USER GUIDE

inseego

Inseego Wavemaker™ PRO
5G Industrial Gateway S2000e

INSEEGO COPYRIGHT STATEMENT

© 2021 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 Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp.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: 90029653 Rev E

Contents

Introduction and Getting Started 5
Overview 6
Key Features 6
Description 7
Front View 7
Back View 7
Indicator LEDs 8
Getting Started 9
Installing a SIM Card 9
Installation Options 10
Identifying a Location 12
Power Options 13
Connecting Devices to the Gateway 15
Connecting to the Web UI 15
Description 16
Front View 16
Back View 16
Indicator LEDs Resetting your Gateway 17
Resetting with the RESET Button 17
Resetting from the Admin Web UI 17
Technical Support 18
Software Configuration 19
Overview 20
Home Page 20
Side Menu 20
Header Icons 21
Getting Help 21
Admin Password 22
Changing the Admin Password 22
Managing Data Usage 23
Data Usage Page 24
Managing Settings 26
Preferences Tab 27
Software Update Tab 28
Backup and Restore Tab 29
GPS Tab 31
GPIO Tab 36
Advanced Tab 37
Viewing Info About the Gateway 38
Internet Status Tab 39
Internet Sessions Tab 41
Diagnostics Tab 42
Device Info Tab 43
Logs Tab 44
Getting Support 45
Customer Support Tab 45
Advanced Settings 46
Overview 47
Using Advanced Settings 47
Cellular Tab 48

Manual DNS Tab 49
SIM Tab 50
LAN Tab 53
Firewall Tab 55
MAC Filter Tab 56
Port Filtering Tab 57
Port Forwarding Tab 60
Inseego Connect Tab 63
HTTPS Tab 64
Remote Admin Tab 67
Product Specifications and Regulatory Information 68
Product Specifications 69
Device 69
Environmental 70
Cellular Technology 70
Bluetooth 70
Positioning 70
Networking 70
Security 71
Regulatory Information 72
Product Certifications and Supplier's Declarations of Conformity 76
Wireless Communications 76
Limited Warranty and Liability 77
Safety Hazards 78
Glossary 79
Glossary 80

1

Introduction and Getting Started

Overview

Description

Indicator LEDs

Getting Started

Description

Resetting your Gateway

Technical Support

Overview

The 5G Industrial Gateway S2000e delivers ultra-reliable cellular Internet service with 5G NR connectivity. The S2000e supports any public or private network while also supporting all carriers. It connects to any routing system or remote endpoint with Ethernet or USB. The S2000e provides continuous multi-Gigabit connectivity and sub-second latency for enterprise settings.

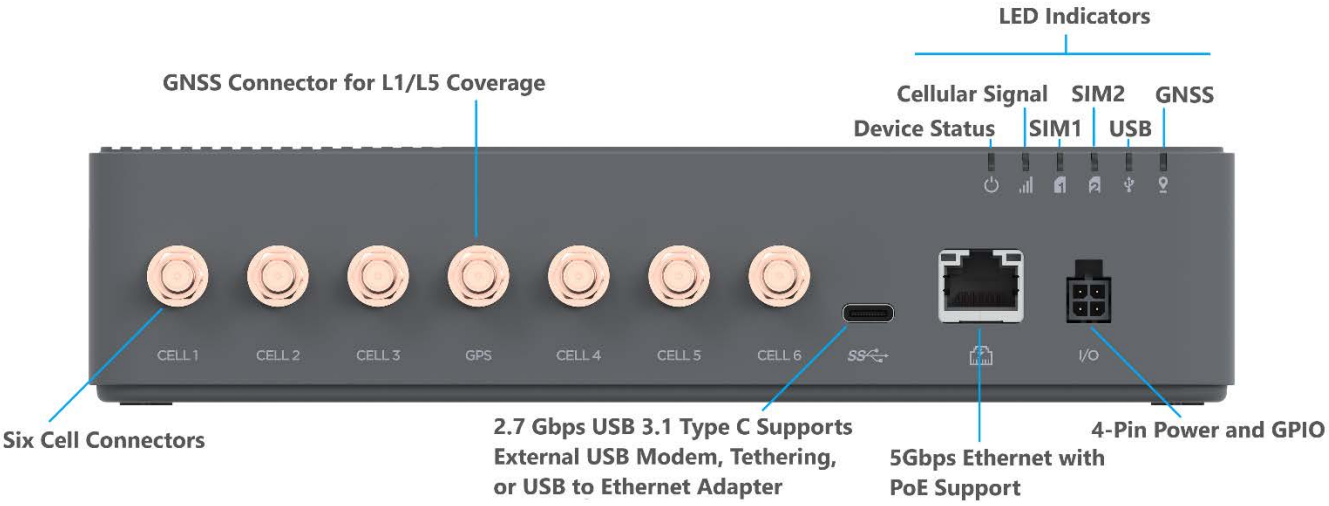
Key Features

- Ultra reliable global connectivity with support for any public or private network and supporting all carriers in every region.
- Multi-gig speeds for any enterprise needs, such as large file transfers or multiple 4k video streams.
- Millisecond latency allow rapid communications and reactions to changes in remote or factory automation applications.
- Class-leading thermal design allows for operation in extreme temperatures from -30°C to 65°C (-22 to 158°F) while running multi-gigabit throughput.
- Complete device management, visibility, and security with the Inseego Manage software suite.

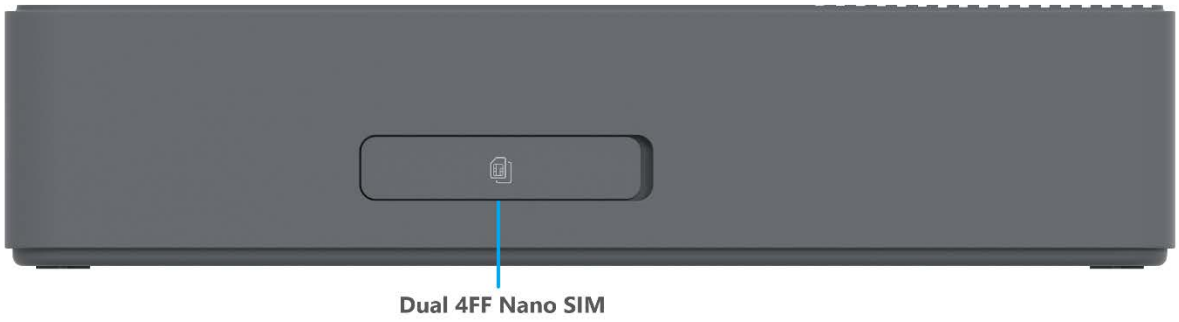
Description

Inside the box you will find a 5G Industrial Gateway S2000e and a 4-pin power cable. Additional accessories, including antennas, brackets, and other power equipment, are available for individual purchase. To order an accessory, contact your Inseego sales representative.

Front View



Back View



Indicator LEDs

The S2000e has indicator LEDs that communicate current states for the device.

LED	LED Color	Operation	Meaning
Device Status	**White**	Solid Slow Blink*	Starting Up or Updating Low Power Mode
	Red	Solid	Device On, No Connection
	Yellow	Solid	Device On, External Connection
	Green	Solid	Device On, Internal LTE Connection
	Blue	Solid	Device On, Internal 5G Connection
Cellular Signal	**Red**	Solid	RSRP >/= -102 dBm
	Yellow	Solid	RSRP -90 dBm - -102 dBm
	Green	Solid	RSRP -80 dBm - -90 dBm
	Blue	Solid	RSRP <= -80 dBm
SIM (SIM1 and SIM2)	**Off**	Off	No SIM
	Red	Solid	SIM Error
	Yellow	Solid Blinking†	SIM Installed, Slot Inactive SIM Installed, Slot Active, Not Connected
	Green	Solid	SIM Installed, Slot Active, Connected
USB	**Off**	Off	No USB
	Red	Solid	USB Error
	Yellow	Solid Blinking	USB Connected, Not Active USB Active, Not Connected
	Green	Solid	USB Connected, Active
GNSS	**Off**	Off	No SIM
	Red	Solid	GPS Error
	Yellow	Blinking	Searching/Acquiring
	Green	Solid	Signal Acquired

The Ethernet connector port also has an indicator LED.

LED	Color	Operation	Meaning
Ethernet Speed	**Green** **Yellow**	Solid Solid	5GbE 100Mbps – 2.5GbE
Ethernet Activity	**Green**	Solid Blinking	No activity Activity

* Slow Blink is one second on, five seconds off.

† Blinking is one second on, one second off.

Getting Started

This section provides instructions for getting your S2000e up and running, as well as reset and support information.

Installing a SIM Card

Your SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The S2000e supports only Nano SIM cards.

CAUTION! Always use a factory-made SIM card supplied by the service provider. Do not bend or scratch your SIM card. Avoid exposing your SIM card to static electricity, water, or dirt.

To install a SIM card:

1. Remove the cover from the SIM slots on the back of the device.

2. If necessary, remove the SIM card from the protective sleeve, being careful not to touch the gold colored contacts.
3. Insert the SIM card into the appropriate slot with the gold-colored contact points facing down.

   NOTE: The SIM card will click when properly installed.

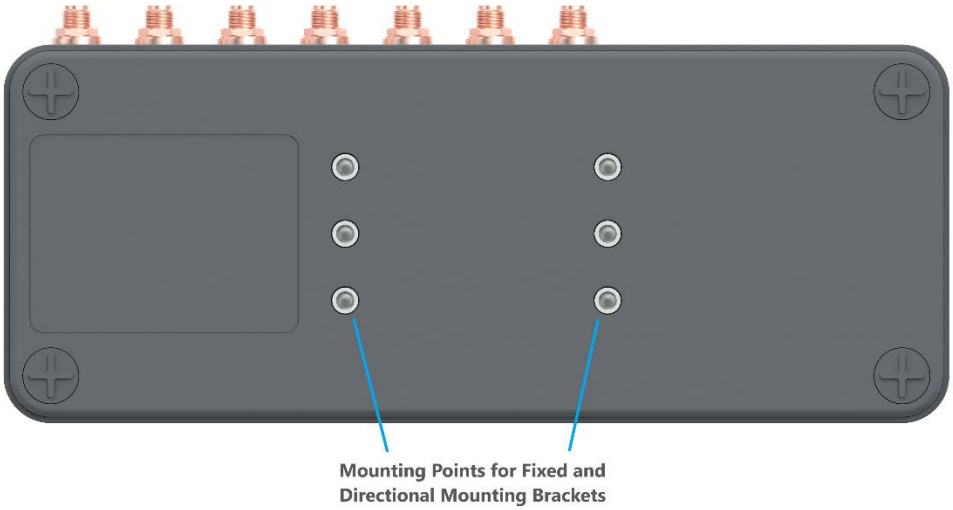
4. Replace the cover.

NOTE: Should your SIM card be lost or damaged, contact your network operator.

Installation Options

You can install the S2000e to a wall or pole, or in a cabinet or enclosure.

The S2000e has integrated mounting points that allow you to mount to a wall or pole with brackets.



Fixed Bracket

You can use a fixed bracket when installing your S2000e on a wall.

Adjustable Bracket

You can use an adjustable bracket when installing your S2000e on a wall or pole. An adjustable bracket allows you to point your S2000e directly at an indoor 5G node. For the best signal with an adjustable bracket, point the top of the device directly towards a 5G node or tower.

DIN Rail

If you are installing in a cabinet or enclosure, use a customer-provided DIN rail.

Identifying a Location

Use the Inseego Connect App to identify the optimal location for your S2000e.

1. Scan the QR code to install the Inseego Connect App from AppStore or Google Play, or visit https://inseego.com/inseego-connect-get-app to download the App.

2. Follow instructions within the Inseego Connect App to connect to your S2000e and perform a location survey to identify the ideal location for your S2000e.

Power Options

Your S2000e has four power options:

- 4-Pin AC Power Supply
- 4-Pin DC Power and I/O Supply
- 30W PoE Injector
- 60W PoE Injector

NOTE: If an additional power option is needed, please contact Inseego sales.

Connecting 4-Pin DC Power (for Cabinet/Enclosure Installations)

WARNING: Electrical installations can be hazardous and should be performed only by licensed professionals.

Consider the following when installing your S2000e with DC power:

- Ensure easy access for connecting cables.
- Ensure minimum bend radius for cables.
- Avoid sharp edges or existing wiring.
- Avoid proximity to high amperages or extreme temperatures.
- Avoid direct exposure to harmful elements such as water, dust, and heat.

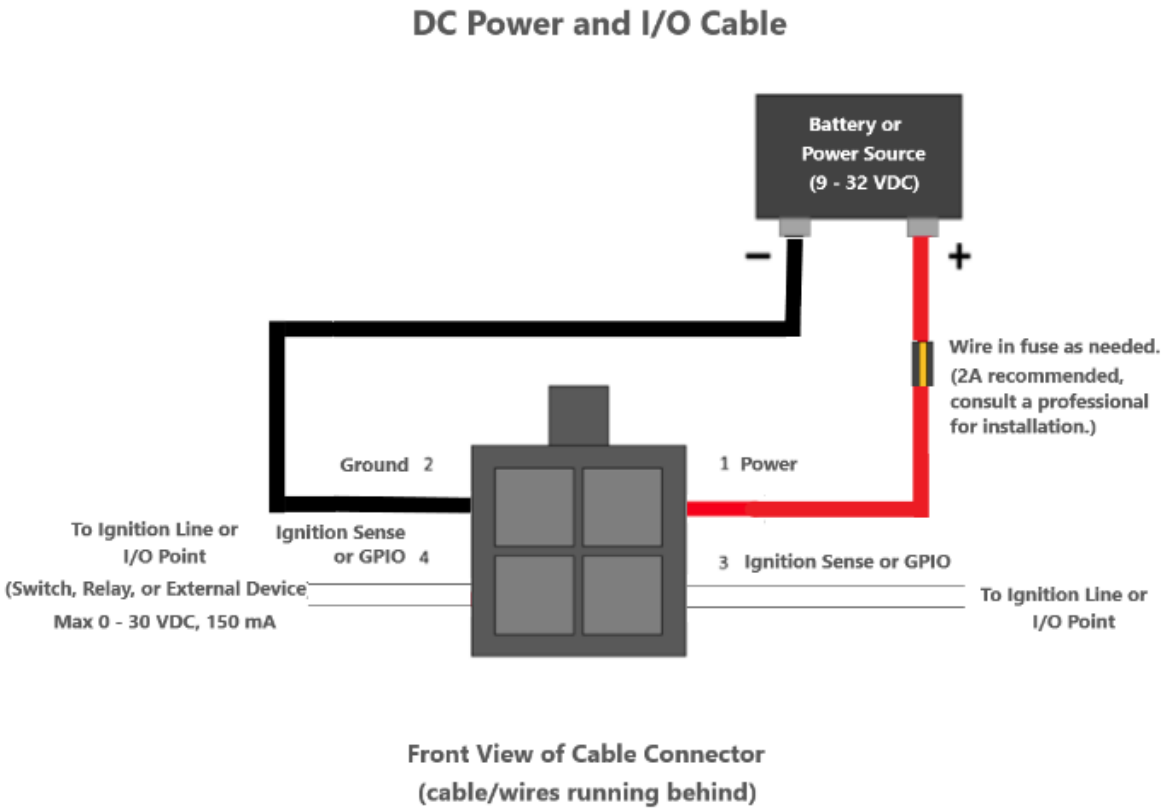
Installing and Grounding

To install and ground your device:

1. Use a DIN rail to secure the device in place.
2. Ground the device.
3. If you are installing in a high vibration setting, use cable strain relief to reduce the effects of vibration. Install the strain relief to the same surface as the S2000e, within eight inches of the device. This allows the device and cable to vibrate together. Ensure the cable is not pulling on the power connection.

Connecting to a DC Power Source

The DC cable harness includes power and I/O pins.



To connect your S2000e to a DC power source:

1. Disconnect the power source, if applicable.
2. Connect the black (ground) wire on the DC power cable to the cabinet, enclosure, or chassis ground.
3. Ensure the S2000e device is also grounded.
4. Fuse the red power wire on the DC power cable to the power source through the fuse box, if appropriate.
5. Connect the power wire on the DC power cable to the power source.
6. If you are using Ignition Sense, connect an I/O wire to the ignition switch.

   NOTE: Ignition Sense ensures a controlled shutdown of the S2000e when the ignition is turned off. You can configure a delay between the time the ignition shuts off and when the S2000e shuts off. See GPIO Settings on page 36.
7. Connect the DC power cable to the S2000e.
8. Reconnect the power source, if applicable.

Connecting Devices to the Gateway

You can connect to the S2000e gateway with Ethernet, USB, or digital I/O.

Connecting Devices with Ethernet

You can connect to a device via Ethernet.

1. Plug one end of an Ethernet cable into the Ethernet port on the S2000e.
2. Plug the other end of the cable into the Ethernet port of the device you wish to connect.

NOTE: If you are connecting devices via Ethernet using your S2000e as a Dynamic Host Configuration Protocol (DHCP) server on a switch, select **Setting> Advanced > LAN** to view and configure DHCP settings.

Connecting Devices with USB

You can tether to a device with the USB-C port.

1. Connect the USB-C end of a USB cable into the USB-C port on the S2000e. Or, connect a wireless USB-C adapter
2. Connect the USB-A end of a USB cable into the device you wish to connect.

Connecting I/O Devices

You can use the configurable digital GPIO pins to provide on/off data and functionality.

I/O inputs convey information to the S2000e about the state of an external device or system, or can provide Ignition Sense.

I/O outputs are used for the S2000e to tell a device or system to turn on or off.

Connecting to the Web UI

Once your S2000e is connected to a network with a device that supports Web browsing, you can use the Web User Interface to customize settings, change your password, and access information.

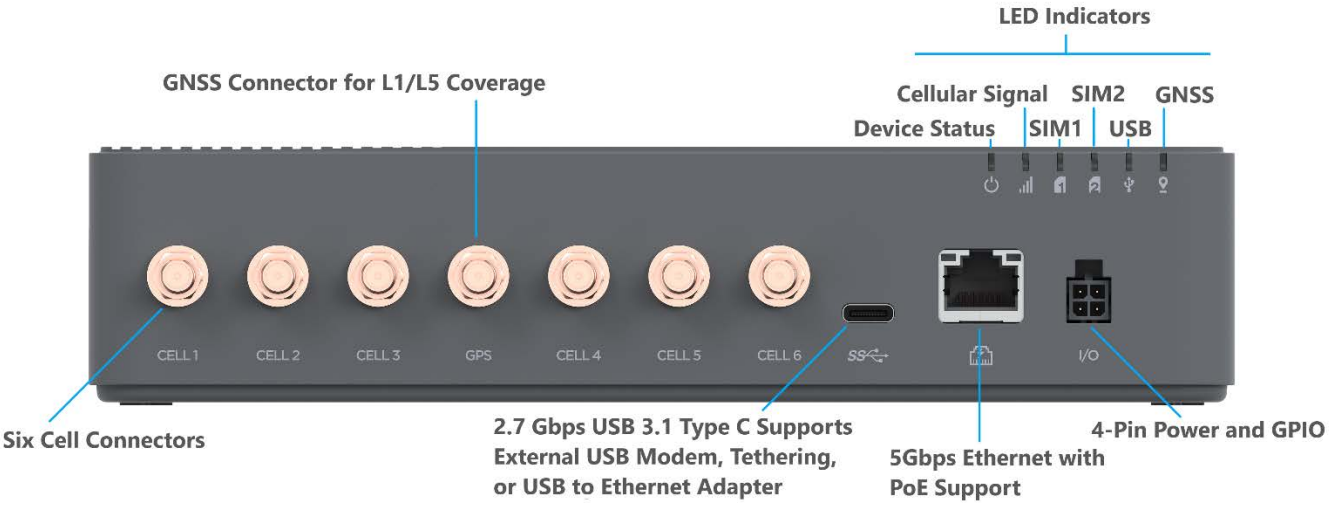
On a device connected to the S2000e, open any Web browser and go to http://192.168.1.1 .

Select Sign In (in the top-right corner of the screen), and enter the Admin password printed on the label of the S2000e.

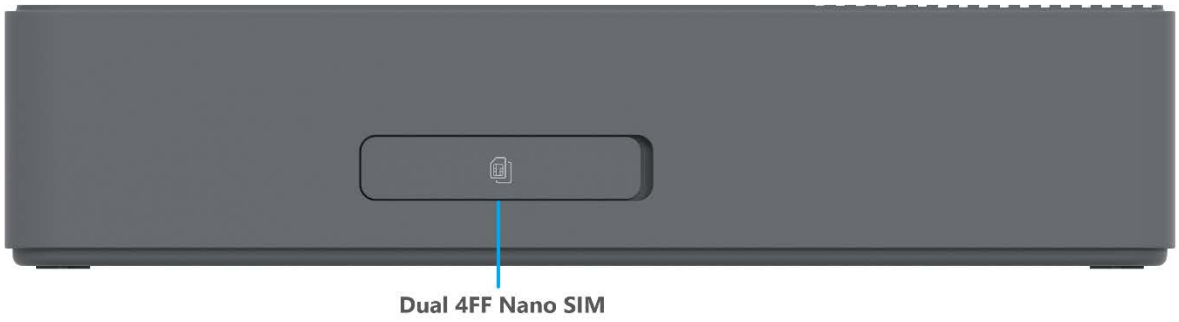
Description

Inside the box you will find a 5G Industrial Gateway S2000e and a 4-pin power cable. Additional accessories, including antennas, brackets, and other power equipment, are available for individual purchase. To order an accessory, contact your Inseego sales representative.

Front View



Back View



Indicator LEDs Resetting your Gateway

This section provides information on general care and restoring your S2000e to factory default settings.

You can reset your S2000e to factory settings using the RESET button on the device or from the Admin Web UI.

CAUTION! Resetting returns your S2000e to factory settings.

Resetting with the RESET Button

The master reset button is in a small hole located in the SIM compartment on the back of the device. This button returns the device to factory settings, including resetting the admin password.

To reset the S2000e:

1. Remove the SIM cover.
2. Place one end of an unfolded paper clip into the master reset button hole.

   To restart the S2000e: Press the paper clip on the button for three to five seconds. The S2000e will restart.

   To restore the S2000e to factory default settings: Press and hold the RESET button for over five seconds. This resets all settings to their factory default values.

Resetting from the Admin Web UI

To reset the S2000e from the Admin Web UI, select **Settings > Backup and Restore** and select **Restart Device** to restart the S2000e, or **Restore Factory Defaults** to reset all settings to their factory default values.

Technical Support

IMPORTANT: Before contacting Support, be sure to restart both your connected device and your S2000e and ensure that your SIM card is inserted correctly.

Customer Service and Troubleshooting

Contact your reseller for assistance.

More Information

Documentation for your S2000e is available online. Go to www.inseego.com/support-documentation. Or, from the Admin website, select **Support > Customer Support**.

2

Software Configuration

Overview

Admin Password

Managing Data Usage

Managing Settings

Viewing Info About the Gateway

Getting Support

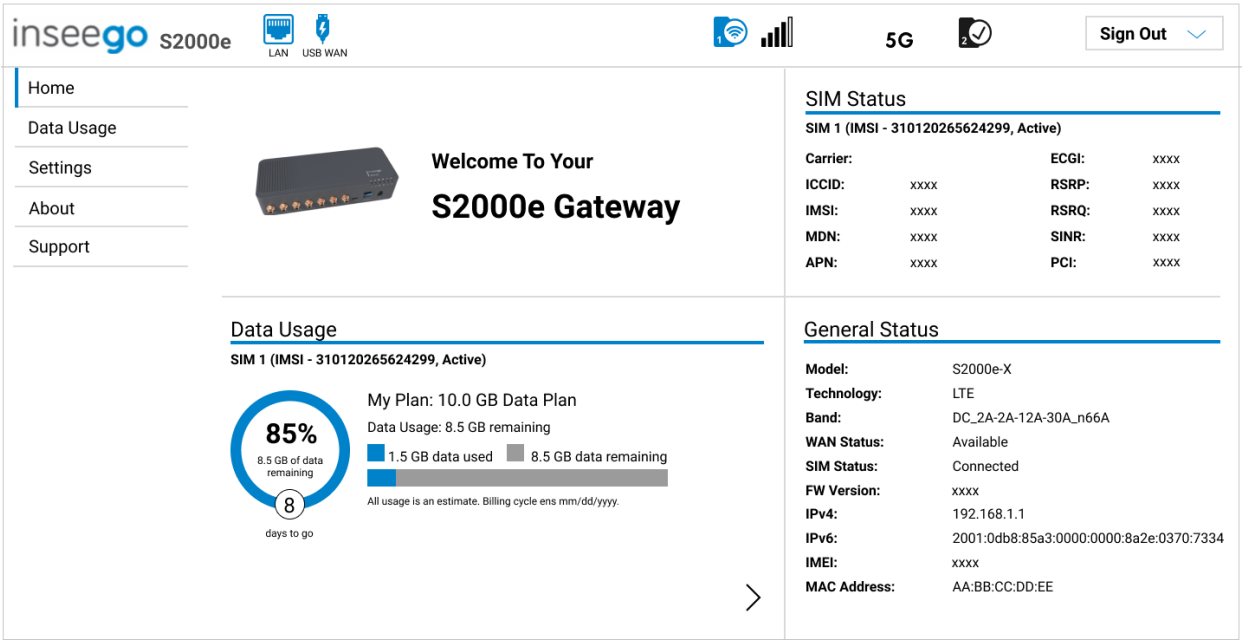
Overview

Use the S2000e Admin Web User Interface to manage your gateway experience. On a computer or device connected to your S2000e, open any Web browser and go to http://192.168.1.1.

Home Page

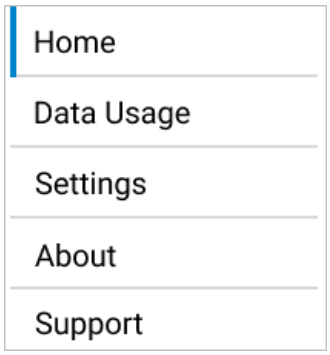
The Home page is the local gateway to configuring and managing your S2000e. It displays the SIM status, data usage and provides general status information.

Click › in the bottom-right corner of a panel to access screens with further information and options.



Side Menu

Each subscreen in the S2000e includes a menu on the left, which you can use to return to the Home page or jump to other pages. The current page is indicated by a blue bar.



Header Icons

The top of each S2000e Web UI page displays status indicators and icons.

Header Icon		Description
LAN (Blue)		Routed
LAN (Black)		Available/Online
LAN (Grayed Out)		Disabled/Offline/No Physical Connection
USB (Blue)		Routed
USB (Black)		Available/Online
USB (Grayed Out)		Disabled/Offline/No Physical Connection
Network Signal Strength		Network Signal Strength Indicator. More bars indicate more signal strength.
SIM (Blue)		Routed
SIM (Black with Checkmark)		Available/Online
SIM (Grayed Out)		Disabled/Offline/No SIM

Getting Help

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

Admin Password

The Admin password is what you use to sign into the S2000e. A default Admin password is assigned to each individual device and is printed on the label of the device. You can change the Admin password to something easier to remember, and set up a security question that will help you securely recover your password if you forget what you changed it to.

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

Changing the Admin Password

To change the Admin password:

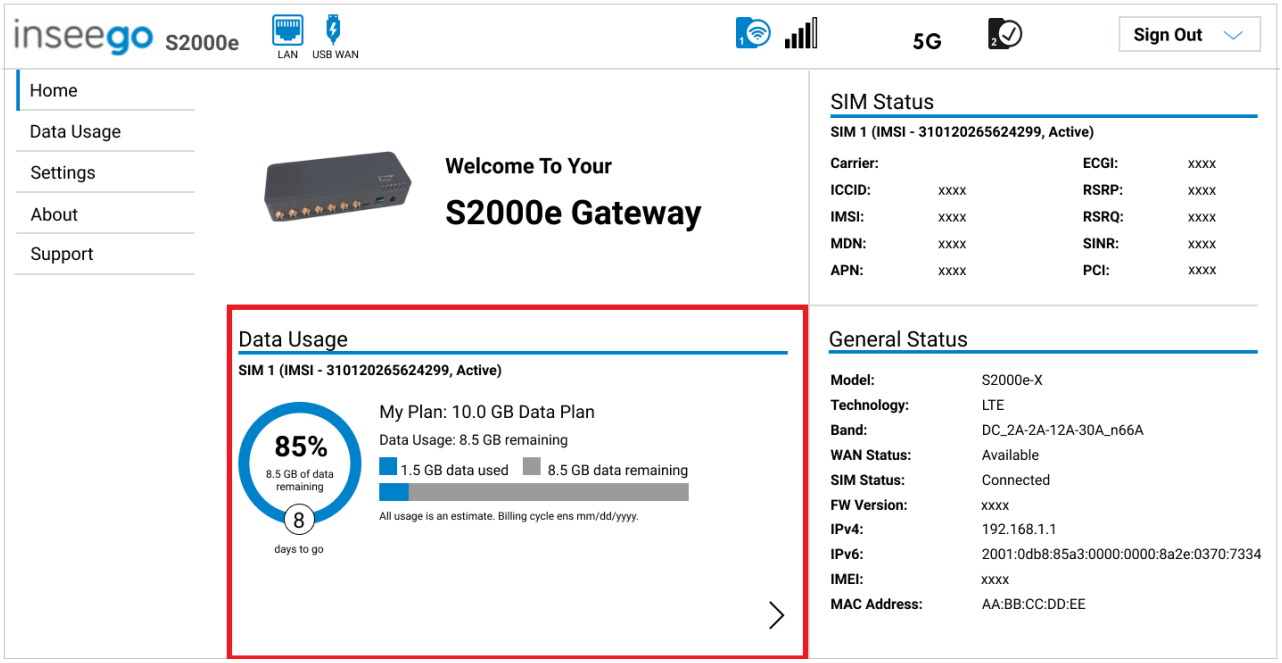
1. Click the down arrow next to **Sign Out** in the top-right corner of any Web User Interface page and select **Change Password**.
2. Enter your current Admin password, then enter a new password and confirm it.
3. Select a security question from the drop-down list and type an answer to question in the **Answer** field. **NOTE:** Answers are case-sensitive.
4. Click **Save Changes**.

The next time you sign in to the S2000e, 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.

Managing Data Usage

You can monitor and manage data usage on your S2000e using the Data Usage page.

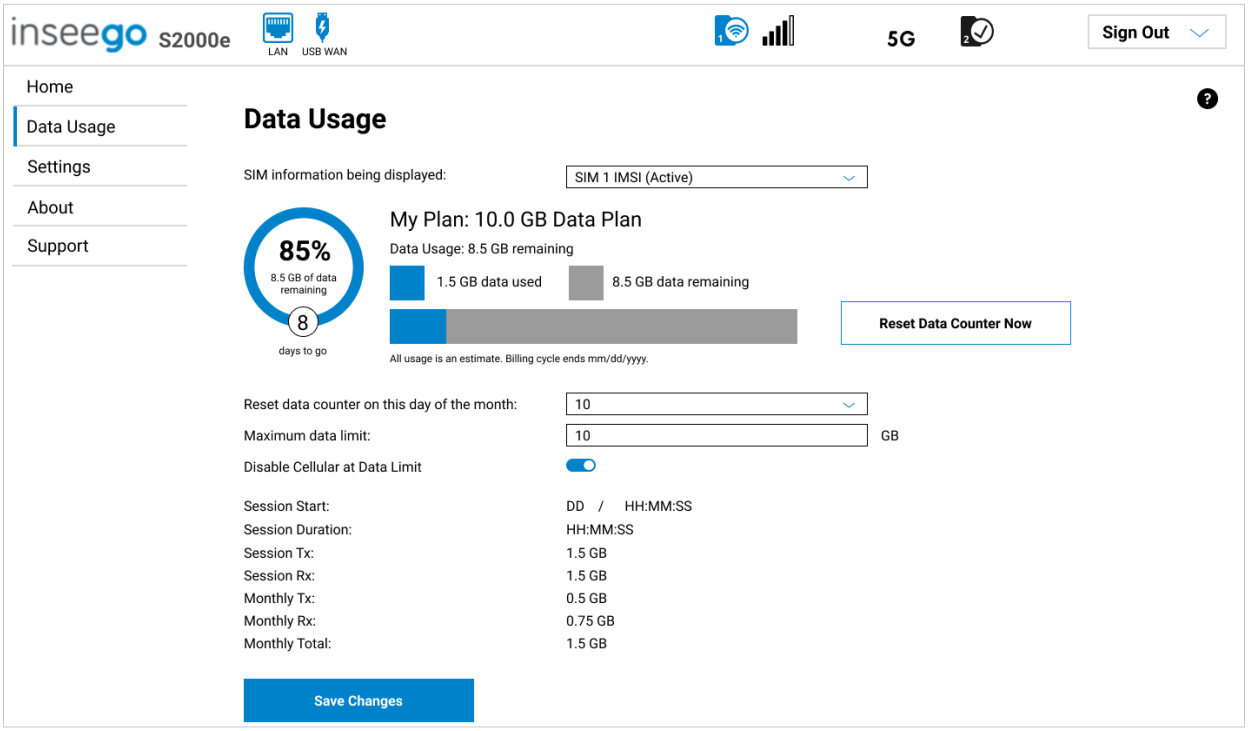
On the Web UI Home page, the Data Usage panel shows current data usage information.



To manage or view data usage, select > from the Home page Data Usage panel or select **Data Usage** from the Web UI side menu. The Data Usage page appears.

Data Usage Page

Use the Data Usage page to view details and manage your S2000e data usage.



SIM information being displayed: Use the drop-down to change the SIM on which data usage is displayed.

The data usage graph displays vary according to plan, but generally include:

- Estimated percentage of data remaining for the current billing cycle
- Number of days left in the billing cycle
- Data limit on your plan
- Estimated amount of data used in the current billing cycle
- Estimated amount of data remaining for the current billing cycle
- Date the billing cycle ends

Use the **Reset Data Counter Now** button to restart the data usage shown on this page to zero.

Reset data counter on this day of the month: Use the drop-down to select a day of the month for the counter displayed on this page to reset.

Maximum data limit: Enter a maximum data limit, if desired.

Disable Cellular at Data Limit: When the slider is on, data is disabled after reaching the maximum data limit set above.

Session Start: The date and time the current Internet session began.

Session Duration: The amount of time that has elapsed since the connection for the current Internet session was established.

Session Tx: The amount of data transmitted for the current Internet session. This counter starts at zero when the connection is established.

Session Rx: The amount of data received for the current Internet session. This counter starts at zero when the connection is established.

Monthly Tx: The amount of data transmitted for the current billing cycle.

Monthly Rx: The amount of data received for the current billing cycle.

Monthly Total: The total amount of data for the current billing cycle.

Select **Save Changes** to enact changes.

Managing Settings

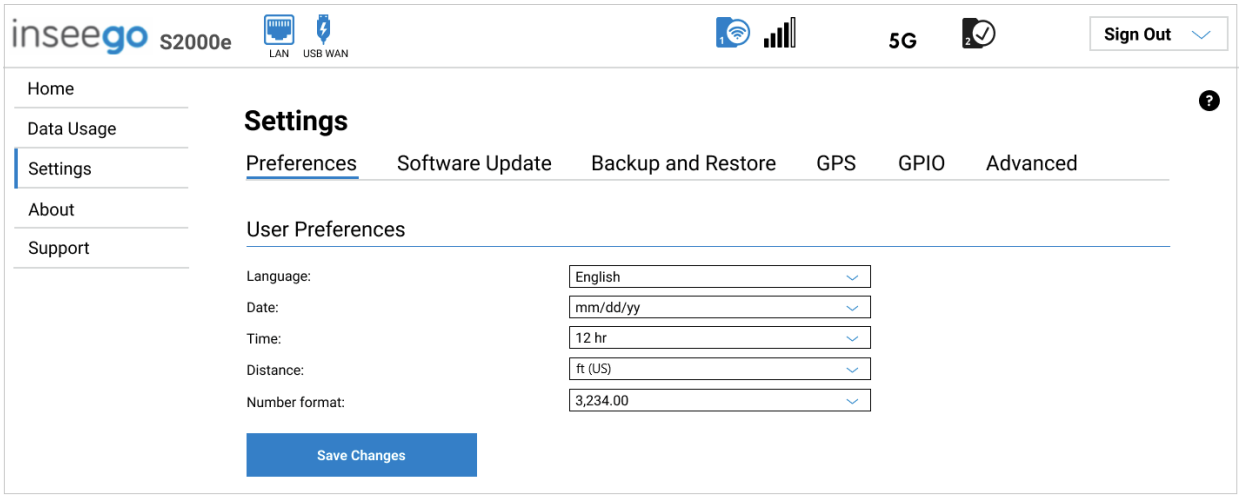
To view and configure settings for your S2000e, select **Settings** from the Web UI side menu.

The Settings page includes the following tabs:

- Preferences
- Software Update
- Backup and Restore
- GPS
- GPIO
- Advanced

Preferences Tab

This tab allows you to change how dates, time, distance, and numbers are displayed, and what language is used, in the S2000e Web UI. **NOTE:** These preferences affect packets sent to remote servers. For example, if you select a 24 hour time format, the Web UI, and any packets reporting time somewhere else, will display time in 24 hour format.



User Preferences

Language: Select a language for the Web UI.

Date: Select the format for dates displayed in the Web UI (mm/dd/yyyy or dd/mm/yyyy).

Time: Select the format for time displayed in the Web UI (12 or 24 hour).

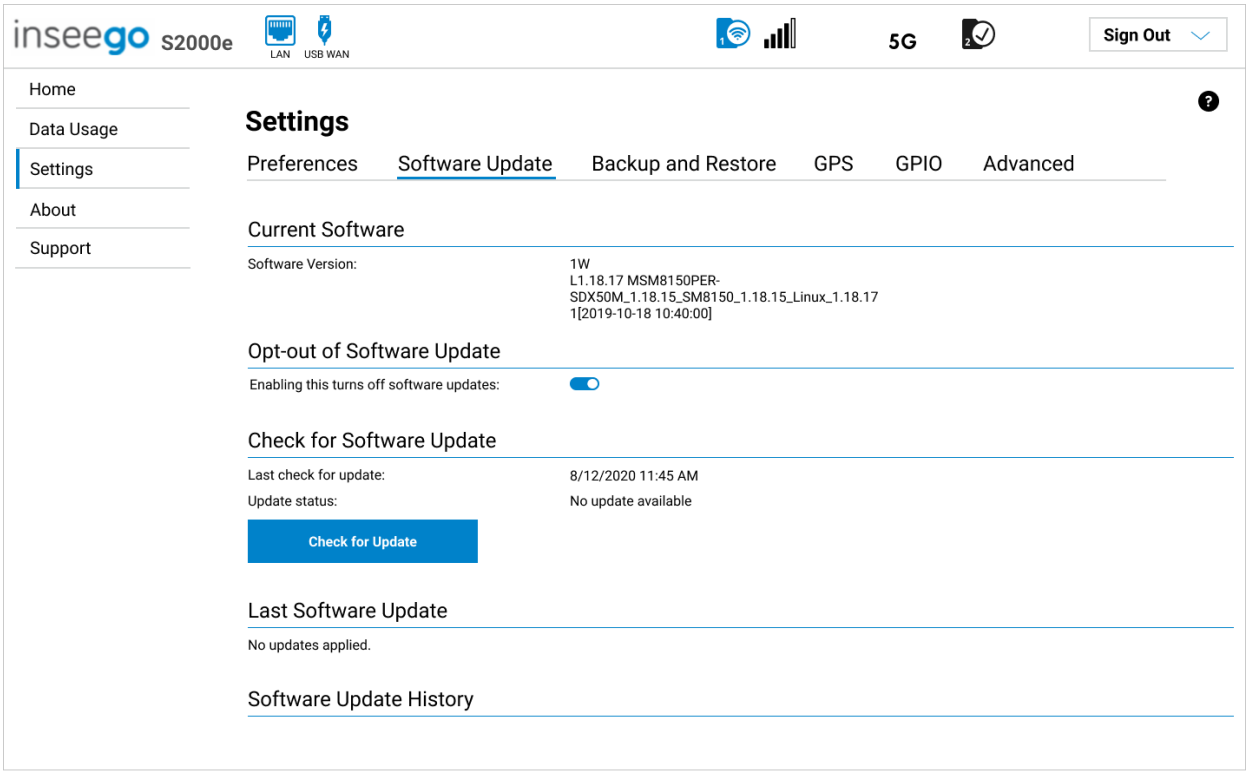
Distance: Select the format for distance displayed in the Web UI (feet or meters).

Number format: Choose the format for decimal numbers displayed in the Web UI (using a period or comma as the decimal point).

Select your display choices from the drop-down menus and click **Save Changes** to update settings.

Software Update Tab

Software updates are delivered to the S2000e automatically over the mobile network. This tab displays your current software version, last system update information, software update history, allows you to check for new software updates, and to opt-out of automatic software updates.



Current Software

Software Version: The version of the software currently installed on your S2000e.

Opt-out of Software Update

By default, software updates are automatically delivered to your S2000e. This setting allows you to opt-out of automatic software updates. If you do not want software updates automatically delivered, move the **ON/OFF** slider to **ON**.

Check for New Software Update

Last check for update: The date and time the S2000e 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. If a new software update is available, it is automatically downloaded.

Last Software Update

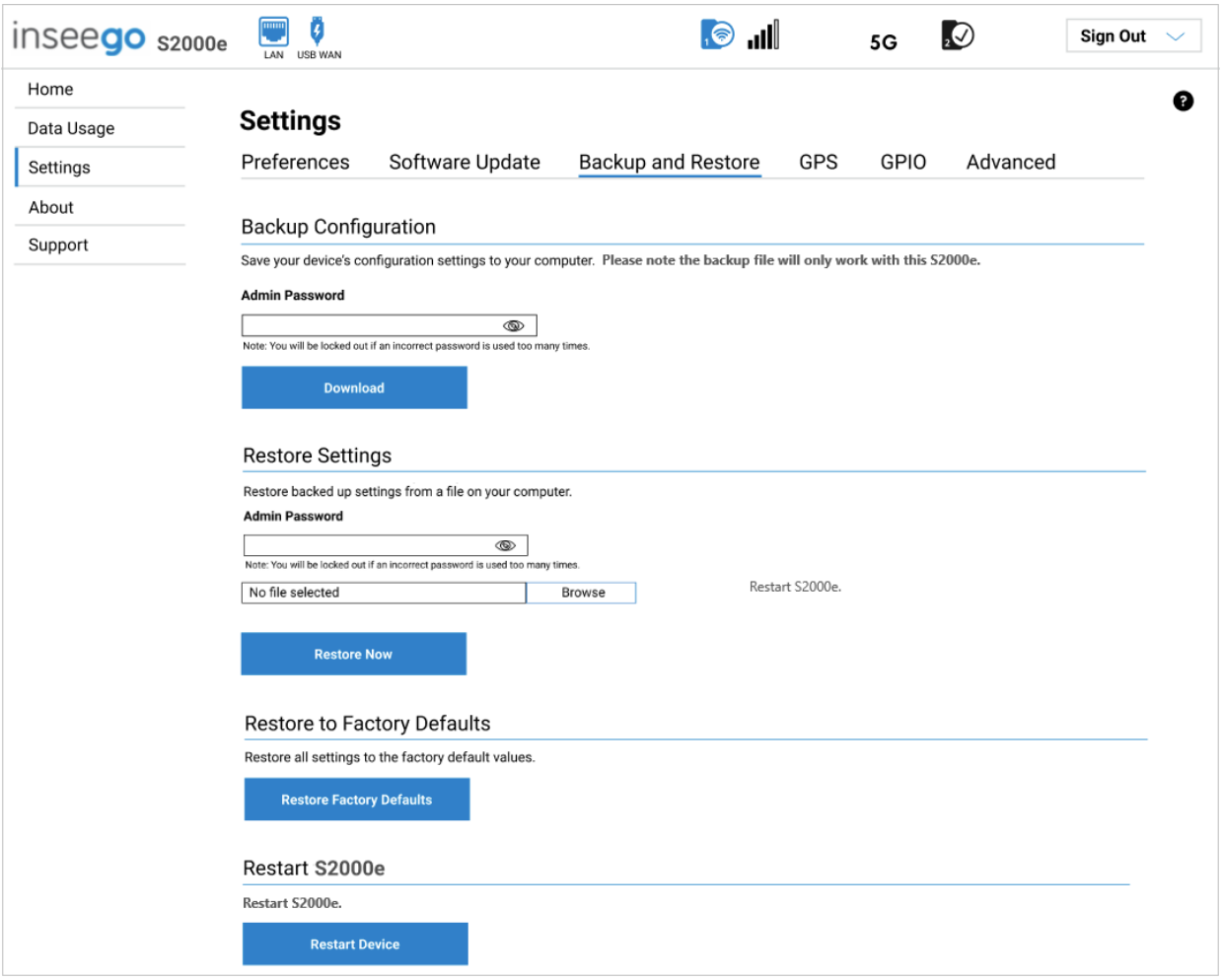
This section displays details about the last software update.

Software Update History

This section displays details of the last updates that have been downloaded and installed to this device. If no updates have been installed, this section is not displayed.

Backup and Restore Tab

Use this tab to back up current S2000e settings to a file on your computer, restore (upload) a previously-saved configuration file, reset the S2000e to factory defaults, or restart it.



Backup Configuration

To back up current S2000e settings to a file on your computer, enter your Admin password in the **Admin Password** field.

The default Admin password is printed on the label of the S2000e. If you have changed the Admin password and don't remember it, select **Sign In** in the top-right corner of the Home page, click **I forgot the Admin password**, and answer the displayed 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 your S2000e.

Click the **Download** button. The file is automatically downloaded to the default Downloads folder on the device connected to the Admin Web UI. This configuration file contains all settings for your S2000e.

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 S2000e, and settings can only be viewed or changed using the Web UI.

Restore Settings

CAUTION! Restoring settings (uploading a configuration file) changes ALL of the existing settings to match the configuration file.

To restore system settings from a backup settings file, click **Browse** and choose a backup settings file to restore.

Enter your Admin password in the **Admin Password** field.

NOTE: You can only restore a file that was created for this model of S2000e.

Click the **Restore Now** button.

Restore to Factory Defaults

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

CAUTION! This initiates a restart and resets all settings to factory default values.

Restart S2000e

Restart S2000e: This button turns your S2000e off and on again.

GPS Tab

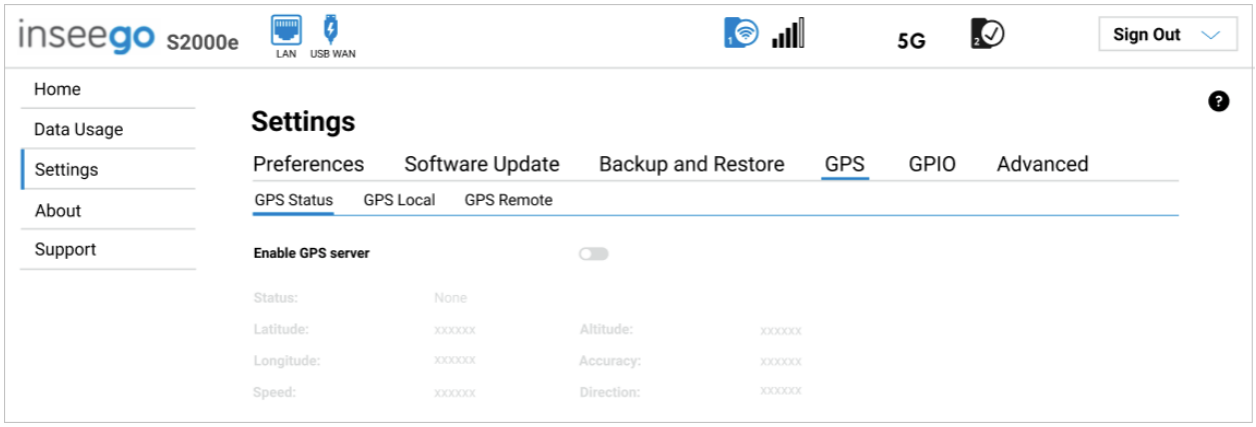
The S2000e incorporates a GPS receiver. The GPS receiver can determine your current location. Current location information can be shared with connected devices by using the Local GPS Streaming Interface on the Local tab.

The GPS page includes three sub tabs:

- GPS Status
- GPS Local
- GPS Remote

GPS Status Sub Tab

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



Enable GPS server: This setting enables or disables the GPS radio on your S2000e. When the **ON/OFF** slider is **ON**, the device acquires GPS and makes GPS location data available on this page. A GPS Agreement appears, click **Confirm** to proceed. When **OFF**, no GPS data is available.

Status: The current status of your GPS connection. When searching, the device is making the connection to satellites in order to populate GPS data.

Latitude: Latitude for the last location fix.

Longitude: Longitude for the last location fix.

Speed: Speed the device is traveling at.

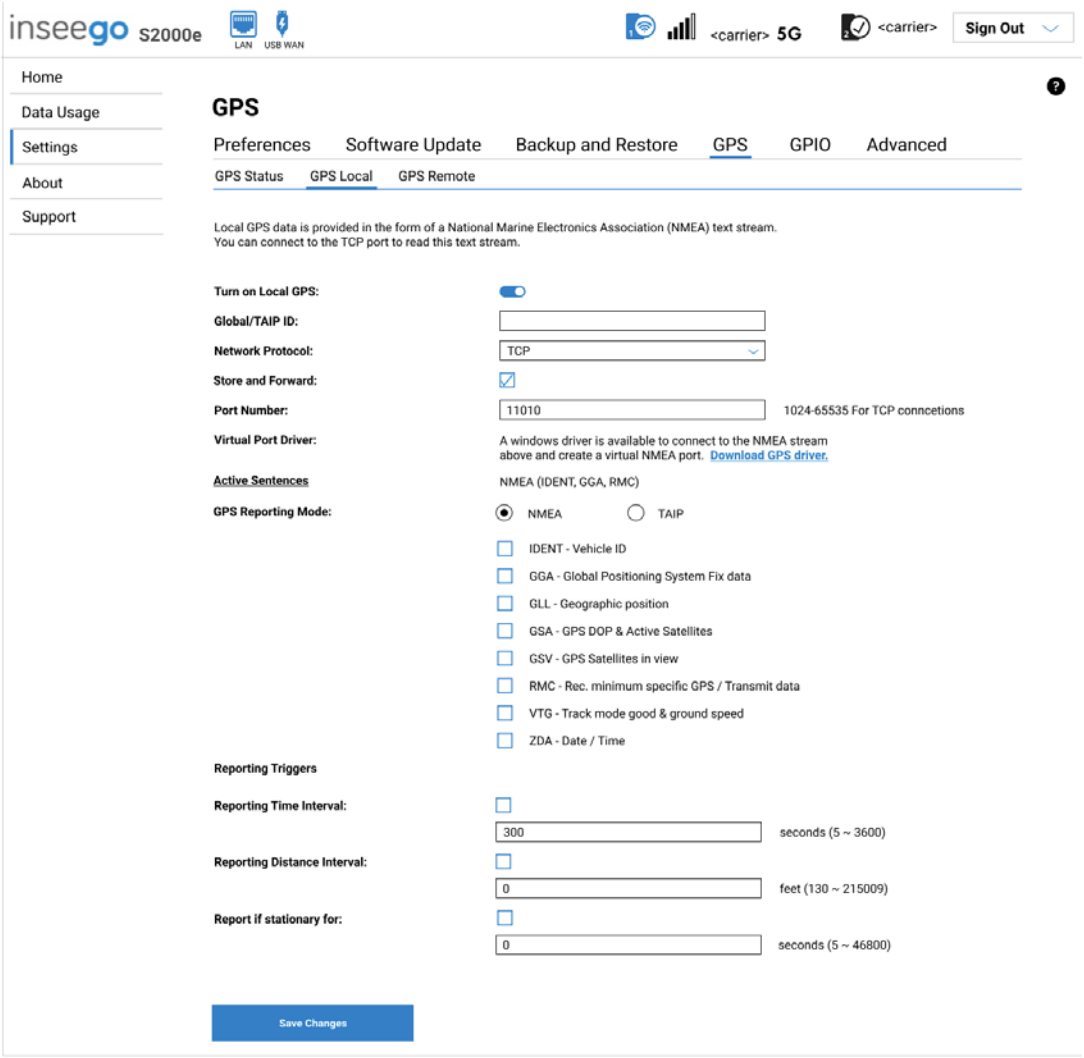
Altitude: Altitude for the last location fix.

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

Direction: Direction the device is traveling relative to North.

GPS Local Sub Tab

Use this tab to enable GPS streaming to client devices on the local network. Raw GPS data is provided by the S2000e 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.

Global/TAIP ID: You can enter a 4-digit ID that is inserted into your GPS packet for routing to servers, identifying your S2000e. If left blank, the ID is left off the local broadcast.

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 s2000e 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.

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 S20003, and makes this GPS data available to NMEA-aware third-party applications.

GPS Reporting Mode: The S2000e 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.

Reporting Triggers

Reporting Time Interval: You can set a time interval, in seconds, for reporting frequency. For example, if you select 900, a GPS packet is sent every 15 minutes. Check the box if you want to use the time interval.

Reporting Distance Interval: You can set a distance interval to trigger when packets will be routed to the server. For example, if you select 1000, a GPS packet will be sent to the server every time your device moves 1000 feet. Check the box if you want to use the distance interval.

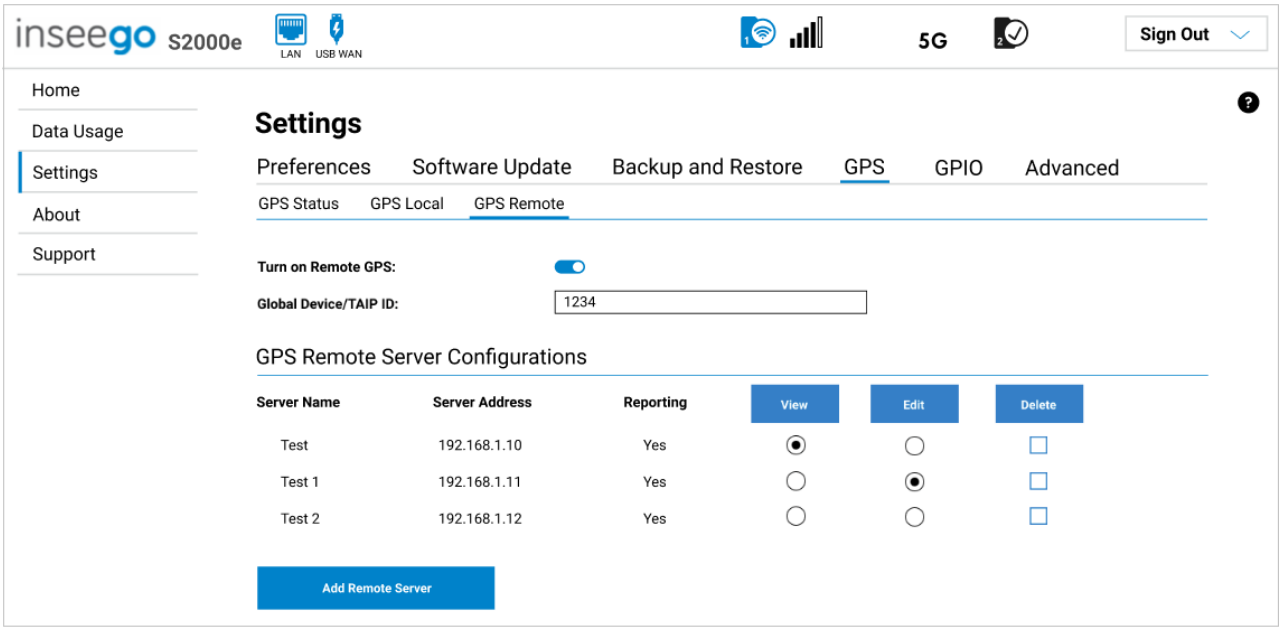
NOTE: If you set both a time and distance interval, the device routes packets based on which event occurs first.

Report if Stationary for: You can set a stationary timer that monitors for movement and only routes packets if the S2000e is continuously moving within the time range (in seconds). For example, if you set this value to 300 and your device has not moved within 5 minutes, a packet will not be routed. Once your device begins registering GPS movement again, packet routing will resume. Check the box if you want to use the stationary timer.

Click **Save Changes** to update settings.

GPS Remote Sub 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.

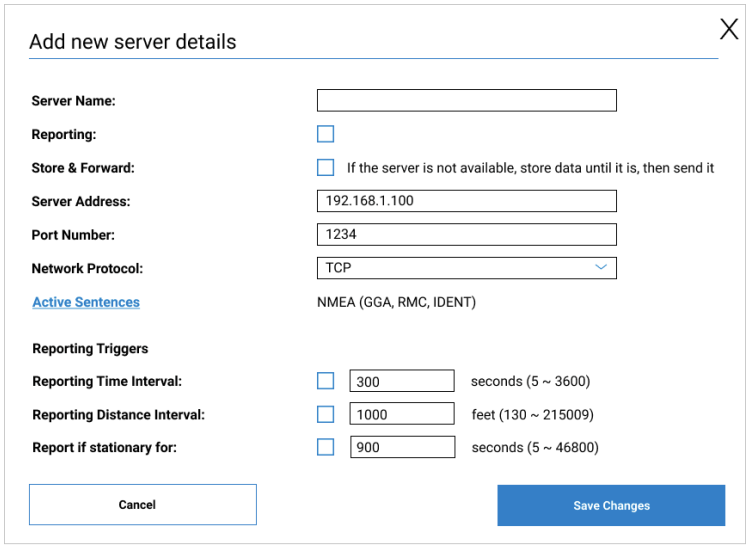


Turn on Remote GPS: Check this box to turn on GPS streaming to remote servers.

Global Device/TAIP ID: A 4-digit ID identifying your S2000e that is inserted into your GPS packet for routing to remote servers. By default this is 1234.

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 S2000e 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 S2000e 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.

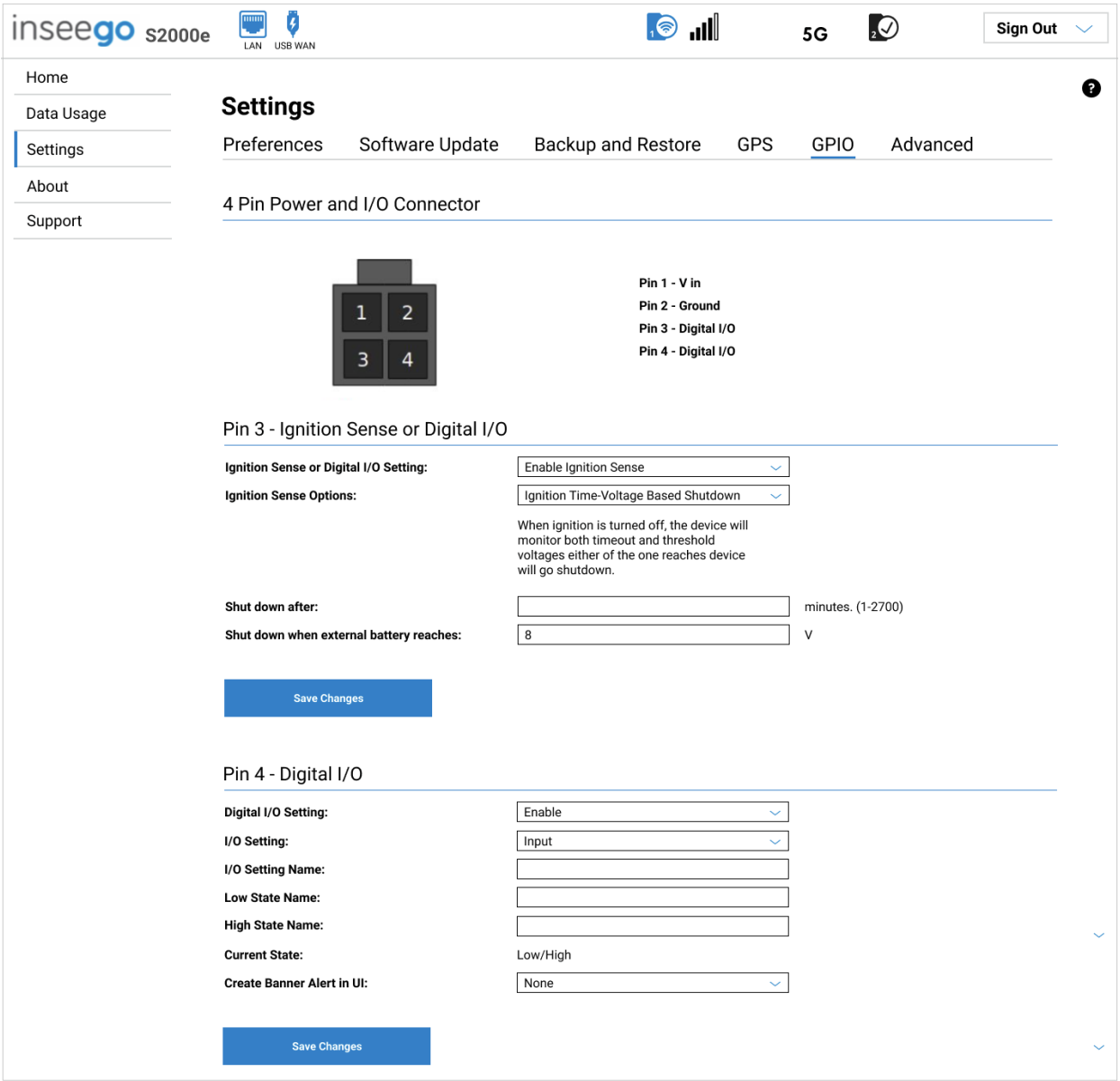
  NOTE: You can choose both Time and Distance as your interval specification. The device will route packets based on which event occurs first.
- **Report if stationary for** — You can set a stationary timer that monitors for movement and only route packets if the device is continuously moving within the 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.

GPIO Tab

The S2000e includes configurable digital General Purpose Input Output (GPIO) pins for external system monitoring or control. Use settings on this tab to enable or disable pins and view or configure pin settings.



4 Pin Power and I/O Connector

The S2000e power port includes voltage in, ground, and two digital I/O pins as shown.

Pin 3 – Ignition Sense or Digital I/O

Ignition Sense or Digital I/O Setting: Use the drop-down to select **Enable Ignition Sense** or **Enable Digital I/O**.

If you select **Enable Ignition Sense**:

Ignition Sense Options: Select an option from the drop-down:

- **Ignition Time-Voltage Based Shutdown –** Allows you to specify an amount of time and battery level. When the ignition is turned off, the device stays on until one of the thresholds is met, at which point it shuts down.
- **Ignition Time Based Shutdown –** Allows you to specify the amount of time you want the S2000e to remain on after the ignition is turned off.
- **Ignition Voltage Based Shutdown - Voltage Level:** Allows you to specify the battery level at which you want the S2000e to turn off.

Shut down after: Enter the number of minutes you want the S2000e to stay on after the ignition is turned off.

Shut down when external battery reaches: Enter the number of volts to use as a battery level threshold. When the battery reaches that amount of voltage, the S2000e will shut down.

If you select **Enable Digital I/O:**

Input Setting: Select **Input** or **Output**.
NOTE: Input can be Input, used to tell the S2000e the state of an external device or system. Output is used to turn another device or system on (low) or off.

I/O Setting Name: Enter a user-friendly name for the setting.

Low State Name: Enter a user-friendly name for the low state.

High State Name: Enter a user-friendly name for the high state.

Current State: The current state of the pin: low or high.

Create Banner Alert in UI: Select an option for state change alerting in Inseego Connect.

Pin 4 – Digital I/O

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

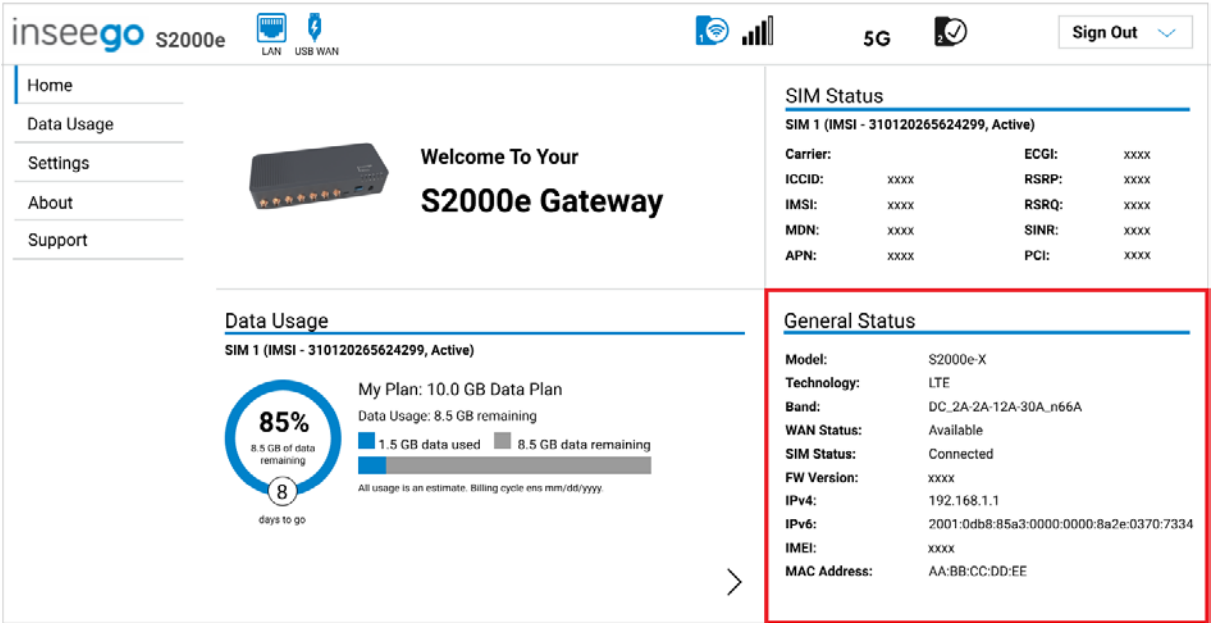
Digital I/O options are the same as for Pin 3.

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 47.

Viewing Info About the Gateway

On the Web UI Home page, the General Status panel shows current connection status and general status information.



Model: The model of the device.

Technology: Indicates the current cellular data connection, for example, 5G Sub6.

Band: The band in use for the current connection.

WAN Status: The current status of the WAN connection.

SIM Status: The current status of the SIM card.

FW Version: The version of the firmware (software) currently installed on your S2000e.

IPv4: The network IP address of the S2000e.

IPv4: The Local-Link IPv6 address of the S2000e.

IMEI: The International Mobile Equipment Identity (IMEI) for your S2000e. This is a 15 digit code used to uniquely identify an individual mobile station. The IMEI does not change when the SIM is changed.

MAC Address: The Media Access Controller (MAC) Address for your S2000e. The MAC address is a unique network identifier assigned when a network device is manufactured.

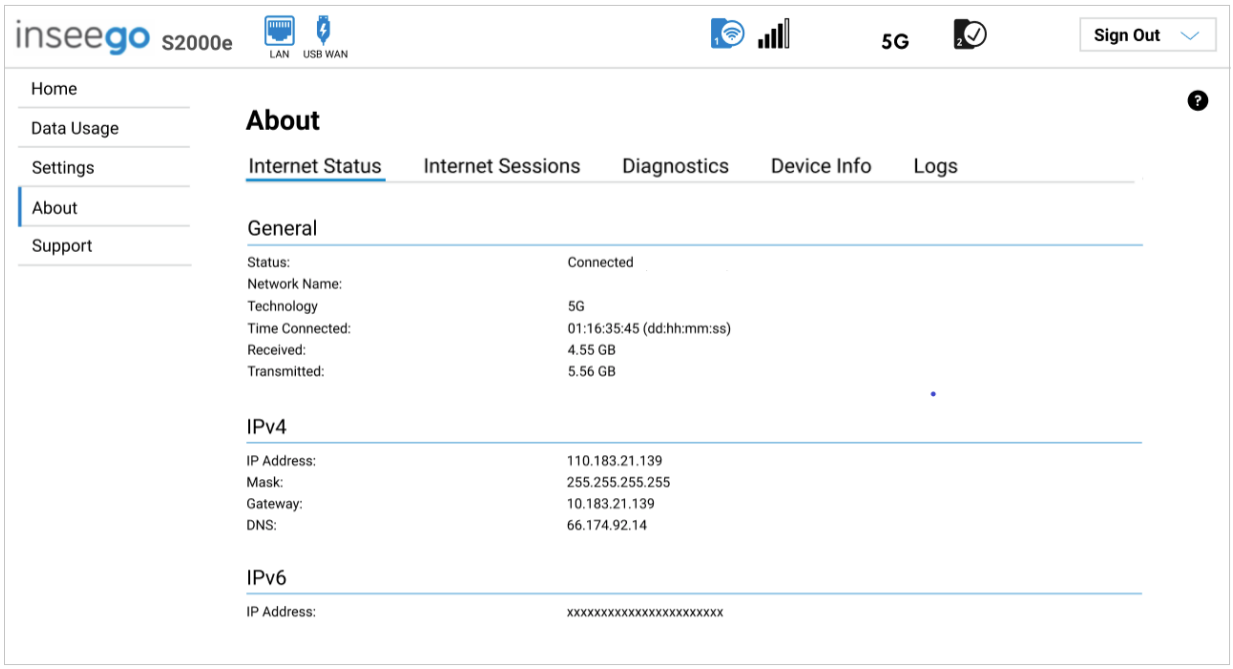
To view more detailed information about your S2000e and its use, select **About** from the Web UI side menu).

The About page includes the following tabs:

- Internet Status
- Internet Sessions
- Diagnostics
- Device Info
- Logs

Internet Status Tab

Use the Internet Status tab to view general Internet connection and system information.



General

Status: The current status of the S2000e connection.

Network Name: The name of the network for the current Internet session established.

Technology: Indicates the current cellular data connection, for example, 5G.

Time Connected: The amount of time that has elapsed since the connection for the current Internet session was established.

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

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

IPv4

IP Address: The Internet IP address assigned to the S2000e.

Mask: The network mask associated with the IPv4 address.

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

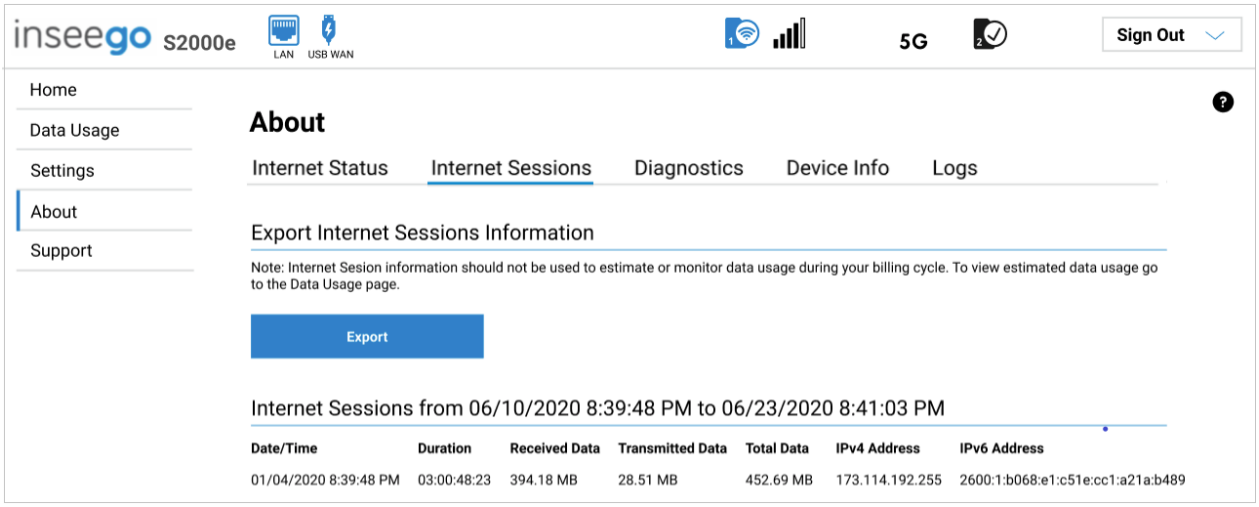
DNS: The Domain Name Server currently used by the S2000e.

IPv6

IP Address: The global IPv6 address for the S2000e (blank if IPv6 is turned off or is not supported by the current network connection or operator).

Internet Sessions Tab

Use the Internet Sessions tab to export and view Internet session data.



Export Internet Sessions Information

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

Internet Sessions

NOTE: Internet Sessions are presented in date order.

Date/Time: The date and time the Internet session began.

Duration: The total amount of time for the Internet session.

Received Data: The amount of data received for the Internet session. This counter starts at zero when the connection is established.

Transmitted Data: The amount of data transmitted for the Internet session. This counter starts at zero when the connection is established.

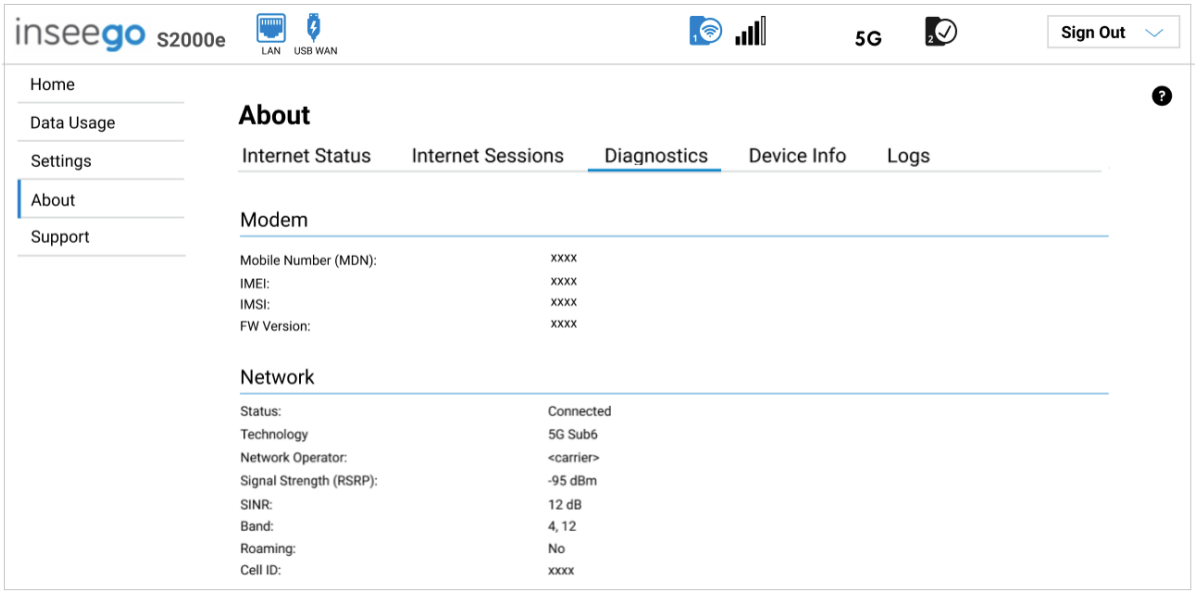
Total Data: The total amount of data for the Internet session. This is the sum of Received Data and Transmitted Data.

IPv4 Address: The IP address for the session.

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

Diagnostics Tab

This tab displays detailed information used solely for troubleshooting or technical support.



Modem

Mobile Number (MDN): The phone number of your S2000e.

IMEI: The International Mobile Equipment Identity (IMEI) for your S2000e. This is a 15 digit code used to uniquely identify an individual mobile station. The IMEI does not change when the SIM is changed.

IMSI: The International Mobile Subscriber Identity (IMSI) for your S2000e. This is a unique number, usually fifteen digits, that identifies a Global System for Mobile Communications (GSM) subscriber.

FW Version: The version of the firmware (software) currently installed on your S2000e.

Network

Status: The status of the network.

Technology: Indicates the current cellular data connection, for example, 5G Sub6.

Network Operator: The name of the Mobile Network Operator (MNO).

Signal Strength (RSRP): The strength of the cellular signal, measured in dBm. Higher absolute values indicate a stronger signal, for example: -80 dBm is a stronger signal than -90 dBm.

SINR: Signal to Interference plus Noise Ratio. An LTE-specific measure of signal quality, taking interference and noise into account. SINR is a positive value, and higher numbers are better.

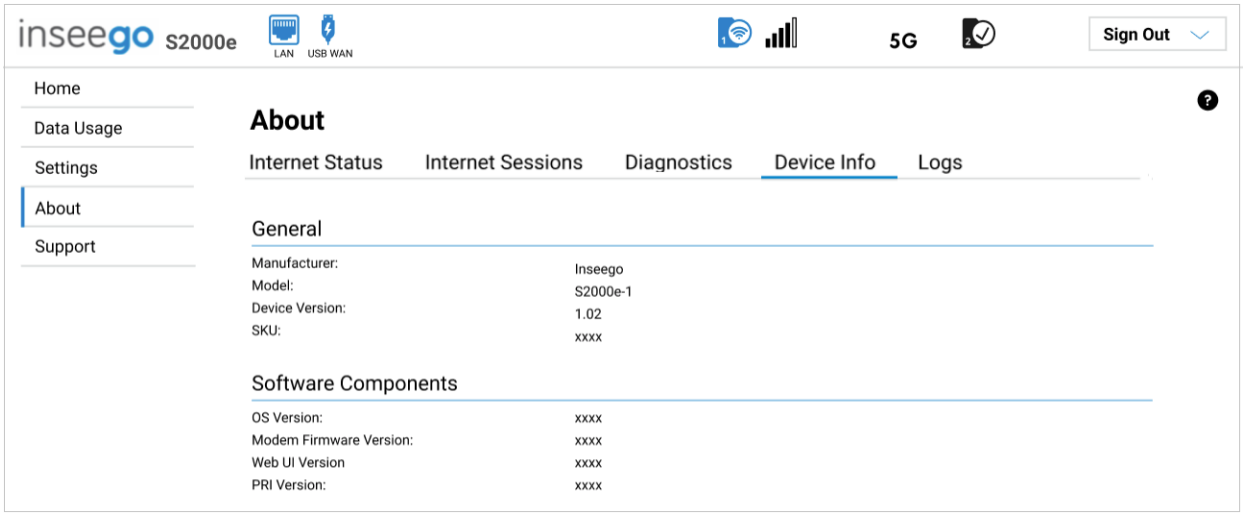
Band: The band in use for the current connection.

Roaming: Indicates whether roaming is on.

Cell ID: The ECGI code used to identify cells globally.

Device Info Tab

Use this tab to view details about your S2000e.



General

Manufacturer: Inseego.

Model: Model of the device.

Device Version: The version of firmware (software) currently installed.

SKU: The SKU for your S2000e.

Software Components

OS Version: The version number for the Operating System and its components.

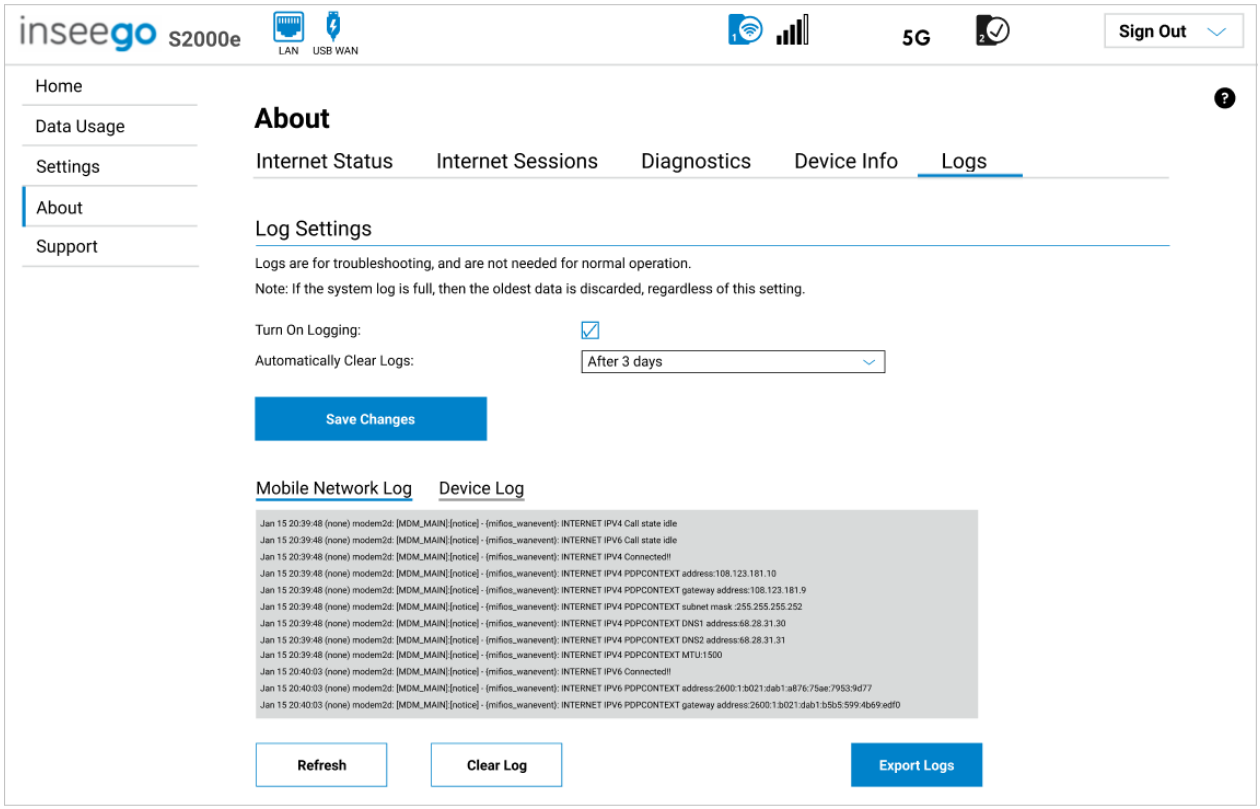
Modem Firmware Version: The version of firmware (software) currently installed for the modem component.

Web UI Version: The version number for the S2000e Web UI.

PRI Version: The configuration version currently applied to the S2000e.

Logs Tab

Use this tab to view log information for troubleshooting.



Log Settings

Turn On Logging: Check this box to turn on logs as needed.

Automatically Clear Logs: Use the drop-down list to select when logs are cleared. **NOTE:** If the log is full, the oldest data is deleted regardless of this setting.

Click **Save Changes** to enact changes.

If logs are turned on, the following are visible:

Click on **Mobile Network Log** for log data of connections to the mobile network.

Click on **Device Log** for log data of events other than mobile data connections that occurred on this device.

Refresh: Updates the displayed log data.

Clear Log: Deletes all existing log data. This makes new data easier to read.

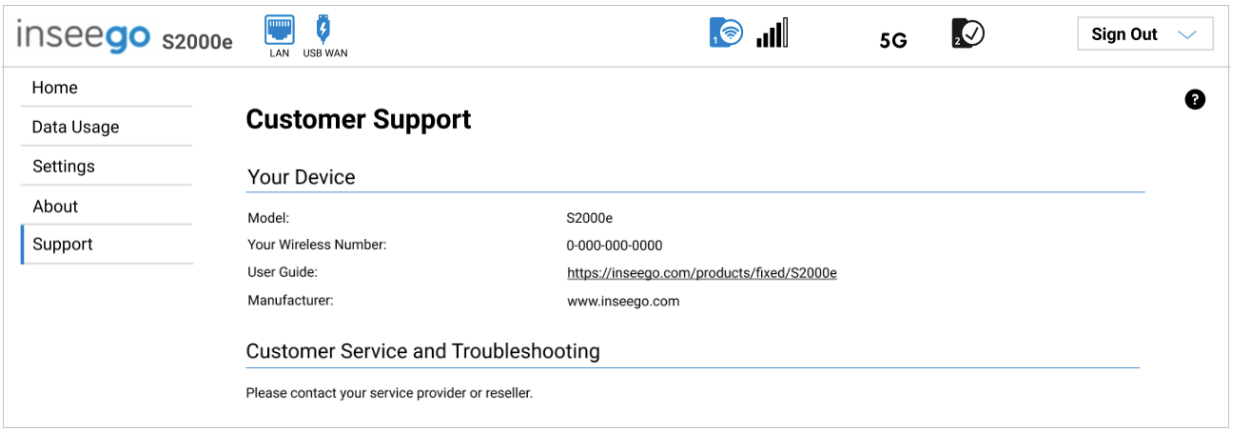
Export Logs: Allows you to export log data.

Getting Support

For Support, select Support from the Web UI side menu.

Customer Support Tab

Use the Customer Support tab for useful links and support information.



3

Advanced Settings

Overview

Using Advanced Settings

Overview

The Advanced Settings pages on the S2000e website 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 S2000e.

Using Advanced Settings

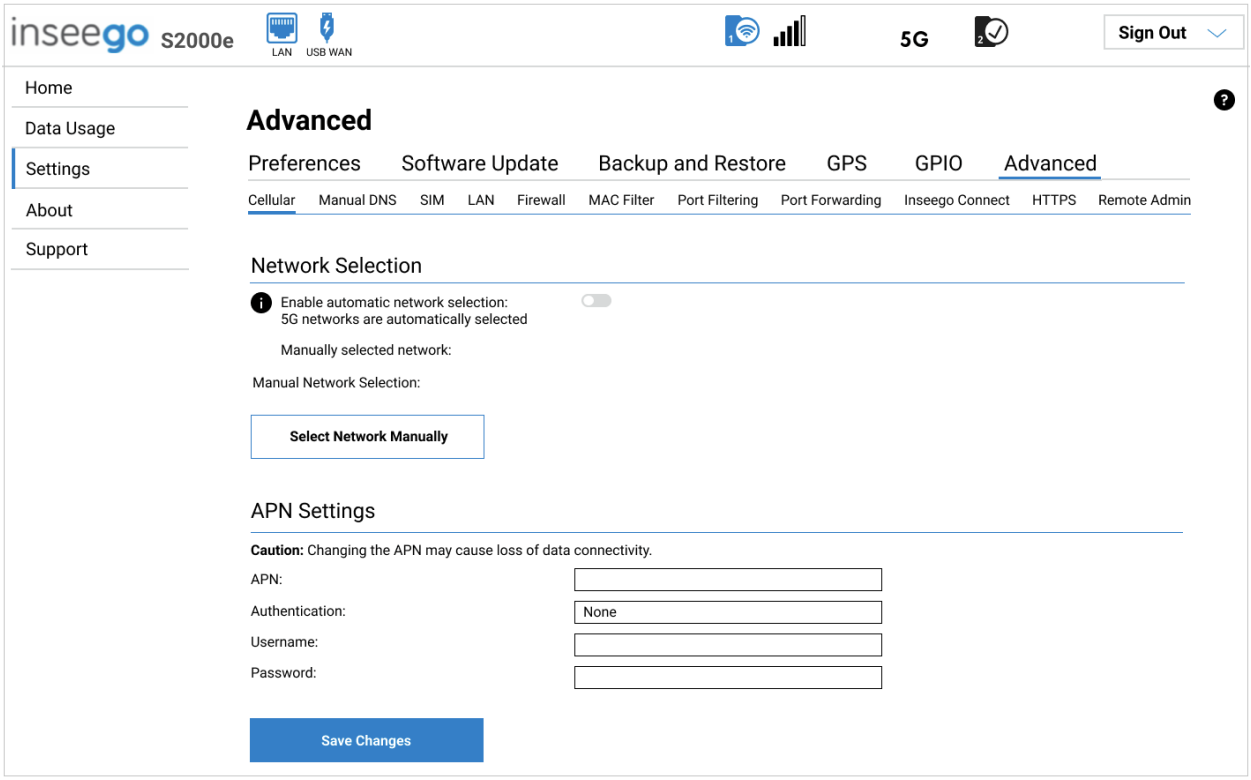
When you select the **Advanced** tab on the Settings page, a warning message appears. If you click **Continue**, the Cellular tab of the Advanced Settings page appears.

The Advanced Settings page includes the following tabs:

- Cellular
- Manual DNS
- SIM
- LAN
- Firewall
- MAC Filter
- Port Filtering
- Port Forwarding
- Inseego Connect
- HTTPS
- Remote Admin

Cellular Tab

In most configurations, the S2000e 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 the APN on this tab for the network to communicate with the S2000e.



Network Selection

Enable automatic network selection: When the **ON/OFF** slider is **ON**, your S2000e automatically selects the best 5G available network and you cannot use the **Select Network Manually** button below.

Select Network Manually: You may wish to use this option if multiple networks are available and you have a preference. **NOTE:** This option is available only if **Enable automatic network selection** is off. Click the button to scan for available networks, then choose the preferred network.

APN Settings

APN: Enter the APN for your private network.

CAUTION! Changing the APN may cause a loss of data connectivity.

Authentication: Select the authentication method for your private network from the drop-down (PAP, CHAP, or None).

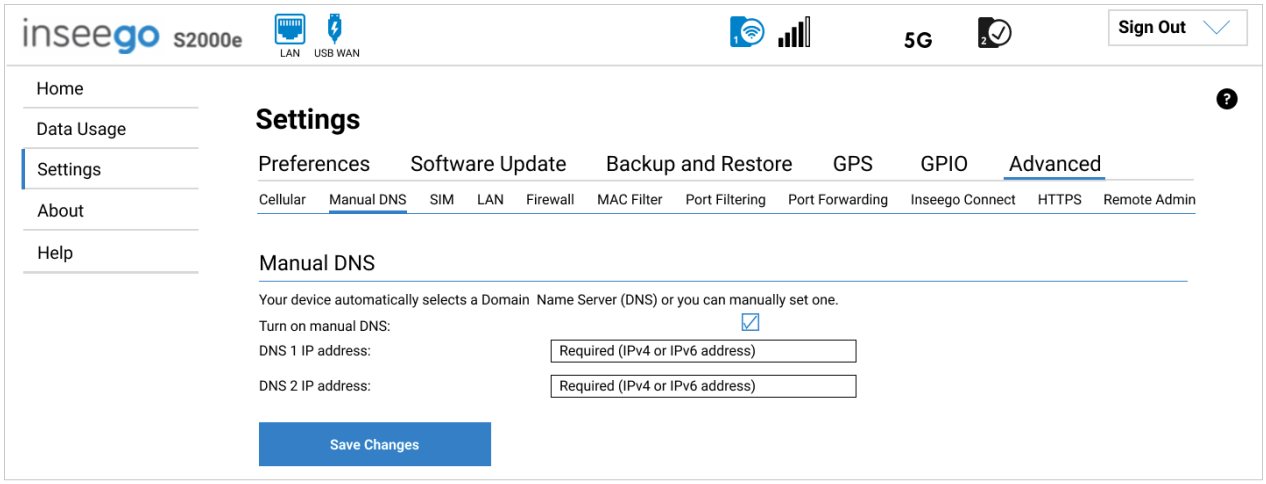
Username: Enter the user name for your private network.

Password: Enter the password for your private network.

Click **Save Changes**. The device will reboot for changes to take effect.

Manual DNS Tab

The S2000e automatically selects a Domain Name Server (DNS). This page allows you to manually assign up to two DNS IP addresses.



Manual DNS

Turn on manual DNS: Check this box to manually select a DNS.

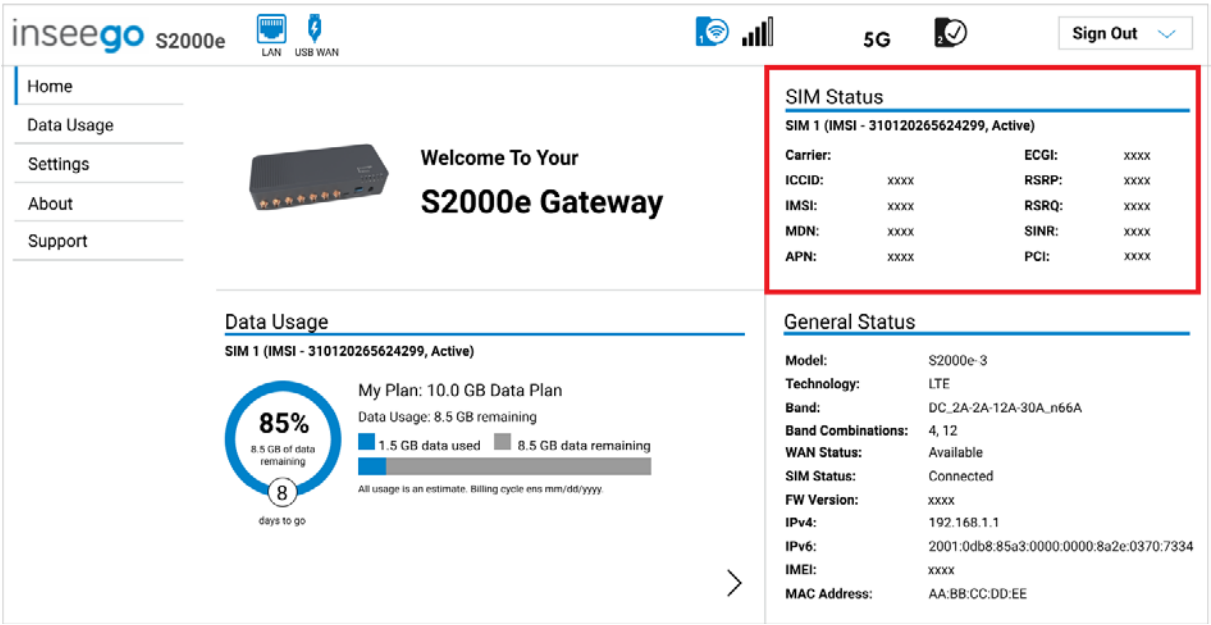
DNS 1 IP address: Enter the IP address for the primary DNS. This address is required to use the Manual DNS feature.

DNS 2 IP address: Enter the IP address for the secondary (backup) DNS. This address is optional and may be left blank if desired.

Click **Save Changes**.

SIM Tab

On the Web UI Home page, the SIM Status panel shows SIM status information.



Carrier: The name of the Mobile Network Operator.

ICCID: The unique ID number assigned to the SIM card.

IMSI: The International Mobile Subscriber Identity (IMSI) for your S2000e. This is a unique number, usually fifteen digits, that identifies a Global System for Mobile Communications (GSM) subscriber.

MDN: The phone number of your S2000e.

APN: The access point name for your S2000e.

ECGI: E-UTRAN Cell Global Identifier. This is a 15-digit code used to identify cells globally.

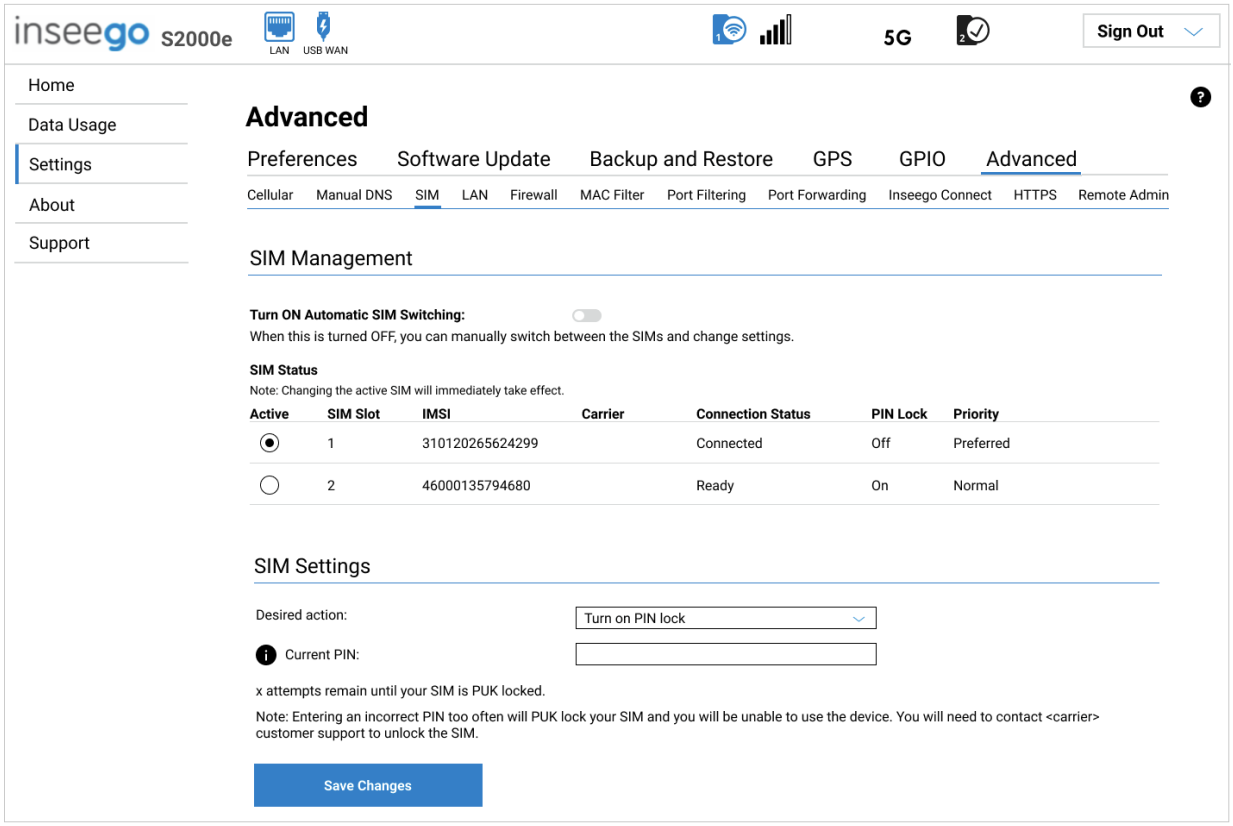
RSRP: The strength of the cellular signal, measured in dBm. Higher absolute values indicate a stronger signal, for example: -80 dBm is a stronger signal than -90 dBm.

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

SINR: Signal to Interference plus Noise Ratio. A measure of signal quality, taking interference and noise into account. SINR is a positive value, and higher numbers are better.

PCI: The Physical Cell ID.

To turn on automatic SIM switching or enter a SIM PIN, select Settings from the Web UI side menu. Then select Advanced >SIM.



NOTE: The SIM card in your S2000e can be locked using a PIN. If the SIM card is locked, you must enter the PIN before connecting to the mobile network. Once entered, the PIN is remembered until the next shutdown. You may also need to provide the existing PIN to change a SIM. The default PIN is available from your service provider.

SIM Management

Turn ON Automatic SIM Switching: Move the **ON/OFF** slider to **ON** to turn on automatic SIM switching. When enabled, the SIM is switched automatically if the active SIM is disconnected. When **OFF**, you can manually switch between SIMs and change SIM settings.

SIM Status

Active: Select the SIM you want to be active. **NOTE:** The change will take effect immediately.

SIM Slot: The SIM slot number.

IMSI: The International Mobile Subscriber Identity (IMSI) for your S2000e. This is a unique number, usually fifteen digits, that identifies a Global System for Mobile Communications (GSM) subscriber.

Carrier: The cellular carrier associated with the SIM.

Connection Status: The current status of the SIM.

PIN Lock: 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.

Priority: Indicates whether the SIM is Normal or Preferred priority.

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

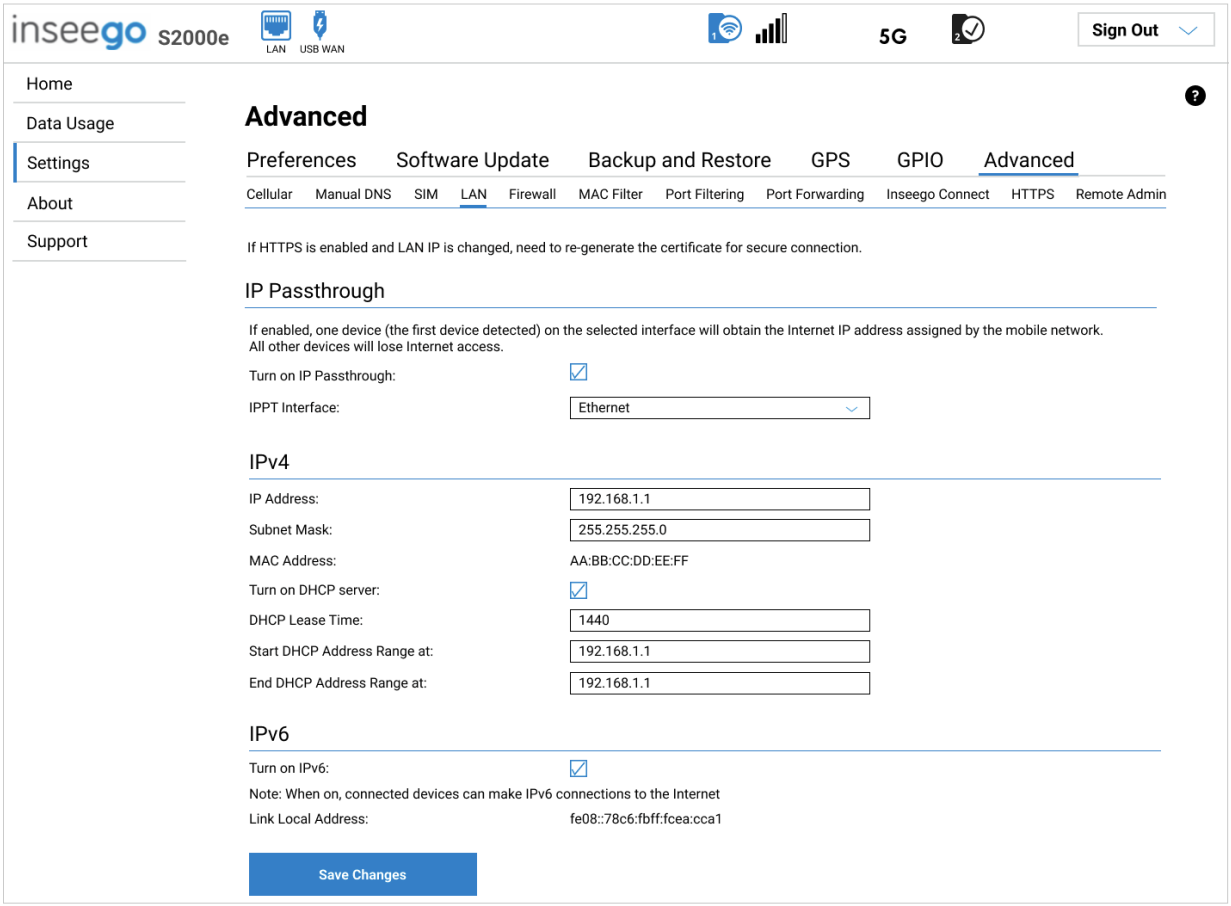
- **PIN Lock** - If the SIM is currently PIN locked, you are prompted to enter the PIN.
  NOTE: If an incorrect PIN is entered too many times, the SIM becomes PUK locked. A counter indicates how many incorrect entries will cause PUK lock. Once PUK locked, the PUK must be obtained from your service provider.
- **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. **NOTE:** The default SIM PIN is available from your service provider.

Click **Save Changes**.

LAN Tab

This page provides settings and information about the S2000e local area network (LAN). The LAN consists of the device and all connected devices.



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.

IPv4

IP Address: The IP address for your S2000e, as seen from the local network. Normally, you can use the default value.

Subnet Mask: The subnet mask network setting for the S2000e. 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 your S2000e. The MAC address is a unique network identifier assigned when a network device is manufactured.

Turn on 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.

IPv6

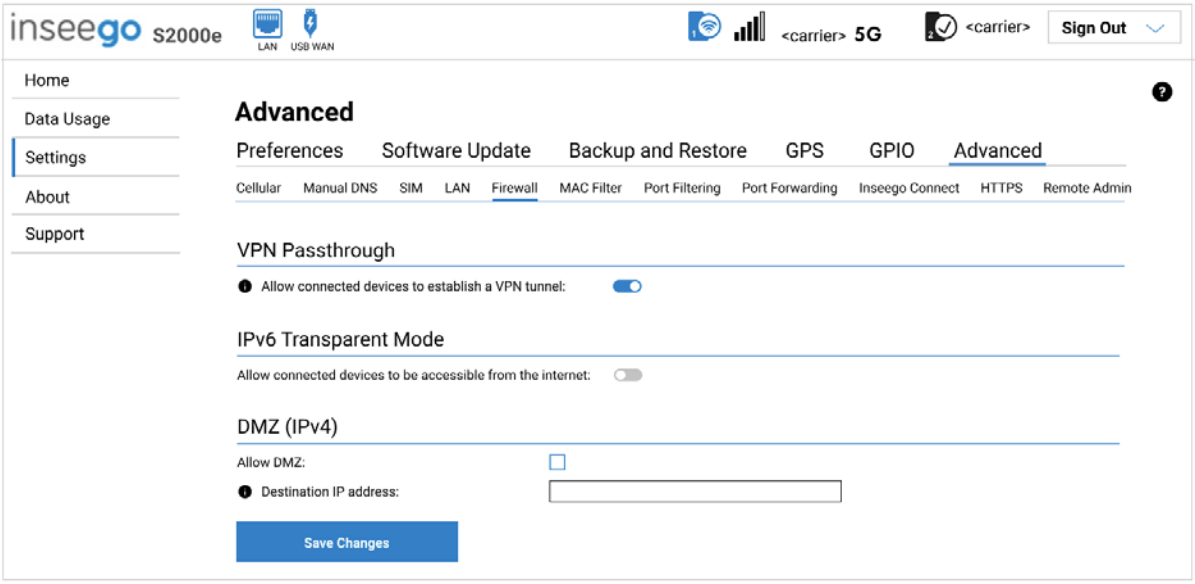
Turn on IPv6: Check the box if the connected device supports IPv6. This enables IPv6 connected devices to make IPv6 connections to the Internet.

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

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

Firewall Tab

The S2000e firewall determines which Internet traffic is allowed to pass between the gateway 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 your S2000e.

IPv6 Transparent Mode

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

DMZ (IPv4)

Allow DMZ: Check this box to allow DMZ. DMZ allows the connected device specified as the DMZ IP address (Destination IP address) 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.

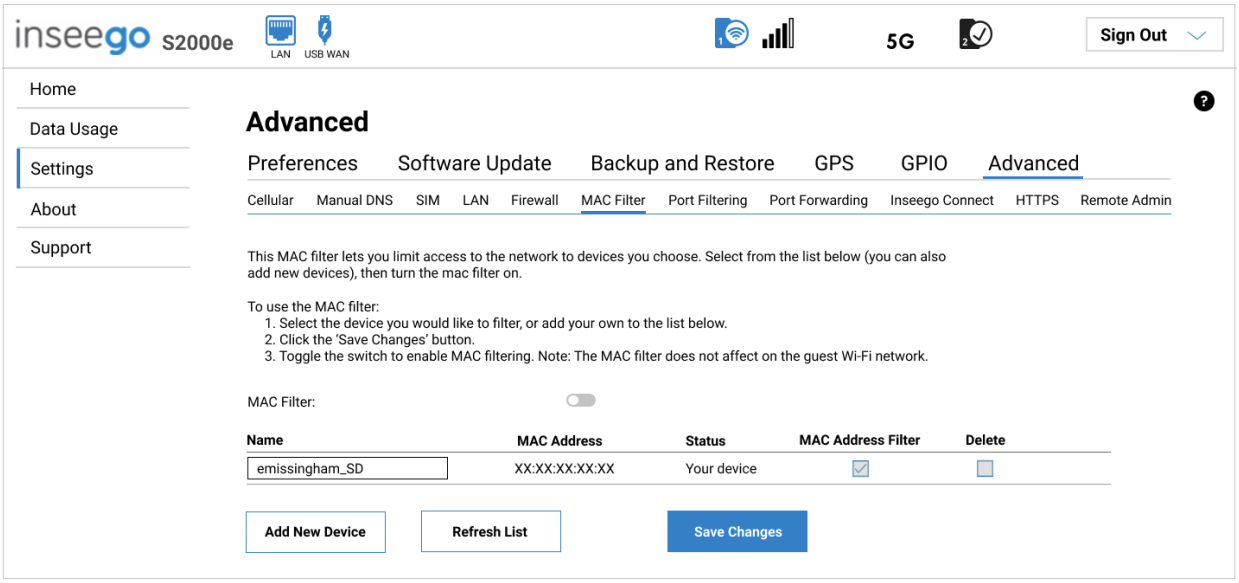
Destination IP address: Enter the IP address of the connected device you wish to become the DMZ device (the DMZ destination). **NOTE:** You can check the IP address of each connected device on the Connected Devices screen.

Click **Save Changes**.

MAC Filter Tab

The MAC filter allows only selected devices to access the S2000e network through DHCP. By default, MAC filter is turned off.

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



MAC Filter

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

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

Device List

This list includes all devices currently connected to the S2000e.

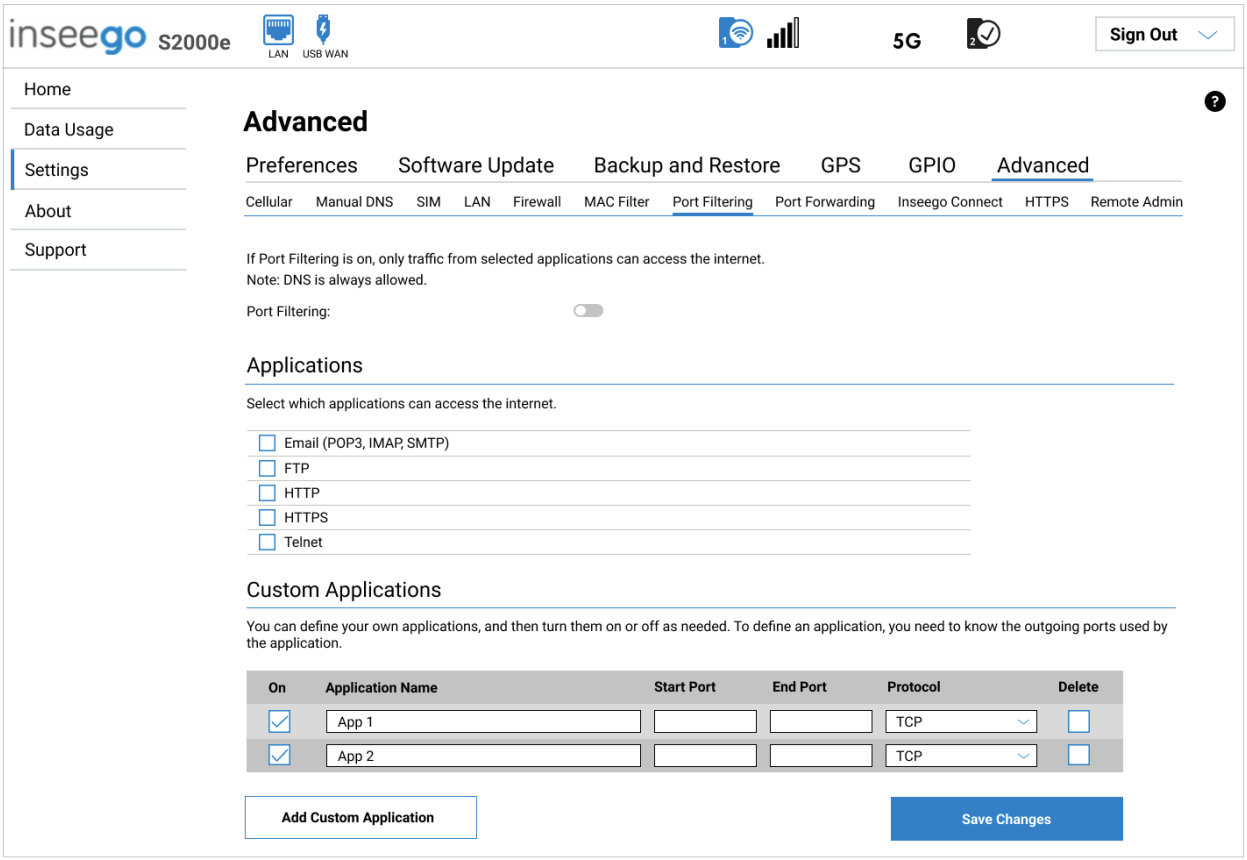
Add new device: Use this button to add a device to the device list, then enter the device name, MAC address, choose whether to select the **MAC Address Filter** checkbox, and click **Save Changes**.

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** and **Confirm**.

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

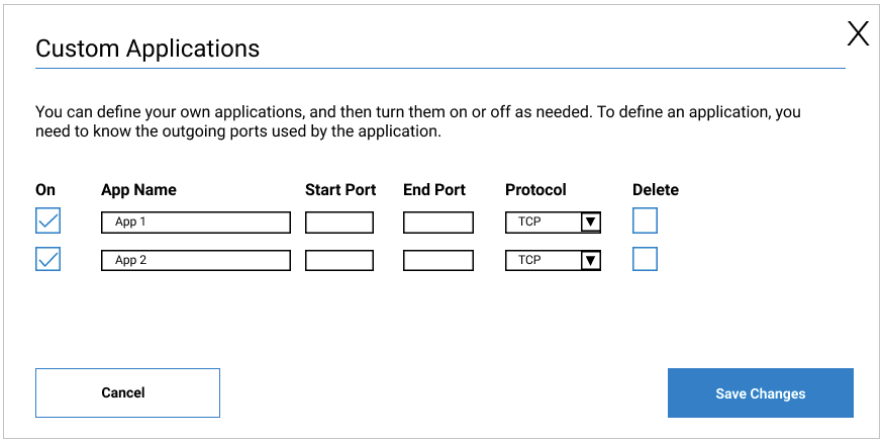
Select the applications you want to be able to access the Internet.

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

Add 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.

* **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.

- **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.

  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.

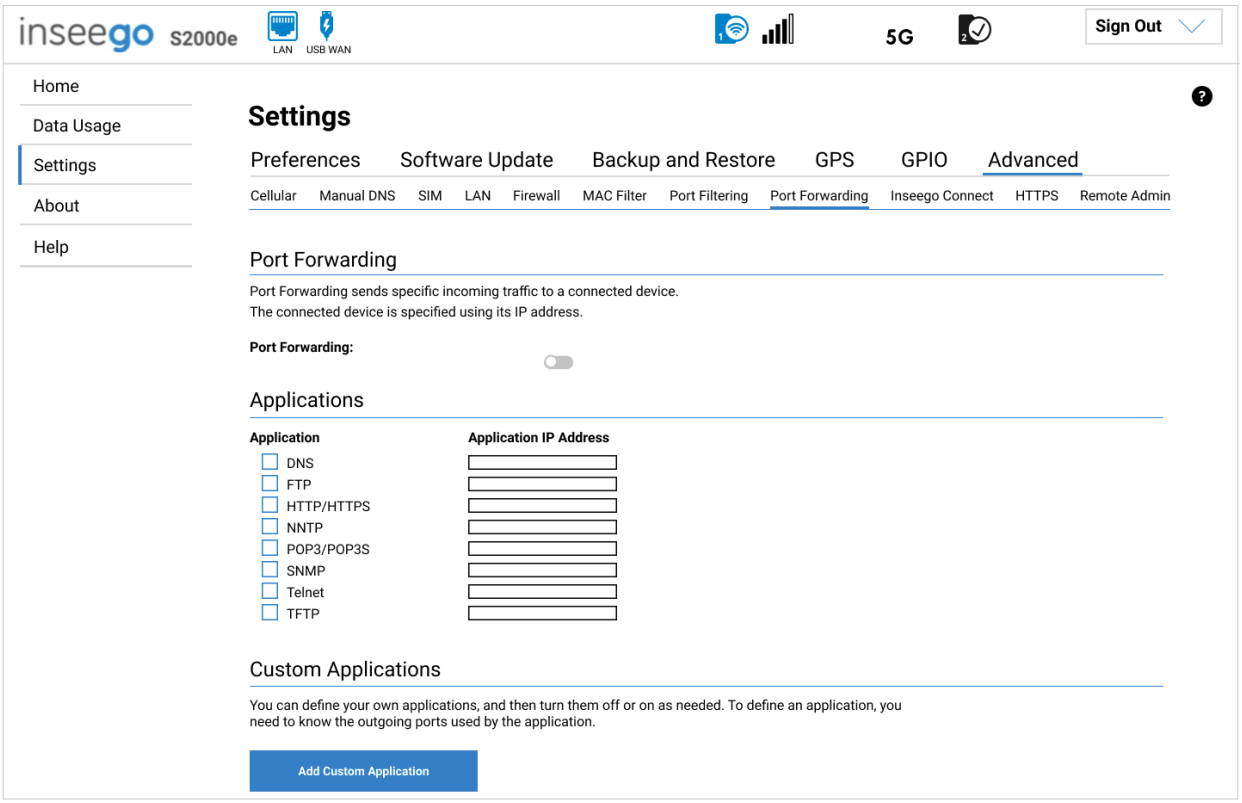
Click **Save Changes** to save any changes made to the custom applications.

Port Forwarding Tab

Port Forwarding allows specific applications to be forwarded to a particular device connected to your 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.

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

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**.

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 IP Address** field.

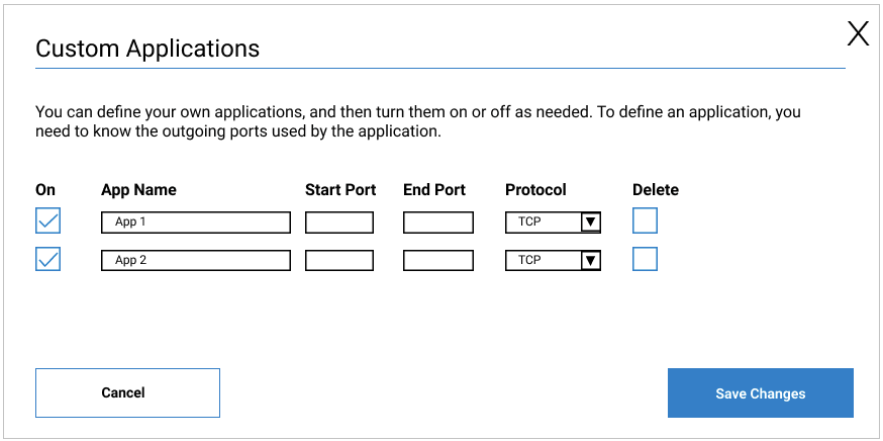
The following table provides port numbers and protocol information for each port forwarding application listed.

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.



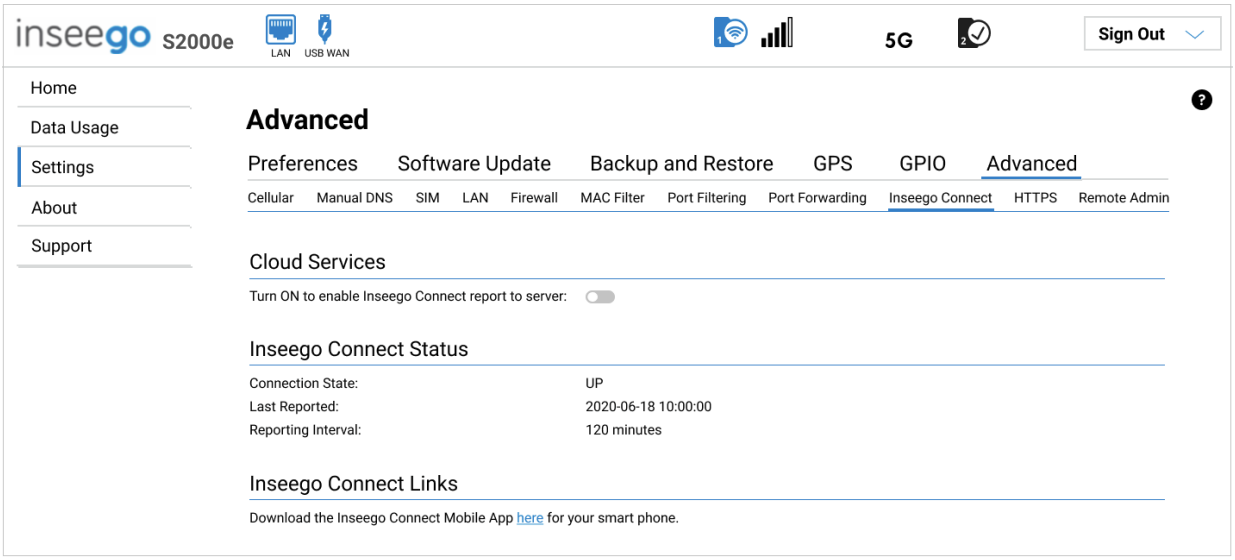
- **On:** Check this box if you want the new application to be able to access the Internet (enabling port forwarding).
- **App Name**: Enter a name for the custom application.
- **Start Port:** Enter the beginning of the range of port numbers to be forwarded.
- **End Port:** Enter the end of the range of port numbers to be forwarded.

  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 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.

Inseego Connect Tab

Use this page to enable and configure settings for 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.



Cloud Services

By default, the connection to Inseego Connect is **OFF**. Slide the **ON/OFF** slider to **ON** to enable the connection.

Inseego Connect Status

Connection State: The status of the Inseego Connect connection.

- **UP** – S2000e is communicating with Inseego Connect servers.
- **DOWN** – S2000e is NOT communicating with Inseego Connect servers.

Last Reported: The time when S2000e last sent a packet to Inseego Connect servers.

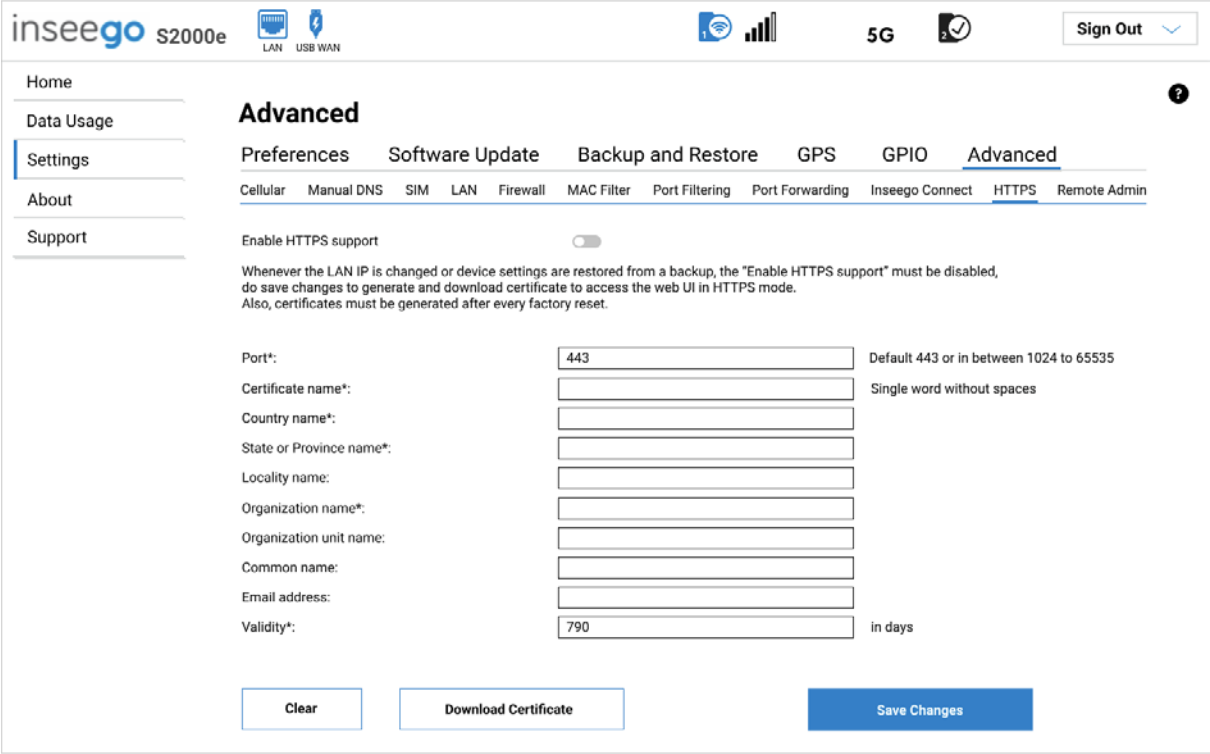
Reporting Interval: This is the interval at which your S2000e will send packets to the Inseego Connect server. **NOTE:** A shorter interval means more data usage.

Inseego Connect Links

Use the link to download the Inseego Connect Mobile App.

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**.

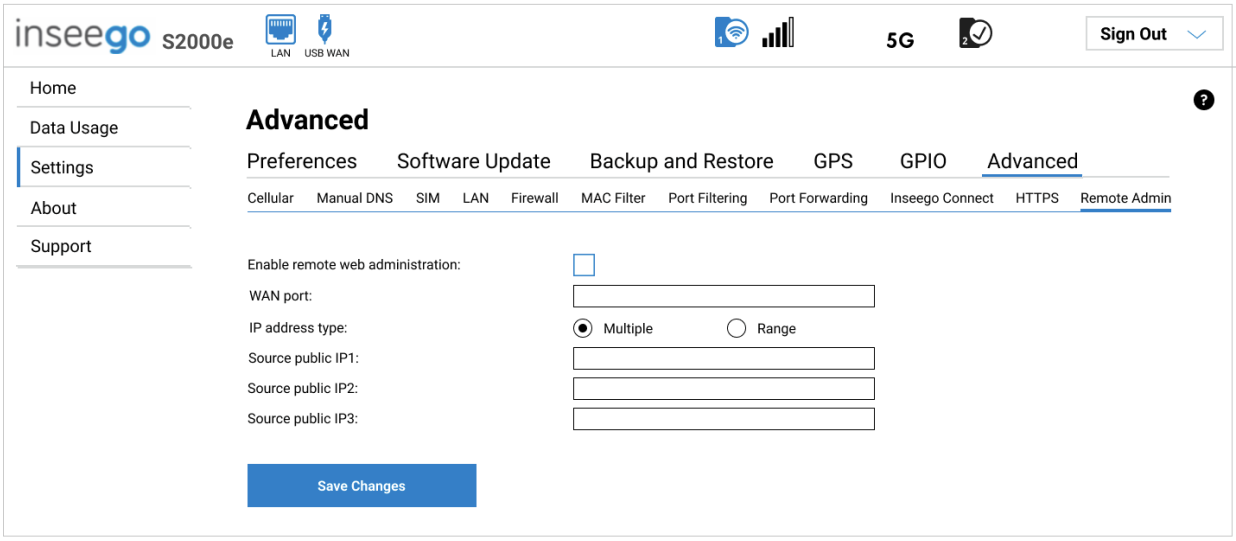
Mozilla Firefox Browser

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 S2000e.



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**.

4

Product Specifications and Regulatory Information

Product Specifications

Regulatory Information

Product Certifications and Supplier's Declarations of Conformity

Wireless Communications

Limited Warranty and Liability

Safety Hazards

Proper Battery Use and Disposal

Product Specifications

Device

Name:	5G Industrial Gateway S2000e
Model:	S2000e-3
Standards, Approvals, Certifications:	FCC, ISED, CE GCF, PTCRB, EN/IEC 62368 REACH, RoHS, WEEE, Halogen Free
Dimensions:	200 x 80 x 45mm
Weight:	500 g
Ports:	1x 5 Gbps RJ45 with Power over Ethernet 1 x USB 3.1 Type C (USB Tethering, USB WAN Modem, USB to Ethernet RJ45 Adapter) 6 x Female SMA for Cellular 1 x Female SMA for GNSS 1 x 4 Pin Power with 2 x Digital I/O Pins
SIM:	2 x 4FF Nano SIM
Chipset:	Qualcomm® Snapdragon™ SDX55
Memory:	1 GB Flash 1 GB RAM
LED:	1 x RGB for Device Health 1 x RGB for Cellular Signal 2 x RG for SIM Status 1 x RG for USB Status 1 x RG for GNSS Status 2 x LED for Ethernet Status
Power Options:	4 Pin AC Power Supply 4 Pin DC Power and I/O Supply 30W PoE Injector 90W PoE Injector
Web UI OS Support:	Windows® 8, 10 Mac OS® X 10.10 or Higher Linux® Ubuntu 14.04 or Higher Chrome OS v79 or Higher

Environmental

Operating Temperature:	-30°C to 65°C

NOTE: The PoE injector is an indoor device and considered support equipment. It can operate at a maximum temperature of 35°C (95°F).

Ingress Protection:	IP41

Cellular Technology

- 5G NR Sub 6 Stand Alone (SA) & Non-Stand Alone (NSA) Support
- CAT 22 LTE
- Dynamic Spectrum Sharing (DSS) Support
- Up to 256 QAM DL

Bluetooth

- Bluetooth for Inseego Connect Installation App Only

Positioning

- L1/L5 Active GNSS Band Support
- Active Antenna Support
- Assisted Cellular GNSS Support

GNSS Constellations:	GPS GLONASS Galileo BDS

Networking

- Port Filtering
- DHCP
- DMZ
- Configurable DNS
- MAC Address Filtering
- IP Passthrough (Bridge Mode)
- Private APN Support
- Private 5G/Private LTE Support

Security

NAT Firewall
Device Cybersecurity Agent
VPN PassThrough
MACsec Ethernet Security
Security Hardened Web Interface
Fully Encrypted Log Files
Fully Encrypted Cloud Agent
Anti-CSRF
Session Timeout
Incorrect Password Lockout
Admin Portal to Block Factory Reset

Regulatory Information

Federal Communications Commission Notice (FCC – United States)

FCC ID: PKRISGS2000E3

Electronic devices, including computers and wireless modems, generate RF energy incidental to their intended function and are therefore subject to FCC rules and regulations.

This equipment has been tested to, and found to be within, the acceptable 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 when the equipment is operated in a residential environment.

This equipment generates radio frequency energy and is designed for use in accordance with the manufacturer's user manual. However, there is no guarantee that interference will not occur in any particular installation. If this equipment causes harmful interference to radio or television reception, which can be determined by turning the equipment off and on, you are 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 the 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/television technician for help.

This device complies with Part 15 of the Federal Communications Commission (FCC) Rules. Operation is subject to the following two conditions.

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

WARNING: DO NOT ATTEMPT TO SERVICE THE WIRELESS COMMUNICATION DEVICE YOURSELF. SUCH ACTION MAY VOID THE WARRANTY. THIS DEVICE IS FACTORY TUNED. NO CUSTOMER CALIBRATION OR TUNING IS REQUIRED. CONTACT INSEEGO CORP TECHNICAL SUPPORT FOR INFORMATION ABOUT SERVICING YOUR WIRELESS COMMUNICATION DEVICE.

FCC CAUTION: Any changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

MODIFICATIONS: The FCC requires that you be notified that any changes or modifications made to this device that are not expressly approved by Inseego Corp. may void your authority to operate the equipment.

NOTE: The Radio Frequency (RF) emitter installed in your modem must not be located or operated in conjunction with any other antenna or transmitter, unless specifically authorized by INSEEGO CORP.

Innovation, Science and Economic Development Notice (ISED – Canada)

IC: 3229A-S2000E3

ISED RSS-Gen Notice

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique 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;
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISED Canada ICES-003 Compliance

CAN ICES-3 (B)/NMB-3(B)

FCC and ISED RF Exposure Guidance Statement

In order to comply with FCC/ISED RF Exposure requirements, this device must be installed to provide at least 20 cm separation from the human body at all times.

Afin de se conformer aux exigences d'exposition RF FCC / ISED, cet appareil doit être installé pour fournir au moins 20 cm de séparation du corps humain en tout temps.

Cellular External Antenna Considerations:

1. External Antenna(s): Not Included
2. To comply with RF Exposure Requirements, the Maximum Cellular Antenna Gain Must Not Exceed:

Cellular Band	**Antenna Gain (dBi) Including Cable Loss**
4G-LTE: B30	-0.6
4G-LTE: B71 5G-FR1: n71	3.1
4G-LTE: B12/B17 5G-FR1: n12	3.2
4G-LTE: B13/B42/B43/B48 4G-LTE: B14	3.5 3.6
3G-UMTS: B5 4G-LTE: B5/B26 5G-FR1: n5	4
4G-LTE: B41 5G-FR1: n41	5
3G-UMTS: B2/B4 4G-LTE: B2/B4/B25/B66 5G-FR1: n2/n25/n66	6
4G-LTE: B7/B38	7

CE

Inseego Corp. declares that S2000e-3 is in Compliance with the Radio Equipment Directive 2014/53/EU, its essential requirements and other relevant provisions of the directive.

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

The Declaration of Conformity may be also consulted at Inseego Corp., 9710 Scranton Rd., Suite 200 San Diego, USA.

RF Radiation Exposure Guidance Statement

This device must be installed to provide at least 20 cm separation from the human body at all times.

Radio Frequency and Transmitted Output Power Information

Band	Max Power	Frequency
WCDMA BAND I	24 dBm	1920-1980 MHz
WCDMA BAND VIII	24 dBm	880-915 MHz
LTE BAND 1	24 dBm	1920-1980 MHz
LTE BAND 3	24 dBm	1710-1785 MHz
LTE BAND 7	24 dBm	2500-2570 MHz
LTE BAND 8	24 dBm	880-915 MHz
LTE BAND 20	24 dBm	832-862 MHz
LTE BAND 28	24 dBm	703–748 MHz
LTE BAND 38	24 dBm	2570–2620 MHz
LTE BAND 40	24 dBm	2300–2400 MHz
LTE BAND 42	19.5 dBm	3400–3600 MHz
LTE BAND 43	19.5 dBm	3600–3800 MHz
FR1 n1 (NSA)	24 dBm	1920-1980 MHz
FR1 n3 (NSA)	24 dBm	1710-1785 MHz
FR1 n7 (NSA)	24 dBm	2500-2570 MHz
FR1 n8 (NSA)	24 dBm	880-915 MHz
FR1 n20 (NSA)	24 dBm	832–862 MHz
FR1 n28 (NSA)	24 dBm	703-748 MHz
FR1 n38 (NSA)	24 dBm	2570–2620 MHz
FR1 n40 (NSA)	24 dBm	2300-2400 MHz
FR1 n78 (NSA)	24 dBm	3300–3800 MHz
Bluetooth (BLE)	4 dBm	2.4 GHz

Product Certifications and Supplier's Declarations of Conformity

Product Certifications and Supplier's Declarations of Conformity documentation may be consulted at Inseego Corp., 9710 Scranton Road Suite 200, San Diego CA 92121, USA. https://www.inseego.com/support/.

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 S2000e device, or failure of the S2000e device to transmit or receive such data.

Limited Warranty and Liability

THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE (OR BY COUNTRY OR PROVINCE). OTHER THAN AS PERMITTED BY LAW, INSEEGO CORP DOES NOT EXCLUDE, LIMIT OR SUSPEND OTHER RIGHTS YOU MAY HAVE, INCLUDING THOSE THAT MAY ARISE FROM THE A PARTICULAR SALES CONTRACT.

INSEEGO CORP warrants for the 12-month period (or 24-month period if required by statute where you purchased the Product) immediately following your receipt of the Product that the Product will be free from defects in material and workmanship under normal use. TO THE EXTENT PERMITTED BY LAW, 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 CORP'S option, of defective or non-conforming materials, parts, components or the device. 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 CORP'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 CORP'S specifications or authorized by INSEEGO CORP, (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 CORP, (VII) products designated by INSEEGO CORP 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. There is no warranty that information stored in the Product will be retained following any Product repair or replacement.

EXCEPT AS PROVIDED IN THIS WARRANTY AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, INSEEGO CORP IS NOT RESPONSIBLE FOR DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM ANY BREACH OF WARRANTY OR CONDITION, OR UNDER ANY OTHER LEGAL THEORY.

THE FOREGOING LIMITATION SHALL NOT APPLY TO DEATH OR PERSONAL INJURY CLAIMS, OR ANY STATUTORY LIABILITY FOR INTENTIONAL AND GROSS NEGLIGENT ACTS AND/OR OMISSIONS. SOME STATES (COUNTRIES AND PROVINCES) DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

Safety Hazards

Do not operate the S2000e 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.

5

Glossary

Glossary

- **4G LTE** —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

- **5G**—Fifth Generation. The successor to 4GLTE technology, offering greater bandwidth and higher download speeds. In addition to serving cellular networks, 5G networks can be used as internet service providers, competing with other ISPs. 5G also opens up new IoT and M2M possibilities. Wireless devices must be 5G enabled to use 5G networks.

- **802.11 (a, b, g, n, ax)** — 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.
- **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.
- **IP type** — The type of service provided over a network.
- **IP address**—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.
- **MAC Address**—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.
- **Network Operator**—The vendor that provides your wireless access. Known by different names in different regions, some examples are: wireless provider, network provider, or cellular carrier.
- **Network Technology**—The technology on which a particular network provider's system is built; such as LTE or GSM.
- **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.

- **Port Forwarding** — A process that allows remote devices to connect to a specific computer within a private LAN.
- **Port Number** — 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.
- **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.
- **Router** — A device that directs traffic from one network to another.
- **RSSI** — Received Signal Strength Indicator. An estimated measure of how well a device can hear a signal from an access point or router. RSSI value is pulled from the device's Wi-Fi card (hence "received" signal strength), so it is not the same as transmit power from an access point or router.
- **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.
- **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.

- **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 6** — The sixth generation of Wireless Fidelity, using 802.11ax on licensed exempt bands between 1 and 6 GHz. This standard was developed in 2020.
- **Wi-Fi Client** — A wireless device that connects to the Internet via Wi-Fi
- **WPA/WPA2** — Wi-Fi Protected Access. A security protocol for wireless 802.11 networks from the Wi-Fi Alliance.
- **WPA3** — The next generation of Wi-Fi Protected Access. WPA3 simplifies security, provides more robust authentication, increased cryptographic strength, and offers additional capabilities for personal and enterprise networks. WPA3 retains interoperability with WPA2 devices.