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

© 2020 RedPort Global I Powered by Pivotel America Inc.
I All Rights Reserved.

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) 7
4. Getting Started - User Interface (UI) Access 8
    4.1. Access the Home Page 8
        4.1.1. Onsite Administrator Login (Admin) 8
        4.1.2. Installer/Network Administrator Login (Superadmin) 9
    4.2. How to Use with Default Setup 10
        4.2.1. Email and Web Browsing 10
        4.2.2. Voice Calls 11
        4.2.3. SMS Messaging 11
    4.3. Router 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
        5.4.1. Configure Connection to the Halo 21
        5.4.2. Connect to the External Wi-Fi Network. 21
        5.4.3. Route Network Traffic through the Halo 23
        5.4.4. Manage the Firewall (Optional) 24
        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
    6.1. Access System Log 32

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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

© 2020 RedPort Global I Powered by Pivotel America Inc.
I All Rights Reserved.

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 redportglobal.com and as white-label solutions for the world's premier satellite data service providers.

Optimizer is a satellite Wi-Fi router that combines a powerful satellite data router with voice capabilities, including a full PBX. It is more than just a voice device. It gives you everything you need to create a local voice and data network with your satellite device. You can 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. I All Rights Reserved.

- 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.

© 2020 RedPort Global I Powered by Pivotel America Inc.
I All Rights Reserved.

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:

© 2020 RedPort Global I Powered by Pivotel America Inc.
I All Rights Reserved.

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.

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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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

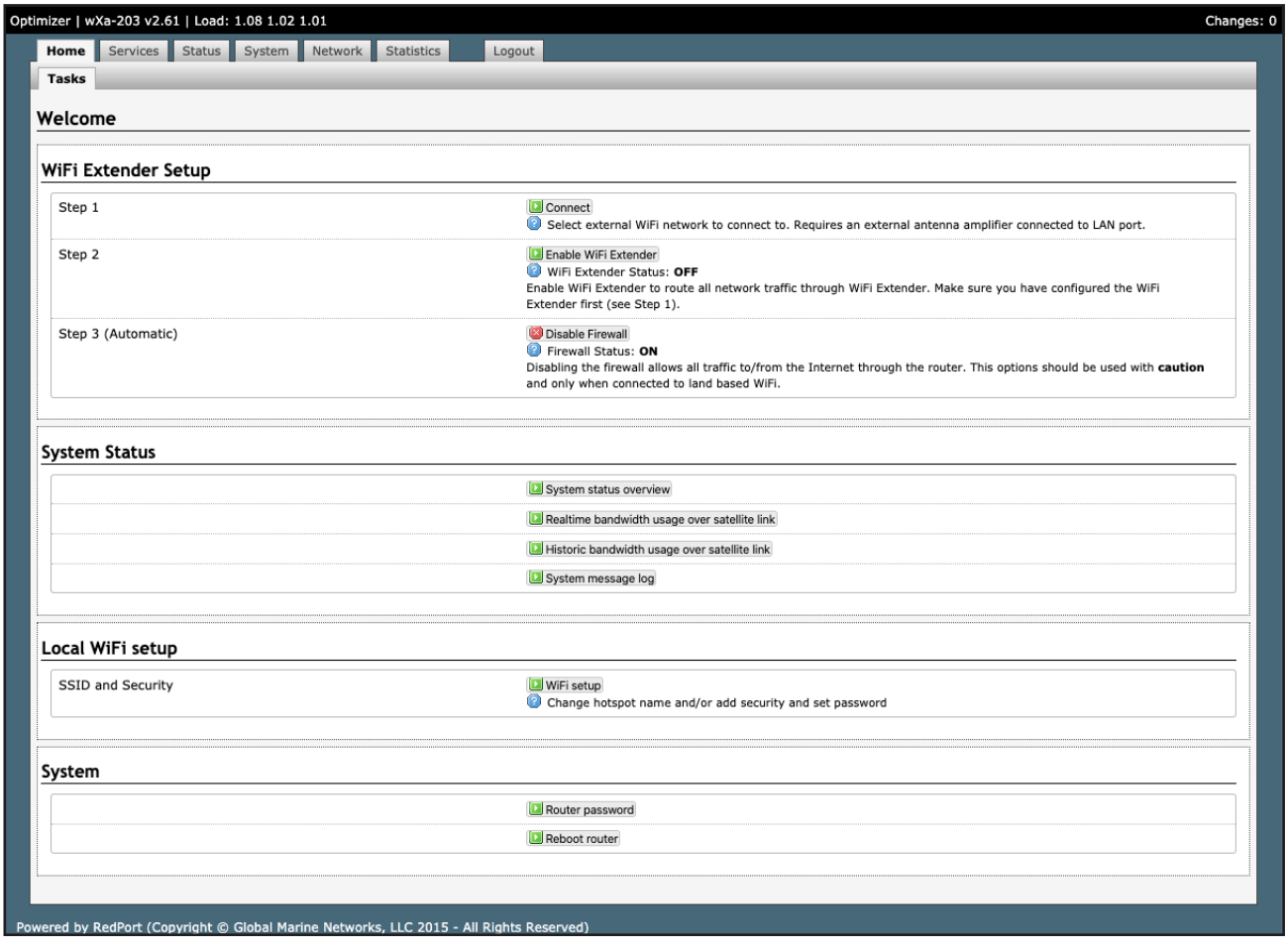
- Monitor the system status.
- Reboot the router, if necessary.
- Change the router password for the admin account, if necessary.

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):



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.

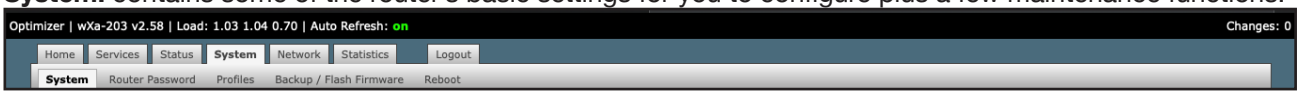
© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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.

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.



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.

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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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.

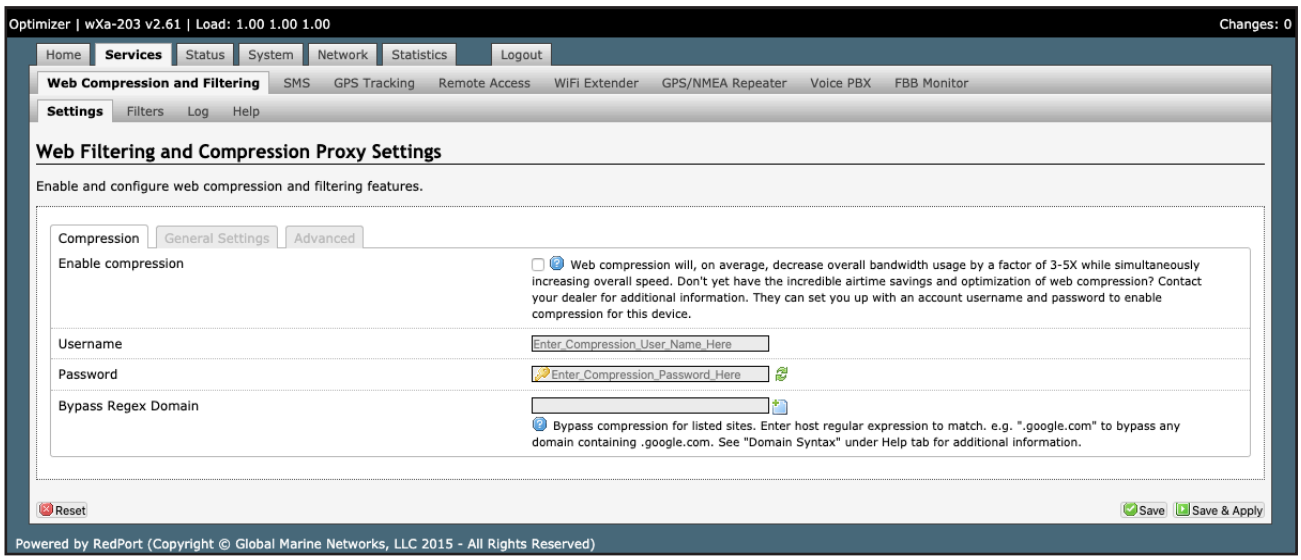
When you have completed and tested your configuration and are confident that it is working as desired, you can remove the Anti-Lock rule in System > System Settings. Now you can Enable the BLOCK ALL from WAN firewall rule in Network > Firewall > Firewall Rules.

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



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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

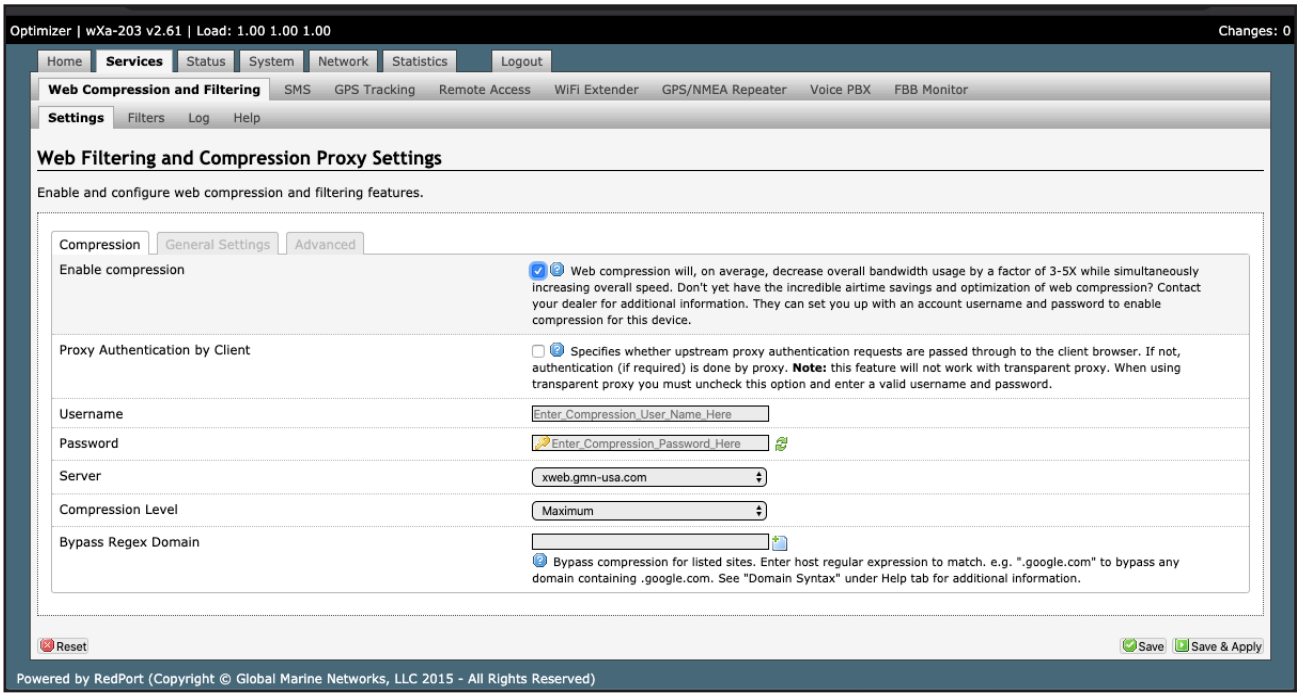
Enable Compression: If you have purchased Web Compression service, click the checkbox to Enable compression. The page will expand; see With Compression Enabled below.

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.



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.

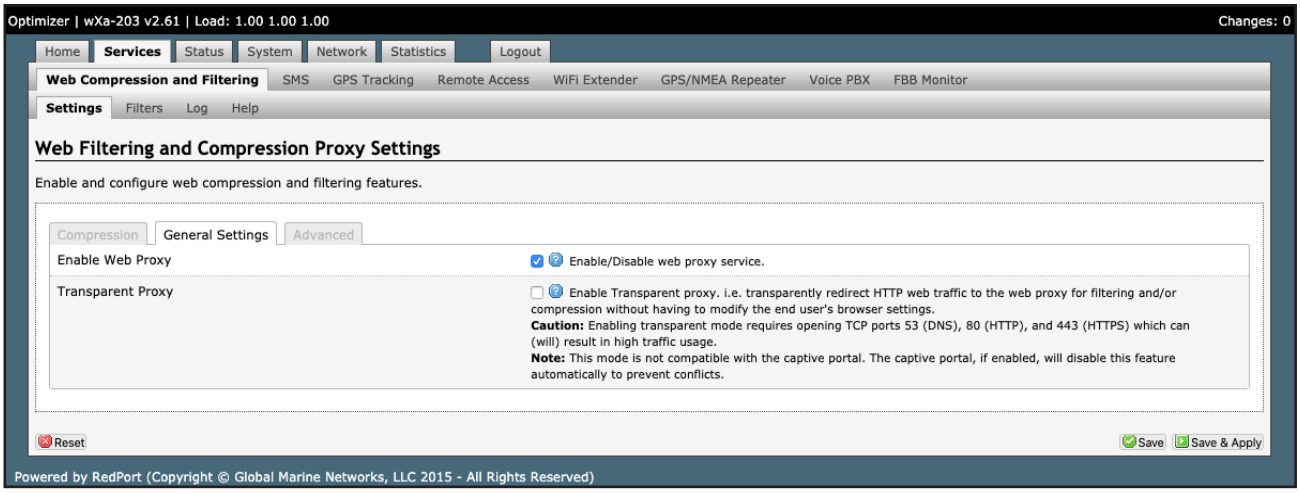
Server: Do not change this unless instructed to do so by your service provider.

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.

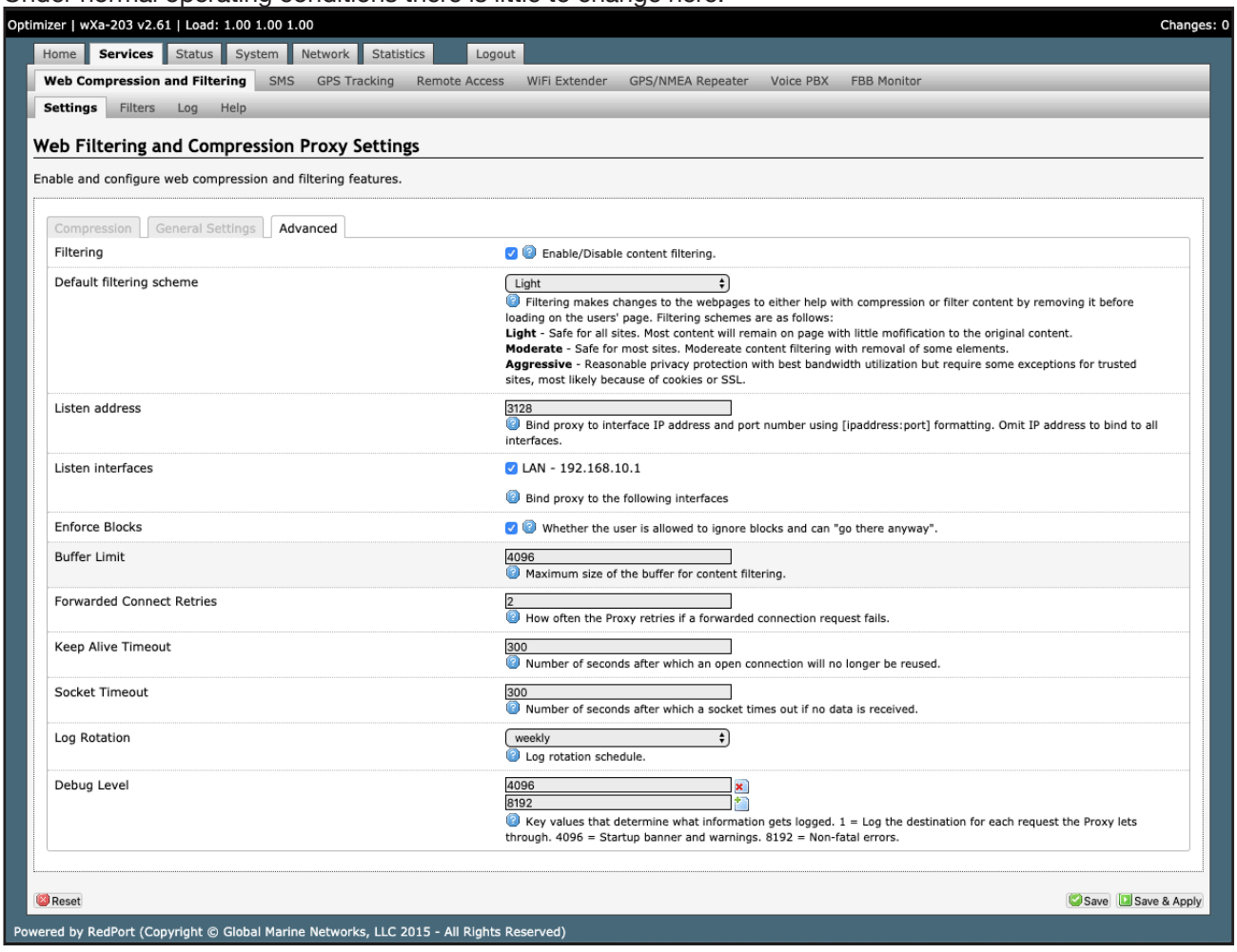
© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



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.



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

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

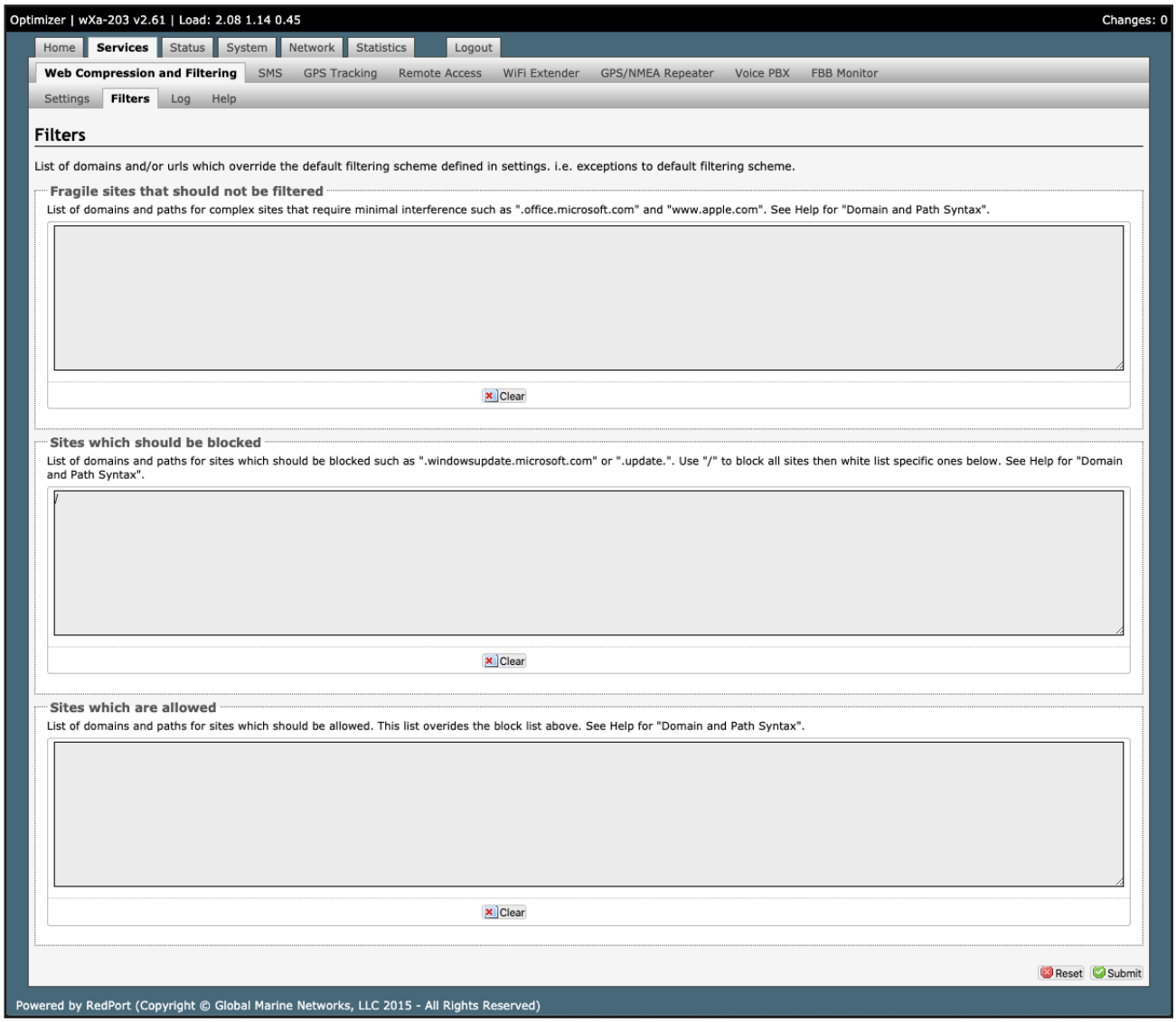
level of “1”, all URLs will be logged and will appear on the Log page, one line per URL.

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.



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.

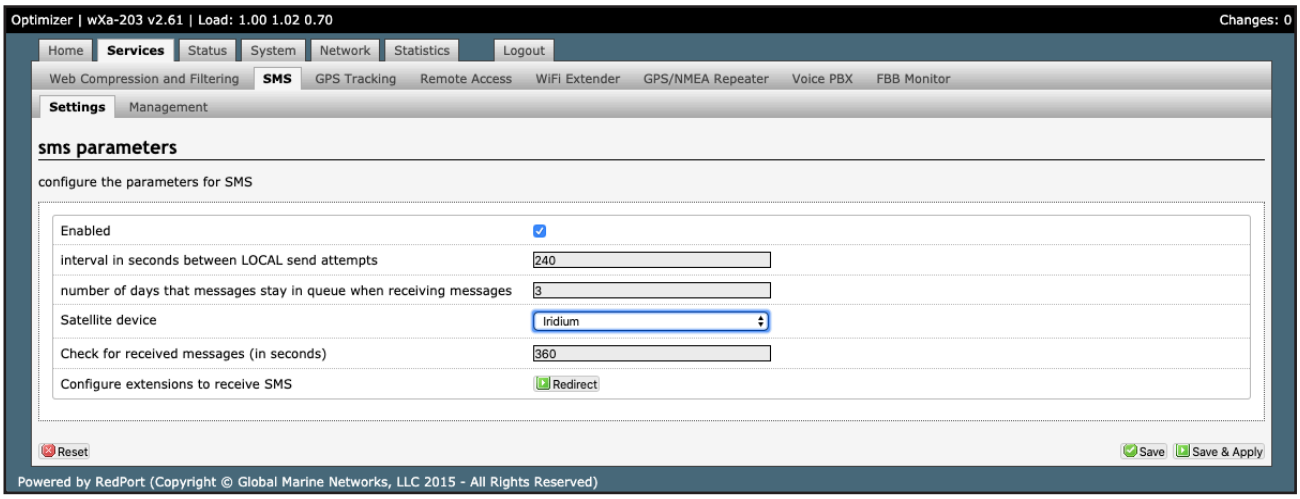
© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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.



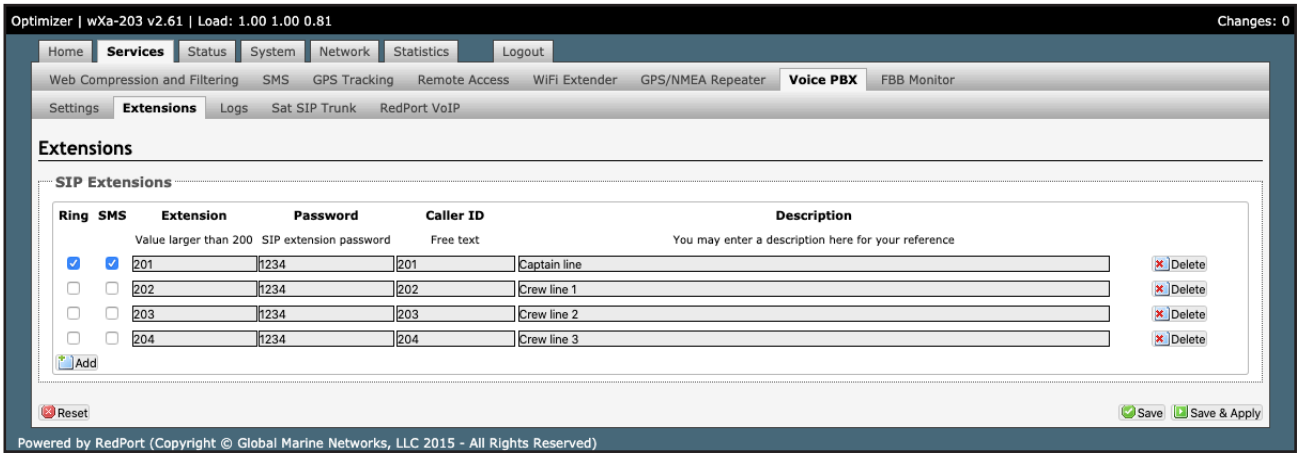
1. Click the checkbox to enable SMS.

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.

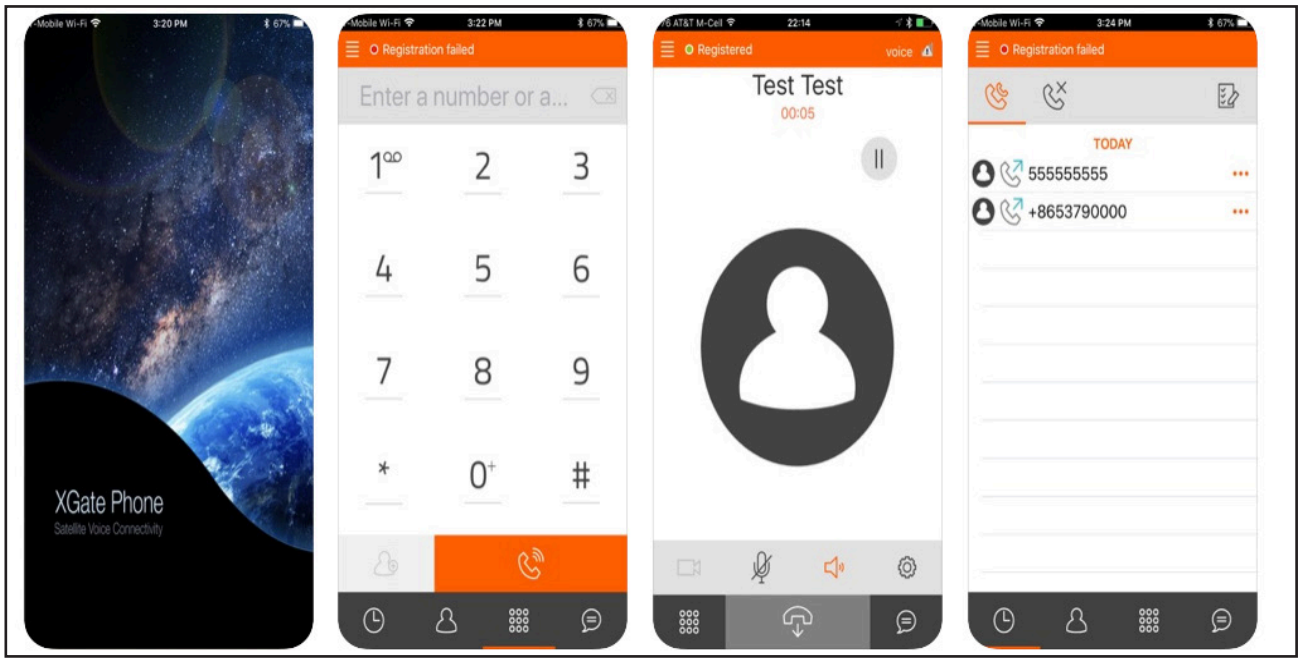


© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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.

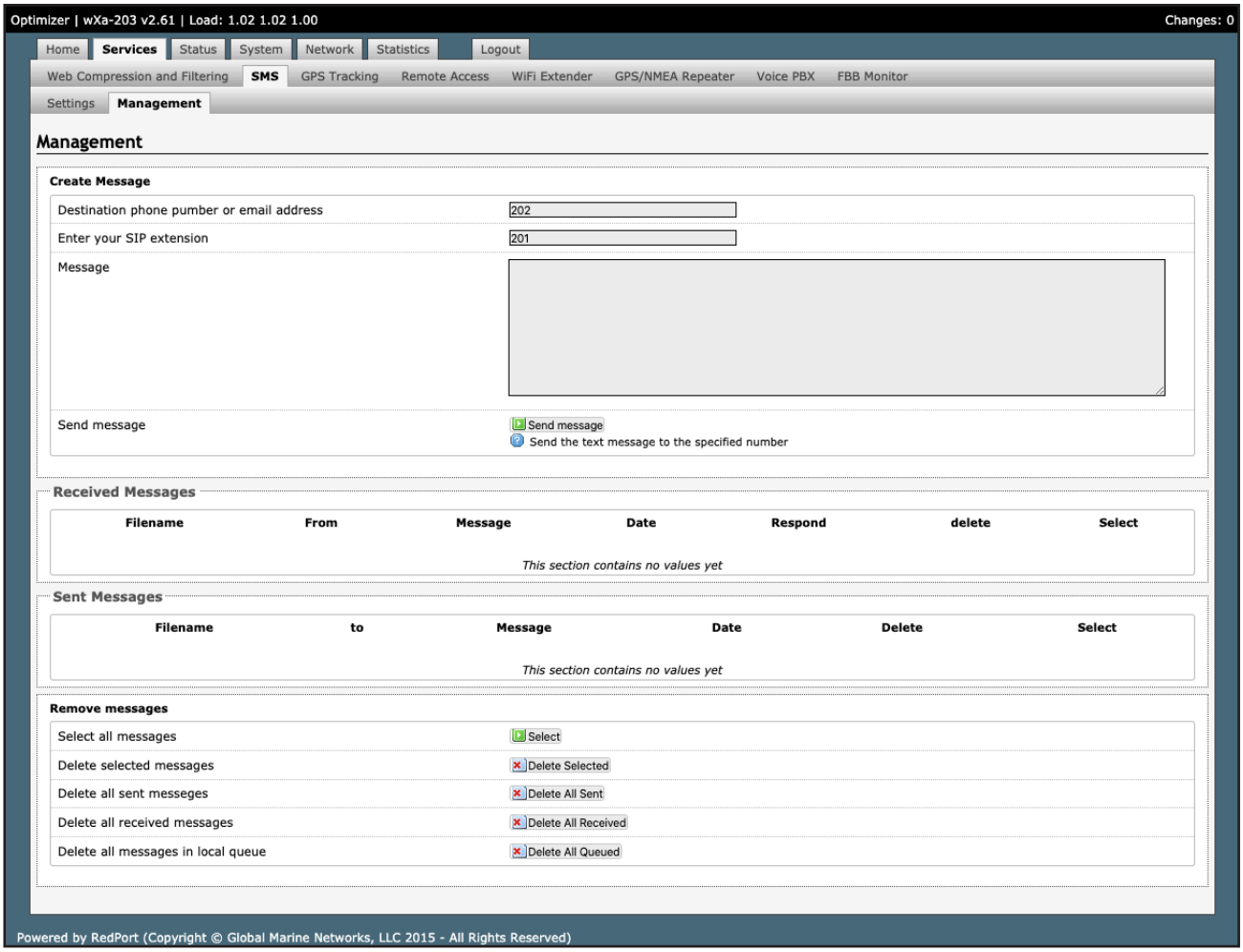


Only one SMS message can be sent at a time. Standard SMS message rates apply. (Multi-user Voice and SMS is possible with the optional RedPort VoIP service. Contact your service provider for details.)

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.

© 2020 RedPort Global I Powered by Pivotel America Inc.
I All Rights Reserved.



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

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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

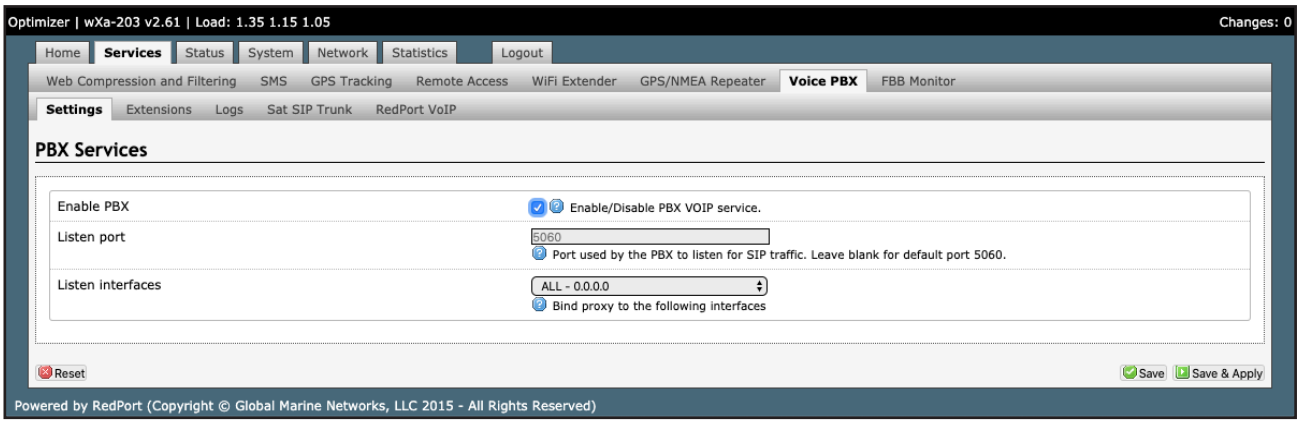
The Optimizer allows unlimited SIP extensions with free local calling and text messaging within your local area network using the XGate Phone app*.

*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.

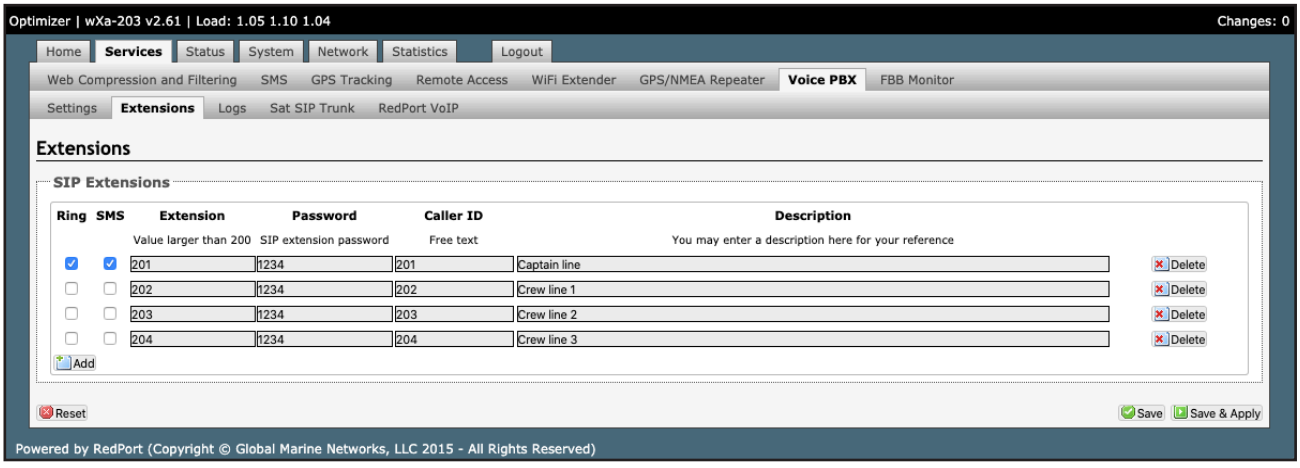


5.3.2. Setup Extensions

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.



© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights 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

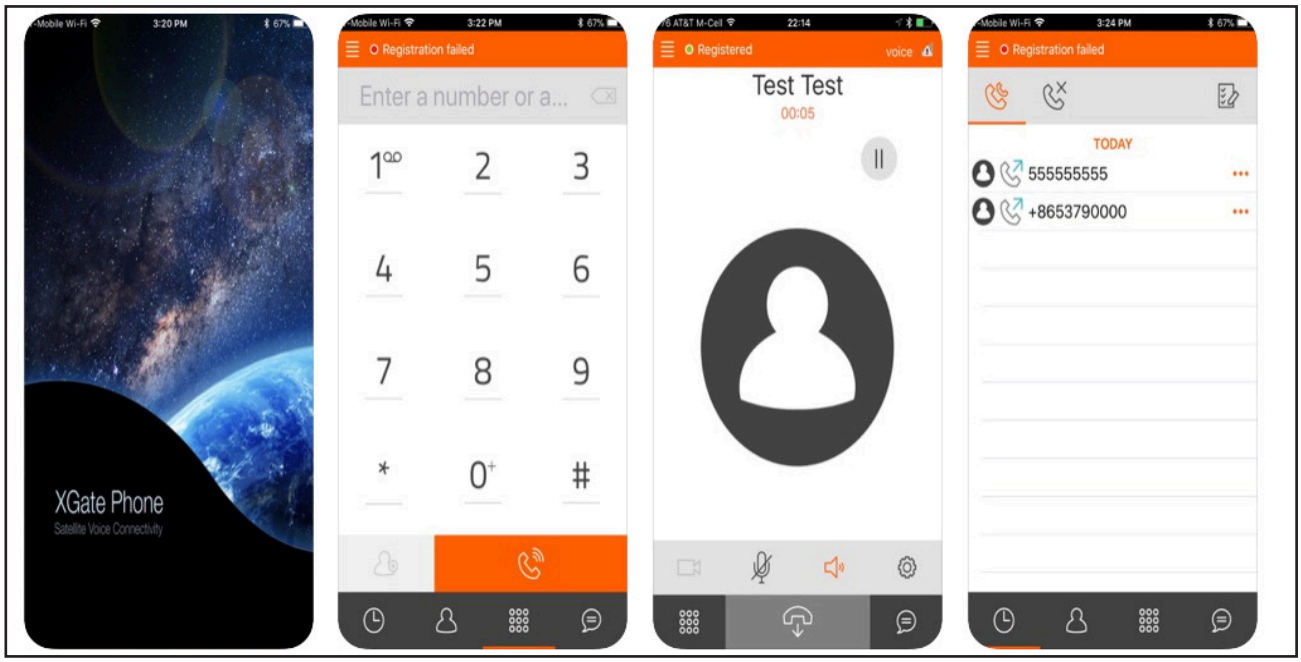
5.3.3. How to Make/Receive Voice Calls

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.

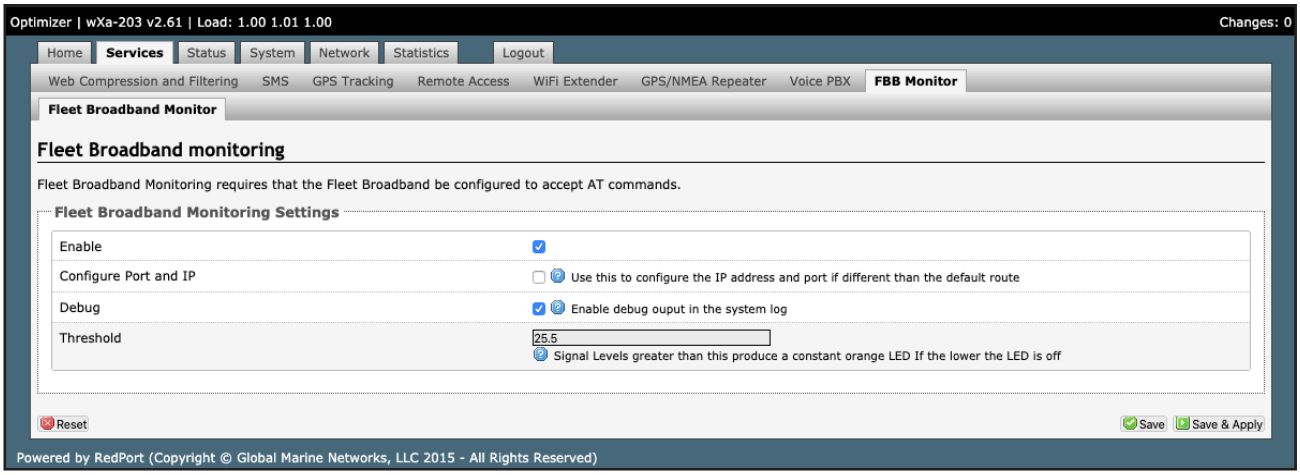
Only one phone call can be active at a time. (Multi-user Voice and SMS is possible -- up to four consective sessions -- with the optional RedPort VoIP service. Contact your service provider for details.



5.3.4. Fleet Broadband Monitoring (FBB)

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

© 2020 RedPort Global I Powered by Pivotel America Inc.
I All Rights 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.

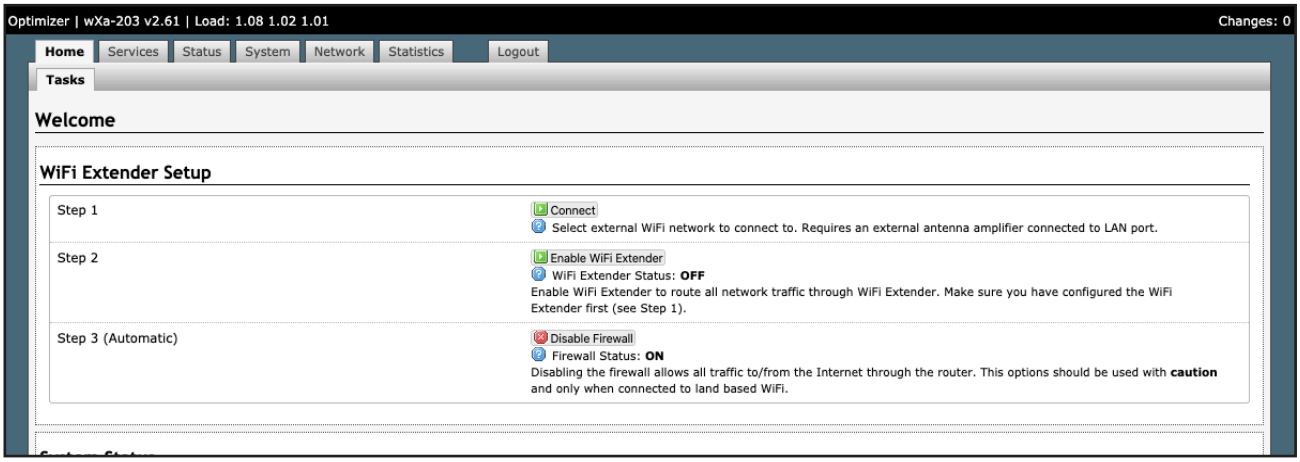
For your convenience, the Halo Wi-Fi Extender Quick Start Guide can be found in Appendix B of this document. It includes important information regarding the physical connection setup.

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

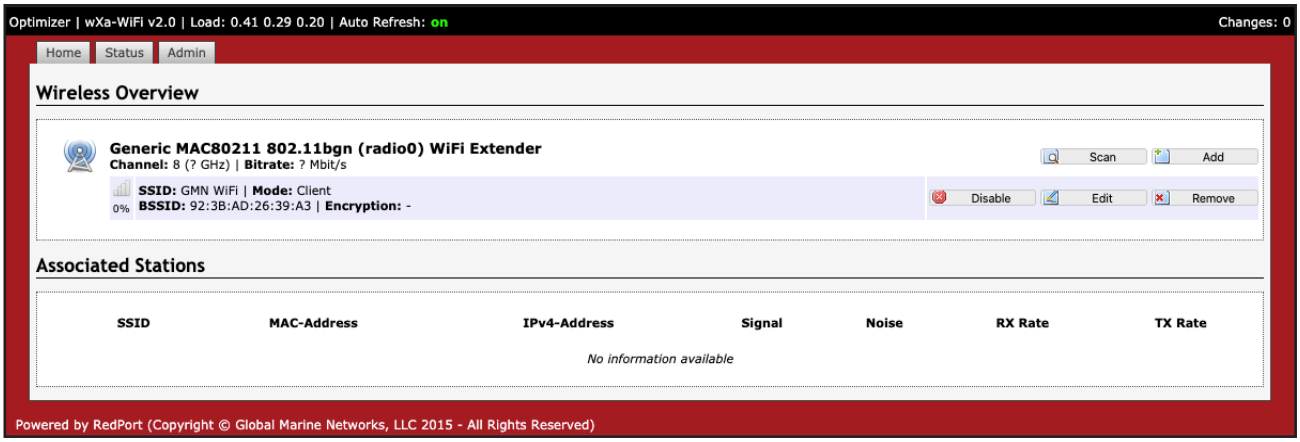
With the Halo powered ON and connected to the Optimizer. Login to the Optimizer router with either username = admin or with username = superadmin (see Chapter 4 Getting Started for details). Configuration requires two steps to connect:

5.4.2. Connect to the External Wi-Fi Network.

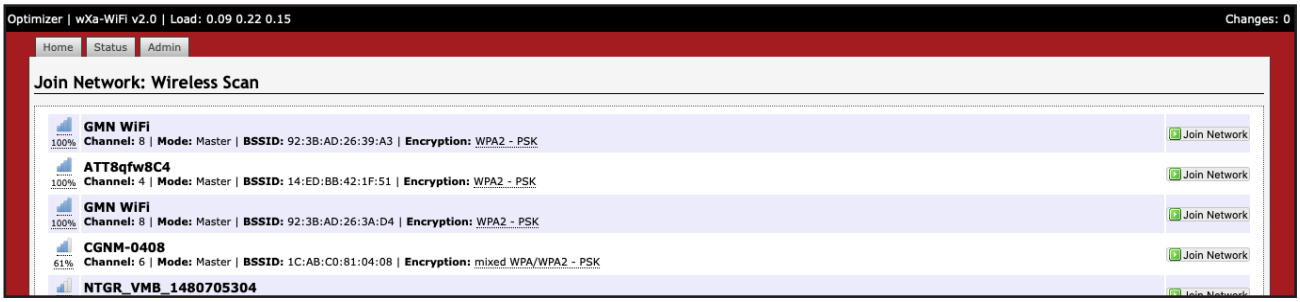


1. Click <Connect> button.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

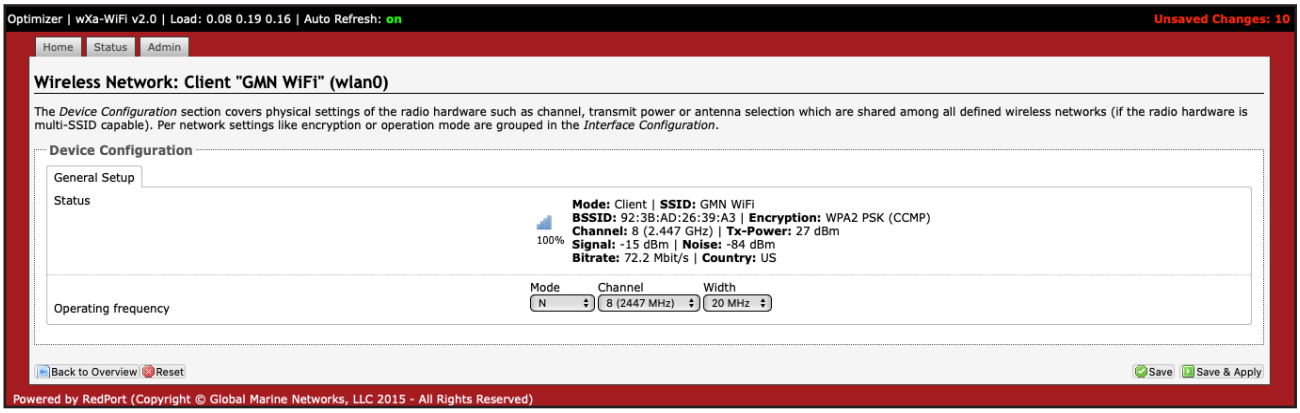


2. Click <Scan> to see what wireless networks may be available.



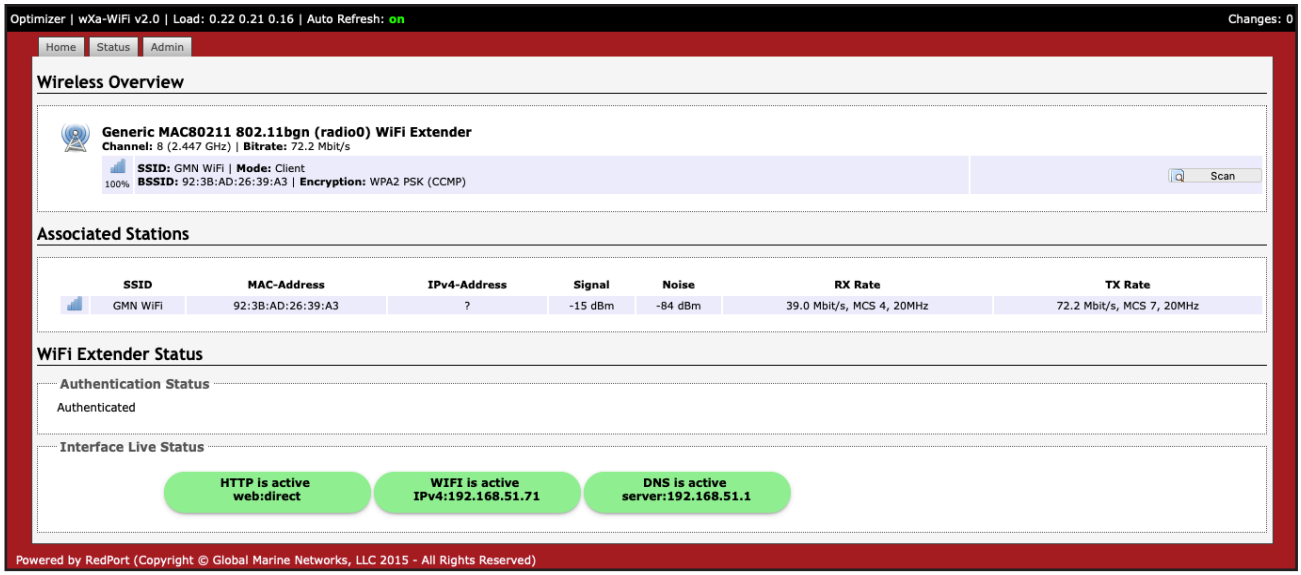
3. Click the wireless network you want to connect to and press <Join Network>.

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



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

© 2020 RedPort Global | Powered by Pivotel America Inc. | All Rights Reserved.

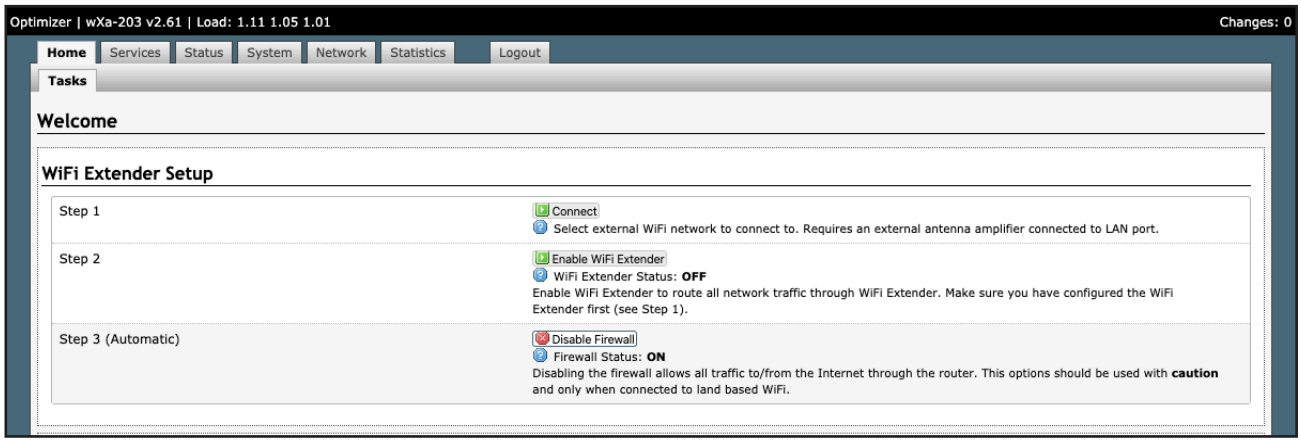


Notice that now the signal strength now registers greater than 0%.

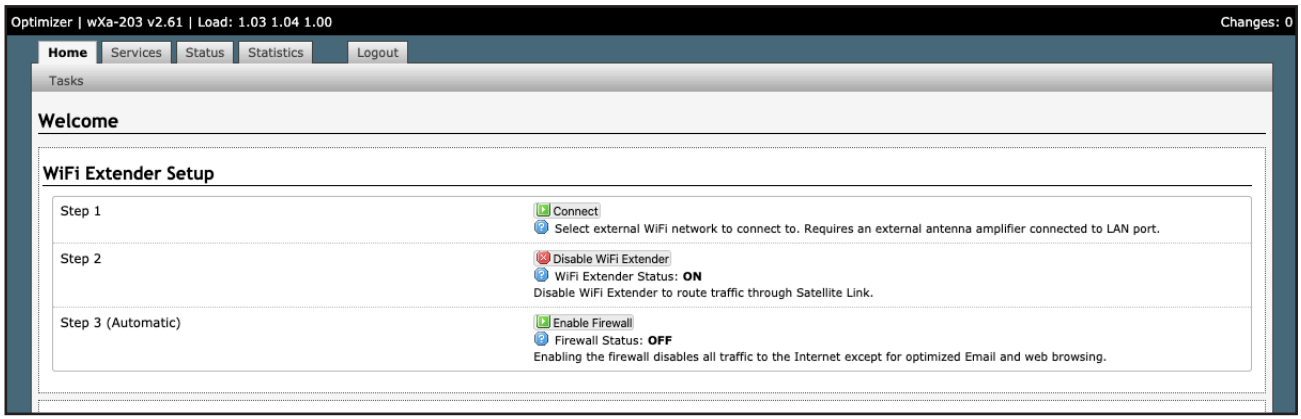
NOTE: If the signal status is blinking from 0% to 100% this typically means that the Wi-Fi Network Password/Key was entered incorrectly. Check with the external Wi-Fi Network Administrator to confirm the correct password. Click the Wireless Security tab and enter the correct password in the Key field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

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

5.4.3. Route Network Traffic through the Halo



1. Click <Enable Wi-Fi Extender>.



© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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>.

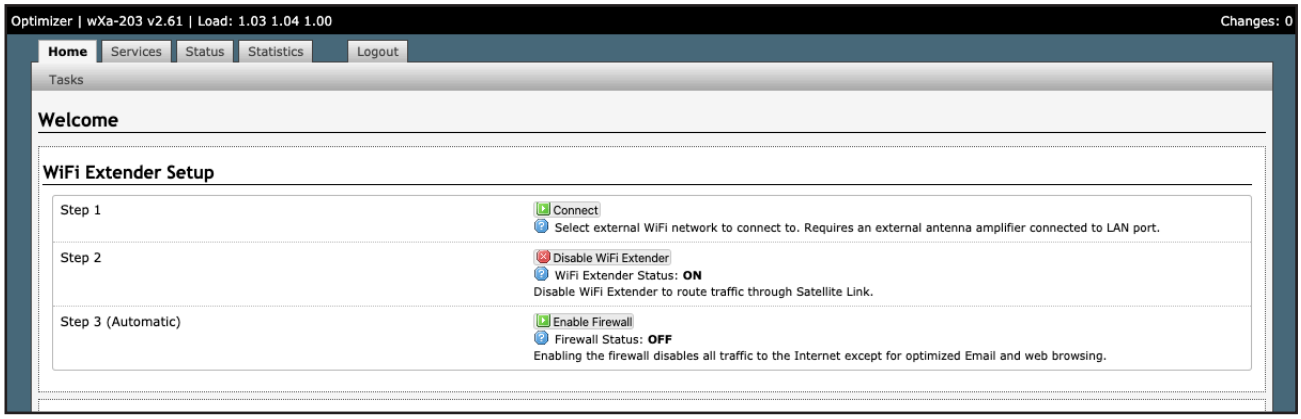
5.4.4. Manage the Firewall (Optional)

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:

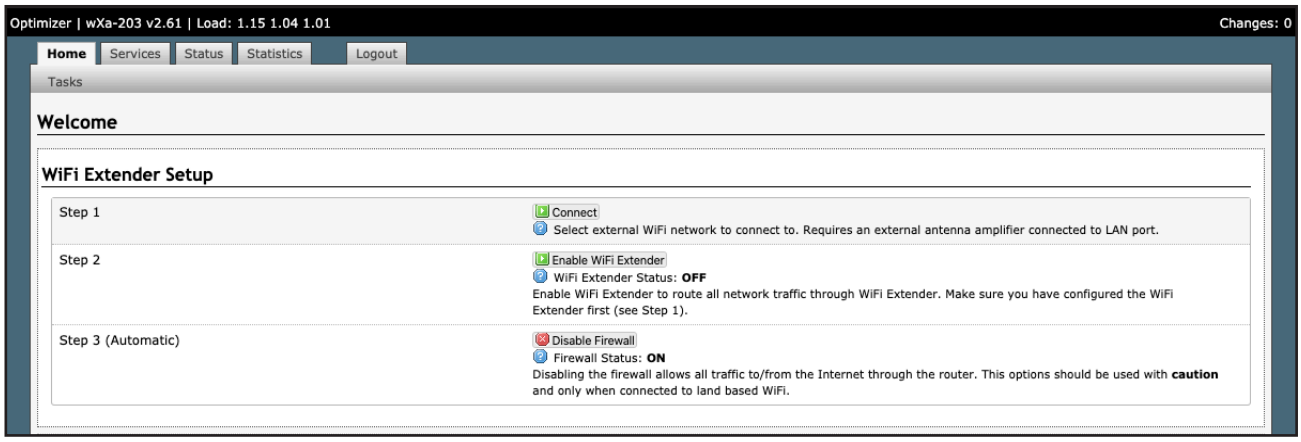


To Disable the Firewall, Click <Disable Firewall>.
To Enable the Firewall, Click <Enable Firewall>.

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>.



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

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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

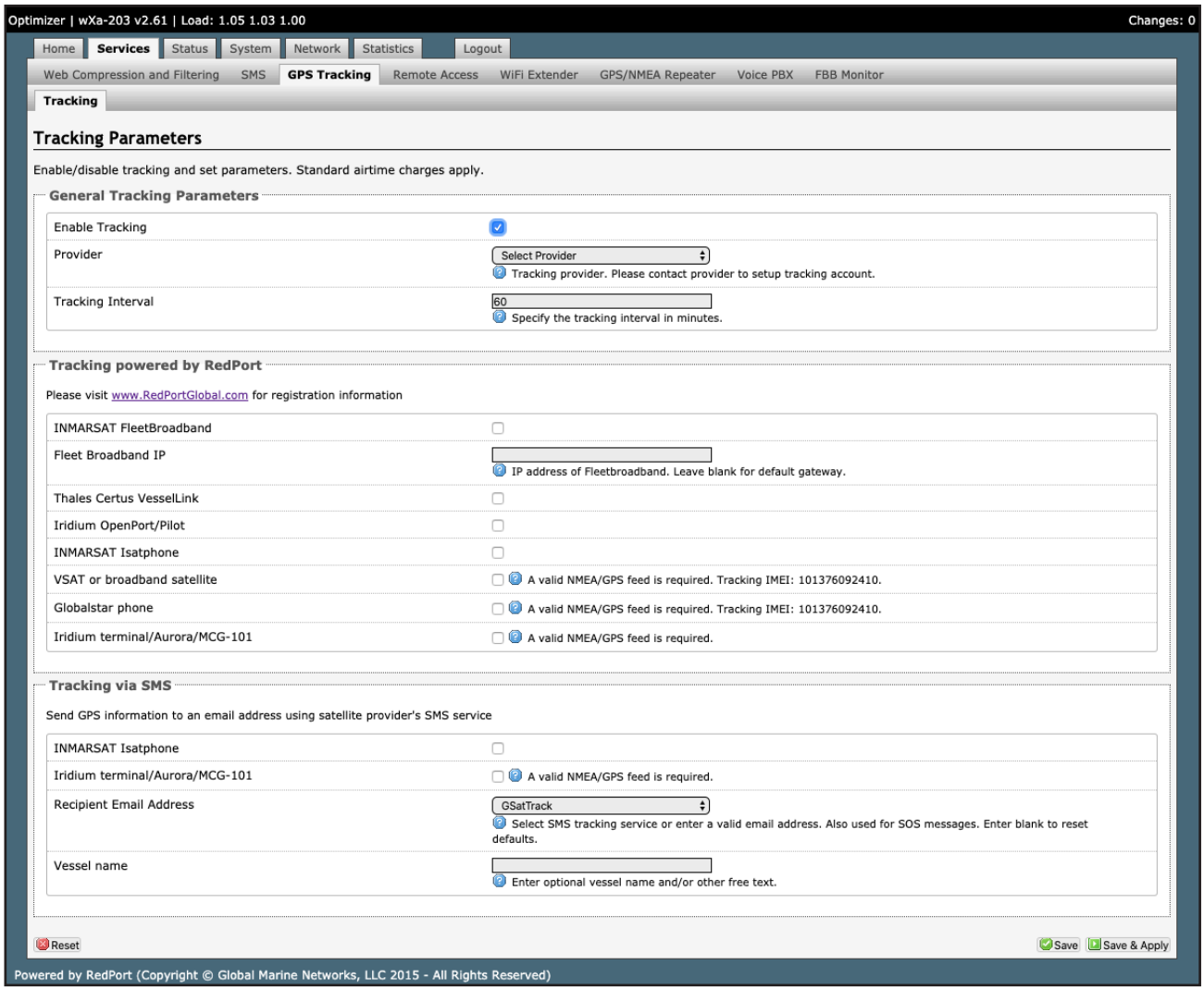
If you wish to have tracking service using your satellite device, the Optimizer offers GPS Tracking service powered by GSatTrack or Tracking service via SMS message.

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.



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.

© 2020 RedPort Global | Powered by Pivotel America Inc. | All Rights Reserved.

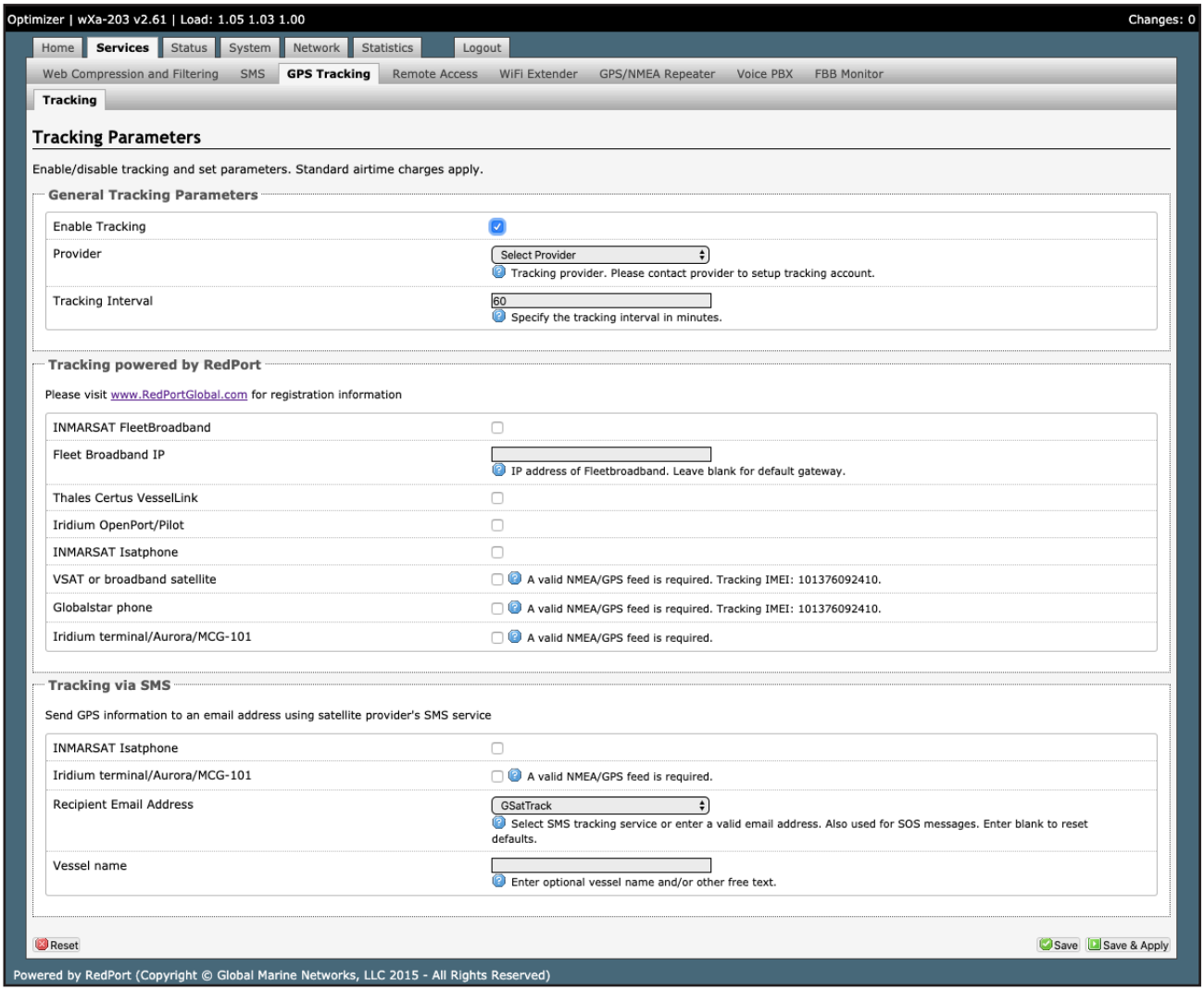
2. Select the satellite terminal you are using.

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.



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>.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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.

© 2020 RedPort Global I Powered by Pivotel America Inc.
I All Rights Reserved.

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.

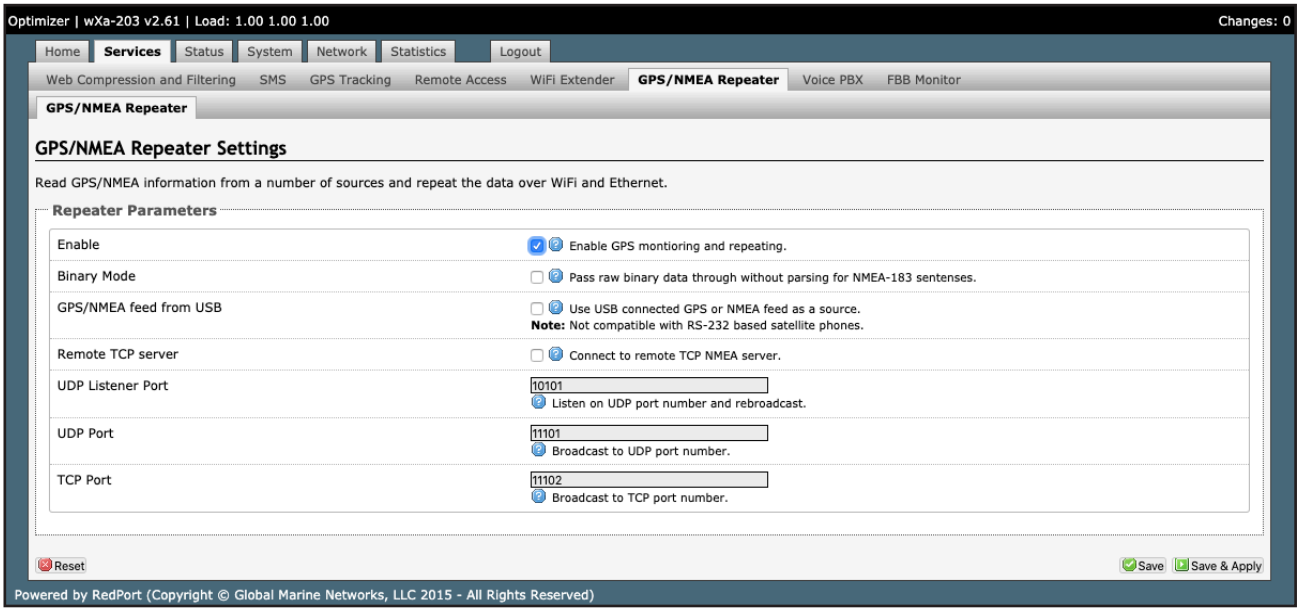
NOTE: The Optimizer supports RS232. If you have a NMEA RS-422 device, adding a properly wired RS-422 to RS-232 converter to your setup may allow the sharing of data.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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.



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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

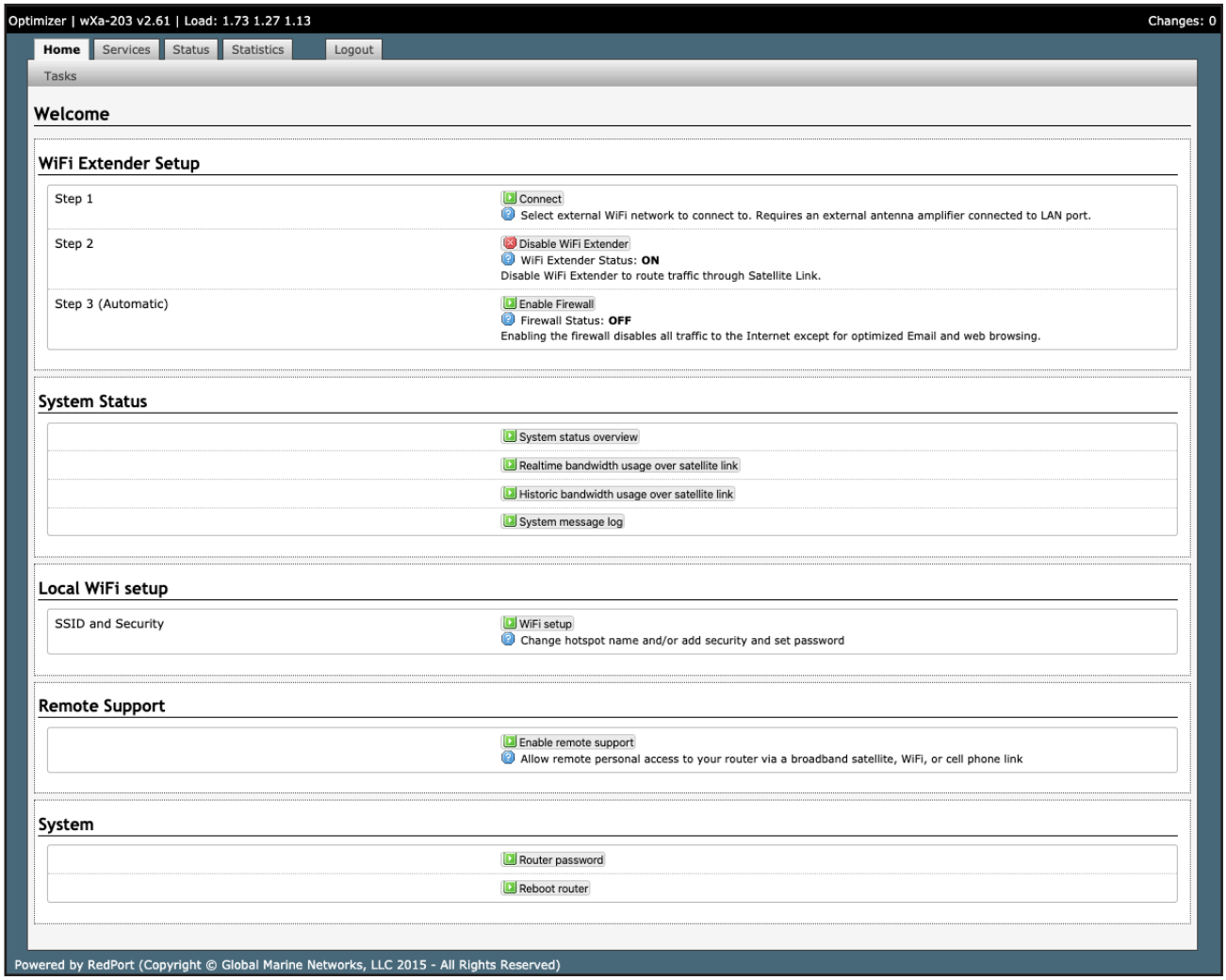
5.7. Remote Support

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.

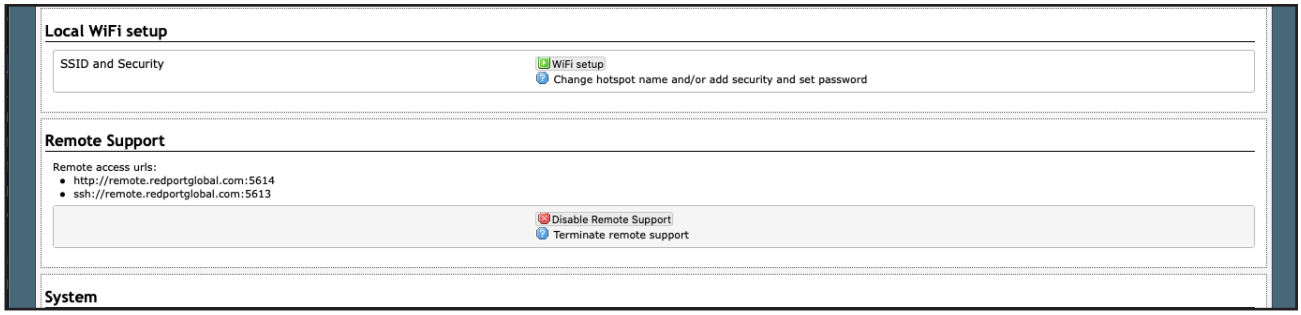
To enable Temporary Remote Support Access, click <Home> tab, scroll down to the "Remote Access" section.



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

When remote support is enabled Remote Access URLs are displayed.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

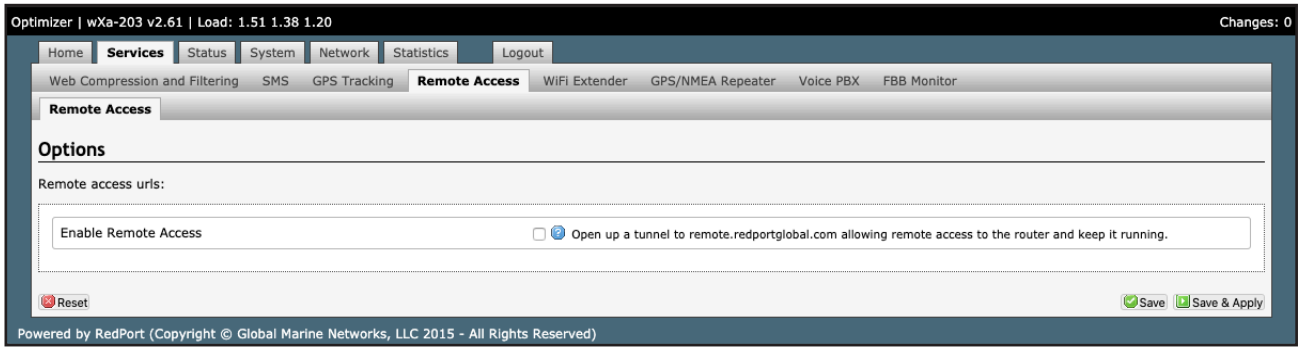


Disabling this Remote Support will not disable the persistent Remote Support. To disable this remote support access, either:

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

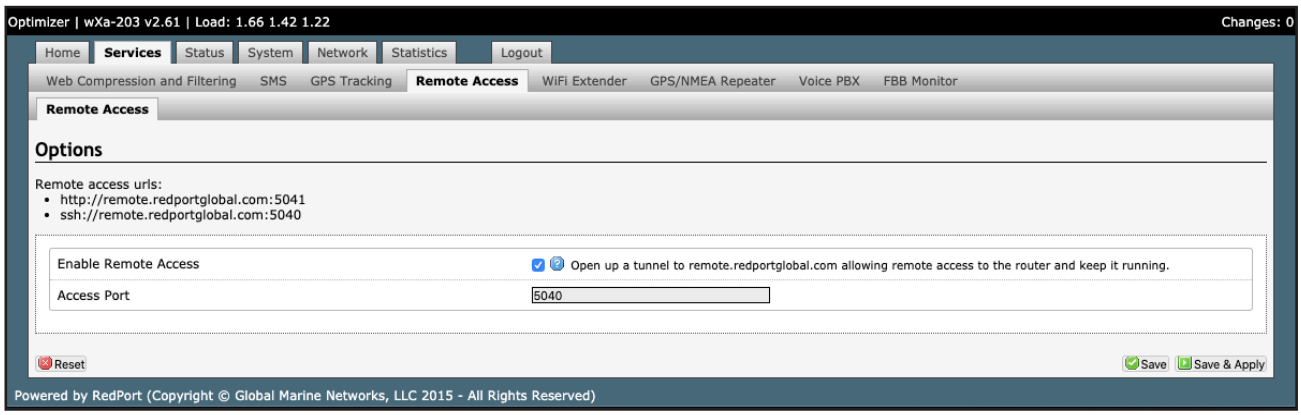
- Persistent Remote Support Access - The second remote support login access is located from the Services tab and permits persistent access. Even if the router is rebooted, this access will remain.

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



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

When remote support is enabled Remote Access URLs are displayed.



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

- Click <Services> tab, then click “Enable Remote Access”.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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:

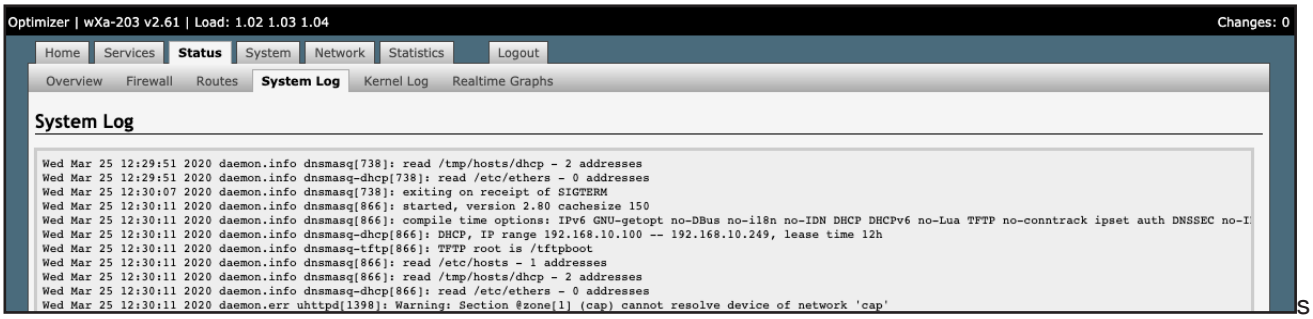
• How much memory the router is currently using
• Who is currently connected via wifi
• Error messages reported in the System Log and can be useful when troubleshooting connection issues.
• Realtime Graphs report how much data is being used by the different interfaces.

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.



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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

6.2. System Status for Monitoring Usage

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

7. System

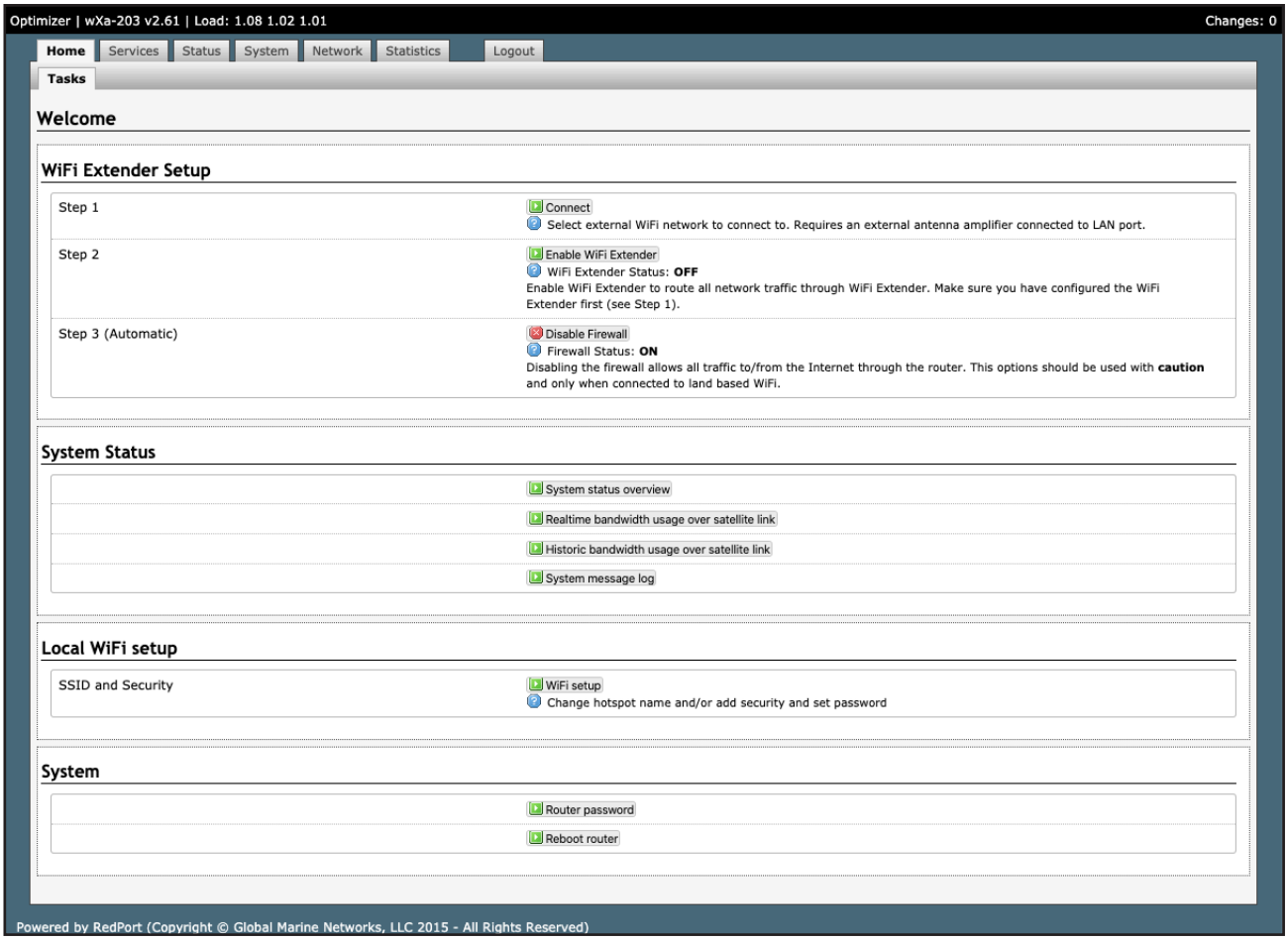
7.1. Change Superadmin and/or Admin Password

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.

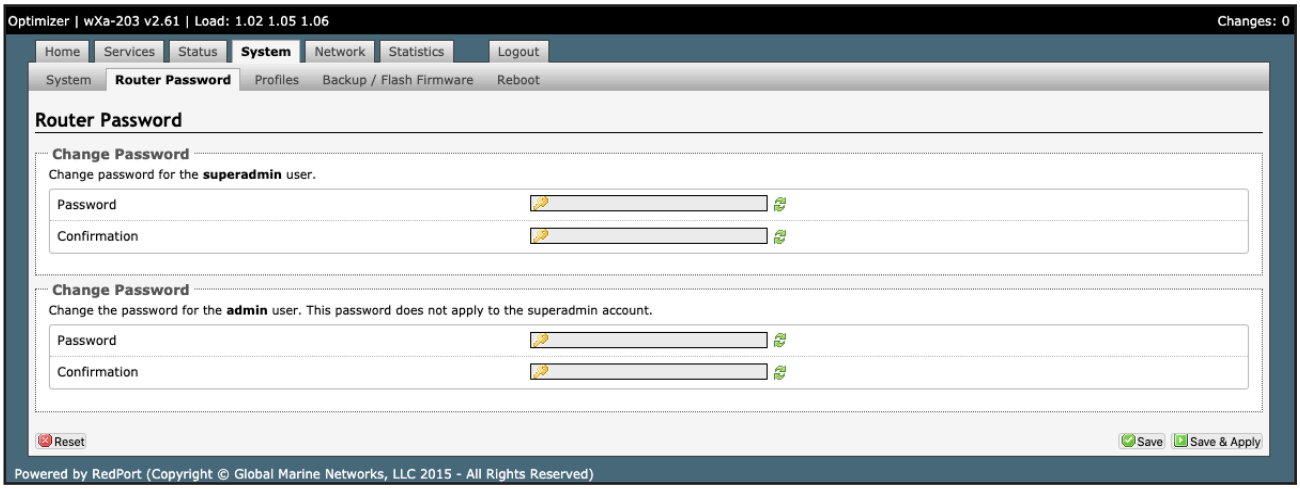
To change the password(s), login to the Optimizer:

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



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.



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

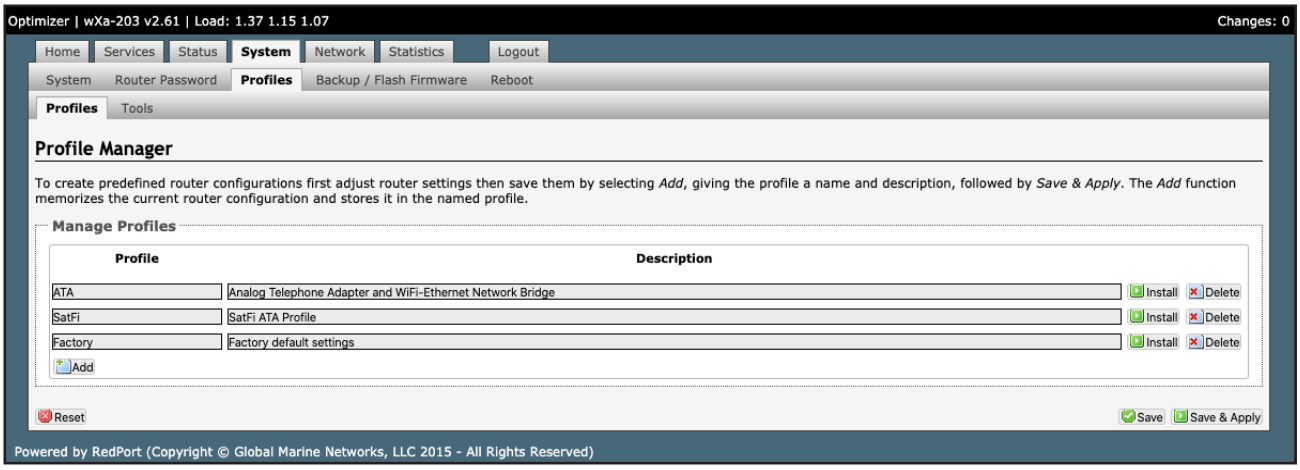
© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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.



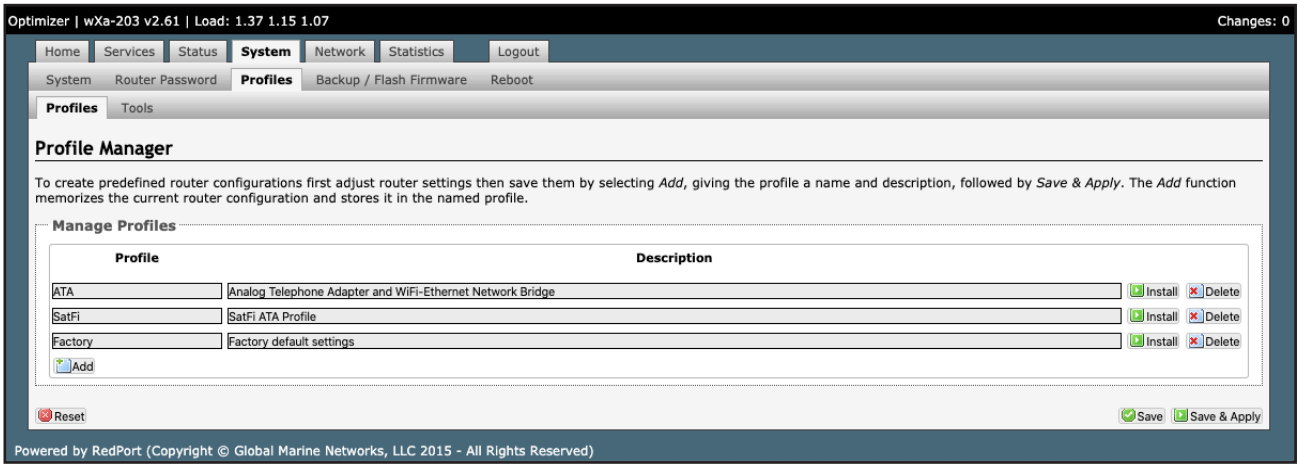
There are three default profiles:

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:



1. Click <Add>.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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

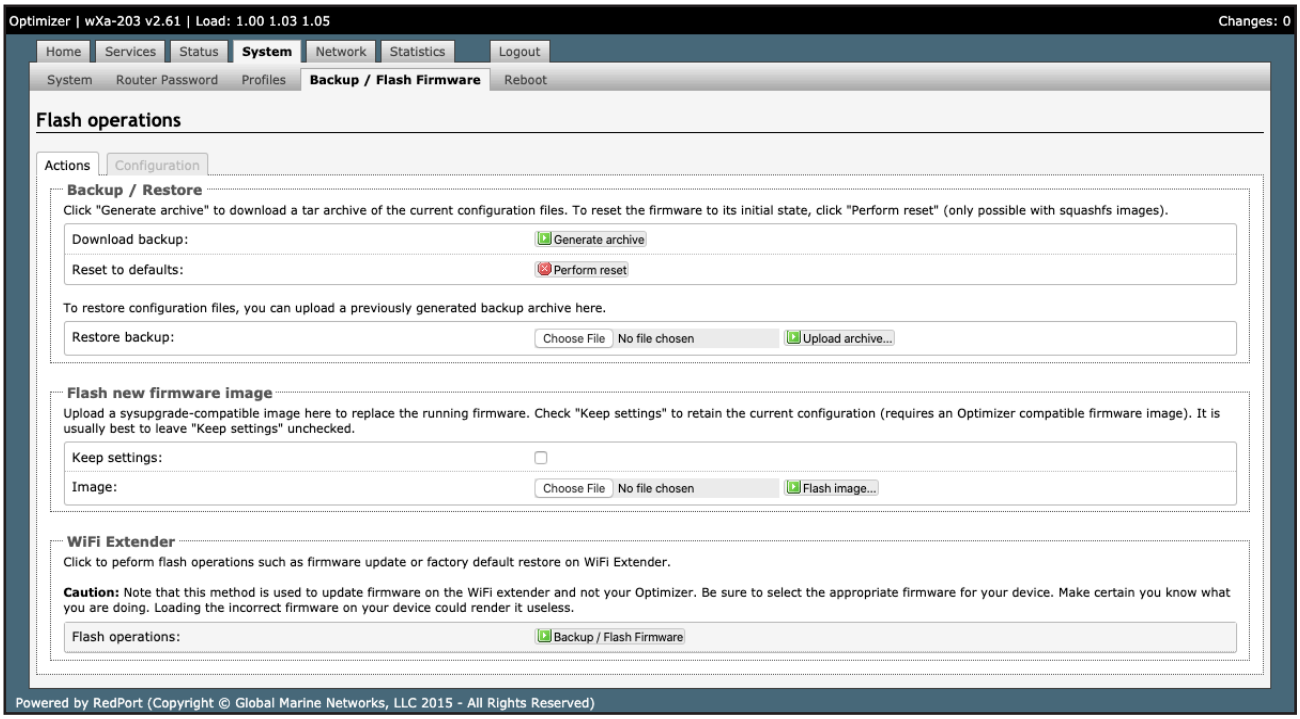
Get the latest Optimizer firmware version from here:

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.



1. Keep Settings: remove the check in the box to uncheck Keep Settings.

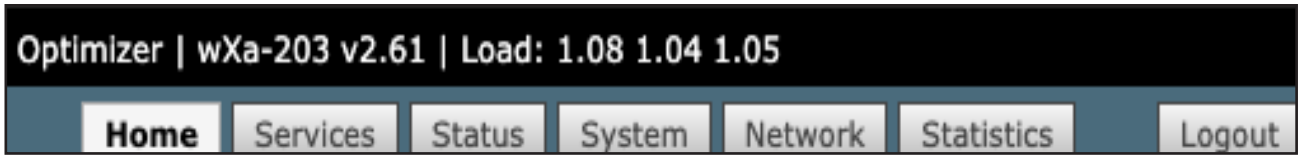
2. <Browse> to where you saved the .bin file and Click that file.

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.

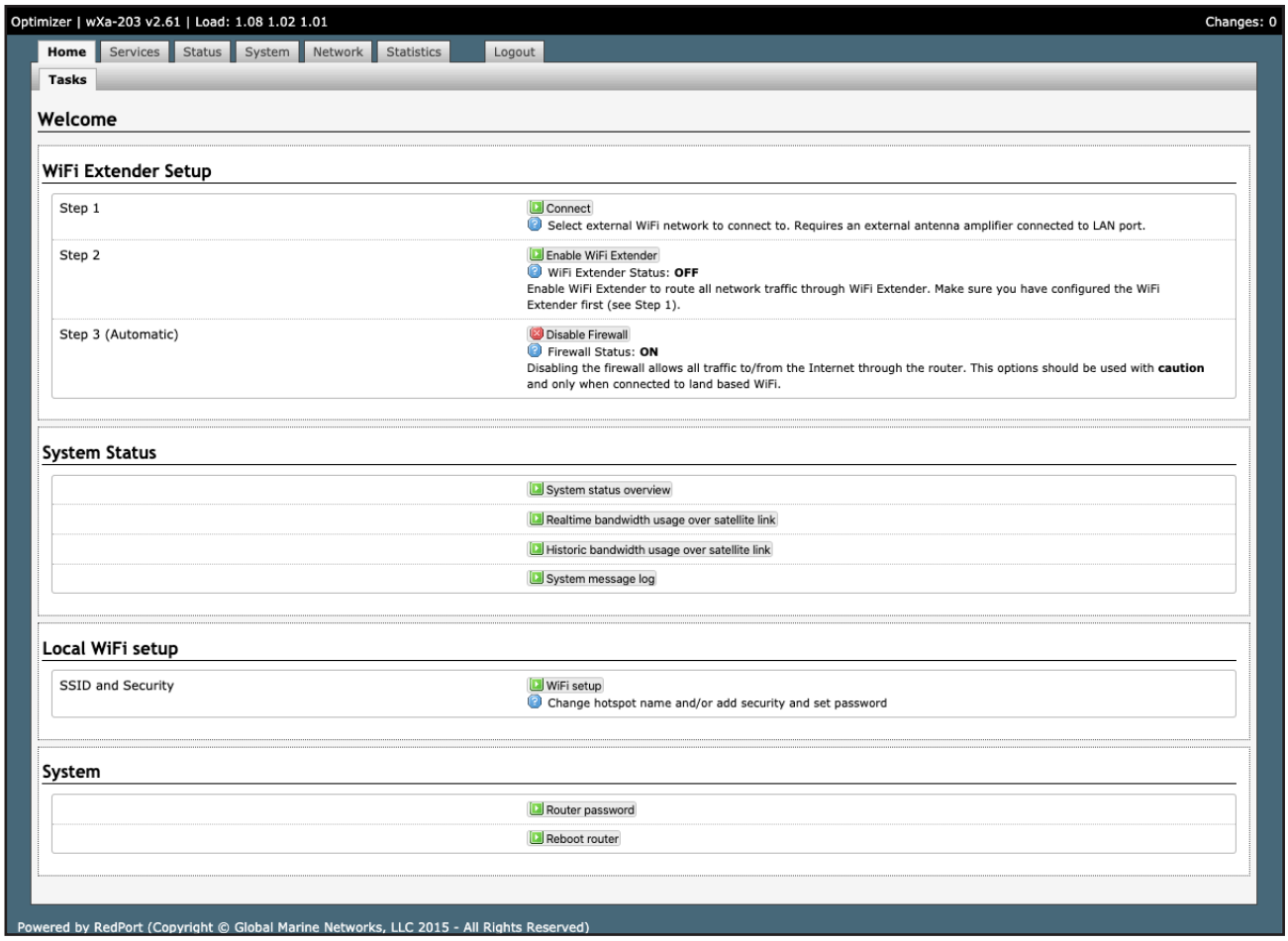
© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



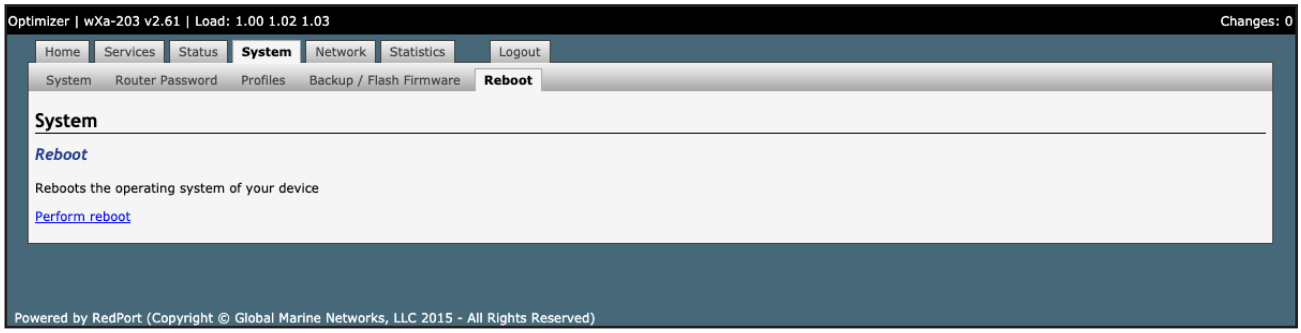
7.4. Reboot the Optimizer Router

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.



2. Click <Reboot Router>.



© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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).

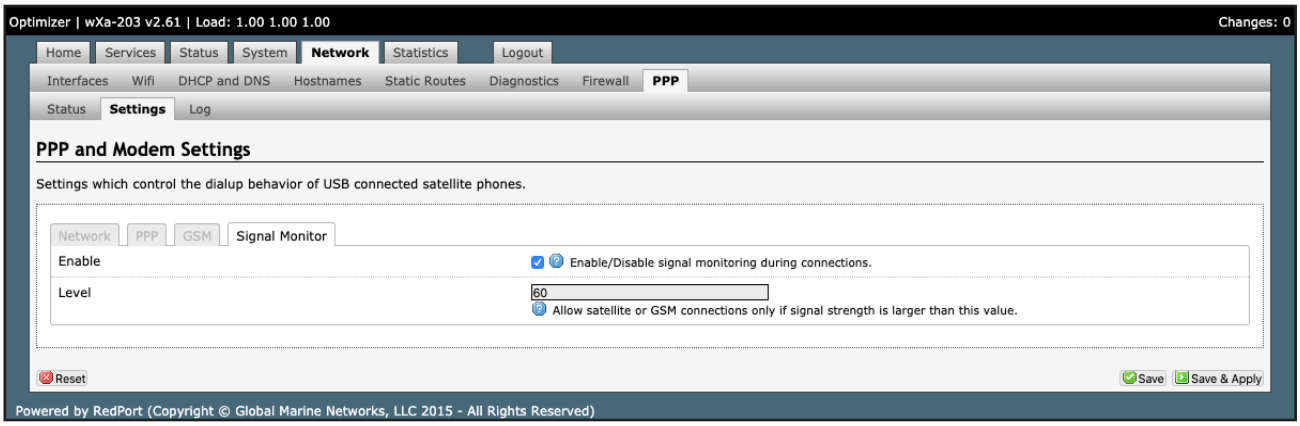
8. Network

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.



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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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.

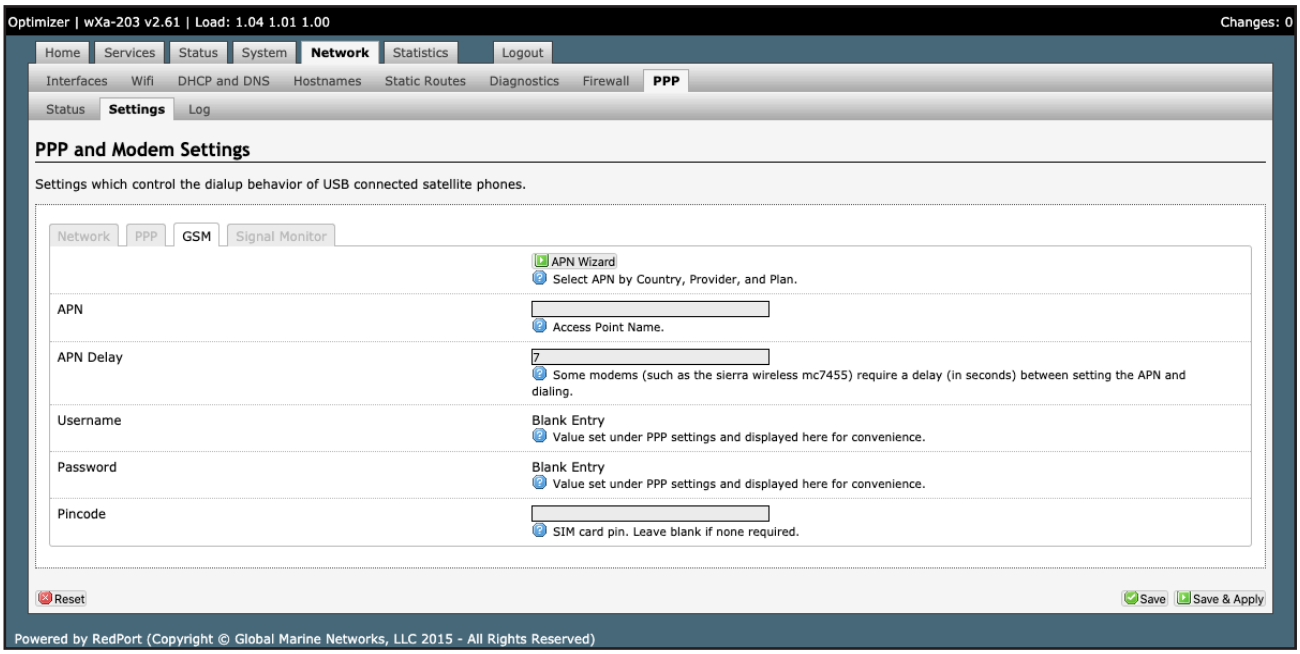
8.2.1. GSM Configuration in Optimizer

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.



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

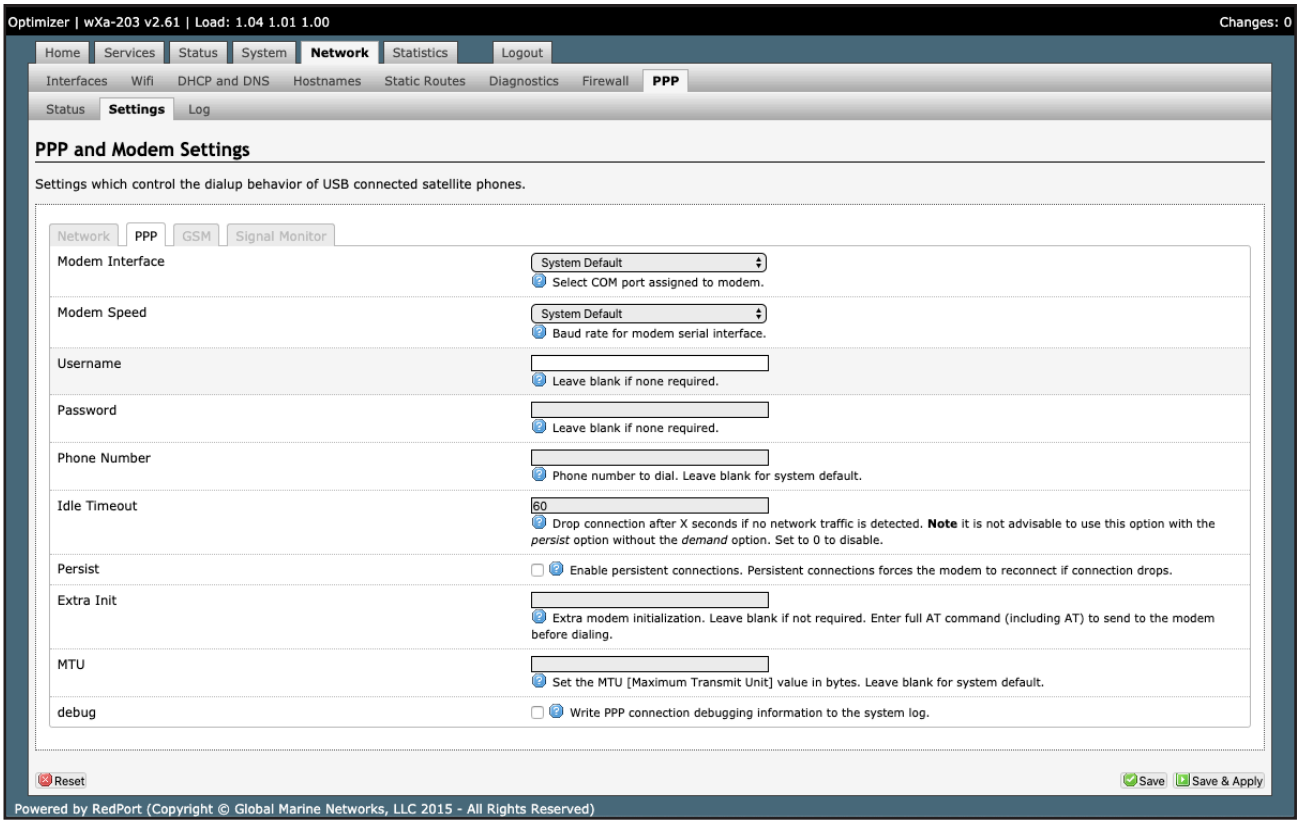
2. If you have protected your cellular SIM card with a pincode, enter the pincode here.

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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



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

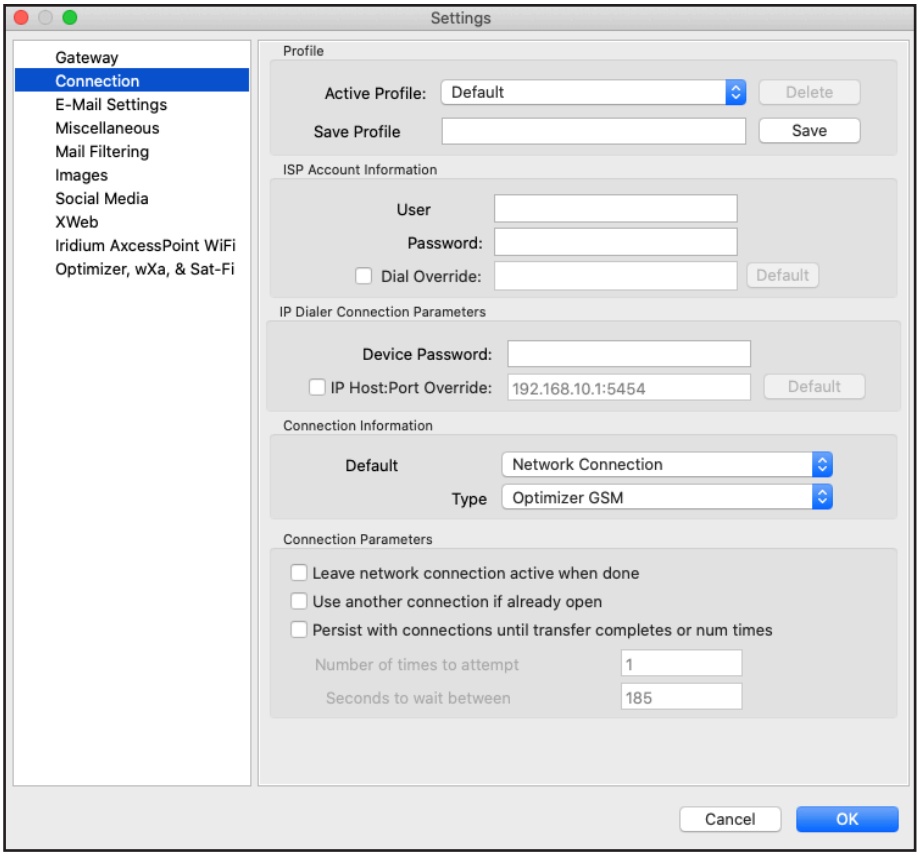
When you want to use GSM service instead of satellite service:

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

© 2020 RedPort Global | Powered by Pivotel America Inc. | All Rights Reserved.



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.

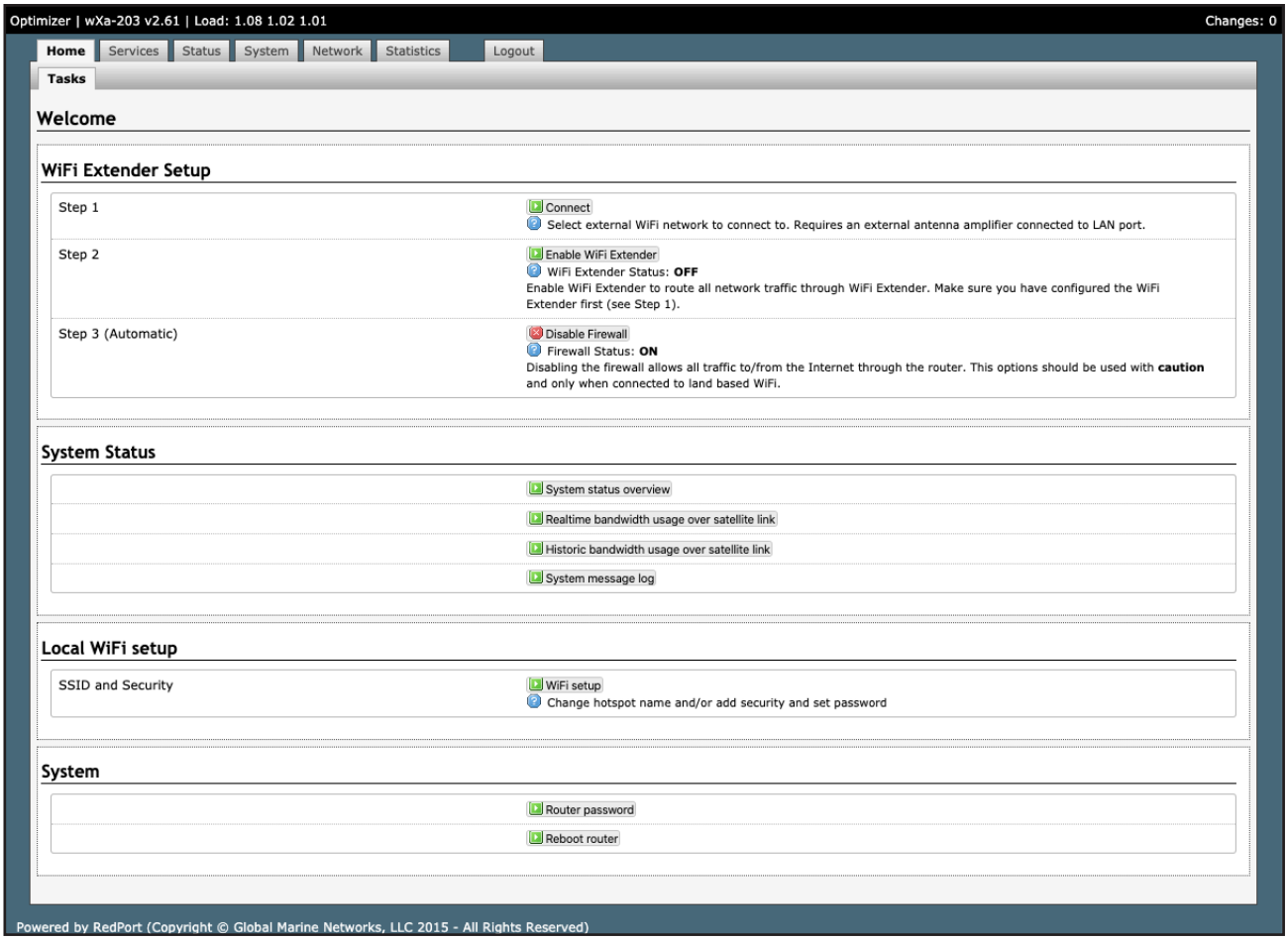
8.3. Restrict Wireless Network Access (Add or Change Network Password)

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.

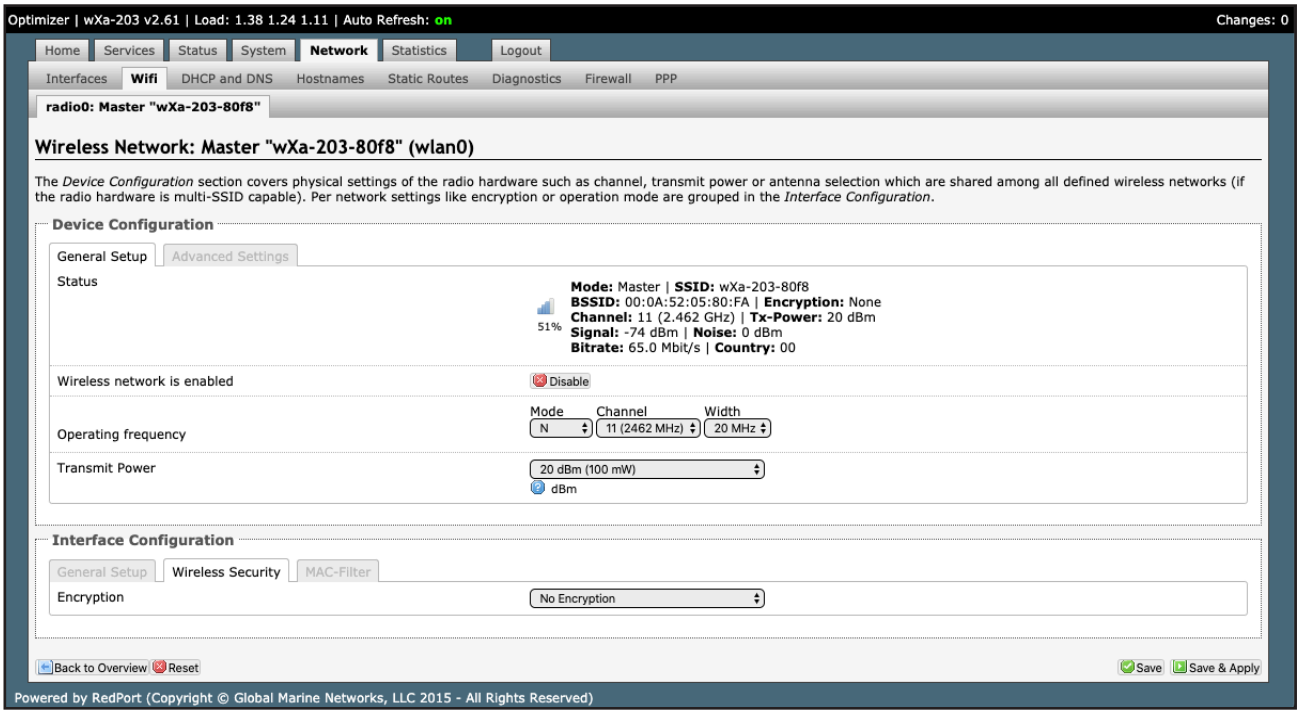
Add/change a password to the Wi-Fi Hotspot (wXa-203-xxxx).

1. Login to the Optimizer:

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



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



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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

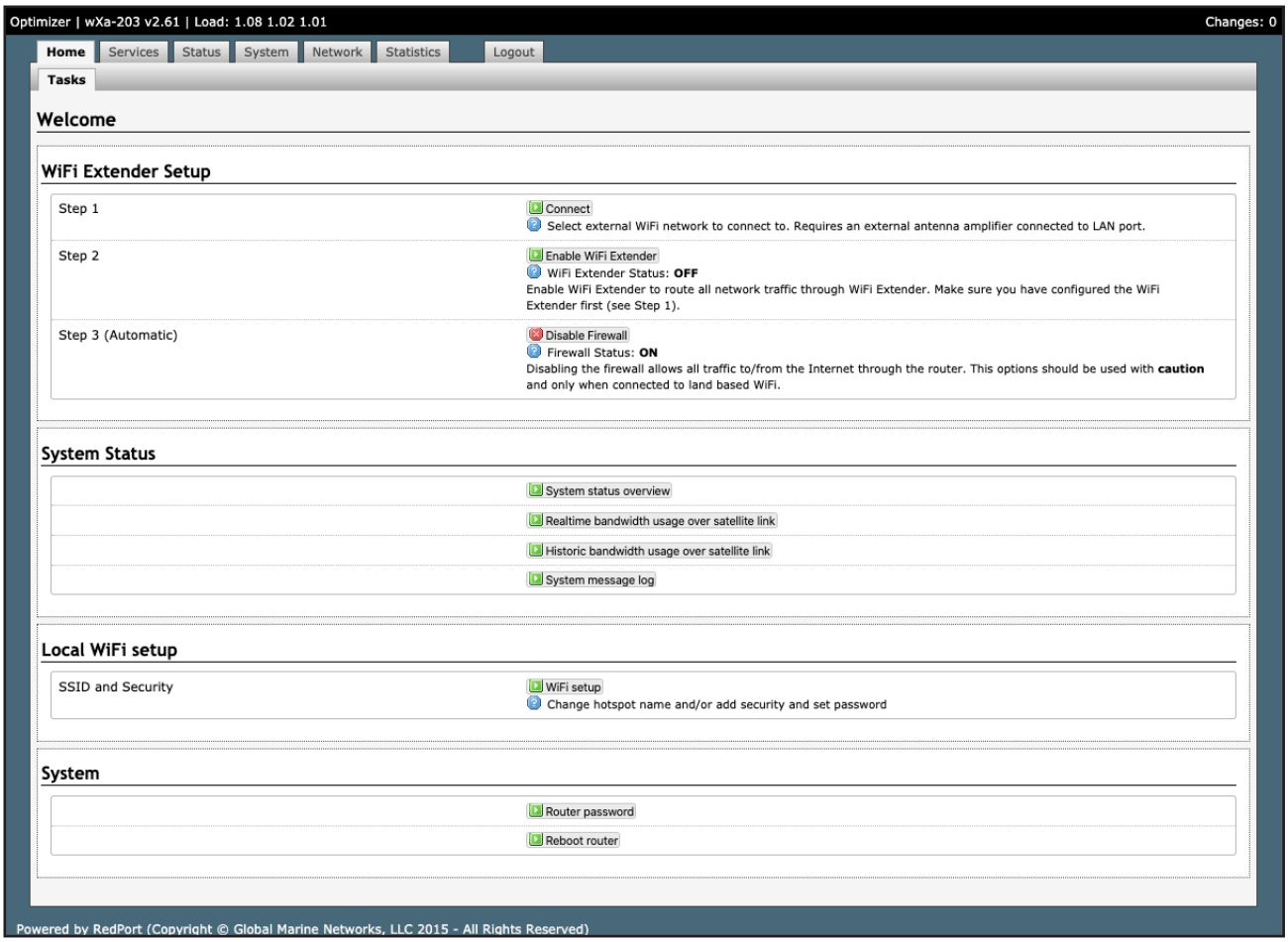
5. Click <Save & Apply>

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)

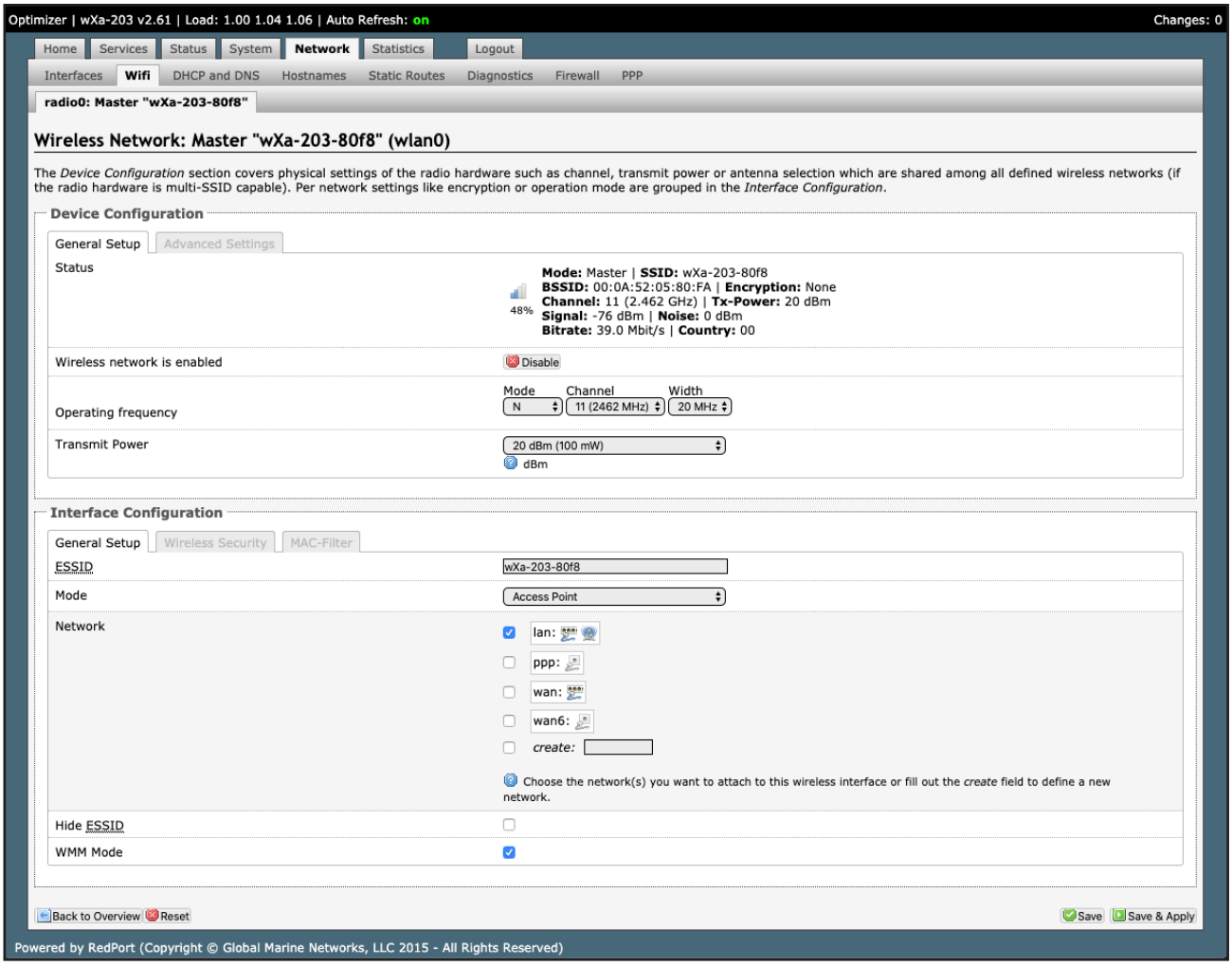
NOTE: Renaming the Wireless Network (SSID Name) will not transfer into a Profile Save as each router needs to have a unique Wireless Network (SSID Name) to avoid network conflict.

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.



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

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



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.

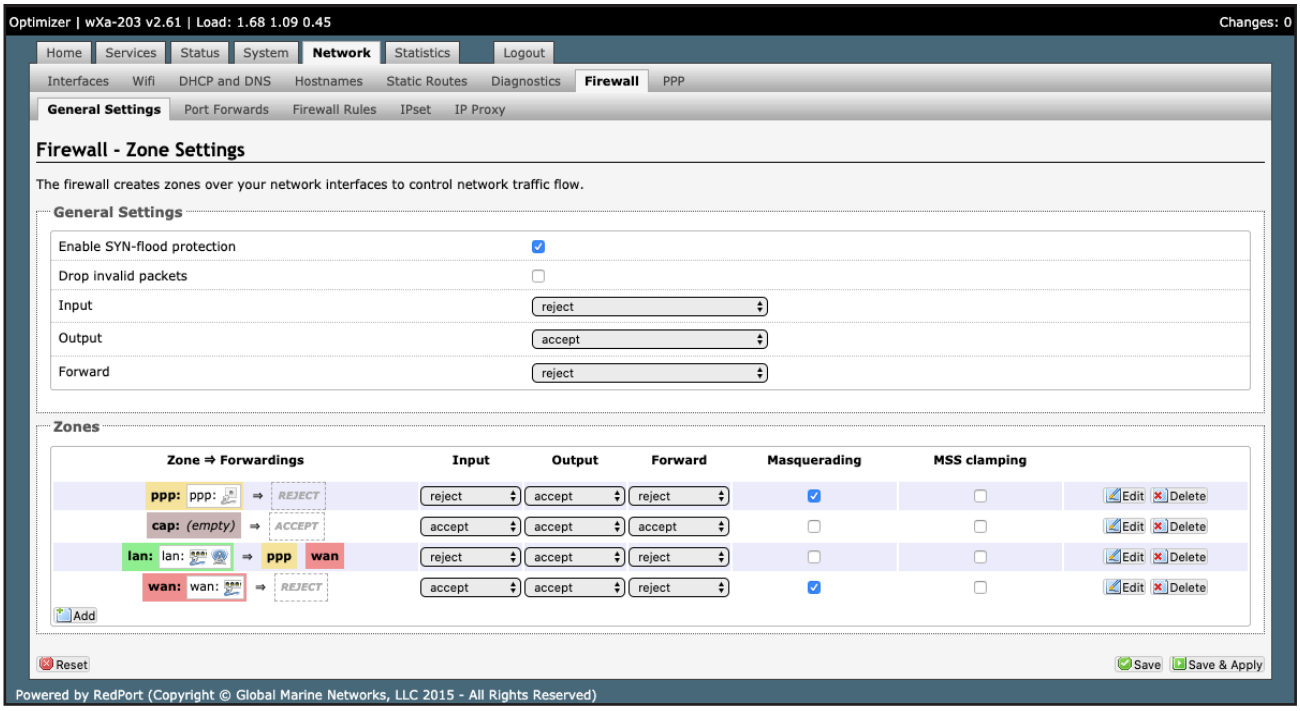
The Firewall allows you to control network traffic flow, allow port forwarding for remote access, has a table of pre-defined traffic rules, and allows you to edit existing rules and create new rules. Most installations do not require any firewall.

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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



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.

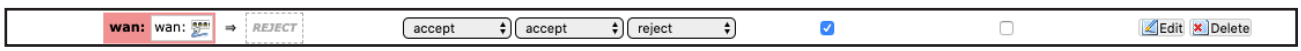
Drop: this setting drops the traffic with no indication to the end user.

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

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.

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.

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.

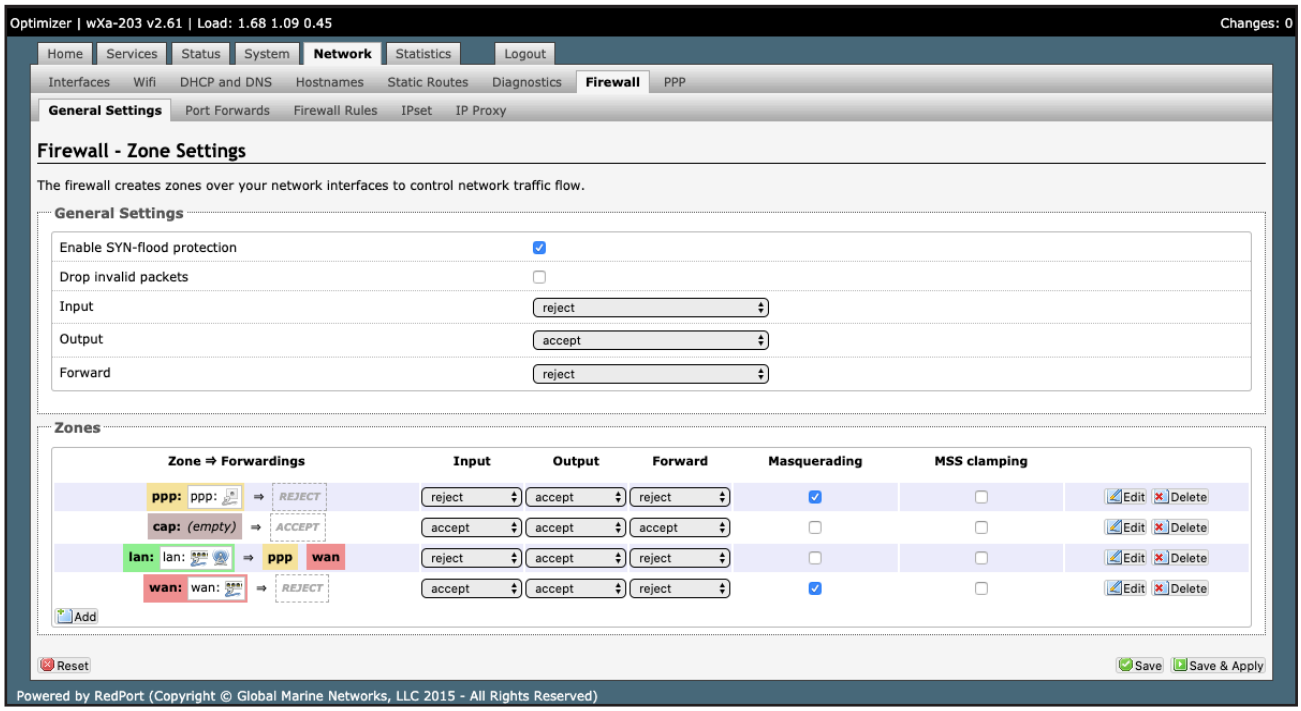


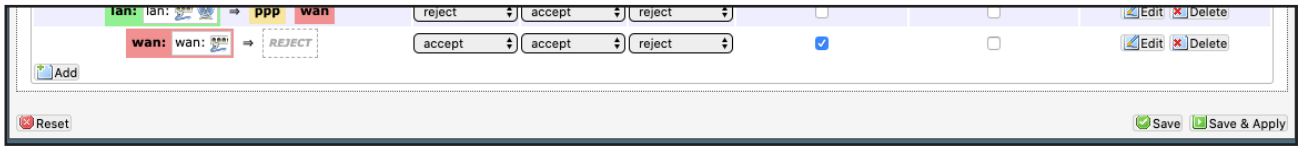
The “wan” firewall zone has the wan interface assigned to it. This is the zone for satellite connections and Wi-Fi extenders. In this default configuration, only Output traffic is allowed.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

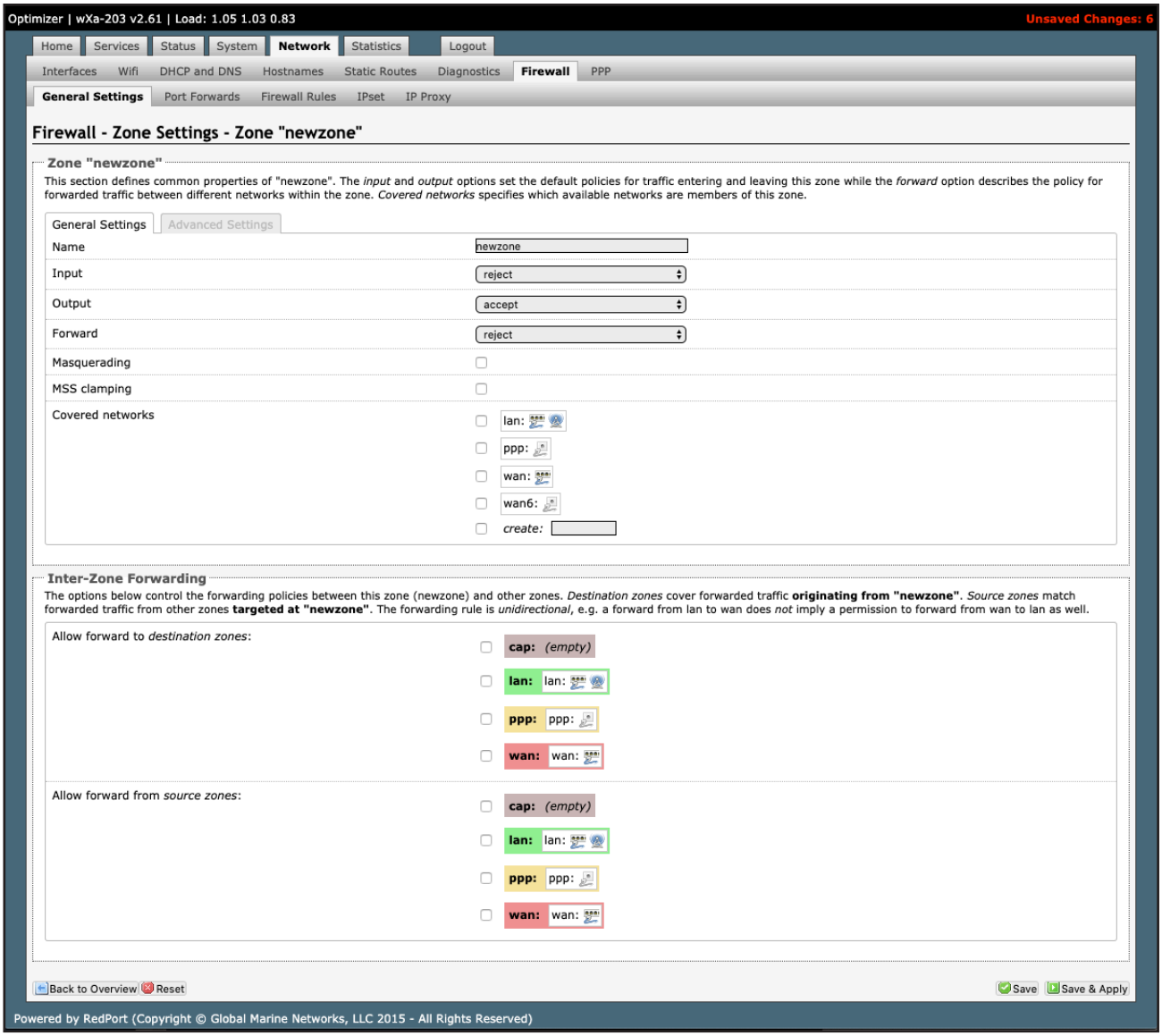
8.5.2. Add a Firewall Zone

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





© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



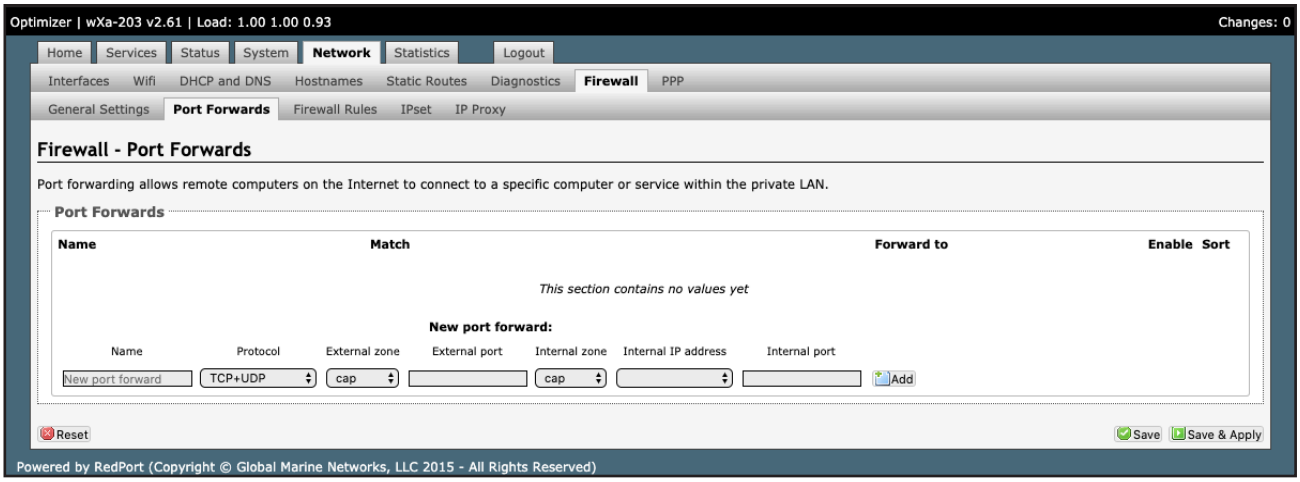
Enter the desired General and Advanced Settings. Click <Save & Apply>.

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.

© 2020 RedPort Global | Powered by Pivotel America Inc. | All Rights Reserved.



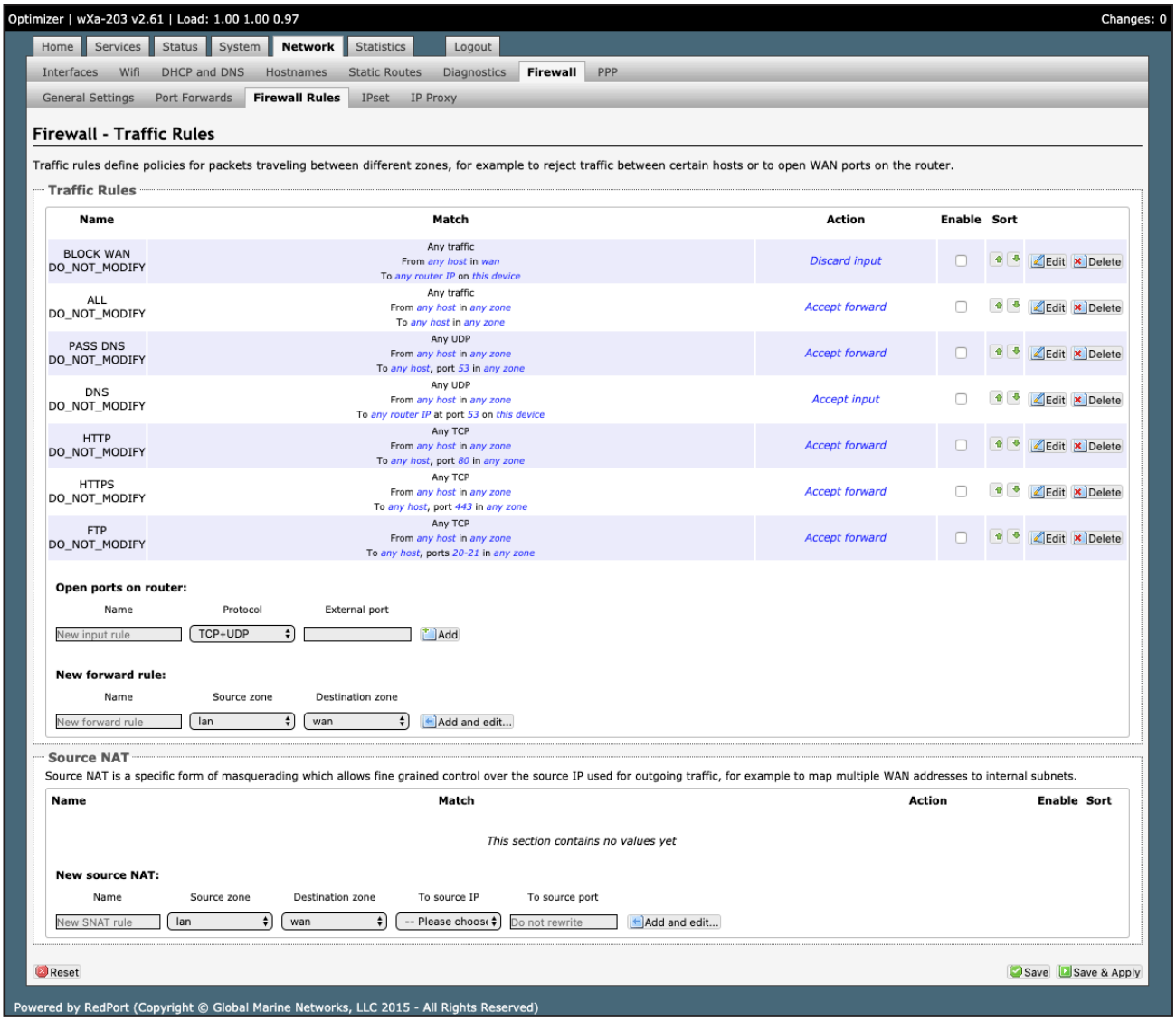
This page shows a list of the enabled port forwards configured. To add a new port forward, enter the desired parameters and click <Add>. To save the configuration, click <Save & Apply>. The new port forward will appear in the list.

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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



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.

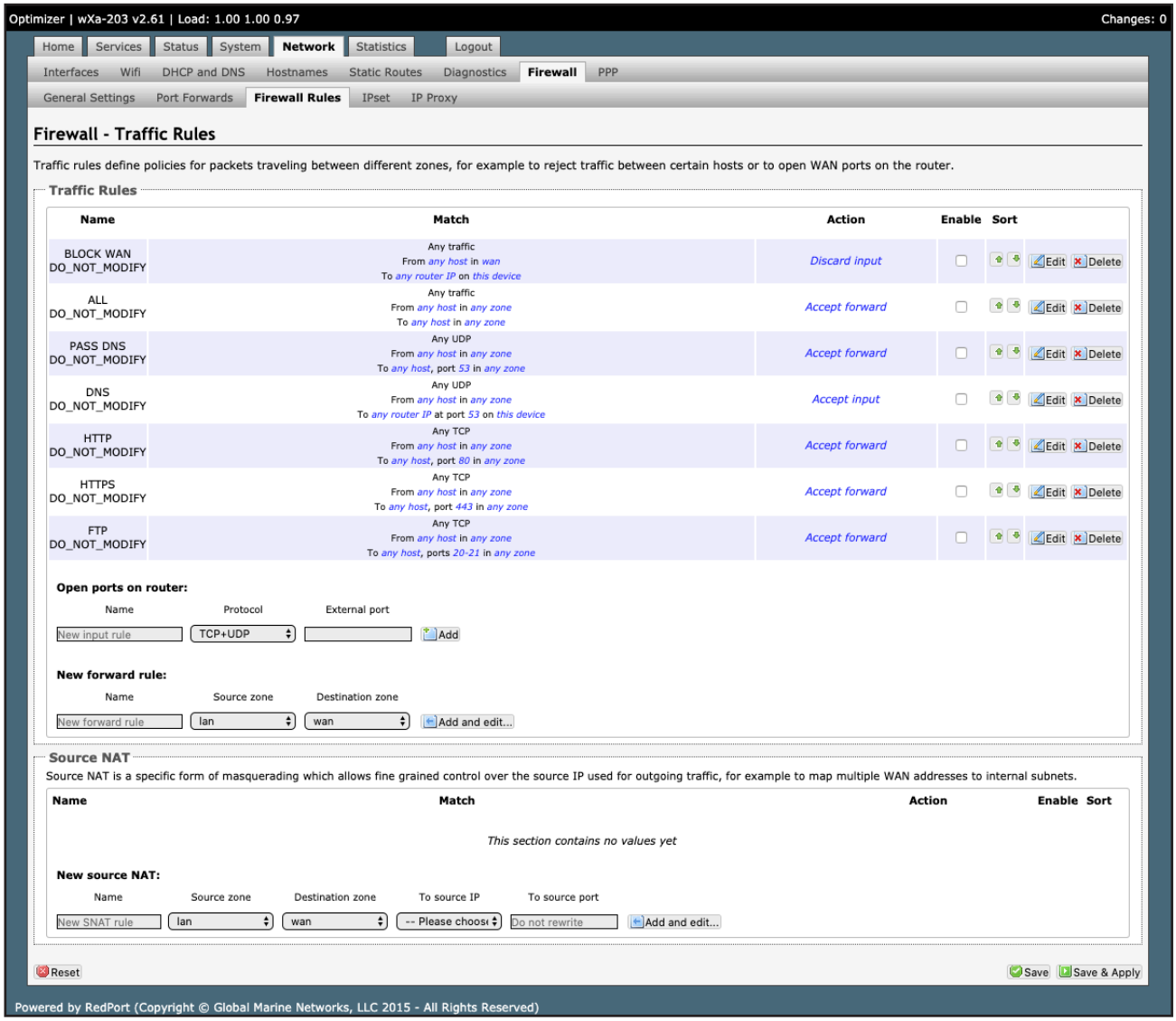
For example, if you want to allow all traffic except http traffic:

- 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.

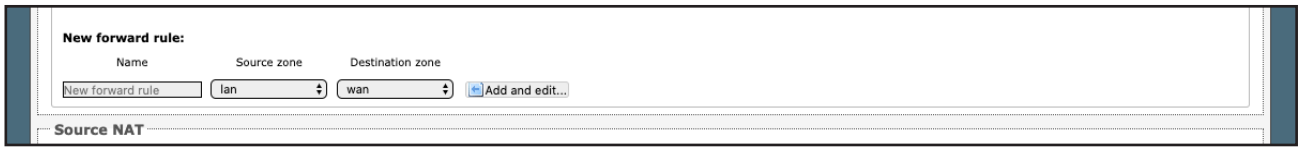
With the ALL rule disabled (unchecked) you can enable/disable the others very quickly. The next one is DNS. Do you want DNS? Yes (checked), No (unchecked). Do you want http? Yes (checked), No (unchecked), etc. You can also create a custom rule.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

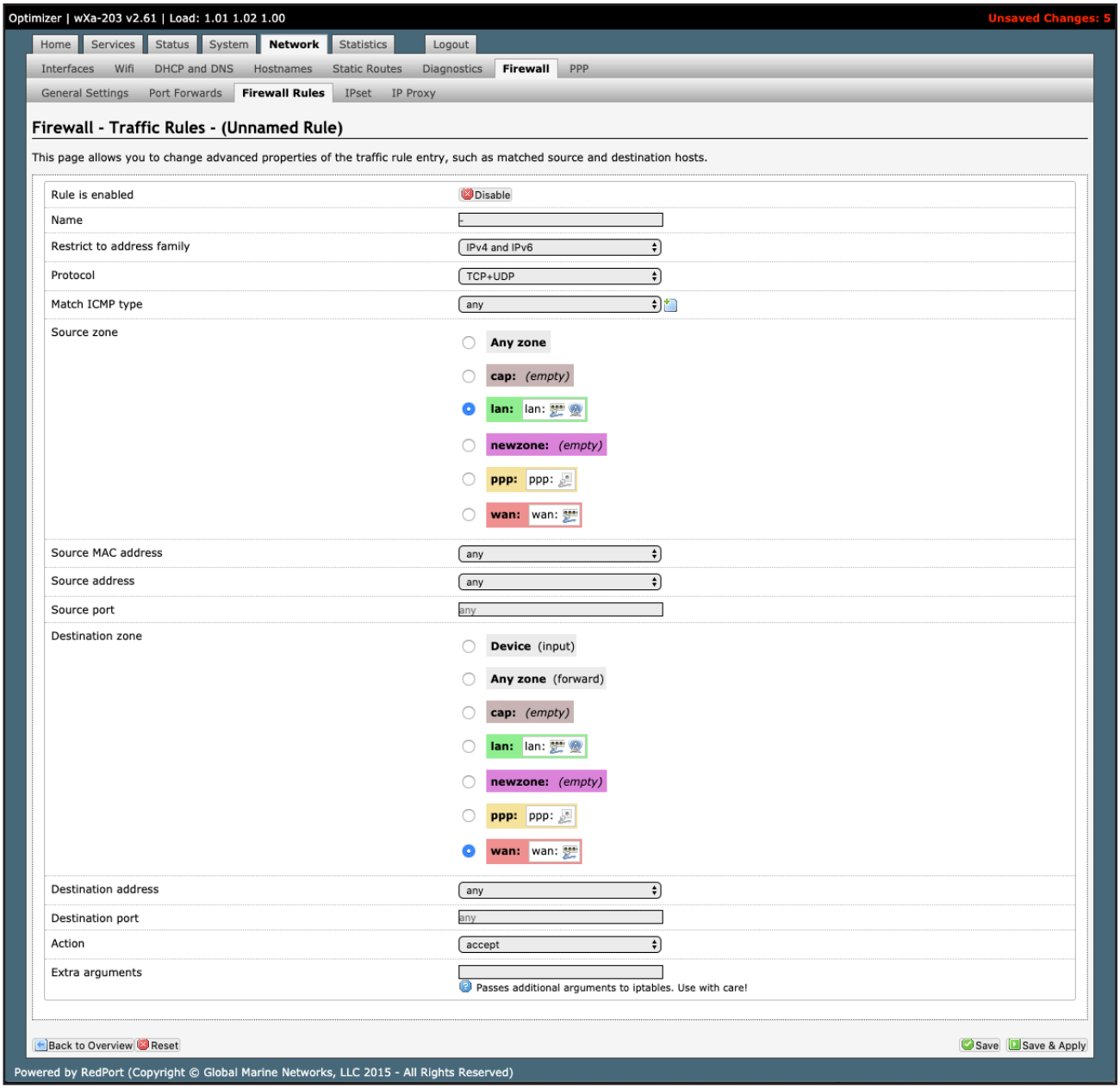
8.5.4.1. Create a Custom Firewall Rule



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



© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



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.

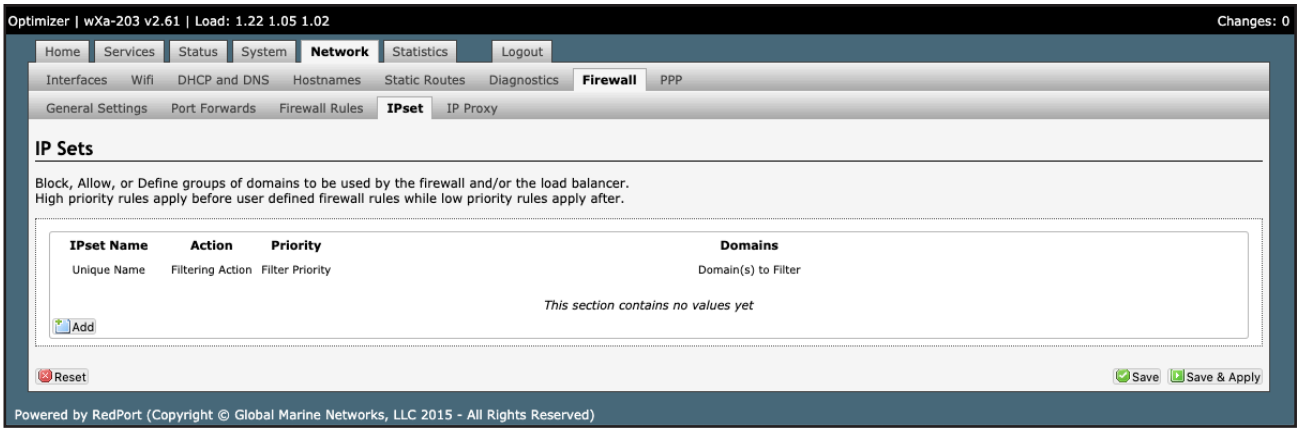
This is a full-featured firewall that you can customize to meet your needs.

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.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



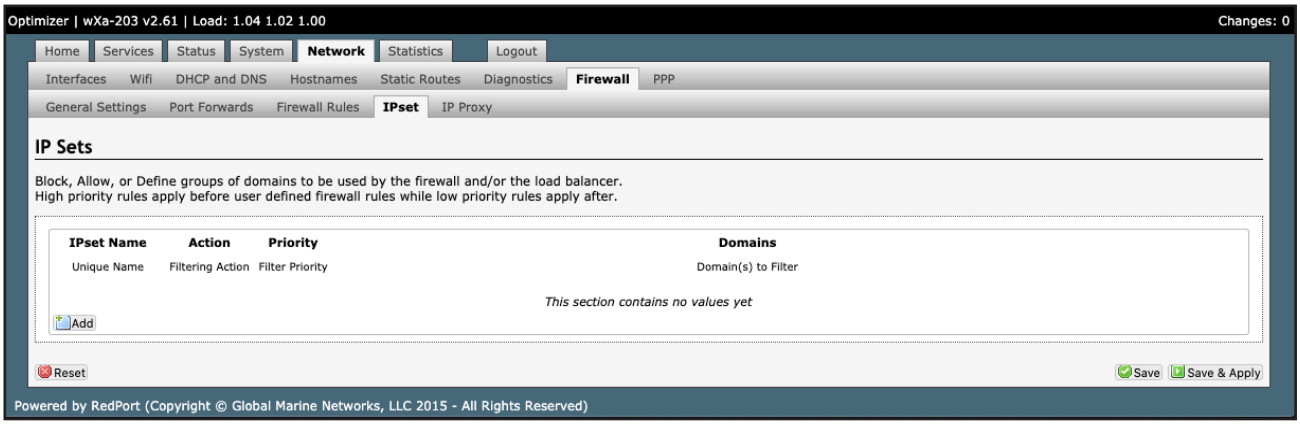
Click <Add> to create a new IP set rule.

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

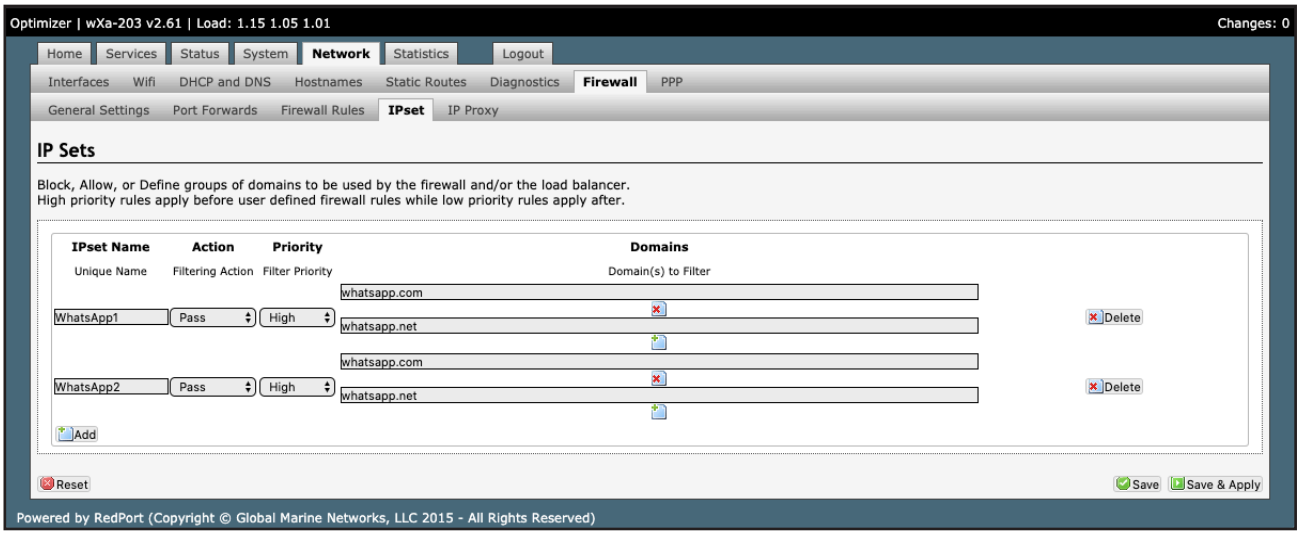
You can group multiple domain names into one IP set rule.

8.5.5.1. IP Sets Example (WhatsApp Configuration)

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



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



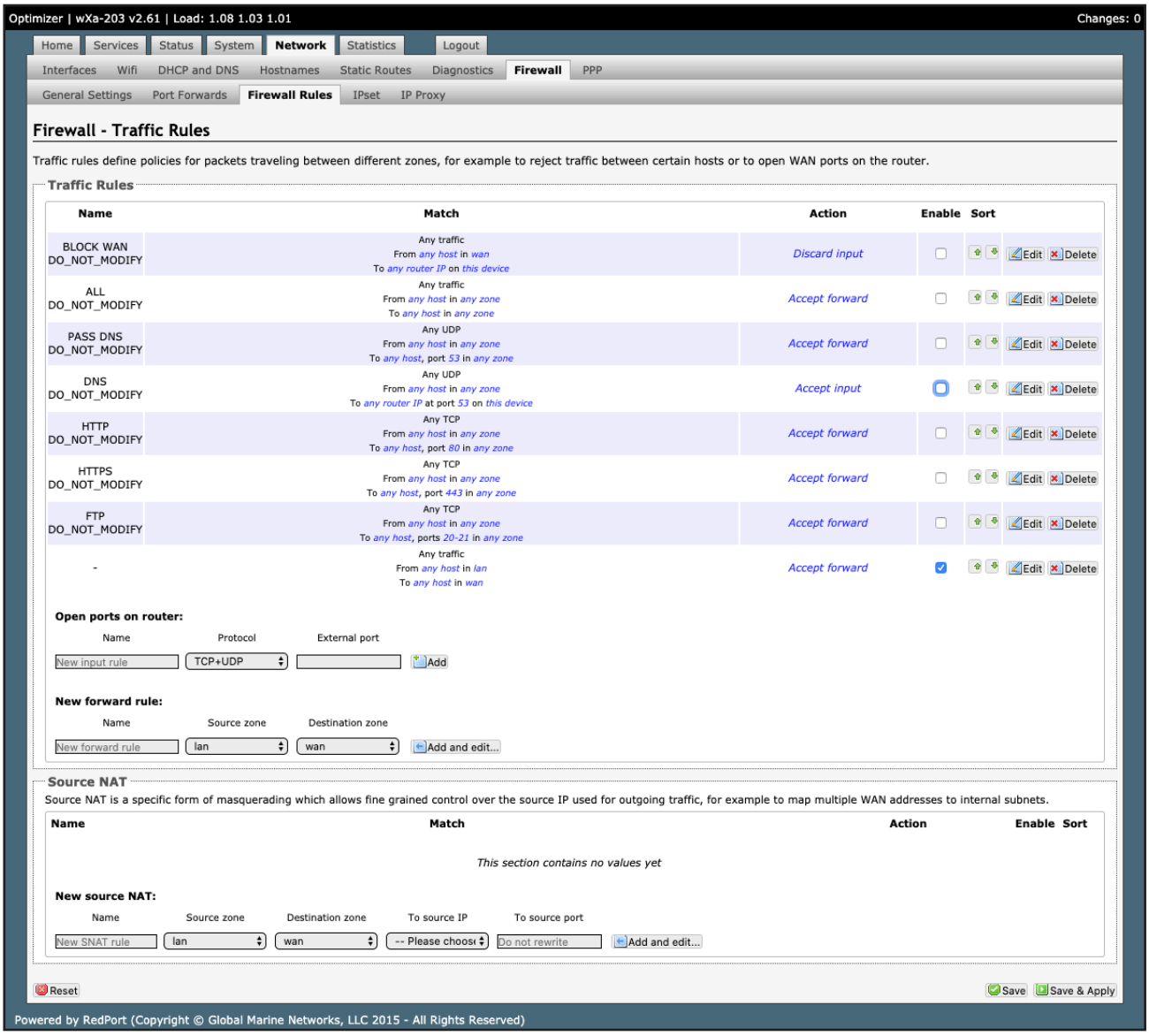
© 2020 RedPort Global | Powered by Pivotel America Inc. | All Rights Reserved.

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

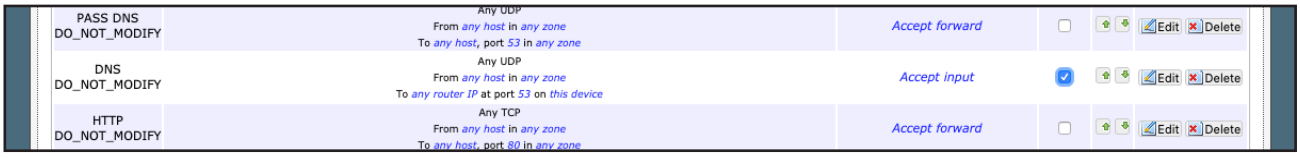
3. For each new IP set rule give each two Domains of whatsapp.com and whatsapp.net.

4. Click <Save & Apply>.

5. Click on the <Firewall Rules> tab.



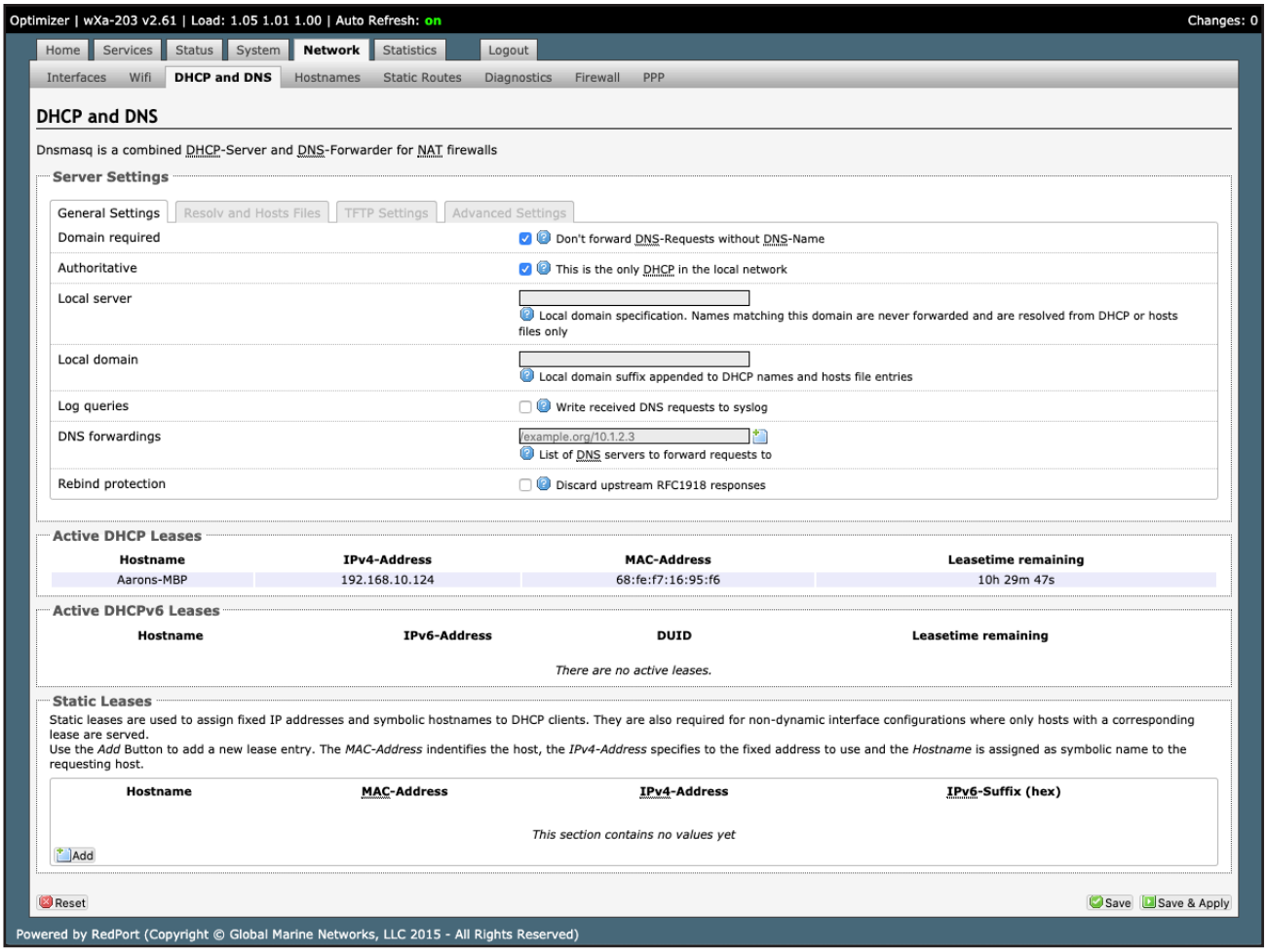
6. Click the checkbox for the DNS traffic Rule (not the Pass DNS traffic Rule).



7. Click <Save & Apply>.

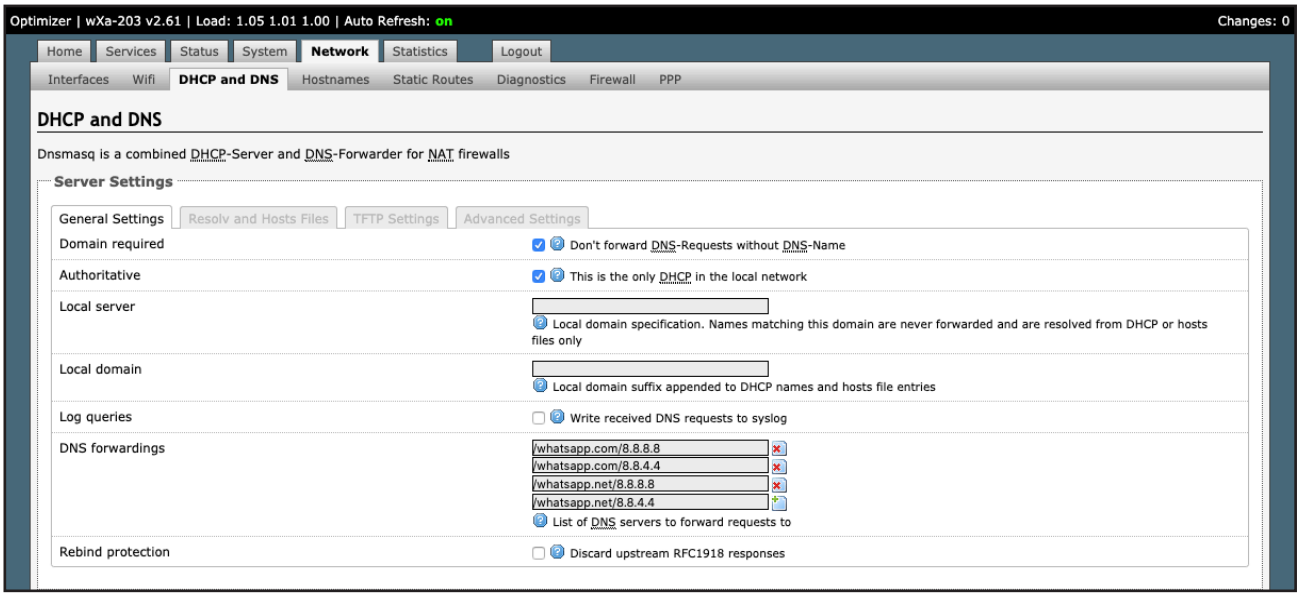
8. Click on the <Network> tab and then click on the <DHCP and DNS> tab.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.



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

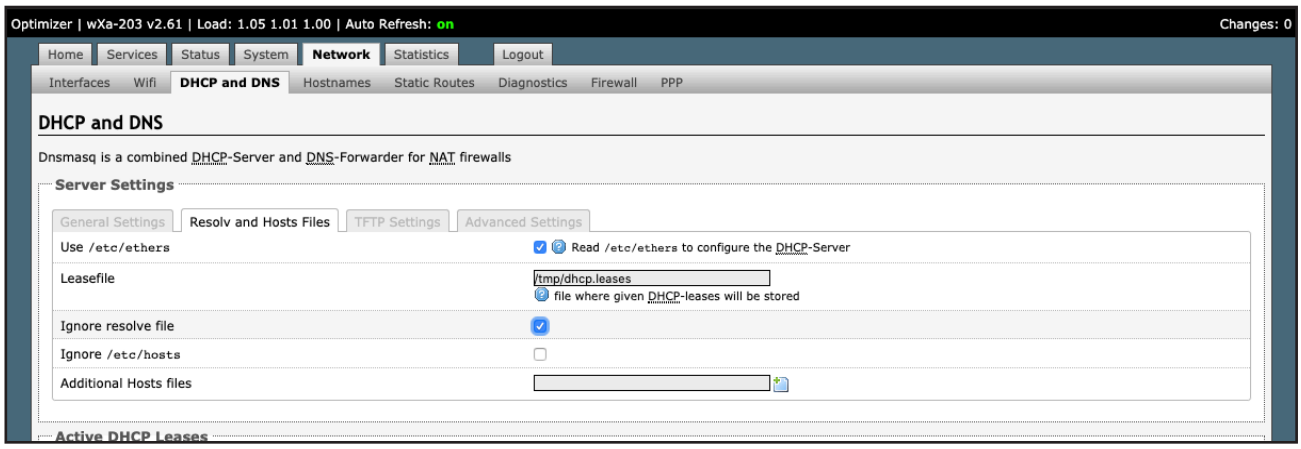
- /whatsapp.com/8.8.8.8
- /whatsapp.com/8.8.4.4
- /whatsapp.net/8.8.8.8
- /whatsapp.net/8.8.4.4



10. Click <Save & Apply>.

© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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

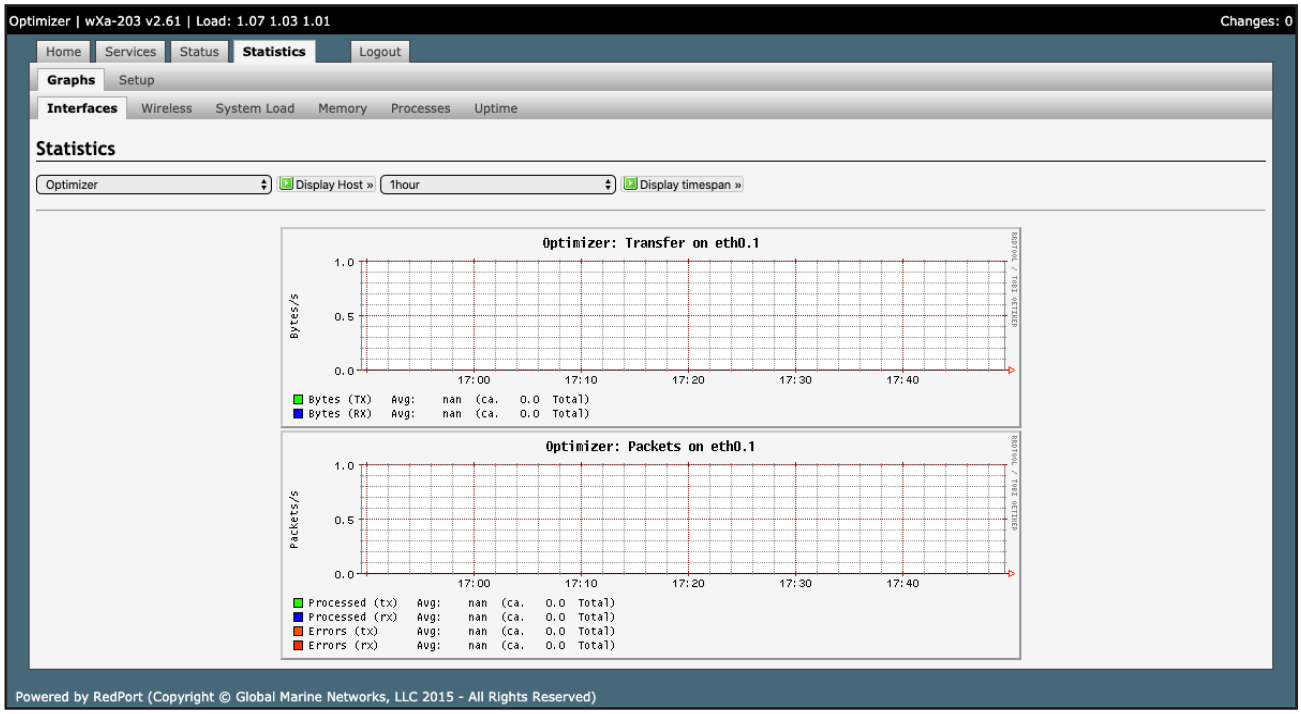


12. Click <Save & Apply>.

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 .



© 2020 RedPort Global I Powered by Pivotel America Inc. I All Rights Reserved.

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

© 2020 RedPort Global I Powered by Pivotel America Inc.
I All Rights Reserved.