SatStation EdgeMate User's Guide

Welcome to the SatStation EdgeMate, your gateway to monitoring, configuring, and logging high performance DC changing systems. EdgeMate is a small appliance that once installed can be used to:

- Combine 2 independent CAN bus networks allowing all or selected data to transfer between them.
- Sample, display, and log NMEA 0183 and NMEA 2000.
- Provide Internet connectivity to many devices on a vessel with flexible routing and firewall filtering capabilities. Internet connections supported are USB connected Android or iOS devices, Wi-Fi bridge to an internet connected hotspot such as a Netgear Aircard or Verizon JetPack, or an Ethernet connection to an Internet connected satellite terminal or vessel router.
- Allow remote support connectivity to experts and technicians for analysis, diagnostics, and configuration of DC changing systems.

Table of Contents

Powering the EdgeMate

The EdgeMate can be powered with either the supplied AC/DC power supply or directly from the vessel's house battery bank. The unit requires 9-60 VDC and is reverse polarity protected. The center pin of the power connector is positive.

To wire the EdgeMate directly to the vessel's house battery, start by cutting the power lead off of the supplied AC/DC adapter. Connect a 1 amp fuse to the positive power lead (The Black wire is Positive, the wire with a White stripe is Negative) and wire to the vessel’s switch panel. Before powering the EdgeMate, use a voltmeter to ascertain that the center pin in the connector has positive current. Reversing the polarity on the connector will not damage the EdgeMate, but it will prevent it from powering on.

You will notice a blue status LED on the top of the unit illuminates when the unit is correctly powered on.

Accessing the Web User Interface

Once powered on, the EdgeMate needs to be configured to select the GPS data source, establish an Internet connection, to enable and set the tracking interval, and to password secure it's Wi-Fi.

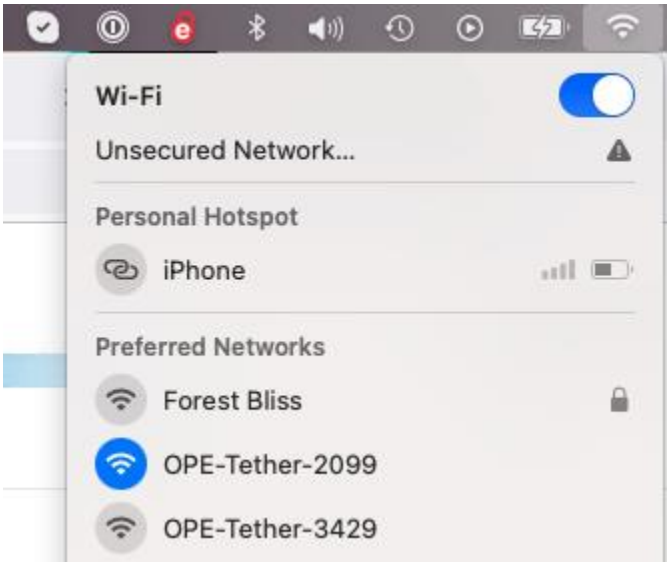
Before you can start the configuration process, you must first establish a connection either via Ethernet or Wi-Fi to login to its web administrative interface.

The EdgeMate web interface is mobile friendly and supports all popular web browsers.

Access via Wi-Fi

The EdgeMate advertises itself via Wi-Fi with an SSID "OPE-Tether-XXXX" where XXXX is an alphanumeric sequence specific to the device. By default, the EdgeMate Wi-Fi is unprotected. As part of the configuration process, you may change the SSID of the unit and encrypt and password protect the unit. Procedures for assigning a password are discussed later on in the "Securing EdgeMate" section of this document.

To Wi-Fi connect to the EdgeMate, scan for available access point SSIDs and select the one that corresponds to your unit. The following image depicts the process for Mac OS X. Other OS's use a similar process.



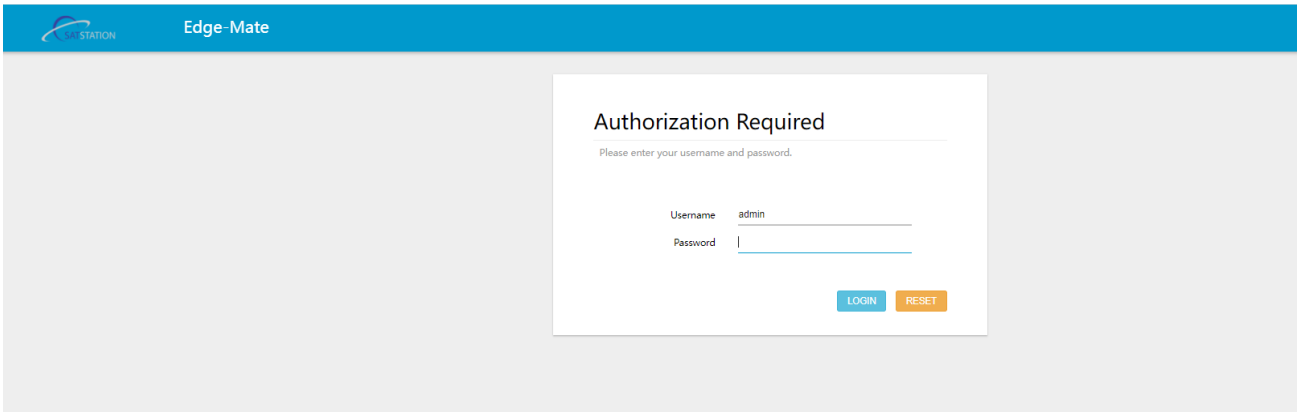
Access via Ethernet

To access the unit via a wired connection, run an Ethernet cable between the RJ45 port on your laptop computer and the LAN port on the EdgeMate. The LAN port is the RJ45 port closest to the power connector labeled as LAN.

Accessing the Web UI

To login to EdgeMate's administrative web page, open a web browser and browse to http://10.10.10.1

You should see a login page pop up in your browser. Login with the default username: "admin" and password: "admin". Then push the "Login" button to access the administration pages.

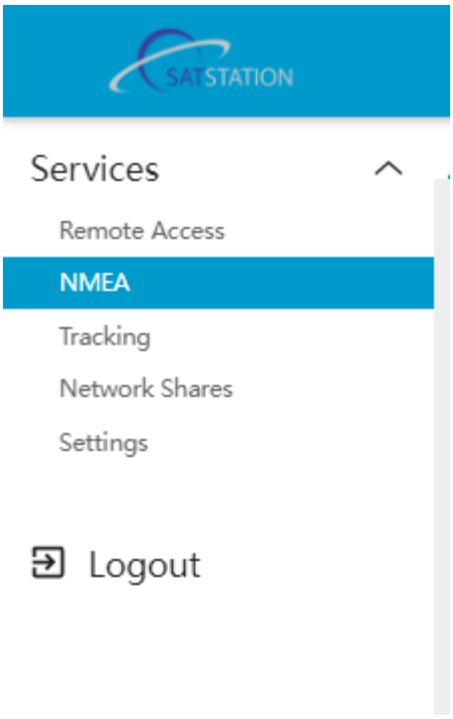


Configuring the EdgeMate

A GPS feed, an Internet connection, and tracking at a minimum need to be configured to allow the tracking of your vessel on your personal tracking and blogging page at OPE.

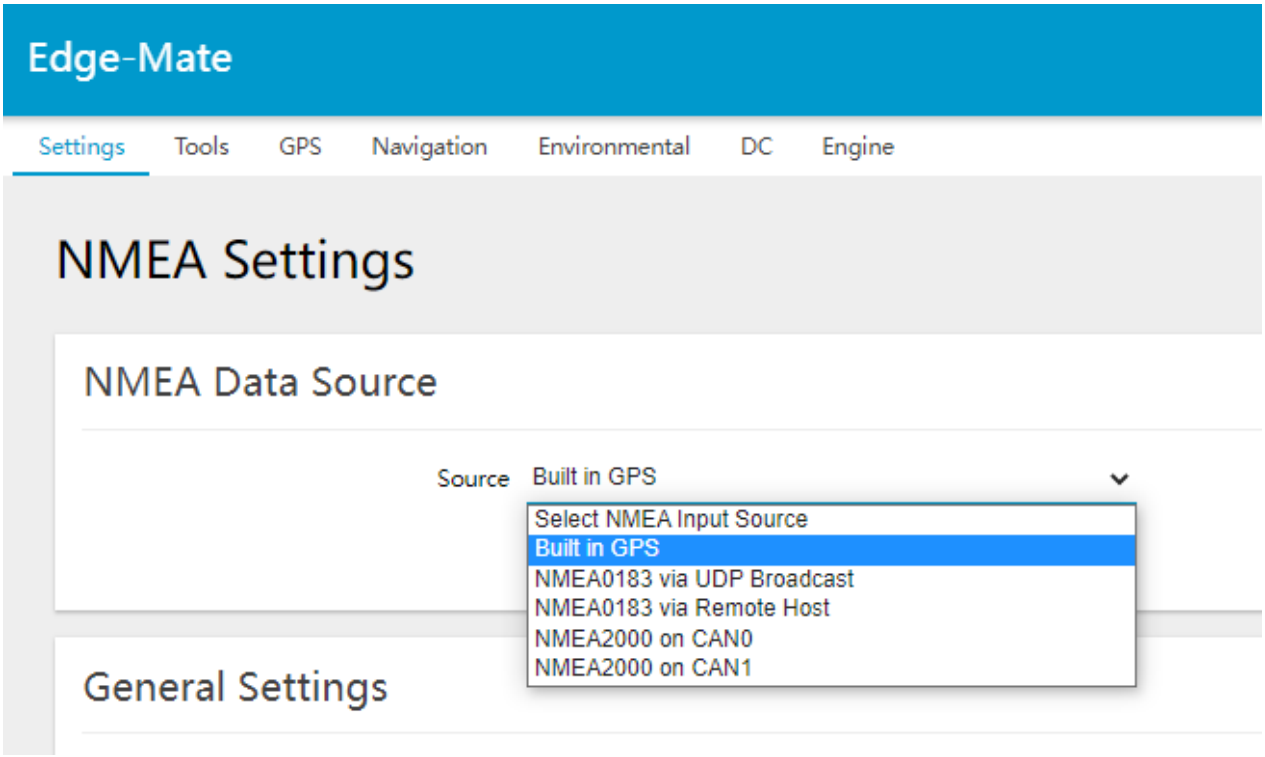
Configuring the GPS feed

Once logged into EdgeMate's administrative website, browse to "Services->NMEA" to configure the GPS feed. On a mobile device you do this by clicking on the "Hamburger" icon on the top left of the page and under "services" selecting "NMEA". On a laptop with a larger display area, you will see the "Services" menu on the left.



Using the built-in GPS

Use the “Source” pull down menu to select the GPS source. If using the built-in GPS, make sure that the EdgeMate is installed with the supplied GPS antenna and with good access to the GPS signal.



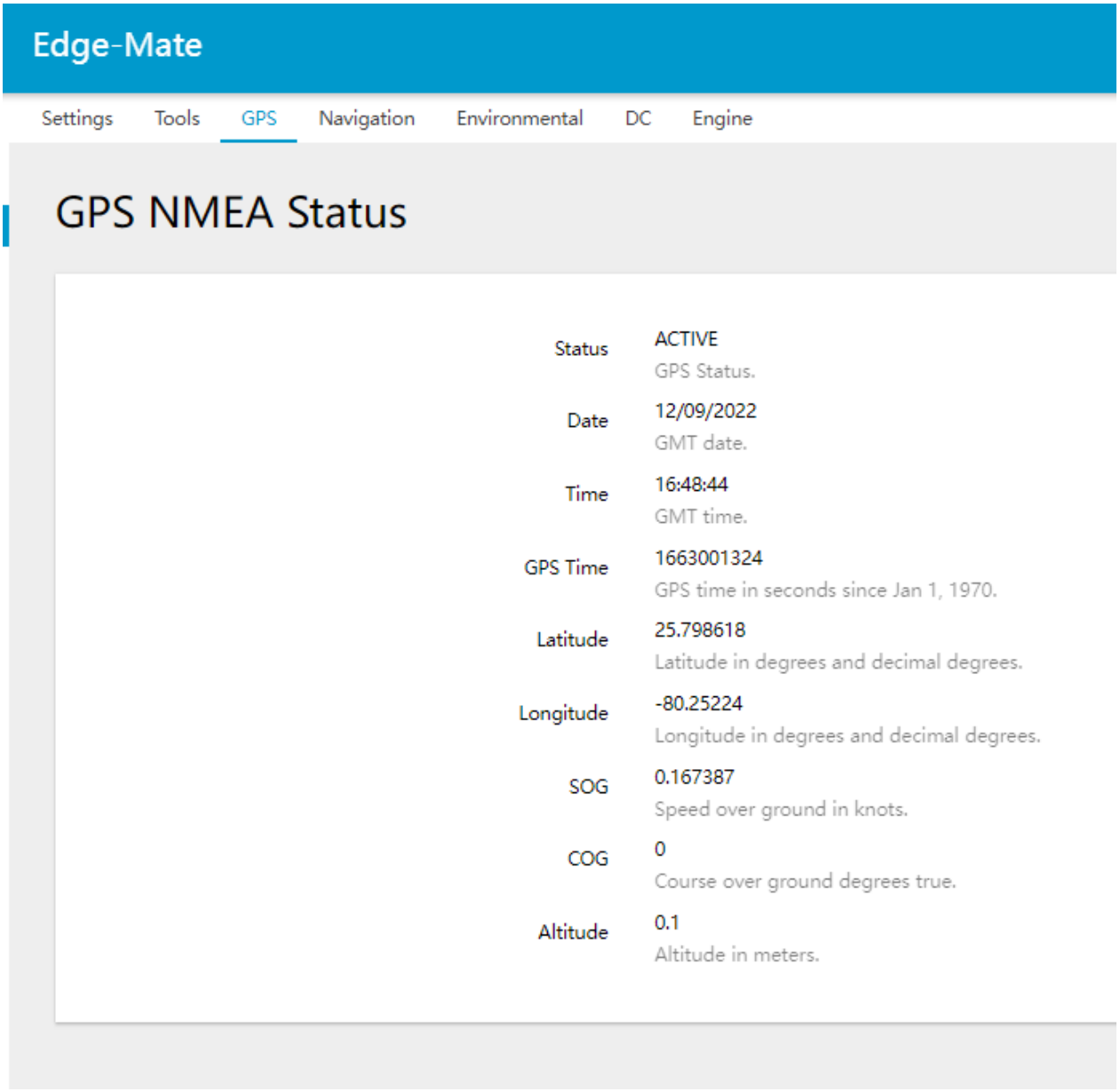
Using NMEA 2000 for GPS

If using your vessel's NMEA 2000 network, then connect the optional device cable from the M12 connector on the back of the EdgeMate to a tee on your NMEA 2000 backbone. NMEA 2000 device cables and tees can be purchased directly from SatStation with your EdgeMate order.

Once connected to the NME2000 network, select "NMEA2000 on CAN0" as the GPS source.

Verifying your GPS data feed

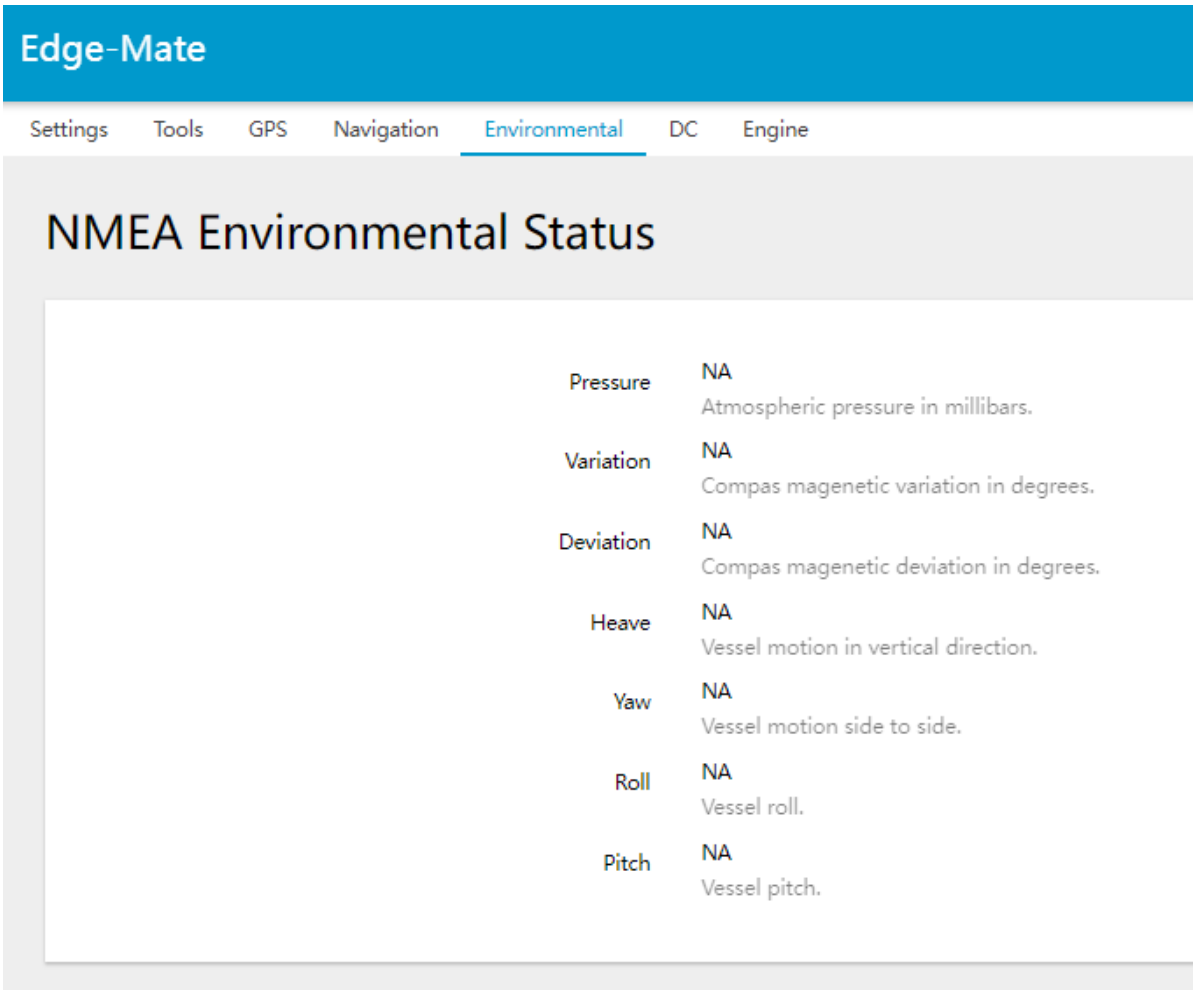
Selecting the "Status" tab in the NMEA section will display live GPS data as it streams into the device.

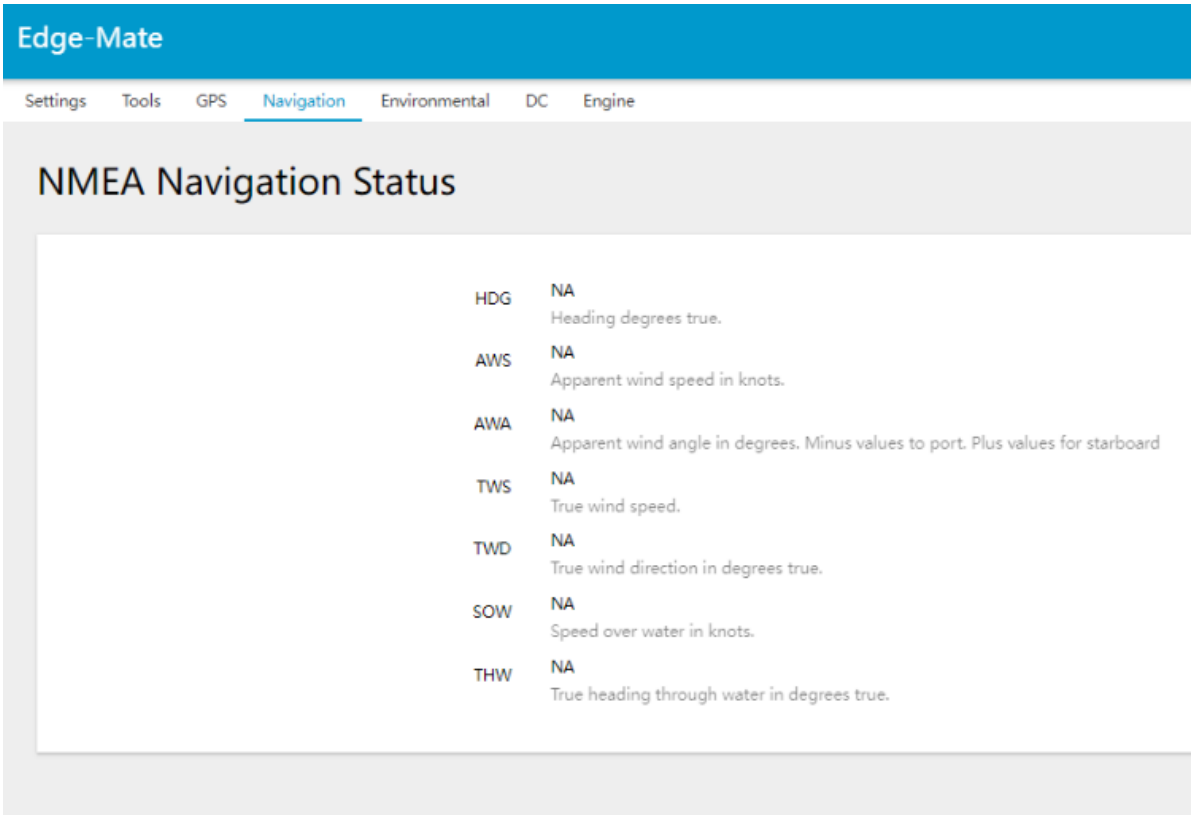


“ACTIVE” under “Status” means that you have valid GPS data. A “Status” of “VOID” indicates that NO or invalid GPS data is being received.

Please confirm that you are indeed getting valid GPS data before proceeding.

NMEA status tabs can be used for more than just verifying GPS data. Tabs are included to display GPS, Navigation, Environmental, DC Alternator and Battery, and Engine NMEA data if available. Click on the tabs to view available data on the NMEA 2000 bus.

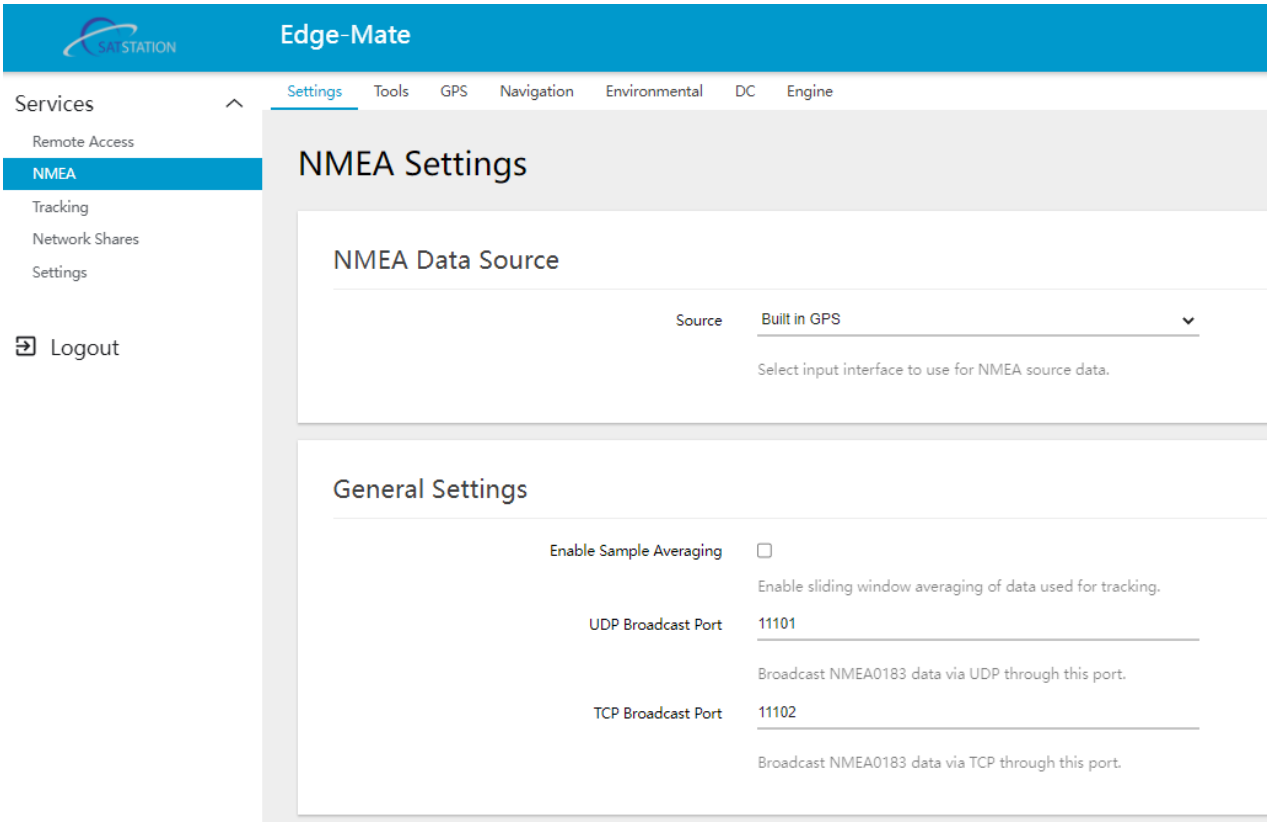

Edge-Mate
Settings
Tools
GPS
Navigation
Environmental
DC
Engine
NMEA Environmental Status
Pressure
NA
Atmospheric pressure in millibars.
Variation
NA
Compas magenetic variation in degrees.
Deviation
NA
Compas magenetic deviation in degrees.
Heave
NA
Vessel motion in vertical direction.
Yaw
NA
Vessel motion side to side.
Roll
NA
Vessel roll.
Pitch
NA
Vessel pitch.



NMEA2000 to NMEA183 Repeater via Wi-Fi

One of the nice features of the EdgeMate is that it will broadcast NMEA 0183 data via Wi-Fi regardless of the GPS input source. This Wi-Fi broadcast allows external navigation applications such as Aquamap, GPS Nav X, Navionics Boating App, etc. to use your vessel's GPS for navigation. This results in much more accurate GPS data with the addition of other NMEA 2000 data such as wind speed and direction, depth, etc.

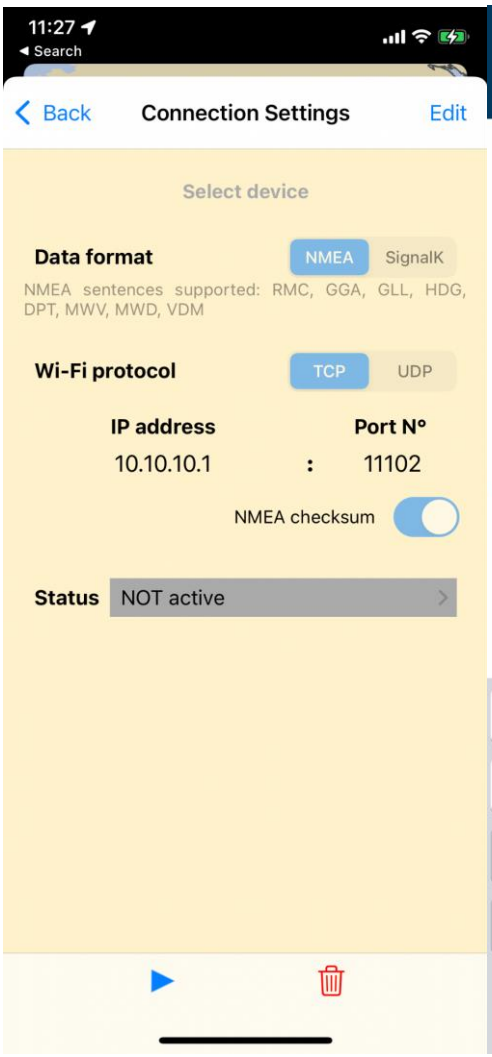
NMEA 0183 data is broadcast by default via UDP (User Datagram Protocol) on port 11101 and TCP (Transmission Control Protocol) on port 11102. The ports are user selectable and can be changed under “Settings” in the NMEA configuration section.



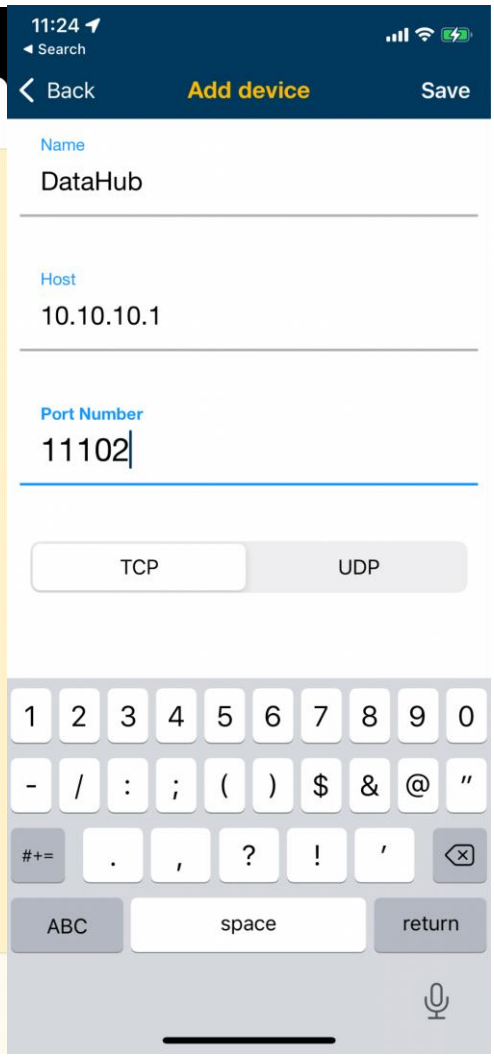
To configure your charting application to use EdgeMate generated data, please refer to the software documentation for the software. You will need to configure the following

- Host: 10.10.10.1
- Protocol: UDP or TCP
- Port number: 11101 (for UDP) or 11102 (for TCP)
- Wi-Fi connection between mobile or laptop and EdgeMate.

Following are the configuration settings for the iOS version of Navionics Boating and Acquamap apps.



Aqua Map

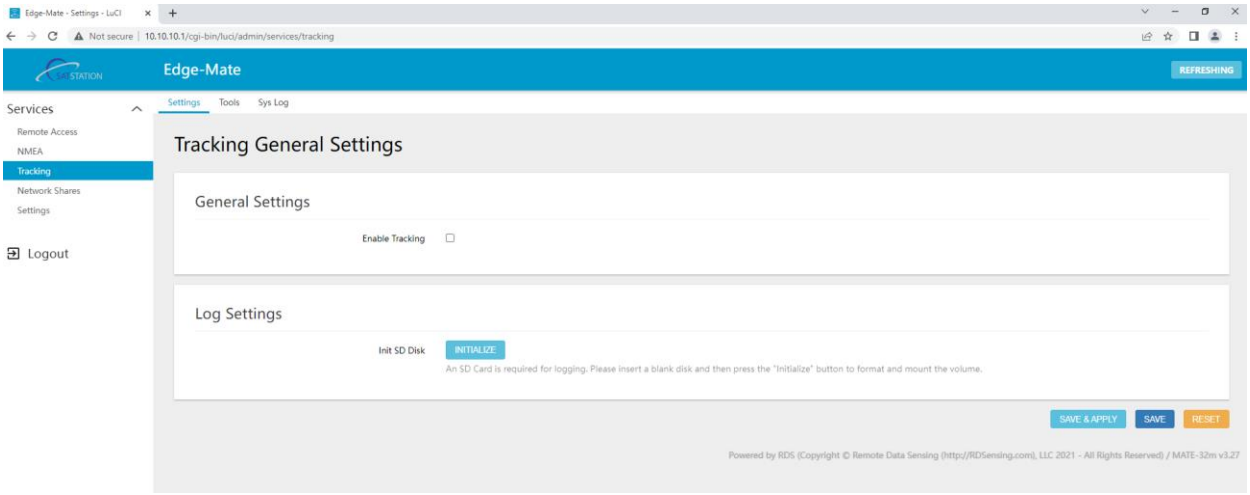


Navionics Boating

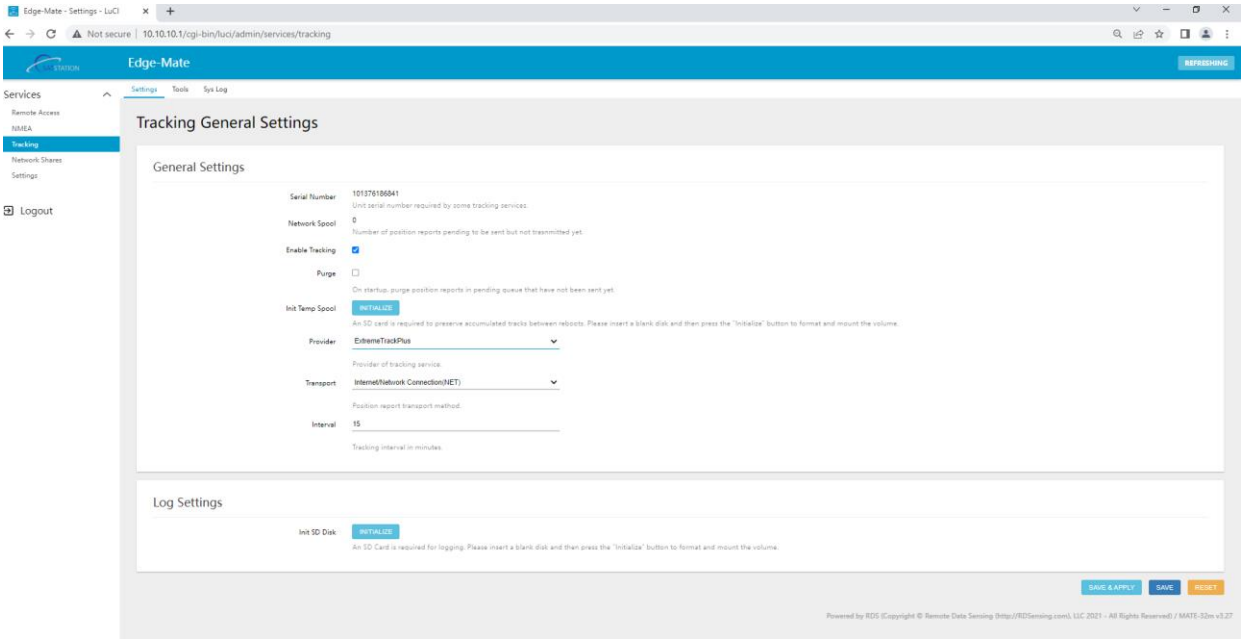
EdgeMate Tracking

Enabling Tracking

Navigate to Services->Tracking, click on Enable Tracking and then click SAVE & APPLY on the bottom of the page to enable tracking for the unit.



After enabling tracking, click on Initialize. This will format and initialize the pre-installed SD card for EdgeMate.



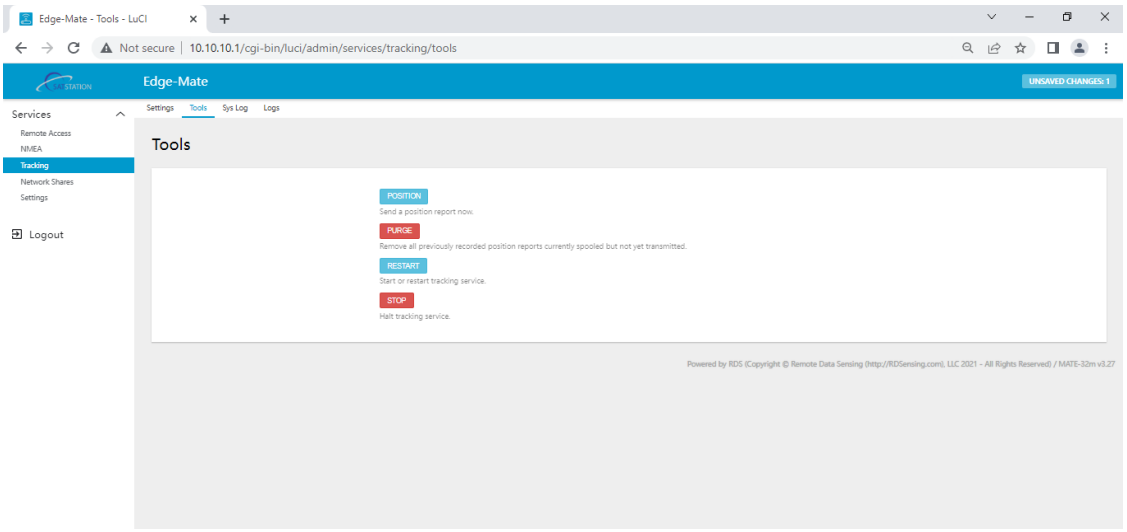
Select your preferred Tracking Provider and click Save & Apply.

Tracking Tools

Navigating to Tools in the tabbed menu above brings you to the Tracking Tools. The different options do the following:

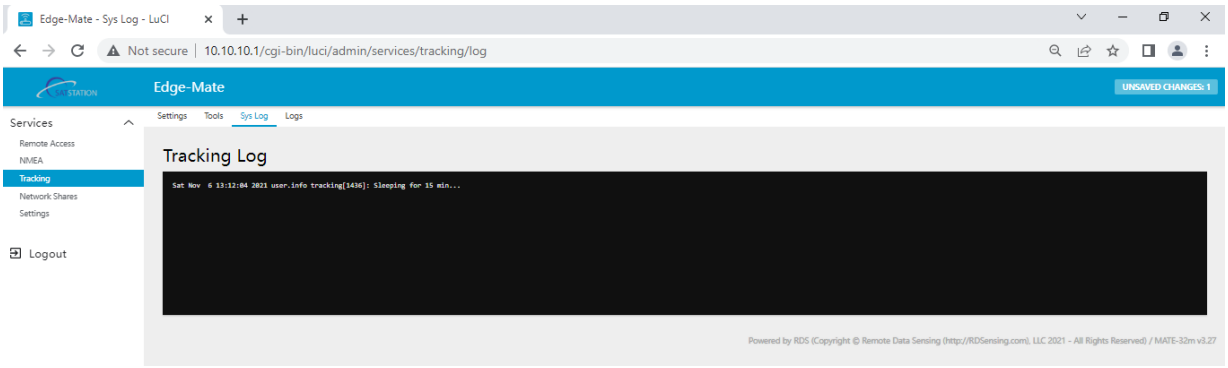
- Position – Sends a position report immediately if able.
- Purge – Removes all recorded position reports that are stored on the device but have not been transmitted yet (does not apply to Logs being stored on the device).
- Restart – Starts or Restarts your tracking service.

- Stop – Immediately stops your tracking service.



Sys Log

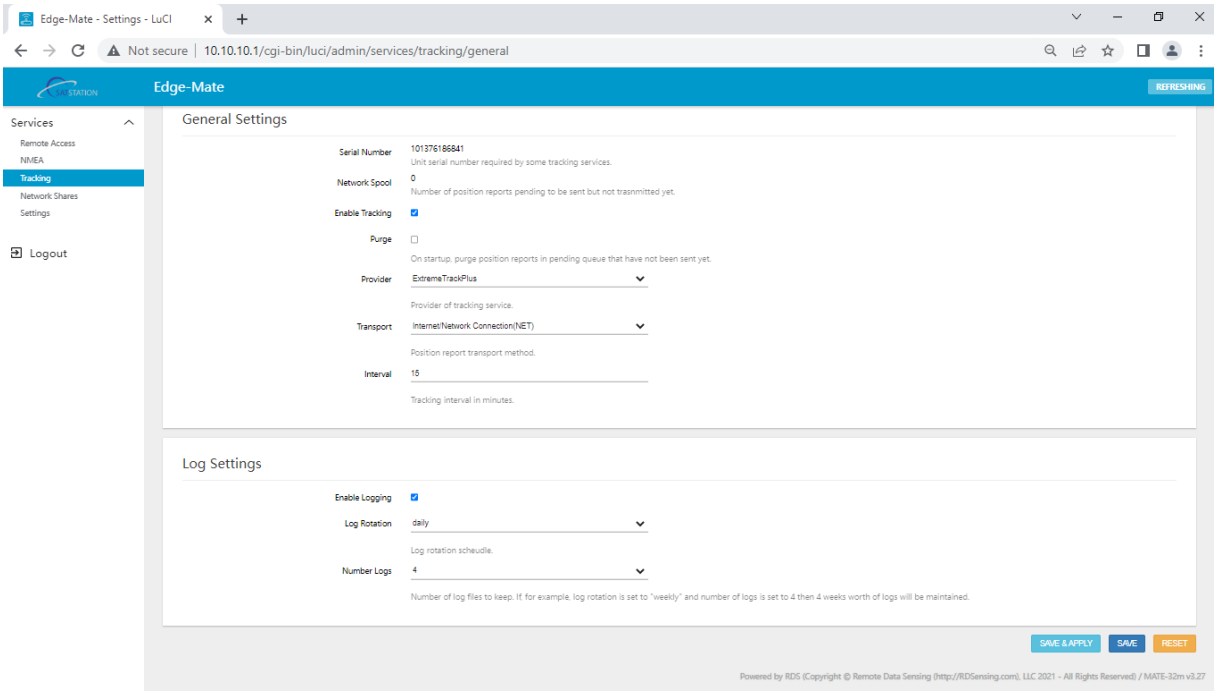
The Sys Log tab gives access to a live log where every action EdgeMate takes is shown in real time.



Logging

EdgeMate can log position reports and store it in its internal non-volatile storage for later analysis. Logged data can be viewed, downloaded, and deleted.

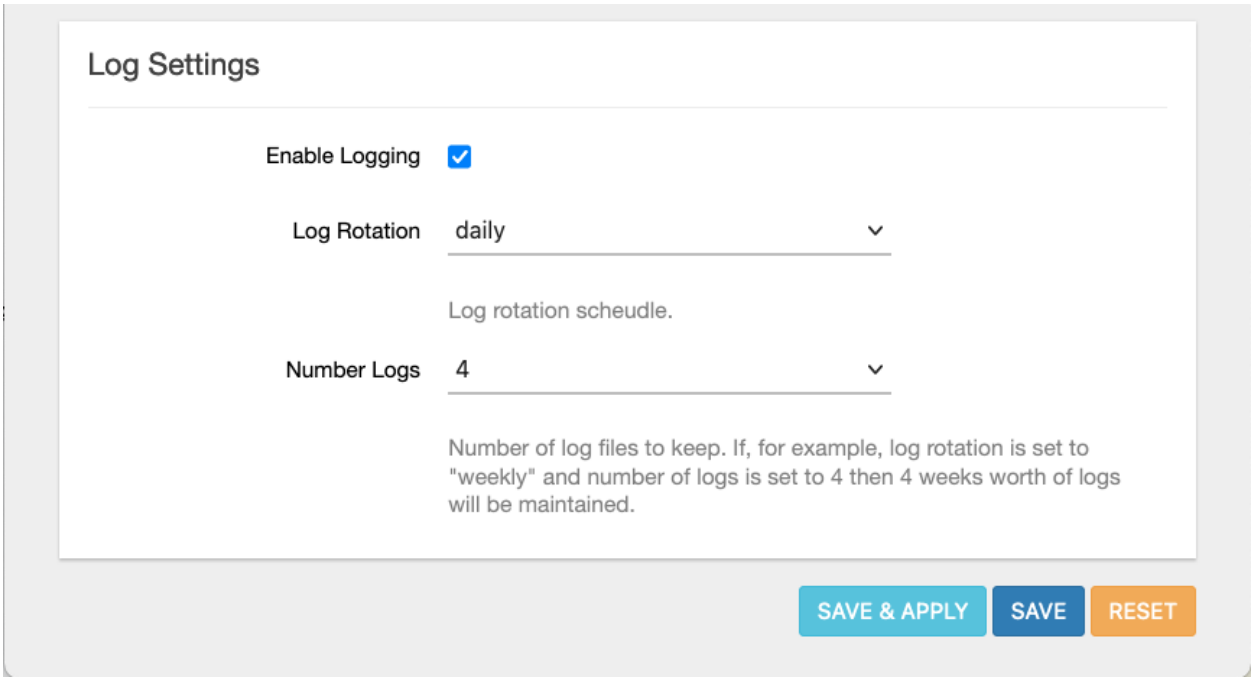
Logging is enabled by checking the “Enable Logging” checkbox at the bottom of the “Tracking” page after initializing the SD Card. Check the box followed by pushing the “Save & Apply” button to enable logging.



Manage Tracking Logs

The EdgeMate is supplied with non-volatile memory. Log rotation prevents the log data from growing forever and filling up available storage space. This is done by storing the logs in individual files and then periodically deleting the older data sets.

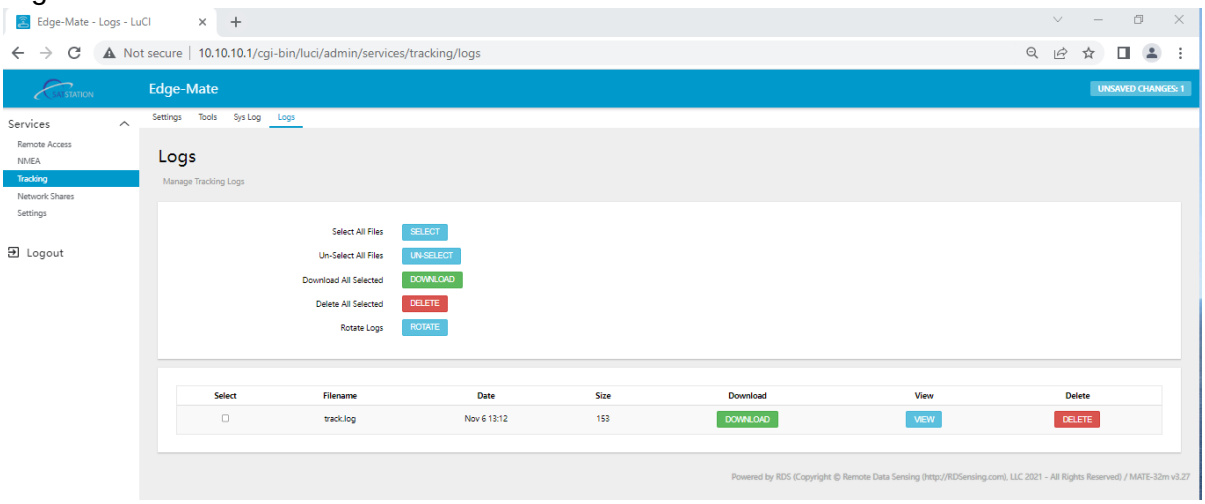
A log rotation scheduling dialog appears when logging is enabled.



In the above screen shot we have selected the logs to be rotated daily with a maximum of 5 log files (4 days worth) to be stored. File names are logged by name followed by a '.' and a number. The larger the number the older the data set.

Logs can be rotated on a "daily", "weekly", or "monthly" schedule. A maximum of 10 log files can be stored in EdgeMate's internal memory.

If Tracking and Logs are both enabled the Logs tab will grant access to logs stored directly on EdgeMate.



Configuring Internet Access

Access to the Internet is required to allow SatStation specialists to access your system for monitoring, diagnosis, and configuration of your DC charging systems. Although a dedicated Internet connection is desired it is not required.

EdgeMate provides four different ways to connect to the Internet. These include:

- USB Connected iOS devices
- USB Connected Android Devices
- Ethernet connected router with Internet access such as a broadband satellite device (Iridium Certus, Inmarsat Fleet Broadband, KVH Vsat, etc.) or an LTE enabled router such as a Pepwave.
- Wi-Fi bridge to MyFi devices such as a Netgear Aircard, Cricket wireless router, Verizon Jetpack and others.

Multiple Internet connections can be configured at the same time. For example, users could use a USB connected Android phone as well as an Ethernet connected satellite terminal. When the satellite phone is on, then data is routed through it. If the satellite phone is off, then data is routed through the Android connected device. If neither of the two are available, then the

position reports are stored internally in non-volatile memory until an Internet connection is available.

Internet via USB connected iOS device

Use a standard lightning iOS USB charging cable to connect your iPhone or iPad to the USB port on the EdgeMate.

Once connected, iOS will prompt you whether the EdgeMate should be trusted or not. Select “Trust”.

On the iOS device, navigate to “Settings->Settings->Personal hotspot” and enable it as depicted below.

The EdgeMate should now be connected to the Internet if your iOS device has Internet connectivity. See section below called "Verifying Internet Connectivity" to confirm that the device is connected to the Internet.

Internet via Android

To establish an Internet connection via Android, connect the devices USB charging cable to EdgeMate's USB connection.

On the Android device now navigate to “Settings->Network & Internet->Hotspot & tethering” and enable USB tethering.

The EdgeMate should now be connected to the Internet. See section below called “Verifying Internet Connectivity” to confirm that the device is connected to the Internet.

You will need to repeat the process every time you disconnect and reconnect the Android device to EdgeMate’s USB port. However, there is a good trick that allows you to automate this process so that the phone enters USB tethering mode automatically when you plug it in. Detailed instructions on configuring automatic USB tethering are beyond the scope of this guide, but are described in detail in the following article.

Internet via Ethernet WAN port

This is the simplest of all methods. Run an Ethernet cable from your vessel's router LAN port to the port labeled WAN on the EdgeMate. EdgeMate’s WAN port is the RJ-45 jack furthest away from the power connector.

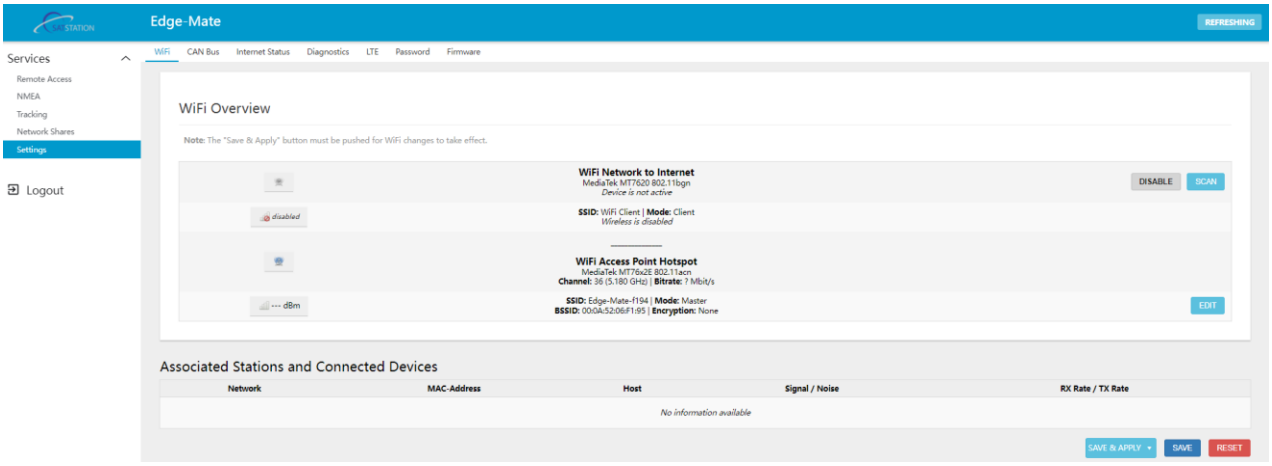
The EdgeMate should now be connected to the Internet. See section below called “Verifying Internet Connectivity” to confirm that the device is connected to the Internet.

Internet connection via Wi-Fi Tethering

Although Wi-Fi tethering is the most complex of all Internet connectivity methods, it is quite effective and once configured very convenient to use. The EdgeMate will persistently search for the remote access point and once found will automatically connect to it. No buttons or settings need to be changed between power up/down. The Hub searches and automatically connects.

Access points can be your phone in mobile hotspot mode or a dedicated Wi-Fi access point. When using your phone, enable hotspot mode and the EdgeMate will automatically connect to it. This for many is more convenient than plugging the phone into the USB port on the EdgeMate since the EdgeMate connects to the phone wirelessly. If you have your EdgeMate installed in a cabinet, then you will probably want to use this method for Internet connectivity.

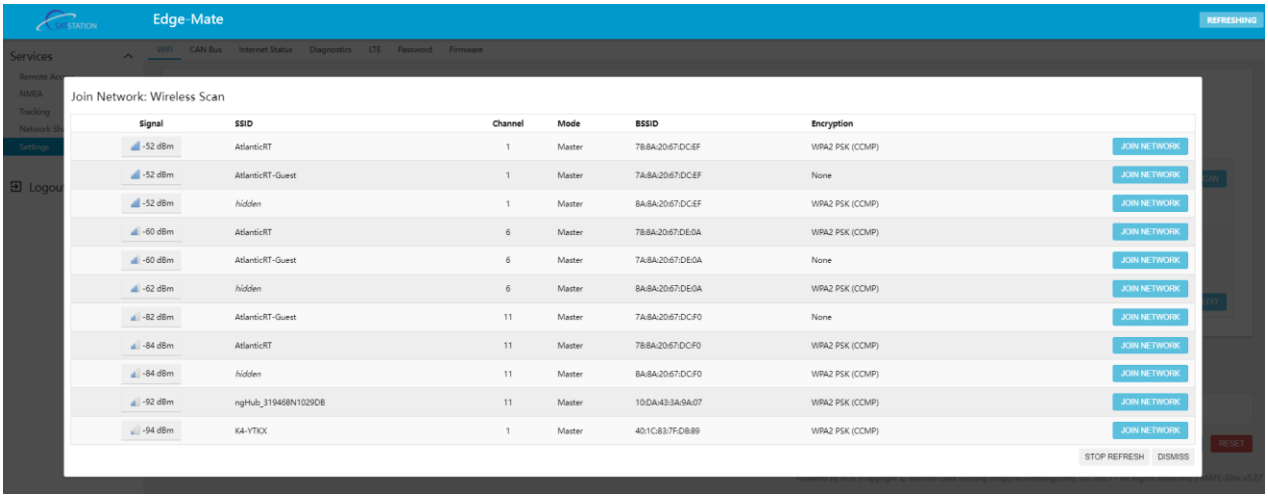
To configure Wi-Fi tethering, login into the web administrator and browse to “Settings” under “Services” and navigate to the Wi-Fi tab.



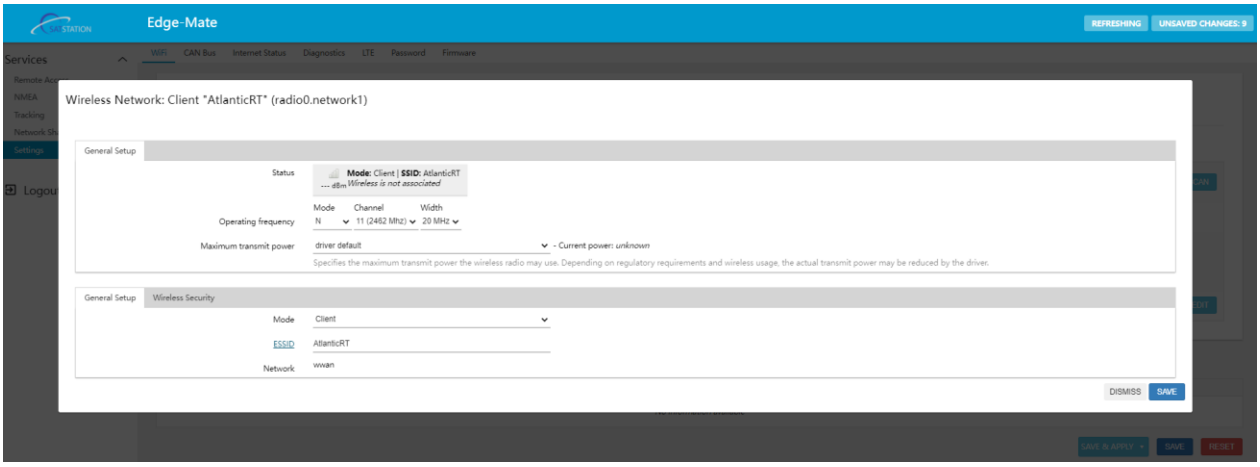
Under “Wi-Fi Overview” you will see two Wi-Fi transmitters listed. The first called “Wi-Fi Network to Internet” is used to establish a Wi-Fi link to a remote hotspot that provides Internet access. This transmitter in essence can be used to connect the EdgeMate to the Internet via a Wi-Fi link.

The second transmitter called “Wi-Fi Access Point Hotspot” is the transmitter used by the EdgeMate to provide Wi-Fi connectivity to devices on the vessel wishing to access the web administrator and the Internet. Notice the SSID for this transmitter is listed as “SSID” PW-Hub-XXXX” where the Xs represent alphanumeric digits unique to the unit. This is the SSID that clients use to Wi-Fi connect to the EdgeMate. We will return to this transmitter later in the guide when we discuss how to password protect the Wi-Fi connection to your EdgeMate and change its broadcast Wi-Fi name or SSID.

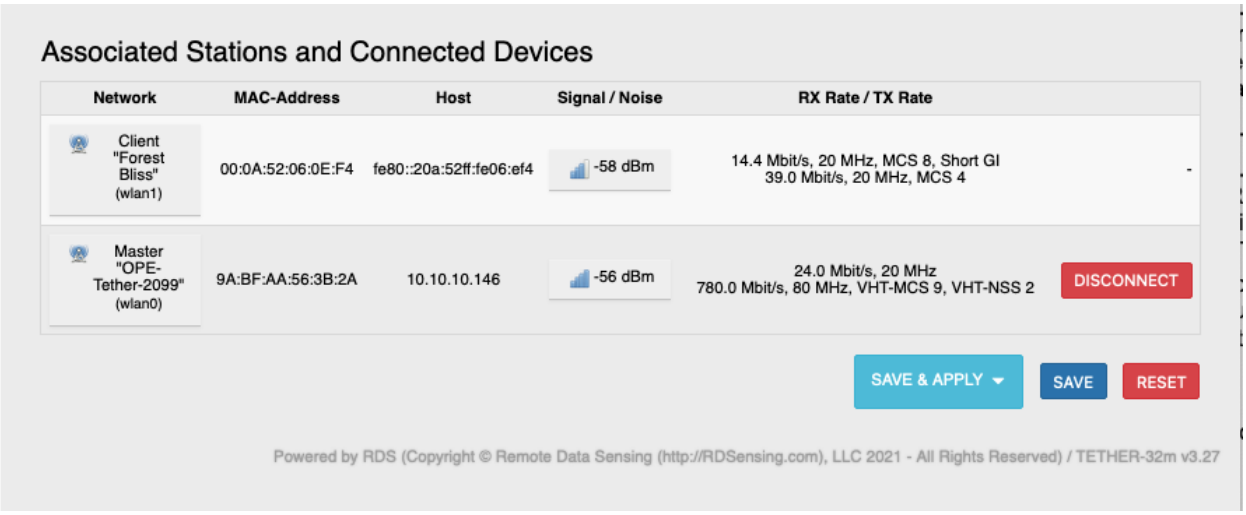
Push the “SCAN” button to list all the available Wi-Fi access points near you. Select the one you desire to connect to and tap “JOIN NETWORK”. In this example I am selecting my iPhone in hotspot mode. Next enter the passphrase for the Wi-Fi access point then tap “SUBMIT” at the bottom of the page. Note the “WPA passphrase” field will not be present for open Wi-Fi networks without passwords.



On the following page, review and hit “SAVE” at the bottom of the page. Back on the wireless overview page, scroll to the bottom and push “SAVE & APPLY” to confirm your settings and activate them. You can push the “UNSAVED CHANGES” button at the top right of the page if you want to discard the session without connecting.



You know if you have successfully Wi-Fi tethered to the remote access point by looking at the status in “Associated Stations and Connected Devices”.



You will see the SSID of the remote station listed with signal strength and a transmit (TX) and receive (RX) rate. You will know that the station is not available, or you were not successful (if say you entered the password incorrectly) when the signal bounces between 0 and some value and the RX/TX rates drop to zero.

But… note there are easier and better ways to know if you are connected to the internet as described in the “Verifying Internet Connectivity” section.

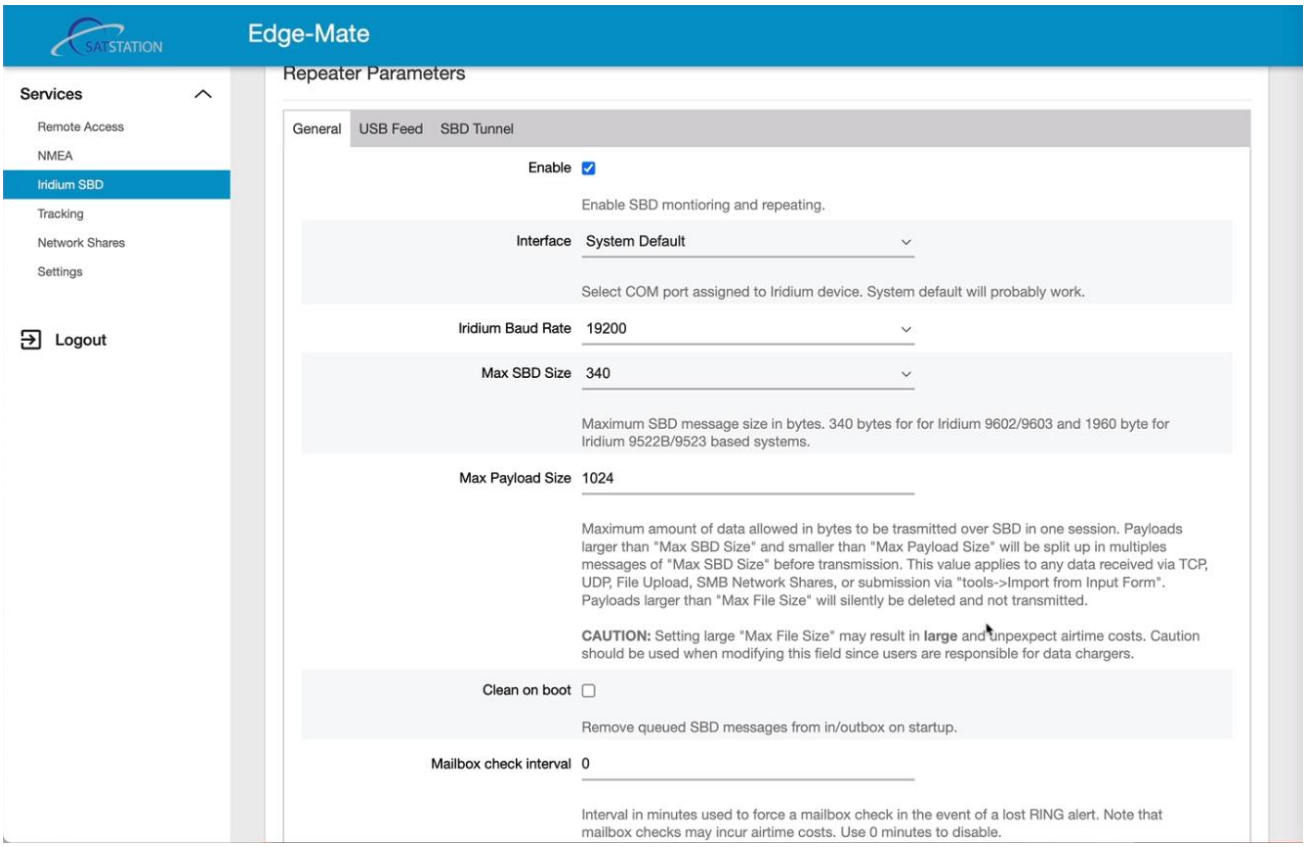
SBD

Connecting the Iridium Edge to EdgeMate allows EdgeMate to send information over satellite via Iridium Short Burst Data (SBD).

Enabling SBD

Navigate to Iridium SBD, click enable and hit Save & Apply.

SBD Settings



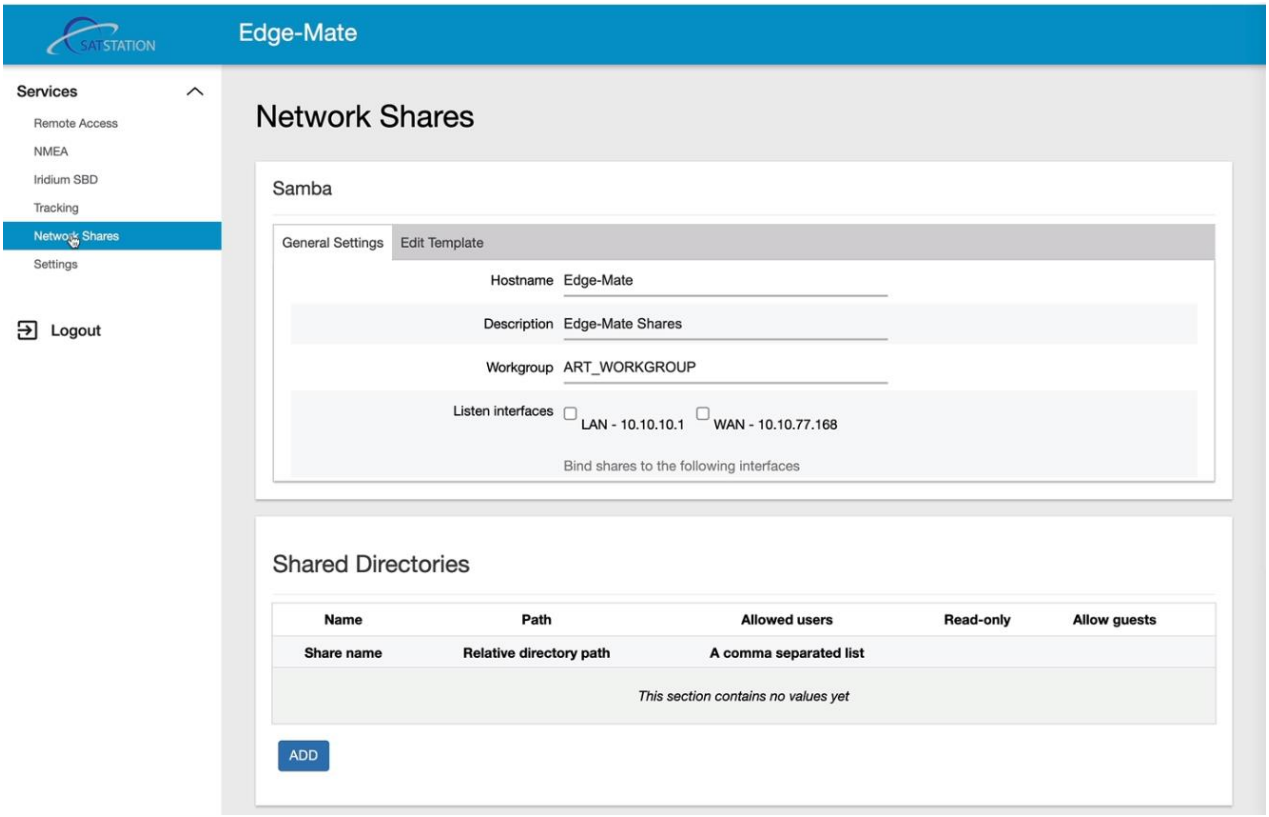
- **Interface** is the device being interfaced by the Edge. By default, the EdgeMate automatically recognizes when an Iridium Edge is connected to it, making “system default” point to the Edge. This will also show interfaces which are connected to the USB port, including Irdium SBD modems, or satellite phones such as the 9555 and/or 9575. So the unit is not limited only to the Edge, it'll work on any Iridium system that supports SBD, and those systems would have to be connected through the USB port.
- **Baud rate** is the serial port baud rate between the Mate and the Edge, or whatever Iridium device you're connected to. The default is 19200.
- **SBD Max packet size** allows you to change the max allowed SBD packet size. Now this is important because 9523 devices, or LBTs, have the ability to send much larger SBD

messages, as large as 1960 bytes. Whereas the Edge, which is based on a 9602, is limited to a maximum of 340 bytes.

- **Maximum payload size** - it's just a way for you to prevent bill shock. In other words the Mate will take a file of any size, and once transferred to the Mate, will split it up into messages that are 340 bytes or less, and transmit those over SBD.
- **Clean on boot** - as we send messages to the unit, or files to the unit, it'll split them up and put them in a spool to be sent out. And as messages arrive they'll be stored in an inbox until they are transmitted via one of the several different mechanisms that we have to share SBD data that arrives. So if you wanted to have the outbox and the inbox cleaned out when you reboot the unit, you just put a checkmark there.
- **Mailbox Check Interval** - is an interval that is used to tell the Mate to just every once in a while during that interval to just check to see if there's anything on the server. So you can set this for example to 60 minutes. And then every 60 minutes, regardless of whether a ring alert has arrived or not, it will log into the server to say, hey, do you have any messages, and if you do then download them and then distribute them to the app. So the mailbox check is kind of a safety thing.

Network Shares

Now, a very convenient way if you're doing this from the PC or from a Mac, is to actually use network folders. We can create network folders that receive SBD messages or send SBD messages. These are network folders where I drag a file into the network folder. It will send an SBD message. And SBD messages that come into the Mate will magically appear in the network folder, which is assigned to be the in folder.

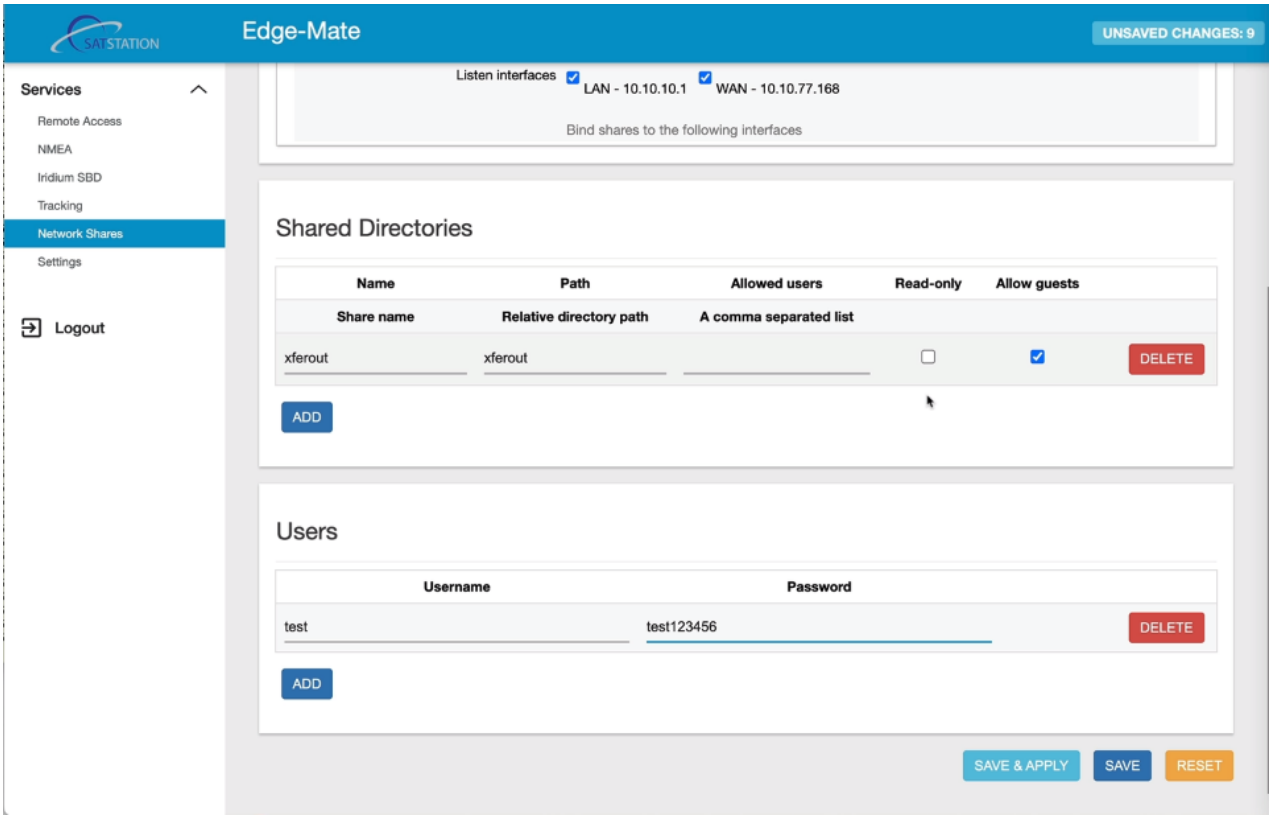


Once you click ADD, you will be able to add a Shared Directory to your EdgeMate.

- **Share Name** is the name you will see on your network.
- **Relative Directory Path** is the actual internal path on EdgeMate, where the files will be stored. This is not something you will see on your PC, only the Share Name.
- **Allowed Users** allows you to add Users access to these network shares.
- **Allow Guests** allow guests to read and write files in network shares. You do not need an account on EdgeMate to do this. But if you're in a secure install you can actually add a user name and password.

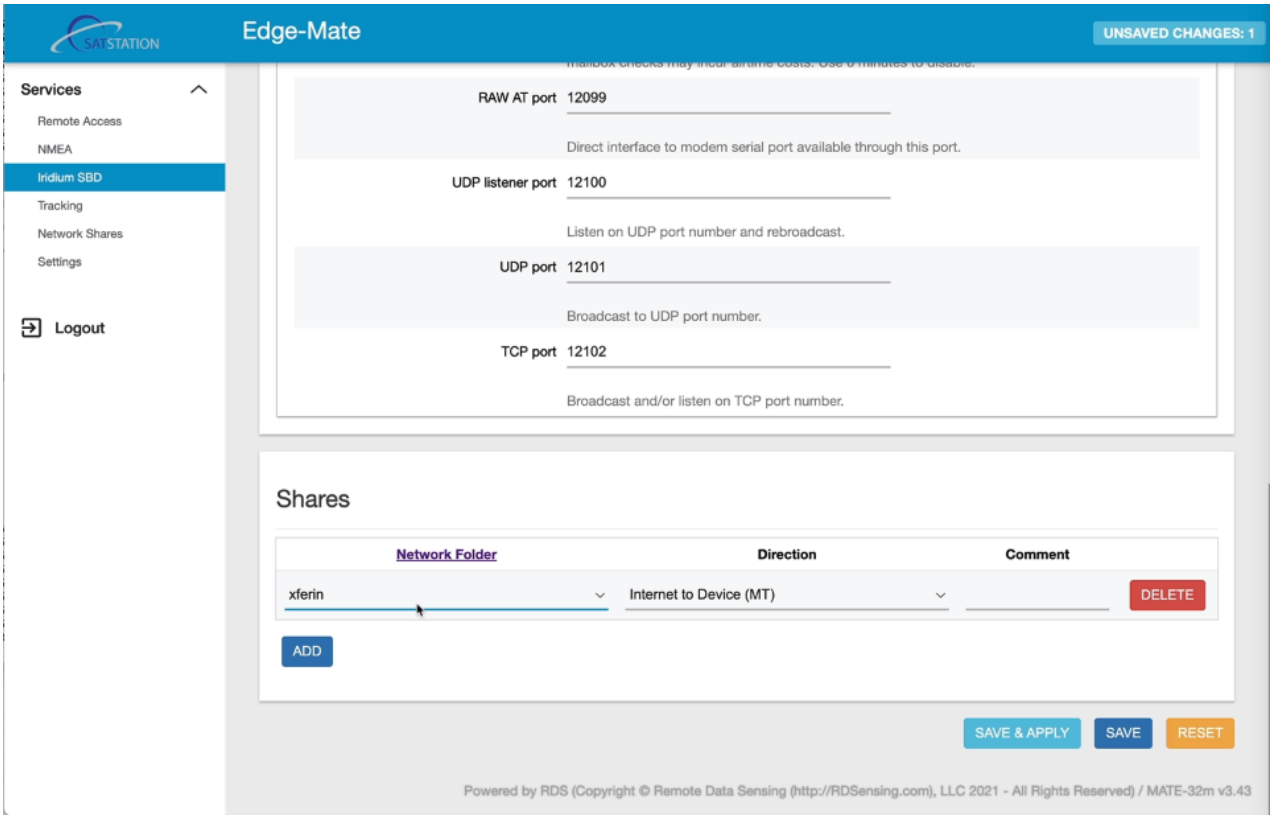
Users

EdgeMate allows you to add multiple Users with access to EdgeMate network share folders.



Bind Network Shares to SBD Subsystem

After creating the Network Shares navigate back to Iridium SBD in the Services menu on the left. Scroll to the bottom to the Shares section.



- **Network Folder** allows you to select from the Network Shares you created in the previous section.
- **Direction** select which way you want to route traffic to this Network Folder.
- **Comment** creates an internal comment only visible on the EdgeMate.

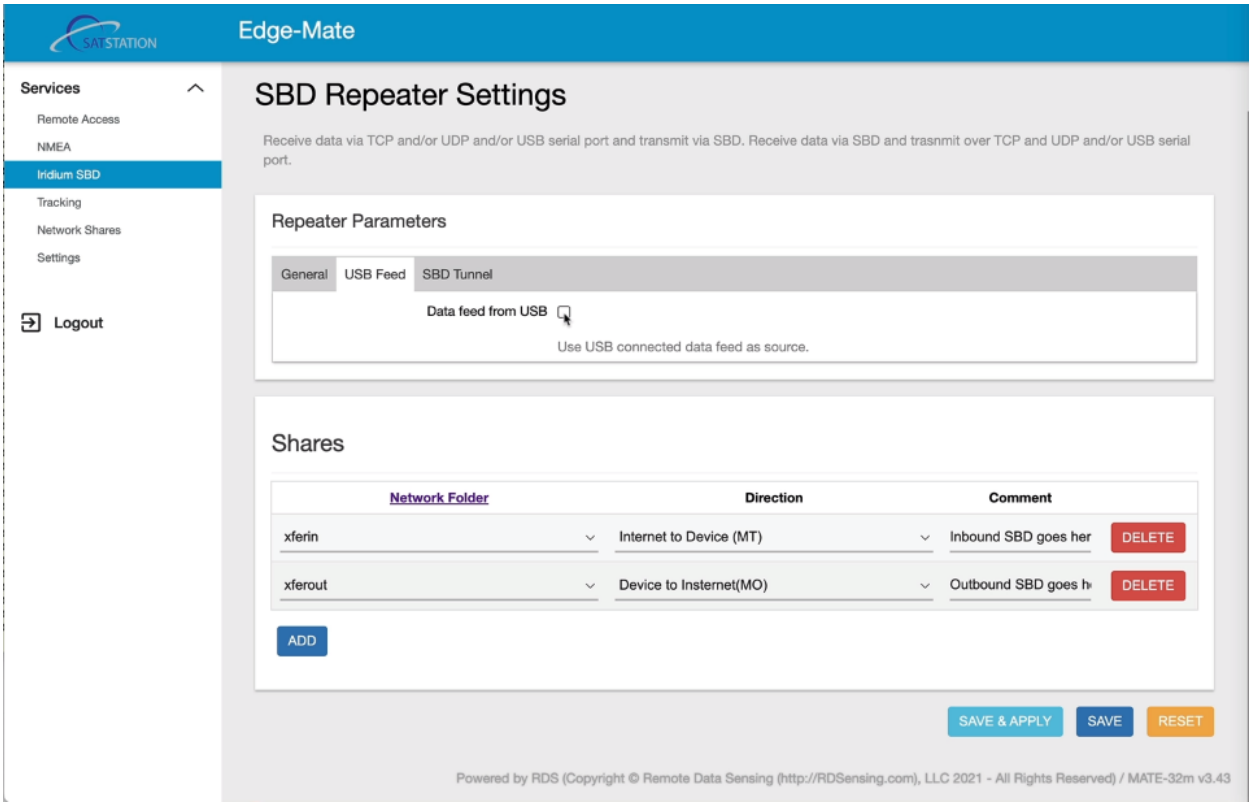
Please note if the file is larger than 1000 bytes, it's going to ignore it. So if you're going to send large files you'll need to change that. Also if it's larger than 340 bytes it's going to split it up into messages and send them off in first-come-first-serve type order.

In the example in the screenshot above, any inbound SBD messages will show up in the xferin folder. It won't recombine those for you, so those will be all a maximum of 340 bytes long. But they'll be there and then your application can read them out of there and then recombine them if it needs to do that.

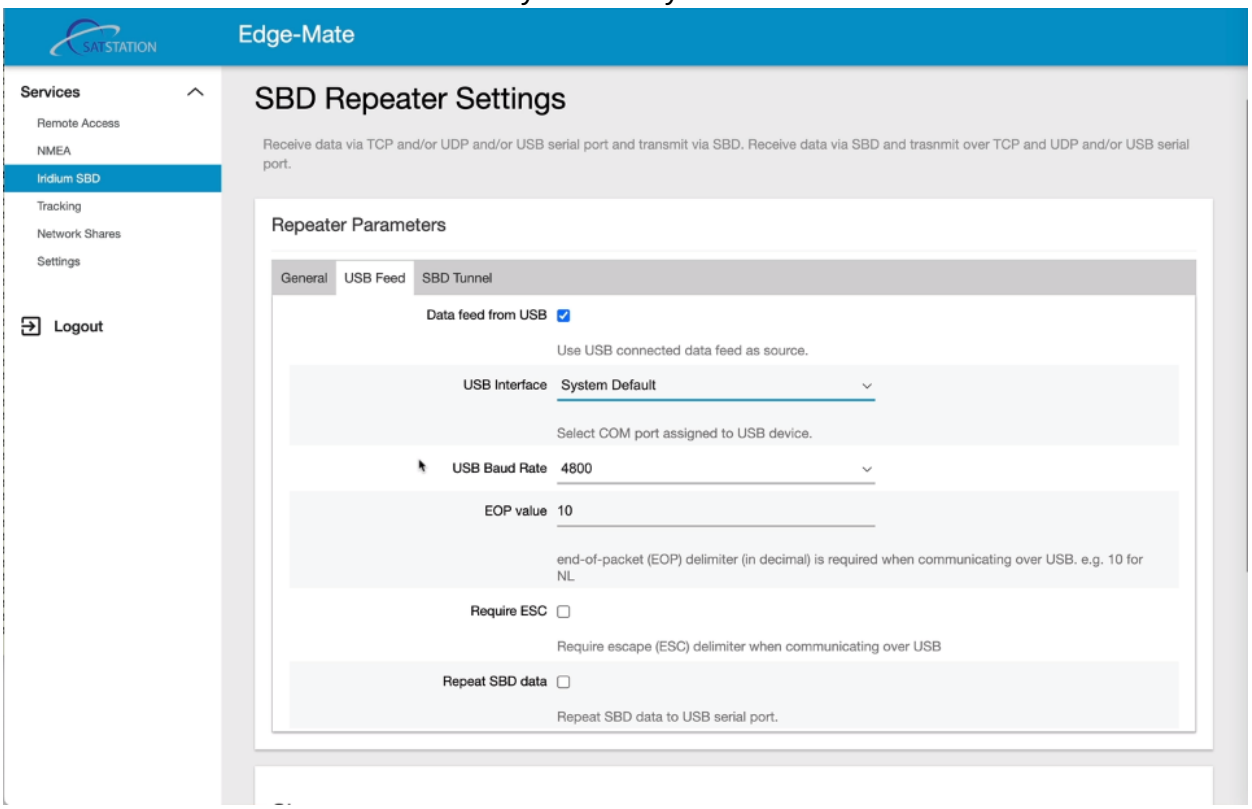
USB-to-Serial SBD Connection

You can have a USB serial port connected to the EdgeMate. And you can read data from the serial port, and you can send data through the serial port. So if you've got some device, some log, or something that is actually generating serial data, you can have it automatically packetize that and send it.

First we need to enable this option by going to the USB Feed tab in the Iridium SBD menu and check “Data feed from USB”



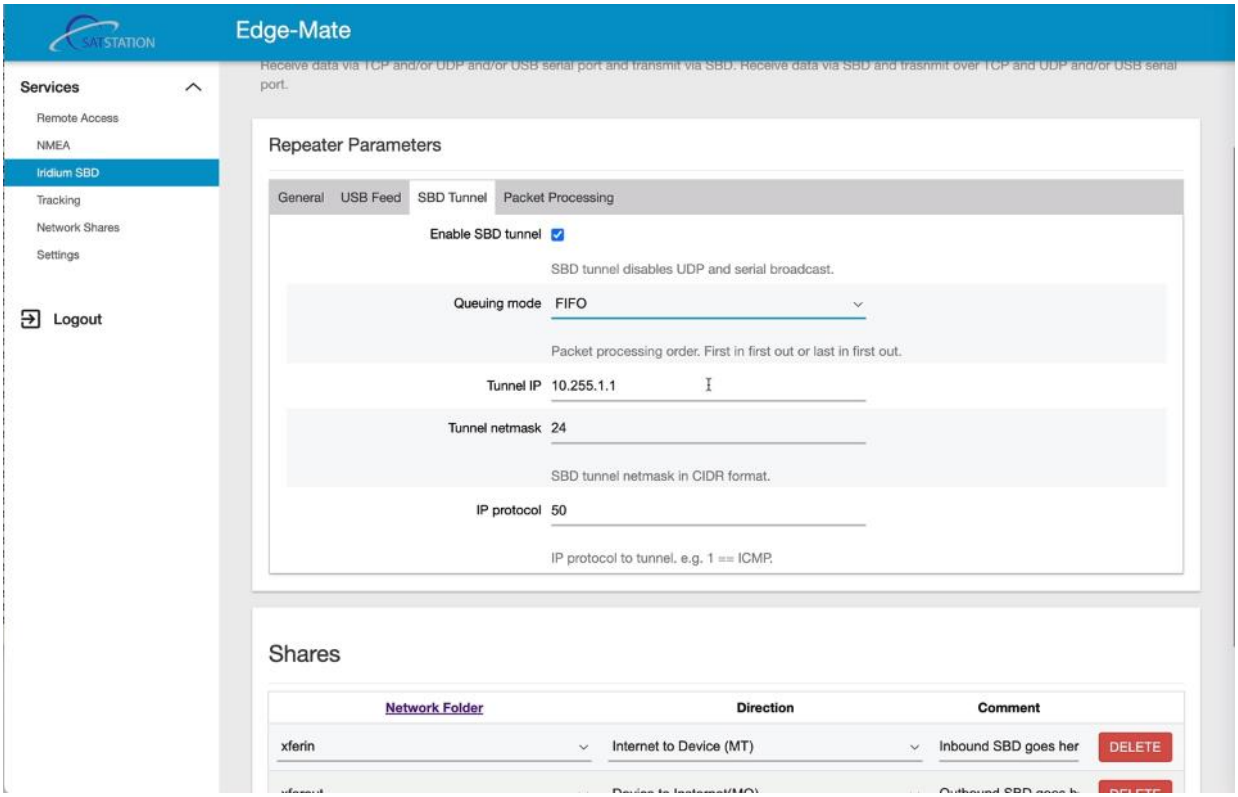
This will unlock the rest of the menu for you to add your local SBD device.



- **USB Interface** when you plug a USB-to-serial adapter into a Mate you will see it show up here. Note your USB interface for your logger might be called ACM0. It might be called USB5. It'll have some specific name that'll show up in this list and you can select it.
- **USB Baud Rate** can set the baud rate for the interface.
- **ECP Value** is an end-of-packet delimiter. And the end-of-packet delimiter means that you receive the data coming in through the serial port, and as soon as you see the end-of-packet delimiter, which in this case is defined as a new line, the SBD, it'll packet ties that data and send it over SBD.
- **Require ESC** allows you to require an escape sequence. That just means that if you've got an escape character, like for example you're sending binary data and that binary data has new lines in it, you will want to escape the new lines so that it doesn't terminate that particular thing. Because we know that the new lines are defined to be the end-of-packet terminator. So we want to escape those if they happen to be in the middle of the message. So you can do that by requiring the escape, and then specifying the escape character that you want to use to do the escaping.
- **Repeat SBD Data r**epeats SBD data back onto the serial port. That means that any inbound data coming in through SBD will be written to the serial port.

SBD Tunnel

Finally, the most complex method is an SBD tunnel. An SBD tunnel allows you to connect a device to EdgeMate via IP. Navigate to the SBD Tab in the Iridium SBD settings to enable SBD tunneling.



- **Queuing Mode** means that as data comes in to the tunnel, it's transmitted and first come first serve. So first in first out. That's the queuing methodology. You can also do last in first out. So as data is being streamed into this thing, you can always send, oh, the latest data that came in goes out, and it transmits it in reverse order. So you get to specify the order in which the data gets transferred.
- **Tunnel IP** can be made anything, but needs to be a different IP address than the network address of the EdgeMate.
- **Tunnel Netmask** the tunnel mask is just going to be 24, so that's going to be a class C type network.
- **IP Protocol** is the IP Protocol that you want to capture, in this case, 50. ICMP is one. This means that any data that's in the network that matches that protocol number will be sent through the tunnel.

EdgeMate Status LEDs

EdgeMate provides a status LED on its top cover that rapidly allows you to know the status of the GPS feed, Internet connectivity, and if you have position reports stored on the device that have not yet been sent to OPE.

There are a total of 4 LEDs, Blue, Orange, Red, and Green.

The blue LED is illuminated when power is supplied to the EdgeMate.

The red LED indicates system processing.

The orange and green LEDs serve multiple purposes to display both GPS status and Internet connectivity.

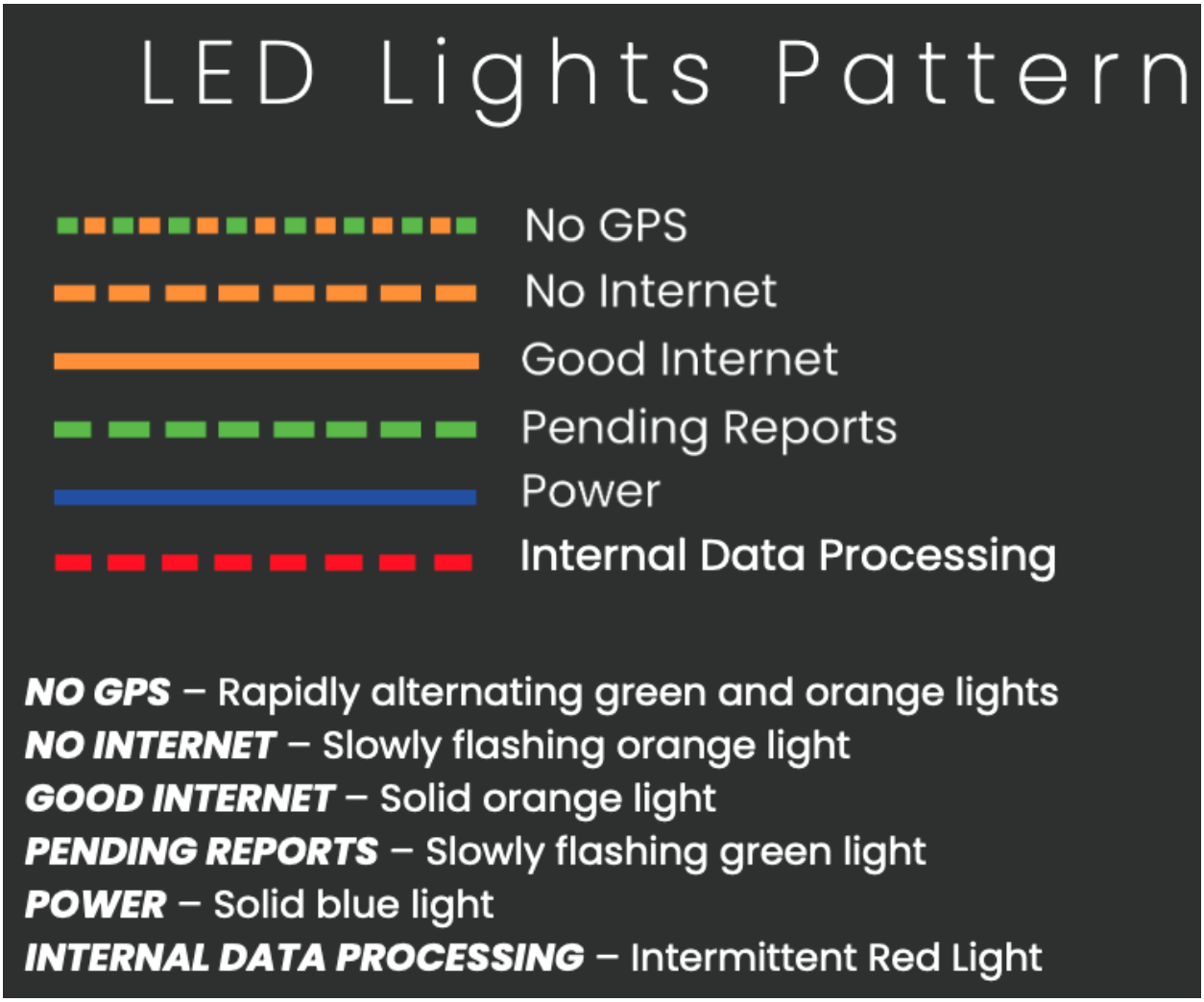
Invalid GPS

The orange and green LED will blink very rapidly in alternating succession when there is invalid or NO GPS data. Read the section “Configuring the GPS Feed” to address this problem.

No Internet

With valid GPS positions, a NO Internet connectivity issue is displayed by a slow blinking orange LED. The orange LED blinks once every 3 seconds when there is no active Internet connection.

We suggest you print and attach the following legend to your unit.



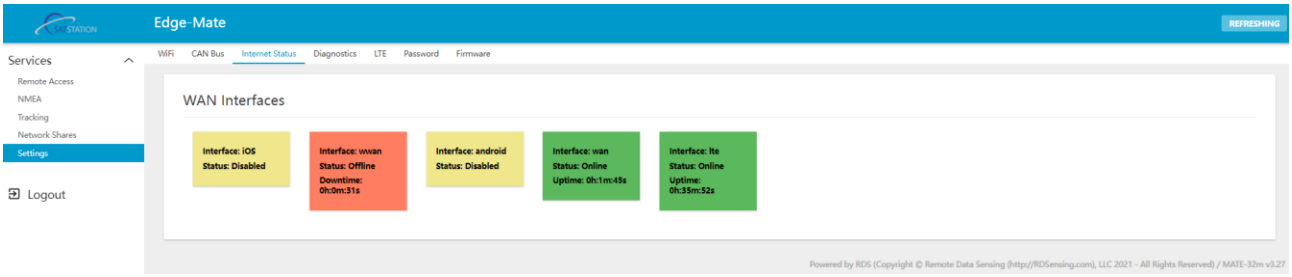
Verifying Internet Connectivity

The EdgeMate provides several methods to determine if you are Internet connected. The simplest way to know if you are connected to the Internet is to Wi-Fi connect to the unit and try to browse pages online. Try Google.com. If the page shows up, then you are Internet connected.

Alternatively a solid orange LED on the top of the EdgeMate indicates a valid Internet connection.

There is a detailed Internet status page found under “Services->Settings” under the “Internet Status” tab. A green square represents an active Internet connection. In the image displayed below, we see that “wwan” or wireless wan (wide area network) is active as well as wan (the Ethernet WAN connection). The squares indicate that the interfaces are online and the uptime for the connection. A red box means that the interface is available, but there is no internet

connection through it. In other words, the interface exists, but it's offline. A yellow box indicates that there is no interface. In this case an Android phone or USB LTE modem has been detected by the EdgeMate.



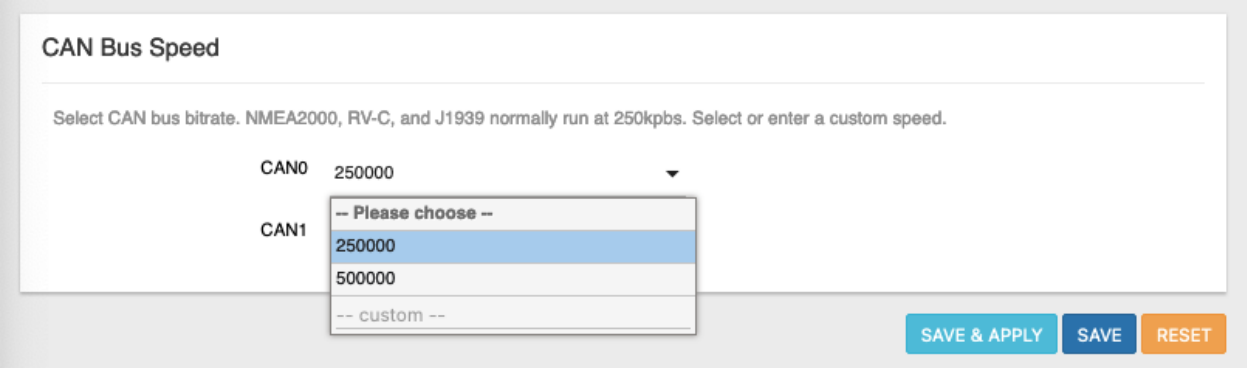
More advanced users can use the tools under the “Diagnostics” tab under “Services->Settings” to diagnose Internet connectivity problems.

CAN Bus Configurator

By default EdgeMate comes configured with two fully functional and independent CAN buses configured to operate at 250000 bits per second. The CAN buses are identical and either can be used to supply NMEA2000 and/or R-VC to EdgeMate. The EdgeMate can be configured to accept data on either CAN Bus port. You could, for example, have NMEA2000 and RV-C data connected to CAN0 on EdgeMate and have an app read data from that connector.

Altering CAN Bus Speed

On occasion, although very rare, it might be necessary to change the default speed on one of the can connectors. This happens for some batteries manufactured in China where the CAN bus operates at 500000 bps. To change the speed of one of the CAN connectors navigate to “settings->CAN Bus”, set the appropriate speed from the pull down menu, and then press “Save & Apply”. Note that a custom speed can be entered by typing the appropriate value at the bottom of the speed pull down where it says “--custom–”.



Joining CAN Bus Networks

At times it may be desirable to join two separate CAN bus networks so that data may be shared between them. This can be accomplished in either one of two ways, using a CAN bus bridge or alternately a CAN bus gateway. In both cases the two CAN buses are logically connected so that they look and act as a single physical network. Data can flow from the bus on CAN0 to the one on CAN1 and vice versa much as if the two networks were physically joined with a connector albeit with some restrictions.

CAN Bus Bridge

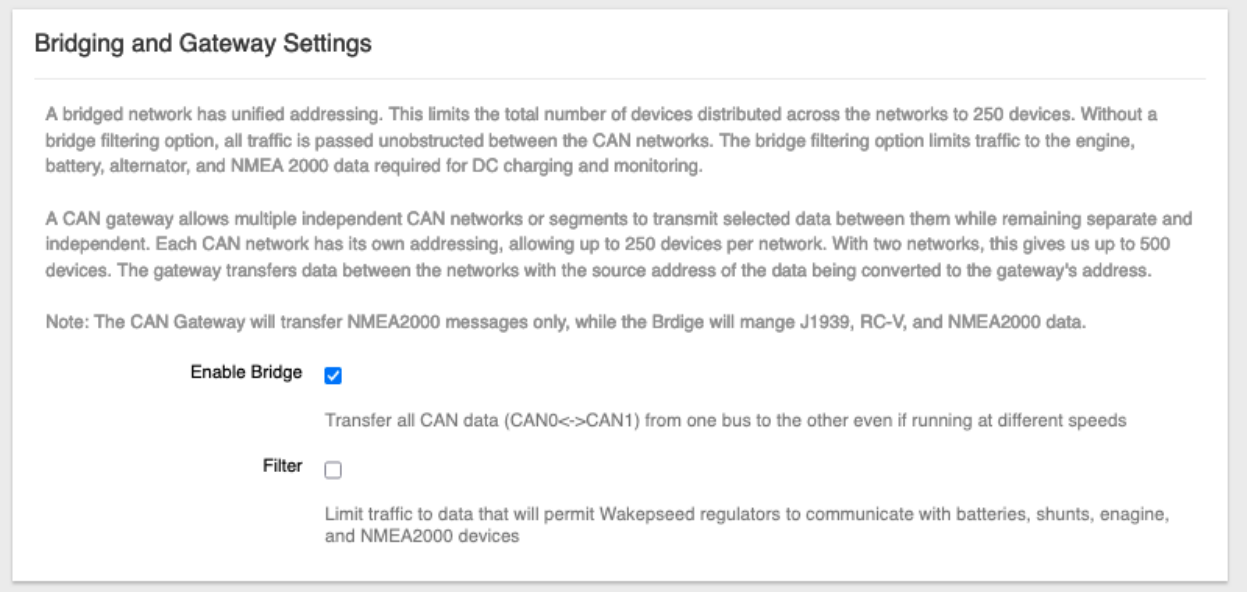
A bridge network has unified addressing which limits the total number of devices across both networks to 250 units. Data is allowed to pass unobstructed between the networks allowing devices on one CAN network to directly communicate with a device on a different network. Electrically the two networks are distinct and separate but logically they act as if they were joined together with a connector.

By default all traffic is passed between the CAN interfaces when in bridge mode which could result in a considerable increase in traffic across both networks. EdgeMate offers an optional bridge filtering mode which reduces traffic. With bridge filtering enabled, you can dramatically reduce traffic. Following is a list of PGNs passed through the bridge when filtering is enabled:

```
61183L,  // EEFF RVC Address Claim ACK
61184L,  // EF00 J1939 Proprietary message
61443L,  // F003 J1939 load
61444L,  // F004 J1939 speed
61588L,  // F094 J1939 High voltage energy storage system
61600L,  // F0A0 J1939 High voltage energy starage system
64788L,  // FD14 J1939 Battery Charger 2
64789L,  // FD15 J1939 Battery Charger 1
65237L,  // FED5 J9139 Alternator
65240L,  // SO Commanded Address
65242L,  // FEDA J1939 Software ID
65259L,  // FEEB J1939 Component ID
```

```
65360L,   // FF50 J1939 Proprietary see J1939-21 for PG details
97792L,   // 17E00,&RVCTerminal

126208L,   // NMEA - Request group function
126464L,   // PGN List - Transmit PGNs group function

126720L,   // 1EF00 RVC Proprietary message
126977L,
126979L,

126993L,   // Heartbeat
126996L,   // Product Information
126998L,   // Configuration Information
127488L,   // Engine Parameters, Rapid Update
127489L,   // Engine Parameters, Dynamic
127501L,   // Binary Status Report
127506L,   // DC Detailed Status
127507L,   // Charger Status
127508L,   // Battery Status
127510L,   // Charger Configuration Status
127513L,   // Battery Configuration Status
127750L,   // Converter (Inverter/Charger) Status

130512L,  // 1FDD0 DC source connection status
130688L,  // 1FE80 Solar controller battery status
130720L,  // 1FEA0,&RVCDateTime
130723L,  // 1FEA3,&RVCChrgStat2
130725L,  // 1FEA5,&RVCDCStatus11
130739L,  // 1FEB3 Solar controller status
130751L,  // 1FEBF,&RVCChargerConfigStat4
130759L,  // 1FEC7,&RVCDCStatus6
130760L,  // 1FEC8,&RVCDCStatus5
130761L,  // 1FEC9,&RVCDCStatus4
130762L,  // 1FECA,&ISODiagnostics
130764L,  // 1FECC Charger configuration status 3
130767L,  // 1FECF DC disconnect command
130768L,  // 1FED0 DC disconnect staus
130795L,  // 1FEEB,&RVCProdID
130966L,  // 1FF96,&RVCChargerConfigStat2
130968L,  // 1FF98,&RVCChargerEqualConfigStat
130969L,  // 1FF99,&RVCChargerEqualStat
131014L,  // 1FFC6,&RVCChargerConfigStat
131015L,  // 1FFC7,&RVCChrgStat
131020L,  // 1FFCC,&RVCChargerConfigStat3
131034L,  // 1FFDA Generator command
131067L,  // 1FFFB,&RVCDCStatus3
131068L,  // 1FFFC,&RVCDCStatus2
131069L,  // 1FFFD,&RVCDCStatus1
131070L,  // 1FFFE,&RVCDateTime
131071L,  // 1FFFF,&RVCDateTime
```

Bridge mode and optional filtering are enabled under the Settings->CAN Bus dialog.



NMEA 2000 CAN Bus Gateway

A CAN gateway allows multiple independent CAN networks or segments to transmit selected data between them while remaining separate and independent. Unlike a bridge, each CAN network has its own addressing allowing up to 250 devices per network for a total of 500 devices connected to EdgeMate. EdgeMate registers itself with each network substituting the source device's address with its own when transferring data between the CAN interfaces. This means that devices on separate networks can not communicate directly between each other. They do so through an intermediary.

By default all NMEA2000 data is transferred through the gateway, although EdgeMate does support a filtering option to reduce traffic. Traffic can be forced to flow in one direction (from CAN0 to CAN1 or vice versa) or uniformly across both CAN interfaces. Filters that limit traffic to DC subsystems (batteries and alternators) and/or engine data can be selected. Although more limited than a CAN bridge, EdgeMate's gateway mode is much more effective at reducing traffic between CAN networks.

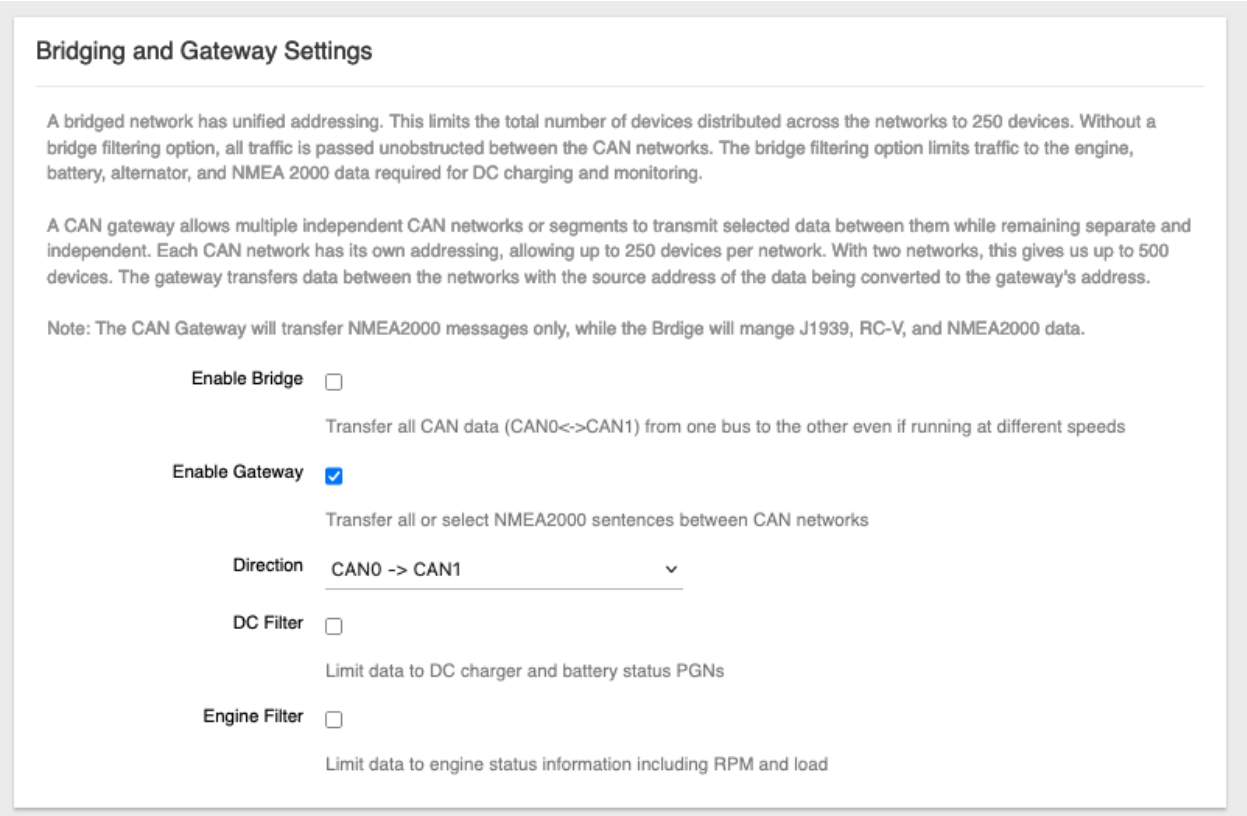
The following NMEA2000 PGNs are allowed through the gateway with filtering enabled:

NMEA2000 DC Filter
- 127506L // DC Detailed Status
- 127507L // Charger Status
- 127508L // Battery Status
- 127510L // Charger Configuration Status
- 127513L // Battery Configuration Status
- 127750L // Converter (Inverter/Charger) Status

NMEA2000 Engine Filter
- 127488L // Engine Parameters, Rapid Update

127489L // Engine Parameters, Dynamic
127497L // Trip Fuel Consumption, Engine
127498L // Engine Parameter, Static

NMEA 2000 gateway mode with optional filtering enabled under the “Status->CANBus” dialog:

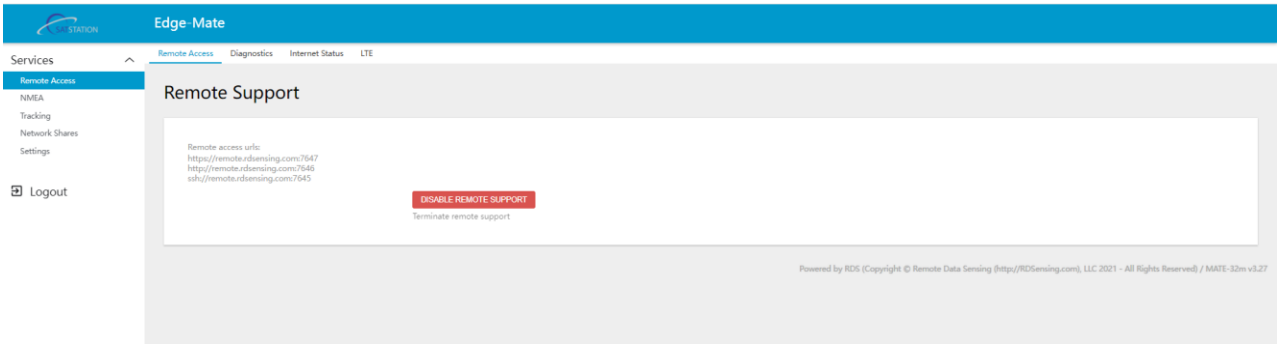


Remote Support

The remote support feature allows technicians on shore to access the EdgeMate and vessels network over the Internet. This is a very powerful feature that allows not only the ability of support personnel to aid you in solving problems with your EdgeMate but also remote access to real time logs for viewing and analysis as you sail along.

To use remote support your EdgeMate must have access to the Internet (see section “Configuring Internet Access”). EdgeMate will only make the feature available if it detects a good Internet connection.

To enable remote support, browse to the “Remote Access” menu entry under “Services” and push the “Enable Remote Support” button. As an option, a short description of a problem can be entered before pushing the “Enable Remote Support” button. This information is sent via EMail to SatStation support personnel.



This action results in the creation of 3 URLs allowing HTTP, HTTPS, and SSH access to your unit. These URLs are randomly unique and only exist until either the “Disable Remote Support” button is pressed or Internet connectivity is lost. In this example we generated 3 URLs that look like

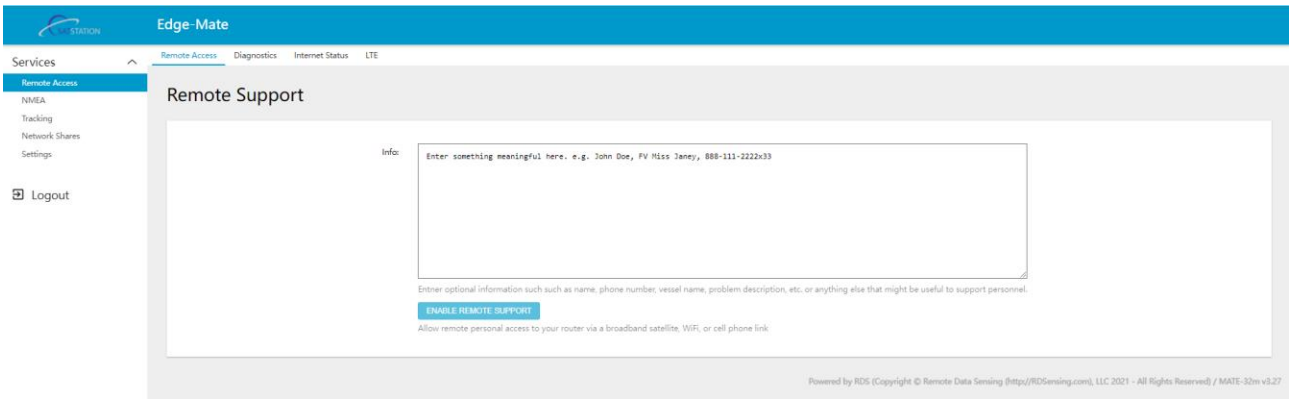
Remote access urls:

- https://remote.rdsensing.com:7647
- http://remote.rdsensing.com:7646
- ssh://remote.rdsensing.com:7645

The EdgeMate is accessible via these URLs in “exactly” the same way as over Wi-Fi on your vessel. Remote service personnel will have access to all the features and services of EdgeMate that you do on your vessel.

Remote Support User

EdgeMate provides a restricted account to enable remote access if for some reason the admin or superadmin user password is lost. Logging into the unit with username “support” with password “support” allows access to only the “Remote Access” menus. No configuration changes to EdgeMate can be made when logged in as the support user, only enabling remote access is permitted.

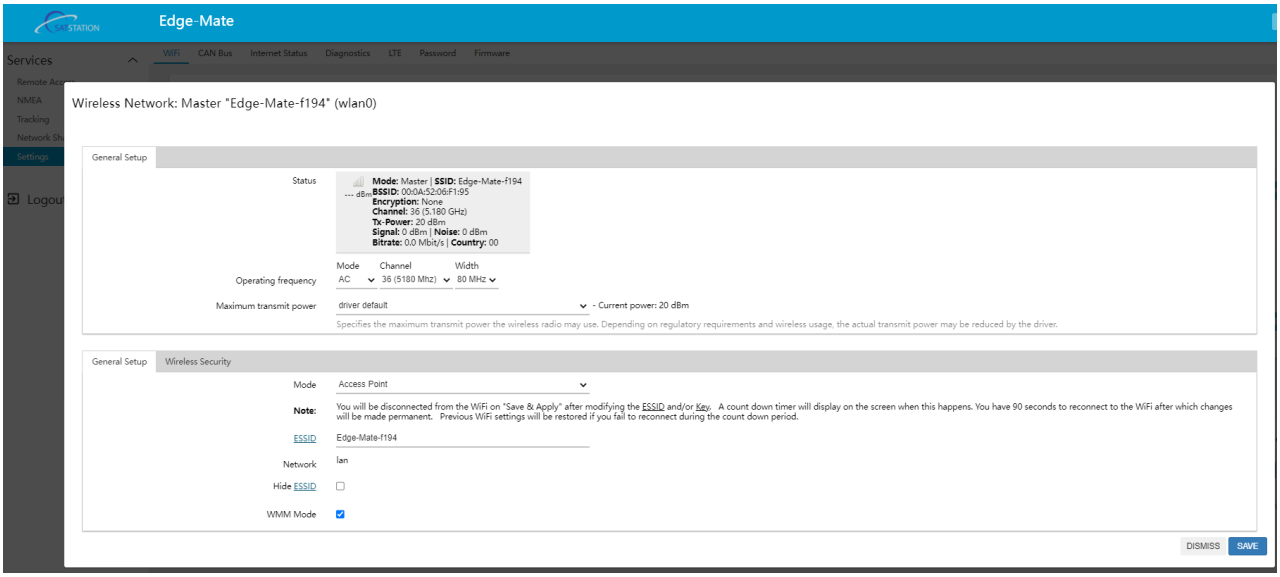


Securing EdgeMate

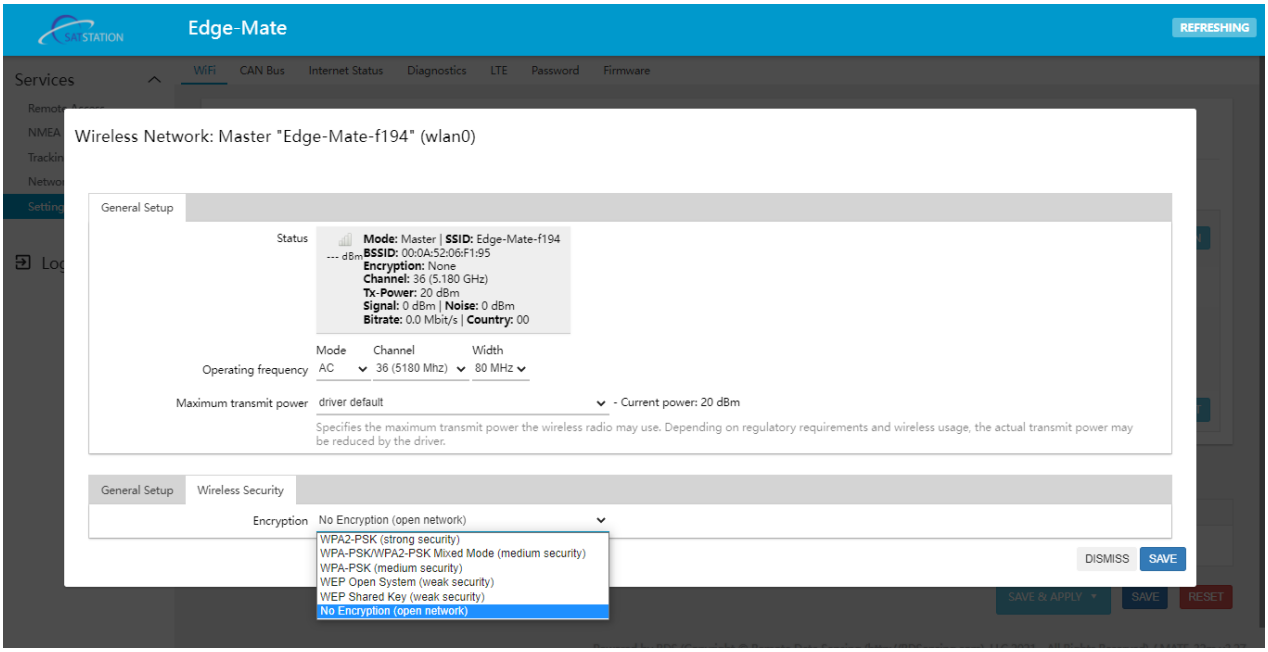
By default, EdgeMate's Wi-Fi is open and unencrypted and the administrator username and password is well known. Since the EdgeMate can provide Internet access to any Wi-Fi client connected to it, it is best to secure the Wi-Fi connection to prevent unintended network access.

Changing the Wi-Fi SSID and Securing with a Password

Wi-Fi connect to the EdgeMate and browse to "Services->Settings" and select "Wi-Fi". Scroll down towards the bottom of the page and push the "EDIT" button for the "Wi-Fi Access Point Hotspot". Under the "General" tab in the next page, scroll towards the button and find the ESSID entry. The ESSID is the SSID that is broadcast by the EdgeMate. My vessel is called 'Bliss' so I want my EdgeMate to advertise itself as "Bliss". Change the ESSID entry to the desired broadcast name.

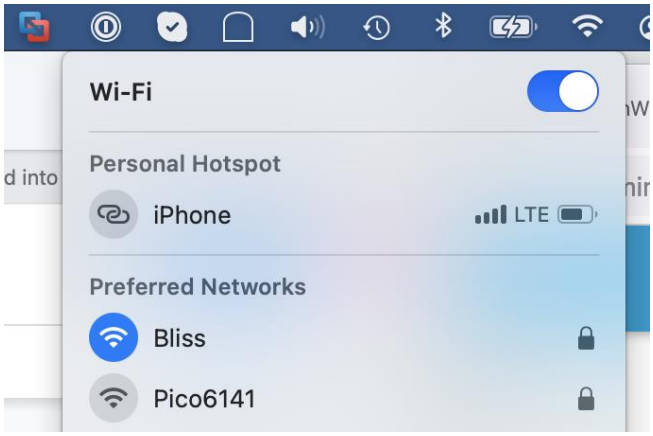


Next, click on the “Wireless Security” tab and select “WPA2-PSK (strong security)”, leave “cipher” on “auto”, and finally enter a password for Wi-Fi. Scroll to the bottom of the page and push “SAVE”. Back on the “Wireless Overview” scroll down to the bottom and push “SAVE & APPLY” to activate the changes. You will be momentarily disconnected from the Wi-Fi and then when you reconnect you will be prompted for the new password.



Important: When changing the SSID and password on the EdgeMate you will be disconnected from the unit if you are Wi-Fi connected to it. You are making changes to the same Wi-Fi that you are connected to. Once the changes are made you will be forced off of the Wi-Fi. You have 90 seconds to connect to the new Wi-Fi SSID using the password you entered to complete the process. Failing to reconnect to the new Wi-Fi SSID during this period will result in the EdgeMate restoring the original SSID and password (which by default is none). This is done as a safety precaution in the event you misstyped in the password. The EdgeMate reminds you of this in the notice displayed right about the “SAVE” button.

Note below that “Bliss” now shows up in a Wi-Fi scan as encrypted when scanning on my Mac.



Changing the Password for Admin

Connect to the EdgeMate via Wi-Fi and login with username “admin” using the default password (“admin”).

To change the admin password, browse to the “Password” tab and enter the new password twice.

Now logout from the EdgeMate by selecting the “Logout” menu entry under “Settings”.

Log back into the router using username “superadmin” with password “superadmin” and repeat the process.

Although we have not discussed “superadmin” this login provides advanced features. Advanced users may enjoy exploring the advanced features of the EdgeMate, but most users will not require these. Nonetheless, the superadmin account should be secured.

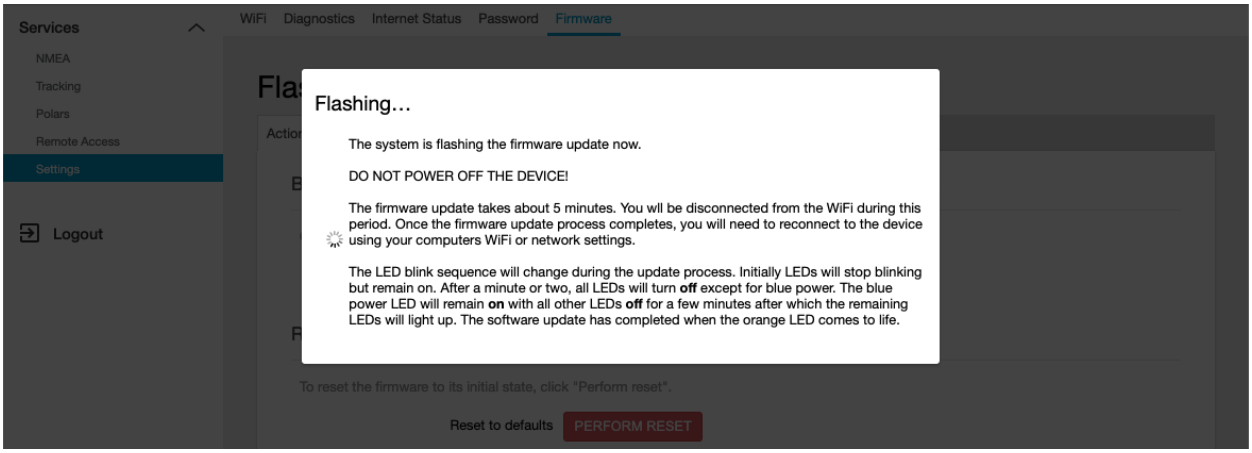
Firmware Updates

On occasion SatStation may provide updates to the EdgeMate software that includes enhancements and bug fixes. Users wishing to update their devices should download the latest version of the firmware from SatStation and store it on their computer.

To upgrade the firmware, login to the EdgeMate via Wi-Fi (or Ethernet/WAN), login as admin, and browse to “Services->Settings”. Select the “Firmware” tab and select “FLASH IMAGE…” at the bottom of the page and follow the prompts. You will need to browse for the software image you downloaded to your computer, upload it to the EdgeMate, and then confirm that you wish to update the firmware.

You have the option of keeping the current configuration. Normally you would want to check this option, otherwise you would need to go through the full setup of the unit as described in this document.

The following screen will pop up once you confirm to proceed with the update.



Firmware update is complete. The firmware update takes about 5 minutes to complete. Note that you will be disconnected from Wi-Fi during the update period since the unit will be off-line. On completion of the software update, you will need to reconnect to the device using your computer's Wi-Fi or network settings.

The LEDs will blink during the update process in the following sequence. First the lights will stop blinking. After a few minutes all the LEDs, except the blue one, will go off as the unit reboots. The blue power LED remains on during the reboot. After a few additional minutes the LEDs will resume their normal blinking pattern. The software update is complete once the orange LED comes on.

Reconnect to the unit as usual and verify the new software version by examining the page footer in any view.

Factory Reset

The EdgeMate can be returned to its original factory defaults (i.e., the way you originally received it) by one of two methods.

Software

If you are able to Wi-Fi or Ethernet connect to the unit and can login to the web admin UI, browse to "Services->Settings" and select the "Firmware" tab. Push the "PERFORM RESET" button to restore the factory default settings.

Note that it takes 5-10 minutes for the process to complete. Do not interrupt the EdgeMate during the reset process.

Hardware Reset Switch

A hardware reset is in order if you have either lost the Wi-Fi password or admin password, or are unable to otherwise access the web admin UI for the EdgeMate.

To perform a hardware reset, locate the reset button next to the power inlet for the unit. You will find it through a small pin hole through the enclosure. Use a paper clip or other small object to depress the button for 15 seconds while the unit is powered on. After 15 seconds, release the button. The unit will then perform a factory reset. Note that a quick push of the button will reboot the unit, but not reset it to its defaults. The button must be held for more than 10 seconds and less than 30 for the reset action to occur.

Legal

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

. Reorient or relocate the receiving antenna.
. Increase the separation between the equipment and receiver.
. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
. Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC ID: 2A23ZEdgeMate
Model: EdgeMate

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.