Optimizer Premier

Advanced User's Guide

for Installers/Network Administrators

RedPort Router:
wXa-165 (Optimizer Premier)

RedPort

Table of Contents

Revision History

Date	Revision	Author
April 15, 2016	Initial Release	D. Brickhouse
September 21, 2016	Version 1.3	D. Brickhouse

1.0 About this Guide

This guide is intended for installers and network administrators of the RedPort Optimizer Premier wXa-165 routers. 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 PIN-Codes, create users, and look at call data records for the Captive Portal, create and manage crew email accounts, etc. *See the Optimizer Premier Onsite Administrator Guide for details.*

For information regarding the installation of the hardware, please see the *RedPort Optimizer Premier QuickStart Guide*.

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

2.0 Introduction to Optimizer Premier

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, 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 Premier is a VoIP gateway and data router that provides an all-in-one solution for those looking to get the most out of all available data connections including long-range cellular, WiFI, and satellite broadband services.

2.1 Key Features

- Configurable to automatically select among available data connections to choose the lower-cost or preferred available service. Full-featured load balancing and least-cost routing.
- VoIP to circuit-switch conversion allows calls using a smartphone over the satellite connection. Some satcomm systems may require additional hardware.
- Compatible with RedPort VoIP service for voice call savings and controlled use.
- Flexible Routing to manage even the most complex network.
- Proxy Server enables HTTP filtering: whitelist/blacklist of URL's, domains, and rudimentary content filtering.
- Powerful firewall accommodates virtually any installation scenario, with advanced features including block or allow any range of port, IP address and protocols; port forwarding, network address translation and detailed whitelisting and blacklisting of websites and services.
- GSM Compatibility with optional GSM modem (and your own SIM card) and optional GSM external antenna and/or amplification.
- Remote Router Access available to manage the network from any Internet connection.
- Supports Shared Web Compression with transparent proxy service.
- Captive Portal included for locally controlled access by crew and passenger.
- Supports RedPort XGate Email Service via included full POP/SMTP RedPort Mail Server for easy local email access.
- Supports GPS Tracking.
- Multi-Interface Failover and Load Balancing support.

- GPS NMEA Repeater reads the built-in GPS in any satellite broadband terminal and rebroadcasts via WiFi for access by an NMEA compliant device.
- Long-range WiFi compatibility with optional compatible WiFi systems
- Broadcasts data connection for use with WiFi enabled devices.
- Compatible with virtually any IP-based satellite broadband terminal.

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 5.6.*
- **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*. See Chapter 5.4.*
- **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. *See Chapter 5.7*.
- **WiFi Extender** support. *See Chapter 8.2.*
- **GPS SMS Tracking** via satellite provider's SMS service with compatible satellite device. *See Chapter 5.5.*
- **Transparent Proxy** to redirect HTTP traffic for filtering. *See Chapter 5.2.*
- **GSM Support** with optional GSM modem and your own GSM SIM card. *See Chapter 8.8.*
- **Automatic Failover** as WiFi > GSM > Sat1 > Sat2. Easily configurable to meet your needs. *See Chapter 8.9.*

2.3 Premium Services Available

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

- **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. *See Chapter 5.7.*
- **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 Optimizer RedPort Email Administrator's Guide.*
- **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.*

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

- *(COMING SOON) **Shared Captive Portal Pincode Service** - Upgrade the Captive Portal to our upstream pincode server for shared pincode service for your crew/team. These pincodes can be used at any of your installations with the Optimizer Premier router and Shared Pincode Service enabled. See Chapter x.x for details.*

3.0 Important Things to Know Before Getting Started

3.1 More Than Just a Router

The Optimizer Premier 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 Pin-Code or Mac address of a specific PC. The Captive Portal is enabled by default.

2. 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.

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. In a multi-wan environment, each interface can have separate rules applied.

IMPORTANT NOTE: This router is shipped to you with all WAN ports open, POP and SMTP are open to the WAN if you enable Email, if you enable the 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.

3.2 Designed Use of the Optimizer Premier

This router is designed for use in a multi-comm device environment for one or more users with the convenience of BYOD (bring your own device) for crew and passenger access to Email, Web Browsing and Voice. 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.

IMPORTANT NOTE: Prior to installation, review Chapter 4.3.1 How to Secure Your Router.

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 PIN-Codes, 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 Premier Onsite Administrator Guide.*

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

We ship the router ready for use with Captive Portal enabled for Crew Internet Access, Voice and SMS are enabled for use with compatible satellite devices, and Automatic Failover is configured in the order of WiFi Network > GSM > WAN1(Sat1) > WAN2(Sat2) to take advantage of the typically lower cost connections of WiFi Networks and GSM, if/when they are available.

Prior to making modifications to the router configuration, please see Section 3.4 How Data Flows Through the Router to determine the customization required to best meet your needs.

Best Practice is to have a knowledgeable technician (someone who knows about proxy servers, firewalls, and routers) go through and generate a custom configuration.

Using the guidelines in *Appendix A*, the installer will want to address the following areas prior to first use:

- configure the Captive Portal for Crew Internet Access
- configure the internal proxy server (Transparent Proxy)
- configure GSM (requires configuration of PPP interface)
- configure automatic failover/load balancing
- configure SMS
- configure Voice PBX

OPTIONAL:

- enable the upstream proxy for the benefit and cost savings of Shared Web Compression Service
- enable RedPort VoIP Service for savings on voice calls
- configure GPS interface

In a fleet environment, the custom configuration can be recorded and used on other Optimizer Premier routers within the organization.

IMPORTANT NOTE: This router is shipped to you with all WAN ports open, POP and SMTP are open to the WAN if you enable Email, if you enable the 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.

3.4 How Data Flows Through the Router

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

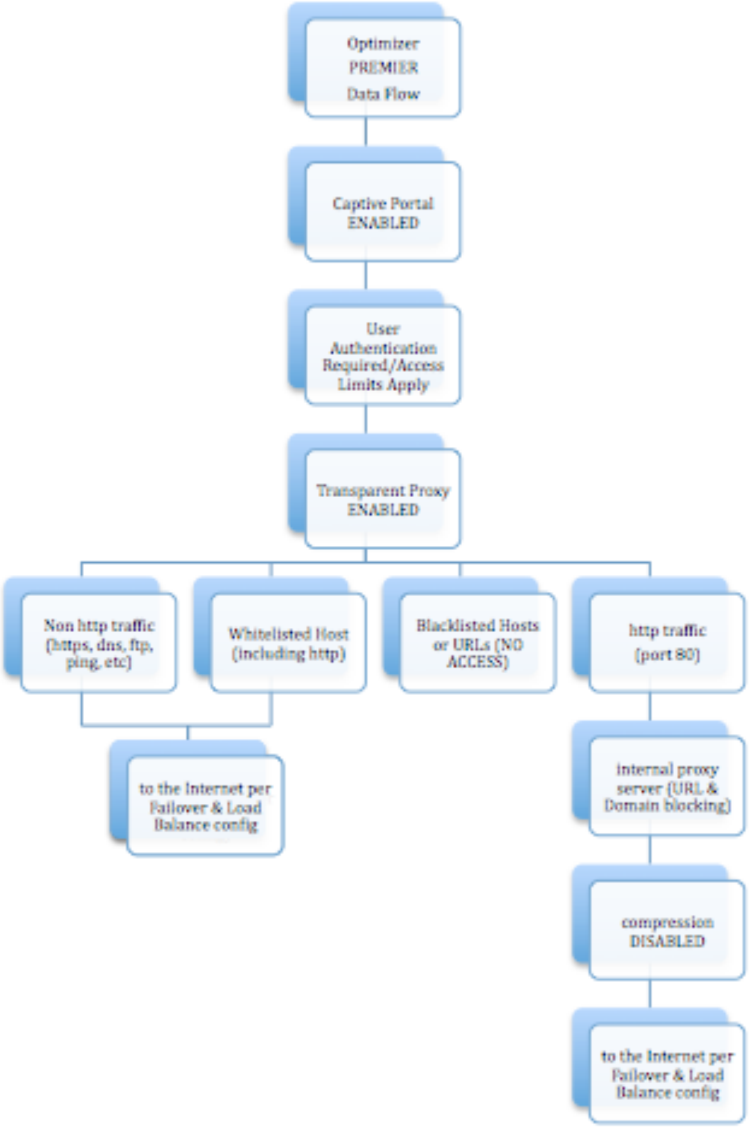
3.4.1 Default Configuration

Captive Portal (Crew Internet Access) - enabled
Internal Transparent Proxy for http URL and content filtering - enabled
Firewall - open
DNS - open
SMS - enabled, for compatible satellite devices
Voice Capability - for compatible satellite devices, disabled
Automatic Failover/Load Balance (All Traffic) - Wifi > GSM > WAN1 > WAN2
Web Compression Service - disabled
RedPort Email Service - disabled
GPS Tracking Service - disabled
RedPort VoIP Service - disabled

With the Captive Portal enabled, the firewall is automatically modified to allow data traffic through the router and users must 'authenticate' in order to access the Internet. You have several methods available for controlling user access to the Internet: you can whitelist and/or blacklist hosts and urls; you can modify the firewall, you can modify the load balance to allow only certain traffic types thru a certain interface, and you can require the use of PIN-Codes. When generating PIN-Codes you can set the amount of data the user can download, you can limit access to certain hours of the day, and you can limit the speed of their connection.

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.*


Optimizer PREMIER Data Flow
Captive Portal ENABLED
User Authentication Required/Access Limits Apply
Transparent Proxy ENABLED
Non http traffic (https, dns, ftp, ping, etc)
Whitelisted Host (including http)
Blacklisted Hosts or URLs (NO ACCESS)
http traffic (port 80)
to the Internet per Failover & Load Balance config
internal proxy server (URL & Domain blocking)
compression DISABLED
to the Internet per Failover & Load Balance config

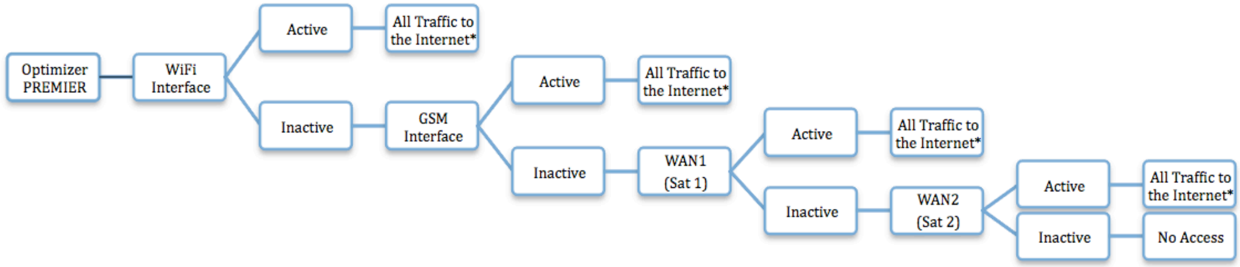
2. Traffic to a Whitelisted Host in the Captive Portal, including http, goes straight to the Internet, bypassing the internal proxy server. If you whitelist a webserver, that traffic goes straight to the Internet, bypassing the internal proxy server, so there is no filtering. Typically you would not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

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.

- In the default state of compression 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.*

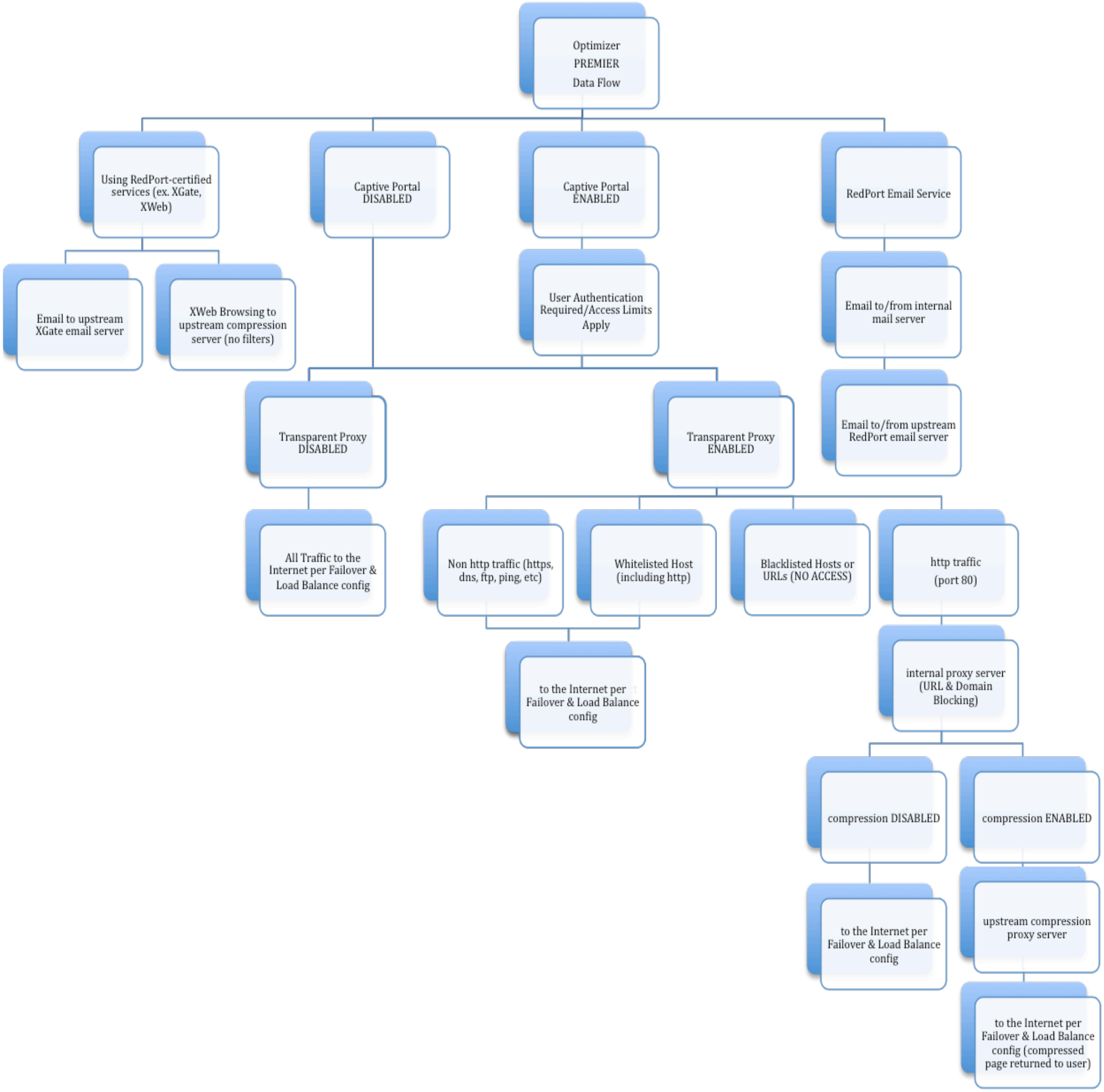
*The default Failover /Load Balancing configuration is as follows:



Setup is required for the GSM Interface

NOTE: All traffic to the Internet is subject to the firewall and load balance configuration. You can change the Failover configuration and you can Load Balance between and among the interfaces. For example, you can create rules to send all http traffic through the WiFi Interface but never through the WAN ports. See Chapter 8.9.

3.4.2 Data Flow - All Paths

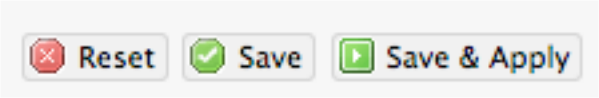

Optimizer PREMIER Data Flow
Using RedPort-certified services (ex. XGate, XWeb)
Captive Portal DISABLED
Captive Portal ENABLED
RedPort Email Service
Email to upstream XGate email server
XWeb Browsing to upstream compression server (no filters)
User Authentication Required/Access Limits Apply
Email to/from internal mail server
Email to/from upstream RedPort email server
Transparent Proxy DISABLED
Transparent Proxy ENABLED
All Traffic to the Internet per Failover & Load Balance config
Non http traffic (https, dns, ftp, ping, etc)
Whitelisted Host (including http)
Blacklisted Hosts or URLs (NO ACCESS)
http traffic (port 80)
to the Internet per Failover & Load Balance config
internal proxy server (URL & Domain Blocking)
compression DISABLED
compression ENABLED
to the Internet per Failover & Load Balance config
upstream compression proxy server
to the Internet per Failover & Load Balance config (compressed page returned to user)

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 many pages in the user interface you will see three buttons in the bottom corners:



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 Premier router arrives to you with the following services enabled:

- Captive Portal (Crew Internet Access)
- Internal Transaparent Proxy for Web Filtering
- SMS Messaging using smartphones (for compatible devices)
- GPS/NMEA Repeater
- Voice Capability using smartphones (for compatible devices)
- Automatic Failover from WiFi to GSM to WAN1 to WAN2 (Note: GSM must be configured)

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)
- RedPort VoIP for multi-user calls and SMS (additional fees may apply)

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

The Network Name will look something like: 'wxa-165-XXXX' where 'XXXX' is the last four digits of the Optimizer Premier's Mac address. Select this wireless network.

For alternative Home Page access methods, see the *Optimizer Premier QuickStart Guide.*

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

http://192.168.10.1

3. The Optimizer Premier ships with two existing administrative accounts:
- Admin - for normal day-to-day operation by the onsite administrator.
- Superadmin - for configuration and maintenance by the installer/technician, etc.

4.1.1 Onsite Administrator Login (Admin)

Onsite Administrator: username=admin, password=webxaccess

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

- generate PIN-Codes (for captive portal use)
- send/receive email (if email is enabled)
- manage crew email accounts (if email is enabled)
- monitor the system status
- manage the local WiFi setup (change the network name, password, etc.)
- modify traffic routing if configured for Manual mode
- enable remote support for diagnostics and/or maintenance
- change the router password for the admin account, if necessary
- reboot the router, if necessary

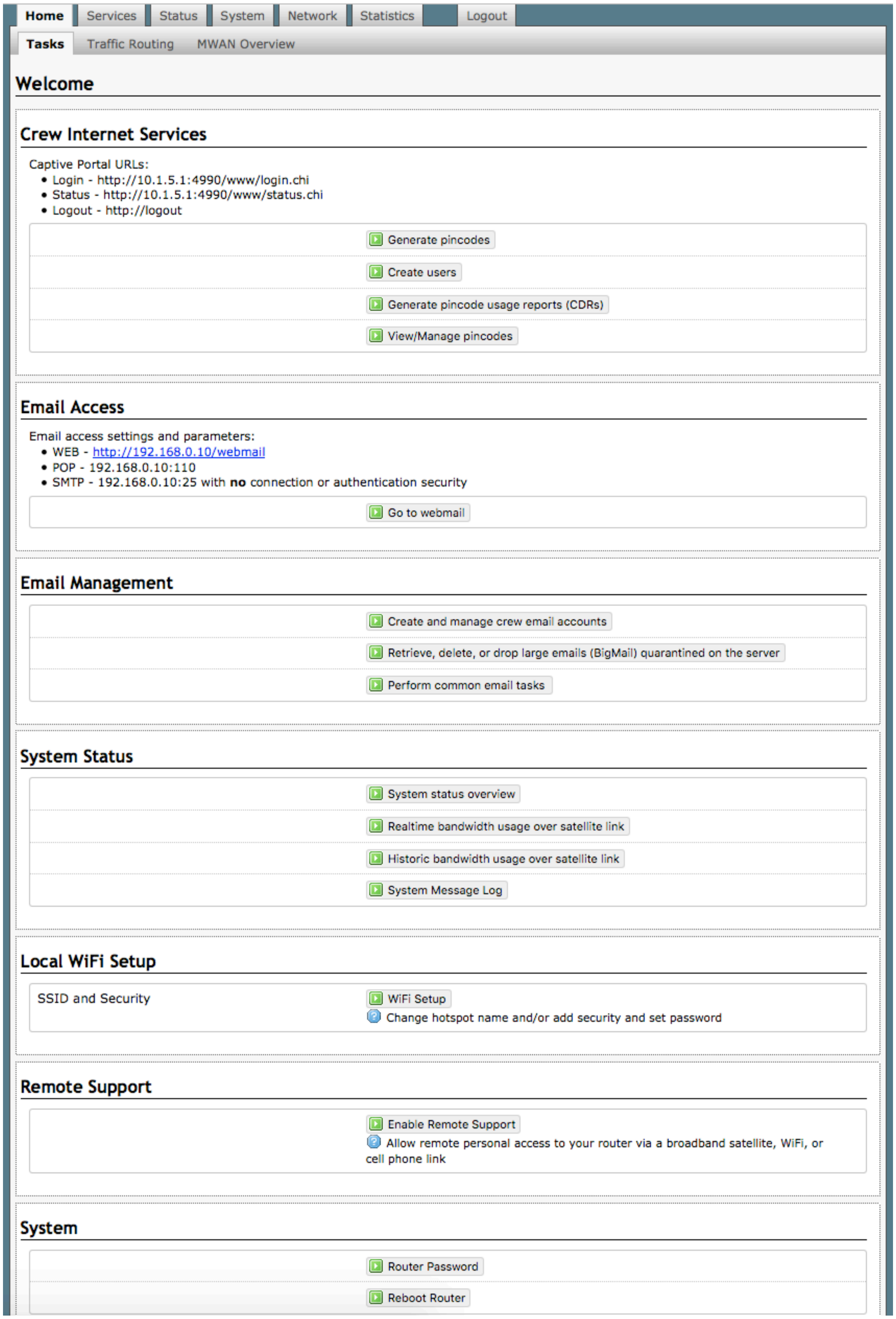
See the *Optimizer Premier Onsite Administrator Guide* for information in administering the most-used features.

4.1.2 Installer/Network Administrator Login (Superadmin)

Technician: username=superadmin, password=webxaccess

This login opens to the Home page and 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.


Home
Services
Status
System
Network
Statistics
Logout
Tasks
Traffic Routing
MWAN Overview

Welcome

Crew Internet Services

Captive Portal URLs:

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

Generate pincodes
Create users
Generate pincode usage reports (CDRs)
View/Manage pincodes

Email Access

Email access settings and parameters:

- WEB - http://192.168.0.10/webmail
- POP - 192.168.0.10:110
- SMTP - 192.168.0.10:25 with **no** connection or authentication security

Email Management

Create and manage crew email accounts
Retrieve, delete, or drop large emails (BigMail) quarantined on the server
Perform common email tasks

System Status

System status overview
Realtime bandwidth usage over satellite link
Historic bandwidth usage over satellite link
System Message Log

Local WiFi Setup

SSID and Security

Change hotspot name and/or add security and set password

Remote Support

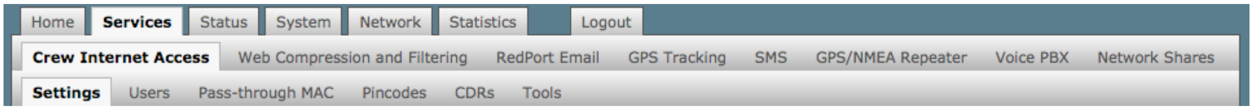
Allow remote personal access to your router via a broadband satellite, WiFi, or cell phone link

System

This Home Page is the onsite administrator's gateway to the most used features. See the Optimizer Premier Onsite Administrator Guide for Home Page details and use.

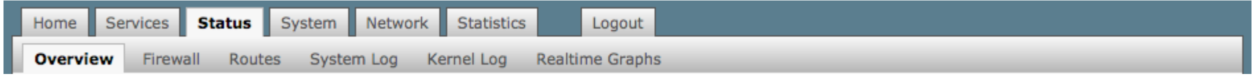
From the Home Page you have access to the remaining sections of the user interface.

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



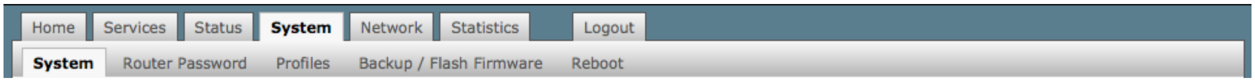
Each service is contained in its own tab under the Services section. This is where you will enable/disable the services and configure them for use.

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



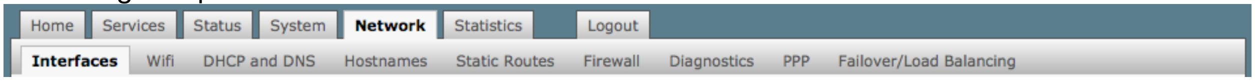
The System Log contains detailed information of the router's performance. It will report error messages and can be useful when troubleshooting connection issues. Realtime Graphs report how much data is being using by the different interfaces. All Status information is Read Only.

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



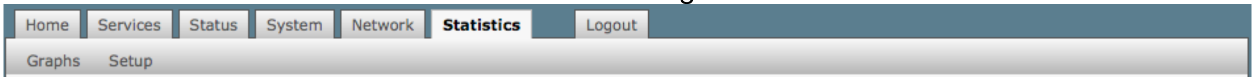
Use this section to set your time zone, change the 'admin' and/or 'superadmin' password, flash new firmware to the router, reboot the router if necessary. Profiles is a way to 'clone' the router configuration for use on another Optimizer Premier router.

Network: contains access to the network Interfaces, the Firewall, and Failover and Load Balancing setup.



Use this section to configure network interfaces, run diagnostics, or modify the firewall. You can also change the Failover sequence and configure the load balance.

Statistics: contains information about resource usage.



4.2 How to Use with Default Setup

We ship the router ready for use as follows:

- Anyone with an existing Primary Account with a RedPort-certified compression email service (such as XGate) and/or web browsing account (such as XWeb) is able to immediately use the router to send/receive email or browse the web. There are no Internet access restrictions when using these services. They simply connect their computer, iOS or Android device to the Optimizer Premier's wireless network, set the email Connection Type to "Optimizer xxxx" where xxxx represents the satellite connection. *See the XGate Help file for more information*.

- Captive Portal and Transparent Proxy are enabled to control access to the Internet so anyone opening a web browser (outside of XGate/XWeb) and entering a URL will be re-directed to the Captive Portal. They will not be able to access the Internet until they are setup as a user. Users that are given access via the Captive Portal can go anywhere on the Internet unless the installer has configured the proxy server to restrict access. Individual user access can be restricted by time; by data; by time of day; by speed. *See Chapter 5.1*.

- Voice is enabled for use with compatible satellite devices using standard satellite airtime. *See Chapter 5.7.*

- SMS is enabled for use with compatible satellite devices using standard satellite airtime. *See Chapter 5.4.*

- Failover sequence is set to Automatic - WiFi > GSM > WAN1 > WAN2. GSM must be configured for use. *See Chapter 8.8 and Chapter 8.9.*

- Load Balance is set to ALL traffic thru the one Active interface. *See Chapter 8.9.*

- Firewall is Open allowing all traffic to pass*. See Chapter 8.6.*

This out-of-the-box configuration works well for single broadband users with an XGate and/or XWeb primary account and can be suitable for the multi-interface, multi-user environment where each person has a separate primary XGate email and/or XWeb browsing account.

If in a mutli-user environment we recommend the optional RedPort Email service for easy access and management of crew accounts. *See Chapter 5.3.* Additional fees may apply. Contact your service provider for current pricing.

Enabling Web Compression Service will direct all http traffic to the upstream compression proxy server and return a compressed page to the user. 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 the effective per Mb cost of your connection. *See Chapter 5.2*. Additional fees may apply. Contact your service provider for current pricing.

Transform your satellite device into a multi-user voice unit with the optional RedPort VoIP Service. 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. *See Chapter 5.7*. Additional fees may apply. Contact your service provider for current pricing.

IMPORTANT NOTE: This router is shipped to you with all WAN ports open, POP and SMTP are open to the WAN if you enable Email, if you enable the 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.

4.3 Router Security

By default, your router is open to the Internet:

- WAN ports are open
- Voice PBX, if enabled, is listening on all ports
- POP and SMTP are open to the WAN, if Email is enabled

This setup 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.

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. *(See Chapter 7.1)* 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 anti-lock rule is enabled (unchecked). If you lock yourself out of the router you must perform a factory reset.

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

Go to Services > Crew Internet Access > Tools and change the Admin password for the Captive Portal admin access. *See Chapter 5.1.4.1.*

Go to System > Router Password and change the router password for both the "superadmin" and the "admin" access. *See Chapter 7.2*.

If RedPort Email is enabled, the POP and SMTP servers are listening on ALL ports so they are open to the WAN, leaving them vulnerable. If you enable RedPort Email, you should configure the firewall to block all but desired email traffic. *See Chapter 8.6*. Note that 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 Captive Portal or LAN) in Services > Voice PBX > Settings (*see Chapter 5.7*). OR, you can leave it to listening on all interfaces and use a firewall rule to restrict traffic (*see Chapter 8.6*). Note that 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. *See Chapter 7.1*.

Now you can Enable the BLOCK ALL from WAN firewall rule in Network > Firewall > Firewall Rules.

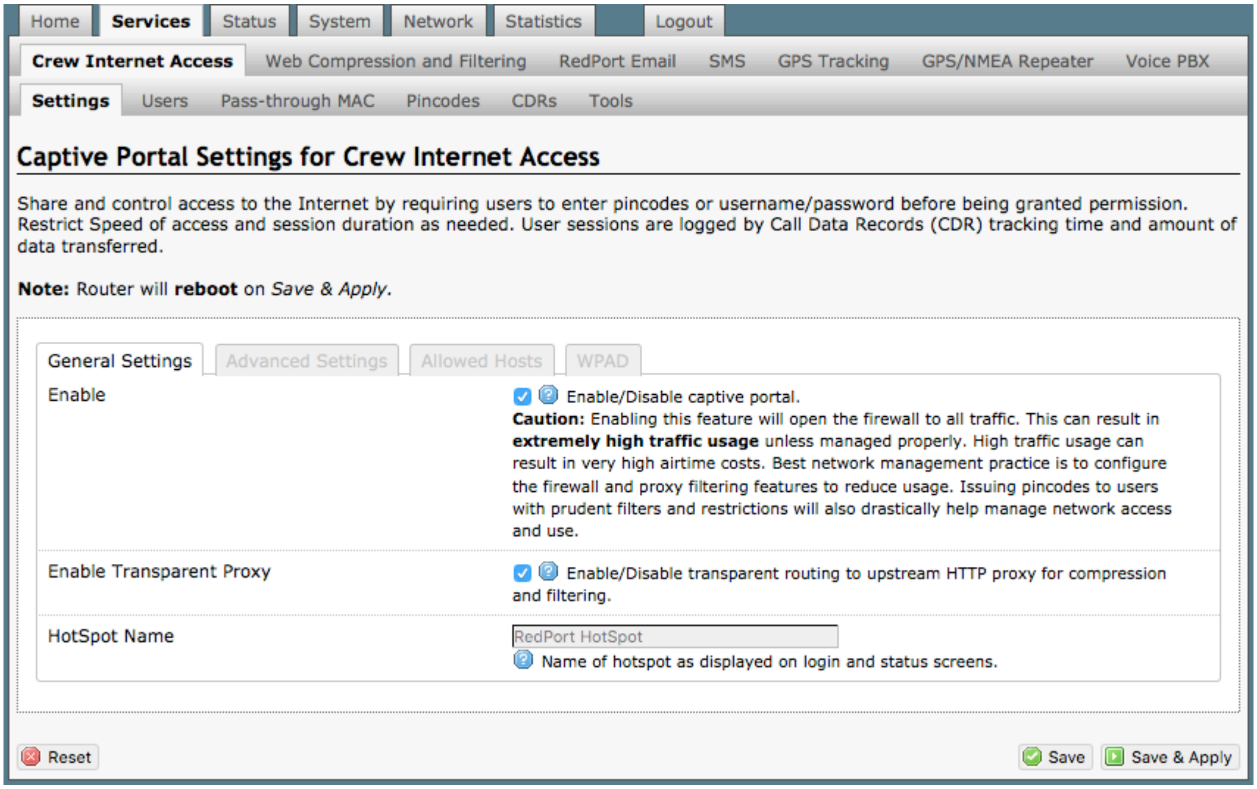
5.0 Services

5.1 Crew Internet Services (Captive Portal)

The Optimizer Premier is shipped with Captive Portal enabled. This allows controlled access to the Internet by requiring authentication by users. It blocks access to the Internet without authentication. Authentication can be via username and password or PIN-Code or Mac address of a specific PC. *See Chapter 5.1.2.*

PIN-Codes to restrict access can be created by the Onsite Administrator. In addition, the speed of access can be limited by the PIN-Code as can the duration/or time of the session. *See Chapter 5.1.2.3.*

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 Chapter 5.1.3.*



Captive Portal Settings for Crew Internet Access

Share and control access to the Internet by requiring users to enter pincodes or username/password before being granted permission. Restrict Speed of access and session duration as needed. User sessions are logged by Call Data Records (CDR) tracking time and amount of data transferred.

Note: Router will **reboot** on *Save & Apply*.

Enable: ☑ Enable/Disable captive portal.
Caution: Enabling this feature will open the firewall to all traffic. This can result in **extremely high traffic usage** unless managed properly. High traffic usage can result in very high airtime costs. Best network management practice is to configure the firewall and proxy filtering features to reduce usage. Issuing pincodes to users with prudent filters and restrictions will also drastically help manage network access and use.

Enable Transparent Proxy: ☑ Enable/Disable transparent routing to upstream HTTP proxy for compression and filtering.

HotSpot Name: RedPort HotSpot
Name of hotspot as displayed on login and status screens.

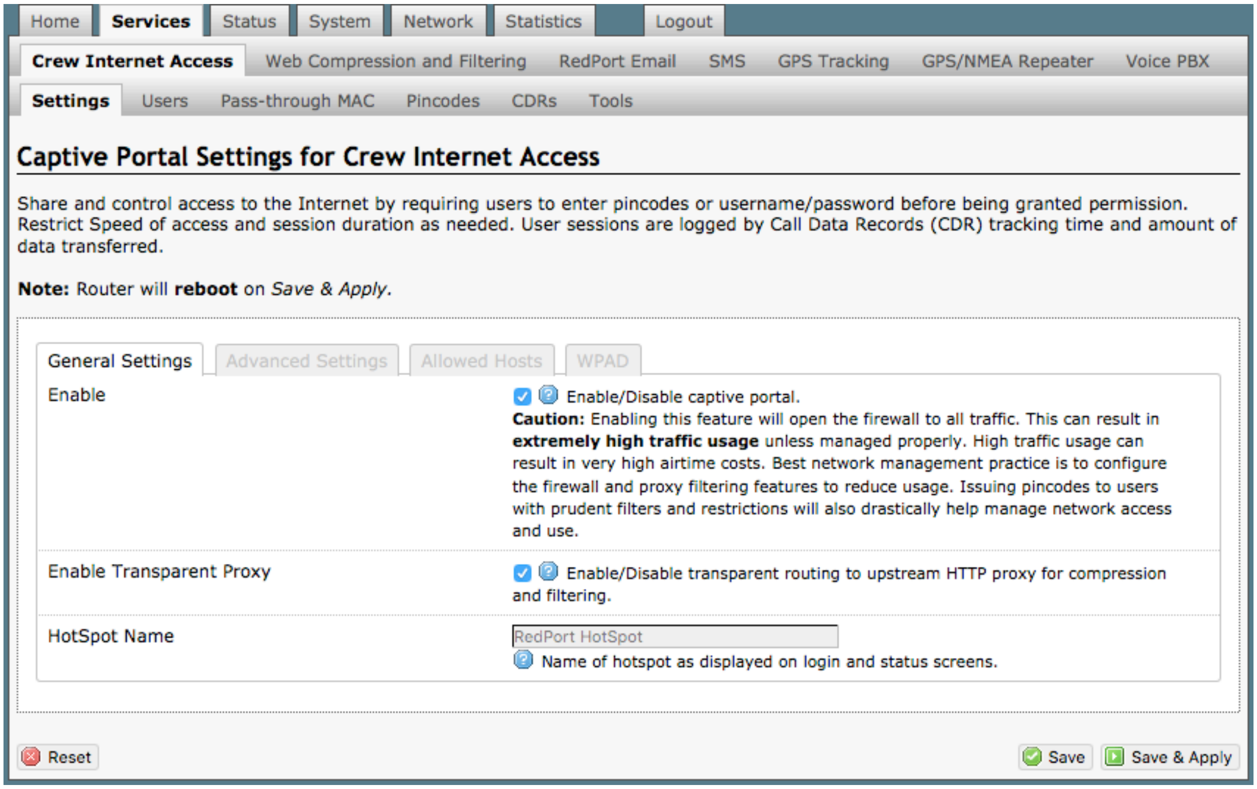
The image above is the default state of the Captive Portal Settings as the router is shipped to you. See the *Optimizer Premier Onsite Administrator Guide* for information on how the onsite administrator manages Captive Portal use.

5.1.1 Captive Portal Settings

5.1.1.1 General Settings

Requires 'superadmin' login.

With the **Captive Portal enabled**, all users trying to use the Internet will be redirected to a screen where they will be required to enter a PIN-Code 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.***



Captive Portal Settings for Crew Internet Access

Share and control access to the Internet by requiring users to enter pincodes or username/password before being granted permission. Restrict Speed of access and session duration as needed. User sessions are logged by Call Data Records (CDR) tracking time and amount of data transferred.

Note: Router will **reboot** on *Save & Apply*.

Enable	☑ Enable/Disable captive portal. **Caution:** Enabling this feature will open the firewall to all traffic. This can result in **extremely high traffic usage** unless managed properly. High traffic usage can result in very high airtime costs. Best network management practice is to configure the firewall and proxy filtering features to reduce usage. Issuing pincodes to users with prudent filters and restrictions will also drastically help manage network access and use.
Enable Transparent Proxy	☑ Enable/Disable transparent routing to upstream HTTP proxy for compression and filtering.
HotSpot Name	RedPort HotSpot Name of hotspot as displayed on login and status screens.

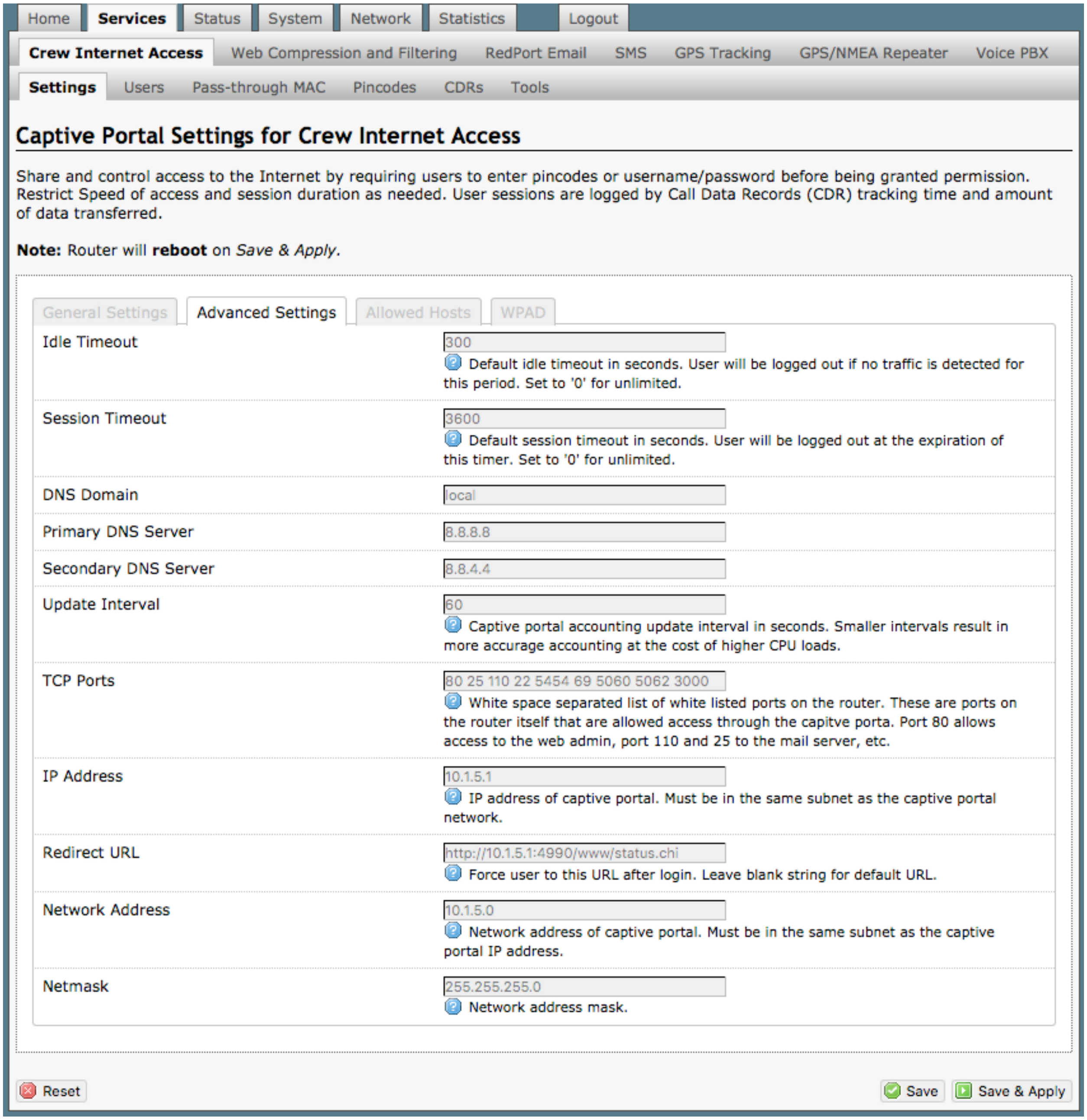
Internal **Transparent Proxy** is enabled which means that all http traffic that is not whiltelisted or blacklisted is redirected to the router's internal proxy server. This internal proxy server can be configured for URL blocking and domain blocking. ***CAUTION: If you Disable Transparent Proxy then 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

Requires 'superadmin' login.

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



Captive Portal Settings for Crew Internet Access

Share and control access to the Internet by requiring users to enter pincodes or username/password before being granted permission. Restrict Speed of access and session duration as needed. User sessions are logged by Call Data Records (CDR) tracking time and amount of data transferred.

Note: Router will **reboot** on *Save & Apply*.

Idle Timeout	300	Default idle timeout in seconds. User will be logged out if no traffic is detected for this period. Set to '0' for unlimited.
Session Timeout	3600	Default session timeout in seconds. User will be logged out at the expiration of this timer. Set to '0' for unlimited.
DNS Domain	local	
Primary DNS Server	8.8.8.8	
Secondary DNS Server	8.8.4.4	
Update Interval	60	Captive portal accounting update interval in seconds. Smaller intervals result in more accurage accounting at the cost of higher CPU loads.
TCP Ports	80 25 110 22 5454 69 5060 5062 3000	White space separated list of white listed ports on the router. These are ports on the router itself that are allowed access through the capitve porta. Port 80 allows access to the web admin, port 110 and 25 to the mail server, etc.
IP Address	10.1.5.1	IP address of captive portal. Must be in the same subnet as the captive portal network.
Redirect URL	http://10.1.5.1:4990/www/status.chi	Force user to this URL after login. Leave blank string for default URL.
Network Address	10.1.5.0	Network address of captive portal. Must be in the same subnet as the captive portal IP address.
Netmask	255.255.255.0	Network address mask.

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.

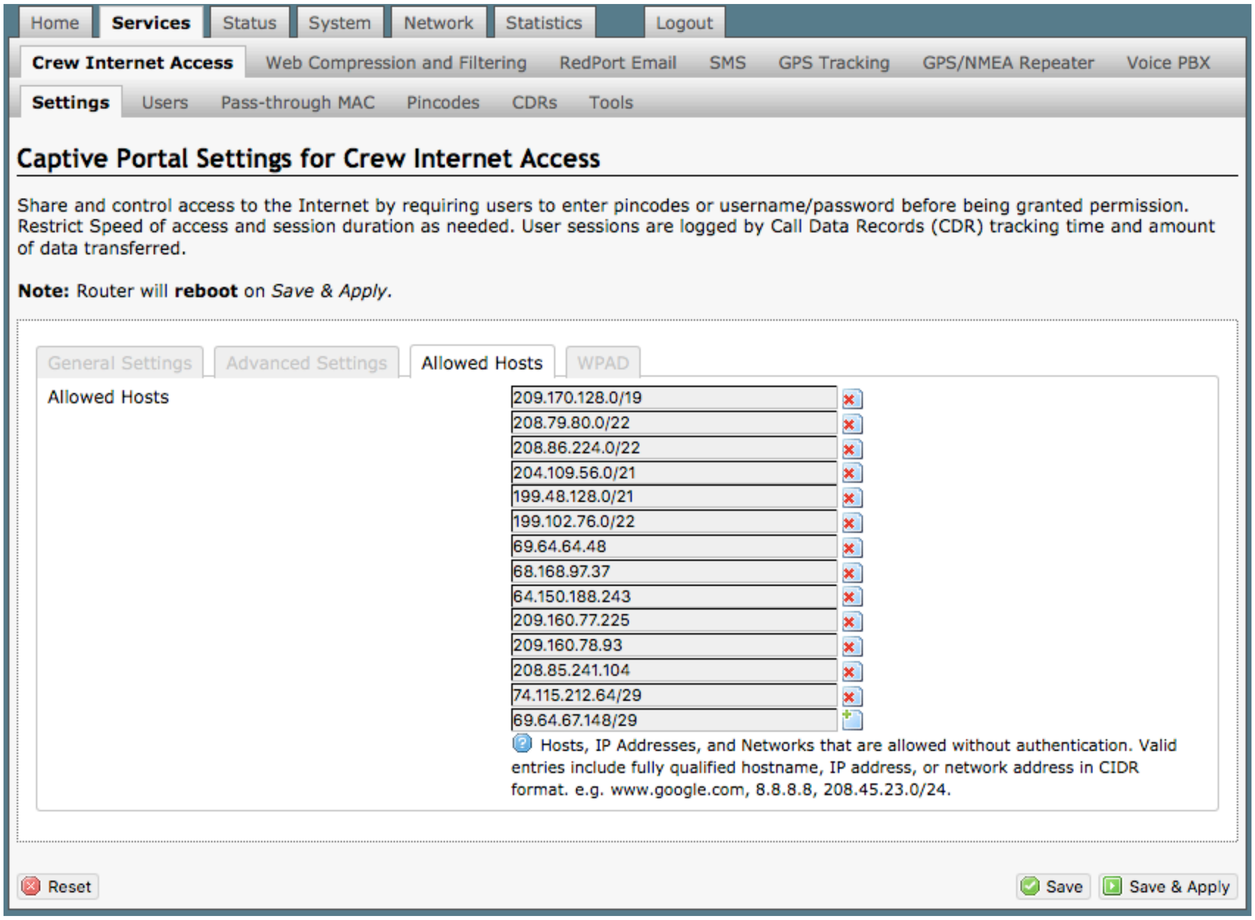
Session Timeout - The default is set to 3600 seconds (60 minutes). The user will be automatically logged out at the end of the session timeout period. They must log in again to continue.

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

Requires 'superadmin' login.

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



Captive Portal Settings for Crew Internet Access

Share and control access to the Internet by requiring users to enter pincodes or username/password before being granted permission. Restrict Speed of access and session duration as needed. User sessions are logged by Call Data Records (CDR) tracking time and amount of data transferred.

Note: Router will **reboot** on *Save & Apply*.

Allowed Hosts

209.170.128.0/19
208.79.80.0/22
208.86.224.0/22
204.109.56.0/21
199.48.128.0/21
199.102.76.0/22
69.64.64.48
68.168.97.37
64.150.188.243
209.160.77.225
209.160.78.93
208.85.241.104
74.115.212.64/29
69.64.67.148/29

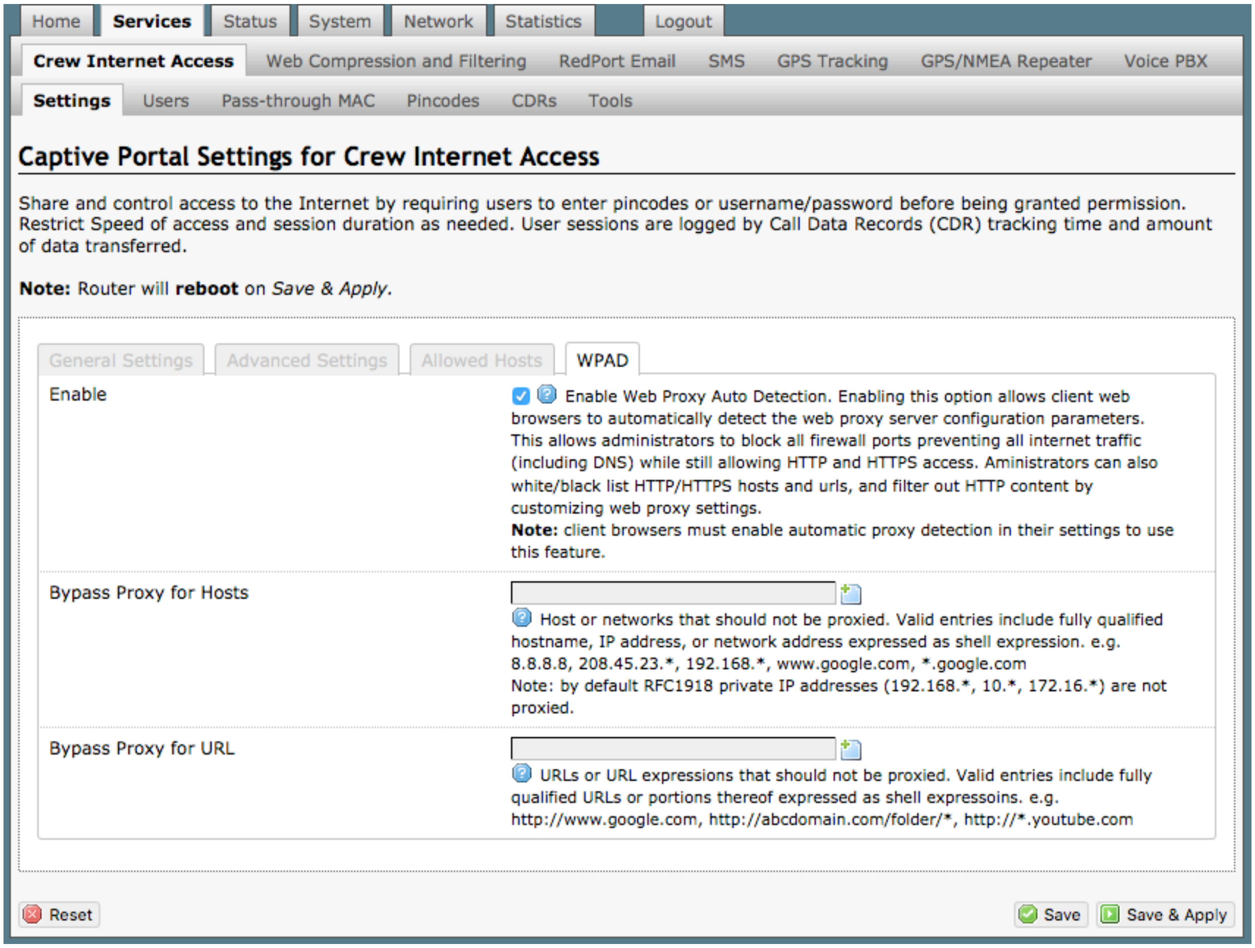
Hosts, IP Addresses, and Networks that are allowed without authentication. Valid entries include fully qualified hostname, IP address, or network address in CIDR format. e.g. www.google.com, 8.8.8.8, 208.45.23.0/24.

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

Requires 'superadmin' login.

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.



Captive Portal Settings for Crew Internet Access

Share and control access to the Internet by requiring users to enter pincodes or username/password before being granted permission. Restrict Speed of access and session duration as needed. User sessions are logged by Call Data Records (CDR) tracking time and amount of data transferred.

Note: Router will **reboot** on *Save & Apply*.

Enable	☑ Enable Web Proxy Auto Detection. Enabling this option allows client web browsers to automatically detect the web proxy server configuration parameters. This allows administrators to block all firewall ports preventing all internet traffic (including DNS) while still allowing HTTP and HTTPS access. Aministrators can also white/black list HTTP/HTTPS hosts and urls, and filter out HTTP content by customizing web proxy settings. **Note:** client browsers must enable automatic proxy detection in their settings to use this feature.
Bypass Proxy for Hosts	Host or networks that should not be proxied. Valid entries include fully qualified hostname, IP address, or network address expressed as shell expression. e.g. 8.8.8.8, 208.45.23.*, 192.168.*, www.google.com, *.google.com Note: by default RFC1918 private IP addresses (192.168.*, 10.*, 172.16.*) are not proxied.
Bypass Proxy for URL	URLs or URL expressions that should not be proxied. Valid entries include fully qualified URLs or portions thereof expressed as shell expressoins. e.g. http://www.google.com, http://abcdomain.com/folder/*, http://*.youtube.com

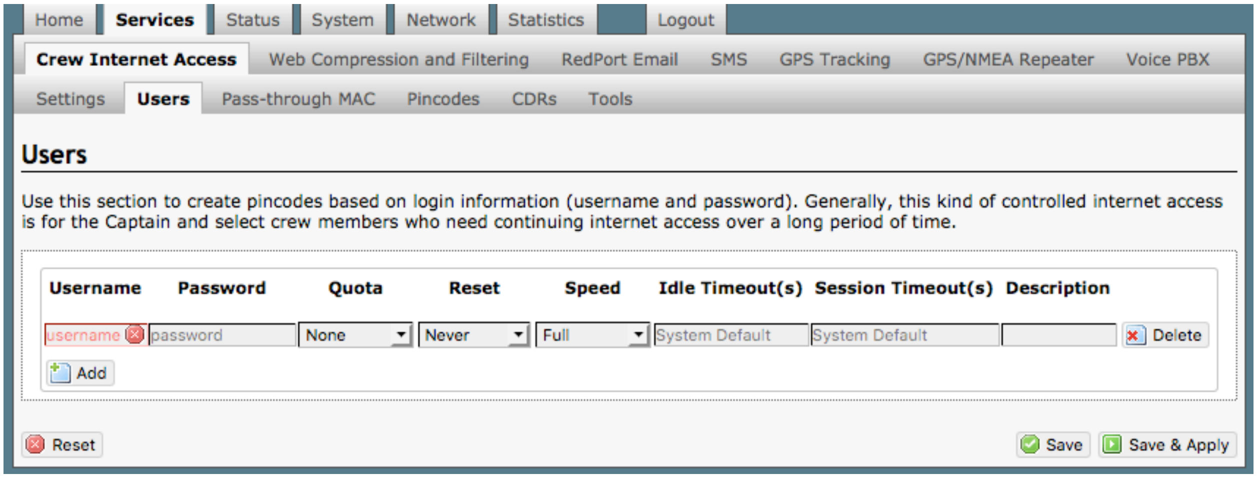
5.1.2 Allowing Individuals Access to the Internet

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

5.1.2.1 Users with Username and Password

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

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



Users

Use this section to create pincodes based on login information (username and password). Generally, this kind of controlled internet access is for the Captain and select crew members who need continuing internet access over a long period of time.

Username	Password	Quota	Reset	Speed	Idle Timeout(s)	Session Timeout(s)	Description	
username	password	None	Never	Full	System Default	System Default		☒ Delete

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

Username: A unique character string that this user will enter at login.

Password: A character string that the user will enter at login. The Password must be different from the username.

Quota: You can restrict the username to a specific amount of data transferred. The default is no restriction. To set a maximum, use the drop-down menu. When you set a maximum, the user has Internet access until the maximum is reached. When the maximum is reached the user will be disconnected from the Internet.

Reset: The Quota assigned to a Username can be configured to reset periodically (daily, weekly, monthly) using the drop down menu. When a reset period is selected, the Quota will renew automatically at the start of the new reset period.

Speed: Set the maximum bandwidth allowed for this user. Note: maximum speed is dependent upon the speed of the satellite device/service.

Idle Timeout(s): Expressed in seconds, enter the idle timeout period to change it from the default. At the end of the idle period, the user will be logged out if no traffic has been detected during the period. The default period is configured at installation and can be found in Services > Crew Internet Access > Settings > Advanced Settings.

Session Timeout(s): Expressed in seconds, enter the session timeout period to change it from the default. At the end of the timeout period the user will be logged out of the session. The default period is configured at installation and can be found in Services > Crew Internet Access > Settings > Advanced Settings.

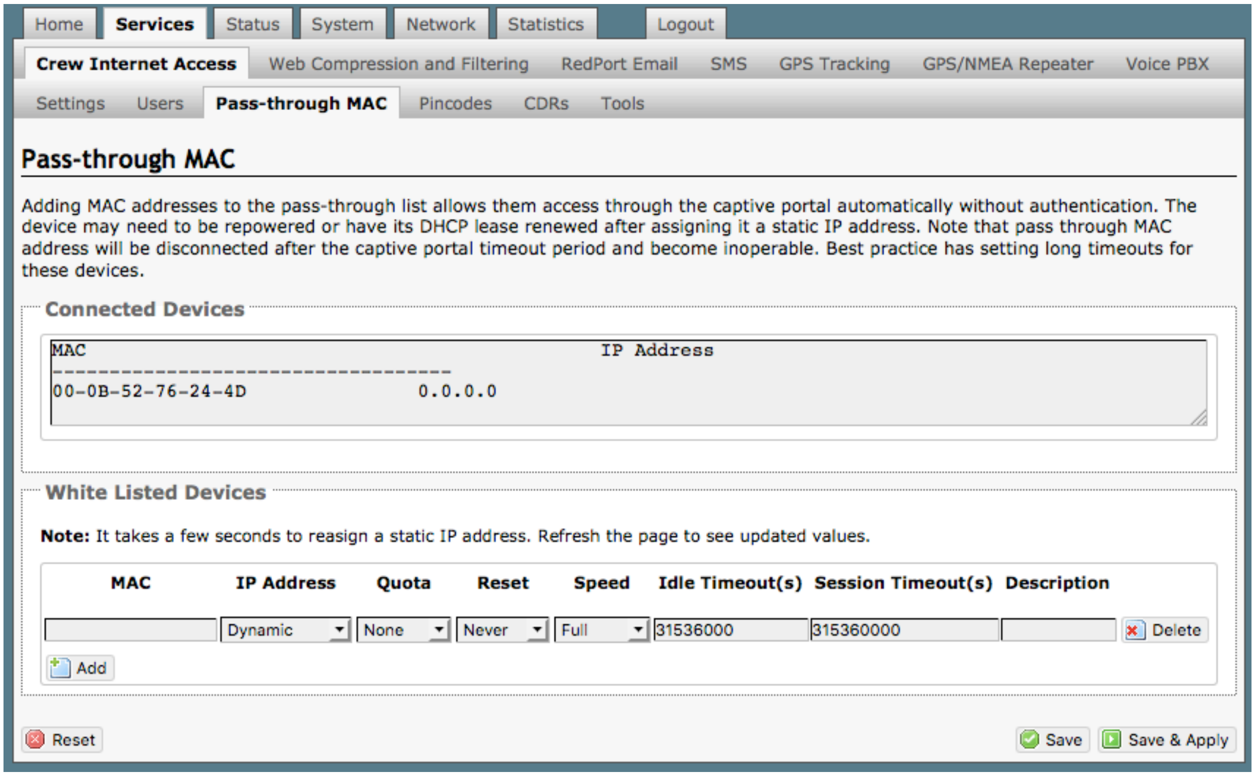
Description: Optional - Enter a short description of the account.

Select <Save> to enter more users or <Save & Apply> when all users are entered. Wait for the message "Configuration Applied".

5.1.2.2 Pass-Through MAC

Requires 'superadmin' login.

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)



Pass-through MAC

Adding MAC addresses to the pass-through list allows them access through the captive portal automatically without authentication. The device may need to be repowered or have its DHCP lease renewed after assigning it a static IP address. Note that pass through MAC address will be disconnected after the captive portal timeout period and become inoperable. Best practice has setting long timeouts for these devices.

Connected Devices

```
MAC                                                IP Address
-----------------------------------
00-0B-52-76-24-4D                0.0.0.0
```

White Listed Devices

Note: It takes a few seconds to reasign a static IP address. Refresh the page to see updated values.

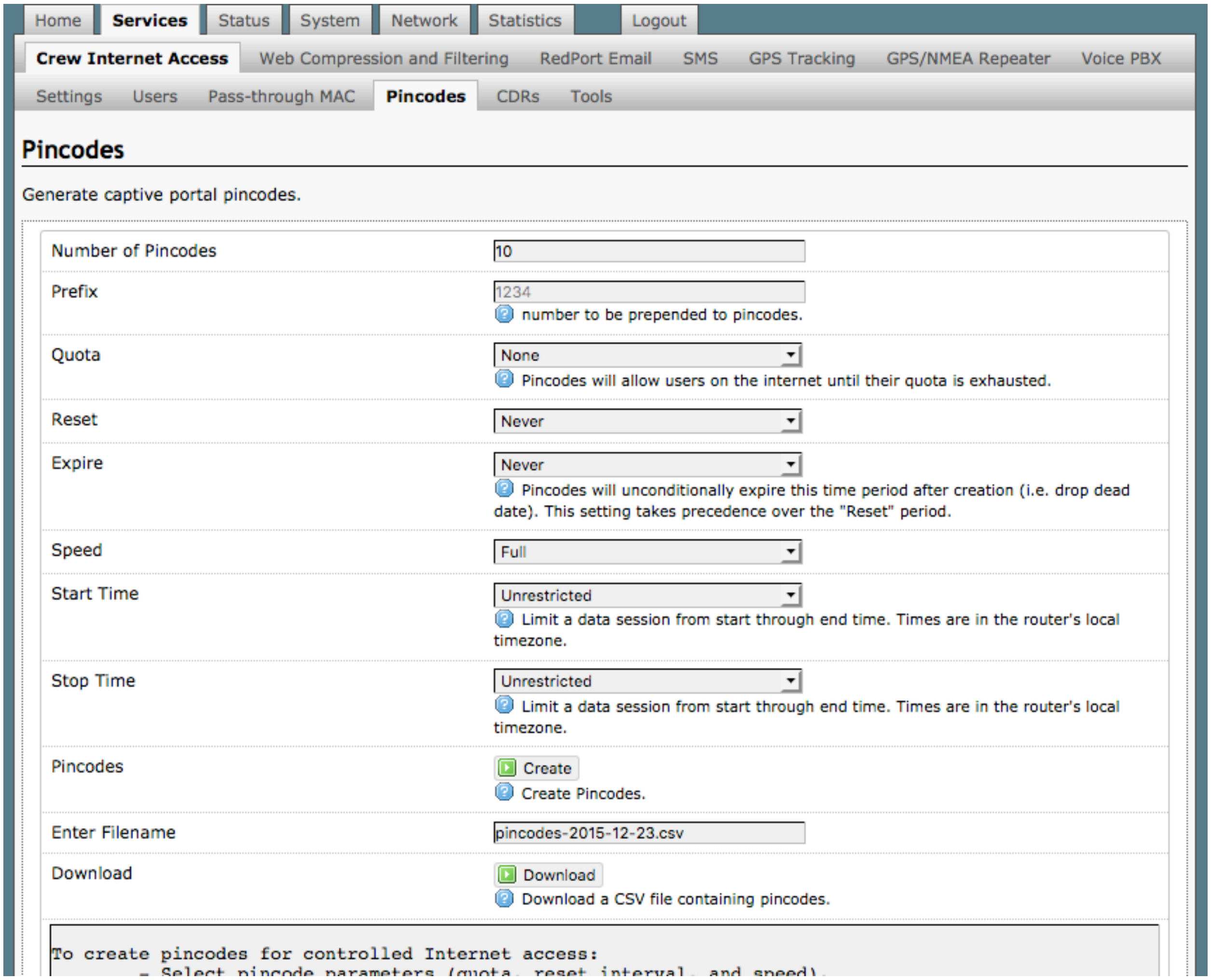
MAC	IP Address	Quota	Reset	Speed	Idle Timeout(s)	Session Timeout(s)	Description	
	Dynamic	None	Never	Full	31536000	315360000		Delete

See Chapter 5.1.2.3 for Quota, Reset, Speed and Timeout descriptions.

5.1.2.3 PIN-Codes

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

Generate PIN-Codes to limit Internet access. Sell them or give them to transient crew, passengers, or visitors.



Pincodes

Generate captive portal pincodes.

Number of Pincodes	10
Prefix	1234 number to be prepended to pincodes.
Quota	None Pincodes will allow users on the internet until their quota is exhausted.
Reset	Never
Expire	Never Pincodes will unconditionally expire this time period after creation (i.e. drop dead date). This setting takes precedence over the "Reset" period.
Speed	Full
Start Time	Unrestricted Limit a data session from start through end time. Times are in the router's local timezone.
Stop Time	Unrestricted Limit a data session from start through end time. Times are in the router's local timezone.
Pincodes	Create Create Pincodes.
Enter Filename	pincodes-2015-12-23.csv
Download	Download Download a CSV file containing pincodes.

```
To create pincodes for controlled Internet access:
     - Select pincode parameters (quota, reset interval, and speed).
```

Number of Pincodes: Enter the quantity of pincodes that will have the same configuration/restrictions, up to the maximum of 100 pincodes can be created in a batch.

Prefix: This can be useful for tracking pincode inventory. Enter up to a five-digit number that will be added to the pincode.

Quota: You can restrict a pincode to a specific amount of data transferred. The default is no restriction. To set a maximum, use the drop-down menu. When you set a maximum, the user has Internet access until the maximum is reached. When the maximum is reached the pincode will stop working.

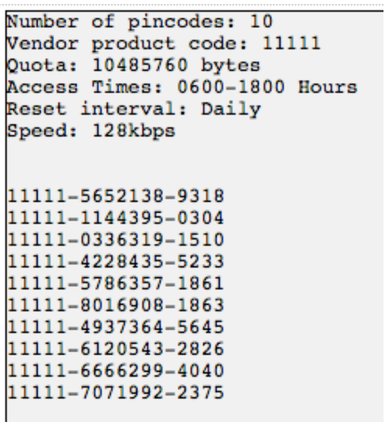
Reset: The pincode can be configured to reset periodically (daily, weekly, monthly) using the drop down menu. When a reset period is selected, the pincode configuration will renew automatically at the start of the new reset period. For example, if a pincode has a quota of 10Mb of data and the reset period is set to daily, that user will be allowed to transfer a maximum of 10Mb of data each day. Once the maximum data transfer of 10Mb is acheived the pincode will temporarily stop working until the start of the next period. If the Reset period is set to Never, once the maximum quota is acheived the pincode expires and it cannot be renewed.

Speed: Set the maximum bandwidth allowed for this pincode. Note: maximum speed is dependent upon the speed of the satellite device/service.

Start Time: Use Start Time in conjunction with Stop Time to limit the time of day a pincode can be used. Select a Start Time from the drop down menu. Note: a Stop Time must also be selected.

Stop Time: Use Stop Time in conjunction with Start Time to limit the time of day a pincode can be used. Select a Stop Time from the drop down menu. Note: a Start Time must also be selected.

Pincodes: When all the parameters of the pincode are selected in the fields above, select <Create> to generate the pincodes. The list of pincodes will display in the text window.



```
Number of pincodes: 10
Vendor product code: 11111
Quota: 10485760 bytes
Access Times: 0600-1800 Hours
Reset interval: Daily
Speed: 128kbps


11111-5652138-9318
11111-1144395-0304
11111-0336319-1510
11111-4228435-5233
11111-5786357-1861
11111-8016908-1863
11111-4937364-5645
11111-6120543-2826
11111-6666299-4040
11111-7071992-2375
```

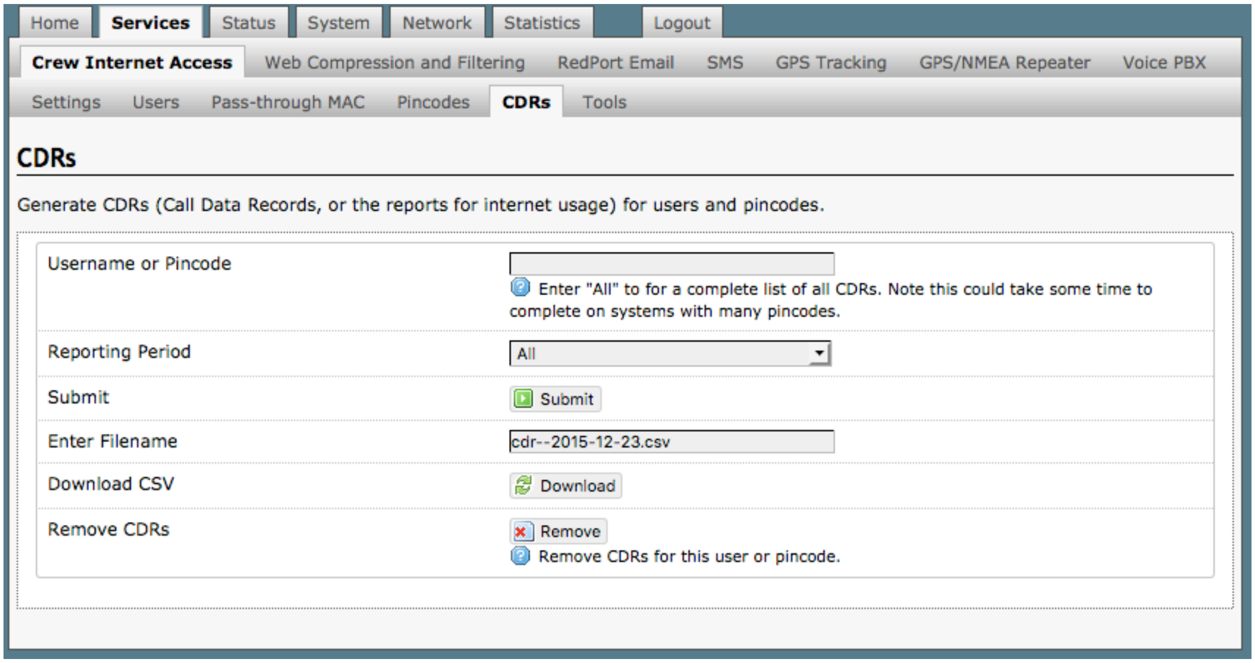
Enter Filename: Use in conjunction with Download to create a .csv file as the new pincodes are generated. Enter a name for the .csv file.

Download: Use in conjunction with Enter Filename to create a .csv file as the new pincodes are generated. Select <Download> and Save the file to the computer. Open the .csv file to see the pincodes.

5.1.3 CDRs (Call Data Records)

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

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 PIN-Code or any username or any MAC address.



CDRs

Generate CDRs (Call Data Records, or the reports for internet usage) for users and pincodes.

Username or Pincode	Enter "All" to for a complete list of all CDRs. Note this could take some time to complete on systems with many pincodes.
Reporting Period	All
Submit	Submit
Enter Filename	cdr--2015-12-23.csv
Download CSV	Download
Remove CDRs	Remove Remove CDRs for this user or pincode.

Username or Pincode: Enter the username or pincode for the CDR you want to view, download or remove.

Reporting Period: Select the period from the drop down menu.

Submit: Select this to view the log for the username or pincode entered above.

Enter Filename: Use in conjunction with Download to create a .csv file of the CDR. Enter a name for the .csv file.

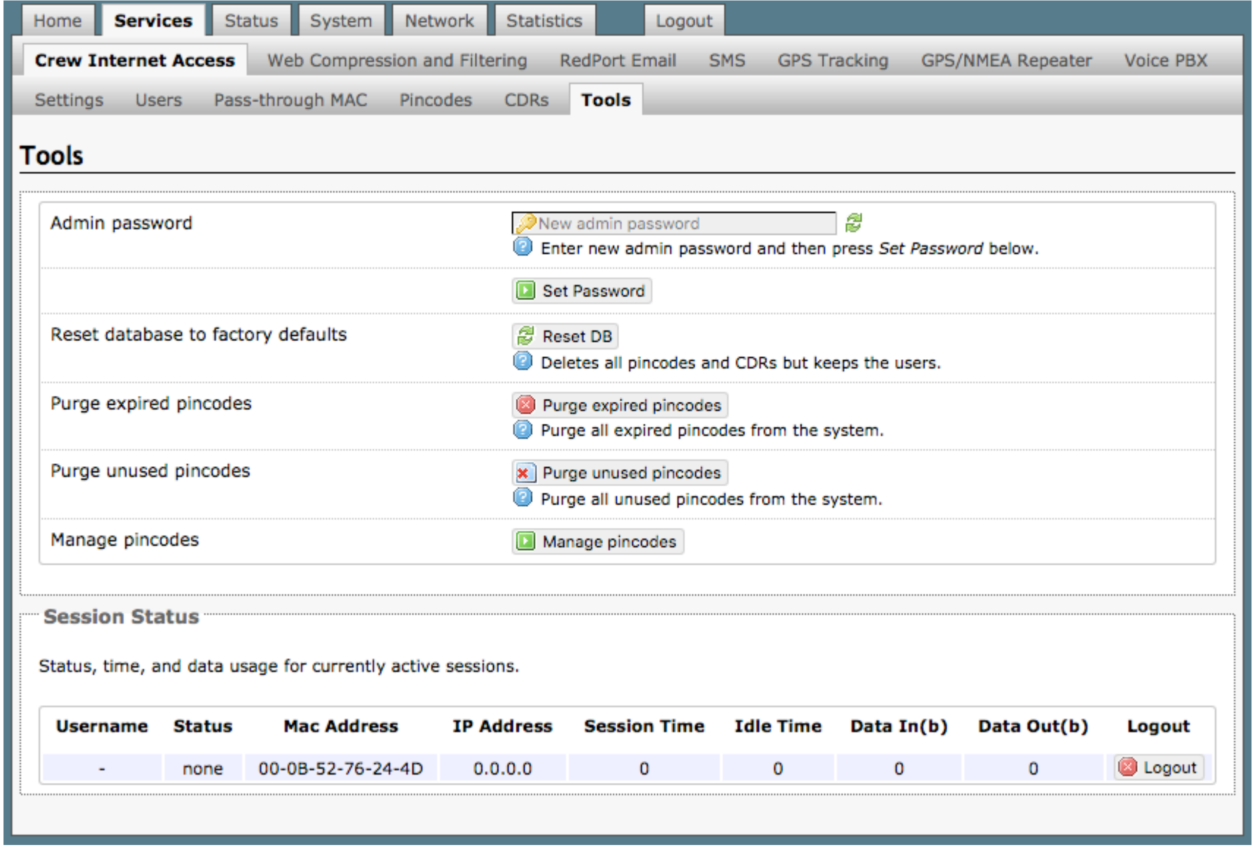
Download CSV: Use in conjunction with Enter Filename to create a .csv file of the CDR. Select <Download> and Save the file to the computer. Open the .csv file to see the CDR.

Remove CDRs: Select <Remove> to delete the CDRs for the username or pincode.

5.1.4 Tools

Requires 'superadmin' login.

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



Tools

Admin password	New admin password Enter new admin password and then press *Set Password* below.
	Set Password
Reset database to factory defaults	Reset DB Deletes all pincodes and CDRs but keeps the users.
Purge expired pincodes	Purge expired pincodes Purge all expired pincodes from the system.
Purge unused pincodes	Purge unused pincodes Purge all unused pincodes from the system.
Manage pincodes	Manage pincodes

Session Status

Status, time, and data usage for currently active sessions.

Username	Status	Mac Address	IP Address	Session Time	Idle Time	Data In(b)	Data Out(b)	Logout
-	none	00-0B-52-76-24-4D	0.0.0.0	0	0	0	0	Logout

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 here 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 pincode database including CDRs. ***CAUTION: This action CANNOT be undone.***

5.1.4.3 Purge Expired PIN-Codes

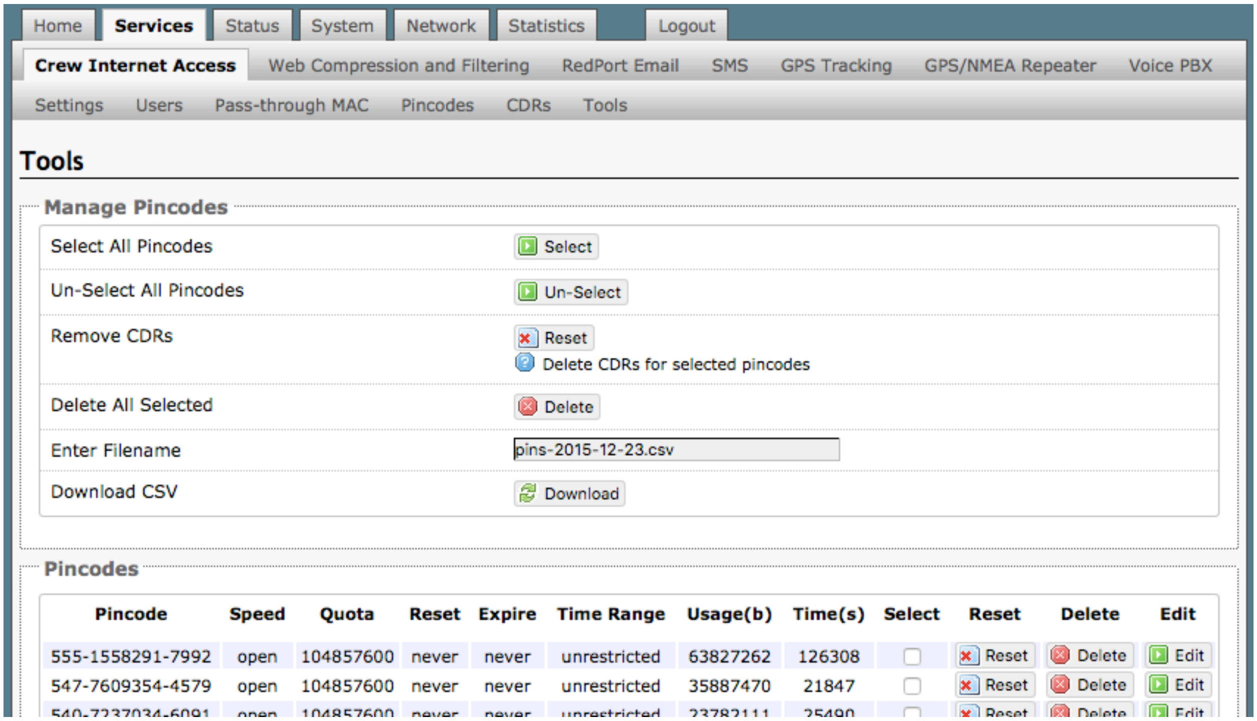
Over time, as the database builds, you may want to purge expired PIN-Codes to free up space.

5.1.4.4 Purge Unused PIN-Codes

Use this to purge unused PIN-Codes from the system.

5.1.4.5 Manage PIN-Codes

This will show a summary of all the PIN-Codes, 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 PIN-Codes table.



Tools

Manage Pincodes

Select All Pincodes	Select
Un-Select All Pincodes	Un-Select
Remove CDRs	Reset Delete CDRs for selected pincodes
Delete All Selected	Delete
Enter Filename	pins-2015-12-23.csv
Download CSV	Download

Pincodes

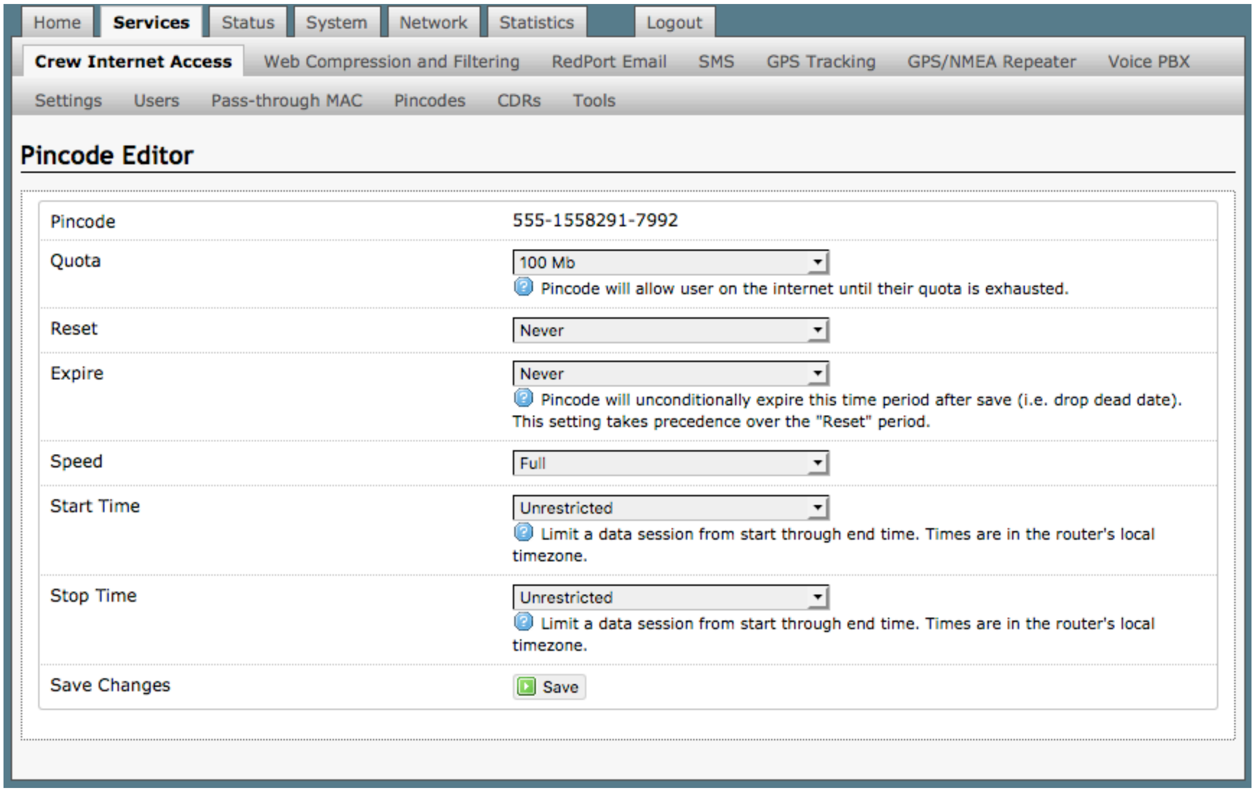
Pincode	Speed	Quota	Reset	Expire	Time Range	Usage(b)	Time(s)	Select	Reset	Delete	Edit
555-1558291-7992	open	104857600	never	never	unrestricted	63827262	126308	□	Reset	Delete	Edit
547-7609354-4579	open	104857600	never	never	unrestricted	35887470	21847	□	Reset	Delete	Edit
540-7237034-6091	open	104857600	never	never	unrestricted	23782111	25490	□	Reset	Delete	Edit

Using the top section of this screen you can:

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

In addition, using the buttons in the PIN-Codes table, you can:

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



Pincode Editor

Pincode	555-1558291-7992
Quota	100 Mb Pincode will allow user on the internet until their quota is exhausted.
Reset	Never
Expire	Never Pincode will unconditionally expire this time period after save (i.e. drop dead date). This setting takes precedence over the "Reset" period.
Speed	Full
Start Time	Unrestricted Limit a data session from start through end time. Times are in the router's local timezone.
Stop Time	Unrestricted Limit a data session from start through end time. Times are in the router's local timezone.
Save Changes	Save

In the example above, we have elected to edit the PIN-Code 555-1558291-7992. *See Chapter 5.1.2.3 for information on PIN-Code parameters.*

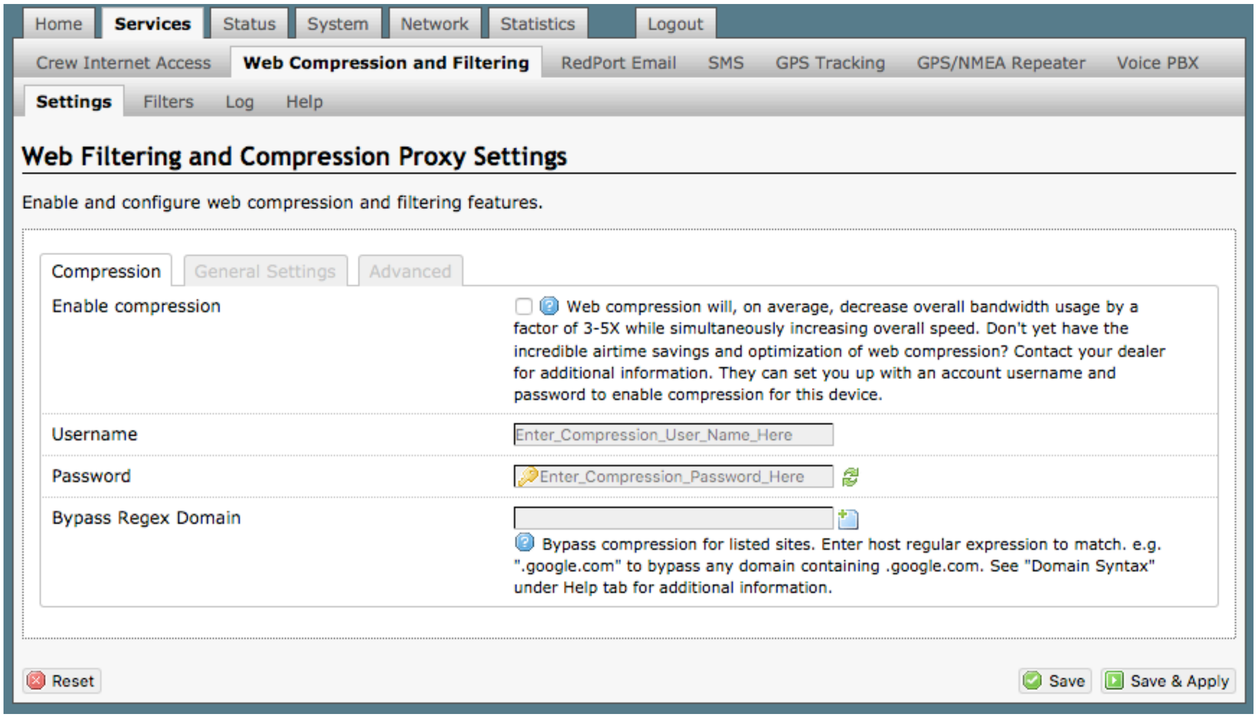
5.2 Web Compression and Filtering

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

Requires 'superadmin' login.



Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

Enable compression	□ Web compression will, on average, decrease overall bandwidth usage by a factor of 3-5X while simultaneously increasing overall speed. Don't yet have the incredible airtime savings and optimization of web compression? Contact your dealer for additional information. They can set you up with an account username and password to enable compression for this device.
Username	Enter_Compression_User_Name_Here
Password	Enter_Compression_Password_Here
Bypass Regex Domain	Bypass compression for listed sites. Enter host regular expression to match. e.g. ".google.com" to bypass any domain containing .google.com. See "Domain Syntax" under Help tab for additional information.

5.2.1.1 Compression

Requires 'superadmin' login.

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.

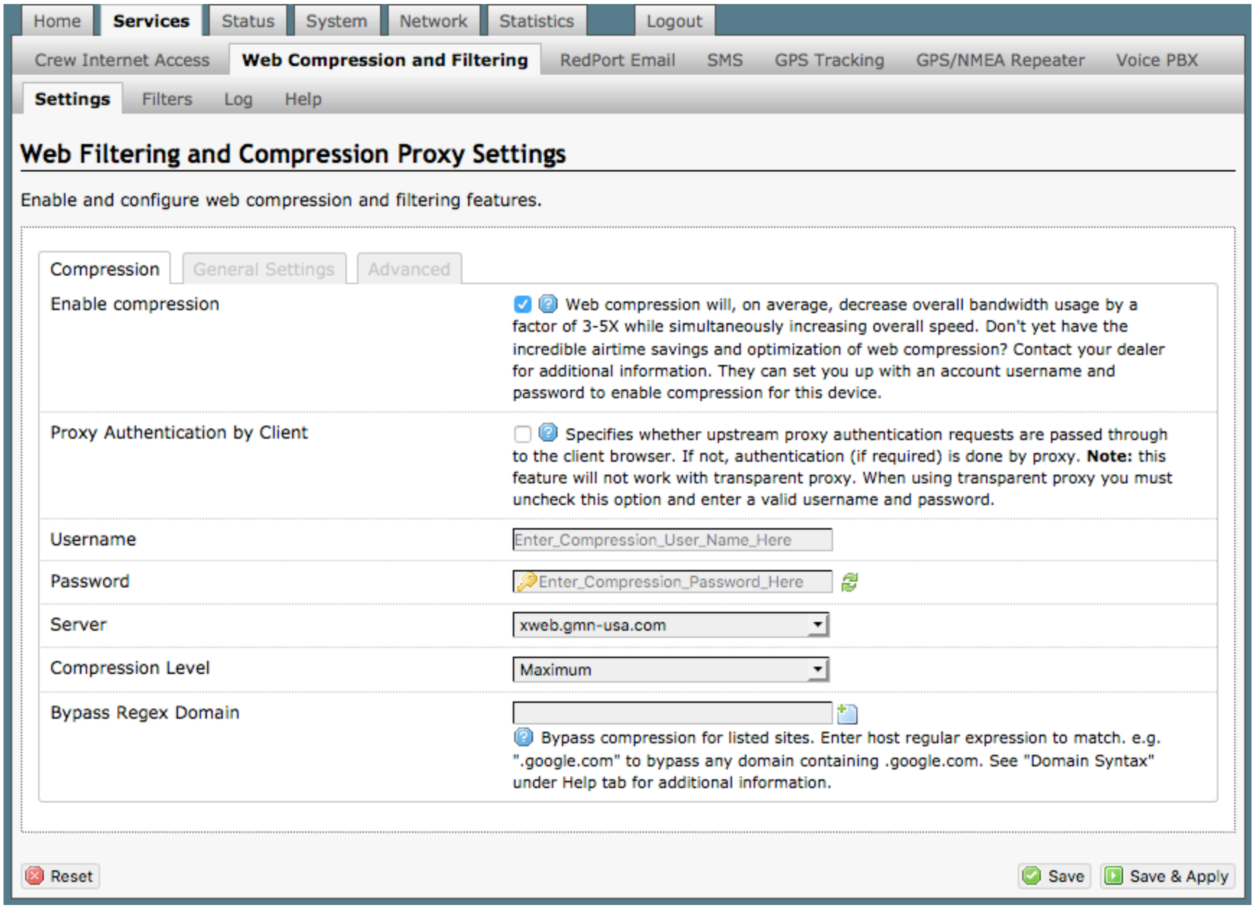
Enable Compression: If you have purchased Shared Web Compression service, select the checkbox to Enable compression. The page will expand, see With Compression Enabled below.

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.



Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

Enable compression	☑ Web compression will, on average, decrease overall bandwidth usage by a factor of 3-5X while simultaneously increasing overall speed. Don't yet have the incredible airtime savings and optimization of web compression? Contact your dealer for additional information. They can set you up with an account username and password to enable compression for this device.
Proxy Authentication by Client	□ Specifies whether upstream proxy authentication requests are passed through to the client browser. If not, authentication (if required) is done by proxy. **Note:** this feature will not work with transparent proxy. When using transparent proxy you must uncheck this option and enter a valid username and password.
Username	Enter_Compression_User_Name_Here
Password	Enter_Compression_Password_Here
Server	xweb.gmn-usa.com
Compression Level	Maximum
Bypass Regex Domain	Bypass compression for listed sites. Enter host regular expression to match. e.g. ".google.com" to bypass any domain containing .google.com. See "Domain Syntax" under Help tab for additional information.

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 airtime plans should select "Maximum". Those on high data plans may prefer "Standard" or "Minimum".

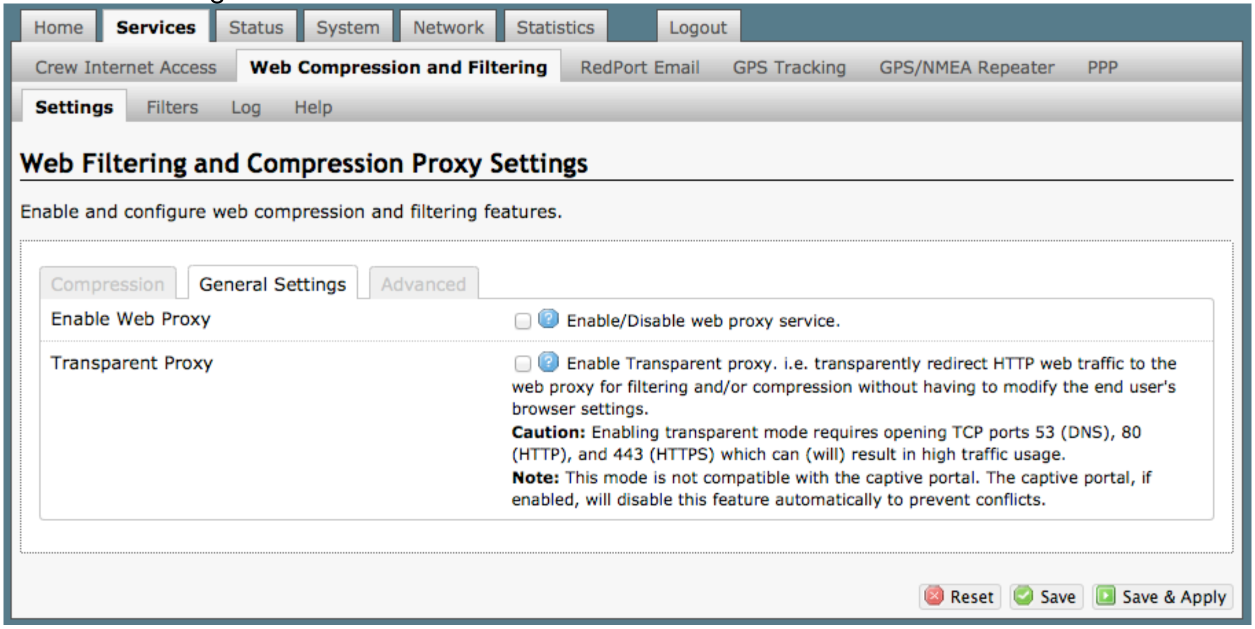
5.2.1.2 General Settings

Requires 'superadmin' login.

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.

You can still use the internal proxy server and enable transparent proxy to redirect all http traffic for filtering.



Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

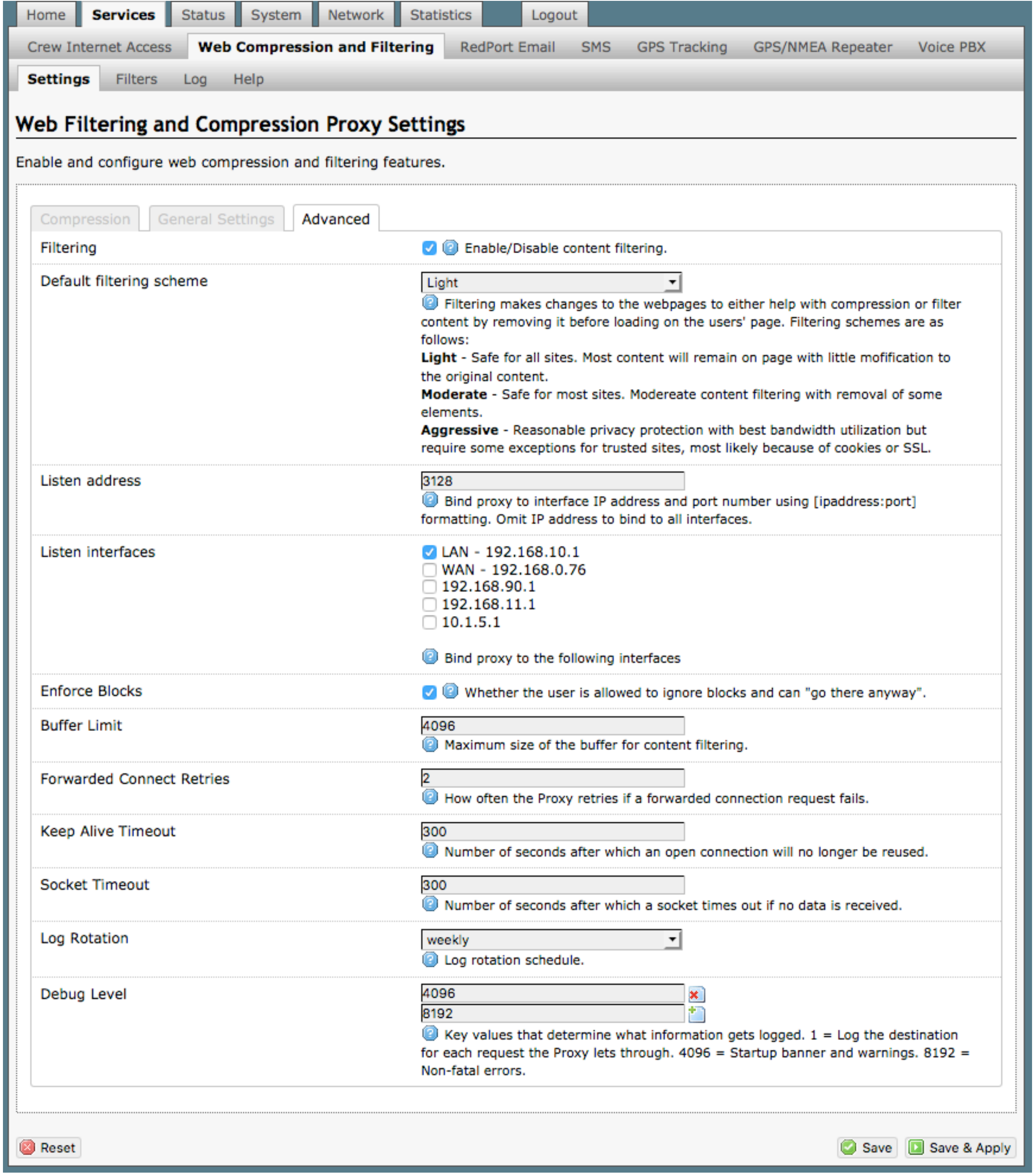
Enable Web Proxy: □ Enable/Disable web proxy service.

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

5.2.1.3 Advanced Settings

Requires 'superadmin' login.

Under normal operating conditions there is little to change here. See the next page for possible exceptions.



Web Filtering and Compression Proxy Settings

Enable and configure web compression and filtering features.

Filtering: ☑ Enable/Disable content filtering.

Default filtering scheme: Light

Filtering makes changes to the webpages to either help with compression or filter content by removing it before loading on the users' page. Filtering schemes are as follows:
Light - Safe for all sites. Most content will remain on page with little mofification to the original content.
Moderate - Safe for most sites. Modereate content filtering with removal of some elements.
Aggressive - Reasonable privacy protection with best bandwidth utilization but require some exceptions for trusted sites, most likely because of cookies or SSL.

Listen address: 3128
Bind proxy to interface IP address and port number using [ipaddress:port] formatting. Omit IP address to bind to all interfaces.

Listen interfaces:
☑ LAN - 192.168.10.1
□ WAN - 192.168.0.76
□ 192.168.90.1
□ 192.168.11.1
□ 10.1.5.1

Bind proxy to the following interfaces

Enforce Blocks: ☑ Whether the user is allowed to ignore blocks and can "go there anyway".

Buffer Limit: 4096
Maximum size of the buffer for content filtering.

Forwarded Connect Retries: 2
How often the Proxy retries if a forwarded connection request fails.

Keep Alive Timeout: 300
Number of seconds after which an open connection will no longer be reused.

Socket Timeout: 300
Number of seconds after which a socket times out if no data is received.

Log Rotation: weekly
Log rotation schedule.

Debug Level: 4096
8192
Key values that determine what information gets logged. 1 = Log the destination for each request the Proxy lets through. 4096 = Startup banner and warnings. 8192 = Non-fatal errors.

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 airtime plans. "Aggressive" has the most impact and is suggested for the best bandwidth utilization. The Aggressive setting 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.

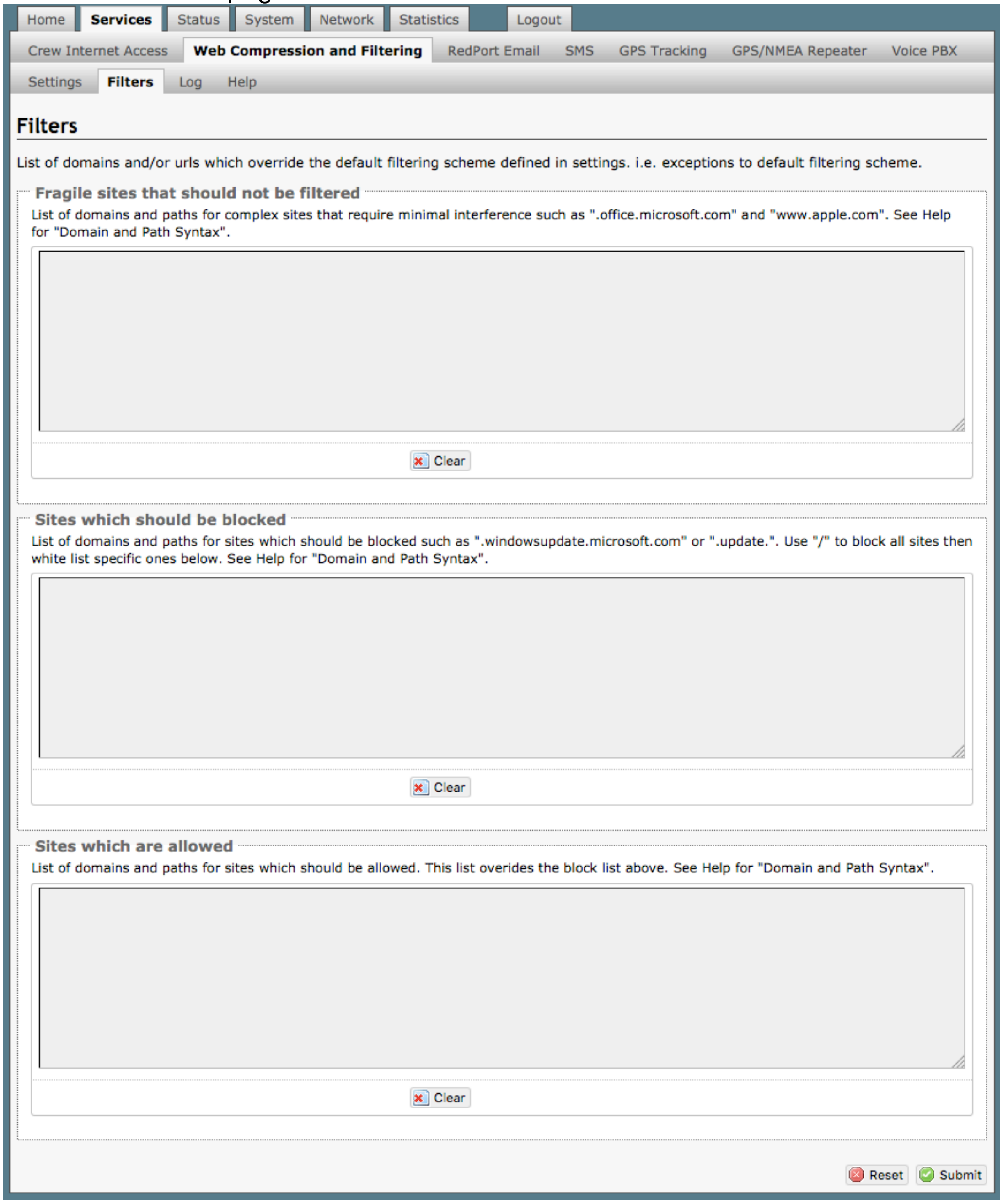
CAUTION: Utilization of debug level 1 is not recommended for normal operation. The Log files are kept in RAM and with debug level 1 activated you run the risk of RAM filling up, the Swap Partition filling up and the router may crash.

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

Requires 'superadmin' login.

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 compression enabled. See next page for details.



Filters

List of domains and/or urls which override the default filtering scheme defined in settings. i.e. exceptions to default filtering scheme.

Fragile sites that should not be filtered

List of domains and paths for complex sites that require minimal interference such as ".office.microsoft.com" and "www.apple.com". See Help for "Domain and Path Syntax".

Sites which should be blocked

List of domains and paths for sites which should be blocked such as ".windowsupdate.microsoft.com" or ".update.". Use "/" to block all sites then white list specific ones below. See Help for "Domain and Path Syntax".

Sites which are allowed

List of domains and paths for sites which should be allowed. This list overides the block list above. See Help for "Domain and Path Syntax".

There are three filter categories:

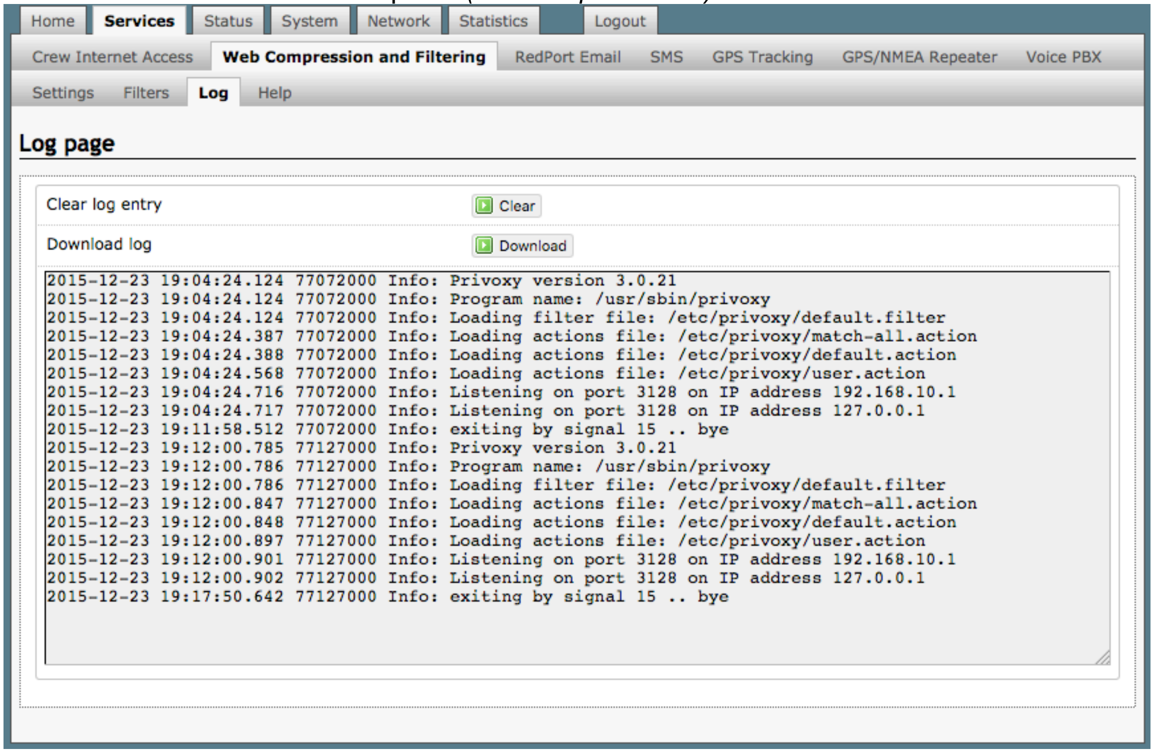
Fragile Sites: list sites that you want the content kept intact without any modification.
Sites Blocked: the blacklist; users are prevented from viewing these sites.
Sites Allowed: the whitelist; these sites are allowed for viewing. This list overrides the blocked list.

Filters respond to POSIX Regular Expressions (*see Chapter 5.2.4*). 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

Requires 'superadmin' login.

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 Chapter 5.2.4).*



```
2015-12-23 19:04:24.124 77072000 Info: Privoxy version 3.0.21
2015-12-23 19:04:24.124 77072000 Info: Program name: /usr/sbin/privoxy
2015-12-23 19:04:24.124 77072000 Info: Loading filter file: /etc/privoxy/default.filter
2015-12-23 19:04:24.387 77072000 Info: Loading actions file: /etc/privoxy/match-all.action
2015-12-23 19:04:24.388 77072000 Info: Loading actions file: /etc/privoxy/default.action
2015-12-23 19:04:24.568 77072000 Info: Loading actions file: /etc/privoxy/user.action
2015-12-23 19:04:24.716 77072000 Info: Listening on port 3128 on IP address 192.168.10.1
2015-12-23 19:04:24.717 77072000 Info: Listening on port 3128 on IP address 127.0.0.1
2015-12-23 19:11:58.512 77072000 Info: exiting by signal 15 .. bye
2015-12-23 19:12:00.785 77127000 Info: Privoxy version 3.0.21
2015-12-23 19:12:00.786 77127000 Info: Program name: /usr/sbin/privoxy
2015-12-23 19:12:00.786 77127000 Info: Loading filter file: /etc/privoxy/default.filter
2015-12-23 19:12:00.847 77127000 Info: Loading actions file: /etc/privoxy/match-all.action
2015-12-23 19:12:00.848 77127000 Info: Loading actions file: /etc/privoxy/default.action
2015-12-23 19:12:00.897 77127000 Info: Loading actions file: /etc/privoxy/user.action
2015-12-23 19:12:00.901 77127000 Info: Listening on port 3128 on IP address 192.168.10.1
2015-12-23 19:12:00.902 77127000 Info: Listening on port 3128 on IP address 127.0.0.1
2015-12-23 19:17:50.642 77127000 Info: exiting by signal 15 .. bye
```

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

Requires 'superadmin' login.

For your convenience the Help page includes:

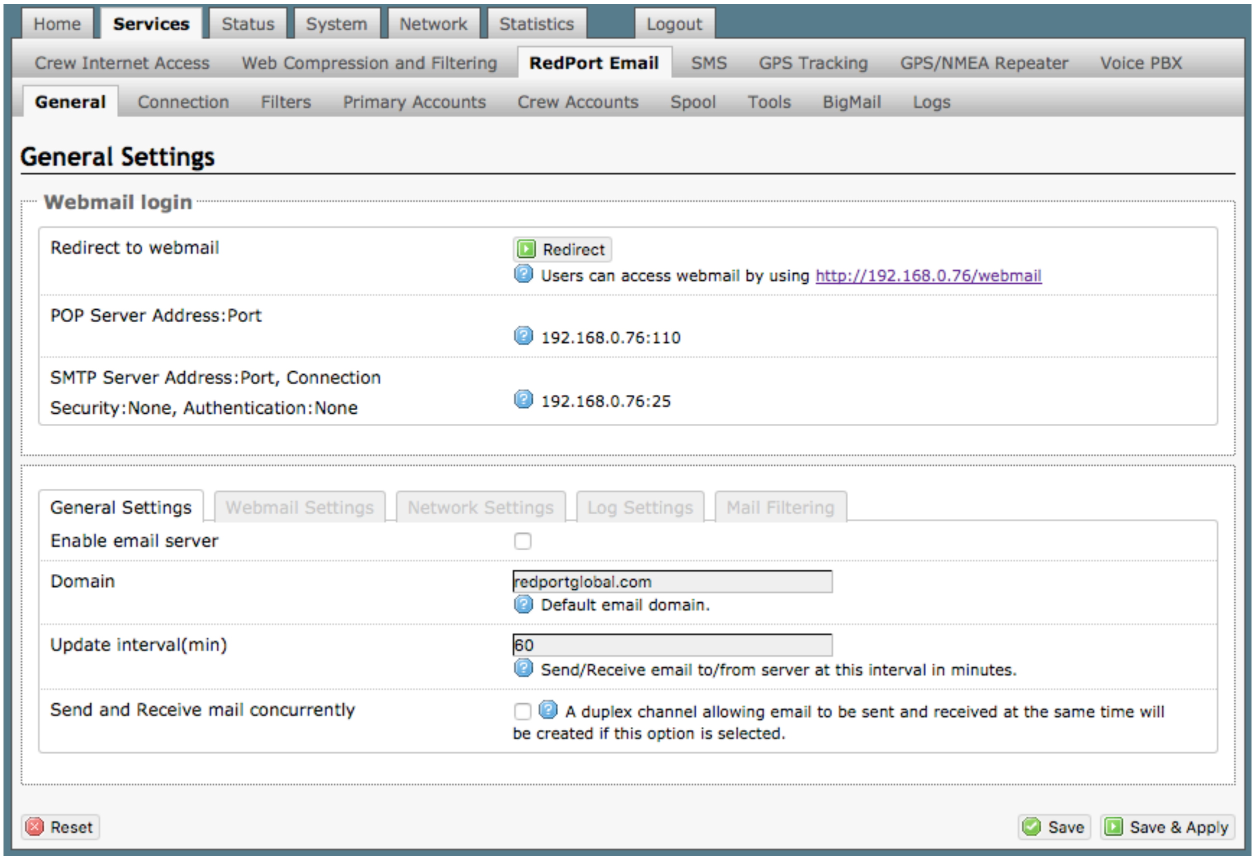
- A list of Debug Levels and their description.
- A brief explanation and some examples of the POSIX Regular Expressions that must be used for the Domain and/or Path Syntax when creating Filters.

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

5.3 RedPort Email

Requires 'superadmin' login.

This is a full-featured Crew 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.



General Settings

Webmail login

Redirect to webmail	Redirect Users can access webmail by using http://192.168.0.76/webmail
POP Server Address:Port	192.168.0.76:110
SMTP Server Address:Port, Connection Security:None, Authentication:None	192.168.0.76:25

Enable email server	□
Domain	redportglobal.com Default email domain.
Update interval(min)	60 Send/Receive email to/from server at this interval in minutes.
Send and Receive mail concurrently	□ A duplex channel allowing email to be sent and received at the same time will be created if this option is selected.

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 Premier is a POP and SMTP server as well so users can access email using their preferred email client instead of webmail access, if desired.

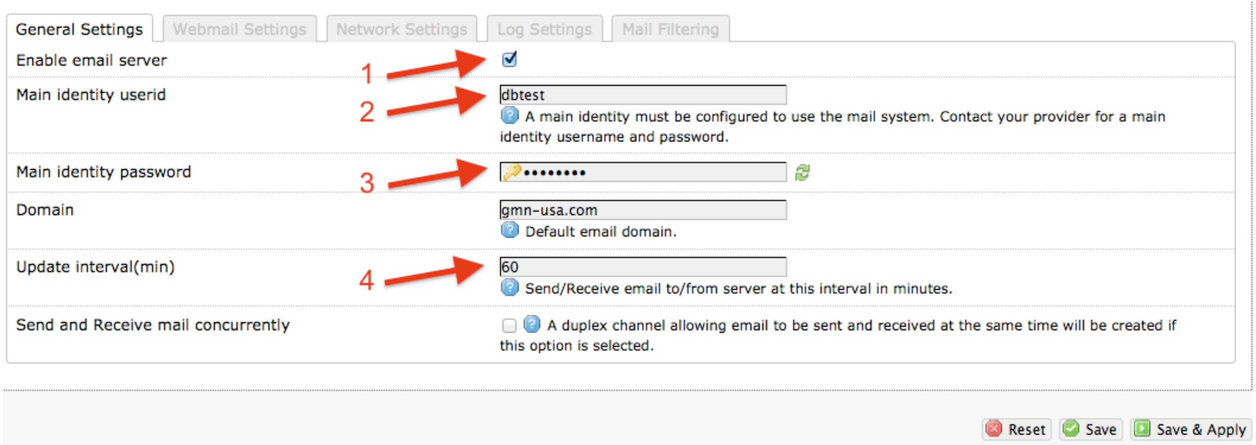
Contact your service provider for details and pricing.

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

Requires 'superadmin' login.

In the RedPort Email General Settings:



Enable email server ☑

Main identity userid: dbtest
A main identity must be configured to use the mail system. Contact your provider for a main identity username and password.

Main identity password: ••••••••

Domain: gmn-usa.com
Default email domain.

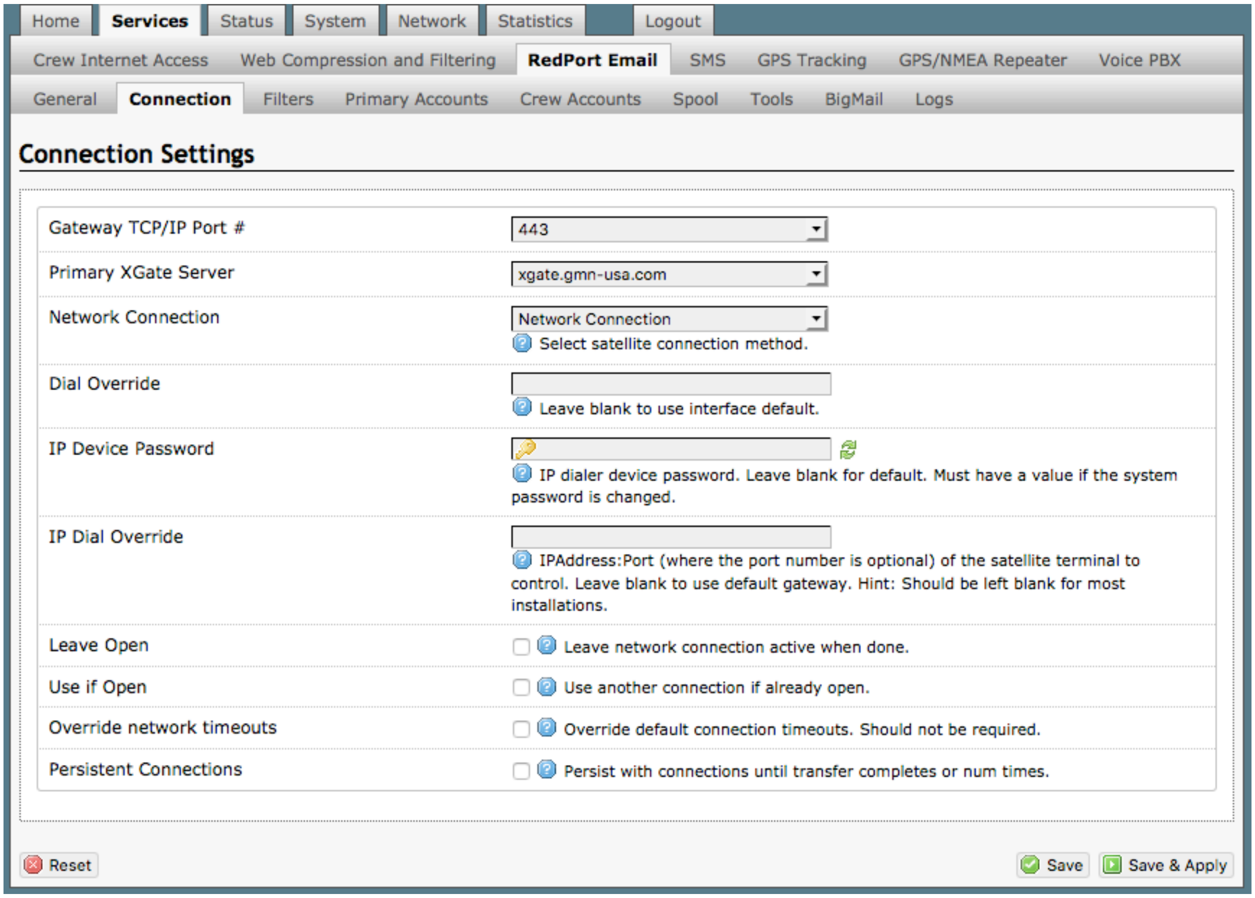
Update interval(min): 60
Send/Receive email to/from server at this interval in minutes.

Send and Receive mail concurrently ☐
A duplex channel allowing email to be sent and received at the same time will be created if this option is selected.

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: Typicially 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 Chapter 5.3.2 for more information regarding primary accounts.

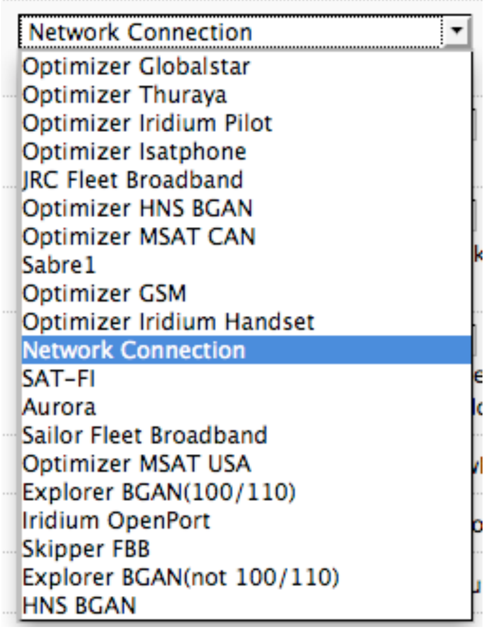
6. Go to the **Connection** tab:



Connection Settings

Gateway TCP/IP Port #	443
Primary XGate Server	xgate.gmn-usa.com
Network Connection	Network Connection Select satellite connection method.
Dial Override	Leave blank to use interface default.
IP Device Password	IP dialer device password. Leave blank for default. Must have a value if the system password is changed.
IP Dial Override	IPAddress:Port (where the port number is optional) of the satellite terminal to control. Leave blank to use default gateway. Hint: Should be left blank for most installations.
Leave Open	□ Leave network connection active when done.
Use if Open	□ Use another connection if already open.
Override network timeouts	□ Override default connection timeouts. Should not be required.
Persistent Connections	□ Persist with connections until transfer completes or num times.

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 comprehensive information about RedPort Email setup and use, please see the separate document, *Optimizer - RedPort Email Guide*.

5.3.2 Primary Accounts

Requires 'superadmin' login.

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/RedPort 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 Optimizer-RedPort Email Guide for details)*
- Inbound Mail Filter *(See Chapter 7.0 of the Optimizer-RedPort Email Guide for details)*
- Outbound Mail Filter *(See Chapter 7.0 of the Optimizer-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 Onsite Email Administrator. The Onsite Email Administrator does NOT have a crew/sub account. With this arangement, the Onsite Email Administrator will receive the system messages that cannot be viewed via a crew/sub account.

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

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

5.4 SMS Messaging

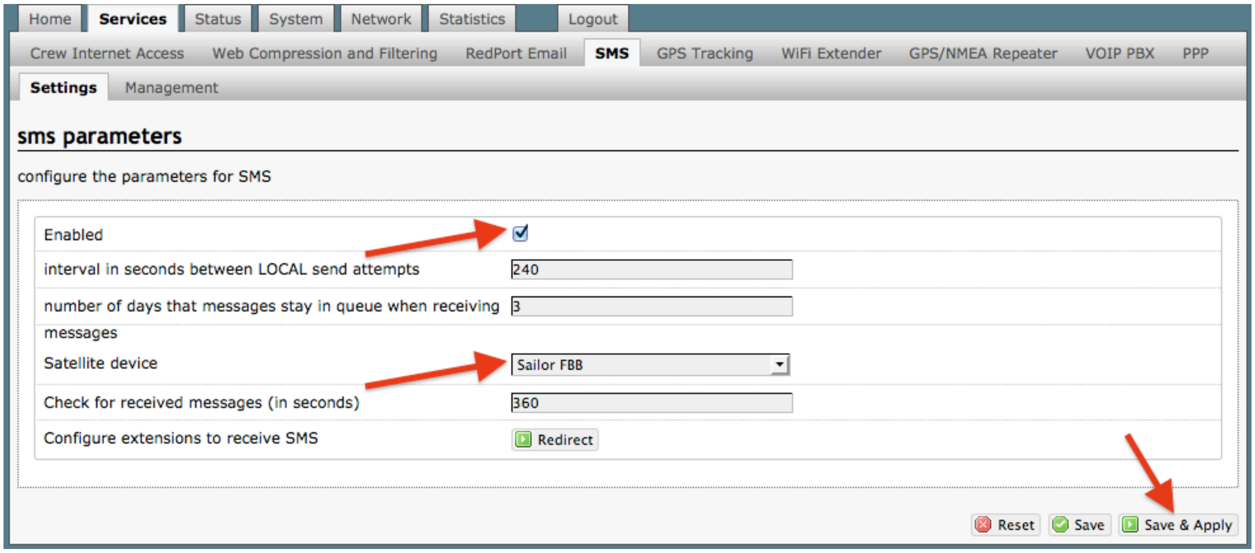
Requires 'superadmin' login.

If using a compatible satellite device, it is possible to send and receive SMS messages directly from the Optimizer Premier router and to route incoming SMS messages to one or more smartphones connected to the local wireless network.

5.4.1 SMS Settings

Requires 'superadmin' login.

Use Settings to enable and configure the SMS parameters.



sms parameters

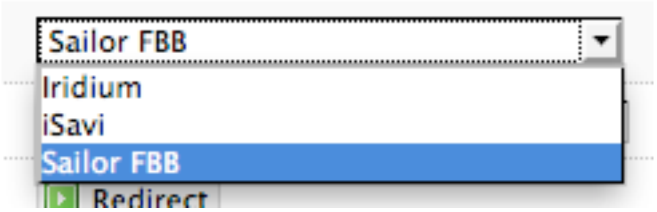
configure the parameters for SMS

Enabled	☑
interval in seconds between LOCAL send attempts	240
number of days that messages stay in queue when receiving messages	3
Satellite device	Sailor FBB
Check for received messages (in seconds)	360
Configure extensions to receive SMS	Redirect

1. Select the checkbox to enable SMS.

2. Select the appropriate Satellite device from the drop down menu.

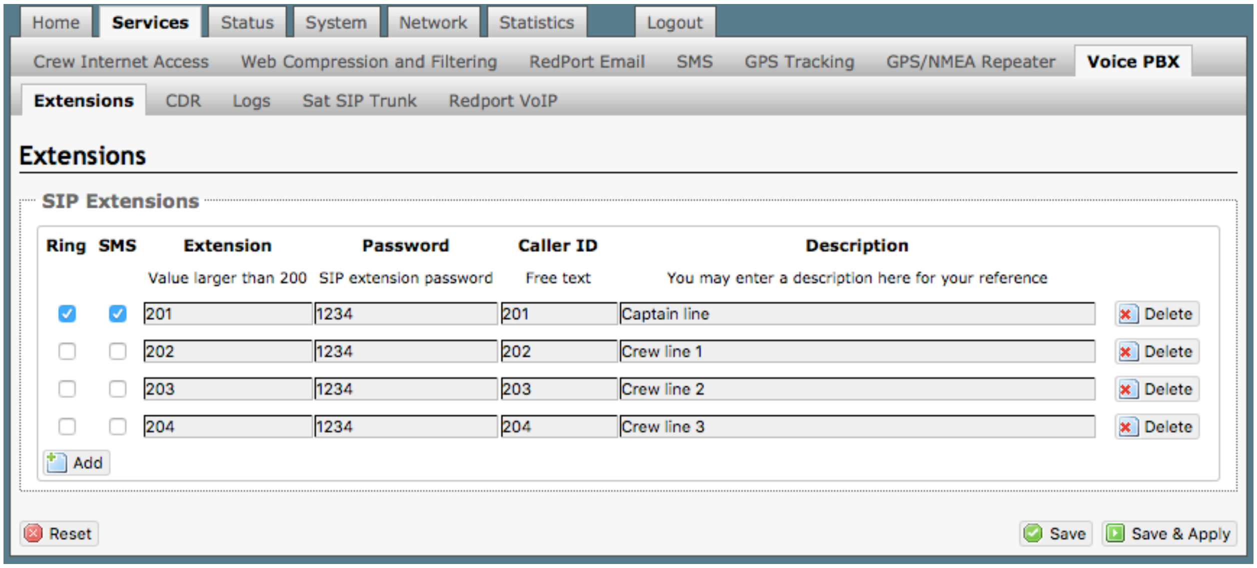
3. Select <Save & Apply>.



5.4.2 Configure SIP Extensions to Receive SMS Messages

Requires 'superadmin' login.

With SMS enabled, select <Redirect> (see SMS Settings screen above) to configure which extensions are to receive incoming SMS messages.



Extensions

SIP Extensions

Ring	SMS	Extension	Password	Caller ID	Description	
		Value larger than 200	SIP extension password	Free text	You may enter a description here for your reference	
☑	☑	201	1234	201	Captain line	☒ Delete
☐	☐	202	1234	202	Crew line 1	☒ Delete
☐	☐	203	1234	203	Crew line 2	☒ Delete
☐	☐	204	1234	204	Crew line 3	☒ Delete

To enable an extension to receive SMS messages, use the checkbox in the SMS column. For more information on configuring SIP Extensions *see Chapter 5.7.1*.

5.4.3 How to Send/Receive SMS Messages

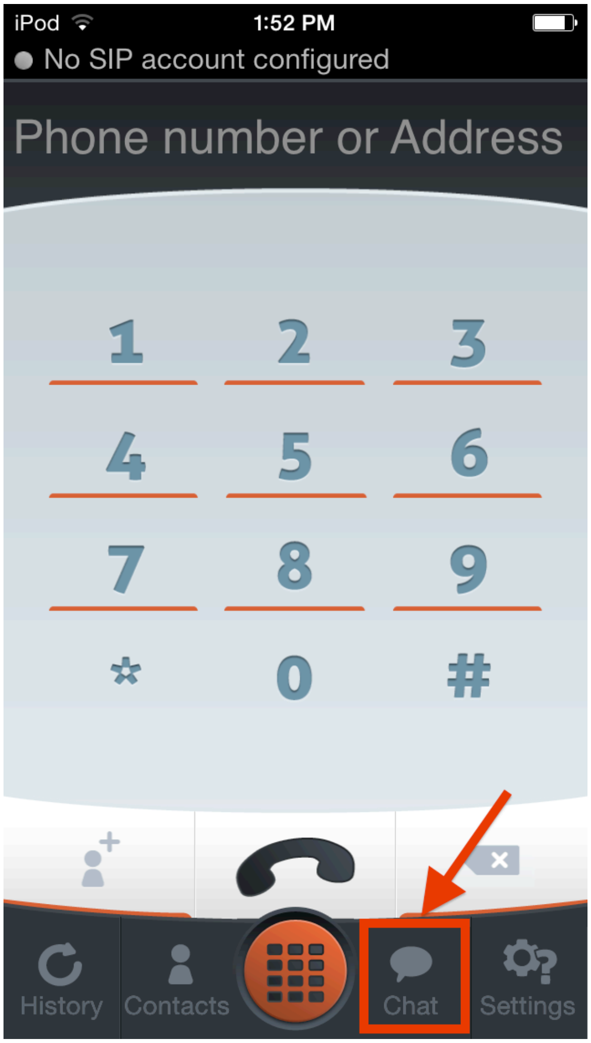
To use a smartphone or tablet to send/receive SMS messages requires XGate Phone App installed on the smartphone or tablet. The XGate Phone App can be found in Apple iTunes App Store for iOS devices and the Google Playstore for Android devices.

Using the smartphone or tablet Settings, connect to the Optimizer Premier wireless network 'wxa-165-xxxx'.

Open the XGate Phone App. Select <Chat> to send a SMS message or to view a SMS message received.

Only one SMS message can be sent at a time. Standard SMS message rates apply.

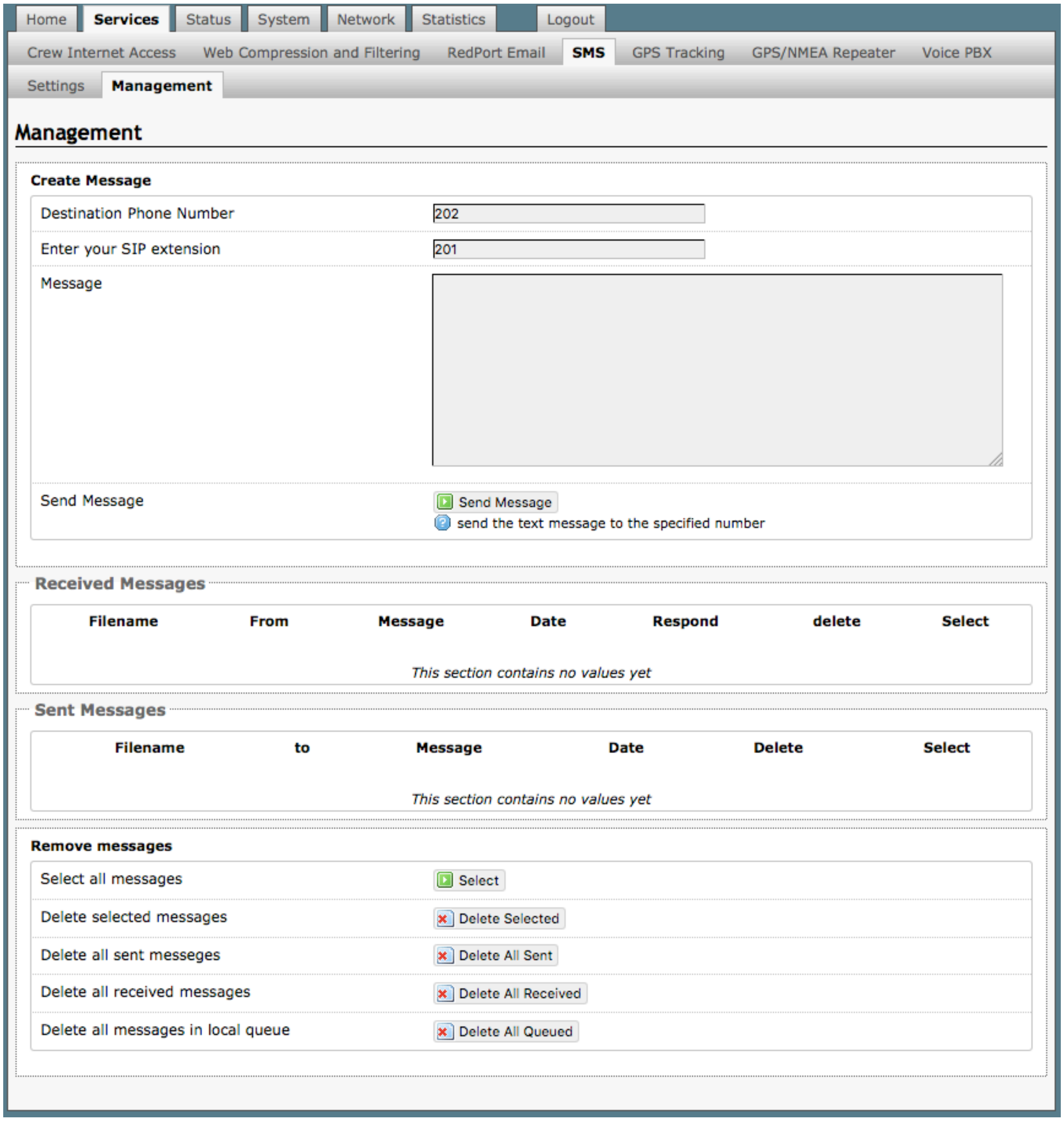
Multi-user Voice and SMS is possible with the optional RedPort VoIP service. Contact your service provider for details.



5.4.4 SMS Management

Requires 'superadmin' login.

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



Management

Create Message

Destination Phone Number	202
Enter your SIP extension	201
Message	
Send Message	Send Message send the text message to the specified number

Received Messages

Filename	From	Message	Date	Respond	delete	Select

This section contains no values yet

Sent Messages

Filename	to	Message	Date	Delete	Select

This section contains no values yet

Remove messages

Select all messages	Select
Delete selected messages	☒ Delete Selected
Delete all sent messeges	☒ Delete All Sent
Delete all received messages	☒ Delete All Received
Delete all messages in local queue	☒ Delete All Queued

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

5.5 GPS Tracking

Requires 'superadmin' login.

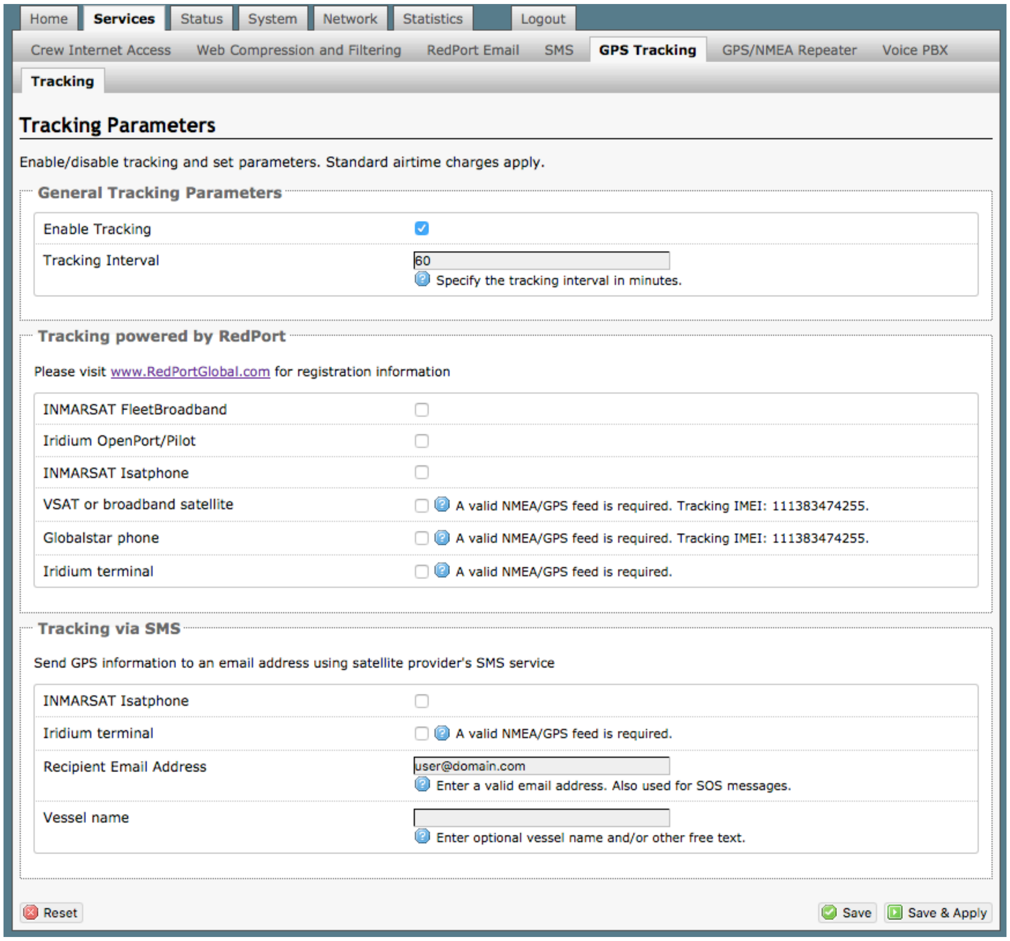
If you wish to have tracking service using your satellite device, the Optimizer offers GPS Tracking service powered by GSatTrack or Tracking service via SMS message.

5.5.1 Tracking powered by RedPort with GSatTrack

Requires 'superadmin' login.

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.



Tracking Parameters

Enable/disable tracking and set parameters. Standard airtime charges apply.

General Tracking Parameters

Enable Tracking	☑
Tracking Interval	60 Specify the tracking interval in minutes.

Tracking powered by RedPort

Please visit www.RedPortGlobal.com for registration information

INMARSAT FleetBroadband	□
Iridium OpenPort/Pilot	□
INMARSAT Isatphone	□
VSAT or broadband satellite	□ A valid NMEA/GPS feed is required. Tracking IMEI: 111383474255.
Globalstar phone	□ A valid NMEA/GPS feed is required. Tracking IMEI: 111383474255.
Iridium terminal	□ A valid NMEA/GPS feed is required.

Tracking via SMS

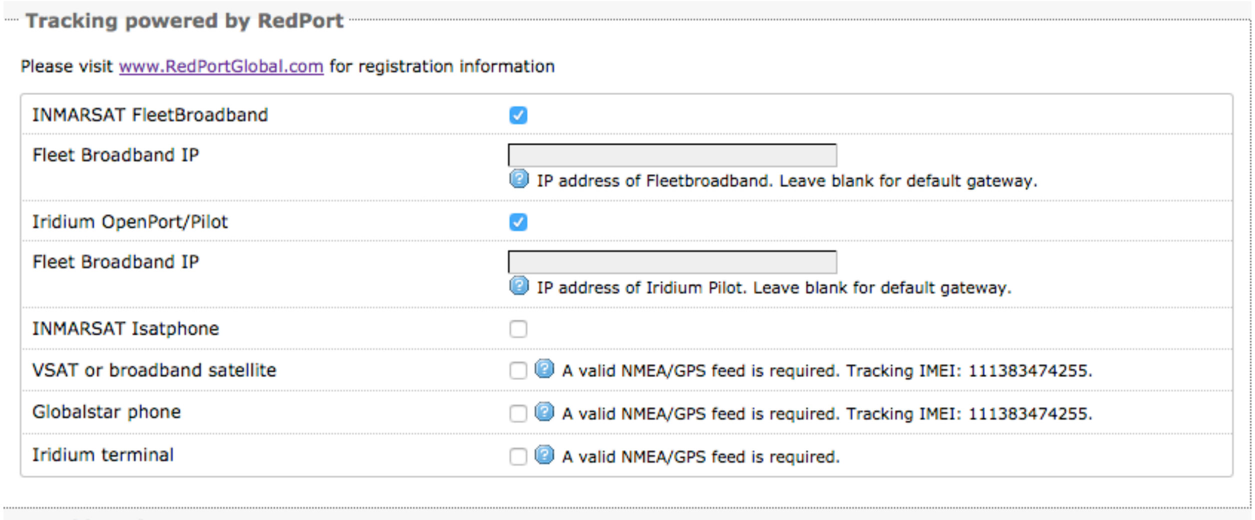
Send GPS information to an email address using satellite provider's SMS service

INMARSAT Isatphone	□
Iridium terminal	□ A valid NMEA/GPS feed is required.
Recipient Email Address	user@domain.com Enter a valid email address. Also used for SOS messages.
Vessel name	 Enter optional vessel name and/or other free text.

1. **Enable Tracking** by selecting the checkbox.

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

2. Go to **Tracking powered by RedPort** and select the satellite terminal you are using. Note: a valid NMEA/GPS feed is required when using some satellite devices.



Tracking powered by RedPort

Please visit www.RedPortGlobal.com for registration information

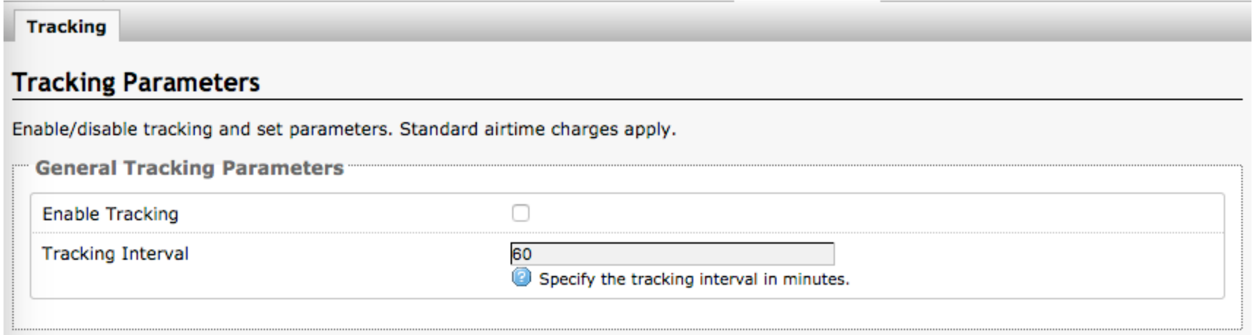
INMARSAT FleetBroadband	☑
Fleet Broadband IP	? IP address of Fleetbroadband. Leave blank for default gateway.
Iridium OpenPort/Pilot	☑
Fleet Broadband IP	? IP address of Iridium Pilot. Leave blank for default gateway.
INMARSAT Isatphone	☐
VSAT or broadband satellite	☐ ? A valid NMEA/GPS feed is required. Tracking IMEI: 111383474255.
Globalstar phone	☐ ? A valid NMEA/GPS feed is required. Tracking IMEI: 111383474255.
Iridium terminal	☐ ? A valid NMEA/GPS feed is required.

3. Select <Save & Apply>.

5.5.2 Tracking via SMS

Requires 'superadmin' login.

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.



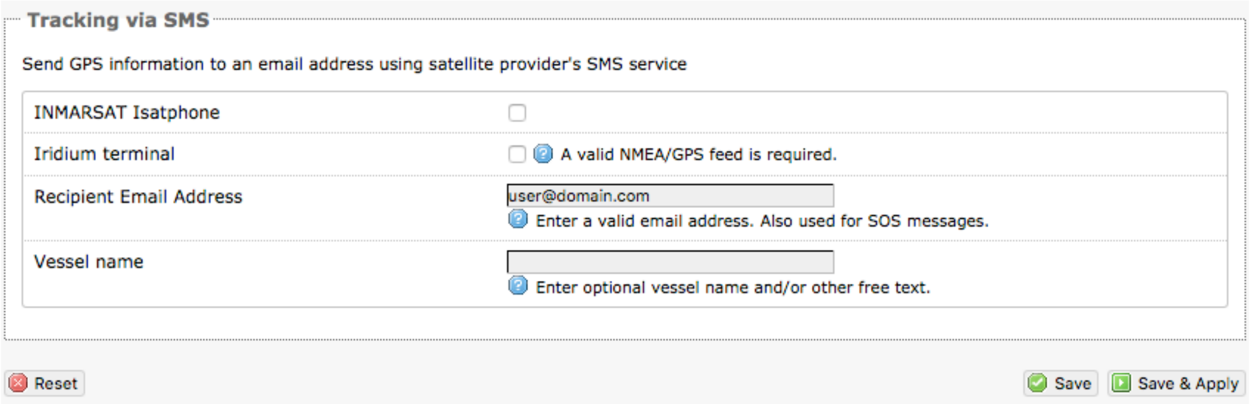
Tracking Parameters

Enable/disable tracking and set parameters. Standard airtime charges apply.

General Tracking Parameters

Enable Tracking	□
Tracking Interval	60 Specify the tracking interval in minutes.

-- / / --



Tracking via SMS

Send GPS information to an email address using satellite provider's SMS service

INMARSAT Isatphone	□
Iridium terminal	□ A valid NMEA/GPS feed is required.
Recipient Email Address	user@domain.com Enter a valid email address. Also used for SOS messages.
Vessel name	 Enter optional vessel name and/or other free text.

1. **Enable Tracking** by selecting the checkbox.

2. Enter the **Tracking Interval** in minutes; the default is set to hourly reporting (60 minutes). This means that every 60 minutes a position report will be transmitted 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.

3. Go to **Tracking via SMS** and 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.

4. 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.

5. Select <Save & Apply>.

5.6 GPS/NMEA Repeater

Requires 'superadmin' login.

The Optimizer Premier 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:

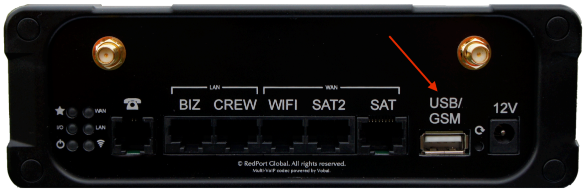
- A USB connected GPS or NMEA device.
- A serial port connected GPS or NMEA device with appropriate USB to Serial Adapter.

5.6.1 Equipment Setup

A physical connection is required from the source (GPS/NMEA device) to the Optimizer.

5.6.1.1 USB NMEA Device

When using a NMEA device that supports a USB connection, connect the NMEA device to the USB port on the rear of the Optimzer with an appropriate USB to NMEA device cable as indicated by the NMEA device manufacturer.



CAUTION: It is not recommended to have a USB Satphone and GSM modem connected at the same time via a USB Hub. It may create conflicts.

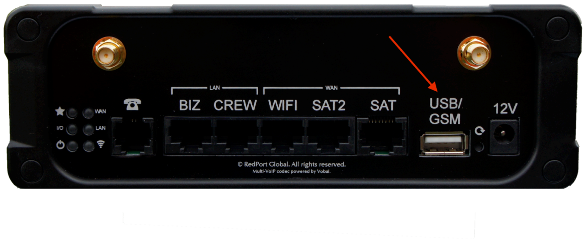
The Optimizer will broadcast the GPS signal over WiFi, so you can connect your computer to the WiFi network in order to establish a successful connection with your destination software.

5.6.1.2 RS-232 NMEA Device

With Serial Port Connector

When using a NMEA device with Serial Port connection, a USB to Serial Adapter (PL-2303HX or FTDI Chip) is required.

CAUTION: While all standard USB to serial adapters may work, the PL-2303HX and the FTDi Chip are the only USB to Serial Adapters that we recommend as compatible with the Optimizer.



Connect the NMEA device to the USB port on the rear of the Optimizer with an approriate USB to Serial Adapter.

The Optimizer will broadcast the GPS signal over WiFi, so you can connect your computer to the WiFi network 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 a PL-2302HX or a FTDI Chip USB to serial adapter as noted above.

5.6.1.3 Connecting Multiple NMEA Devices

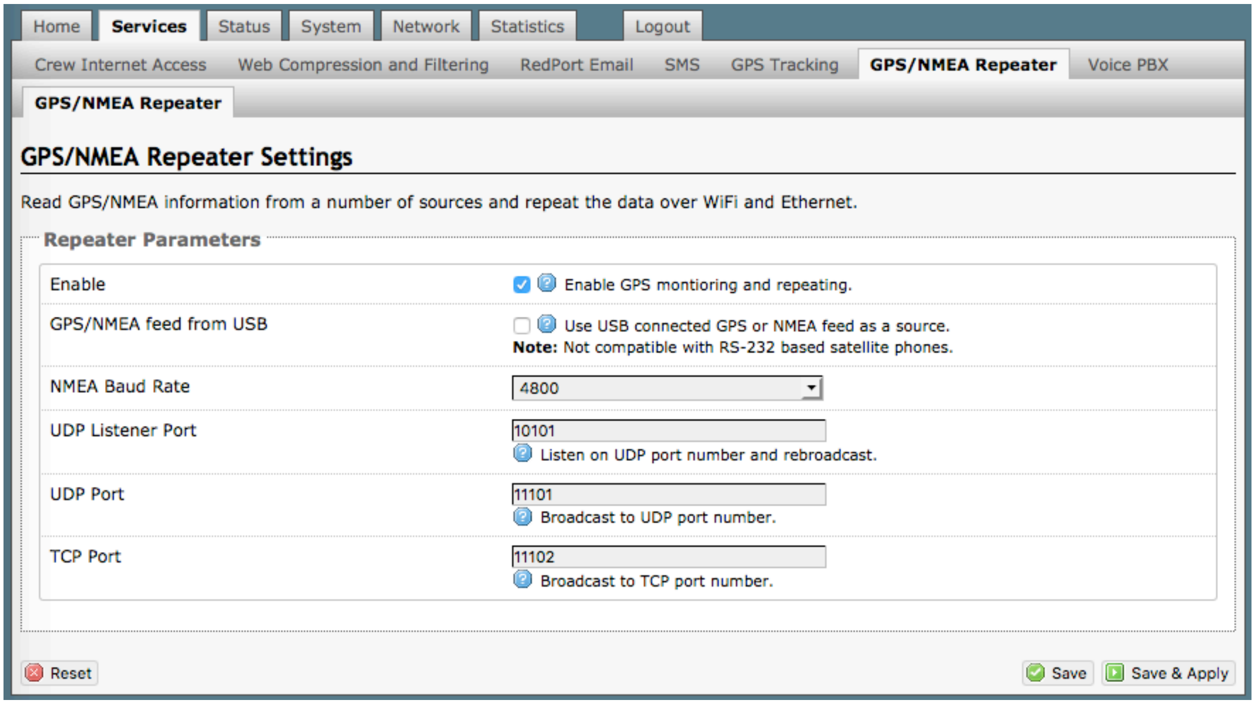
It is possible to connect up to four NMEA devices if you have the proper hardware. It will require a USB to RS-232 4-port Hub or a RS-232 4-port terminal block that you would simply plug into the Optimizer's USB port.

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

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.



GPS/NMEA Repeater Settings

Read GPS/NMEA information from a number of sources and repeat the data over WiFi and Ethernet.

Repeater Parameters

Enable	☑ Enable GPS montioring and repeating.
GPS/NMEA feed from USB	□ Use USB connected GPS or NMEA feed as a source. **Note:** Not compatible with RS-232 based satellite phones.
NMEA Baud Rate	4800
UDP Listener Port	10101 Listen on UDP port number and rebroadcast.
UDP Port	11101 Broadcast to UDP port number.
TCP Port	11102 Broadcast to TCP port number.

1. **Enable** - Select this checkbox to Enable GPS monitoring and repeating.

2. **GPS/NMEA feed from USB -** Select this when connecting a GPS or NMEA device via USB cable.

3. **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.

4. **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.

5. **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.)

6. **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 (i.e. the BIZ port and the WAN ports, by default, are open). Any port that is configured to go through the Captive Portal will not work with the GPS/NMEA Repeater feature.

5.7 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*. (See Chapter 5.7.4)
- IsatHub iSavi - requires IsatHub Control app and either IsatHub Voice app or XGate Phone app*. (*See Optimizer Voice iSavi Addendum for information on how to pair the iSavi with the Optimizer Premier.)*
- Any satellite terminal with a RJ-11 port - requires XGate Phone app* AND an ATA adapter. (We support the Grandstream HT701 and the Cisco SPA 112)

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. *See Chapter 5.7.5.*

As of this writing, Multi-VoIP is compatible with the following:

- FBB
- BGAN
- VSAT
- RedPort Aurora
- Iridium Pilot
- Thuraya IP
- IsatHub iSavi

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

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

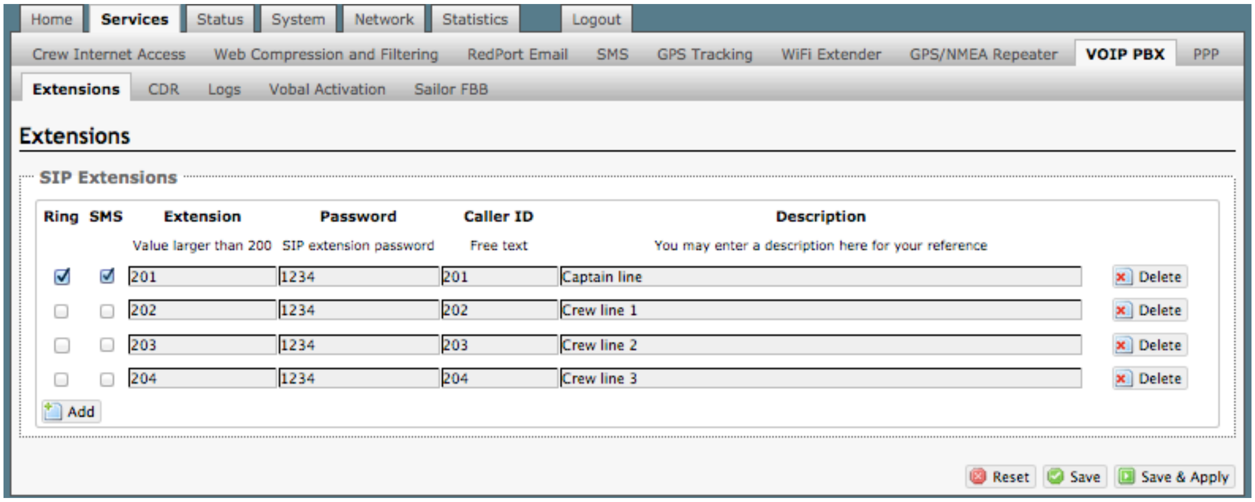
5.7.1 Setup Extensions

Requires 'superadmin' login.

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 on those extensions with Ring enabled.

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



Extensions

SIP Extensions

Ring	SMS	Extension	Password	Caller ID	Description	
		Value larger than 200	SIP extension password	Free text	You may enter a description here for your reference	
☑	☑	201	1234	201	Captain line	☒ Delete
□	□	202	1234	202	Crew line 1	☒ Delete
□	□	203	1234	203	Crew line 2	☒ Delete
□	□	204	1234	204	Crew line 3	☒ Delete

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

5.7.1.1 How to Make/Receive Voice Calls

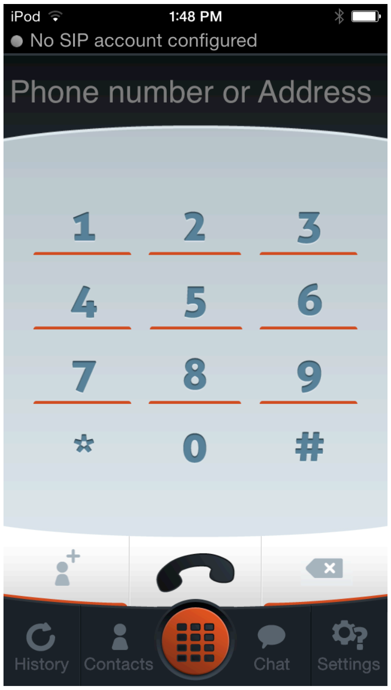
Using the smartphone or tablet Settings, connect to the Optimizer wireless network 'wxa-163-xxxx'.

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. *See Section 5.8.4*)

IMPORTANT: Inmarsat IsatHub (iSavi) users. *Please see Appendix C for the iSavi Quick Start Guide containing information and instructions for setup and use of the Optimizer with the iSavi terminal for voice calls and sms messaging.*



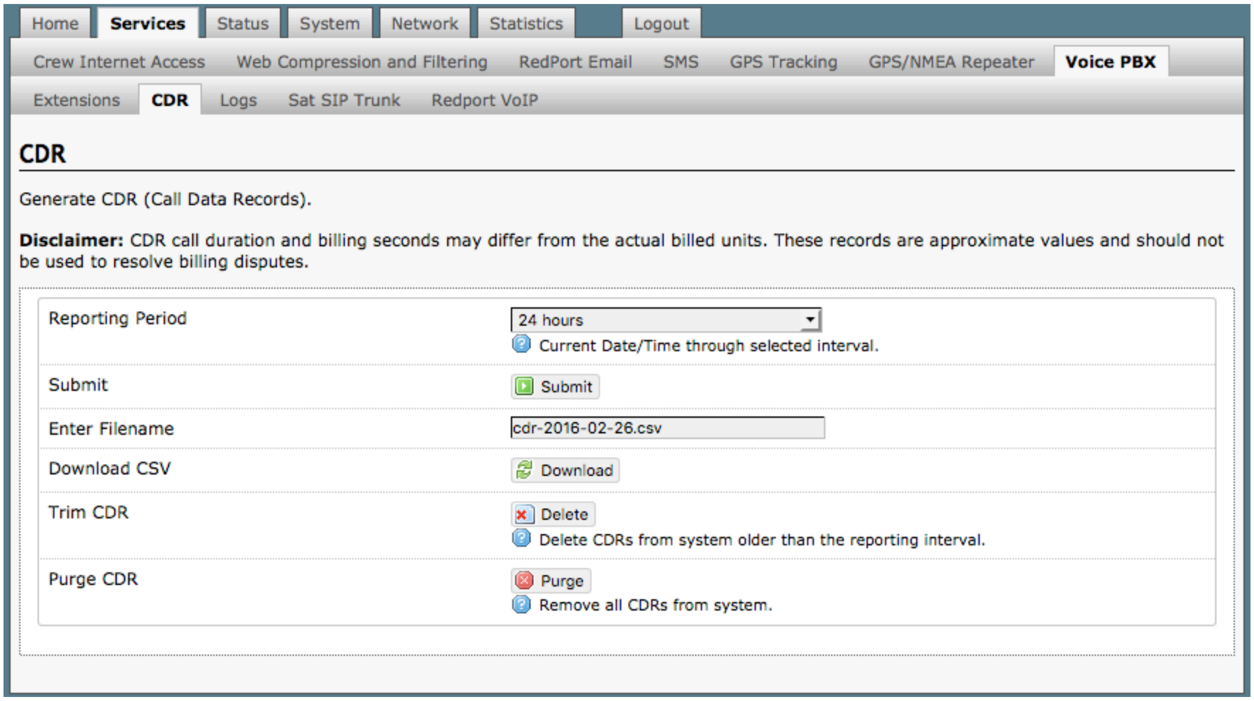
No SIP account configured

Phone number or Address

5.7.2 CDR (Call Data Records)

Requires 'superadmin' login.

It is possible to view and download the Call Data Records. The Call Data Records stored on the Optimizer are approximate values and should not be used to resolve billing disputes. They are presented here for your convenience.



CDR

Generate CDR (Call Data Records).

Disclaimer: CDR call duration and billing seconds may differ from the actual billed units. These records are approximate values and should not be used to resolve billing disputes.

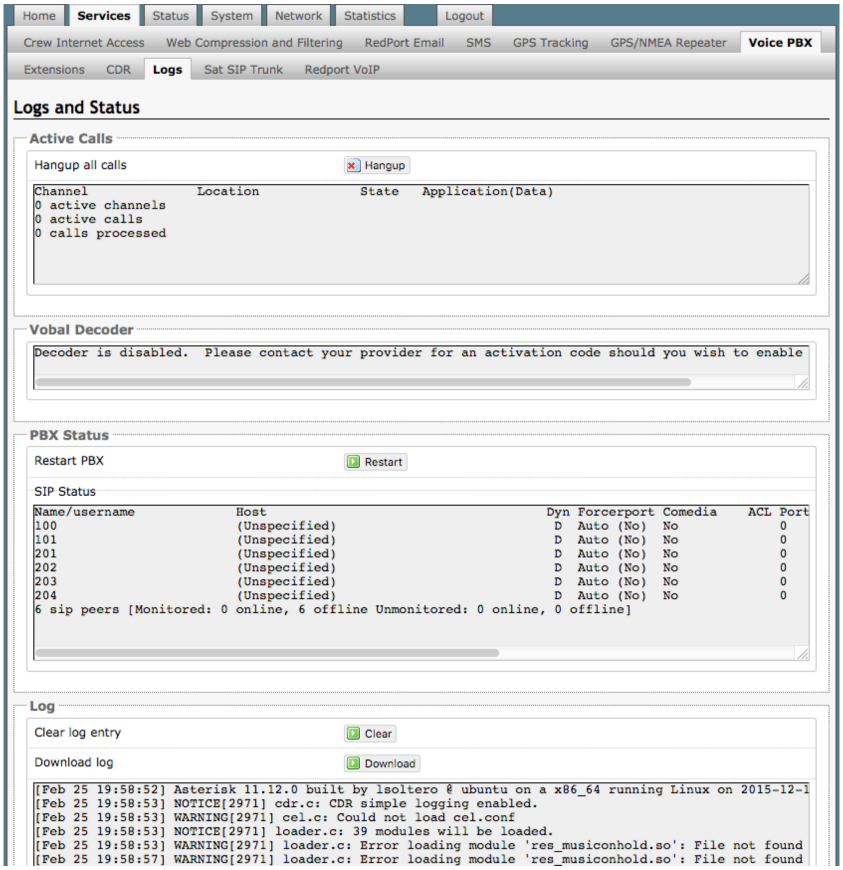
Reporting Period	24 hours Current Date/Time through selected interval.
Submit	Submit
Enter Filename	cdr-2016-02-26.csv
Download CSV	Download
Trim CDR	Delete Delete CDRs from system older than the reporting interval.
Purge CDR	Purge Remove all CDRs from system.

On active systems, the call data records can quickly use up memory. It is recommend that you periodically **Trim CDR** or **Purge CDR** records from the system.

5.7.3 Logs

Requires 'superadmin' login.

This screen provides PBX status information and some management.



Logs and Status

Active Calls

Hangup all calls ☒ Hangup

```
Channel              Location             State    Application(Data)
0 active channels
0 active calls
0 calls processed
```

Vobal Decoder

```
Decoder is disabled.  Please contact your provider for an activation code should you wish to enable
```

PBX Status

Restart PBX ▶ Restart

SIP Status

```
Name/username             Host                                   Dyn Forcerport Comedia    ACL Port
100                       (Unspecified)                           D  Auto (No)  No             0
101                       (Unspecified)                           D  Auto (No)  No             0
201                       (Unspecified)                           D  Auto (No)  No             0
202                       (Unspecified)                           D  Auto (No)  No             0
203                       (Unspecified)                           D  Auto (No)  No             0
204                       (Unspecified)                           D  Auto (No)  No             0
6 sip peers [Monitored: 0 online, 6 offline Unmonitored: 0 online, 0 offline]
```

Log

Clear log entry ▶ Clear

Download log ▶ Download

```
[Feb 25 19:58:52] Asterisk 11.12.0 built by lsoltero @ ubuntu on a x86_64 running Linux on 2015-12-1
[Feb 25 19:58:53] NOTICE[2971] cdr.c: CDR simple logging enabled.
[Feb 25 19:58:53] WARNING[2971] cel.c: Could not load cel.conf
[Feb 25 19:58:53] NOTICE[2971] loader.c: 39 modules will be loaded.
[Feb 25 19:58:53] WARNING[2971] loader.c: Error loading module 'res_musiconhold.so': File not found
[Feb 25 19:58:57] WARNING[2971] loader.c: Error loading module 'res_musiconhold.so': File not found
```

Active Calls: displays all active channels in use. Select <Hangup> to immediately hangup all active calls.

Vobal Decoder: Displays the VoIP Activation Key when RedPort VoIP service is enabled. *See Chapter 5.7.5.*

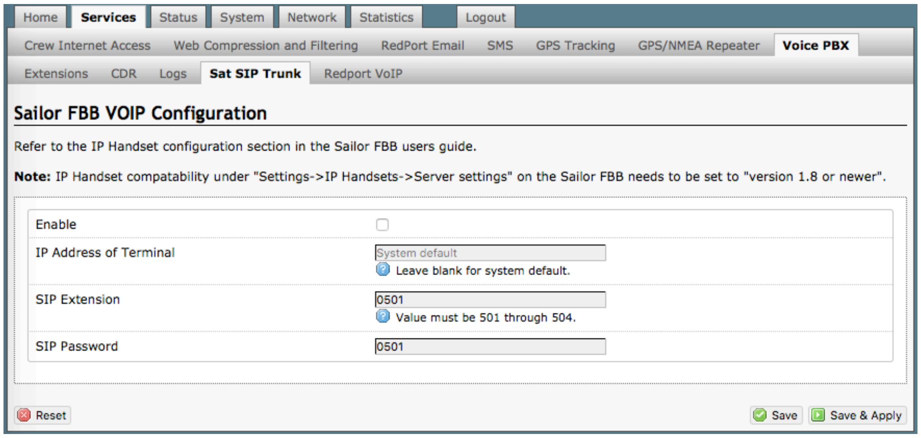
PBX Status: Displays the current status of all SIP extensions. Select <Restart> to reboot the PBX service.

Log: Displays the current Log of PBX usage. Select <Clear> to remove the log content. Select <Download> to Open or Save the PBX Log.

5.7.4 Sat SIP Trunk (for Sailor FBB terminal only)

Requires 'superadmin' login.

Use this screen to enable and configure SIP calling when using a Sailor FBB terminal.



Sailor FBB VOIP Configuration

Refer to the IP Handset configuration section in the Sailor FBB users guide.

Note: IP Handset compatability under "Settings->IP Handsets->Server settings" on the Sailor FBB needs to be set to "version 1.8 or newer".

Enable	□
IP Address of Terminal	System default Leave blank for system default.
SIP Extension	0501 Value must be 501 through 504.
SIP Password	0501

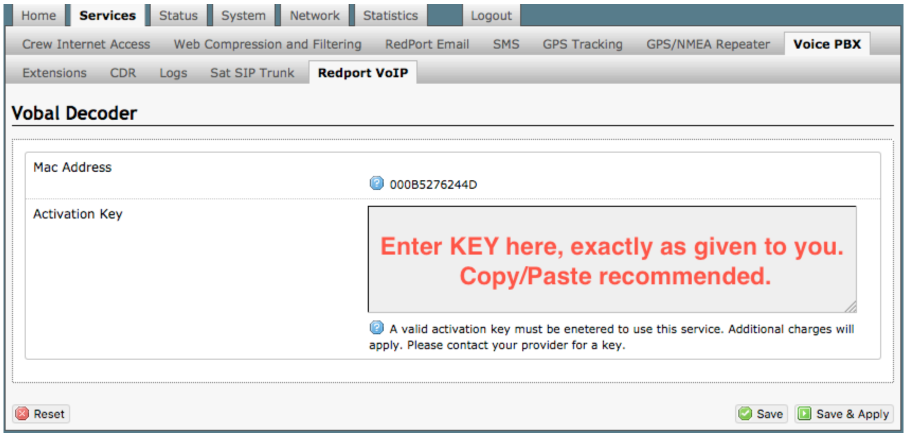
NOTE: You may need to edit the IP Handset configuration in the Sailor FBB user interface. Settings > IP Handsets > Server Settings on the Sailor FBB must be set to version 1.8 or newer. (Refer to the Sailor FBB users guide for how to access the Sailor FBB Settings).

5.7.5 RedPort VoIP Activation

Requires 'superadmin' login.

With optional RedPort VoIP service, up to four users can send/receive phone calls and/or text messages simultaneously. Outbound calls are typically less expensive VoIP calls than standard circuit switch (PSTN) calls at regular satellite airtime rates. Contact your satellite service provider to purchase the RedPort VoIP service.

When the service is activated, you will be given a "Key". This key is a long alpha-numeric string that must be entered into the Optimizer user interface.



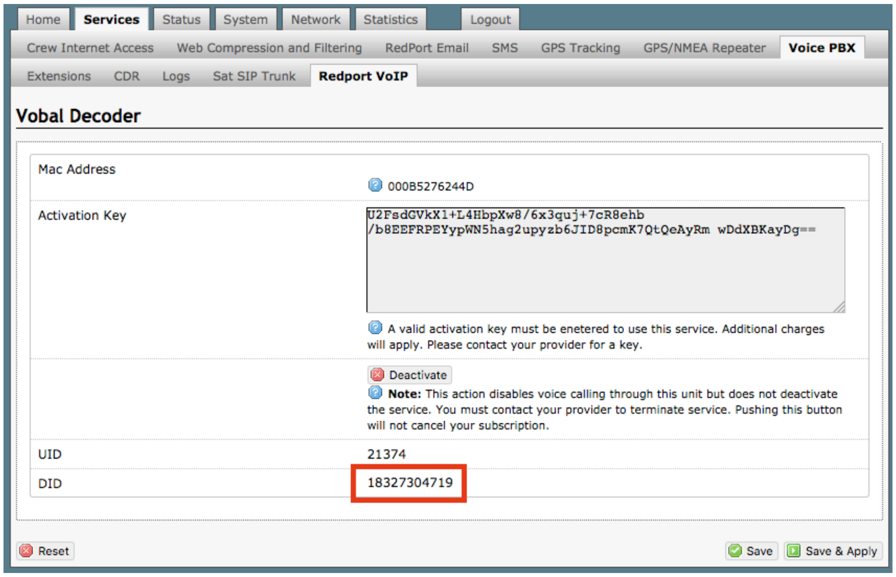
Vobal Decoder

Mac Address: 000B5276244D

Activation Key: Enter KEY here, exactly as given to you. Copy/Paste recommended.

A valid activation key must be enetered to use this service. Additional charges will apply. Please contact your provider for a key.

Enter the Key and select <Save & Apply>.



Vobal Decoder

Mac Address: 000B5276244D

Activation Key:

```
U2FsdGVkX1+L4HbpXw8/6x3quj+7cR8ehb
/b8EEFRPEYypWN5hag2upyzb6JID8pcmK7QtQeAyRm wDdXBKayDg==
```

A valid activation key must be enetered to use this service. Additional charges will apply. Please contact your provider for a key.

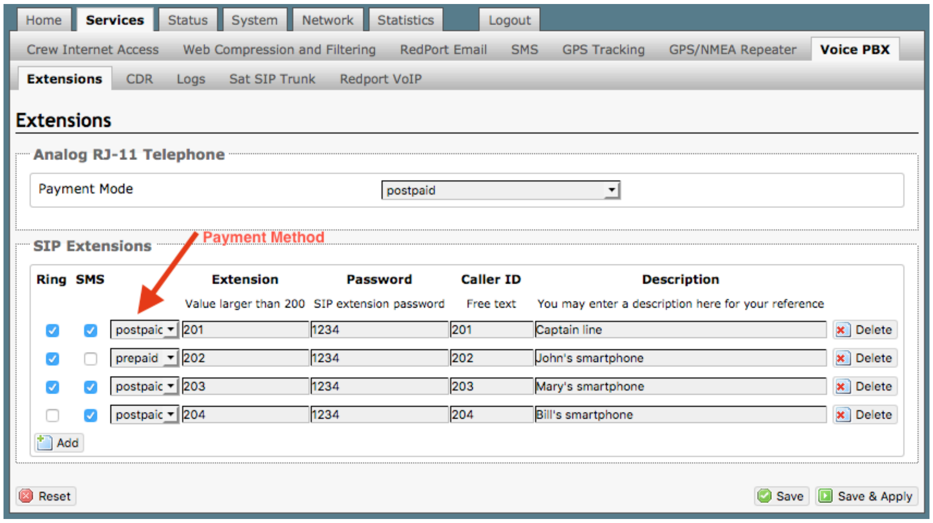
Note: This action disables voice calling through this unit but does not deactivate the service. You must contact your provider to terminate service. Pushing this button will not cancel your subscription.

UID: 21374

DID: 18327304719

With RedPort VoIP service activated, the new RedPort VoIP telephone number is displayed.

Configure the SIP extensions for Ring and/or SMS by selecting the checkbox next to the SIP extension. *See Chapter 5.7.1.*



Extensions

Analog RJ-11 Telephone

Payment Mode: postpaid

SIP Extensions

Ring	SMS		Extension Value larger than 200	Password SIP extension password	Caller ID Free text	Description You may enter a description here for your reference	
☑	☑	postpaic	201	1234	201	Captain line	Delete
☑	☐	prepaid	202	1234	202	John's smartphone	Delete
☑	☑	postpaic	203	1234	203	Mary's smartphone	Delete
☐	☑	postpaic	204	1234	204	Bill's smartphone	Delete

Select the payment method of each SIP extension (prepaid or postpaid). There must be at least one postpaid line. By default, Line 1 always Postpaid.

On this page, you can also:

- change the SIP extension password
- change the outgoing CallerID display
- enter a description for your reference

In the example above, when an incoming call arrives, only the phones of the Captain, John, and Mary will ring. Incoming SMS messages will appear on the phones of the Captain, Mary, and Bill.

When the configuration of the SIP extensions is complete, select <Save & Apply>

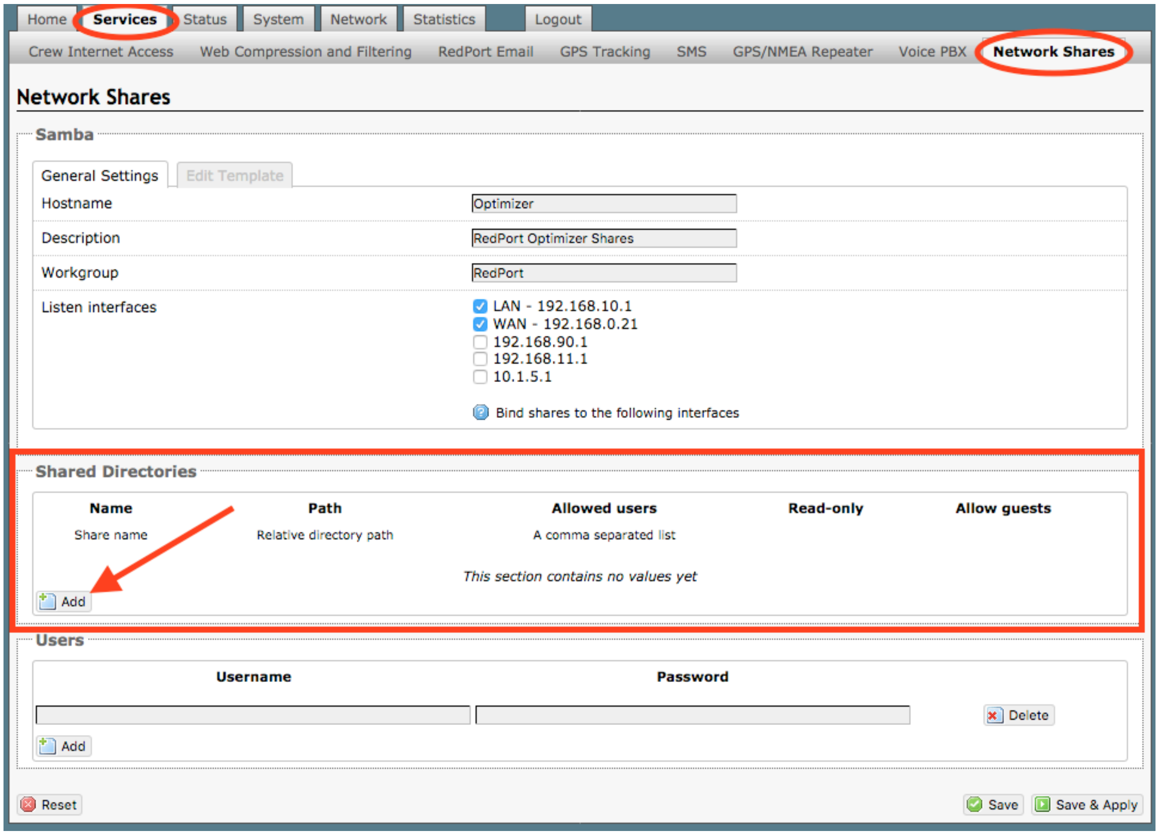
5.8 Network Shares

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

Network Shares allows the sharing of files without the requirement of a wired local network of computers. The Optimizer router can be configured with one or more Shared Directories that are available, with or without password protection, to any Windows or Mac PC that has access to the Optimizer's WiFi Hotspot.

Network Shares also allows the ability to automatically transfer files via inbound and outbound email *(see Optimizer-RedPort Email Guide > Appendix: File Transfer for details).*

5.8.1 Create a Shared Directory



Network Shares

Samba

General Settings | Edit Template

Hostname	Optimizer
Description	RedPort Optimizer Shares
Workgroup	RedPort
Listen interfaces	☑ LAN - 192.168.10.1 ☑ WAN - 192.168.0.21 □ 192.168.90.1 □ 192.168.11.1 □ 10.1.5.1 Bind shares to the following interfaces

Shared Directories

Name	Path	Allowed users	Read-only	Allow guests
Share name	Relative directory path	A comma separated list		

This section contains no values yet

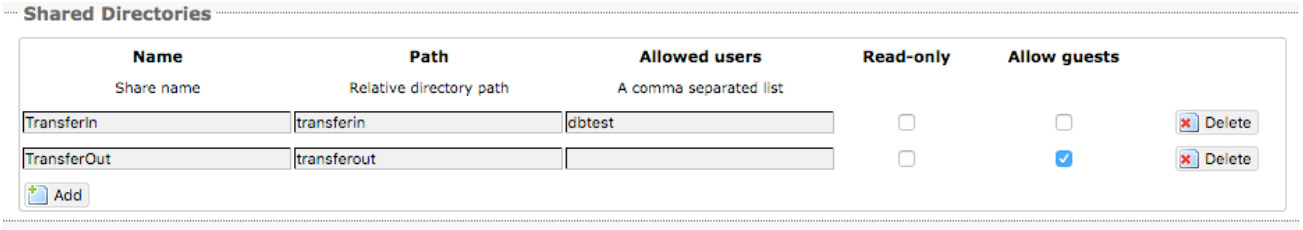
Add

Users

Username	Password	
		Delete

Add

Select <Add> to create a new Shared Directory:



Shared Directories

Name	Path	Allowed users	Read-only	Allow guests	
Share name	Relative directory path	A comma separated list			
TransferIn	transferin	dbtest	□	□	Delete
TransferOut	transferout		□	☑	Delete

Name: This is the Share Name that is visible on the network. It is the 'volume' name that you will use when connecting to the shared directory.

Path: This is the name of the Folder that appears on the Optimizer that will be used to store files.

Allowed users: You can limit the users that have access to the files in the Path Folder by assigning usernames and passwords to selected individuals (see Add Users below). Enter the usernames here, separated by a comma if more than one user will have access to the files.

Read-only: Use this checkbox to protect the files in the Path Folder from being changed.

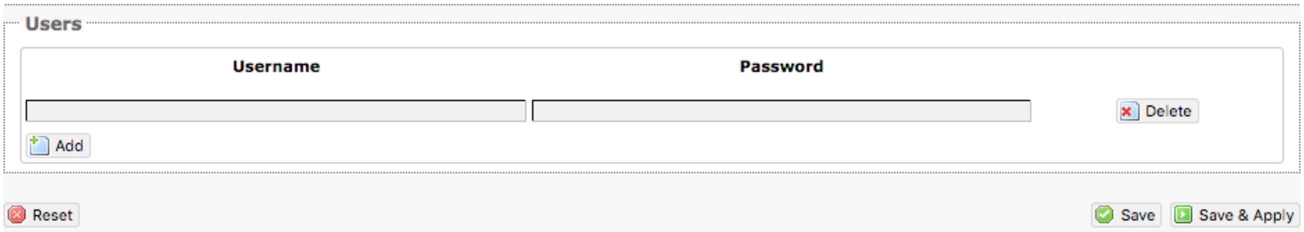
Allow guests: Use this checkbox to make the files available to anyone with network access. With this box checked, users will not be prompted to enter a username and password when accessing the Path Folder.

Delete: Use this to delete the Shared Directory.

Select <Save & Apply>.

5.8.2 Add Users

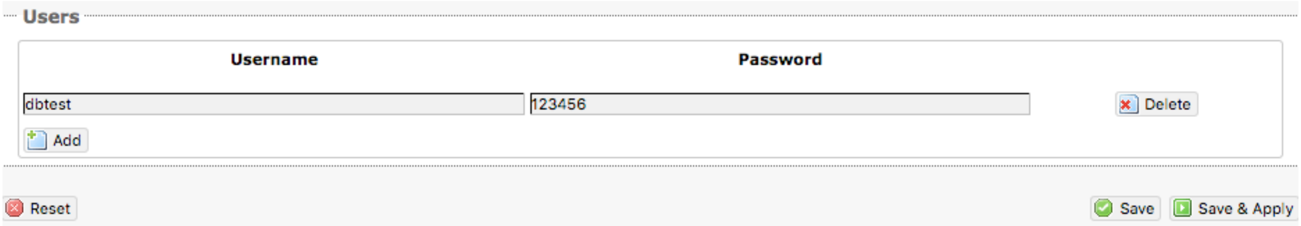
If you want to password protect access to the Shared Directories, you can assign usernames and passwords to each directory.



Users

Username	Password	
		Delete

Select <Add> to add a new username and password.



Users

Username	Password	
dbtest	123456	☒ Delete

Select <Save & Apply>.

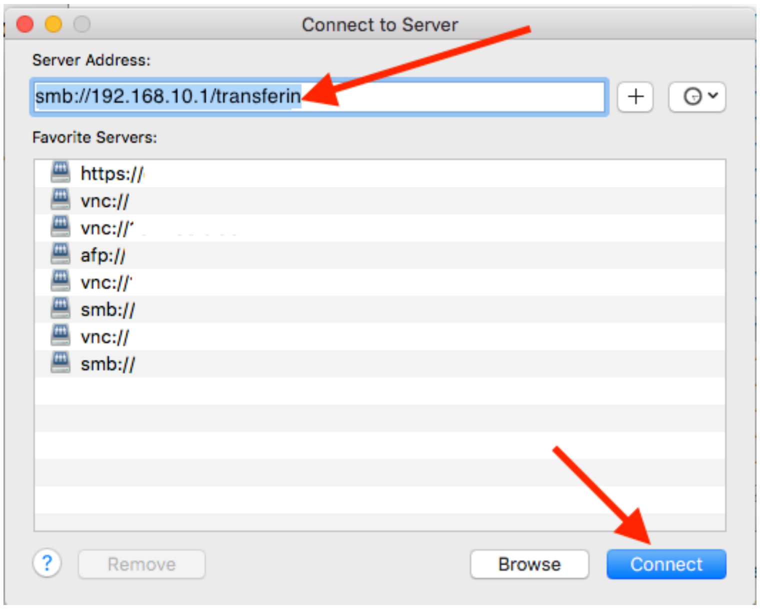
5.8.3 How to Access the Shared Directory and Path Folders:

5.8.3.1 From a Mac PC

Go to Finder > Go > Connect to Server

Enter the Server Address as the LAN address for the Optimizer / plus the Path Folder.

Select <Connect>

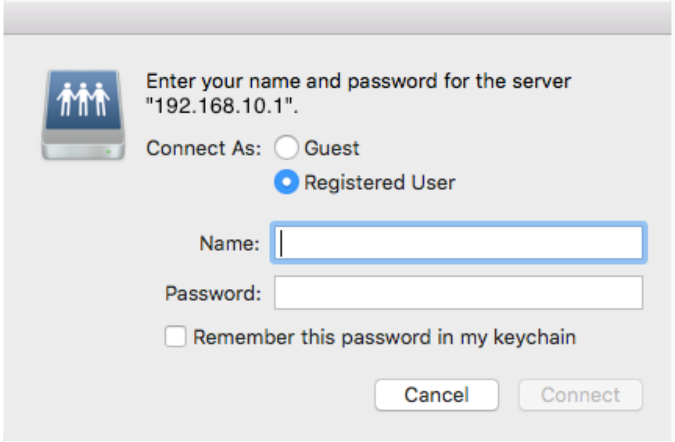


Connect to Server

Server Address: smb://192.168.10.1/transferin

Favorite Servers:

- https://
- vnc://
- vnc://
- afp://
- vnc://
- smb://
- vnc://
- smb://



Enter your name and password for the server "192.168.10.1".

Connect As: ○ Guest ● Registered User

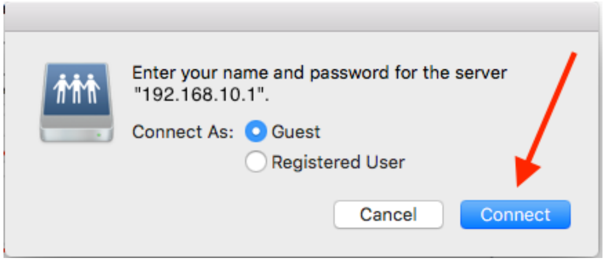
Name:

Password:

□ Remember this password in my keychain

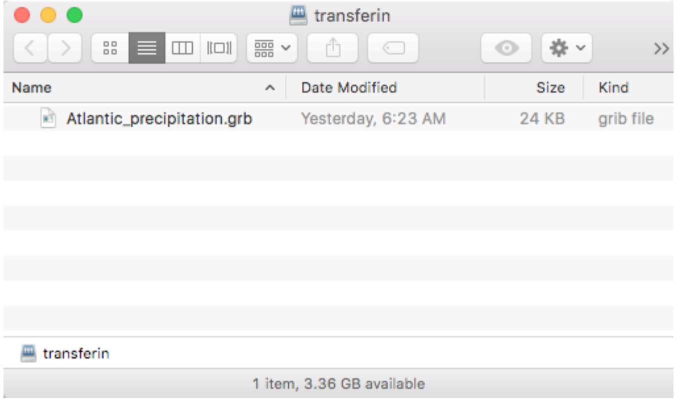
If the Shared Directory is restricted (i.e. does not Allow Guests) you must enter a username and password to access the files.

If the Shared Directory is not restricted (i.e. Allow Guests is checked in Network Shares) you can connect as a Guest without entering a username and password.



Enter your name and password for the server "192.168.10.1".

Connect As: ● Guest ○ Registered User



transferin

Name	Date Modified	Size	Kind
Atlantic_precipitation.grb	Yesterday, 6:23 AM	24 KB	grib file

transferin

1 item, 3.36 GB available

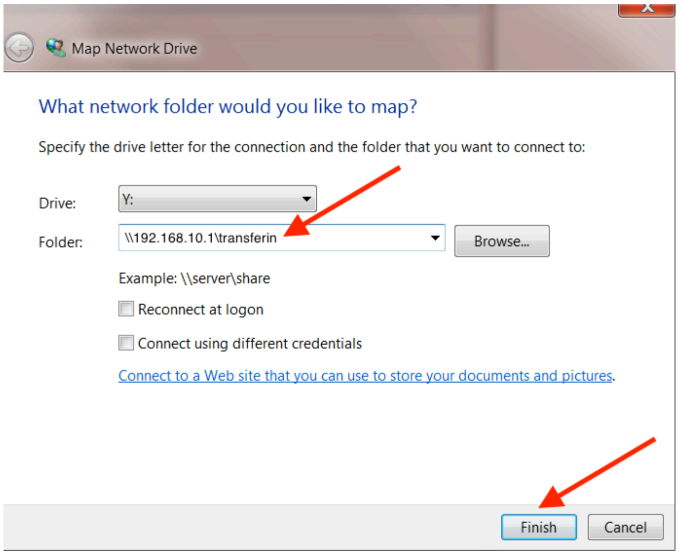
A Finder window opens to the selected Folder for access to the transferred file(s).

5.8.3.2 From a Windows PC

Map a Network drive to the appropriate location.

Go to Start Menu > Computer > Map Network Drive

In the Folder box, following the Example, enter \\the LAN address for the Optimizer\the Path Folder.



Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: Y:

Folder: \\192.168.10.1\transferin

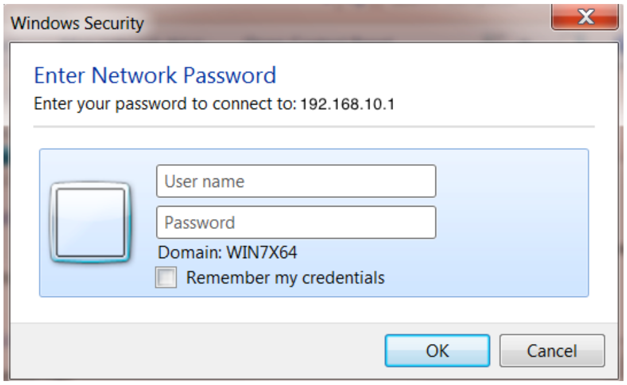
Example: \\server\share

□ Reconnect at logon

□ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

Select <Finish>.



Windows Security

Enter Network Password

Enter your password to connect to: 192.168.10.1

User name

Password

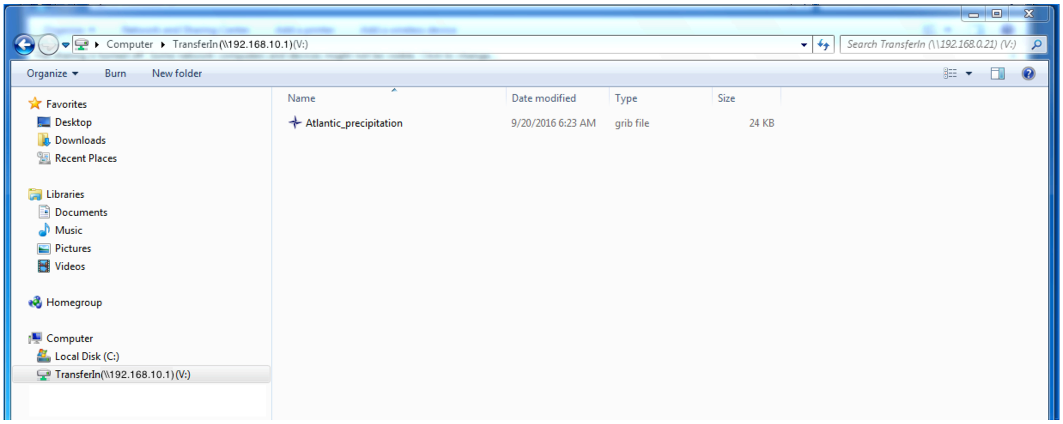
Domain: WIN7X64

□ Remember my credentials

If the Shared Directory is restricted (i.e. does not Allow Guests) you must enter a username and password to access the files.

If the Shared Directory is not restricted (i.e. Allow Guests is checked in Network Shares) you can connect as a Guest without entering a username and password.

An Explorer window opens to the selected Folder for access to the transferred file(s).



Computer ▸ TransferIn(\\192.168.10.1)(V:)

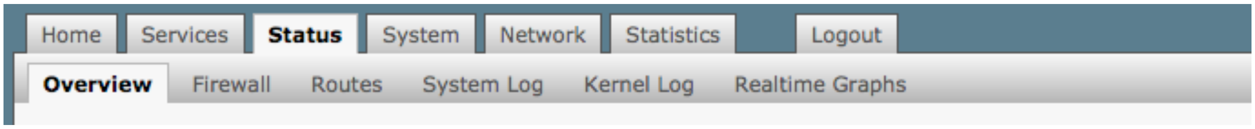
Search TransferIn (\\192.168.0.21) (V:)

Name	Date modified	Type	Size
Atlantic_precipitation	9/20/2016 6:23 AM	grib file	24 KB

6.0 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.

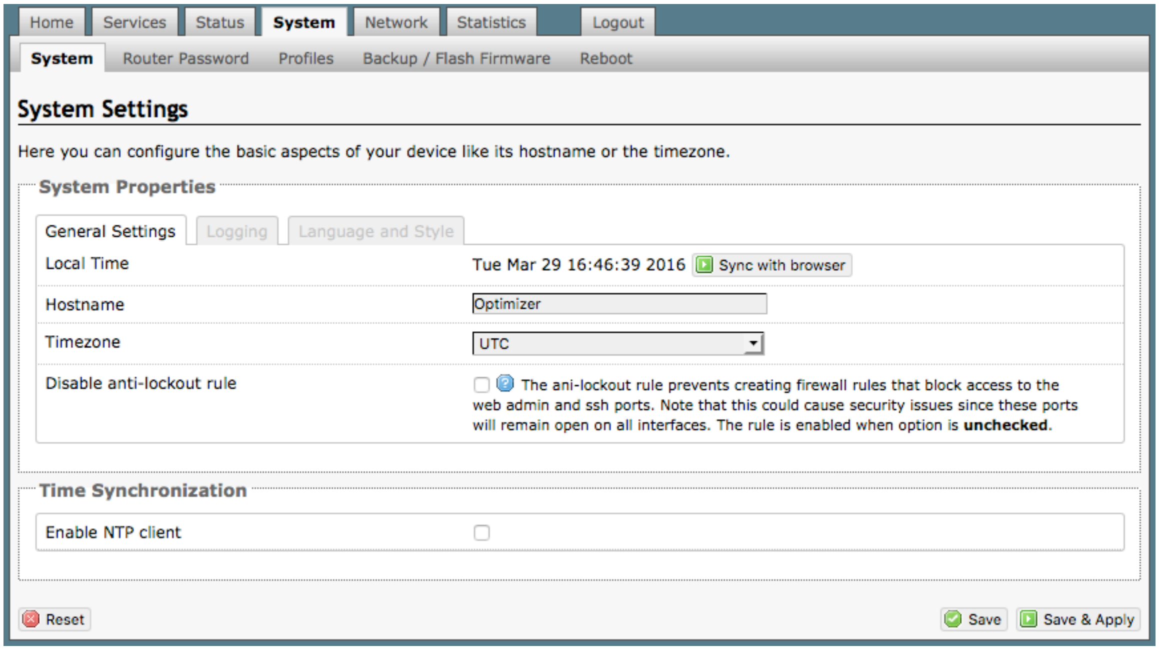
7.0 System

Requires 'superadmin' login.

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

7.1 System Settings

Use this section to configure the basic aspects of your device (i.e hostname and/or timezone).



System Settings

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

Local Time	Tue Mar 29 16:46:39 2016
Hostname	Optimizer
Timezone	UTC
Disable anti-lockout rule	□ The ani-lockout rule prevents creating firewall rules that block access to the web admin and ssh ports. Note that this could cause security issues since these ports will remain open on all interfaces. The rule is enabled when option is **unchecked**.

Time Synchronization

Enable NTP client	□

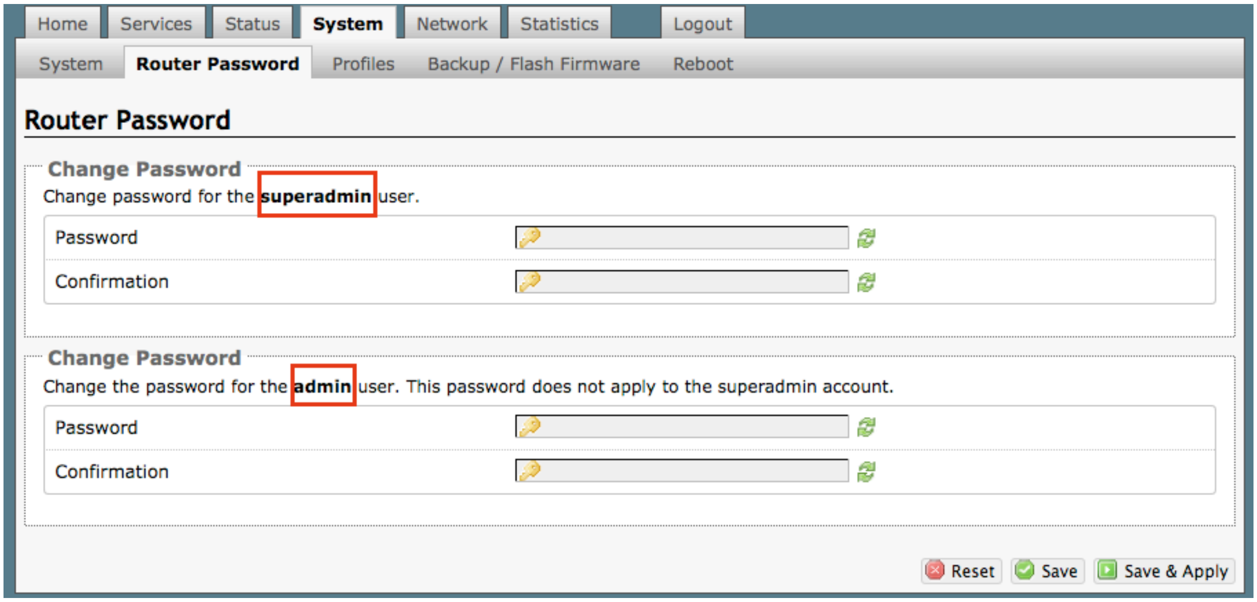
Disable anti-lockout rule: The anti-lock rule prevents you from creating a firewall rule that will lock you out of the router. The rule is Enabled when the box is Unchecked. ***Best Practice is to complete the router configuration, test it thoroughly to make sure everything works as intended, then disable the anti-lock role.***

For example, if you want to be able to login to the router from your office, once the router has been installed on a vessel; if you have WAN blocked and the Anti-Lock Rule is enabled, you will not be able to login. First you want to create a firewall rule to allow the office IP into the router, then "Disable anti-lock rule" by checking the checkbox and now you can Block WAN in the Firewall Rules, if desired.

CAUTION: If you lock yourself out of the router, you must perform a factory reset. This will eliminate your custom configuration requiring you to start a new configuration.

7.2 Router Password

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 for the "admin" login only, from the Home Page. Anyone using the 'superadmin" login can change the password for both "admin" and "superadmin" login.



Router Password

Change Password

Change password for the **superadmin** user.

Password

Confirmation

Change Password

Change the password for the **admin** user. This password does not apply to the superadmin account.

Password

Confirmation

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

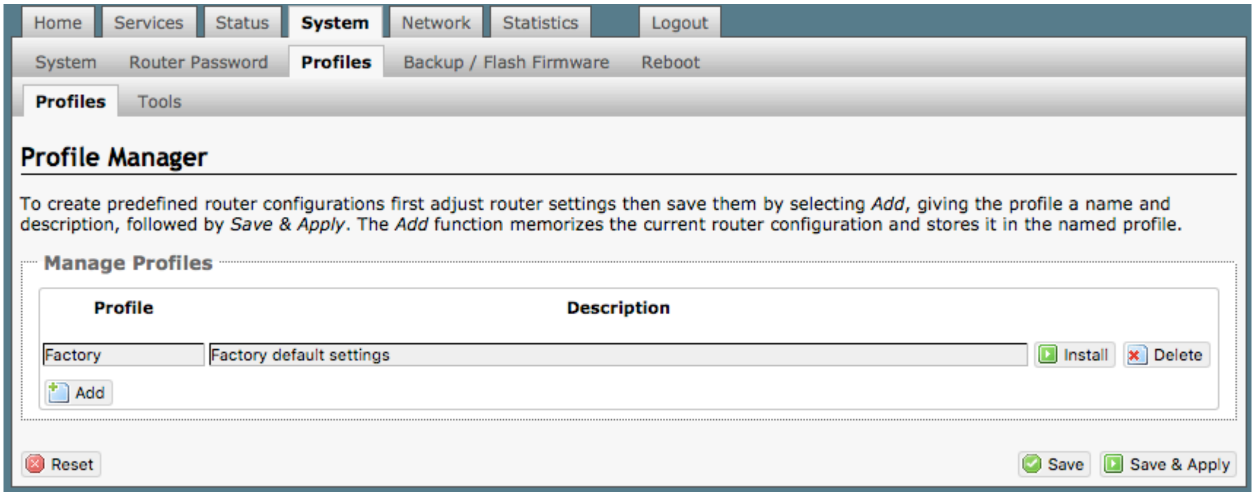
Step 1. Enter the new password in the password text box.
Step 2. Enter the same password again in the Confirmation text box.
Step 3. Click <Save & Apply>

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

Requires 'superadmin' login.

Profiles is designed for users of multiple satellite devices and integrators of custom installations.



Profile Manager

To create predefined router configurations first adjust router settings then save them by selecting *Add*, giving the profile a name and description, followed by *Save & Apply*. The *Add* function memorizes the current router configuration and stores it in the named profile.

Manage Profiles

Profile	Description		
Factory	Factory default settings	Install	Delete

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 Premier router.

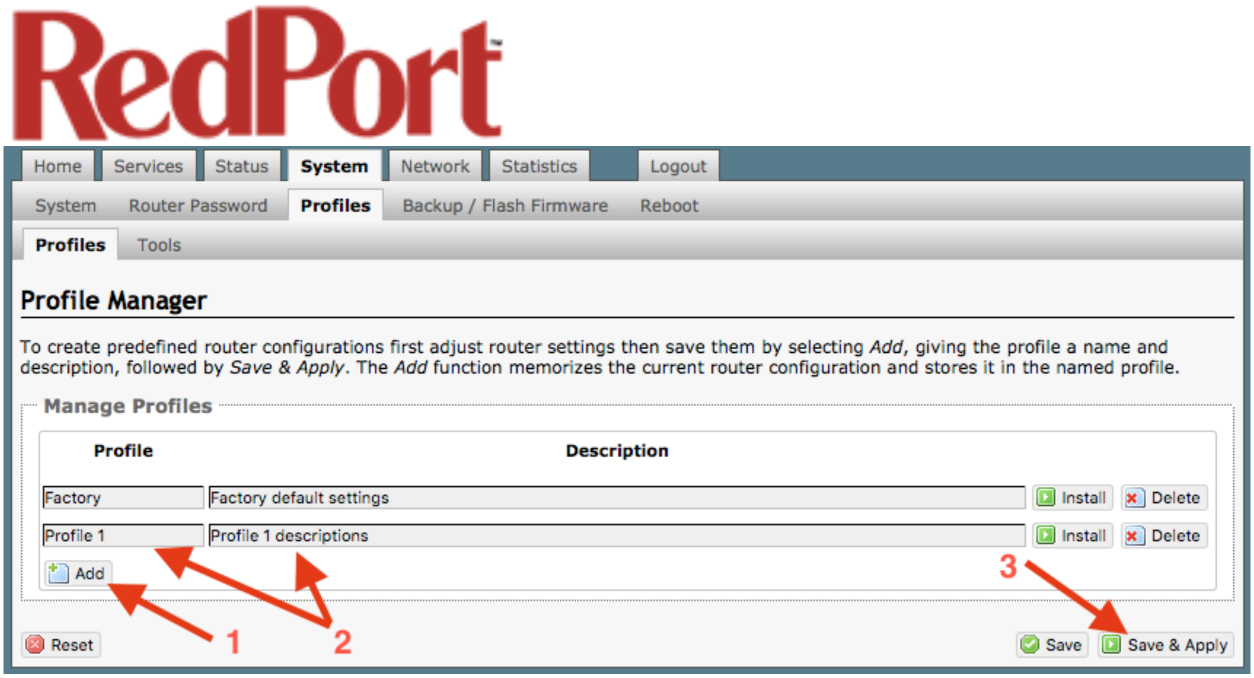
7.2.1 Add a Profile

Before adding a Profile, complete the router configuration.

Then access the Profile Manager.

To create and use the new Profile:

1. Select <Add>



Profile Manager

To create predefined router configurations first adjust router settings then save them by selecting *Add*, giving the profile a name and description, followed by *Save & Apply*. The *Add* function memorizes the current router configuration and stores it in the named profile.

Manage Profiles

Profile	Description
Factory	Factory default settings
Profile 1	Profile 1 descriptions

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

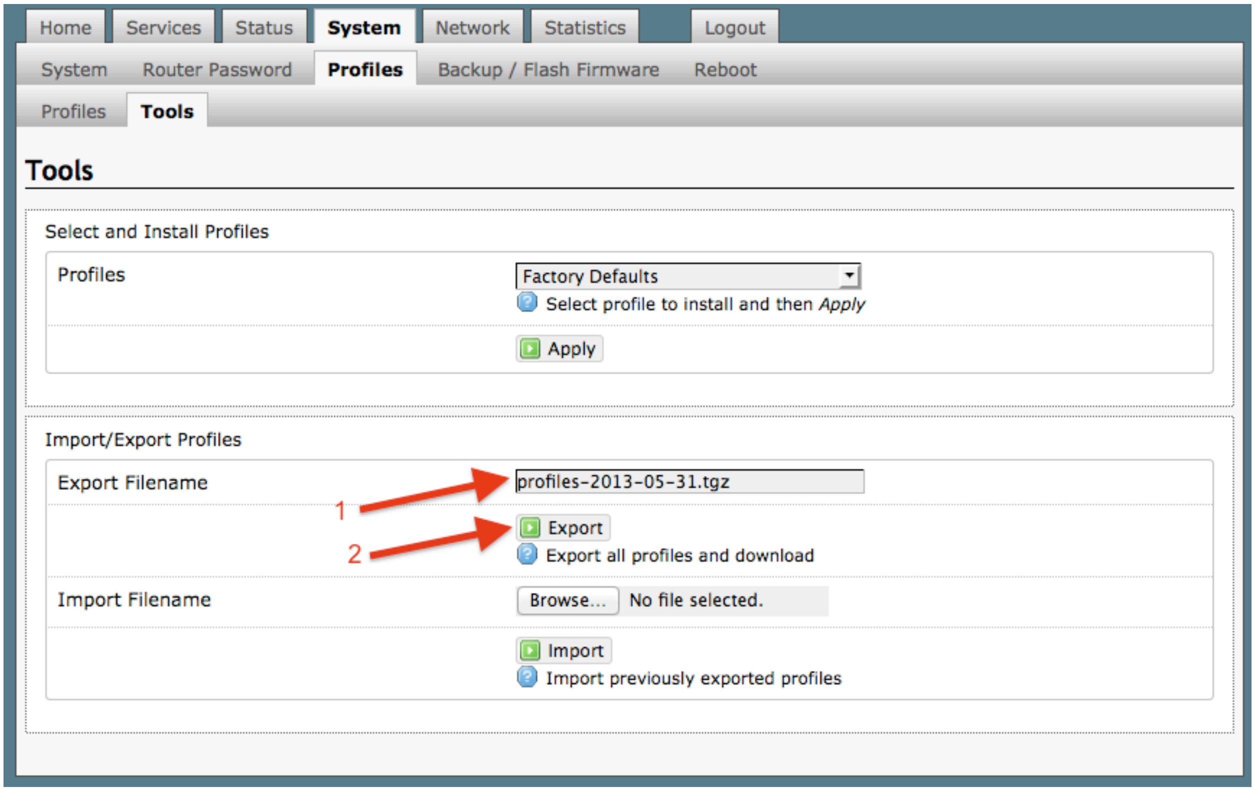
The Add function memorized the current router configuration and stores it in the named profile.

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 Premier router in System > Profiles > Tools.



Tools

Select and Install Profiles

Profiles: Factory Defaults
Select profile to install and then *Apply*

Import/Export Profiles

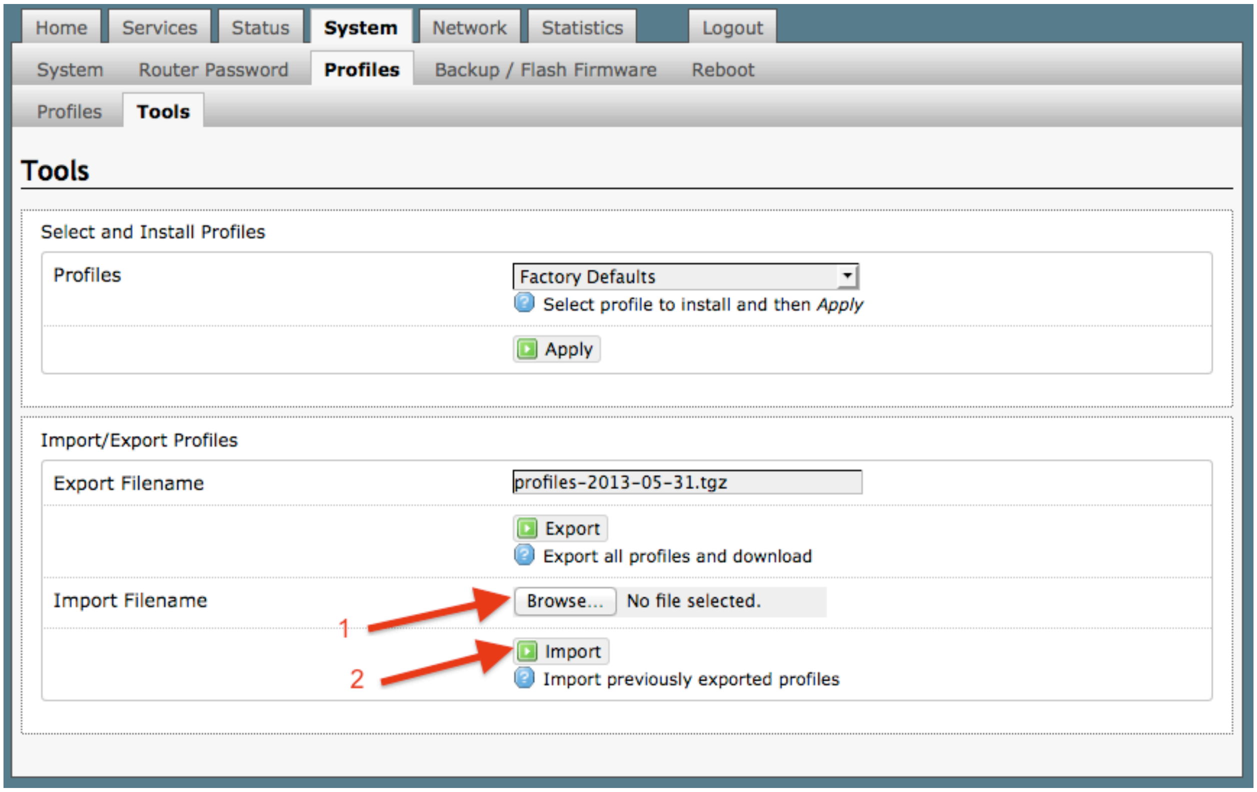
Export Filename: profiles-2013-05-31.tgz
Export all profiles and download

Import Filename: No file selected.
Import previously exported profiles

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 Premier router in System > Profiles > Tools.



Tools

Select and Install Profiles

Profiles: Factory Defaults

Select profile to install and then *Apply*

Import/Export Profiles

Export Filename: profiles-2013-05-31.tgz

Export all profiles and download

Import Filename: Browse... No file selected.

Import previously exported profiles

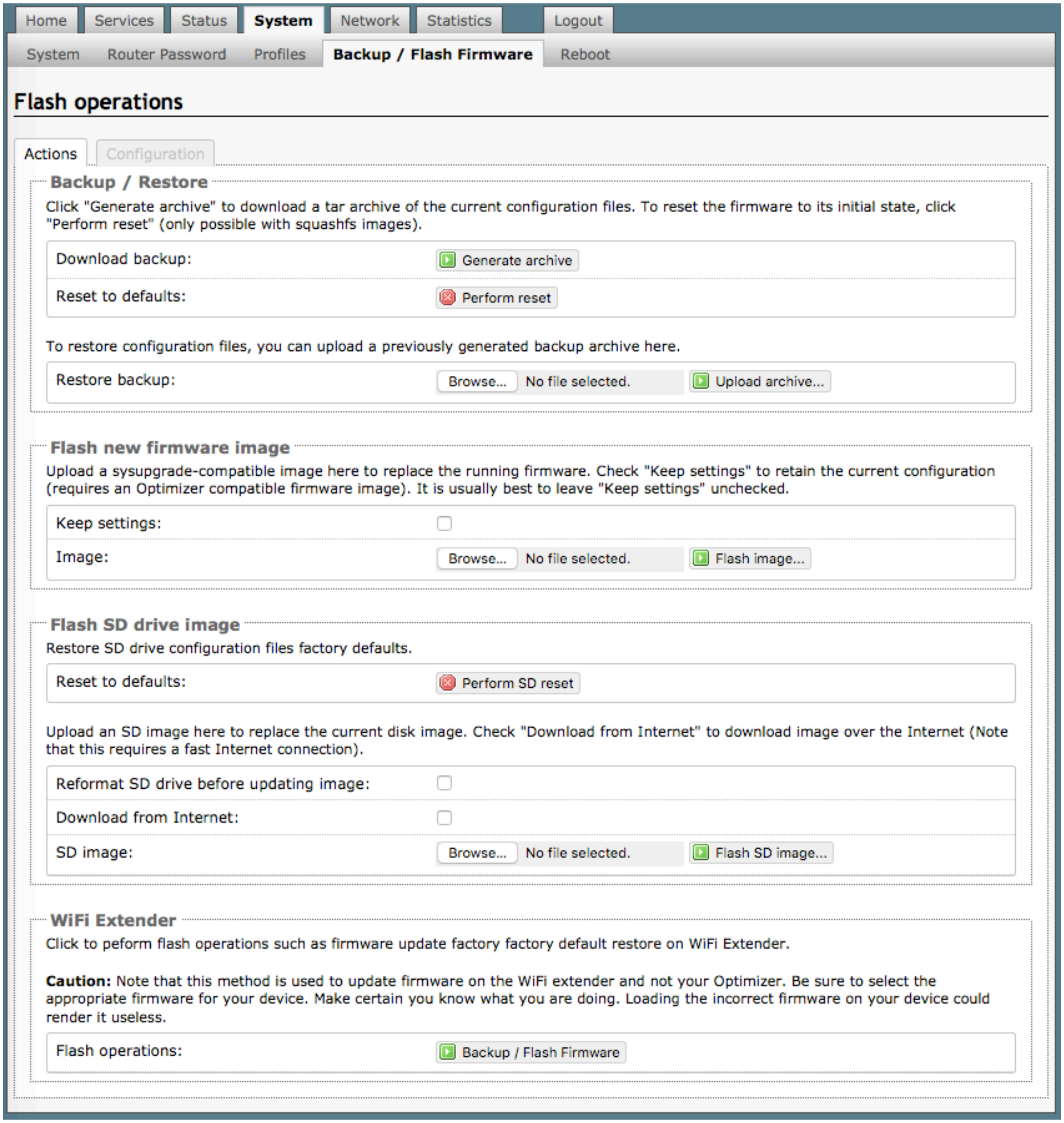
1. Select <Browse> to locate the saved profiles .tgz file.

2. Select <Import>

7.3 Backup/Flash Firmware

Requires 'superadmin' login.

Use this screen to generate backups of current configuration files, resets, restores, and firmware upgrades.



Flash operations

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup: Generate archive

Reset to defaults: Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: Browse... No file selected. Upload archive...

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an Optimizer compatible firmware image). It is usually best to leave "Keep settings" unchecked.

Keep settings: ☐

Image: Browse... No file selected. Flash image...

Flash SD drive image

Restore SD drive configuration files factory defaults.

Reset to defaults: Perform SD reset

Upload an SD image here to replace the current disk image. Check "Download from Internet" to download image over the Internet (Note that this requires a fast Internet connection).

Reformat SD drive before updating image: ☐

Download from Internet: ☐

SD image: Browse... No file selected. Flash SD image...

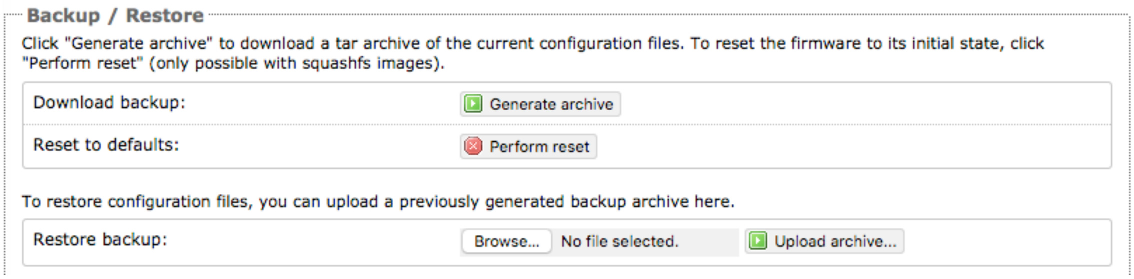
WiFi Extender

Click to peform flash operations such as firmware update factory factory default restore on WiFi Extender.

Caution: Note that this method is used to update firmware on the WiFi extender and not your Optimizer. Be sure to select the appropriate firmware for your device. Make certain you know what you are doing. Loading the incorrect firmware on your device could render it useless.

Flash operations: Backup / Flash Firmware

7.3.1 Backup/Restore



Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:	Generate archive
Reset to defaults:	Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup:	Browse...	No file selected.	Upload archive...

Download backup: Create and save a Backup archive of the current configuration.

Restore backup: Restore the router to a previously saved configuration.

Reset to defaults: Reset the router to the default configuration.

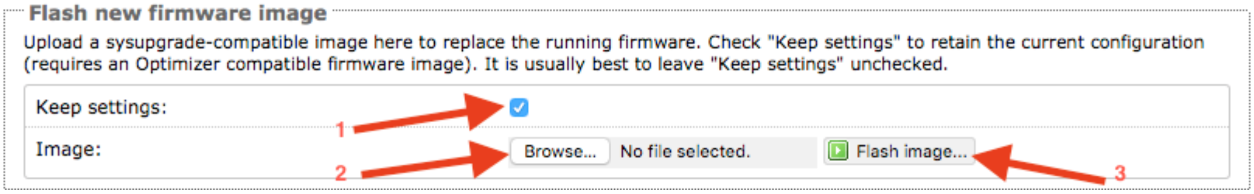
To apply the same configuration among several Optimizer Premier routers (for example in a fleet situation) create and save a Profile of the configuration that can be applied to other Optimizer Premier routers*. See Chapter 7.2.*

7.3.2 Flash New Firmware Image

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.



Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an Optimizer compatible firmware image). It is usually best to leave "Keep settings" unchecked.

Keep settings: ☑

Image: Browse... No file selected. Flash image...

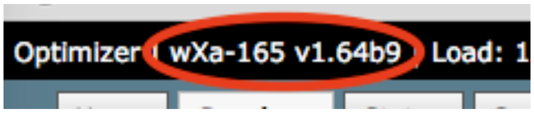
1. **Keep Settings**: check this box to maintain current settings if you have made changes to the congifuration. Failure to check this box will revert the Optimizer back to the default settings.

2. **<Browse>** to where you saved the .bin file and select that file. ***CAUTION: Loading incorrect firmware on your device could render it useless. Be sure to select the appropriate firmware for your device.***

3. **<Flash Image>**

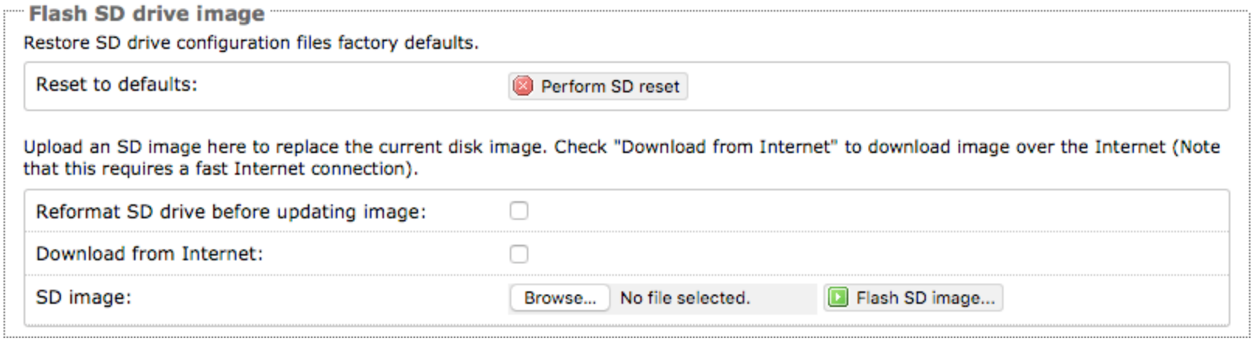
4. Wait for the lights on the front of the Optimizer to begin flashing. When the flashing lights stop, the firmware update is complete. This typically takes several minutes.

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



Optimizer wXa-165 v1.64b9 Load: 1

7.3.3 Flash SD Drive Image



Flash SD drive image

Restore SD drive configuration files factory defaults.

Reset to defaults:	Perform SD reset

Upload an SD image here to replace the current disk image. Check "Download from Internet" to download image over the Internet (Note that this requires a fast Internet connection).

Reformat SD drive before updating image:	□
Download from Internet:	□
SD image:	Browse... No file selected. Flash SD image...

Reset to defaults: Restores the SD drive configuration to its default state.

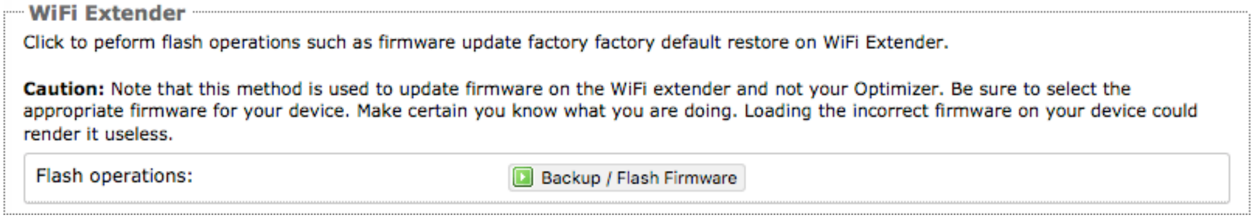
Reformat SD drive before updating image: If the SD drive goes bad, use this to reformat the drive before updating the image.

Download from Internet: Use this only if you have a fast Internet connection to obtain the file. As an alternative, you can obtain the disk image file from our website and save it for use: http://www.redportglobal.com/support/technical-downloads/

SD image: Select <Browse> if you have the file saved to your computer. Select <Flash SD Image> to start the flash process.

7.3.4 WiFi Extender

Requires 'superadmin' login.



WiFi Extender

Click to peform flash operations such as firmware update factory factory default restore on WiFi Extender.

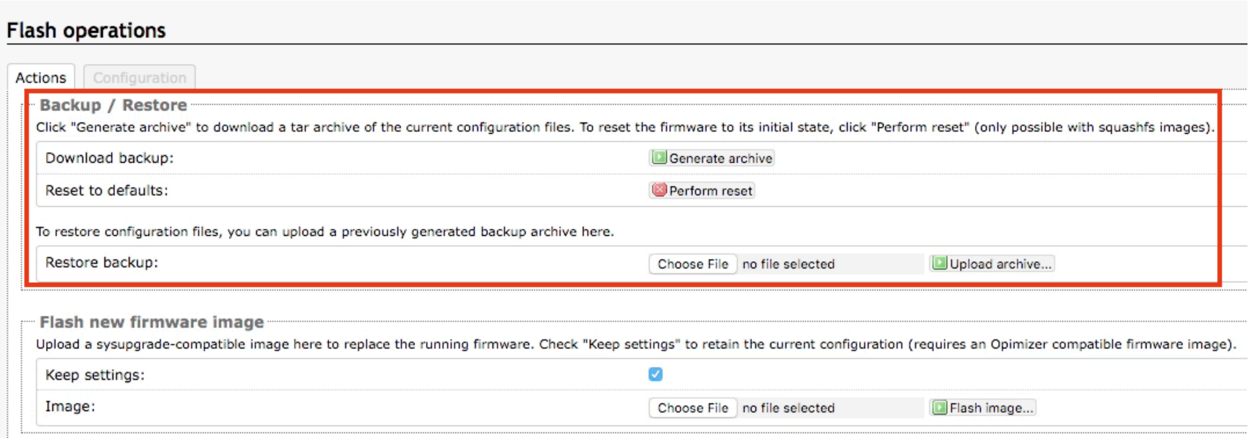
Caution: Note that this method is used to update firmware on the WiFi extender and not your Optimizer. Be sure to select the appropriate firmware for your device. Make certain you know what you are doing. Loading the incorrect firmware on your device could render it useless.

Flash operations:	Backup / Flash Firmware

Use this to backup the configuration settings and/or update the firmware for the RedPort WiFi Extender ONLY!

Select <Backup/Flash Firmware> to open the Flash operations screen.

7.3.4.1 Backup / Restore



Flash operations

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup: Generate archive

Reset to defaults: Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: Choose File no file selected Upload archive...

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an Opimizer compatible firmware image).

Keep settings: ☑

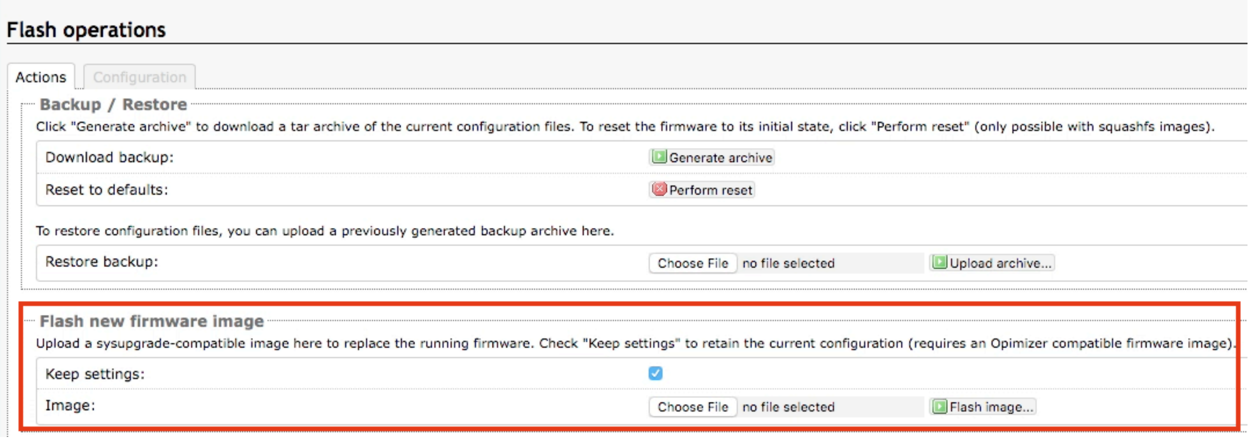
Image: Choose File no file selected Flash image...

Download Backup: select <Generate archive> to create a backup of the current configuration of the WiFi Extender. A backup file (.tar) will be generated and saved to your computer.

Reset to defaults: select <Perform reset> to reset the WiFi Extender to the factory defaults.

Restore backup: select <Choose File> to browse and select the .tar backup file. Select <Upload archive> to restore.

7.3.4.2 Flash New Firmware Image



Flash operations

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:	Generate archive
Reset to defaults:	Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup:	Choose File no file selected Upload archive...

Flash new firmware image

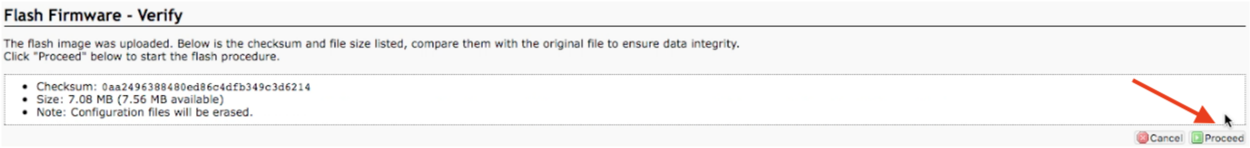
Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an Opimizer compatible firmware image).

Keep settings:	☑
Image:	Choose File no file selected Flash image...

Keep Settings: select this only if you want to retain the current configuration.

Image: you must have the new firmware image saved to your computer. You can obtain the latest WiFi Extender Firmware image from our website: www.redportglobal.com/support/technical-downloads/

Select <Choose File> to browse and select the .bin firmware image file. Select <Flash Image> to start the flash operation.



Flash Firmware - Verify

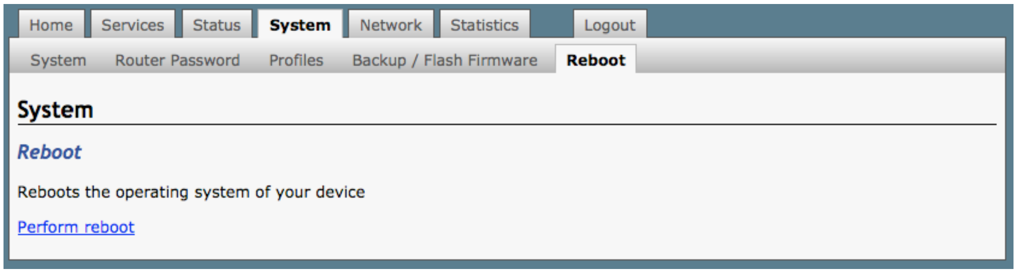
The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.
Click "Proceed" below to start the flash procedure.

- Checksum: 0aa2496388480ed86c4dfb349c3d6214
- Size: 7.08 MB (7.56 MB available)
- Note: Configuration files will be erased.

Select <Proceed> to complete the process.

7.4 Reboot

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



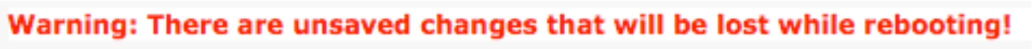
System

Reboot

Reboots the operating system of your device

Perform reboot

If you have made changes to the configuration without selecting <Save & Apply> you will receive a Warning message:



Warning: There are unsaved changes that will be lost while rebooting!

8.0 Network

Requires 'superadmin' login.

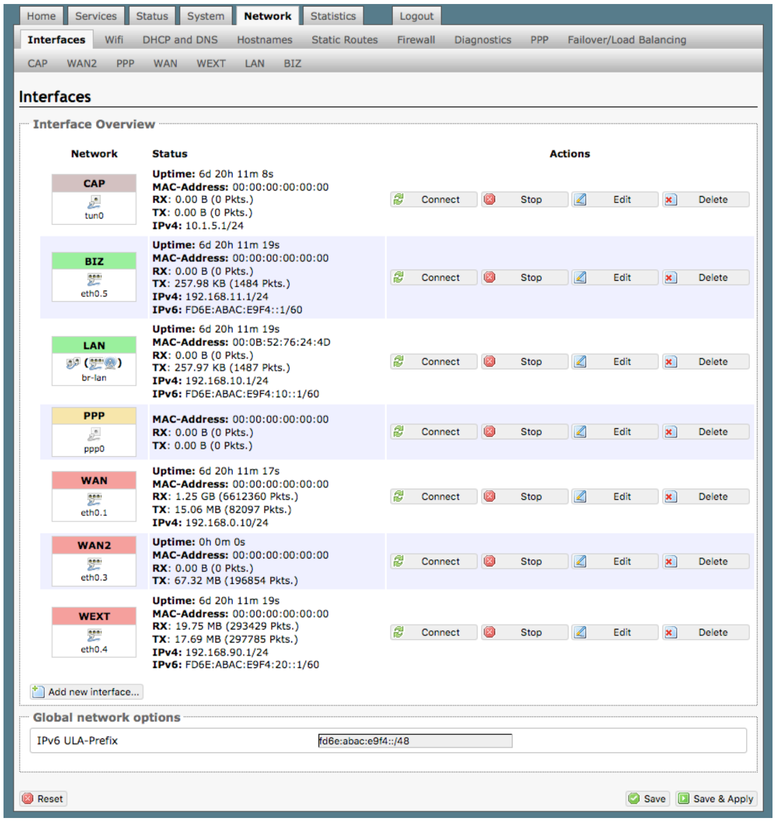
Use this section to configure network interfaces, run diagnostics, or modify the firewall.

CAUTION: This gives you complete control over the router behavior.

BEST PRACTICE: Modifications to the default configuration is best left to those with a full understanding of router/network behavior, firewall rules, etc. Creating conflicts in the configuration may render the router useless.

8.1 Interfaces Overview

This screen is an at-a-glance view of the current status of each network interface and provides easy access to edit the interface. Each interface can have its own firewall rules *(see Chapter 8.8).*



Interfaces

Interface Overview

Network	Status	Actions
CAP tun0	**Uptime:** 6d 20h 11m 8s **MAC-Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.) **IPv4:** 10.1.5.1/24	Connect Stop Edit Delete
BIZ eth0.5	**Uptime:** 6d 20h 11m 19s **MAC-Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 257.98 KB (1484 Pkts.) **IPv4:** 192.168.11.1/24 **IPv6:** FD6E:ABAC:E9F4::1/60	Connect Stop Edit Delete
LAN br-lan	**Uptime:** 6d 20h 11m 19s **MAC-Address:** 00:0B:52:76:24:4D **RX**: 0.00 B (0 Pkts.) **TX**: 257.97 KB (1487 Pkts.) **IPv4:** 192.168.10.1/24 **IPv6:** FD6E:ABAC:E9F4:10::1/60	Connect Stop Edit Delete
PPP ppp0	**MAC-Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)	Connect Stop Edit Delete
WAN eth0.1	**Uptime:** 6d 20h 11m 17s **MAC-Address:** 00:00:00:00:00:00 **RX**: 1.25 GB (6612360 Pkts.) **TX**: 15.06 MB (82097 Pkts.) **IPv4:** 192.168.0.10/24	Connect Stop Edit Delete
WAN2 eth0.3	**Uptime:** 0h 0m 0s **MAC-Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 67.32 MB (196854 Pkts.)	Connect Stop Edit Delete
WEXT eth0.4	**Uptime:** 6d 20h 11m 19s **MAC-Address:** 00:00:00:00:00:00 **RX**: 19.75 MB (293429 Pkts.) **TX**: 17.69 MB (297785 Pkts.) **IPv4:** 192.168.90.1/24 **IPv6:** FD6E:ABAC:E9F4:20::1/60	Connect Stop Edit Delete

Add new interface...

Global network options

IPv6 ULA-Prefix: fd6e:abac:e9f4::/48

CAP: this is reserved for the Captive Portal. If the Captive Portal is enabled, all traffic that comes through the Captive Portal will be subject to this interface configuration. This allows you to create rules that apply to the Captive Portal only.

BIZ: this is the business port. By default, it is wide open; any computer directly connected to the BIZ port on the router has full access to the Internet without restrictions.

> *BEST PRACTICE: Restrict access to this port, protect the router under lock and key OR disable the BIZ interface.*

LAN: this is reserved for the local area network. All traffic not routing through the Captive Portal will be subject to this interface configuration.

PPP: this is reserved for USB connected satellite phones and GSM or LTE modems.

WAN: this is typically used for the primary satellite system.

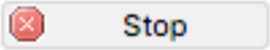
WAN2: this is typically used for the secondary satellite system.

WEXT: this is reserved for the RedPort WiFi Extender.

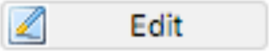
> *If you have a different wifi extender you may be able to use it by plugging it into a wan port (Sat1 or Sat2) on the Optimizer. It will not work if plugged into the WiFi port on the Optimizer. However, when plugged into a wan port the Captive Portal will not work through that wifi interface. Best Practice would be to disable the wifi extender (unplug) when outside the wifi broadcast area.*

8.1.1 Interface Actions

Enable an interface.



Disable an interface.

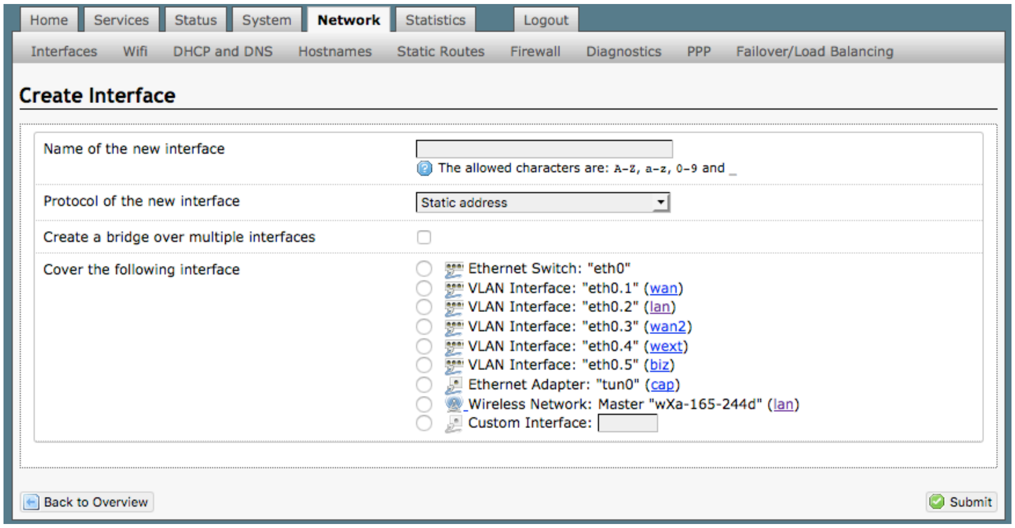


Modify the configuration of the interface.

Remove the interface. ***CAUTION: This action cannot be Undone!***

8.1.2 Add a New Interface

To add a new interface select the <Add new interface> button on the Interface Overview page.



Create Interface

Name of the new interface	The allowed characters are: A-Z, a-z, 0-9 and _
Protocol of the new interface	Static address
Create a bridge over multiple interfaces	□
Cover the following interface	○ Ethernet Switch: "eth0" ○ VLAN Interface: "eth0.1" (wan) ○ VLAN Interface: "eth0.2" (lan) ○ VLAN Interface: "eth0.3" (wan2) ○ VLAN Interface: "eth0.4" (wext) ○ VLAN Interface: "eth0.5" (biz) ○ Ethernet Adapter: "tun0" (cap) ○ Wireless Network: Master "wXa-165-244d" (lan) ○ Custom Interface:

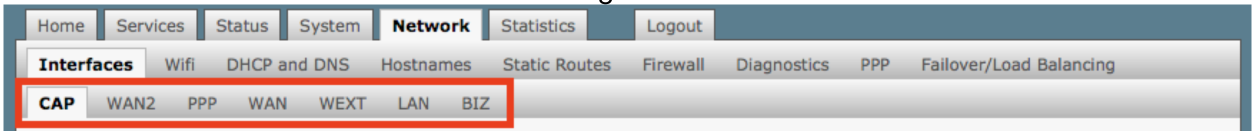
Complete the Create Interface screen and select <Submit> to apply the change. Once configured, the new interface will show on the Interface Overview screen and it will have its own Tab at the top of the Interface Overview page.

The name of the new interface must not match the name of a current interface, member, policy or rule.

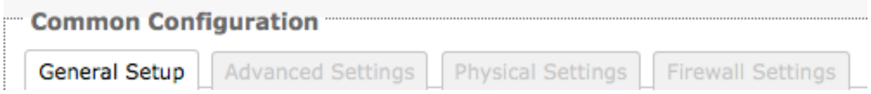
If adding a new WAN Interface, be sure to Edit the Interface to complete the configuration.

8.1.3 Select Interfaces Tabs

Use these tabs to select an interface for configuration and/or modification.



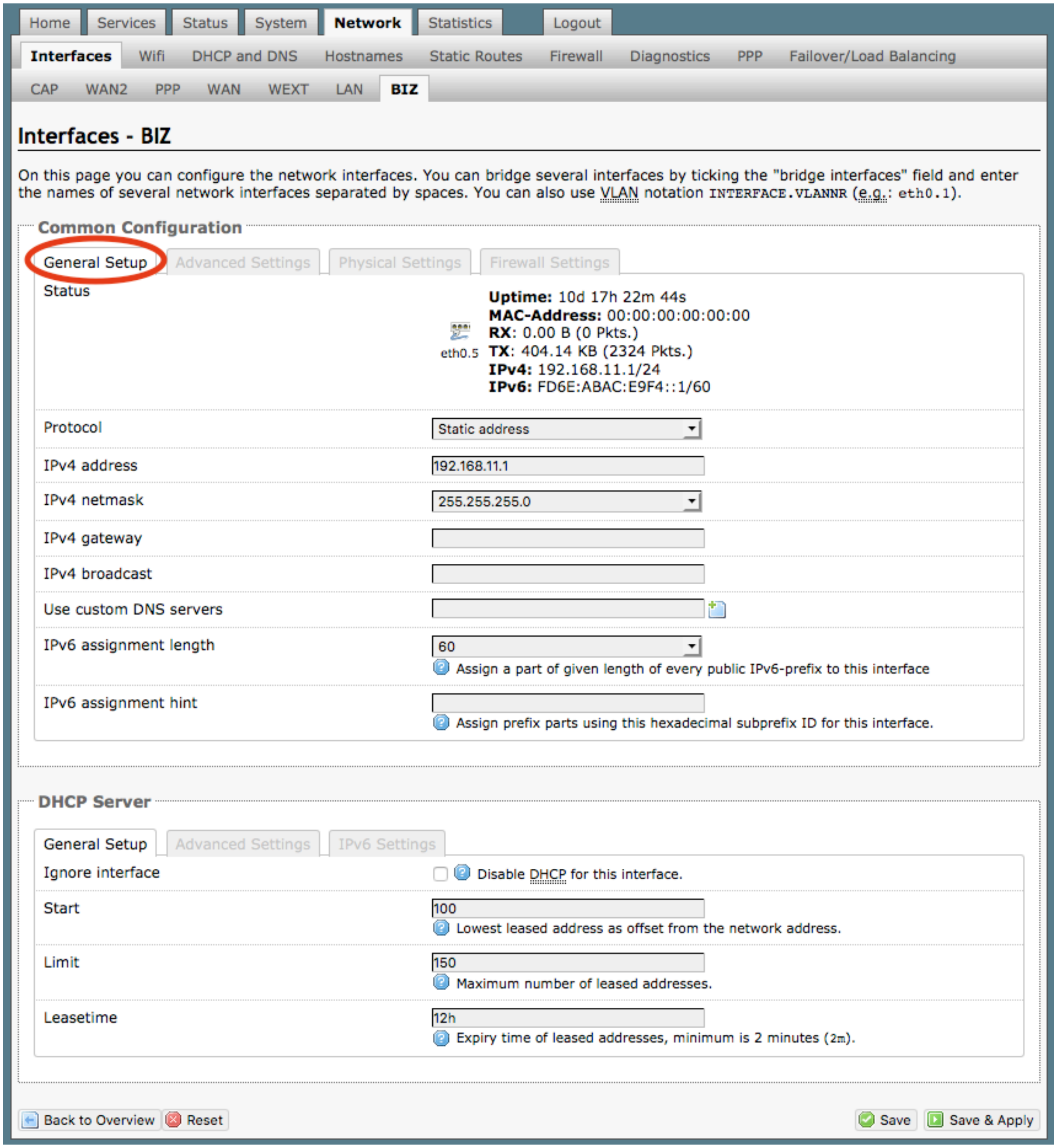
Use these pages to configure the network interfaces.



The information and selections available will depend upon the Protocol selection for that interface.

8.1.3.1 General Setup

Use General Setup to switch the protocol for the interface and configure the setup for that protocol including Static IP Addresses, DHCP Server Setup, etc.



Interfaces - BIZ

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

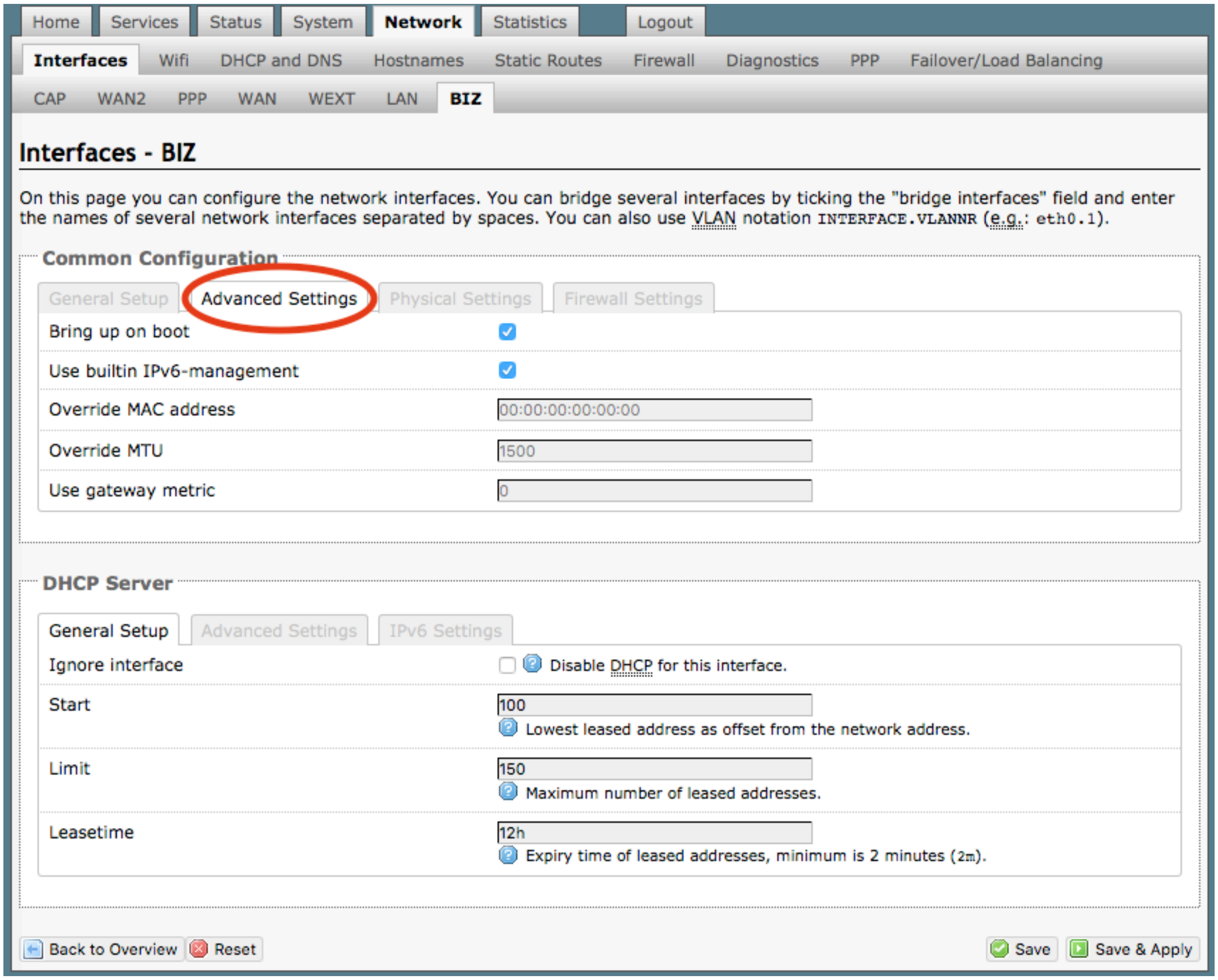
Status	eth0.5 **Uptime:** 10d 17h 22m 44s **MAC-Address:** 00:00:00:00:00:00 **RX:** 0.00 B (0 Pkts.) **TX:** 404.14 KB (2324 Pkts.) **IPv4:** 192.168.11.1/24 **IPv6:** FD6E:ABAC:E9F4::1/60
Protocol	Static address
IPv4 address	192.168.11.1
IPv4 netmask	255.255.255.0
IPv4 gateway	
IPv4 broadcast	
Use custom DNS servers	
IPv6 assignment length	60 Assign a part of given length of every public IPv6-prefix to this interface
IPv6 assignment hint	 Assign prefix parts using this hexadecimal subprefix ID for this interface.

DHCP Server

Ignore interface	□ Disable DHCP for this interface.
Start	100 Lowest leased address as offset from the network address.
Limit	150 Maximum number of leased addresses.
Leasetime	12h Expiry time of leased addresses, minimum is 2 minutes (`2m`).

8.1.3.2 Advanced Settings

Use Advanced Settings if you want to bring up the interface automatically on boot up of the router and to configure the DHCP Server Settings.



Interfaces - BIZ

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bring up on boot	☑
Use builtin IPv6-management	☑
Override MAC address	00:00:00:00:00:00
Override MTU	1500
Use gateway metric	0

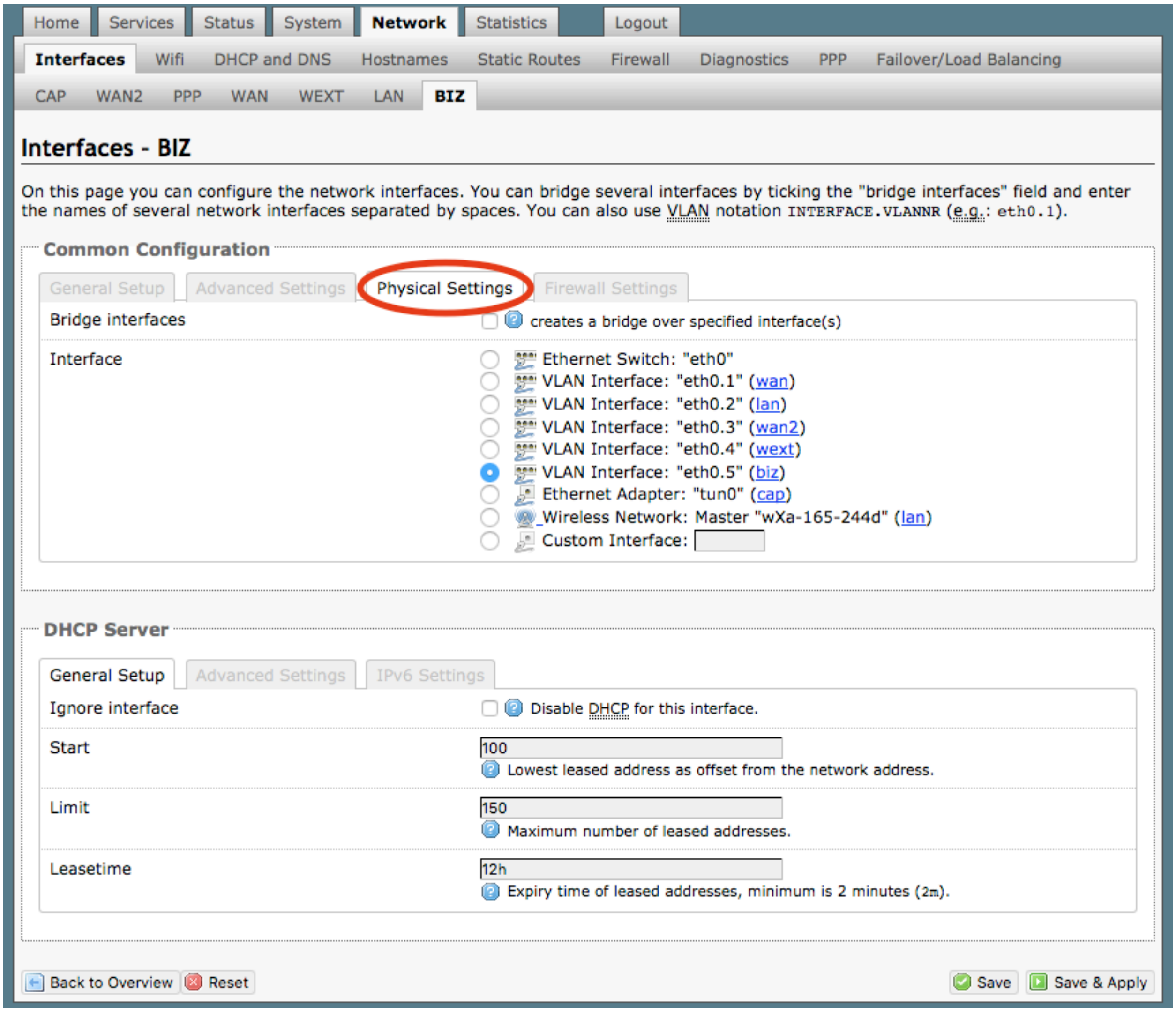
DHCP Server

Ignore interface	☐ Disable DHCP for this interface.
Start	100 Lowest leased address as offset from the network address.
Limit	150 Maximum number of leased addresses.
Leasetime	12h Expiry time of leased addresses, minimum is 2 minutes (`2m`).

Note: Each WAN interface must be assigned a unique number in the "Use gateway metric" field. This number is required for configuring Failover/Load Balancing.

8.1.3.3 Physical Settings

Use this page to bridge interfaces and configure the DHCP Server Settings.



Interfaces - BIZ

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Bridge interfaces: □ creates a bridge over specified interface(s)

Interface:

- ○ Ethernet Switch: "eth0"
- ○ VLAN Interface: "eth0.1" (wan)
- ○ VLAN Interface: "eth0.2" (lan)
- ○ VLAN Interface: "eth0.3" (wan2)
- ○ VLAN Interface: "eth0.4" (wext)
- ● VLAN Interface: "eth0.5" (biz)
- ○ Ethernet Adapter: "tun0" (cap)
- ○ Wireless Network: Master "wXa-165-244d" (lan)
- ○ Custom Interface:

DHCP Server

General Setup | Advanced Settings | IPv6 Settings

Ignore interface: □ Disable DHCP for this interface.

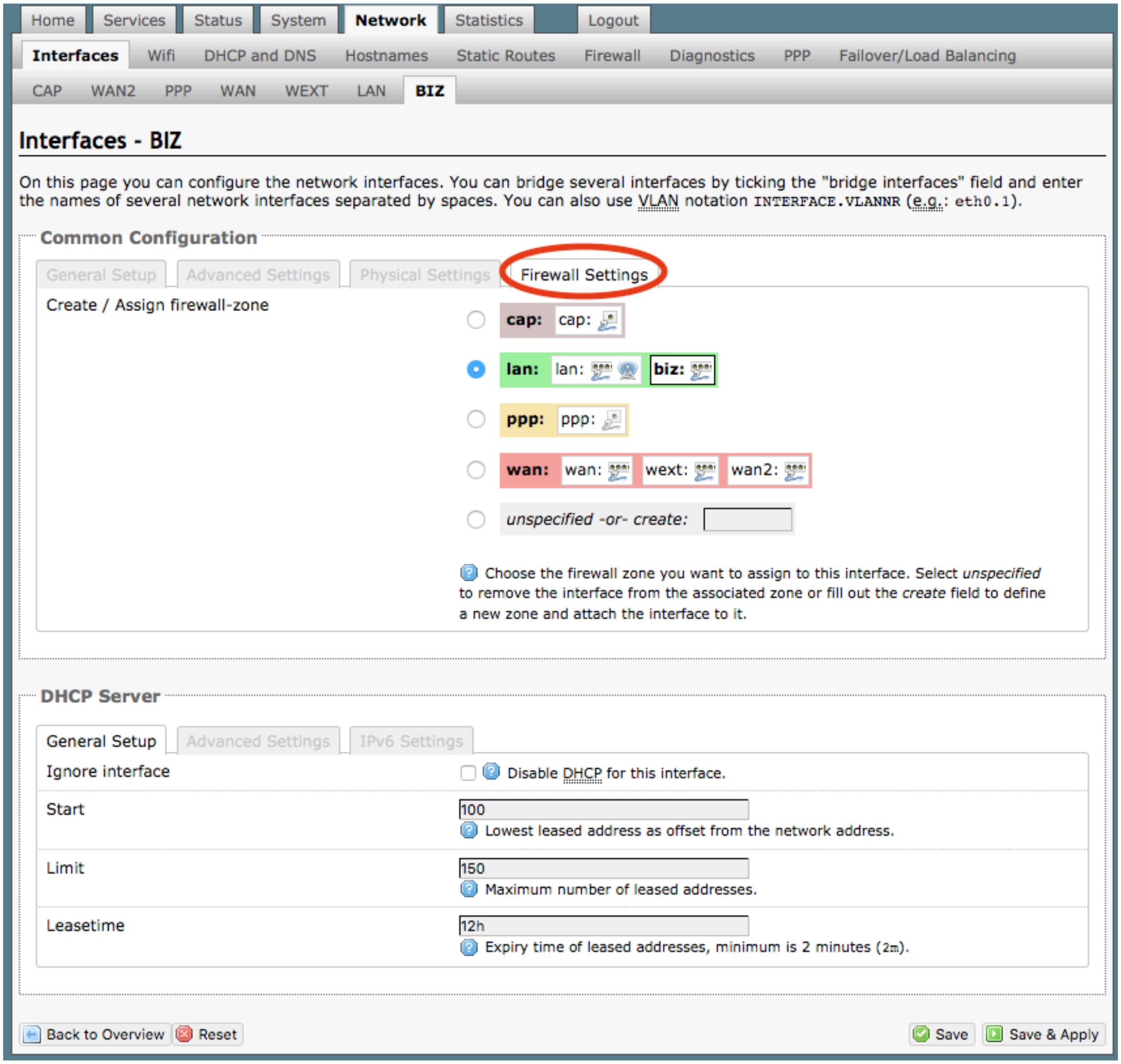
Start: 100
Lowest leased address as offset from the network address.

Limit: 150
Maximum number of leased addresses.

Leasetime: 12h
Expiry time of leased addresses, minimum is 2 minutes (`2m`).

8.1.3.4 Firewall Settings

Use this to select the Firewall Zone you want to assign to the Interface. *See Chapter 8.6 for Firewall Zone details.* You can also configure the DHCP Server Settings from this page.



Interfaces - BIZ

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Create / Assign firewall-zone

○ cap: cap:

● lan: lan: biz:

○ ppp: ppp:

○ wan: wan: wext: wan2:

○ *unspecified -or- create:*

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

DHCP Server

Ignore interface □ Disable DHCP for this interface.

Start: 100
Lowest leased address as offset from the network address.

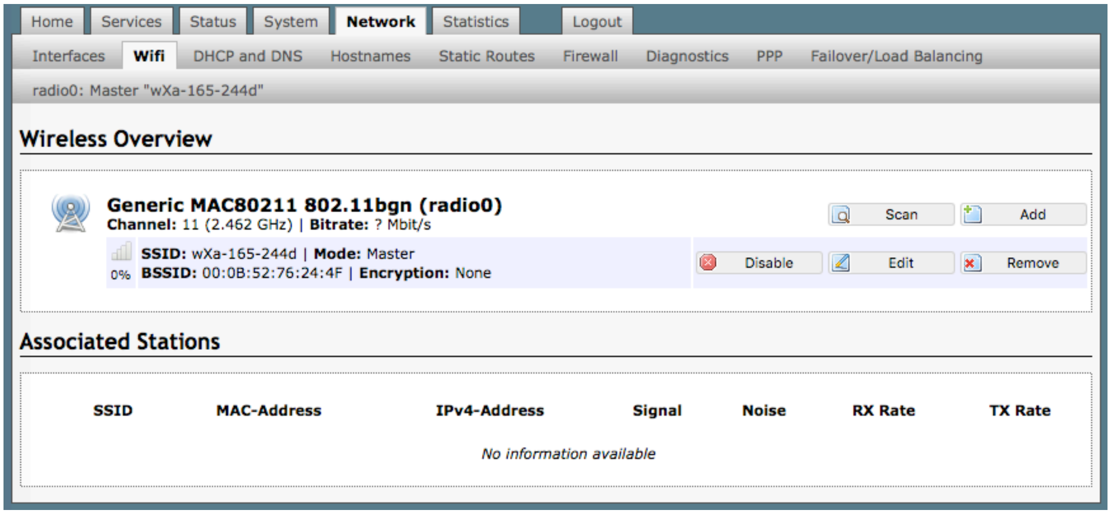
Limit: 150
Maximum number of leased addresses.

Leasetime: 12h
Expiry time of leased addresses, minimum is 2 minutes (`2m`).

8.2 Wifi

Requires "superadmin" login.

This screen shows the current status of the wireless hotspot created by the Optimizer Premier.



radio0: Master "wXa-165-244d"

Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** ? Mbit/s

0% **SSID:** wXa-165-244d | **Mode:** Master
BSSID: 00:0B:52:76:24:4F | **Encryption:** None

Associated Stations

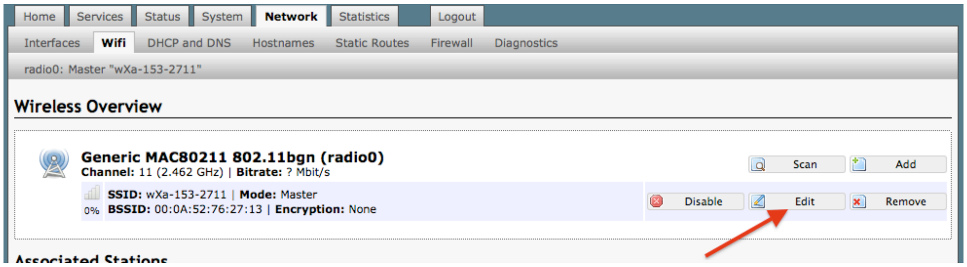
SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate

No information available

Scan: scans for other wireless hotspot signals available in the area.
Add: Add a new Wifi interface.
Disable: Disable the selected Wifi interface but it remains on the list.
Edit: Edit the selected Wifi interface
Remove: Remove the selected Wifi interface

8.2.1 Rename the Wireless Network

The default name of the Optimizer Premier's wireless network is wXa-165-xxxx where the xxxx represents a unique number. This is the name of the wireless network that you connect to using your computer or iOS or Android device. It is possible to change the name of your wireless network.



radio0: Master "wXa-153-2711"

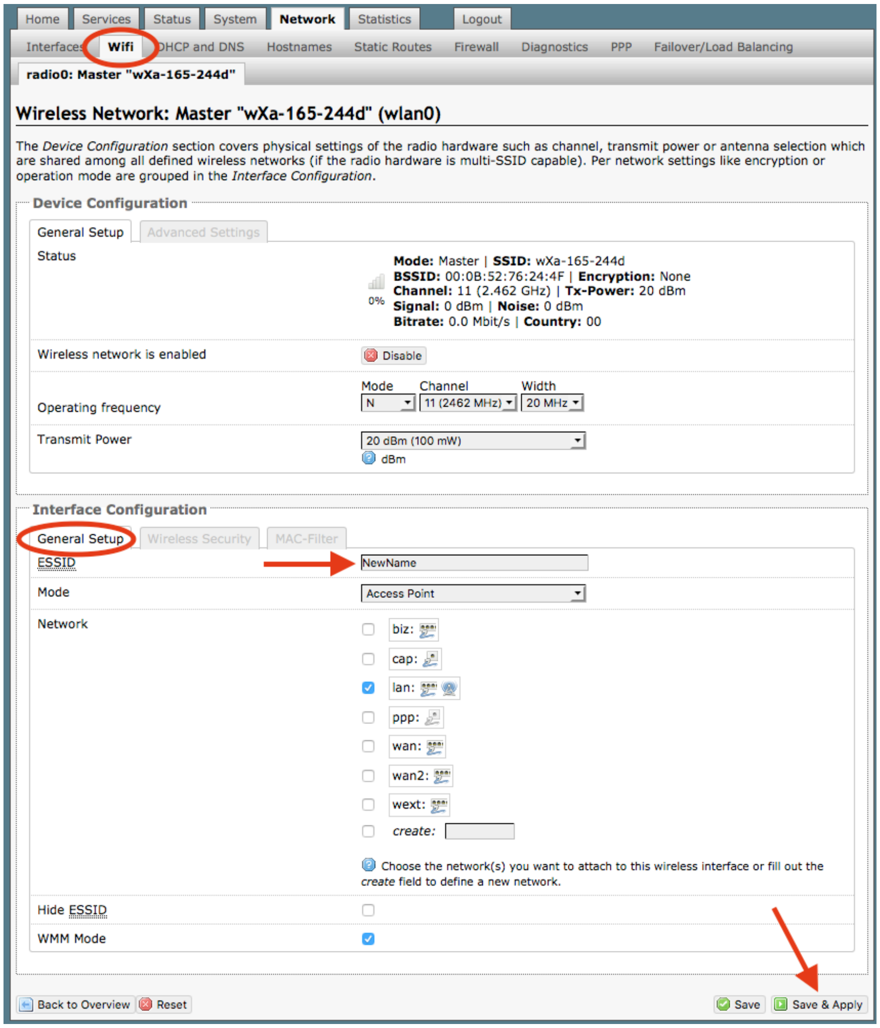
Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** ? Mbit/s

0% **SSID:** wXa-153-2711 | **Mode:** Master
BSSID: 00:0A:52:76:27:13 | **Encryption:** None

Associated Stations

Locate the wXa wifi network and select <Edit>



Wireless Network: Master "wXa-165-244d" (wlan0)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

General Setup | Advanced Settings

Status: 0% **Mode:** Master | **SSID:** wXa-165-244d
BSSID: 00:0B:52:76:24:4F | **Encryption:** None
Channel: 11 (2.462 GHz) | **Tx-Power:** 20 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** 00

Wireless network is enabled: Disable

Operating frequency: Mode N, Channel 11 (2462 MHz), Width 20 MHz

Transmit Power: 20 dBm (100 mW)
dBm

Interface Configuration

General Setup | Wireless Security | MAC-Filter

ESSID: NewName

Mode: Access Point

Network:
☐ biz:
☐ cap:
☑ lan:
☐ ppp:
☐ wan:
☐ wan2:
☐ wext:
☐ *create:*

Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide ESSID: ☐

WMM Mode: ☑

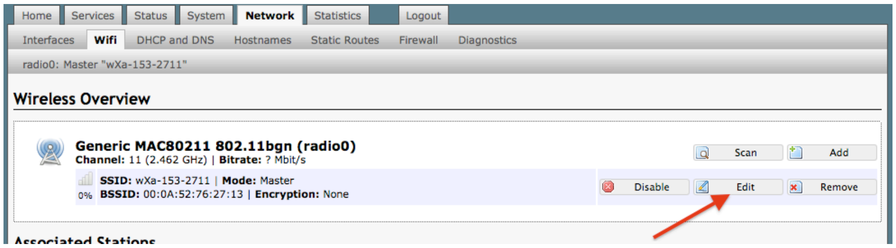
1. Enter the new wireless network name in ESSID field.

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.

8.2.2 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.



radio0: Master "wXa-153-2711"

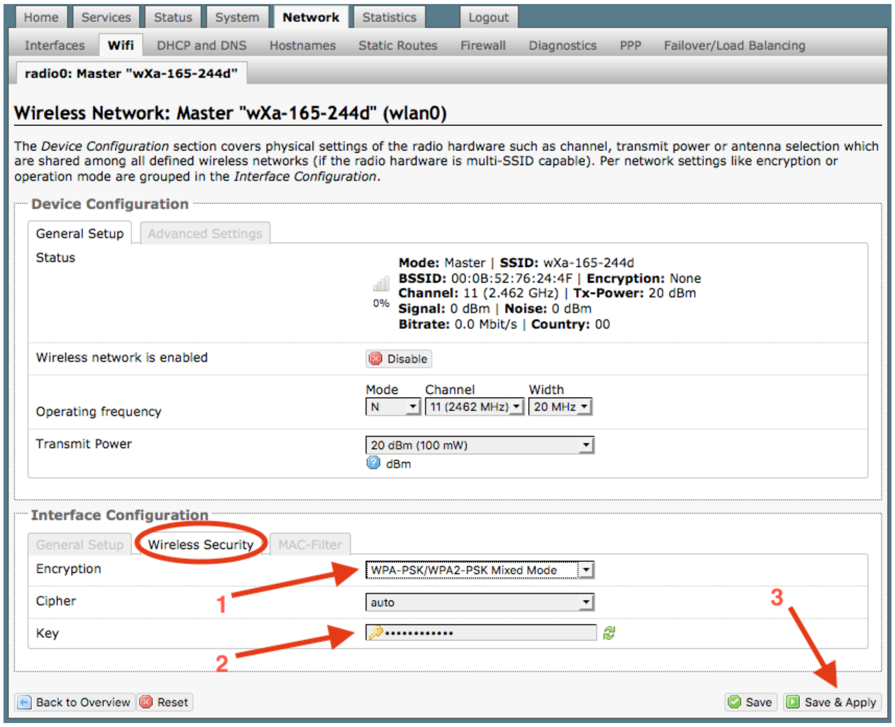
Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** ? Mbit/s

0% **SSID:** wXa-153-2711 | **Mode:** Master
BSSID: 00:0A:52:76:27:13 | **Encryption:** None

Associated Stations

Locate the wXa wifi network and select <Edit>



radio0: Master "wXa-165-244d"

Wireless Network: Master "wXa-165-244d" (wlan0)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

Status: 0%
Mode: Master | **SSID:** wXa-165-244d
BSSID: 00:0B:52:76:24:4F | **Encryption:** None
Channel: 11 (2.462 GHz) | **Tx-Power:** 20 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** 00

Wireless network is enabled

Operating frequency: Mode N, Channel 11 (2462 MHz), Width 20 MHz

Transmit Power: 20 dBm (100 mW)
dBm

Interface Configuration

Encryption: WPA-PSK/WPA2-PSK Mixed Mode

Cipher: auto

Key: •••••••••••••

1. Select the Encryption mode from the drop down menu.
2. Enter your desired password in the Key field.
3. Click <Save & Apply>

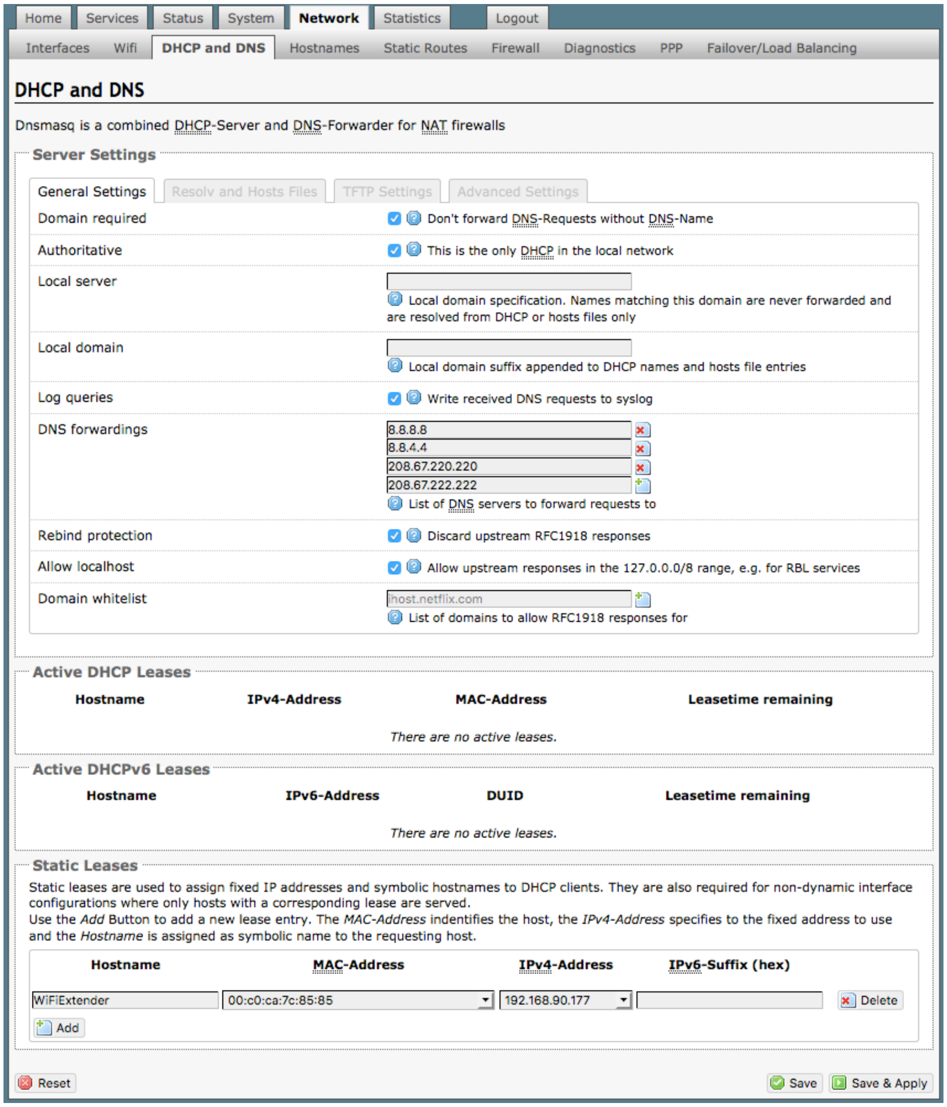
This procedure adds/changes the password for the WiFi hotspot only. When connecting your computer, iOS or Android device to the wireless network, this is the password you will use. This password does not change the router superadmin or admin password when logging in to access the Optimizer user interface.

8.3 DHCP and DNS

Requires "superadmin" login.

The Optimizer Premier is a DNS server.

With the Captive Portal enabled, DHCP and DNS all happen within the Captive Portal, therefore there is no reason to modify these settings.



DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

Domain required	☑ Don't forward DNS-Requests without DNS-Name
Authoritative	☑ This is the only DHCP in the local network
Local server	Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only
Local domain	Local domain suffix appended to DHCP names and hosts file entries
Log queries	☑ Write received DNS requests to syslog
DNS forwardings	8.8.8.8 8.8.4.4 208.67.220.220 208.67.222.222 List of DNS servers to forward requests to
Rebind protection	☑ Discard upstream RFC1918 responses
Allow localhost	☑ Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services
Domain whitelist	ihost.netflix.com List of domains to allow RFC1918 responses for

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining

There are no active leases.

Active DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining

There are no active leases.

Static Leases

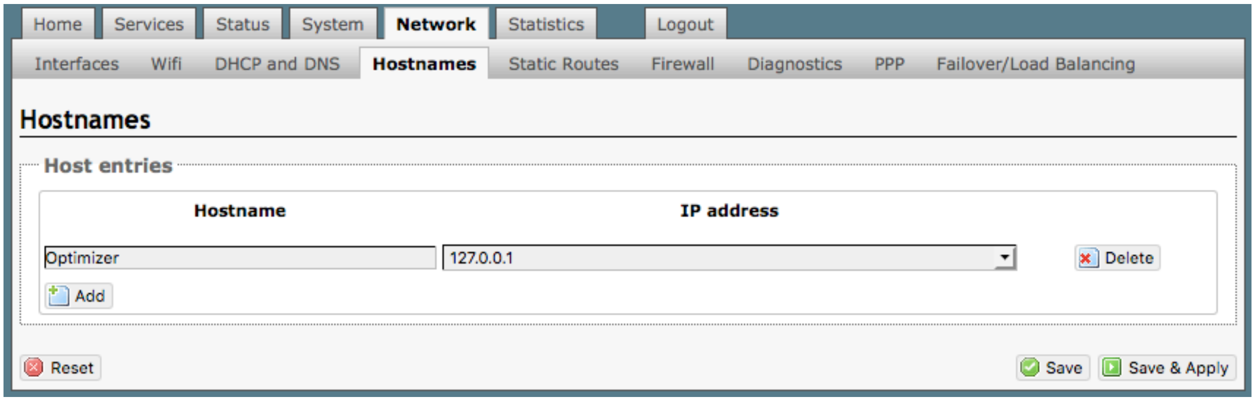
Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
Use the *Add* Button to add a new lease entry. The *MAC-Address* indentifies the host, the *IPv4-Address* specifies to the fixed address to use and the *Hostname* is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)
WiFIExtender	00:c0:ca:7c:85:85	192.168.90.177	

8.4 Hostnames

Requires "superadmin" login.

Use this page to associate a hostname with an IP address.

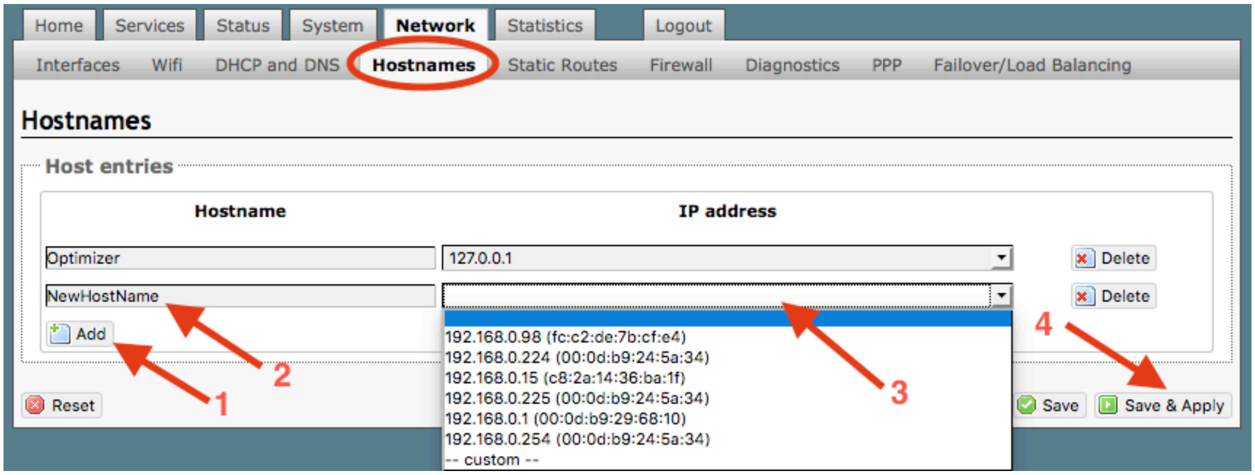


Hostnames

Host entries

Hostname	IP address
Optimizer	127.0.0.1

8.4.1 Add Hostname


Home
Services
Status
System
Network
Statistics
Logout
Interfaces
Wifi
DHCP and DNS
Hostnames
Static Routes
Firewall
Diagnostics
PPP
Failover/Load Balancing
Delete
Delete
Add
Reset
Save
Save & Apply
192.168.0.98 (fc:c2:de:7b:cf:e4)
192.168.0.224 (00:0d:b9:24:5a:34)
192.168.0.15 (c8:2a:14:36:ba:1f)
192.168.0.225 (00:0d:b9:24:5a:34)
192.168.0.1 (00:0d:b9:29:68:10)
192.168.0.254 (00:0d:b9:24:5a:34)
-- custom --
1
2
3
4

Hostnames

Host entries

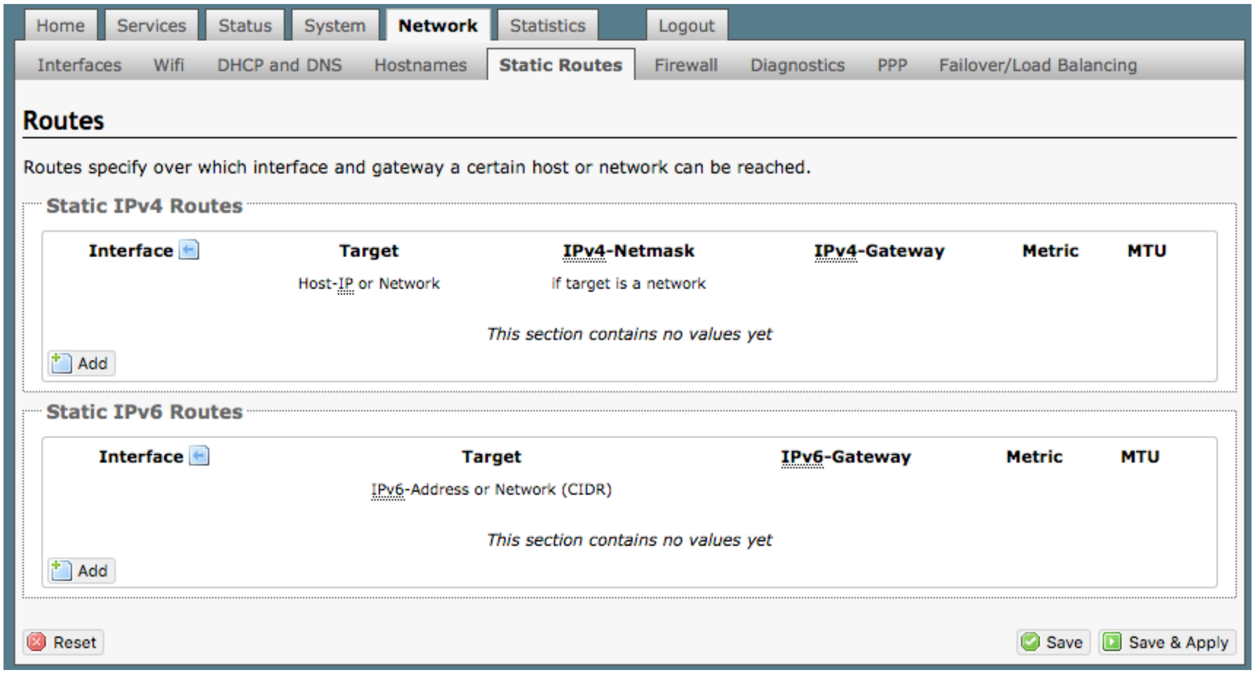
Hostname	IP address
Optimizer	127.0.0.1
NewHostName	

1. Select <Add>.
2. Enter the new Hostname.
3. Select the IP address from the drop-down list OR select custom to enter the IP address.
4. Select Save & Apply.

8.5 Static Routes

Requires "superadmin" login.

This Static Routes table is available for those with a complex network that may include multiple routers. Use this page to specify how a certain host or network can be reached.



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU
	Host-IP or Network	if target is a network			

This section contains no values yet

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
	IPv6-Address or Network (CIDR)			

This section contains no values yet

Static routes take precedent over MWAN Traffic Rules.

8.6 Firewall

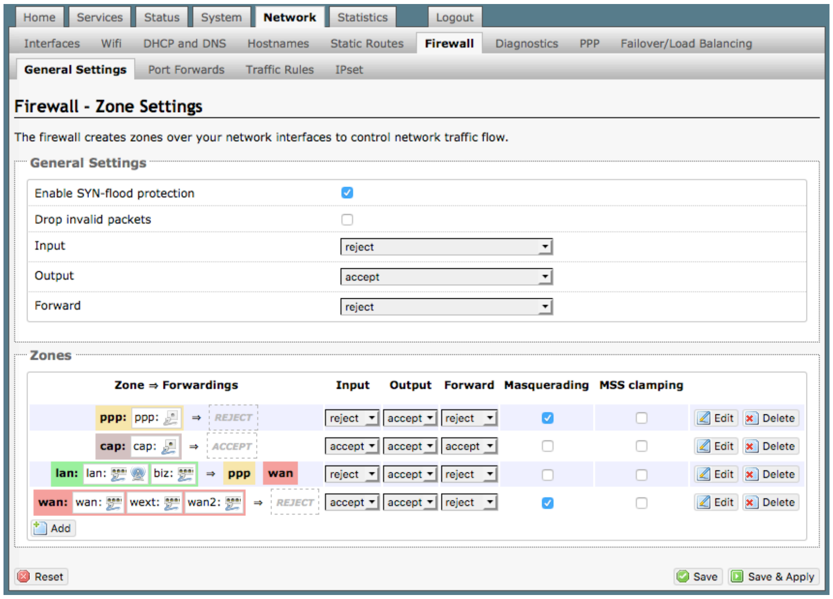
Requires "superadmin" login.

The Firewall allows you to control network traffic flow over each interface. Most installations do not require any firewall modifications due to the flexibility of the Captive Portal configuration *(see Chapter 5.1)* and the Failover/Load Balancing configuration *(see Chapter 8.9).*

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 Premier. USE WITH CAUTION AND AT YOUR OWN RISK!

8.6.1 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 *(see Chapter 8.6).*



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection	☑
Drop invalid packets	□
Input	reject
Output	accept
Forward	reject

Zones

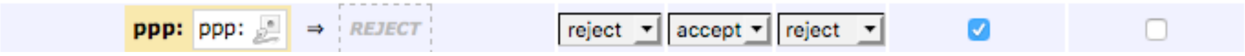
Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
ppp: ppp: ⇒ REJECT	reject	accept	reject	☑	□	Edit Delete
cap: cap: ⇒ ACCEPT	accept	accept	accept	□	□	Edit Delete
lan: lan: biz: ⇒ ppp wan	reject	accept	reject	□	□	Edit Delete
wan: wan: wext: wan2: ⇒ REJECT	accept	accept	reject	☑	□	Edit Delete

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. *(see Chapter 8.6.1.1)*

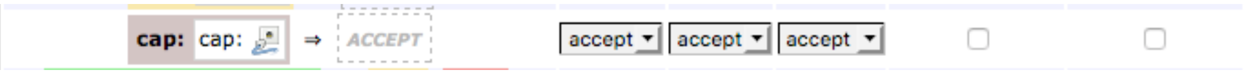
Accept: this setting allows traffic unless there is a Rule to block it. *(see Chapter 8.9.2)*
Reject: this setting blocks traffic unless there is a Rule to allow it. *(see Chaptger 8.9.2)* An error is displayed to the end user.
Drop: this setting drops the traffic with no indication to the end user.

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



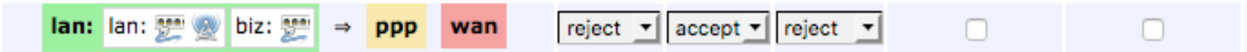
ppp: ppp: ⇒ REJECT reject accept reject ☑ □

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



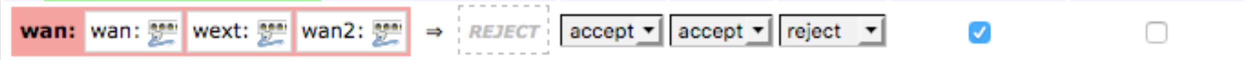
cap: cap: ⇒ ACCEPT accept accept accept □ □

The "cap" firewall zone has only the cap interface assigned to it. This is the zone for the Captive Portal. In this default configuration, all traffic is allowed but subject to the Captive Portal settings.



lan: lan: biz: ⇒ **ppp** **wan** reject accept reject □ □

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



wan: wan: wext: wan2: ⇒ REJECT accept accept reject ☑ □

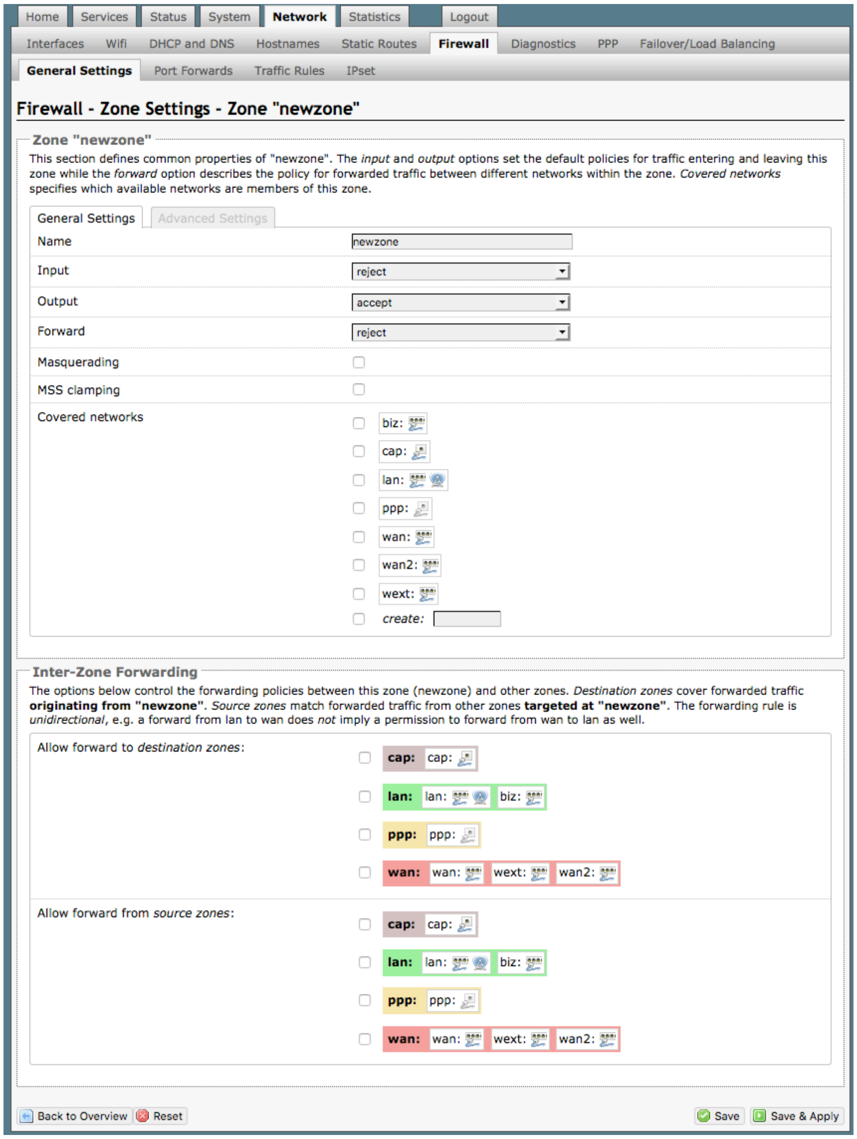
The "wan" firewall zone has the wan, wan2 and wext interfaces assigned to it. This is the zone for satellite connections and wifi extenders. In this default configuration, only Output traffic is allowed.

CAUTION: While it is possible to edit these zones and add new zones, Best Practice is to leave these zones alone and create MWAN Traffic Rules instead, assigning the new rules to a Zone. See Chapter 8.9.

FOR EXAMPLE: If a system administrator wants to create firewall zones that are different for each device, such as firewall rules for wifi to allow all, rules for vsat to allow dns and http but nothing else, for fbb do not allow anything but email. You could create three new zones; one for each wan interface, then create firewall rules that pertain to each of the new zones. You then edit the lan interface to add the three new zones. OR, do not create zones but use IP addresses added to the mwan traffic rules (not the firewall rules). Leave the zones the same, use MWAN traffic rules, assigning the rule to a zone and use IP source address or a specific IP address. The destination can be any address and apply to any zone. See Chapter 8.9.

8.6.1.1 Add a Firewall Zone

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



Firewall - Zone Settings - Zone "newzone"

Zone "newzone"

This section defines common properties of "newzone". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name	newzone
Input	reject
Output	accept
Forward	reject
Masquerading	□
MSS clamping	□
Covered networks	□ biz: □ cap: □ lan: □ ppp: □ wan: □ wan2: □ wext: □ *create:*

Inter-Zone Forwarding

The options below control the forwarding policies between this zone (newzone) and other zones. *Destination zones* cover forwarded traffic **originating from "newzone"**. *Source zones* match forwarded traffic from other zones **targeted at "newzone"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination zones*:	□ **cap:** cap: □ **lan:** lan: biz: □ **ppp:** ppp: □ **wan:** wan: wext: wan2:
Allow forward from *source zones*:	□ **cap:** cap: □ **lan:** lan: biz: □ **ppp:** ppp: □ **wan:** wan: wext: wan2:

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

8.6.1.2 Delete a Firewall Zone

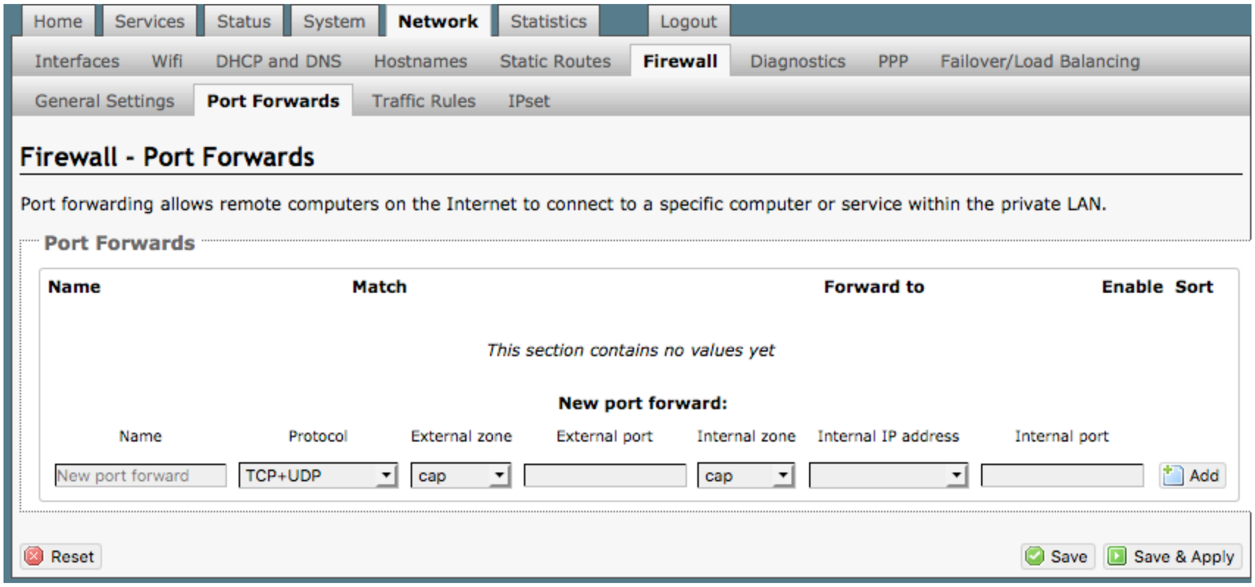
To permanently remove a firewall zone, select the Delete icon. ☒ Delete

CAUTION: This action CANNOT be undone.

8.6.2 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.



Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

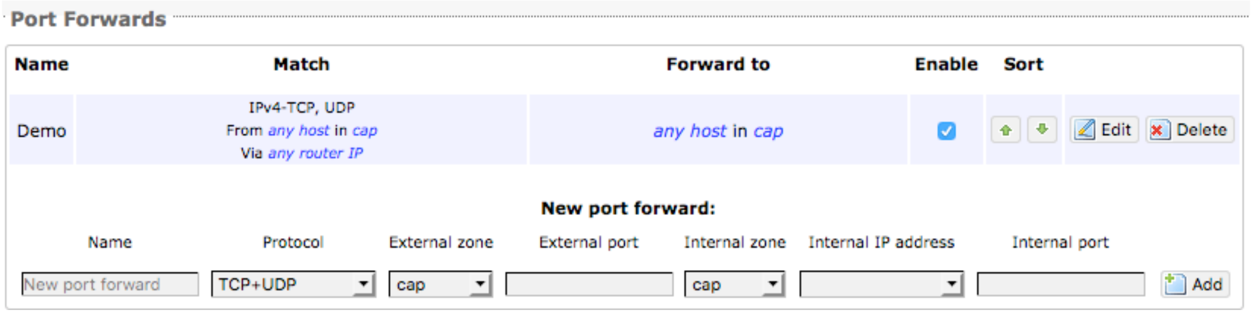
Name	Match	Forward to	Enable	Sort

This section contains no values yet

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
New port forward	TCP+UDP	cap		cap		

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



Port Forwards

Name	Match	Forward to	Enable	Sort
Demo	IPv4-TCP, UDP From *any host* in *cap* Via *any router IP*	*any host* in *cap*	☑	

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
New port forward	TCP+UDP	cap		cap		

You can now enable/disable them, change the sort order, and edit the parameters.

CAUTION: The Delete function cannot be undone.

8.6.3 Firewall - Traffic Rules

This page is 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.

While you can add rules, delete rules and each interface can have its own set of rules, BEST PRACTICE is to manage router traffic via the Failover/Load Balancing MWAN Traffic Rules (see Chapter 8.9).

By default, the router is shipped to you with six rules that all 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 Firewall Traffic Rules Table. When enabled, these rules Allow that particular traffic to pass through the firewall. This means that the Firewall is totally OPEN by default. When you configure the Captive Portal and Failover/Load Balancing you can restrict the allowed traffic thru an interface.

All the firewall 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.

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

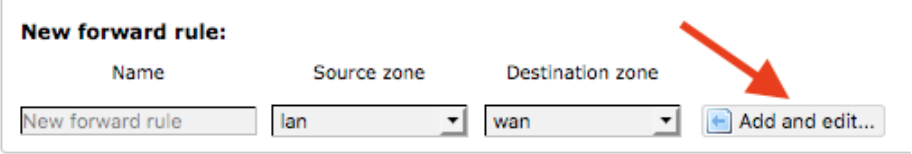
- Disable (uncheck) the first rule "ALL-DO NOT MODIFY". This forces the remaining rules to take precedent.
- Disable (uncheck) the rule "HTTP-DO NOT MODIFY". This blocks http traffic from passing through the firewall.

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.

8.6.3.1 Create a Custom Rule

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



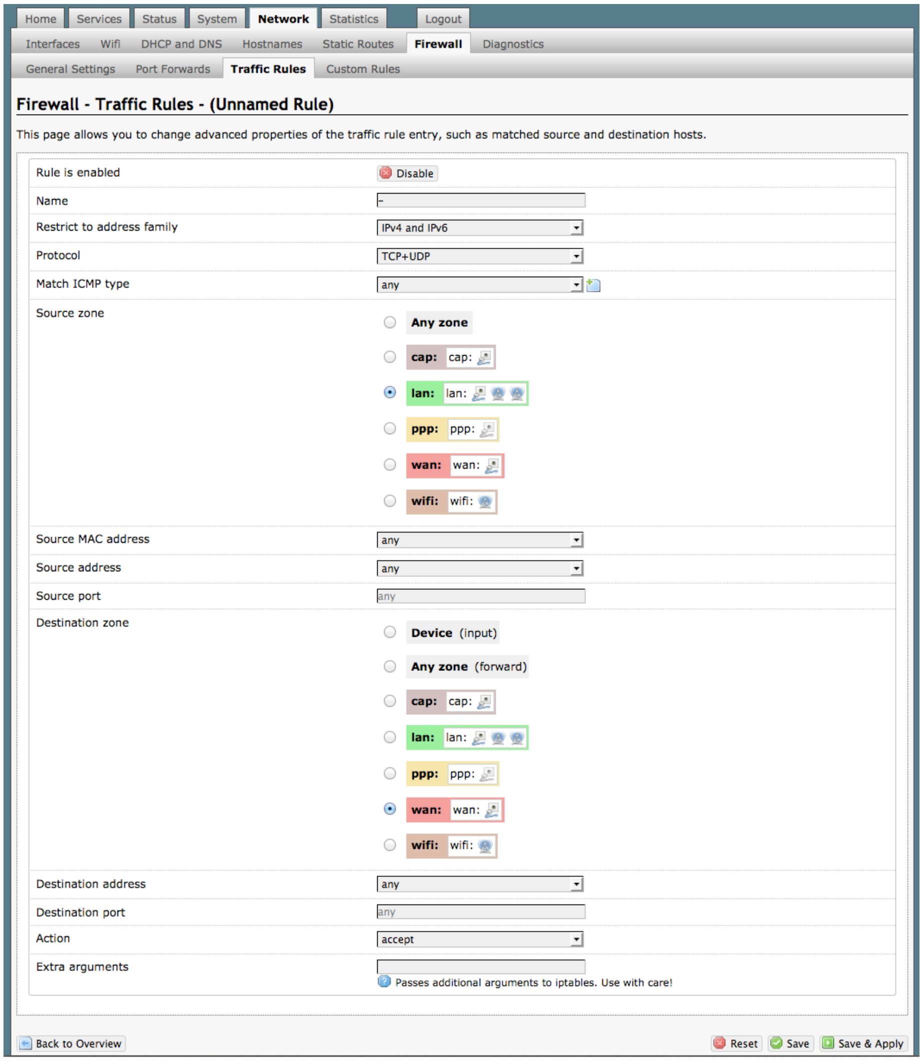
New forward rule:

Name	Source zone	Destination zone	
New forward rule	lan	wan	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.



Firewall - Traffic Rules - (Unnamed Rule)

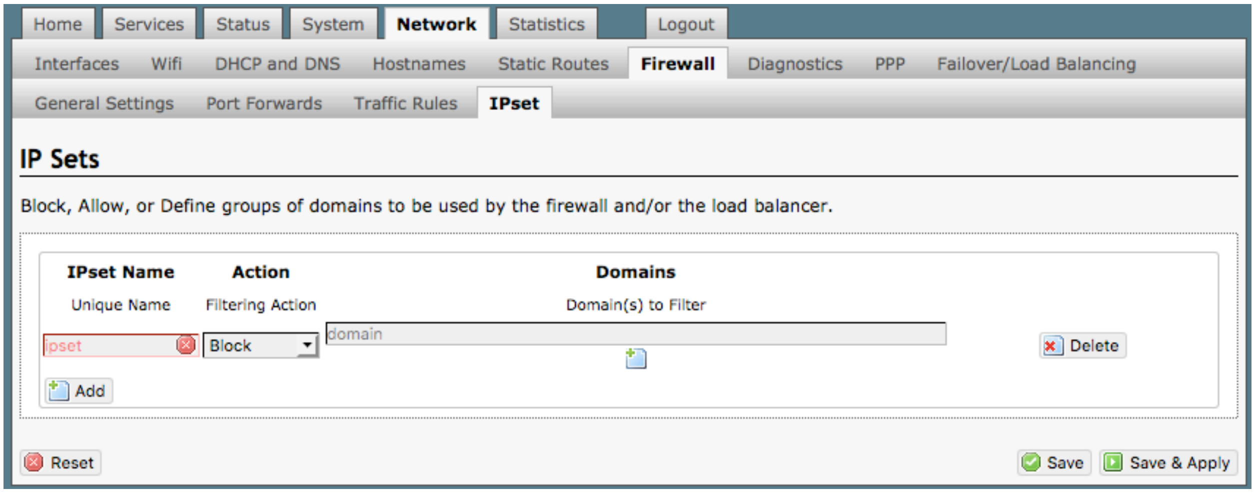
This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled	Disable
Name	-
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	○ Any zone ○ cap: cap: ● lan: lan: ○ ppp: ppp: ○ wan: wan: ○ wifi: wifi:
Source MAC address	any
Source address	any
Source port	any
Destination zone	○ Device (input) ○ Any zone (forward) ○ cap: cap: ○ lan: lan: ○ ppp: ppp: ● wan: wan: ○ wifi: wifi:
Destination address	any
Destination port	any
Action	accept
Extra arguments	Passes additional arguments to iptables. Use with care!

See IP Sets *(Chapter 8.6.4)* for creating block and allow rules by domain name instead of ip address.

8.6.4 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.



IP Sets

Block, Allow, or Define groups of domains to be used by the firewall and/or the load balancer.

IPset Name Unique Name	Action Filtering Action	Domains Domain(s) to Filter	
ipset	Block	domain	Delete

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

Action Definitions:

- **Block**: rejects the domain
- **Pass**: allows the domain
- **Define**: defines the domain only. It neither blocks nor allows. You can specify how routing occurs for that domain in the Failover/Load Balancing Rules. *(see Chapter 8.9)*

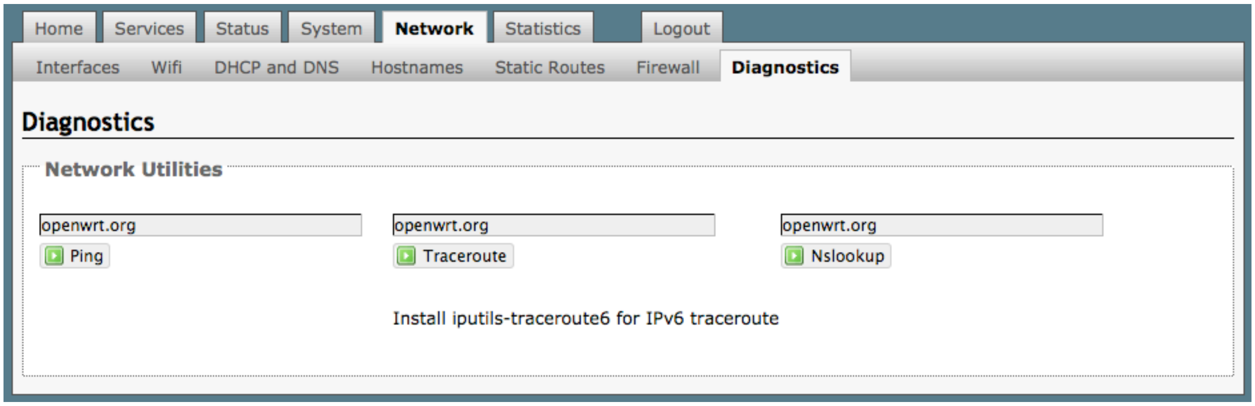
You can group multiple domain names into one IP set rule.

Each IP set rule must be assigned to a *Policy (see Chapter 8.9.2).*

8.7 Diagnostics

Requires "superadmin" login.

There are several Diagnostic tools available:



Diagnostics

Network Utilities

openwrt.org

openwrt.org

openwrt.org

Install iputils-traceroute6 for IPv6 traceroute

Ping: tells you if you have ip connectivity

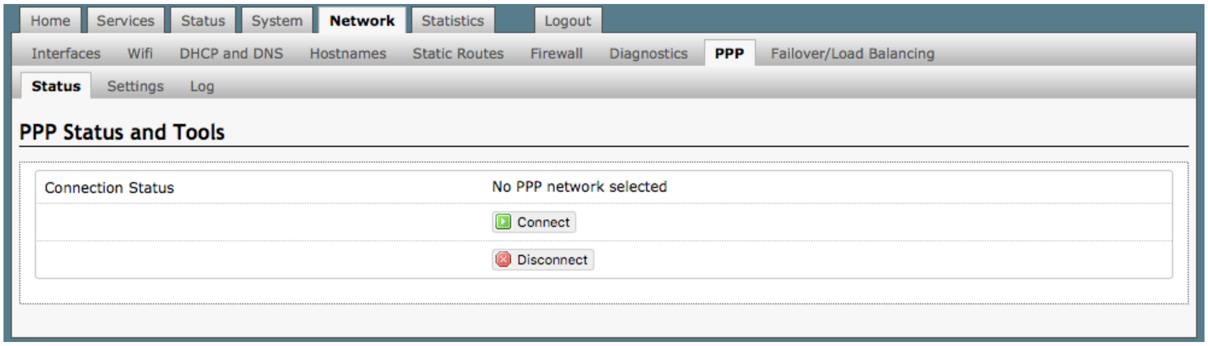
Traceroute: gives you all the ip addresses in a hop to the final destination.

Nslookup: gives you the ip address of whatever you enter into the text box.

8.8 PPP

Requires "superadmin" login.

It is possible to use a USB connected satellite phone or GSM modem that does PPP 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.)



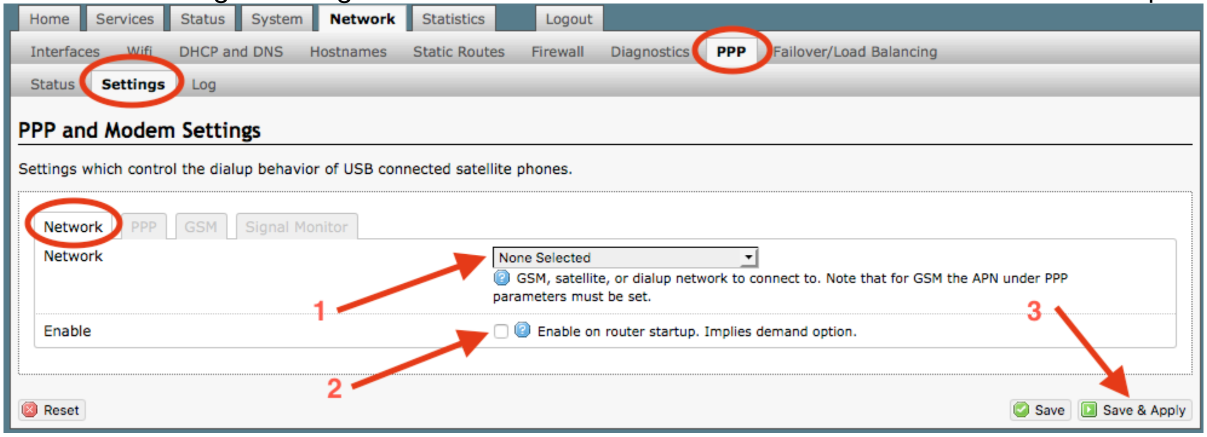
PPP Status and Tools

Connection Status	No PPP network selected
	Connect
	Disconnect

With PPP configured, you can bring up the connection manually; it will stay connected until you disconnect or the idle timeout is reached. If not using the Demand feature, you must bring up the PPP connection manually. *See Chapters 8.8.1 and 8.8.2.*

8.8.1 PPP Settings Configuration for USB Connected Satellite Device

Use the following to configure the PPP interface for use with a USB connected satellite phone.

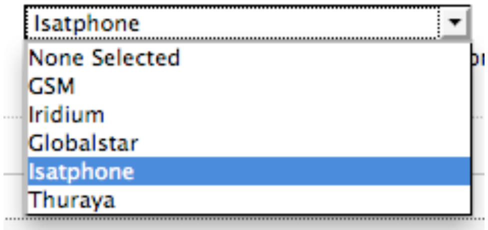


PPP and Modem Settings

Settings which control the dialup behavior of USB connected satellite phones.

Network: None Selected
GSM, satellite, or dialup network to connect to. Note that for GSM the APN under PPP parameters must be set.

Enable: □ Enable on router startup. Implies demand option.

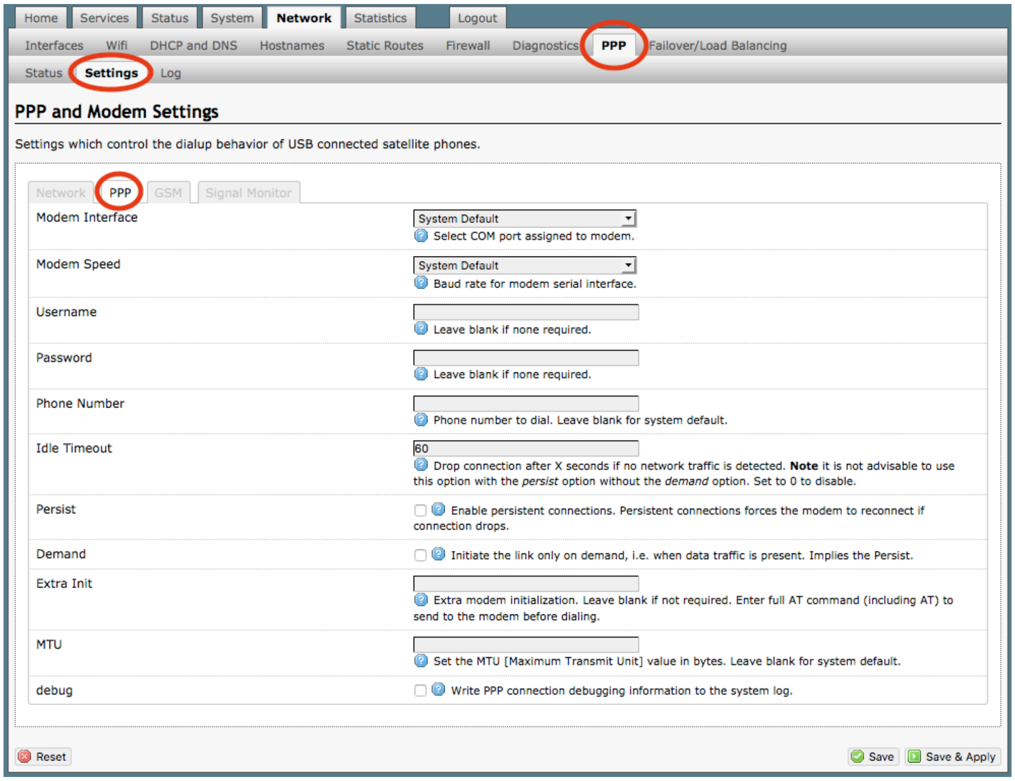


1. Using the drop-down menu, select the appropriate satellite network.

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 the Settings > PPP Tab:



PPP and Modem Settings

Settings which control the dialup behavior of USB connected satellite phones.

Modem Interface	System Default Select COM port assigned to modem.
Modem Speed	System Default Baud rate for modem serial interface.
Username	Leave blank if none required.
Password	Leave blank if none required.
Phone Number	Phone number to dial. Leave blank for system default.
Idle Timeout	60 Drop connection after X seconds if no network traffic is detected. **Note** it is not advisable to use this option with the *persist* option without the *demand* option. Set to 0 to disable.
Persist	□ Enable persistent connections. Persistent connections forces the modem to reconnect if connection drops.
Demand	□ Initiate the link only on demand, i.e. when data traffic is present. Implies the Persist.
Extra Init	Extra modem initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modem before dialing.
MTU	Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.
debug	□ Write PPP connection debugging information to the system log.

Configure the PPP Settings as necessary. These PPP Settings apply to both USB connected satellite phones and GSM (cellular) modems.

Modem Interface: Do not modify from "System Default" unless you have trouble connecting. If required, use the drop-down list, select the COM port assigned to the USB connected satphone.

Modem Speed: Do not modify from "System Default" unless you have trouble connecting. If required, use the drop-down list, select the baud rate for the USB connected satphone.

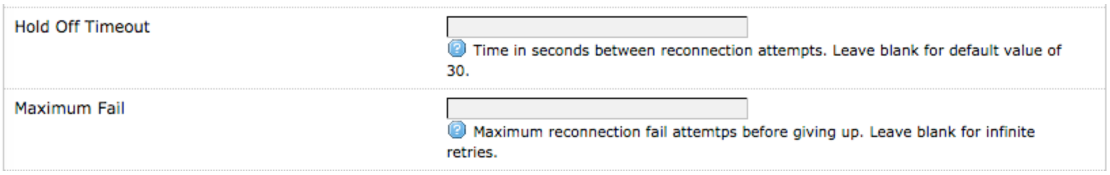
Username: If the satellite network provider requires a username in order to connect to their network, enter it here. (If you use the APN Wizard, this will be completed automatically.)

Password: If the satellite network provider requires a password in order to connect to their network, enter it here. (If you use the APN Wizard, this will be completed automatically.

Phone number: The Optimizer is pre-configured with the standard number to dial for the different satellite networks. Unless your satellite airtime provider requires an alternate phone number, this field can be left blank in order to use the default dialup number.

Idle Timeout: The default is set to 60 seconds. If no network traffic is detected during this Idle Timeout period, the connection will drop. To disable the Idle Timeout feature, set to 0. *Note: If Persist is enabled with Demand disabled, the Idle Timeout is ignored.*

Persist: Check this box to enable persistent connections. If the connection drops the modem will attempt to reconnect. With Persist selected, two additional settings appear:



Hold Off Timeout	Time in seconds between reconnection attempts. Leave blank for default value of 30.
Maximum Fail	Maximum reconnection fail attemtps before giving up. Leave blank for infinite retries.

Hold Off Timeout: The default is 30 seconds. If the link is dropped, this is the time it will wait to try connection again.

Maximum Fail: The default is never. This is the number of times it will try to re-connect. If re-connection does not happen within this number, it will stop trying.

Demand: Check this box to bring up the link only on demand, such as when data traffic is present. The satphone or GSM modem that does PPP, the link remains down until it detects network traffic. It will bring up the link automatically and stay up when there is traffic or until the Idle Timeout setting reached. With Demand selected, Persist is implied. See Persist above.

Best Practice: when using GSM in the load-balancing mode, enable this Demand feature so that when there is PPP traffic the modem will go online, when no traffic the connection is terminated.

Extra Init: If required, enter the full AT command to send to the modem before dialing.

MTU (Maximum Transmit Unit): This should be blank to use the system default; or, you can set the limit here, in bytes. Only change this setting if required to do so by your satellite provider.

debug: If you are having trouble with the PPP connection this debug log may help you diagnose the problem.

Select <Save & Apply>.

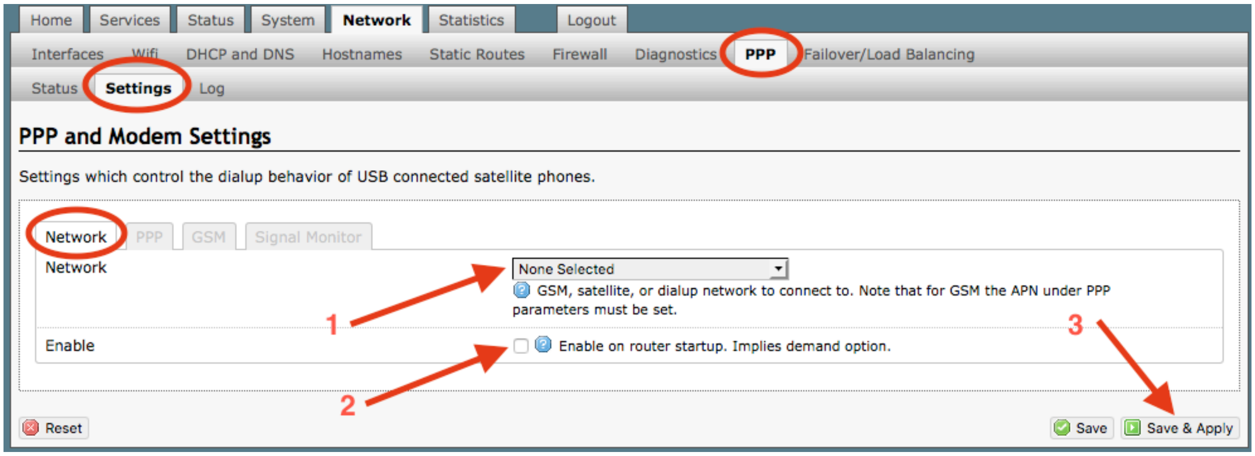
8.8.2 PPP Settings Configuration for GSM Modems

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 connection. If you run into any difficulties you must contact your cellular network provider for support.

If you have a GSM-based or LTE-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 and LTE-based service can be configured here. CDMA-based service will NOT work. If you are unsure of which service you have, contact your cellular provider before attempting to configure for connection.

Use the following to configure the PPP interface for use with a GSM modem.

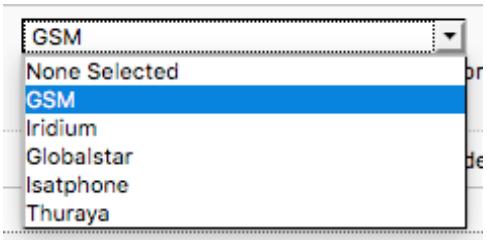


PPP and Modem Settings

Settings which control the dialup behavior of USB connected satellite phones.

Network: None Selected
GSM, satellite, or dialup network to connect to. Note that for GSM the APN under PPP parameters must be set.

Enable: □ Enable on router startup. Implies demand option.

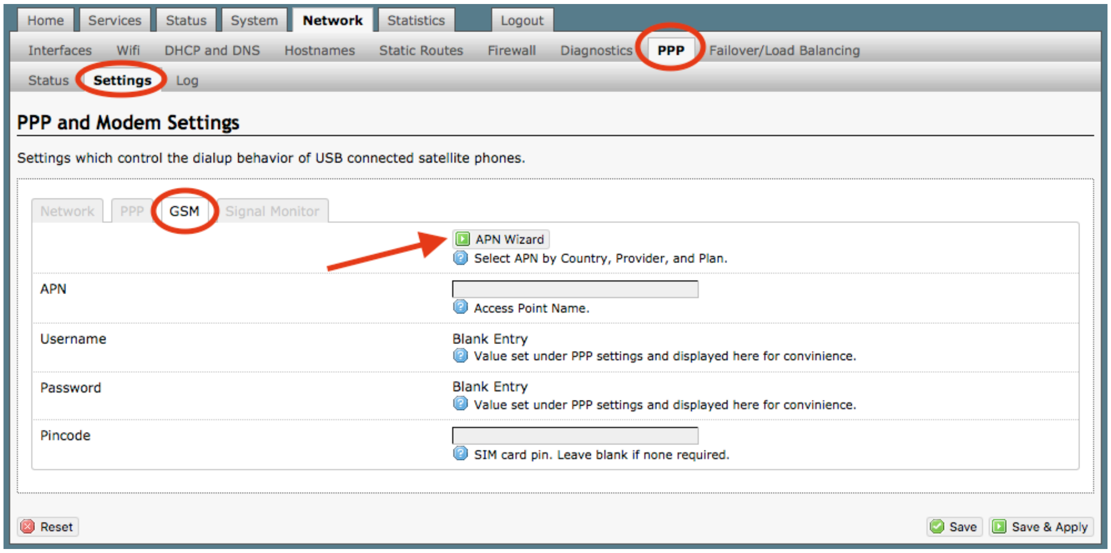


1. Using the drop-down menu, select GSM.

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 the Settings > GSM Tab:



PPP and Modem Settings

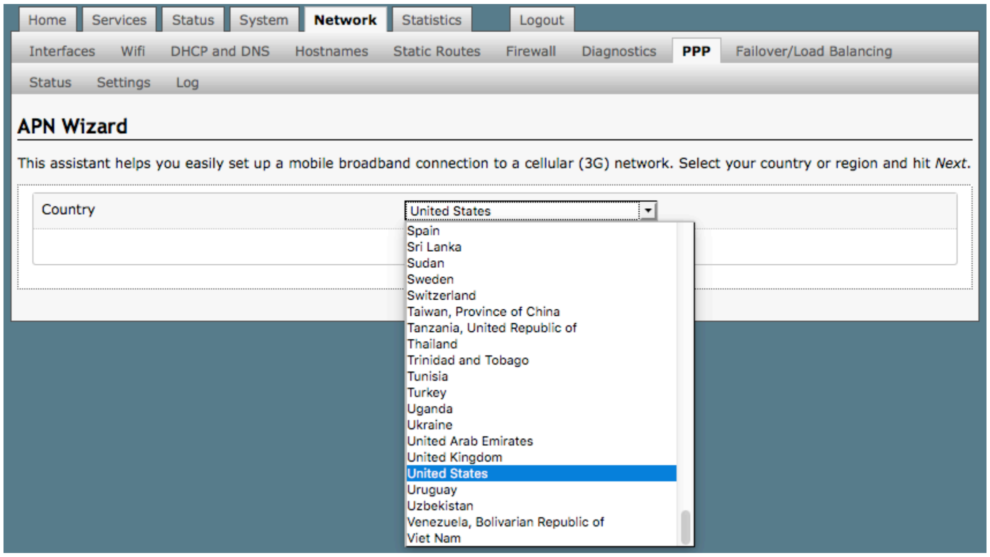
Settings which control the dialup behavior of USB connected satellite phones.

	Select APN by Country, Provider, and Plan.
APN	Access Point Name.
Username	Blank Entry Value set under PPP settings and displayed here for convinience.
Password	Blank Entry Value set under PPP settings and displayed here for convinience.
Pincode	SIM card pin. Leave blank if none required.

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.

The APN Wizard contains many providers and plans. Using it will automatically set the configuration for you. Select <APN Wizard> to start the configuration:

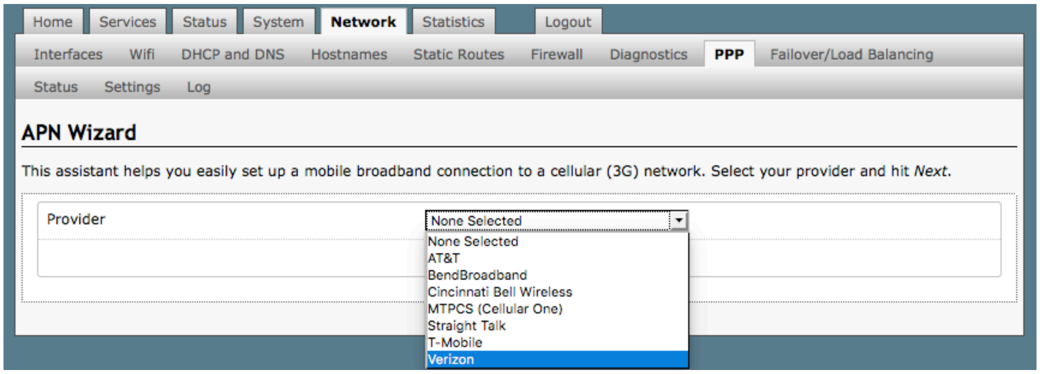


APN Wizard

This assistant helps you easily set up a mobile broadband connection to a cellular (3G) network. Select your country or region and hit *Next*.

Country: United States

Select the appropriate country from the drop down list and then, <Next>.

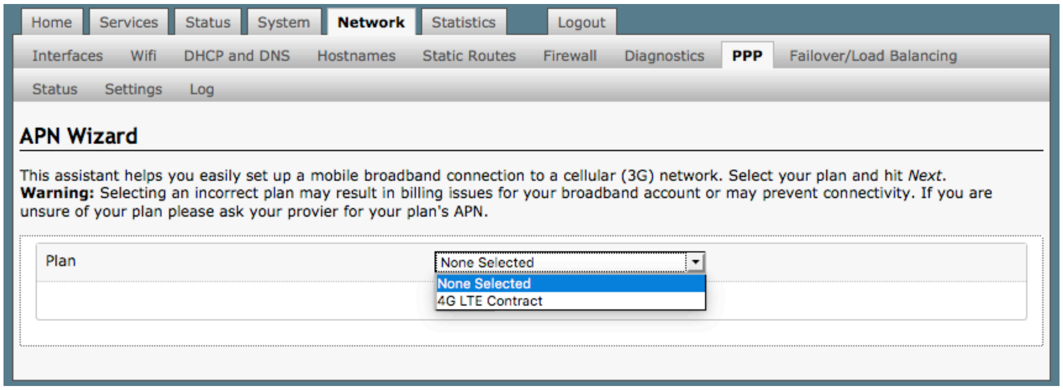


APN Wizard

This assistant helps you easily set up a mobile broadband connection to a cellular (3G) network. Select your provider and hit *Next*.

Provider: None Selected

Select your Cell Provider from the drop down list and then, <Next>.

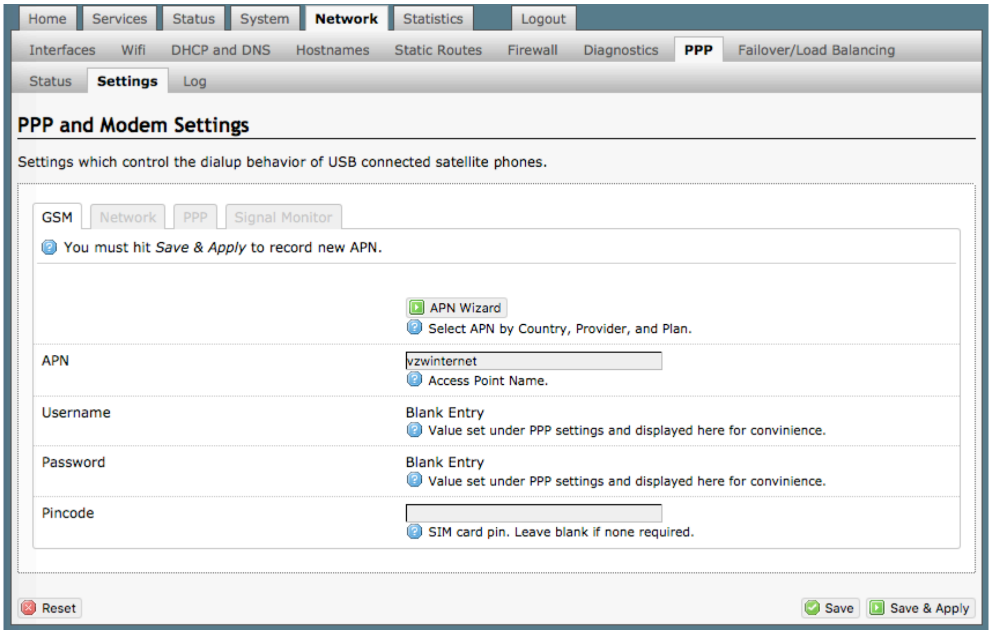


APN Wizard

This assistant helps you easily set up a mobile broadband connection to a cellular (3G) network. Select your plan and hit *Next*. **Warning:** Selecting an incorrect plan may result in billing issues for your broadband account or may prevent connectivity. If you are unsure of your plan please ask your provier for your plan's APN.

Plan: None Selected

Select your Plan from the drop down list and then, <Next>.



PPP and Modem Settings

Settings which control the dialup behavior of USB connected satellite phones.

You must hit *Save & Apply* to record new APN.

Select APN by Country, Provider, and Plan.

APN: vzwinternet
Access Point Name.

Username: Blank Entry
Value set under PPP settings and displayed here for convinience.

Password: Blank Entry
Value set under PPP settings and displayed here for convinience.

Pincode:
SIM card pin. Leave blank if none required.

If you have protected your cellular SIM card with a PIN-Code, enter the PIN-Code in the Pincode text box.

Select <Save & Apply> to complete the configuration.

NOTE: If the APN Wizard does not contain the information for your provider or plan, 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

Enter the required information in the PPP Settings pages.

See Section 8.8.1 for additional PPP Settings.

8.8.2.1 Using GSM

When you want to use GSM service instead of satellite service we recommend that you disconnect the satellite terminal from the Optimizer before attempting a GSM connection.

Plug the USB data dongle you obtained from your cellular provider into the USB/GSM port of the Optimizer.

With the GSM interface properly configured, it becomes an important component of the Failover sequence.

8.8.2.2 Changing from GSM service to satellite service

When you travel beyond GSM range you must:

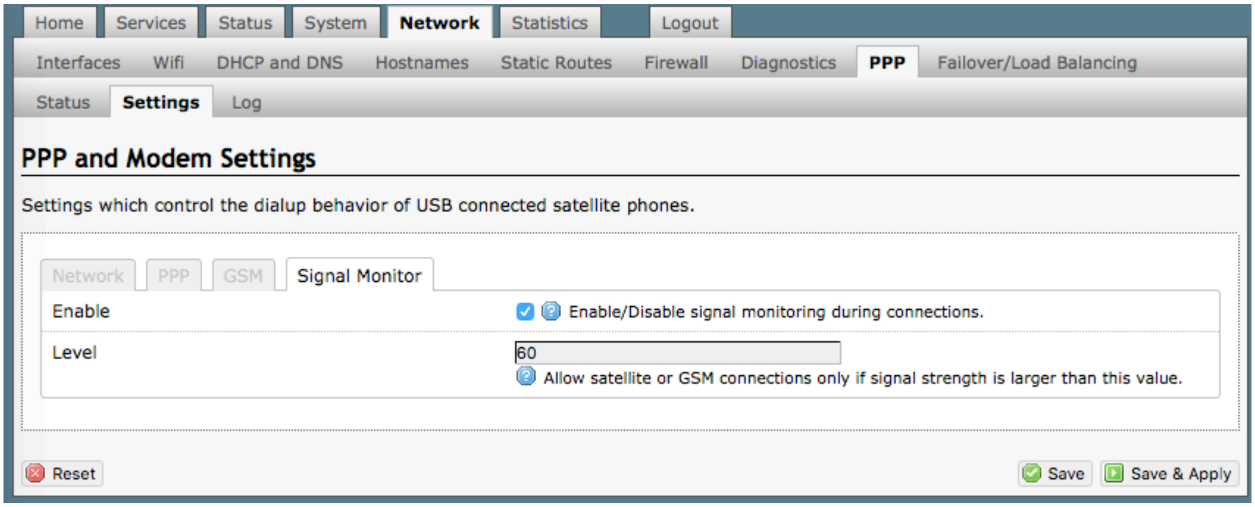
- Remove the GSM data dongle from the Optimizer's USB/GSM port.
- Reconnect your satellite phone/terminal to the Optimizer.

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.

8.8.3 Signal Monitor

Signal monitor queries your satellite device or GSM modem 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.



PPP and Modem Settings

Settings which control the dialup behavior of USB connected satellite phones.

Enable ☑ Enable/Disable signal monitoring during connections.

Level 60
Allow satellite or GSM connections only if signal strength is larger than this value.

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

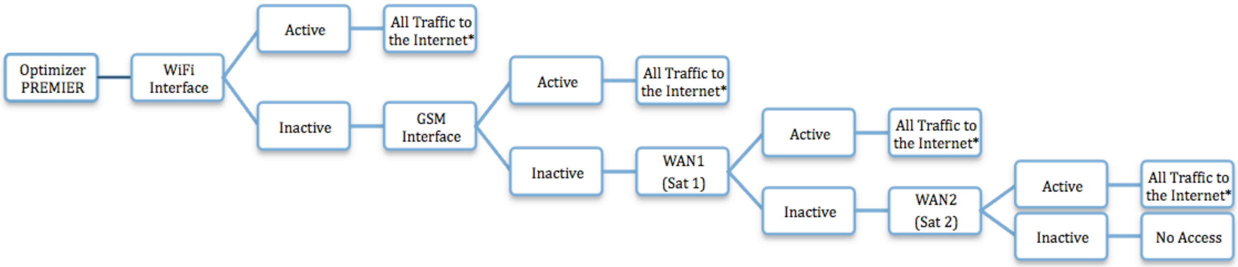
You can change the level of the Signal Monitor. Keep in mind that 60% is typically the minimum required for a successful data connection. If you must change the Signal Monitor, we recommend lowering the Level vs. disabling it. Many IsatPhonePro users have had success by lowering the level to 40 or 30.

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>.

8.9 Failover/Load Balancing

The default Failover sequence and Load Balance configuration are as follows:



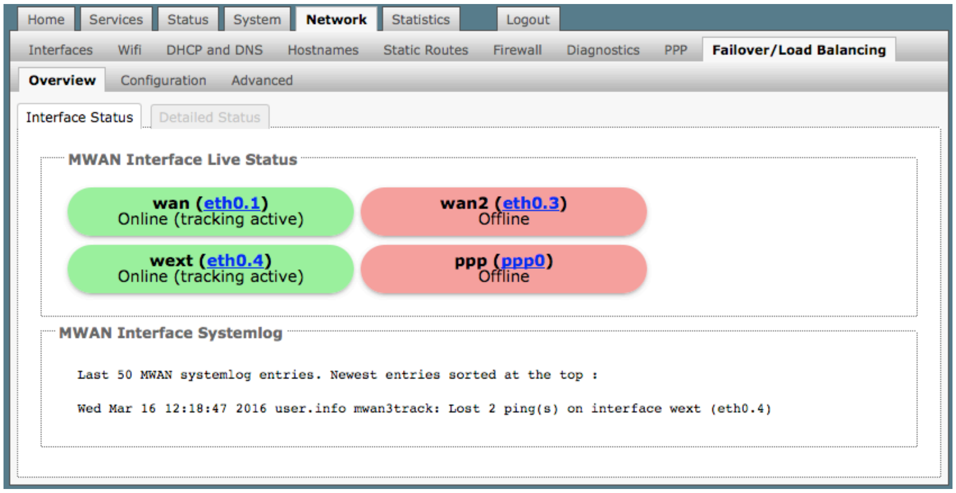
Setup is required for the GSM Interface

****All traffic to the Internet is subject to the firewall and the load balance configuration. You can change the Failover configuration and you can Load Balance between and among the interfaces. For example, you can create rules to send all http traffic through the WiFi Interface but never through the WAN ports. See Chapter 8.9.2. MWAN Configuration.***

This default configuration will work out-of-the-box for those with the RedPort WiFi Extender, a GSM connection and one or two satellite systems. If your setup differs from the default you will need to modify the Failover/Load Balancing configuration using the information in this chapter. There are examples of a few failover/load balancing configurations in *Chapter 8.9.5.*

8.9.1 MWAN Overview

The Interface Status screen shows you an at-a-glance view of which interfaces are currently online and which interfaces are offline. In addition, the MWAN Interface System Log shows the most recent log entries.



MWAN Interface Live Status

wan (eth0.1) Online (tracking active)

wan2 (eth0.3) Offline

wext (eth0.4) Online (tracking active)

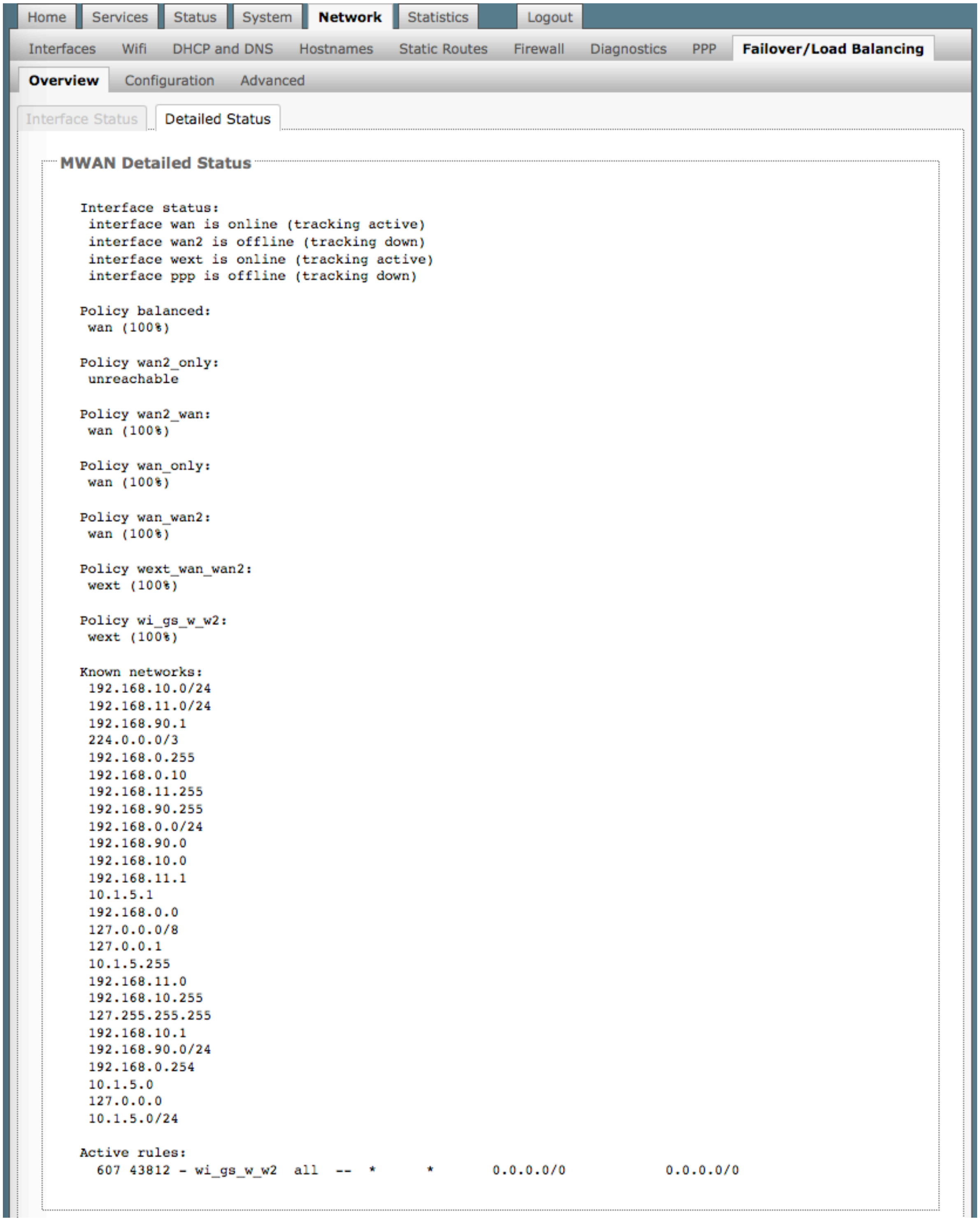
ppp (ppp0) Offline

MWAN Interface Systemlog

```
Last 50 MWAN systemlog entries. Newest entries sorted at the top :

Wed Mar 16 12:18:47 2016 user.info mwan3track: Lost 2 ping(s) on interface wext (eth0.4)
```

The Detailed Status screen shows more details of the current state of the rotuer.



MWAN Detailed Status

```
Interface status:
 interface wan is online (tracking active)
 interface wan2 is offline (tracking down)
 interface wext is online (tracking active)
 interface ppp is offline (tracking down)

Policy balanced:
 wan (100%)

Policy wan2_only:
 unreachable

Policy wan2_wan:
 wan (100%)

Policy wan_only:
 wan (100%)

Policy wan_wan2:
 wan (100%)

Policy wext_wan_wan2:
 wext (100%)

Policy wi_gs_w_w2:
 wext (100%)

Known networks:
 192.168.10.0/24
 192.168.11.0/24
 192.168.90.1
 224.0.0.0/3
 192.168.0.255
 192.168.0.10
 192.168.11.255
 192.168.90.255
 192.168.0.0/24
 192.168.90.0
 192.168.10.0
 192.168.11.1
 10.1.5.1
 192.168.0.0
 127.0.0.0/8
 127.0.0.1
 10.1.5.255
 192.168.11.0
 192.168.10.255
 127.255.255.255
 192.168.10.1
 192.168.90.0/24
 192.168.0.254
 10.1.5.0
 127.0.0.0
 10.1.5.0/24

Active rules:
  607 43812 - wi_gs_w_w2  all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

8.9.2 MWAN Configuration

The Optimizer Premier offers sophisticated Failover and Load Balancing options. You can block or allow certain traffic over one or more specific interfaces.

First, let's define the various components discussed in this section:

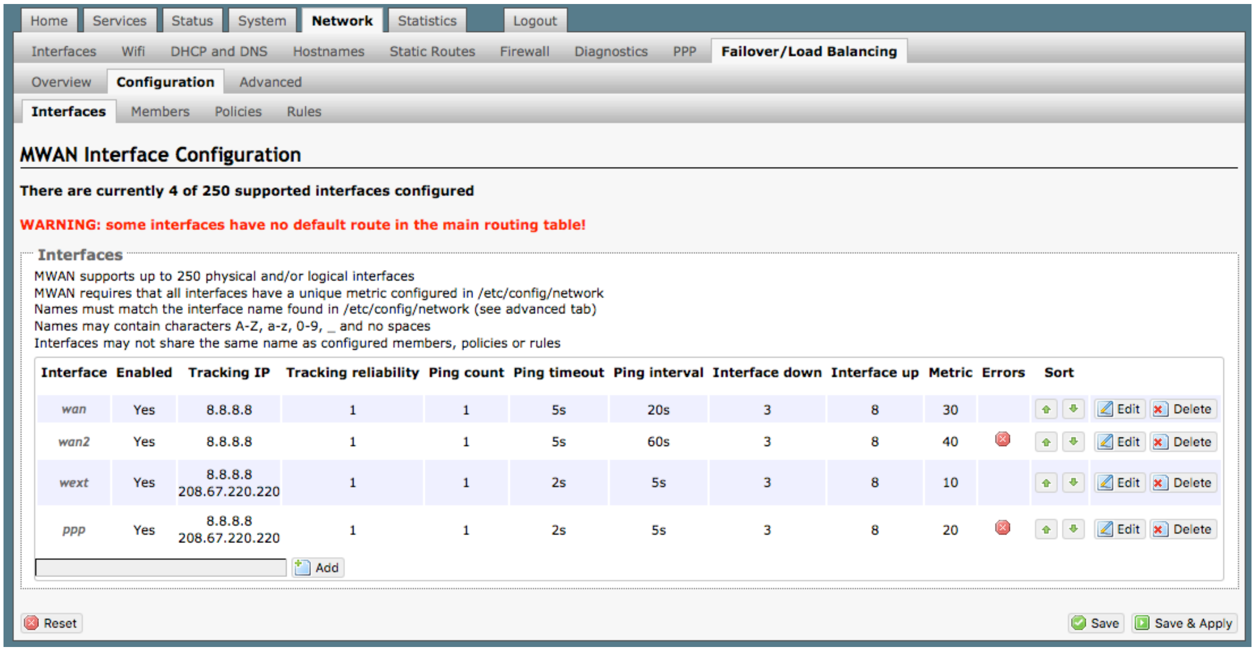
MWAN Interfaces: this is the connection "type" to the Internet. The default is four interfaces. *See Chapter 8.9.2.1.*

MWAN Members: these are profiles whereby each interface is assigned a level of importance relative to the other interfaces. The default is 16 members*. See Chapter 8.9.2.2.*

MWAN Policies: these are member groupings that control how traffic is distributed among the interfaces. The default is 7 policies. *See Chapter 8.9.2.3.*

MWAN Rules: these are rules that specify which traffic will use a particular interface. The default is 1 rule*. See Chapter 8.9.2.4.*

8.9.2.1 Interfaces



MWAN Interface Configuration

There are currently 4 of 250 supported interfaces configured

WARNING: some interfaces have no default route in the main routing table!

Interfaces

MWAN supports up to 250 physical and/or logical interfaces
MWAN requires that all interfaces have a unique metric configured in /etc/config/network
Names must match the interface name found in /etc/config/network (see advanced tab)
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Interfaces may not share the same name as configured members, policies or rules

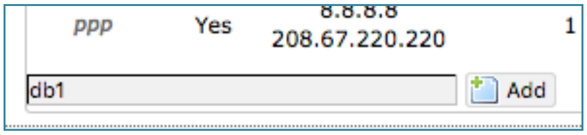
Interface	Enabled	Tracking IP	Tracking reliability	Ping count	Ping timeout	Ping interval	Interface down	Interface up	Metric	Errors	Sort			
wan	Yes	8.8.8.8	1	1	5s	20s	3	8	30		↑ ↓	Edit	Delete
wan2	Yes	8.8.8.8	1	1	5s	60s	3	8	40	⊗	↑ ↓	Edit	Delete
wext	Yes	8.8.8.8 208.67.220.220	1	1	2s	5s	3	8	10		↑ ↓	Edit	Delete
ppp	Yes	8.8.8.8 208.67.220.220	1	1	2s	5s	3	8	20	⊗	↑ ↓	Edit	Delete

An MWAN Interface represents the connection type to the Internet. The default interfaces are:

wan: the primary satellite device
wan2: the backup satellite device
wext: the WiFi Extender device
ppp: the ppp/gsm device

If you have added a new interface to Network > Interfaces *(see Chapter 8.1)* and want to include that new interface into the MWAN Failover/Load Balancing distribution it must be added to the MWAN Interface Configuration:

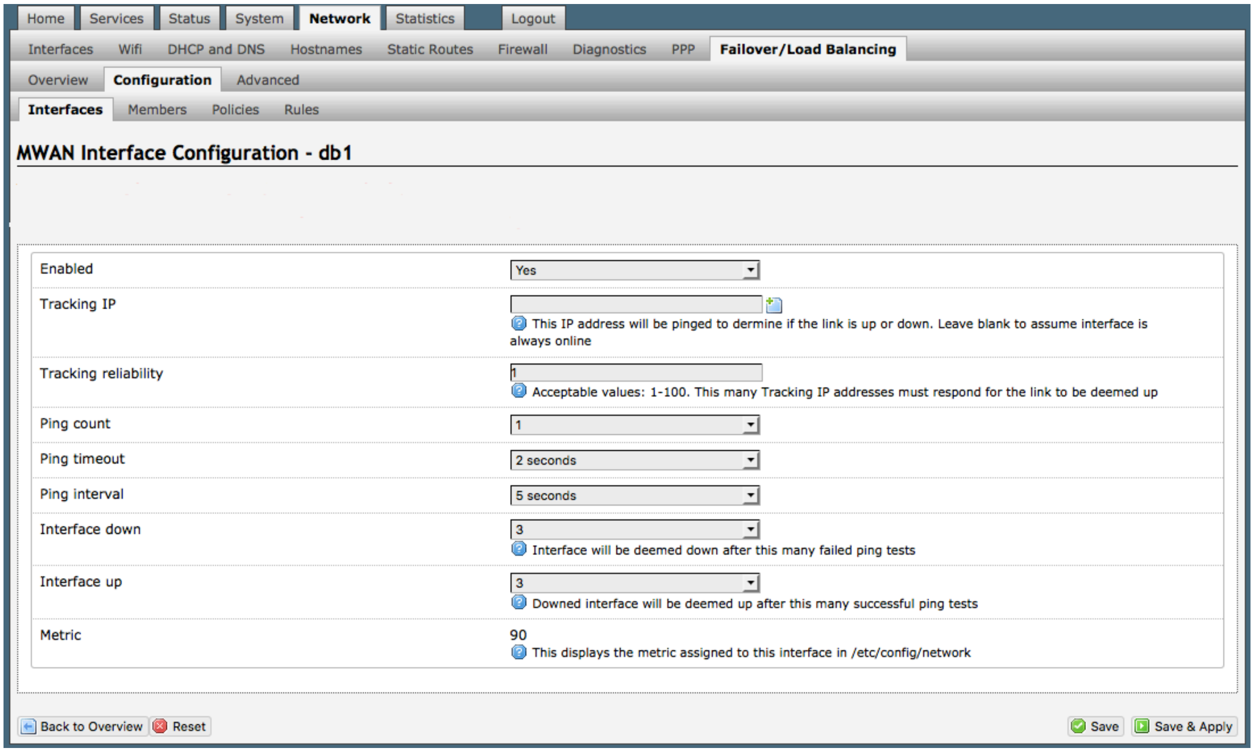
Enter the name of the interface into the text box and select <Add>.



ppp	Yes	8.8.8.8 208.67.220.220	1

db1

You may accept these settings as they are or modify if required.



MWAN Interface Configuration - db1

Enabled	Yes
Tracking IP	This IP address will be pinged to dermine if the link is up or down. Leave blank to assume interface is always online
Tracking reliability	1 Acceptable values: 1-100. This many Tracking IP addresses must respond for the link to be deemed up
Ping count	1
Ping timeout	2 seconds
Ping interval	5 seconds
Interface down	3 Interface will be deemed down after this many failed ping tests
Interface up	3 Downed interface will be deemed up after this many successful ping tests
Metric	90 This displays the metric assigned to this interface in /etc/config/network

Enabled: Yes to Enable, No to Disable this MWAN interface. The default is "Yes".

Tracking IP: IP address(es) to be pinged to determine if the link is up or down. If left blank, it is assumed the interface is always online. *Note: In some cases, it may be advantageous and more cost effective to track the IP address of the interface itself rather than an IP address on the Internet.*

Tracking reliability: Number of IP addresses (in Tracking IP above) that must respond in order for the link the be determined as Up. The default is "1".

Ping count: Number of pings to be sent in the ping burst. The default is "1".

Ping timeout: How long (in seconds) to wait to see if the ping fails. The default is "2". *Iridium Pilot users please see suggestions below.*

Ping interval: How long (in seconds) to wait between pings. *Iridium Pilot users please see suggestions below.*

Interface down: Number of failed responses before determing that the interface is Down.

Interface up: Number of successful responses before determining that the interface is Up.

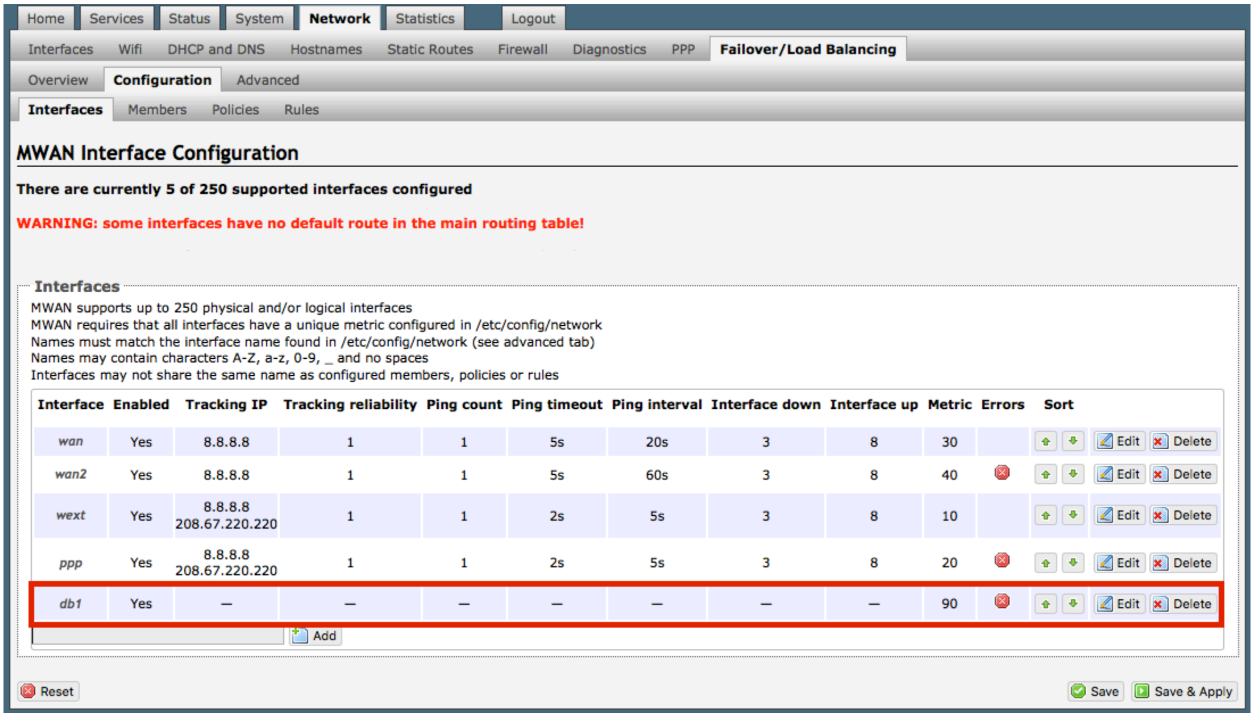
Metric: Read-only display of the gateway metric assigned to the interface when it was created in Network > Interfaces*. See Chapter 8.1.*

Select <Save & Apply>.

Some suggestions:

*When you have a **PPP interface** in the failover sequence you may want to set the Ping Timeout to 10 seconds, set the Ping Count to 2. The PPP interface has to come up at least once so the system knows that it is a viable interface, so it must ping at least once. In addition, you may want to change the Tracking IP to the IP of the router, so you are pinging yourself instead of pinging an address on the Internet.*

For Iridium Pilot Users:
*The default settings for wan2 is Ping Timeout = 5 seconds and Ping Interval = 1 minute. This is designed to keep bandwidth usage low. If you have an **Iridium Pilot** as your wan2 interface, however, these settings are not helpful because the Pilot automatically goes offline after 20 seconds of idle time and it takes about 10-15 seconds to bring it back online. Doing a ping every minute with a 5 second timeout is most likely to fail. Changing the Tracking IP to the IP Address of the Pilot unit itself assures that the ping will always work so the interface will show as available for failover. With wan2 at the end of your failover sequence, this tricks the Optimizer into believing there is connectivity, minimizing bandwidth usage.*



MWAN Interface Configuration

There are currently 5 of 250 supported interfaces configured

WARNING: some interfaces have no default route in the main routing table!

Interfaces

MWAN supports up to 250 physical and/or logical interfaces
MWAN requires that all interfaces have a unique metric configured in /etc/config/network
Names must match the interface name found in /etc/config/network (see advanced tab)
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Interfaces may not share the same name as configured members, policies or rules

Interface	Enabled	Tracking IP	Tracking reliability	Ping count	Ping timeout	Ping interval	Interface down	Interface up	Metric	Errors	Sort		
wan	Yes	8.8.8.8	1	1	5s	20s	3	8	30		⬆ ⬇	Edit	Delete
wan2	Yes	8.8.8.8	1	1	5s	60s	3	8	40	✖	⬆ ⬇	Edit	Delete
wext	Yes	8.8.8.8 208.67.220.220	1	1	2s	5s	3	8	10		⬆ ⬇	Edit	Delete
ppp	Yes	8.8.8.8 208.67.220.220	1	1	2s	5s	3	8	20	✖	⬆ ⬇	Edit	Delete
db1	Yes	–	–	–	–	–	–	–	90	✖	⬆ ⬇	Edit	Delete

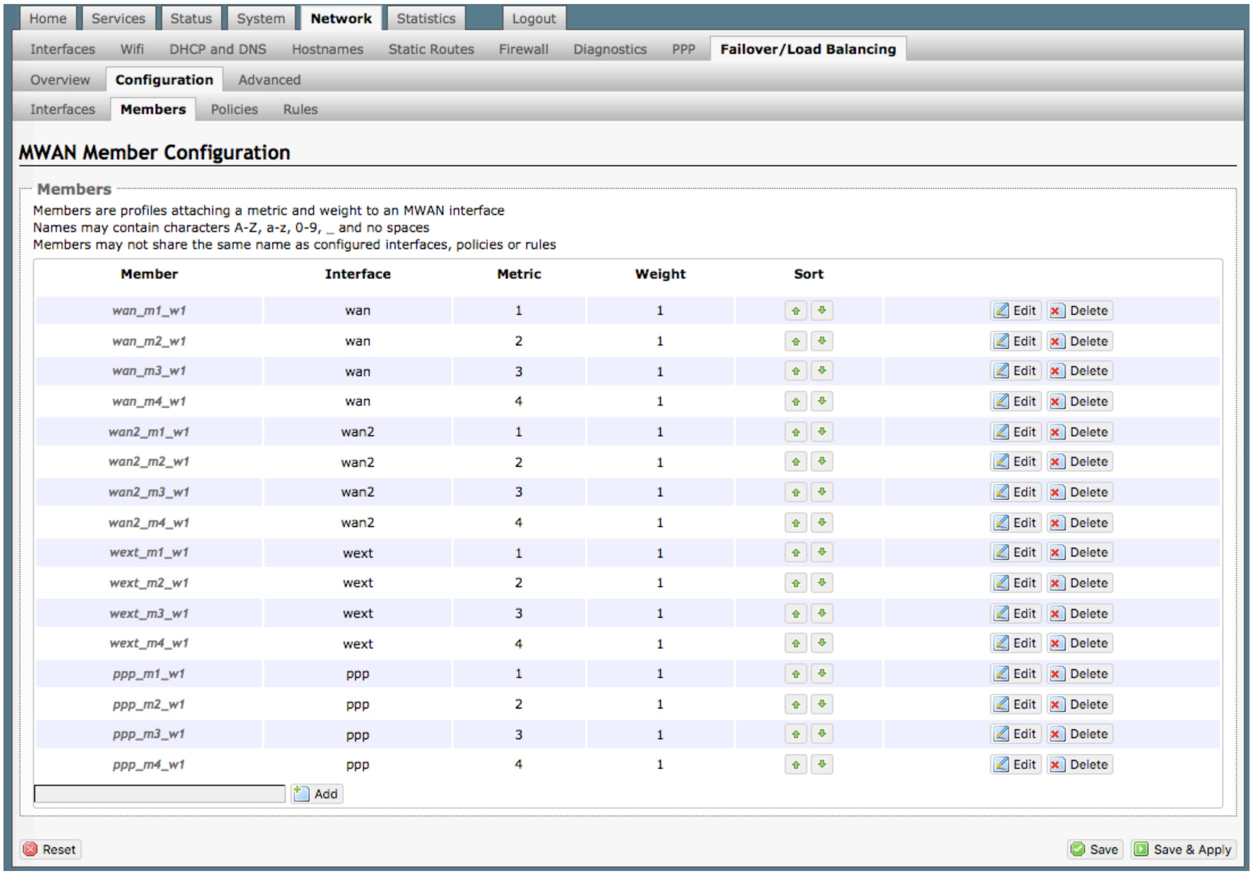
The new MWAN Interface is now available for Failover/Load Balancing configuration.

Use the <Edit> button to edit a MWAN Interface.

Use the <Delete> button to remove a MWAN Interface. ***The Delete action cannot be undone.***

8.9.2.2 Members

Each MWAN Interface should have one or more Member profiles.



MWAN Member Configuration

Members

Members are profiles attaching a metric and weight to an MWAN interface
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Members may not share the same name as configured interfaces, policies or rules

Member	Interface	Metric	Weight	Sort	
wan_m1_w1	wan	1	1	↑ ↓	Edit Delete
wan_m2_w1	wan	2	1	↑ ↓	Edit Delete
wan_m3_w1	wan	3	1	↑ ↓	Edit Delete
wan_m4_w1	wan	4	1	↑ ↓	Edit Delete
wan2_m1_w1	wan2	1	1	↑ ↓	Edit Delete
wan2_m2_w1	wan2	2	1	↑ ↓	Edit Delete
wan2_m3_w1	wan2	3	1	↑ ↓	Edit Delete
wan2_m4_w1	wan2	4	1	↑ ↓	Edit Delete
wext_m1_w1	wext	1	1	↑ ↓	Edit Delete
wext_m2_w1	wext	2	1	↑ ↓	Edit Delete
wext_m3_w1	wext	3	1	↑ ↓	Edit Delete
wext_m4_w1	wext	4	1	↑ ↓	Edit Delete
ppp_m1_w1	ppp	1	1	↑ ↓	Edit Delete
ppp_m2_w1	ppp	2	1	↑ ↓	Edit Delete
ppp_m3_w1	ppp	3	1	↑ ↓	Edit Delete
ppp_m4_w1	ppp	4	1	↑ ↓	Edit Delete

There are 16 default Members (four profiles for each of the four default interfaces).

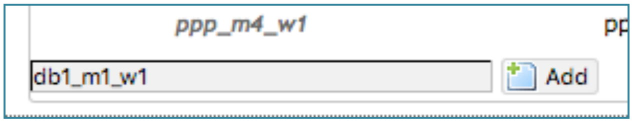
Each Member is assigned a Metric and a Weight.

The Metric hierarchy is lowest number to highest number; therefore Metric 1 (m1) has a higher standing than Metric 2 (m2), etc.

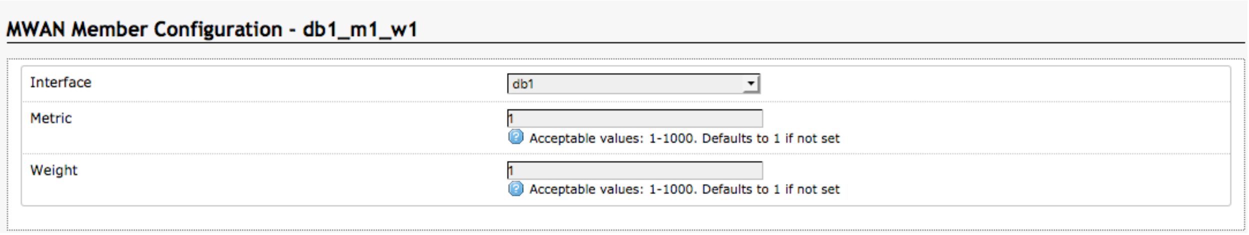
The Weight hierarchy is the reverse; highest number to lowest number; therefore Weight 4 (w4) has a higher standing than Weight 3 (w3), etc.

Metric and Weight play an important role in controlling the distribution of traffic. *See Chapter 8.9.2.3 Policies.*

To add a new Member, enter the Member name in the text box and select <Add>.



When creating new Members it is a good idea to include the metric number and weight number in the Member name for easy identification on the page.

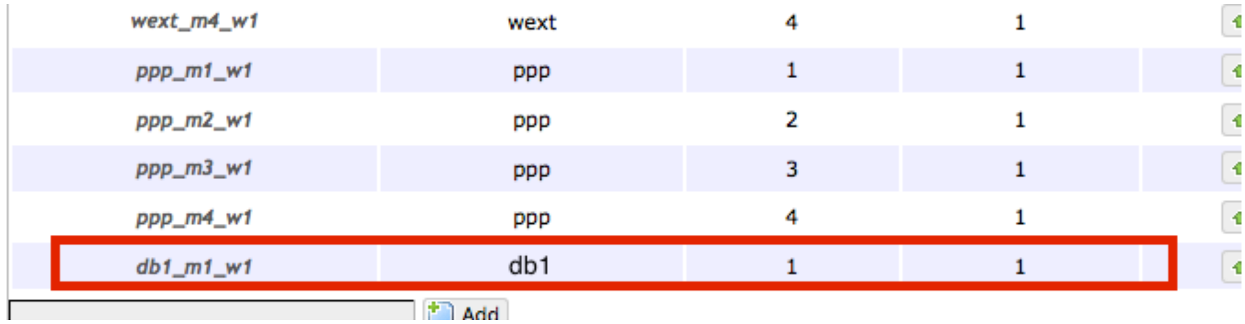


MWAN Member Configuration - db1_m1_w1

Interface	db1
Metric	1 Acceptable values: 1-1000. Defaults to 1 if not set
Weight	1 Acceptable values: 1-1000. Defaults to 1 if not set

Select the MWAN Interface associated with this Member and assign a Metric (1-4) and a Weight (4-1).

Select <Save & Apply>.



wext_m4_w1	wext	4	1
ppp_m1_w1	ppp	1	1
ppp_m2_w1	ppp	2	1
ppp_m3_w1	ppp	3	1
ppp_m4_w1	ppp	4	1
db1_m1_w1	db1	1	1

The new Member now appears on the list.

Use the <Edit> button to edit a Member.

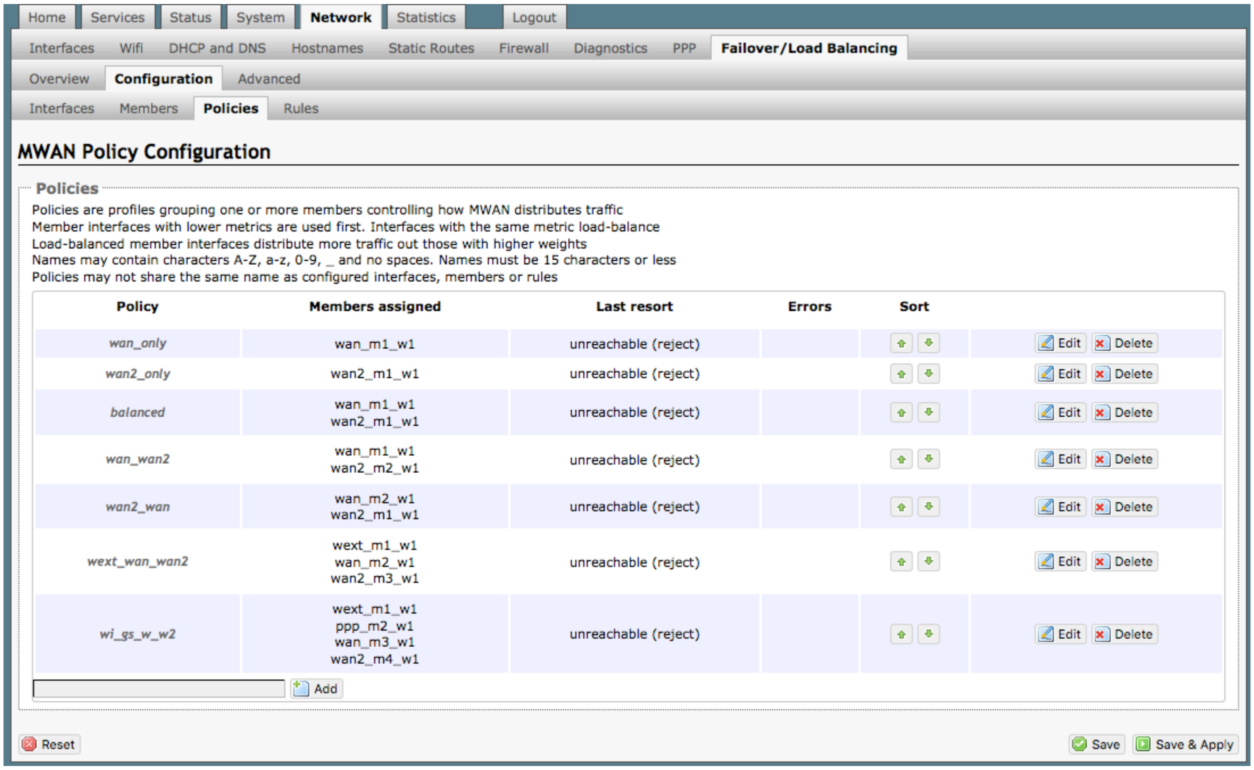
Use the <Delete> button to remove a Member. ***The Delete action cannot be undone.***

8.9.2.3 Policies

Policies are groupings of members. Each policy must have one or more members. As you create Rules *(see Chapter 8.9.2.4)* you must assign the rule to one of these policies.

These policies will be used to control how MWAN distributes traffic.

There are 7 default Policies:



MWAN Policy Configuration

Policies

Policies are profiles grouping one or more members controlling how MWAN distributes traffic
Member interfaces with lower metrics are used first. Interfaces with the same metric load-balance
Load-balanced member interfaces distribute more traffic out those with higher weights
Names may contain characters A-Z, a-z, 0-9, _ and no spaces. Names must be 15 characters or less
Policies may not share the same name as configured interfaces, members or rules

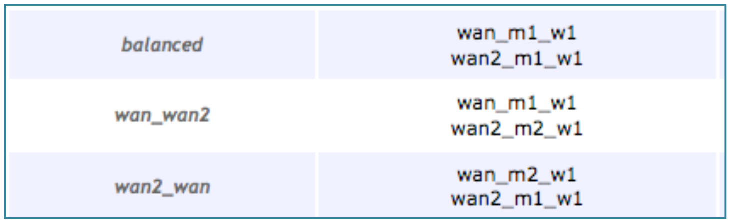
Policy	Members assigned	Last resort	Errors	Sort	
wan_only	wan_m1_w1	unreachable (reject)		⇧ ⇩	Edit Delete
wan2_only	wan2_m1_w1	unreachable (reject)		⇧ ⇩	Edit Delete
balanced	wan_m1_w1 wan2_m1_w1	unreachable (reject)		⇧ ⇩	Edit Delete
wan_wan2	wan_m1_w1 wan2_m2_w1	unreachable (reject)		⇧ ⇩	Edit Delete
wan2_wan	wan_m2_w1 wan2_m1_w1	unreachable (reject)		⇧ ⇩	Edit Delete
wext_wan_wan2	wext_m1_w1 wan_m2_w1 wan2_m3_w1	unreachable (reject)		⇧ ⇩	Edit Delete
wi_gs_w_w2	wext_m1_w1 ppp_m2_w1 wan_m3_w1 wan2_m4_w1	unreachable (reject)		⇧ ⇩	Edit Delete

When there is only one Member assigned to a Policy, all traffic matching the Rule will flow thru the one interface.

When multiple Members are assigned to a policy, the traffic will be distributed based on the Metric and Weight of the Members assigned.

Here are some examples:

balanced: because the Metric is 1 for both Member profiles, 1/2 the traffic will flow thru the wan interface and 1/2 the traffic will flow thru the wan2 interface.



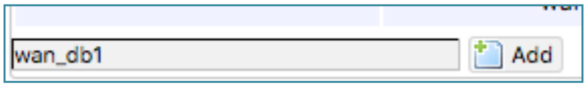
balanced	wan_m1_w1 wan2_m1_w1
wan_wan2	wan_m1_w1 wan2_m2_w1
wan2_wan	wan_m2_w1 wan2_m1_w1

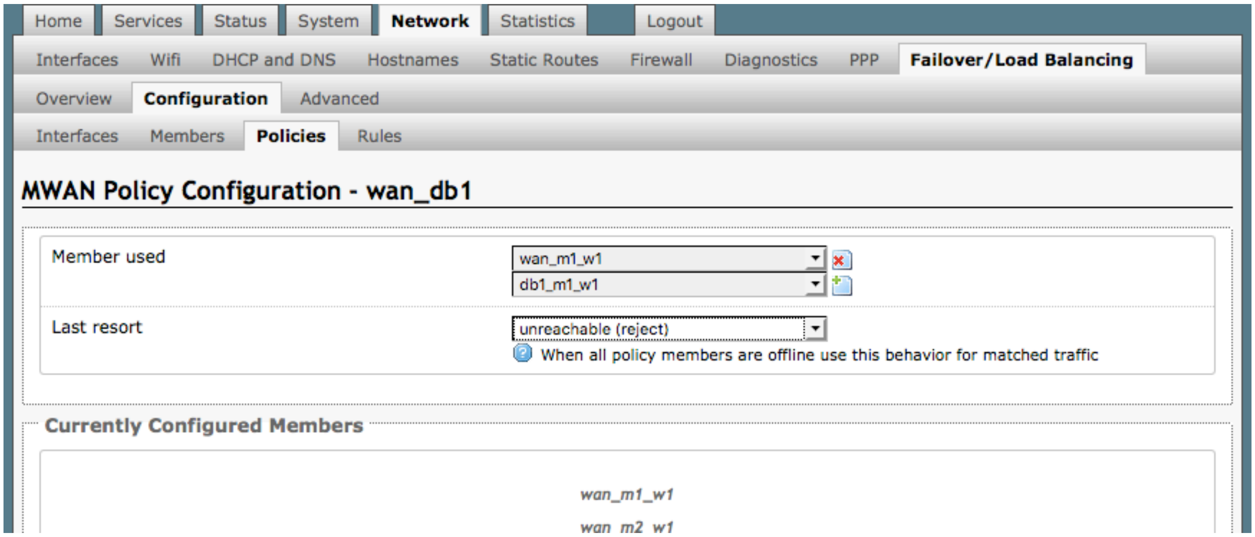
wan_wan2: because the Metric is 1 for the wan and the Metric is 2 for the wan2 and the Weight is 1 for both; all traffic will flow thru the wan interface if it is Active. If the wan interface is not available, the traffic will automatically failover to the wan2 interface.

wan2_wan: this policy is the reverse of the one above. All traffic will flow thru the wan2 interface if it is active and if not, it will failover to the wan interface.

wan_heavy: This example is not on the default list but helps further explain how Metric and Weight are applied. In the fictional Policy "wan_heavy" there are two Members assigned to it: "wan_m1_w4" and "wan2_m1_w1". This looks alot like the balanced policy, however, because the Weight value is higher for the wan interface (w4) than it is for the wan2 interface (w1), the wan interface will pass more traffic than the wan2 interface. On average, for every four packets that flow thru the wan, only one packet will flow thru the wan2.

To add a new Policy, enter the new Policy name in the text box and select <Add>.


wan_db1



MWAN Policy Configuration - wan_db1

Member used: wan_m1_w1, db1_m1_w1

Last resort: unreachable (reject)

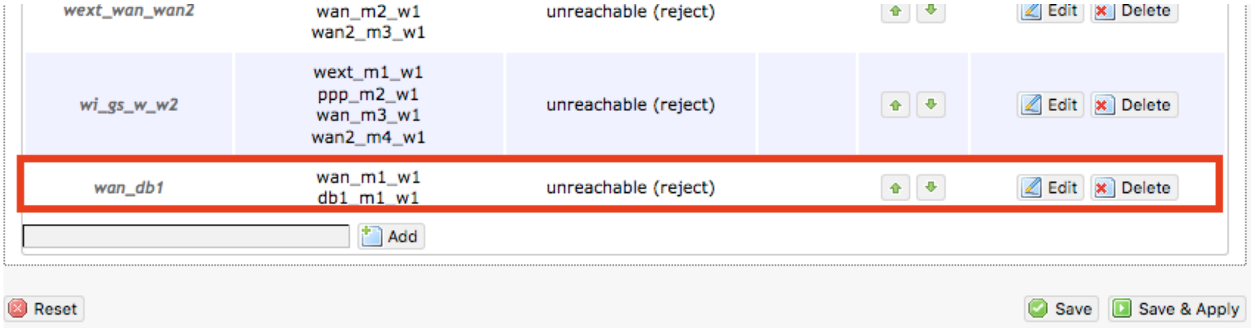
When all policy members are offline use this behavior for matched traffic

Currently Configured Members

wan_m1_w1

wan_m2_w1

Using the drop-down list, select one or more Members to assign to the new Policy in accordance with how you want traffic distributed when a Rule invokes this Policy. Select <Save & Apply>.



wext_wan_wan2	wan_m2_w1 wan2_m3_w1	unreachable (reject)		↑ ↓	Edit Delete
wi_gs_w_w2	wext_m1_w1 ppp_m2_w1 wan_m3_w1 wan2_m4_w1	unreachable (reject)		↑ ↓	Edit Delete
wan_db1	wan_m1_w1 db1_m1_w1	unreachable (reject)		↑ ↓	Edit Delete

The new Policy now appears on the list. Notice that when this Policy is used traffic will be balanced between wan interface and the db1 interface.

Use the <Edit> button to edit a Policy.

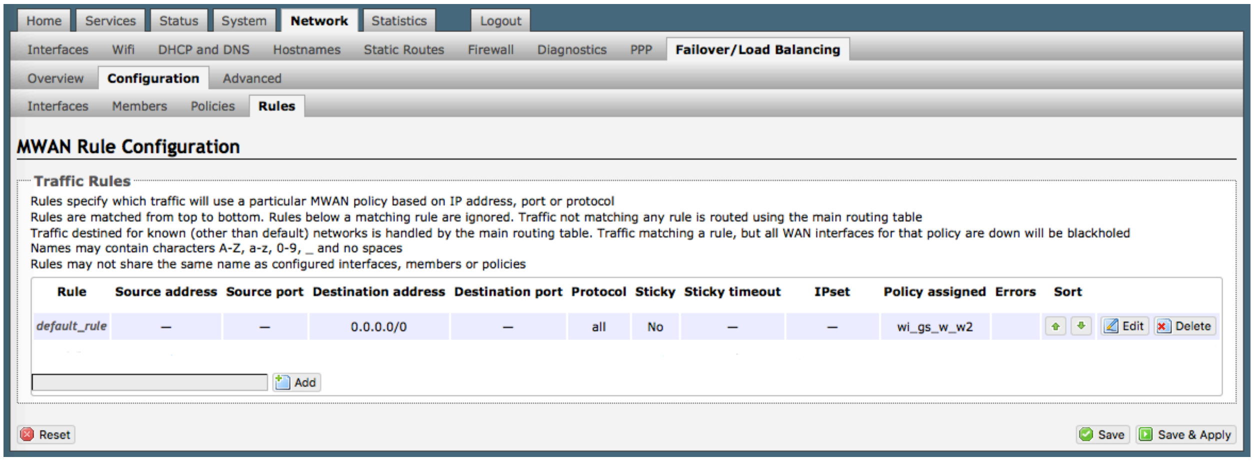
Use the <Delete> button to remove a Policy. ***The Delete action cannot be undone.***

8.9.2.4 Rules

Rules allow you flexibility in the distribution of MWAN traffic. They can be based on IP address, port, or protocol.

Rules are matched from top to bottom. When a Rule is matched, the rules below that match are ignored. If traffic does not match any rule, it is routed to the main routing table. (The main routing table can be found in under the Status Tab > Routes.) If traffic does match a rule, but the interface is down for that policy, the traffic will be blackholed.

There is one default rule:



MWAN Rule Configuration

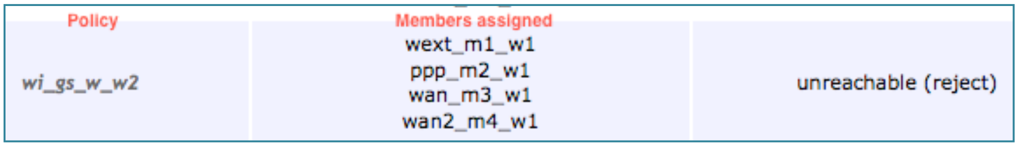
Traffic Rules

Rules specify which traffic will use a particular MWAN policy based on IP address, port or protocol
Rules are matched from top to bottom. Rules below a matching rule are ignored. Traffic not matching any rule is routed using the main routing table
Traffic destined for known (other than default) networks is handled by the main routing table. Traffic matching a rule, but all WAN interfaces for that policy are down will be blackholed
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Rules may not share the same name as configured interfaces, members or policies

Rule	Source address	Source port	Destination address	Destination port	Protocol	Sticky	Sticky timeout	IPset	Policy assigned	Errors	Sort	
default_rule	–	–	0.0.0.0/0	–	all	No	–	–	wi_gs_w_w2		⬆ ⬇	Edit Delete

With this Default Rule, any traffic FROM any source and TO any destination (i.e. ALL traffic) will use the Policy "wi_gs_w_w2".

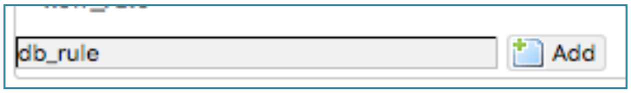
Taking a look at the Policy "wi_gs_w_w2" we can see the Members assigned to this policy and determine the failover/load balancing sequence. Because the Weight value is 1 (w1) for each Member this means that all traffic will be routed through the "wext" interface if it is up. If "wext" is down, all traffic will be routed through the "ppp" interface if it is configured and up. If the "ppp" interface is down then all traffic will be routed through the "wan" interface, if it is up. If the "wan" interface is down then all traffic will be routed through the "wan2" interface, if it is up. If the "wan2" interface is down then all traffic will be blackholed.

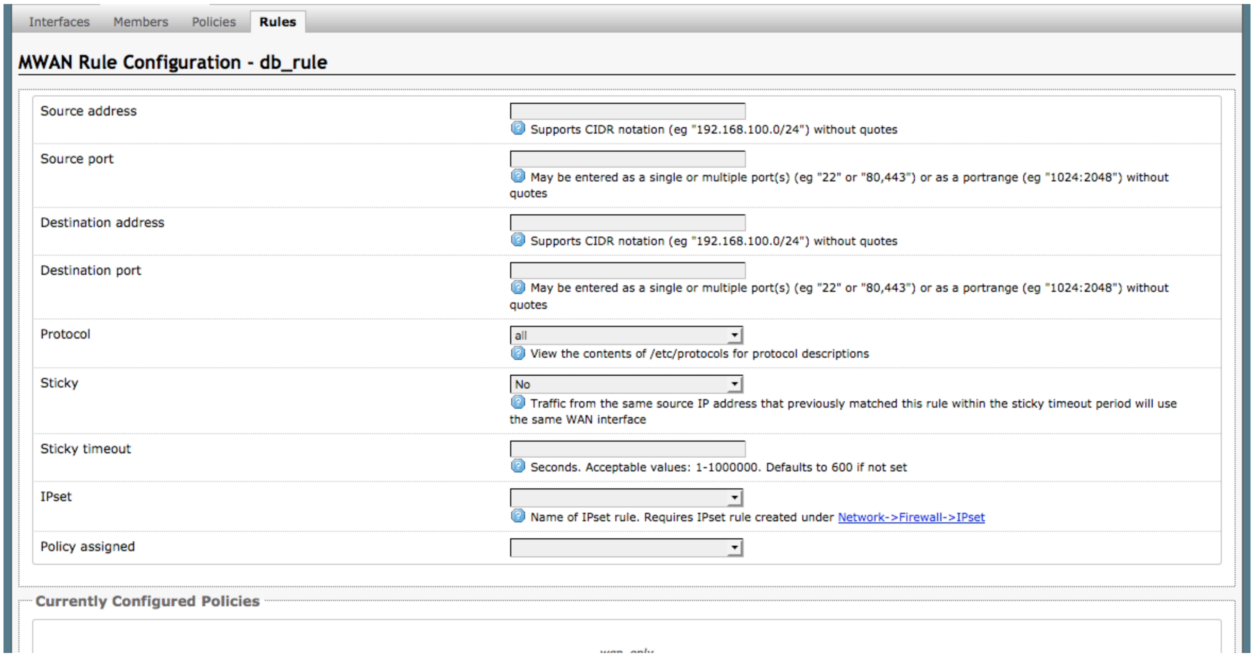


Policy	Members assigned	
wi_gs_w_w2	wext_m1_w1 ppp_m2_w1 wan_m3_w1 wan2_m4_w1	unreachable (reject)

If the Weight values varied traffic would be allocated among the interfaces in accordance with the Weight values assigned to the Members.

To add a new Rule, enter the new Rule name in the text box and select <Add>.


db_rule



MWAN Rule Configuration - db_rule

Source address	Supports CIDR notation (eg "192.168.100.0/24") without quotes
Source port	May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes
Destination address	Supports CIDR notation (eg "192.168.100.0/24") without quotes
Destination port	May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes
Protocol	all View the contents of /etc/protocols for protocol descriptions
Sticky	No Traffic from the same source IP address that previously matched this rule within the sticky timeout period will use the same WAN interface
Sticky timeout	Seconds. Acceptable values: 1-1000000. Defaults to 600 if not set
IPset	Name of IPset rule. Requires IPset rule created under Network->Firewall->IPset
Policy assigned	

Currently Configured Policies

Complete this screen in accordance with the Rule you want to create:

Source address: Restrict incoming traffic arriving from a specific IP address or range.

Source port: Restrict incoming traffic arriving from a certain port or multiple ports.

Destination address: Restrict outgoing traffic to a specific IP address or range.

Destination port: Restrict outgoing traffic to a specific port or multiple ports.

Protocol: Restrict only traffic of a cetain protocol, select from the drop-down list, or select --custom-- and enter the protocol here.

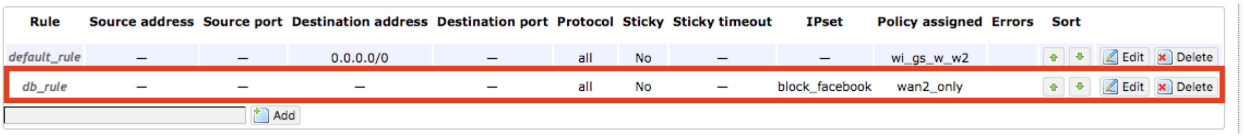
Sticky: This is important for smooth traffic flow when load-balancing among interfaces with different Weight values. With <Yes> selected, once connected, the same interface will be used for that traffic up to the Sticky Timeout period.

Sticky Timeout: This is like an idle timeout period. If Sticky is set to <Yes> above, Sticky Timeout represents the number of seconds the system will wait for more traffic to flow thru the specific interface. Once the Sticky Timeout period is reached it will revert back to the original load balance configuration.

IPset: If you have an IPset defined in Network > Firewall > IPset (see section xx.xx), you can restrict traffic to that location by selecting the IPSet rule from the drop down list.

Policy assigned: Select which Policy you want this Rule assigned to using the drop down menu. ***Every Rule MUST be assigned to a Policy.***

Select <Save & Apply>.



Rule	Source address	Source port	Destination address	Destination port	Protocol	Sticky	Sticky timeout	IPset	Policy assigned	Errors	Sort		
default_rule	–	–	0.0.0.0/0	–	all	No	–	–	wi_gs_w_w2		⇧ ⇩	Edit	Delete
db_rule	–	–	–	–	all	No	–	block_facebook	wan2_only		⇧ ⇩	Edit	Delete

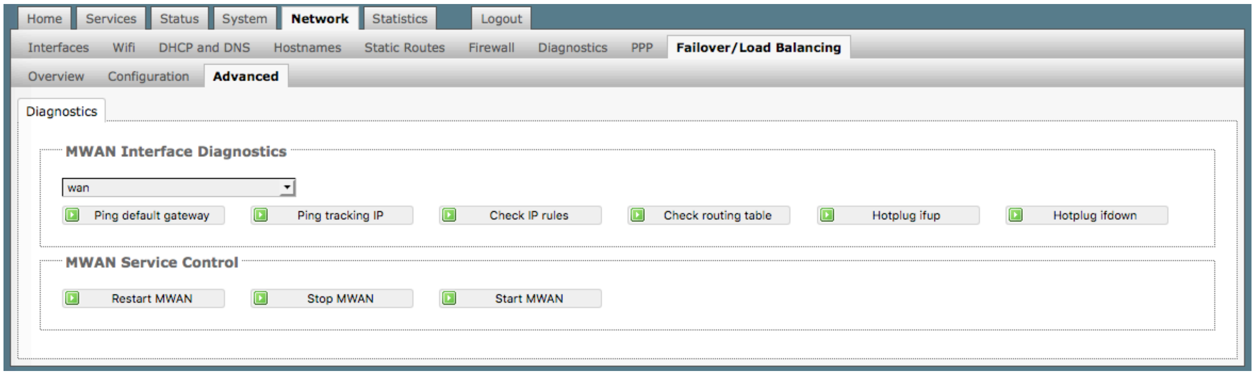
The new rule now appears on the list. This Rule will never allow facebook traffic over the wan2 interface. However, in order for the Rule to apply, it must be moved up the list using the Sort Up button so that it appears before the default rule that allows all traffic.

Use the <Edit> button to edit a Rule.

Use the <Delete> button to remove a Rule. ***The Delete action cannot be undone.***

8.9.3 Advanced

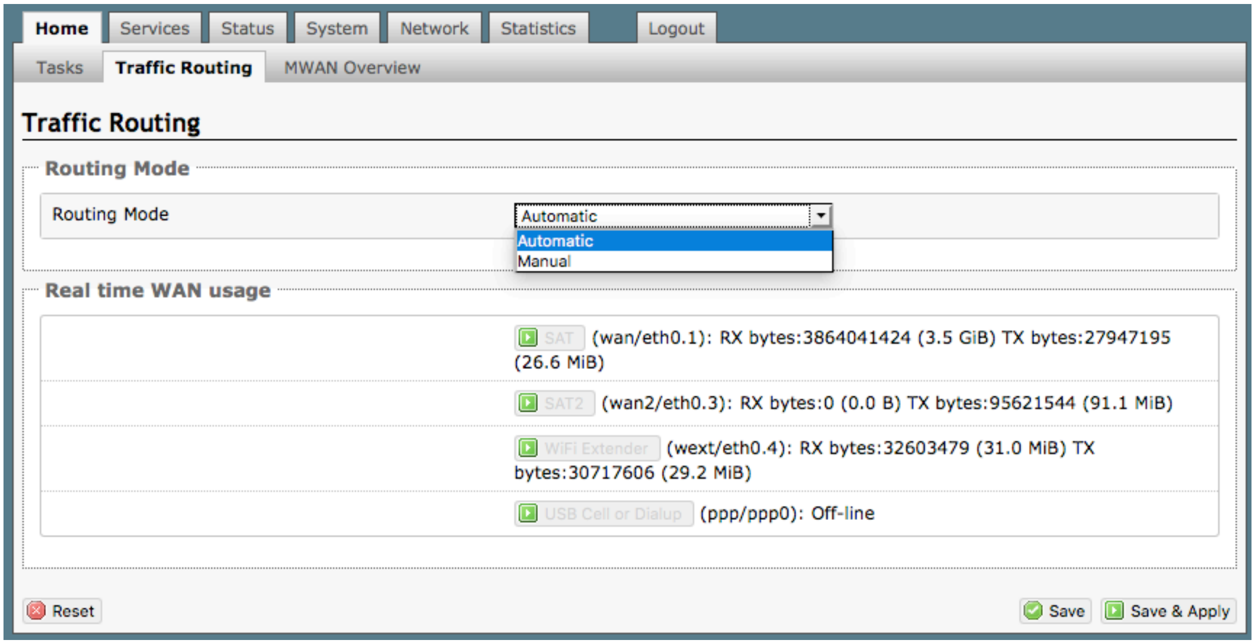
Select the MWAN Interface using the drop down list and run diagnostics for that interface.



Use MWAN Service Control to manually bring up or take down interfaces.

8.9.4 Failover Mode - Automatic or Manual

There are two Failover modes available:



Traffic Routing

Routing Mode

Routing Mode: Automatic

Real time WAN usage

SAT (wan/eth0.1): RX bytes:3864041424 (3.5 GiB) TX bytes:27947195 (26.6 MiB)

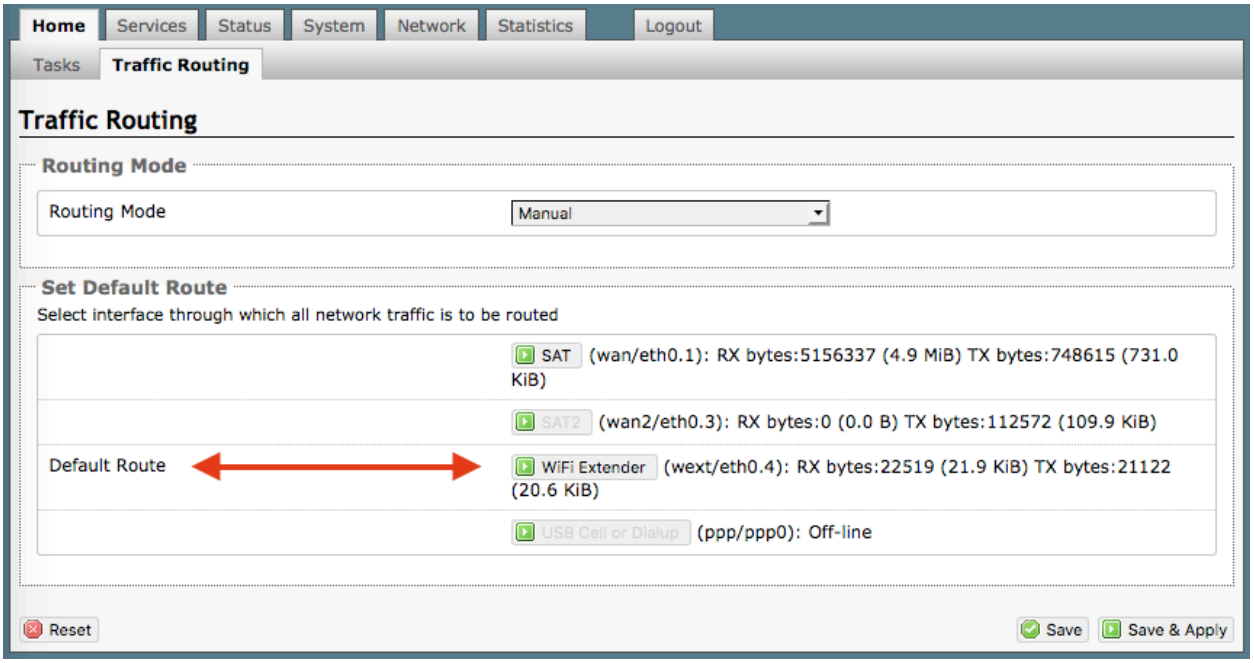
SAT2 (wan2/eth0.3): RX bytes:0 (0.0 B) TX bytes:95621544 (91.1 MiB)

WiFi Extender (wext/eth0.4): RX bytes:32603479 (31.0 MiB) TX bytes:30717606 (29.2 MiB)

USB Cell or Dialup (ppp/ppp0): Off-line

Automatic Failover (default setting) requires no intervention; if a MWAN interface is unavailable, traffic will automatically by routed per the Failover/Load Balancing Rules. Real time WAN usage is also displayed on this screen.

Manual Failover requires the "superadmin" or "admin" to select which available interface to use for ALL traffic. Real time WAN usage is also displayed on this screen. Only available interfaces can be enabled. Unavailable interfaces with no route to the Internet are disabled. In the screen below, only <SAT> and <WiFi Extender> are available routes. Only one can be selected. The "Default Route" designation indicates which interface is currently routing traffic.



Traffic Routing

Routing Mode

Routing Mode: Manual

Set Default Route

Select interface through which all network traffic is to be routed

Default Route

SAT (wan/eth0.1): RX bytes:5156337 (4.9 MiB) TX bytes:748615 (731.0 KiB)

SAT2 (wan2/eth0.3): RX bytes:0 (0.0 B) TX bytes:112572 (109.9 KiB)

WiFi Extender (wext/eth0.4): RX bytes:22519 (21.9 KiB) TX bytes:21122 (20.6 KiB)

USB Cell or Dialup (ppp/ppp0): Off-line

Some Important Things to Know:

- Only the 'superadmin' login can change the Failover Traffic Routing mode.
- The "admin" login displays the Failover Traffic Routing mode as read-only.
- Real time usage for each interface is displayed in either automatic or manual mode.
- The currently selected Default Route only displays in Manual mode.
- When set to Manual mode both "superadmin" and "admin" logins can select which interface to use for routing.

8.9.5 Failover/Load Balancing Scenarios

The scenarios below represent some commonly requested configurations.

8.9.5.1 Satcomm setup is a FleetBroadband Terminal, a handheld satphone like an Iridium 9555 and a WiFi Extender.

A more useful Failover configuration may be: wifi > fbb > ppp.

1. Configure the PPP interface for the Iridium 9555 satphone under Network > PPP *(See Chaper 8.8).*

2. Connect the Iridium satphone to the Optimizer Premier's USB port with the appropriate cable.

3. Create a MWAN Policy in Network > Failover/Load Balancing > Configuration > Policies *(See Chapter 8.9.2.3).*

   The Policy might be named "wext_wan_ir".

   The Members Assigned should be "wext_m1_w1", "wan_m1_w1" and "ppp_m1_w1".

4. Create a MWAN Rule in Network > Failover/Load Balancing > Configuration > Rules *(see Chapter 8.9.2.4).* Give the rule a unique name.

   When defining the Rule, the only field that requires an entry is the Policy Assigned field.

   Select the Policy name that you created in step 3 "wext_wan_ir".

5. Move this new Rule to the top of the list using the Sort Up button.

With this setup, all traffic will flow thru the RedPort WiFi Extender interface, if it is up. If the WiFi Extender is not up, all traffic will flow thru the FleetBroadband satellite terminal, if it is up. If the FBB is not up, all traffic will flow thru the Iridium 9555.

8.9.5.2 Allow all http traffic thru the WiFi interface only and never through the satellite terminal.

Use the following to restrict all http traffic to the WiFi interface only.

1. Create a MWAN Policy in Network > Failover/Load Balancing > Configuration > Policies *(See Chapter 8.9.2.3).*

   The Policy might be named "wifionly".

   The Members Assigned should be "wext_m1_w1".

   Last resort should be set to "reject" as you do not want the last resort to route through the default rule.

2. Create a MWAN Rule in Network > Failover/Load Balancing > Configuration > Rules *(see Chapter 8.9.2.4).* Give the rule a unique name.

   When defining the Rule, set:

   Destination Port = 80,443

   Protocol = tcp

   Policy Assigned = select the Policy name that you created in step 1 "wifionly"

3. Move this new Rule to the top of the list using the Sort Up button.

With this setup, all http traffic (i.e. port 80 and port 443) will flow thru the RedPort WiFi Extender interface only, if it is up. If the WiFi Extender is not up, all http traffic will be rejected.

8.9.5.3 How to Block Skype or other P2P applications

Skype and other Peer-to-Peer Applications are designed to circumvent firewalls allowing users to communicate and share data. They consume a lot of satellite airtime resources and are very difficult to block. In order to block Skype or other Peer-to-Peer Applications you must configure the firewall to block all traffic and then route all http and https traffic through Optimizer Premier Proxy Server that allows you to Block sites. The Captive Portal must be Enabled.

This configuration blocks all traffic to the Internet. Users must login through the Captive Portal to have access to http and https traffic.

1. Captive Portal must be enabled. *(See Chapter 5.1)*

2. Go to Services > Web Compression and Filtering > Filters to enter the sites you wish to block. *(See Chapter 5.2.2)*

3. Go to Network > Firewall > Firewall Rules and disable (uncheck) these six rules:

ALL
PASS DNS
DNS
HTTP
HTTPS
FTP

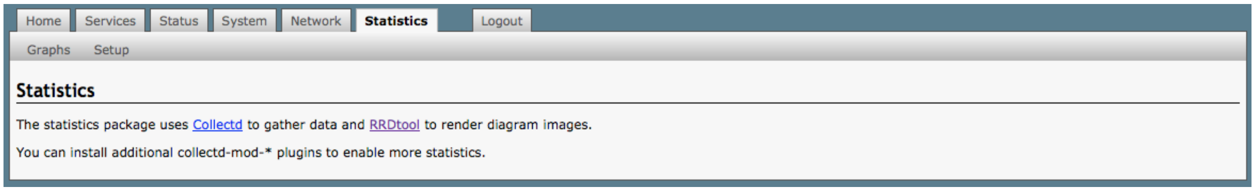
4. Select <Save & Apply>. This will modify the firewall to block acces to all traffic, including DNS.

5. The web browser configuration of each end user's device must be modified to enable "Automatic Proxy Detection." (PC users with Firefox do this in Preferences > Advanced > Network > Settings by selecting "Auto-detect proxy settings for this network". Other browsers can be configured similarly.)

6. Users will login to the Captive Portal by entering: http://10.1.5.1:4990/www/login.chi

9.0 Statistics

Requires "superadmin" login



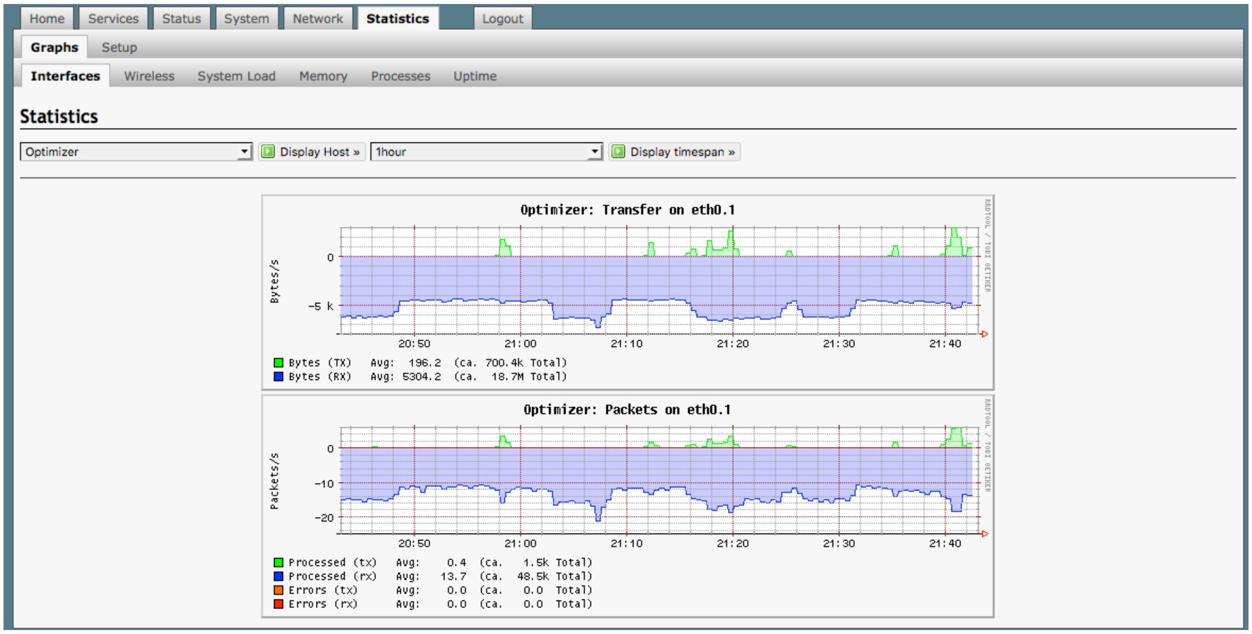
Statistics

The statistics package uses Collectd to gather data and RRDtool to render diagram images.

You can install additional collectd-mod-* plugins to enable more statistics.

9.1 Graphs

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



Statistics

Optimizer ▾ | 1hour ▾

```
🟩 Bytes (TX)   Avg:  196.2  (ca. 700.4k Total)
🟦 Bytes (RX)   Avg: 5304.2  (ca.  18.7M Total)
```

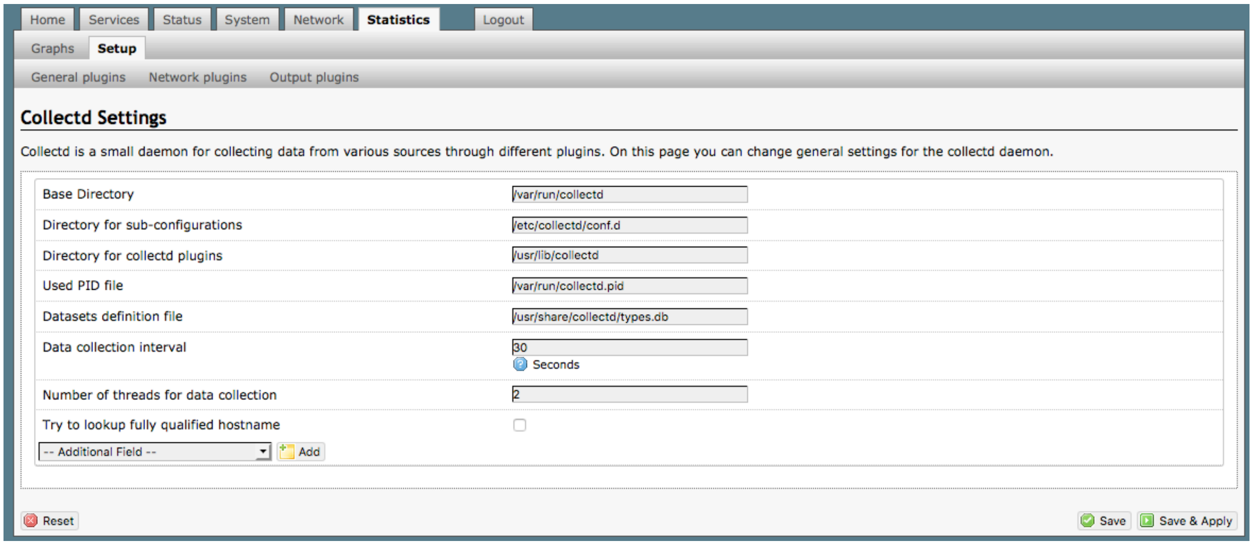
```
🟩 Processed (tx)   Avg:    0.4  (ca.   1.5k Total)
🟦 Processed (rx)   Avg:   13.7  (ca.  48.5k Total)
🟧 Errors (tx)      Avg:    0.0  (ca.   0.0  Total)
🟥 Errors (rx)      Avg:    0.0  (ca.   0.0  Total)
```

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

9.2 Setup

The Optimizer Premier uses several tools for collecting data statistics.

Use Setup to change general settings for the collectd daemon.



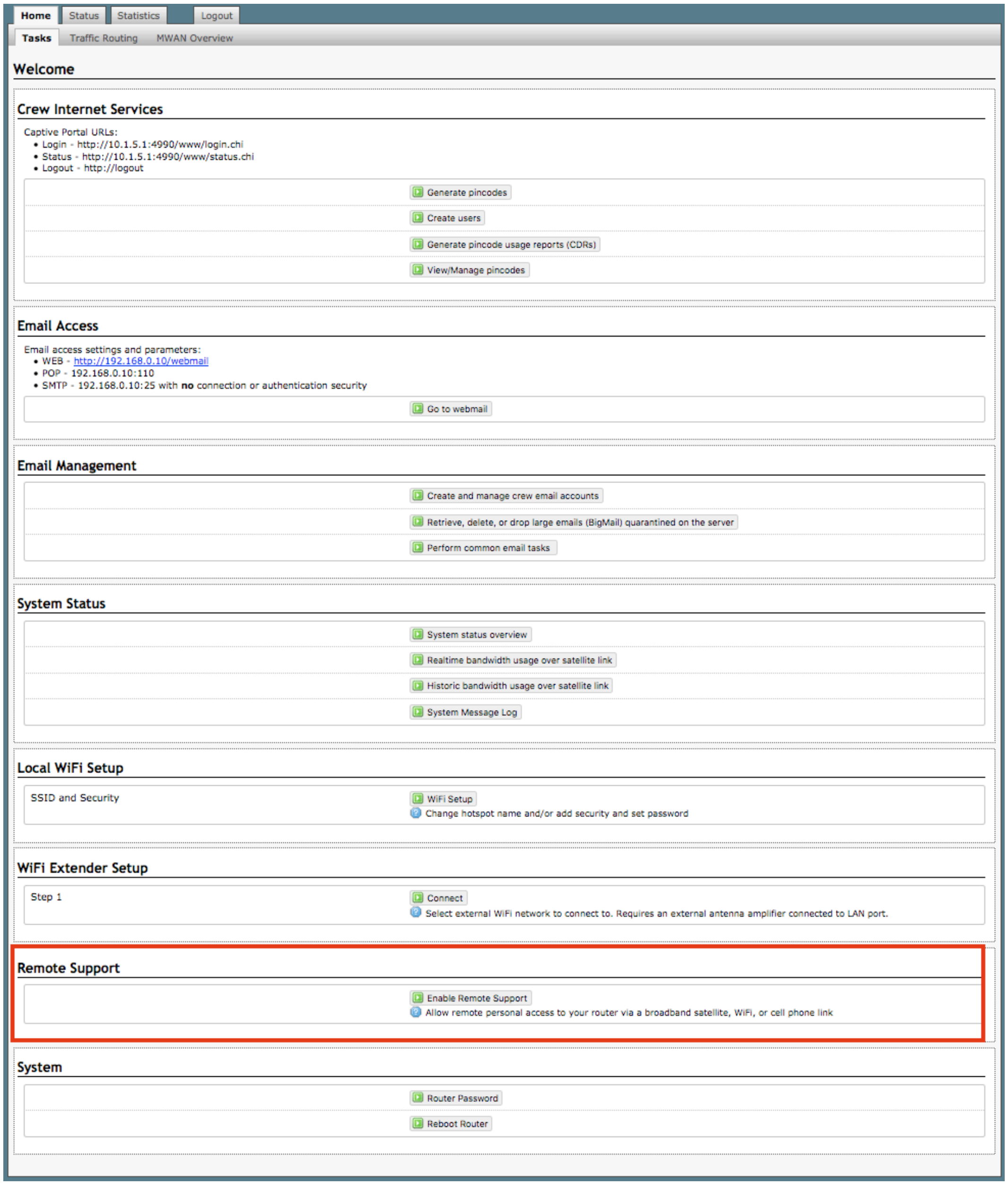
Collectd Settings

Collectd is a small daemon for collecting data from various sources through different plugins. On this page you can change general settings for the collectd daemon.

Base Directory	/var/run/collectd
Directory for sub-configurations	/etc/collectd/conf.d
Directory for collectd plugins	/usr/lib/collectd
Used PID file	/var/run/collectd.pid
Datasets definition file	/usr/share/collectd/types.db
Data collection interval	30 Seconds
Number of threads for data collection	2
Try to lookup fully qualified hostname	□

10.0 Remote Support

The On-site Administrator ("admin" login) does NOT have access to all of the router's features and settings. They are limited to the Tasks required in day-to-day operations as shown on the Home screen. If support is required after the router is installed, the On-site administrator can <Enable Remote Support> to give you access. Remote Support requires an active broadband satellite, WiFi or cell phone link.


Home
Status
Statistics
Logout
Tasks
Traffic Routing
MWAN Overview

Welcome

Crew Internet Services

Captive Portal URLs:
- Login - http://10.1.5.1:4990/www/login.chi
- Status - http://10.1.5.1:4990/www/status.chi
- Logout - http://logout

Generate pincodes
Create users
Generate pincode usage reports (CDRs)
View/Manage pincodes

Email Access

Email access settings and parameters:
- WEB - http://192.168.0.10/webmail
- POP - 192.168.0.10:110
- SMTP - 192.168.0.10:25 with **no** connection or authentication security

Email Management

Create and manage crew email accounts
Retrieve, delete, or drop large emails (BigMail) quarantined on the server
Perform common email tasks

System Status

System status overview
Realtime bandwidth usage over satellite link
Historic bandwidth usage over satellite link
System Message Log

Local WiFi Setup

SSID and Security

Change hotspot name and/or add security and set password

WiFi Extender Setup

Step 1

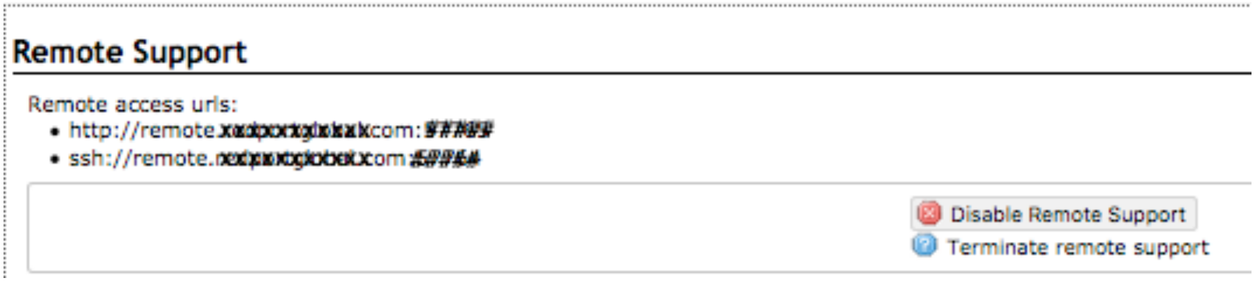
Select external WiFi network to connect to. Requires an external antenna amplifier connected to LAN port.

Remote Support

Allow remote personal access to your router via a broadband satellite, WiFi, or cell phone link

System

When remote support is enabled Remote Access URLs are displayed.



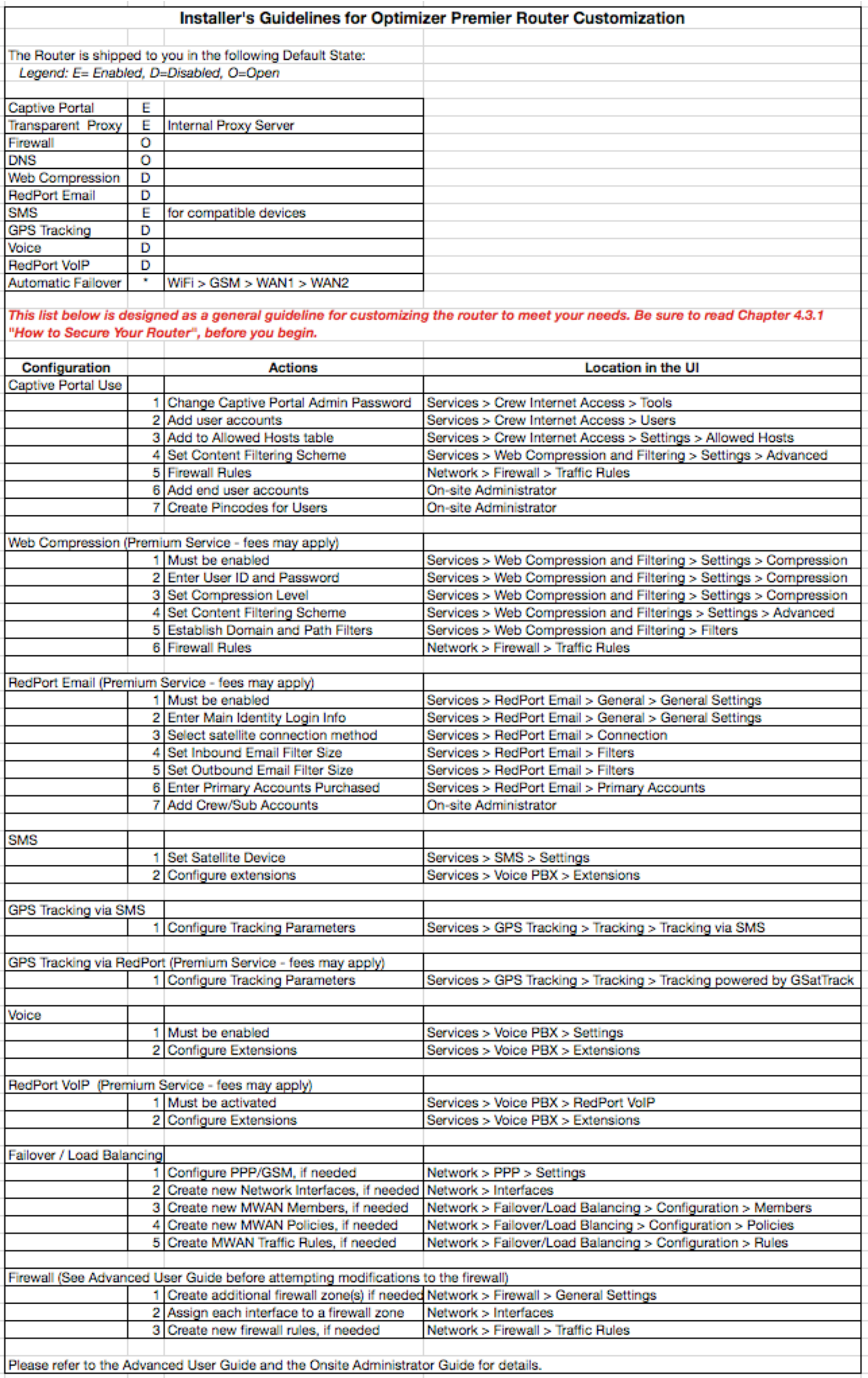
Remote Support

Remote access urls:

- http://remote.[redacted]com:[redacted]
- ssh://remote.[redacted]com:[redacted]

Remote Support will remain enabled until Disabled.

APPENDIX A



Installer's Guidelines for Optimizer Premier 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	
SMS	E	for compatible devices
GPS Tracking	D	
Voice	D	
RedPort VoIP	D	
Automatic Failover	*	WiFi > GSM > WAN1 > WAN2

This list below is designed as a general guideline for customizing the router to meet your needs. Be sure to read Chapter 4.3.1 "How to Secure Your Router", before you begin.

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	Set Content Filtering Scheme	Services > Web Compression and Filterings > Settings > Advanced
	5	Establish Domain and Path Filters	Services > Web Compression and Filtering > Filters
	6	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
SMS			
	1	Set Satellite Device	Services > SMS > Settings
	2	Configure extensions	Services > Voice PBX > Extensions
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
Voice			
	1	Must be enabled	Services > Voice PBX > Settings
	2	Configure Extensions	Services > Voice PBX > Extensions
RedPort VoIP (Premium Service - fees may apply)			
	1	Must be activated	Services > Voice PBX > RedPort VoIP
	2	Configure Extensions	Services > Voice PBX > Extensions
Failover / Load Balancing			
	1	Configure PPP/GSM, if needed	Network > PPP > Settings
	2	Create new Network Interfaces, if needed	Network > Interfaces
	3	Create new MWAN Members, if needed	Network > Failover/Load Balancing > Configuration > Members
	4	Create new MWAN Policies, if needed	Network > Failover/Load Blancing > Configuration > Policies
	5	Create MWAN Traffic Rules, if needed	Network > Failover/Load Balancing > Configuration > Rules
Firewall (See Advanced User Guide before attempting modifications to the firewall)			
	1	Create additional firewall zone(s) if needed	Network > Firewall > General Settings
	2	Assign each interface to a firewall zone	Network > Interfaces
	3	Create new firewall rules, if needed	Network > Firewall > Traffic Rules

Please refer to the Advanced User Guide and the Onsite Administrator Guide for details.

APPENDIX B

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

	Login	
	admin	superadmin
Home Page	✔	✔
Tasks	✔	✔
Traffic Routing	✔	✔
MWAN Overview	✔	✔
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	✔
File Transfer		✔
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		✔
GPS/NMEA Repeater		✔
Voice PBX		✔
Extensions		✔
CDR		✔
Logs		✔
Sat SIP Trunk		✔
RedPort VoIP		✔
Network Shares	✔	✔
General Settings	✔	✔
Edit Template	✔	✔

	Login	
	admin	superadmin
Status Tab - All	✔	✔
System Tab		✔
System Settings		✔
General Settings		✔
Logging		✔
Language and Style		✔
Router Password	from Home Page	✔
Profiles		✔
Profiles Manager		✔
Tools		✔
Back/Flash Firmware		✔
Actions		✔
Configuration		✔
Router 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		✔
IPset		✔
Diagnostics		✔
PPP		✔
Status		✔
Settings		✔
Network		✔
PPP		✔
GSM		✔
Signal Monitor		✔
Log		✔
Failover / Load Balancing		✔
Overview		✔
Interface Status		✔
Detailed Status		✔
Configuration		✔
Interfaces		✔
Members		✔
Policies		✔
Rules		✔
Advanced		✔
Diagnostics		✔
Statistics Tab - All	✔	✔
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.