SA2100X-UG001

SA2100



User Guide

Version 2.0

inseego

August 7,2015

INSEEGO COPYRIGHT STATEMENT

©2015 Inseego Corporation. All rights reserved. The information contained in this document is subject to change without notice and should not be construed as a commitment by

INSEEGO CORPORATION TRADEMARKS AND SERVICE MARKS

Inseego is a trademark of Inseego Corporation, and the other trademarks, logos, and service marks (collectively the "Trademarks") used in this user manual are the property of Inseego Corporation, or their respective owners. Nothing contained in this user manual should be construed as granting by implication, estoppel, or otherwise, a license or right of use of Inseego Corporation or any other Trademark displayed in this user manual without the written permission of Inseego Corporation or its respective owners.

Inseego and the Inseego Corporation logo are all trademarks of Inseego Corporation.

MiFi® and the MiFi logo are registered trademarks of Inseego Corporation.

Contents

Introduction **1**

Device Description and Label 2

Technical Specifications 4

Features and Functions **7**

LEDs 8

Connectors 10

Reset Button 11

Installation **12**

SIM Installation 13

Battery 14

Precautions and Guidelines 16

Mounting Methods 17

Driver Installation 18

Using the Device **23**

Powering the Device 24

Positioning Your Router 25

Connecting to the SA 2100 Router 26

Using the Web User Interface **27**

Logging In 28

Home 30

Connected Devices 32

Data Usage 35

Settings 36

- Device Settings 36
- Hotspot Settings 50
- Mobile Network Settings 53
- Advanced Settings 57

Messages 70

GPS 71

Customer Support 73

About 74

- Current Status 75
- Device Info 78
- Diagnostics 80
- Logs 84

Software Update 86

Accessories **88**
Accessories List 89
Antenna 90
Backup Battery 92
Power Cable 93
USB Cable Part 95

Compliance and Regulatory **96**
General Disclaimer 97
Warranty Information 98
Regulatory Compliance 101

1

Introduction

Device Description and Label
Technical Specifications

Device Description and Label

The compact SA 2100 is cellular router designed with multiple mounting options and connectivity interfaces for M2M applications including Fixed Telemetry, Fleet Management and Asset Tracking, and Connected Car, right out of the box. Internal antennas minimize installation time and cost, while auto switching between internal and external antennas provides options to ensure the best RF performance in any situation. The SA 2100 is shown in the following image.



Fast and Future-Proof

With connectivity to 4G LTE and 3G networks, the SA 2100 provides the highest wireless data rates and the longest device service life. Now managers can upgrade firmware remotely, manage devices centrally and reduce the number of costly site visits, all while being assured that their solution will support carrier network updates for years to come.

Reliability

The rugged SA 2100 is designed to get connected easily and stay connected. The MiFi® Powered™ platform offers unique features to ensure business continuity. Battery backup delivers instant failover during power outages. Advanced security of encryption and authentication protocols offers peace of mind. The extended operating temperature range makes the SA 2100 the reliable choice.

Easy Deployment, Easy Integration, Easy Usage

Securely connect, collect and transmit valuable field data quickly and easily, just install and deploy – no complicated configurations or programming necessary. Designed with multiple interfaces, internal

antennas, intuitive web UI, preconfigured default settings, and self-registration to the central management already enabled, the SA 2100 is built with "Power it up, ready to connect" in mind.

Cloud Management

With cloud-enabled N4A™ Device Manager software, any number of devices can be easily managed and monitored around the globe in a cost-efficient and scalable manner. The N4A™ Device Manager features remote management and monitoring from a central location to configure, monitor, manage, and even update devices and assets all over the air minimizing costly on-site visits.

System Requirements

The SA 2100 Cellular Router allows you to set up a network and provides both wired and wireless connectivity.

NOTE: This device is intended for professional installation and not for consumer use.

Requirements include:

- A computer or computing device supporting Wi-Fi 802.11 b/g/n
- Internet browser software, such as Microsoft Internet Explorer 8.0 or higher, Firefox, Safari, Opera, or Chrome

Label

The label is located on the back panel of the router displays the following information:

- MAC Address
- IMEI or ESN Number
- SSID (Factory preset, unique to each device)
- Wi-Fi Key (Factory preset, unique to each device)

Here is a sample label that shows placement of the various fields:



Technical Specifications

Case

Dimensions:	(L x W x H) 107 x 81 x 30 mm
Weight:	220 g
Mounting Options:	Mounting bracket, Velcro tape, tie-wrap, bolts, adhesive

Cellular Technology

	SA2100-xx-AT	**SA2100-xx-VZ**
Frequency	4G LTE: 750/850/AWS/1900 MHz 3G UMTS/HSPA/HSPA+: 850/900/AWS/1900/2100 MHz 2G GPRS/EDGE: 850/900/1800/1900 MHz GSM/GPRS Radio 850/900/1800/1900 MHz	4G LTE: 700/1700 MHz 3G CDMA 2000: 850/1900 MHz
Bands	LTE: B2, B4, B5, B17 WCDMA: B1, B2, B4, B5, B8 GSM: B8, B9, B13, B14	LTE: B4, B13 CDMA: BC0, BC1
Data Speed	LTE: 100 Mbps DC-DSPA+: 42 Mbps HSPA+: 21 Mbps	LTE: 100 Mbps CDMA: 3.1 Mbps
Routing	DHCP server, DNS, static or dynamic IP address, port filtering, port forwarding	
Security	NAT, SPI Firewall, VPN pass-through, IPSec VPN, MAC access control	
Wireless Network	Wi-Fi 802.11 b/g/n, 10 clients, pre-configurable security: WPA/WPA2	
Certifications	FCC, CE, IC, PTCRB, GCF, Wi-Fi Alliance, eMark, Safety, AT&T	FCC, Wi-Fi Alliance, Safety, Verizon

Power

Input Power Range:	9 - 32 VDC (Molex Connector); 12V or 24V vehicle ready
Current Consumption:	800 mA @ 12 VDC (max power, normal operation) 147 mA @ 12 VDC (min power, normal operation) 57 mA avg (suspend mode) 8 mA avg (deep sleep mode)
Lithium Battery (Optional):	Rechargeable 3.7 V 2900 mAh 1073 Wh Li-ion battery

Environment

Operating Temperature:	-30° C to 70° C (external power) -20° C to 60° C (battery)
Storage Temperature:	-40° C to 85° C (external power) -40° C to 60° C (battery)
Relative Humidity:	Up to 95% non-condensing

Antenna

Internal Cellular Antenna:	(primary + diversity)
External Cellular Antenna:	(primary + diversity) Automatically switches between internal and external; SMA Connector
Internal Wi-Fi Antenna:	2.4 GHz
Internal GPS Antenna:	1575 MHz

Interfaces, I/O, and LED

1 Ethernet Port (RJ45 Connector)
1 Micro-SIM Card Slot (Inside Battery Compartment)

2 Digital Inputs, 1 Digital Output
1-Wire® Interface
1 Micro USB On-The-Go (latched)
USB to Serial Supported
2 User-Controlled I/O
LED Indicators: Power, Wi-Fi, Network, Signal Strength

Device Management

Production Environment:	Cloud-based (Optional)
Testing Environment:	Cloud-based; 90-day free access with engineering support
Bulk Provisioning:	Over-the-air or local
Firmware Upgrade:	FOTA (Firmware-over-the-air) or local

Additional Features

FOTA
On-Board, Configurable Smart Agent: GPS, Accelerometer, GPIO, 1-Wire, Exception-Based Reporting
3-Axis Digital Accelerometer
I/O Control

Models

SA2100-xx-AT (AT&T variations)

SA2100-xx-VZ (Verizon Wireless variations)
SA2100-10-R (ROW Telematics)
SA2100-20-R (ROW Telemetry)

Document References

Guide Number	Guide Title
SA2100X-AT002	SA 2100 Telemetry AT Command Reference Guide
SA2100X-AT003	SA 2100 Telematics AT Command Reference Guide
ENF0000AN002	FOTA Application Note
ENF0000CB001	API Reference
ENF0000AN014	Access the Inseego Corporation M2M Test Server

2

Features and Functions

LEDs
Connectors
Reset Button

LEDs

The SA 2100 router has LEDs that verify status, signal, and connectivity.



The following table describes each LED:

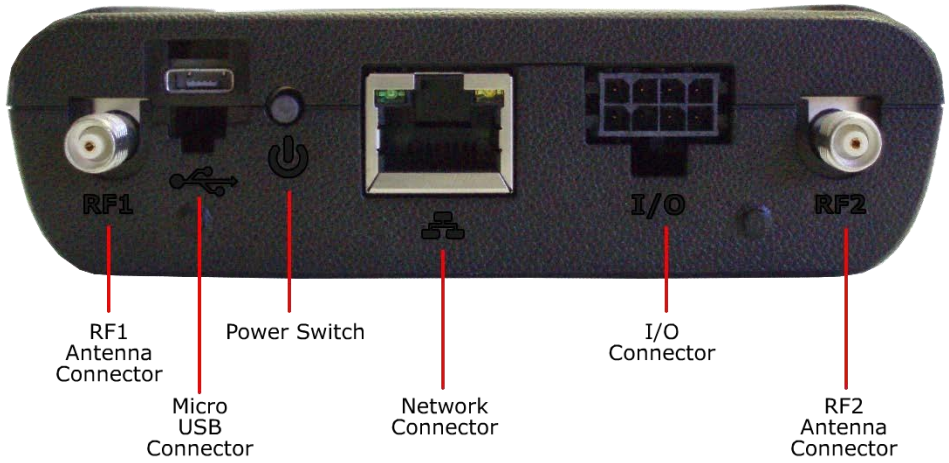
Symbol	LED	Color	State	Description
	Power	Green	On	Normal operation (External or Battery Power) **NOTE:** When operating on Battery power, all other LEDs are OFF. The LED blinks slowly, once every 5 seconds, when running on the battery.
			Blinking 1 sec On 2 sec Off	During device Reset or Power-up sequence
	WiFi	Green	Off	Wi-Fi not enabled or No Wi-Fi connected devices or device is powered from Battery
			On	External Power - Wi-Fi devices attached but no Wi-Fi traffic
			Blinking 1 sec On 1 sec Off	Wi-Fi traffic
Symbol	LED	Color	**State**	**Description**
	WAN – LTE	Green	On	Attached (LTE) – no traffic
			Blinking 1 sec On 1 sec Off	PDP Activity

	WAN – 4G/3G	Blue	On	Attached (4G/3G) – no traffic
			Blinking 1 sec On 1 sec Off	PDP Activity
	WAN – 2G	Orange	On	Attached (2G) – no traffic
			Blinking 1 sec On 1 sec Off	PDP Activity
	Cellular 5-bar signal strength	Green	Off	No SIM/No Signal/Operating from battery
			On	Active only when external power is present.

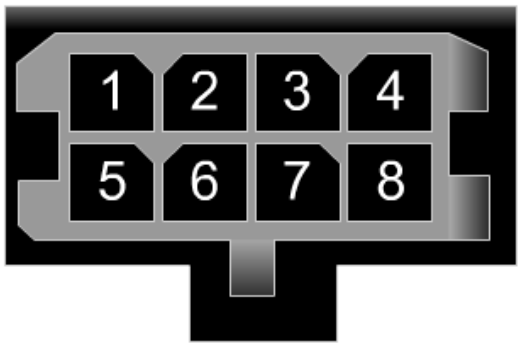
NOTE: While the SA 2100 is operating on battery power, the Power LED is the only LED that operates.

Connectors

The SA 2100 router has the following connectors:



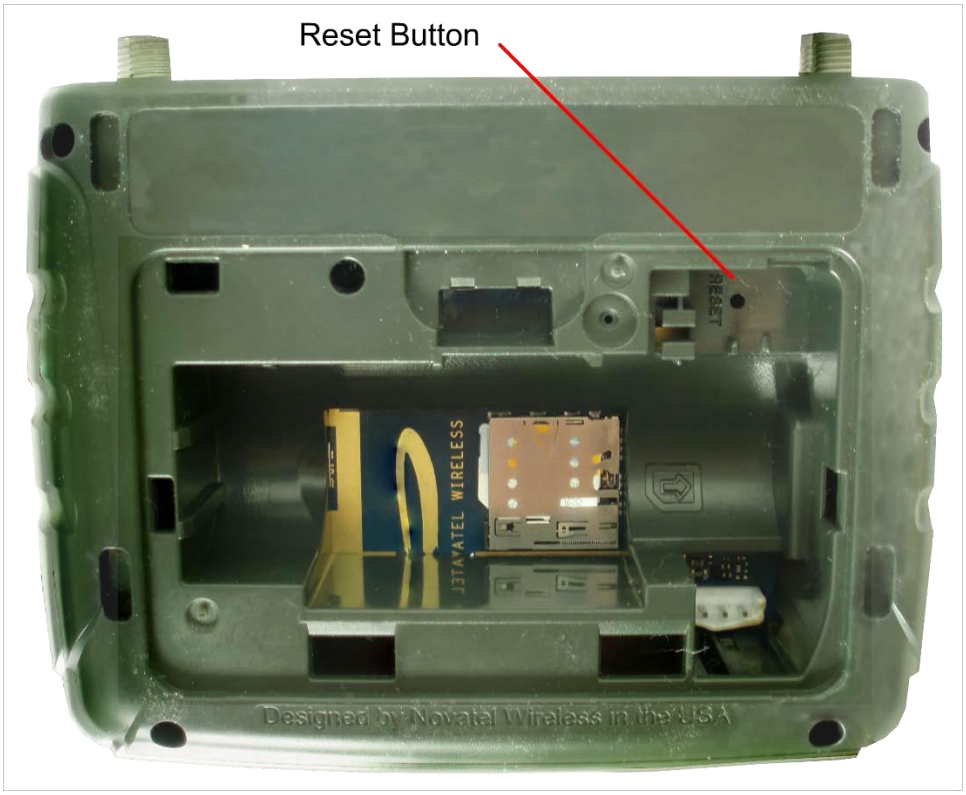
RF1	Cellular Antenna Connector RF1 (Primary)
	Micro USB Connector
	Graceful Shutdown Button
	Network Connector (Ethernet)
I/O	8-Pin I/O Connector (Includes Power)
RF2	Cellular Antenna Connector RF2 (Diversity)



For Pin Out descriptions, see the Power Cable section.

Reset Button

The Reset Button is located inside a corner of the battery compartment. The button is a small hole about 1.5mm in diameter, with the word "RESET" below it. The location is shown in the following image.



NOTE: If a reset is required, use a small pointed object, such as a paperclip, to push the Reset button.

3

Installation

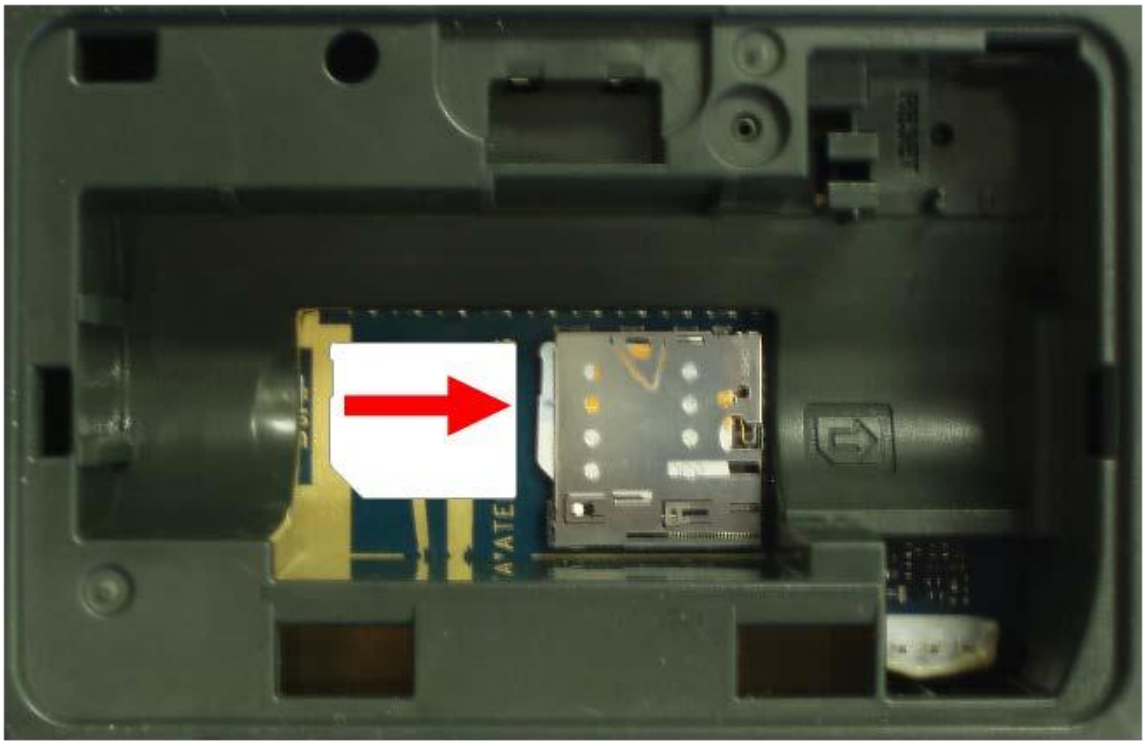
SIM Installation
Battery
Precautions and Guidelines
Mounting Methods
Driver Installation

SIM Installation

To insert the SIM card:

1. Open the device by removing the lid for the battery compartment.
2. Remove the battery to uncover the SIM card holder.
3. Insert the SIM card into the SIM holder.

   You should hear a "click" when the SIM card is in place.



4. Insert the device "door" plate into the opening and snap into place.

   The SIM Installation is complete.

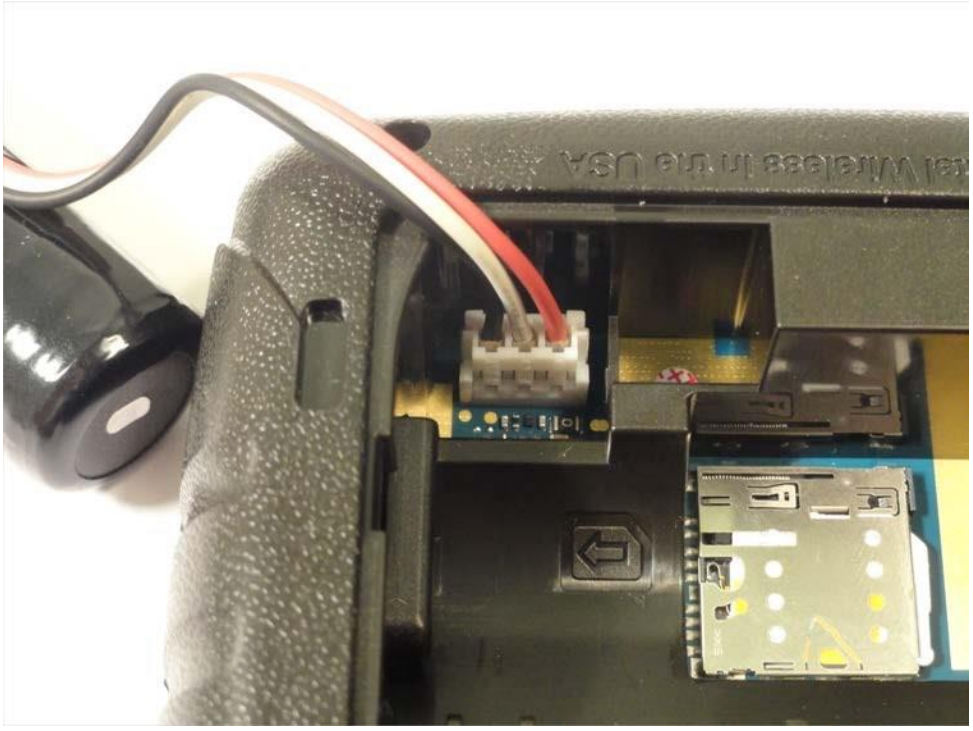
Battery

To insert the battery:

1. Open the device by removing the lid for the battery compartment.



2. Connect the battery plug to the battery jack in the device as shown in the following photo.



3. Place the battery into the recessed compartment as shown in the following photo.



4. Finally, replace the battery compartment cover.

Precautions and Guidelines

As you determine the mounting location and prepare to install the device, be sure to heed the following precautions and guidelines:

- Place the router in an area free from liquids, dust, and extreme temperatures.
- Store the router back in its box when not in use.
- Do not block any ventilation openings by applying adhesives or labels to the router as this might cause the device to overheat or it might interfere with the antenna.
- Clean only with a clean, dry cloth.
- Protect the cord from being crushed or pinched.
- Route the cord so that it is not easily damaged by someone walking on it, or by items sitting on or against it.
- Avoid dropping or shaking the router.
- Avoid moving the router when it is powered on.

Mounting Methods

To mount the device using the Mounting Bracket, use the accessory SKU # 21915042.

WARNING! While performing these steps, do not apply excessive force to the retention legs or snap feature prior to inserting the device as this may deform the mounting bracket.



Mounting Bracket

Secure the mounting bracket to the desired mounting surface using one of the following methods:

- Two (2) # 6 screws
- Double-sided tape

Insert the device into the mounting bracket as shown in the figure above. The device should be inserted with the battery compartment down. Take care to position the device so that the top of the device has the best unobstructed path to the sky.

Double-Sided Tape

CAUTION! If securing the device using double-sided tape or a method not described in this manual, note the following precautions:

- Excessive force in the middle of the device may cause damage to the device.

- If using rigid mounting hardware, apply pressure only to the ends of the device. Limit the mounting pressure only to the amount needed to secure the device.

Driver Installation

Use the following steps t o correctly install the drivers in Windows 7 using the Inseego Corporation Driver Setup Utility.

To install the drivers:

1. Double-click the **Inseego Corporation Factory Driver Installer** executable file to run the Inseego Corporation Driver Setup Utility.



The Inseego Corporation Factory Driver Installer Welcome window opens.



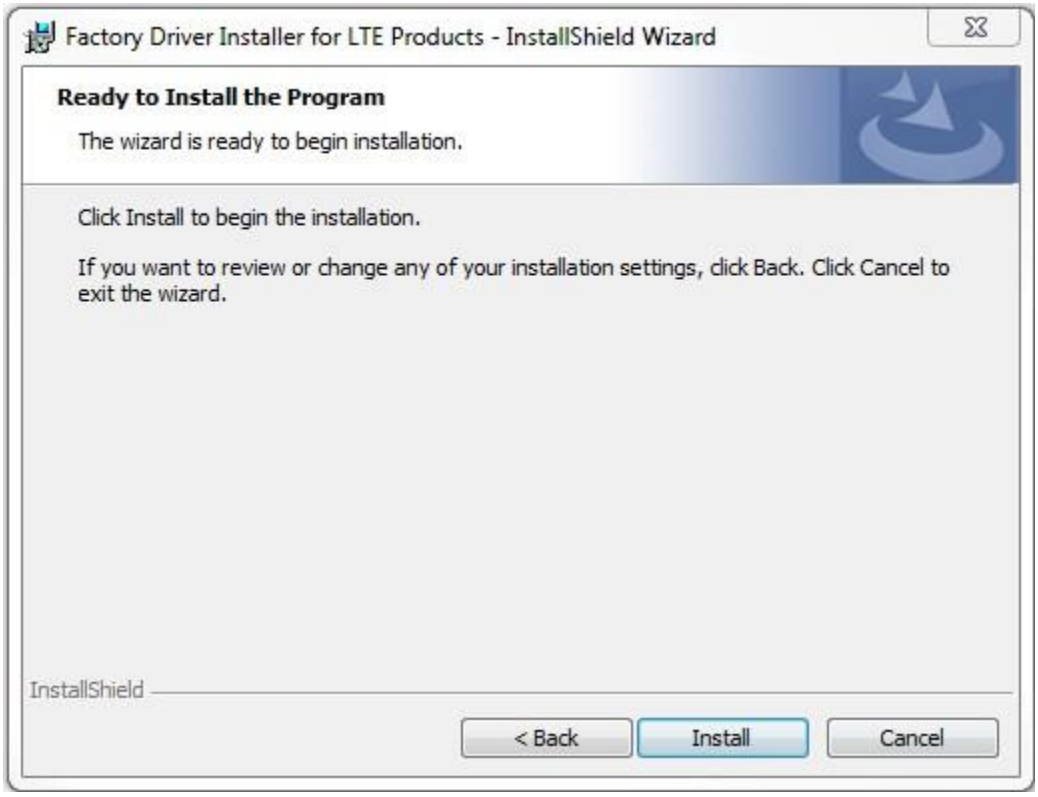
2. Click **Next**.

   The Inseego Corporation Factory Driver Installer License Agreement Window opens.



3. Read the terms, and if you agree, select **I accept the terms in the license agreement** and click **Next**.

The Ready to Install the Program window opens.

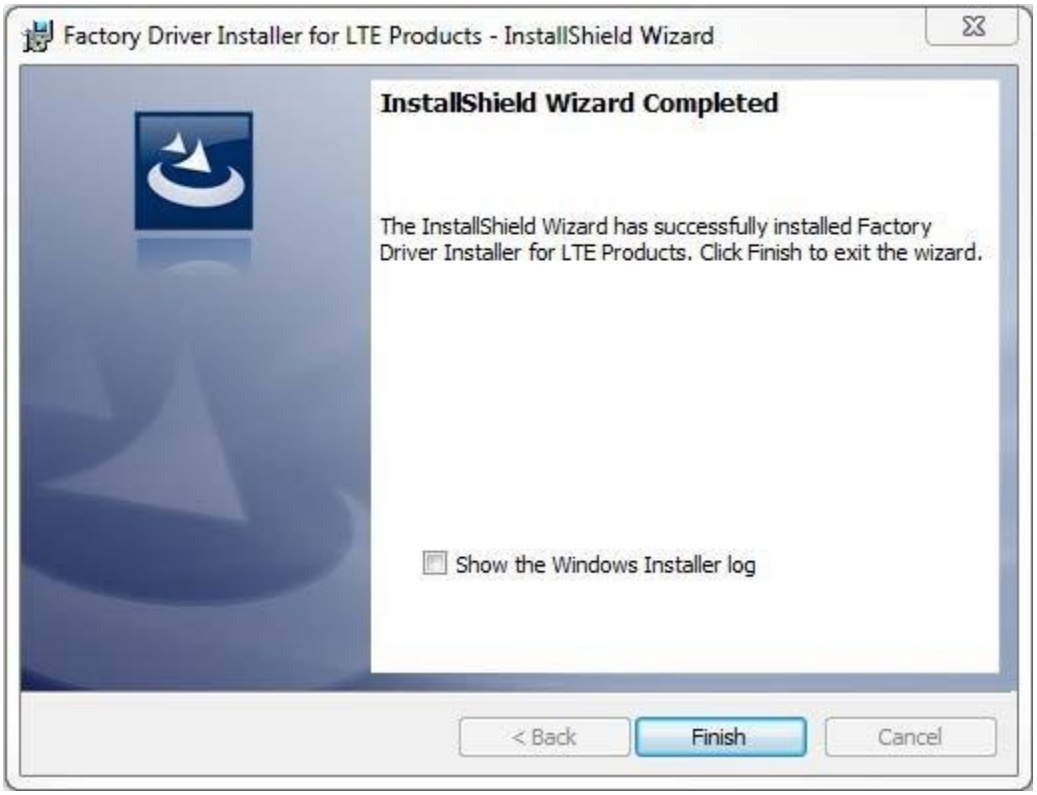


4. Click **Install**.

The Installation Progress window opens.



Once the installer has successfully installed the driver, the Installation Complete window opens.



5. Click **Finish.**

4

Using the Device

Powering the Device
Positioning Your Router
Connecting to the SA 2100 Router

Powering the Device

When the power adapter is connected, the SA 2100 powers up automatically. It takes approximately two minutes for the device to power up and register on the cellular network.

To power the device:

1. Connect the device to a power source.
2. Push the Power switch that is located in the back of the device.

   To view the Power switch location, see the Connectors section.
3. The device power LED lights up to indicate that it is powered on.

   It may take approximately two minutes for the device to power up.

Using the Battery

To power the device using the battery:

1. See the Inserting a Battery section for instructions.
2. Push the Power switch that is located in the back of the device.

   To view the Power switch location, see the Connectors section.
3. The device power LED should lights up to indicate that it is powered on.

   It may take approximately two minutes for the device to power up.

Positioning Your Router

The router allows you to access your network almost anywhere within a given operating range. However, this range depends on where you place your router. The placement of furniture, the thickness of walls, and the number of walls a signal must travel through can limit this range.

For best results, place your router:

- Away from interference such as microwaves, ceiling fans, security systems, or cordless phones
- Away from large containers of glass or concrete (fish tanks, mirrors, brick or concrete walls)
- Away from large metal surfaces (cook tops, metal doors, aluminum studs, appliances)
- Close to a window but out of the way of direct sunlight (great for 4G reception)
- Close to an AC outlet and near Ethernet computer cables

- In an elevated location
- In line-of-sight to wireless devices
- Near the computers or other devices that communicate with the router
- On an upper floor (if applicable)

When using multiple points of access, use different radio frequency channels for adjacent access points. We recommend leaving 5 spaces between channels (1 and 6, or 3 and 8).

Connecting to the SA 2100 Router

Users can connect to the SA 2100 router using either USB cable or Wi-Fi connection.

Connecting using USB

To connect using USB:

1. Install the USB and network adapter drivers using the driver installation executable file provided by Inseego Corporation. (Detailed instructions for installing these drivers are provided in the Driver Installation section of this document.)

2. Ensure the SA 2100 router is powered on.
3. Connect the router to a USB port on the computer using a micro-USB cable.

Connecting using Wi-Fi

To connect using Wi-Fi:

1. Ensure the SA 2100 router is powered on.
2. Connect to the router using the SSID and WPA key information provided on the label.

5

Using the Web User Interface

Logging In
Home
Connected Devices
Data Usage
Settings
Messages
GPS
Customer Support
About

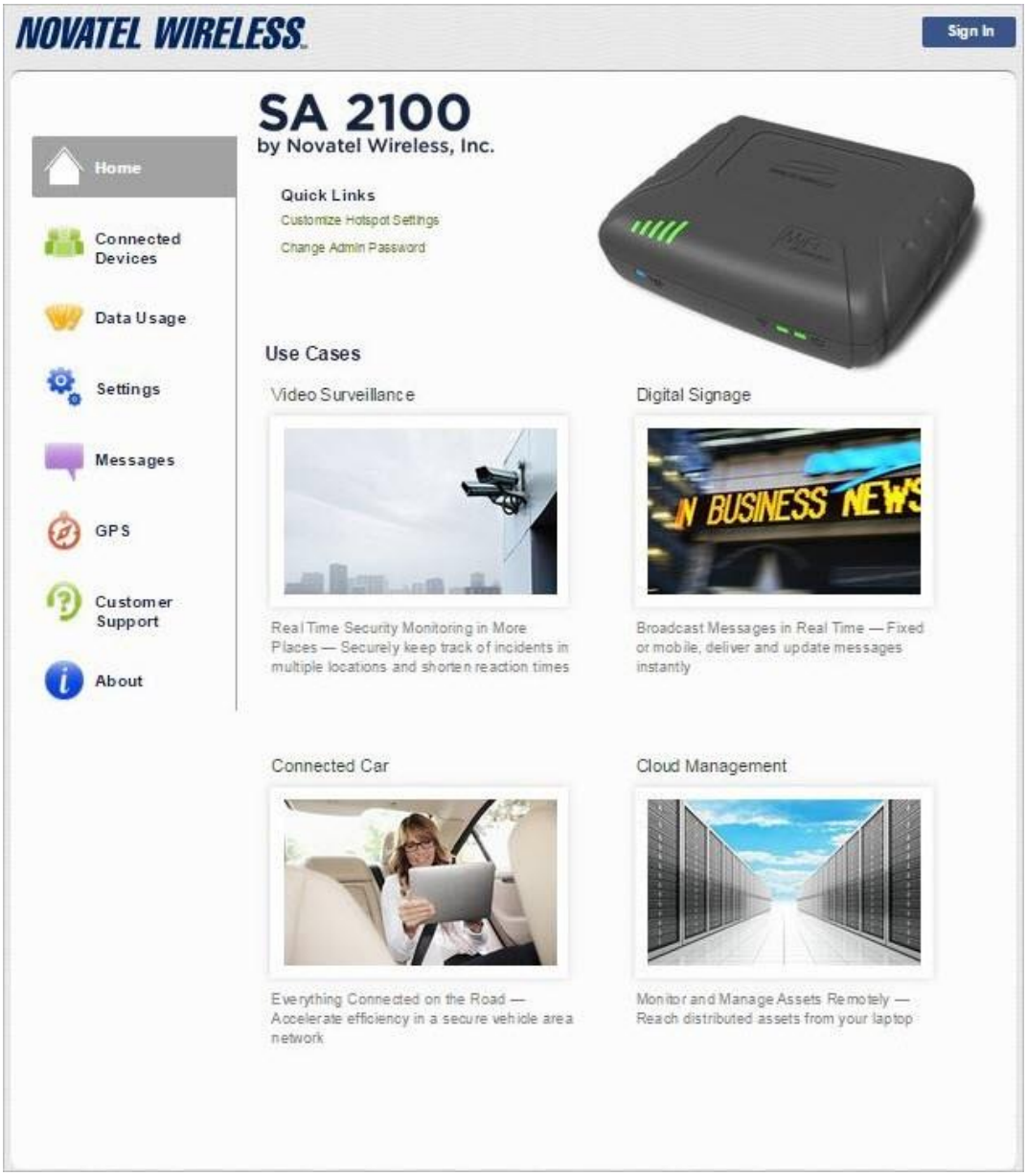
Logging In

To log in to your SA 2100 Web Interface:

1. Open your Internet browser and navigate to one of the following URLs:

   - 192.168.1.1
   - http://my.sa2100/

   The SA 2100 Home Page opens.



2. Click the **Sign In** link in the top right corner of the page to open the SA 2100 Web Interface Sign-In page.



3. Enter your Administrator password and click **Sign in**.

NOTE: The default Administrator password is "admin" (without the quotation marks).

Home

To access the home page of the SA 2100 Web User Interface:

- Click the **Home** tab.

The homepage displays quick links and navigation tabs on the left side of the page.



The left side of the page displays navigation tabs for:

- Home
- Connected Devices
- Data Usage
- Settings
- Messages
- GPS
- Customer Support
- About

The SA 2100 Home page has Quick Links for the following:

- Customize Hotspot Settings
- Change SA 2100 Administrator Password

The Quick Links are shortcuts to the most commonly used settings. Details of these settings are discussed in the Settings section of this document.

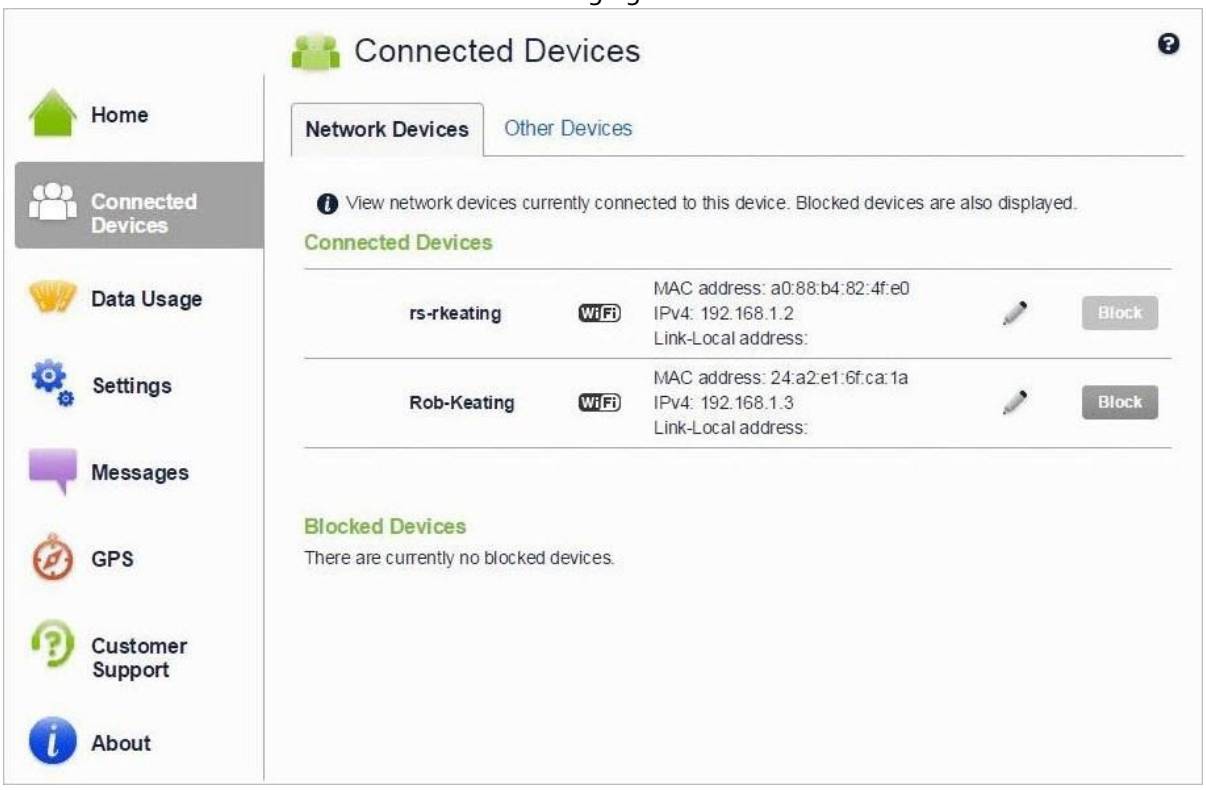
Connected Devices

This page displays details of each network device connected to this SA 2100, including any computer connected via a USB/Ethernet connection.

The Connected Devices screen has two tabs: Network Devices and Other Devices.

Network Devices

The Network devices tab is shown in the following figure.



Connected Device List

The following information is displayed for each network device which is currently connected.

Type

The first column uses an icon to indicate the type of connected device. You can use the "Edit" option to set or change the type.

If the type has not been set, no icon is displayed. Once you set the device type, an appropriate icon is displayed.

Name

Normally, this is the hostname of the connected device, as set on the connected device. If you have used this interface to assign a name to a connected device, the assigned name displays in place of the hostname. In rare cases, the hostname may be unavailable.

You can use the "Edit" option to change the name of any connected device.

Connection Type

An icon indicates the network connection type for each connected device.

MAC Address

The MAC Address is a unique network identifier for this connected device.

IP Address

The IP address of the connected device.

Link-Local

If supported and used, the IPv6 address (Link-Local address) of the connected device is displayed.

Blocking and Unblocking Devices

Block Button

Clicking the "Block" button disconnects the connected device and prevents it from reconnecting. The blocked device then appears in the Blocked list. This option is available for use with each connected device, except for your own device, and any device connected via USB.

Blocked Devices

This lists any devices you have blocked. Note that since these devices are not currently connected, and are blocked from connecting, they do not have an IP address. Instead, they are identified by their name and MAC address.

Unblock Button

Clicking the Unblock button unblocks a previously blocked device, freeing it to connect again. The unblocked device is deleted from the Blocked List, and will reappear in the Connected Devices list when it connects.

Other Devices

This page lists non-network devices which are physically connected to the SA 2100. The Other Devices tab is shown in the following figure.



USB Devices

This panel lists any USB devices which are connected to the USB host on the SA 2100, using the USB On-The-Go (OTG) feature to switch the SA 2100 micro-USB port to host mode. (A micro-USB OTG adapter is required.)

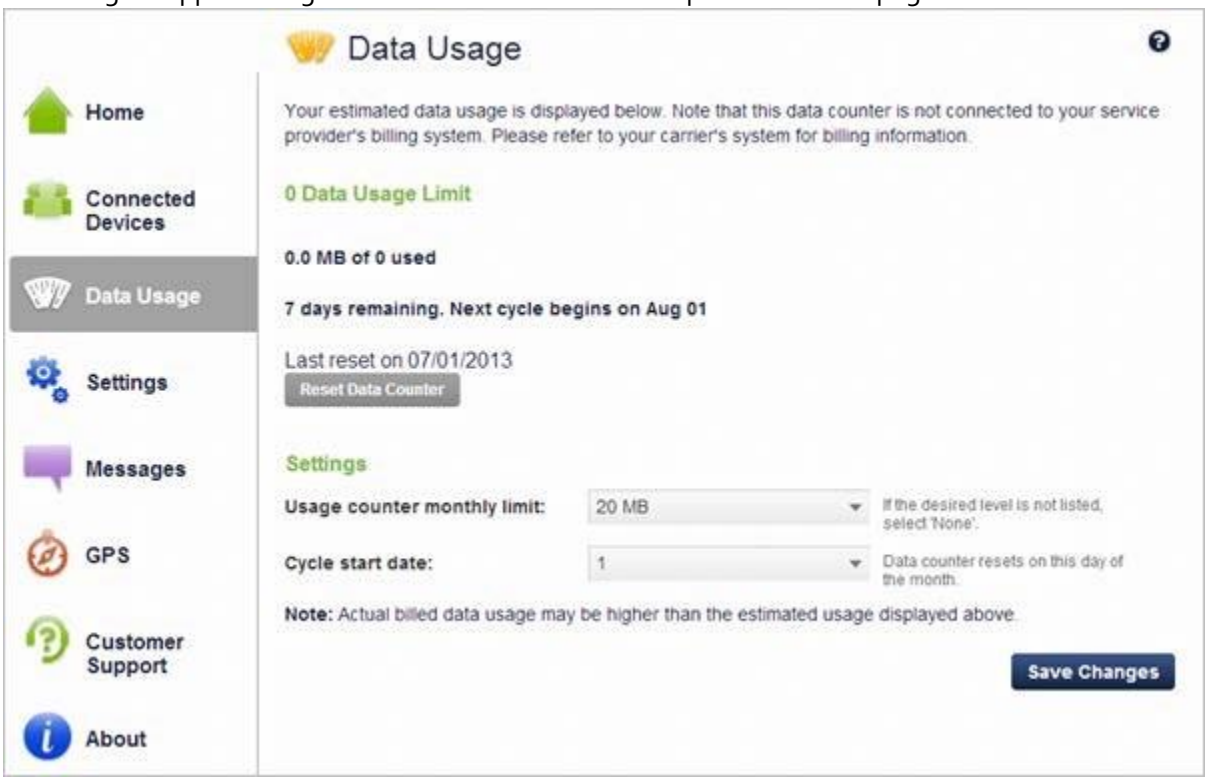
NOTE: If a computer is connected to the SA 2100 then the computer is the host, and the USB connection becomes a network connection. The computer would then be listed in "Network Devices" rather than in this list.

1-Wire Devices

If any 1-Wire devices are attached to the SA 2100, they are listed here.

Data Usage

The Data Usage screen displays your current data usage. You can also reset the data counter and cycle start date, and select the desired data usage monthly limit. Alerts will be generated to warn you that data usage is approaching or has reached the alert level specified on this page.



Data Usage Settings

Reset

You can use the **Reset Data Counter** button to restart the data counter and set the last reset date to today's date.

Usage Counter Monthly Limit

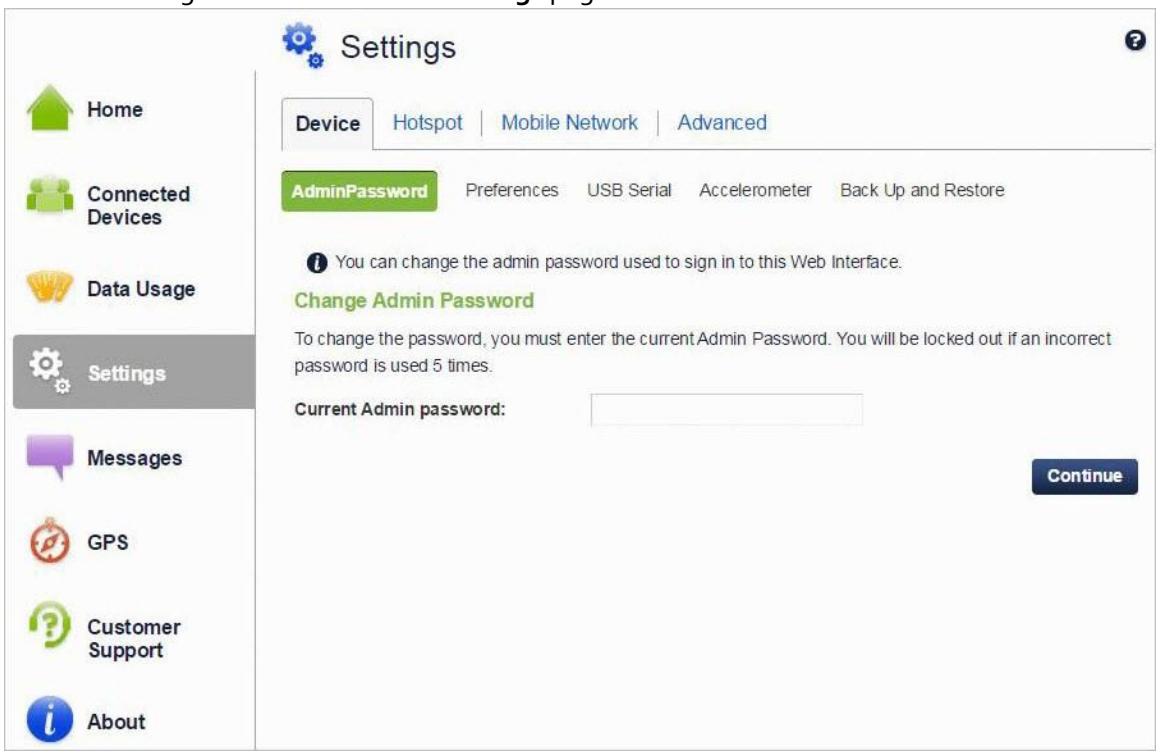
Select the desired option. If the desired option is not available, select 'None'. In this case, data usage will be recorded and displayed, but cannot be compared to a monthly limit.

Cycle Start Date

Select the day of the month when you wish the data counter to reset to zero.

Settings

The SA 2100 settings are located on the **Settings** page.



There are four settings tabs:

- Device Settings
- Hotspot Settings
- Mobile Network Settings
- Advanced Settings

Device Settings

By default, when the Settings Icon is selected, the Settings page opens and displays the Device tab.

The Device tab contains 5 menu options:

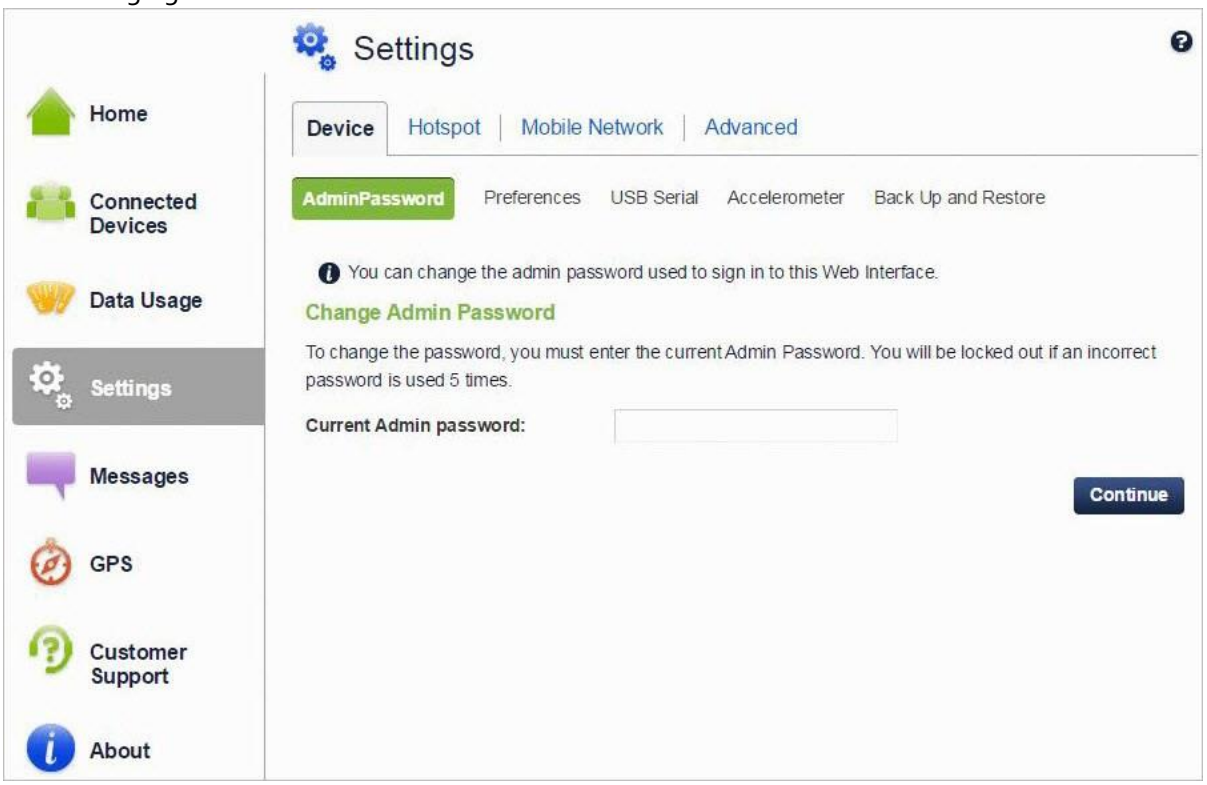
- Admin Password
- Preferences
- USB Serial
- Accelerometer

- Back Up and Restore

By default, the Admin Password option is displayed. The following paragraphs describe each of the five menu options available from the Device Settings page.

Settings | Device | Admin Password

The following figure shows the Admin Password screen.



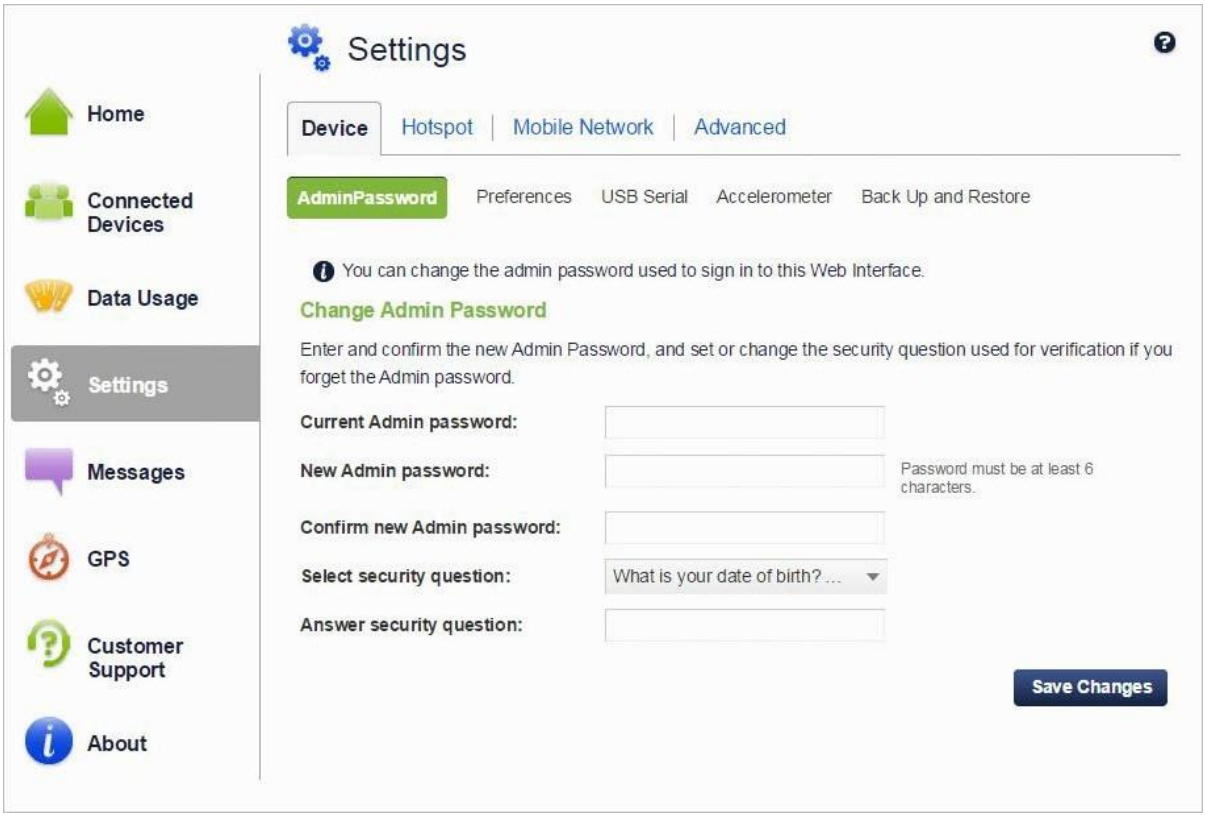
The Admin Password is used to sign in to this Web-based management interface. This page allows you to change the Admin Password.

To change the Admin password:

1. Enter the current Admin Password ("admin" by default) and click the **Continue** button.

   NOTE: If you enter an incorrect Admin Password too many times, you will be locked out of this Web Interface.

   The change Admin Password screen will appear as shown in the following figure.



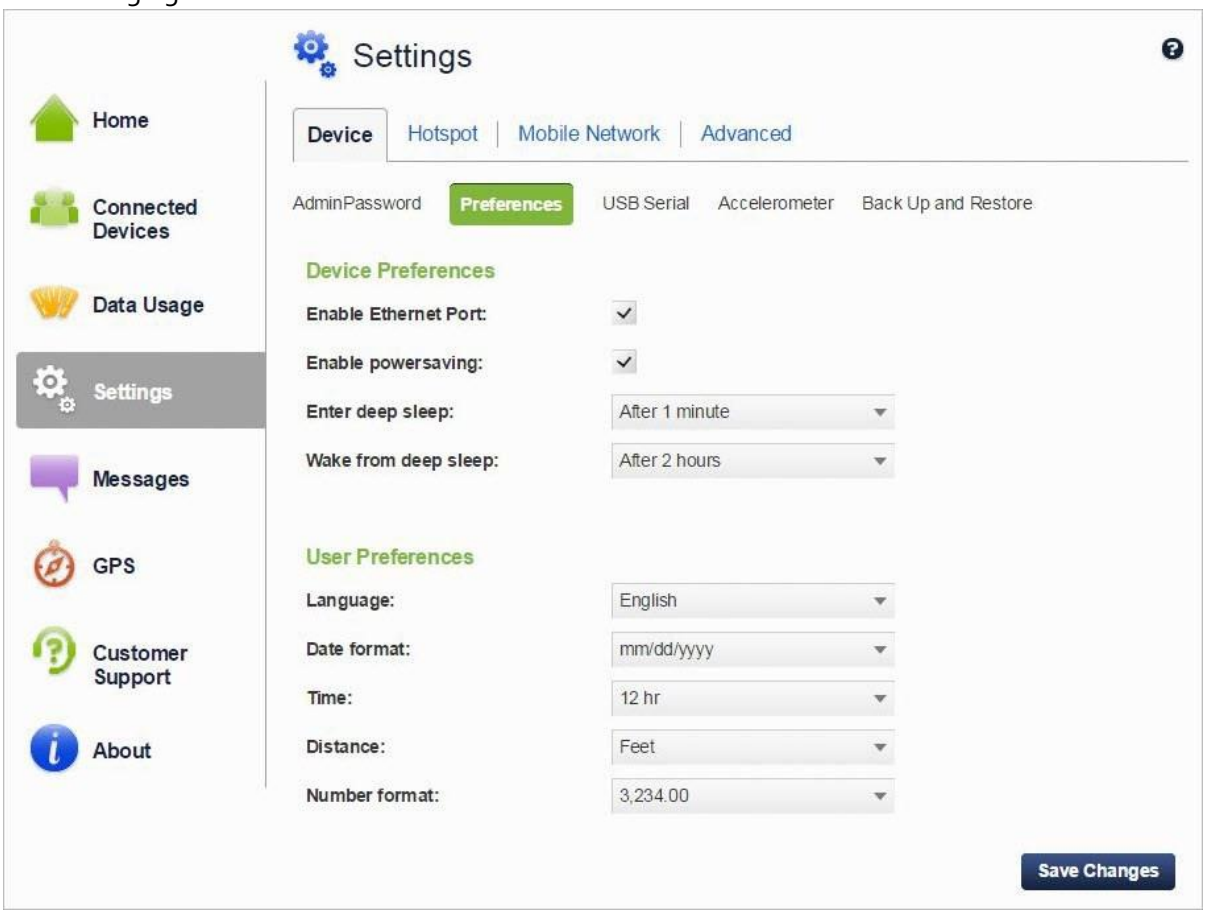
2. Enter the new password, using only letters, numbers, and standard punctuation symbols. The password must be at least 6 characters long.
3. Confirm the new Admin Password by re-entering the new password in the Confirm new Admin password field.
4. Select a security question.

   The security question is used if the Admin Password is lost, and the "I forgot the Admin Password" option is used.
5. On the Answer security question field, type in your answer.

   NOTE: The answers are case-sensitive.
6. Click **Save Changes**.

Settings | Device | Preferences

The following figure shows the Device Preferences screen.



Device Preferences

Enable Ethernet Port

Use this option to enable or disable the Ethernet port as needed.

Enable powersaving

This option should be enabled if the SA 2100 uses its own internal battery, or if you are concerned that the external battery connected to the SA 2100 could become fully discharged due to the SA 2100.

NOTE: The following Deep Sleep settings are only applicable if powersaving is enabled.

* Enter deep sleep

Unless set to "Never", the SA 2100 enters sleep mode after a period of inactivity. While in sleep mode, the SA 2100 will be unresponsive, and will neither generate nor accept network traffic. However, the following "Wake from deep sleep" setting can be used to periodically wake up the SA 2100 and resume normal operation.

If powersaving is disabled, this setting is unavailable. If powersaving is enabled, select the desired time period to enter sleep mode. Select "Never" if you do not want the SA 2100 to enter sleep mode.

* Wake from deep sleep

The setting determines when the SA 2100 will periodically wake up from sleep mode. Once awake, the SA 2100 will resume normal operation. The "Enter deep sleep" setting above will determine when sleep mode is resumed.

Select the desired time interval to wake from sleep mode.

User Preferences

Language

Select the desired language option.

Date Format

Specify the format in which the date is displayed on this Web-based interface.

Time

Specify the format in which the time is displayed on this Web-based interface.

Distance

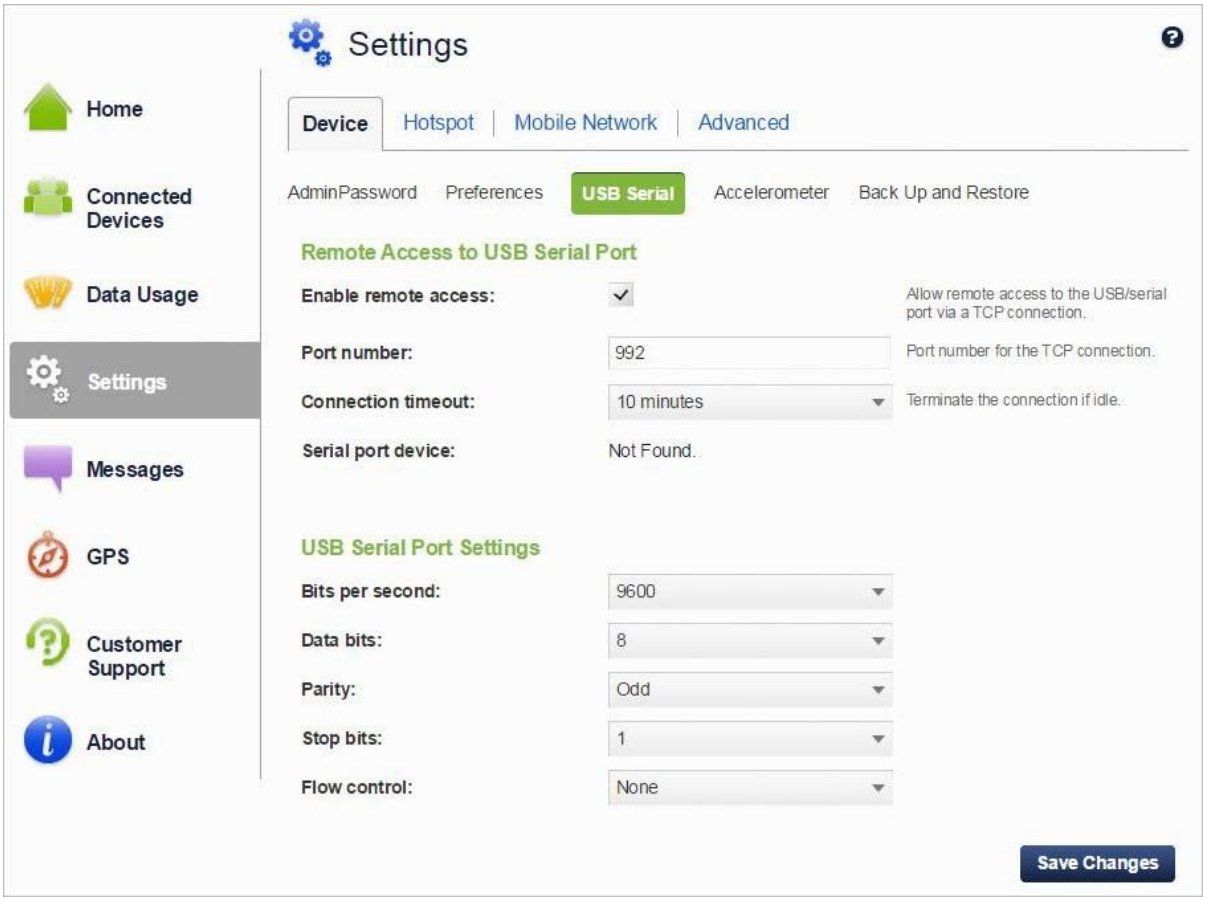
Select the option used for the GPS altitude and accuracy.

Number Format

Specify how decimal numbers are displayed. Period (.) or Comma (,) can be selected for use as the decimal point.

Settings | Device | USB Serial

The following figure shows the USB Serial Devices screen.



This feature is only useful if you have connected a USB/serial port adapter and a serial port device to the SA 2100. Once this is done, you can use the USB Serial feature to remotely access the serial port device.

Remote Access to USB Serial Port

Enable remote access

Use this option to enable or disable remote access as needed. If enabled, the SA 2100 will allow a TCP connection to the specified port. Telnet or a similar application can be used to establish this connection.

Port Number

Enter the port number to be used for the USB Serial Port connection to the SA 2100.

Connection Timeout

This option will terminate the connection if idle for the specified period. If you do not want the connection to be terminated by the SA 2100, select "Never".

Serial Port Device

If a serial port device is currently connected and recognized, details of the device are displayed here. Note that only 1 USB serial port device is available for remote access.

USB Serial Port Settings

These are standard serial port settings, and should be set to match the connected serial device.

Bits per second

Select the desired option. Supported speeds range from 300 bps to 115200 bps.

Data Bits

Select 7 or 8 to match your serial device.

Parity

The available options are Odd, Even, and None. Select the option to match your serial device.

Stop Bits

Select 1 or 2, as used by your serial device.

Flow Control

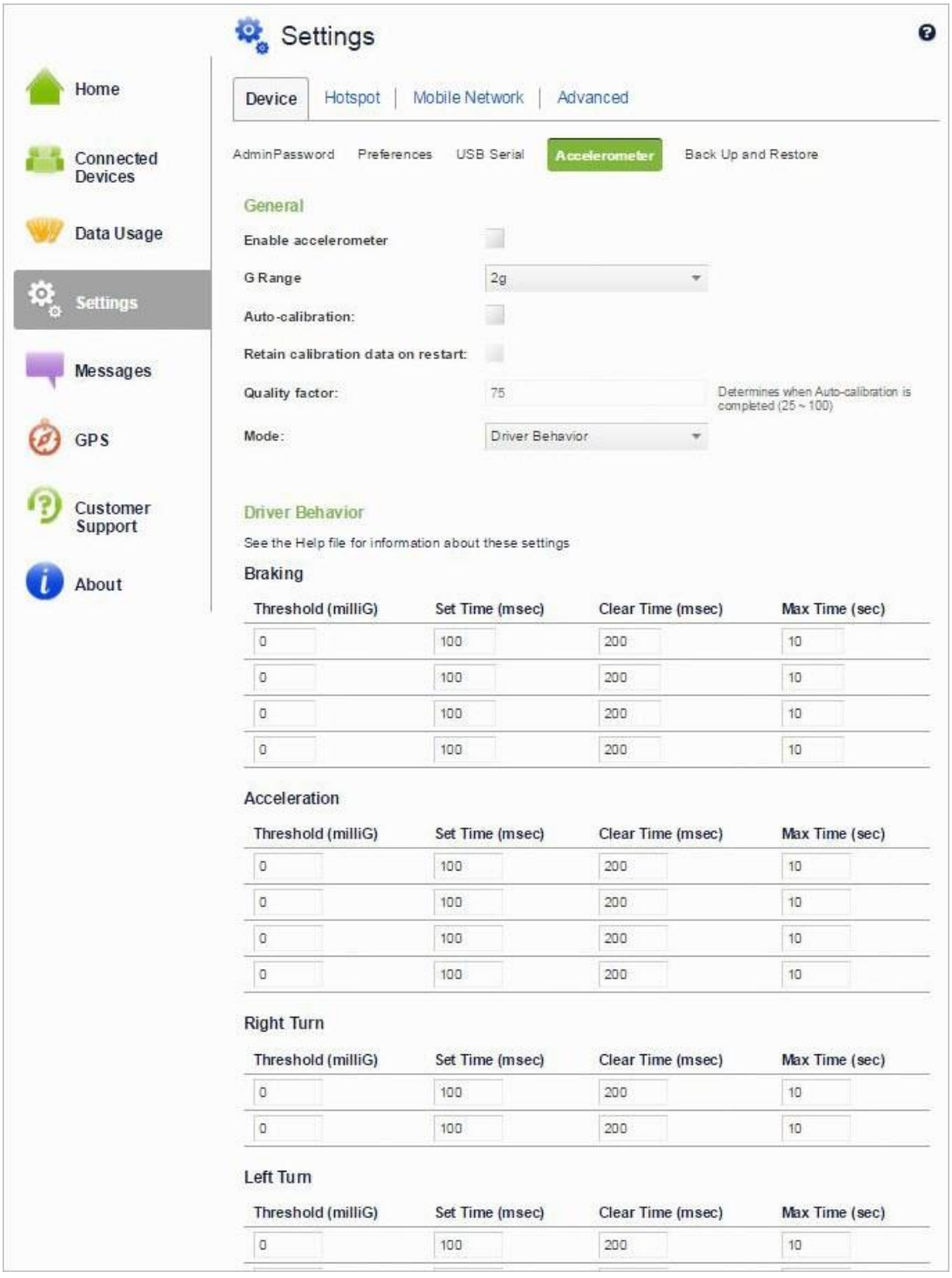
The available options are None, XON/XOFF, and Hardware. Select the option used by your serial device.

Settings | Device | Accelerometer

The accelerometer settings screen displays different options depending on the mode selected. The two mode options are driver behavior and motion detection. These settings are used by the Smart Agent software installed in the SA 2100 to generate events which are then passed to the Inseego Corporation server. The settings on this page determine which movements trigger Accelerometer events. Reports of these events are available on the Inseego Corporation server.

Driver Behavior

The following figure shows the Accelerometer settings screen when the mode is set to Driver Behavior.



Enable Accelerometer

Use this to turn the built-in Accelerometer On or Off as needed.

G Range

This is the maximum G value which can be recorded accurately. The wider the range, the less accurate the readings will be. The default is 2g, which is more than sufficient for normal vehicles. Any value above 2g must be a crash.

Auto-Calibration

Enable this to have the Accelerometer perform auto-calibration when the SA 2100 is powered up. Normally this is necessary and should be enabled.

Retain calibration data on restart

If enabled, the Accelerometer will be able to perform auto-calibration faster. This setting can be turned on if the SA 2100 is in a fixed location in a particular vehicle. Otherwise, it should be turned off.

Quality factor

This is similar to a % confidence level for auto-calibration. If set to 75, then auto-calibration is considered complete when the device calculates that there is a 75% probability that it is correct. Values below 25% are not allowed because the results would be unreliable.

Mode

When Driver Behavior is selected, this option is intended for the situation where the SA 2100 is installed in a vehicle, and you wish to monitor vehicle operation. Events are generated and recorded for exceptional (above threshold) changes in motion of the vehicle while it is being used. You can set different thresholds and parameters for changes in different directions (braking, acceleration, left turn, right turn, vertical) plus the "Magnitude", which is a change in any direction. When the threshold is exceeded for a period greater than the "Set Time", an event is triggered.

NOTE: Auto-calibration is necessary for the SA 2100 to determine which direction is "forward" so that acceleration/braking and left/right changes can be measured correctly.

Braking, Acceleration, Left Turn, Right Turn, Vertical, Magnitude

These groups of settings allow you to specify different values to trigger events for changes in different directions.

The settings are explained below. You can specify 4 thresholds for Braking and Acceleration, 2 thresholds for Right Turn, Left Turn, and Vertical, and 1 threshold for Magnitude. Magnitude refers to a change in motion in any direction.

NOTE: A single change may trigger multiple events. For example, if the Braking thresholds are set to 100, 200, 300, and 400, then a 500 milliG motion would trigger all 4 events.

Threshold

This value is the G force - measured in milliG (1000th of G force) to allow precise definition - which will trigger a motion change event. When multiple thresholds are available, it is normal practice to have a series of thresholds at different levels.

Set Time

When the threshold above is exceeded, it must remain above the threshold value for the period specified by the corresponding Set Time (specified in milliseconds) in order to trigger an event. If the measured time period above the threshold is less than Set Time, the event is not triggered.

Clear Time

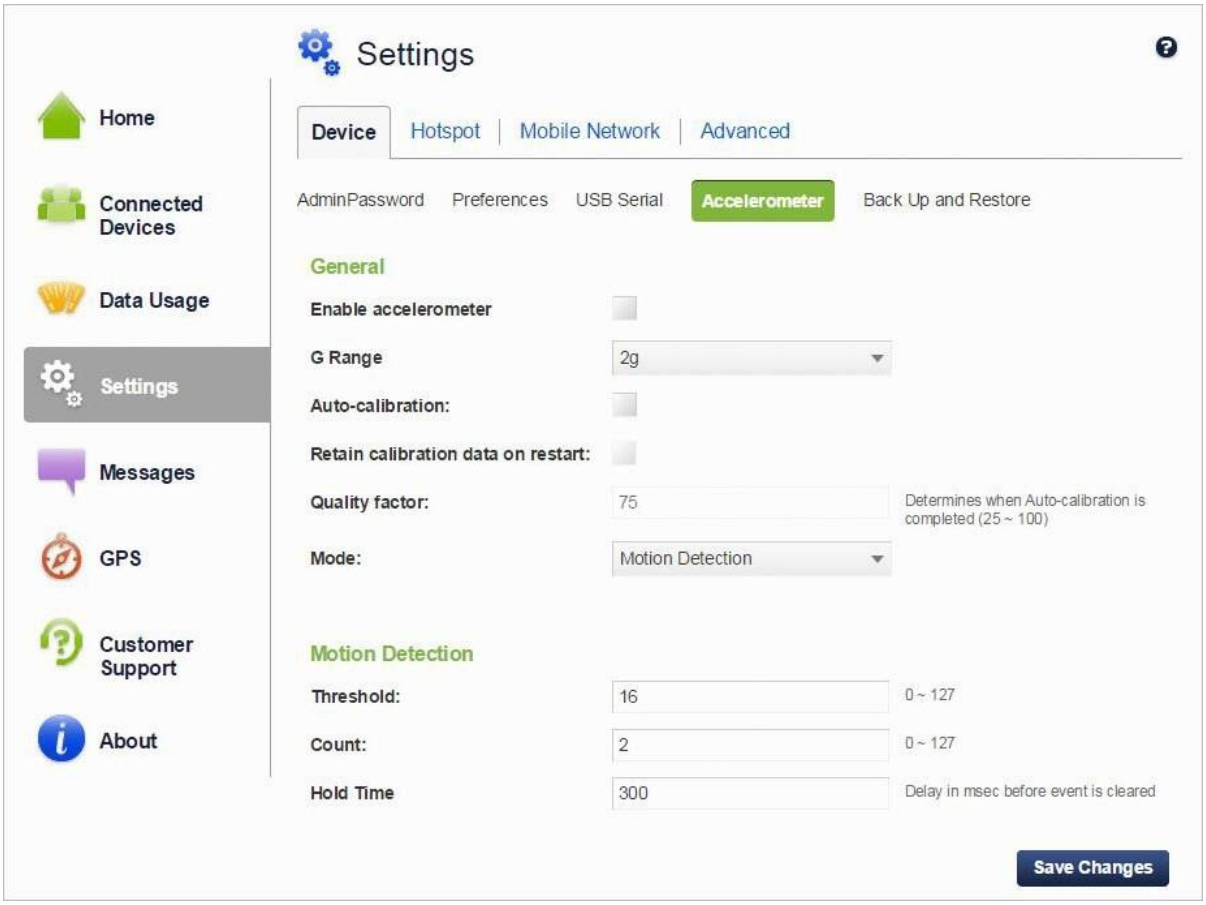
This is the delay, in milliseconds, before an event is cleared. Once an event is triggered, it will last until the "Max Time" (below) is reached, or a time interval equal to Clear Time has elapsed without any readings above the threshold. A new event cannot be triggered until the previous event has been cleared.

Max Time

This setting, measured in seconds, determines how long a single event can last. If the above-threshold reading persists after this time period has elapsed, a new event will be triggered.

Motion Detection

The following figure shows the Accelerometer settings screen when the mode is set to Motion Detection.



Enable Accelerometer

Use this to turn the built-in Accelerometer On or Off as needed.

G Range

This is the maximum G value which can be recorded accurately. The wider the range, the less accurate the readings will be. The default is 2g, which is more than sufficient for normal vehicles. Any value above 2g must be a crash.

Auto-Calibration

Enable this to have the Accelerometer perform auto-calibration when the SA 2100 is powered up. Normally this is necessary and should be enabled.

Retain calibration data on restart

If enabled, the Accelerometer will be able to perform auto-calibration faster. This setting can be turned on if the SA 2100 is in a fixed location in a particular vehicle. Otherwise, it should be turned off.

Quality factor

This is similar to a % confidence level for auto-calibration. If set to 75, then auto-calibration is considered complete when the device calculates that there is a 75% probability that it is correct. Values below 25% are not allowed because the results would be unreliable.

Mode

When Motion Detection is selected, this option generates events when the device is moved, regardless of the direction of the motion. This is normally used when the SA 2100 is installed in machinery or a vehicle which should not move, and you wish to be alerted if it does move.

Threshold

This value is the G force which will trigger a motion event. The following settings — Count and Hold Time — are used to ensure that the motion event is genuine, rather than spurious.

Count

This refers to the number of consecutive samples above the threshold which are needed to trigger a motion event. For example, if count is 100, and there are 98 consecutive samples above the threshold, then 1 sample below the threshold, the count would be reset to 0, and no motion event is triggered. Note that the sampling rate is 10 Hz (10 samples per second) so the "Count" may be converted to a time interval (in seconds) by dividing the count by 10.

Hold Time

This is the delay, in seconds, before a motion event is cleared. This setting has two effects:

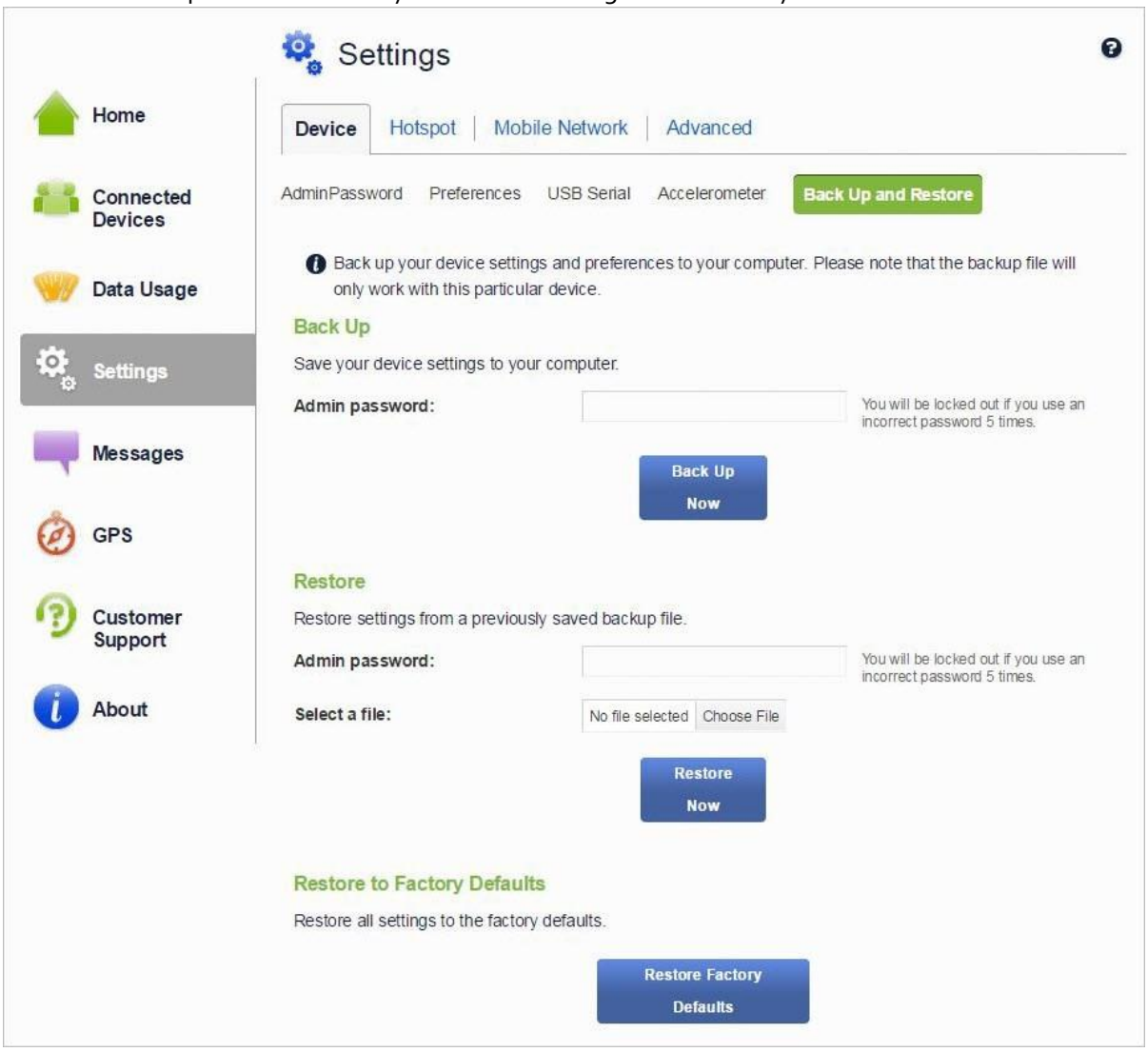
- The Accelerometer will wait for this time interval to determine if the event is finished. If additional readings above the threshold are received during the Hold Time interval, they are considered to be part of the same event, and the "Hold Time" timer will be restarted. When no additional readings above the threshold are received for a period equal to the Hold Time, the event is considered to be finished.
- Because of the delay to clear an event once it has started, this setting will also limit the number of motion events which can be generated within a given time period. However, this is unlikely to have much effect in practice.

Settings | Device | Backup and Restore

The following figure shows the Backup and Restore screen. Use this feature to back up (download) a copy of the configuration settings from this device to a file on your computer, or restore (upload) a previously-saved configuration file. This configuration file contains all settings for the device, router and system

functions. It does not contain any settings or data for the 4G modem. Note that you can only restore a file to the same device it came from.

This screen also provides the ability to reset all settings to the factory default values.



Backup

Admin Password

Enter the current password in this field.

Back Up Now

Click this button to download a copy of the current configuration file to your computer. If your browser prompts you to save the file, you can rename it if desired.

Restore

Admin Password

Enter the current password in this field.

Select a file

Select the configuration file you previously downloaded from this SA 2100 device to your computer.

Restore Now

After selecting a configuration file, click this button to begin the file upload. After uploading, the configuration file is immediately applied, and this device restarted.

NOTE: Uploading a configuration file changes ALL of the existing settings to match the configuration file. This may change the current Wi-Fi settings, breaking all existing connections to this SA 2100, including this web browser session.

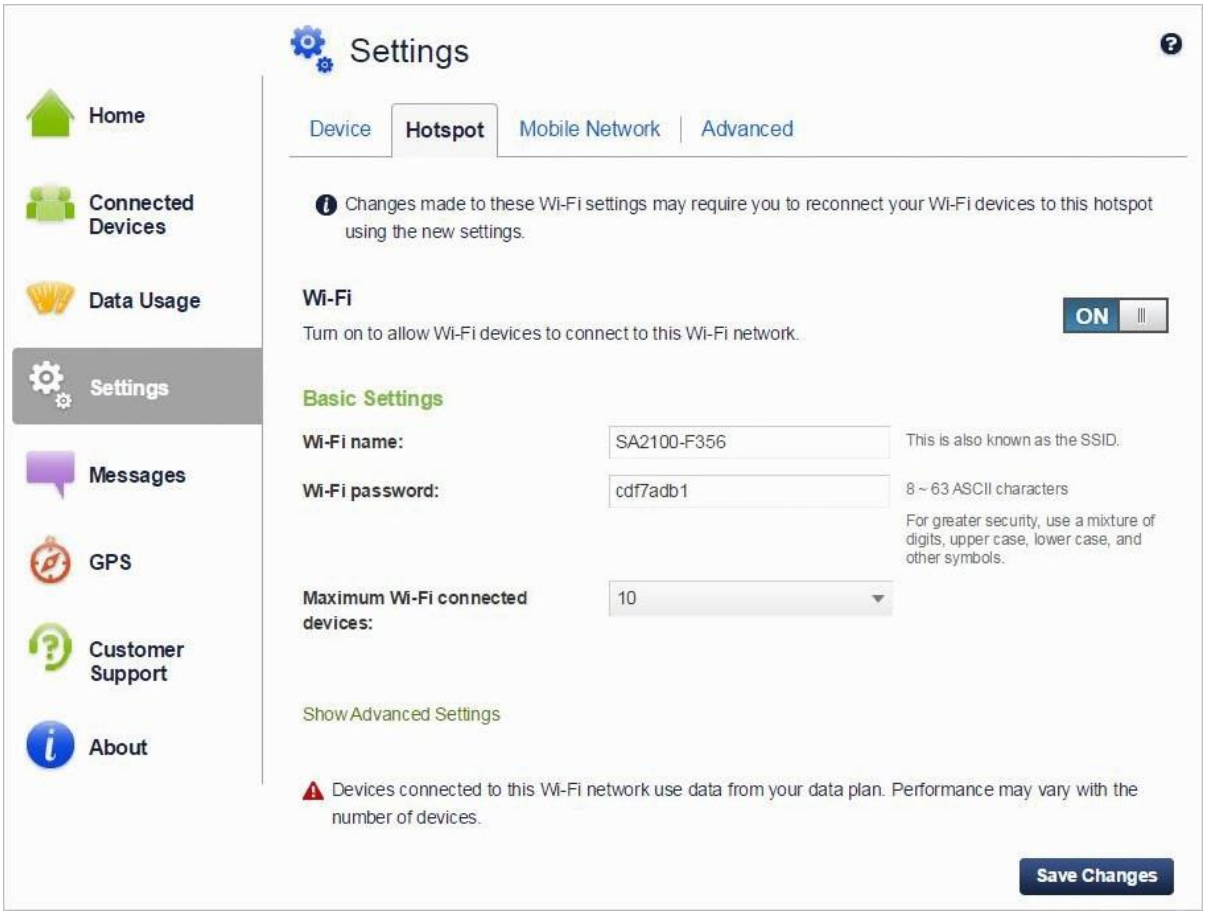
Restore to Factory Defaults

Click the Restore Factory Defaults button to reset all settings to their factory default values. This causes a restart, and may change the current Wi-Fi settings, breaking all existing connections to this device, including this web browser session.

Hotspot Settings

By default, when the Settings Icon is selected, the Settings page opens and displays the Device tab. To display the Hotspot Settings page, click the **Hotspot** tab.

The following figure shows the Hotspot Settings page.



All Wi-Fi connected devices must use these Wi-Fi settings in order to connect to the SA 2100's Wi-Fi network. If you change these settings, existing connected devices may lose their Wi-Fi connection.

Wi-Fi On/Off

Use this control to turn the Wi-Fi network on or off as needed. When off, network devices must use the Ethernet or USB connection.

Basic Settings

Wi-Fi Name

This sets the network name or SSID for the Wi-Fi network created by this device. Enter a suitable name. The name can be up to 32 characters long.

Wi-Fi Password

If a setting other than Open was selected in the Security field, a Wi-Fi password is required. Enter the WiFi Password in this field. An on-page hint indicates the password requirements for the current security option.

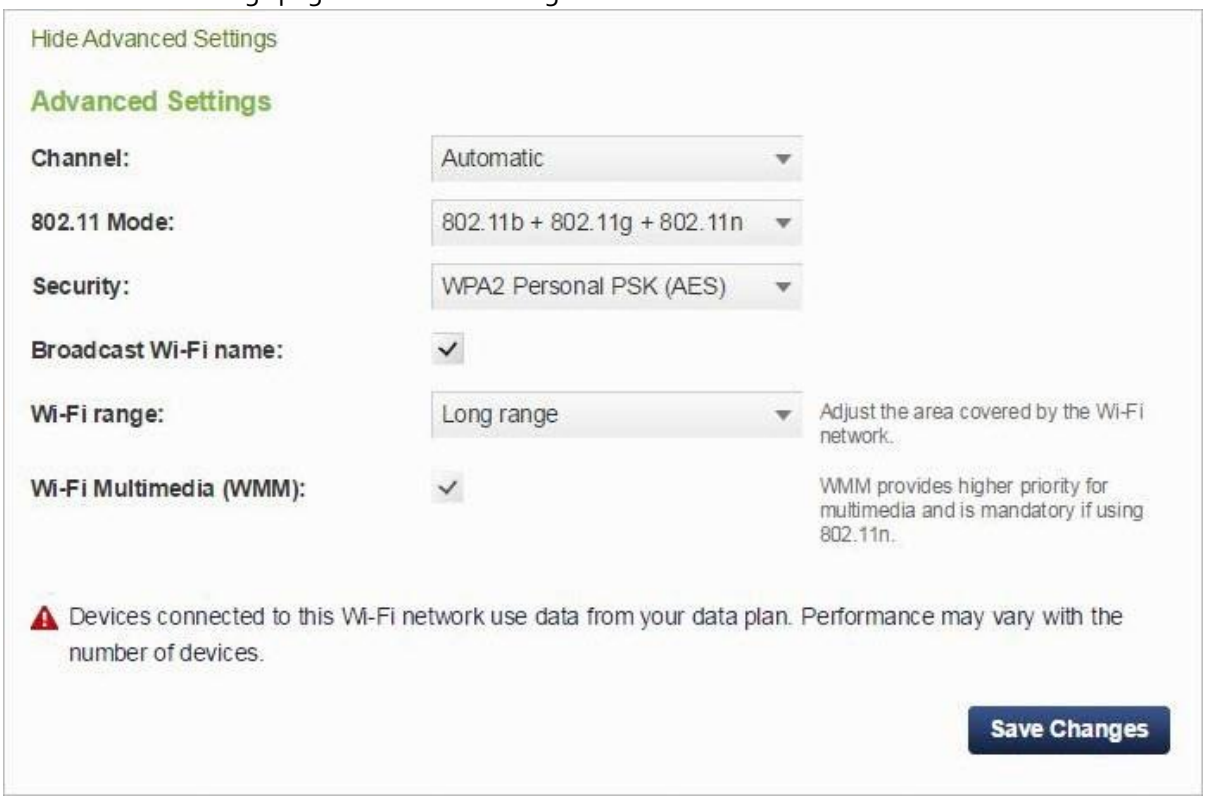
Maximum Wi-Fi Connected Devices

Specify how many devices can simultaneously connect to this SA 2100.

Advanced Settings

Click the **Show Advanced Settings** link to display the advanced settings.

The advanced settings page is shown in the figure below.



Channel

This should be left on Automatic unless you need to choose a particular channel for your environment.

802.11 Mode

Use this setting to change the Wi-Fi mode, if required. If all of your connected devices support 802.11n, selecting the option "802.11n only" will provide the best performance. In other cases, it is recommended that you leave this setting at its default value.

Security

Select the desired option for Wi-Fi security. WPA2 is the latest and most secure method, and should be used if possible. None allows other people to monitor your Wi-Fi traffic and use your data plan to access the Internet.

CAUTION! If at all possible, using None should be avoided. Using WPA2 is strongly recommended, as this is the most secure method supported.

Broadcast Wi-Fi Name

If this setting is enabled, this Wi-Fi network appears in the list of available Wi-Fi networks on your connected devices. If disabled, this network will be invisible.

Wi-Fi Range

Use this option to determine the strength of the Wi-Fi signal, and hence the size of the Wi-Fi network. If running on the battery, the longer range or higher power option will deplete the battery more quickly.

Wi-Fi Multimedia (WMM)

This setting should normally be enabled to assist throughput. If using 802.11n, it must be enabled.

Mobile Network Settings

By default, when the Settings Icon is selected, the Settings page opens and displays the Device tab. To display the Mobile Network page, click the **Mobile Network** tab.

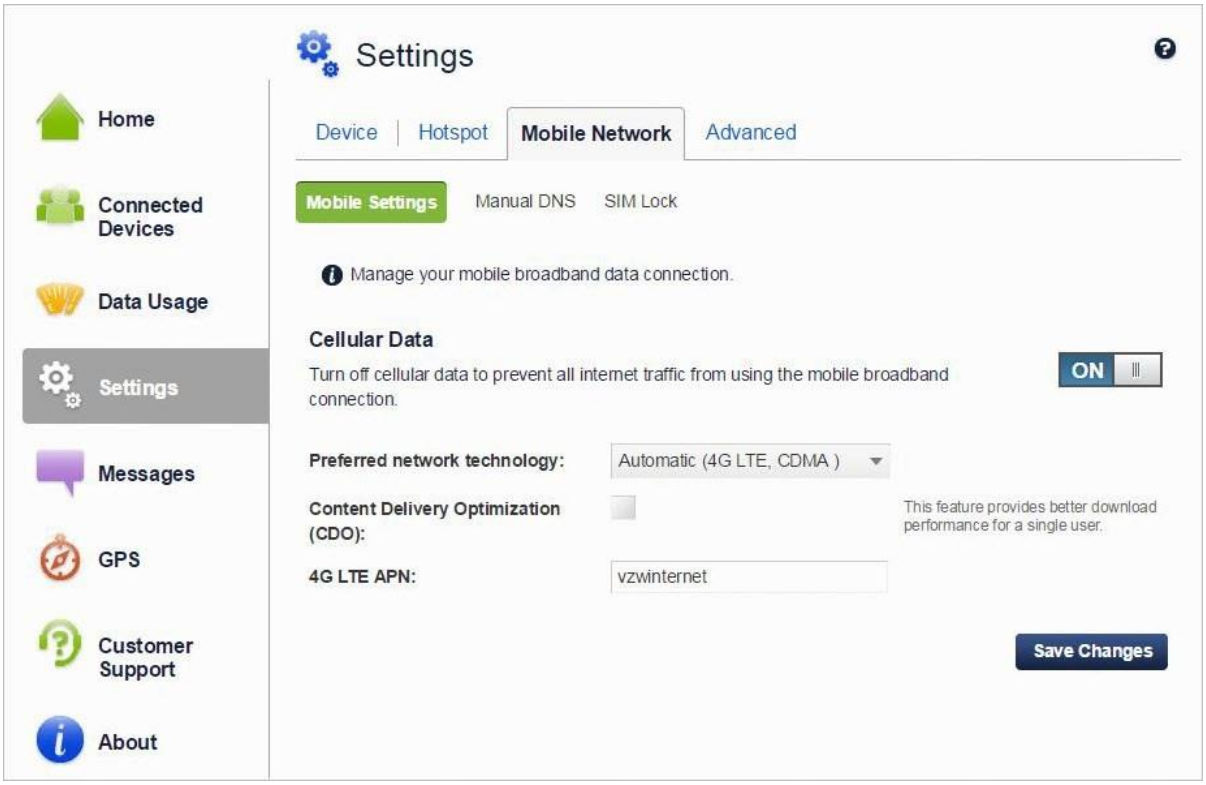
The Mobile Network tab contains 3 menu options:

- Mobile Settings
- Manual DNS
- SIM Lock

By default, the Mobile Settings option is displayed. The following paragraphs describe each of the three menu options available from the Mobile Network page.

Settings | Mobile Network| Mobile Settings

The following figure shows the Mobile Settings screen. These settings affect the connection to the mobile network.



Cellular Data

You can use this setting when necessary to turn off cellular data and prevent access to the mobile network. This prevents connected devices from connecting to the Internet and using your mobile data plan. For normal operation, this setting must be left on.

Preferred Network Technology

The default value is "Automatic". The SA 2100 device will select the best available technology. If desired, you can change this to limit the network technologies which will be used.

Content Delivery Optimization (CDO)

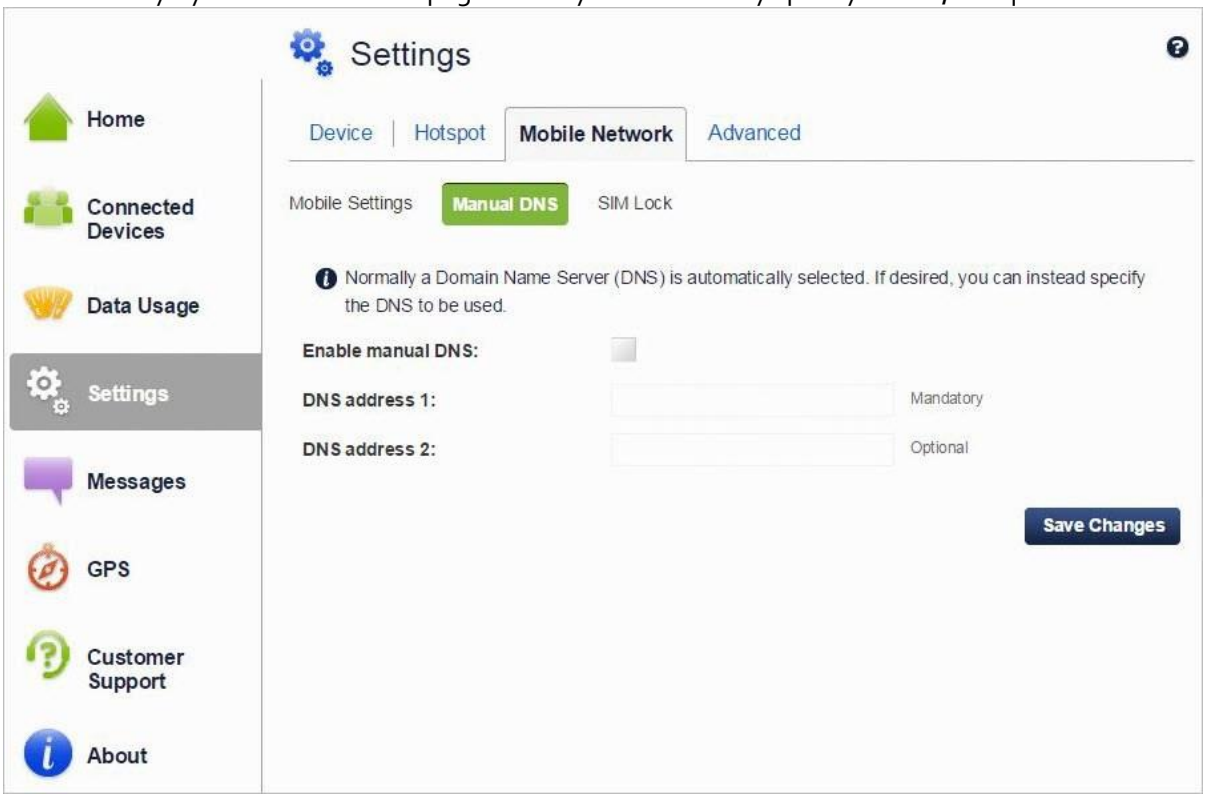
This feature provides better download performance, but can only assist one connected device at any time. Normally, this feature should be enabled.

4G LTE APN

This APN is pre-configured to access the Verizon Wireless network. You should not change the APN unless you have a corporate account (with your own APN) or you change the SIM.

Settings | Mobile Network| Manual DNS

The following figure shows the Manual DNS screen. Normally, the DNS address is provided automatically by the network. This page allows you to manually specify a DNS, if required.



Enable Manual DNS

Use this setting to enable or disable the Manual DNS feature. If enabled, provide the following data.

DNS a ddress 1

Enter the IP address of the desired primary DNS. This address is required if the Manual DNS feature is enabled.

DNS address 2

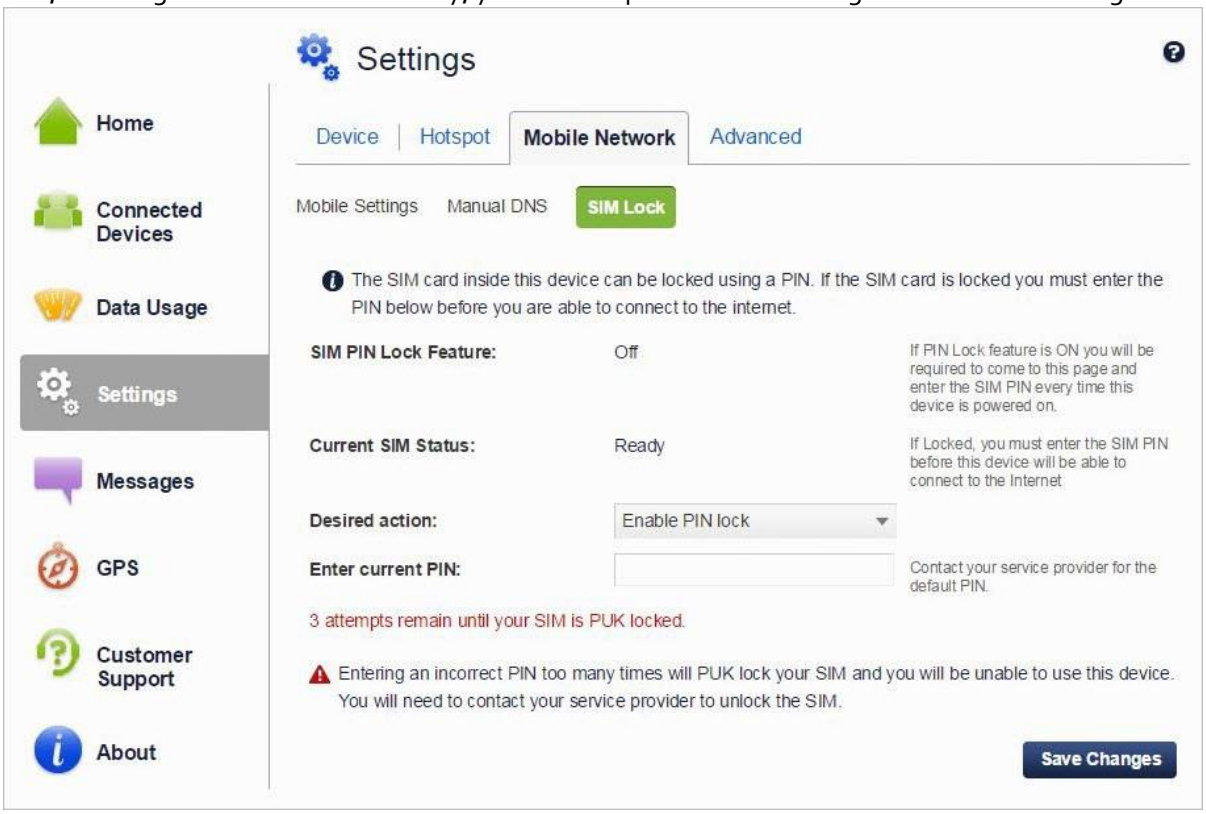
Enter the IP address of the desired secondary (backup) DNS. This address is optional and may be left blank if desired.

Settings | Mobile Network| SIM Lock

The following figure shows the SIM Lock screen.

The SIM card inside your SA 2100 device can be locked using a PIN. If the SIM card is locked, you must enter the PIN before connecting to the mobile network. Once entered, the PIN is remembered until the next shutdown.

In addition to enabling you to enter the SIM PIN when needed, this page also allows you to unlock your SIM, or change the SIM PIN. Generally, you need to provide the existing PIN in order to change the SIM.



SIM PIN Lock feature

The field indicates whether or not the PIN lock feature is in use. If "On", the PIN lock has been turned on, and the SIM PIN must be entered in order to connect to the mobile network. If "Off", the PIN lock feature is not turned on, and the SIM PIN is not required.

Current SIM status

The field indicates the current status of the SIM card. Possible values are:

- Ready - this is the normal state. The SIM PIN is not used.
- PIN Locked - the SIM PIN must be entered before you can use the mobile network.
- PUK Locked - the PUK for the SIM must be entered in order to continue. The PUK can be obtained from your service provider.
- Unlocked - the SIM PIN is needed, but has already been entered.
- No SIM - no SIM was detected. If you do have a SIM, check that it is inserted correctly.
- Invalid SIM - a SIM was detected, but it is not usable in this device.

- SIM Error - a SIM was detected, but it did not respond as expected, and cannot be used.

Desired Action

The actions available depend on the current SIM status. If multiple operations are possible, a "Desired action" select list is visible. Use this to choose the desired operation.

PIN Lock

WARNING! If the SIM is currently PIN locked, you are prompted to enter the PIN. Note that if an incorrect PIN is entered too many times, the SIM becomes PUK locked. An on-page counter indicates how many incorrect entries will cause PUK lock. Once PUK locked, the PUK must then be obtained from your service provider.

PUK Lock

WARNING! If the SIM is currently PUK locked, the only operation possible is to enter the PUK. Note that if an incorrect PUK is entered too many times, the SIM becomes permanently unusable. An onpage counter indicates how many entry attempts remain.

Enable PIN Lock

This sets the SIM so that entry of a PIN is required upon startup to connect to the mobile network. To perform this operation, you must enter the current PIN.

Disable PIN Lock

You can use this setting to disable a previously enabled PIN lock. It reverses the PIN lock, so that entry of a PIN is no longer required to connect to the mobile network. To perform this operation, you must enter the current PIN.

Change PIN

To change the existing PIN, select this option and then enter the required data (For most SIMs, the new PIN must consist of 4 digits. The default value is often 0000 or 1111):

- Current PIN
- New PIN
- Confirm New PIN

Advanced Settings

By default, when the Settings Icon is selected, the Settings page opens and displays the Device tab.

To display the Advanced page, click the **Advanced** tab.

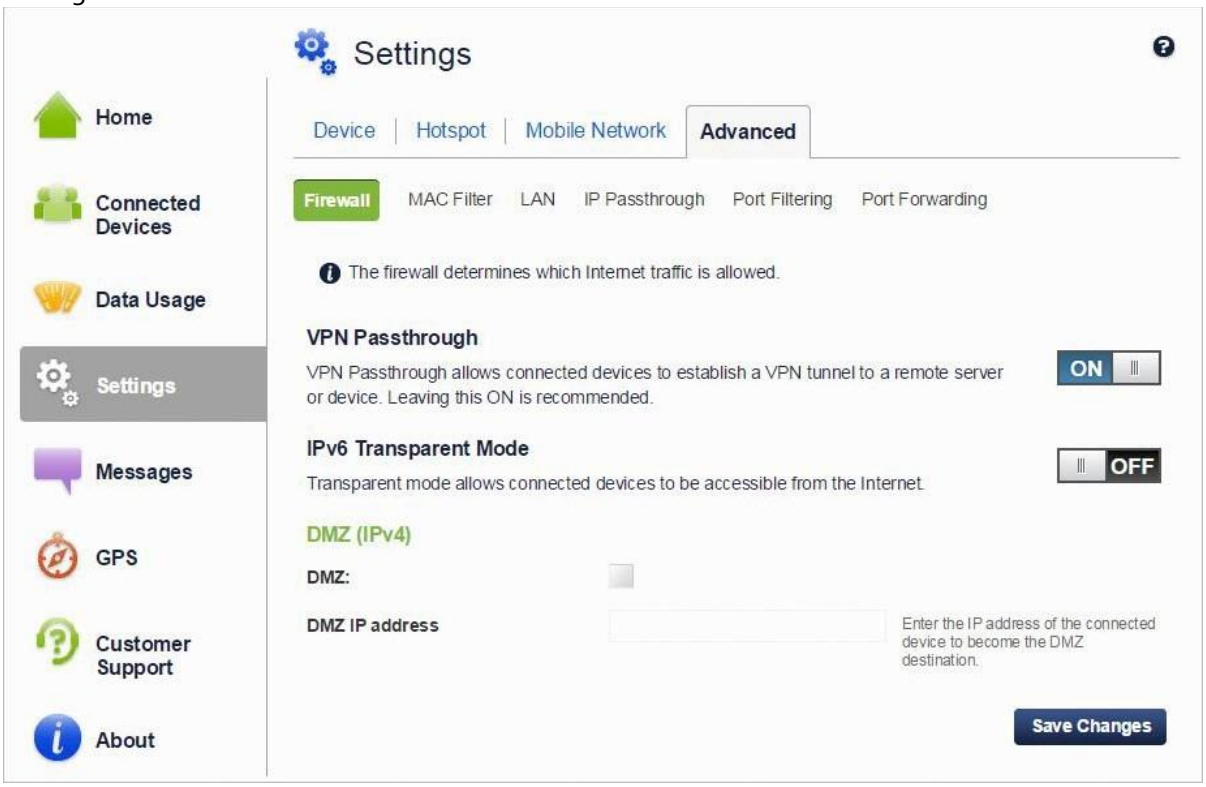
The Advanced tab contains six menu options:

- Firewall
- MAC Filter
- LAN
- IP Passthrough
- Port Filtering
- Port Forwarding

By default, the Firewall option is displayed. The following paragraphs describe each of the six menu options available from the Advanced page.

Settings | Advanced| Firewall

The following figure shows the Firewall Settings screen. A firewall helps protect your connected devices against malicious incoming traffic from the Internet. The firewall cannot be disabled, but the following settings are available.



VPN Passthrough

This feature allows VPN client software on connected devices to connect through this device to remote VPN servers. Normally, this option should be left enabled.

IPv6 Transparent Mode

If your device and service provider support IPv6, this option will be available.

Normally, the firewall will block incoming IPv6 connection requests intended for an IPv6-enabled connected device.

If you wish to allow these incoming connection requests to reach the intended connected device, enable this setting. Transparent Mode should only be enabled when necessary, as it reduces the protection provided by the firewall.

DMZ (IPv4)

If enabled, then the connected device specified as the DMZ IP address (DMZ destination) will receive all traffic which would otherwise be blocked by the firewall. This may assist some troublesome network applications to function properly, but the DMZ device should have its own firewall to protect itself against malicious traffic.

DMZ checkbox

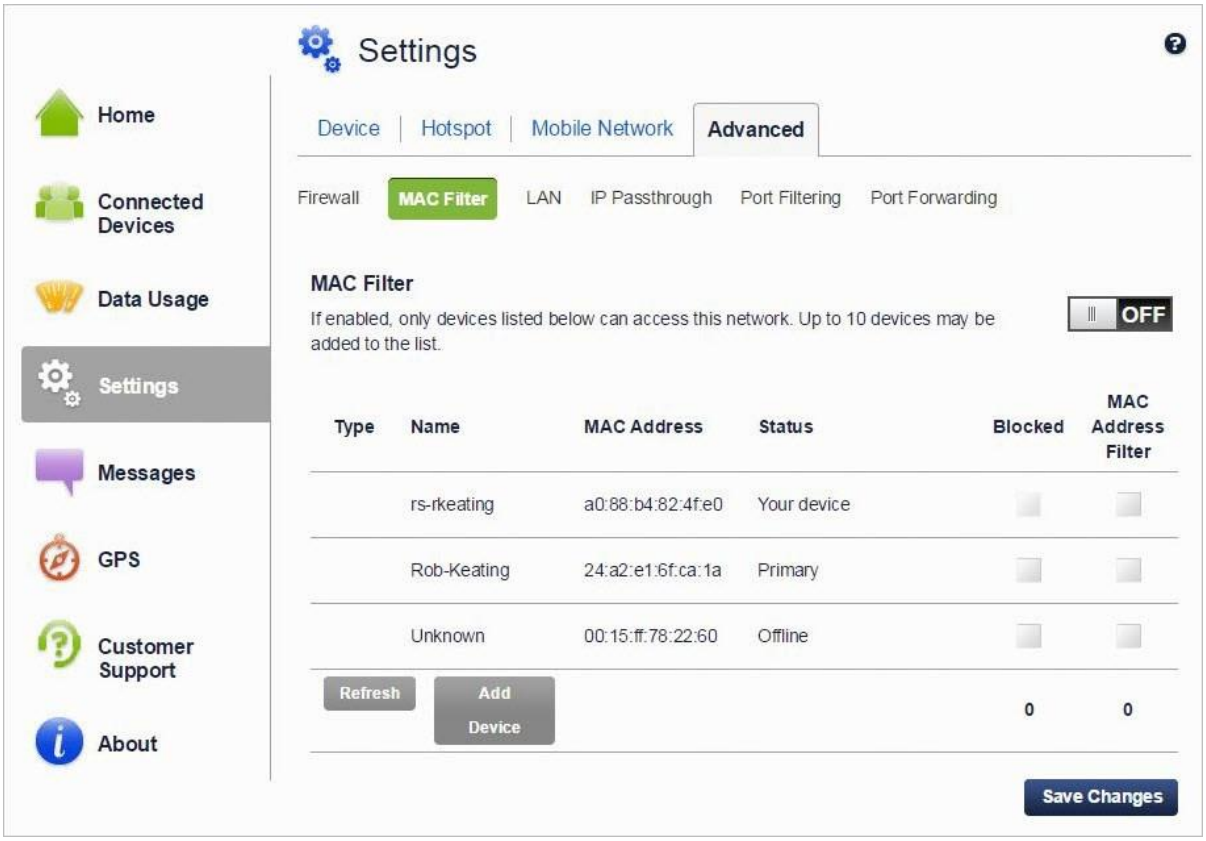
Use this to enable and disable this feature as needed. Generally, DMZ should be disabled unless really necessary.

DMZ IP Address

Enter the IP address of the connected device you wish to become the DMZ device (DMZ destination) into this field. You can check the IP address of each connected device on the connected devices screen.

Settings | Advanced| MAC Filter

The following figure shows the MAC Filter Settings screen. The MAC Filter feature, if turned on, will prevent access to this network by any device which is not included in the "MAC Address Filter" list. The filter applies to both the Wi-Fi and Ethernet interfaces, but has no effect on USB devices.



ON/OFF Control

Use this control to turn on or turn off the MAC Filter as needed. Before turning it on, you need to ensure that some devices are allowed. Note that when the MAC Filter is turned on, any Connected Device which is not in the "MAC Address Filter" list will immediately be disconnected.

Device List

All known devices are listed here. Use the provided checkboxes to include or exclude devices from the "Blocked" or "MAC Address Filter" lists.

Operation

Blocked versus MAC Filter

The interaction between the "Blocked" devices and the "MAC Filter" is:

- Blocked devices are always blocked, regardless of whether the MAC Filter is on or off.
- If the MAC Filter is on, and a device is in the Blocked list, but not in the MAC Address Filter list, then it will not be able to connect. Both the MAC Filter and the Block would prevent connection.

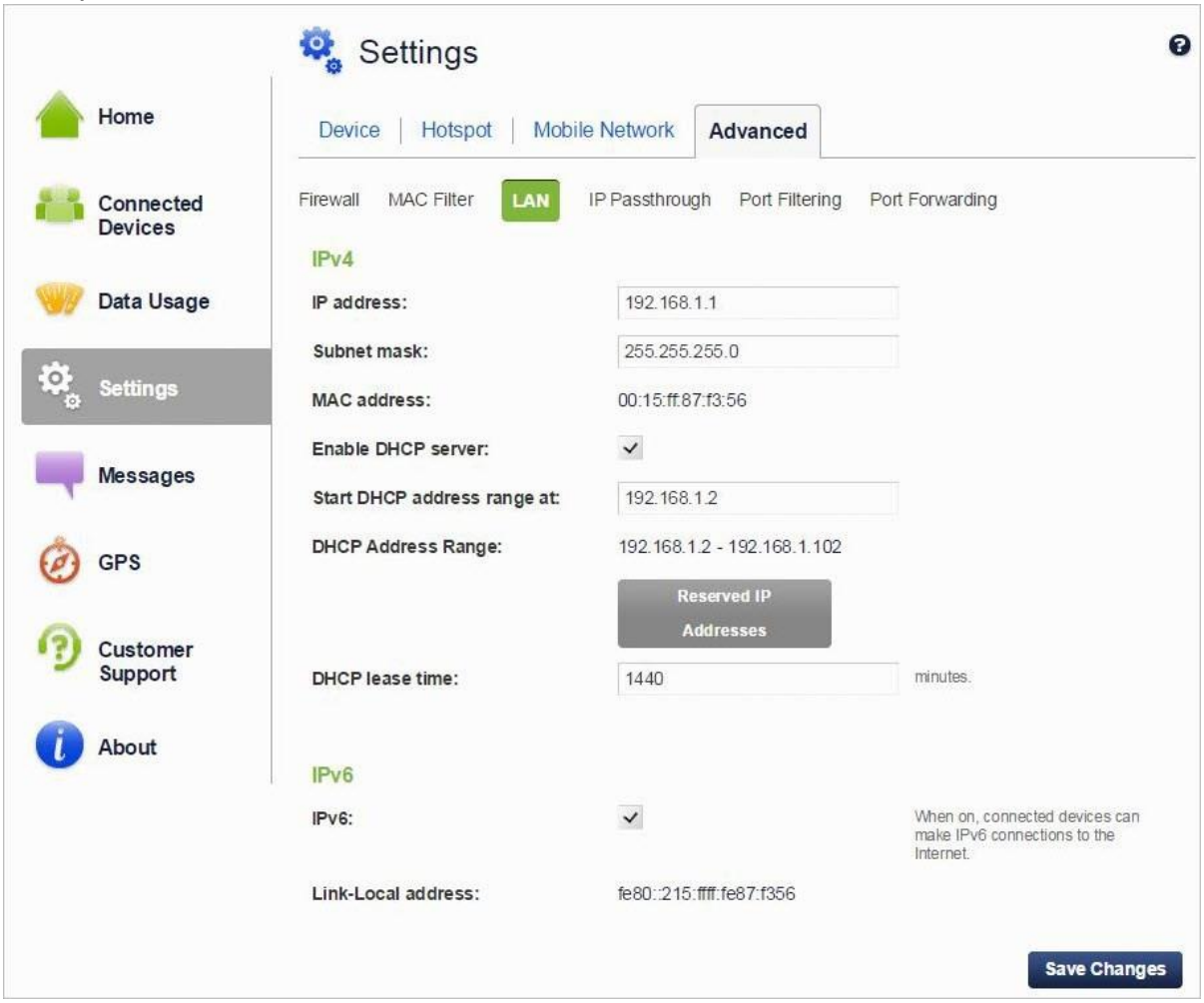
- If the MAC Filter is on, and a device is in the MAC Address Filter list, then the device will be able to connect. Having connected, it can then be blocked either by removing it from the MAC Address Filter list, or by using the "Block" feature. Generally, the "Block" should be used for temporary blocking, and the MAC Filter for permanent blocking.

Add Device

Use this button to add a new device to the devices list.

Settings | Advanced| LAN

The following figure shows the LAN Settings screen. These settings apply to your local network or LAN. For this device, the LAN consists of this device and all connected devices (including the USB connected device, if it exists).



IPv4

IP Address

The IP address for this device, as seen from the local network. Normally, you can use the default value.

Subnet Mask

The default value 255.255.255.0 is standard for small (class "C") networks. If you change the LAN IP Address, ensure you use the correct Subnet Mask.

MAC Address

The MAC address is a unique network identifier, assigned when a network device is manufactured. This read-only field displays the MAC Address associated with the IP address above.

DHCP Server

Normally, this should be left on. The DHCP server allocates an IP address to each connected device. If the DHCP Server was disabled, then each connected device would need to be assigned a fixed IP address.

Start DHCP Address Range at

If you wish to change the IP address range used by the DHCP server, you can do so by changing this value. This option is for expert users only.

DHCP Address Range

This indicates the range of IP addresses which may be allocated to connected devices. If using a fixed IP address on a connected device, you should use an IP address that is outside this range.

Reserved IP Addresses

This feature can be used to ensure that a connected device will always be allocated the same IP Address by the SA 2100. Click this button to access the setup screen for this feature.

DHCP Lease Time

This field determines how often connected devices must renew the IP address assigned to them by the DHCP server. Normally, this can be left at the default value, but if you have special requirements you can change this value.

IPv6

If your device and your service provider support IPv6, this section will be visible.

Enable IPv6

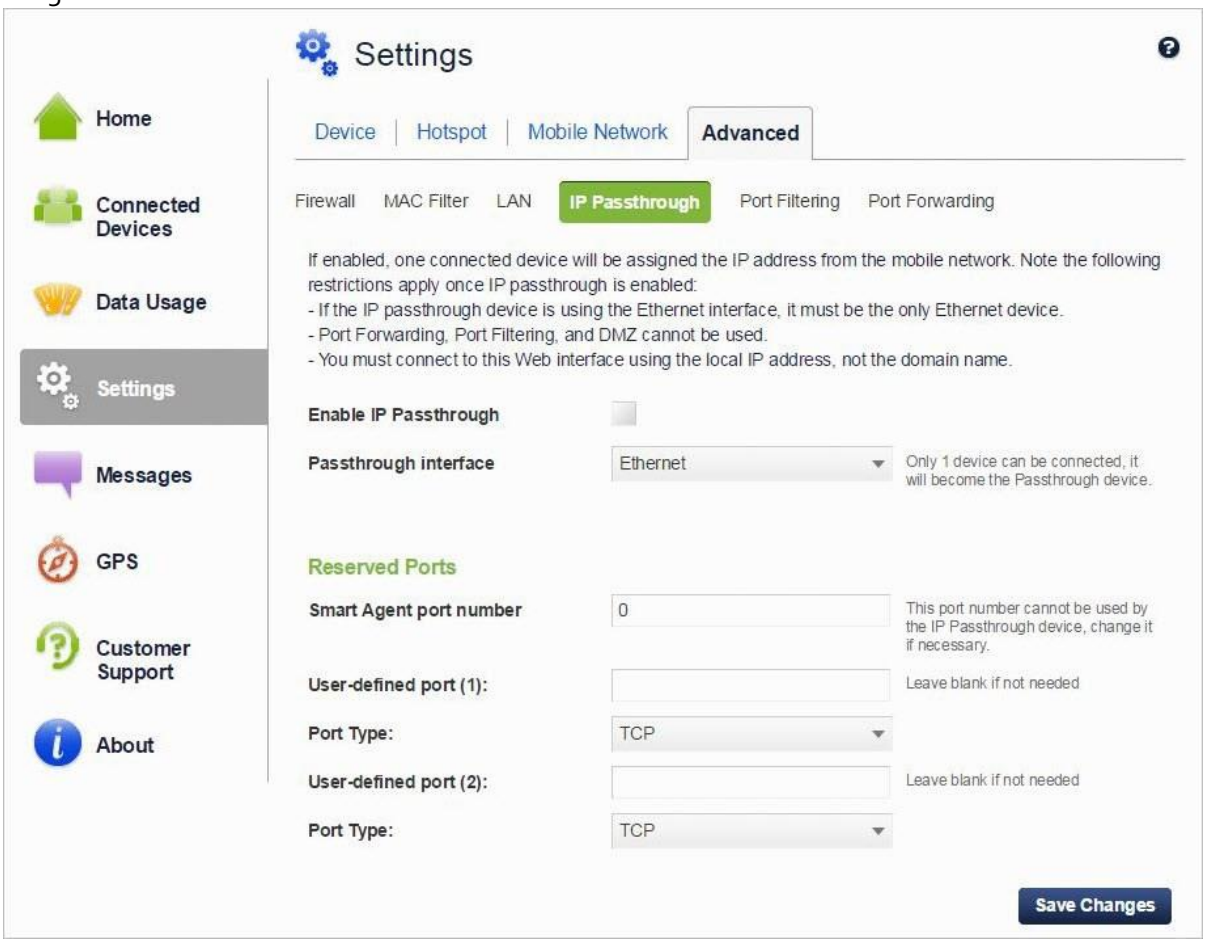
If some of your connected devices support IPv6, this setting should be enabled. IPv6-enabled connected devices will then be able to make IPv6 connections to the Internet.

Link-Local address

This is the IPv6 address of this device. The Link-Local address is used for IPv6 communication between devices on the same network, such as communication between the SA 2100 and its connected network devices.

Settings | Advanced| IP Passthrough

The following figure shows the IP Passthrough Settings screen. If used, the IP Passthrough features assigns the Internet IP address to one connected device.



Overview

The following limitations apply to IP Passthrough:

- The passthrough device must be the only device on the selected interface. Other devices on this interface will be ignored, and will not have Internet access.
- Devices on the other interface or interfaces function normally.
- When IP passthrough is enabled, the following features cannot be used:
  - Port Forwarding
  - Port Filtering

- DMZ

- Reserved ports cannot be used by the passthrough device. Traffic on these ports will not reach the IP Passthrough device. If the default port numbers conflict with traffic needed by the IP Passthrough device, then the reserved ports must be changed to prevent conflict.
- When IP Passthrough is enabled, the SA 2100 must restart. Normally, this means a new Internet IP address will be assigned to the SA 2100 after the restart.

Settings

Enable IP Passthrough

Use this to turn the IP Passthrough feature on or off as needed.

Passthrough Interface

Select the interface used by the network device you wish to become the IP Passthrough device. The IP Passthrough device must be the only connected device on this interface.

IP Address

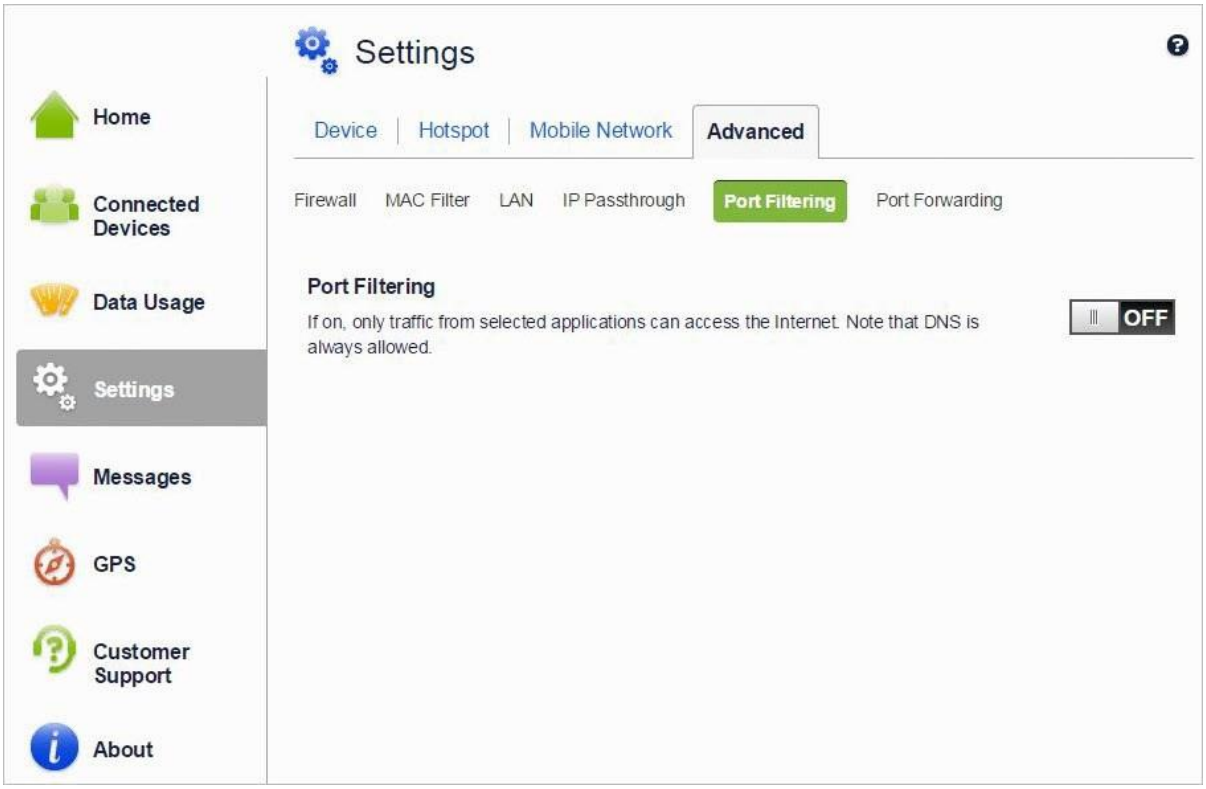
Once the IP Passthrough feature is enabled, the IP address allocated to the IP Passthrough device is displayed here. Note that if there is no connection to the mobile network, the IP Passthrough device will be allocated an IP address on the local network. This address is automatically updated with the Internet IP address once the connection to the mobile network is established.

Reserved Ports

These ports are not available to the IP Passthrough device - traffic using these ports will not reach the IP Passthrough device. If this creates a problem, you should change these ports to values which are not used by the IP Passthrough device.

Settings | Advanced| Port Filtering

The following figure shows the Port Filtering Settings screen.



Overview

Use the Port Filtering feature as needed to block outgoing Internet traffic. If this setting is enabled, only traffic from the selected applications can access the Internet. Traffic is identified by port numbers. Some applications are pre-defined. You can define additional applications, but you need to know details of the traffic used and generated by the applications you wish to define.

Applications

Enable/Disable Checkbox

Use these check boxes to enable access to the Internet for each application while the Port Filtering feature is enabled. Traffic from selected applications can access the Internet. Otherwise, the traffic is blocked.

Custom Applications

This feature allows you to define your own applications - up to 10. Once defined, these applications can be enabled and disabled the same way as pre-defined applications. To define an application, you need to know the ports and protocol (TCP, UDP) used by the application for outgoing traffic. To start, click the Add Custom Application button, then provide the following data.

NOTE: Any changes to a Custom Application are not saved until you click **Save Changes** to save the page contents.

Enable

Use this check box to enable an application after you have defined it. If selected, traffic from this application can access the Internet. Otherwise, the traffic is blocked.

App Name

Enter a suitable name for the application you are defining.

Port Range (Start Port/End Port)

Each application has its own port range. Enter the beginning and end of the port range for each application.

- For a single port, enter the port number in both the Start Port and End Port fields
- For a port range, enter the beginning of the range in the Start Port field and the end of the range in the End Port field.

Protocol

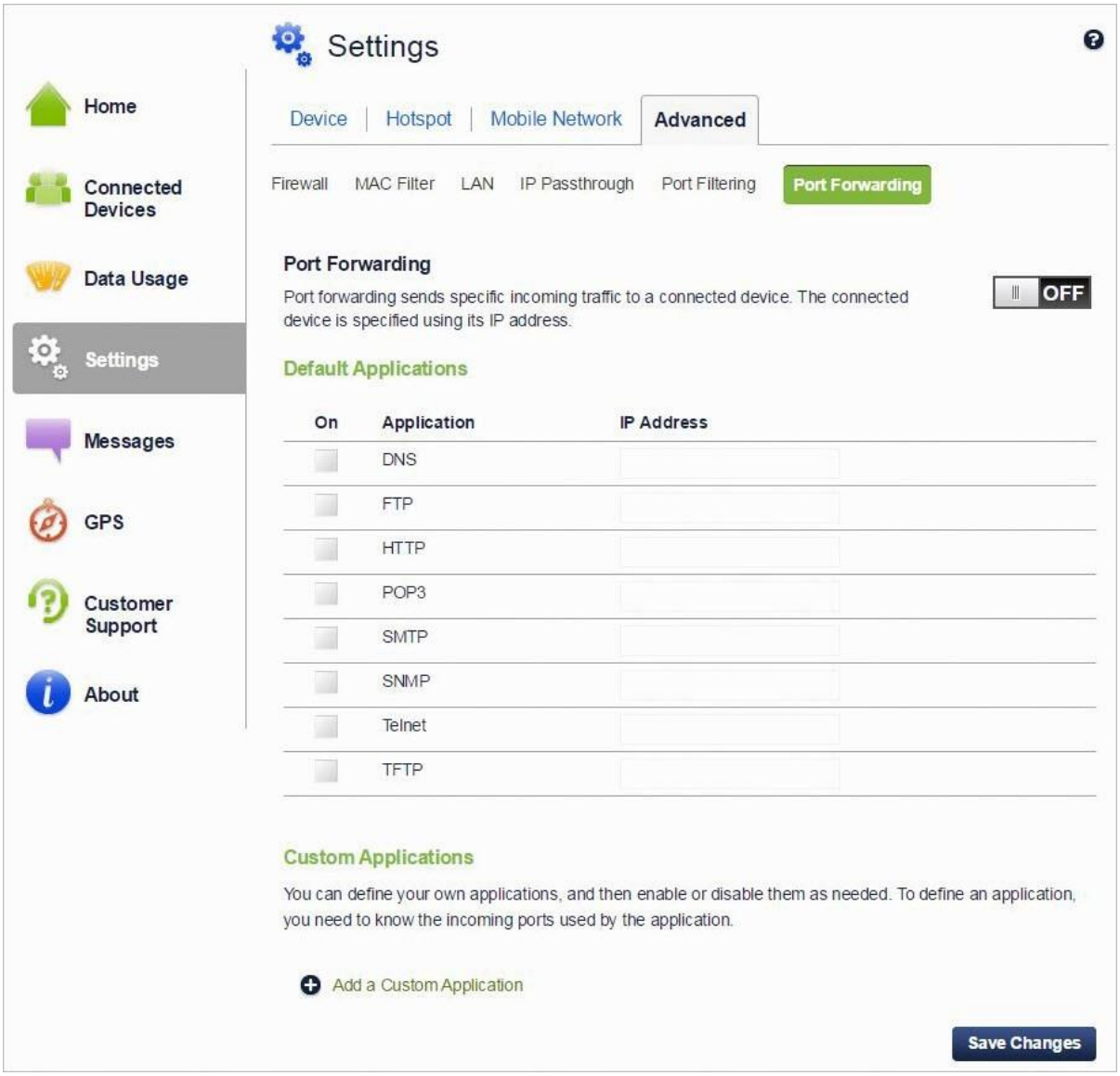
For each port range, select the protocol (TCP or UDP) used by that port range.

Delete

Use this checkbox to delete a custom application.

Settings | Advanced| Port Forwarding

The following figure shows the Port Forwarding Settings screen.



Overview

The Port Forwarding feature allows incoming traffic from the Internet to be forwarded to a particular computer or device on your Wi-Fi network. Normally, the built-in firewall blocks incoming traffic from the Internet. Use Port Forwarding to allow Internet users to access any server you are running on your computer, such as a Web, FTP, or E-mail server. For some online games, Port Forwarding must be used in order for the games to function correctly. Note that the use of Port Forwarding creates a security risk and should be disabled when not required.

NOTE: Some Mobile Wireless Networks provide you with an IP address on their own network rather than an Internet IP address. In this case, Port Forwarding cannot be used because Internet users cannot reach your IP address.

Port Forwarding Applications

Enable/Disable Checkbox

The Port Forwarding screen lists common server applications. The applications listed are: DNS, FTP, HTTP, POP3, SMTP, SNMP, Telnet, and TFTP.

To enable any of these applications, follow this procedure:

1. Install the application on a computer that is connected to this device's Wi-Fi network.
2. Enable the application from the Default Applications list by selecting its checkbox in the **On** column.

   When you choose to enable an application, the IP Address field is activated for you to type in the IP Address.
3. On the computer, locate the IP address for the Wi-Fi network. Alternatively, you can use the computer's IP address that is on the Connected Devices screen.
4. Enter the IP Address in the **IP Address** field that appears next to the application that you chose to enable.
5. Click **Save Changes**.

On the Current Status screen, make a note of the Internet IP address of this device. Ask users on the Internet to connect to the Internet IP address of this device. These connection requests will be forwarded to the IP address that you typed in on the Port Forwarding screen.

Custom Applications

This feature allows you to define your own applications. Once defined, these applications can be enabled and disabled in the same way as pre-defined applications. To define an application, you need to know the ports and protocol (TCP, UDP) used by the application for incoming traffic.

To define your own applications:

- Click the Add Custom Application button, then provide the following data.

Enable/Disable Checkbox

Use this to enable an application after you have defined it.

Application Name

Enter a suitable name for the application you are defining.

Port Range

Each application has its own port range. Enter the beginning and end of the port range for each application.

- For a single port, enter the port number in both the Begin Port and End Port fields.
- For a port range, enter the beginning of the range in the Begin Port field and the end of the range in the End Port field.

Protocol

For each port range, select the protocol (TCP or UDP) used by that port range.

Connected Device IP Address

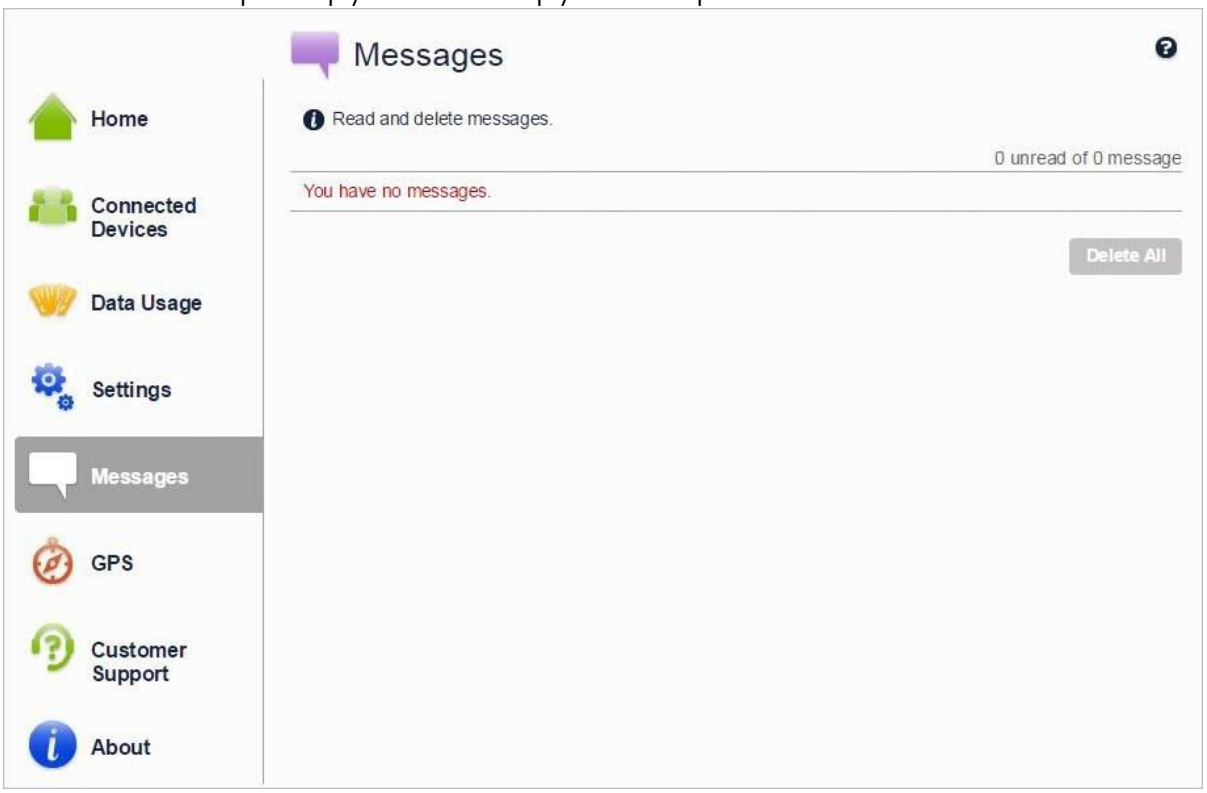
Enter the IP address of the connected device which will receive this traffic.

Delete

Use this checkbox to delete a custom application.

Messages

The Messages screen is shown below. These SMS messages are normally from your service provider. You should not attempt to reply because no reply feature is provided.



Message Counters

Two counters at the top of the screen indicate the total number of messages, and the number of unread (new) messages.

NOTE: All messages are set to "read" once they are displayed on this screen.

Message List

All messages are listed in date order. Unread (new) messages are indicated by an icon. Messages are automatically marked as "read" once they are displayed on this page, so the next time the page is entered, they will no longer be shown as unread.

Delete Button

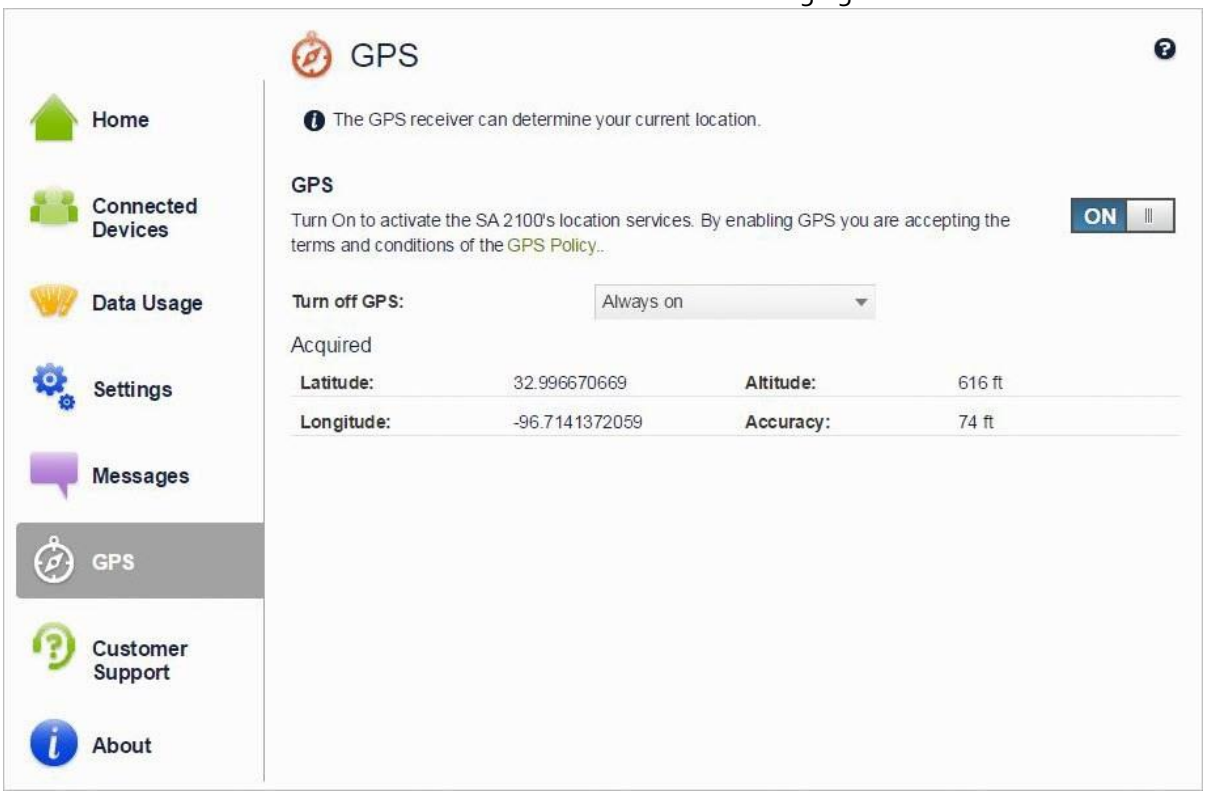
Each message has an individual "Delete" icon. Use this to delete messages.

Delete All Messages

This button is at the end of the message list. Use it as needed to delete all messages.

GPS

This device incorporates a GPS receiver. The GPS receiver can determine your current location and share this location information with connected devices. The following figure shows the GPS screen.



Using GPS

Enable GPS

Use this ON/OFF control to enable or disable the GPS feature.

Turn off GPS

This setting determines when the GPS receiver will turn off, once it is on.

If the "Turn off on power down" option is chosen, the GPS receiver will turn off once the SA 2100 is shut down. You will need to turn it on again the next time the GPS receiver is needed.

If the "Always on" option is chosen, the GPS receiver will remain on until you turn it off.

GPS Status

If the GPS receiver has not yet obtained a fix (location), an Searching status appears. Once a fix has been obtained, the following Current Location information is displayed, and a Google map appears to visually indicate the current location.

Current Location

Latitude

The Latitude for the last location fix.

Longitude

The Longitude for the last location fix.

Altitude

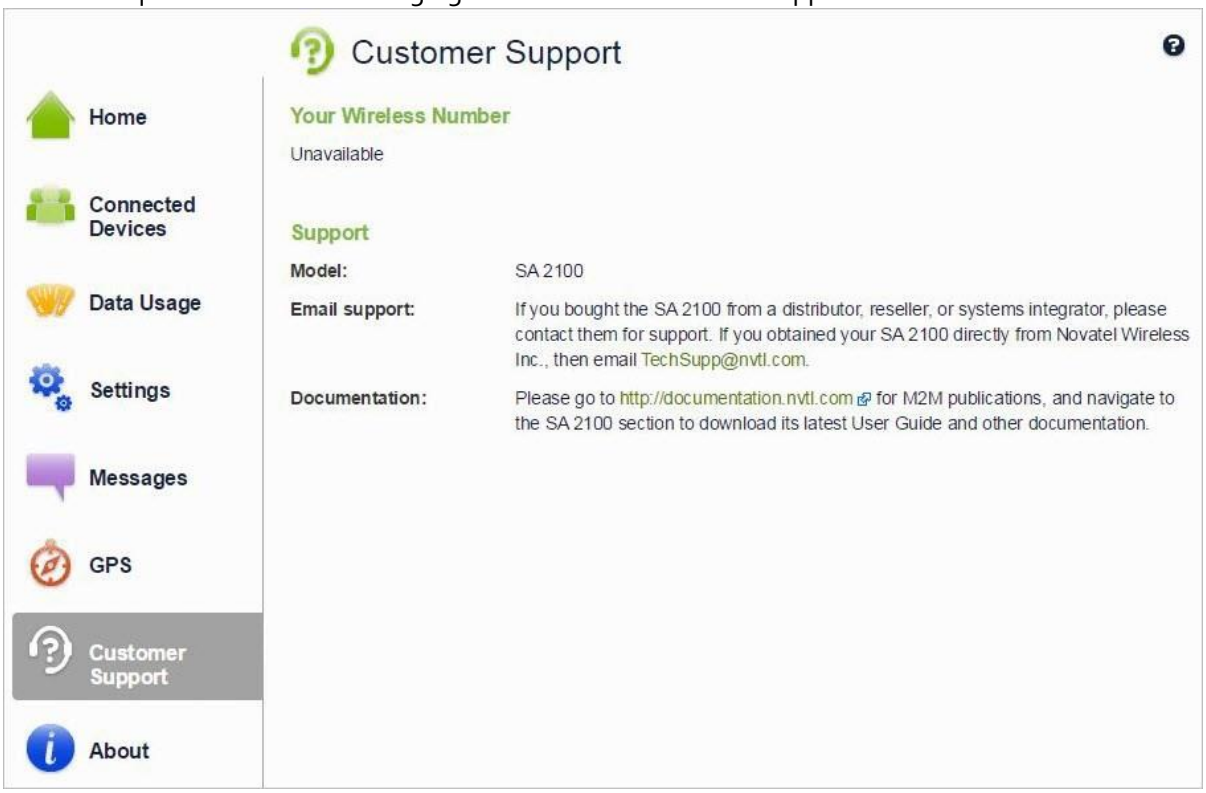
The Altitude for the last location fix.

Accuracy

This is a measure of the accuracy of the horizontal position obtained by the GPS receiver.

Customer Support

The Customer Support page provides links and contact information to assist you if you have any problems or questions. The following figure shows the Customer Support screen.



Your Wireless Number

This is the phone number for this device. Support staff will often ask for this number.

Support

Use this information to access the user guide or to obtain additional information or support.

About

The About page contains five tabs:

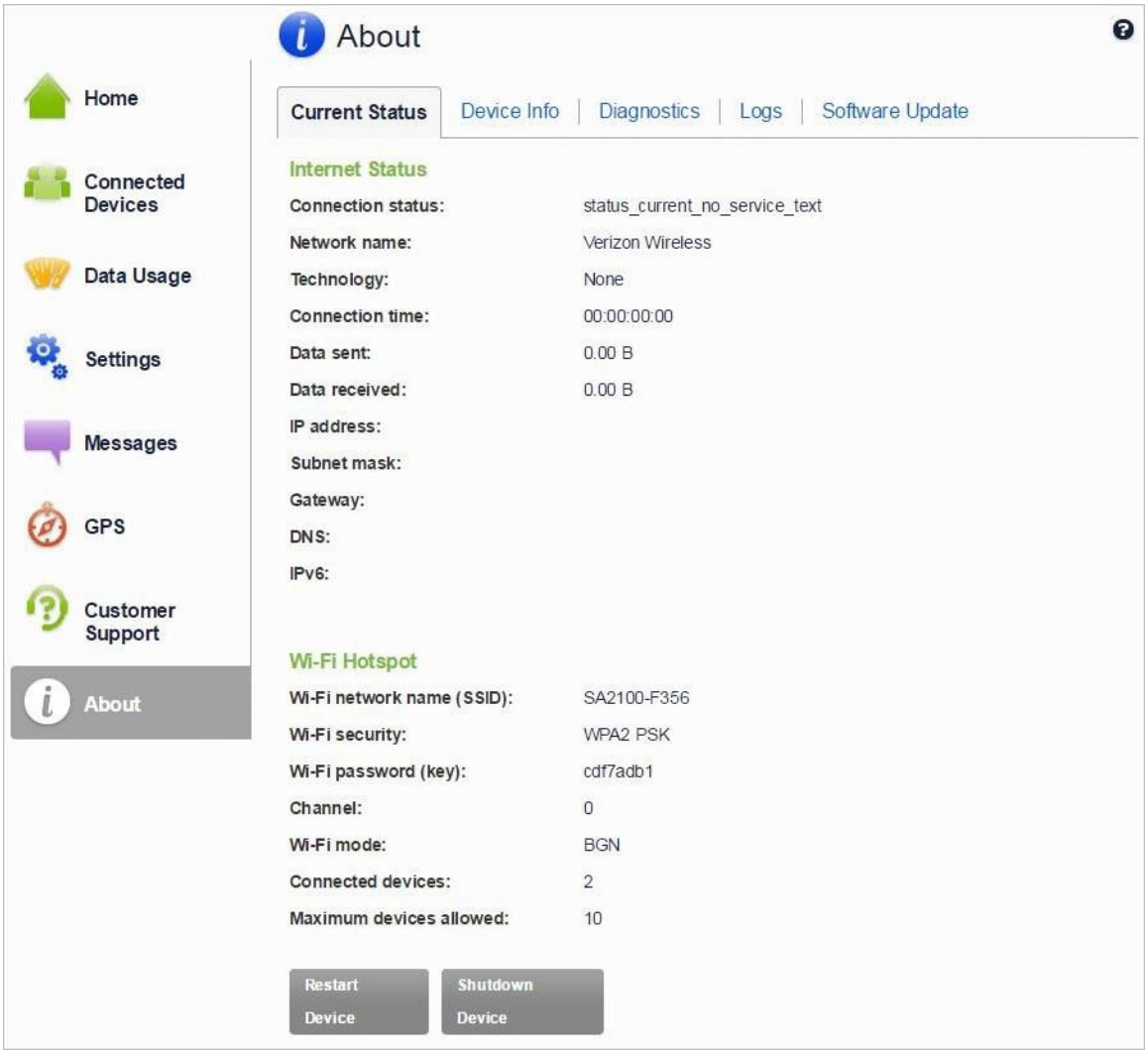
- Current Status
- Device Info

- Diagnostics
- Logs
- Software Update

By default, when the About Icon is selected, the About page opens and displays the current status tab.

Current Status

The following figure shows the Current Status screen. This screen displays status information for this device.



Internet Status

Connection Status

This displays the connection status for the Internet connection and indicates if an error condition exists.

Network Name

The name of the network to which this device is currently connected.

Technology

The network technology used for the current connection. LTE is the fastest available technology.

Connection Time

For the current Internet session, the period of time that has elapsed since the connection was established.

Data Sent

For the current Internet session, the amount of data transmitted. This counter starts from zero when the connection is established.

Data Received

For the current Internet session, the amount of data received. This counter starts from zero when the connection is established.

IP Address

The Internet IP address assigned to this device.

Subnet Mask

The network mask associated with the IP address above.

Gateway

The gateway IP address associated with the IP address above.

DNS

The Domain Name Server currently used by this device.

IPv6

The global IPv6 address for the SA 2100 is displayed here. This will be blank if IPv6 is turned off, or is not supported by the current network connection.

Wi-Fi Hotspot

Wi-Fi Network Name (SSID)

The name of the Wi-Fi network.

Wi-Fi Security

The current setting for Wi-Fi security.

Wi-Fi Password (Key)

The current password value.

Channel

The Wi-Fi channel currently in use. If the channel setting is Automatic, this displays the automatically selected channel.

Wi-Fi Mode

The 802.11 mode in use.

Connected Devices

The number of currently connected devices. For details, use the Connected Devices menu option.

Maximum Devices Allowed

This is the maximum number of devices that can connect to this SA 2100 device at any time.

Operations

Restart

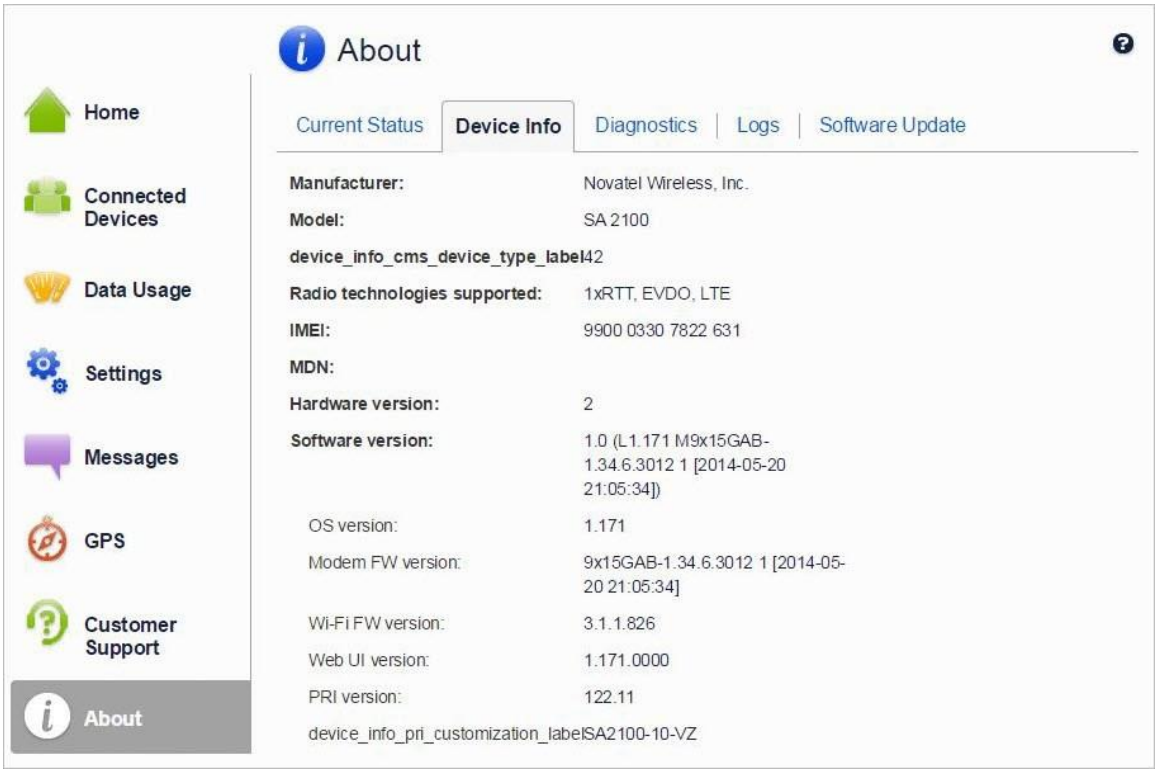
Click this button to restart the device. All Internet connections and all Wi-Fi connections will be lost during the restart.

Shutdown

Click this button to shut down the device. All existing connections will be lost.

Device Info

The following figure shows the Device Info screen.



Manufacturer

The manufacturer of this device.

Model

The official model name and number for this device.

Radio technologies supported

This lists the different radio technologies supported by this device.

NOTE: Note that this list refers to this device, and not the mobile network.

IMEI

The IMEI (International Mobile Equipment Identity) for this device. The IMEI is a 15 or 17 digit code used to uniquely identify an individual mobile station on a LTE network. The IMEI does not change when the SIM is changed.

MDN

This is the phone number assigned to this device. It will change when the SIM is changed.

Hardware Version

This indicates the hardware version for your particular device.

Software Version

The version of currently installed software. This is the main version number; the following version information relates to various software components.

OS version

This is the version number for the OS (Operating System) and its components.

Modem INSEEGO version

For the 4G Modem component, this is the version of the firmware (software) currently installed.

Wi-Fi INSEEGO version

For the Wi-Fi component, this is the version of the firmware (software) currently installed.

Web UI version

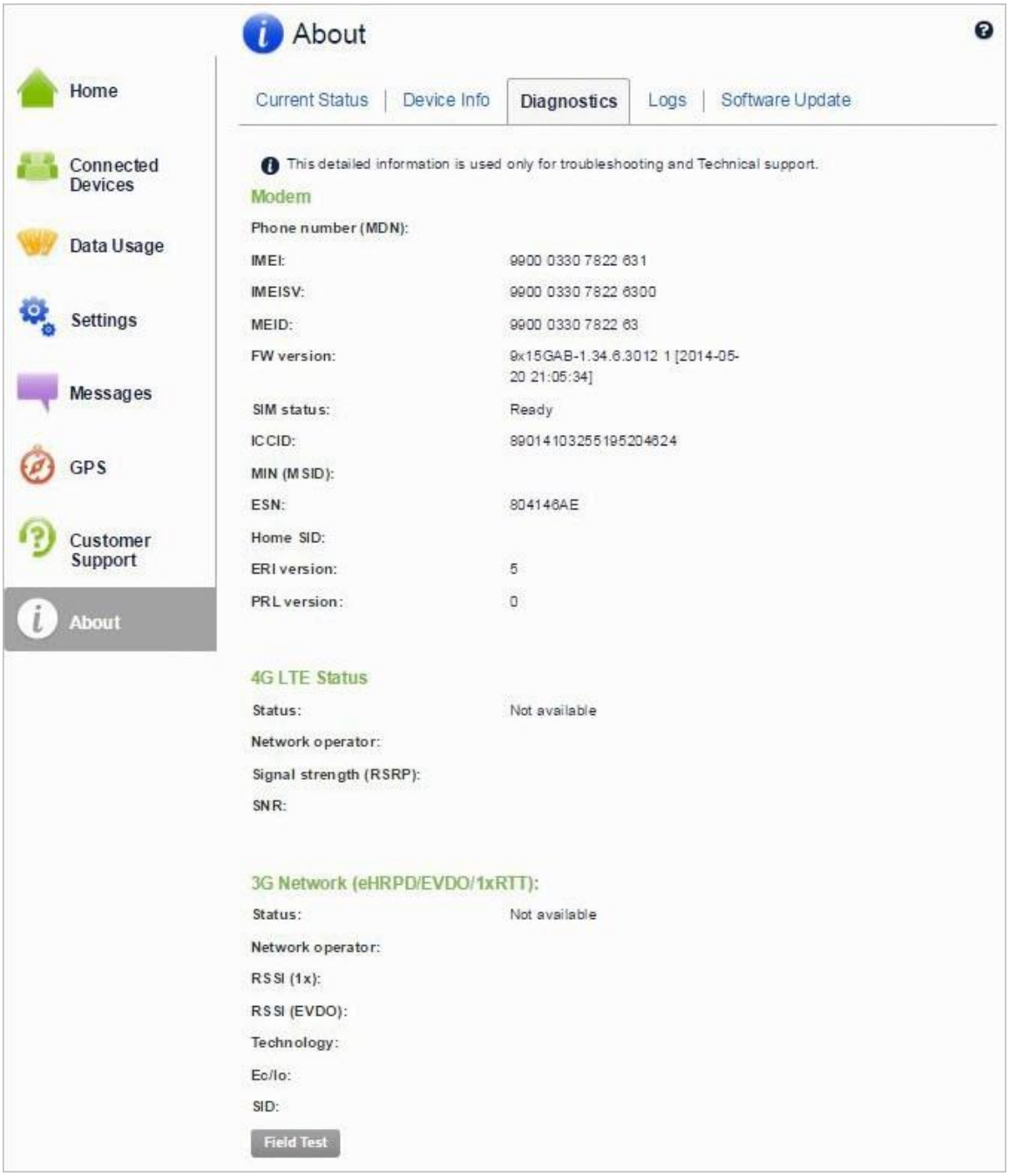
The version number for the SA 2100 Web Interface.

PRI version

This identifies the configuration version currently applied to this device.

Diagnostics

The following figure shows the Diagnostics screen. This page contains information about SA 2100 and the available networks. Use it as needed for troubleshooting; it is not required for normal operation.



Modem

Phone number (MDN)

Although this device does not support voice calls, it has a normal phone number, which is displayed here.

IMEI

The IMEI (International Mobile Equipment Identity) for this device. The IMEI is a 15 or 17 digit code used to uniquely identify an individual mobile station on a LTE network. The IMEI does not change when the SIM is changed.

IMEISV

This field combines the IMEI with an approval number for this type of device.

MEID

The MEID (Mobile Equipment ID) is a unique number used to identify an individual mobile station on a CDMA network.

INSEEGO Version

The version of the firmware (software) currently installed in the 4G modem.

SIM Status

This indicates the status of the SIM card. If the SIM card is missing, or this field indicates some form of SIM error, connection to the mobile network is not possible.

ICCID

This unique ID number is assigned to the SIM card. It does not display if there is no SIM card, or a SIM error condition exists.

MIN (MSID)

This ID is used to identify a subscriber on the mobile data network.

ESN

Electronic Serial Number (ESN) is the traditional method to uniquely identify devices on CDMA networks, but it has been supplanted by the MEID. For devices which use a MEID (like this device), the ESN is either blank or a pseudo-ESN which is not guaranteed to be unique.

Home SID

The SID (System ID) is a network identifier which indicates the attachment point to the mobile data network.

ERI version

The ERI (Enhanced Roaming Indicator) table contains information about each roaming network to which the mobile device is allowed to connect. This field indicates the ERI version currently installed. The ERI table is updated automatically.

PRL version

The PRL (Preferred Roaming List) is used to select a network, when multiple networks are available. This field indicates the version of the PRL currently installed. The PRL is updated automatically.

4G LTE Status

Status

For the LTE network, the possible status values are:

- Disabled - access to LTE networks is disabled.
- Not available - no LTE network has been detected.
- Available - LTE is enabled, and a LTE network has been detected.

**The following data items are only provided if the 4G LTE network is available.*

*Network operator

This is the name of the LTE network.

*Signal strength (RSRP)

This indicates the strength of the LTE signal, measured in dBm. Higher absolute values indicate a stronger signal, so -80 dBm is a stronger signal than -90 dBm. Note that LTE signal strength is typically lower than 3G signal strength.

*SNR

SNR (Signal-to-Noise Ratio) is a measure of signal quality. Higher numbers indicate a better signal.

3G Network (eHRPD/EVDO/1xRTT)

Status

For the 3G network, the possible status values are:

- Disabled - access to 3G networks is disabled.
- Not available - no 3G network has been detected.
- Available - a 3G network has been detected.

**The following data items are only provided if the 3G network is available. In this context, 3G means eHRPD, all versions of EVDO, and 1xRTT.*

*Network Operator

This is the name of the 3G network.

*RSSI (1x)

RSSI is a measure of signal strength. The unit is decibels, relative to 1 milliwatt, and is always negative because mobile radio devices are much less powerful than 1 milliwatt. Higher absolute values indicate a stronger signal, so -50 dBm is a stronger signal than -70 dBm. This field indicates the RSSI for the 1xRTT signal.

*RSSI (EVDO)

This field indicates the signal strength for the EVDO signal. See above for a description of RSSI.

*Technology

The current technology for the 3G network. Possible values, from slower to faster, are:

- 1xRTT
- EVDO • HRPD
- eHRPD

*Ec/Io

Ec/Io is a measure of how "clean" the signal is, and is a type of signal-to-noise ratio. Typical values range from -10 to -40. A value of -4 would be a very "clean" signal.

*SID

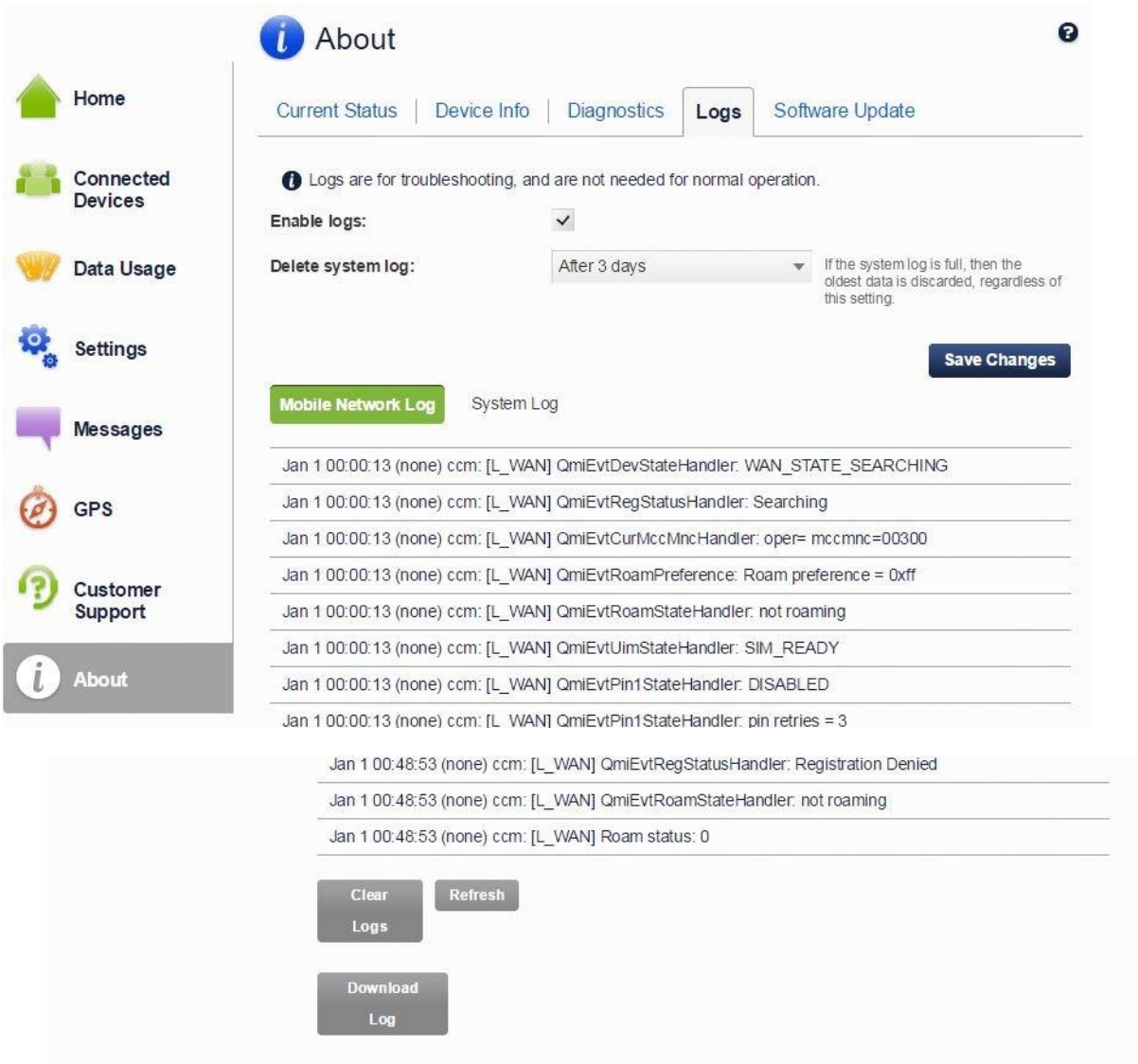
SID (System ID) is a network identifier which indicates the current attachment point to the mobile data network. A group of cell towers may have the same SID value. This field indicates the current SID.

Field Test

The "Field Test" button will provide a list of low-level network parameters which can be helpful for technical support staff when they troubleshoot network connectivity issues.

Logs

The following figure shows the Logs screen. The Log information is useful for troubleshooting, but is not required for normal operation.



Settings

Enable logs

Enable the Logs as needed.

Delete System Log

This setting determines for how long the system log data is retained. Select the desired option.

NOTE: If the log is full, the oldest data is deleted, regardless of this setting.

Log Data

The provided tabs allow you to select the type of Log data to view.

Mobile Network Log

This log contains data regarding connections to the mobile network.

System Log

This log records events - other than mobile data connections - which occurred on this device.

Buttons

Clear Log

Clicking this button will delete all existing log data. This makes new data easier to read.

Refresh

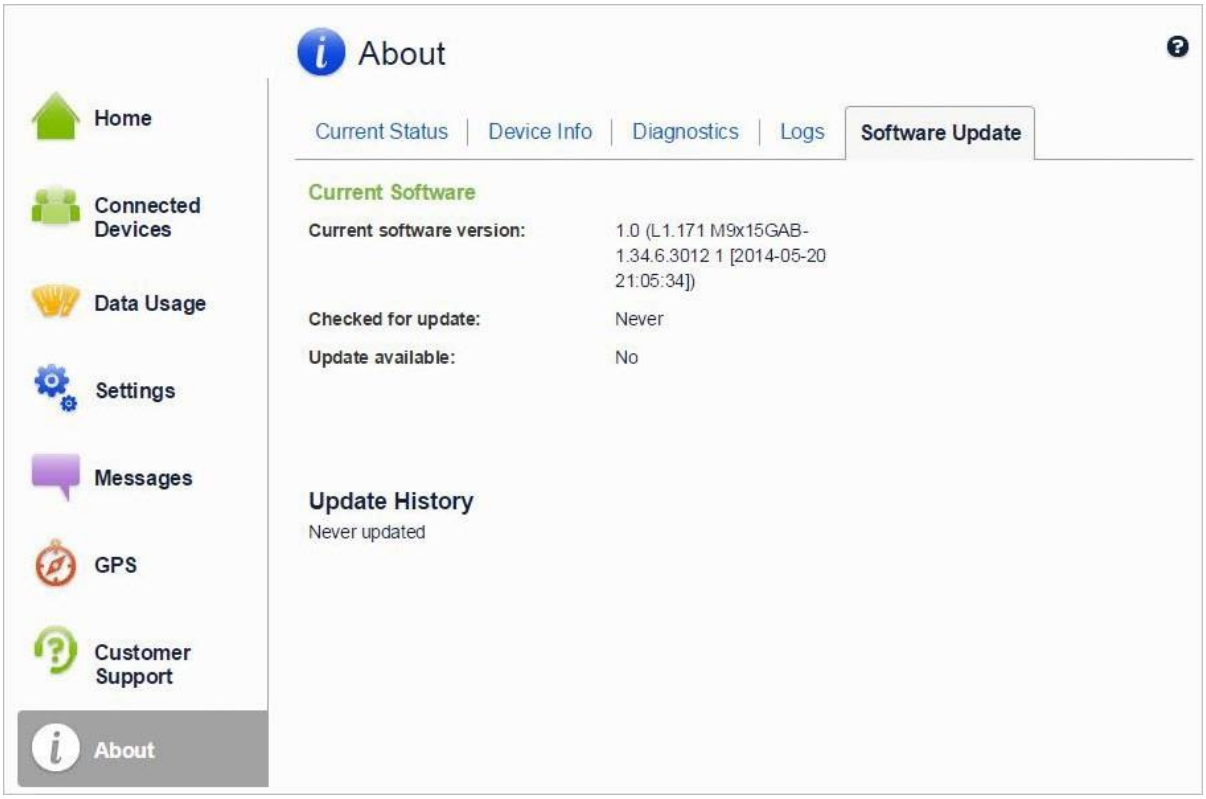
Use this to update the log data which is displayed.

Download Log

Use this button if you wish to download log data to your computer or connected device.

Software Update

The following figure shows the Software Update screen. Software updates are delivered automatically over the mobile network. This page allows you to monitor these updates.



Current Software Version

This field indicates the version of the software currently installed on this device.

Checked for update

This device automatically checks for updates; this field indicates when the last check was performed.

Update available

This indicates if an update is available. If an update is available, it is automatically downloaded and installed.

Last Update

This panel displays the details of the last update installed on this SA 2100 device. If no updates have been installed, this panel is blank.

Update History

The Update History panel displays the details of all updates that have been downloaded and installed to this SA 2100 device. If no updates have been installed, this panel is blank.

6

Accessories

Accessories List
Antenna
Backup Battery
Power Cable
USB Cable Part

Accessories List

The following table shows the available accessories and SKUs for the SA 2100. To order an accessory, contact your Inseego Corporation sales representative.

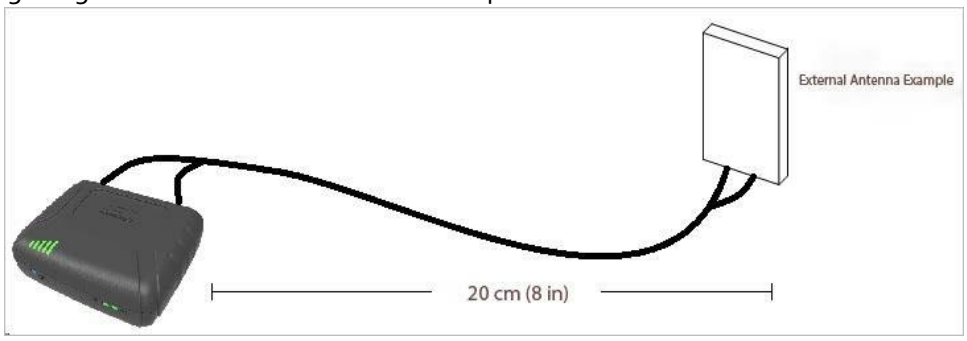
Accessory	SKU
USB	.01019886.
USB (latched)	.60715094.
Mounting	.21915041.
Mounting (vehicle)	.21915042.
Power Cable	.60715093.
Power Adapter NA (-30 TO 70C)	.40123113.01.
Power Adapter EU (-30 TO 70C)	.40123113.01.
Battery	.40115130-001.

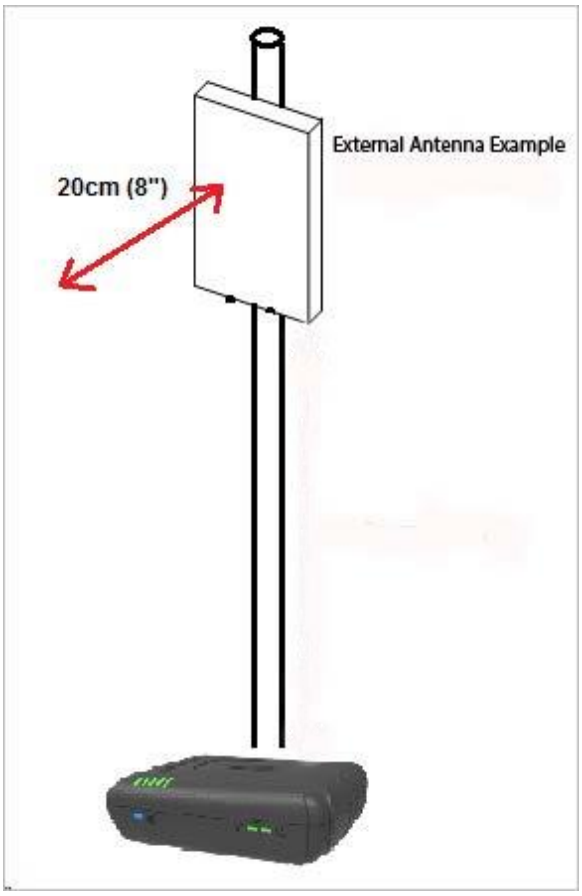
Antenna

WARNING! The following installation practices are required to comply with FCC rules on RF exposure. Failure to follow these guidelines can result in operations that exceed RF Exposure limits.

WARNING! Maintain a minimum distance of at least 20 cm (8 in) from all persons regardless of how the antenna is mounted (stand assembly or wall mount).

The following images show how the antenna can be placed with a 20 cm distance from the SA 2100.





The gain of the antenna (including cable loss) will not exceed the following:

Frequency	Maximum Antenna Gain (dBi)
704 - 787	3.5
824 - 849	4.0
1710-1755	3.5
1850 - 1910	2.0

NOTE: For any questions regarding the safe operation of this device please contact Inseego Corporation at www.inseego.com.

Backup Battery

The Backup Battery is a rechargeable 3.7V 2900 mAh 1073Wh Li-ion Battery.



The backup battery is charged when the power adapter is connected to the device. The backup battery does not charge using a USB cable.

Power Cable

The Power cable has an 8-pin Molex connector that supplies power to the SA 2100.

The Black wire goes to the chassis ground.

The Red wire goes to a 12 V or 24 V vehicle-ready power supply.



8-Pin Molex Connector

Pin #	Function
Pin -1	User Controlled Input1
Pin -2	User Controlled Input2 (For the SA 2100's in-vehicle deployment, this pin is intended for ignition sense.)
Pin -3	1-Wire
Pin -4	GND
Pin -5	Supply Voltage

Pin - 6	User Controlled IO1
Pin -7	User Controlled IO2
Pin - 8	User Controlled Output

Power Supply

The Power Adapter has an 8-pin Molex connector that supplies power to the SA 2100.

Input:

- 100-240v
- 50/60 Hz
- 0.45A

Output:

- 12V
- 1.5A



USB Cable Part

An industry standard Micro USB (not included) is required only if communication through the Com port is required.



7

Compliance and Regulatory

General Disclaimer
Warranty Information
Regulatory Compliance

General Disclaimer

TERMS OF USE OF NEW MATERIALS - PLEASE READ CAREFULLY

From time to time, Inseego Corporation, in its sole discretion, may make available for download on its website (www.inseego.com), or may transmit via mail or email, updates or upgrades to, or new releases of, the firmware, software or documentation for its products (collectively, 'New Materials'). U se of such New Materials is subject to the terms and conditions set forth below, and may be subject to additional terms and conditions as set forth in Inseego Corporation's Technical Support Policy (posted on its website) and/or any written agreement between the user and Inseego Corporation.

All New Materials are provided AS IS. Inseego Corporationmakes no warranty or representation with respect to the merchantability, suitability, functionality, accuracy or completeness of any such New Materials. The user of such New Materials assumes all risk (known or unknown) of such use. Inseego Corporationreserves all rights in such New Materials. The user shall have only a revocable and limited license to use such New Materials in connection with the products for which they are intended. Distribution or modification of any New Materials without Inseego Corporation's consent is strictly prohibited.

IN NO EVENT WILL INSEEGO CORPORATION BE RESPONSIBLE FOR ANY INCIDENTAL, INDIRECT, CONSEQUENTIAL OR SPECIAL DAMAGES AS A RESULT OF THE USE OF ANY NEW MATERIALS. N OVATEL WIRELESS'S MAXIMUM LIABILITY FOR ANY CLAIM BASED ON THE NEW MATERIALS SHALL NOT EXCEED FIFTY U.S. DOLLARS ($50).

Version Verification

Please ensure you have the latest version of this document by downloading it from www.inseego.com

Warranty Information

This warranty applies to (a) products sold directly by Inseego Corporation, unless a different warranty is specified in a written agreement between Inseego Corporation and the purchaser; and (b) products sold to end users through a distributor authorized by Inseego Corporation, but only where the authorized distributor does not provide a separate warranty on such products, and Inseego Corporation has agreed to provide this warranty to such end users. I f you purchased the product from an authorized distributor, please check whether this warranty from Inseego Corporation, or a separate warranty from the distributor, applies to your purchase. This warranty does not apply to any (i) accessories or batteries for the products; or (ii) demonstration samples or prototypes of the products. Unless otherwise provided in a written agreement between Inseego Corporation and the purchaser, all such accessories, batteries, samples or prototypes are provided by Inseego Corporation AS IS without any warranty of any kind.

Inseego Corporation warrants to the original purchaser of the product from Inseego Corporation or its authorized distributor (as applicable) that, for a period of one (1) year from the date of shipment of the product from Inseego Corporation, the product hardware will be substantially free from defects in material or workmanship under normal operation, and the product firmware will perform substantially

in accordance with the product documentation provided by Inseego Corporation. Inseego Corporation does not warrant that (a) the product hardware or firmware will meet the purchaser's requirements; (b) the operation of the product hardware or firmware will be uninterrupted or error-free; or (c) the product, when integrated in, or combined with, other products or software not supplied by Inseego Corporation, will continue to perform substantially in accordance with the product documentation. This limited warranty is for the benefit of the original purchaser, and is not transferable.

During the warranty period, Inseego Corporation, at its expense and in its sole discretion, will repair the product, or replace the product with a corresponding or equivalent product, if it is determined to have a covered defect, provided that the purchaser first notifies Inseego Corporation (directly or through its authorized distributor from which the product was purchased) of any such defect, furnishes Inseego Corporation with a proof of purchase (if required), requests and obtains a return merchandize authorization (RMA) number from Inseego Corporation, and returns the product under that RMA to Inseego Corporation (or, at Inseego Corporation's option, to its authorized distributor), with the shipping charges being prepaid by purchaser. If, upon reasonable examination of the returned product, Inseego Corporation does not substantiate the defect claimed by purchaser, or determines that the defect is not covered under this limited warranty, Inseego Corporation will not be required to repair or replace the product, but may instead reship the product to the purchaser (or, at Inseego Corporation's option, to its authorized distributor where the product can be made available to purchaser), in which case the purchaser shall be responsible for paying Inseego Corporation's cost for reshipping the product to purchaser (or to Inseego Corporation's authorized distributor), and Inseego Corporation's usual charges for unpacking, testing, and repacking the product for reshipment to purchaser (or to Inseego Corporation's authorized distributor). Purchaser shall bear the risk of loss or damage in transit to any product returned by purchaser to Inseego Corporation, or any returned product not found to be defective or covered under this warranty, and reshipped by Inseego Corporation to purchaser (or to Inseego Corporation's authorized distributor). I n the event Inseego Corporation repairs or replaces a defective product covered by this limited warranty, the repaired or replacement product will be covered under this limited warranty for the remainder of the original warranty period on the defective product, or a period of ninety (90) days, whichever is longer. If Inseego is unable to repair or replace a defective product covered by this limited warranty, Inseego Corporation will provide to purchaser a credit or a refund (at Inseego Corporation's option) of the original purchase price (excluding taxes and shipping charges). A ny returned and replaced product, or any product for which Inseego Corporation has furnished a credit or a refund, becomes the property of Inseego Corporation.

Inseego Corporation shall not have any obligation to provide any firmware bug fixes, upgrades or new releases except as may be necessary to correct any covered defect of which purchaser notifies Inseego Corporation in writing during the warranty period. N ovatel Wireless, from time to time and in its sole discretion, may make available for download on its website (www.inseego.com), or may provide via email, certain firmware bug fixes, upgrades or new releases for the product. D ownload and use of any such bug fixes, upgrades or new releases is subject to all of the applicable terms and conditions of Inseego Corporation's technical support policy as posted and updated on its website.

Inseego Corporation shall have no obligation under this limited warranty for (a) normal wear and tear; (b) the cost of procurement of substitute products; or (c) any defect that is (i) discovered by purchaser during the warranty period but for which purchaser does not request an RMA number from Inseego Corporation, as required above, until after the end of the warranty period, (ii) caused by any accident, misuse, abuse, improper installation, handling or testing, or unauthorized repair or modification of the product, (iii) caused by use of any materials not supplied by Inseego Corporation, or by use of the product other than in accordance with its documentation, or (iv) the result of electrostatic discharge, electrical surge, fire, flood or similar causes.

The purchaser (or its customers, as applicable) shall be solely responsible for the proper configuration, testing and verification of the Inseego Corporation product prior to deployment in the field, and for ensuring that any end user product or system into which the Inseego Corporation product is integrated or incorporated operates as intended and meets the requirements of purchaser (or its customers). Inseego shall have no responsibility whatsoever for the integration, configuration, testing, verification, installation, upgrade, support or maintenance of any such end user product or system, or for any liabilities, damages, costs or expenses associated therewith.

INSEEGO CORPORATION'S SOLE RESPONSIBILITY AND PURCHASER'S SOLE REMEDY UNDER THIS LIMITED
WARRANTY SHALL BE FOR INSEEGO CORPORATION TO REPAIR OR REPLACE THE PRODUCT (OR IF REPAIR
OR REPLACEMENT IS NOT POSSIBLE, PROVIDE A CREDIT OR REFUND OF THE PURCHASE PRICE) AS
PROVIDED ABOVE. INSEEGO CORPORATION EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY, SATISFACTORY PERFORMANCE AND FITNESS FOR A PARTICULAR
PURPOSE. I N NO EVENT SHALL INSEEGO CORPORATION BE LIABLE FOR ANY INDIRECT, SPECIAL, EXEMPLARY, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOSS
OR INTERRUPTION OF USE, DATA, REVENUES OR PROFITS) RESULTING FROM A BREACH OF THIS WARRANTY OR BASED ON ANY OTHER LEGAL THEORY, EVEN IF INSEEGO CORPORATION H AS BEEN ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF SUCH DAMAGES.

Some jurisdictions may require a longer warranty period than specified above and, accordingly, for products sold in those jurisdictions the applicable warranty period shall be extended as required under the laws of those jurisdictions. Furthermore, some jurisdictions may not allow the disclaimer of implied warranties or the exclusion or limitation of incidental or consequential damages, so the above disclaimer, limitation or exclusion may not apply to products sold in those jurisdictions. This limited warranty gives the purchaser specific legal rights and the purchaser may have other legal rights that vary from jurisdiction to jurisdiction.

This limited warranty shall be governed by the laws of the State of Texas, United States of America, without regard to conflict of laws principles. This limited warranty shall not be governed in any respect by the United Nations Convention on Contracts for the International Sale of Goods.

Regulatory Compliance

FCC CERTIFICATION

Inseego Corporation M2M certifies that the Enabler HS 3001 CDMA Radio Module (FCC ID: MIVXXXXXXX) complies with the RF requirements applicable to broadband PCS equipment operating under the authority of 47 CFR Part 24, Subpart E and Part 22 of the FCC Rules and Regulations. This certification is contingent upon installation, operation and use of the Inseego Corporation M2M Enabler IIIG module and its host product in accordance with all instructions provided to both the OEM and end user. When installed and operated in a manner consistent with the instructions provided, the Enabler HS 3001 module meets the maximum permissible exposure (MPE) limits for general population / uncontrolled exposure at defined in Section 1.1310 of the FCC Rules and Regulations.

The Enabler HS 3001 module is designed for use in a variety of host units, "enabling" the host platform to perform wireless data communications. However, there are certain criteria relative to integrating the modem into a host platform such as a PC, laptop, handheld, monitor and control unit, etc. that must be considered to ensure continued compliance with FCC compliance requirements.

In order to use the Enabler IIIG module without any additional FCC certification the installation must meet the following conditions:

- The system antenna(s) connected to the Enabler IIIG module must be installed to provide at least 20cm separation from the human body during normal operation.
- The system antennas must not be co-located with any other transmitter or antenna.
- The system antenna(s) used with the Enabler HS 3001 module must not exceed the following levels:
  - Band Class 0: the maximum gain is TBD.
  - Band Class 1: the maximum gain is TBD.

If any of these conditions are not met then additional information should be sought from the FCC or an FCC qualified test laboratory.

The system user manuals and other documentation must also include appropriate caution and warning statements and information.

FCC NOTICE TO USERS

Inseego Corporation has not approved any changes or modifications to this device by the user. Any changes or modifications could void the users authority to operate the device. See 47 CFR Sec. 15.21.

The 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. See 47 CFR Sec. 15.19.

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 or more 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.

If the FCCID of the module is not visible when installed in the host platform, then a permanently attached or marked label must be displayed on the host unit referring to the module.

The label should contain wording such as:

Contains FCC ID: MIDCNN0301

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.

ROHS COMPLIANCE

As a part of Enfora's corporate policy of environmental protection, Inseego Corporation takes every step to ensure that the Enabler HS 3001 modules are designed and manufactured to comply to the European Union Directive 2002/95/EC for the Restriction of Hazardous Substances (RoHS).