile					Save
Mail Filtering	ISP Account Information					
Social Media XWeb	User					
Iridium AxcessPoint WiFi	Pass	word:			_	
Optimizer, wXa, & Sat-Fi	Dial Ove	erride:				efault
	IP Dialer Connection Para	imeters				
	Device Pas	ssword:				
	IP Host-Port O	verride: 192	168 10 1.5/	154	_	Default
		192		+0-+		
	Connection Information					
	Default	Net	work Conne	ection		۵
		Type Op	timizer GSM	I		٥
	Connection Parameters					
	Leave network co	nnection acti	ve when do	ne		
	Use another conr	ection if alread	ady open			
	Persist with conn	ections until t	transfer con	npletes or n	um time:	S
	Number of times	to attempt		1		
	Seconds to wait	t hetween		185		
	Coondo to Hai	C DOCHOON		100		
					Cancel	ОК
				_		

Click the Connection Type <Optimizer GSM>. Click <OK> to apply the change.

#### 8.2.3. Changing from GSM service to satellite service

When you travel beyond GSM range you must:

- Remove the GSM data dongle from the Optimizer's USB port.
- Connect your satellite phone/terminal to the Optimizer (either via USB port or SAT port).
- Change the XGate > Settings > Connection Type back to the appropriate Optimizer setting.

NOTE: There is no need to change anything in the Optimizer user interface.

IMPORTANT: We are not able to support the GSM feature. If you experience any connection difficulties when using this feature, you must contact your GSM network provider for support.

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

When in public locations, for example, a crowded marina or anchorage, you may want to restrict access to your Wi-Fi hotspot created by your satellite device and the Optimizer. You can password protect your Wi-Fi hotspot so others cannot use it.

Add/change a password to the Wi-Fi Hotspot (wXa-203-xxxx).

1. Login to the Optimizer:

ter   wxa-203 v2.61   Load: 1.08 1.02 1.01	Char
ome Services Status System Networ	rk Statistics Logout
asks	
elcome	
'iFi Extender Setup	
Step 1	Connect
	Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
Step 2	Enable WiFi Extender
	WiFi Extender Status: OFF Fable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi
	Extender first (see Step 1).
Step 3 (Automatic)	Sisable Firewall
	Firewall Status: ON Disability the frequent allows all traffic to from the Internet through the router. This options should be used with caution
	and only when connected to land based WiFi.
etom Status	
	Suctom status nuerview
	Dealtime handwidth usane over satellite link
	Historic handwidth usage over satellite link
	System message log
	System message log
ocal WiFi setup	System message log
ocal WiFi setup SSID and Security	WiFi setup Change betred part and (an old acquisity and at partures)
ocal WiFi setup SSID and Security	System message log  WiFi setup  Change hotspot name and/or add security and set password
ocal WiFi setup SSID and Security /stem	<ul> <li>System message log</li> <li>WiFi setup</li> <li>Change hotspot name and/or add security and set password</li> </ul>
ocal WiFi setup SSID and Security /stem	System message log  WiFi setup  Change hotspot name and/or add security and set password  Ruiter nassword
ocal WiFi setup SSID and Security ystem	System message log  WiFi setup  Change hotspot name and/or add security and set password  Router password
ocal WiFi setup SSID and Security /stem	System message log  WiFi setup  Change hotspot name and/or add security and set password  Router password  Router password  Rebot router
ocal WiFi setup SSID and Security /stem	System message log  WiFi setup  Change hotspot name and/or add security and set password  Router password  Router password  Rebot router

2. Click <Wi-Fi Setup> and go to: Interface Configuration > Wireless Security.

ptimizer   wXa-203 v2.61   Load: 1.38 1.24 1.11   Auto Refresh: on	Changes
Home Services Status System Network Statistics Log	jout
Interfaces Wifi DHCP and DNS Hostnames Static Routes Diag	nostics Firewall PPP
radio0: Master "wXa-203-80f8"	
Wireless Network: Master "wXa-203-80f8" (wlan0)	
The Device Configuration section covers physical settings of the radio hardw the radio hardware is multi-SSID capable). Per network settings like encrypt	are such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if ion or operation mode are grouped in the <i>Interface Configuration</i> .
Device Configuration	
General Setup Advanced Settings	
Status	Mode:         Master   SSID:         wXa-203-80f8           BSSID:         00:0A:52:05:80:FA   Encryption:         None           Channel:         11 (2.462 GHz)   Tx-Power: 20 dBm           S1%         Signal:         74 dBm   Noise:           Bitrate:         65.0 Mbit/s   Country:         00
Wireless network is enabled	( Disable
Operating frequency	Mode         Channel         Width           N         +)         (11 (2462 MHz) +)         20 MHz +)
Transmit Power	(20 dBm (100 mW) €
Interface Configuration	
General Setup Wireless Security MAC-Filter	
Encryption	No Encryption
Back to Overview Beset	Save 🗈 Save & Apply
Powered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Right	s Reserved)

- 3. Click the Encryption mode from the drop down menu. We suggest WPAPSK/WPA2-PSK Mixed Mode.
- 4. Enter your desired password in the Key field.

#### 5. Click <Save & Apply>

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.

## 8.4. 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-203-xxxx where the xxxx represents a unique number. There is no default password to connect to the network.

me Services Status System Netwo	ork Statistics Locaut
status System Netw	
583	
lcome	
Fi Extender Setup	
itep 1	Connect
	Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.
tep 2	Enable WiFi Extender
	Enable WiFi Extender to route all network traffic through WiFi Extender. Make sure you have configured the WiFi
	Extender first (see Step 1).
Step 3 (Automatic)	( Disable Firewall
	Firewall Status: ON Disabling the firewall allows all traffic to/from the Internet through the router. This options should be used with caution
	and only when connected to land based WiFi.
stem Status	
	System status overview
	System status overview  Realtime bandwidth usage over satellite link
	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> <li>Historic bandwidth usage over satellite link</li> </ul>
	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> <li>Historic bandwidth usage over satellite link</li> <li>System message log</li> </ul>
	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> <li>Historic bandwidth usage over satellite link</li> <li>System message log</li> </ul>
cal WiFi setup	<ul> <li>System status overview</li> <li>Realtime bandwidth usage over satellite link</li> <li>Historic bandwidth usage over satellite link</li> <li>System message log</li> </ul>
cal WiFi setup SSID and Security	System status overview  Realtime bandwidth usage over satellite link  System message log  WiFi setup
cal WiFi setup SID and Security	System status overview  Realtime bandwidth usage over satellite link  System message log  WiFi setup  Change hotspot name and/or add security and set password
cal WiFi setup SSID and Security	System status overview  Realtime bandwidth usage over satellite link  System message log  WiFi setup  Change hotspot name and/or add security and set password
cal WiFi setup SSID and Security stem	System status overview  Realtime bandwidth usage over satellite link  System message log  WiFi setup  Change hotspot name and/or add security and set password
cal WiFi setup SSID and Security Stem	System status overview  Realtime bandwidth usage over satellite link  System message log  System message
cal WiFi setup SSID and Security stem	System status overview  Realtime bandwidth usage over satellite link  System message log  System message
cal WiFi setup ISID and Security	System status overview  Realtime bandwidth usage over satellite link  System message log  System message log  System message log  System message log  Realtime band/or add security and set password

Click <Wi-Fi Setup> and go to: Interface Configuration > General Setup.

tome Services Status System Network Statistics Logout   Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics Firew adio0: Master "wXa-203-80f8" (wlan0) e Device Configuration section covers physical settings of the radio hardware such as chare e radio hardware is multi-SSID capable). Per network settings like encryption or operation Device Configuration General Setup Advanced Settings Status Wireless network is enabled Operating frequency Interface Configuration General Setup Wireless Security Mode: Interface Configuration General Setup Wireless Security MAC-Filter ESSID Wireless Security Mode Access Point Node Node Interface Configuration General Setup Wireless Security Mode Mode Interface Configuration General Setup Wireless Security MAC-Filter ESSID Wireless Security Mode Interface Configuration General Setup Wireless Security Mode Mode Interface Configuration General Setup Wireless Security Mode Mode Mode Interface Configuration General Setup Wireless Security Mode Mode Mode Interface Configuration General Setup Wireless Security Mode Mode Mode Interface Configuration General Setup Wireless Security Mode Mode Interface Configuration General Setup Wireless Security Mode Mode Mode Interface Configuration General Setup Wireless Security Mode Mode Interface Configuration General Setup Interface Configuration General S	I       PPP         hel, transmit power or antenna selection which are shared among all defined wireless networks (if node are grouped in the Interface Configuration.         aster   SSID: wXa-203-80f8         00:0A:52:05:80:FA   Encryption: None         11 (2.462 Gitz)   Tx-Power: 20 dBm         76 dBm   Noise: 0 dBm         30. Mbi/c1   Country: 00
Interfaces       Wifi       DHCP and DNS       Hastnames       Static Routes       Diagnostics       Firewisadio0:         adio0:       Master "wXa-203-80f8"       Image: Static Routes       Diagnostics       Firewisadio0:         adio0:       Master "wXa-203-80f8"       Image: Static Routes       Diagnostics       Firewisadio0:         adio0:       Master 'swXa-203-80f8"       Image: Static Routes       Image: S	I       PPP         nel, transmit power or antenna selection which are shared among all defined wireless networks (if node are grouped in the Interface Configuration.         aster   SSID: wXa-203-80f8         00:00:52:05:80:FA   Encryption: None         11 (2.462 Gitz)   Tx-Power: 20 dBm         76 dBm   Noise: 0 dBm         30. Mbi/s1 [Country: 00
adio0: Master "wXa-203-8078"  ireless Network: Master "wXa-203-8078"  e Device Configuration section covers physical settings of the radio hardware such as char e radio hardware is multi-SSID capable). Per network settings like encryption or operation Device Configuration General Setup Advanced Settings  Wireless network is enabled  Operating frequency  Interface Configuration General Setup Wireless Security MAC-Filter  SSID Mode Access Point Network  Interface Configuration  General Setup Wireless Security MAC-Filter  SSSID  wXa-203-8076 Mode Access Point Network  Ide ESSID  Hide ESSID	nel, transmit power or antenna selection which are shared among all defined wireless networks (if mode are grouped in the <i>Interface Configuration</i> . aster   <b>SSID:</b> wXa-203-80f8 0:00:52:05:80:FA   <b>Encryption:</b> None 1:1 (2.462 GHz)   <b>Tx-Power</b> : 20 dBm 76 dBm   <b>Noise:</b> 0 dBm 30. OMbi/5. <b>Country:</b> 00
Treless Network: Master "wXa-203-80f8" (wlan0)         e Device Configuration section covers physical settings of the radio hardware such as char e radio hardware is multi-SSID capable). Per network settings like encryption or operation         Device Configuration         General Setup       Advanced Settings         Status       Mode: 1         Wireless network is enabled       Image: 1         Operating frequency       Mode: 1         Transmit Power       20 dBm (100 m image: dBm         General Setup       Wireless Security         Mode       Access Point         Node       Access Point         Network       Image: 1         Network       Image: 1         Wireless Security       MAC-Filter         ESSID       Wixa-203-80f8         Mode       Access Point         Network       Image: 1         Network       Image: 1         Interface Configuration       Image: 1         Mode       Access Point         Network       Image: 1         Image: 2       Image: 2         Image: 2 <td< td=""><td>hel, transmit power or antenna selection which are shared among all defined wireless networks (if mode are grouped in the Interface Configuration. aster   SSID: wXa-203-80f8 00:0A:52:05:80:FA   Encryption: None 11 (2.462 GHz)   Tx-Power: 20 dBm 76 dBm   Noise: 0 dBm 30.0 Mbi/s. I Country: 00</td></td<>	hel, transmit power or antenna selection which are shared among all defined wireless networks (if mode are grouped in the Interface Configuration. aster   SSID: wXa-203-80f8 00:0A:52:05:80:FA   Encryption: None 11 (2.462 GHz)   Tx-Power: 20 dBm 76 dBm   Noise: 0 dBm 30.0 Mbi/s. I Country: 00
e Device Configuration section covers physical settings of the radio hardware such as char e radio hardware is multi-SSID capable). Per network settings like encryption or operation Device Configuration General Setup Advanced Settings Status Mode: [	el, transmit power or antenna selection which are shared among all defined wireless networks (if node are grouped in the Interface Configuration. aster   SSID: wXa-203-80f8 00:0A:52:05:80:FA   Encryption: None 11 (2.462 GHz)   Tx-Power: 20 dBm 76 dBm   Noise: 0 dBm 30. Mbi/s. I Country: 00
Device Configuration         General Setup       Advanced Settings         Status       Image: Status         Wireless network is enabled       Image: Status         Operating frequency       Image: Status         Transmit Power       20 dBm (100 m Image: dBm         General Setup       Image: Status         Interface Configuration       Image: Status         General Setup       Image: Status         Mode       Access Point         Node       Access Point         Network       Image:	aster   <b>SSID:</b> wXa-203-80f8 00:0A:52:05:80:FA   <b>Encryption:</b> None <b>:</b> 11 (2.462 GHz)   <b>Tx-Power:</b> 20 dBm 76 dBm   <b>Noise:</b> 0 dBm 30. Oblifs. <b>I Country:</b> 00
General Setup       Advanced Settings         Status       Mode: 1         Wireless network is enabled       @ Disable         Operating frequency       Mode: 1         Transmit Power       20 dBm (100 m or dBm)         General Setup       Wireless Security         Interface Configuration       Mode: 20 dBm dBm         General Setup       Wireless Security         Mode       Access Point         Network       @ Ian: ***         Ppp: ?       war: **         Ward6: ?       create: [         @ Choose the r       network.         Hide ESSID	aster   <b>SSID:</b> wXa-203-80f8 00:0A:52:05:80:FA   <b>Encryption:</b> None <b>:</b> 11 (2.462 GHz)   <b>Tx-Power:</b> 20 dBm 76 dBm   <b>Noise:</b> 0 dBm 30. Oblifs. <b>I Country:</b> 00
Status       Mode: 1         Wireless network is enabled       Image: 1         Operating frequency       Mode: 1         Transmit Power       20 dBm (100 m of dBm)         General Setup       Wireless Security         Mode       Access Point         Network       Image: 1         Network       Image: 1         Interface Configuration       Image: 1         General Setup       Wireless Security         Mode       Access Point         Network       Image: 1         Image: 1       Image: 1         Network       Image: 1         Image: 1       Image: 1         Image: 1       Image: 1         Image: 1       Image: 1         Image: 2       Image: 2         Image: 2       Image: 2 <tr< td=""><td>aster   <b>SSID:</b> wXa-203-80f8 J0:0A:52:05:80:FA   <b>Encryption:</b> None <b>:</b> 11 (2.462 GHz)   <b>Tx-Power:</b> 20 dBm 76 dBm   <b>Noise:</b> 0 dBm 30. Mbi/tS. <b>I Country:</b> 00</td></tr<>	aster   <b>SSID:</b> wXa-203-80f8 J0:0A:52:05:80:FA   <b>Encryption:</b> None <b>:</b> 11 (2.462 GHz)   <b>Tx-Power:</b> 20 dBm 76 dBm   <b>Noise:</b> 0 dBm 30. Mbi/tS. <b>I Country:</b> 00
Wireless network is enabled       Mode Cha         Operating frequency       N ± 11         Transmit Power       20 dBm (100 m         Interface Configuration       Image: Character of the second seco	
Operating frequency       Mode Cha         Transmit Power       20 dBm (100 m         @ dBm       Interface Configuration         General Setup       Wireless Security         Mode       Access Point         Mode       Access Point         Network       Ian: :: Image Security         Wan: :: Image Security       Wac-Filter         ESSID       WXa-203-B0/8         Mode       Access Point         Network       Ian: :: Image Security         Wan: :: Image Security       Wan: :: Image Security         Wan: :: Image Security       Wan: :: Image Security         Image Security       Image Security         Network       Image Security         Image Security       Image Security </td <td></td>	
Transmit Power	nel Width 462 MHz) \$) 20 MHz \$
Interface Configuration General Setup Wireless Security MAC-Fliter ESSID Mode Access Point Network I an:   ppp:   wan:   create:  create:  Concose the r network. Hide ESSID	n ÷
Interface Configuration General Setup Wireless Security MAC-Fliter ESSID WXa-203-B0f8 Mode Access Point Network I an:   ppp: 2 Wan:   wan:   create: C	
General Setup       Witeless Security       MAC-Hitter         ESSID       WXa-203-80/8         Mode       Access Point         Network       Image:	
Mode Access Point Network I Ian:  Ppp: 2 Wan:  Wan:  Wan:  Wan:  Wan:  Wan:  Create:  Create:	
Network	÷
<ul> <li>✓ Iah: ഈ</li> <li>ppp: </li> <li>wan: </li> <li>wan6: </li> <li>create: </li> <li>@ Choose the r</li> <li>network.</li> </ul>	
□ ppp: 2 □ wan: 2 □ create: [ @ Choose the r network. Hide ESSID	
wan: ***         wan6: **         create: [         @ Choose the r         network.	
Warts: 22     create: [     @ Choose the r     network.  Hide ESSID	
Genetic [     Genetic [     Genetic [     network.	
Hide ESSID	
	etwork(s) you want to attach to this wireless interface or fill out the create field to define a new
WMM Mode	etwork(s) you want to attach to this wireless interface or fill out the create field to define a new
	etwork(s) you want to attach to this wireless interface or fill out the <i>create</i> field to define a new
Back to Overview 🔯 Reset	etwork(s) you want to attach to this wireless interface or fill out the <i>create</i> field to define a new

1. Enter the new wireless network name in ESSID field.

#### 2. 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.

## 8.5. Firewall

Requires "superadmin" login.

The Firewall allows you to control network traffic flow, allow port forwarding for remote access, has a table of pre-defined traffic rules, and allows you to edit existing rules and create new rules. Most installations do not require any firewall.

CAUTION: It is important to have an in-depth understanding of network administration including managment and maintenance of routers, firewalls, etc. before attempting to modify the firewall settings of the Optimizer. USE WITH CAUTION AND AT YOUR OWN RISK!

#### 8.5.1. General Settings

Use this screen to create and edit Firewall zones. Each Firewall Zone can have its own firewall rules. Each Interface must be assigned a Firewall Zone.

mizer   wXa-203 v2.61   Load: 1.68 1.09 0.45					Change
Home Services Status System Network S	tatistics Logout				
Interfaces Wifi DHCP and DNS Hostnames Sta	atic Routes Diagnostics	Firewall PPP			
General Settings Port Forwards Firewall Rules	IPset IP Proxy				
Firewall - Zone Settings					
The firewall creates zones over your network interfaces to	control network traffic flow.				
General Settings					
Enable SYN-flood protection					
Drop invalid packets					
Input	reject		\$		
Output	accept		\$		
Forward	reject		\$		
Zones					
Zone ⇒ Forwardings	Input Outp	ut Forward	Masquerading	MSS clamping	
ppp: ppp: → REJECT	reject \$ accept	¢ reject			ZEdit Delete
<b>cap:</b> (empty) → ACCEPT	accept \$ accept	¢ accept ¢			Edit Delete
lan: lan: ﷺ ∰ ⇒ ppp wan	(reject \$) accept	(reject )			Edit Delete
wan: wan: 🕎 → REJECT	accept \$ accept	¢) reject \$			Edit Delete
Add					
8 Reset					Save Save Apply
vered by RedPort (Convright @ Global Marine Networks	IC 2015 - All Pights Records	d)			Course Course a Apply

It is important to understand the following before considering modifications:

Input: this is accessing the router itself.

Output: this is the router accessing the "lan". DO NOT MODIFY.

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

Accept: this setting allows traffic unless there is a Rule to block it.

Reject: this setting blocks traffic unless there is a Rule to allow it. An error is displayed to the end user.

Drop: this setting drops the traffic with no indication to the end user.

The router is shipped to you with several Firewall Zones configured and interfaces assigned to them:

ppp: ppp:		Edit Edit
-----------	--	-----------

The "ppp" firewall zone has only the ppp interface assigned to it. This is the zone for dialup connections. In this default configuration, only Output traffic is allowed. Input and Forwarded traffic is rejected.

	cap: (empty)	⇒	ACCEPT	accept	\$	accept	\$	accept	ŧ)			ZEdit Delete
--	--------------	---	--------	--------	----	--------	----	--------	----	--	--	--------------

The "cap" firewall zone is reserved for Optimizer routers that have Captive Portal available. Captive Portal is not available on the Optimizer or Optimizer Voice. If Captive Portal to restrict Crew Internet Access is required please see your service provider about the Optimizer Premier.

lan: ﷺ ∰ → ppp wan reject + accept + reject +	Edit 🙁 Delete
---	---------------

The "lan" firewall zone has the lan interface assigned to it. This is the zone for the internal local network. In this default configuration, only Output traffic is allowed.

wan: wan: ﷺ ⇒ REJECT accept \$ (reject \$ 200 Control of the second secon
---

The "wan" firewall zone has the wan interface assigned to it. This is the zone for satellite connections and Wi-Fi extenders. In this default configuration, only Output traffic is allowed.

# 8.5.2. Add a Firewall Zone

To create a new Firewall Zone, select the <Add> icon on the General Settings page.

ome Servi	ces Status Sy	Network	Statistics	Logout		_				
terfaces \	Vifi DHCP and DI	NS Hostnames	Static Routes	Diagnostics	Firewal	PPP	_			
eneral Setti	ngs Port Forward	ds Firewall Rule	s IPset IP Pro	ху			_			
ewall - Z	one Settings									
firewall crea	ates zones over voi	ir network interfac	es to control netw	ork traffic fl	0144					
General Se	ttinas									
Enable SVN-	flood protection									
Dron invalid	nackets									
Input	puekees				ct		•			
Outout										
ουιρυί				acc	ерт		Ţ			
Forward				reje	ct		÷			
lones										
	Zone ⇒ Forwa	ardings	Input	0	utput	Forward		Masquerading	MSS clamping	
	ppp: ppp: 🗾 =	→ REJECT	reject	acce	ot 🗘	reject	•			Edit Delete
	cap: (empty)	ACCEPT	accept	¢ acce	ot 🗘	accept	•			ZEdit Delete
la	an: lan: 🕎 👳 ⇒	ppp wan	reject	¢) (acce	ot 🗘	reject	•			Edit Delete
	wan: wan: 🕎	→ REJECT	accept	¢ acce	ot \$	reject	•			Edit Delete
Add										
Reset										Save 🛛 Save & Ap

	lan: lan: 💯 💇 ⇒ ppp wan	reject 🗘 accept	reject		ZEdit Delete
	wan: wan: 💯 ⇒ REJECT	accept \$ accept	¢ reject		Edit Delete
Add					
L					
🖾 Reset					Save 🛄 Save & Apply

rfaces Wifi DHCP and DNS Hostnames Static	Routes Diagnostics Firewall PPP
eral Settings Port Forwards Firewall Rules IPse	at IP Proxy
wall - Zone Settings - Zone "newzone"	
ne "newzone"	
varded traffic between different networks within the zone.	for and output options set the default policies for trainic entering and leaving this zone while the <i>forward</i> option describes the policy of Covered networks specifies which available networks are members of this zone.
eneral Settings Advanced Settings	
ime	newzone
put	reject 🗘
Itput	(accept +
rward	
asquerading	, 
SS clamping	<u>_</u>
vered networks	
	🗌 wan: 💯
	🗌 wan6: 🚈
	create:
ter-Zone Forwarding options below control the forwarding policies between this varded traffic from other zones targeted at "newzone".	3 zone (newzone) and other zones. Destination zones cover forwarded traffic originating from "newzone". Source zones match The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.
ow forward to destination zones:	cap: (empty)
	🗌 lan: 📰 🙊
	ppp: ppp:
	🗆 wan: 🕎
ow forward from source zones:	cap: (empty)
	🗌 lan: 📰 👷
	ppp: ppp: D
	wan: wan:

Enter the desired General and Advanced Settings. Click <Save & Apply>.

#### 8.5.3. Port Forwards

To allow remote access to a specific computer or service within the private LAN requires Port forwarding.

CAUTION: It is important to understand networking before making changes to Port Forwards.

Optimiz	zer   wXa-203 v2	2.61   Load: 1.00 1.00 0.93	Changes: 0
н	lome Services	Status System Network Statistics Logout	
I	nterfaces Wifi	DHCP and DNS Hostnames Static Routes Diagnostics Firewall PPP	
G	Seneral Settings	Port Forwards Firewall Rules IPset IP Proxy	
Fi	rewall - Port	t Forwards	
Por	rt forwarding allo	ows remote computers on the Internet to connect to a specific computer or service within the private LAN.	
r-1	Port Forwards	S	
	Name	Match Fo	rward to Enable Sort
		This section contains no values yet	
		New port forward:	
	Name	Protocol External zone External port Internal zone Internal IP address Internal port	
	New port forward	d TCP+UDP 🗘 Cap 🛊 Cap 🛊 计	Add
0	Reset		Save 🔝 Save & Apply
Power	ed by RedPort (C	Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)	

This page shows a list of the enabled port forwards configured. To add a new port forward, enter the desired parameters and click <Add>. To save the configuration, click <Save & Apply>. The new port forward will appear in the list.

#### 8.5.4. Firewall Rules

This page is the firewall traffic rules table. The table includes all the firewall rules on the router. If you are using the Optimizer with XGate (or other RedPort certified email service) for email and web compression there is no need to modify this page.

If you have a specific need, you can Add, Edit and Delete firewall rules.

zer   wXa-203 v2.61   Load: 1	1.00 1.00 0.97		Chan
ome Services Status	System Network Statistics Logout		
nterfaces Wifi DHCP and	DNS Hostnames Static Routes Diagnostics Firewall P	PP	
eneral Settings Port Forwar	rds Firewall Rules IPset IP Proxy		
rewall - Traffic Rules			
remain marine naies			
iffic rules define policies for pa	ackets traveling between different zones, for example to reject traff	ic between certain hosts or to open WAN ports on the	e router.
Traffic Rules			
Name	Match	Action	Enable Sort
BLOCK WAN DO_NOT_MODIFY	Any traffic From any host in wan To any router IP on this device	Discard input	C C Edit X Delete
ALL DO_NOT_MODIFY	Any traffic From <i>any host</i> in <i>any zone</i> To <i>any host</i> in <i>any zone</i>	Accept forward	C C Edit Edit Delete
PASS DNS DO_NOT_MODIFY	Any UDP From any host in any zone To any host, port 53 in any zone	Accept forward	Edit KDelete
DNS DO_NOT_MODIFY	Any UDP From any host in any zone To any router IP at port 53 on this device	Accept input	Edit Edit Edit
HTTP DO_NOT_MODIFY	Any TCP From any host in any zone To any host, port 80 in any zone	Accept forward	C C Edit K Delete
HTTPS DO_NOT_MODIFY	Any ICF From any host in any zone To any host, port 443 in any zone	Accept forward	Edit Edit Delete
FTP DO_NOT_MODIFY	From any host in any zone To any host, ports 20-21 in any zone	Accept forward	Edit KDelete
Open ports on router:			
Name	Protocol External port		
New input rule TCP	P+UDP €		
New forward rule:			
Name S	Source zone Destination zone		
New forward rule	<ul> <li>♦ (wan</li> <li>♦ Madd and edit</li> </ul>		
Source NAT			
ource NAT is a specific form of	masquerading which allows fine grained control over the source IP use	ed for outgoing traffic, for example to map multiple WAN	addresses to internal subnets.
Name	Match		Action Enable Sort
	This section contains a	no values yet	
New source NAT:			
Name Source	e zone Destination zone To source IP To source port		
New SNAT rule	<ul> <li>(wan</li> <li>( Please choos(</li> <li>Do not rewrite</li> </ul>	Add and edit	
Reset			Cave Dave 9 Ann
			Save Save & App

By default, the router is shipped to you with seven rules that all say DO NOT MODIFY. They are: BLOCK WAN, ALL, PASS DNS, DNS, HTTP, HTTPS and FTP.

The BLOCK WAN rule is designed to prevent you from locking yourself out of the router as you perform your initial configuration.

The remaining rules, when Enabled, Allow that particular traffic to pass through the firewall. All the firewall rules can easily be enabled (checked) or disabled (unchecked).

The rule name "ALL", when enabled, means the firewall is totally open and all traffic goes straight through the firewall. To disable the rule, uncheck it, scroll to the bottom of the page and click <Save & Apply>. With the ALL rule disabled, the remaining rules spring into action, if enabled.

Rules are evaluated from top to bottom. As soon as traffic hits a rule that matches, it will stop.

For example, if you want to allow all traffic except http traffic:

- Disable (uncheck) the first rule "ALL-DO NOT MODIFY". This forces the remaining "enabled" rules to take precedent.
- Disable (uncheck) the rule "HTTP-DO NOT MODIFY". This blocks http traffic from passing through the firewall.

With the ALL rule disabled (unchecked) you can enable/disable the others very quickly. The next one is DNS. Do you want DNS? Yes (checked), No (unchecked). Do you want http? Yes (checked), No (unchecked), etc. You can also create a custom rule.

neral Settings Port F	orwards Firewall Rules	IPset IP P	roxy					
	1							
ewall - Traffic Ri	lies							
fic rules define policies	for packets traveling betwee	en different zon	es, for example to reject t	raffic between certain hosts o	r to open WAN ports on the r	outer.		
raffic Rules								
Name			Match		Action	Enable	Sort	
BLOCK WAN		A From a	ny traffic		Discard input		•	Edit X Delete
O_NOT_MODIFY		To any rout	er IP on this device		biscure input			
ALL		A From any	ny traffic host in any zone		Accept forward		•	Edit Delete
O_NOT_MODIFY		To any I	ost in any zone			_		
PASS DNS		From any	Any UDP host in any zone		Accept forward		•	ZEdit Delete
0_101_100111		To any host,	port 53 in any zone					
DNS 0 NOT MODIFY		From any	host in any zone		Accept input		•	ZEdit Nolete
		To any router IP	at port 53 on this device Anv TCP					
HTTP O_NOT_MODIFY		From any	host in any zone		Accept forward		•	ZEdit Nolete
UTTRE		To any host,	Any TCP					
0_NOT_MODIFY		From any To any host.	host in any zone port 443 in any zone		Accept forward		<b>1</b>	ZEdit Nolete
FTP		10 0117 11000,	Any TCP			-		
O_NOT_MODIFY		From any To any host, p	host in any zone orts 20-21 in any zone		Accept forward			ZEdit Edit
Open ports on router:	Protocol Exte	rnal port						
New input rule			Add					
ivew input rule			Add					
New forward rule:								
Name	Source zone Destin	ation zone						
New forward rule	lan 🗘 wan	\$	Add and edit					
ource NAT is a specific fo	rm of masquerading which al	llows fine graine	d control over the source IP	used for outgoing traffic, for ex	ample to map multiple WAN a	ddresses to	interna	l subnets.
lame			Match		A	ction		Enable Sort
			This section conta	ins no values yet				
New source NAT:								
Name	Source zone Destination	n zone To	source IP To source p	ort				
Now SNAT rule	t 🕯 (wan	1 Ple	ase choose 1	Add and edit				

Scroll down to the bottom of the page to the section "New forward rule". Click <Add and edit>.

New forward rule: Name	Source zone Destination zone	
New forward rule	Image: the second se	

terfaces Wifi DHCP and DNS Hostnames Static R	toutes Diagnostics Firewall PPP
neral Settings Port Forwards Firewall Rules IPset	IP Proxy
ewall - Traffic Rules - (Unnamed Rule)	
page allows you to change advanced properties of the train	ffic rule entry, such as matched source and destination hosts.
Rule is enabled	( Disable
Name	-
Restrict to address family	(IPv4 and IPv6 t)
Protocol	TCP+UDP \$
Match ICMP type	any 🗘 📋
Source zone	Any zone
	Cap: (empty)
	Ian: Ian: 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
	o newzone: (empty)
	O ppp: ppp: 🔊
	o wan: wan: 🕎
Source MAC address	(any 🛟
Source address	any 🗘
Source port	any
Destination zone	O Device (input)
	Any zone (forward)
	Cap: (empty)
	🔿 lan: 📰 👷
	o newzone: (empty)
	O ppp: ppp: 2
	💿 wan: 🕎
Destination address	(any 🗘
Destination port	any
Action	accept
Extra arguments	Passes additional arguments to iptables. Use with care!

Here you can give the new rule a name, specify the protocol, restrict the rule to a certain zone, identify the source ip address, the destination ip address, port numbers. etc.

This is standard firewall convention. Once the rule is created, click <Save & Apply>. Place the rule where you want it on the traffic rule list using the Sort column arrows for up and down.

This is a full-featured firewall that you can customize to meet your needs.

See IP Sets section of this document for creating block and allow rules by domain name instead of ip address.

#### 8.5.5. IP Sets

Use IP sets for cloud-based services where standard firewall rules will not work. This allows block and allow rules by domain name instead of by ip address. IP sets rules take priority over anything in the firewall.

Optimi	zer   wXa-203 v2	.61   Load: 1.2	2 1.05 1.02							Changes: 0
	Home Services	Status Sy:	stem Network	Statistics	Logout					
	interfaces Wifi	DHCP and DN	IS Hostnames	Static Routes	Diagnostics	Firewall	PPP			_
	General Settings	Port Forwards	Firewall Rules	IPset IP Pr	оху					_
IP	Sets									
				hu tha firmuu lla		l halan ara			 	
Hi	gh priority rules a	pply before use	r defined firewall r	by the firewall a ules while low p	nd/or the load riority rules ap	ply after.				
	IPset Name	Action	Priority				Domains			
	Unique Name	Filtering Action	Filter Priority				Domain(s) to Fi	ilter		
					This	section cont	ains no values yet			
	Add									
	Reset								Save 🕑	Save & Apply
Powe	red by RedPort (C	opyright © Glol	bal Marine Networl	ks, LLC 2015 - A	II Rights Reser	ved)				

Click <Add> to create a new IP set rule.

Action Definitions:

- Block: rejects the domain
- Pass: allows the domain

You can group multiple domain names into one IP set rule.

## 8.5.5.1. IP Sets Example (WhatsApp Configuration)

Navigate to the <Network> tab, under <Firewall> tab, and then the <IPset> tab.

ptimizer   wXa-203 v2.61   Load: 1.04 1.02 1.00	Changes: 0
Home Services Status System Network Statistics Logout	
Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics Firewall PPP	
General Settings Port Forwards Firewall Rules IPset IP Proxy	
IP Sets	
Block, Allow, or Define groups of domains to be used by the firewall and/or the load balancer. High priority rules apply before user defined firewall rules while low priority rules apply after.	
IPset Name Action Priority Domains	
Unique Name Filtering Action Filter Priority Domain(s) to Filter	
This section contains no values yet	
Sav Sav	e 🚺 Save & Apply
owered by RedPort (Copyright © Global Marine Networks, LLC 2015 - All Rights Reserved)	

1. Click <Add> to create a new IP set rule.

Optimizer   wXa-203 v2.61   Load: 1.15 1.05 1.01	Changes: 0
Home Services Status System Network Statistics Logout	
Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics Firewall PPP	
General Settings Port Forwards Firewall Rules IP Proxy	
IP Sets	
Block, Allow, or Define groups of domains to be used by the firewall and/or the load balancer. High priority rules apply before user defined firewall rules while low priority rules apply after.	
IPset Name Action Priority Domains	
Unique Name Filter Priority Domain(s) to Filter	
WhatsApp1 Pass (High ) whatsapp.net	* Delete
whatsapp.com	
WhatsApp2 Pass +) (High +) whatsapp net	× Delete
1 Add	
	Save 🛛 Save & Apply

2. For WhatsApp you will be adding two new IP set rules. Give each a unique name such as WhatsApp1 and WhatsApp2.

- 3. For each new IP set rule give each two Domains of whatsapp.com and whatsapp.net.
- 4. Click <Save & Apply>.
- 5. Click on the <Firewall Rules> tab.

nterfaces Wifi DHCP	and DNS Hostnames Static Routes Diagnostics Firewall PPP			
eneral Settings Port For	wards Firewall Rules IPset IP Proxy			
rewall - Traffic Rul	es			
ffic rules define policies fo	n nackets traveling between different zones, for example to reject traffic between certain	n basts or to open WAN parts on the re	outer	
Traffic Rules				
Name	Match	Action	Enable Sort	
BLOCK WAN	Any traffic			
DO_NOT_MODIFY	From any host in wan To any router IP on this device	Discard input		Edit Edit
ALL	Any traffic			
DO_NOT_MODIFY	From any host in any zone To any host in any zone	Accept forward		ZEdit Delete
PASS DNS	Any UDP			
DO_NOT_MODIFY	From any host in any zone To any host, port 53 in any zone	Accept forward		Edit Delete
DNS	Any UDP		•	
DO_NOT_MODIFY	From any host in any zone To any router IP at port 53 on this device	Accept input		Edit Edit
нттр	Any TCP	Annual Connect		
DO_NOT_MODIFY	To any host, port 80 in any zone	Accept forward		Edit Delet
HTTPS	Any TCP	Accent femuend		
DO_NOT_MODIFY	To any host, port 443 in any zone	Accept forward		Lait Muelet
FTP	Any TCP	Accent forward		
DO_NOT_MODIFY	To any host, ports 20-21 in any zone	Accept forward		ZEdit Delete
	Any traffic	Accept forward		Edit Delet
	To any host in wan	Acceptionard		
Open ports on router:				
Name	Protocol External port			
New input rule	TCP+UDP +			
New forward rule:				
Name	Source zone Destination zone			
New forward rule	lan			
Source NAT				
ource NAT is a specific form	n of masquerading which allows fine grained control over the source IP used for outgoing tra	ffic, for example to map multiple WAN a	dresses to internal	subnets.
Name	Match	A	ction	Enable Sort
	This section contains no values yet			
New source NAT:				
Name S	ource zone Destination zone To source IP To source port			
New SNAT rule	wan     the set of the set o	it		

6. Click the checkbox for the DNS traffic Rule (not the Pass DNS traffic Rule).

PASS DNS DO_NOT_MODIFY	Any UDP From any host in any zone To any host, port 53 in any zone	Accept forward	🔹 🔮 🗶 Edit 💌 D	elete
DNS DO_NOT_MODIFY	Any UDP From any host in any zone To any router IP at port 53 on this device	Accept input	e 🖲 🖉 Edit 🗶 D	elete
HTTP DO_NOT_MODIFY	Any TCP From any host in any zone To any host, port 80 in any zone	Accept forward	e s ZEdit XD	elete

7. Click <Save & Apply>.

8. Click on the <Network> tab and then click on the <DHCP and DNS> tab.

mizer   wXa-203 v2.61   Load: 1.05 1.0	01 1.00   Auto Refresh: on		Change			
Home Services Status System	Network Statistics Logout					
Interfaces Wifi DHCP and DNS	Hostnames Static Routes Diagnos	stics Firewall PPP				
DHCP and DNS						
Desmans is a sembled DHCD Converte	nd DNC Ennuarday fay NAT frauvalla					
Server Settings	nu DNS-Forwarder for MAT firewalls					
Server Settings						
General Settings Resolv and Hos	ts Files TFTP Settings Advanced Se	ettings				
Domain required	<b>V</b>	Don't forward DNS-Requests without DNS-Nar	ne			
Authoritative	<u></u>	General State only DHCP in the local network				
Local server		Local domain specification. Names matching this	domain are never forwarded and are resolved from DHCP or hosts			
Least demain		es only				
Local domain	(	Local domain suffix appended to DHCP names an	d hosts file entries			
Log queries		Write received DNS requests to syslog				
DNS forwardings [example.org/10.1.2.3						
	(	List of DNS servers to forward requests to				
Rebind protection		Discard upstream RFC1918 responses				
Active DHCP Leases						
Aarons-MBP	192 168 10 124	MAC-Address	Leasetime remaining			
Active DHCDuf Leases	172.100.1012.1					
Hostname	IPv6-Address	DUID	Leasetime remaining			
		inere are no active leases.				
Static Leases Static leases are used to assign fixed II lease are served. Use the Add Button to add a new lease requesting host.	addresses and symbolic hostnames to DH entry. The MAC-Address indentifies the ho	CP clients. They are also required for non-dynan st, the <i>IPv4-Address</i> specifies to the fixed address.	nic interface configurations where only hosts with a corresponding ss to use and the <i>Hostname</i> is assigned as symbolic name to the			
Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)			
Add		This section contains no values yet				
Reset			Save Save Apply			
red by RedPort (Copyright © Global N	larine Networks, LLC 2015 - All Rights Re	eserved)				

9. Under the "Server Settings" section on the <General Settings> tab, add four new "DNS forwardings":

- /whatsapp.com/8.8.8.8
- /whatsapp.com/8.8.4.4
- /whatsapp.net/8.8.8.8
- /whatsapp.net/8.8.4.4

timizer   wXa-203 v2.61   Load: 1.05 1.01 1.00   Auto Refresh: on Change		
Home Services Status System Network	Statistics Logout	
Interfaces Wifi DHCP and DNS Hostnames	Static Routes Diagnostics Firewall PPP	
DHCP and DNS		
onsmasq is a combined <u>DHCP</u> -Server and <u>DNS</u> -Forwa	Irder for <u>NAT</u> firewalls	
Server Settings		
General Settings Resolv and Hosts Files TFT	P Settings Advanced Settings	
Domain required	<table-cell> 🐵 Don't forward <u>DNS</u>-Requests without <u>DNS</u>-Name</table-cell>	
Authoritative	(i) This is the only <u>DHCP</u> in the local network	
Local server	Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only	
Local domain	Local domain suffix appended to DHCP names and hosts file entries	
Log queries	Write received DNS requests to syslog	
DNS forwardings	whatsapp.com/8.8.8.8     X       whatsapp.com/8.8.4.4     X       whatsapp.net/8.8.8.8     X       whatsapp.net/8.8.4.4     T       Watsapp.net/8.8.4.4     T	
Rebind protection	Iniscard unstream RFC1918 responses	

10. Click <Save & Apply>.

11. Click on the <Resolv and Host Files> tab under the "Server Settings" section, and click the checkbox associated with "Ignore resolve file".

Optimizer   wXa-203 v2.61   Load: 1.	.05 1.01 1.00   Auto Refresh: on Chan	iges: 0	
Home Services Status S	System Network Statistics Logout		
Interfaces Wifi DHCP and	DNS Hostnames Static Routes Diagnostics Firewall PPP	- 1	
DHCP and DNS			
Dnsmasq is a combined <u>DHCP</u> -Server and <u>DNS</u> -Forwarder for <u>NAT</u> firewalls			
Server Settings			
General Settings Resolv an	nd Hosts Files TFTP Settings Advanced Settings		
Use /etc/ethers	☑ ☑ ☑ ☑ ☑ ☑ ☑ ☑		
Leasefile	/tmp/dhcp.leases		
Tanara recelus file	The metric given given and a solid		
Ignore /etc/hosts			
Additional Hosts files	· · · · · · · · · · · · · · · · · · ·		
Active DHCP Leases			

12. Click <Save & Apply>.

# 9. Statistics

Available to both 'admin' and 'superadmin' login.

Use the Statistics tab to display graphs of Optimizer connectivity load/transfer rates as well as .



# 10. Corporate Contact Information

For any questions, concerns, or recommendations, please contact us:

#### **RedPort Company Information**

For product orders, support or returns, please contact: Phone: International: +1 865.379.8723 USA: 877.379.8723 Email: info@redportglobal Sales: sales@redportglobal.com Web: redportglobal.com

#### **RedPort Address**

RedPort 3224 Wrights Ferry Road Louisville, TN 37777