USER GUIDE

inseego

SKYUS 160 Series

Skyus 160NE / 160AP

INSEEGO COPYRIGHT STATEMENT

© 2025 Inseego Corp. All rights reserved. Complying with all copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose without the expressed written permission of Inseego Corp.

SOFTWARE LICENSE

Proprietary Rights Provisions:
Any software drivers provided with this product are copyrighted by Inseego Corp. and/or Inseego Corp.'s suppliers. Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp. and/or Inseego Corp. suppliers. The disassembly, decompilation, and/or Reverse Engineering of the software drivers for any purpose is strictly prohibited by international law. The copying of the software drivers, except for a reasonable number of back-up copies is strictly prohibited by international law. It is forbidden by international law to provide access to the software drivers to any person for any purpose other than processing the internal data for the intended use of the software drivers.

U.S. Government Restricted Rights Clause:
The software drivers are classified as "Commercial Computing device Software" and the U.S. Government is acquiring only "Restricted Rights" in the software drivers and their Documentation.

U.S. Government Export Administration Act Compliance Clause:
It is forbidden by US law to export, license or otherwise transfer the software drivers or Derivative Works to any country where such transfer is prohibited by the United States Export Administration Act, or any successor legislation, or in violation of the laws of any other country.

TRADEMARKS AND SERVICE MARKS

Inseego Corp. is a trademark of Inseego Corp., and the other trademarks, logos, and service marks (collectively the "Trademarks") used in this user manual are the property of Inseego Corp. 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 Corp. or any other Trademark displayed in this user manual without the written permission of Inseego Corp. or its respective owners.

- MiFi® and the MiFi logo are registered trademarks of Inseego Corp.
- Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

The names of actual companies and products mentioned in this user manual may be the trademarks of their respective owners.

Document Number: MKT-00073 Rev 6

Contents

1 Introduction 5
Overview 6
Key Features 6
Description 7
Front View 7
Back View 7
Bottom View 7
Indicator LEDs 8
2 Installation and Getting Started 9
Installation Overview 10
System Requirements 10
Installing a SIM Card 11
Installing the Battery 12
Connecting Antennas 12
Mounting Precautions and Guidelines 13
Positioning your Device 13
Mounting the Device 14
Powering the Device 15
Using the Backup Battery 16
Connecting your Device 17
Connecting via Ethernet 17
Connecting via USB 17
Connecting via Wi-Fi 17
Connecting to the Web UI 18
Connecting External Sensors via Bluetooth 18
Resetting your Router 18
Getting Support 18
3 Software Configuration 19
Overview 20
Logging In 20
Home Page 21
Side Menu 22
Getting Help 22
Managing Bluetooth Sensors 23
Bluetooth Sensors Page 23
Managing Connected Devices 25
Connected Devices Page 26
Configuring GPS 27
Status Tab 27
Local Tab 29
Remote Tab 30
Managing Settings 33
Wi-Fi Hotspot Tab 33
Device Tab 36
Mobile Network Tab 46
Advanced Tab 52
GPIO Tab 52
Accessing Messages 54
Messages Page 54

Viewing Info About the Router 55
Current Status Tab 56
Data Usage Tab 58
Device Info Tab 59
Diagnostics Tab 61
Logs Tab 63
Software Update Tab 64
Support Tab 65
4 Advanced Settings 66
Overview 67
Using Advanced Settings 67
Firewall Tab 68
Mac Filter Tab 69
LAN Tab 71
Port Filtering Tab 73
Port Forwarding Tab 76
IPPT Tab 79
HTTPS Tab 80
Remote Admin Tab 83
VPN Tab 84
Inseego Connect Tab 85
5 Accessories 86
Included Accessories 87
Optional Accessories 88
Power Cable 89
AC Power Cable 89
DC Power and IO Cable 90
USB Cable and Adapter 91
6 Product Specifications and Regulatory Information 92
Product Specifications 93
Device 93
Environmental 93
Cellular Bands 93
Bluetooth Sensors 94
Technology 94
Power 94
OS Support 94
Regulatory Information 95
Wireless Communications 98
Limited Warranty and Liability 98
Safety Hazards 99
7 Glossary 101
Glossary 102

1

Introduction

Overview

Description

Indicator LEDs

Overview

The compact Skyus™ 160 Series is a cellular gateway (cloud-enabled cellular modem and router) designed to support numerous Industrial IoT use cases in both fixed and mobile environments. With LTE connectivity, the Skyus 160 Series router provides features that are purpose-built for IoT. Cloud connectivity to Inseego Connect™ enables remote device/fleet/deployment management.



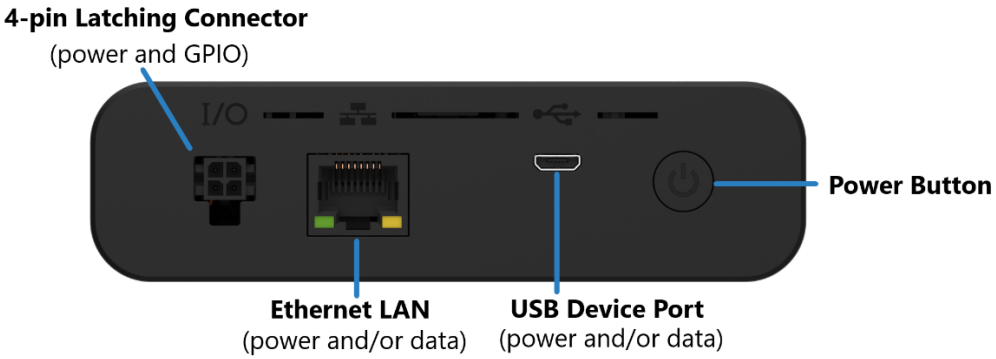
Key Features

- LTE Cat 6 (up to 300 Mbps)
- Multi-Carrier support
- aGNSS (with active and passive GNSS antenna support)
- Rugged design for continuous operation in harsh environments
- Advanced security encryption and authentication protocols
- Wi-Fi 5 and Bluetooth 5.0 *
- Standard 4400 mAh backup battery
- Multiple data interfaces: Ethernet, USB, Wi-Fi
- Multiple power interfaces: PoE, USB, or 4 Pin
- Cloud services, FOTA and remote configuration
- On-board memory to support edge processing

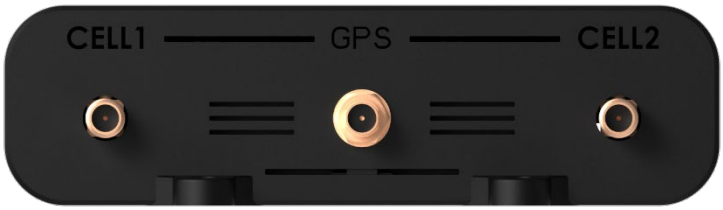
* See Bluetooth Sensors on page 94 for supported sensors.

Description

Front View

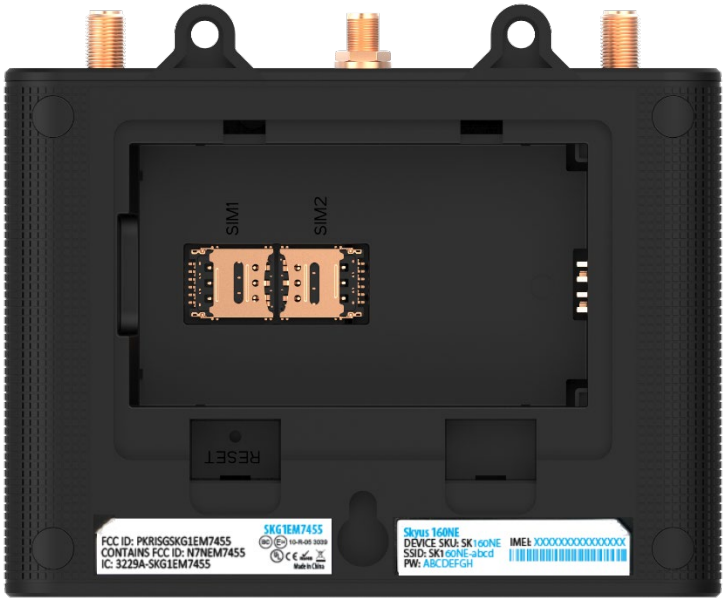


Back View



Bottom View

The battery compartment, SIM sockets, and device label are located on the bottom of the device.



Indicator LEDs

The Skyus 160 Series router has a power button with LED, as well as three LEDs that indicate cellular, Wi-Fi / Bluetooth, and GPS status.

LED	LED Color	Meaning
Power	**Blue**	On / Battery Power (High)
	Green	On / External Power
	Yellow	On / Battery Power (Low)
	Red	On / Battery Power (Critical) Error (when blinking)
Cellular*	**Blue**	Great Signal
	Green	Good Signal
	Yellow	Okay Signal
	Magenta	Poor Signal
	Orange	No SIM / Inactive SIM
	Red	Error
Wi-Fi / Bluetooth†	**Blue**	Bluetooth On – Connected Clients
	Green	Wi-Fi On – Connected Clients
	Blue and Green	Both Bluetooth and Wi-Fi On
	Orange	No Clients
	Red	Error
GPS	**Blue**	Dead Reckoning Active, Location Acquired
	Green	Assisted GPS/GNSS Active, Location Acquired
	Yellow	Standalone GPS/GNSS Active; Location Acquired
	Orange	Searching/Acquiring
	Red	Error

The Ethernet / LAN connector port also has indicator LEDs.

LED	LED Color	Operation	Meaning
LAN	**Green**		Indicates Ethernet connection speed
		Solid	1000 Mbps (Gigabit)
		Off	10/100 Mbps
	Amber		Indicates link status
		Solid	Link
		Blinking	Activity
		Off	No link

* A blinking cellular LED indicates data activity over the connection.

† See Bluetooth Sensors on page 94 for supported sensors.

2

Installation and Getting Started

Installation Overview

System Requirements

Installing a SIM Card

Installing the Battery

Connecting Antennas

Mounting Precautions and Guidelines

Mounting the Device

Powering the Device

Connecting your Device

Connecting to the Web UI

Connecting External Sensors via Bluetooth

Resetting your Router

Getting Support

Installation Overview

This chapter provides system requirements and instructions for installing and getting your Skyus 160 Series up and running.

The installation process consists of the following steps:

- Installing a SIM Card
- Installing the Battery
- Connecting Antennas
- Mounting Precautions and Guidelines
- Mounting the Device
- Powering the Device
- Connecting your Device
- Connecting to the Web UI
- Connecting External Sensors via Bluetooth

System Requirements

The Skyus 160 Series router allows you to set up a network and provides both wired and wireless connectivity.

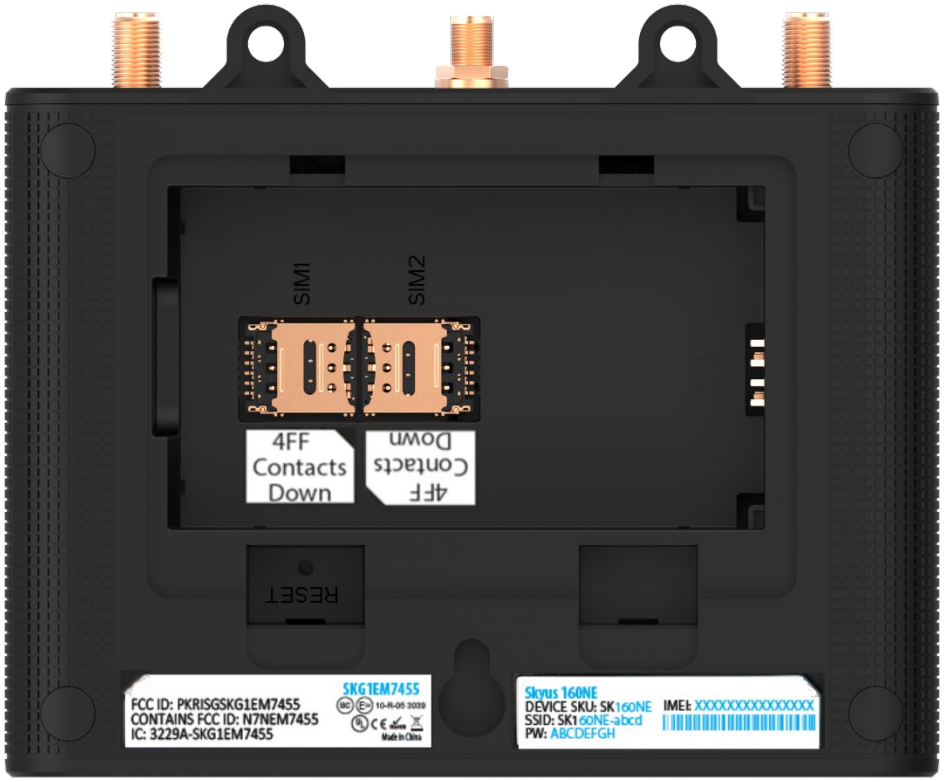
NOTE: This device is recommended for professional installation. Requirements include:

- A computer or computing device supporting Wi-Fi 802.11 b/g/n, Ethernet, or USB 2.0
- Internet browser software, such as Microsoft Internet Explorer 8.0 or higher, Firefox, Safari, Opera, or Chrome

Installing a SIM Card

To insert the SIM card:

1. Open the battery door on the bottom of the device and, if installed, remove the battery.
2. Slide the SIM socket retainer to the unlocked position and lift it.



3. Insert the SIM card into the appropriate slot in the orientation shown.
4. Press the retainer down and move it to the locked position.
5. Replace the battery and the battery door.

Installing the Battery

To install or remove the backup battery:

1. Remove the battery door on the bottom of the device.
2. Install or remove the battery.

   NOTE: The battery will only fit into the device in the correct orientation.

3. Replace the battery door.

CAUTION! Risk of explosion if replaced by an incorrect type. Dispose of used batteries according to the instructions.

Connecting Antennas

Finger tighten the appropriate antennas for your desired configuration. Check the label on each antenna to ensure correct placement. At minimum, connect antennas to CELL 1 and CELL 2 ports.

NOTE: Recommended torque is 5 in-lbs (56 N-cm).



Mobile Configuration

Antenna Ports	Frequency Range	Connector Type
1. CELL 1	690–960 MHz; 1700–2700 MHz	SMA
2. GPS*	1570 - 1580 MHz	SMA
3. CELL 2	690–960 MHz; 1700–2700 MHz	SMA

* Ensure GPS antenna is located with clear access to GNSS satellites.

Mounting Precautions and Guidelines

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

- Locate the router in an area free from liquids, dust, and extreme temperatures. If it is possible for the device to experience contact with fluids, extreme mechanical shock, or extreme thermal conditions (outside of the thermal specs listed in this User Guide), you run the risk of damaging the device and/or the battery. If the battery is subject to these conditions, the battery may fail and cause significant damage to the device and the surrounding area.
- 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 antenna performance.
- Clean only with a clean, dry cloth.
- Protect the cord from being crushed or pinched.
- Take care to locate and route cords and wires to minimize the risk of damaged caused by users or other objects that are located near the device.
- Avoid dropping or shaking the router to reduce the risk of damaging the device or disrupting operation.

Positioning your Device

The size and mounting options available for the Skyus 160 Series router allow you to install the device in the location that best suits your needs. The reception and coverage range depends on where you mount the router. Keep in mind that the placement of furniture, the thickness of walls, and the number of walls a signal must travel through can limit cellular, Wi-Fi, and Bluetooth 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)
- More than 20 cm away from a person
- Close to a window but out of the way of direct sunlight (great for 4G LTE reception)
- Close to an AC outlet and near Ethernet computer cables
- In an elevated location

- In line-of-sight to Wi-Fi and Bluetooth devices
- Near the computers or other devices that communicate with the router
- On an upper floor for best cellular signal (if applicable)

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

Mounting the Device

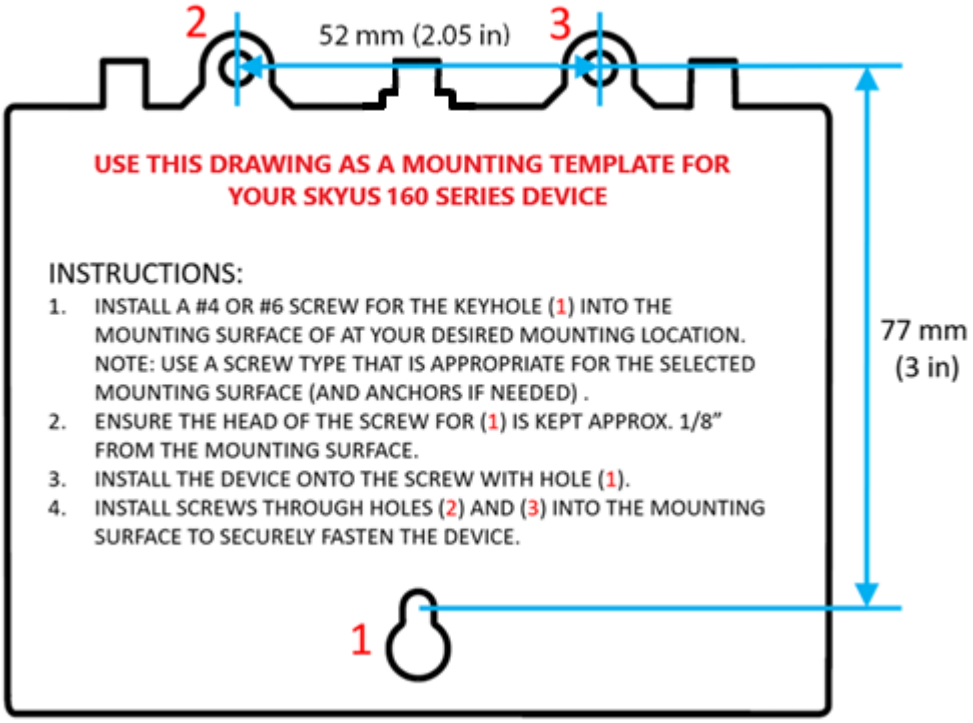
WARNING! While mounting your device, do not apply excessive force to the mounting brackets as this may cause the tabs to fail. Installation is recommended to be completed by a professional.



CAUTION! 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.

To mount your device using screws, follow the directions below, using two #4 or #6 screws.

1. Identify the optimal installation location. Make sure you consider the physical space requirements of the device, any needed connectors, cables, and antennas. In addition, make sure you consider mounting location to optimize cellular coverage.
2. Identify the optimal mounting equipment. Depending on installation location, you may want to select wood screws, metal self-tapping screws, drywall anchors, concrete anchors, or others.
3. Locate and install a screw for Hole 1. Make sure the screw head remains 1/8" (3mm) away from the wall.



4. Install the device onto the screw using Hole 1 and slide the device all the way onto the slot of Hole 1.

5. Install a screw into the mounting surface through Hole 2. Tighten screw to 5 in-lbs. to ensure a snug fit. Take caution to ensure the device will be installed level.

6. Install the final screw into the mounting surface through Hole 3. Tighten screw to 5 in-lbs. to ensure a snug fit.

Powering the Device

You can power your device using an external power source. When a power source is connected, the Skyus 160 Series powers up automatically. When loaded with an active SIM, **it may take up to two minutes** for the device to power up and register on the cellular network.

To power on the device using an external power source:

Connect the device to a power source. This can be a 4 pin connector, USB, or Ethernet (see Connecting your Device on page 17).

The LEDs will all blink white, signaling the device is starting up. When LEDs stabilize with green/yellow/blue/red colors, the device is ready for use. The power button should be green showing the device has sufficient external power.

WARNING! HOT SURFACE DO NOT TOUCH. The antenna connectors and PoE connector may reach hot temperatures during normal use.

Important: Your Skyus 160 Series router has a variety of possible power sources, offering flexible deployment. External power sources include 4-pin AC or DC power, USB, and Power over Ethernet. In addition, your Skyus 160 Series router has a backup battery that allows the router to run without an external power source during power loss. The Skyus 160 Series usually transitions between power sources without interruption to service and connectivity. However, in some cases, removing or adding a power source may cause your Skyus 160 Series router to restart. If a restart is triggered, service is recovered within two to three minutes. **If you require fully uninterrupted service, include a dedicated uninterruptible power supply (UPS) in your power design.**

Using the Backup Battery

The Skyus 160 Series features a rechargeable 3.8 V 4400 mAh 16.7 Wh Li-ion backup battery that provides up to 12 hours* of critical power for alerting during power loss in stationary environments and usage in vehicle environments when the vehicle is off. The battery will charge when connected to any external power source.

NOTE: The backup battery is not designed for primary use.

WARNING! The backup battery will charge when external device temperatures are within 0 – 55° C. Outside of this range, the battery charging circuit will be disabled. Li-ion batteries are not safe to use in environments outside of -20 – 60 C. If it is possible that the device will see temperatures outside of this range, please remove the battery from the device and discontinue use with the battery. Failure to comply with these operating ranges may result in extensive damage to the device and/or the device's surrounding area. If the battery is not needed in your use case or you wish to operate the device outside of this range, please properly store or dispose of the battery according to your local waste management authority.

To power on the device using the backup battery:

1. Press and hold the power button on the front of the device until the LEDs start blinking.



2. The LEDs will all blink white, signaling the device is starting up. When LEDs stabilize with green/yellow/blue/red colors, the device is ready for use. The power button should show blue/yellow/red to indicate battery level status.

* Heavy data usage may lessen battery life.

Connecting your Device

You can connect your Skyus 160 Series device in multiple ways:

- Via Ethernet
- Via USB
- Via Wi-Fi

Connecting via Ethernet

To connect using Ethernet:

1. Connect an Ethernet cable from the device to the host system.
2. Connect the device to a power source.
    - If the host system offers PoE or PoE+, the device can be powered by the host system and pass traffic via Ethernet.
    - If PoE or PoE+ is not available from the host system, the device needs to be powered using the 4 Pin power port.
3. When powered and plugged in, the device should automatically turn on and establish a connection.

Connecting via USB

To connect to a host system using USB:

Using the USB A to USB Micro-B cable, connect the Micro-B side to the Skyus 160 Series router and the A side to the host system.

When plugged in to a USB 2.0 port, the device should automatically turn on and be ready for use in Windows-based (8 or later) or Linux-based (kernel 2.6.32 or later; Ubuntu 14.04 or later) environments.

NOTE: If the device is not connected through a powered USB port, the device can still operate via USB while using the 4 Pin power cable to power the device.

Connecting via Wi-Fi

To connect using Wi-Fi:

1. Ensure the Skyus 160 Series router is powered on.
2. Connect to the router using the SSID and Password information provided on the label on the bottom of the router.

3. It is strongly recommended to change the SSID and Password from the default for security reasons after initial use. Make sure to save the updated information in a secure location.

Connecting to the Web UI

On the device connected to your Skyus 160 Series router, open any web browser and go to http://my.skyus/ or http://192.168.1.1.

Select **Sign In** (in the top-right corner of the screen), and enter the password printed on the bottom of your router.

Connecting External Sensors via Bluetooth

To connect external sensors via Bluetooth:

1. In the Web UI, select **Bluetooth Sensors** from the side menu.
2. Turn the **ON/OFF** slider to **ON**. Bluetooth scanning starts immediately.
3. When scanning is complete, the **Available Sensors** section lists all of the available Bluetooth sensors. Select the device you wish to pair and click the **Pair** button.

NOTE: See Bluetooth Sensors on page 94 for supported sensors.

Resetting your Router

You can restart your Skyus 160 Series router, or restore settings to the factory defaults. You can do this using the Web UI at **Settings > Backup and Restore**, or by clicking the Sign Out drop-down in the top-right corner of any Web Interface page and selecting **Restart**.

Alternately, you can use the **RESET** button on the device, 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. Use a small pointed object, such as a paperclip, to push the RESET Button.

To restart the router: Press the **RESET** button quickly (less than one second). This turns your router off and on again and does not affect settings.

To restore the router to factory default settings: Press and hold the **RESET** button for three seconds or longer. This resets all settings to their factory default values.

CAUTION! This initiates a restart and may change the current Wi-Fi settings, breaking all existing connections to this router and disconnecting you from the Web UI.

Getting Support

Documentation for your Skyus 160 Series router is available online. Go to www.inseego.com/support-documentation.

For additional information and technical support, email Technical Support at technicalsupportus@inseego.com or call Customer Support (Toll Free) at **1-877-698-6481**.

3

Software Configuration

Overview

Managing Bluetooth Sensors

Managing Connected Devices

Configuring GPS

Managing Settings

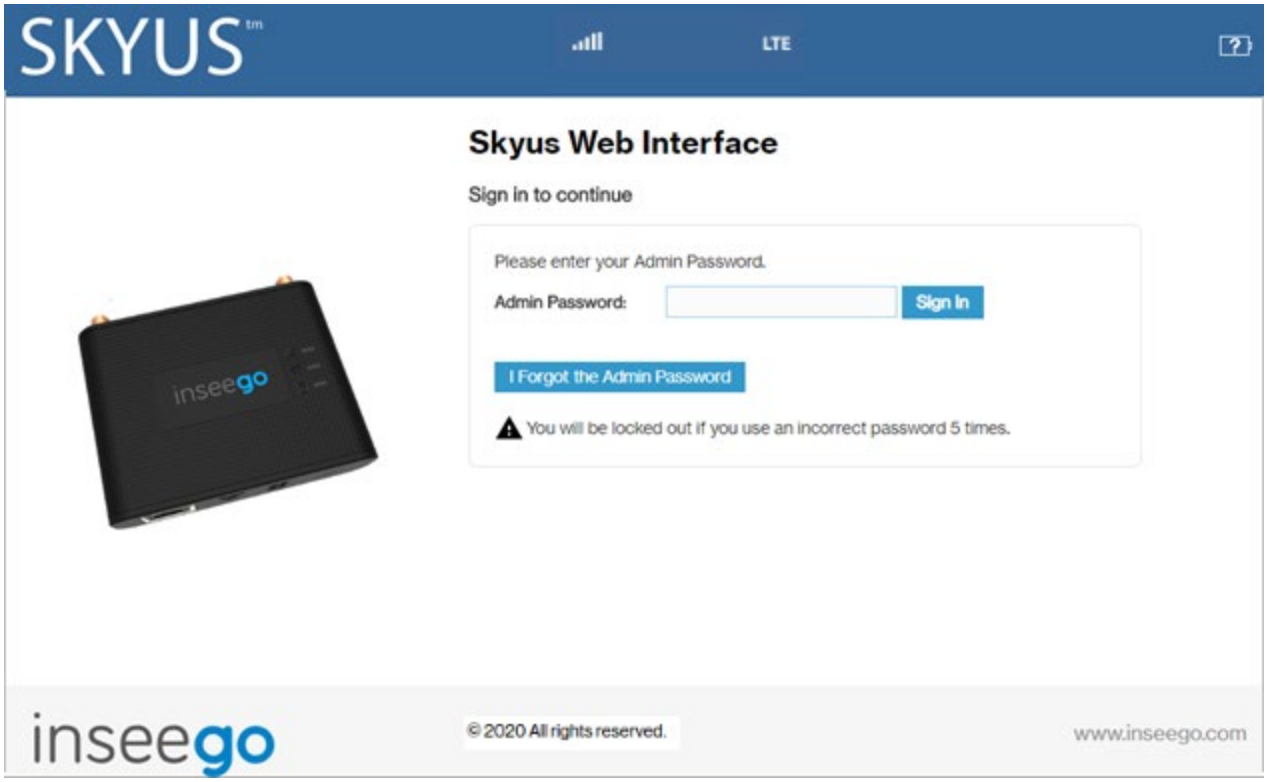
Accessing Messages

Viewing Info About the Router

Overview

Logging In

1. On the device connected to your Skyus 160 Series router, open any web browser and go to http://my.skyus/ or http://192.168.1.1.



2. Enter the Admin password. By default, this is the password printed on the label on the bottom of the router. The Home page appears.

NOTE: You can set up a separate Wi-Fi password in **Settings > Wi-Fi Hotspot** (see Wi-Fi Hotspot Tab), but that is different from the Admin password, which is for this Web Interface.

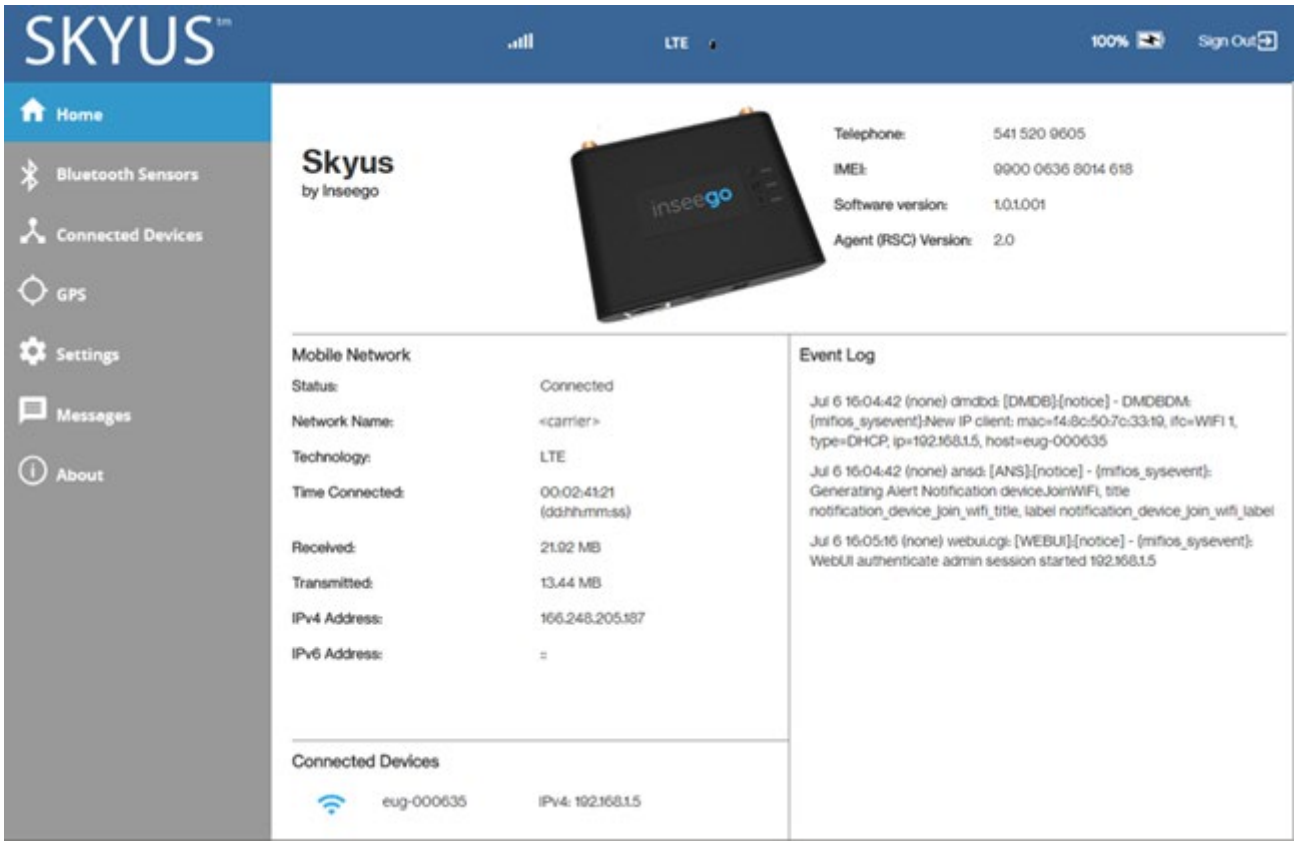
Important: It is critical that you change the Admin password from the default to keep the device and your network secure. To change the Admin password, go to **Settings > Device > Admin Password**, see Admin Password Sub Tab on page 37.

Home Page

The Skyus 160 Series Home page is the local gateway to configuring and managing your router. It displays current router and mobile network status, lists currently connected devices, provides an event log, and offers links to other pages with option settings.

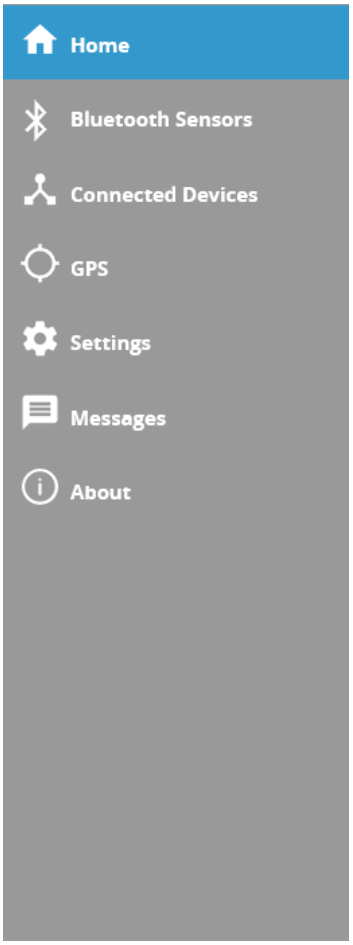
After logging in, you will automatically be taken to the Home page.

From any other page, click on the Home icon from the navigation pane on the left of the screen to return to the Home page.



Side Menu

Each page in the Skyus 160 Series Web Interface includes a menu on the left, which you can use to return to the Home page or jump to other screens. The current screen is indicated by a blue bar.



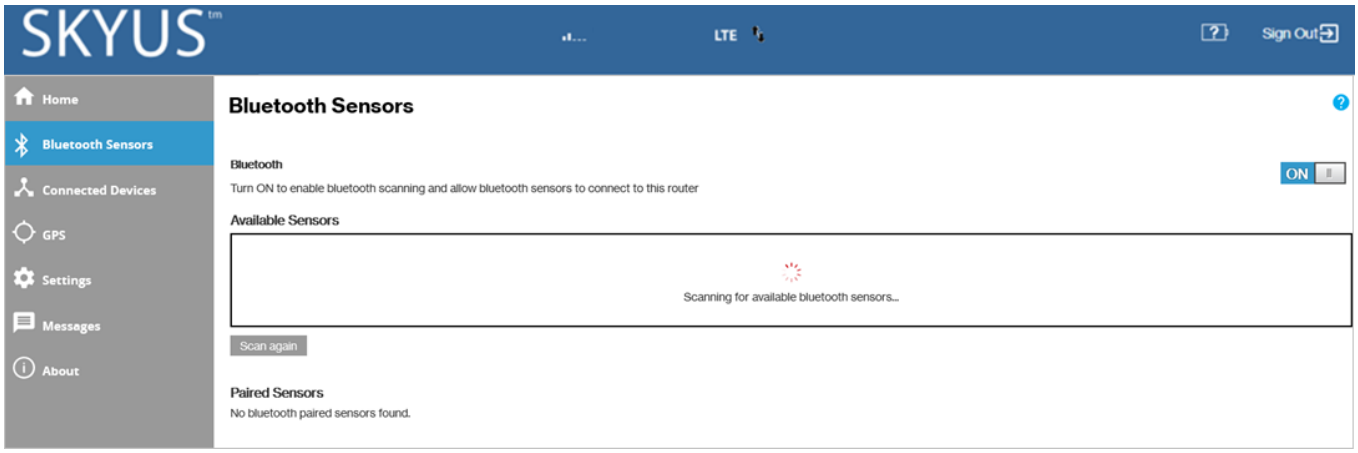
Getting Help

Select the question mark (?) in the upper right hand corner of a topic page to view Help on that topic.

Managing Bluetooth Sensors

To manage Bluetooth sensors, select **Bluetooth Sensors** from the Web UI side menu. The Bluetooth Sensors page appears.

NOTE: This feature is only available for Bluetooth enabled models. See Bluetooth Sensors on page 94 for supported sensors.



Bluetooth Sensors Page

Use this page to enable Bluetooth scanning and allow Bluetooth sensors to connect to your Skyus 160 Series router.

Bluetooth

Use the **ON/OFF** slider to enable or disable Bluetooth. Details in the Bluetooth page are hidden when turned off; all details are displayed when turned on. Bluetooth scanning starts immediately when turned on.

Available Sensors

When scanning is complete, this section lists all of the available Bluetooth sensors.

Select the device you wish to pair and select **Pair**.

You can select **Scan again** to restart the scan for available sensors. It may take a few seconds to complete the scan and update the available sensors list.

Paired Sensors

Lists all of the Bluetooth sensors that are paired with your Skyus device.

Use the **View** button view the following details of paired sensors.

Name: The name of the sensor.

Serial Number: The serial number of the sensor.

Model: The model number of the sensor.

Type: The type of sensor.

Battery: The battery charge level of the sensor.

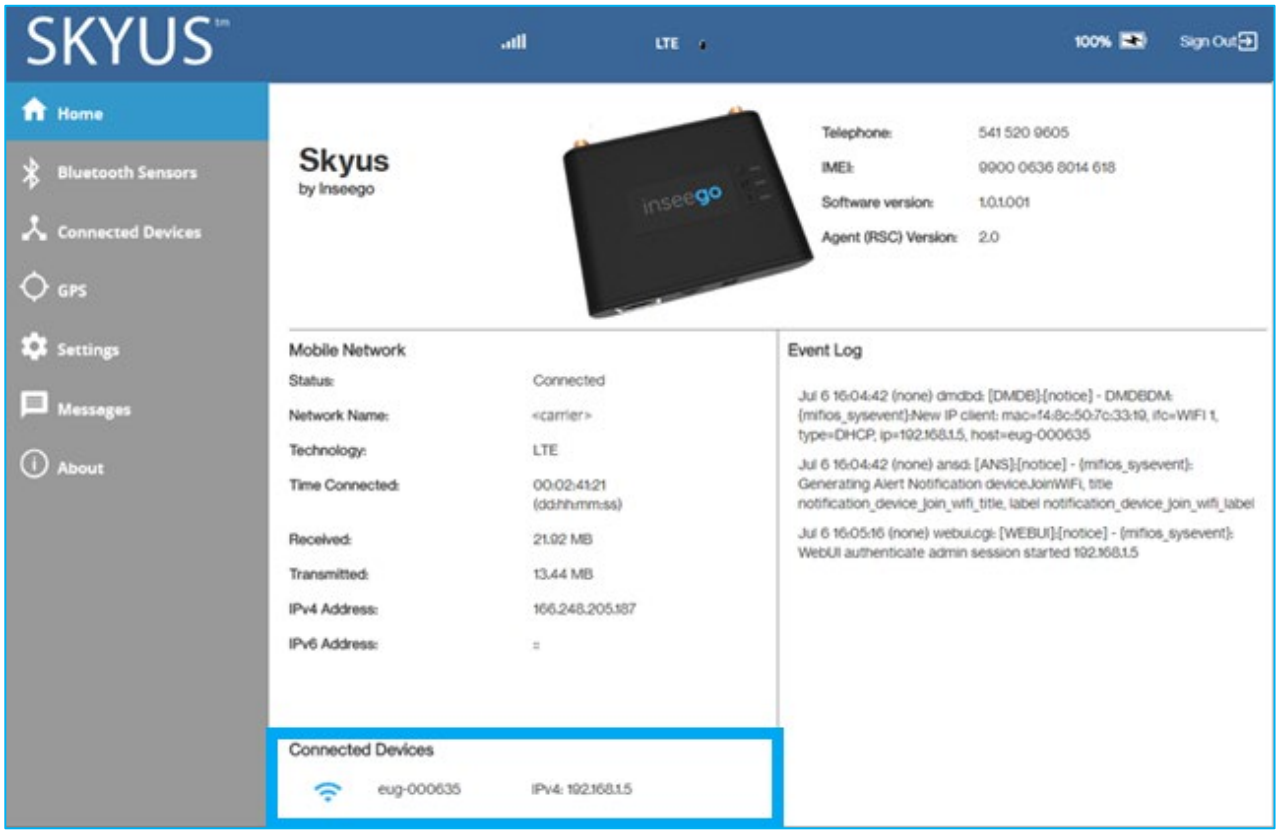
Signal Strength: The signal strength of the sensor.

Use the **Edit** button to update editable details of paired sensors, such as Name and Type, and to set alarms visible in Inseego Connect.

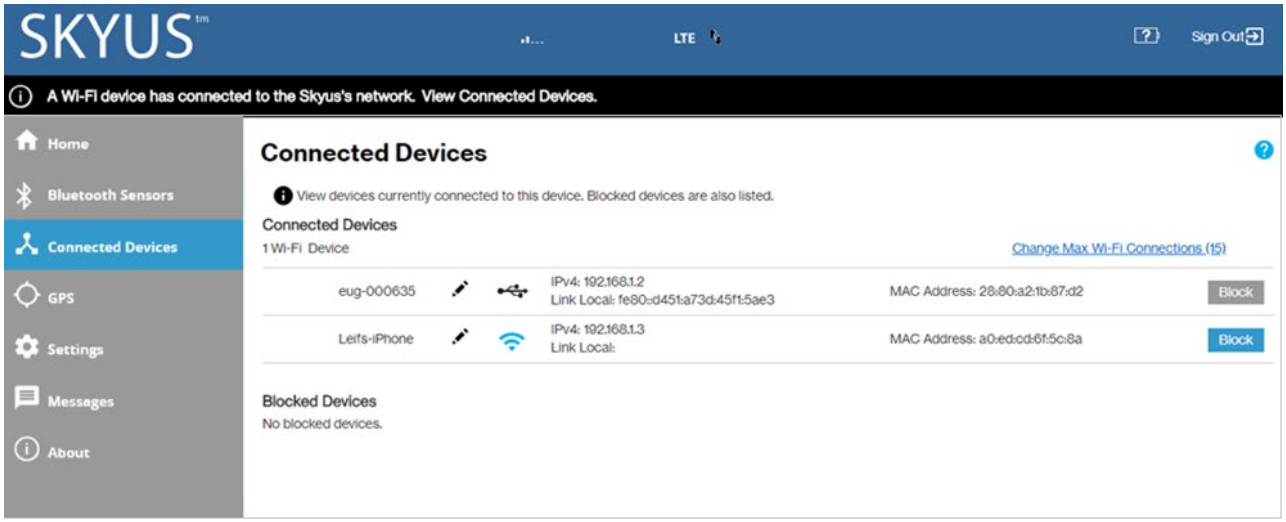
Use the **Unpair** button to unpair the sensor from your Skyus device.

Managing Connected Devices

On the Web UI Home page, the Connected Devices section lists all devices currently connected to your Skyus 160 Series router, along with the connection type they are using and their IP Address.



To manage connected devices, select **Connected Devices** from the Web UI side menu. The Connected Devices page appears.



Connected Devices Page

This page provides details about each device connected to the Skyus 160 Series and allows you to edit how device names appear in the Web UI. You can also block or unblock a device from Internet access.

Connected Devices

This table lists all devices connected to the Skyus 160 Series:

Device: This is usually the hostname set on the connected device. In rare cases, the hostname may be unavailable.

Edit: Click on the Edit icon to change the name of a device as it appears in the Skyus 160 Series Web UI. **NOTE:** This only changes the how the device name appears in the Web UI.

Connection: An icon indicates the connection type (Wi-Fi, Ethernet, USB, or Bluetooth) for each device. (You can hover over the icon to read the type of connection.)

IPv4: The IP address of the connected device.

Link Local: The Link-Local IPv6 address if the connected device supports IPv6.

MAC Address: The MAC Address (unique network identifier for this connected device).

Block: Select this box to disconnect a device and prevent it from reconnecting. Select **Save Changes**. The device is removed from the **Connected Devices** list and appears in the **Blocked Devices** list below.

NOTE: The Block option is available for each device connected through Wi-Fi, but is not available for your own device or devices connected via Ethernet.

Change MAX Wi-Fi Connections: This link takes you to **Settings > Wi-Fi Hotspot** where you can change the number of connections that can use Wi-Fi.

Blocked Devices

This section lists all devices blocked from connecting to the Skyus 160 Series router.

NOTE: Since blocked devices are not currently connected, they do not have an IP address. Instead, they are identified by their name and MAC address.

To unblock a blocked device, click the **Unblock** button and select **Save Changes**. The device is removed from the **Blocked Devices** list and appears in the **Connected Devices** list above.

Configuring GPS

The Skyus 160 Series router incorporates a GPS receiver. The GPS receiver can determine your current location, often even indoors. Current location information can be shared with connected devices by using the Local Streaming feature on the Local tab.

NOTE: To use GPS, a GPS antenna must be connected.

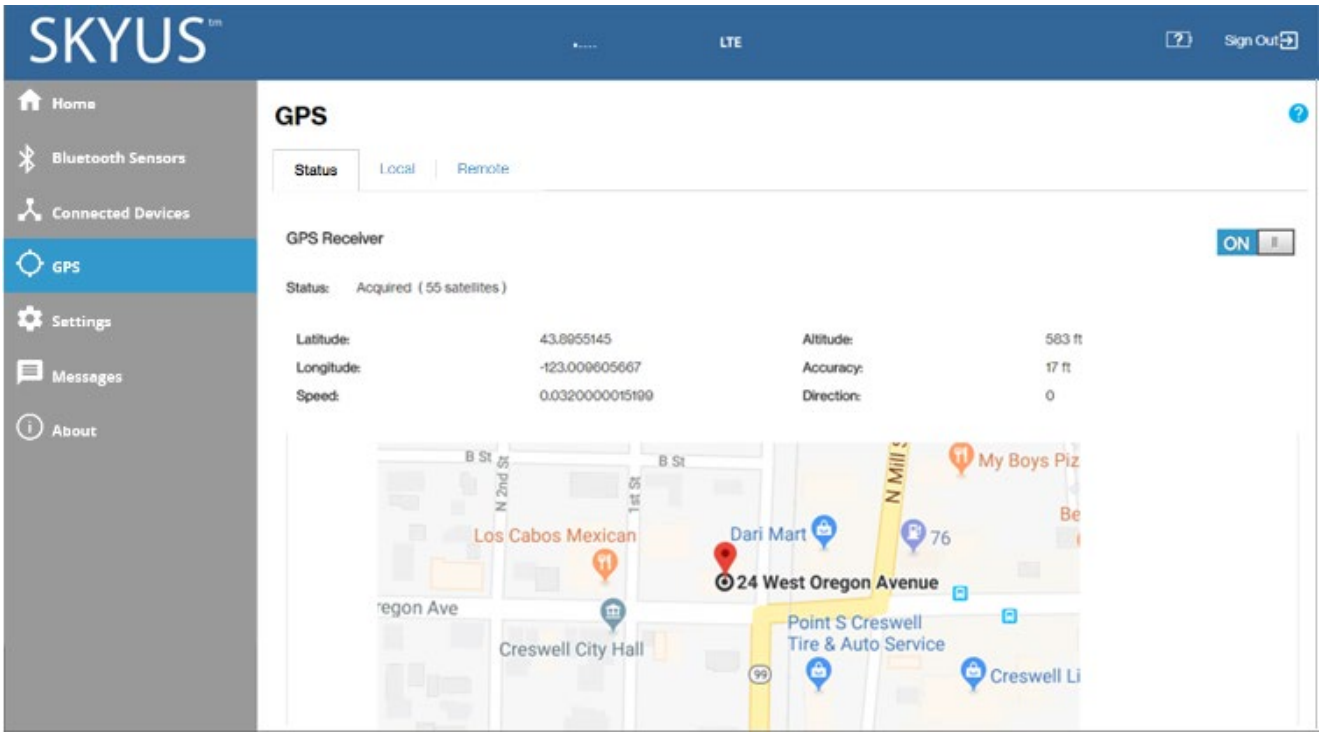
To configure GPS, select **GPS** from the Web UI side menu.

The GPS page includes three tabs:

- Status
- Local
- Remote

Status Tab

Use settings on this tab to enable or disable GPS and to view current location and the current status of your GPS connection.



GPS Receiver

This setting enables or disables the GPS radio on your device. When the **ON/OFF** slider is **ON**, the device acquires GPS and makes the data available to applications running on the device. A GPS Agreement appears, click **Confirm** to proceed. When **OFF**, no GPS data is available.

NOTE: For fixed location models (SK160XXX- ACR), the GPS will be **OFF** by default. For mobile location models (SK160XXX- DCR), GPS will be **ON** by default.

When turning on the GPS for the first time, it may take up to several minutes to acquire a signal lock.

Status

The current status of your GPS connection. If the GPS receiver has not yet obtained a fix (location), a Searching status appears. When searching, the device is making the connection to satellites in order to populate GPS data. Once a fix has been obtained, the following information is displayed and a Google map appears to visually indicate the current location.

Latitude: Latitude for the last location fix.

Longitude: Longitude for the last location fix.

Speed: Speed the device is traveling at.

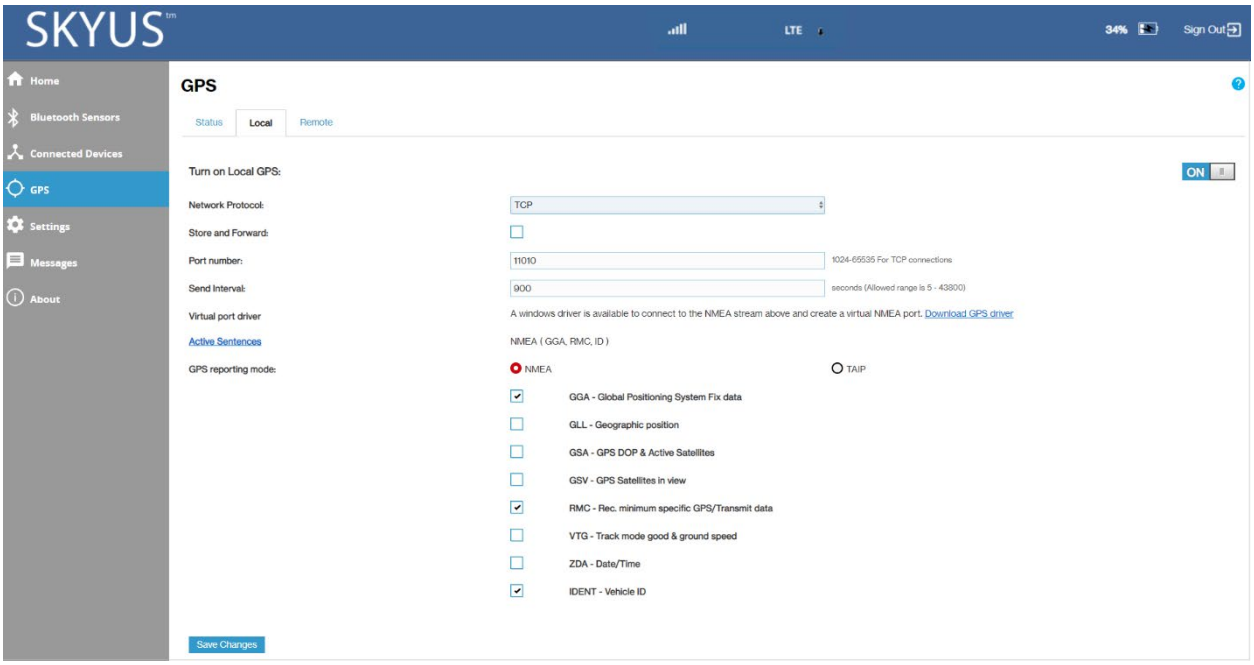
Altitude: Altitude for the last location fix.

Accuracy: A measure of the accuracy of the horizontal position obtained by the GPS receiver.

Direction: Direction the device is traveling relative to North.

Local Tab

Use this tab to enable GPS streaming to client devices on the local network. Raw GPS data is provided by the Skyus 160 Series in the form of a National Marine Electronics Association (NMEA) text stream. You can use third-party applications to utilize or forward the GPS data to a remote server.



Turn on Local GPS: Check this box to turn on GPS streaming on the local network.

Network Protocol: Select the protocol to use for local GPS streaming from the drop-down (**TCP** or **UDP**).

- **Store and Forward:** If there is an interruption in the WAN interface, the system can store packets and forward them once the WAN interface connection returns. If you select **TCP** as the Network Protocol, you can check the Store and Forward box if you want the system to store and forward packets.
- **IP Address:** If you select **UDP** as the Network Protocol, the IP Address field appears.

Port number: The TCP port number used by the software on your computer to establish a connection to your Skyus 160 Series router and obtain GPS data. Unless there is a good reason to do so, you should not change the port number. Acceptable TCP port values are between 1024 and 65535.

Send Interval: You can set a time interval for reporting frequency. For example, if you select 900 seconds, a GPS packet is sent every 15 minutes.

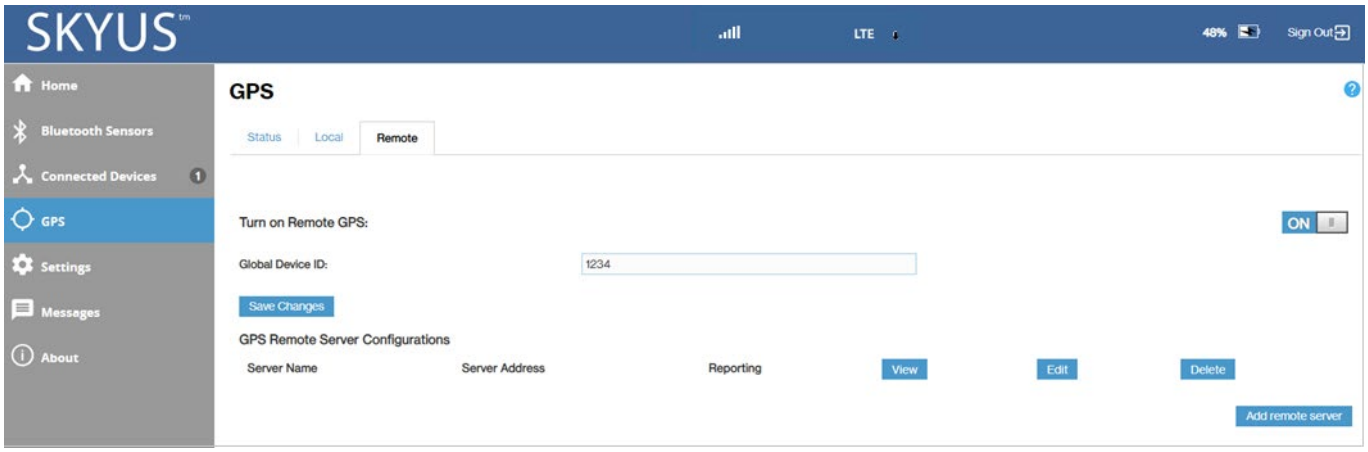
Virtual port driver: If you want to access the GPS data stream from a virtual COM port instead of the TCP port (above), click the **Download GPS driver** link to download and install a GPS driver for your Windows platform. This driver creates a virtual NMEA port, obtains GPS data from the Skyus 160 Series router, and makes this GPS data available to NMEA-aware third-party applications.

GPS reporting mode: The Skyus 160 Series router is capable of routing NMEA or TAIP sentences to the local server. Select **NMEA** or **TAIP**. The available options for your selection are displayed in **Active Sentences**. Select or de-select any option. All options that are checked will be part of the packet routed to the local server.

Click **Save Changes** to update settings.

Remote Tab

Use this tab to configure the system to stream GPS data to remote servers. **NOTE:** These servers are not Inseego Connect. Use **Settings > Advanced > Inseego Connect** to enable Inseego Connect remote servers.

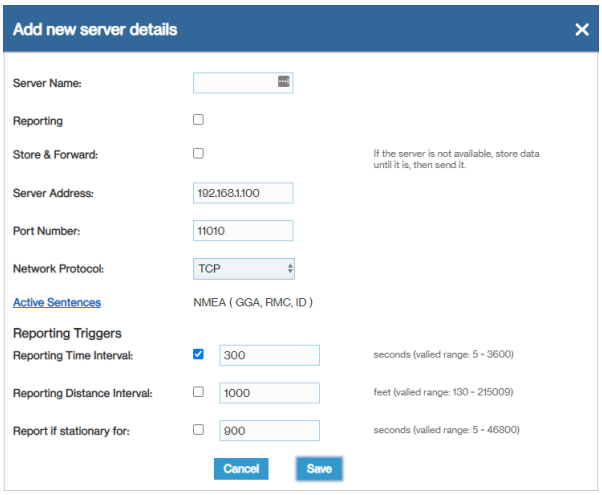


Turn on Remote GPS: Check this box to turn on GPS streaming to remote servers.

Global Device ID: The 4-digit unique ID specific to your Skyus 160 Series router that is inserted into your GPS packet for routing to remote servers.

GPS Remote Server Configurations

Add remote server: Use this button to add a remote server. The **Add new server details** dialog appears.



- **Server Name** — Enter a name for the GPS remote server.
- **Reporting** — To begin streaming GPS data from your Skyus 160 Series router to this remote server, check this box.
- **Store & Forward** — If there is an interruption in the WAN interface, the system can store packets and forward them once the WAN interface connection returns. Check this box if you want the system to store and forward packets.
- **Server Address** — Enter the address for the remote server to which you would like to route packets.
- **Port Number** — Enter the port for the remote server to which you would like to route packets. Acceptable port values are between 1024 and 65535.
- **Network Protocol** — Select the protocol to use for routing packets to your remote serve from the drop-down (TCP or UDP).
- **Active Sentences** — The Skyus 160 Series router is capable of routing NMEA or TAIP sentences to remote servers. Click the link to select NMEA or TAIP and the available options. All options that are selected will be part of the packet routed to the remote server.

Reporting Triggers

- **Reporting Time interval** — You can set a time interval to trigger when packets will be routed to the remote server. For example, if you select 900 seconds, a GPS packet will be sent to the remote server every 15 minutes.

- **Reporting Distance interval** — You can set a distance interval to trigger when packets will be routed to the remote server. For example, if you select 1000 feet, a GPS packet will be sent to the remote server every time your device moves 1000 feet.

  NOTE: You can choose both Time and Distance as your interval specification. The device will route packets based on which event occurs first.

- **Report if stationary for** — You can set a stationary timer that monitors for movement and only route packets if the device is continuously moving within the time range. For example, if you set this value to 60 seconds and the device has not moved within 60 seconds, a packet will not be routed. Once your device begins registering GPS movement again, packet routing will resume. **NOTE:** The stationary timer minimum is constrained by the Reporting Time Interval. You cannot have a stationary timer value that is less than the Reporting Time Interval.

Click **Save** to implement your settings or **Cancel** to cancel. You return to the Remote page. The new remote server is now listed under GPS Remote Server Configurations.

Use the **View**, **Edit**, and **Delete** buttons to view, edit, or delete listed remote servers.

Managing Settings

To change system settings, select **Settings** from the Web UI side menu.

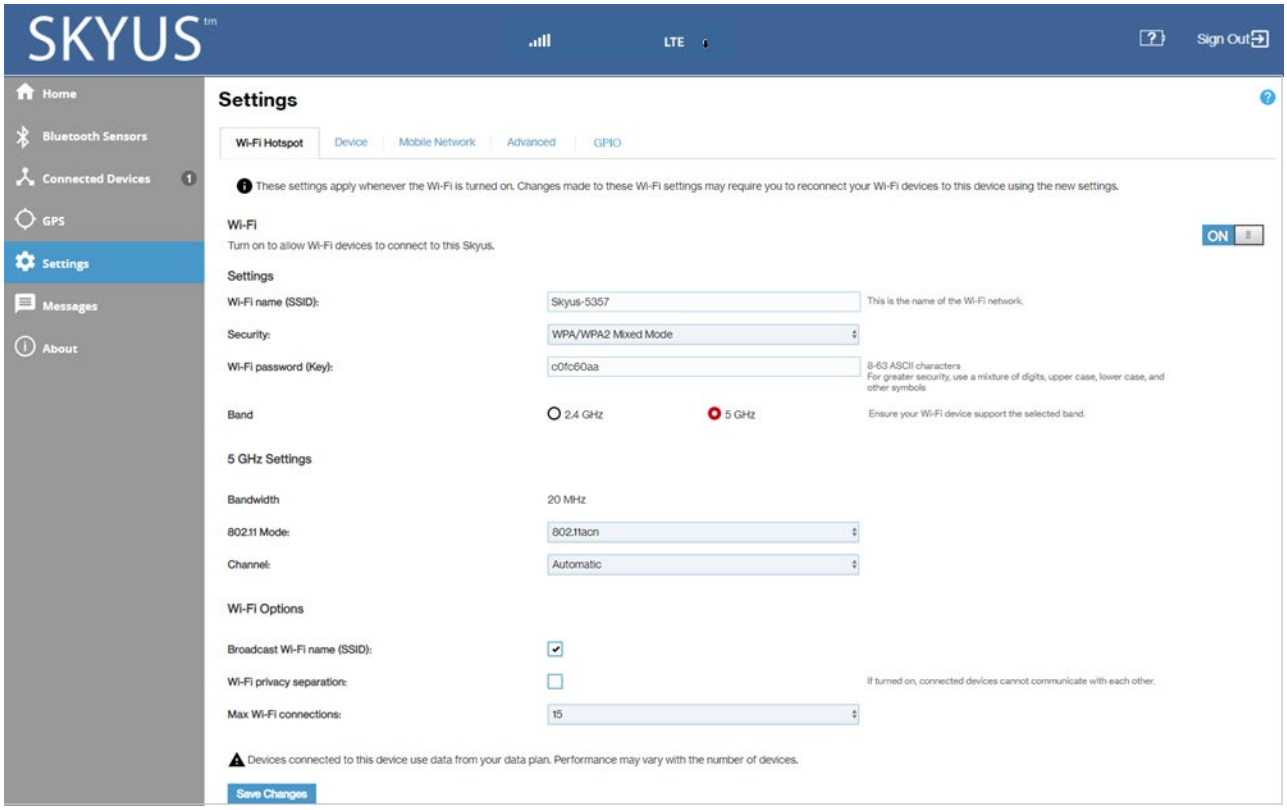
Use the Settings pages to configure and program your device. When you are done configuring your device, you can save your current settings as a template for future use to back up your device if needed.

The Settings page includes five tabs:

- Wi-Fi Hotspot
- Device
- Mobile Network
- Advanced
- GPIO

Wi-Fi Hotspot Tab

Use this tab to adjust the Wi-Fi settings for your device. Connected devices must use the Wi-Fi settings shown on this screen.



NOTE: If you change these settings, existing connected devices may lose their connection.

Wi-Fi

Use the **ON/OFF** slider to allow Wi-Fi devices to connect to this router, or not.

Settings

Wi-Fi name (SSID): Enter a Wi-Fi name (SSID) to set up or change the Wi-Fi name. The name can be up to 28 characters long.

Security: Select an option for Wi-Fi security:

- **WPA2 Personal PSK (AES)** can be used for WPA2 devices.
- **WPA/WPA2 Mixed Mode** can be used if some of your older devices do not support WPA2.
- **None** allows others to monitor your Wi-Fi traffic and use your data plan to access the Internet. **NOTE:** Avoid using this option.

Wi-Fi password (Key): Enter a Wi-Fi password.

Important: It is critical that you change the password from the default ***and*** use a different password from your Admin password to keep the device and your network secure.

Band: Wi-Fi can be accessed over two bands, depending on your Wi-Fi device: 2.4 GHz and 5 GHz:

- The 2.4 GHz band is supported by all devices with Wi-Fi and should be used by devices that are a few years old or older. This band passes through walls better and propagates over longer distances, so it may have a longer range.
- The 5 GHz band is best for newer devices. It offers better throughput, reduced interference and faster data speeds, but does not pass through walls as well as the 2.4 GHz band.

2.4 GHz Settings

802.11 Mode: Displays which 802.11 protocol is used when the 2.4 GHz band is active.

Channel: Select **Automatic** or specify a Wi-Fi channel to use. **NOTE:** Selecting the appropriate channel will help reduce signal loss when near another Wi-Fi device.

5 GHz Settings

Bandwidth: The bandwidth when 5 GHz band is active.

NOTE: Leave the Bandwidth at the default setting unless you experience interference with other Wi-Fi devices. If you experience interference, try lowering the Bandwidth setting to reduce the interference.

802.11 Mode: Specify which 802.11 protocol is to be used when the 5 GHz band is active.

Channel: Select **Automatic** or specify a Wi-Fi channel to use. **NOTE:** Selecting the appropriate channel will help reduce signal loss when near another Wi-Fi device.

Wi-Fi Options

Broadcast Wi-Fi name (SSID): Check this box to allow Wi-Fi devices in the area to see the Wi-Fi name (SSID) on their list of available networks. If not selected, the Wi-Fi name will need to be manually entered for devices to connect to the network.

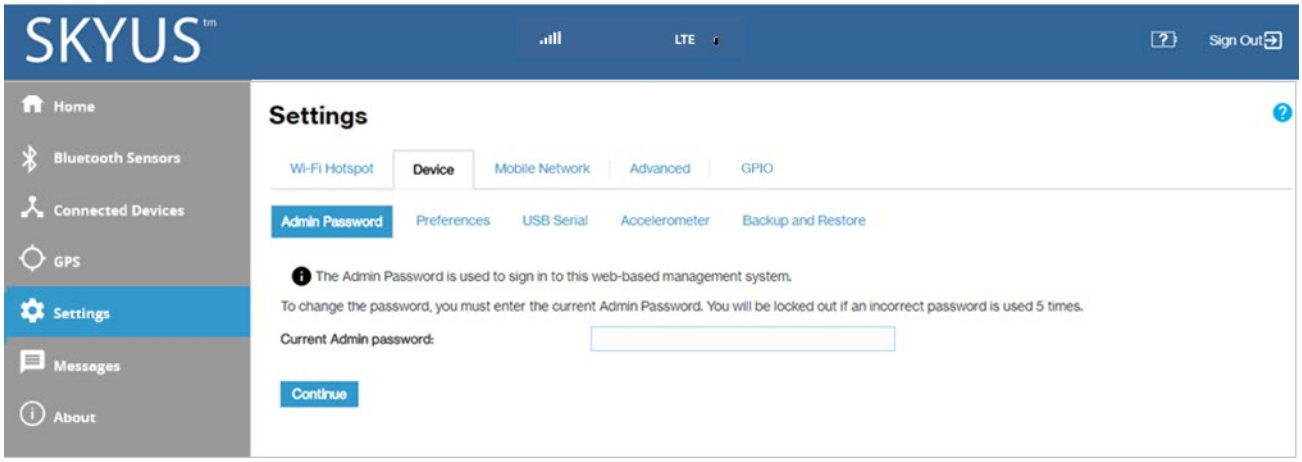
Wi-Fi privacy separation: Check this box to prevent Wi-Fi data transfer between devices. For normal operation, this should be unchecked. If checked, each connected device is isolated from all other connected devices. This provides additional security if some connected devices are unknown or not completely trusted.

Max Wi-Fi connections: Specify the number of connections that can simultaneously connect to the Skyus Wi-Fi network.

Select **Save Changes** to store new settings.

Device Tab

Use this tab to configure device-specific settings, including resetting the Admin password for your device.



The Device tab includes five sub tabs:

- Admin Password
- Preferences
- USB Serial
- Accelerometer
- Backup and Restore

Admin Password Sub Tab

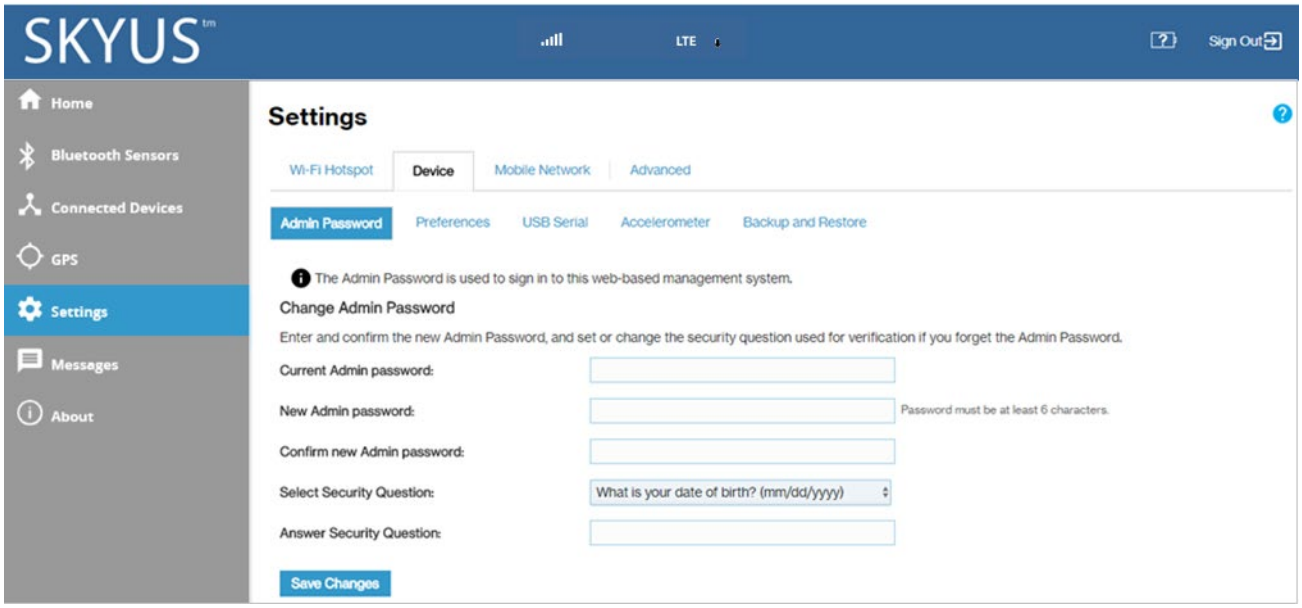
This page allows you to change the Admin Password and to set security options related to the Admin Password. The Admin Password is used to sign in to the Skyus 160 Series Web Interface.

Important: It is critical that you change the Admin password from the default to keep the device and your network secure.

To change your Admin password:

1. Enter the Current Admin password and click **Continue**. The Admin Password sub tab appears.

   NOTE: If you enter an incorrect value too many times, you will be locked out of the Admin Web Interface. To clear this lock, restart your Skyus device.



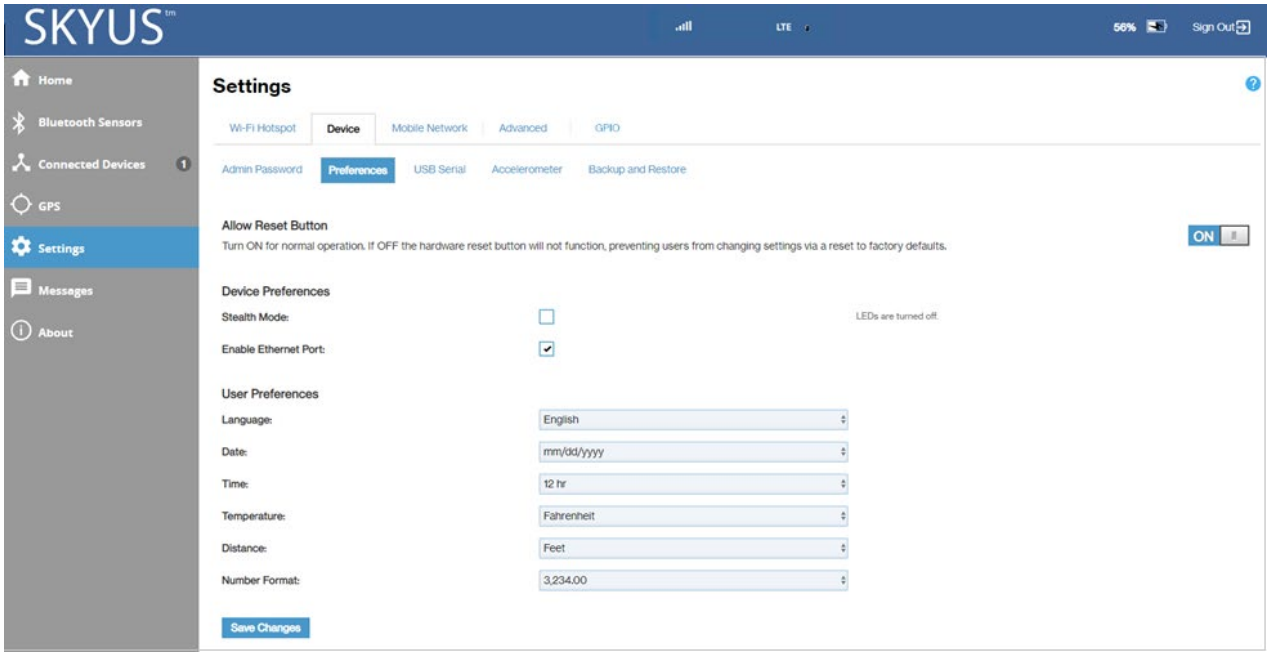
2. Enter your current Admin password again, then enter a new password and confirm it.
3. Select a security question from the drop-down list and type an answer to the question in the **Answer Security Question** field. **NOTE:** Answers are case-sensitive.
4. Click **Save Changes**.

The next time you sign in to the Skyus 160 Series Web Interface, use the new Admin password. If you cannot remember the password, click **I forgot the Admin password**. After you correctly answer the security question you set up, the current password is displayed.

NOTE: You can set up a separate Wi-Fi password in **Settings > Wi-Fi Hotspot** (see Wi-Fi Hotspot Tab), but that is different from the Admin password, which is for this Web Interface. DO NOT use the same password for both.

Preferences Sub Tab

Use this page to turn off the hardware reset button, enable/disable LEDs and the Ethernet Port, and set user preferences such as language and date/time formats.



Use the **Allow Reset Button ON/OFF** slider to turn off the hardware reset button. This ensures that device settings cannot be reset to factory default by using the reset button on the bottom of the router.

Device Preferences

Stealth Mode: Check this box to turn off the indicator LEDs on the router.

Enable Ethernet Port: This box is checked when the Ethernet port is enabled. Deselect to disable the Ethernet port on your router.

User Preferences

Language: Only English is available currently.

Date: Select the date format to be used on the Web Interface (mm/dd/yyyy or dd/mm/yyyy).

Time: Select the time format to be used on the Web Interface (12 or 24 hour).

Temperature: Select the temperature format to be used on the Web Interface (Fahrenheit or Celsius).

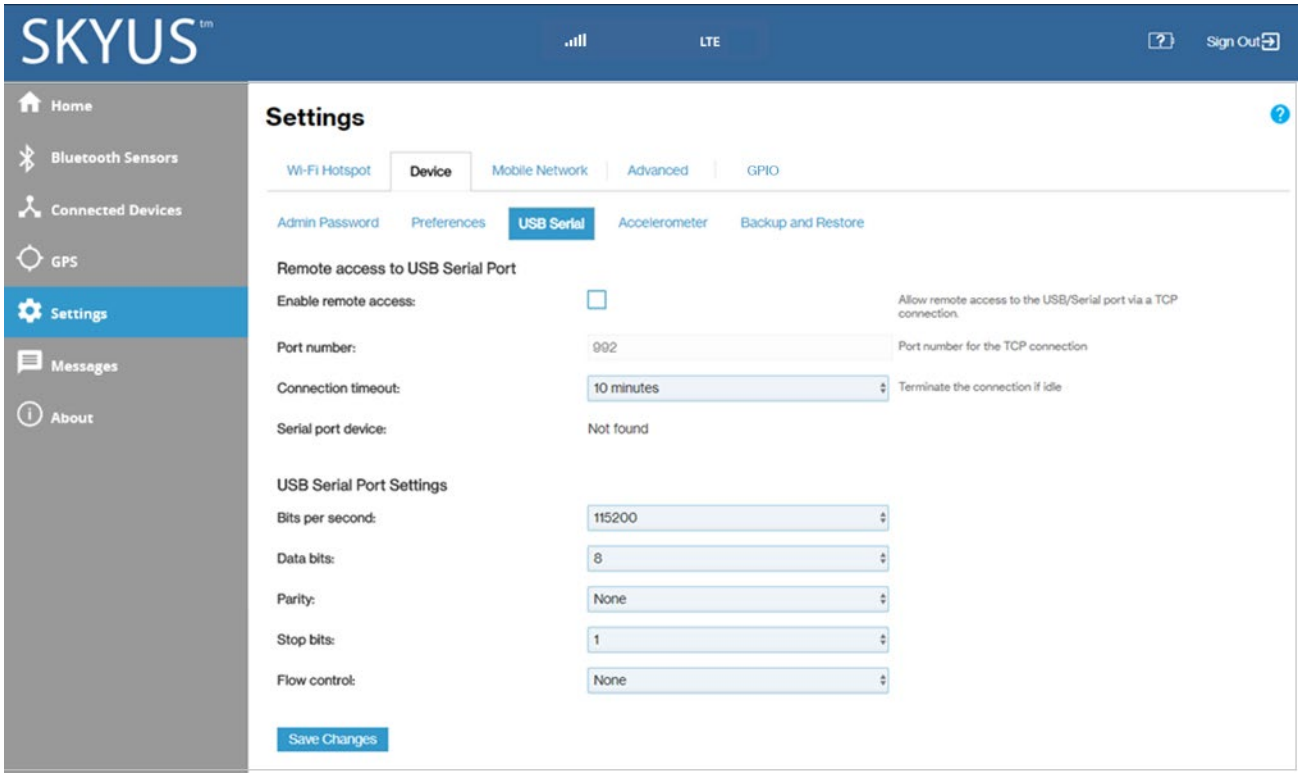
Distance: Choose the units of measure for distance on the Web Interface (Feet or Meters).

Number Format: Choose the format for decimal numbers (using a period or comma as the decimal point).

Select your display choices and click **Save Changes** to update settings.

USB Serial Sub Tab

If you have connected a USB/serial port adaptor and a serial port device to the Skyus router, you can use this page to remotely access the serial port device.



Remote access to USB Serial Port

Check the **Enable remote access** box to enable the remote TCP connection to the device's USB/serial port. You can use Telnet or a similar application to establish this connection.

NOTE: You cannot make changes to the following fields unless this box is checked.

Port number: Specify the desired port to establish the TCP connection.

Connection timeout: Specify the amount of idle time at which the connection will be automatically terminated. If you do not want the connection to be terminated by the Skyus router, select **Never**.

Serial port device: The connected serial port device.

USB Serial Port Settings

Serial port settings should be set to match the connected serial device.

Bits per second: Specify the rate of data flow. Supported speeds range from 300 bps to 115200 bps.

Data bits: Select 7 or 8 to match the serial device.

Parity: Select Odd, Even, or None to match the serial device.

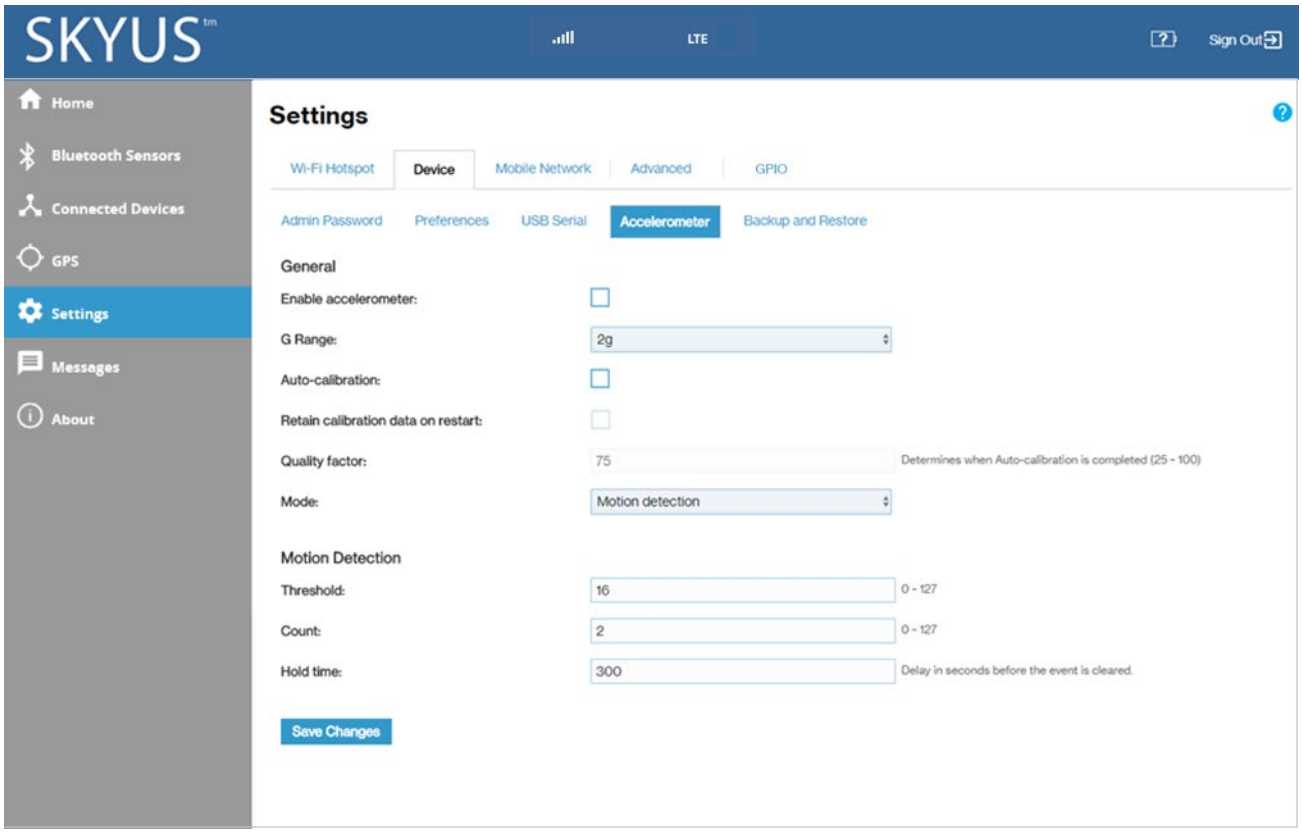
Stop bits: Select 1 or 2 stop bits to end a packet, as used by the serial device.

Flow control: Select the option of how the packets will be controlled used by the serial device: None, XON/XOFF, Hardware.

Select your choices and click **Save Changes** to update settings.

Accelerometer Sub Tab

Use this page to enable and configure accelerometer settings. Accelerometer settings are typically used in mobile (automotive) environments. Settings can be used to drive actions in Inseego Connect.



General

Check the **Enable accelerometer** box to turn on the accelerometer.

NOTE: The following settings apply regardless of the mode selected (Motion detection or Driver behavior).

G Range: Specify the gravity (G) force range. This is the maximum value that can be recorded accurately. The wider the range, the less accurate the readings will be. The default value is 2g, which is sufficient for normal vehicles. A value above 2g indicates a crash.

Check the **Auto-calibration** box to enable auto-calibration. **NOTE:** It is recommended to always check this box if the accelerometer is going to be used.

Retain calibration data on restart: When this box is checked, the device automatically re-calibrates on restart. Use this feature if the Skyus device is in a fixed location in a vehicle. In that case, it will allow the accelerometer to perform auto-calibration faster. In other settings it should remain turned off.

Quality factor: Specifies the accuracy of calibration needed prior to completion of the calibration process. **NOTE:** This is similar to a % confidence level for auto-calibration. If set to 75, then calibration is considered complete when the device calculates that there is a 75% probability that is correct. Values below 25% are not allowed because the results would be unreliable. A higher number will enable a more accurate calibration, but it will take longer to complete the calibration process.

Mode: Choose between Motion detection and Driver behavior. The selections below will change depending on your choice.

Motion Detection

Motion detection detects, monitors, and reports only for bulk movements that will show that the device is moving or not. This mode is generally used when the Skyus device is installed in machinery or a vehicle that should not move, so as to cause an alert if motion is detected.

Threshold: The G force that triggers a motion event. Count and Hold time settings are used to ensure the motion event is genuine.

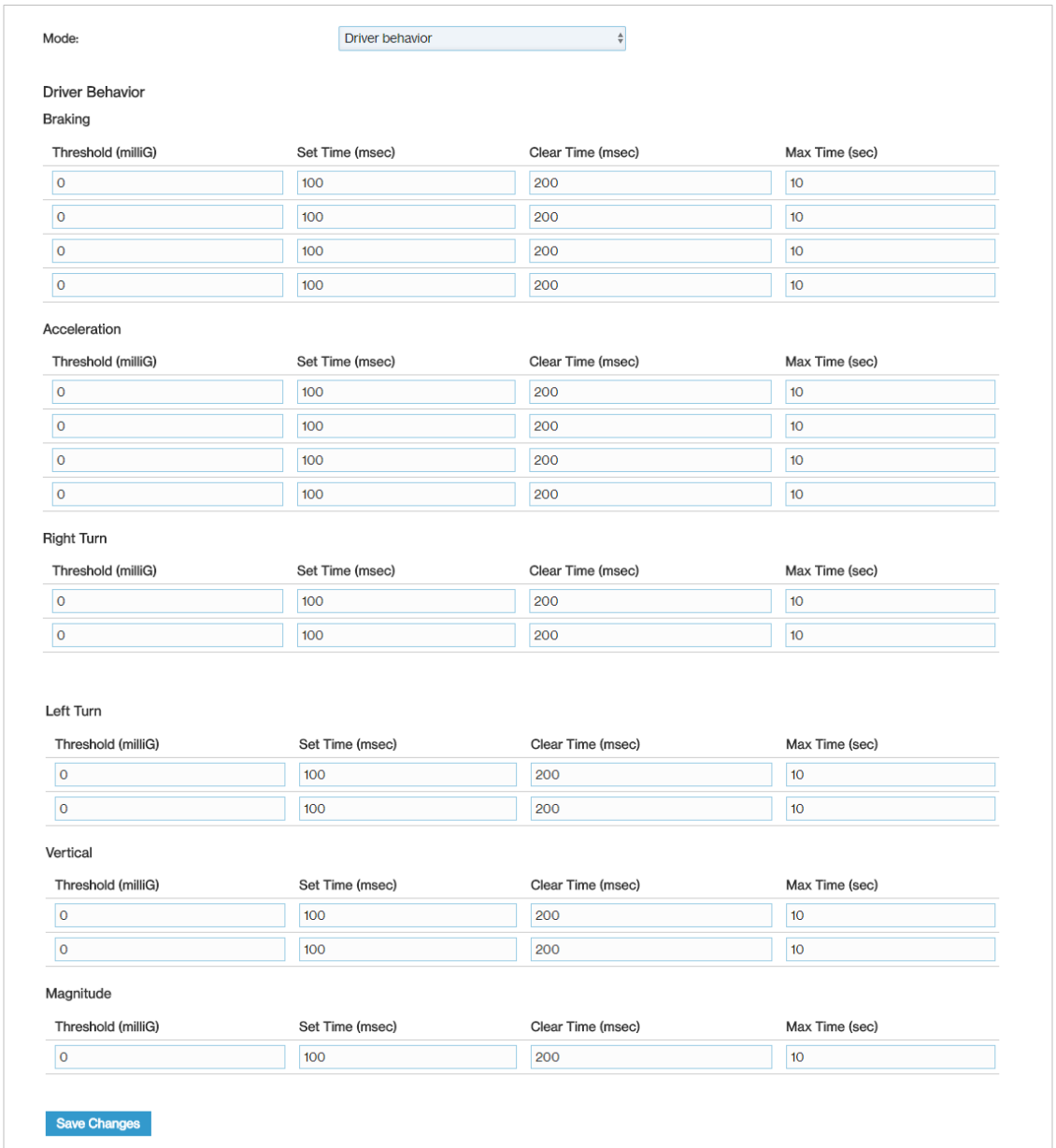
Count: The number of consecutive samples above the Threshold (G force) needed to trigger a motion event. For example, if Count is set to 100 and there are 98 consecutive samples above the Threshold value, then one sample below the Threshold, the count restarts at 0 and no motion event is triggered. **NOTE:** The sampling rate is 10 Hz (10 samples per second). You can convert the Count value to a time interval (in seconds) by dividing the Count value by 10.

Hold time: The delay, in seconds, before a motion event is cleared. The accelerometer waits for this amount of time to determine if the event is finished. If additional readings above the Threshold value are received during the Hold time interval, they are considered part of the same event and the Hold time timer is restarted. When no additional readings above the Threshold value are received for a period equal to the Hold time, the event is considered finished.

Click **Save Changes**.

Driver Behavior Detection

Driver behavior detects and monitors motion, direction, rates, and accelerations to provide information related to driver behavior. This mode is used when the Skyus device is installed in a vehicle and you wish to monitor vehicle operation.



If you select **Driver behavior** as the **Mode**, configure the fields for Braking, Acceleration, Right Turn, Left Turn, Vertical, and Magnitude (a change in any direction). You can specify a Threshold for each of the behaviors that will trigger an event (can be used to create alarms through Inseego Connect). You can also define Set Time, Clear Time, and Max Time.

NOTE: Auto-calibration must be enabled for the Skyus device to determine which direction is forward, so that vehicle motion can be measured correctly.

Threshold: The G force (measured in milliG to allow precise definition) that triggers a motion change event. For fields where multiple thresholds are available, set a series of thresholds at different levels.

Set Time: The amount of time, in milliseconds, the G force must remain above the Threshold value in order for an event to be triggered.

Clear Time: The amount of time, in milliseconds, before an event is cleared. When an event is triggered, it lasts until the Max Time value is reached, or until the Clear Time has elapsed without any further readings above the threshold. A new event cannot be triggered until the previous event has been cleared.

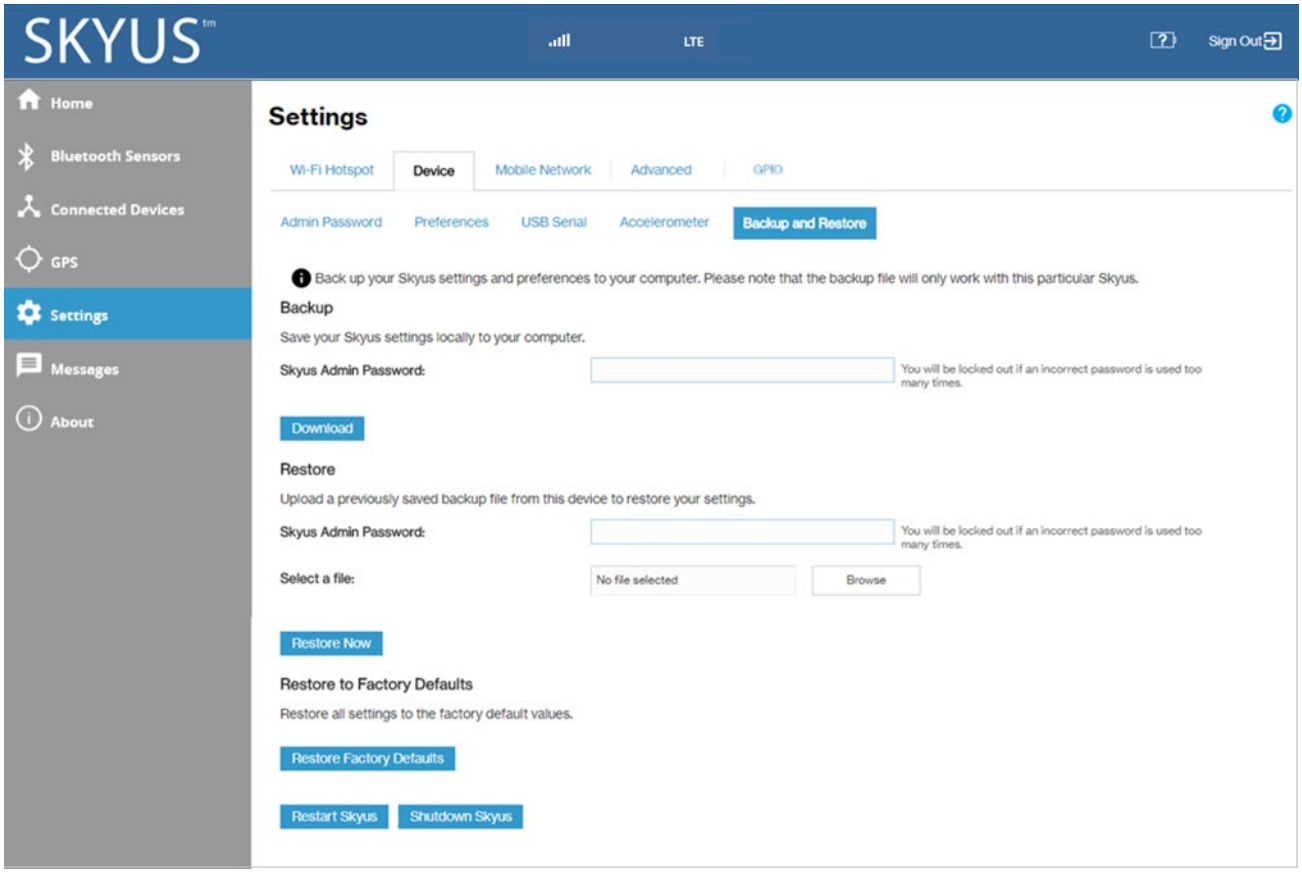
Max Time: The amount of time, in seconds, an event can last. If readings above the Threshold value persist after this amount of time, a new event is triggered.

NOTE: A single change can trigger multiple events. For example, if the Thresholds for Braking are set to 100, 200, 300, and 400, a 500 milliG motion triggers events for all four Thresholds.

Click **Save Changes.**

Backup and Restore Sub Tab

Use this page to create a device configuration file that can be used to backup and restore your custom settings. You can also restore all settings to the factory default values.



Backup

To back up current Skyus 160 Series settings to a file on your computer, enter your Admin password in the **Skyus Admin Password** field.

The default Admin password is printed on the bottom of the router. If you have changed the Admin password and don't remember it, select **Sign Out** in the top-right corner of the Home page, click **I forgot the Admin password**, and answer the security question. The current Admin password will be displayed.

NOTE: If you enter an incorrect password five times in a row, you will be locked out of the Web UI. To unlock it, restart the router.

Click the **Download** button. The file is automatically downloaded to your Downloads folder. This configuration file contains all settings for the device, router and system functions. It does not contain any modem settings or data.

NOTE: The backup file cannot be edited or viewed on the downloaded system or on any other device. This file can only be restored for this model of Skyus router, and settings can only be viewed or changed using the Web UI.

Restore

CAUTION! Restoring settings (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 router and disconnecting you from the Web UI.

To restore system settings from a backup settings file, enter your Admin password in the **Skyus Admin Password** field.

In the **Select a file** field, click **Browse** and choose a backup settings file to restore. **NOTE:** You can only restore a file that was created for this model of Skyus router.

Click the **Restore Now** button.

Your device will automatically reset and you will need to log back into the user interface.

Restore to Factory Defaults

Restore Factory Defaults: This button resets all settings to their factory default values.

CAUTION! This initiates a restart and may change the current Wi-Fi settings, breaking all existing connections to this router and disconnecting you from the Web UI.

Restart Skyus: This button turns your router off and on again.

Shutdown Skyus: This button turns off your router if you are using battery only. If you are using another power source, your Skyus will restart.

Mobile Network Tab

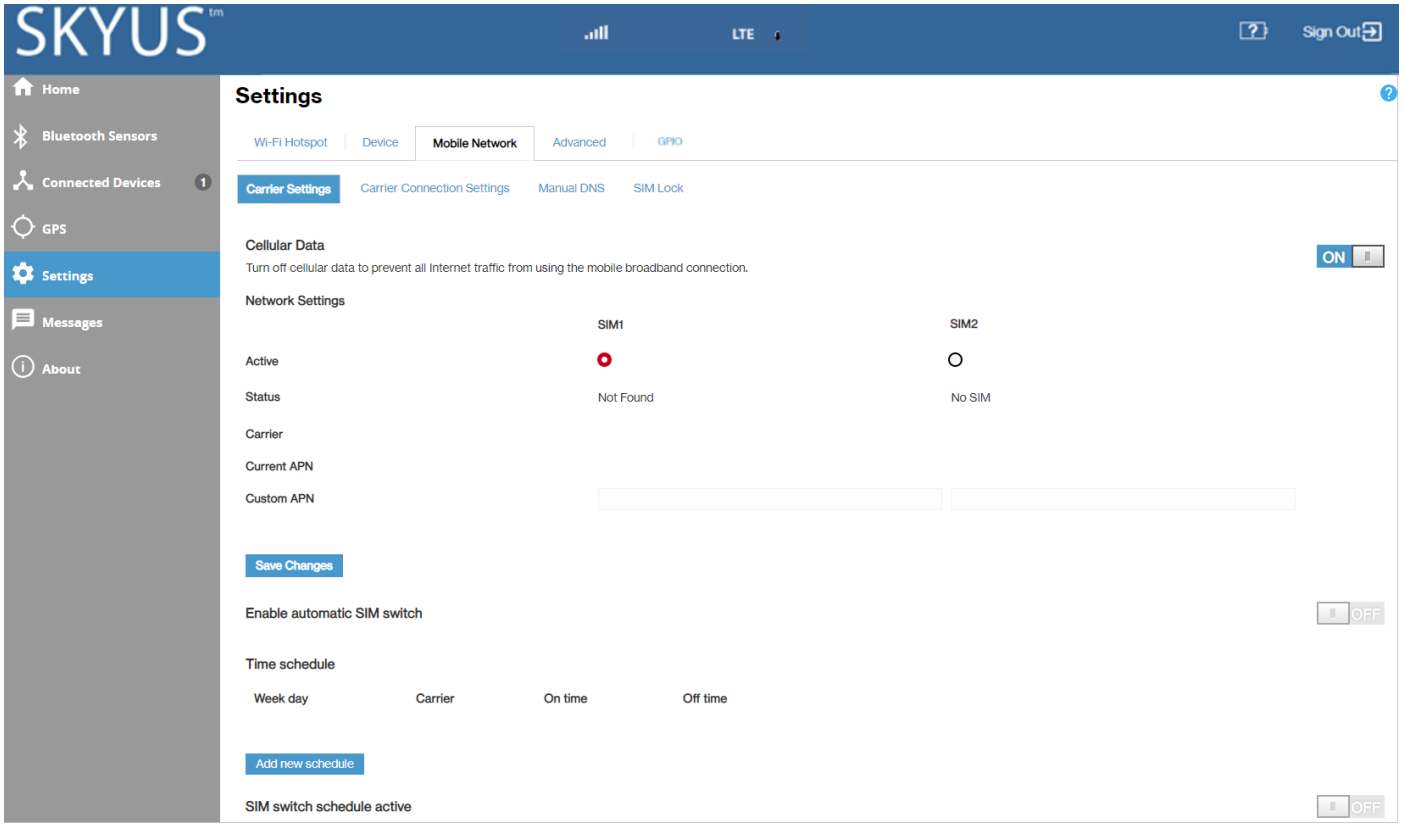
Use this tab to modify the mobile network settings on your Skyus 160 Series router.

The Mobile Network Tab contains four sub tabs:

- Carrier Settings
- Carrier Connection Settings
- Manual DNS
- SIM Lock

Carrier Settings Sub Tab

Use this page to modify the carrier settings on your Skyus 160 Series router. You can set up multiple schedules for SIM usage for each SIM.



Cellular Data

By default, cellular data is turned on. To turn off cellular data, move the **ON/OFF** slider to **OFF**.

CAUTION! If you turn cellular data off, Internet access via this device will not be possible. All connections will be terminated.

Network Settings

Active: Select the SIM you want to be active, or for which you want to set a time schedule.

Status: The current status of the SIM.

Carrier: The cellular carrier associated with the SIM.

Current APN: The Access Point Name (APN) currently used to connect to the cellular network associated with the SIM. The APN is pre-configured and, in most cases, should not be changed.

Custom APN: In most configurations, the Skyus 160 Series router is used with a dynamic IP and SIM and the Access Point Name (APN) is available from the network, for example: *internet*. However, if you are on a private network, you may need to set a custom APN for the network to communicate with the Skyus device.

The following table includes some commonly used APNs. Contact your carrier to confirm the correct APN for your line of service.

Carrier	APN Type	APN
Verizon	**Public Dynamic**	vzwinternet
	Public Static-West	we01.vzwstatic
	Public Static-Northwest	nw01.vzwstatic
	Public Static-Northeast	ne01.vzwstatic
	Public Static-South	so01.vzwstatic
	Public Static-Midwest	mw01.vzwstatic
AT&T	**Public Dynamic**	broadband
	Public Dynamic	i2gold
T-Mobile	**Public Dynamic**	fast.t-mobile.com

Enable automatic SIM switch

To enable automatic SIM switching, move the **ON/OFF** slider to **ON**. When enabled, the SIM is switched automatically if the active SIM is disconnected.

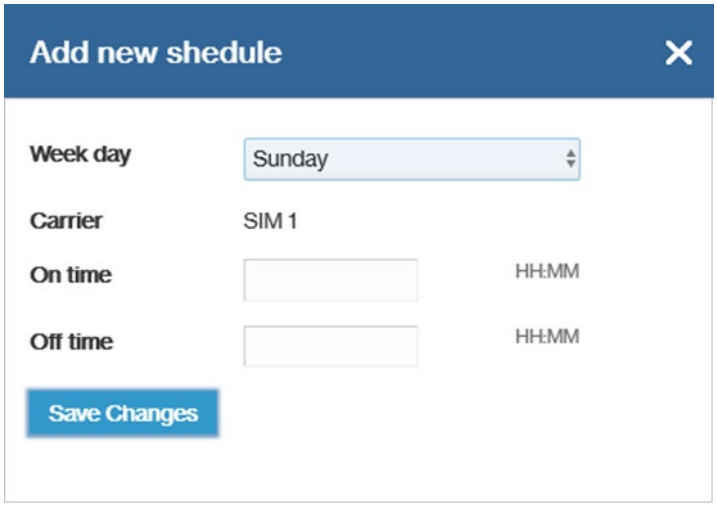
Time schedule

This section provides a list of the schedules you have set up for each SIM. Use the **Add new schedule** button to create schedules.

Add new schedule Button

NOTE: Select the SIM on which you want to set a schedule in the **Active** setting above before selecting the **Add new schedule** button.

Select this button to create a new schedule. You can create multiple schedules for each SIM. The Add new schedule dialog box appears.



Week day: Use the drop down to choose a day of the week for the schedule.

Carrier: The SIM on which you are setting a schedule. To change the SIM, close this dialog and select the correct SIM in the **Active** section above.

On time: Enter the time (local device time) you want the SIM switched on for the selected day, using military time in HH:MM format, for example: enter 08:00 for 8 AM.

Off time: Enter the time (local device time) you wish the SIM switched off for the selected day, using military time in HH:MM format, for example: enter 17:00 for 5 PM.

Click **Save Changes**.

The new schedule is listed in the **time schedule** section. Use the **Edit** and **Delete** buttons to edit or delete a schedule.

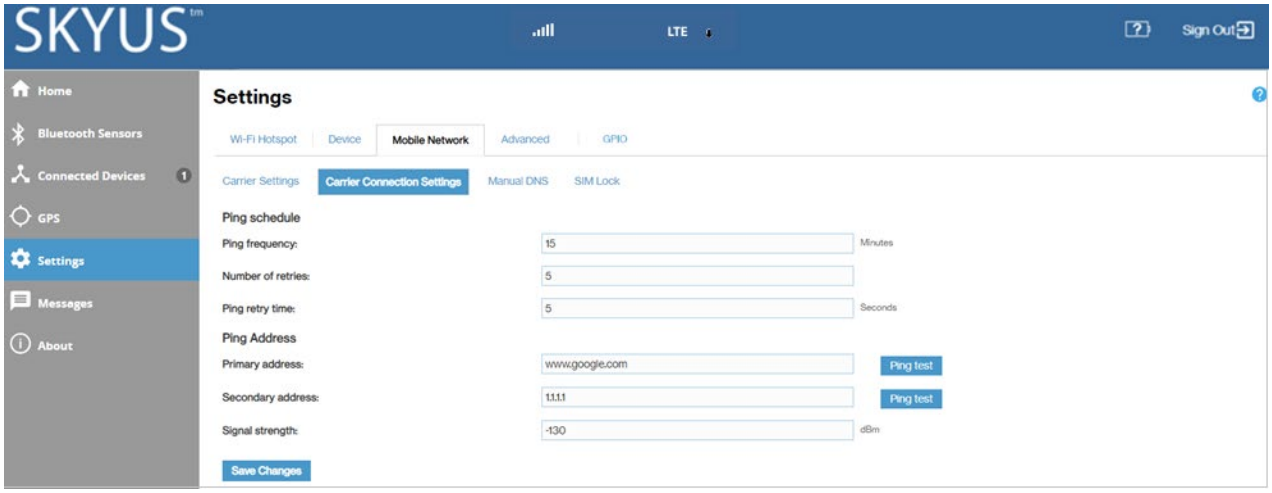
SIM switch schedule active

Move the **ON/OFF** slider to **ON** to activate or deactivate the SIM switch schedules listed under **Time schedule**.

Click **Save Changes** to save settings.

Carrier Connection Settings Sub Tab

Use this page to modify the ping settings on your Skyus 160 Series router. Ping attempts are used to test whether the modem is connected. When ping tests fail, a reboot is needed.



Ping schedule

Ping frequency: The number of minutes between ping attempts.

Number of retries: The number of times to retry after a ping failure to both the primary and secondary ping addresses.

Ping retry time: The time interval, in seconds, between ping retries.

Ping Address

Primary address: The address of the primary server to ping. Use the **Ping test** button to test.

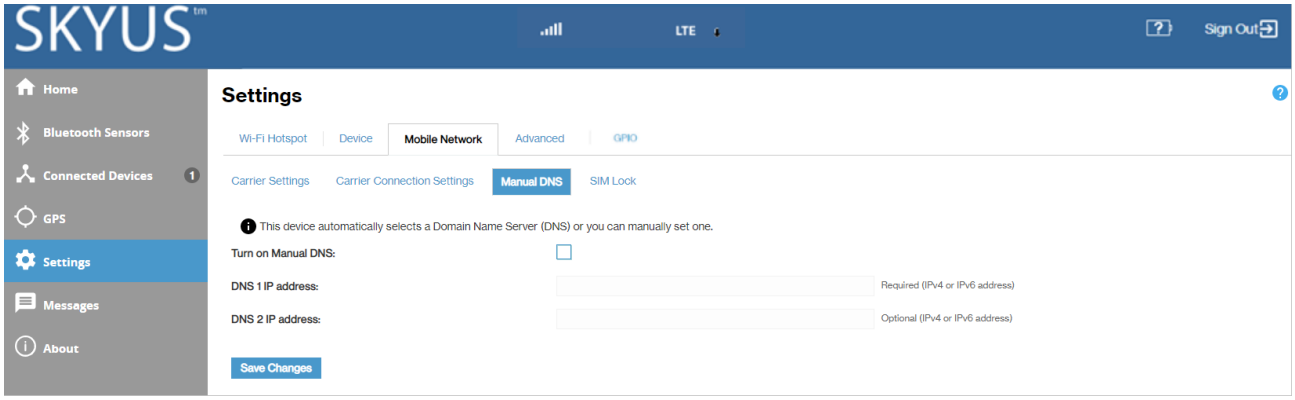
Secondary address: The address of the secondary server to ping. Use the **Ping test** button to test.

Signal strength: If signal strength falls below this level, the carrier is either switched or reset. **NOTE:** The carrier is switched automatically when **Enable automatic SIM switch** on the **Carrier Settings** sub tab is set to **ON**.

Click **Save Changes**.

Manual DNS Sub Tab

By default, the Skyus 160 Series router will automatically select the proper Domain Name Server (DNS). However, this page allows you to select a manual DNS.

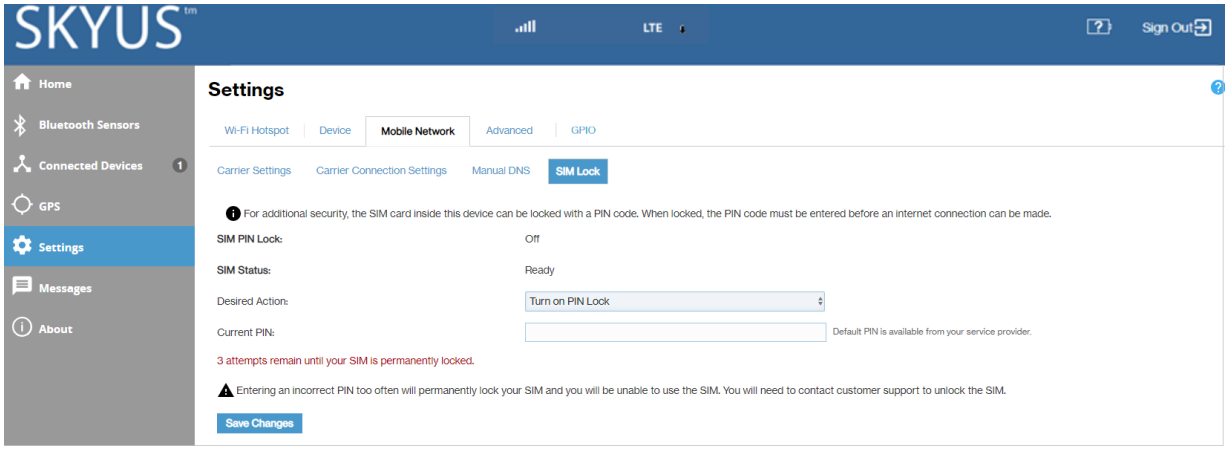


To turn on Manual DNS:

1. Check the **Turn on Manual DNS** box.
2. Enter the appropriate required address (IPv4 or IPv6) in the **DNS 1 IP address** box. This address is required.
3. Enter the appropriate optional address (IPv4 or IPv6) in the **DNS 2 IP address** box. This address is optional.
4. Click **Save Changes**.

SIM Lock Sub Tab

Use this page to set up a lock on your SIM card. If you lock the SIM, a PIN is required to connect.



SIM PIN Lock: Indicates whether the PIN lock feature is in use. If On, the PIN lock has been turned on, and the SIM PIN must be entered to connect to the mobile network. If Off, the PIN lock feature is not turned on and the SIM PIN is not required.

SIM Status: The current status of the SIM card. Possible states include:

- **Ready** – No SIM PIN is needed.
- **PIN Locked** - SIM PIN must be entered before you can use the mobile network.
- **PUK Locked** - PUK (personal unblocking key) for the SIM must be entered in order to continue. The PUK can be obtained from your service provider.
- **Unlocked** - SIM PIN was needed, but has already been entered.
- **No SIM** - No SIM is detected. Check that the SIM is inserted correctly.
- **SIM Error** - SIM is detected, but is not responding as expected and cannot be used.

Desired Action: The actions available depend on the SIM status. Possible operations include:

- **PIN Lock** - If the SIM is currently PIN locked, you are prompted to enter the PIN.
  NOTE: If an incorrect PIN is entered too many times, the SIM becomes PUK locked. A counter indicates how many incorrect entries will cause PUK lock. Once PUK locked, the PUK must be obtained from your service provider.
- **PUK Lock** - If the SIM is currently PUK locked, the only operation possible is to enter the PUK.
  NOTE: If an incorrect PUK is entered too many times, the SIM becomes permanently unusable. You will need to obtain a new SIM. A counter indicates how many entry attempts remain.
- **Turn on PIN Lock** - 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.
- **Turn off PIN Lock** - Turns off a PIN lock that was previously turned on 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.

Current PIN: Enter the current PIN. The default SIM PIN is available from your service provider.

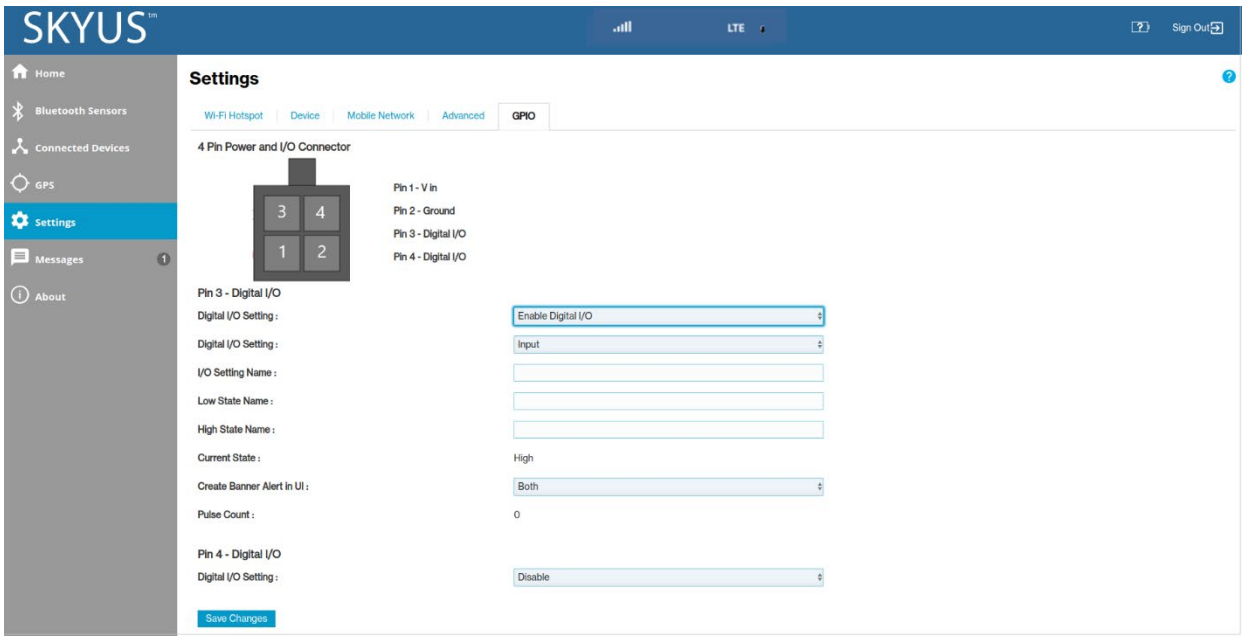
Click **Save Changes**.

Advanced Tab

Advanced settings are intended only for users with advanced technical knowledge. For information about the Advanced Settings page, go to Chapter 4, “Advanced Settings” on page 66.

GPIO Tab

The Skyus 160 Series router includes two configurable digital General Purpose Input Output (GPIO) pins. Use settings on this tab to view or configure pin settings.



4 Pin Power and I/O Connector

The Skyus 160 Series power port includes voltage in, ground, and two digital I/O pins.

NOTE: The diagram shows the pins from the front of the cable connector (with the wires running behind).

Pin 3 – Digital I/O

Digital I/O Setting: Use the drop-down to enable digital I/O on Pin 3.

Digital I/O Setting: Select **Input** or **Output** from the drop-down.

I/O Setting Name: Enter a name to identify the setting.

Low State Name: Enter a name to identify the low state of the pin.

High State Name: Enter a name to identify the high state of the pin.

Current State: Indicates the current state of the pin (**Low** or **High**).

Create Banner Alert in UI: Use the drop-down to select an option.

Pulse Count (visible for Input): Displays the number of times the state has moved from low to high or high to low.

Pin 4 – Digital I/O

Digital I/O Setting: Use the drop-down to enable digital I/O on Pin 4.

Digital I/O Setting: Select **Input** or **Output** from the drop-down.

I/O Setting Name: Enter a name to identify the setting.

Low State Name: Enter a name to identify the low state of the pin.

High State Name: Enter a name to identify the high state of the pin.

Current State: Indicates the current state of the pin (**Low** or **High**).

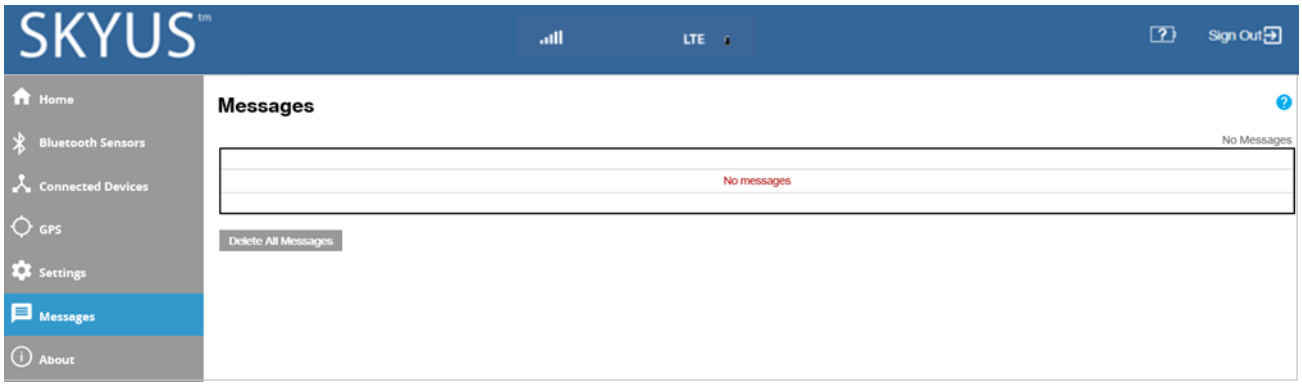
Create Banner Alert in UI: Use the drop-down to select an option.

Pulse Count (visible for Input): Displays the number of times the state has moved from low to high or high to low.

Click **Save Changes**.

Accessing Messages

To access messages, select **Messages** from the Web UI side menu. The Messages page appears.



Messages Page

This page displays text messages sent to your device. These are typically messages from your service provider and cannot be replied to, so no reply feature is provided.

Messages

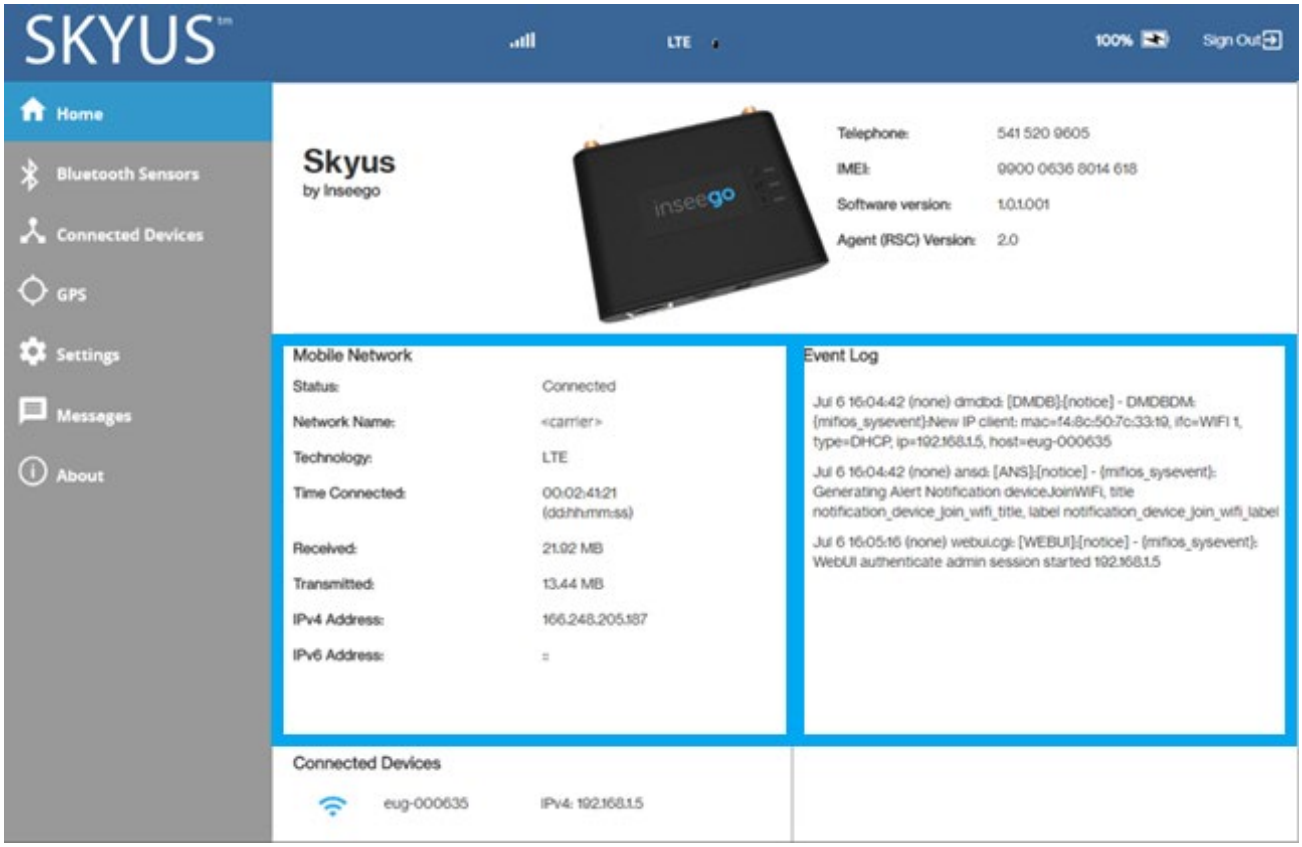
Counters at the top of the screen indicate the number of unread (new) messages and the total number of messages.

Messages are listed in order of date. Unread (new) messages are indicated by an icon. Messages are set to Read once they are displayed on this page, so the next time the page is entered, they will no longer be marked as Unread.

Use the **Delete All Messages** button to delete all messages.

Viewing Info About the Router

On the Web UI Home page, the Mobile Network section shows current status information about your router and mobile network. It also provides an event log.



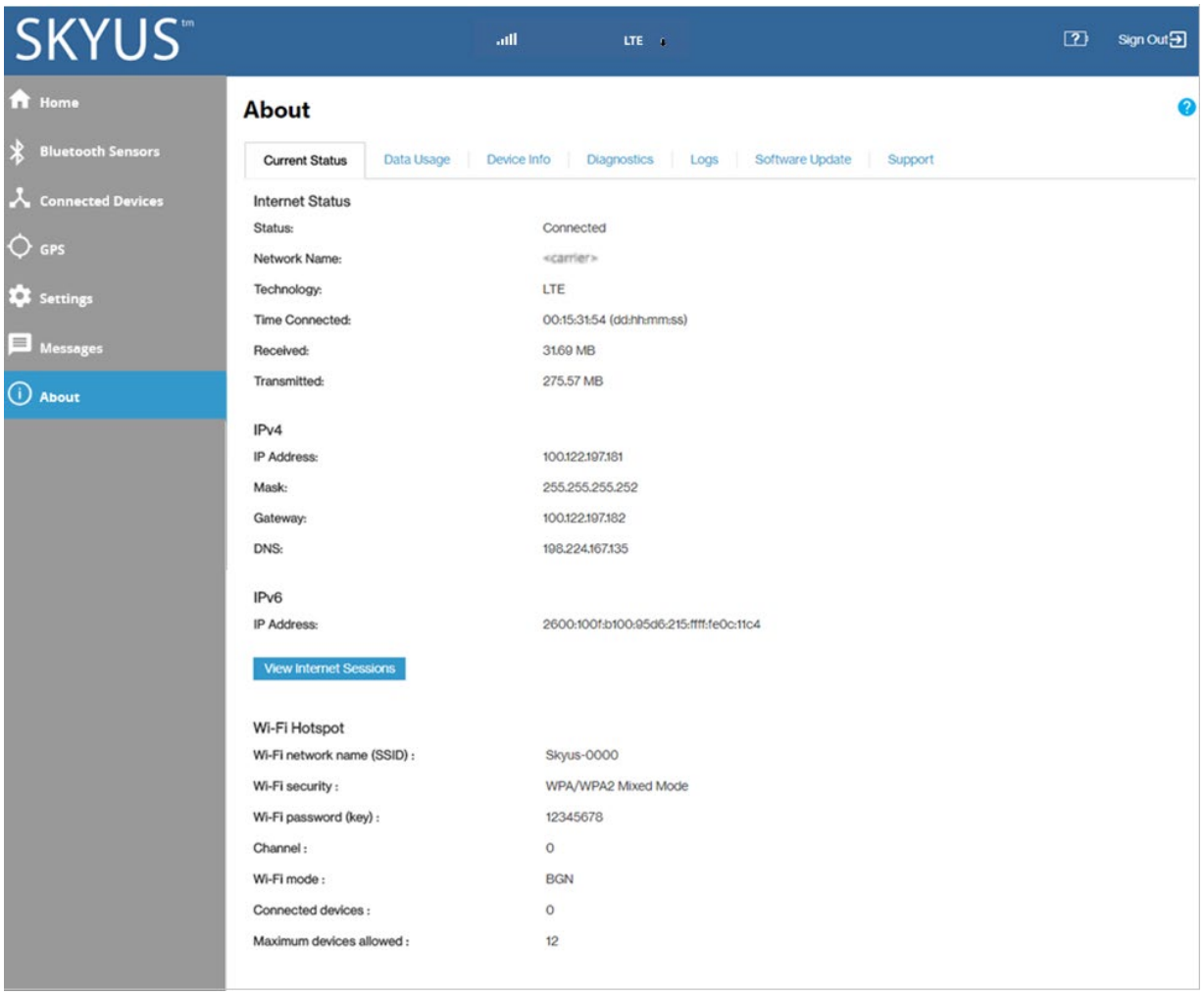
To view more detailed information about your router and its use, select **About** from the Web UI side menu.

The About page includes seven tabs:

- Current Status
- Data Usage
- Device Info
- Diagnostics
- Logs
- Software Update
- Support

Current Status Tab

Use the Current Status tab to view Internet status, Wi-Fi hotspot information, and internet session details.



Internet Status

Status: Indicates whether your router is Connected or Disconnected.

Network Name: The cellular carrier network (for example, AT&T)

Technology: The cellular technology (for example, LTE or 3G)

Time Connected: The cumulative time connected

Received: The amount of data received for the most recent 24 hours of the current Internet session. This counter starts at zero when the connection is established.

Transmitted: The amount of data transmitted for the most recent 24 hours of the current Internet session. This counter starts at zero when the connection is established.

IPv4

IPv4 Address: The Internet IP address assigned to the router.

Mask: The network mask associated with the IPv4 address.

Gateway: The gateway IP address associated with the IPv4 address.

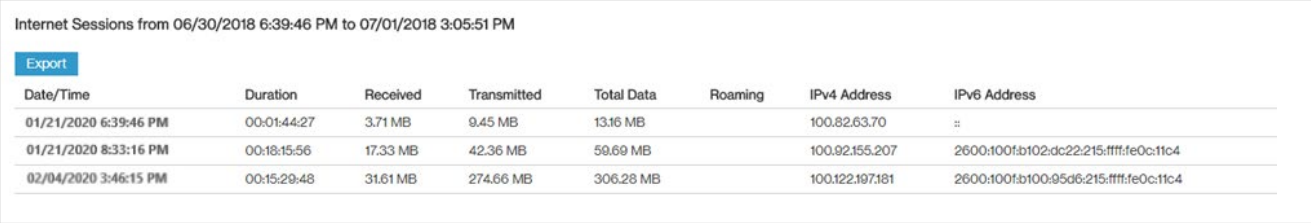
DNS: The Domain Name Server currently used by this device.

IPv6

IPv6 Address: The global IPv6 address for the router (blank if IPv6 is turned off or is not supported by the current network connection or carrier).

View Internet Sessions

Select the **View Internet Sessions** button to see detailed information on internet activity.


Internet Sessions from 06/30/2018 6:39:46 PM to 07/01/2018 3:05:51 PM

Export

Date/Time	Duration	Received	Transmitted	Total Data	Roaming	IPv4 Address	IPv6 Address
01/21/2020 6:39:46 PM	00:01:44:27	3.71 MB	9.45 MB	13.16 MB		100.82.63.70	::
01/21/2020 8:33:16 PM	00:18:15:56	17.33 MB	42.36 MB	59.69 MB		100.92.155.207	2600:100f:b102:dc22:215:ffff:fe0c:11c4
02/04/2020 3:46:15 PM	00:15:29:48	31.61 MB	274.66 MB	306.28 MB		100.122.197.181	2600:100f:b100:95d6:215:ffff:fe0c:11c4

Click the **Export** button to export the Internet session data.

Wi-Fi Hotspot

Wi-Fi network name (SSID): The Wi-Fi network name.

Security: The type of security.

Wi-Fi password (key): The Wi-Fi password.

Channel: The Wi-Fi channel.

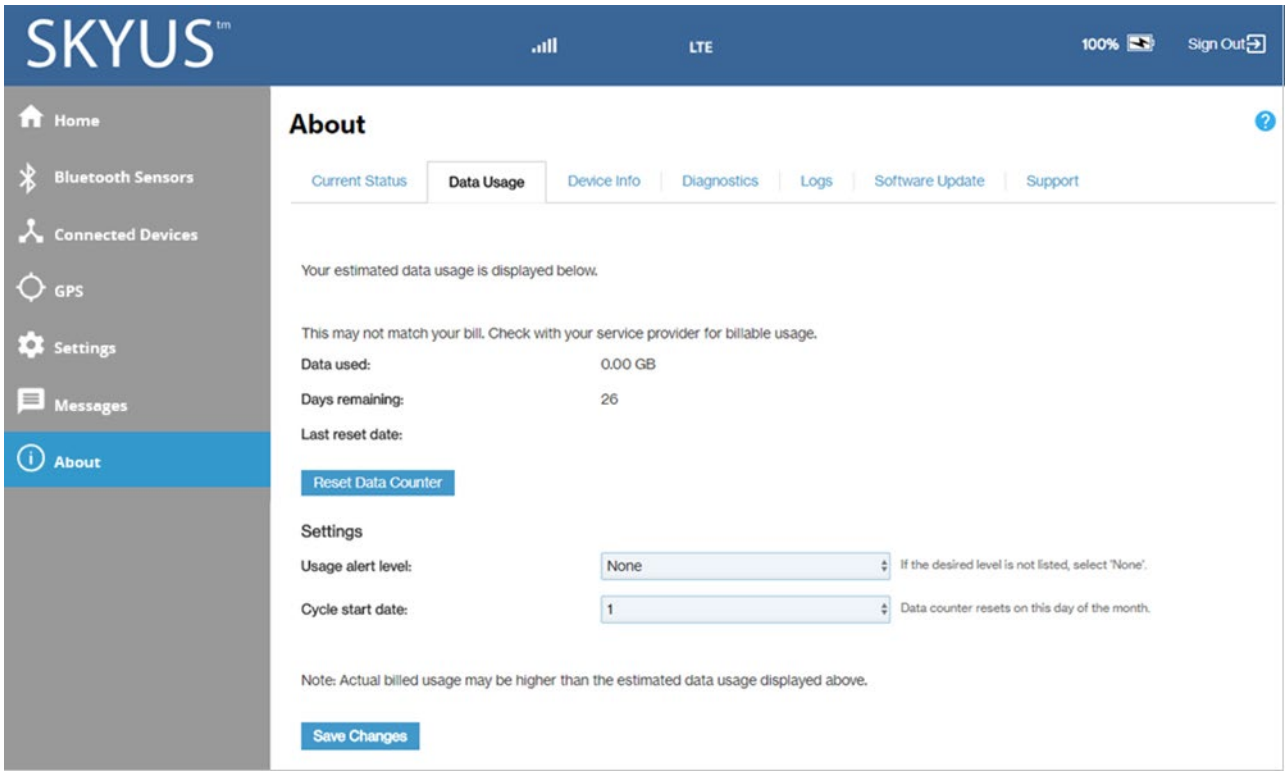
Wi-Fi mode: The Wi-Fi mode.

Connected devices: The number of connected devices.

Maximum devices allowed: The maximum number of connected devices allowed.

Data Usage Tab

Use the Data Usage tab to view details about data usage or to reset the data counter and settings.



Estimated Data Usage

This section may vary according to your plan. It contains a graphical representation of data usage. Information is displayed for the current reporting period (starting from the **Cycle start date** you set), unless you use the **Reset Data Counter** button.

Data used: An estimation of the amount of data used during the current reporting period.

Days remaining: The number of days left before the current reporting period ends.

Last reset date: The date when the data was last manually reset.

Select the **Reset Data Counter** button to restart the **Data used** field.

Settings

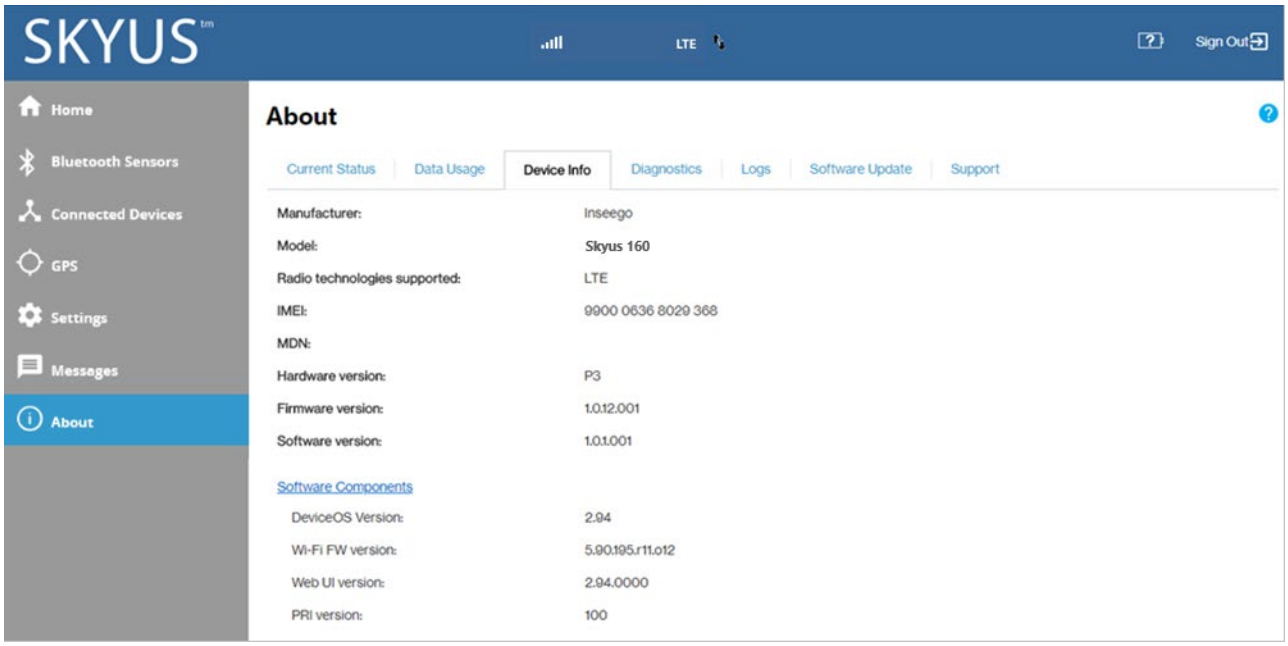
Usage alert level: Specify an alerting threshold for data usage (from 20 MB to 20 G).

Cycle start date: Specify the start day of the month for your data counter cycle. **NOTE:** You can set this to correspond to the start day of your billing cycle.

Make your selections and click **Save Changes**.

Device Info Tab

This page presents useful information that will be needed in the event Support is required.



Manufacturer: The manufacturer of this router.

Model: The model name and number for this device.

Radio technologies supported: The radio technologies supported by your Skyus device. This refers to the Skyus 160 Series router and not the mobile network.

IMEI: The IMEI (International Mobile Equipment Identity) for this device. This is a 15 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: The MDN (Mobile Directory Number) is the phone number assigned to the Skyus device. This changes when the SIM is changed.

Hardware version: The hardware version for your Skyus device.

Firmware version: The version of the firmware (software) currently installed for the modem component.

Software version: The version of currently installed software.

Software Components

Select the Software Components link to see the following version information for various software components.

DeviceOS Version: The version number for the operating system (OS) and its components.

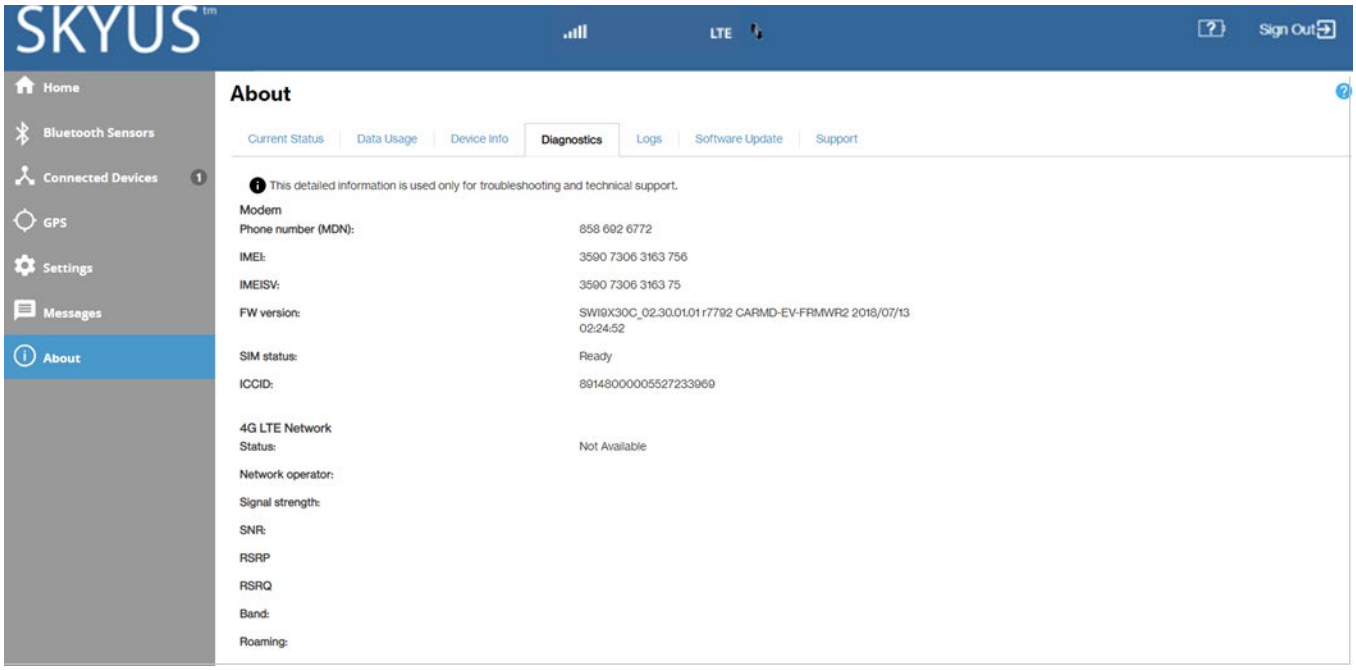
Wi-Fi FW version: The version of the firmware (software) currently installed for the Wi-Fi component.

Web UI version: The version number for the Web Interface.

PRI version: The configuration version currently applied to this device.

Diagnostics Tab

The information presented on this page is typically only needed for troubleshooting and technical support. If you need to contact Support, please record this information and be ready to share it with your Inseego Support Representative.



Modem

Phone number (MDN): The phone number assigned to the Skyus device. This changes when the SIM is changed.

IMEI: The IMEI (International Mobile Equipment Identity) for this device. This is a 15 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.

FW version: The version of the firmware (software) currently installed for the modem component.

SIM status: 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: The unique ID number assigned to the SIM card. This will be blank if there is no installed SIM or a SIM error.

4G LTE Network

Status: Indicates whether the LTE network has been detected (Not Available or Available).

The following fields are filled when the LTE network is Available.

Network operator: The name of the LTE network.

Signal strength: The strength of the LTE signal, measured in dBm. Higher absolute values indicate a stronger signal, for example: -80 dBm is a stronger signal than -90 dBm. **NOTE:** LTE signal strength is typically lower than 3G signal strength.

SNR: Signal-to-noise ratio (SNR) measures signal quality. Higher values indicate a better signal.

RSRP: Reference Signal Receive Power. A measure of signal strength, similar to Signal strength, but RSRP measures lower due to the method of calculation.

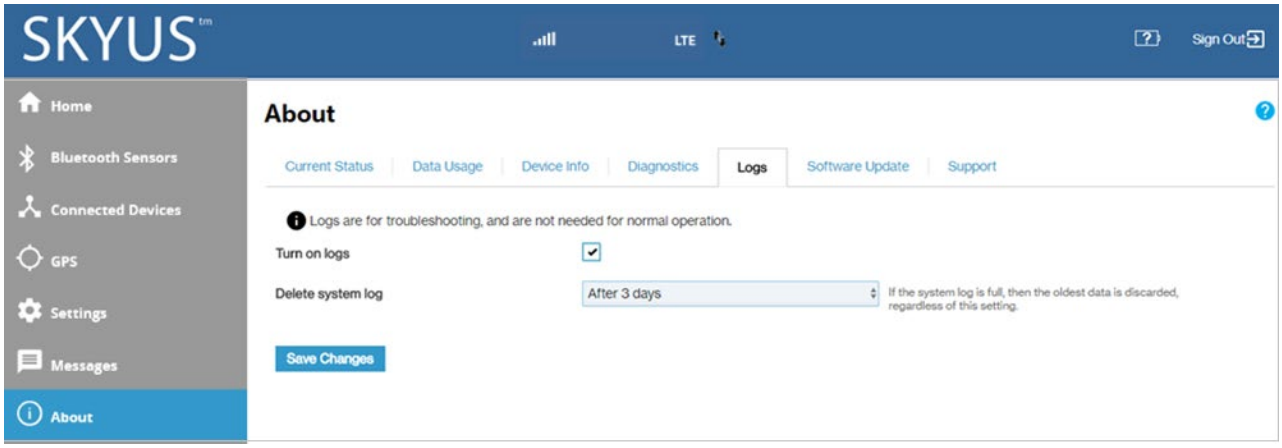
RSRQ: Reference Signal Received Quality. A calculated value from RSRP and Signal strength that provides a measure of signal and interference.

Band: Indicates the band used for the current LTE connection. **NOTE:** LTE networks may use different bands in different regions.

Roaming: Indicates whether the current connection is a roaming connection.

Logs Tab

Use this tab if you are experiencing issues with your device. Logging an issue is the best way to identify a root cause.



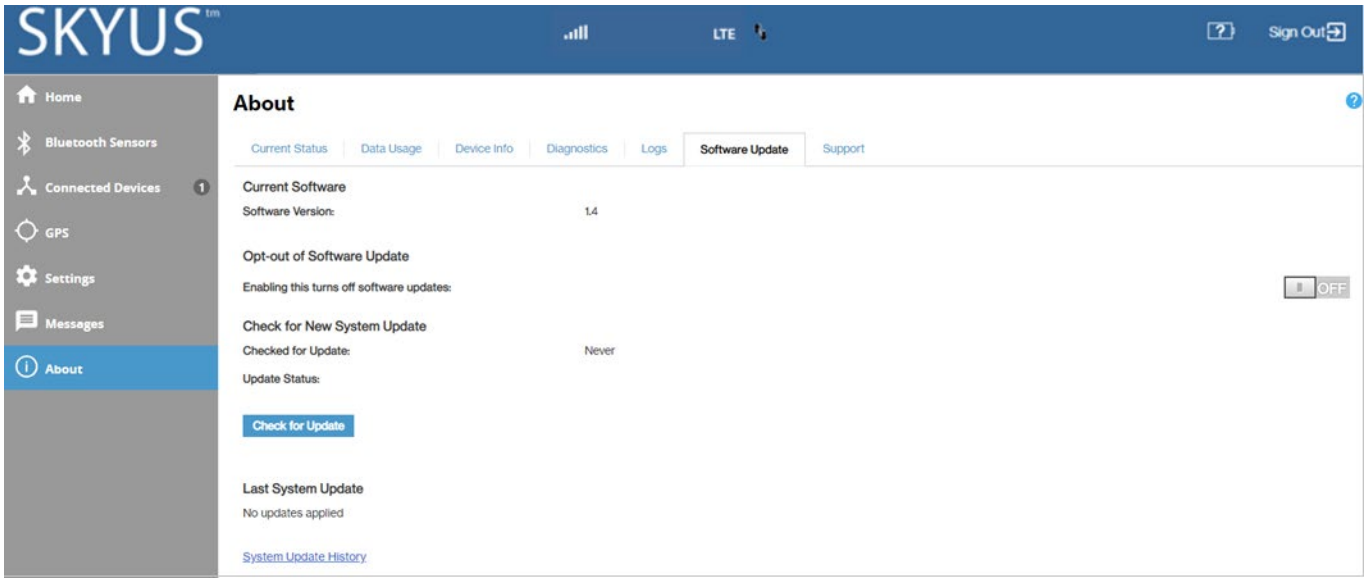
Turn on logs: Check this box to enable logging. When checked, the log information appears below.

Delete system log: Use this drop-down to select how long the log data is retained. **NOTE:** The oldest data is deleted when the log is full, regardless of this setting.

Click **Save Changes**.

Software Update Tab

Software updates are delivered to the Skyus 160 Series router automatically over the mobile network. This tab displays your current software version, last system update information, and allows you to check for new software updates.



Current Software

Software Version: The version of the software currently installed on your Skyus 160 Series device.

Opt-out of Software Update

This setting enables or disables turning off software updates on your device. When the **ON/OFF** slider is **ON**, the Skyus 160 Series router turns off software updates. When **OFF**, software updates are delivered automatically to the device.

Check for New System Update

Checked for Update: The date and time the Skyus router last checked to see if an update was available.

Update Status: This is area is usually blank. If you check for an update, the result of that check, or the download progress of an update displays.

Check for Update: Click this button to manually check for available software updates. **NOTE:** Normally this is not necessary, as updates are automatically pushed to the Skyus device.

- If a new software update is available, click **Download now** to install it.
- If a new system update is available, you are given an option to install it now or later.
- If a configuration update is available, it is installed automatically.

Last System Update

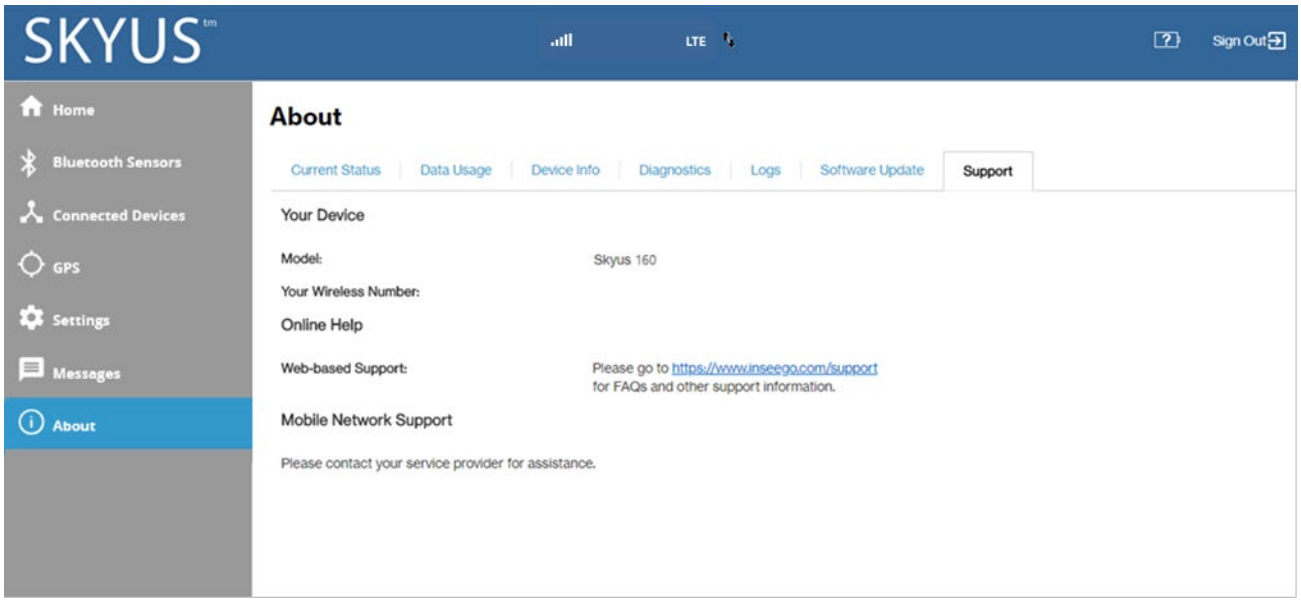
This section displays details about the last software update, including the date and time of the last update, and the name, source, package version and size of the update.

System Update History

Click the System Update History link to view details of the last updates (up to 20) that have been downloaded and installed to this device. If no updates have been installed, this section will display the current software version.

Support Tab

If you need Support for your Skyus 160 Series device, use the Support tab to visit https://www.inseego.com/support.



4

Advanced Settings

Overview

Using Advanced Settings

Overview

The Advanced Settings pages are intended for users with technical expertise in the area of telecommunication and networking.

WARNING! Changing the Advanced settings may be harmful to the stability, performance and security of the Skyus 160 Series router.

Using Advanced Settings

Advanced settings are available when you select **Settings** from the Web UI side menu, then select the **Advanced** tab.

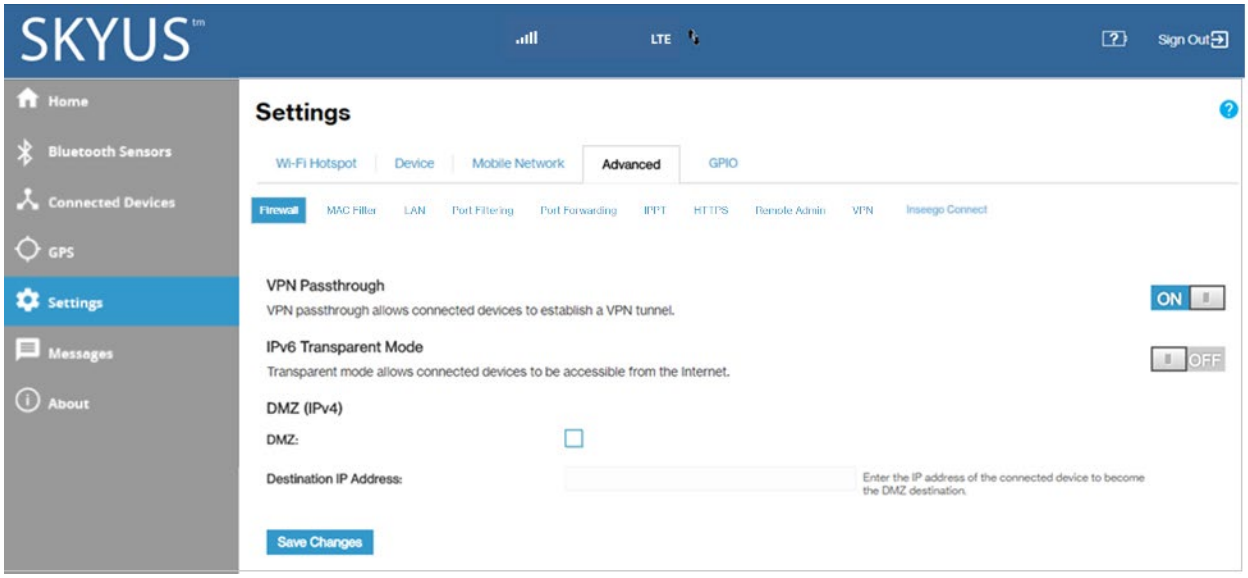
The Advanced Settings page includes the following sub tabs:

- Firewall
- Mac Filter
- LAN
- Port Filtering
- Port Forwarding
- IPPT
- HTTPS
- Remote Admin
- VPN
- Inseego Connect

Firewall Tab

The Skyus 160 Series firewall determines which Internet traffic is allowed to pass between the router and connected devices and protects your connected devices from malicious incoming traffic from the Internet. The firewall cannot be turned off.

Use the Firewall tab to adjust the general security level of the firewall, designate a specific device to receive all traffic, and set up specific firewall rules.



VPN Passthrough

To use the **VPN Passthrough**, ensure the **ON/OFF** slider is **ON**. This allows you to establish a VPN tunnel while using the Skyus 160 Series router.

IPv6 Transparent Mode

To use **IPv6 Transparent Mode**, slide the **ON/OFF** slider to **ON**. This allows connected devices to be accessible from the Internet.

DMZ (IPv4)

DMZ allows the connected device specified as the DMZ IP address (the DMZ destination) to receive all traffic that would otherwise be blocked by the firewall. **NOTE:** Allowing DMZ 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: Check this box to allow DMZ.

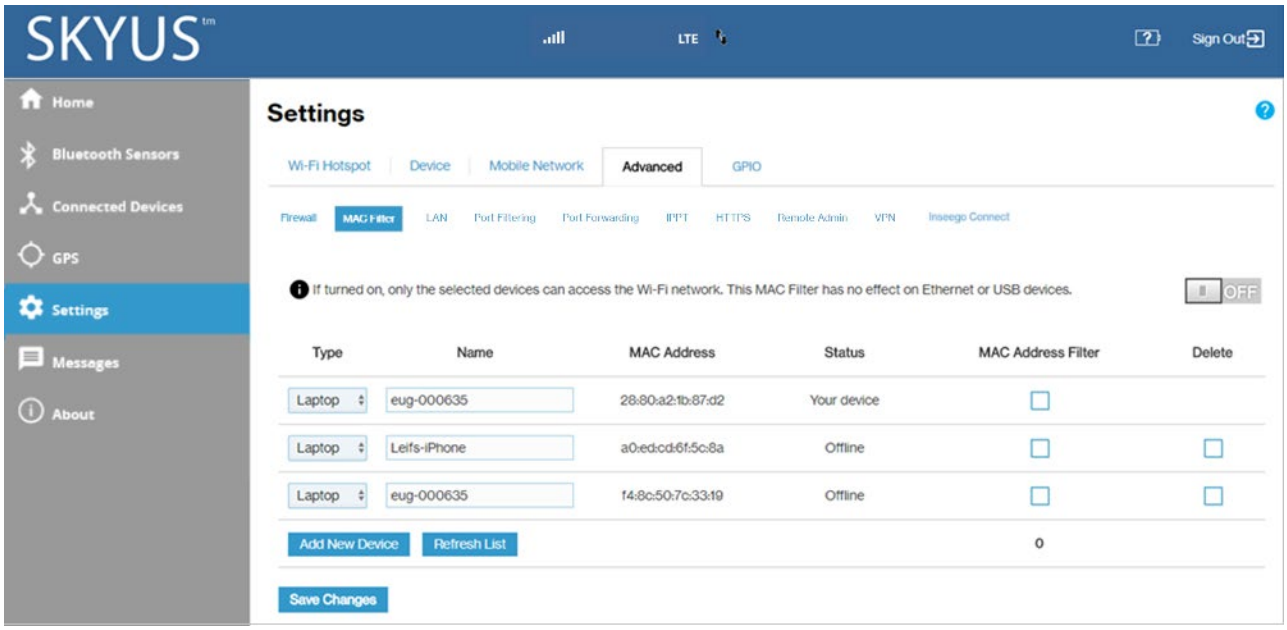
Destination IP Address: Enter the IP address of the connected device you wish to become the DMZ device (the DMZ destination). **NOTE:** You can check the IP address of each connected device on the Connected Devices screen.

Click **Save Changes**.

Mac Filter Tab

The MAC filter allows only selected devices to access the Skyus 160 Series network. By default, MAC filter is turned OFF.

Use this tab to turn the MAC Filter ON and specify device access.



To use the MAC filter, select the device(s) from the device list that you want to be allowed to connect to the network and move the **ON/OFF** slider to **ON**.

CAUTION! Turning on MAC filtering immediately disconnects all devices that are not included in the filter from the network.

NOTE: This device list includes all devices currently connected to the Skyus 160 Series router, except those connected via Ethernet.

Add New Device: Use this button to add a device to the device list, then enter the device name, MAC address, choose whether to select the MAC Address Filter checkbox, and click **Save Changes**.

To delete a device from the list, select its **Delete** checkbox and click **Save Changes**.

To discard any unsaved changes and refresh the list, click **Refresh List**.

Notes on Blocking Devices

There are two ways to block devices from connecting to the Skyus 160 Series router:

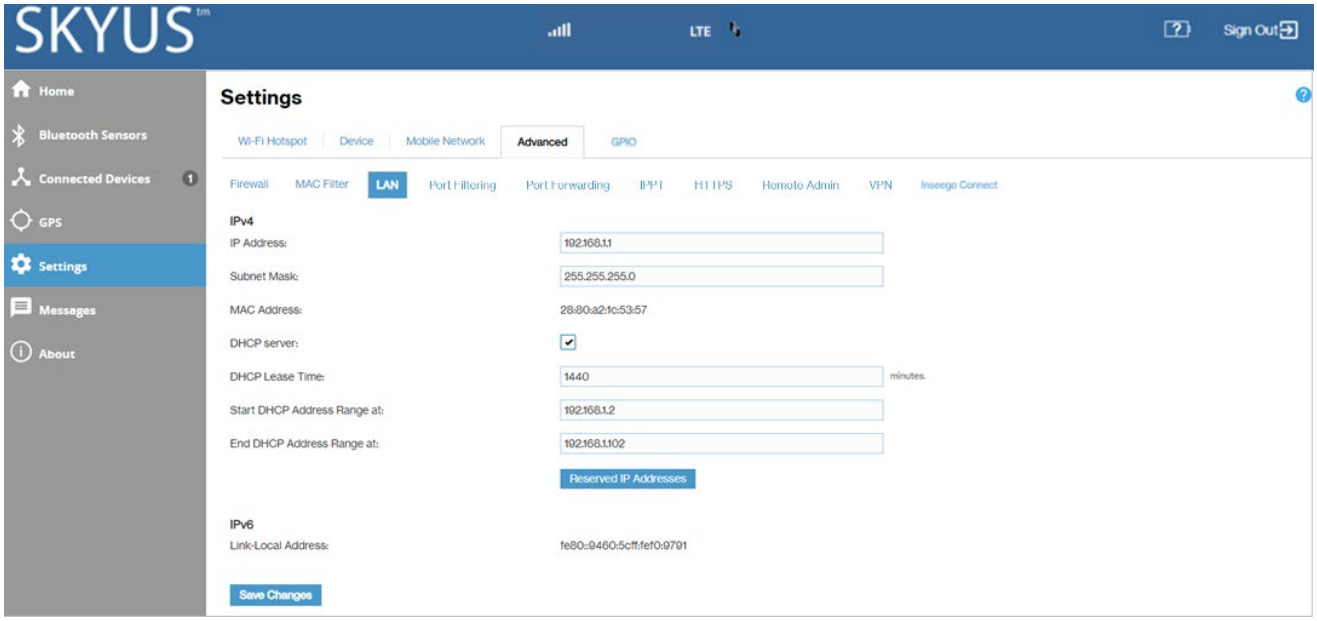
- **Temporarily block a device from connecting to the router, including devices connected via Ethernet.**
  To use this method, go to the **Connected Devices** page and click the **Block** button next to the device.
- **Permanently block a device from connecting to your router's network.**
  Use the **MAC Filter**.

When blocking devices, the following information applies:

- Devices blocked with **Connected Devices > Block** are blocked from the network, even if the **MAC Filter** is on and the device is enabled for the MAC Filter.
- If the **MAC Filter** is on, and a device is blocked with **Connected Devices > Block**, and is not enabled for the MAC Filter, then it will not be able to connect. Both the MAC Filter and the Block prevent connection.
- If the **MAC Filter** is on, and a device is enabled for the MAC Filter, then the device will be able to connect. However, it can still be blocked using **Connected Devices > Block** or by disabling the **MAC Filter**.

LAN Tab

This tab provides settings and information about the Skyus 160 Series router's local area network (LAN). For this device, the LAN consists of this device and all Wi-Fi and Ethernet connected devices.



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 subnet mask network setting for the Skyus 160 Series router. The default value 255.255.255.0 is standard for small (class "C") networks. If you change the LAN IP Address, make sure to use the correct Subnet Mask for the IP address range of the LAN IP address.

MAC Address: (read-only) The Media Access Controller (MAC) Address for the Wi-Fi interface on this device. The MAC address is a unique network identifier assigned when a network device is manufactured.

DHCP server: This checkbox turns the DHCP Server feature on or off. This should be left checked. The DHCP server allocates an IP address to each connected device. **NOTE:** If the DHCP Server is turned off, each connected device must be assigned a fixed IP address.

DHCP Lease Time: The number of minutes in which 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.

Start DHCP Address Range at: The start of the IP address range used by the DHCP server. If the IP is set on the client device, use an IP address outside of this DHCP range; if the IP address is set using an IP reservation, it will usually be inside this range. **NOTE:** Only expert users should change this setting.

End DHCP Address Range at: The end of the IP address range used by the DHCP server. If the IP is set on the client device, use an IP address outside of this DHCP range; if the IP address is set using an IP reservation, it will usually be inside this range. **NOTE:** Only expert users should change this setting.

To ensure that a connected device will always be allocated the same IP Address by the Skyus 160 Series router, click the **Reserved IP Addresses button**. A list of devices with their MAC Address, Current IP Address, and a field to enter a Reserved IP Address appears.

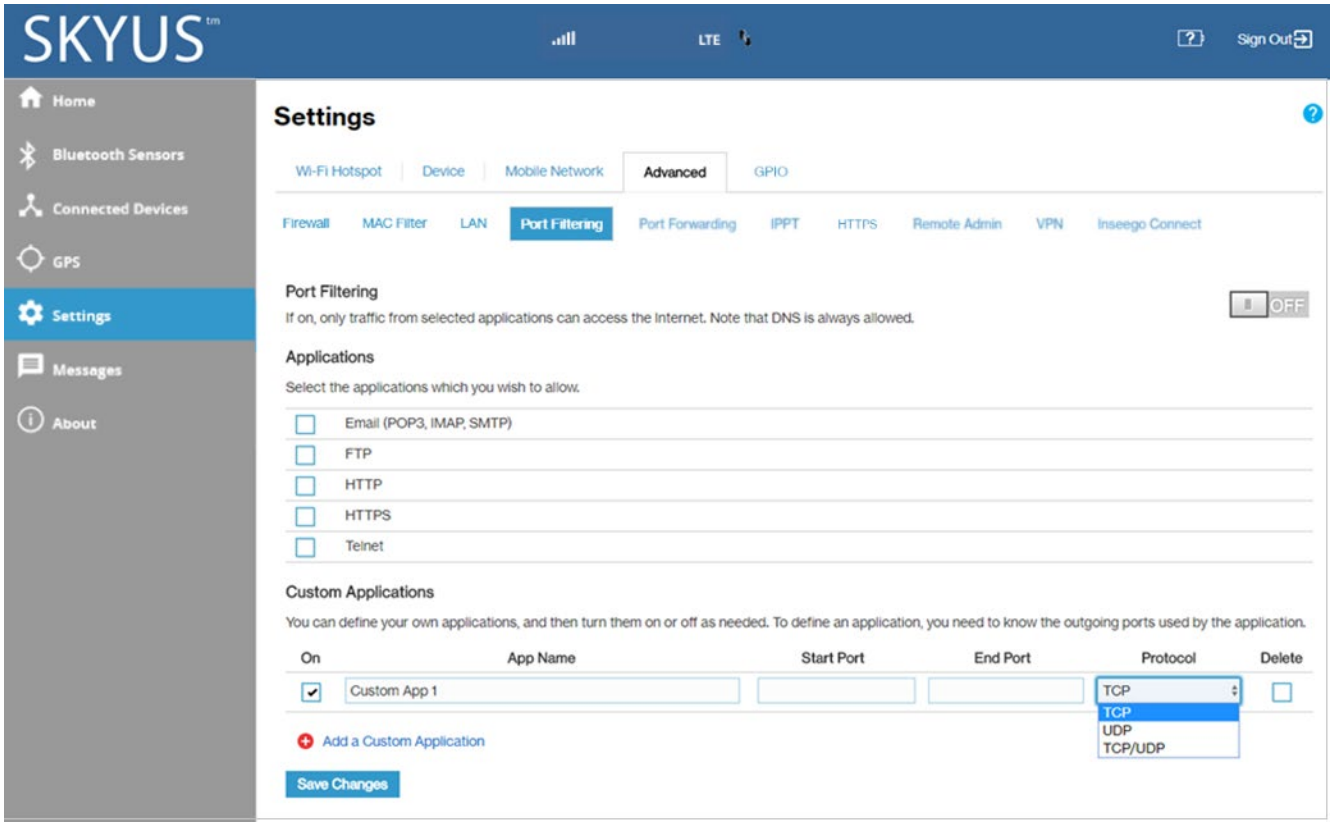
IPv6

Link-Local Address: The Link-Local IPv6 address if the connected device supports IPv6.

Click **Save Changes** to activate and save new settings.

Port Filtering Tab

Port Filtering allows you to block outgoing Internet connections and permit only selected applications to access the Internet. Traffic is identified by port numbers. Some applications are pre-defined. You can define additional applications if you know the details of the traffic used and generated by the applications.



Port Filtering

To turn on port filtering, move the **ON/OFF** slider to **ON**.

To turn off port filtering, so that any application can connect to the Internet, move the slider to **OFF**.

Applications

Select the applications you want to be able to access the Internet and click **Save Changes**.

The following table provides port numbers and protocol information for each port filtering application listed.

Application Name	Port	TCP*	STCP*	UDP*
Email				
POP3	110	Yes	No	Assigned
POP3S	995	Yes	No	Yes
IMAP	143	Yes	No	Assigned
IMAPS	993	Yes	No	Assigned
SMTP	25	Yes	No	Assigned
SecureSMTP	465	Yes	No	No
FTP control (command)	21	Yes	Yes	Assigned
FTP data transfer	20	Yes	Yes	Assigned
HTTP	80	Yes	Yes	Assigned
HTTPS	443	Yes	Yes	Assigned
Telnet	23	Yes	No	Assigned

Custom Applications

You can define up to ten custom applications.

Add a Custom Application: Use this button to add a new row to the custom application list.

On: Check this box if you want the new application to be able to access the Internet.

App Name: Enter a name for the custom application.

Start Port: Enter the beginning of the range of port numbers used by outgoing traffic for the custom application being added.

End Port: Enter the end of the range of port numbers used by the application.

* **Yes** indicates the protocol is standardized for the port number.
No indicates the protocol is standardized for the port number.
Assigned indicates the port number is assigned by IANA (Internet Assigned Numbers Authority) for protocol use, but may not be standardized.

NOTE: If the application uses a single port instead of a range, type the same value for both the **Start Port** and the **End Port**.

Protocol: Select the protocol used by the port range from the drop-down list (TCP, UDP, or both).

Delete: Check this box to delete a custom application. **NOTE:** Click on the Port Filtering tab again to remove deleted custom applications from view on the screen.

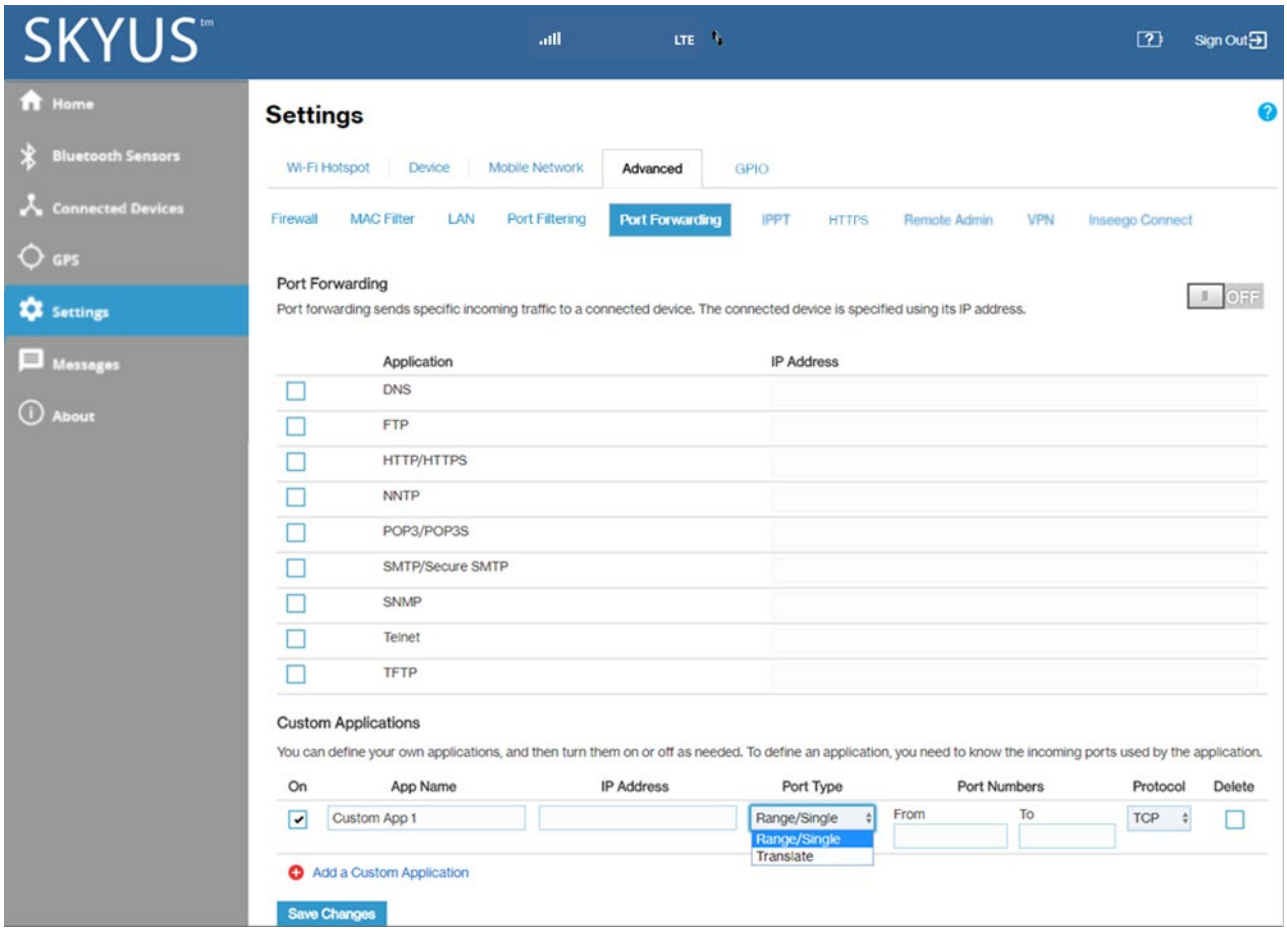
Click **Save Changes** to save any changes made to the custom applications.

Port Forwarding Tab

Port Forwarding 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. Port forwarding allows Internet users to access any server you are running on your computer, such as a Web, FTP, or Email server. For some online games, port forwarding must be used in order for the games to function correctly.

IMPORTANT: Port forwarding creates a security risk and should not be turned on unless it is required.

Some mobile 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

To turn on port forwarding, move the **ON/OFF** slider to **ON**.

To turn off port forwarding, so that no inbound traffic is forwarded to a LAN client, move the slider to **OFF**.

Port Forwarding Applications

Check the box next to each Port Forwarding application that you want to allow.

To forward all inbound WAN traffic on a specific port to a single LAN client, enter the IP address of the target device in the application's **IP Address** field.

Click **Save Changes**.

The following table provides port numbers and protocol information for each port forwarding application listed.

Application Name	Port	TCP*	STCP*	UDP*
DNS	53	Yes	No	Yes
FTP control (command)	21	Yes	Yes	Assigned
FTP data transfer	20	Yes	Yes	Assigned
HTTP	80	Yes	Yes	Assigned
HTTPS	443	Yes	Yes	Assigned
NNTP	119	Yes	No	Assigned
POP3	110	Yes	No	Assigned
POP3S	995	Yes	No	Yes
SMTP	25	Yes	No	Assigned
SecureSMTP	465	Yes	No	No
SNMP	161	Assigned	No	Yes
Telnet	23	Yes	No	Assigned
TFTP	69	Assigned	No	Yes

* **Yes** indicates the protocol is standardized for the port number.
No indicates the protocol is standardized for the port number.
Assigned indicates the port number is assigned by IANA (Internet Assigned Numbers Authority) for protocol use, but may not be standardized.

Custom Applications

You can add up to ten custom applications. Once defined, these applications can be turned on and off the same way as pre-defined applications.

Add a Custom Application: Use this button to add a new row to the custom applications list.

On: Check this box if you want the application to be able to access the Internet (enabling port forwarding).

App Name: Enter a name for the custom application.

IP Address: To forward all inbound WAN traffic on a specific port to a single LAN client, enter the IP address of the target device. To find the IP address of a device, go to the Connected Devices page. **NOTE:** To ensure the device you are forwarding to does not have a different IP address after a reboot, either statically assign the IP address on the client device, or set up a DHCP reservation.

Port Type: Select **Range** or **Translate** from the drop-down list.

Port Numbers: Use the **From** and **To** fields to specify the range of port numbers to be forwarded. **NOTE:** If the application uses a single port instead of a range, type the same value in both the **From** and **To** fields.

For translate ports, use the **Ext.** and **Int.** to specify ports. **NOTE:** Forwarding takes inbound traffic on a port to the same port on a client device. Use translate ports to send traffic to a different port on the client device. For example, instead of having inbound traffic on port 1234 forward to port 1234 of the client device, you can have it forward to port 5678.

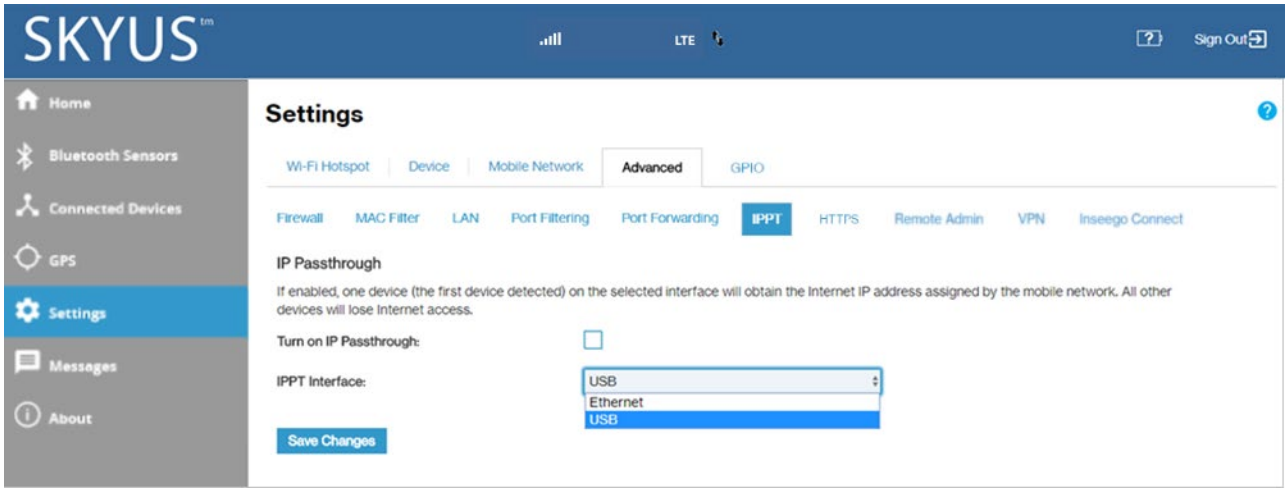
Protocol: Select the protocol used by the port range from the drop-down list (TCP, UDP, or both).

Delete: Check this box to delete a custom application. **NOTE:** Click on the Port Forwarding tab again to remove deleted custom applications from view on the screen.

Click **Save Changes** to save any changes made to the custom applications.

IPPT Tab

Use this tab to enable IP Passthrough on your Skyus 160 Series device. IP Passthrough enables you to assign a public IP address to a device connected on your network.



IP Passthrough

Turn on IP Passthrough: Check the box to enable IP Passthrough. This will enable the first device detected on the specified interface to obtain the IP address assigned by the mobile network.

NOTE: When IPPT is turned on, all other devices will lose internet access.

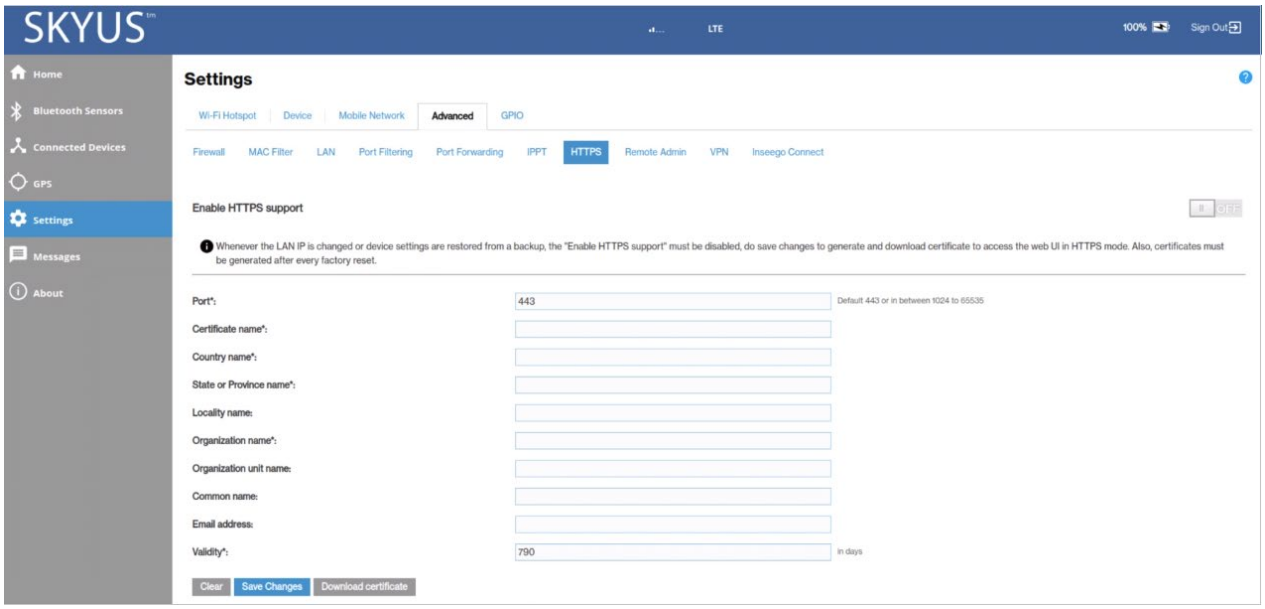
IPPT Interface: Select an interface from the drop-down.

NOTE: When IPPT is enabled on an interface, all other interfaces will be disabled.

Select **Save Changes**.

HTTPS Tab

Use this tab to configure HTTPS and obtain an SSL certificate for a secure connection.



Enable HTTPS support

Before enabling HTTPS support you must fill out the information below, download a certificate, and install it on the client device.

To turn on HTTPS support, move the **ON/OFF** slider to **ON**. To turn off HTTPS support, move the **ON/OFF** slider to **OFF**.

If the LAN IP is changed, device settings are restored from backup, or device is factory reset, you must disable HTTPS support, make and save any changes to the certificate fields, and download and install a new certificate to have a secure connection.

NOTE: Once enabled, if the port is 443 in HTTPS configuration, you can access the Web UI at https://(IP address or domain name). For other ports, you can access at https://(IP address or domain name):(port number).

Certificate Settings

Port: Use the default of 443 or enter a port number between 1024 and 65535.

Certificate name: Enter a name for the self-signed SSL certificate. A certificate with this name and a .crt extension is created. You can install the certificate on the client device to enable secure connection while accessing the Web UI.

Country name: Enter two-letter country code (for example, US) where your company is legally located.

State or Province name: Enter the state or province where your company is legally located.

Locality name: Enter the city where your company is legally located. This is optional.

Organization name: Enter the organization or company name to be used for the SSL certificate.

Organization unit name: Enter an internal department name within the organization. This is optional.

Common name: Enter the fully-qualified domain name (FQDN) (for example, www.example.com) or a suitable name to identify the certificate in a unique way. This is optional.

Email address: Enter an email address to be associated with the certificate. This is optional.

Validity: Enter the number of days for which the certificate is valid.

User the **Clear** button to clear and change entries. **NOTE:** You can only use the Clear button when HTTPS support is not enabled.

Select **Save Changes**. **NOTE:** You can only edit and save changes when HTTPS support is not enabled.

After you have saved changes, use the **Download certificate** button to download a certificate.

Once you have downloaded the SSL certificate, you must install it on the client device and mark it as trusted for secure SSL connection while accessing the Web UI.

Perform the following the steps based on the operating system and browser:

Windows

1. Click on the downloaded certificate file. The Manage Certificates App automatically opens.
2. Select **Install Certificate**.
3. Select **Current User** or **Local Machine** and click **Next**.
4. Select **Place all certificates in the following store** and click **Browse**.
5. Select the **Trusted Root Certification Authorities** folder and click **OK**.
6. Click **Finish**. A message will display that the import was successful.

Ubuntu Linux

1. Install libnss3-tools, if not installed:
   ```
   sudo apt-get install libnss3-tools
   ```
2. Install the downloaded certificate using the following command:
   ```
   certutil -d sql:$HOME/.pki/nssdb -A -t "CP,," -n skyuswebui.crt -
   i skyuswebui.crt
   ```
   NOTE: skyuswebui is the certificate name provided when selecting Save Changes:
3. Check installed certificates.
   ```
   certutil -d sql:$HOME/.pki/nssdb -L
   ```

Mac OS

1. Click on the downloaded certificate file. The Keychain Access App automatically opens with an Add Certificates popup.
2. Click the **Add** button in the popup.
3. Locate the certificate in the Certificates section.
4. Double-click the certificate. In the **trust** section, under **When using this certificate**, select **Always Trust**.

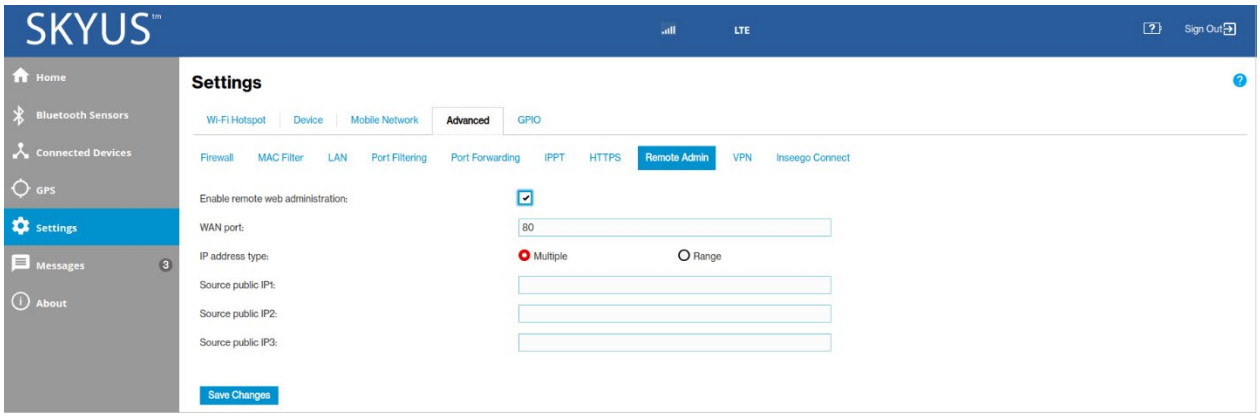
Mozilla Firefox Browser

1. In Firefox, type **about:config** in the address bar and click **Enter**.
2. Accept any warnings and click **Show All**.
3. Scroll down to **security.enterprise_roots.enabled** and click the button on the right to change the value to **true**.
4. Restart the browser.

NOTE: In some Linux variants, with certain versions of Firefox, a warning page may display when you attempt to open the Web UI url. In the warning page, select **Advanced…** and click the button to accept and continue.

Remote Admin Tab

Use this page to enable remote web administration of your Skyus 160 Series router.



Enable remote web administration: To enable remote web administration, move the **ON/OFF** slider to **ON**. To disable remote web administration, move the **ON/OFF** slider to **OFF**.

WAN port: The port number associated with the WAN.

IP address type: Select the desired type of IP address – **Multiple** or **Range**.

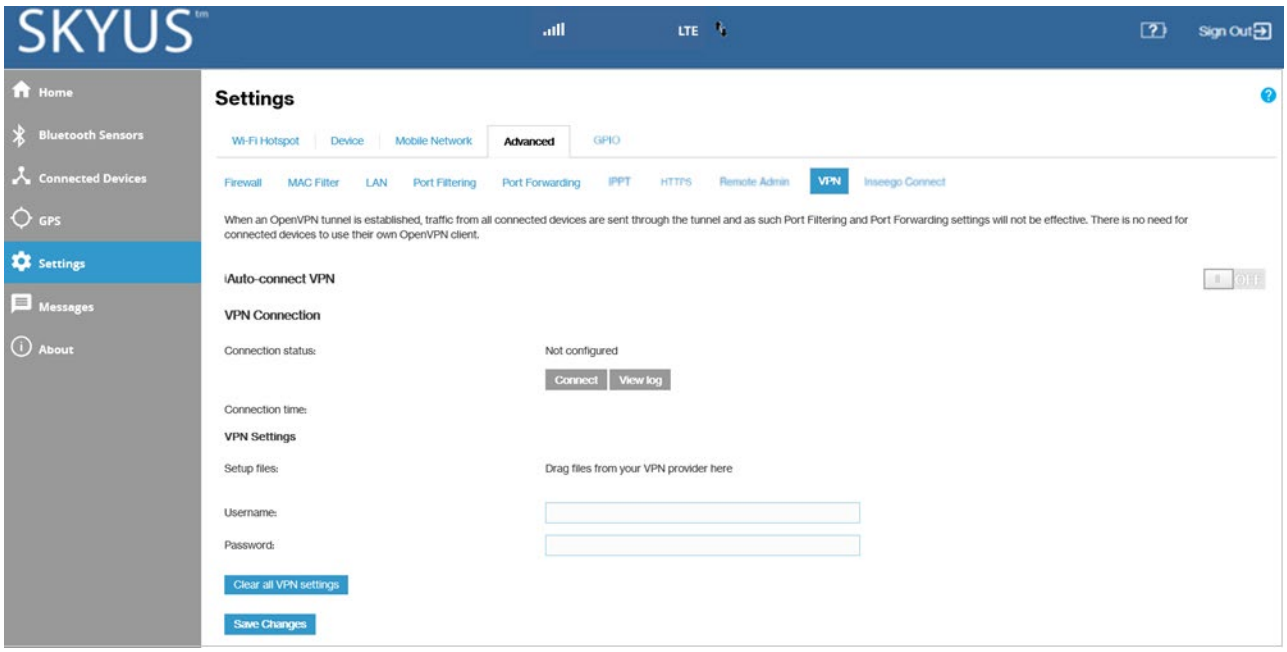
If you select **Multiple** as the IP address type, enter the desired IP addresses in the **Source public IP** boxes.

If you select **Range** as the IP address type, enter the beginning of the range of IP addresses in the **Source public IP from** box, and the end of the range of IP addresses in the **Source public IP to** box.

Select **Save Changes**.

VPN Tab

Use this page to establish a tunnel connection to an OpenVPN server and route all traffic on connected devices through the tunnel.



Auto-connect VPN

When the **Auto-connect VPN ON/OFF** slider is **ON**, the VPN tunnel will automatically be established whenever an Internet connection is made. When **OFF**, the VPN connection must be established manually.

VPN Connection

Connection status: The status of the VPN connection.

Connection time: The amount of time the VPN connection has been established.

VPN Settings

Setup files: Drag and drop the OpenVPN configuration files from your OpenVPN provider in the file upload area.

Username: Enter your OpenVPN connection username here.

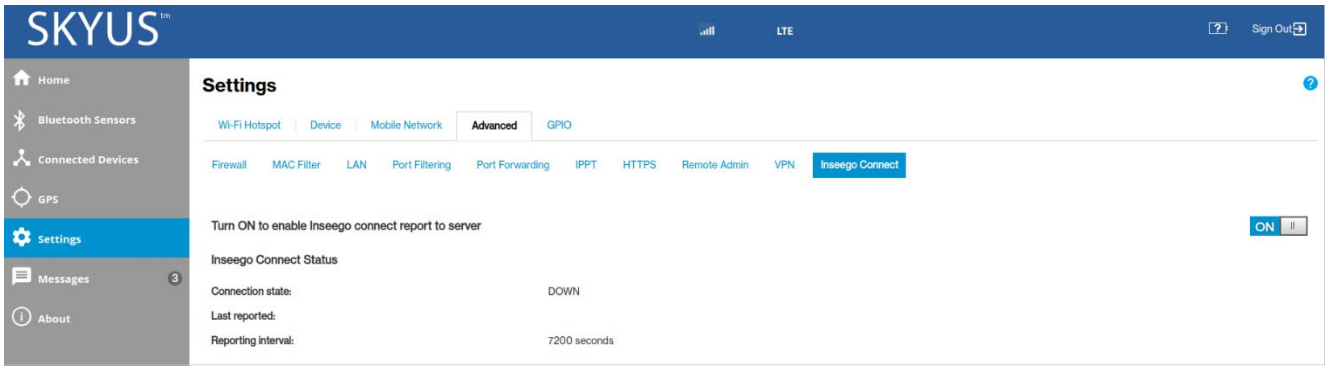
Password: Enter your OpenVPN connection password here.

Clear all VPN settings: This button deletes all VPN files, logs, and resets all VPN settings.

Select **Save Changes**.

Inseego Connect Tab

Use this page to view information about your Skyus 160 Series router's connection with Inseego Connect. Inseego Connect is a cloud platform product that provides 360 degree visibility and secure accessibility into your deployment from a single platform.



By default, the connection to Inseego Connect is active. To turn it off, move the **ON/OFF** slider to **OFF**.

Inseego Connect Status

Connection state: A report on your router's connection to the Inseego Connect server. **Up** indicates Skyus 160 Series router is communicating with Inseego Connect Servers. **Down** means Skyus 160 Series router is not communicating with Inseego Connect servers.

Last reported: The time when your router last sent a packet to the Inseego Connect servers.

Reporting interval: The interval at which your device sends packets to the Inseego Connect server.

5

Accessories

Included Accessories

Optional Accessories

Power Cable

USB Cable and Adapter

Included Accessories

Your Skyus 160 Series router may include the following accessories. These items are also available for individual purchase if needed. To order an accessory, contact your Inseego sales representative.

SKU: SK160NE-ACR Skyus 160 LTE Gateway, AC, Fixed Installation	
Accessory	**PN**
Whip Antennas	ANT-00007
Backup Battery	40123117
120 VAC Power Cable	CBL-00005

SKU: SK160NE-DCR Skyus 160 LTE Gateway, DC, Mobile/Remote Installation	
Accessory	**PN**
Whip Antennas	ANT-00007
Backup Battery	40123117
DC Power and IO Cable with Open Leads	CBL-00004

SKU: SK160AP-ACR Skyus 160 LTE Gateway, AC, Fixed Installation	
Accessory	**PN**
Whip Antennas	ANT-00007
Backup Battery	40123117
120 VAC Power Cable	CBL-00005

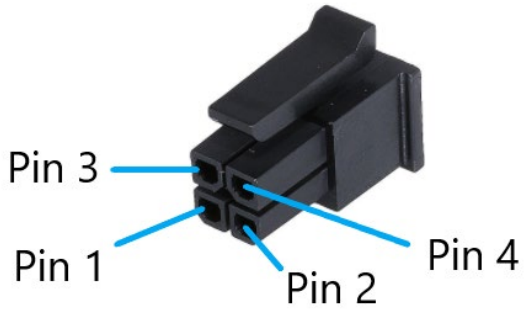
Optional Accessories

The following accessories are optional. These items are available for individual purchase if needed. For more information or to order an accessory, contact your Inseego sales representative.

Accessory	PN
USB Cable (USB A to USB Micro-B)	CBL-00003
USB Cable 120 VAC Adapter	ACC-00028
USB Cable and 120 VAC Adapter	CBL-00007
PoE (Power over Ethernet, 30 W) Injector	ACC-00029
3 ft Ethernet Cable	FW6829
5 ft Ethernet Cable	FW6605
30 ft Ethernet Cable	FW7920
50 ft Ethernet Cable	FW6678
Serial to USB Adapter	TBD

Power Cable

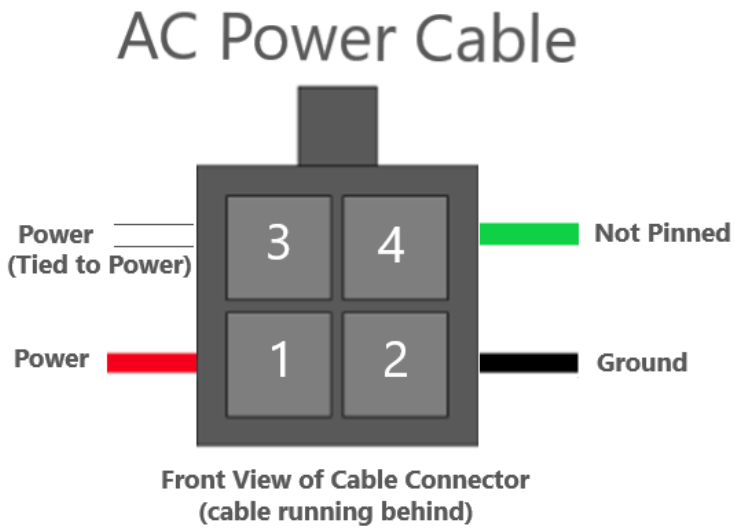
There are two standard power cables available, depending on which SKU is purchased. Both power cables utilize a 4 pin Molex connector.



Pin #	AC Power Cable	DC Power and IO Cable	Color
1	Power	Power	Red
2	Ground	Ground	Black
3	Power (Tied to Power)	Ignition Sense	White
4	NA (Not Pinned)	GPIO	Green

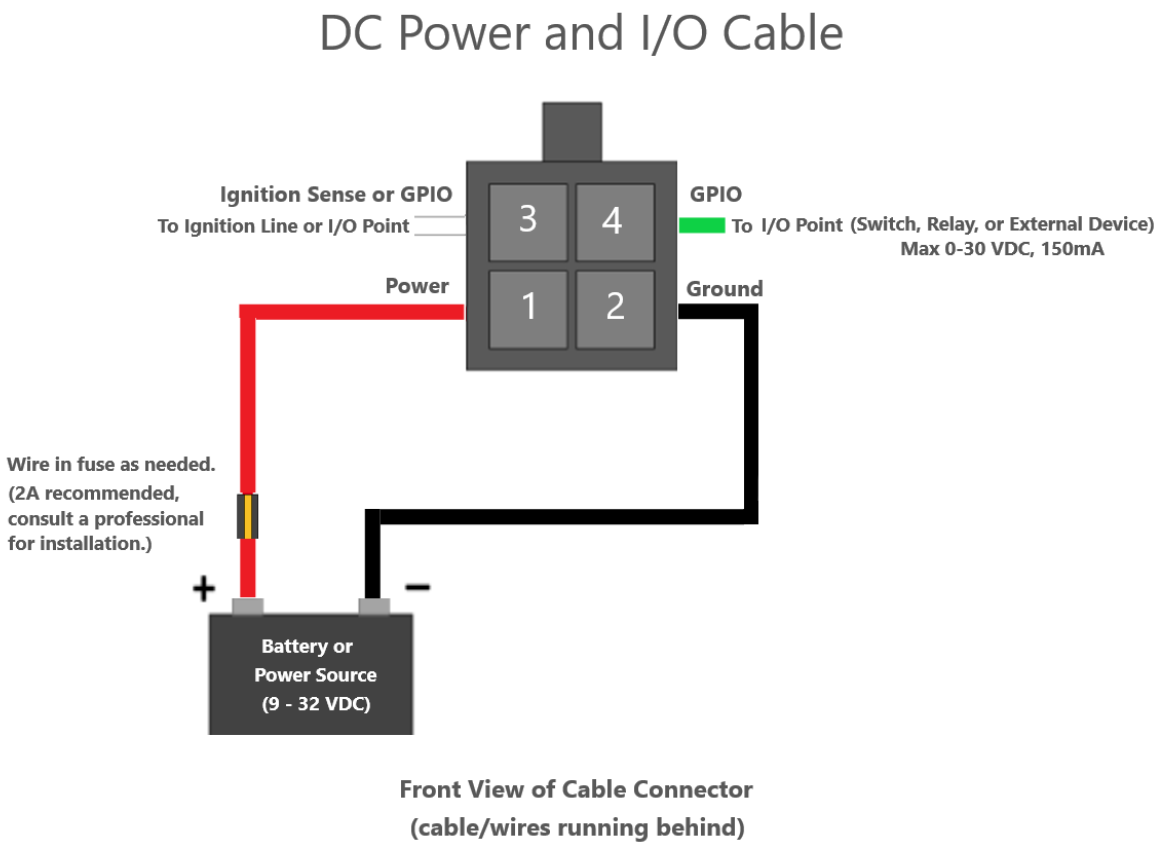
AC Power Cable

The AC power cable connects the Skyus 160 Series device from the 4 pin Molex connector to a 120 VAC outlet.



DC Power and IO Cable

The DC power and I/O cable connects the Skyus 160 Series device from the 4 pin Molex connector to open leads.



NOTE: In mobile applications, the backup battery will ensure the device does not cut out due to power loss during engine cranking.

USB Cable and Adapter

Skyus 160 Series devices can be powered by USB when connected to a powered host device or when connected using a USB to AC adapter. The following are sold as an optional accessory.

USB Cable (CBL-00003)

USB 2.0 A to USB Micro-B, 1.5 m



USB AC Adapter (ACC-00028)

120 VAC 1.5 A to 5 VDC 2 A



6

Product Specifications and Regulatory Information

Product Specifications

Regulatory Information

Wireless Communications

Limited Warranty and Liability

Safety Hazards

Installation and Operating Instructions

Product Specifications

Device

Product:	SK160NE	SK160AP
Model Number:	SKG1EM7455	SKG1EM7430
SKU:	SK160NE-DCR (Mobile/Remote Install) SK160NE-ACR (Fixed Install)	SK160AP-ACR (Fixed Install)
Chassis:	Ruggedized Reinforced Plastic	
Dimensions:	118 x 98 x 33 mm (4.65 x 3.85 x 1.31 in)	
Weight:	250 g (8.5 oz) – with battery	
Mounting:	Integrated Mounting Tabs for #4 or #6 Screws	
SIM:	2 x 4FF Nano SIM, Hinged Slide Lock SIM Sockets, (Accessible in Battery Tray)	
Antennas:	2x SMAs for External Cellular Antennas 1x SMA for External GNSS Antenna Internal Wi-Fi/BT Antennas	
I/O:	1x Ignition Sense or Digital I/O, 1x Digital I/O	
Backup Battery:	4400 mAh Li-ion Rechargeable Pack, 12+ Hours of Active Use	

Environmental

Operating Temperature (with Battery):	0 – 55 °C (32 – 131 °F)
Storage Temperature (with Battery):	-20 – 60 °C (-4 – 140 °F)
Operating Temperature (without Battery):	-30 – 65 °C (-22 – 149 °F)
Storage Temperature (without Battery):	-40 – 85 °C (-4 – 185 °F)

Cellular Bands

Skyus 160 LTE (NE)
LTE: B1-B5, B7, B12, B13, B20, B25, B26, B29, B30, B41(Supports 2 Carrier Aggregation Downlink) 3G (HSPA+, UMTS): B1, B2, B3, B4, B5, B8
Skyus 160 LTE (AP)
LTE: B1,B3, B5, B7, B8, B18, B19, B21, B28, B38-41(Supports 2 Carrier Aggregation Downlink)3G (HSPA+, UMTS): B1, B5, B6, B8, B9, B19 3G (TD-SCDMA): B39

Bluetooth Sensors

Marathon Products EDL-BT04
Marathon Products EDL-BT55

Technology

Wi-Fi:	Wi-Fi 5 (802.11 b/g/n/ac) up to 20 clients
GNSS:	aGNSS (GPS, GLONASS, Galileo), NMEA or TAIP Protocol, SUPL 2.0 Support, Local UDP and Remote Streaming
Networking:	Port Forwarding/Filtering, VPN Support, IP Passthrough, MAC Filtering, Serial over USB, etc.
User Interface:	Skyus Web UI (https://my.skyus/ or 192.168.1.1), Inseego Connect Secure Cloud Platform
Data Interfaces:	1x USB Micro-B (host or device), 1x GB RJ45 10/100/1000 Ethernet (PoE in), Wi-Fi/Bluetooth
Data Rates:	Cat-6 LTE: 300 Mbps Downlink, 50 Mbps Uplink*

Power

5 ± 0.25 VDC @ 2A (powered USB 2.0 connection required) via USB Micro-B Connector
9-32 VDC via 4-pin Connector
PoE in from PoE host (minimum of 802.3af, 15.4 W)

OS Support

Windows 7 or newer
Linux Ubuntu 14.04 or newer, Linux Kernel 2.6.32 or newer

* Theoretical speeds only. Actual speeds depend on carrier network implementation.

Regulatory Information

PRODUCT: **SKYUS 160NE, SKYUS 160AP**

MODEL NUMBER: **SKG1EM7455, SKG1EM7430**

FCCID: **PKRISGSKG1EM7455**

IC ID: **3229A-SKG1EM7455**

FEDERAL COMMUNICATIONS COMMISSION NOTICE (FCC - UNITED STATES)

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.

This device 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 radiated 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.

Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This equipment must be installed and operated in accordance with provide instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

CE RED:

Hereby, Inseego Corp. declares that the radio equipment type is in compliance with

Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at the following internet address: https://www.inseego.com/support/

Notice: The device complies with RF specifications when the device used at least 20cm from human body.

The device operates on the 5150−5350 MHz frequency range. It is restricted indoor environment only. This product can be used across EU member states.



AT	BE	BG	HR	CY	CZ	DK
EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL
PT	RO	SK	SI	ES	SE	UK

Band	Max Power	Frequency
WCDMA BAND I	24 dBm	880-915 MHz
WCDMA BAND VIII	24 dBm	1920-1980 MHz
LTE BAND 1	24 dBm	1920-1980 MHz
LTE BAND 3	24 dBm	1710-1785 MHz
LTE BAND 7	23 dBm	2500-2570 MHz
LTE BAND 20	24 dBm	832-862 MHz
WIFI	16 dBm	2412-2472 MHz
BLE	8 dBm	2402-2480 MHz
5G WIFI	15 dBm	5150MHz-5825MHz

IC:

(EN)The device operates on the 5150~5350 MHz frequency range. It is restricted indoor environment only.

(FR)L'appareil fonctionne sur la plage de fréquences 5150 ~ 5350 MHz. C'est un environnement intérieur restreint seulement.

(EN)This device complies with the applicable industry Canada) License exempt radio apparatus, the operation is authorized under the conditions as follows: (1) this device may not cause interference, and (2) the user of this device must accept any interference caused, even if the interference is likely to affect its performance.

(FR)Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

(EN)Radio frequency (RF) Exposure Information The radiated output power of the Wireless Device is below the industry Canada(IC) radio frequency exposure limits. The Wireless Device should be used in

such a manner such that the potential for human contact during normal operation is minimized. The device has also been evaluated and shown compliant with the IC RF Exposure limits under mobile exposure conditions (antennas at least 20cm from a person’s body).

(FR) informations sur l'exposition de radiofréquences (rf) la puissance de rayonnement de l'appareil sans fil est inférieure à la fréquence radio d'industrie canada (ic) limites d'exposition.l'appareil sans fil devrait être utilisé de façon telle que le potentiel de contact pendant le fonctionnement normal est réduit au minimum. le dispositif a été évalué et qui semble conforme à l'ic des limites d'exposition aux rf sous des conditions d'exposition mobile (antennes d'au moins 20 cm du corps d'une personne).

(EN)The following statement must be included with all versions of this document supplied to an OEM or integrator, but should not be distributed to the end user.

This device is intended for OEM integrators only. Please see the full Grant of Equipment document for other restrictions.

(FR) l'énoncé suivant la déclaration suivante doit être incluse dans toutes les versions de ce document fourni à un oem ou intégrateur, mais ne devrait pas être distribuées à l'utilisateur final.

ce dispositif est destiné aux intégrateurs de oem. voir le document de subvention d'équipement

d'autres restrictions.

(EN) The Innovation, Science and Economic Development Canada certification label of a module shall be clearly visible at all times when installed in the host product; otherwise, the host product must be labelled to display the Innovation, Science and Economic Development Canada certification number for the module, preceded by the word "Contains" or similar wording expressing the same meaning, as follows:

Contains IC: N7NEM7455

whereN7NEM7455 is the module's certification number

(FR)L'étiquette de certification d'un module d'Innovation, Sciences et Développement économique Canada doit être clairement visible en tout temps, une fois installée dans le produit hôte. sinon, le produit hôte doit porter une étiquette indiquant le numéro de certification d'Innovation, Sciences et Développement économique Canada du module, précédé du mot "contient" ou d'un libellé similaire exprimant le même sens, comme suit:

Contient IC: N7NEM7455

OùN7NEM7455 est le numéro de certification du module

Wireless Communications

IMPORTANT: Due to the transmission and reception properties of wireless communications, data occasionally can be lost or delayed.

This can be due to the variation in radio signal strength that results from changes in the characteristics of the radio transmission path. Although data loss is rare, the environment where you operate the modem might adversely affect communications.

Variations in radio signal strength are referred to as fading. Fading is caused by several different factors including signal reflection, the ionosphere, and interference from other radio channels.

Inseego Corp. or its partners will not be held responsible for damages of any kind resulting from the delays or errors in data transmitted or received with the Skyus 160 Series device, or failure of the Skyus 160 Series device to transmit or receive such data.

Limited Warranty and Liability

Inseego Corp. warrants for the 12-month period immediately following receipt of the Product by Purchaser that the Product will be free from defects in material and workmanship under normal use. THESE WARRANTIES ARE EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The exclusive remedy for a claim under this warranty shall be limited to the repair or replacement, at Inseego's option, of defective or non-conforming materials, parts or components. The foregoing warranties do not extend to (I) non-conformities, defects or errors in the Products due to accident, abuse, misuse or negligent use of the Products or use in other than a normal and customary manner, environmental conditions not conforming to Inseego's specification, of failure to follow prescribed installation, operating and maintenance procedures, (II) defects, errors or nonconformities in the Product due to modifications, alterations, additions or changes not made in accordance with Inseego's specifications or authorized by Inseego, (III) normal wear and tear, (IV) damage caused by force of nature or act of any third person, (V) shipping damage, (VI) service or repair of Product by the purchaser without prior written consent from Inseego, (VII) products designated by Inseego as beta site test samples, experimental, developmental, reproduction, sample, incomplete or out of specification Products, or (VIII) returned products if the original identification marks have been removed or altered.

Safety Hazards

WARNING! This equipment is to be installed by qualified personnel only.

NOTE: This product is intended for restricted access whereby access is controlled through the use of a means of security (for example, key, lock, tool, badge access) and personnel authorized for access have been instructed on the reasons for the restrictions and any precautions that need to be taken.

This device is designed to be connected to a grounded power source. The socket (outlet) supplied with a grounded supply source, in order to maintain the security provided by a grounded power source to the device.

Do not operate the Skyus 160 Series device in an environment that might be susceptible to radio interference resulting in danger, specifically:

Areas where prohibited by the law

Follow any special rules and regulations and obey all signs and notices. Always turn off the host device when instructed to do so, or when you suspect that it might cause interference or danger.

Where explosive atmospheres might be present

Do not operate your device in any area where a potentially explosive atmosphere might exist. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Be aware and comply with all signs and instructions.

Users are advised not to operate the device while at a refueling point or service station. Users are reminded to observe restrictions on the use of radio equipment in fuel depots (fuel storage and distribution areas), chemical plants or where blasting operations are in progress.

Areas with a potentially explosive atmosphere are often but not always clearly marked. Potential locations can include gas stations, below deck on boats, chemical transfer or storage facilities, vehicles using liquefied petroleum gas (such as propane or butane), areas where the air contains chemicals or particles, such as grain, dust or metal powders, and any other area where you would normally be advised to turn off your vehicle engine.

Near medical and life support equipment

Do not operate your device in any area where medical equipment, life support equipment, or near any equipment that might be susceptible to any form of radio interference. In such areas, the host communications device must be turned off. The device can transmit signals that could interfere with this equipment.

On an aircraft, either on the ground or airborne

In addition to FAA requirements, many airline regulations state that you must suspend wireless operations before boarding an airplane. Please ensure that the modem is turned off prior to boarding aircraft in order to comply with these regulations. The modem can transmit signals that could interfere with various onboard systems and controls.

While operating a vehicle

The driver or operator of any vehicle should not operate a wireless data device while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some countries, operating such communications devices while in control of a vehicle is an offense.

Electrostatic Discharge (ESD)

Electrical and electronic devices are sensitive to electrostatic discharge (ESD). Macintosh native connection software might attempt to reinitialize the device should a substantial electrostatic discharge reset the device. If the software is not operational after an ESD occurrence, then restart your computer.

ROHS COMPLIANCE

As a part of Inseego's corporate policy of environmental protection, Inseego takes every step to ensure that devices are designed and manufactured to comply to the European Union Directive 2015/863 amending 2011/65/EU for the Restriction of Hazardous Substances (RoHS).

7

Glossary

Glossary

- **4GLTE**—Fourth Generation Long Term Evolution. LTE is a standard for wireless data communications technology and an evolution of the GSM/UMTS standards. The goal of LTE is to increase the capacity and speed of wireless data networks using new DSP (digital signal processing) techniques and modulations that were developed around the turn of the millennium. A further goal is the redesign and simplification of the network architecture to an IP-based system with significantly reduced transfer latency compared to the 3G architecture. The LTE wireless interface is incompatible with 2G and 3G networks, so that it must be operated on a separate wireless spectrum.
- **802.11(a,b,g,n,ac)**— A set of WLAN Wi-Fi communication standards in the 2.4 and 5 GHz frequency bands.
- **APN** — Access Point Name. The name of a gateway between a mobile network and another computer network, often the Internet.
- **bps** — Bits per second. The rate of data flow.
- **Broadband** — High-capacity high-speed transmission channel with a wider bandwidth than conventional modem lines. Broadband channels can carry video, voice, and data simultaneously.
- **DHCP** — Dynamic Host Configuration Protocol. Software found in servers and routers that automatically assigns IP addresses and other configuration data to computers, tablets, printers, and other devices connection to the IP network.
- **DHCP Server** — A server or service with a server that assigns IP addresses.
- **DMZ** — demilitarized zone. A sub-network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.
- **DNS** — Domain Name System. A system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol.
- **Firmware**— A computer program embedded in an electronic device. Firmware usually contains operating code for the device.
- **FTP** — File Transfer Protocol. A standard network protocol used to transfer computer files between a client and server.
- **GB**— Gigabyte. A multiple of the unit byte for digital information storage. Usage depends on context. When referring to disk capacities it usually means 10^9 bytes. It also applies to data transmission quantities over telecommunication circuits.
- **Gbps** — Gigabits per second. The rate of data flow.
- **Hotspot**— A Wi-Fi (802.11) access point or the area covered by an access point. Used for

connecting to the Internet.

- **HTTP**—Hypertext Transfer Protocol. An application-level protocol for accessing the World Wide Web over the Internet.
- **IEEE**—Institute of Electrical and Electronics Engineers. An international technical/professional society that promotes standardization in technical disciplines.
- **IMAP**— Internet Message Access Protocol. An Internet standard protocol for accessing email from a remote server from email clients. IMAP allows access from multiple client devices.
- **IMEI**— International Mobile Equipment Identity. Used in LTE networks to identify the device. It is usually printed on the device and can often be retrieved using a USSD code.
- **IP**— Internet Protocol. The mechanism by which packets are routed between computers on a network.
- **IPType**— The type of service provided over a network.
- **IPaddress**—Internet Protocol address. The address of a device attached to an IP network (TCP/IP network).
- **ISP**—Internet Service Provider. Also referred to as the service carrier, an ISP provides Internet connection service (*See* Network Operator).
- **Kbps**— Kilobits per second. The rate of data flow.
- **LAN**— Local Area Network. A type of network that lets a group of computers, all in close proximity (such as inside an office building), communicate with one another. It does not use common carrier circuits though it can have gateways or bridges to other public or private networks.
- **MACAddress**—Media Access Control. A number that uniquely identifies each network hardware device. MAC addresses are 12-digit hexadecimal numbers. This is also known as the physical or hardware address.
- **Mbps**— Megabits per second. The rate of data flow.
- **MSID**— Mobile Station IDentifier. A number for a mobile phone that identifies that phone to the network.
- **NetworkOperator**—The vendor that provides your wireless access. Known by different names in different regions, some examples are: wireless provider, network provider, or cellular carrier.
- **NetworkTechnology**—The technology on which a particular network provider's system is built; such as LTE or GSM.
- **NMEA port** — National Marine Electronics Association port. The port through which applications can access a GPS data stream.
- **NNTP** —Network News Transfer Protocol. The primary protocol used to connect to Usenet servers and transfer news articles between systems over the Internet.

- **POP3**—Post Office Protocol 3. A protocol in which email is received and held for you by your Internet server until you download it.
- **Port**— A virtual data connection used by programs to exchange data. It is the endpoint in a logical connection. The port is specified by the port number.
- **PortForwarding**— A process that allows remote devices to connect to a specific computer within a private LAN.
- **PortNumber**— A 16-bit number used by the TCP and UDP protocols to direct traffic on a TCP/IP host. Certain port numbers are standard for common applications.
- **PRL**— Preferred Roaming List. A list that your wireless phone or device uses to determine which networks to connect with when you are roaming (Network operator specific).
- **Protocol**— A standard that enables connection, communication, and data transfer between computing endpoints.
- **Proxy**— A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.
- **RADIUS**— Remote Authentication Dial-In User Service. A networking protocol, operating on port 1812, that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.
- **Router**— A device that directs traffic from one network to another.
- **RP-SMA** — Reverse Polarity Sub-Miniature Version A. A connector interface with a screw-type coupling mechanism for coaxial cables.
- **RSSI**— Received signal strength indicator.
- **SIM**— Subscriber Identification Module. Found in LTE and GSM network technology, the SIM is a card containing identification information for the subscriber and their account. The SIM card can be moved to different devices.
- **SMA** — Sub-Miniature Version A. A variation of the SMA connector where the gender of the interface is reversed.
- **SMTP** — Simple Mail Transfer Protocol. The standard protocol for sending emails across the Internet.
- **SNMP** — Simple Network Management Protocol. An Internet protocol used to manage and monitor network devices and their functions.
- **SSID**— Service Set IDentifier. The name assigned to a Wi-Fi network.
- **TCP/IP**—Transmission Control Protocol/Internet Protocol. The set of communications protocols used for the Internet and other similar networks.
- **TFTP**—Trivial File Transfer Protocol. An Internet software utility for transferring files that is simpler to use than FTP, but does not provide user authentication and directory visibility supported by FTP.

- **Telnet** — A user command and underlying TCP/IP protocol that allows a user on one computer to log into another computer that is part of the same network.
- **TTY** — Text Telephones (TTY), also known as Telecommunications Device for the Deaf (TDD), are used by the deaf, hard–of–hearing, and individuals with speech impairments to communicate.
- **UDP** — User Datagram Protocol (UDP) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.
- **USB** — Universal Serial Bus. A connection type for computing device peripherals such as a printer, mobile modem, etc.
- **USB Port Types** — The USB ports on computers and hubs have a rectangular Type A socket, and peripheral devices have a cable with a Type A plug. Peripherals that do not have an attached cable have a square Type B socket on the device and a separate cable with a Type A and Type B plug. Ports and connectors are available in different sizes (for example, standard, mini, and micro).
- **USSD** — Unstructured Supplementary Service Data (USSD), also known as "Quick code" or "Feature code", is a communications protocol used to send data between a mobile device and network service provider.
- **VPN** — Virtual Private Network. A secure private network that runs over the public Internet. Commonly used to connect to an office network from elsewhere.
- **Wi-Fi** — Any system that uses the 802.11 standard developed and released in 1997 by the IEEE.
- **Wi-Fi 5** — The fifth generation of Wireless Fidelity, using 802.11ac on 5 GHz. This standard was developed and released in 2013.
- **Wi-Fi Client** — A wireless device that connects to the Internet via Wi-Fi.
- **WPA/WPA2** — Wi-Fi Protected Access. A security protocol fir wireless 802.11 networks from the Wi-Fi Alliance.