RedPort

GMN
Global Marine
NETWORKS

Optimizer Crew

Advanced User's Guide

for Installers/Network Administrators

RedPort Router:
wXa-115 (Optimizer Crew)

RedPort

Table of Contents

1.0 About this guide 07

2.0 Introduction to RedPort Optimizer Crew 08

2.1 Key Features 08

2.2 Services Included 09

2.3 Premium Services Available 09

3.0 Important Things to Know Before Getting Started. 10

3.1 More Than Just a Router 10

3.2 How Data Flows Through the Router 10

3.3 Designed Use of the Optimizer Crew 12

3.4 How It Works At First Launch (out of the box) 12

3.5 Navigating the User Interface 13

4.0 Getting Started - User Interface Access 14

4.1 Access the Home Page 14

4.1.1 Onsite Administrator Login (Admin). 15

4.1.2 Installer/Technician Login (Superadmin) 15

5.0 Services 19

5.1 Crew Internet Services (Captive Portal) 20

5.1.1 Captive Portal Settings 20

5.1.1.1 General Settings 20

5.1.1.2 Advanced Settings 21

5.1.1.3 Allowed Hosts. 22

5.1.1.4 WPAD 23

5.1.2 Allowing Individuals Access to the Internet 24
5.1.2.1 Users with Username and Password. 24
5.1.2.2 Pass-Through MAC 25
5.1.2.3 Pincodes 26
5.1.3 CDRs (Call Data Records) 27
5.1.4 Tools 28
5.1.4.1 Admin Password 28
5.1.4.2 Reset Database to Factory Defaults 28
5.1.4.3 Purge Expired Pincodes 29
5.1.4.4 Purge Unused Pincodes 29
5.1.4.5 Manage Pincodes 29

5.2 Web Compression and Filtering 31
5.2.1 Settings 31
5.2.1.1 Compression 31
5.2.1.2 General Settings 33
5.2.1.3 Advanced Settings 34
5.2.2 Filters 36
5.2.3 Log 38
5.2.4 Help 38

5.3 RedPort Email 40
5.3.1 Enable and Configure RedPort Email 41
5.3.2 Primary Accounts 43

5.4 GPS Tracking 44
5.4.1 Tracking Powered by GSatTrack 44
5.4.2 Tracking via SMS 46

5.5 WiFi Extender. 47

5.6 GPS/NMEA Repeater. 48
5.6.1 Equipment Setup 49
5.6.1.1 Broadband Satellite Terminal with Integrated GPS . . 49
5.6.1.2 Handheld Satellite Phone with Integrated GPS . . 50
5.6.1.3 USB NMEA Device 51
5.6.1.4 RS-232 NMEA Device 52
5.6.1.5 Connecting Multiple NMEA Devices 53
5.6.2 GPS/NMEA Repeater Parameters Configuration . . . 54

5.7 PPP 56
5.7.1 PPP Configuration for Use w/USB Connected Satellite Device . 57
5.7.2 Signal Monitor 58
5.7.3 GSM 59
5.7.3.1 GSM Configuration in Optimizer 59
5.7.3.2 Using GSM 62
5.7.3.3 Changing from GSM Service to Satellite Service . . 63

6.0 Status 64

7.0 System 65
7.1 Change Router Password 65
7.2 Profiles 66
7.2.1 Add a Profile 66
7.2.2 Change to Another Saved Profile 67
7.2.3 Export a Profile 68
7.2.4 Import a Profile 69
7.3 Backup/Flash Firmware 70
7.4 Reboot 72

8.0 Network 73
8.1 Rename the Wireless Network 73
8.2 Restrict Wireless Network Access 75
8.3 Firewall 77
8.4 Diagnostics 80

9.0 Statistics 81

Appendix A - RedPort Optimizer Crew Installation Guide 83
Appendix B - Installer Guidlines for Customization 89
Appendix C - Table of Login Access 90

RedPort

Revision History

Date	Revision	Author
May 01, 2015	Initial Release	D. Brickhouse

1.0 About this Guide

This guide is intended for installers and network administrators of the RedPort Optimizer Crew wXa-115 router. It features only those sections of the user interface that require configuration for a specific service or may need to be accessed to perform a specific function.

During normal daily operation, there is no need to access the full user interface that you see here. A separate document is designed for use by the onsite administrator that includes the login to the Home Page for access to the common tasks that will be used locally: generate pincodes, create users, and look at call data records for the Captive Portal, create and manage crew email accounts, etc. *See the Optimizer Crew Basic User Guide for details.*

For information regarding the installation of the hardware, please see the *RedPort Optimizer Crew Installation Guide in Appendix A of this document*.

wXa refers to the webXaccelerator by RedPort, a trademark of Global Marine Networks, LLC.

2.0 Introduction to the Optimizer Crew

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. The company's products include XGate high-speed satellite email, WeatherNet weather and oceanographic data software, and vessel tracking systems.

Ship to shore network management solutions are sold by GMN under the RedPort Global brand name at www.redportglobal.com and as white-label solutions for the world's premier satellite data service providers.

Optimizer Crew is a satellite WiFi router that provides all you need for multi-person networking on most satellite broadband installations and lets you easily share and control access to your satellite broadband data service via its WiFi or Ethernet network. It is more than just a router; it has some enhanced proxy services plus some basic routing capabilities.

2.1 Key Features

Designed specifically for use with satellite broadband terminals:

- Compatible with virtually any IP-based satellite broadband terminal.
- Replaces a standard router that is typically added to any satellite broadband installation.
- Powerful firewall accommodates virtually 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 Captive Portal Service for Crew Internet Access
- Supports RedPort Email Service
- 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 WiFi.

2.2 Services Included

The following services are included:

- Captive Portal for Crew Internet Access – generate PIN codes that can be given away or sold to crew and/or passengers to control web access. See Chapter 5.1.

- 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. See Chapter 5.7.

2.3 Premium Services Available

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

RedPort Email – is a multi-user satellite email service. Crew and/or passengers can access their RedPort Email account via smartphones, tablets or computers. See Chapter 5.3 and the *RedPort Email Administrator's Guide* for more information.

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. See Chapter 5.2 and the *RedPort Optimizer Crew Installation Guide* for more information.

GPS Tracking - Using a GPS-enabled device, submit position reports to a central database for viewing on the tracking website. See Chapter 5.5.

3.0 Important Things to Know Before Getting Started

3.1 More Than Just a Router

The Optimizer Crew is more than just a router. It has some enhanced proxy services in addition to basic routing capabilities. There are three major data components:

1. Captive Portal - when enabled, it blocks access to the Internet without authentication. Authentication can be via username and password or pincode or Mac address of a specific PC. The Captive Portal is enabled by default so one of the first things you want to do is change the captive portal password and add user accounts.

2. Proxy Server(s) - Internal Transparent proxy is enabled by default. 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.

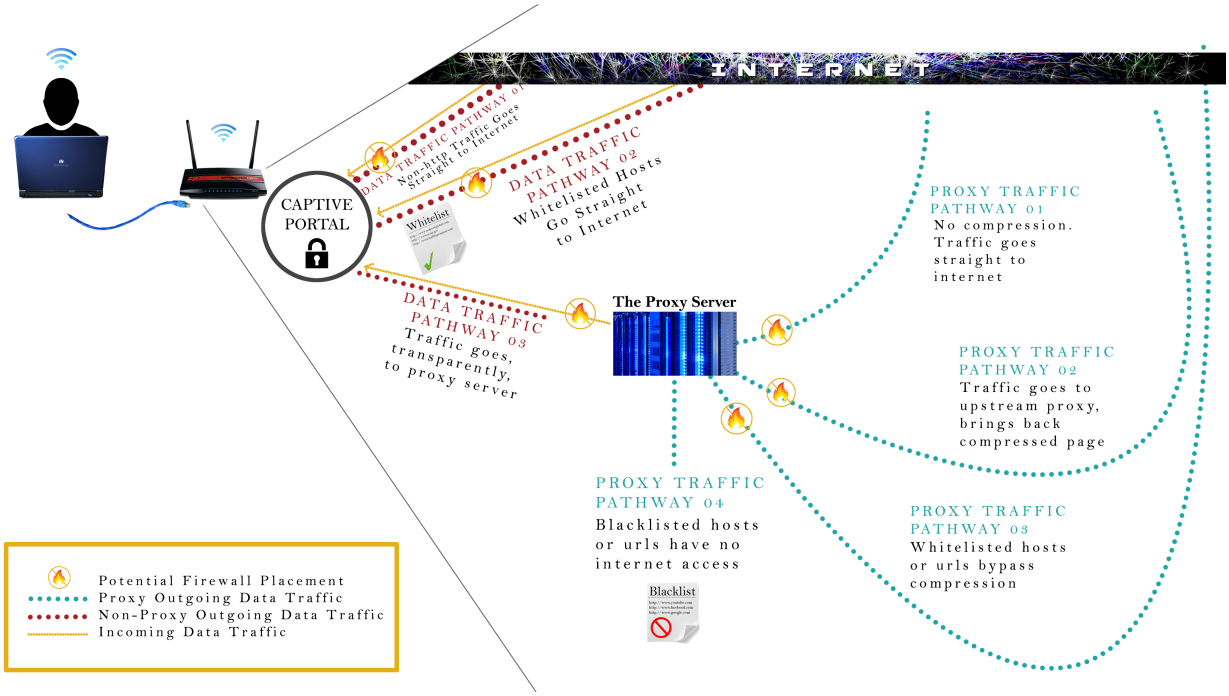
3. Firewall - A full-featured firewall is included. Block or allow IP address/ranges, port ranges, different protocols. Rules can be applied to any path in and out of the router.

3.2 How Data Flows Through the Router

It is important to understand how data flows through the router so you can customize your configuration.

The default configuration is:
Captive portal - enabled, allowing crew Internet access
Internal Transparent Proxy - enabled for http URL and content filtering
Web Compression - disabled
Firewall - open, allowing full access to the Internet once logged into the captive portal
DNS - open, allowing resolutions of IP address for all devices on the LAN/WiFi whether logged in or not through the captive portal
RedPort Email - disabled
GPS Tracking - disabled

Once a user logs in to the Captive Portal, data can take one of three paths:



1. Non-http traffic goes straight to the Internet: https, dns lookups, ftp, ping, scp, etc. The firewall rules are totally open so there is nothing blocking full access to the Internet. You can limit access thru the Captive Portal. See Chapter 5.1.2 for details.

2. Traffic to a Whitelisted Host in the Captive Portal, including http, goes straight to the Internet, bypassing the internal proxy server. If you whitelist a webserver, that traffic goes straight to the Internet, bypassing the internal proxy server, so there is no filtering. Typically you would not want to whitelist a webserver; however, you may want to whitelist a mail server, or a vpn. See Chapter 5.1.1.3 for details.

3. All http traffic (on port 80), that is not Whitelisted, and only http (not https or secure traffic) is intercepted and redirected to the internal proxy server. This is known as transparent proxy. The internal proxy server does URL blocking and domain blocking. Also, the internal proxy server can speak to an upstream proxy server to provide compression (premium service--fees apply). Traffic through the internal proxy server can take one of several paths, dependent upon whether or not compression is enabled.

- If compression is disabled all traffic goes straight to the Internet.
- With compression enabled, all http traffic goes to the upstream compression proxy server and returns a compressed page. Ads are stripped out, text is compressed, images are resampled and more. On average, you will experience 3-5x compression on

http traffic, thereby increasing the speed of your connection and your effective per Mb cost of your connection.

- With compression enabled, Whitelisted Hosts or URLs bypass the upstream compression proxy server and go straight to the Internet, bypassing compression.
- Blacklisted Hosts or URLs have no Internet access, regardless of compression status.

See Chapter 5.2.2 for details.

3.3 Designed Use of the Optimizer Crew

This is a single-user router for use in a multi-user environment. The idea is that you 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: generate pincodes, create users, look at call data records for the Captive Portal, create and manage crew email accounts, etc.

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 Crew Basic User Guide.*

3.4 How It Works At First Launch (Out Of The Box)

We ship the router with the Captive Portal ON and with Internal Transparent Proxy ENABLED.

This means that the onsite administrator can immediately start creating pincodes for Internet access, limit the amount of data users are transferring and track how much data they are using.

By default, you get some performance mainly in terms of monitoring and blocking using the captive portal and using the internal proxy server. This out-of-the-box scenario works well for broadband users with high data plans.

It is not the best setup, however, for those on low data plans because of the high price per megabyte of data. DNS is enabled, by default, which generates a lot of traffic and there is no compression. Therefore, users will deplete their pincodes quickly because as soon as they enter their pincode Windows will update and every other internet-aware program on their computer wants to go on the Internet.

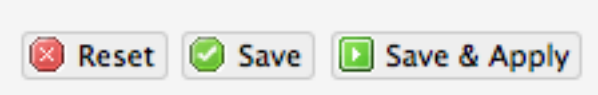
Best Practice is to have a knowledgeable technician (someone who knows about proxy servers and routers) go through and generate a custom configuration, enable the firewall to block unwanted traffic, configure the internal proxy server to tune things, and enable the upstream proxy so you have the benefit and cost savings of compression. This custom configuration can be recorded and used on other Optimizer Crew routers within the organization.

3.5 Navigating the User Interface

Access to the user interface depends upon how you login to the router. There are two logins available: admin and superadmin. See Chapter 4.1.

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.

4.0 Getting Started - User Interface Access

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

- Captive Portal for Crew Internet Access
- Internal Transparent Proxy for Web Filtering

There are also services available that are disabled:

- Web Compression (additional fees may apply)
- RedPort Email (additional fees may apply)
- GPS Tracking (additional fees may apply)
- GPS/NMEA Repeater

This guide is designed to help you understand how the router works so you can customize the configuration to meet your needs.

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 WiFi Hotspot created by the router using a PC. Connect to the WiFi Hotspot just like you would any other WiFi connection:

    On a Windows PC, go to: Windows Start > Control Panel > Network Connections

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

You will notice that there are two WiFi network names in the list.

    There are two transmitters in the Optimizer Crew with frequencies at 2.54 Ghz and one at 5.2 Ghz.

The Network Name will look something like: 'wxa-115-XXXX-frequency' where 'XXXX' is the last four digits of the Optimizer Crew's Mac address and 'frequency' is the transmission frequency of the transmitter. Select one of these wireless networks.

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

2. Open any web browser on the computer and enter one of the following URL's:

    If Captive Portal is enabled (default): http://10.1.5.1

    If Captive Portal is disabled: http://192.168.10.1

3. The Optimizer Crew 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 Administrator: username=admin, password=webxaccess

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

- generate pincodes for captive portal use
- send/receive email (if email is enabled)
- manage crew email accounts (if email is enabled)
- monitor the system status
- reboot the router, if necessary
- change the router password for the admin account, if necessary

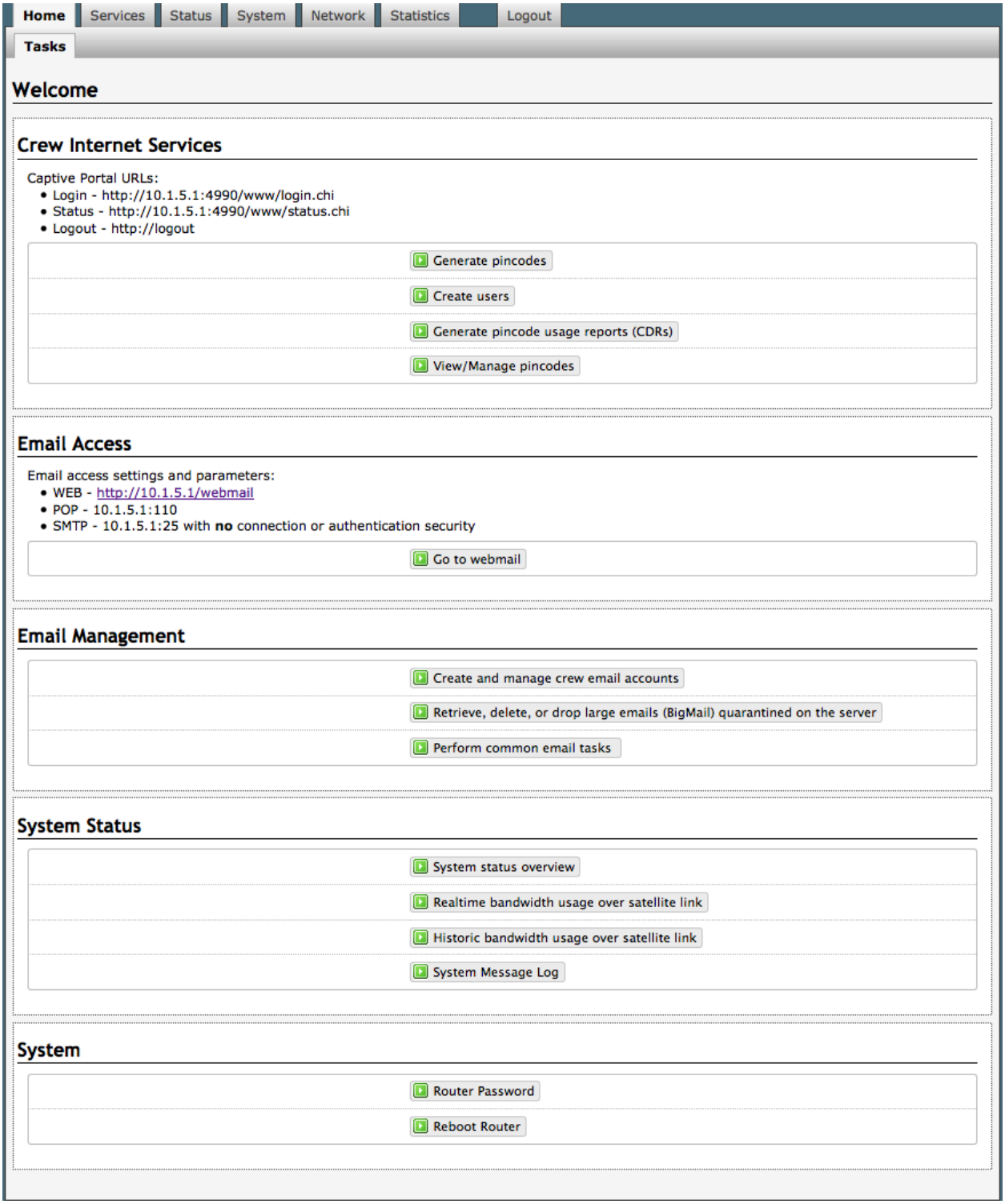
See the *Optimizer Crew Basic User Guide* for information in administering the most-used features of the Optimizer Crew.

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.

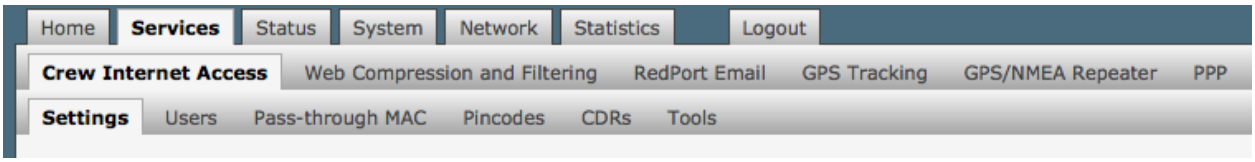
Once logged in, you will see the router's Home page.



This Home Page is the onsite administrator's gateway to the most used features. See the Optimizer Crew Basic User Guide for Home Page details and use.

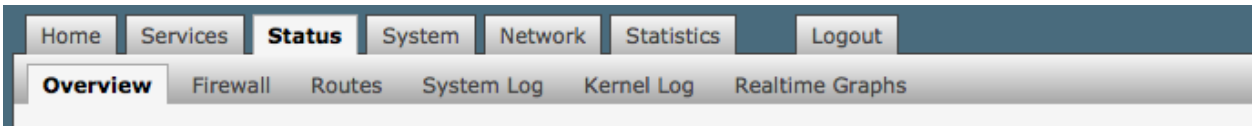
From the Home Page, the 'superadmin' login has access to the remaining sections of the user interface.

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



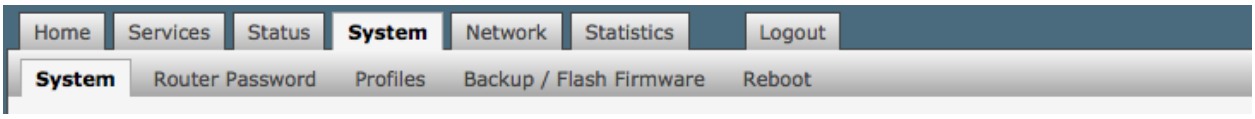
Each service is contained in its own tab under the Services section. This is where you will enable/disable the services and configure them for use.

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



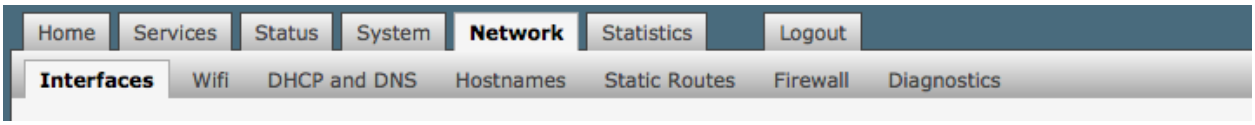
The System Log contains detailed information of the router's performance. It will report error messages and can be useful when troubleshooting connection issues. Realtime Graphs report how much data is being using by the different interfaces. All Status information is Read Only.

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



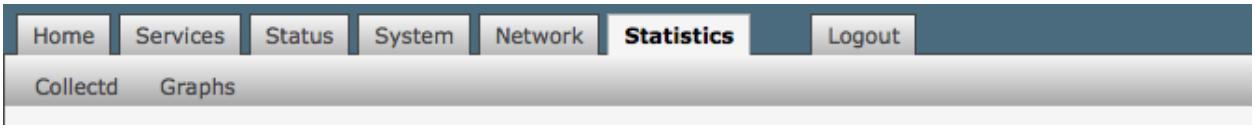
Use this section to set your time zone, change the 'admin' and/or 'superadmin' password, flash new firmware to the router, reboot the router if necessary. Profiles is a way to 'clone' the router configuration for use on another Optimizer Crew router.

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



Use this section to configure network interfaces, run diagnostics, or modify the firewall.

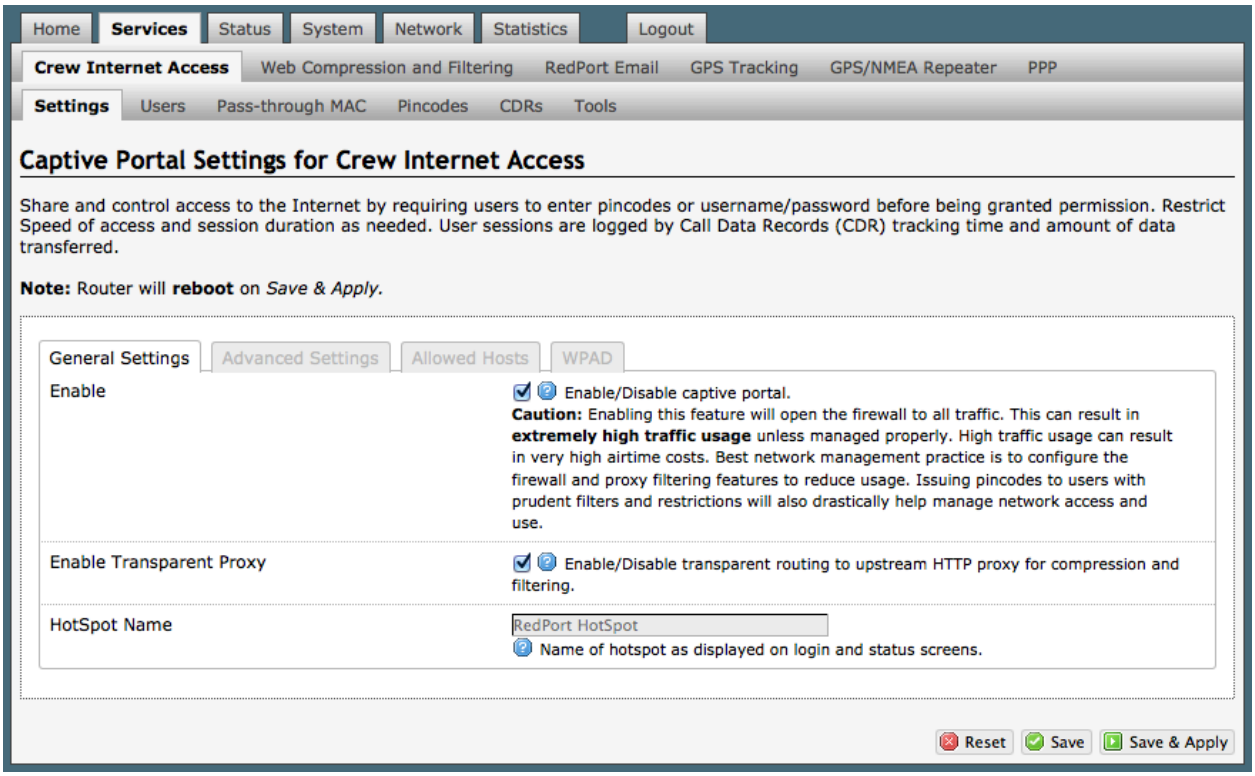
Statistics: contains information about resource usage.



5.0 Services

5.1 Crew Internet Services (Captive Portal)

The Optimizer Crew is shipped with Captive Portal enabled. This allows controlled access to the Internet by requiring users to enter pincodes before being granted permission. In addition, the speed of access can be restricted and/or the duration or timing of the session. User sessions are logged in Call Data Records (CDR) for tracking the amount of time on the service and the amount of data transferred. See the *Optimizer Crew Basic User Guide* for information on how the onsite administrator manages Captive Portal use.

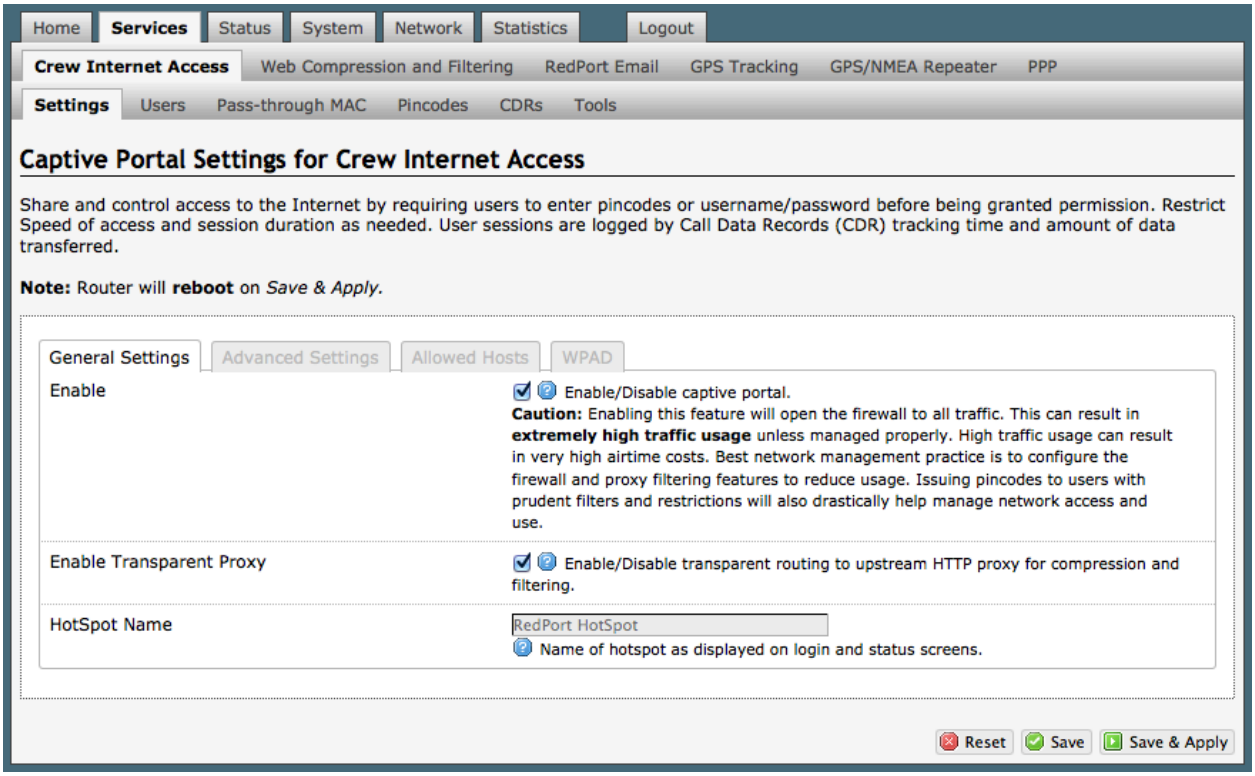


The image above is the default state of the Optimizer Crew as it is shipped to you.

5.1.1 Captive Portal Settings

5.1.1.1 General Settings

The Captive Portal is enabled which means that all users trying to use the Internet will be redirected to a screen where they will be required to enter a pincode or a username and password before they will be allowed to browse the Internet. ***CAUTION: With Captive Portal enabled, the firewall is wide open to all traffic; so, it is important to configure a firewall and/or have internal Transparent Proxy enabled with filtering configured, to control usage.***

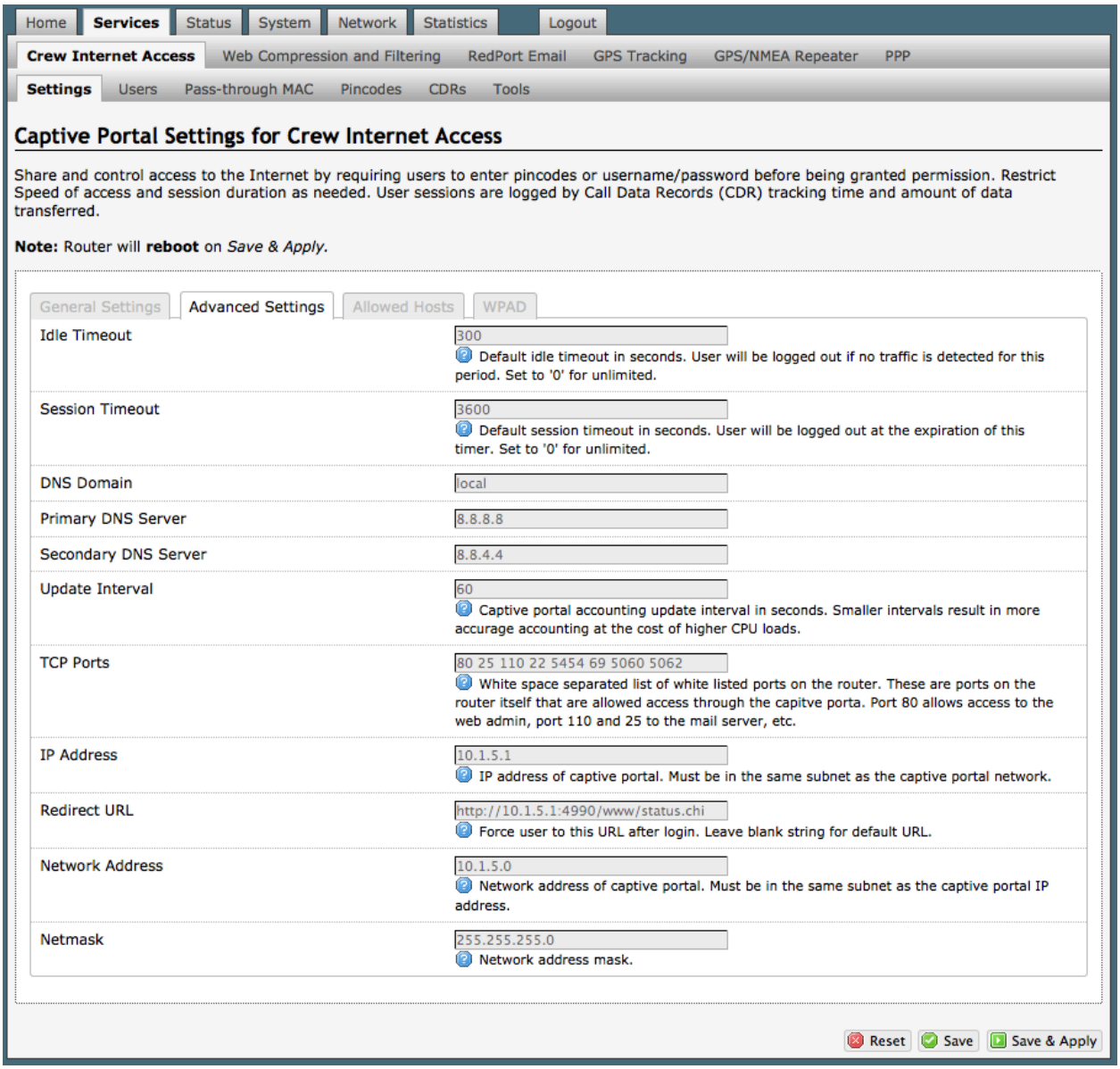


Internal Transparent Proxy is enabled which means that all http traffic that is not whiltelisted is redirected to the router's internal proxy server. This internal proxy server can be configured for url blocking and domain blocking. ***CAUTION: If you Disable Transparent Proxy then all http traffic goes straight to the Internet without any filtering. See Section 5.2.2 for how to configure for url and domain blocking.***

HotSpot Name is the name on the page that is presented to the user when they log in. RedPort HotSpot is the default name. Customize the HotSpot Name by entering the text you prefer.

5.1.1.2 Advanced Settings

In general, there are only two items on this page that may require modification, Idle Timeout and Session Timeout.



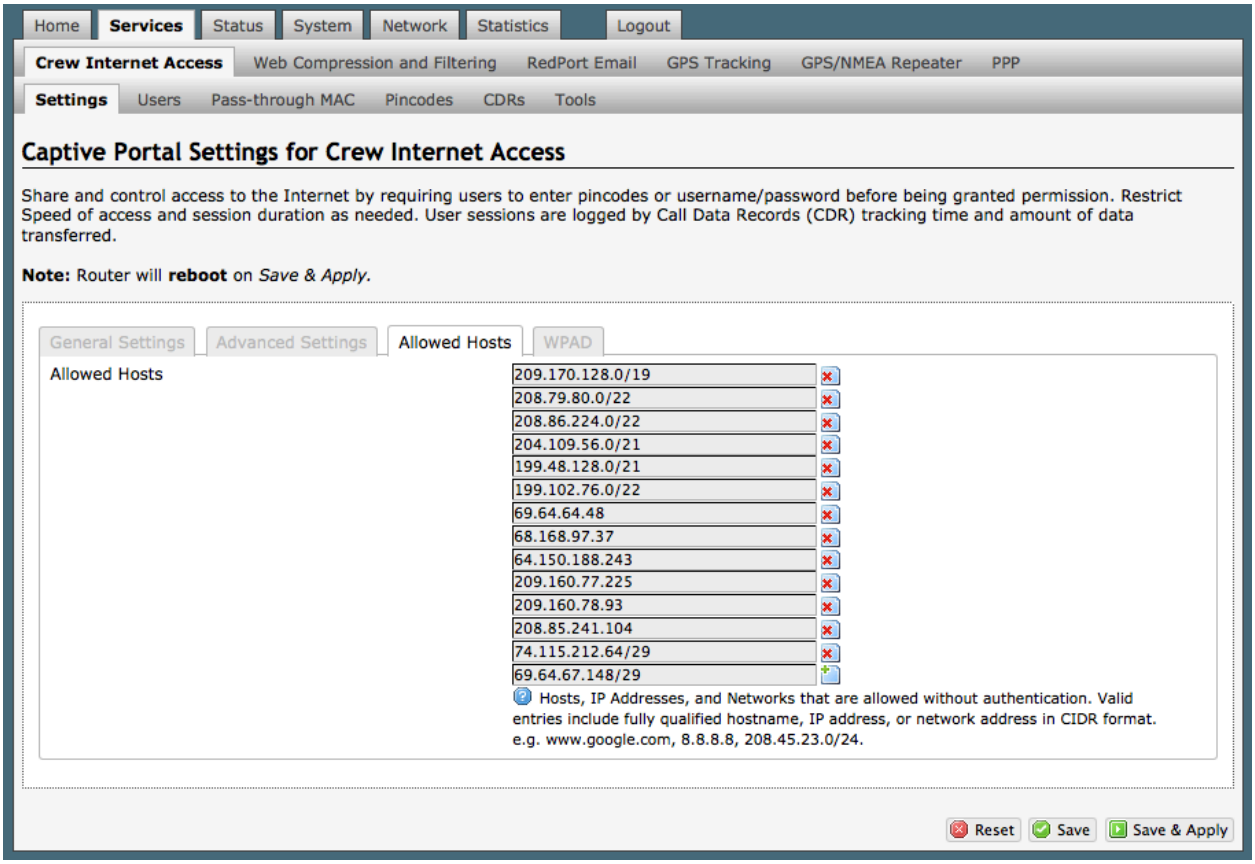
Idle Timeout - The default is set to 300 seconds (5 minutes). If no traffic is detected for the idle timeout period, the user will be automatically logged out. They must log in again to continue.

Session Timeout - The default is set to 3600 seconds (60 minutes). The user will be automatically logged out at the end of the session timeout period. They must log in again to continue.

Both of these timers can be set to '0' for unlimited time period; however, that is NOT recommended. Using Idle Timeout and Session Timeout minimizes the consumption of data without the user's knowledge. For instance, using the default settings as an example, if a user is logged in and has Skype open, and then walks away from the computer, because Skype is running in the background, the Idle Timeout period will never be reached because traffic is detected. However, after 60 minutes, the Session Timeout period will expire. The user must log back in to use the Internet when they return to the computer regardless of the length of time they've been gone, 61 minutes or two days. By having a Session Timeout period, background data is stopped. If there is no background data running the user is logged out at the end of the Idle Timeout period.

5.1.1.3 Allowed Hosts

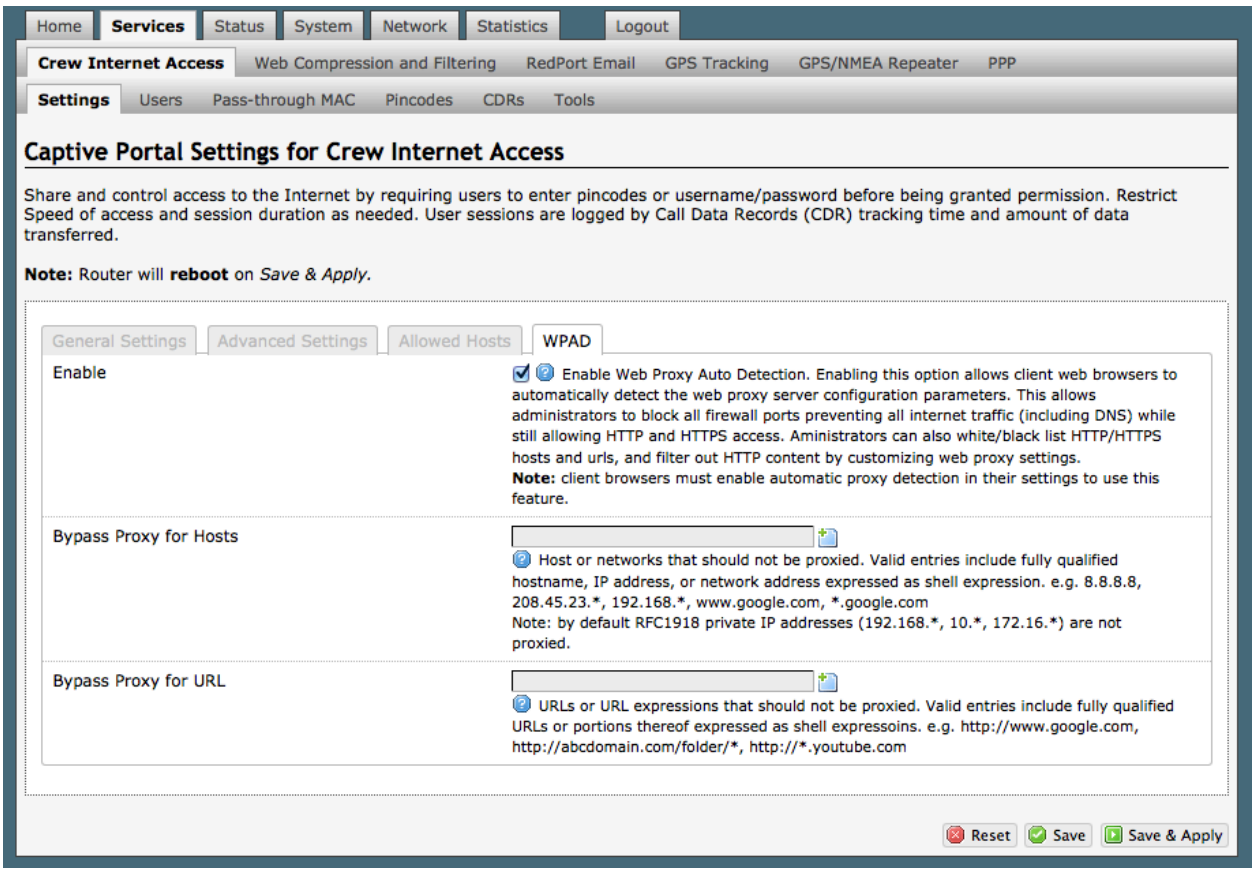
This is the whitelist for the Captive Portal. These are the hosts that can be accessed without having to login thru the captive portal.



By default, there are a number of hosts there. They are all GMN hosts for our services (email, VOIP, etc.) If you don't want them you can delete them. ***(NOTE: If you are using an email service that is not RedPort or XGate, this is where you would add the email servers of your chosen service.)***

5.1.1.4 WPAD

WPAD is a special feature for auto configuring the proxy settings on the client's web browser for tighter control over access to the Internet.

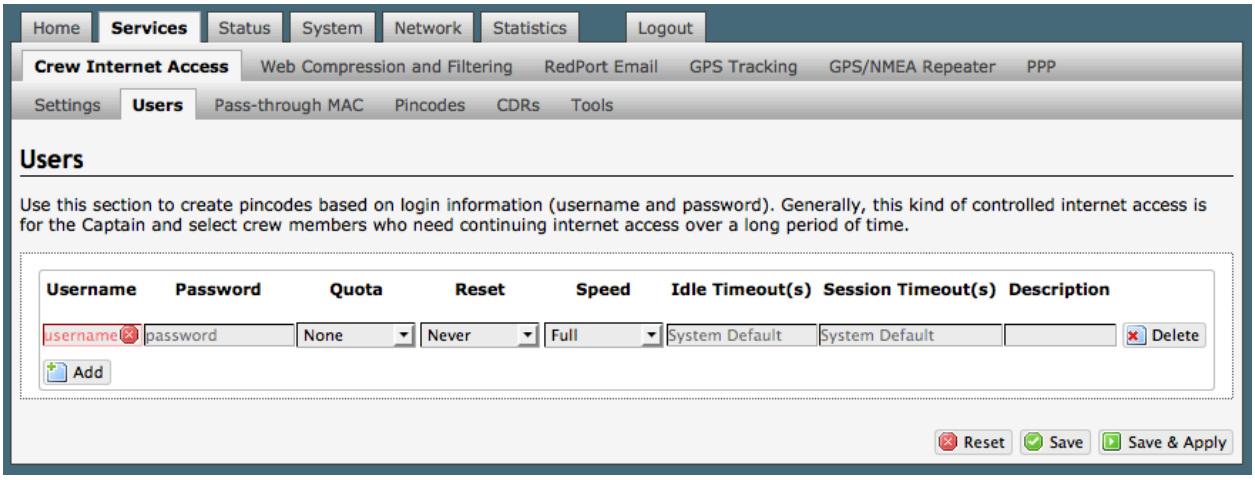


5.1.2 Allowing Individuals Access to the Internet

There are three ways to manage access to the Internet via the Captive Portal:

5.1.2.1 Users with Username and Password

Create Users with a username and password with the Users Tab. Use this section to restrict access in lieu of using pincodes. Typically reserved for the onsite administrator and select crew who need continuing access over a long period of time.

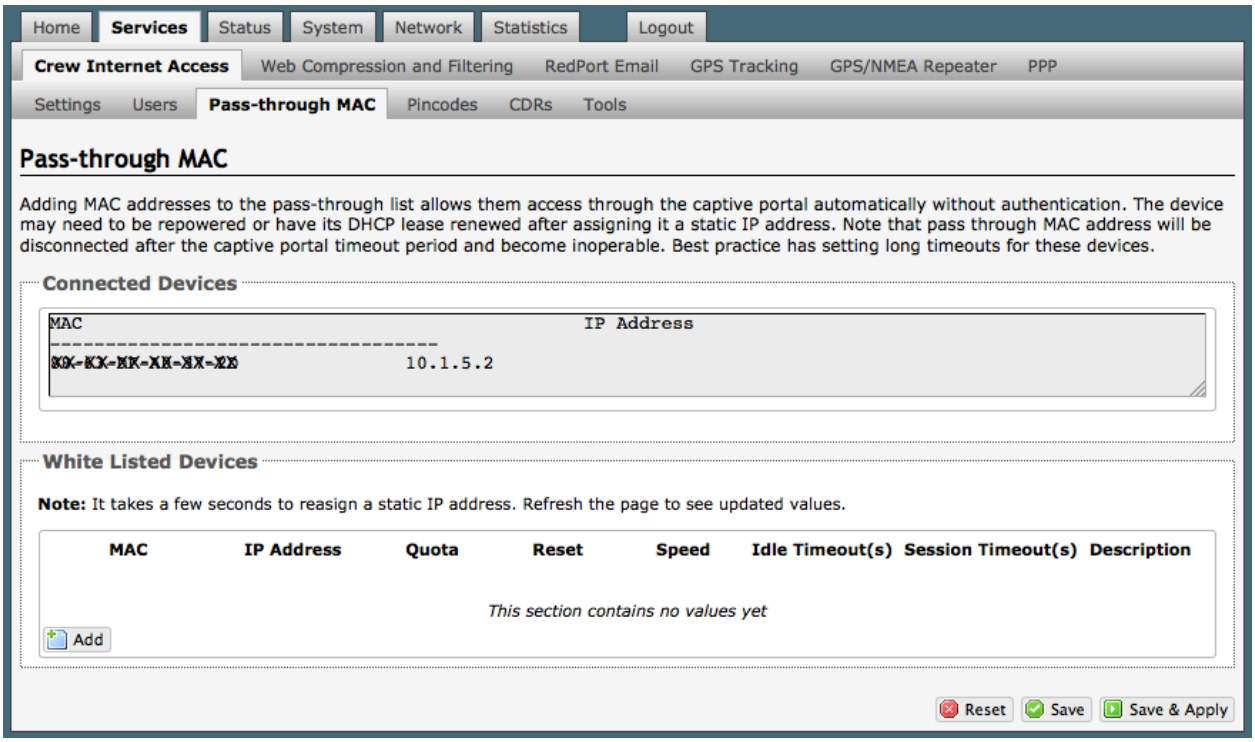


This portion of the user interface is available to both the 'admin' and the 'superadmin' login. See the *Optimizer Crew Basic User Guide* for information on creating accounts in the Users Tab.

NOTE: By default, there is one Captive Portal user that is not visible on this page in the UI. It is username=admin, password=webxaccess. It is recommended that you change the password for this admin user. See section 5.1.4.1 for details.

5.1.2.2 Pass-Through MAC

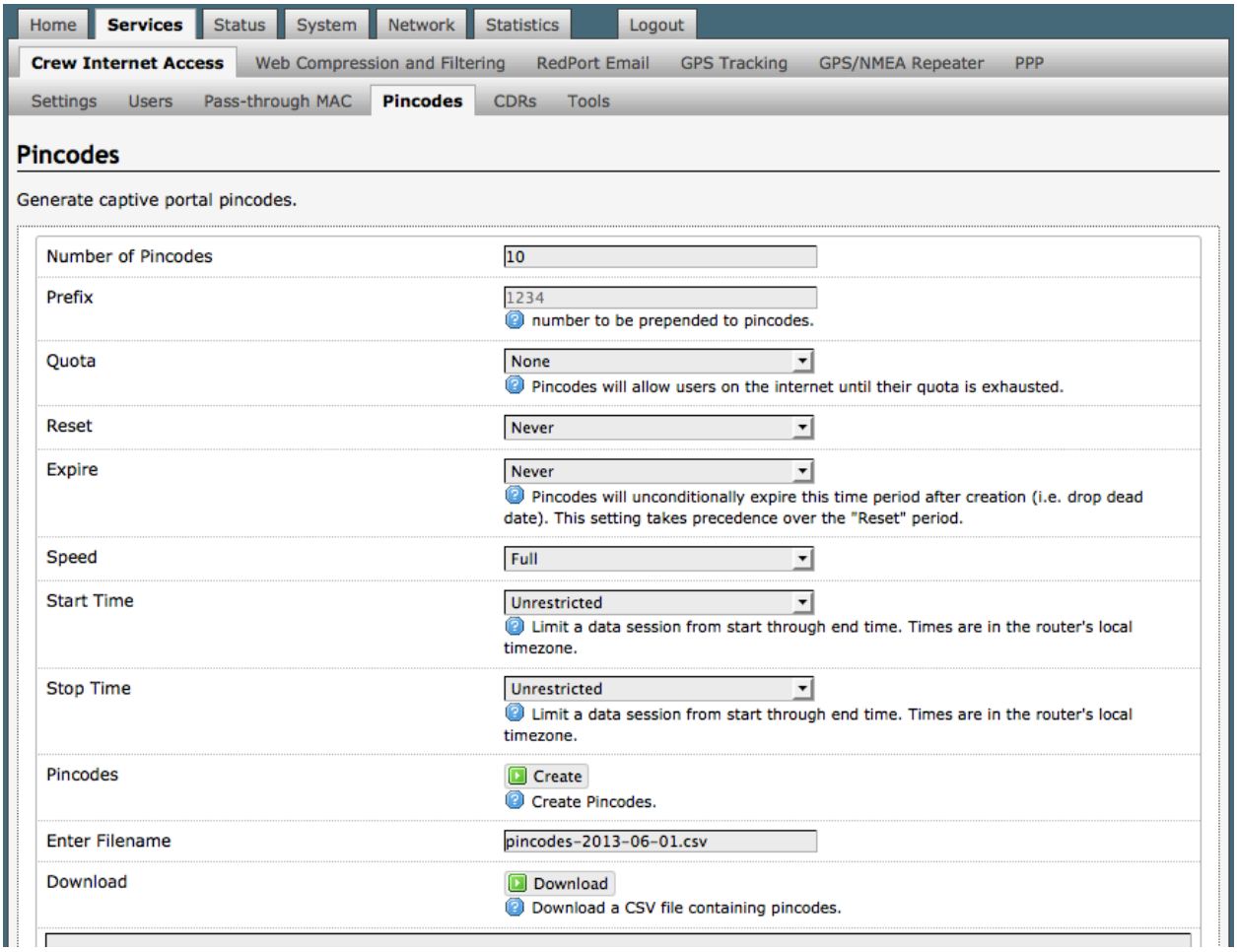
Allow specific devices on the local network to immediately access the Captive Portal without having to login, by adding the MAC address of the device. (Not Recommended)



Access to this portion of the user interface requires the 'superadmin' login.

5.1.2.3 Pincodes

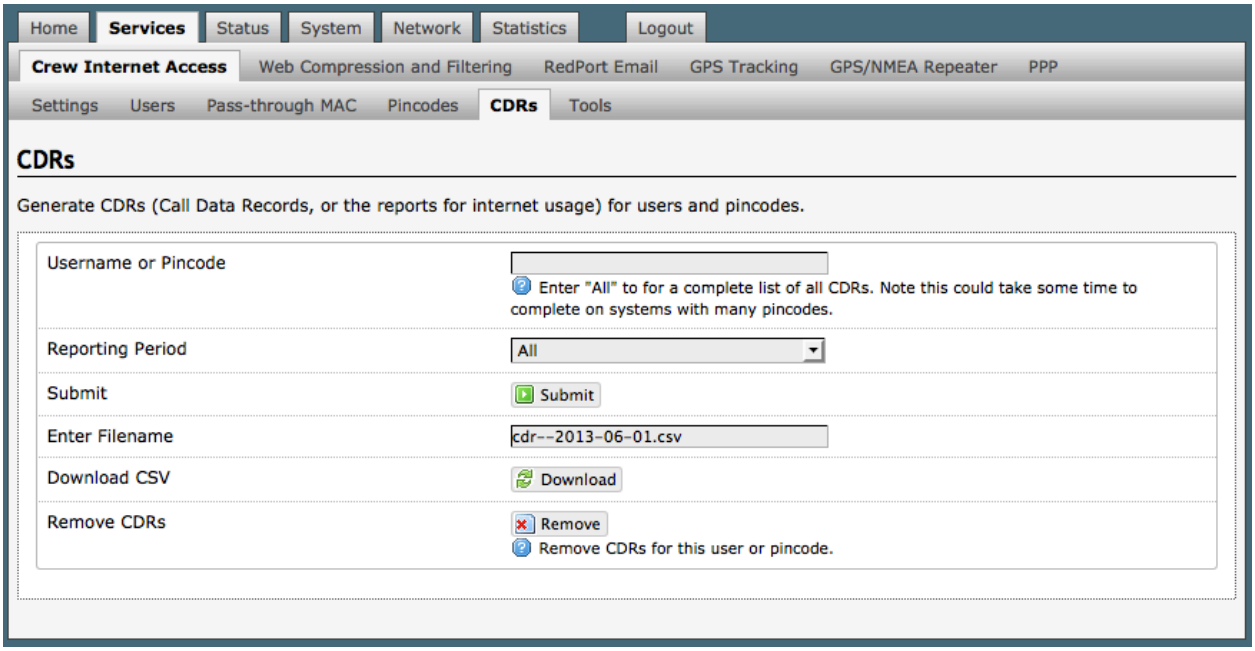
Generate Pincodes to limit Internet access. Sell them or give them to transient crew, passengers, or visitors.



This portion of the user interface is available to both the 'admin' and the 'superadmin' login. See the *Optimizer Crew Basic User Guide* for information on creating Pincodes.

5.1.3 CDRs (Call Data Records)

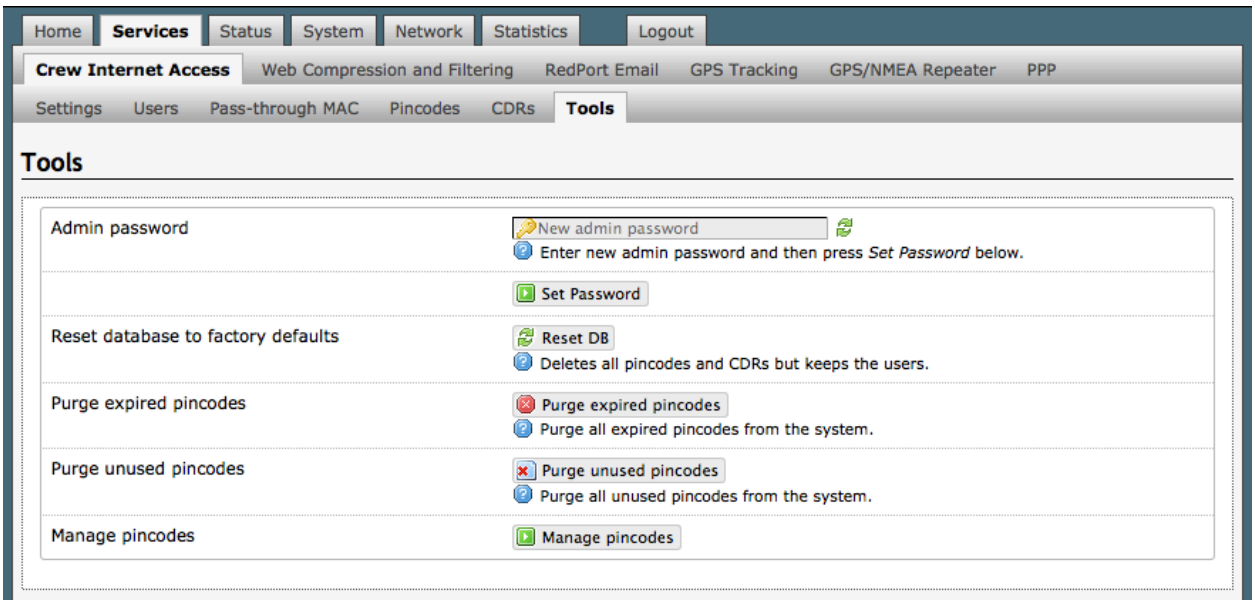
Call Data Records (CDRs) are usage logs. They are the accounting for the Captive Portal system. Usage quotas, time restrictions and resets all use the CDRs. Anyone that logs into the Captive Portal will have a CDR. They can be generated for any pincode or any username or any MAC address.



This portion of the user interface is available to both the 'admin' and the 'superadmin' login. See the *Optimizer Crew Basic User Guide* for information on generating CDRs.

5.1.4 Tools

This section can be used to change the Admin password for the Captive Portal and for a bit of Captive Portal clean up.



Access to Tools requires the 'superadmin' login.

5.1.4.1 Admin password

This can be used to change the admin password for the Captive Portal. This is NOT the admin password to the router itself. By default, the Captive Portal login is: username=admin, password=webxaccess. You will notice that it happens to be the same as the admin password for the router. ***Best Practice: Create a new password for the Captive Portal 'admin' login.***

To change the password, enter the new password in the text box and select <Set Password>.

5.1.4.2 Reset Database to Factory Defaults

This wipes out the entire database and sets the Captive Portal back to the factory defaults. ***CAUTION: This action CANNOT be undone.***

5.1.4.3 Purge Expired Pincodes

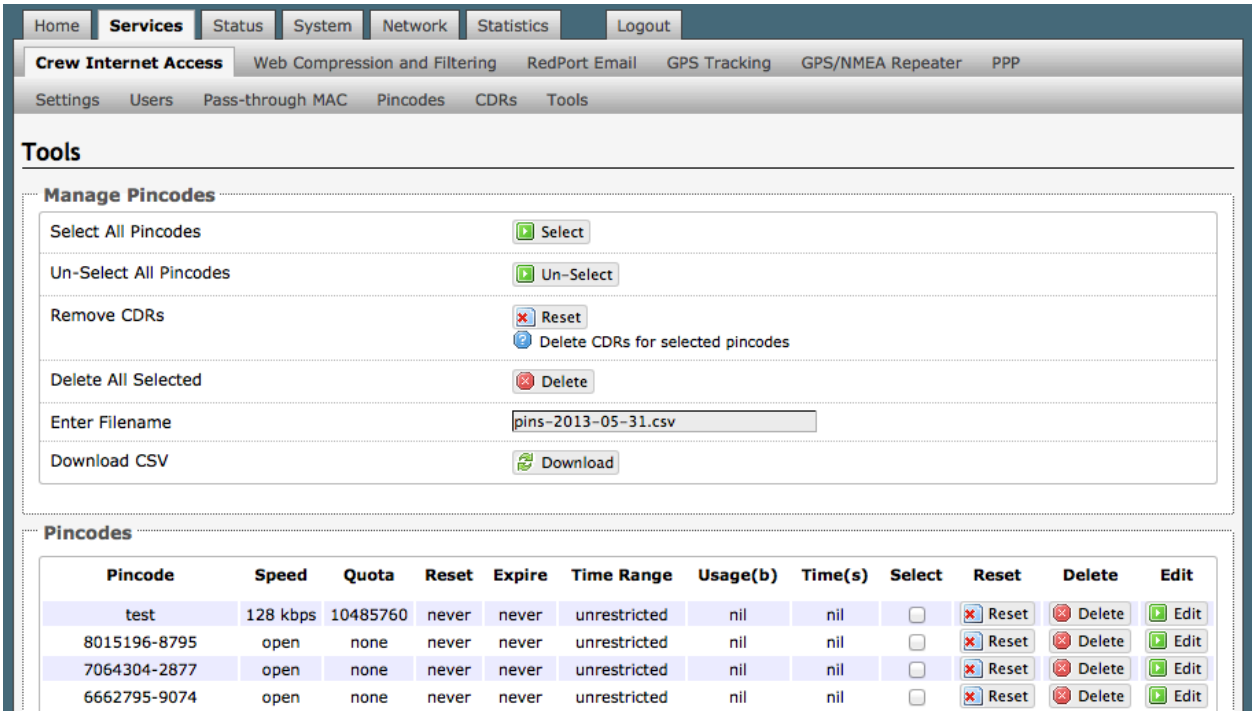
Over time, as the database builds, you may want to purge expired pincodes to free up space.

5.1.4.4 Purge Unused Pincodes

Use this to purge unused pincodes from the system.

5.1.4.5 Manage pincodes

This will show a summary of all the pincodes, all the usernames, and all the MAC addresses that are active in the Captive Portal. Each one appears as a separate line item in the Pincodes table.

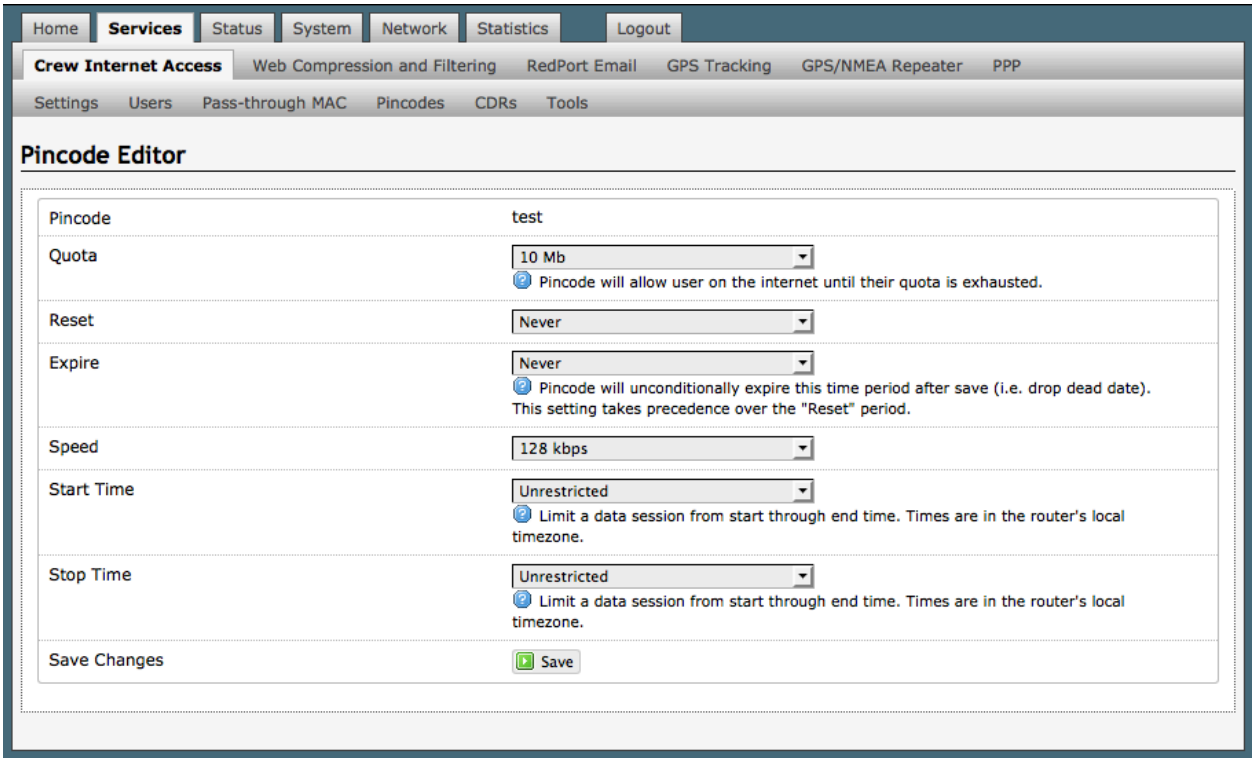


Using the top section of this screen you can:

- Remove CDRs for one or more 'pincodes'.
- Delete one or more 'pincodes'.
- Download the table to a .csv file.

In addition, using the buttons in the Pincodes table, you can:

- Reset the Quota of an individual pincode.
- Delete the pincode from the system, including the CDRs.
- Edit the parameters of the pincode.



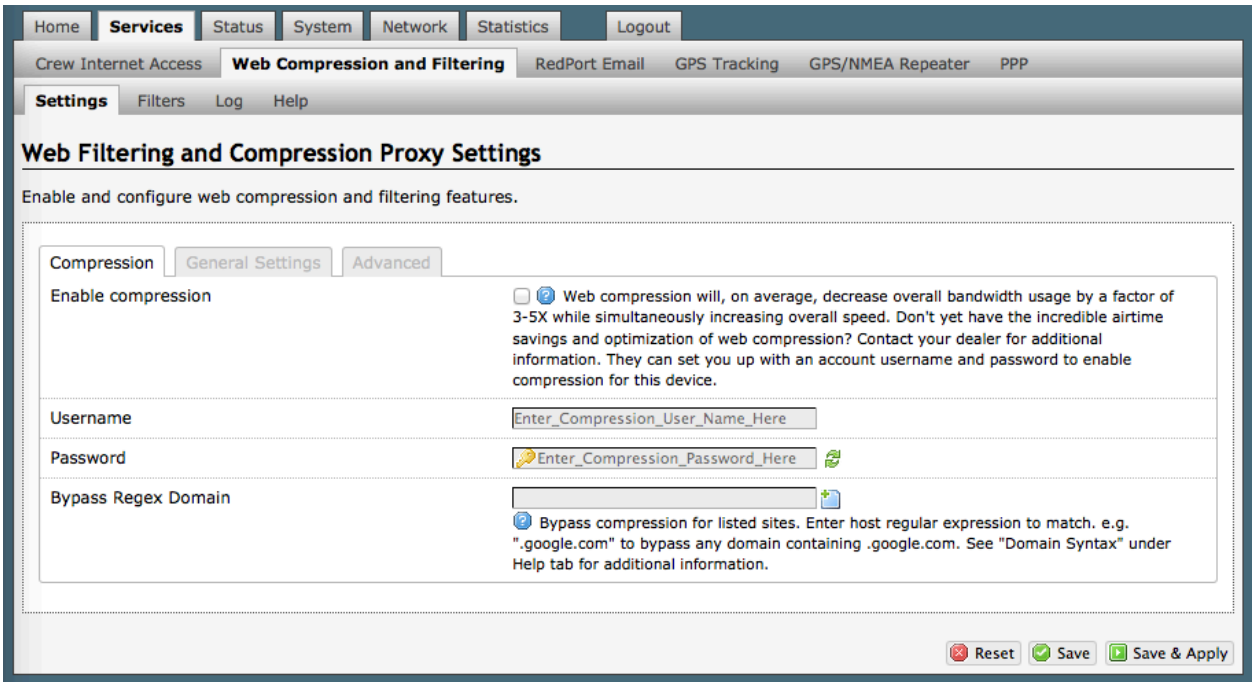
In the example above, we have elected to edit the pincode for the user 'test'. See the *Optimizer Crew Basic User Guide* for information on Pincode parameters.

5.2 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

5.2.1 Settings



5.2.1.1 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.

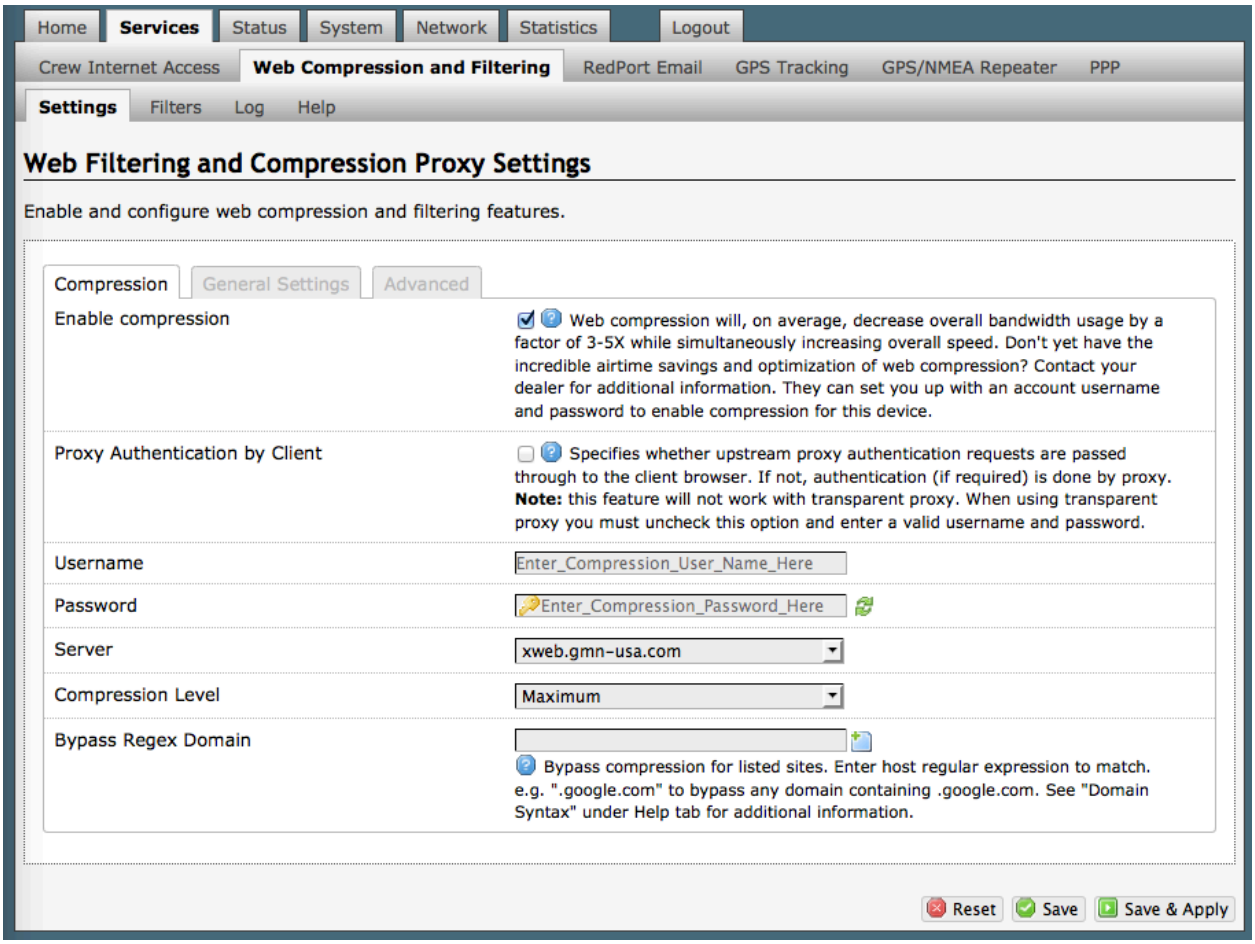
Enable Compression: If you have purchased Web Compression service, select the checkbox to Enable compression. The page will expand; see With Compression Enabled below.

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, select 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.

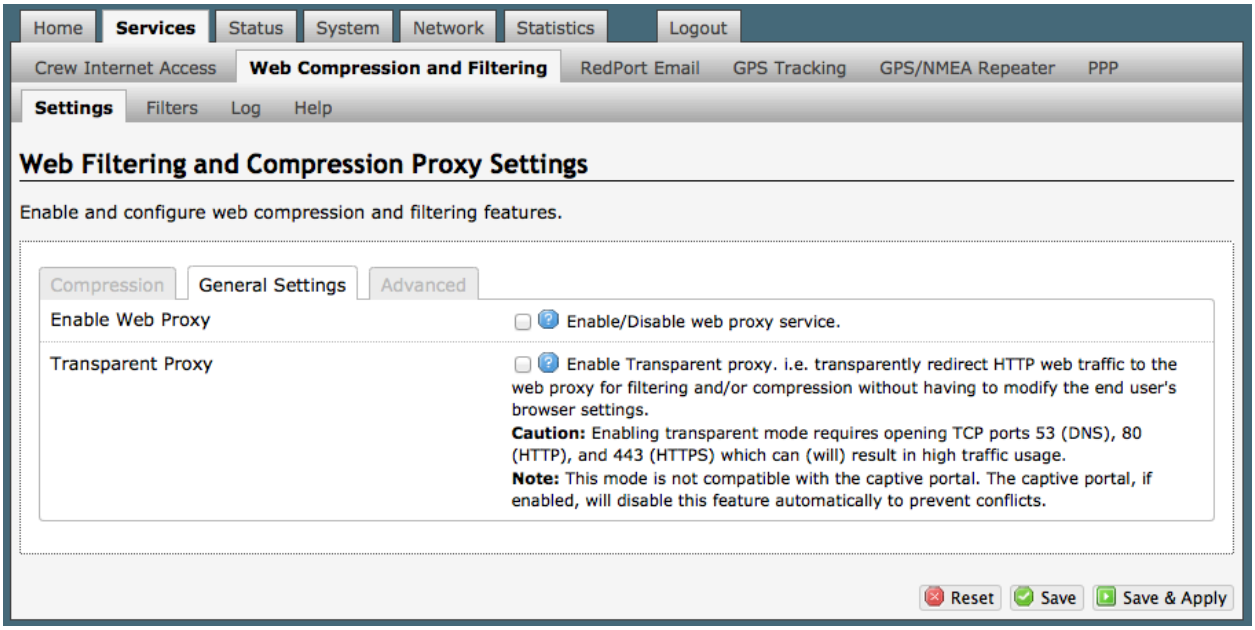
Server: Do not change this unless instructed to do so by your service provider.

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

5.2.1.2 General Settings

These are the general settings for the internal proxy service when the Captive Portal is disabled.

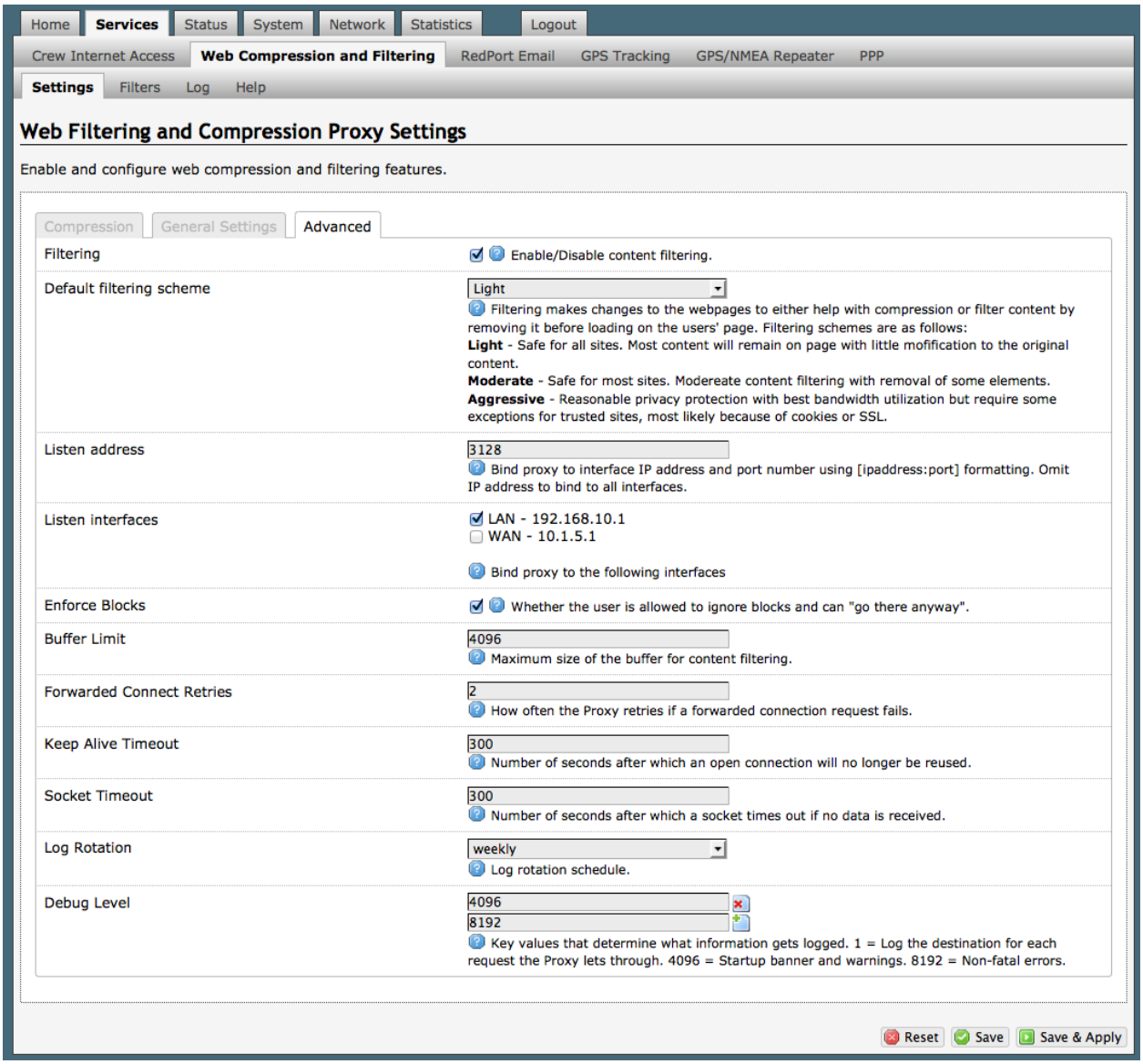
Since the Captive Portal is enabled by default, there is no need to change anything on this page. In fact, if the Captive Portal is enabled, the features on this page will automatically be disabled to prevent conflicts.



If the Captive Portal is disabled you can still use the internal proxy server and enable transparent proxy to redirect all http traffic for filtering.

5.2.1.3 Advanced Settings

Under normal operating conditions there is little to change here.



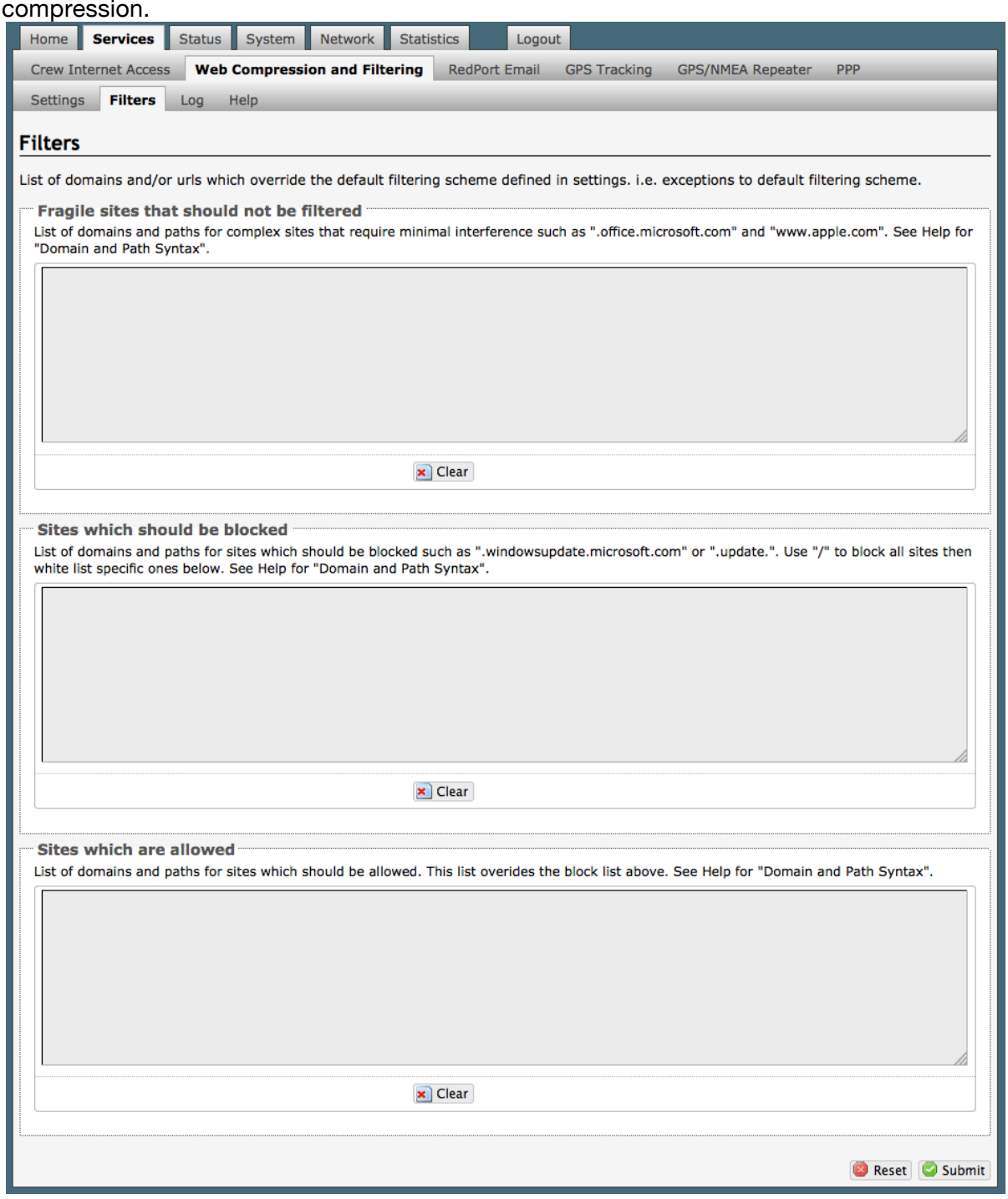
Some items of interest include:

Default Filtering Scheme: This setting affects 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: The settings here 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.***

5.2.2 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.

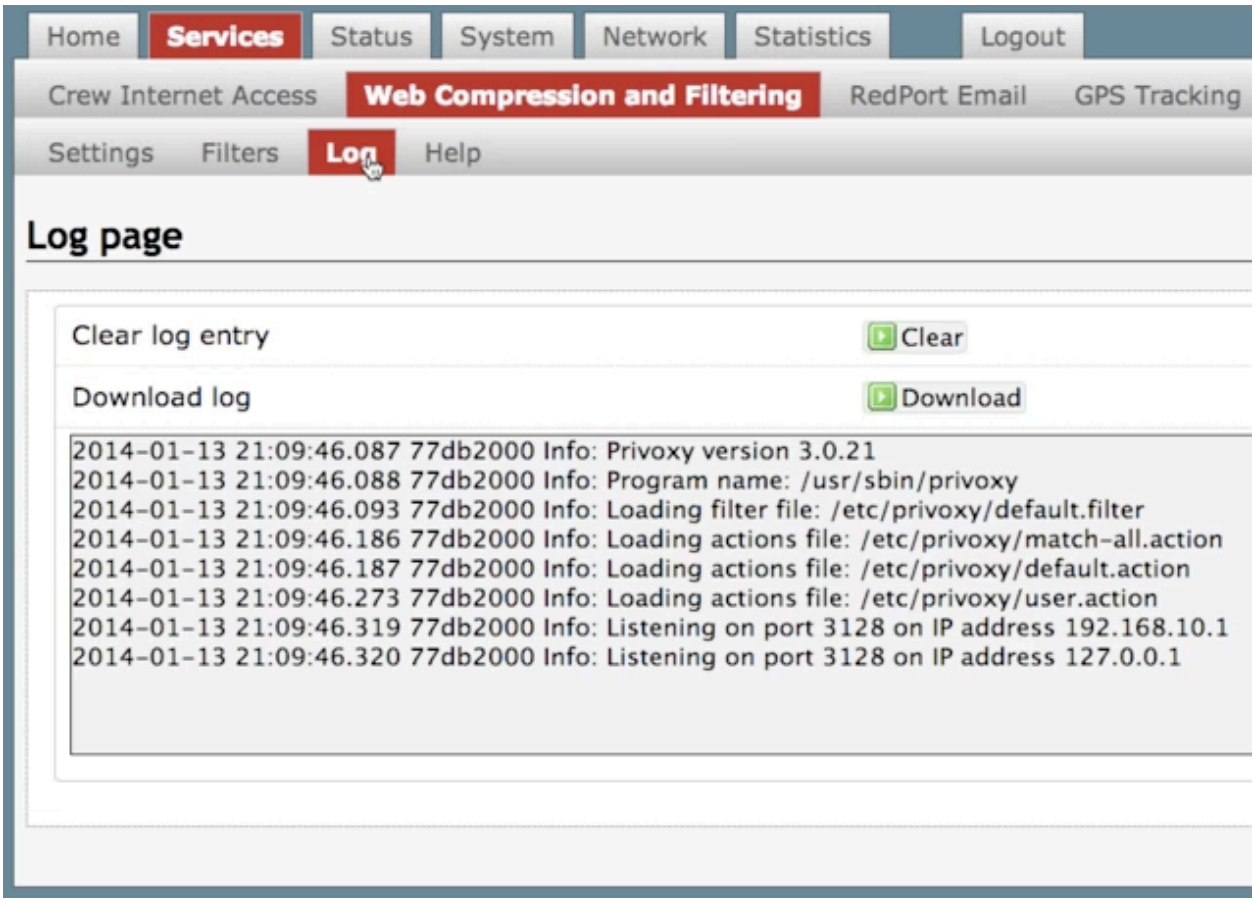
Sites Allowed: the whitelist; these sites are allowed for viewing. This list overrides the blocked list.

Filters respond to POSIX Regular Expressions (see section 5.2.4 for help).

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.

5.2.3 Log

The Log shows activity on the router. How much activity is logged is determined by the entry in Web Compression and Filtering > Settings > Advanced > Debug Level. Descriptions of debug levels can be found in the Help tab (see Section 5.2.4 below).



Log files are kept in RAM and are rotated weekly, by default. You can change the Log Rotation schedule in Web Compression and Filtering > Settings > Advanced > Log Rotation.

Log files can be downloaded to a .csv file if history must be maintained.

5.2.4 Help

For your convenience the Help page includes:

- A list of Debug Levels and their description.

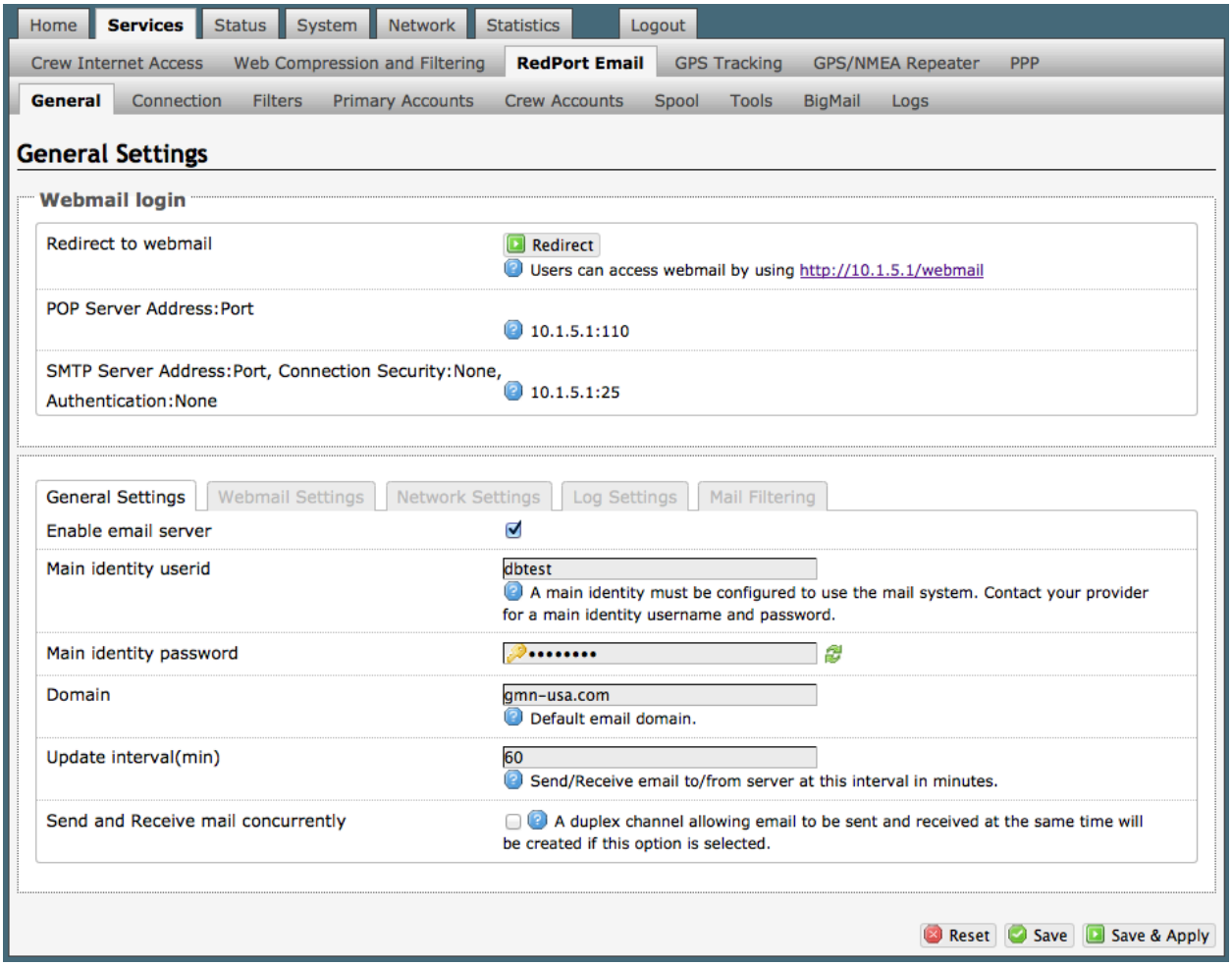
- A brief explanation and some examples of the POSIX Regular Expressions that must be used for the Domain and/or Path Syntax when creating Filters.

If you are unfamilliar with POSIX regular expressons, a web search should reveal more detailed explanations and tutorials.

5.3 RedPort Email

This is a full-featured Crew email solution that runs on the router. RedPort email is designed specifically for use over satellite connections. It uses block compression, mid-file restart, bigmail quarantine and more to maximize data transfers.

Access to Services > RedPort Email requires the 'superadmin' login.



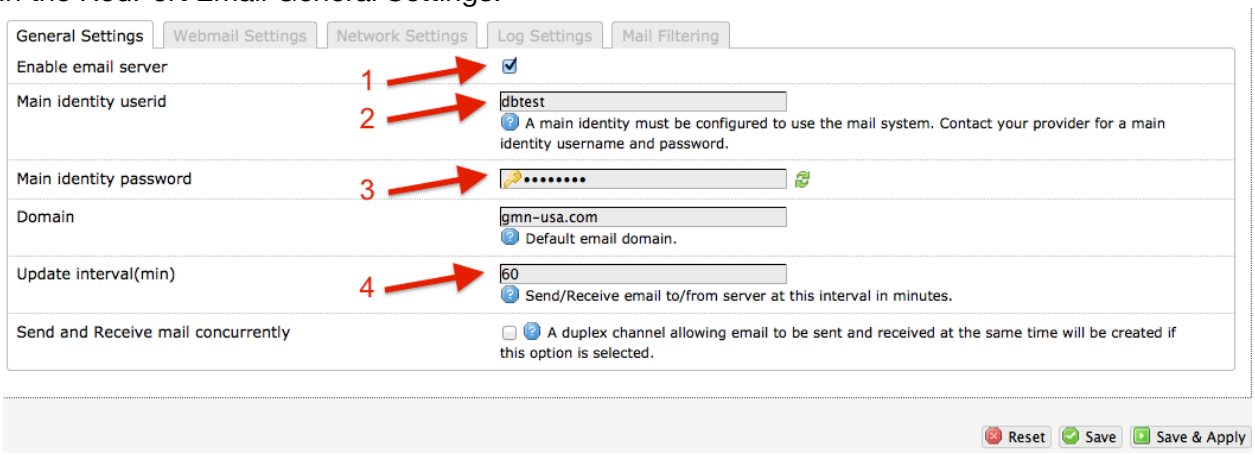
Once enabled, the onsite administrator can manage email for the entire crew. The users can login to a webmail program to view their email so they do not need special software on their computer or device. The Optimizer Crew is a POP and SMTP server as well so users can access email using their preferred email client instead of webmail access, if desired.

Contact your service provider for details and pricing.

The onsite administrator using the 'admin' login to the user interface does not have access to the RedPort Email Settings.

5.3.1 Enable and Configure RedPort Email

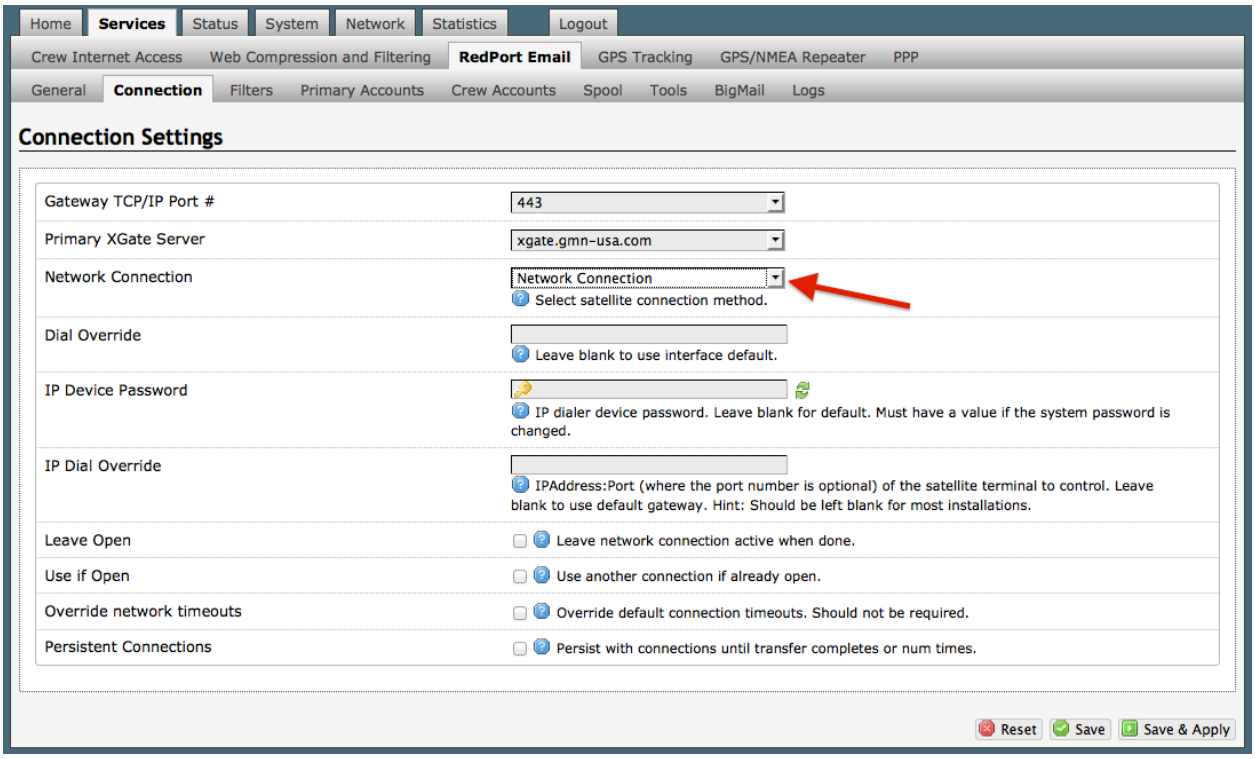
In the RedPort Email General Settings:



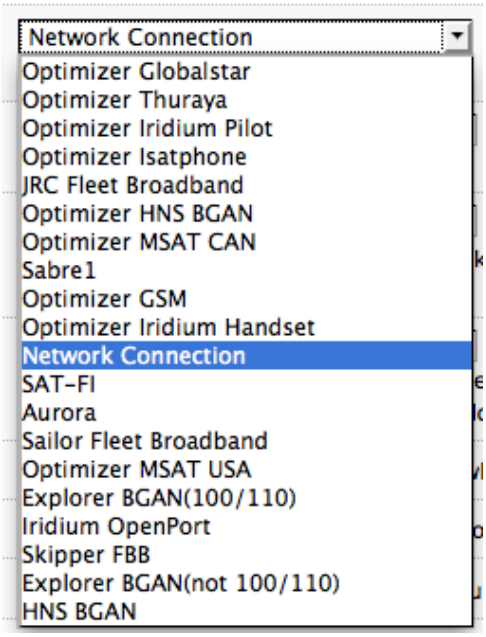
1. **Enable Email Server**: click the checkbox to enable email.
2. **Main Identity Userid**: Enter the username assigned to the Main Identity Primary Account for email, as given to you by your service provider.
3. **Main Identity Password**: Enter the password assigned to the Main Identity Primary Account, as given to you by your service provider.
4. **Update Interval**: This is how often (expressed in minutes) the mail program will automatically login to the satellite device to send any pending email and to receive any email pending. The default is set to 60 minutes, but can be modified to fit business needs. (See Appendix A of the RedPort Email Guide for information on email block compression and its impact on Update intervals.)
5. Click <Save>.

Note: Typically the Main Identity is the onsite email administrator. The Main Identity must be a Primary Account. There must be at least one primary account present on the system before sub/crew accounts can be created. See Section 5.3.2 for more information on Primary Accounts.

6. Go to the **Connection** tab:



7. Click on <Network Connection> to open up the drop-down menu.



8. Select the appropriate setting for your satellite connection method. This tells the router which satellite device you are using and instructs the router to bring up the connection prior to attempting to send email. Otherwise, it will attempt to send email before the connection is up and because it cannot open the socket to the server it will fail due to a timeout error.

The router supports both Managed and Unmanaged connections for broadband terminals.

9. Select <Save & Apply> to apply the change.

For more information about RedPort Email setup and use, please see the separate document, *RedPort Email Guide*.

5.3.2 Primary Accounts

The Main Identity must be a Primary Account. There must be at least one primary account present on the system. The username and password are assigned to you by your service provider.

Typically there is only one Primary Account, however RedPort Email allows access to multiple primary accounts if needed. For example, a fleet manager that travels from vessel to vessel would have a primary account and would need access to that account from each vessel in the fleet.

Primary accounts have access to email whether on or off the vessel as the account exists on the GMN mail servers.

Primary accounts also have access to Filters to customize settings to meet the account needs. These filters include:

- Mail Management including BigMail (See Chapters 6.0 and 8.0 of the RedPort Email Guide for details)
- Inbound Mail Filter (See Chapter 7.0 of the RedPort Email Guide for details)
- Outbound Mail Filter (See Chapter 7.0 of the RedPort Email Guide for details)

The Primary Account receives all Email system messages.

The email address of the primary account will be: username@redportglobal.com. See Appendix A of the RedPort Email Guide for information on using a custom domain name for the email address.

BEST PRACTICE: The Main Identity Primary Account is reserved for the Email Administrator. The Email Administrator does NOT have a sub account. With this configuration, the Email Administrator will receive the system messages that cannot be viewed via a sub account.

Once the Primary Account is set up, the onsite administrator can set up and manage the sub/crew accounts.

Please see the *RedPort Email Guide* for comprehensive information on the use of RedPort Email service.

5.4 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.

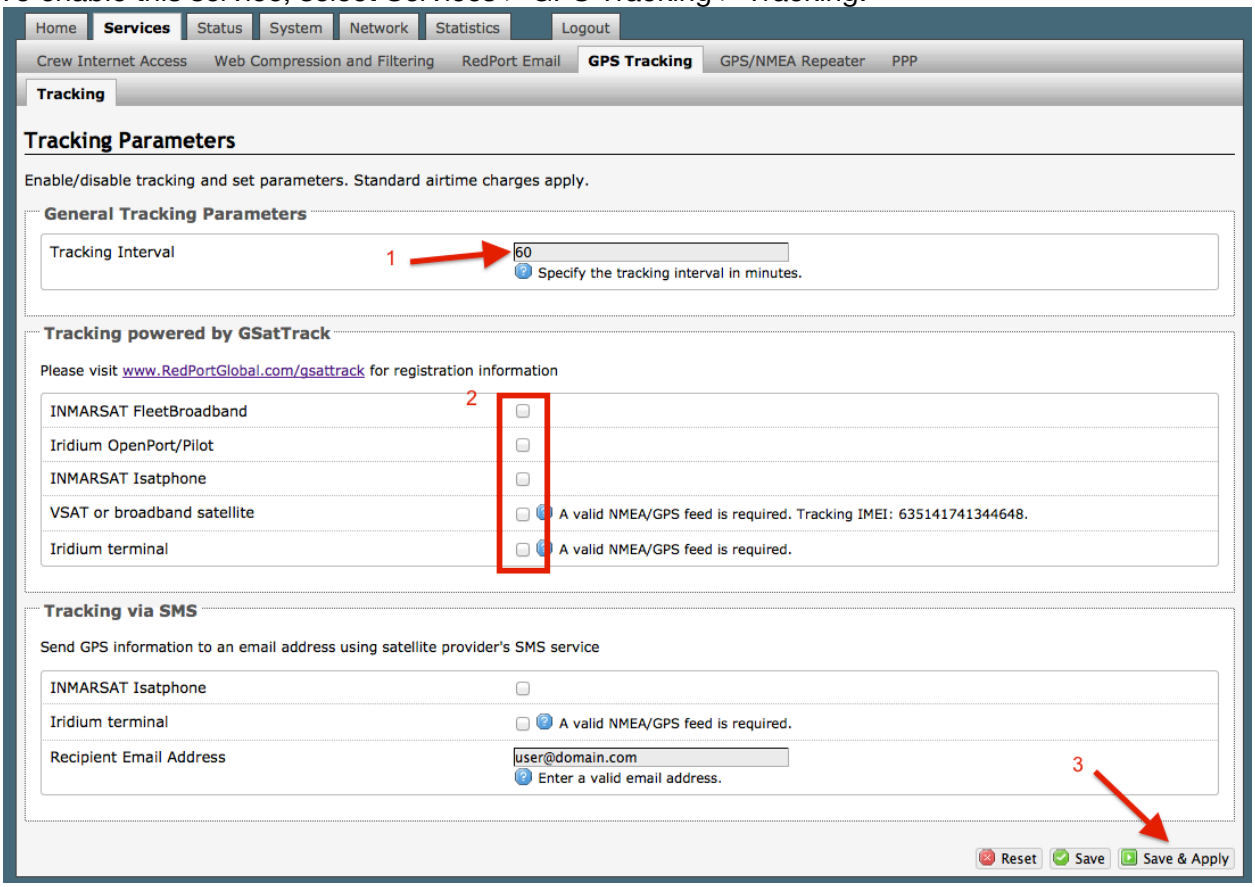
Access to Services > GPS Tracking requires the 'superadmin' login.

5.4.1 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.

> *This tracking service must be purchased separately. See your satellite service provider for details.*

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



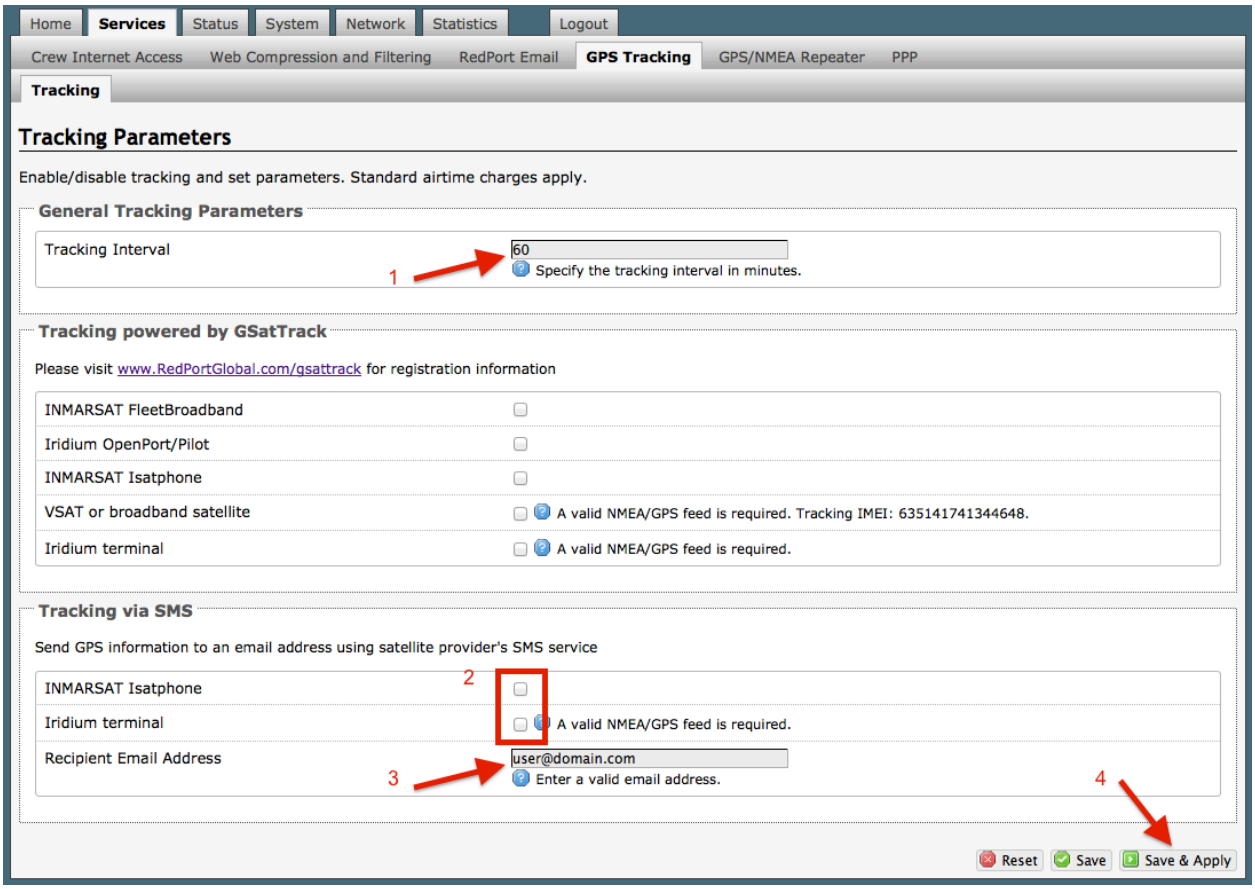
Step 1. Enter the **Tracking Interval** in minutes; the default is set to hourly reporting (60 minutes). This means that every 60 minutes a position report will be transmitted over the satellite link. Keep in mind that standard airtime charges will apply to each postition report. Adjust the Tracking Interval to meet your needs.

Step 2. Select the satellite terminal you are using. Note: a valid NMEA/GPS feed is required when using some satellite devices.

Step 3. Select <Save & Apply>.

5.4.2 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.



Step 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 postition report. Adjust the Tracking Interval to meet your needs.

Step 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.

Step 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.

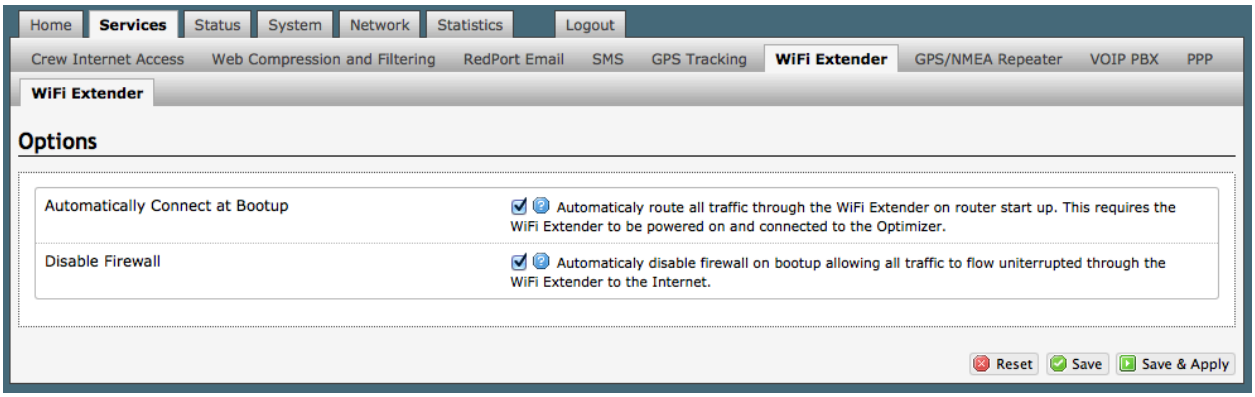
Step 4. Select <Save & Apply>.

5.5 WiFi Extender

If you are using the RedPort Halo WiFi Extender and the Captive Portal is disabled, you can configure the Optimizer to automatically route all traffic through the Halo and you can disable the Optimizer firewall.

IMPORTANT: The RedPort Halo WiFi Extender must be powered ON and connected to the Optimizer before turning the Optimizer ON.

Access to Services > WiFi Extender requires the 'superadmin' login.



When using the RedPort Halo WiFi Extender it is assumed that you are not using a satellite device for the Internet connection, therefore, disabling the firewall allows Internet traffic to flow freely.

For Halo Wifi Extender configuration and use details, see the Optimizer Crew Basic User Guide.

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.) ***WARNING: 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 Internet 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 one of the Optimizer's Ethernet ports.)

The Optimizer will broadcast the GPS signal both over Ethernet and WiFi, 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, you must use a 2-port USB hub (either 1.0 or 2.0) plugged into the Optimizer's USB port to accommodate two USB devices. Plug the small USB drive that came with the Optimizer into one of the USB Hub ports, connect the satellite phone to the other port on the USB Hub using the Mini-USB to USB cable.

(OPTIONAL: Use an ethernet cable to connect the computer with the destination software, like a navigation program, to one of the Optimizer's Ethernet ports.)

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

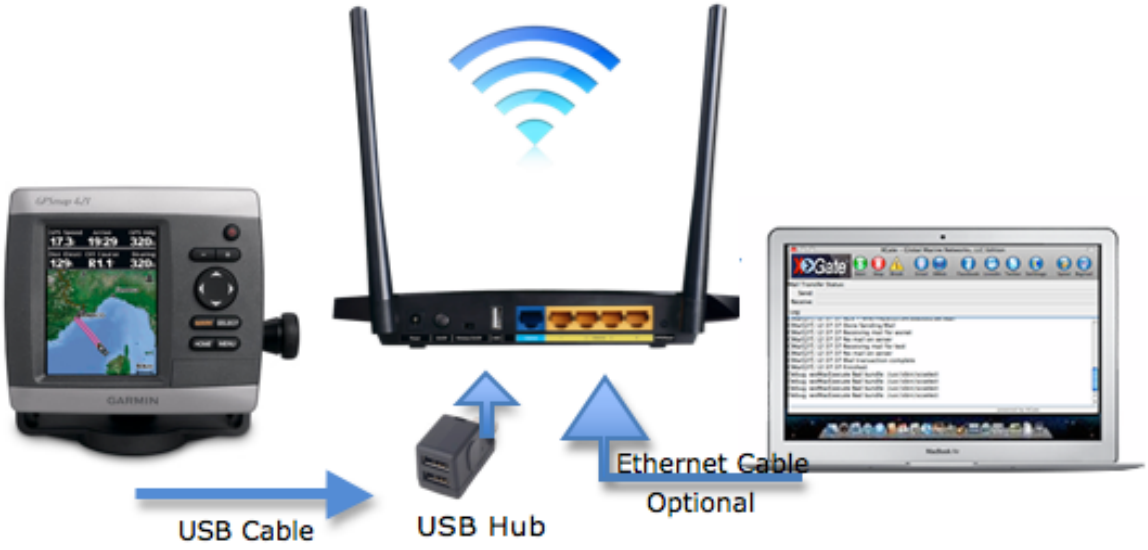
5.6.1.3 USB NMEA Device

When using a NMEA device that supports a USB connection, you must use a USB hub (either 1.0 or 2.0) plugged into the Optimizer's USB port to accomodate multiple USB devices.

Plug the small USB drive that came with the Optimizer into one of the USB Hub ports, connect the NMEA device to the USB Hub 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 one of the Optimizer's Ethernet ports.)

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



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. In addiiton, a USB hub (either 1.0 or 2.0) plugged into the Optimizer's USB is required in order to accomodate multiple USB devices. ***CAUTION: The PL-2303HX is the only USB to Serial Adapter that is compatible with the Optimizer.***

Plug the small USB drive that came with the Optimizer into one of the USB Hub ports, connect the NMEA device to the USB Hub with the USB to Serial Adapter (PL-2303HX).

(OPTIONAL: Use an ethernet cable to connect the computer with the destination software, like a navigation program, to one of the Optimizer's Ethernet ports.)

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

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.

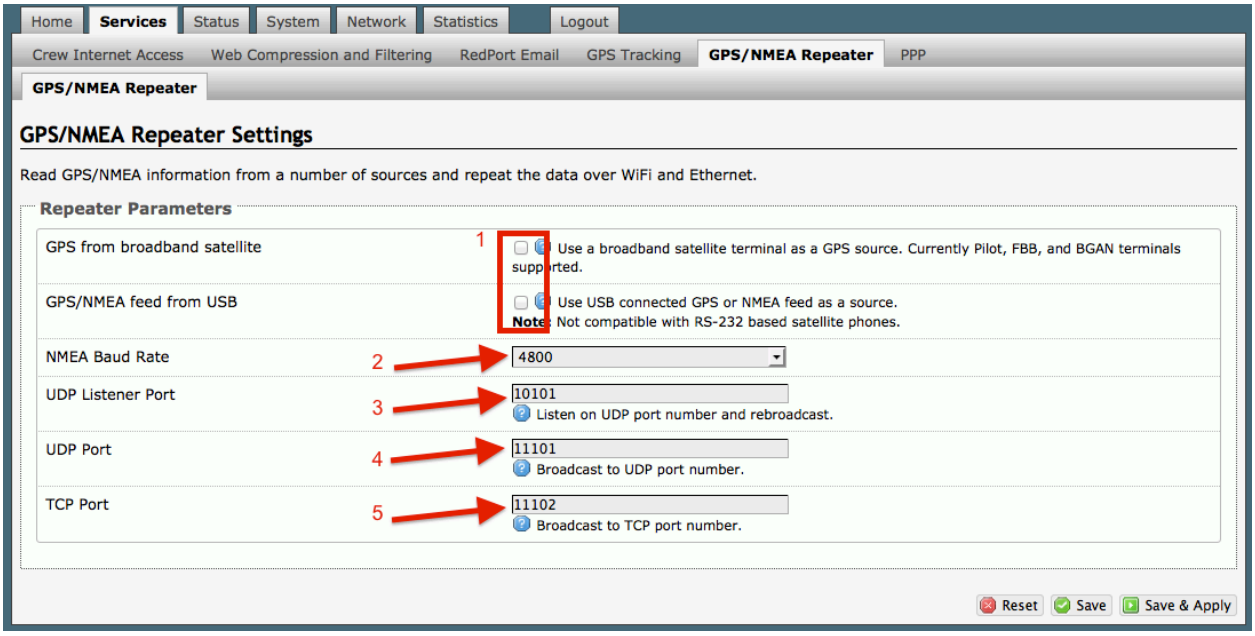
NOTE: The Optimizer supports RS232. If you have a NMEA RS-422 device, adding a properly wired RS-422 to RS-232 converter to your setup may allow the sharing of data.

5.6.2 GPS/NMEA Repeater Parameters Configuration

Access to this section requires 'superadmin' login.

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 select Services > GPS/NMEA Repeater tab.



Step 1. Select the source of the GPS/NMEA information (choose only one):

- **GPS from broadband satellite**: Select this if you are using a broadband satellite terminal with integrated GPS.
- **GPS/NMEA feed from USB**: Select this when connecting a GPS or NMEA device via USB cable.

Step 2. **NMEA Baud Rate** - Using the drop down menu, select the baud rate required for the destination software. By default, most NMEA 183 devices (GPS) and applications use 4800 baud for this setting.

Step 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.

Step 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.)

Step 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.)

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 WiFi network or directly connected to one of the Optimizer's Ethernet ports.

5.7 PPP Tab

Access to this section requires "superadmin" login.

It is possible to use a USB connected satellite device to connect for email and web browsing (for example: IsatPhone Pro or Iridium handheld). (Please note: web browsing is not recommended when using a low bandwidth device.)

When using a supported USB connected satphone, you must use a 2-port USB hub (either 1.0 or 2.0) plugged into the Optimizer's USB port to accommodate two USB devices. Plug the small USB drive that came with the Optimizer into one of the USB Hub ports, connect the satellite phone to the other port on the USB Hub using the Mini-USB to USB cable.

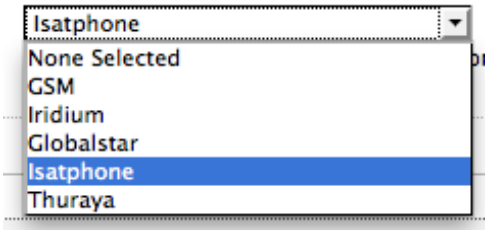
(OPTIONAL: Use an ethernet cable to connect the computer with the destination software, like a navigation program, to one of the Optimizer's Ethernet ports.)

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

5.7.1 PPP Configuration for Use with USB Connected Satellite Device

From the Optimizer Home page select Services > PPP > Settings > Network.

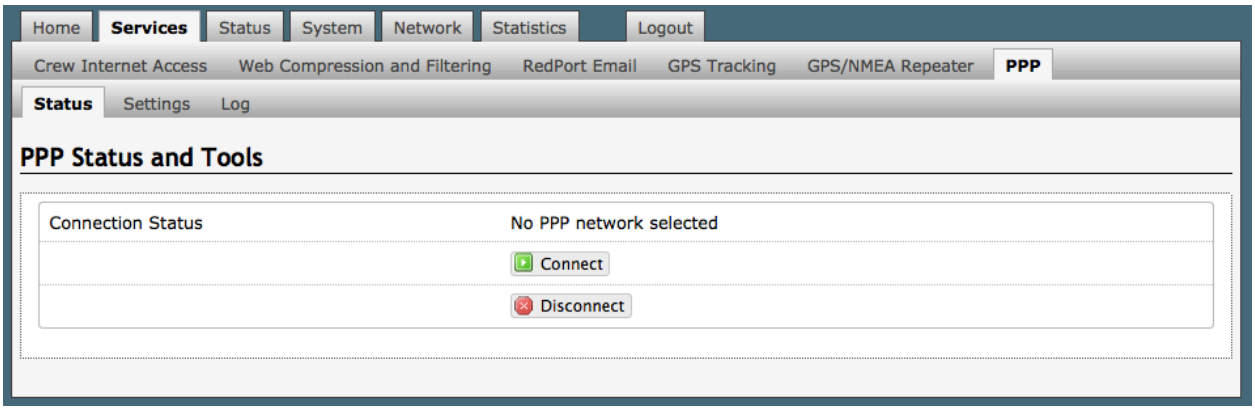
1. Using the drop-down menu, select the appropriate satellite network.



2. Select the Enable checkbox to maintain this setting during router startup. Otherwise, you must re-configure for PPP use with each router startup.

3. Select <Save & Apply> to apply the change.

Move to Services > PPP > Status.



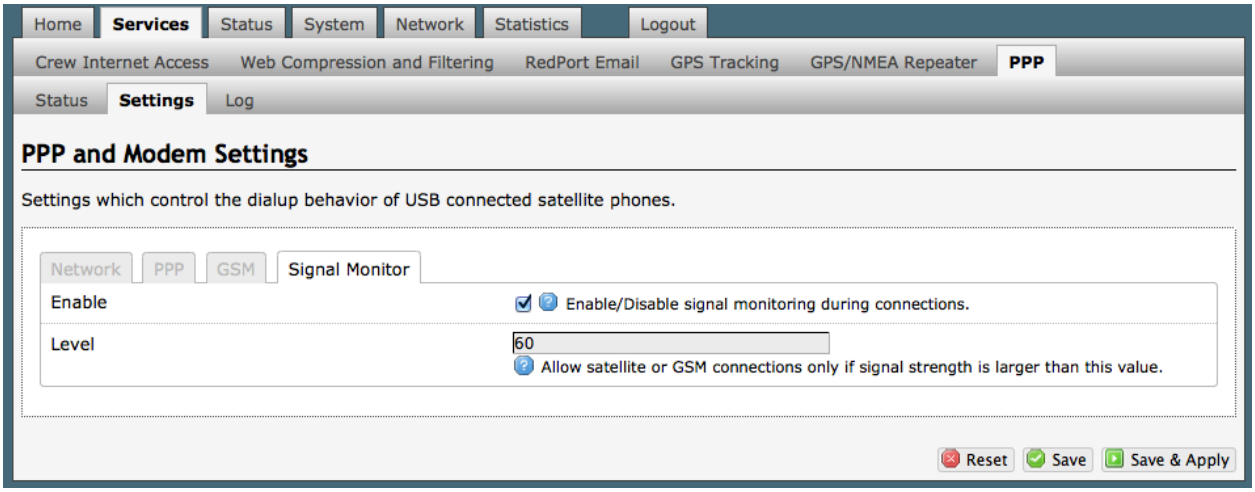
Select <Connect>.

5.7.2 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 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: Services > PPP > Settings > Signal Monitor.



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>.

5.7.3 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 Email and Web Browsing 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.

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.

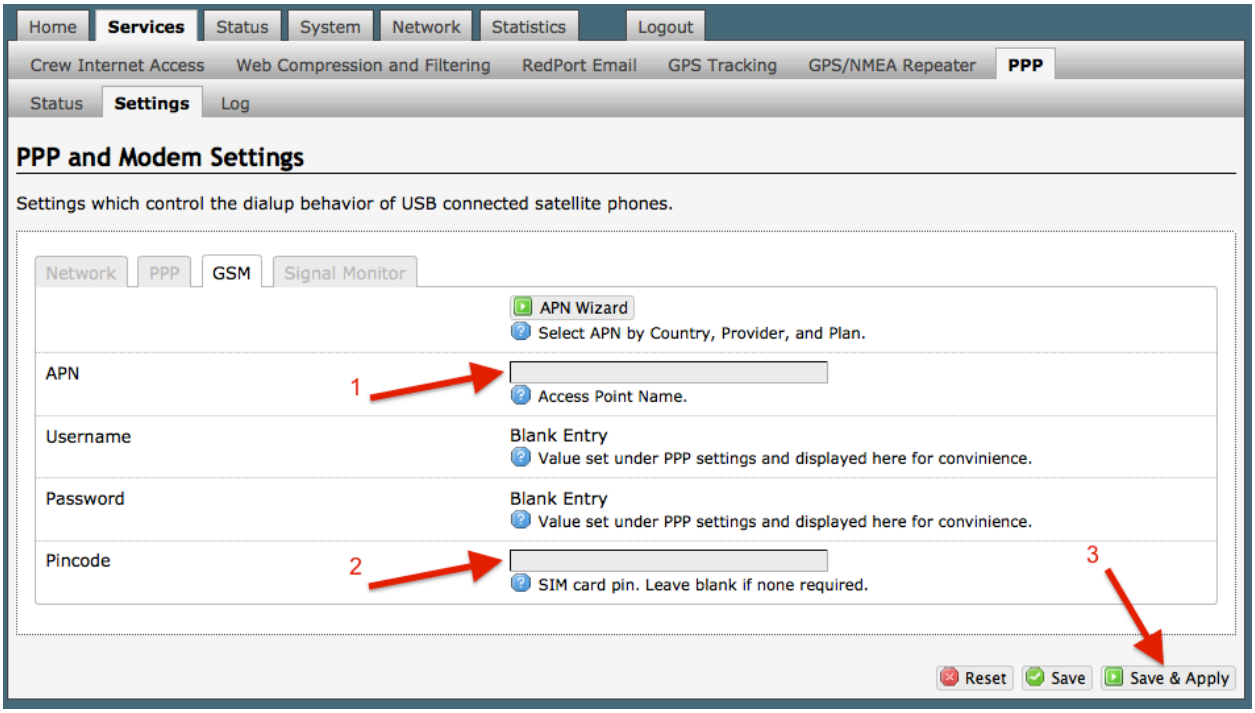
5.7.3.1 GSM Configuration in Optimizer

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: Services > PPP > Settings > GSM.



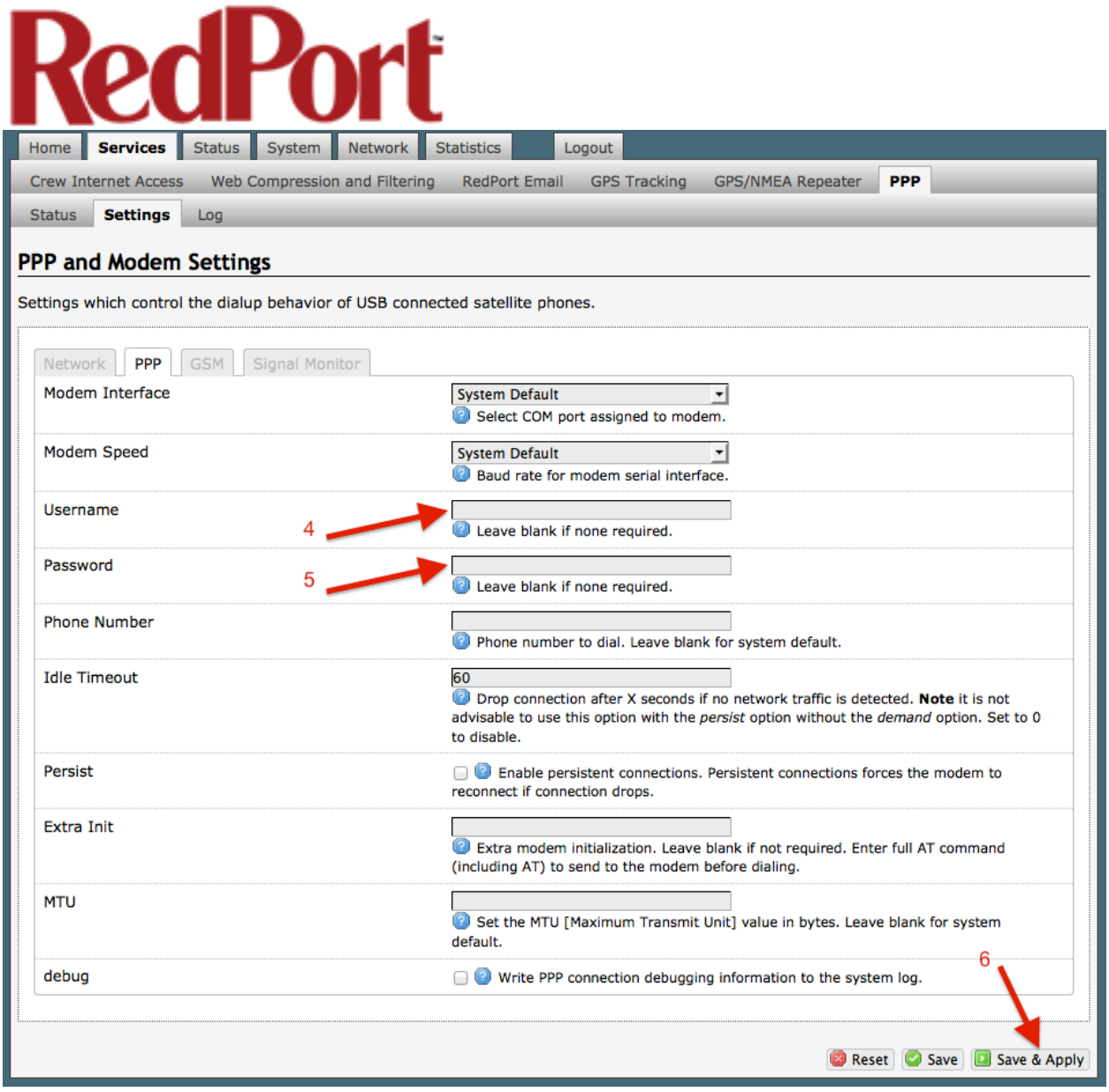
Step 1. Enter the Access Point Name (APN) as provided to you by your cellular carrier.

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

Step 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: Services > PPP > Settings > PPP



Step 4. Enter the username required for access to the APN, if any.

Step 5. Enter the password required for access to the APN, if any.

Step 6. Click <Save & Apply>

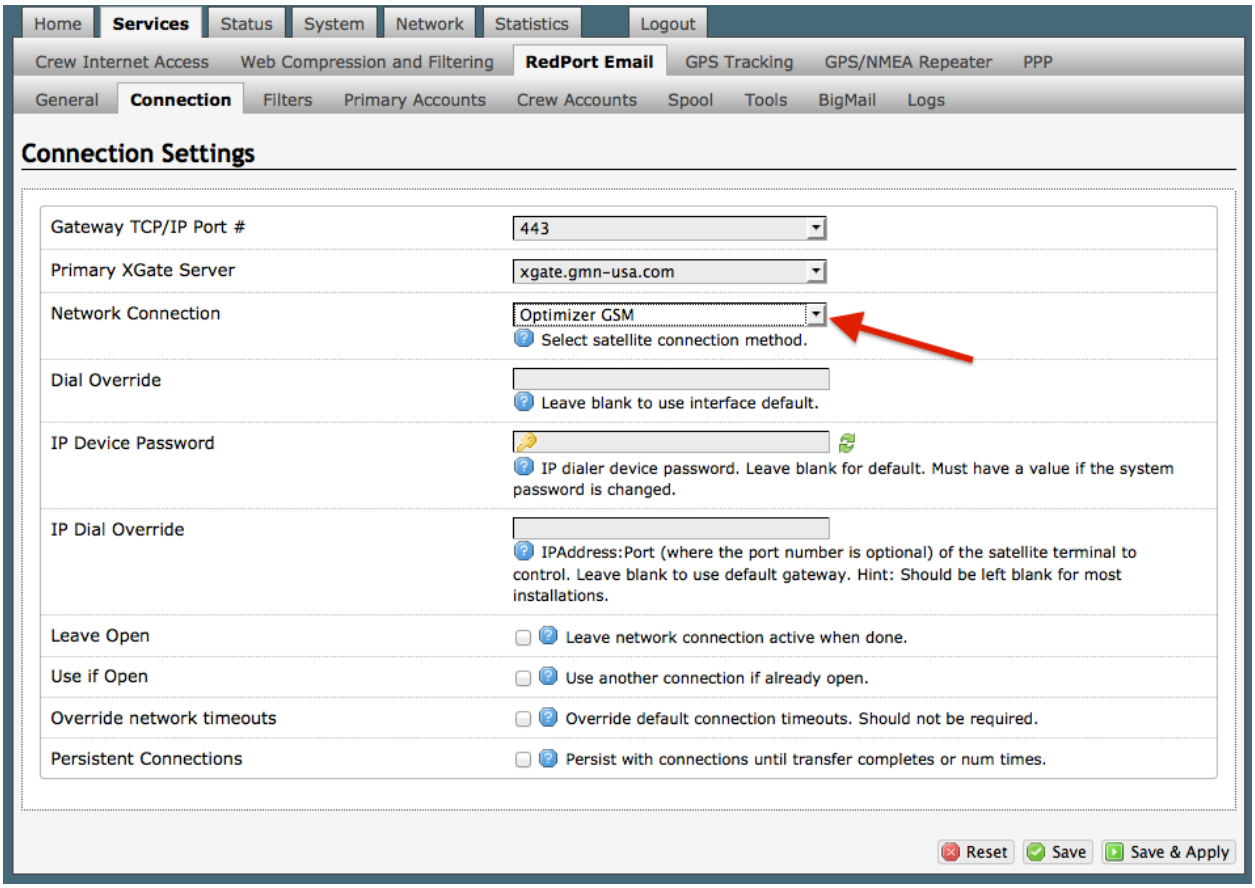
5.7.3.2 Using GSM

When you want to use GSM service instead of satellite service you must use a USB hub (either 1.0 or 2.0) plugged into the Optimizer's USB port to accomodate multiple USB devices.

Plug the small USB drive that came with the Optimizer into one of the USB Hub ports.
Plug the USB data dongle you obtained from your cellular provider into the other port in the USB Hub.

IMPORTANT: If your satellite terminal is connected to the Optimizer, unplug the cable from the Optimizer before attempting a GSM connection.

Configure RedPort Email Connection Settings.



Using the Network Connection drop-down menu, select Optimizer GSM, then <Save & Apply>.

5.7.3.3 Changing from GSM service to satellite service

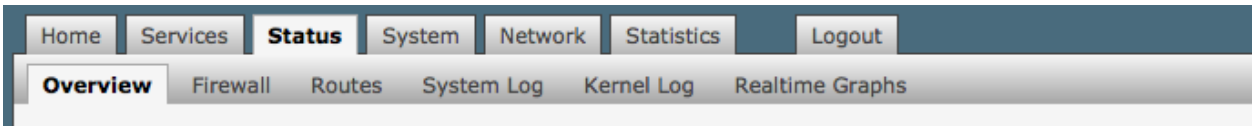
When you travel beyond GSM range you must:

- 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 RedPort Email > Connection Settings > Connection Type back to the appropriate Optimizer setting.

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.

6.0 Status

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.

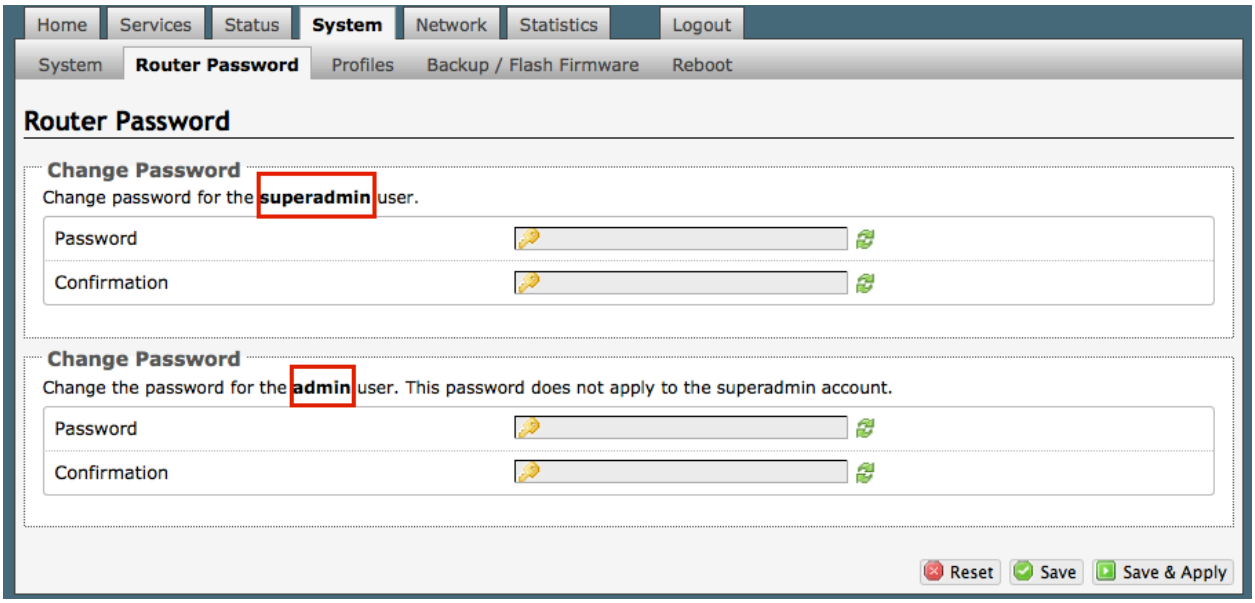
All Status information is READ ONLY.

7.0 System

This section contains some of the router's basic settings for you to configure plus a few maintenance functions. This section also contains the Profiles tab so you can clone a configuration and use it on another router in your organization, saving you setup time.

7.1 Change Router Password (Superadmin or Admin)

The default password to access the Optimizer User Interface for both the "superadmin" login and the "admin" login are set to: "webxaccess". The onsite administrator using the "admin" login can change the password from the Home Page. Anyone using the 'superadmin" login can change the password for both.



Use the top section to change the password for the 'superadmin' user; the bottom section to change the password for the 'admin' user.

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

This procedure changes the password for the Superadmin or the Admin login ONLY. When connecting a computer, iOS or Android device to the wireless network, do NOT use either of these login passwords. These passwords are 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.

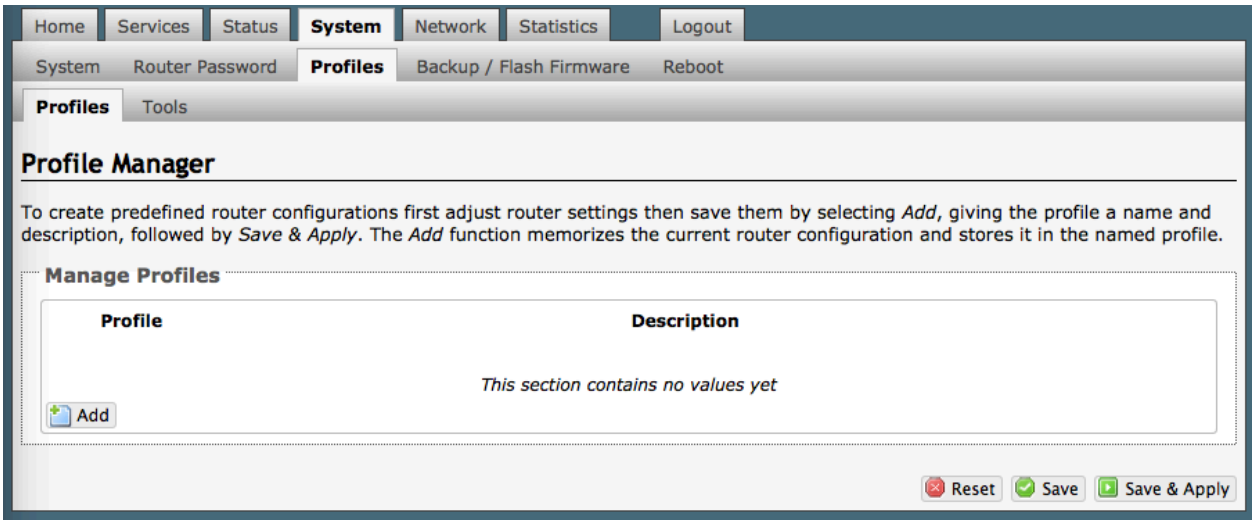
You can configure the Optimizer for a specific satellite device and save the profile. This is good for failover situations when using multiple devices. An extreme example would be that you might have the firewall wide open on a VSAT device but in an emergency must use an Iridium handheld device where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

Once a profile is saved it can be exported for use in another Optimizer Crew router.

7.2.1 Add a Profile

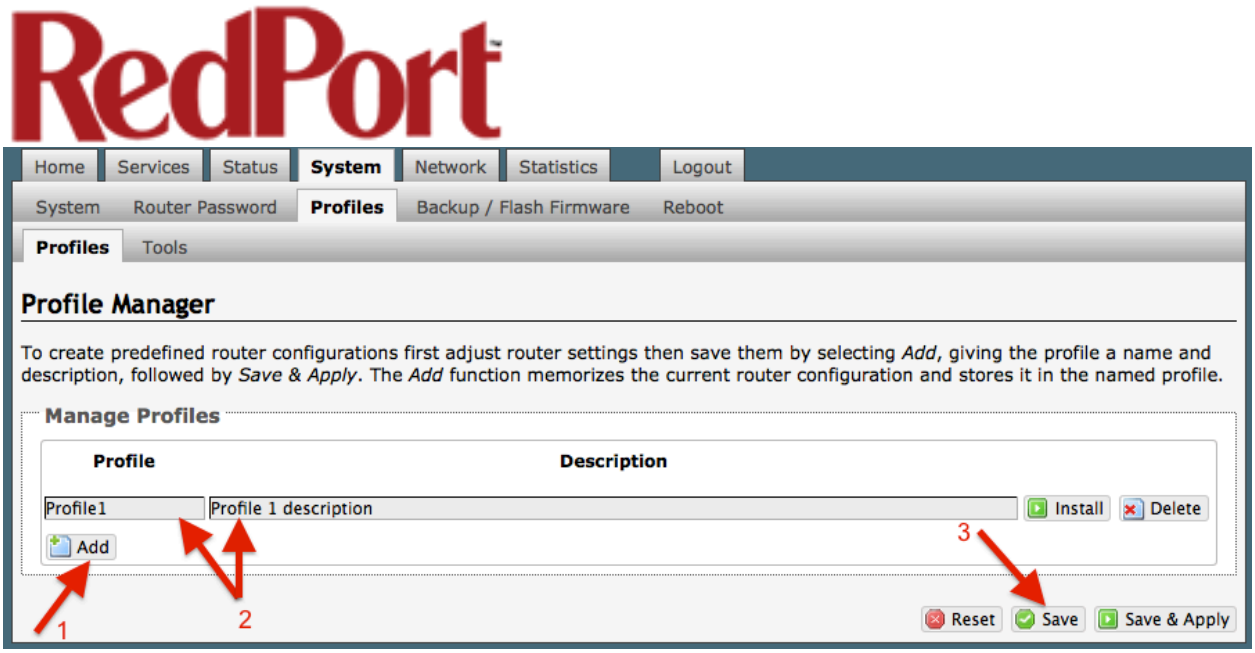
Before adding a Profile, complete the router configuration.

Then access the Profile Manager.



To create and use the new Profile:

1. Select <Add>



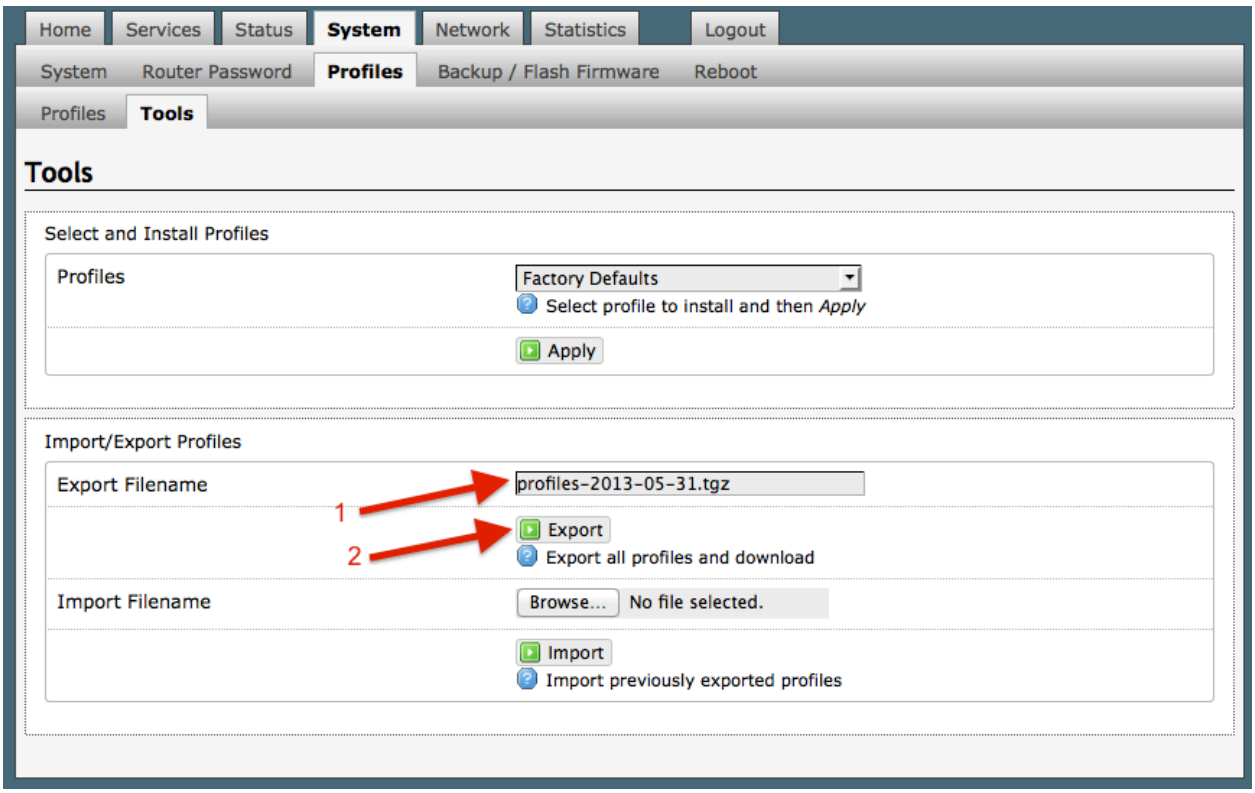
2. Enter a Name of the new profile and a description.
3. Select <Save & Apply>.

7.2.2 Change to Another Saved Profile

To change from using one profile to different profile, simply select <Install> for the desired profille, then <Save & Apply>

7.2.3 Export a Profile

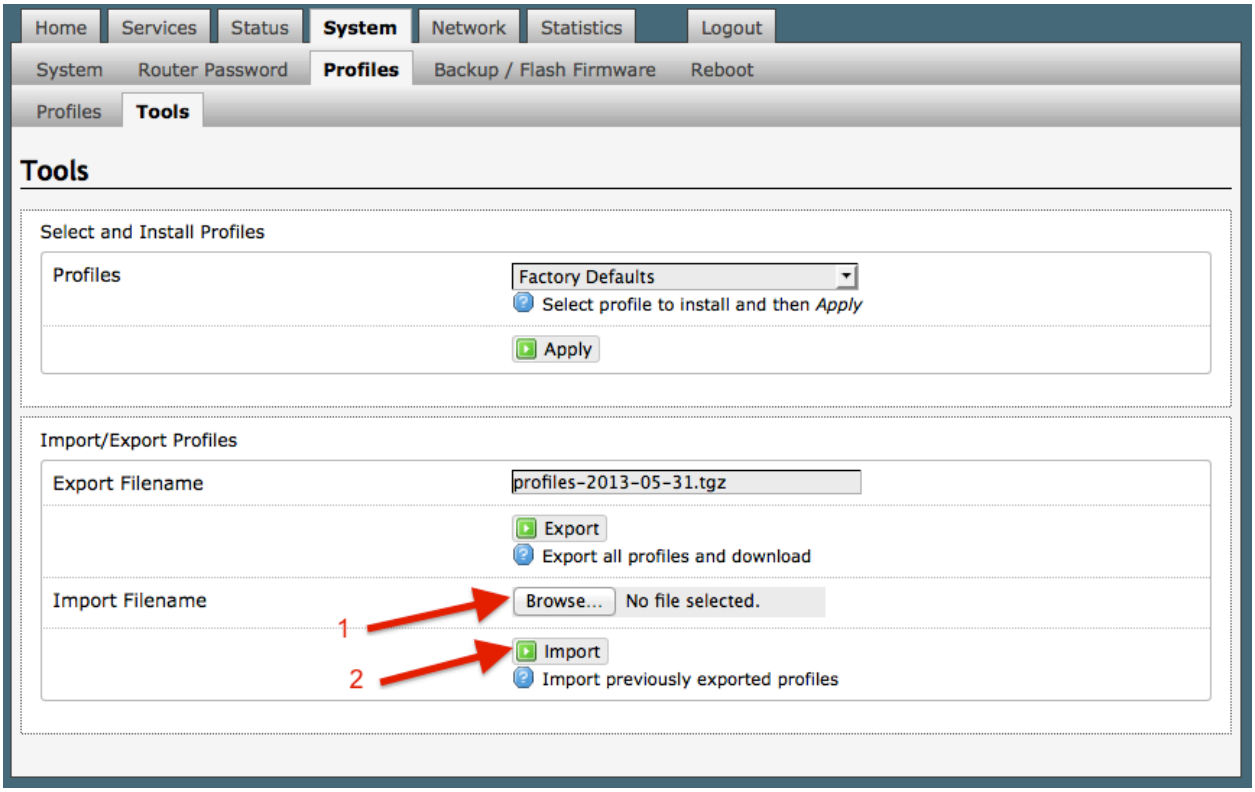
You can export the profiles from the router and use the exported file to 'clone' another Optimizer Crew router in System > Profiles > Tools.



1. Enter a filename or use the default name.
2. Select <Export> and save the file.

7.2.4 Import a Profile

You can import profiles from another Optimizer Crew router in System > Profiles > Tools.



1. Select <Browse> to locate the saved profiles .tgz file.

2. Select <Import>

7.3 Backup/Flash Firmware

You can create backups of the router configuration and restore the configuration to previous backup states.

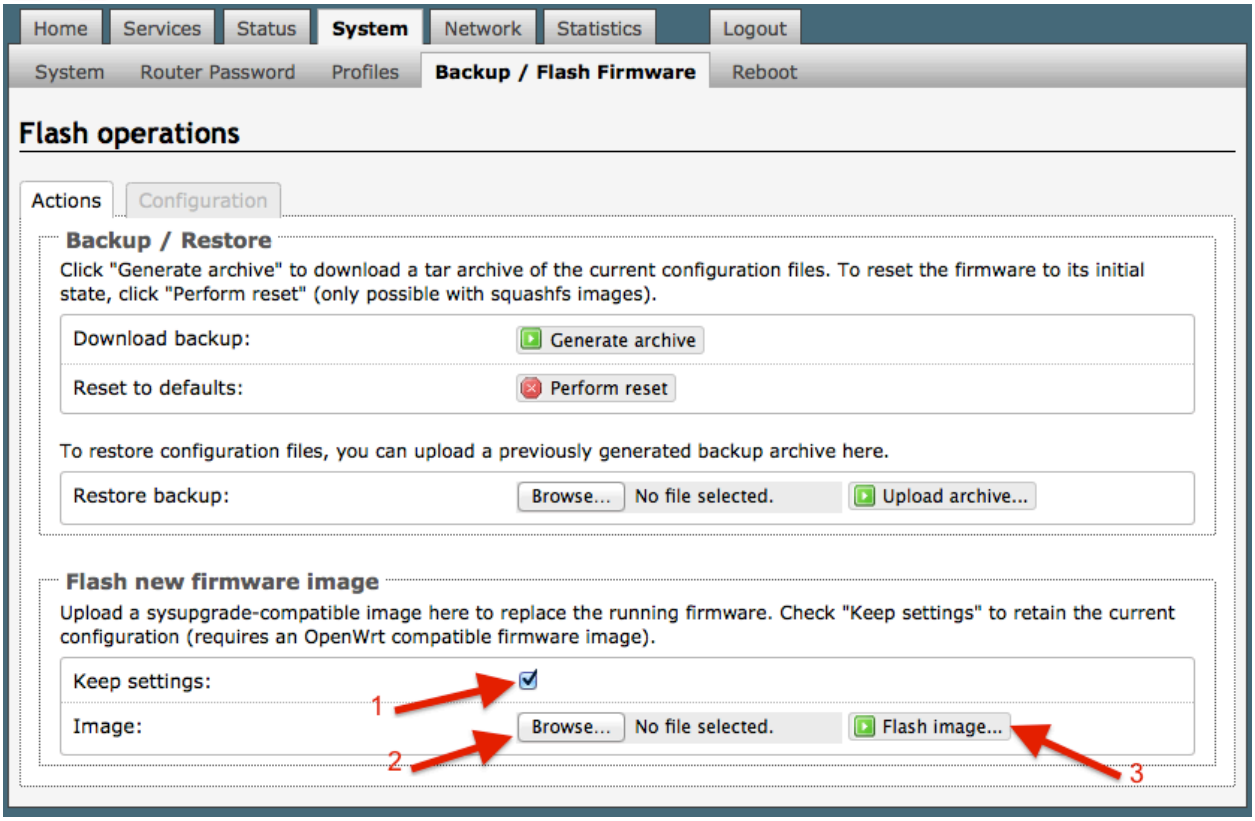
This screen also allows you to upgrade the firmware to the latest version.

Firmware Upgrade

Get the latest Optimizer firmware version from here:
http://www.redportglobal.com/support/technical-downloads/

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

BEST PRACTICE: If you have created any Profiles you may want to Export them before flashing new firmware and Import them when done.



1. **Keep Settings**: check this box to maintain current settings if you have made changes to the congifuration. Failure to check this box will revert the Optimizer back to the default settings.

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

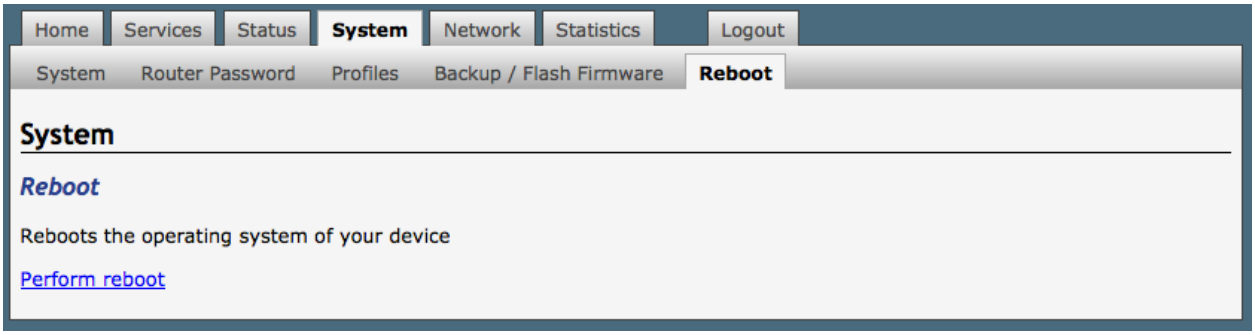
3. **<Flash Image>**

4. Wait for the lights on the front of the Optimizer to begin flashing. When the flashing lights stop, the firmware update is complete. 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

You can reboot the Optimizer from within the user interface in lieu of using the reset button on the router itself.

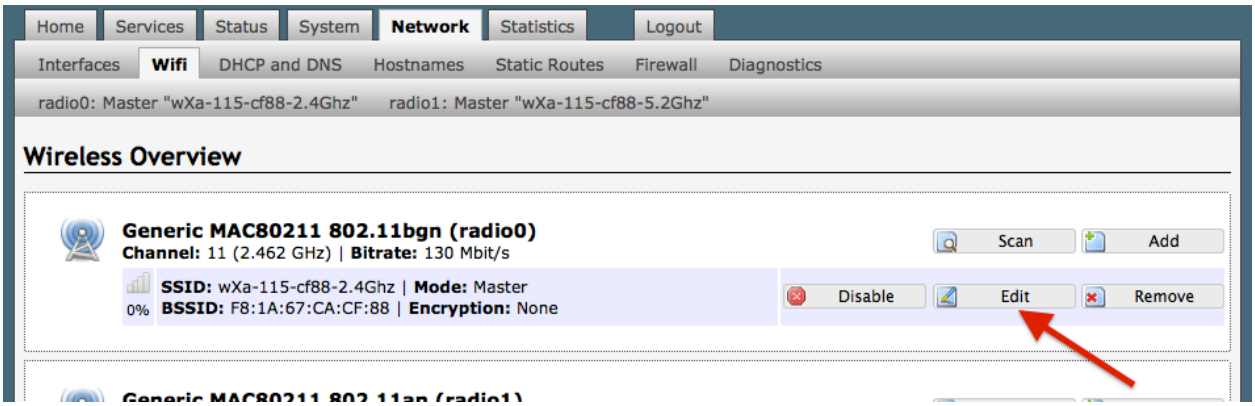


8.0 Network

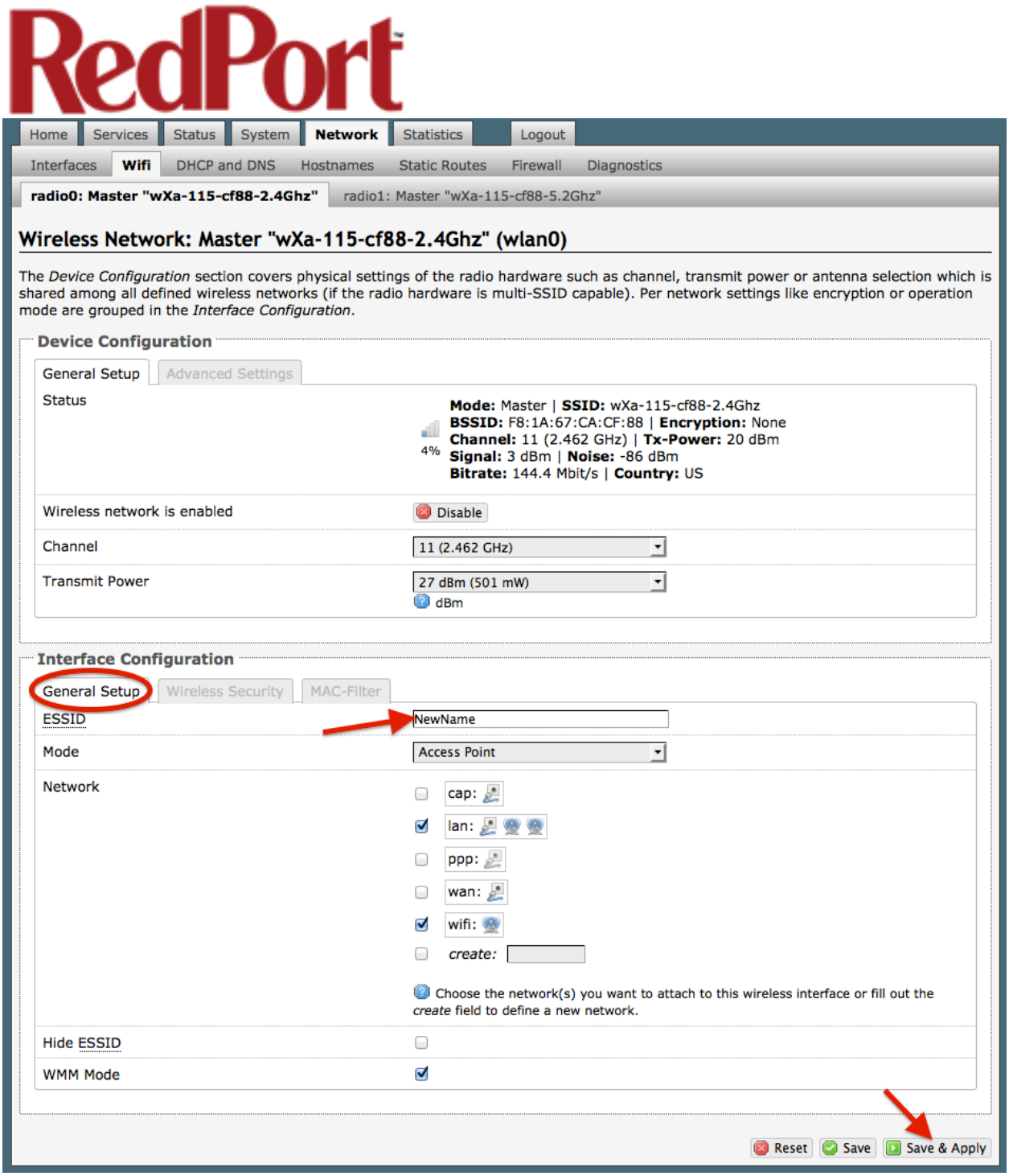
Use this section to configure network interfaces, run diagnostics, or modify the firewall. This gives you complete control over the router behavior.

8.1 Rename the Wireless Network

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-115-xxxx where the xxxx represents a unique number.



Locate the wXa wifi network and select <Edit>



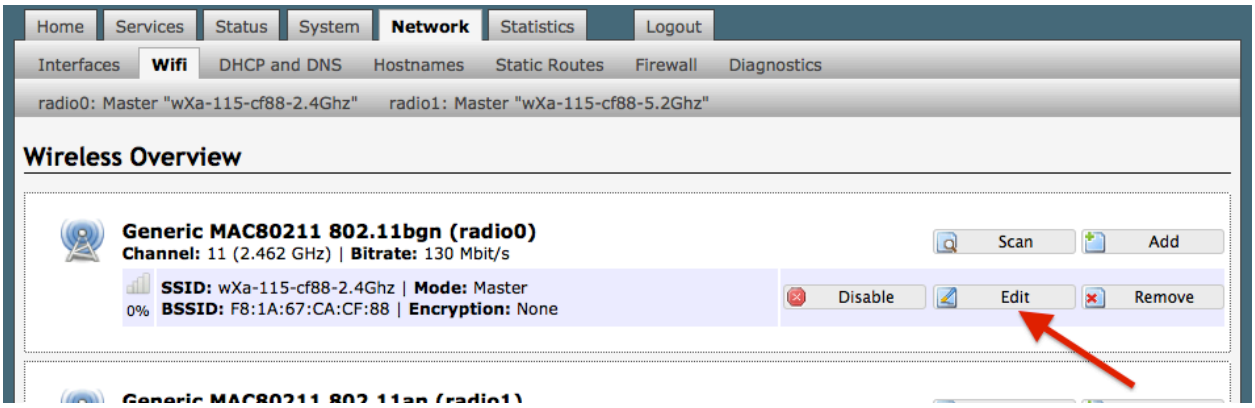
1. Enter the new wireless network name in ESSID field.

2. Click <Save & Apply>

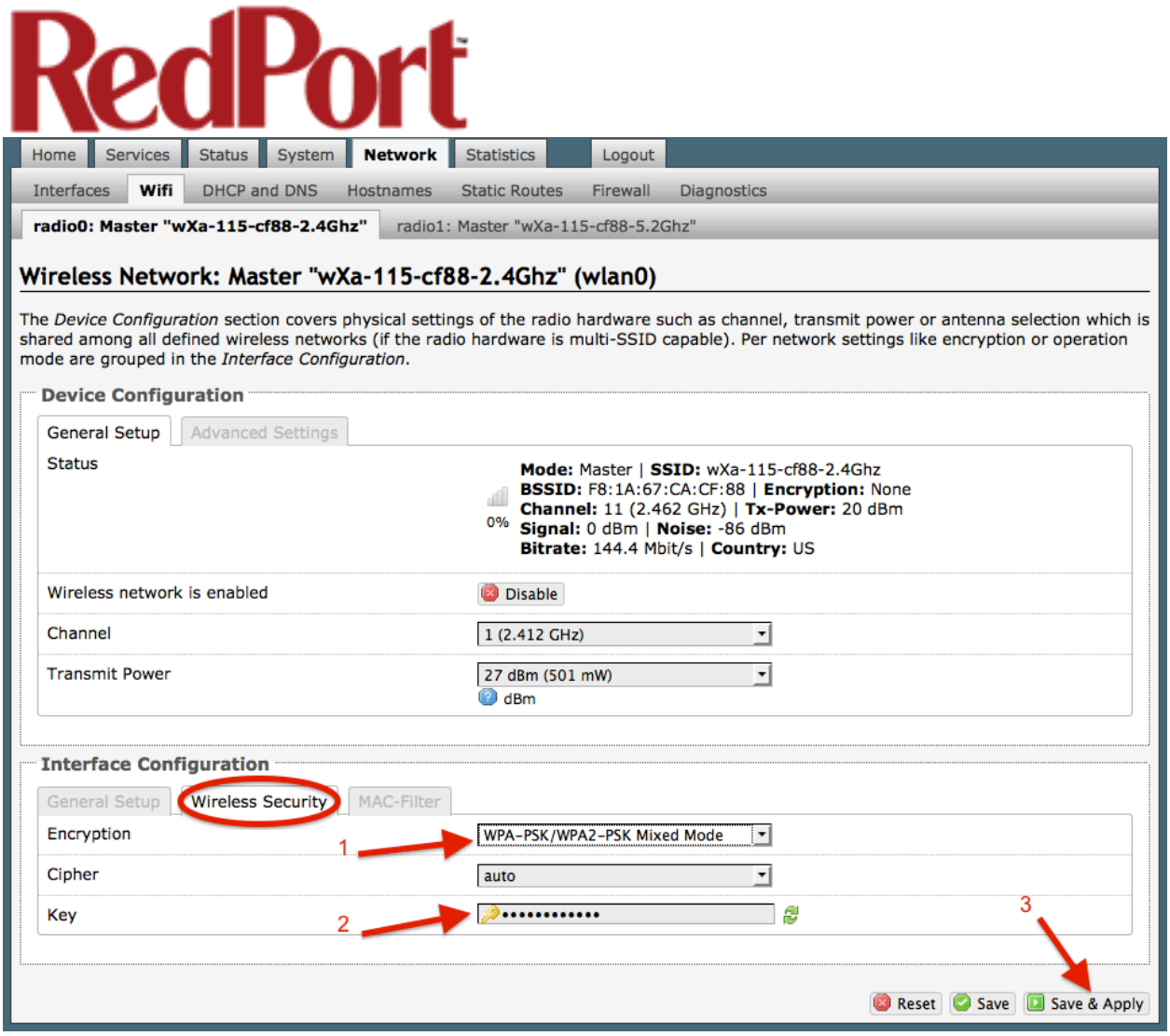
This procedure changes the name for the WiFi hotspot only. When connecting your computer, iOS or Android device to the wireless network, this is the network name that will appear in the wireless network list. This name does not change the router superadmin or admin name when logging in to access the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

8.2 Restrict Wireless Network Access

When in public locations, for example, a busy port, you may want to restrict access to the WiFi hotspot created by your satellite device and the Optimizer. You can password protect the WiFi hotspot so others cannot use it.



Locate the wXa wifi network and select <Edit>



1. Select the Encryption mode from the drop down menu.

2. Enter your desired password in the Key field.

3. Click <Save & Apply>

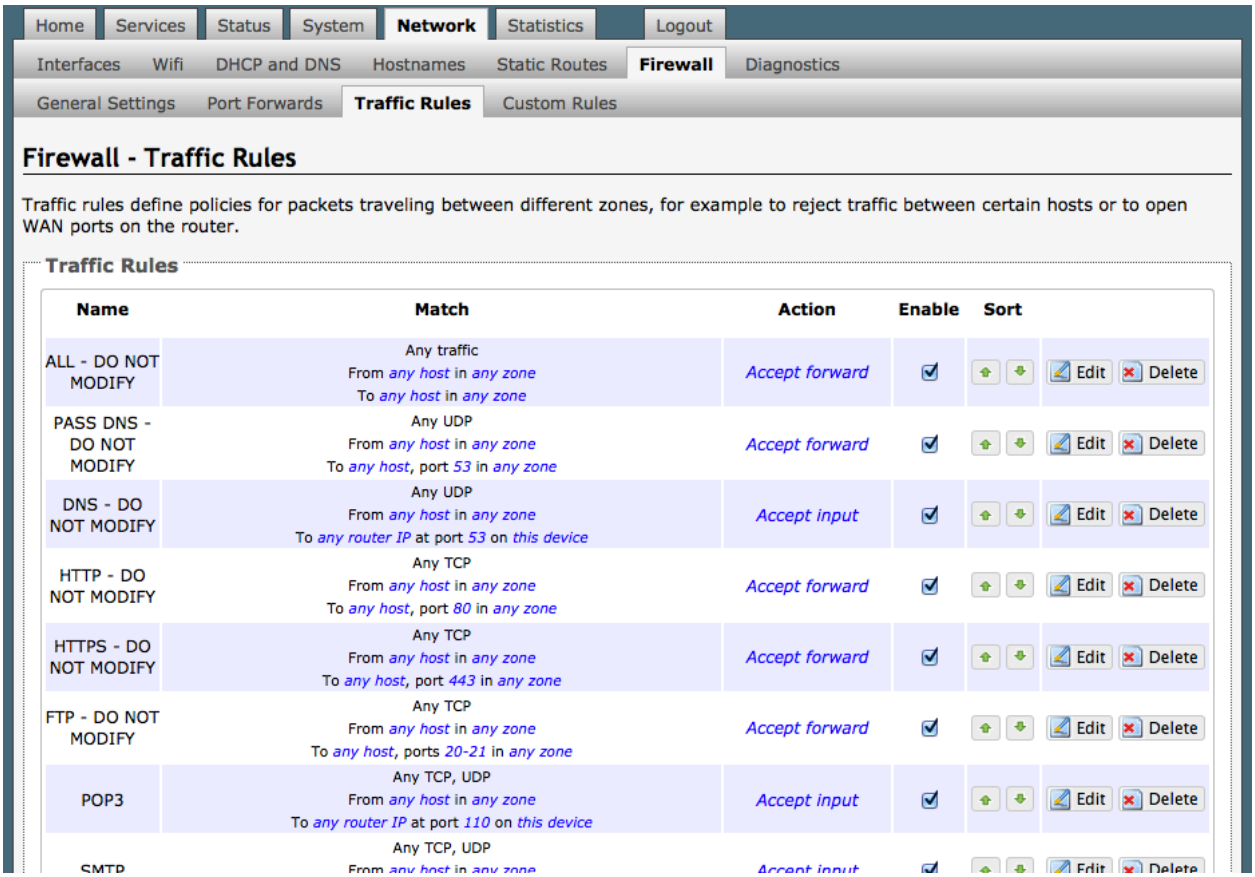
This procedure adds/changes the password for the WiFi hotspot only. When connecting your computer, iOS or Android device to the wireless network, this is the password you will use. This password does not change the router superadmin or admin password when logging in to access the Optimizer user interface.

8.3 Firewall

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 modifications due to the flexibility with the Captive Portal configuration and the Proxy Filters configuration. ***Use with caution and at your own risk!***

Traffic Rules Table

The image below is a small section of the firewall traffic rules table.



The table includes all the firewall rules on the router that will allow you to enable and disable ports and ip address, etc. You can create and add rules. You can delete rules.

By default, the first six rules say DO NOT MODIFY. They are: ALL, Pass DNS, DNS, HTTP, HTTPS and FTP. These are the rules that the Captive Portal and Proxy Server automatically enable and disable so the components work without you having to make modifications to the

Traffic Rules Table. When enabled, these rules Allow that particular traffic to pass through the firewall.

All the rules can easily be enabled (checked) or disabled (unchecked).

The first 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 hit <Save & Apply>. With the ALL rule disabled, the remaining rules spring into action.

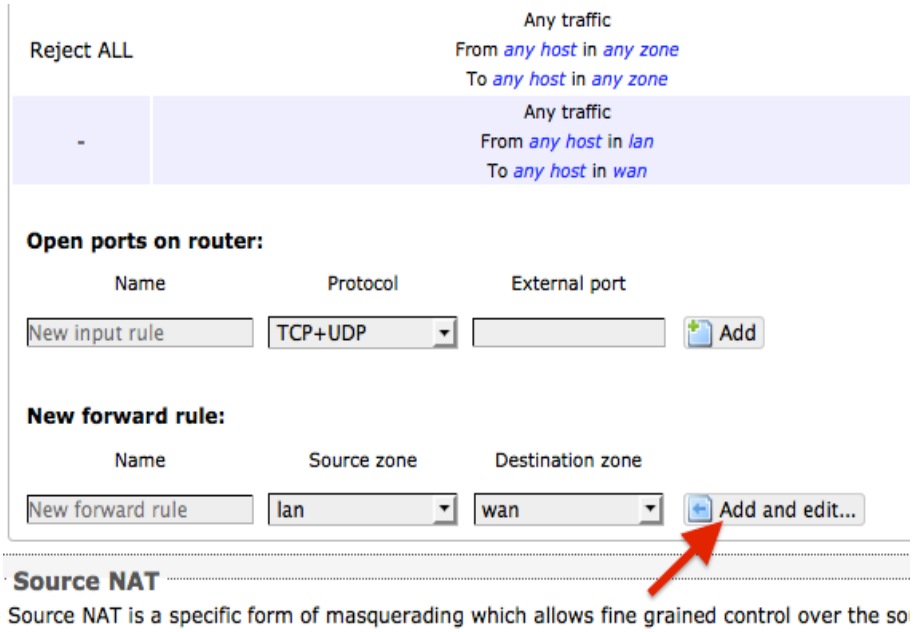
Rules are evaluated from top to bottom. As soon as traffic hits a rule that matches, it will stop. If there is no match it will continue to the bottom, which is the Reject rule.

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

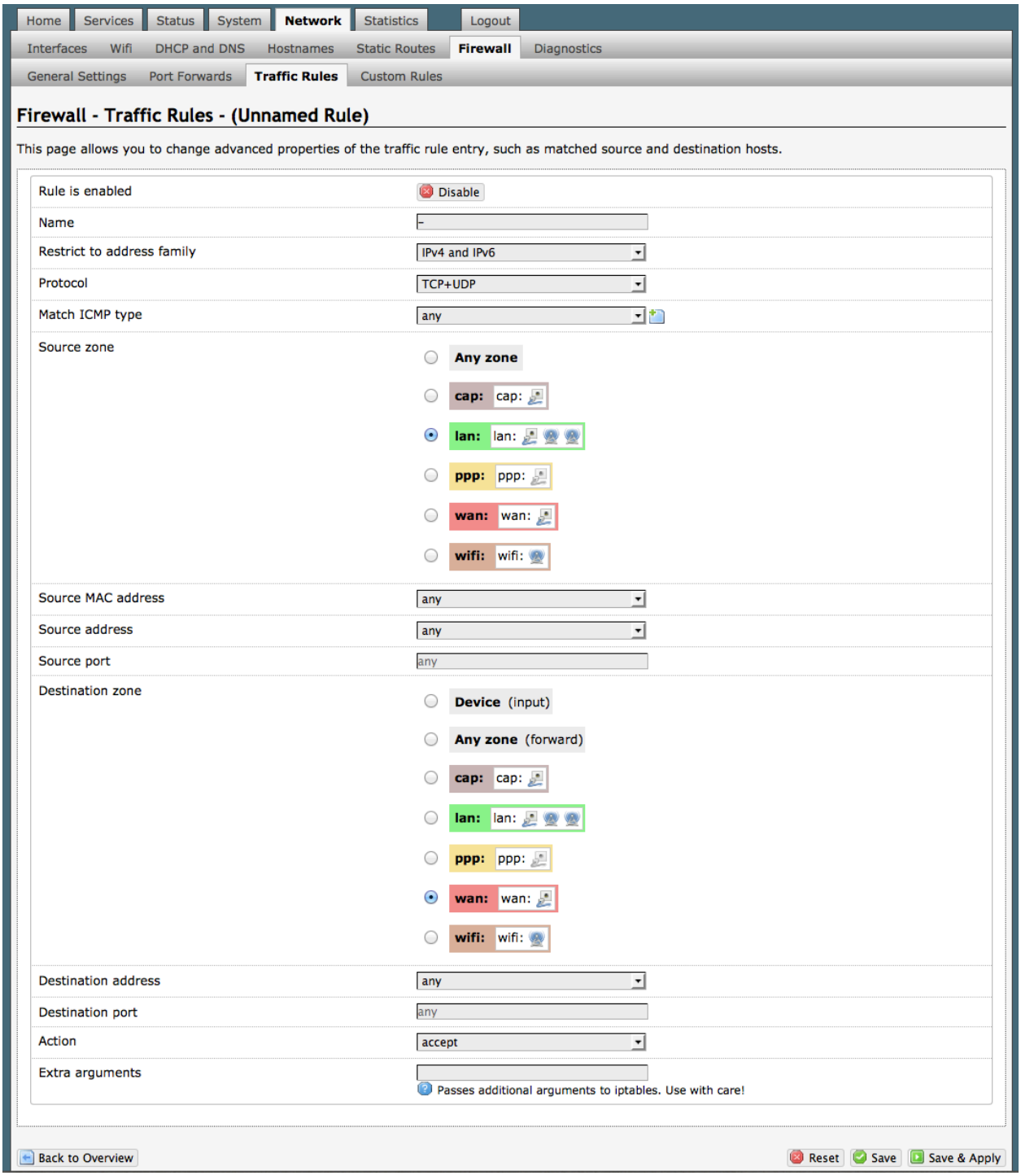
- Disable (uncheck) the first rule "ALL-DO NOT MODIFY". This forces the remaining rules to take precedent.
- Disable (uncheck) the rule "HTTP-DO NOT MODIFY". This blocks http traffic from passing through the firewall.
- When http traffic arrives, it processes down the list of the enabled rules. Because http is not enabled it continues down the list looking for match. Failing to find a match until it reachs the last rule "REJECT".

With the 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. Scroll down to the bottom of the page to the section "New forward rule"



Select <Add and edit>:

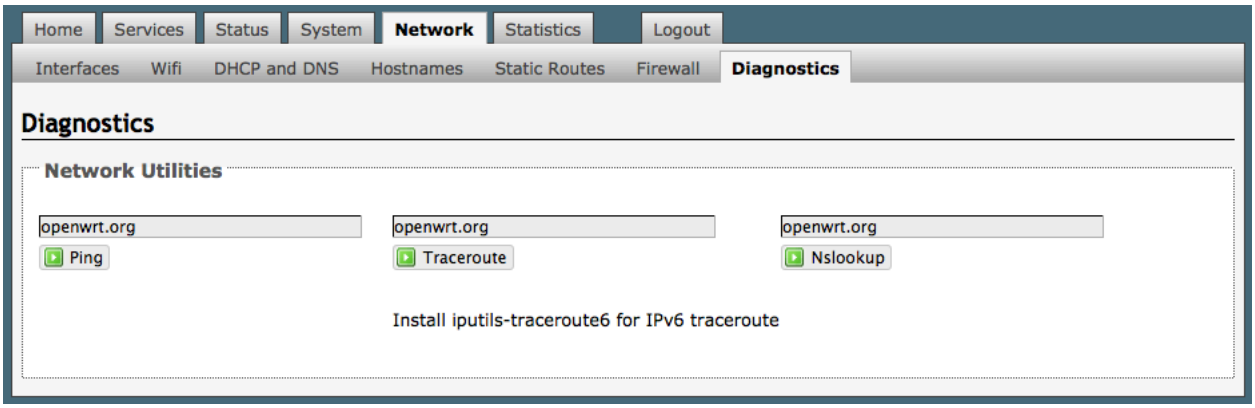


Here you can give the new rule a name, specify the protocol, restrict the rule to a certain zone, identify the source ip address, the destination ip address, port numbers. etc. This is standard firewall convention. Once the rule is created, select <Save & Apply>. Place the rule where you

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.

8.4 Diagnostics

There are several Diagnostic tools available:

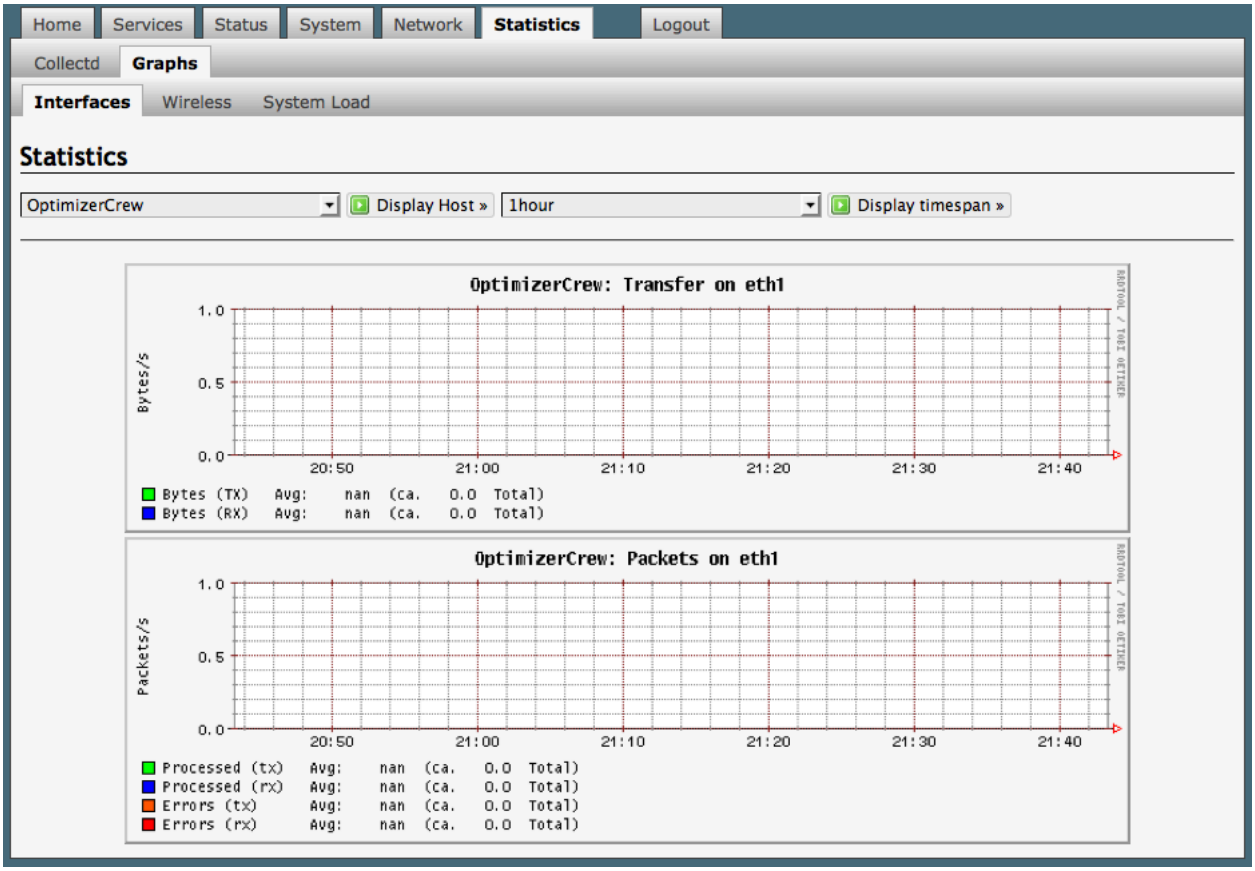


Ping: tells you if you have ip connectivity

Traceroute: gives you all the ip addresses in a hop to the final destination.

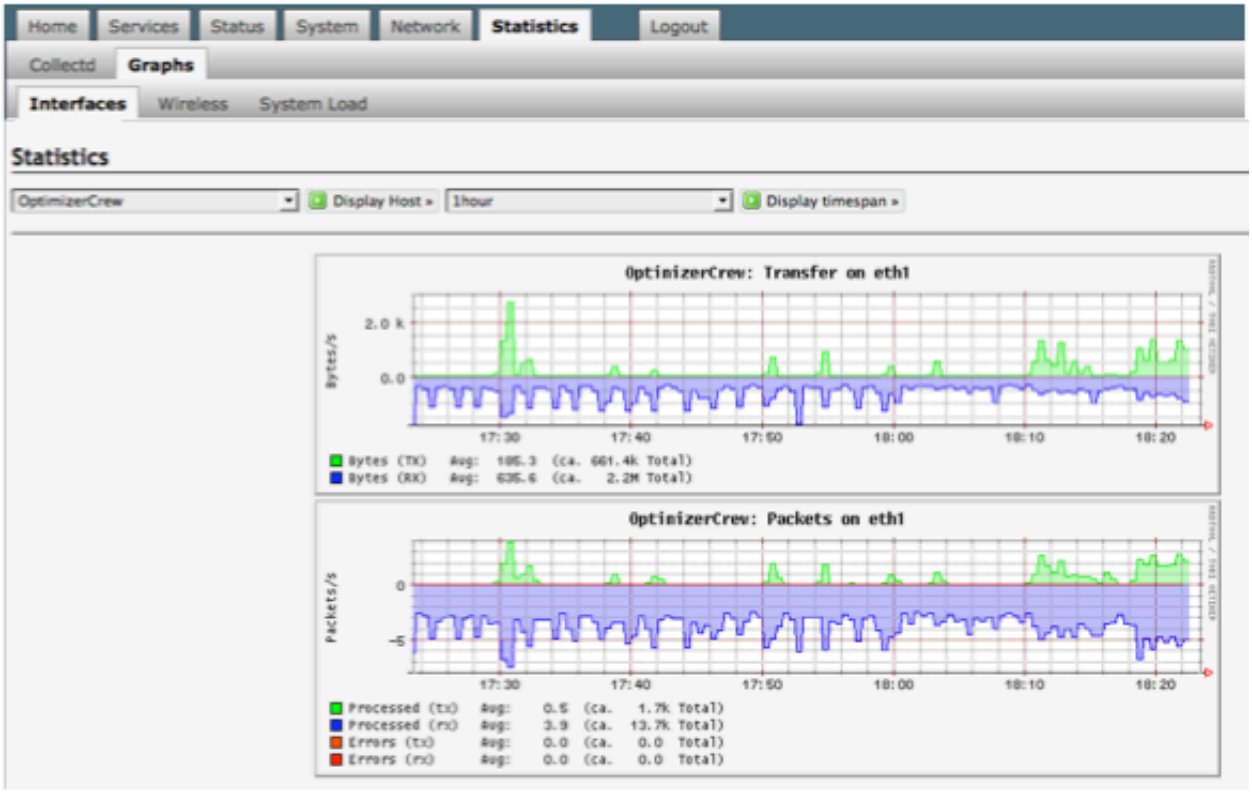
9.0 Statistics

Similar to the Realtime Graphs in the Status tab, Statistics Graphs shows usage over a specific timespan.



To modify the timespan use the down arrow next to <Display timespan>, then select <Display timespan> to view the graph.

RedPort


Home
Services
Status
System
Network
Statistics
Logout
Collectd
Graphs
Interfaces
Wireless
System Load
Statistics
OptimizerCrew
Display Host »
1hour
Display timespan »
OptimizerCrew: Transfer on eth1
Bytes/s
2.0 k
0.0
17:30
17:40
17:50
18:00
18:10
18:20
Bytes (TX) Avg: 185.3 (ca. 661.4k Total)
Bytes (RX) Avg: 635.6 (ca. 2.2M Total)
OptimizerCrew: Packets on eth1
Packets/s
0
-5
17:30
17:40
17:50
18:00
18:10
18:20
Processed (tx) Avg: 0.5 (ca. 1.7k Total)
Processed (rx) Avg: 3.9 (ca. 13.7k Total)
Errors (tx) Avg: 0.0 (ca. 0.0 Total)
Errors (rx) Avg: 0.0 (ca. 0.0 Total)

OPTIMIZERCREW

Installation Notes

Installation

The blue Ethernet connector on the back of the unit should be connected to your broadband satellite device. The broadband satellite unit should be configured as a DHCP server, which is the default for most terminals.

The 4 yellow Ethernet connectors are LAN adapters and are bridged to WiFi. There are 2 WiFi transmitters with frequencies at 2.54 and 5.2 Ghz. The WiFI SSID is of the form "wxa-115-XXXX-frequency" where XXXX is the last 4 digits of the unit's WiFi interface MAC address and "frequency" is the transmission frequency of the transmitter. The WiFi is unsecured so no password is required to connect to this device.

Connecting to the Device

Connect a PC to either the LAN or WiFi on the router. Alternately, administrators can access the unit through the WAN port. The router is configured as a DHCP server so PCs should be able to access the router and the Internet once they are connected.

Router Interface Addresses

LAN/WiFi bridge: 192.168.10.1
Captive Portal: 10.1.5.1
WAN: DHCP

New Feature:

Multi-Level Access To Optimizer Crew User Interface

There are two levels of administrative access for Optimizer Crew:

RedPort

Admin

- Create PIN-codes for controlled Internet access
- Manage users
- Create email subaccounts for guests and crew
- View CDRs (Usage Records)

"Admin" access is designed for the on-site administrator who may not have the technical knowledge required to configure the router. Basic functions (like creating PIN-codes) can be accessed, but more advanced features like router and network configuration require "Superadmin" access.

Superadmin

"Superadmin" access is designed for the installer/technician/network administrator. It allows full access to the user interface for setup, configuration, and maintenance of the router.

Router Admin Login

Superadmin
Username: superadmin
Password: webxaccess

Admin
Username: admin
Password: webxaccess

Default Router Configuration

Optimizer Crew is shipped with the following configuration:

1. Captive portal enabled, allowing for crew Internet access with pincodes or administrator assigned username and password.
2. Transparent proxy for http URL and content filtering.
3. Open firewall allowing full access to the Internet once the crew member logs into the captive portal.
4. Open DNS allowing the resolution of IP addresses for all machines on the LAN/ WiFi whether logged in or not through the captive portal.

5. RedPort email, web compression, and VOIP servers white listed through the captive portal. The captive portal in this configuration does not account for use of XGate/XWeb software or RedPort VOIP.

Note that browsers needing to access the Internet require DNS. DNS will generate traffic that is not accounted for by the captive portal. On networks with multiple PCs this traffic can be considerable.

First Use with XGate, XWeb, and/or RedPort VOIP

No router changes or configuration is required when using XGate, XWeb or RedPort VOIP services. The router is configured to allow this traffic through. The Optimizer Crew blocks all other traffic except for DNS.

XGate/XWeb users should refer to the Optimizer Quick Start Guide when using Optimizer Crew in this mode.

First Use

Users must log in through the captive portal before they can access the Internet. To log in, open a browser and enter a URL such as http://www.amazon.com. The captive portal will intercept the request and redirect the user to a login page. A valid username/password or pincode must be entered before access to the Internet is granted.

Once logged in, any application (web based or otherwise) should have access to the Internet.

Captive Portal Usage

As stated above, entering an http:// URL into a browser redirects the user to the captive portal login page. Alternately, users can access the captive portal directly using one of the following URLs.

- Login – http://10.1.5.1:4990/www/login.chi
- Status – http://10.1.5.1:4990/www/status.chi
- Logout – http://logout

The captive portal status page provides status information for the current active session such as:

- Max Session Time: maximum allowed time before user is forcibly logged off.
- Max Idle Time: user is logged off automatically if no traffic is observed within this period.
- Start Time: session start time.
- Idle time: time of idle activity.
- Downloaded: amount of data transferred to the user.
- Uploaded: amount of data requested by the user.
- Original URL: URL that initiated the login request.

Users can end a captive portal session by either clicking the logout link on the status screen or by entering http://logout in their browser.

The captive portal ships configured with two accounts. They are:
- admin/webxaccess
- test/1234

The admin account is open and has no restrictions. The test account is restricted to 10Mbytes of total usage at a speed of 128kbps.

Router Administration

When the captive portal is enabled, the router admin page is accessed via http://10.1.5.1. However, this URL will not work when the captive portal is disabled and not in use.

When the captive portal is disabled, the router admin page is accessed via http://192.168.10.1.

Web Compression

You must have a valid web compression account before using this feature. Please contact your RedPort dealer and request a username and password for the compression service.

Once you have your account information, log in to the router and browse to Services > Web Compression and Filtering > select the Compression tab. Check the Enable Compression option and enter your assigned credentials. Click <Save & Apply>.

You should now be able to browse the Internet with compression enabled.

RedPort

Optimum Setup

The default configuration works well offering reasonable bandwidth over-utilization protection. With the default, users must log in through the captive portal before they can access Internet resources. However, once logged in, their computers can generate unwanted usage that causes their pincodes to be consumed quickly. Users can also use Skype and other P2P applications that require a lot of bandwidth.

Also note that DNS access must be enabled to use the default configuration. Without DNS, web browsers timeout when trying to resolve host names which prevents them from being redirected to the captive portal login page. DNS can drive unexpected large bandwidth usage because it is accessible to all computers and programs running on the local network. 30-50Mbytes per month in DNS traffic usage is not unusual for vessels with 10 or more computers connected to the LAN and powered on all the time.

The following configuration blocks all traffic to the Internet. Users must log in though the captive portal to have access to HTTP and HTTPS traffic. All other traffic is blocked, preventing Skype and other P2P applications from working. This setup also has the advantage of passing HTTPS traffic through the filtering proxy server that allows the administrator to block sites. Users, when using this alternate setup, will need to change the default settings in their browsers and use the direct captive portal login link to login.

The following procedure will enable the alternate optimum setup:

1. Log in to the Optimizer Crew admin portal.
2. Navigate to Network > Firewall > Traffic Rules
3. Uncheck the first 6 rules at the top of the list labeled "XX – DO NOT MODIFY" where XX is ALL, PASS DNS, DNS, HTTP, HTTPS, and FTP.
4. Select "Save and Apply" at the bottom of the page. This will modify the firewall to block access to all traffic including DNS.
5. Instruct the end user to modify their browser configuration to enable "Automatic Proxy Detection". For Firefox this is done under Preferences > Advanced > Network > Settings by selecting "Auto-detect proxy settings for this network". Other browsers can be configured similarly.
6. Instruct the user to use the captive portal URL to access the login page. This is done by entering http://10.1.5.1:4990/www/login.chi in the browser.
7. Once logged in, the user will have access to all http and https websites.
8. Entering http://logout will log the user out of the captive portal and end his session. Alternately, the user could use the status page at http://10.1.5.1:4990/www/status.chi and log out from there.

Factory Default

Optimizer Crew can be reset to factory default by pressing the reset button on the back of the router for 15 seconds and then releasing it. The router will then reboot and start backup with its default settings.

Optimizer Crew Guides

Usage and administration guides can be found at http://www.redportglobal.com

APPENDIX B

Installer's Guidelines for Optimizer Crew Router Customization

The Router is shipped to you in the following Default State:
Legend: E= Enabled, D=Disabled, O=Open

Captive Portal	E	
Transparent Proxy	E	Internal Proxy Server
Firewall	O	
DNS	O	
Web Compression	D	
RedPort Email	D	
GPS Tracking	D	

This list below is designed as a general guideline for customizing the router to meet your needs.

Configuration		Actions	Location in the UI
Captive Portal Use			
	1	Change Captive Portal Admin Password	Services > Crew Internet Access > Tools
	2	Add user accounts	Services > Crew Internet Access > Users
	3	Add to Allowed Hosts table	Services > Crew Internet Access > Settings > Allowed Hosts
	4	Set Content Filtering Scheme	Services > Web Compression and Filtering > Settings > Advanced
	5	Firewall Rules	Network > Firewall > Traffic Rules
	6	Add end user accounts	On-site Administrator
	7	Create Pincodes for Users	On-site Administrator
Web Compression (Premium Service - fees may apply)			
	1	Must be enabled	Services > Web Compression and Filtering > Settings > Compression
	2	Enter User ID and Password	Services > Web Compression and Filtering > Settings > Compression
	3	Set Compression Level	Services > Web Compression and Filtering > Settings > Compression
	4	Enter Whiteliest sites	Services > Web Compression and Filtering > Settings > Compression
	5	Set Content Filtering Scheme	Services > Web Compression and Filterings > Settings > Advanced
	6	Establish Domain and Path Filters	Services > Web Compression and Filtering > Filters
	7	Firewall Rules	Network > Firewall > Traffic Rules
RedPort Email (Premium Service - fees may apply)			
	1	Must be enabled	Services > RedPort Email > General > General Settings
	2	Enter Main Identity Login Info	Services > RedPort Email > General > General Settings
	3	Select satellite connection method	Services > RedPort Email > Connection
	4	Set Inbound Email Filter Size	Services > RedPort Email > Filters
	5	Set Outbound Email Filter Size	Services > RedPort Email > Filters
	6	Enter Primary Accounts Purchased	Services > RedPort Email > Primary Accounts
	7	Add Crew/Sub Accounts	On-site Administrator
GPS Tracking via SMS			
	1	Configure Tracking Parameters	Services > GPS Tracking > Tracking > Tracking via SMS
GPS Tracking via RedPort (Premium Service - fees may apply)			
	1	Configure Tracking Parameters	Services > GPS Tracking > Tracking > Tracking powered by GSatTrack

Please refer to the Optimzier Advanced User Guide and the Optimizer Basic User Guide for details.

APPENDIX C

This table shows the portions of the user interface that are available when using the different login credentials.

	Login	
	admin	superadmin
Home Page	✔	✔
Services Tab		✔
Crew Internet Access-Captive Portal		✔
Settings		✔
General Settings		✔
Advanced Settings		✔
Allowed Hosts		✔
WPAD		✔
Users	from Home Page	✔
Pass-Through MAC		✔
Pincodes	from Home Page	✔
CDRs	from Home Page	✔
Tools	from Home Page	✔
Web Compression and Filtering		✔
Settings		✔
Compression		✔
General Settings		✔
Advanced Settings		✔
Filters		✔
Log		✔
Help		✔
RedPort Email		✔
General		✔
General Settings		✔
Webmail Settings		✔
Network Settings		✔
Log Settings		✔
Mail Filtering		✔
Connection		✔
Filters		✔
Primary Accounts		✔
Crew Accounts	from Home Page	✔
Spool		✔
Tools	from Home Page	✔
BigMail	from Home Page	✔
Logs		✔
Transaction Log		✔
POP Log		✔
SMTP Log		✔
Usage CDRs		✔
Connection Report		✔
SMS		✔
Settings		✔
Management		✔
GPS Tracking		✔
WiFi Extender		✔
GPS/NMEA Repeater		✔
PPP		✔
Status		✔
Settings		✔
Network		✔
PPP		✔
GSM		✔
Signal Monitor		✔
Log		✔

	Login	
	admin	superadmin
Status Tab - All	✔	✔
System Tab		✔
System		✔
General Settings		✔
Logging		✔
Language and Style		✔
Router Password	from Home Page	✔
Profiles		✔
Profiles Manager		✔
Tools		✔
Back/Flash Firmware		✔
Actions		✔
Configuration		✔
Reboot	from Home Page	✔
Network Tab		✔
Interfaces		✔
WiFi	from Home Page	✔
DHCP and DNS		✔
General Settings		✔
Resolv & Host Files		✔
TFTP Settings		✔
Advanced Settings		✔
Hostnames		✔
Static Routes		✔
Firewall		✔
General Settings		✔
Port Forwards		✔
Traffic Rules		✔
Custom Rules		✔
Diagnostics		✔
Statistics Tab		✔
Collectd		✔
Network Plugins		✔
Output Plugins		✔
System Plugins		✔
Graphs		✔
Interfaces		✔
Wireless		✔
System Load		✔
Logout	✔	✔

If you have questions that are not answered in this guide, please email your service provider for assistance or you can contact us at: support@redportglobal.com and we will direct your inquiry to your service provider.