



Aurora

ADVANCED USER GUIDE

FOR INSTALLERS & NETWORK ADMINISTRATORS

v2.0 – 18DEC2020

Copyright © Pivotal IP LLC. All rights reserved

Table of Contents

1.	ABOUT THIS GUIDE.....	4
2.	INTRODUCTION TO AURORA.....	5
2.1.	KEY FEATURES	5
2.2.	SERVICES INCLUDED	6
2.3.	PREMIUM SERVICES AVAILABLE	6
2.4.	IRIDIUM SATELLITE NETWORK	6
3.	SAFETY	7
4.	THINGS TO KNOW BEFORE GETTING STARTED.....	8
4.1.	DESIGNED USE OF THE AURORA.....	8
4.1.1.	Single User Environment	8
4.1.2.	Multi-User Environment.....	8
4.2.	HOW IT WORKS AT FIRST LAUNCH (OUT OF THE BOX).....	9
4.3.	HOW DATA FLOWS THROUGH THE ROUTER.....	10
4.3.1.	Default Configuration	10
4.3.2.	Without RedPort-Certified Service	10
4.4.	NAVIGATING THE USER INTERFACE.....	11
5.	GETTING STARTED - USER INTERFACE ACCESS.....	12
5.1.	ACCESS THE HOME PAGE.....	12
5.1.1.	Onsite Administrator Login (Admin)	13
5.1.2.	Installer/Network Administrator Login (Superadmin).....	14
5.2.	HOW TO USE WITH DEFAULT SETUP.....	16
5.2.1.	Email and Web Browsing.....	16
5.2.2.	Voice Calls.....	17
5.2.3.	SMS Messaging	17
5.	SERVICES.....	18
5.1.	REDPORT EMAIL	18
5.1.1.	Enable and Configure RedPort Email.....	19
5.1.2.	Primary Accounts	21
5.2.	SMS MESSAGING.....	22
5.2.1.	SMS Settings	22
5.2.2.	Configure SIP Extensions to Receive SMS Messages.....	23
5.2.3.	How to Send/Receive SMS Messages.....	23
5.2.4.	SMS Management.....	24
5.3.	GPS TRACKING	25
5.3.1.	Tracking powered by RedPort with GSatTrack	25
5.3.2.	Tracking via SMS.....	26
5.4.	WI-FI EXTENDER	27
5.5.	GPS/NMEA REPEATER	28
5.6.	VOICE PBX.....	29
5.6.1.	Voice PBX Settings.....	29
5.6.2.	Setup Extensions.....	30
5.6.3.	How to Make/Receive Voice Calls	31
5.6.4.	CDR (Call Data Records).....	32
5.6.5.	Logs	33
5.7.	NETWORK SHARES	34

5.7.1.	Create a Shared Directory	34
5.7.2.	Add Users	36
5.7.3.	How to Access the Shared Directory and Path Folders:	36
6.	STATUS	40
7.	SYSTEM	41
7.1.	SYSTEM SETTINGS	41
7.2.	ROUTER PASSWORD	42
7.3.	PROFILES	43
7.3.1.	Add a Profile	44
7.3.2.	Change to Another Saved Profile	44
7.3.3.	Export a Profile	45
7.4.	BACKUP/FLASH FIRMWARE	46
7.4.1.	Backup/Restore	47
7.4.2.	Flash New Firmware Image	48
7.4.3.	Flash SD Drive Image	49
7.4.4.	Wi-Fi Extender	49
7.5.	REBOOT	52
8.	NETWORK	53
8.1.	INTERFACES	53
8.2.	Wi-Fi	55
8.2.1.	Rename the Wireless Network	56
8.2.2.	Restrict Wireless Network Access	57
8.3.	DHCP AND DNS	58
8.4.	HOSTNAMES	59
8.5.	STATIC ROUTES	60
8.6.	DIAGNOSTICS	61
8.7.	FIREWALL	62
8.7.1.	General Settings	62
8.7.2.	Port Forwards	65
8.7.3.	Firewall Rules	66
8.7.4.	IP Sets	69
8.8.	PPP	70
8.8.1.	PPP Settings for Aurora	70
8.8.2.	PPP Settings for GSM	73
8.8.3.	Signal Monitor	78
9.	STATISTICS	79
9.1.	GRAPHS	79
10.	INSTALLERS GUIDELINES FOR CUSTOMIZATION	80
11.	LOGIN ACCESS TABLE	81
12.	PRODUCT SUPPORT INFORMATION	82
12.1.	PRODUCT WARRANTY INFORMATION	82
12.2.	PRODUCT SUPPORT INFORMATION	83
12.3.	REDPORT COMPANY CONTACT INFORMATION	83

1. About this Guide

This guide is intended for installers and network administrators of the RedPort Aurora Iridium Wi-Fi Terminal. 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.

For information regarding the installation of the hardware, please see the RedPort Aurora QuickStart Guide.

2. Introduction to Aurora

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

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

Aurora is an Iridium satellite Wi-Fi terminal, with a built-in RedPort Optimizer router, that provides satellite voice, data and tracking services all under one dome. It is designed so you can make voice calls and check email with devices you already have - your smartphone, tablet or computer.

2.1. Key Features

Designed specifically for use with Iridium satellite service:

- Built-in RedPort Optimizer router for integrated voice, data and tracking.
- Supports voice calling and SMS messages using smartphones connected to the local network.
- GSM Compatibility with optional bring your own GSM modem and service.
- GPS NMEA Repeater broadcasts the built-in GPS coordinates via Wi-Fi to share with your onboard marine electronics.
- Supports GPS tracking.
- Logging/Reporting to keep track of usage.
- Wi-Fi hotspot makes setup and use easy for crew with compatible computers, tablets and smartphones.
- Supports RedPort Email Service.
- Data optimization powered by RedPort Optimizer hardware.
- Powerful firewall accommodates virtually any common installation scenario, with features including block or allow any range of port, IP address and protocols.

2.2. Services Included

The following services are included:

- Voice PBX - allows smartphones to send/receive calls to others on the local area network for free, or over the satellite link at standard satellite airtime rates. 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 standard satellite airtime rates. See Chapter 5.2.
- GPS NMEA Repeater – allows other devices onboard/on-site to read your GPS location. See Chapter 5.5.
- GSM Compatibility - allows Internet connectivity via your GSM modem or cell phone with your own SIM card. See Chapter 8.8.
- File Sharing - Network Shares allows the sharing of files among Windows and Mac computers via Wi-Fi, without the requirement of a wired local network of computers.

2.3. Premium Services Available

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

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 the Optimizer RedPort Email Administrator's Guide for more information about this service. See Chapter 5.1 and the Optimizer RedPort Email Guide.

GPS Tracking - Using a GPS-enabled device, submit position reports to a central database for viewing on the tracking website. See Chapter 5.3.

2.4. Iridium Satellite Network

RedPort Aurora uses the Iridium satellite network. The Iridium satellite network is comprised of 66 Low-Earth Orbiting (LEO), cross-linked satellites, providing voice and data coverage over Earth's entire surface. The satellites operate in six orbital planes, 781 kilometers (485 miles) from Earth. This ensures that every region on the globe is covered by at least one satellite at all times. Each satellite is cross-linked to four other satellites; two satellites in the same orbital plane and two in an adjacent plane. RedPort recommends the use of Pivotal Iridium airtime service. Pivotal Iridium service plans can be found at pivotal.com.

3. Safety



Shock Hazard

The Glow LTE is a sealed device and is not meant to be opened for repair in the field by operators or technicians. Covers must remain in place at all times on the Terminal Unit to maintain the warranty terms. Make sure the system is correctly grounded and power is off when installing, configuring and connecting components.



Antenna Radiation Hazards

To comply with FCC Radio Frequency radiation exposure limits, the antenna must be installed at a minimum safe distance. During operation, the antenna radiates high power at microwave frequencies that can be harmful to individuals. While the unit is operating, personnel should maintain a minimum safe distance of 1.0 meter (3.3 ft.) from the antenna. The antenna should be mounted in an area that prevent the possibility of close exposure to the antenna's radiation.



Proposition 65

This product can expose you to Acrylonitrile, which is known to the State of California to cause cancer. For more information go to www.P65Warnings.ca.gov.

4. Things to Know Before Getting Started

4.1. Designed Use of the Aurora

This terminal is suitable for two distinctly different audiences:

4.1.1. Single User Environment

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

4.1.2. Multi-User Environment

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

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

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

4.2. How It Works at First Launch (Out Of The Box)

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

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

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

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

Best Practice is to have a knowledgeable technician generate a custom configuration. In a fleet environment, this custom configuration can be recorded and used on other RedPort Aurora terminals within the organization.

4.3. How Data Flows Through the Router

It is important to understand how data flows through the Aurora if you want to customize your configuration.

4.3.1. Default Configuration

The default configuration is ready for use with RedPort certified Email and/or Web:

Firewall - closed, allows Internet access only via RedPort Services

DNS - closed

RedPort Email - disabled

SMS - enabled

GPS Tracking - disabled

GPS/NMEA Repeater - disabled

Voice Capability – enabled

In its default state, without any modifications, one primary account holder at-a-time can connect to send/receive email or web browse using a RedPort-certified email service like XGate or web browsing service like XWeb.

All email requests go directly to the upstream email server. The mail is downloaded to the end-users computer/device and then the mail is purged from the server.

All web browsing requests go directly to the upstream compression server. Compressed webpages are returned to the end-user, whenever compression is possible. The end-user can set the compression level thru the RedPort-certified web service program.

The default state is designed for the single user that uses services like XGate and XWeb for email and web browsing and uses the XGate Phone app on their smartphone for making voice calls.

4.3.2. Without RedPort-Certified Service

In order to use the Aurora for web browsing without a RedPort-certified web service like XWeb, you must first modify the firewall to allow traffic. See Section 8.7.

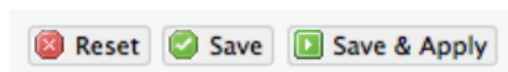
With the firewall open, any user on the local network can browse the web without restrictions, limits, or, compression. All traffic goes straight to the Internet without any filtering or compression.

4.4. Navigating the User Interface

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

The user interface is divided into sections; use the tabs to access the required service or information.

On most pages in the user interface you will see three buttons in the lower right corner:



Reset: returns the page to its previous saved state.

Save: saves the changes but does not yet apply the changes.

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

5. Getting Started - User Interface Access

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

- Email & Web access via RedPort-certified services (Firewall closed to everything else)
- SMS messaging using smartphones
- GPS/NMEA Repeater

There are also services available that are disabled:

- Voice Capability using smartphones
- RedPort Email (additional fees may apply)
- GPS Tracking (additional fees may apply)

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

5.1. Access the Home page

To access the Glow LTE user interface, you must login to the router:

1. Connect to the Wi-Fi Hotspot created by the Aurora using a PC. Connect to the Wi-Fi Hotspot just like you would any other Wi-Fi connection:

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

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

The Network Name will look something like: 'wxa-171-XXXX' where 'XXXX' is the last four digits of Aurora's Mac address.

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

`http://192.168.10.1`

The Aurora ships with two existing accounts:

- **Admin** - for normal day-to-day operation by the onsite administrator.
- **Superadmin** - for configuration and maintenance by the installer/network administrator.

5.1.1. Onsite Administrator Login (Admin)

Onsite Administrator:

username=admin

password=webxaccess

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

- send/receive email (if email is enabled)
- manage crew email accounts (if email is enabled)
- monitor the system status
- modify the local Wi-Fi setup
- request a remote support session
- reboot the router, if necessary
- change the router password for the admin account, if necessary

See the Aurora Onsite Administrator Guide for information in administering the most used features.

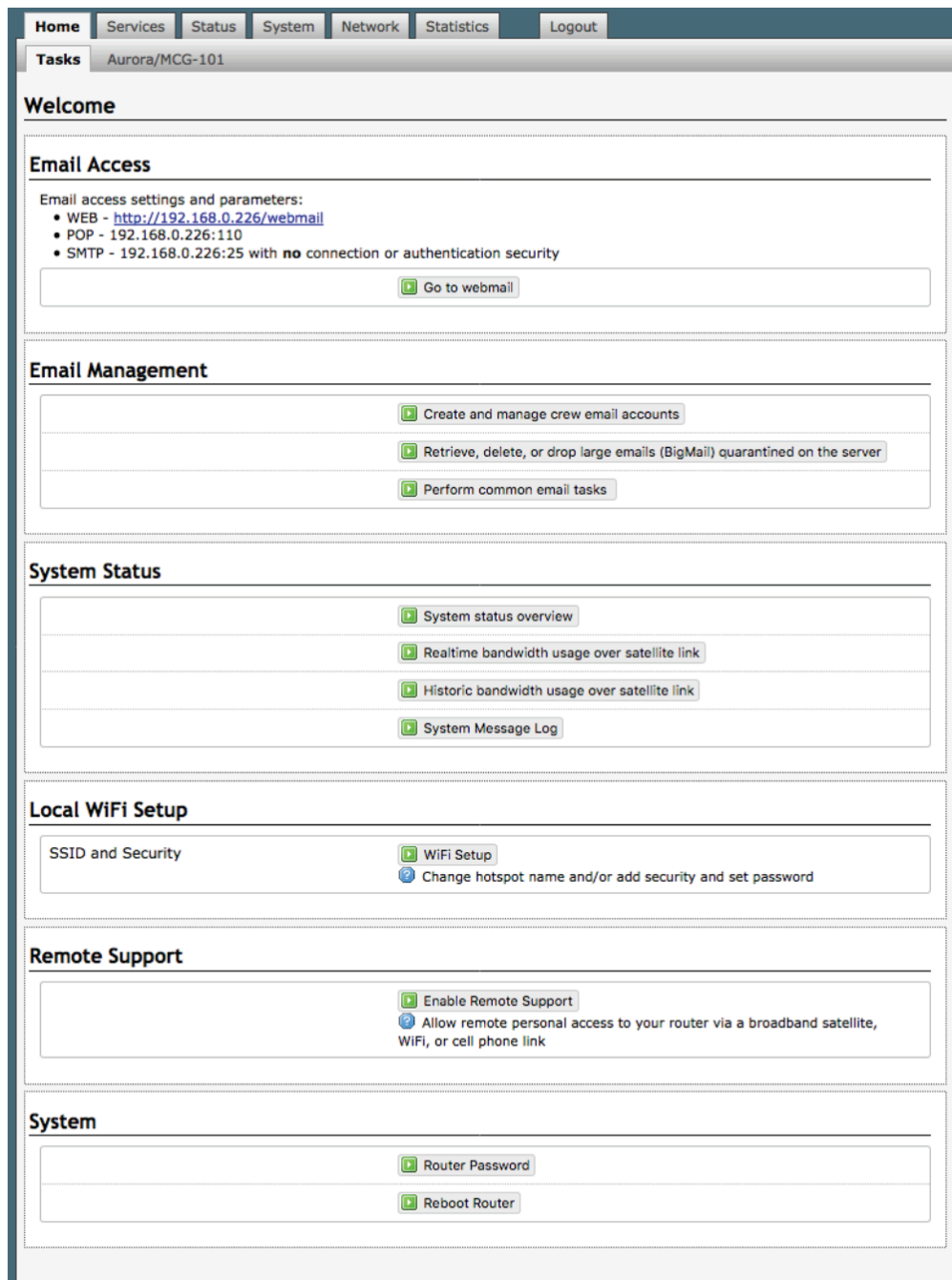
5.1.2. Installer/Network Administrator Login (Superadmin)

Technician:

username=superadmin

password=webxaccess

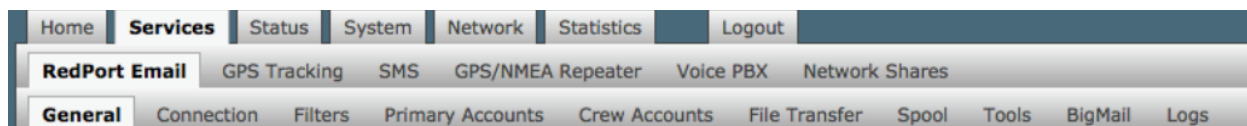
This login provides full access to the user interface for configuration and maintenance. Once logged in, you will see the Home page:



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

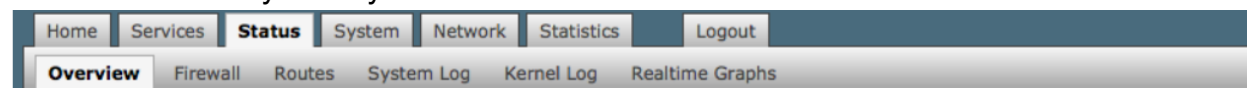
From the Home Page, the 'superadmin' login has access to the remaining sections of the user interface.

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



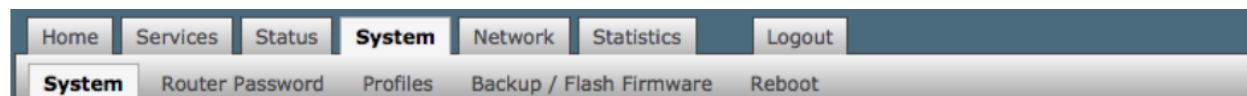
Each service is contained in its own tab under the Services section. This is where you will enable/disable the services and configure them for use.

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



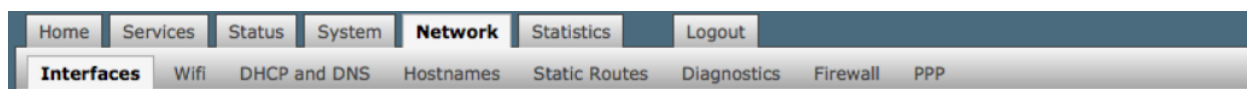
The System Log contains detailed information of the router's performance. It will report error messages and can be useful when troubleshooting connection issues. Realtime Graphs report how much data is being using by the different interfaces. All Status information is Read Only.

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



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

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



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

Statistics: contains information about resource usage.



5.2. How to Use with Default Setup

We ship the Aurora ready for use with a RedPort-certified compression email and/or web browsing account; Voice, SMS and GPS Tracking are ready to be enabled for use.

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

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

5.2.1. Email and Web Browsing

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

Here are the basic instructions:

1. Power the Aurora ON.
2. On your computer, iOS or Android device, connect to the wireless network created by the Aurora. The name of the wireless network will be something like: wxa-171-xxxx, where xxxx may represent the last four digits of the Mac address of the Aurora.
3. Once connected to the wireless network, open the RedPort-certified email program (such as XGate) and go to Settings > Connection > and set the Connection Type to "Aurora". Click [OK].
4. Wait for a strong satphone signal.
5. Start an email or a web browsing session.

4.2.2. Voice Calls

Voice is disabled by default but can be enabled for use with standard satellite airtime. See Section 5.6 for details on configuration and use of the Voice service.

4.2.3. SMS Messaging

SMS is enabled by default and configured for use with one extension. See Section 5.2 for details on configuration and use of the SMS Messaging service.

5. Services

5.1. RedPort Email

Requires 'superadmin' login.

This is a full-featured Crew solution that runs on the Optimizer router in the Aurora. 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.

The screenshot shows the 'RedPort Email' configuration page. At the top, there are tabs for 'Home', 'Services', 'Status', 'System', 'Network', 'Statistics', and 'Logout'. Below these are sub-tabs for 'RedPort Email', 'GPS Tracking', 'SMS', 'GPS/NMEA Repeater', 'Voice PBX', and 'Network Shares'. The 'General' tab is selected, showing 'General Settings'. The 'Webmail login' section includes a 'Redirect to webmail' checkbox (checked), a 'POP Server Address:Port' field (192.168.0.177:110), and an 'SMTP Server Address:Port, Connection' field (192.168.0.177:25). Below this, there are tabs for 'General Settings', 'Webmail Settings', 'Network Settings', 'Log Settings', and 'Mail Filtering'. The 'General Settings' tab is active, showing fields for 'Enable email server' (checked), 'Main identity userid' (test), 'Main identity password' (masked), 'Domain' (redportglobal.com), 'Update interval(min)' (60), and 'Send and Receive mail concurrently' (unchecked). A 'Reset' button is at the bottom left, and 'Save' and 'Save & Apply' buttons are at the bottom right.

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 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 to activate this service.

5.1.1. Enable and Configure RedPort Email

In the RedPort Email General Settings:

General Settings | Webmail Settings | Network Settings | Log Settings | Mail Filtering

Enable email server ☒

Main identity userid
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
Default email domain.

Update interval(min)
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 Optimizer- RedPort Email Guide for information on email block compression and its impact on Update intervals.)
5. Click <Save>.

Note: Typically, the Main Identity is the onsite email administrator. The Main Identity must be a Primary Account. There must be at least one primary account present on the system before sub/crew accounts can be created. See section 5.1.2 for more information regarding primary accounts.

6. Go to the Connection tab:

The screenshot shows the 'RedPort Email' interface with the 'Connection' tab selected. The 'Connection Settings' section contains the following fields and options:

Gateway TCP/IP Port #	443
Primary XGate Server	xgate.gmn-usa.com
Network Connection	Network Connection <small>? Select satellite connection method.</small>
Dial Override	 <small>? Leave blank to use interface default.</small>
IP Device Password	 <small>? IP dialer device password. Leave blank for default. Must have a value if the system password is changed.</small>
IP Dial Override	 <small>? 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.</small>
Leave Open	<input type="checkbox"/> <small>? Leave network connection active when done.</small>
Use if Open	<input type="checkbox"/> <small>? Use another connection if already open.</small>
Override network timeouts	<input type="checkbox"/> <small>? Override default connection timeouts. Should not be required.</small>
Persistent Connections	<input type="checkbox"/> <small>? Persist with connections until transfer completes or num times.</small>

At the bottom, there are three buttons: 'Reset', 'Save', and 'Save & Apply'.

7. Click on <Network Connection> to open up the dropdown menu.
8. Select Aurora.
9. Select <Save & Apply> to apply the change.

5.1.2. Primary Accounts

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

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

Primary accounts have access to email whether on or off the vessel as the account Exists on the Pivotal 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 Optimizer RedPort Email Guide for information on using a custom domain name for the email address.

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

5.2. SMS Messaging

It is possible to send and receive SMS messages directly from the Aurora user interface and to route incoming SMS messages to one or more smartphones connected to the local wireless network.

Access to Services > SMS requires the 'superadmin' login.

5.2.1. SMS Settings

Use Settings to enable and configure the SMS parameters.

The screenshot displays the 'SMS parameters' configuration page. The interface includes a top navigation bar with 'Home', 'Services', 'Status', 'System', 'Network', 'Statistics', and 'Logout'. Below this is a sub-navigation bar with 'RedPort Email', 'GPS Tracking', 'SMS', 'GPS/NMEA Repeater', 'Voice PBX', and 'Network Shares'. The 'SMS' section is active, showing 'Settings' and 'Management' tabs. The 'sms parameters' section is titled 'configure the parameters for SMS'. It contains a form with the following fields: 'Enabled' (checkbox, checked), 'interval in seconds between LOCAL send' (input field, 240), 'attempts' (input field, empty), 'number of days that messages stay in queue' (input field, 3), 'when receiving messages' (input field, empty), 'Satellite device' (dropdown menu, Iridium), 'Check for received messages (in seconds)' (input field, 360), and 'Configure extensions to receive SMS' (button, Redirect). At the bottom of the form are 'Reset', 'Save', and 'Save & Apply' buttons. Red arrows highlight the 'Enabled' checkbox, the 'Satellite device' dropdown, and the 'Save & Apply' button.

1. Select the checkbox to enable SMS.
2. Select the appropriate Satellite device from the drop-down menu.
3. Select <Save & Apply>.

5.2.2. Configure SIP Extensions to Receive SMS Messages

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

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

Buttons: Add, Reset, Save, Save & Apply

To enable an extension to receive SMS messages, use the checkbox in the SMS column. For more information on configuring SIP Extensions see Chapter 5.6.2.

5.2.3. How to Send/Receive SMS Messages

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

Using the smartphone or tablet Settings, connect to the Aurora wireless network 'wxa-171- xxxx'.

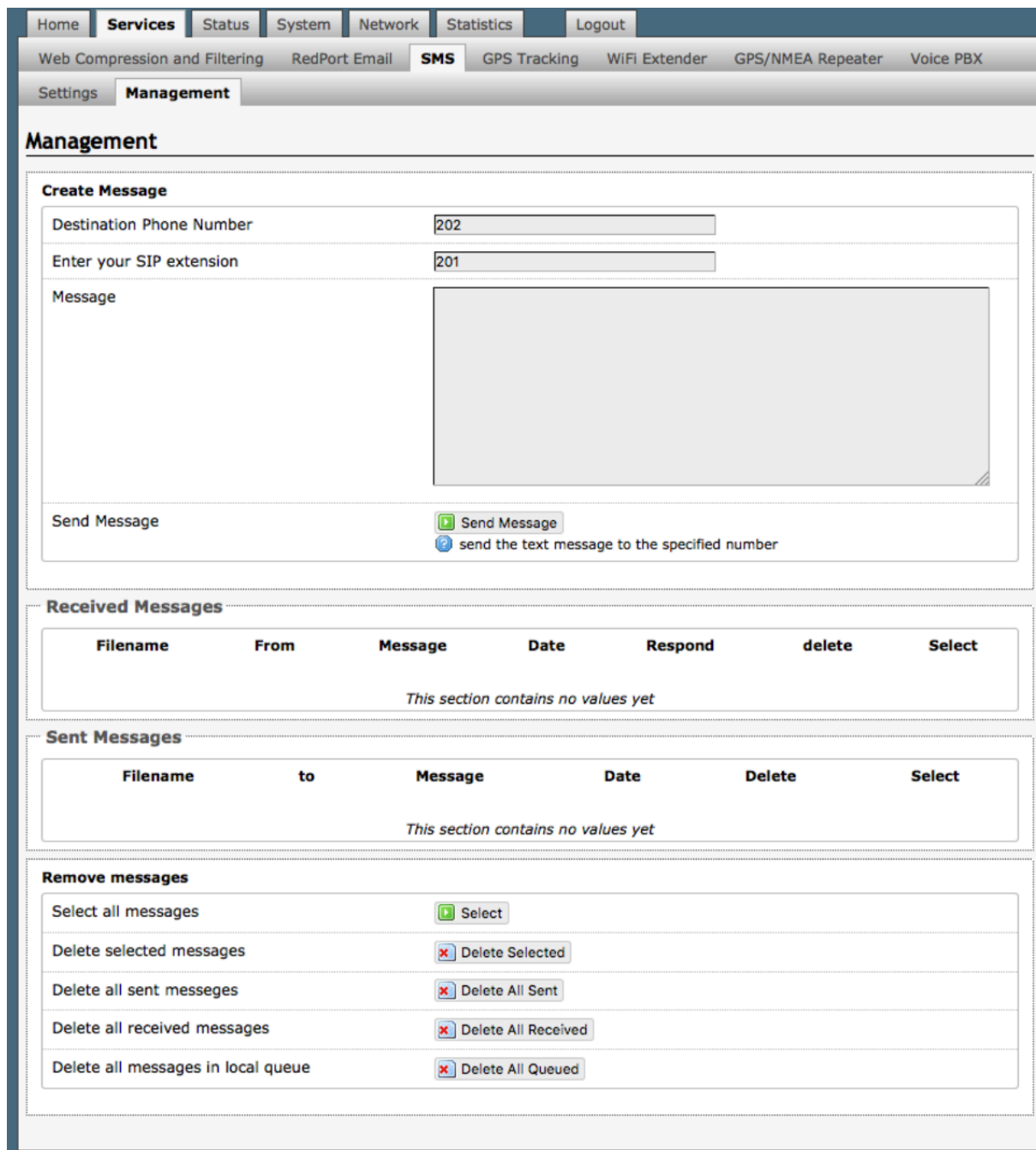
Open the XGate Phone App. Select <Chat> to send a SMS message or to view a SMS message received.

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



5.2.4. SMS Management

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



Home Services Status System Network Statistics Logout

Web Compression and Filtering RedPort Email **SMS** GPS Tracking WiFi Extender GPS/NMEA Repeater Voice PBX

Settings **Management**

Management

Create Message

Destination Phone Number

Enter your SIP extension

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

Delete selected messages

Delete all sent messages

Delete all received messages

Delete all messages in local queue

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

5.3. GPS Tracking

The Aurora includes a built-in GPS chip making tracking possible. Two tracking are available: (1) GPS Tracking service powered by GSatTrack; or, (2) Tracking service via SMS message. Access to Services > GPS Tracking requires the 'superadmin' login.

5.3.1. Tracking powered by RedPort with GSatTrack

The Aurora can be configured to submit position reports to a central database for viewing on the tracking website.

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

1. Select the checkbox to Enable Tracking.
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 position report. Adjust the Tracking Interval to meet your needs.
3. Select Iridium terminal/Aurora/MCG-101.
4. Select <Save & Apply>

The screenshot displays the 'GPS Tracking' configuration interface. At the top, navigation tabs include Home, Services, Status, System, Network, Statistics, and Logout. The 'Services' tab is active, showing sub-tabs for RedPort Email, GPS Tracking, SMS, GPS/NMEA Repeater, Voice PBX, and Network Shares. The 'GPS Tracking' sub-tab is selected, leading to the 'Tracking' page.

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

General Tracking Parameters

- Enable Tracking: ☒
- Tracking Interval: 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: 101376012418.
- Globalstar phone: ☐ A valid NMEA/GPS feed is required. Tracking IMEI: 101376012418.
- Iridium terminal/Aurora/MCG-101: ☒ A valid NMEA/GPS feed is required.

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

- INMARSAT Isatphone: ☐
- Iridium terminal/Aurora/MCG-101: ☐ A valid NMEA/GPS feed is required.
- Recipient Email Address: Enter a valid email address. Also used for SOS messages.
- Vessel name: Enter optional vessel name and/or other free text.

At the bottom, there are buttons for 'Reset', 'Save', and 'Save & Apply'.

5.3.2. Tracking via SMS

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

1. Select the checkbox to Enable Tracking.
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 position report. Adjust the Tracking Interval to meet your needs.
3. Select Iridium terminal/Aurora/MCG-101.
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 2.
5. Select <Save & Apply>.

Home Services Status System Network Statistics Logout

RedPort Email **GPS Tracking** SMS GPS/NMEA Repeater Voice PBX Network Shares

Tracking

Tracking Parameters

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

General Tracking Parameters

Enable Tracking ☒

Tracking Interval 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: 101376012418.

Globalstar phone ☐ A valid NMEA/GPS feed is required. Tracking IMEI: 101376012418.

Iridium terminal/Aurora/MCG-101 ☐ A valid NMEA/GPS feed is required.

Tracking via SMS

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

INMARSAT Isatphone ☐

Iridium terminal/Aurora/MCG-101 ☒ A valid NMEA/GPS feed is required.

Recipient Email Address Enter a valid email address. Also used for SOS messages.

Vessel name Enter optional vessel name and/or other free text.

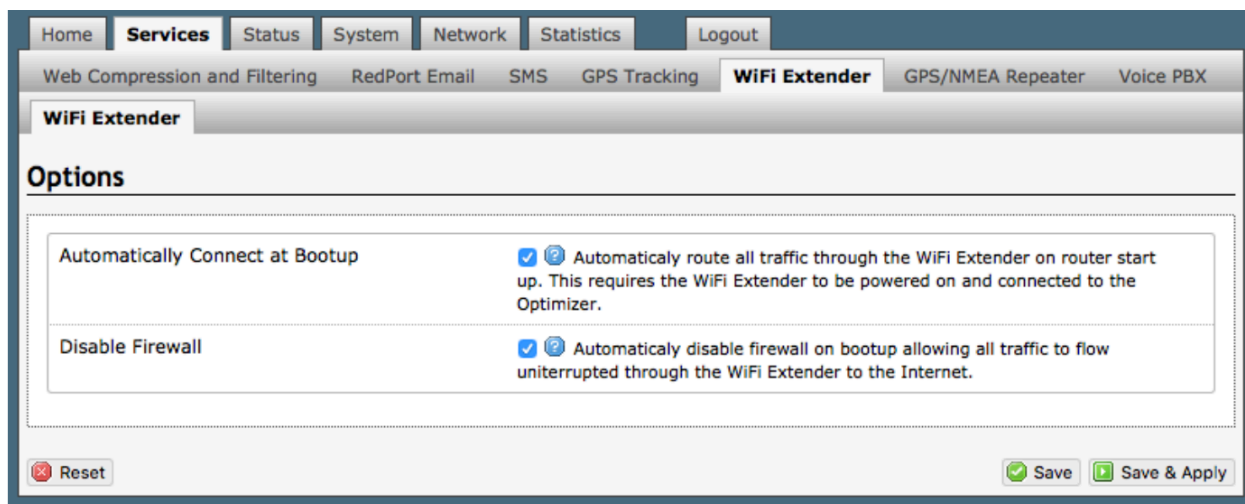
Reset Save Save & Apply

5.4. Wi-Fi Extender

If using the RedPort Wi-Fi Extender (optional, sold separately), you must plug the Aurora data cable and the RedPort Wi-Fi Extender data cable into a switch (not included).

IMPORTANT: The RedPort Wi-Fi Extender must be powered ON and connected to the Aurora before turning the Aurora ON.

Access to Services > Wi-Fi Extender requires the 'superadmin' login and the RedPort Wi-Fi Extender must be powered ON and connected to the Aurora.



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

For RedPort Wi-Fi Extender configuration and use details, see the Aurora Onsite Administrator Guide.

5.5. GPS/NMEA Repeater

Requires 'superadmin' login.

The Aurora includes a built-in GPS chip and can be configured to repeat the GPS coordinates over Wi-Fi for use by other applications.

Note: GPS info only is repeated, no other NMEA information is available via the Aurora built-in GPS chip.

In order for the destination software to properly route the GPS data you must configure the GPS/NMEA Repeater Parameters in the Aurora User Interface.

The screenshot displays the Aurora User Interface with the 'Services' tab selected. Under 'Services', the 'GPS/NMEA Repeater' option is highlighted. The page title is 'GPS/NMEA Repeater Settings'. Below the title, a description reads: 'Read GPS/NMEA information from a number of sources and repeat the data over WiFi and Ethernet.' The main section is titled 'Repeater Parameters' and contains a table of settings:

Enable	<input checked="" type="checkbox"/> Enable GPS monitoring and repeating.
GPS/NMEA feed from USB	<input type="checkbox"/> Use USB connected GPS or NMEA feed as a source. Note: Not compatible with RS-232 based satellite phones.
UDP Listener Port	10101 <input type="button" value="Help"/> Listen on UDP port number and rebroadcast.
UDP Port	11101 <input type="button" value="Help"/> Broadcast to UDP port number.
TCP Port	11102 <input type="button" value="Help"/> Broadcast to TCP port number.

At the bottom of the form, there are three buttons: 'Reset' (with a red 'x' icon), 'Save' (with a green checkmark icon), and 'Save & Apply' (with a green play icon).

Select the checkbox to Enable GPS monitoring and repeating. Once enabled, the GPS data will be broadcast on UDP Port 11101 and TCP port 11102. These are the standard port numbers for GPS devices.

Configure the destination software to match these port numbers; 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.*

5.6. VOICE PBX

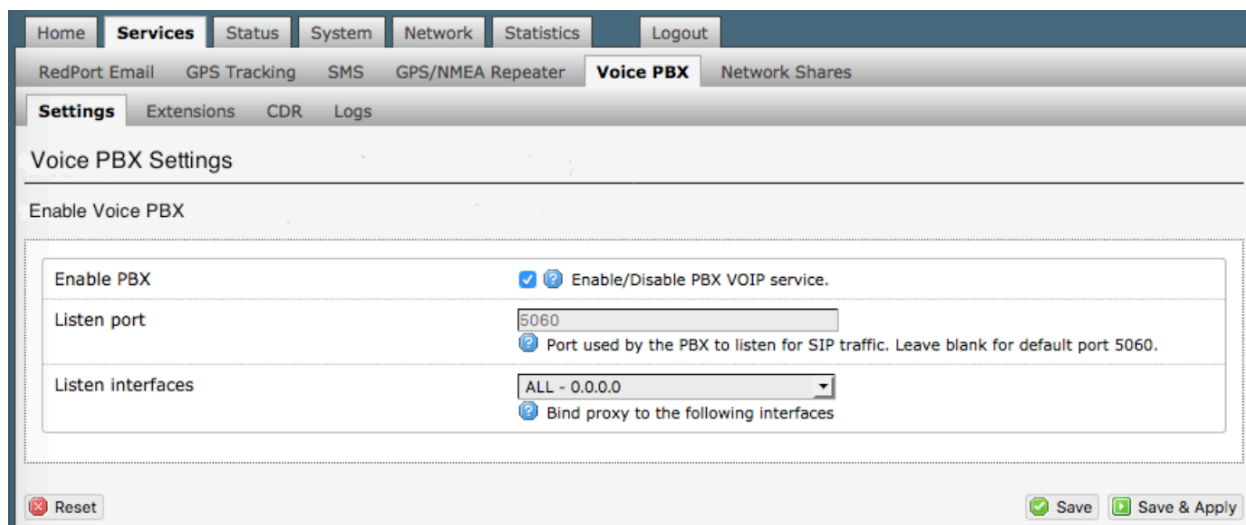
Requires 'superadmin' login.

Users with smartphones can send/receive voice calls and SMS messages over the satellite link, one voice call or one SMS message at a time. Standard satellite voice or SMS airtime rates will apply.

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

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

5.6.1. Voice PBX Settings



The screenshot shows the 'Voice PBX' settings page. At the top, there is a navigation bar with tabs: Home, Services (selected), Status, System, Network, Statistics, and Logout. Below this, there is a sub-navigation bar with tabs: RedPort Email, GPS Tracking, SMS, GPS/NMEA Repeater, Voice PBX (selected), and Network Shares. Under the 'Voice PBX' tab, there are sub-tabs: Settings (selected), Extensions, CDR, and Logs. The main content area is titled 'Voice PBX Settings'. It contains a section 'Enable Voice PBX' with a checkbox 'Enable PBX' which is checked. To the right of the checkbox is a link 'Enable/Disable PBX VOIP service.' Below this, there is a 'Listen port' field with the value '5060' and a help link 'Port used by the PBX to listen for SIP traffic. Leave blank for default port 5060.' There is also a 'Listen interfaces' dropdown menu with the value 'ALL - 0.0.0.0' and a help link 'Bind proxy to the following interfaces'. At the bottom left, there is a 'Reset' button. At the bottom right, there are 'Save' and 'Save & Apply' buttons.

Select the checkbox to Enable the PBX.

5.6.2. Setup Extensions

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

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

Incoming calls will ring only on those extensions with Ring enabled. To enable Ring (or SMS) on an extension simply check the box for the service you want enabled. 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.

On this page, you can also:

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

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.

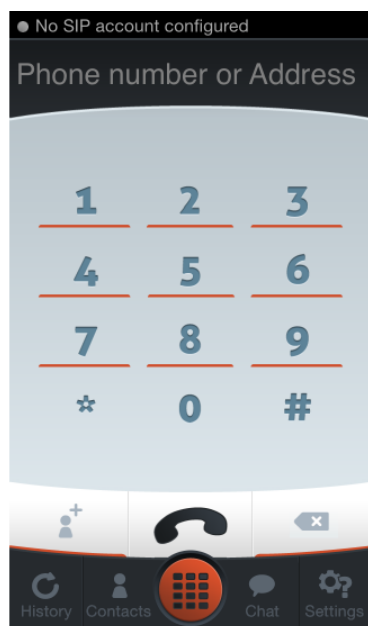
5.6.3. How to Make/Receive Voice Calls

Using the smartphone or tablet Settings, connect to the Auroral wireless network 'wxa-171-xxxx'.

Open the XGate Phone App to make and receive calls.

Note: Standard satellite voice calling rates apply.

Only one phone call can be active at a time.



5.6.4. 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 Aurora are approximate values and should not be used to resolve billing disputes. They are presented here for your convenience.

Home Services Status System Network Statistics Logout

RedPort Email GPS Tracking SMS GPS/NMEA Repeater Voice PBX Network Shares

Settings Extensions CDR Logs

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 <small>Current Date/Time through selected interval.</small>
Submit	<input type="button" value="Submit"/>
Enter Filename	cdr-2016-09-28.csv
Download CSV	<input type="button" value="Download"/>
Trim CDR	<input type="button" value="Delete"/> <small>Delete CDRs from system older than the reporting interval.</small>
Purge CDR	<input type="button" value="Purge"/> <small>Remove all CDRs from system.</small>

On active systems, the call data records can quickly use up memory. It is recommended that you periodically trim or purge the records from the system.

5.6.5. Logs

Call status can be monitored from the Logs screen.

Logs and Status

Active Calls

Hangup all calls

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

PBX Status

Restart PBX

SIP Status

Name/username	Host	Dyn	Forcerport	Comedia
201	(Unspecified)	D	Auto (No)	No
202	(Unspecified)	D	Auto (No)	No
203	(Unspecified)	D	Auto (No)	No
204	(Unspecified)	D	Auto (No)	No
kiab	127.0.0.1		Auto (No)	No

5 sip peers [Monitored: 0 online, 4 offline Unmonitored: 1 online, 0 offline]

IAX Status

No such command 'iax2 show peers' (type 'core show help iax2 show' for other possible commands)

Log

Clear log entry

Download log

```
[Sep 22 22:07:19] Asterisk 11.12.0 built by lsoltero @ ubuntu on a x86_64 running Linux on 2
[Sep 22 22:07:19] NOTICE[2570] cdr.c: CDR simple logging enabled.
[Sep 22 22:07:19] WARNING[2570] cel.c: Could not load cel.conf
[Sep 22 22:07:19] NOTICE[2570] loader.c: 38 modules will be loaded.
[Sep 22 22:07:19] WARNING[2570] loader.c: Error loading module 'res_musiconhold.so': File no
[Sep 22 22:07:19] WARNING[2570] loader.c: Error loading module 'res_musiconhold.so': File no
[Sep 22 22:07:19] WARNING[2570] loader.c: Module 'res_musiconhold.so' could not be loaded.
[Sep 22 22:07:19] WARNING[2570] loader.c: Error loading module 'res_smdi': File not found
[Sep 22 22:07:19] WARNING[2570] loader.c: Module 'res_smdi' could not be loaded.
[Sep 22 22:07:19] WARNING[2570] loader.c: Module 'res_smdi' could not be loaded.
[Sep 22 22:07:19] WARNING[2570] chan_dahdi.c: Ignoring any changes to 'userbase' (on reload)
[Sep 22 22:07:19] WARNING[2570] chan_dahdi.c: Ignoring any changes to 'vmsecret' (on reload)
[Sep 22 22:07:19] WARNING[2570] chan_dahdi.c: Ignoring any changes to 'bass' (on reload)
```

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

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. 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 Aurora 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 Aurora's Wi-Fi Hotspot.

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

5.7.1. Create a Shared Directory

Select <Add> to create a new Shared Directory:

The screenshot shows the Aurora web interface for configuring Network Shares. The top navigation bar includes 'Home', 'Services' (selected), 'Status', 'System', 'Network', 'Statistics', and 'Logout'. Below this, a sub-navigation bar lists various services: 'RedPort Email', 'GPS Tracking', 'SMS', 'GPS/NMEA Repeater', 'Voice PBX', and 'Network Shares' (highlighted with a red circle). The main content area is titled 'Network Shares' and is divided into two sections: 'Samba' and 'Shared Directories'.

The 'Samba' section includes a 'General Settings' tab and an 'Edit Template' button. It contains the following fields:

- Hostname: Optimizer
- Description: RedPort Optimizer Shares
- Workgroup: RedPort
- Listen interfaces: ☐ LAN - 192.168.0.177, ☐ WAN - 192.168.0.6
- Bind shares to the following interfaces: ☐ LAN - 192.168.0.177, ☐ WAN - 192.168.0.6

The 'Shared Directories' section is highlighted with a red box and contains a table with the following columns: Name, Path, Allowed users, Read-only, and Allow guests. A red arrow points to the 'Add' button in the 'Shared Directories' section. The table is currently empty, with the text 'This section contains no values yet' displayed below the columns.

Below the 'Shared Directories' section is the 'Users' section, which includes a table with columns for Username and Password. It also contains an 'Add' button and the text 'This section contains no values yet'.

At the bottom of the page, there are buttons for 'Reset', 'Save', and 'Save & Apply'.

Name	Path	Allowed users	Read-only	Allow guests	
Share name	Relative directory path	A comma separated list			
TransferIn	transferin	dbtest	<input type="checkbox"/>	<input type="checkbox"/>	Delete
TransferOut	transferout		<input type="checkbox"/>	<input checked="" type="checkbox"/>	Delete
Add					

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 Aurora 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.

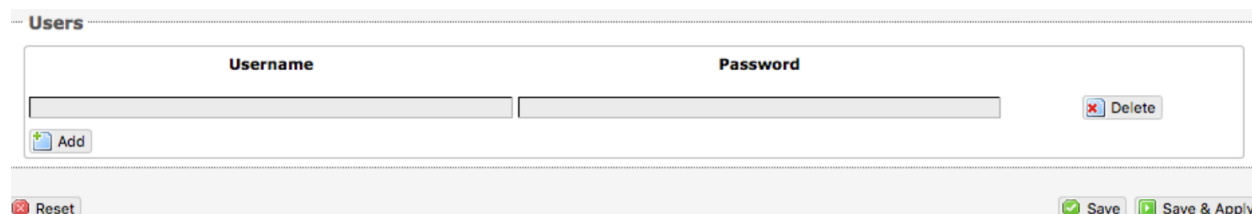
With this box checked, users will not be prompted to enter a username and password when accessing the Path Folder.

Delete: Use this to delete the Shared Directory.

Select <Save & Apply>.

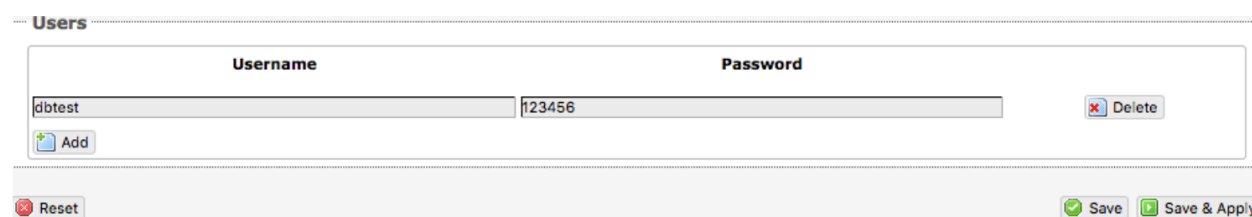
5.7.2. Add Users

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



The screenshot shows a web interface titled "Users". It contains a table with two columns: "Username" and "Password". Below the table, there is an "Add" button with a plus icon and a "Delete" button with a minus icon. At the bottom of the interface, there are three buttons: "Reset", "Save", and "Save & Apply".

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



The screenshot shows the same "Users" interface, but now the table contains one entry with the username "dbtest" and the password "123456". The "Add" button is still present. The "Reset", "Save", and "Save & Apply" buttons are at the bottom.

Select <Save & Apply>.

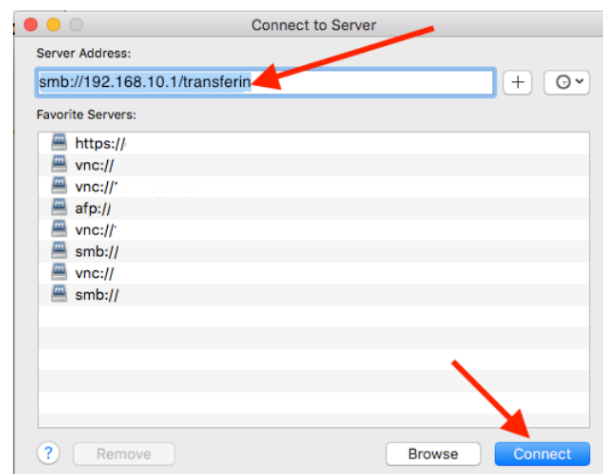
5.7.3. How to Access the Shared Directory and Path Folders:

5.7.3.1. From a Mac PC

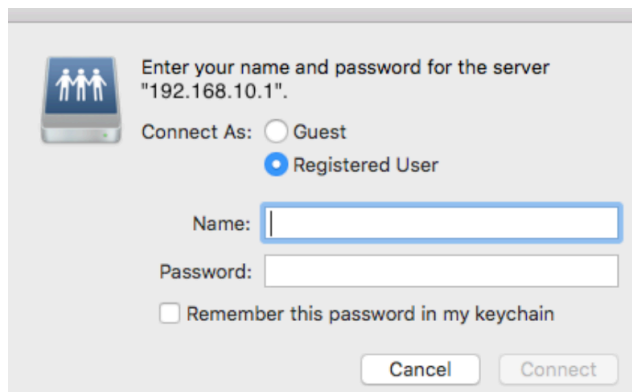
Go to Finder > Go > Connect to Server

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

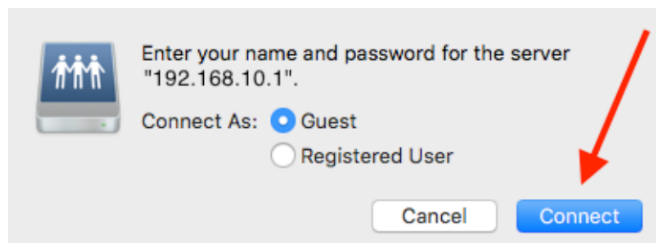
Select <Connect>



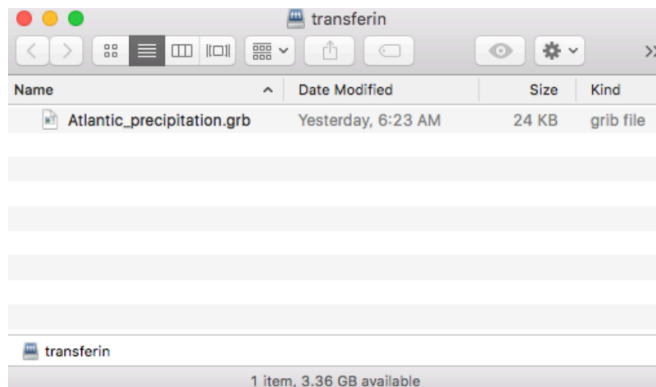
If the Shared Directory is restricted (i.e. does not Allow Guests) you must enter a username and password to access the files.



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.



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

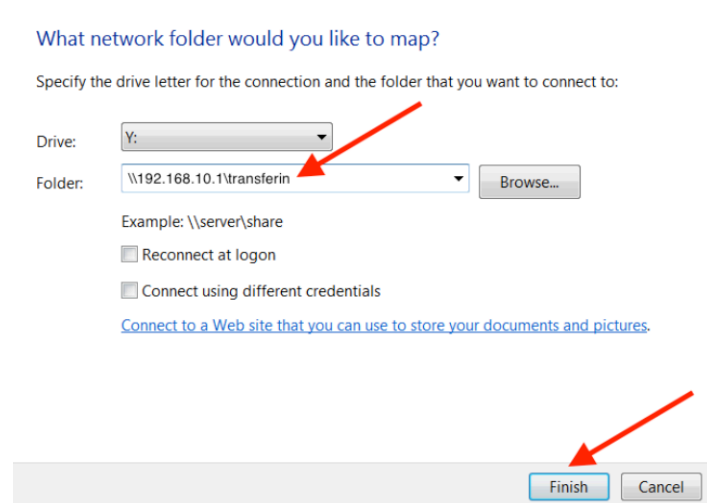


5.7.3.2. From a Windows PC

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 Aurora\the Path Folder.



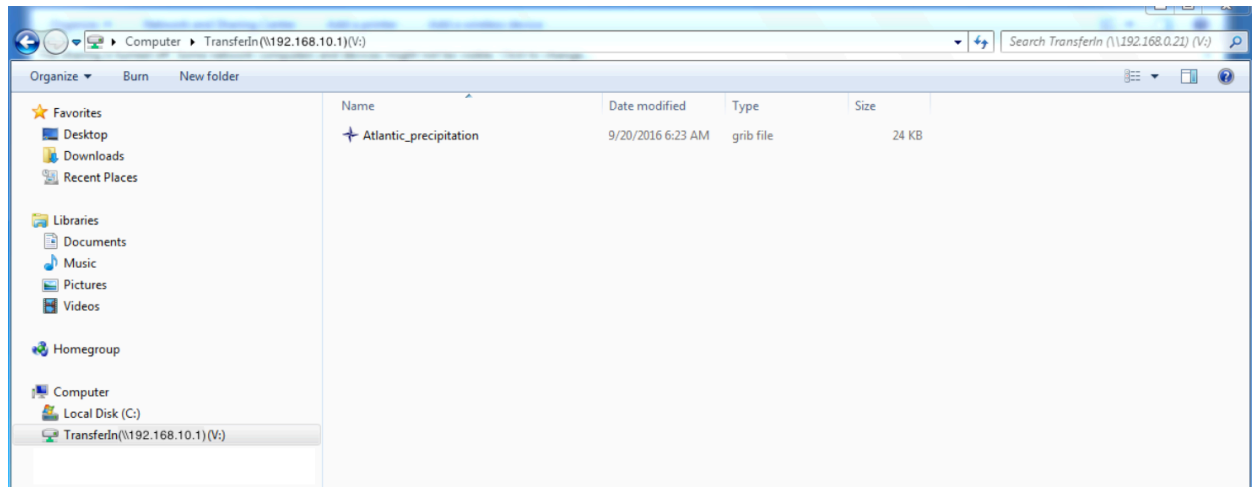
Select <Finish>.

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.

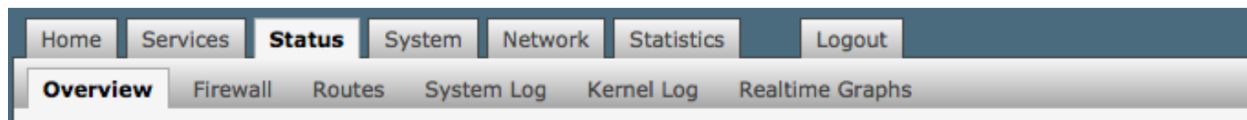
An Explorer window opens to the selected Folder for access to the transferred file(s).



6. Status

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

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



Some of the information provided here includes:

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

All Status information is READ ONLY.

7. 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).

The screenshot shows the 'System Settings' page in the Aurora router web interface. The top navigation bar includes 'Home', 'Services', 'Status', 'System' (selected), 'Network', 'Statistics', and 'Logout'. Below this, a sub-navigation bar shows 'System' (selected), 'Router Password', 'Profiles', 'Backup / Flash Firmware', and 'Reboot'. The main heading is 'System Settings', followed by the instruction: 'Here you can configure the basic aspects of your device like its hostname or the timezone.' Under 'System Properties', there are three tabs: 'General Settings' (selected), 'Logging', and 'Language and Style'. The 'General Settings' tab contains the following fields: 'Local Time' (displaying 'Tue Mar 29 16:46:39 2016' with a 'Sync with browser' button), 'Hostname' (text box containing 'Optimizer'), 'Timezone' (dropdown menu showing 'UTC'), and 'Disable anti-lockout rule' (checkbox, currently unchecked). A help text for the checkbox states: 'The anti-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**.' Below this is the 'Time Synchronization' section with an 'Enable NTP client' checkbox, which is also unchecked. At the bottom, there are three buttons: 'Reset' (with a red 'x' icon), 'Save' (with a green checkmark icon), and 'Save & Apply' (with a green checkmark and a right arrow icon).

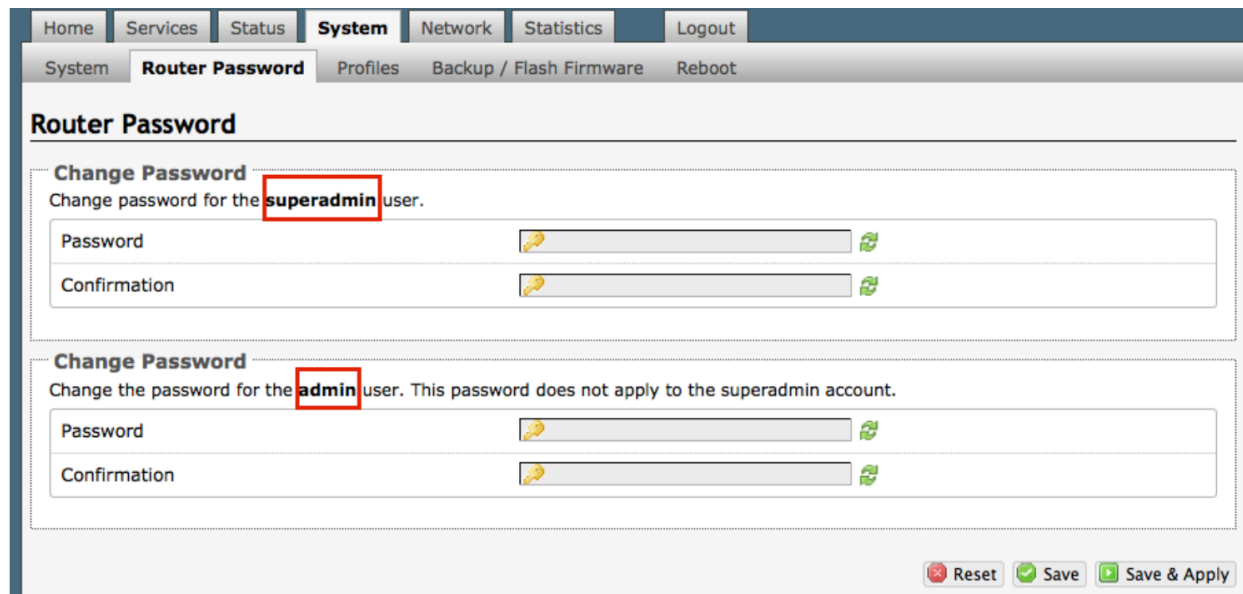
Disable anti-lockout rule: The anti-lock rule prevents you from creating a firewall rule that will lock you out of the router. The rule is Enabled when the box is Unchecked. *Best Practice is to complete the router configuration, test it thoroughly to make sure everything works as intended, then disable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



Use the top section to change the password for the 'superadmin' user. Use 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 User Interface.

7.3. Profiles

Requires 'superadmin' login.

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

The screenshot displays the Aurora web interface. At the top, there is a navigation bar with tabs: Home, Services, Status, System (selected), Network, Statistics, and Logout. Below this, a secondary bar contains links: System, Router Password, Profiles (selected), Backup / Flash Firmware, and Reboot. The main content area is titled 'Profile Manager' and includes a sub-tab 'Profiles' and a 'Tools' link. A text block explains: '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.' Below this is a 'Manage Profiles' section with a table. The table has two columns: 'Profile' and 'Description'. It contains one entry: 'Factory' with the description 'Factory default settings'. To the right of this entry are 'Install' and 'Delete' buttons. An 'Add' button is located below the table. At the bottom left is a 'Reset' button, and at the bottom right are 'Save' and 'Save & Apply' buttons.

Profile	Description	
Factory	Factory default settings	<input type="button" value="Install"/> <input type="button" value="Delete"/>

You can configure the Aurora for a specific configuration and save the profile. Have a profile for each configuration and select the appropriate as needed.

Once a profile is saved it can be exported for use in another Aurora.

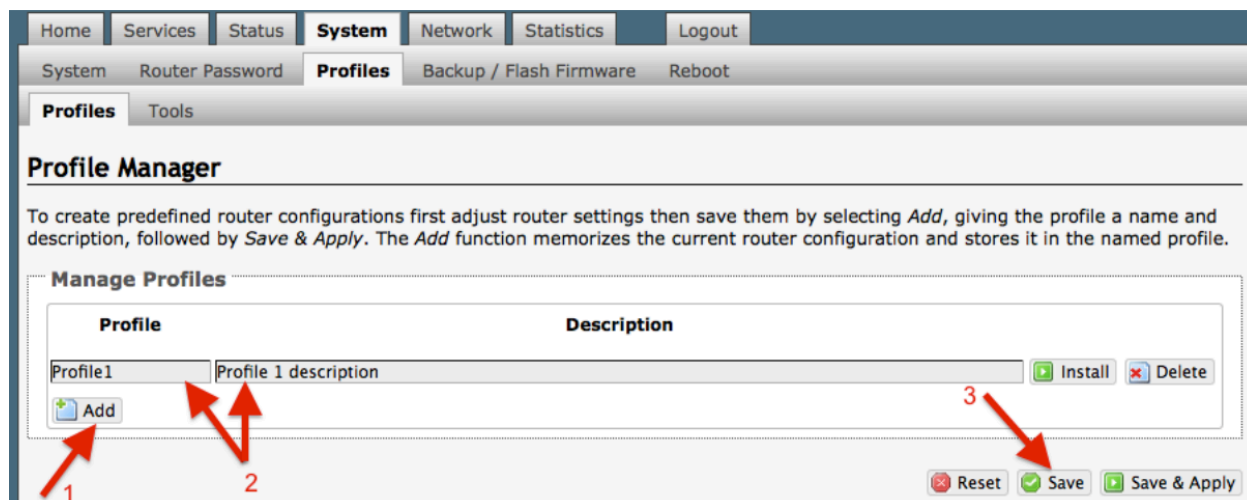
7.3.1. Add a Profile

Before adding a Profile, complete the router configuration.

Then access the Profile Manager.

To create and use the new Profile:

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



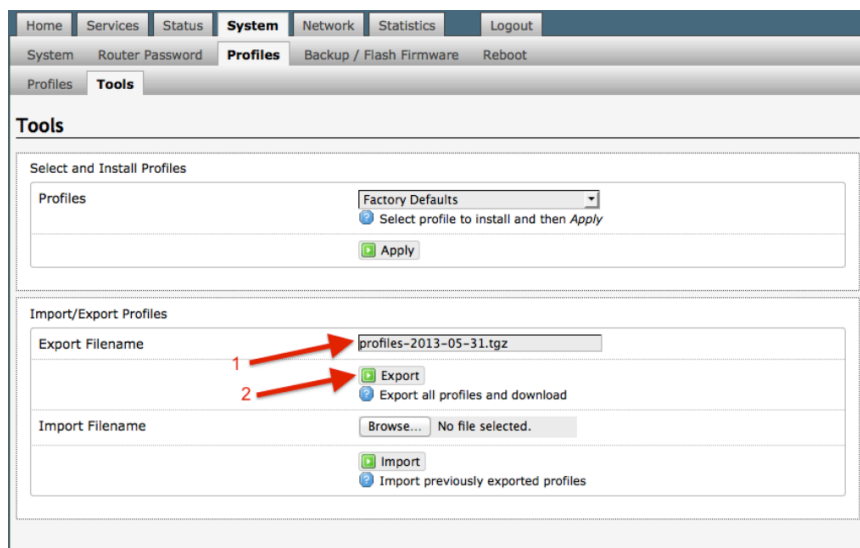
7.3.2. Change to Another Saved Profile

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

7.3.3. Export a Profile

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

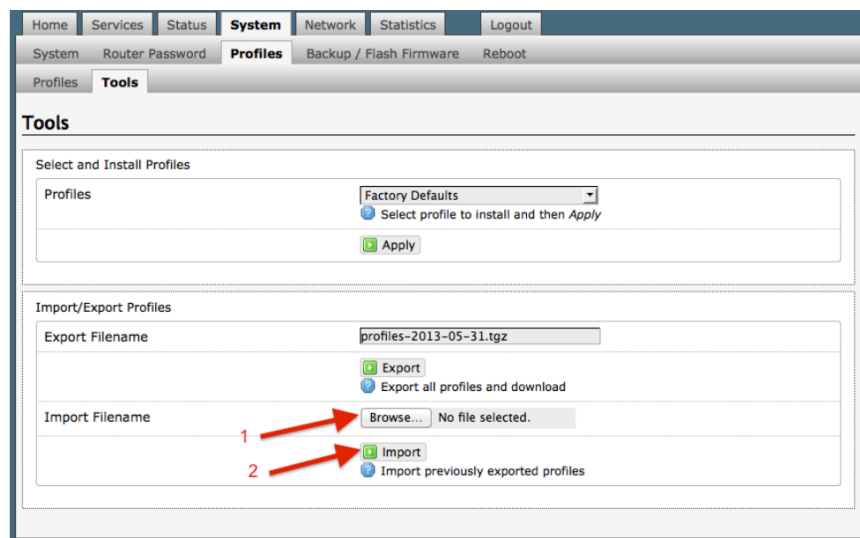
1. Enter a filename or use the default name.
2. Select <Export> and save the file.



7.3.4. Import a Profile

You can import profiles from another Aurora in System > Profiles > Tools.

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



7.4. Backup/Flash Firmware

Requires 'superadmin' login.

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



The screenshot shows the 'Backup / Flash Firmware' page in the Aurora web interface. The page has a navigation bar at the top with tabs: Home, Services, Status, System (selected), Network, Statistics, and Logout. Below the navigation bar, there are sub-tabs: System, Router Password, Profiles, Backup / Flash Firmware (selected), and Reboot.

The main content area is titled 'Flash operations' and contains several sections:



- Actions** (selected) and **Configuration** (unselected).
- 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:
 - Reset to defaults:
 - To restore configuration files, you can upload a previously generated backup archive here.
 - Restore backup: No file selected.
- 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: No file selected.
- Flash SD drive image**
 - Restore SD drive configuration files factory defaults.
 - Reset to defaults:
 - 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: No file selected.
- WiFi Extender**
 - Click to perform flash operations such as firmware update 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:

7.4.1. 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 routers (for example in a fleet situation) create and save a Profile of the configuration that can be applied to other routers. See Chapter 7.3.

7.4.2. Flash New Firmware Image

Get the latest Aurora 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.

The screenshot shows a web interface titled "Flash new firmware image". Below the title is a text instruction: "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." Below this instruction are three elements: a "Keep settings:" label with a checked checkbox (indicated by red arrow 1), an "Image:" label followed by a "Browse..." button and the text "No file selected." (indicated by red arrow 2), and a green "Flash image..." button (indicated by red arrow 3).

1. Keep Settings: check this box to maintain current settings if you have made changes to the configuration. Failure to check this box will revert the Aurora 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...This typically takes several minutes.

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

7.4.3. 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.

7.4.4. Wi-Fi Extender

Requires 'superadmin' login.

WiFi Extender
Click to perform flash operations such as firmware update 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 Wi-Fi Extender ONLY!

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

7.4.4.1. Backup / Restore Wi-Fi Extender

The screenshot shows a web interface titled "Flash operations" with two tabs: "Actions" and "Configuration". The "Configuration" tab is active. Under the "Backup / Restore" section, which is highlighted with a red box, there are three main actions:

- Download backup:** A button labeled "Generate archive" with a green download icon.
- Reset to defaults:** A button labeled "Perform reset" with a red reset icon.
- Restore backup:** A section with the text "To restore configuration files, you can upload a previously generated backup archive here." It includes a "Choose File" button, a status "no file selected", and an "Upload archive..." button with a green upload icon.

Below the "Backup / Restore" section is the "Flash new firmware image" section, which includes a "Keep settings:" checkbox (checked) and an "Image:" field with a "Choose File" button, a status "no file selected", and a "Flash image..." button with a green flash icon.

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

Reset to defaults: select <Perform reset> to reset the Wi-Fi Extender to the factory defaults.

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

7.4.4.2. Flash New Firmware Image - Wi-Fi Extender

Flash operations

Actions Configuration

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:

Reset to defaults:

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

Restore backup: no file selected

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).

Keep settings: ☒

Image: no file selected

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 Wi-Fi 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

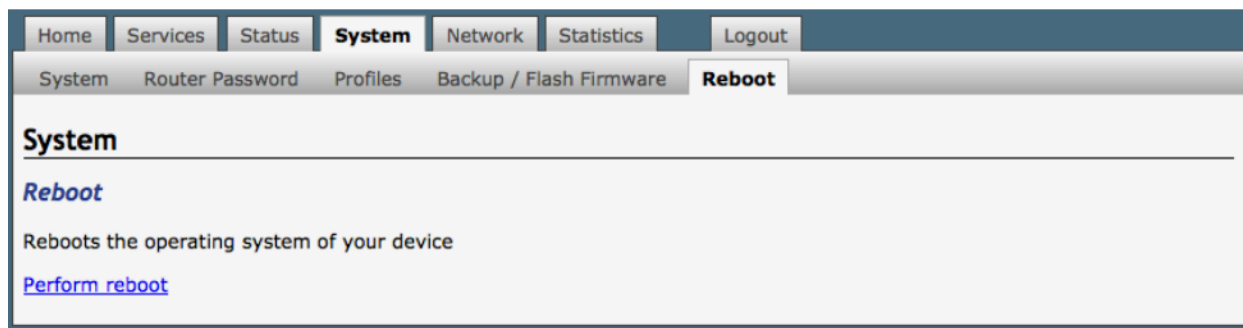
The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity. Click "Proceed" below to start the flash procedure.

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

Select <Proceed> to complete the process.

7.5. Reboot

You can reboot the Aurora Optimizer from within the user interface.



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. Network

Requires 'superadmin' login.

This section can be used to configure network interfaces, run diagnostics, or modify the firewall.

CAUTION: This gives you complete control over the router behavior. Creating conflicts in the configuration may render the router useless.

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

8.1. Interfaces

This screen is an at-a-glance view of the current status of each network interface. Modification to any of the interfaces may render the Aurora inoperative. **DO NOT MODIFY ANY OF THESE INTERFACES.**

The screenshot shows the Aurora web interface with the 'Network' tab selected. Under the 'Interfaces' sub-tab, there is an 'Interface Overview' section. It contains a table with four interfaces: WAN6, LAN, PPP, and WAN. Each interface row shows its name, status, uptime, MAC address, RX/TX statistics, and a set of action buttons (Connect, Stop, Edit, Delete). Below the table is a 'Global network options' section with a text input for 'IPv6 ULA-Prefix' containing the value 'fd6e:abac:e9f4::/48'. At the bottom of the interface are 'Reset', 'Save', and 'Save & Apply' buttons.

Network	Status	Actions
WAN6 @wan	Uptime: 0h 0m 0s MAC-Address: 00:00:00:00:00:00 RX: 29.88 MB (219018 Pkts.) TX: 1.69 MB (6502 Pkts.)	Connect Stop Edit Delete
LAN br-lan	Uptime: 22h 37m 13s MAC-Address: 00:0B:52:76:22:D9 RX: 669.52 KB (4356 Pkts.) TX: 265.43 KB (1087 Pkts.) IPv4: 192.168.10.1/24 IPv6: FD6E:ABAC:E9F4::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 eth0.2	Uptime: 21h 8m 23s MAC-Address: 00:00:00:00:00:00 RX: 29.88 MB (219018 Pkts.) TX: 1.69 MB (6502 Pkts.) IPv4: 192.168.0.25/24	Connect Stop Edit Delete

Global network options

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

Reset Save Save & Apply

The list below is presented for informational purposes only. We do not recommend making any edits to any Interface; doing so may render the Aurora useless. If your needs require modifying an interface, please contact your service provider for guidance.

LAN: this is reserved for the local area network (onsite).

PPP: this is reserved for USB connected satellite phones and GSM or LTE modems. Configuration for GSM use is done in the Network > PPP tab.

WAN: this is reserved for the internal working of the Aurora. DO NOT EDIT. Editing this interface will render the Aurora useless.

WEXT: this is reserved for the RedPort Wi-Fi Extender. DO NOT EDIT.

8.2. Wi-Fi

Requires "superadmin" login.

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

The screenshot shows the Aurora Optimizer web interface. The top navigation bar includes links for Home, Services, Status, System, **Network**, Statistics, and Logout. Below this, a sub-navigation bar shows Interfaces, **Wifi**, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall, and PPP. The main content area is titled "radio0: Master 'wXa-153-22d9'".

Wireless Overview

Generic MAC80211 802.11bgn (radio0)
 Channel: 11 (2.462 GHz) | Bitrate: 104 Mbit/s
 SSID: wXa-153-22d9 | Mode: Master
 BSSID: 00:0B:52:76:22:DB | Encryption: None

Buttons: Scan, Add, Disable, Edit, Remove.

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
wXa-153-22d9	7C:C3:A1:9D:EE:8A	192.168.10.142	-52 dBm	0 dBm	1.0 Mbit/s, MCS 0, 20MHz	104.0 Mbit/s, MCS 13, 20MHz

Scan: scans for other wireless hotspot signals available in the area.

Add: Add a new Wi-Fi interface. (NOT AVAILABLE on the Aurora Optimizer)

Disable: Disable the selected Wi-Fi interface but it remains on the list.

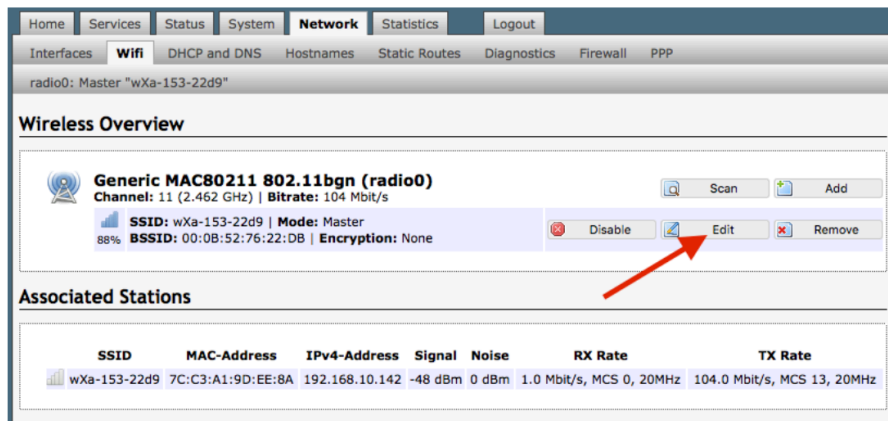
Edit: Edit the selected Wi-Fi interface

Remove: Remove the selected Wi-Fi interface

8.2.1. Rename the Wireless Network

The default name of the Aurora Optimizer wireless network is wXa-171-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.

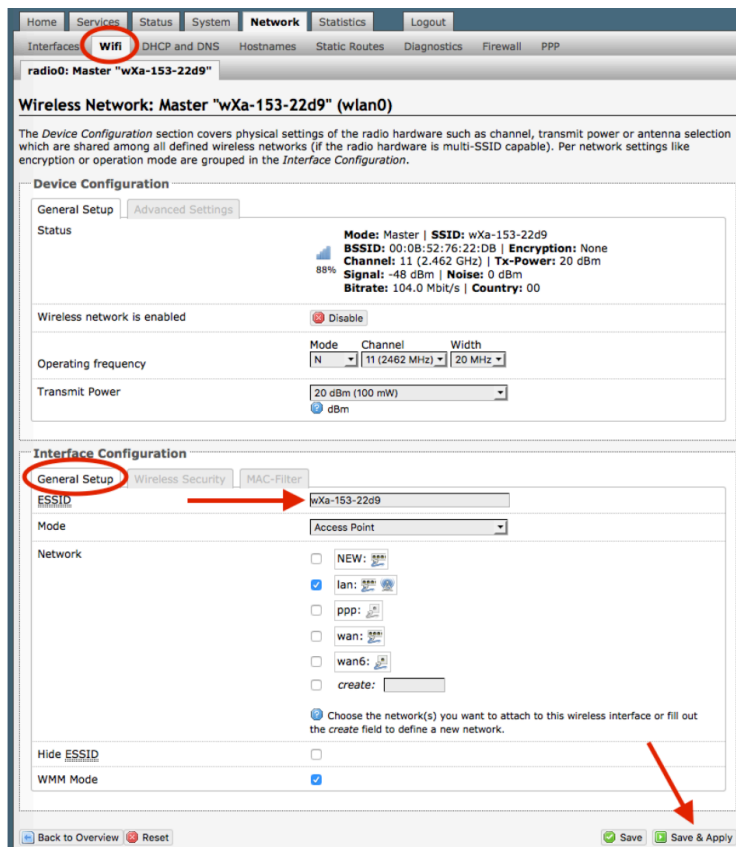
It is possible to change the name of your wireless network. Locate the wXa Wi-Fi network and select <Edit>



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

2. Click <Save & Apply>

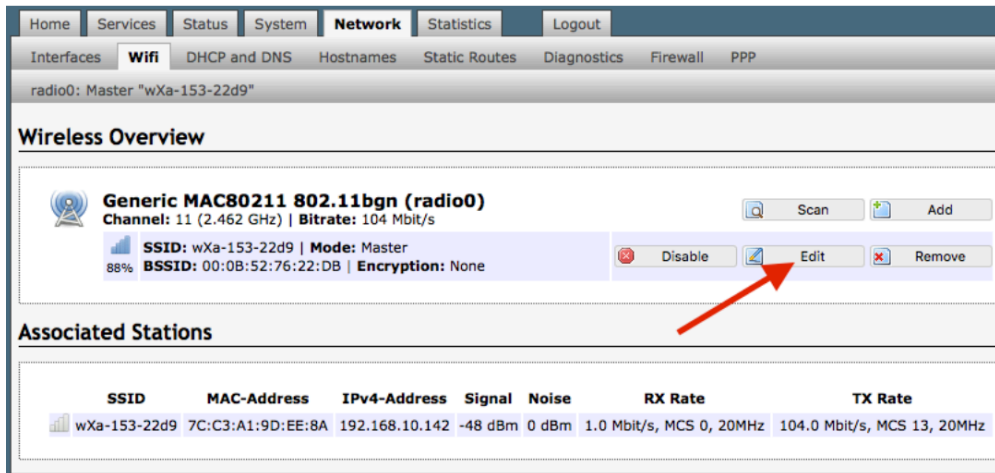
This procedure changes the name for the Wi-Fi hotspot only. When connecting your computer, iOS or Android device to the wireless network, this is the network name that will appear in the wireless network list. This name does not change the router superadmin or admin name when logging in to access the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



8.2.2. Restrict Wireless Network Access

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

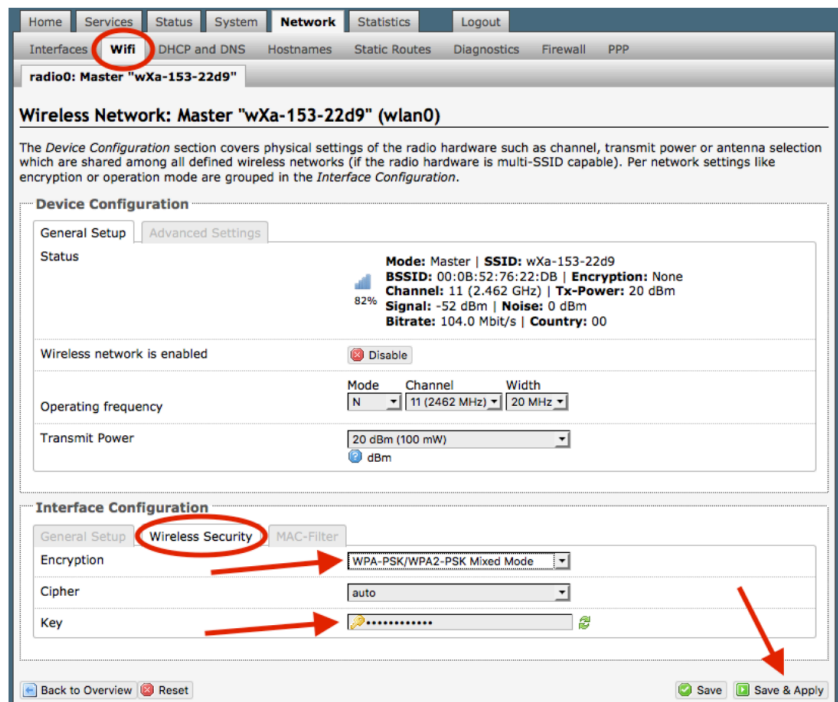
Locate the wXa Wi-Fi network and select <Edit>.



1. Select the Encryption mode from the dropdown menu.

2. Enter your desired password in the Key field.

3. Click <Save & Apply>



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

8.3. DHCP and DNS

Requires "superadmin" login.

The Aurora Optimizer is a DNS server. Under normal operating conditions you should not need to change anything here. If necessary, use this screen to modify the settings.

Home
Services
Status
System
Network
Statistics
Logout

Interfaces
Wifi
DHCP and DNS
Hostnames
Static Routes
Diagnostics
Firewall
PPP

DHCP and DNS

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

Server Settings

General Settings
Resolv and Hosts Files
TFTP Settings
Advanced 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

? 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

? List of domains to allow RFC1918 responses for

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
Marcuss-iMac	192.168.10.142	7c:c3:a1:9d:ee:8a	expired
Tophers-MBP	192.168.10.246	e0:f8:47:11:9f:fc	expired

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 identifies 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)
This section contains no values yet			

8.4. Hostnames

Requires "superadmin" login.

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

The screenshot shows the 'Hostnames' configuration page. At the top is a navigation bar with tabs: Home, Services, Status, System, Network (selected), Statistics, and Logout. Below this is a sub-navigation bar with tabs: Interfaces, Wifi, DHCP and DNS, Hostnames (selected), Static Routes, Diagnostics, Firewall, and PPP. The main content area is titled 'Hostnames' and contains a section 'Host entries'. This section has a table with two columns: 'Hostname' and 'IP address'. The first row shows 'Optimizer' as the hostname and '127.0.0.1' as the IP address. To the right of the IP address is a 'Delete' button. Below the table is an 'Add' button. At the bottom of the page are three buttons: 'Reset', 'Save', and 'Save & Apply'.

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.

This screenshot shows the same 'Hostnames' configuration page as the previous one, but with a red circle around the 'Hostnames' tab in the sub-navigation bar. Below the 'Host entries' table, the 'Add' button is highlighted with a red arrow labeled '1'. The 'NewHostName' input field is highlighted with a red arrow labeled '2'. The 'IP address' dropdown menu is open, showing a list of IP addresses and their corresponding MAC addresses, with the first option '192.168.0.225 (00:0d:b9:24:5a:34)' highlighted in blue. A red arrow labeled '3' points to this option. The 'Save & Apply' button is highlighted with a red arrow labeled '4'.

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.

The screenshot shows the 'Static Routes' configuration page in the Aurora web interface. The page has a top navigation bar with tabs: Home, Services, Status, System, **Network**, Statistics, and Logout. Below this is a sub-navigation bar with tabs: Interfaces, Wifi, DHCP and DNS, Hostnames, **Static Routes**, Firewall, Diagnostics, PPP, and Failover/Load Balancing. The main content area is titled 'Routes' and includes a descriptive text: 'Routes specify over which interface and gateway a certain host or network can be reached.'

There are two main sections for configuring static routes:

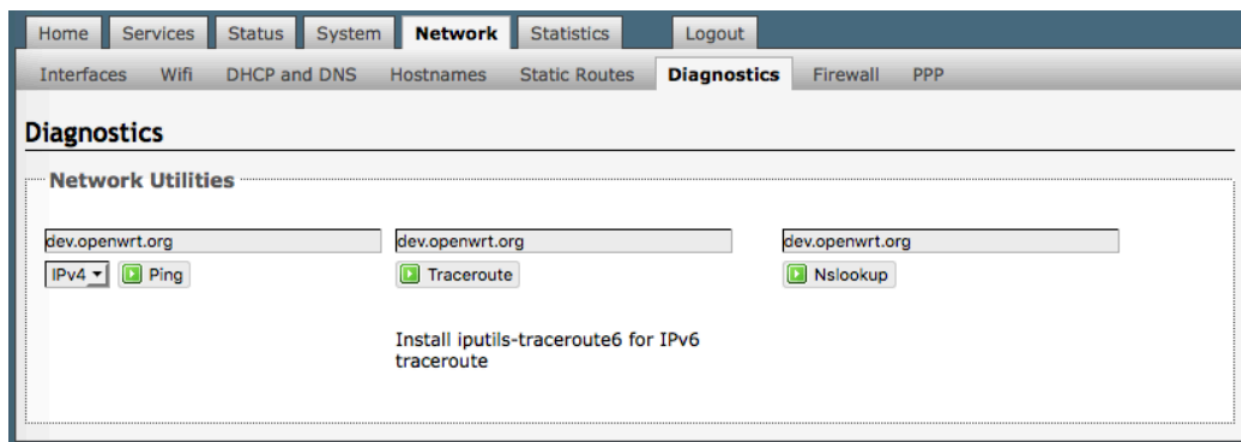
- Static IPv4 Routes:** This section contains a table with the following columns: **Interface** (with a dropdown arrow), **Target** (with a sub-note 'Host-IP or Network'), **IPv4-Netmask** (with a sub-note 'if target is a network'), **IPv4-Gateway**, **Metric**, and **MTU**. Below the table, it states 'This section contains no values yet' and there is an 'Add' button.
- Static IPv6 Routes:** This section contains a table with the following columns: **Interface** (with a dropdown arrow), **Target** (with a sub-note 'IPv6-Address or Network (CIDR)'), **IPv6-Gateway**, **Metric**, and **MTU**. Below the table, it states 'This section contains no values yet' and there is an 'Add' button.

At the bottom of the page, there are three buttons: 'Reset' (with a red 'x' icon), 'Save' (with a green checkmark icon), and 'Save & Apply' (with a green checkmark and a document icon).

8.6. Diagnostics

Requires "superadmin" login.

There are several Diagnostic tools available:



Ping: tells if you have ip connectivity

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

Nslookup: returns the ip address of whatever is entered into the text box.

8.7. Firewall

Requires "superadmin" login.

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

CAUTION: It is important to have an in-depth understanding of network administration including management and maintenance of routers, firewalls, etc. before attempting to modify

8.7.1. 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. **We do not recommend making any edits to any Interface; doing so may render the Aurora useless. If your needs require modifying an interface, please contact your service provider for guidance.**

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.

The screenshot shows the 'Firewall - Zone Settings' page. The top navigation bar includes 'Home', 'Services', 'Status', 'System', 'Network' (selected), 'Statistics', and 'Logout'. Below this, a sub-navigation bar shows 'Interfaces', 'Wifi', 'DHCP and DNS', 'Hostnames', 'Static Routes', 'Diagnostics', 'Firewall' (selected), and 'PPP'. The main content area is titled 'Firewall - Zone Settings' and includes a description: '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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete
cap: (empty)	→ ACCEPT	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
lan: lan	→ ppp wan	reject	accept	reject	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
wan: wan	→ REJECT	accept	accept	reject	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Edit Delete

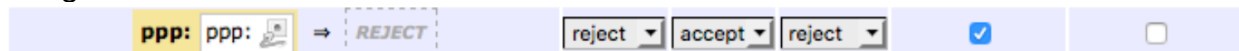
At the bottom of the table is an 'Add' button. At the bottom of the page are 'Reset', 'Save', and 'Save & Apply' buttons.

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

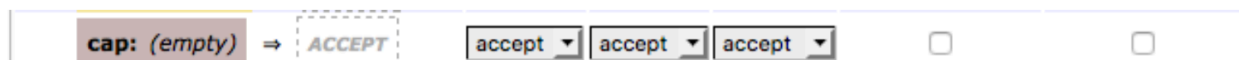
Reject: this setting will block traffic unless there is a Rule to allow it. An error is displayed to the end user.

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

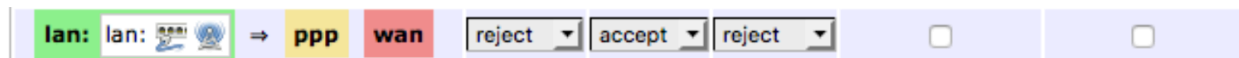
The router is shipped to you with several Firewall Zones configured and interfaces assigned to them:



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



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



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



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

We do not recommend making any edits to any Interface; doing so may render the Aurora useless. If your needs require modifying an interface, please contact your service provider for guidance.

8.7.1.1. Add a Firewall Zone

To create a new Firewall Zone, select the Add icon on the General Settings page. Enter the desired General and Advanced Settings. Select <Save & Apply>.

Firewall - Zone Settings - 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.

General Settings | **Advanced Settings**

Name: newzone

Input: reject

Output: accept

Forward: reject

Masquerading: ☐

MSS clamping: ☐

Covered networks:

- ☐ NEW:
- ☐ lan:
- ☐ ppp:
- ☐ wan:
- ☐ wan6:
- ☐ 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: (empty)
- ☐ lan: lan:
- ☐ ppp: ppp:
- ☐ wan: wan:

Allow forward from source zones:

- ☐ cap: (empty)
- ☐ lan: lan:
- ☐ ppp: ppp:
- ☐ wan: wan:

Buttons: Back to Overview, Save, Save & Apply

8.7.1.2. Delete a Firewall Zone

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

CAUTION: This action **CANNOT** be undone.

Zone ⇒ Forwardings		Input	Output	Forward	Masquerading	MSS clamping		
ppp: ppp:	⇒ REJECT	reject	accept	reject	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
cap: (empty)	⇒ ACCEPT	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>		
lan: lan:	⇒ ppp wan	reject	accept	reject	<input type="checkbox"/>	<input type="checkbox"/>		
wan: wan:	⇒ REJECT	accept	accept	reject	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
newzone: (empty)	⇒ REJECT	reject	accept	reject	<input type="checkbox"/>	<input type="checkbox"/>		

8.7.2. 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		

Reset Save Save & Apply

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	<input checked="" type="checkbox"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

New port forward:

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

Add

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

CAUTION: The Delete function cannot be undone.

8.7.3. Firewall Rules

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

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

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

The BLOCK WAN rule is designed to prevent you from locking yourself out of the router as you perform your initial configuration. See Chapter 7.1.

The remaining rules, when Enabled, Allow that particular traffic to pass through the firewall.

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

The rule name "ALL", when enabled, means the firewall is totally open and all traffic 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, if enabled.

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

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

- Disable (uncheck) the first rule "ALL-DO NOT MODIFY". This forces the remaining "enabled" rules to take precedent.
-

Home Services Status System **Network** Statistics Logout

Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics **Firewall** PPP

General Settings Port Forwards **Firewall Rules** IPset

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	Sort
BLOCK WAN DO_NOT_MODIFY	Any traffic From <i>any host in wan</i> To <i>any router IP on this device</i>	Discard input	<input type="checkbox"/>	
ALL DO_NOT_MODIFY	Any traffic From <i>any host in any zone</i> To <i>any host in any zone</i>	Accept forward	<input type="checkbox"/>	
PASS DNS DO_NOT_MODIFY	Any UDP From <i>any host in any zone</i> To <i>any host, port 53 in any zone</i>	Accept forward	<input type="checkbox"/>	
DNS DO_NOT_MODIFY	Any UDP From <i>any host in any zone</i> To <i>any router IP at port 53 on this device</i>	Accept input	<input type="checkbox"/>	
HTTP DO_NOT_MODIFY	Any TCP From <i>any host in any zone</i> To <i>any host, port 80 in any zone</i>	Accept forward	<input type="checkbox"/>	
HTTPS DO_NOT_MODIFY	Any TCP From <i>any host in any zone</i> To <i>any host, port 443 in any zone</i>	Accept forward	<input type="checkbox"/>	
FTP DO_NOT_MODIFY	Any TCP From <i>any host in any zone</i> To <i>any host, ports 20-21 in any zone</i>	Accept forward	<input type="checkbox"/>	

Open ports on router:

Name	Protocol	External port
New input rule	TCP+UDP	

New forward rule:

Name	Source zone	Destination zone
New forward rule	lan	wan

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort
This section contains no values yet				

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port
New SNAT rule	lan	wan	-- Please choose	Do not rewrite

Reset Save Save & Apply

- Disable (uncheck) the rule "HTTP-DO NOT MODIFY". This blocks http traffic from passing through the firewall.

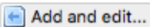
With the ALL rule disabled (unchecked) you can enable/disable the others very quickly. The next one is DNS. Do you want DNS? Yes (checked), No (unchecked). Do you want http? Yes (checked), No (unchecked), etc.

You can also create a custom rule.

8.7.3.1. Create a Custom Rule

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

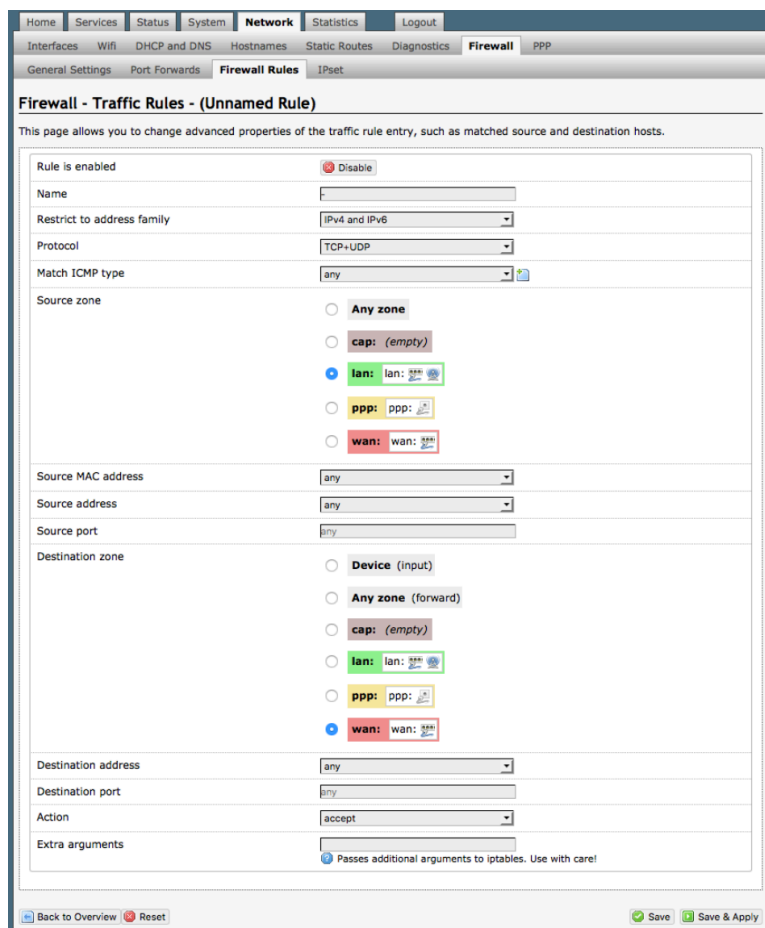
New forward rule:

Name	Source zone	Destination zone	
<input type="text" value="New forward rule"/>	<input type="text" value="lan"/>	<input type="text" value="wan"/>	

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. See IP Sets (Chapter 8.7.4) for creating block and allow rules by domain name instead of ip address.



Home Services Status System **Network** Statistics Logout

Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics **Firewall** PPP

General Settings Port Forwards **Firewall Rules** IPset

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

Protocol

Match ICMP type

Source zone




- ☐ Any zone
- ☐ cap: (empty)
- ☒ lan: lan: 
- ☐ ppp: ppp: 
- ☐ wan: wan: 

Source MAC address

Source address

Source port

Destination zone

- ☐ Device (input)
- ☐ Any zone (forward)
- ☐ cap: (empty)
- ☐ lan: lan: 
- ☐ ppp: ppp: 
- ☒ wan: wan: 

Destination address

Destination port

Action

Extra arguments

☒ Passes additional arguments to iptables. Use with care!

[Back to Overview](#) [Reset](#) [Save](#) [Save & Apply](#)

8.7.4. 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.

The screenshot shows the 'IP Sets' configuration page. At the top, there are navigation tabs: Home, Services, Status, System, Network (selected), Statistics, and Logout. Below these are sub-tabs: Interfaces, Wifi, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall (selected), and PPP. Under the Firewall tab, there are further sub-tabs: General Settings, Port Forwards, Firewall Rules, and IPset (selected). The main heading is 'IP Sets' with a description: 'Block, Allow, or Define groups of domains to be used by the firewall and/or the load balancer.' Below this is a table with three columns: 'IPset Name' (Unique Name), 'Action' (Filtering Action), and 'Domains' (Domain(s) to Filter). The table contains one entry: 'ipset' with a red 'x' icon, 'Block' as the action, and 'domain' as the domain. There is an 'Add' button with a plus icon and a 'Delete' button with a red 'x' icon. At the bottom left is a 'Reset' button, and at the bottom right are 'Save' and 'Save & Apply' buttons.

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

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

Action Definitions:

Block: rejects the domain

Pass: allows the domain

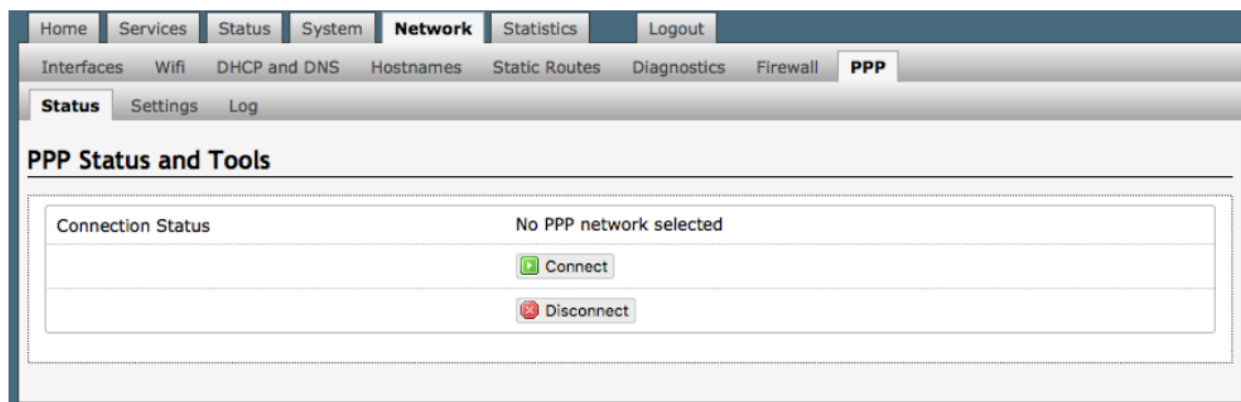
You can group multiple domain names into one IP set rule.

8.8. PPP

Requires "superadmin" login.

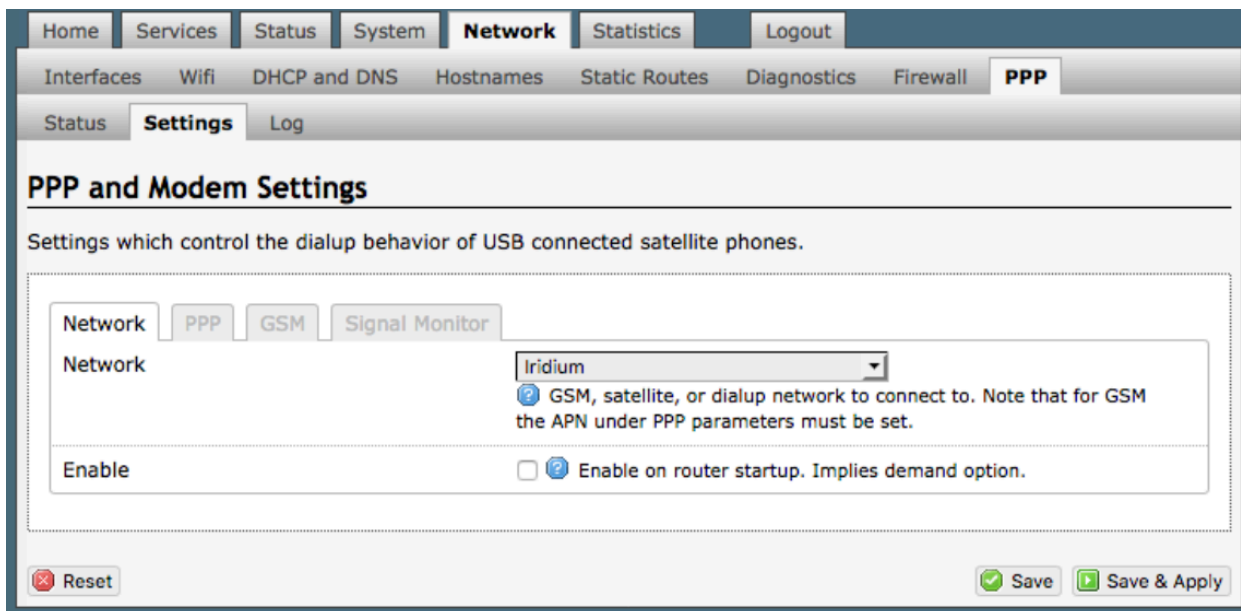
By default, the PPP Settings are configured for the Iridium satellite network. It is possible to use either the Aurora terminal or the optional built-in GSM modem that does PPP to connect for email and web browsing.

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.



8.8.1. PPP Settings for Aurora

The Aurora arrives preconfigured for use on the Iridium network.



The PPP Settings apply to both the Aurora and the optional GSM modem.

The screenshot shows the Aurora web interface with the 'Network' tab selected. Under 'Network', the 'Settings' sub-tab is active and circled in red. Within the 'Settings' sub-tab, the 'PPP' sub-tab is also circled in red. The main heading is 'PPP and Modem Settings'. Below this, a description states: 'Settings which control the dialup behavior of USB connected satellite phones.' The configuration area has four sub-tabs: 'Network', 'PPP' (selected), 'GSM', and 'Signal Monitor'. The 'PPP' sub-tab contains the following settings:

- Modem Interface:** A dropdown menu set to 'System Default'. A help icon indicates: 'Select COM port assigned to modem.'
- Modem Speed:** A dropdown menu set to 'System Default'. A help icon indicates: 'Baud rate for modem serial interface.'
- Username:** A text input field. A help icon indicates: 'Leave blank if none required.'
- Password:** A text input field. A help icon indicates: 'Leave blank if none required.'
- Phone Number:** A text input field. A help icon indicates: 'Phone number to dial. Leave blank for system default.'
- Idle Timeout:** A text input field with '60' entered. A help icon indicates: '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:** A checkbox that is unchecked. A help icon indicates: 'Enable persistent connections. Persistent connections forces the modem to reconnect if connection drops.'
- Demand:** A checkbox that is unchecked. A help icon indicates: 'Initiate the link only on demand, i.e. when data traffic is present. Implies the Persist.'
- Extra Init:** A text input field. A help icon indicates: 'Extra modem initialization. Leave blank if not required. Enter full AT command (including AT) to send to the modem before dialing.'
- MTU:** A text input field. A help icon indicates: 'Set the MTU [Maximum Transmit Unit] value in bytes. Leave blank for system default.'
- debug:** A checkbox that is unchecked. A help icon indicates: 'Write PPP connection debugging information to the system log.'

At the bottom of the form, there are three buttons: 'Reset' (with a red 'x' icon), 'Save' (with a green checkmark icon), and 'Save & Apply' (with a green checkmark icon).

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 Aurora Optimizer is pre-configured with the standard number to dial for the Iridium satellite network. 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	<input type="text"/> <small>Time in seconds between reconnection attempts. Leave blank for default value of 30.</small>
Maximum Fail	<input type="text"/> <small>Maximum reconnection fail attempts before giving up. Leave blank for infinite retries.</small>

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 reconnect. 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 is reached. With Demand selected, Persist is implied. See Persist above.

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 for GSM

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

If you have GSM-based based cellular service, it may be possible to use the GSM network, when available, for Email and Web Browsing data over the Aurora 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. **Requires a valid SIM card inserted into the optional GSM modem built-in to the Aurora dome.**

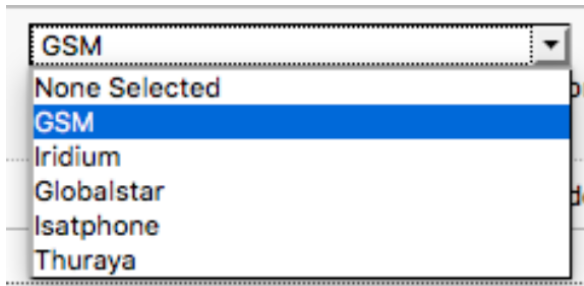
Only GSM-based service and LTE-based service with a valid SIM card can be configured here. CDMA-based service will NOT work. If you are unsure of which service you have, contact your cellular provider before attempting to configure for connection.

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

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

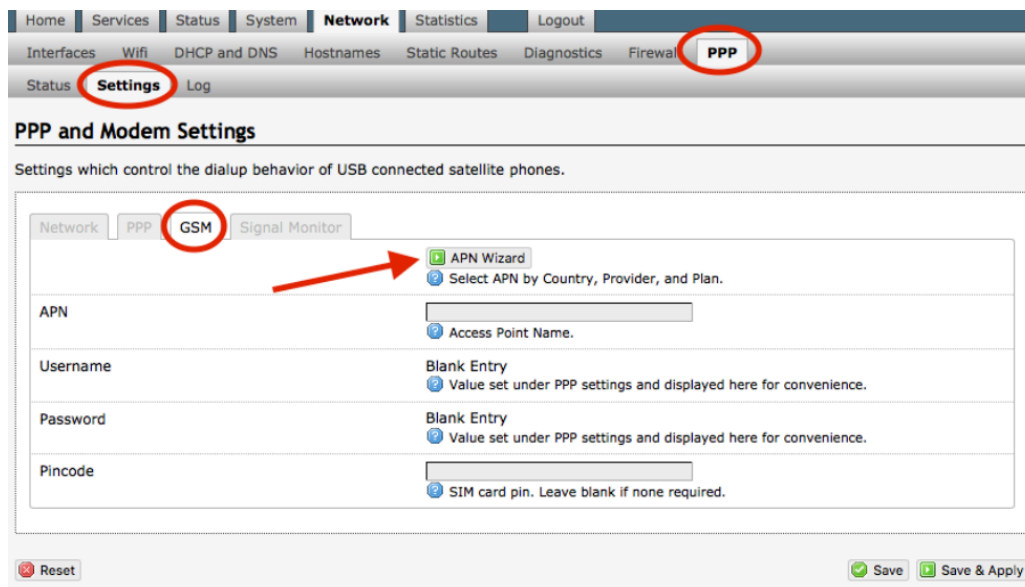
The screenshot shows the Aurora Optimizer web interface. The top navigation bar includes tabs for Home, Services, Status, System, Network, Statistics, and Logout. The 'Network' tab is active, and the 'PPP' sub-tab is selected. Below the navigation bar, the 'Settings' tab is also selected. The main content area is titled 'PPP and Modem Settings' and contains a sub-header: 'Settings which control the dialup behavior of USB connected satellite phones.' There are three tabs: 'Network', 'PPP', and 'GSM'. The 'Network' tab is selected. Under the 'Network' tab, there is a 'Network' label, a dropdown menu showing 'None Selected', and a checkbox labeled 'Enable'. A red arrow labeled '1' points to the 'Enable' checkbox. A red arrow labeled '2' points to the dropdown menu. A red arrow labeled '3' points to the 'Save & Apply' button at the bottom right. At the bottom left, there is a 'Reset' button.

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



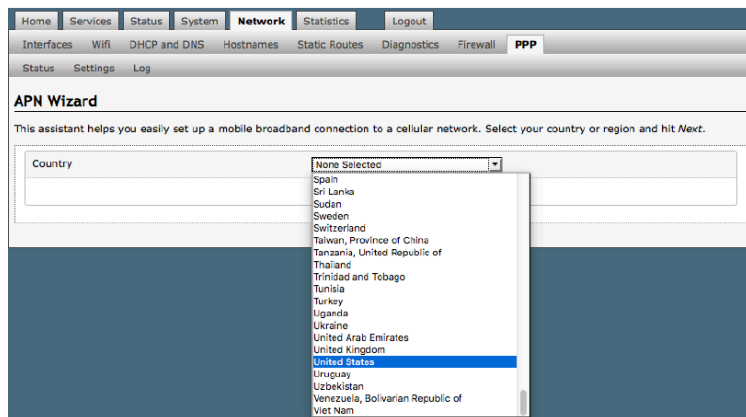
3. Select <Save & Apply> to apply the change. Move to the Settings > GSM Tab: Before you can configure for GSM, you must:

- Activate service with your GSM provider.
- Insert the GSM SIM card into the GSM modem under the dome of the Aurora.

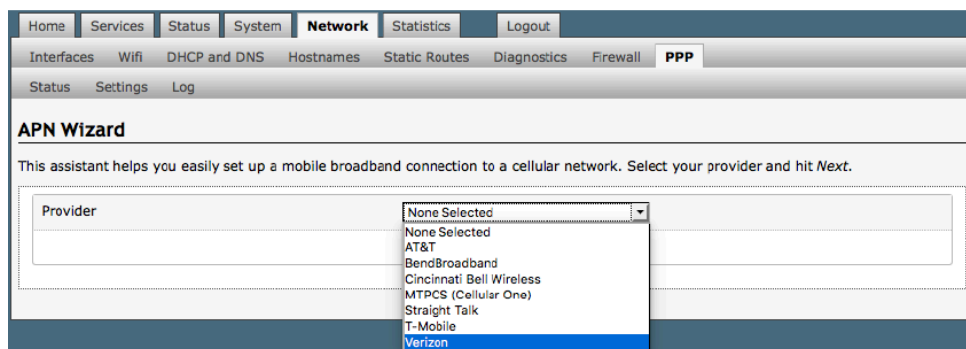


The APN Wizard contains many GSM providers and plans. Using it will automatically set the configuration for you. Select <APN Wizard> to start the configuration:

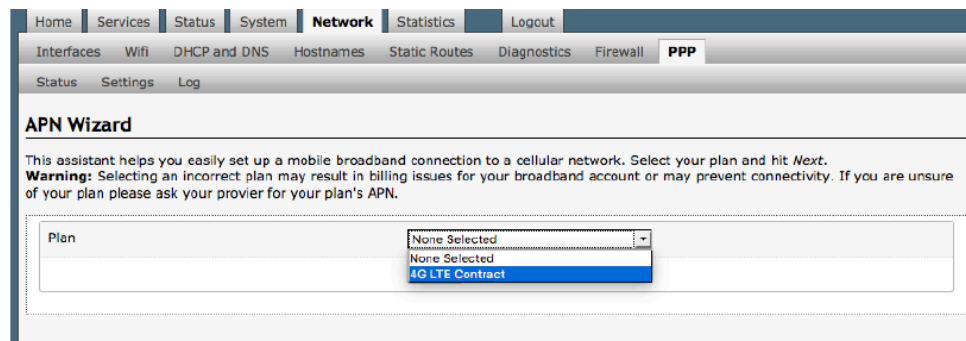
Select the appropriate country from the dropdown list and then, <Next>.



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



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



Home Services Status System **Network** Statistics Logout

Interfaces Wifi DHCP and DNS Hostnames Static Routes Diagnostics Firewall **PPP**

Status **Settings** Log

PPP and Modem Settings

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

GSM Network **PPP** Signal Monitor

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

APN Wizard
 Select APN by Country, Provider, and Plan.

APN	vzwinternet Access Point Name.
Username	Blank Entry Value set under PPP settings and displayed here for convenience.
Password	Blank Entry Value set under PPP settings and displayed here for convenience.
Pincode	SIM card pin. Leave blank if none required.

Reset Save Save & Apply

If you have protected your cellular SIM card with a PIN-Code, enter the PINCode 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:

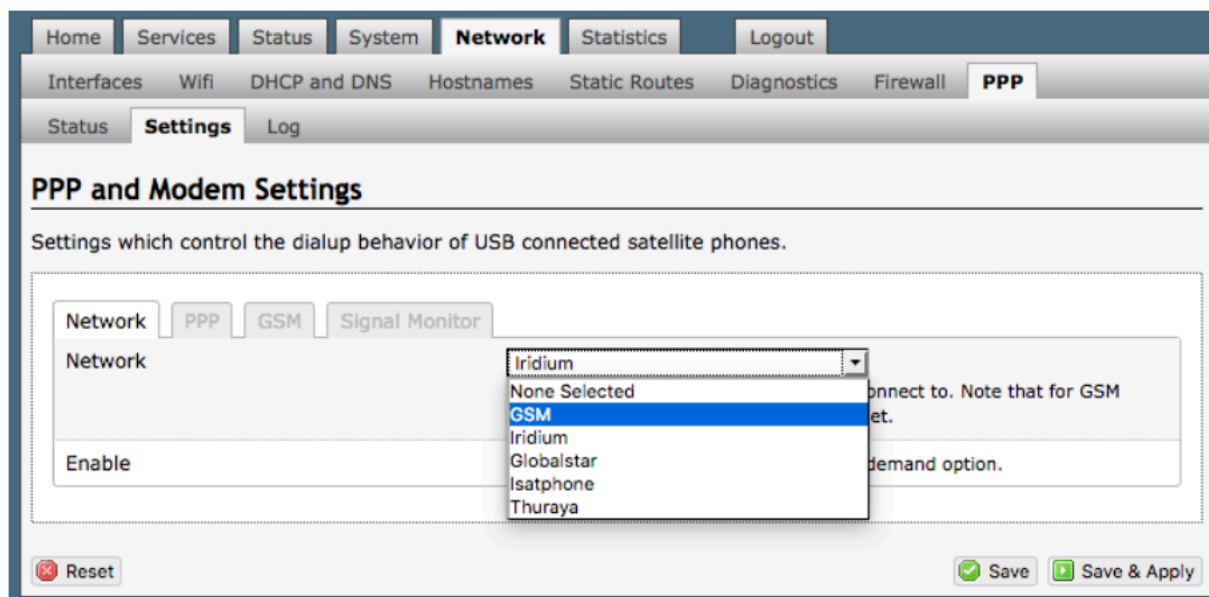
- Access Point Name (APN)
- Username required for access to the APN
- Password required for access to the APN

Enter the required information in the PPP Settings pages.

See Section PPP Settings.

8.8.2.1. Using GSM

When you want to use GSM service instead of satellite service simply change the PPP > Settings > Network selection:



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 Aurora 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.

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

The screenshot shows the Aurora web interface. The top navigation bar includes links for Home, Services, Status, System, Network (selected), Statistics, and Logout. Below this, a sub-navigation bar shows Interfaces, Wifi, DHCP and DNS, Hostnames, Static Routes, Diagnostics, Firewall, and PPP (selected). The main content area is titled 'PPP and Modem Settings' and includes a sub-header 'Settings which control the dialup behavior of USB connected satellite phones.' There are four tabs: GSM, Network, PPP, and Signal Monitor (selected). The Signal Monitor settings include an 'Enable' checkbox which is checked, with a tooltip that says 'Enable/Disable signal monitoring during connections.' Below this is a 'Level' input field set to '60', with a tooltip that says 'Allow satellite or GSM connections only if signal strength is larger than this value.' At the bottom left is a 'Reset' button, and at the bottom right are 'Save' and 'Save & Apply' buttons.

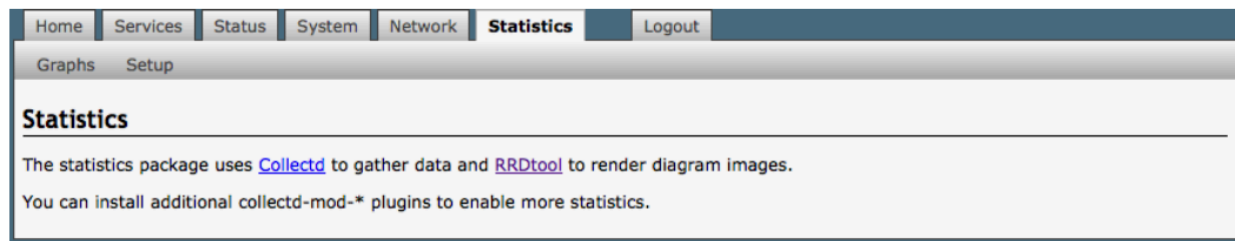
You can change the level of the Signal Monitor. Keep in mind that 60% is typically the minimum required for a successful data connection. If you must change the Signal Monitor, we recommend lowering the Level vs. disabling it.

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>.

9. Statistics

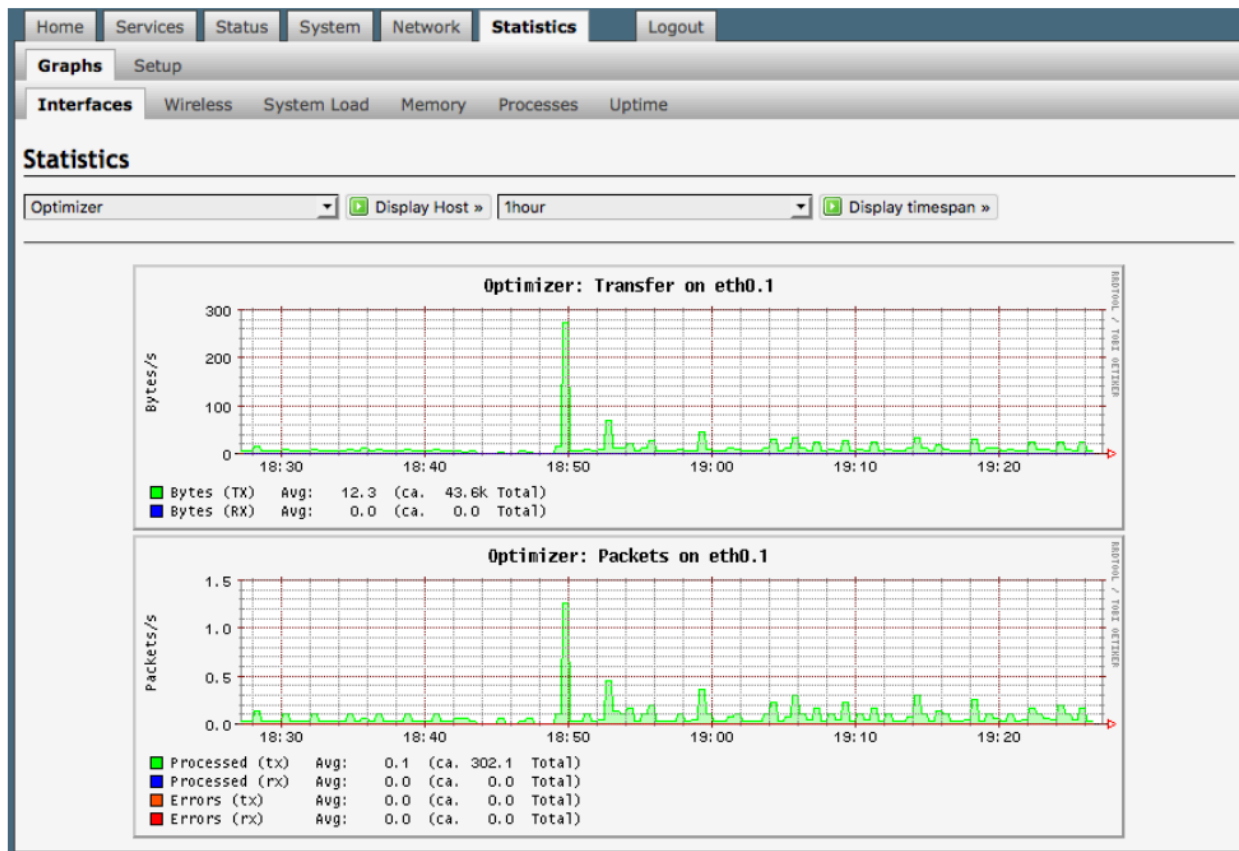
Requires "superadmin" login



9.1. Graphs

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

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



10. Installers Guidelines for Customization

Installer's Guidelines for Aurora Customization		
The Router is shipped to you in the following Default State: <i>Legend: E= Enabled, D=Disabled, O=Open, C=Closed</i>		
Firewall	C	
DNS	C	
RedPort Email	D	
SMS	E	
GPS Tracking	D	
GPS NMEA Repeat	D	
Voice	D	
No customization is required to use with an Active Primary XGate Email and/or XWeb Browsing Account.		
This list below is designed as a general guideline for customizing the router to meet your needs.		
Configuration	Actions	Location in the UI
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 Messaging		
	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 Calls Using Smartphones		
	1 Must be enabled	Services > Voice PBX > Settings
	2 Configure Extensions	Services > Voice PBX > Extensions
Please refer to the Aurora Advanced User Guide for more information.		

11. Login Access Table

This table shows the portions of the user interface that are available when using the different login credentials.					
	Login			Login	
	admin	superadmin		admin	superadmin
Home Page	✓	✓	Status Tab - All	✓	✓
Tasks	✓	✓	System Tab		✓
Aurora/MCG-101	✓	✓	System Settings		✓
			General Settings		✓
Services Tab		✓	Logging		✓
RedPort Email		✓	Language and Style		✓
General		✓	Router Password	from Home Page	✓
General Settings		✓	Profiles		✓
Webmail Settings		✓	Profiles Manager		✓
Network Settings		✓	Tools		✓
Log Settings		✓	Back/Flash Firmware		✓
Mail Filtering		✓	Actions		✓
Connection		✓	Configuration		✓
Filters		✓	Router Reboot	from Home Page	✓
Primary Accounts		✓	Network Tab		✓
Crew Accounts	from Home Page	✓	Interfaces		✓
File Transfer		✓	WiFi	from Home Page	✓
Spool		✓	DHCP and DNS		✓
Tools	from Home Page	✓	General Settings		✓
BigMail	from Home Page	✓	Resolv & Host Files		✓
Logs		✓	TFTP Settings		✓
Transaction Log		✓	Advanced Settings		✓
POP Log		✓	Hostnames		✓
SMTP Log		✓	Static Routes		✓
Usage CDRs		✓	Diagnostics		✓
Connection Report		✓	Firewall		✓
GPS Tracking		✓	General Settings		✓
SMS		✓	Port Forwards		✓
Settings		✓	Traffic Rules		✓
Management		✓	IPset		✓
WiFi Extender		✓	PPP		✓
GPS/NMEA Repeater		✓	Status		✓
Voice PBX		✓	Settings		✓
Settings		✓	Network		✓
Extensions		✓	PPP		✓
CDR		✓	GSM		✓
Logs		✓	Signal Monitor		✓
Network Shares	✓	✓	Log		✓
General Settings	✓	✓	Statistics Tab - All	✓	✓
Edit Template	✓	✓	Logout	✓	✓

12. Product Support Information

12.1. Product Warranty Information

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

What is covered by this limited hardware warranty?

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

What is not covered by this limited hardware warranty?

This limited hardware warranty does not cover:

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

12.2. Product Support Information

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

FEATURE	DESCRIPTION	DETAILS FOR WARRANTY
Remote Email Support	Customer may contact their RedPort dealer or support@redportglobal.com to report an issue.	1 year included in RedPort hardware purchase
Remote Live Technical Support	Customer may contact their RedPort dealer or support@redportglobal.com to report an issue.	Up to 30 minutes of free phone support included during warranty period. Additional time available for purchase.

12.3. RedPort Company Contact Information

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

RedPort Company Information

For product orders, support or returns, please contact:

Phone: +1 865.379.8723

Email: info@redportglobal

Sales: sales@redportglobal.com

Web: redportglobal.com

RedPort Address

RedPort Global

3224 Wrights Ferry Road

Louisville, TN 37777

United States of America