USER GUIDE

inseego

Inseego Wavemaker™

5G outdoor CPE FW3000

INSEEGO COPYRIGHT STATEMENT

© 2023 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 Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp.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.

Revision Number: PRT-14965435 C

Contents

Introduction and getting started 5
- Overview 6
  - Key features 6
  - System requirements 6
- Indicator LEDs 7
- Getting started 8
  - Connecting to the FW3000 8
  - Monitoring and managing your FW3000 8
- Caring for your FW3000 11
  - Replacing SIM cards 11
  - Resetting your FW3000 13

Configuration 15
- Overview 16
  - Home page 17
  - Side menu 17
  - Getting help 17
- Admin password 18
  - Changing the Admin password 18
- Managing data usage 19
  - Data Usage page 20
- Managing settings 22
  - Preferences tab 23
  - Software Update tab 24
  - Backup and Restore tab 26
  - ZTP tab 28
  - SIM 29
  - GPS tab 32
  - APN tab 33
  - Advanced tab 35
- Viewing info about the FW3000 36
  - Internet Status tab 37
  - Internet Sessions tab 39
  - Diagnostics tab 40
  - Device Info tab 42
  - Logs Tab 43
- Getting support 44
  - Help tab 44
  - Support tab 45

Advanced settings 46
- Overview 47
- Using advanced settings 47
  - Cellular tab 48
  - Manual DNS 49
  - Firewall tab 51
  - MAC Filter tab 52
  - LAN tab 53
  - WAN settings 56
  - Port Filtering tab 57
  - Port Forwarding tab 59
  - Inseego Connect tab 62

Heartbeat timer (Inseego Connect) 63
Troubleshooting and support....64
Overview....65
Troubleshooting 65
Will I always get 5G? Can I use the FW3000 outside of 5G coverage?....65
The FW3000 LED is switching from blue to green and sometimes dropping service....65
Indicator LED is blue or green/SIM appears active, but I cannot browse the internet....65
Can I set my FW3000 to use a specific band? 65
I cannot access the Admin web UI 66
My FW3000 is “Waiting for Connection” on the Inseego Mobile app 66
My FW3000 is getting slow speeds/low throughput 66
My connecting device is not obtaining a valid IP address....67
I cannot get streaming platforms to work with my FW3000 67
Technical support....68
Product specifications and regulatory information 69
Product specifications 70
Device 70
Environmental 70
Network connectivity....71
Security....71
Regulatory information 72
Product certifications and supplier’s declarations of conformity 73
Wireless communications 74
Limited warranty and liability 74
Safety hazards....75

1

Introduction and getting started

Overview

Ports and buttons

Indicator LEDs

Getting started

Caring for your FW3000

Overview

The Inseego Wavemaker 5G outdoor CPE FW3000 brings high-speed 5G and LTE connectivity using an advanced antenna design and superior thermal mitigation to ensure superior connectivity for years to come.

Inseego recommends that FW3000 be installed by professional technicians to assure optimal antenna orientation and performance.

Key features

- High-power 5G radio that extends network coverage up to X miles (X km).
- Designed to operate in extreme temperatures from -20°C to 60°C (-4 to 140°F), has an environmental rating of IP67 for water and dust ingress, and an internal heating element for startup and operation in cold environments.
- Best-in-class enterprise-grade security features comprehensive protection of digital information.
- Remote management with the Inseego Connect™ - convenient remote device management capabilities for a single device included, plus tiered upgrade options for advanced device management, monitoring and diagnostics for multiple devices from a single dashboard.
- Support for up to two SIMs and auto switching between service providers. Multi-carrier firmware allows the FW3000 to be used on most major global service providers.

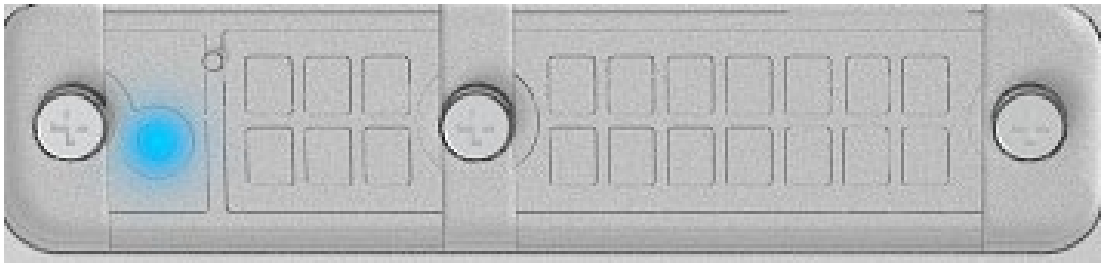
System requirements

Admin web UI operating systems supported include:

- Windows 10 and later
- MacOS 10.14 and later
- Linux® Ubuntu 18.04 LTS and later

Indicator LEDs

The device LED is located in the SIM compartment and is visible through the protective shield. It changes colors and either blinks or glows solid to communicate current states for the device.



LED color	Operation	Meaning
Blue*	Solid Blinking	Strong 5G connection (3 – 5 bars) Weak 5G connection (1 – 2 bars)
Green*	Solid Blinking	Strong 4G connection (3 – 5 bars) Weak 4G connection (1 – 2 bars)
Yellow**	Solid	Software update is in progress
Red	Solid Blinking	Device is booting up No service, SIM error, or locked SIM card

*If the LED is blue or green and the SIM appears active, but you cannot browse the internet, contact your service provider to check the status of the SIM and troubleshoot any APN issues.

** This color can look more lime green than yellow.

The PoE injector also has an indicator LED. **NOTE:** The LED does not indicate data transmission.

LED color	Meaning
Green	FW3000 is NOT connected and there is no load
Red	FW3000 is connected

Getting started

This section provides instructions connecting to your FW3000 and monitoring and managing the CPE.

Connecting to the FW3000

To turn on your FW3000 and connect a device:

1. Check that the PoE cable from the FW3000 is in the **Data & Power Out** port on the PoE power injector and the PoE power injector is plugged into an earthed AC outlet.

2. Insert one end of a Cat6A Ethernet cable into the **Data In** port on the PoE power injector.

3. Insert the other end of the cable into the Ethernet port of the device you wish to connect.
   NOTE: Any time you switch the device you are connecting to the FW3000, you must first disconnect the existing connected device and power cycle the FW3000 before connecting the new device.

WARNING! Use only the PoE power injector supplied with the FW3000. Unapproved power supplies could cause overheating or fires, resulting in serious bodily injury, death, or property damage. Do not defeat the safety purpose of a grounding-type plug. Use the PoE power injector only in combination with an earth-socked outlet.

Monitoring and managing your FW3000

You can use multiple options to monitor and manage your 5G outdoor CPE:

Inseego Mobile app

You can use the same mobile app used to install your FW3000 for routine device monitoring and management.

Admin web UI

Once your FW3000 is connected to a device that supports web browsing, you can use the Admin web UI to customize settings, change your password, and access information. On a device connected to the

FW3000, open any web browser, and go to http://192.168.1.1, http://Inseego.local*, or http://fw3000.com*. The initial sign in password is: "**Fast5G!**".

NOTE: You cannot connect to the web UI through a router. Your computer must be directly connected by Ethernet cable to the Data In port on the FW3000 PoE power injector.

Inseego Connect™

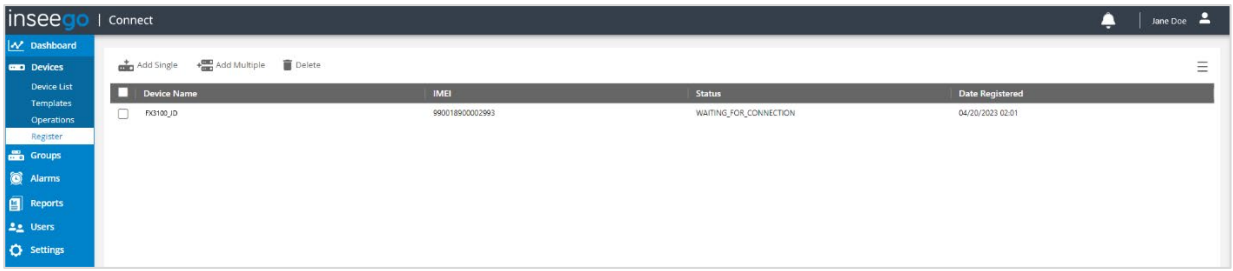
Inseego Connect is a multi-tiered device management platform that allows you to deploy, monitor, and manage Inseego IoT devices remotely from the cloud. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free Inseego Connect account at connect.inseego.

NOTE: Your device may have been added to Inseego Connect during the installation process. When logging in to Inseego Connect, check to see if your device is on the Device List or on Devices > Register. Restart your device to hasten the registration process.

Adding a device to Inseego Connect

To add a device or multiple devices to Inseego Connect:

1. Ensure the device you are adding is powered on and connected to the internet.
2. Sign in to Inseego Connect and navigate to **Devices > Register**.



3. Use the tools along the top of the table to add devices.

   NOTE: When adding a device, make sure the device is powered on and connected to the internet.

   Add Single: Use this button to add a single device.

   - Enter a **Device Name** (optional).
   - Enter the **Device IMEI** printed on the label of the device.

* The Inseego.local and fw3000.com web UI addresses rely on having IPv6 enabled on your connecting device.

- For **Device Password**, enter the current Admin web UI password. If you have already logged into the device's Admin web UI and changed the Admin password, use the new password. If you have not changed the Admin password, the default is "**Fast5G!**"
- Click **Register**. The device enters a Waiting for Connection state while waiting to connect to the Inseego cloud.

Add Multiple: Use this button to add multiple devices by uploading an .xlsx file.

- Click the **Download sample template (.xlsx)** link.
- Open the .xlsx file and enter a **Name** (optional), **IMEI**, and **Password** for each device you wish to register.
- Click **Upload**. The devices enter a Waiting for Connection state while waiting to connect to the Inseego cloud.

IMPORTANT: After adding a device, restart the device immediately. This allows the device to check in and process the registration request.

Once the registration process is complete, the device appears on the Device List page and no longer appears on the Register page.

Caring for your FW3000

This section provides information on replacing SIM cards and restoring your FW3000 to factory default settings.

Replacing SIM cards

A SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. SIM cards are installed in your FW3000 during the technician installation process. These instructions are for replacing a SIM card.

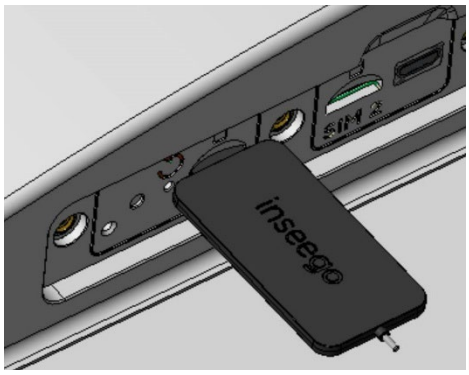
The FW3000 supports only Nano SIM cards.

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 replace the SIM card:

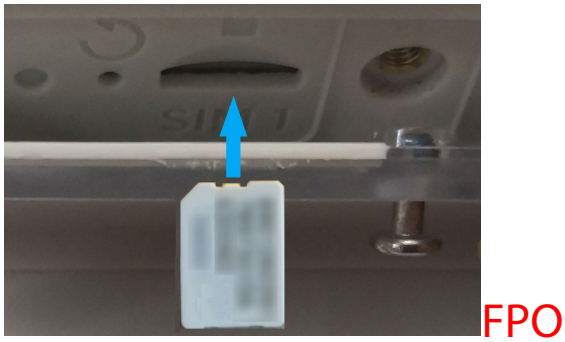
- Disconnect the PoE cable to the FW3000 from the **Data & Power Out** port on the PoE power injector.
- Unscrew the protective cover over the SIM slots using a Phillips-head screwdriver.

- Use the SIM end of the provided SIM tool to remove the existing SIM card.



- If necessary, remove the new SIM card from the protective sleeve, being careful not to touch the gold-colored contacts.

- Use the SIM end of the provided SIM tool to insert the SIM card into the appropriate SIM slot with the gold-colored contact points facing the front of the device. **NOTE:** Do not use excessive force.



- Reattach the protective cover to a torque of .5 Nm (.369 ft/lb).

FPO

Correct tether placement **Incorrect tether placement**

WARNING! If the tether is bunched, it could prevent the compartment from being effectively sealed.

- Insert the PoE cable to the FW3000 back into the **Data & Power Out** port on the PoE power injector.

NOTE: If there is an issue, check the indicator LED (see Indicator LEDs on page 7) to make sure the SIM is working correctly. Should a SIM card be lost or damaged, contact your network operator.

Resetting your FW3000

You can reset your FW3000 to factory settings from the Admin web UI, Mobile app, Inseego Connect, or by using the reset button on the device.

CAUTION! Resetting returns your FW3000 to factory settings, including the Admin password.

Resetting from the Admin web UI

To reset the FW3000 from the Admin web UI, select **Settings** > **Backup and Restore** and click **Restore factory defaults**.

Resetting from the Inseego Mobile app

To reset the FW3000 from the Inseego Mobile app, select **Mobile Options**, then select **Factory Reset.**

Resetting from Inseego Connect

To reset the FW3000 from Inseego Connect, on the **Devices** page, check the box next to the device and select **Factory Reset.**

Resetting with the reset button

The reset button is in a small hole located in the SIM compartment on the bottom of the FW3000 device. This button returns the device to factory settings, including resetting the Admin password.

To reset the FW3000 from the reset button:

1. Unscrew the protective shield over the SIM compartment using a Phillips-head screwdriver.

2. Place the RESET end of the provided SIM tool (or one end of an unfolded paper clip) into the reset hole.

3. Press for five to six seconds, then your FW3000 will restart.

4. Check the indicator LED (see Indicator LED on page 7) to make sure the FW3000 is working correctly.

5. Reattach the protective shield cover to a torque of .5 Nm (.369 ft/lb), making sure the tether passes through the hole of the rear housing and is not bent or bunched.

FPO

Correct tether placement **Incorrect tether placement**

WARNING! If the tether is bunched, it could prevent the compartment from being effectively sealed.

2

Configuration

Overview

Admin password

Managing data usage

Managing settings

Viewing info about the FW3000

Getting support

Overview

You can use multiple tools to configure and troubleshoot your FW3000:

- **Admin web UI** – Provides a local gateway to configure and manage your FW3000. On a device connected to the FW3000, open any web browser, and go to http://192.168.1.1, http://Inseego.local*, or http://fw3000.com*. Select **Sign In** (in the top-right corner of the screen) and enter the **Admin Password** ("**Fast5G!**" is the default).

- **Inseego Connect** – Enables you to monitor and configure an entire deployment of devices remotely from the cloud. You can group devices together to push widespread configurations, troubleshoot individual devices, set alarms, and run reports. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free Inseego Connect account at connect.inseego.

- **Inseego Mobile app** – Allows you to perform basic device monitoring and management. Scan the QR code to download the Inseego Mobile app from Apple Store or Google Play Store, or visit https://inseego.com/products/cloud-management/inseego-mobile-app/#available-now to download the app.

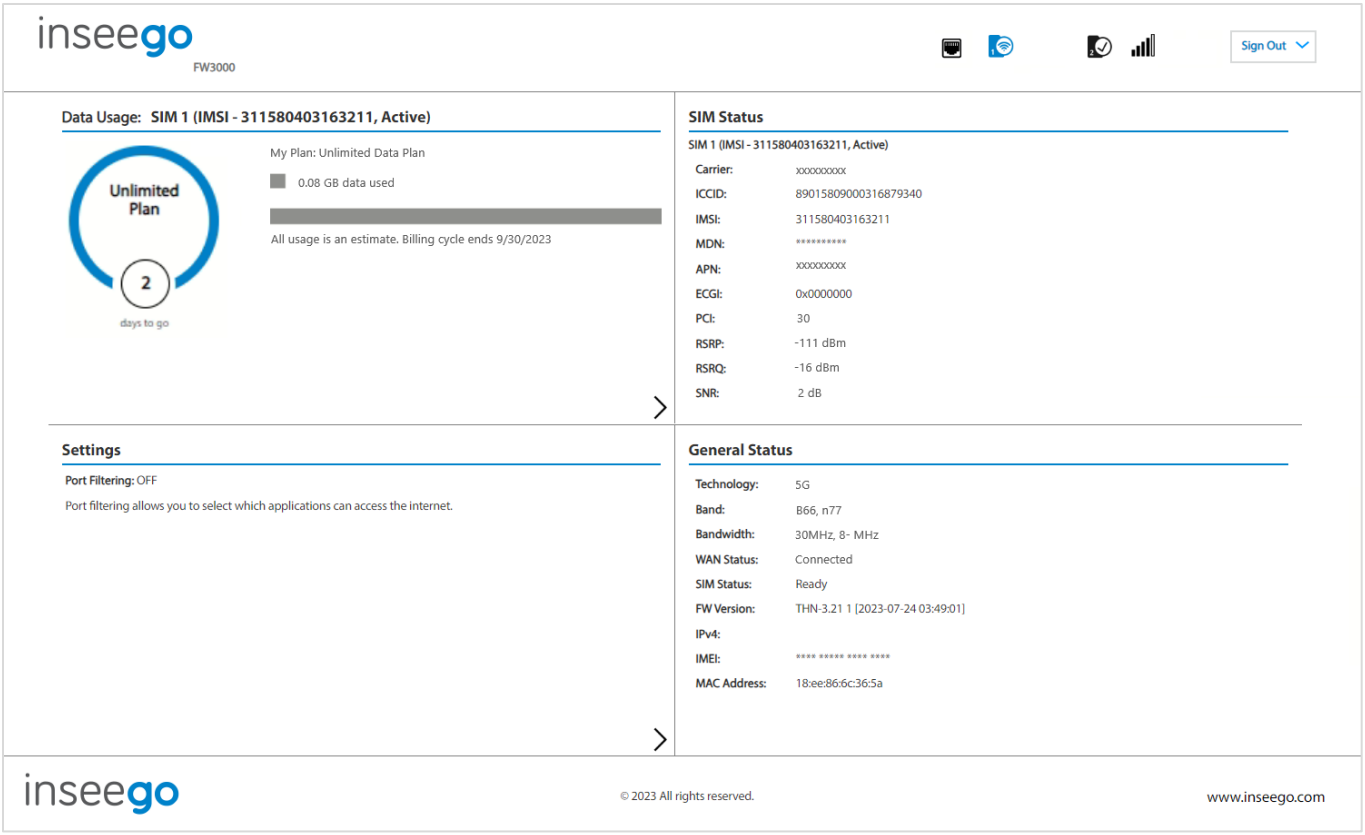
This chapter provides the configuration options available for your FW3000 devices. The configurations shown are from the Admin web UI, unless otherwise noted. Many of these options are also available with Inseego Mobile app and Inseego Connect. Some configurations are available only with Inseego Connect and are marked as such.

* The Inseego.local and fw3000.com web UI addresses rely on having IPv6 enabled on your connecting device.

Home page

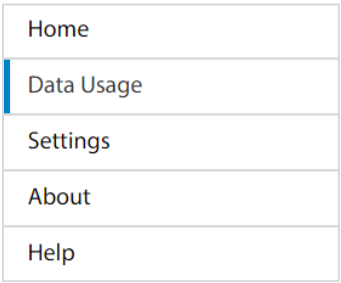
The home page of the Admin web UI is the local gateway to configuring and managing your FW3000. It displays data usage and general status information.

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



Side menu

Each sub screen in the FW3000 Admin web UI includes a menu on the left that you can use to return to the home page or jump to other pages. The current page is indicated by a blue bar. A similar side menu is available when configuring devices with Inseego Connect.



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 FW3000 Admin web UI. The default Admin password is "**Fast5G!**".

You are prompted to change the Admin password upon first login. Change the password to something easy 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:

Important: If you are in the process of adding your FW3000 to Inseego Connect, wait to change your Admin password until the registration process is complete and your FW3000 is listed on the Inseego Connect Device List page.

1. **From the Admin web UI:** Click the down arrow next to **Sign Out** in the top-right corner of any Admin web UI page and select **Change Password.**

   From Inseego Connect: Select **Device** > **Admin Password** from the Configure side menu.

2. Enter your current Admin password, then click **Continue**.

3. Enter a new password and confirm it.

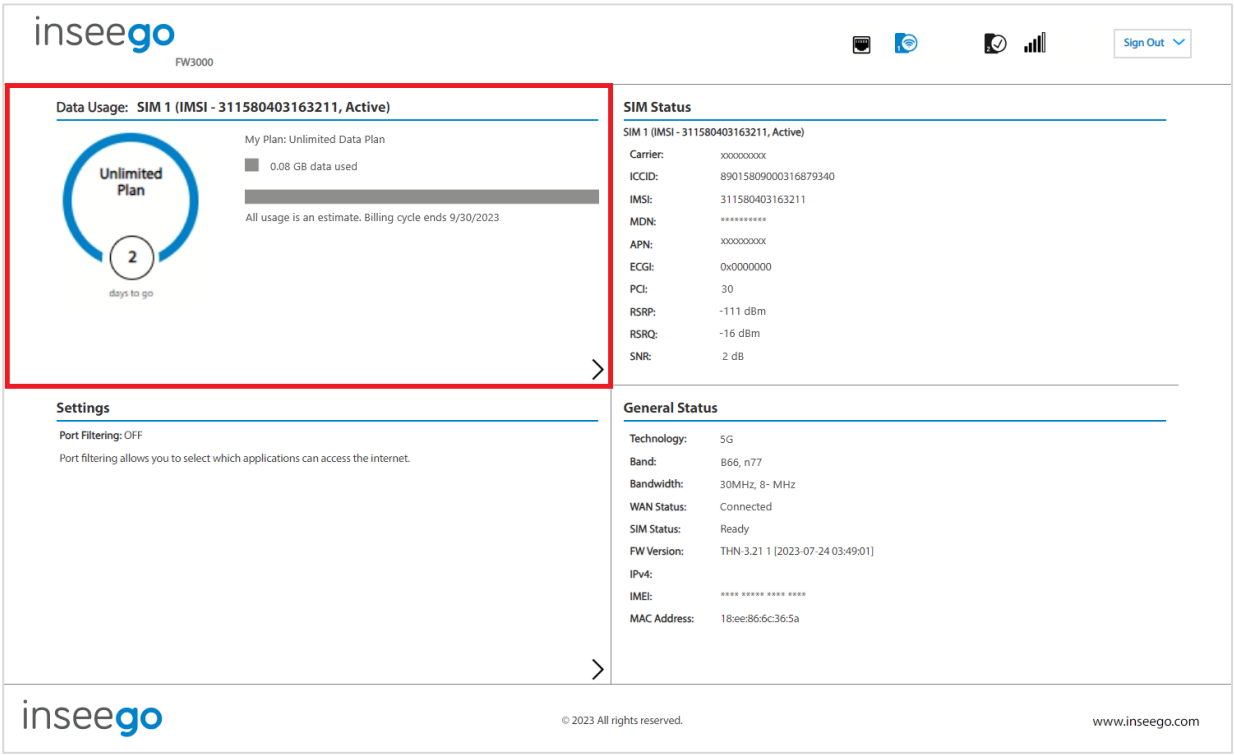
4. Select a security question from the drop-down list and type an answer to the question.
   NOTE: Answers are case-sensitive.

5. Click **Save Changes**.

The next time you sign in to the FW3000 web UI, use the new Admin password. If you cannot remember the password, click **Forgot Admin password**. After you correctly answer the security question you set up, the current password is displayed.

Managing data usage

On the Admin web UI home page, the Data Usage panel shows current data usage information for the active SIM.

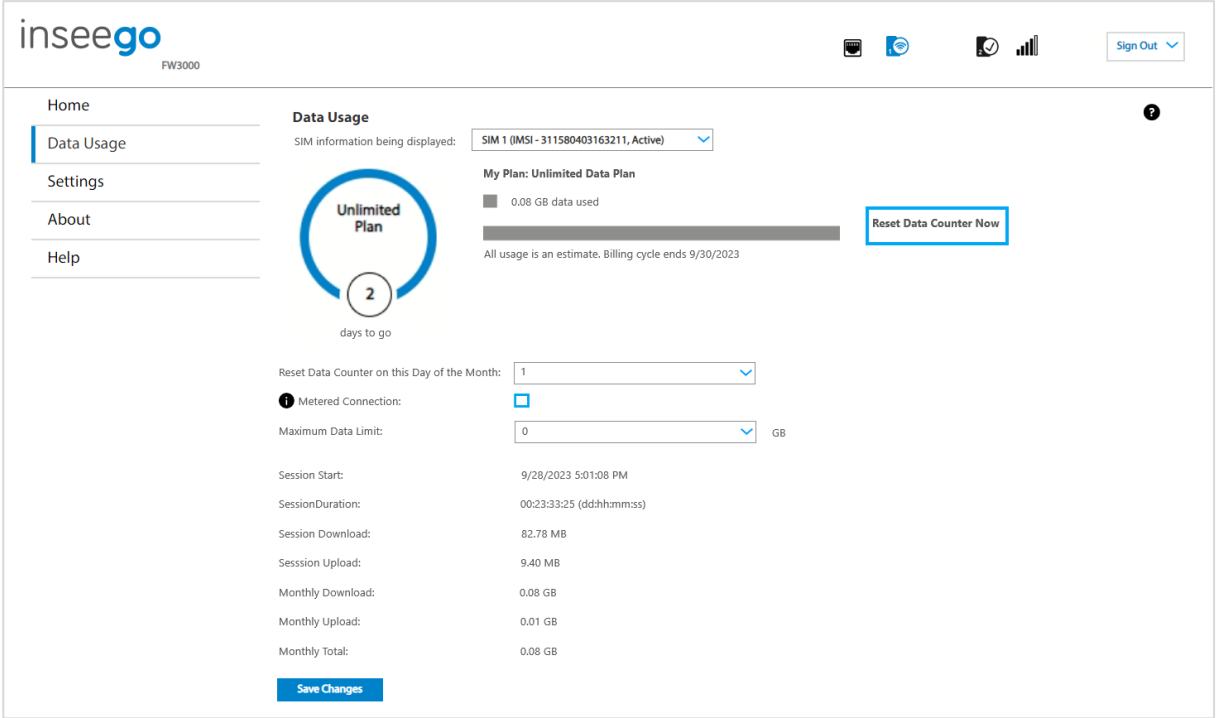


To manage or view data usage, select > from the home page Data Usage panel or select **Data Usage** from the side menu. The Data Usage page appears.

Data Usage page

Use the Data Usage page to view details and manage your FW3000 data usage.

NOTE: Your FW3000 provides only a rough estimate of data usage. Always check with your service provider for exact usage.



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

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

- Estimated amount of data used in the current billing cycle
- Number of days left in the billing cycle
- Date the billing cycle ends

You can configure settings to reflect your monthly data plan.

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.

Metered Connection: Check this box if there is a data limit on your plan.

Maximum Data Limit: Enter a maximum data limit, if applicable.

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 Download: The amount of data downloaded for the current internet session. This counter starts at zero when the connection is established.

Session Upload: The amount of data uploaded for the current internet session. This counter starts at zero when the connection is established.

Monthly Download: The amount of data downloaded for the current billing cycle.

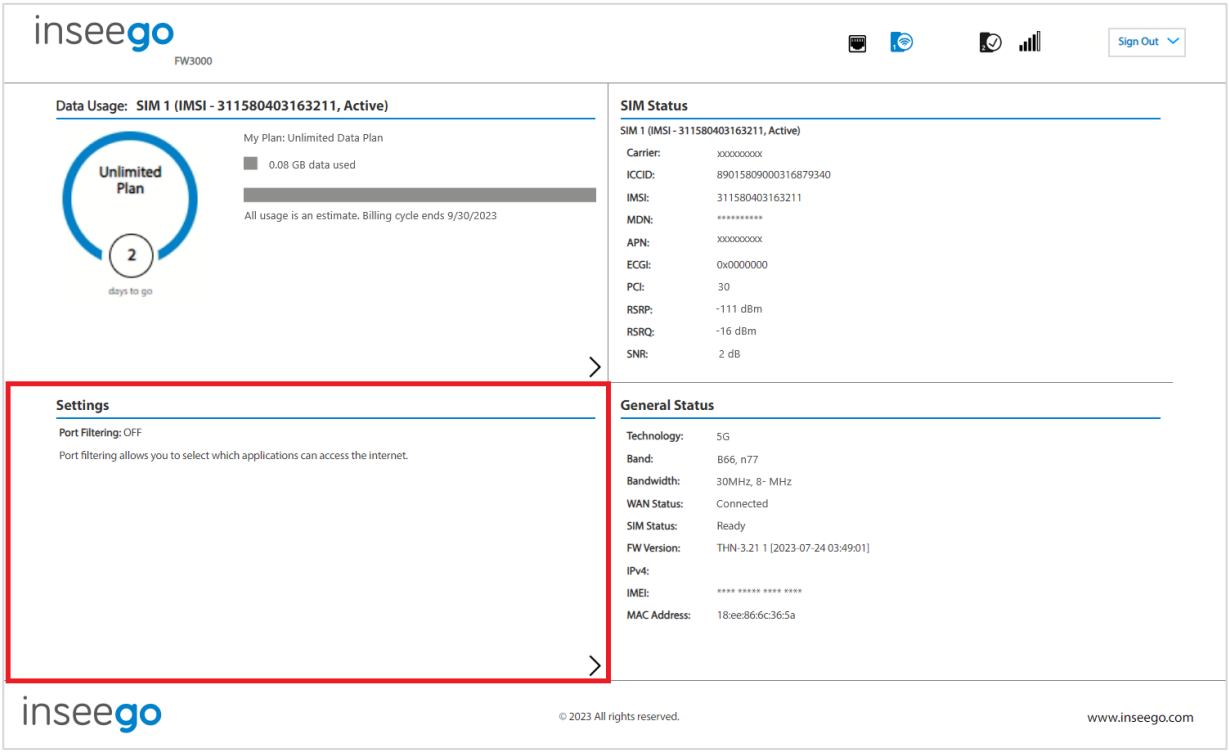
Monthly Upload: The amount of data uploaded for the current billing cycle.

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

Select **Save Changes** to enact changes.

Managing settings

On the Admin web UI home page, the Settings panel shows Port Filtering information.



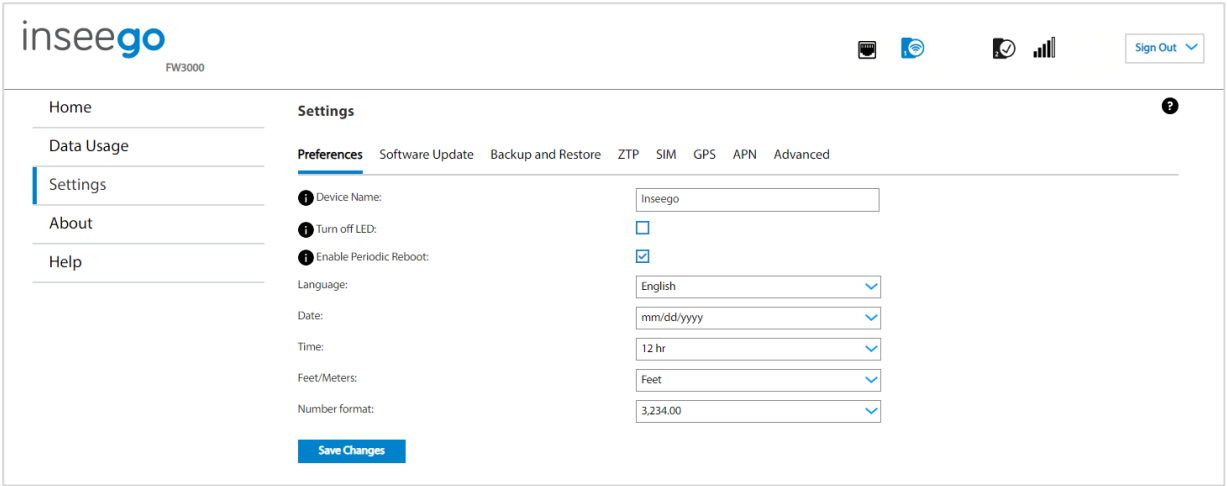
To configure more system settings, select > from the home page Settings panel or select **Settings** from the side menu.

The Settings page includes the following tabs:

- Preferences
- Software Update
- Backup and Restore
- ZTP
- SIM
- GPS
- APN
- Advanced

Preferences tab

You can use this tab to change the FW3000 name that defines the device network, turn off the LED light, and enable periodic reboot. You can also change the language and how dates, time, distance, and numbers are displayed in the web UI.



Device Name: The device name that defines the device network and URL to access the FW3000 local web UI**.** **NOTE:** Depending on your service provider, this selection may be read-only.

Turn off LED: Check the checkbox to turn off the LED display light on your FW3000.

Enable Periodic Reboot: Enables a periodic reboot feature that allows the device to automatically restart every two weeks. **NOTE:** By default, the reboot occurs at 2:00 AM on Sunday. You can change the schedule in Inseego Connect preference settings.

NOTE: The following settings affect packets sent to remote servers. For example, if you select a 24-hour time format, the Admin web UI, and any packets reporting time somewhere else, will display time in 24-hour format.

Language: Select a language for the Admin web UI.

Date: Select the date format to be used throughout the web UI (mm/dd/yyyy or dd/mm/yyyy).

Time: Select the time format to be used throughout the web UI (12 or 24 hour).

Feet/Meters: Select the format for distance displayed in the web UI (feet or meters).

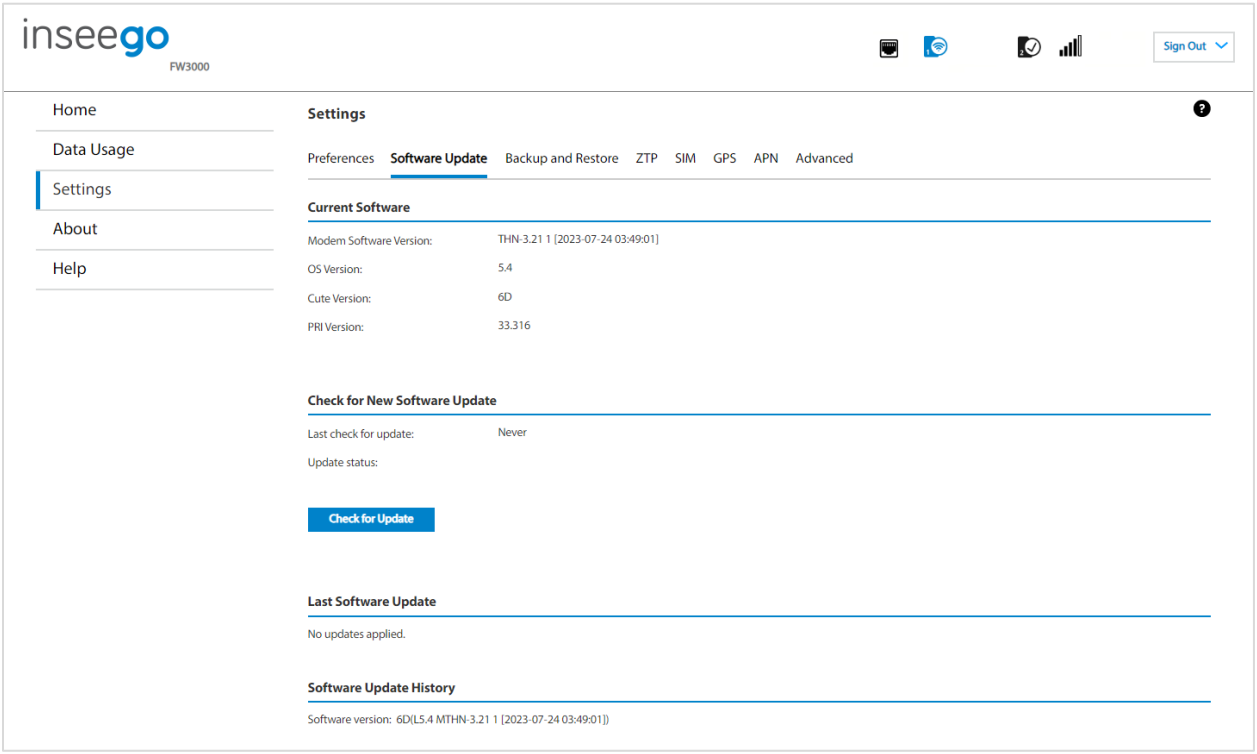
Number format: Choose the format for decimal numbers displayed in the web UI (using a period or comma as the decimal point).

Make your selections and click **Save Changes** to update settings.

Software Update tab

Software updates are delivered to the FW3000 automatically over the mobile network. This tab displays your current software version, last system update information, software update history, and allows you to check for new software updates.

NOTE: You can opt out of software updates using Inseego Connect.



Current Software

Modem Software Version: The version of software currently installed for the modem component.

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

Cute Version: The cute version of the software currently installed on your FW3000.

PRI Version: The configuration version currently applied to your FW3000.

Check for New Software Update

Last check for update: The date and time the FW3000 last checked to see if an update was available.

Update status: This area is usually blank. If you check for an update, the results display.

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

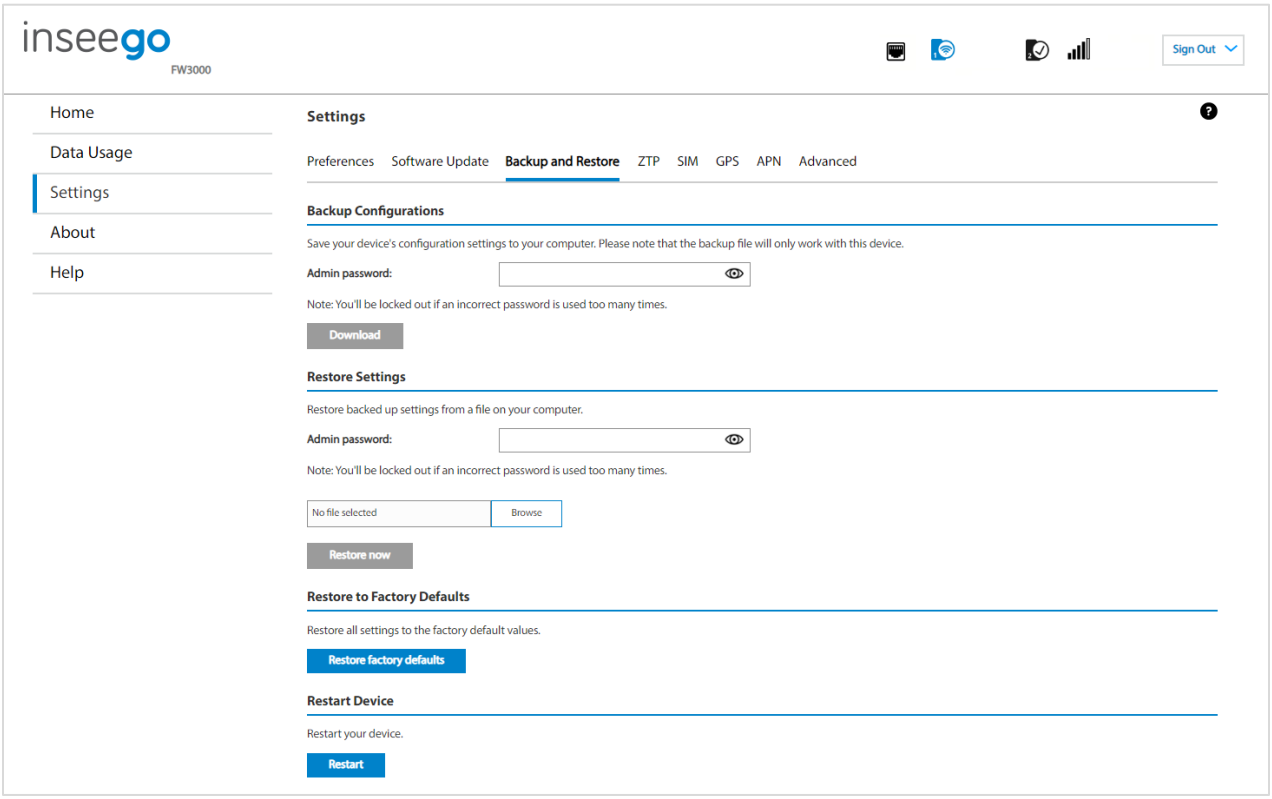
This section displays details about the last software update.

Software Update History

This section provides details of the last two updates downloaded and installed to this FW3000. If no updates have been installed, this section displays the current software version.

Backup and Restore tab

Use this tab to back up current FW3000 settings to a file on your computer, restore (upload) a previously saved configuration file, reset the FW3000 to factory defaults, or restart the FW3000.



Backup Configurations

To back up current FW3000 settings to a file on your computer, enter your Admin password in the **Admin password** field.

The default Admin password is, "**Fast5G!**". If you have changed the Admin password and don't remember it, select **Sign In** in the top-right corner, click **Forgot Admin Password**, and answer the displayed security question. The current Admin password is displayed.

NOTE: If you enter an incorrect password five times in a row, you will be locked out of the Admin web UI. To unlock it, restart your FW3000 and use the default Admin password, "**Fast5G!**".

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 FW3000.

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 FW3000, and settings can only be viewed or changed using the Admin web UI.

Restore Settings

CAUTION! Restoring settings (uploading a configuration file) changes ALL the existing settings to match the configuration file. This may change the current Wi-Fi settings, breaking all existing connections to the FW3000 and disconnecting you from the Admin web UI.

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

Click **Browse** and choose a backup settings file to restore.

NOTE: You can only restore a file that was created for this model of FW3000.

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 may change the current Wi-Fi settings, breaking all existing connections to your FW3000 and disconnecting you from the Admin web UI.

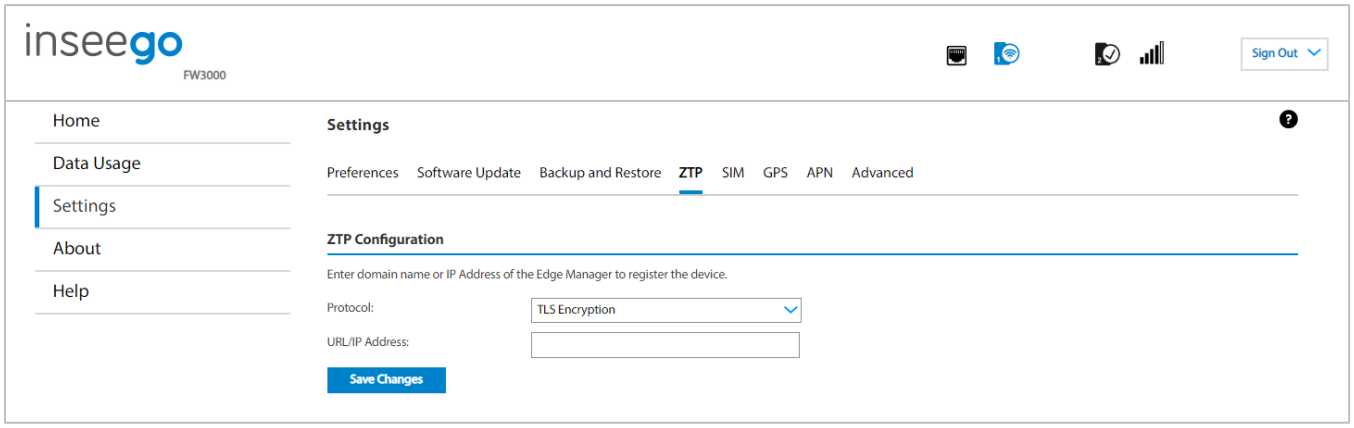
Restart Device

Restart: This button turns your FW3000 off and on again.

ZTP tab

Use this tab to initiate Zero Touch Provisioning (ZTP) when onboarding devices to Inseego 5G SD EDGE™ Manager.

Inseego SD Edge is a cloud-based management system that provides remote monitoring and comprehensive worksite network security. It provides IT teams with real-time visibility, control, and management of critical network infrastructure in a secure manner with advanced authentication, authorization, and encryption. To learn more about Inseego's SD Edge offering go to https://inseego.com/products/cloud-management/inseego-sd-edge/.



ZTP Configuration

Protocol: Use TLS Encryption as the protocol.

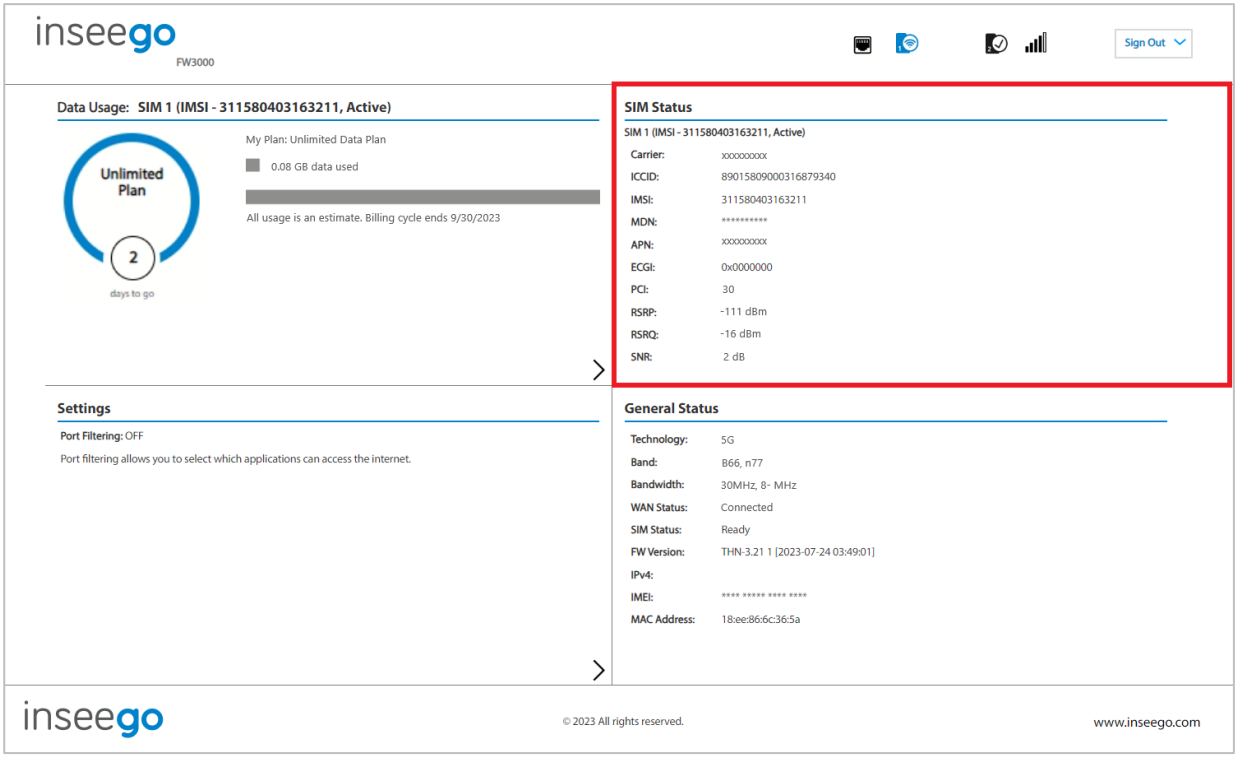
WARNING! **TLS Encryption** is strongly recommended. **Test** is plaintext for testing purposes only and may compromise the security of your network if used for deployment.

URL/IP Address: Enter the domain used for your EDGE Manager instance.

Click **Save Changes** to initiate ZTP.

SIM

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



SIM: The active SIM on which data is displayed.

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 FW3000. This is a unique number, usually fifteen digits, that identifies a Global System for Mobile Communications (GSM) subscriber.

MDN: The phone number of your FW3000.

APN: The access point name for your FW3000.

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

PCI: The Physical Cell ID.

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.

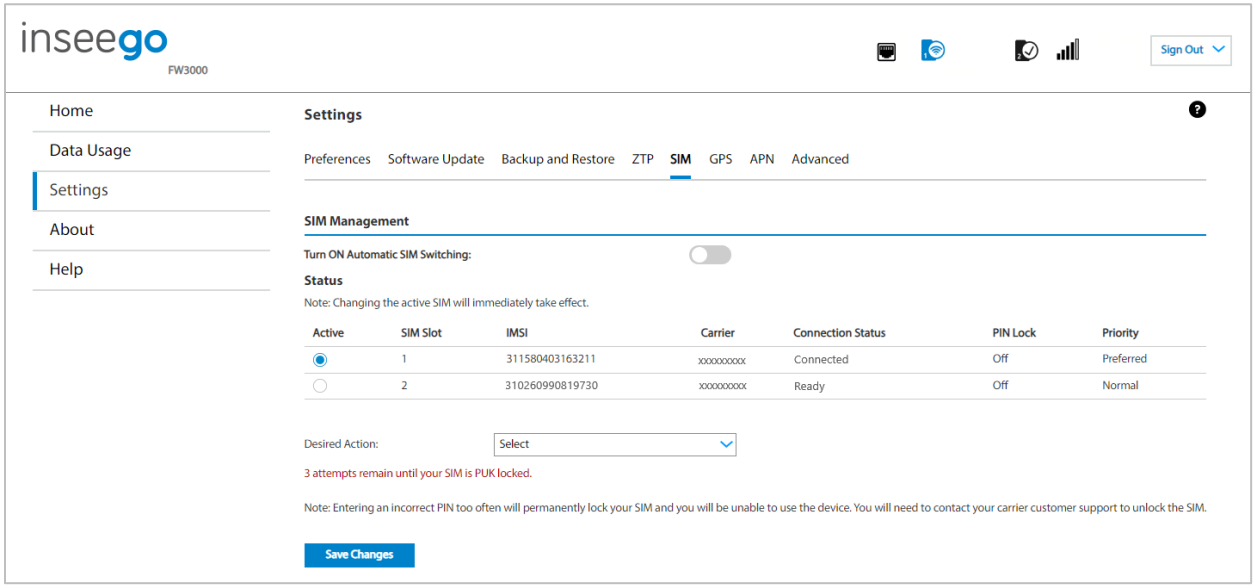
RSRQ: Reference Signal Received Quality. A calculated value from RSRP and RSSI that provides a measure of signal and interference.

SNR: Signal to Noise Ratio. The ratio of signal power to noise power expressed in decibels. SNR is a positive value, and higher numbers are better.

To configure SIM settings, select **Settings** from the side menu. Then select the **SIM** tab.

SIM tab

Use this page to turn on automatic SIM switching, change the active SIM, or enter a SIM PIN.



NOTE: The SIM card in your FW3000 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: 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.

Status

Active: Select the SIM you want to be active. **NOTE:** The change will take effect immediately. If IP Passthrough is enabled, please wait 120 seconds for the SIM switching process to complete.

SIM Slot: The SIM slot number.

IMSI: The International Mobile Subscriber Identity (IMSI) for your FW3000. 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:

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.

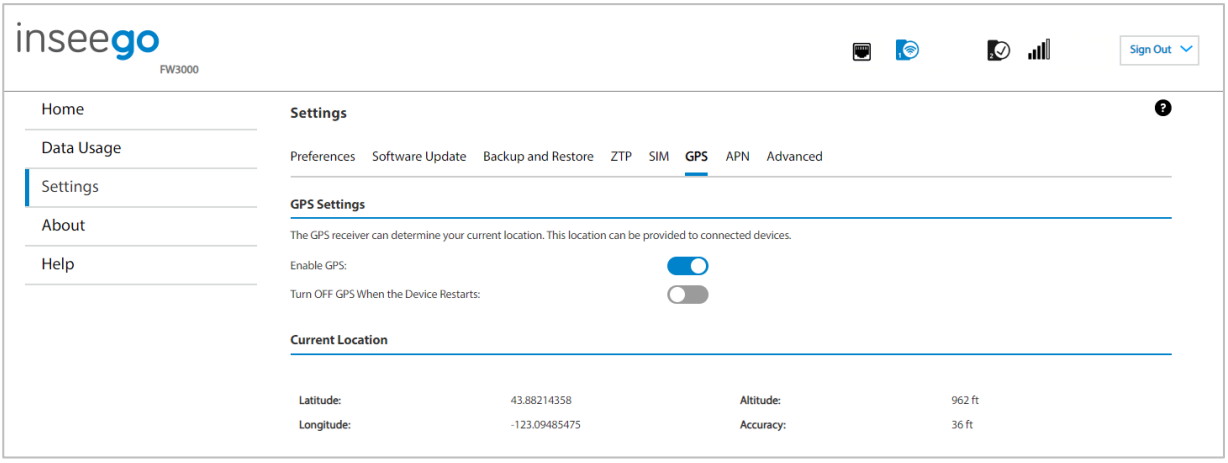
Change PIN - Allows you to change the SIM PIN. You must enter the current PIN, then enter the new PIN and confirm it.

NOTE: The default SIM PIN is available from your service provider.

Click **Save Changes**.

GPS tab

The FW3000 incorporates a GPS receiver. Use this tab to enable GPS and view location information.



GPS Settings

Enable GPS: This setting enables or disables the GPS radio on your FW3000. 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.

Turn off GPS when the Device Restarts: This setting determines when the GPS receiver will turn off, once it is on. When the ON/OFF slider is **ON**, the GPS receiver turns off when the FW3000 is shut down. You will need to turn it on again the next time the GPS receiver is needed.

Current Location

Latitude: Latitude for the last location fix.

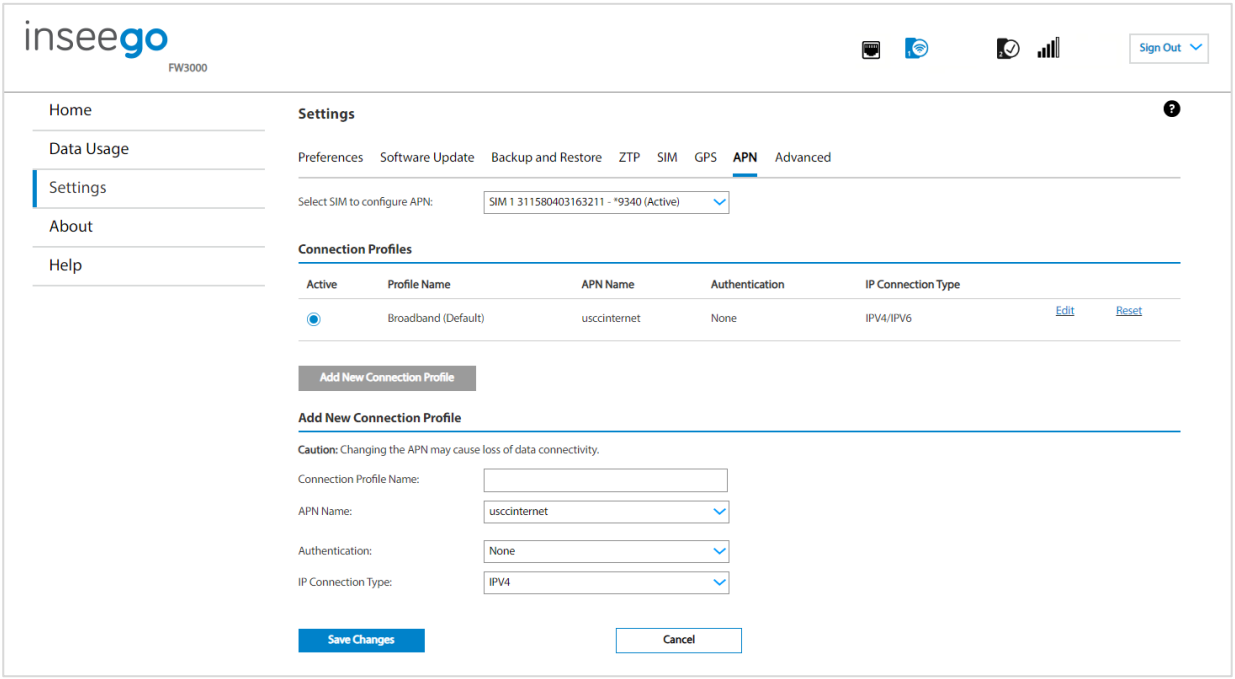
Longitude: Longitude for the last location fix.

Altitude: Altitude for the last location fix.

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

APN tab

In most configurations, the FW3000 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 configure connection profiles for your APN on this tab for the network to communicate with the FW3000.



Select SIM to configure APN: Use the drop-down to select the SIM on which you want to configure the APN.

Connection Profiles

NOTE: Initially, the default APN profile is displayed. You cannot delete this profile, but you can edit it and/or add additional profiles.

Active: Select the connection profile you want to be active.

Profile Name: The name that identifies the connection profile.

APN Name: The access point name.

Authentication: The authentication method for the connection profile.

IP Connection Type: The IP connection type for the connection profile.

Click **Edit** to edit a profile.

Click **Reset** to reset a profile to default values.

Click the **Add New Connection Profile** button to add an additional APN connection profile.

Add New Connection Profile

Connection Profile Name: Enter a name to identify this connection profile.

APN Name: Select an APN supplied by your service provider from the drop-down or select **Add APN** and enter the APN for your private network in the text box that appears below.

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

Carrier	APN Type	APN
Verizon	Public Dynamic	vzwinternet
	Public Static-West	we01.vzwstatic
	Public Static-Northwest	nw01.vzwstatic
	Public Static-Northeast	ne01.vzwstatic
	Public Static-South	so01.vzwstatic
	Public Static-Midwest	mw01.vzwstatic
AT&T	Public Dynamic	broadband
	Public Dynamic	i2gold
T-Mobile	Public Dynamic	fast.t-mobile.com
	Public Static	b2b.static
Telstra	Public Dynamic	telstra.internet

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

NOTE: Information entered in the following fields should come from your service provider based on network requirements.

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

Username: Enter the username for your private network. **NOTE:** This option is not visible when Authentication is set to None.

Password: Enter the password for your private network. **NOTE:** This option is not visible when Authentication is set to None.

IP Connection Type: Select an IP connection type from the drop-down (IPv4, IPv6, or IPv4/IPv6).

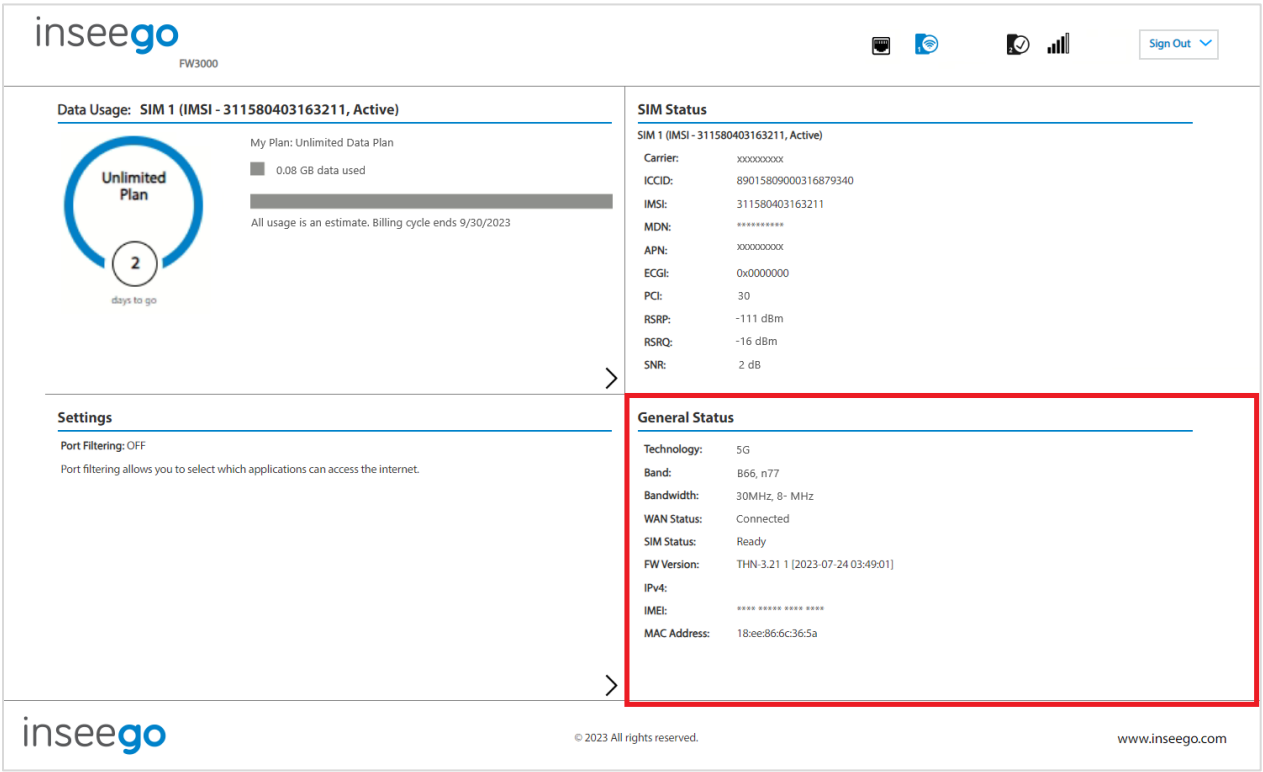
Click **Save Changes**.

Advanced tab

Advanced settings are intended only for users with advanced technical knowledge. For information about the Advanced Settings page, go to Chapter 4, Advanced Settings on page 47.

Viewing info about the FW3000

On the Admin web UI home page, the General Status panel provides an overview of the current FW3000 status.



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

Band: The band in use for the current connection.

Bandwidth: The bandwidth in use for the current connection.

WAN Status: The status of the WAN.

SIM Status: The status of the SIM card. If the SIM card is missing, or there is some form of SIM error, connection to the mobile network is not possible.

FW Version: The version of the firmware (software) currently installed on your FW3000.

IPv4: The internet IP address assigned to the FW3000.

IMEI: The International Mobile Equipment Identity (IMEI) for your FW3000. 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 the Wi-Fi interface on your FW3000. The MAC address is a unique network identifier assigned when a network device is manufactured.

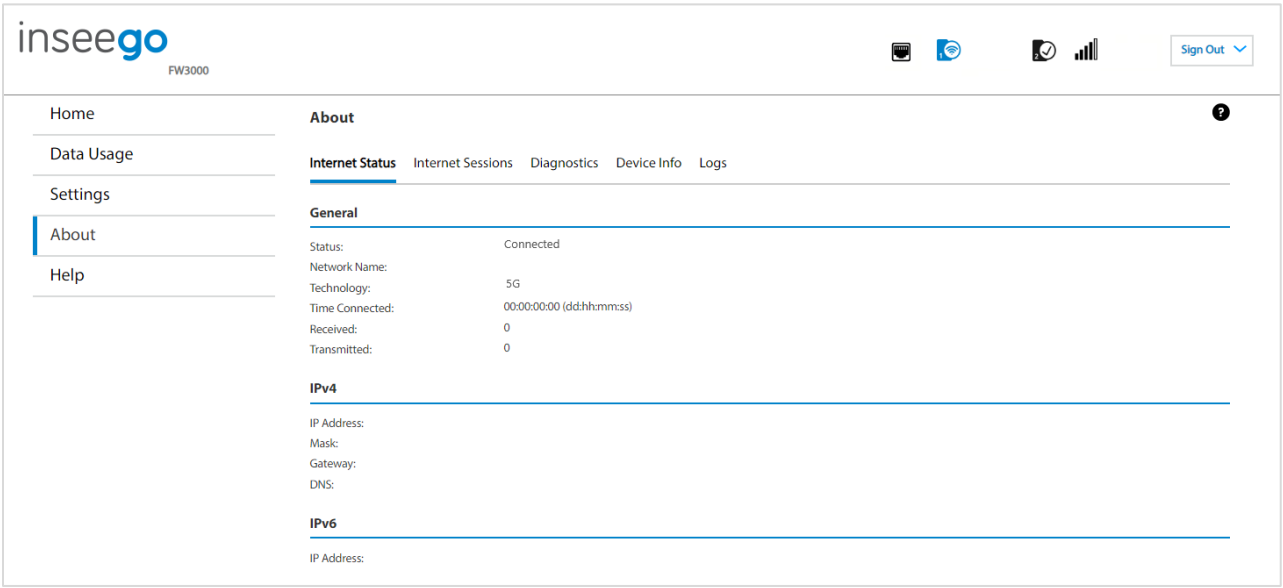
To view more detailed information about your FW3000 and its use, select **About** from the side menu.

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 FW3000 connection.

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

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 FW3000.

Mask: The network mask associated with the IPv4 address.

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

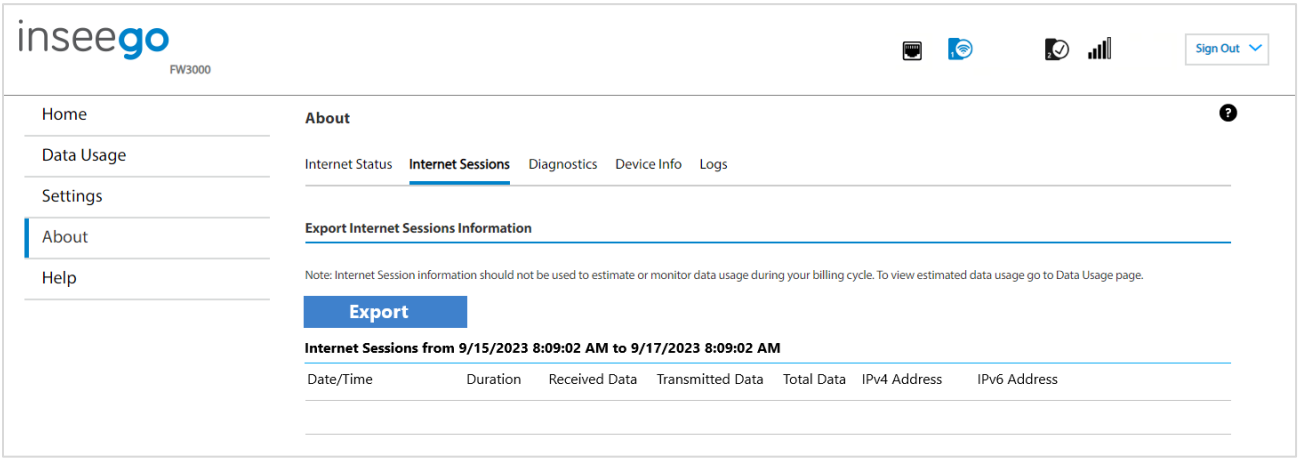
DNS: The Domain Name Server currently used by the FW3000.

IPv6

IP Address: The global IPv6 address for the FW3000 (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.

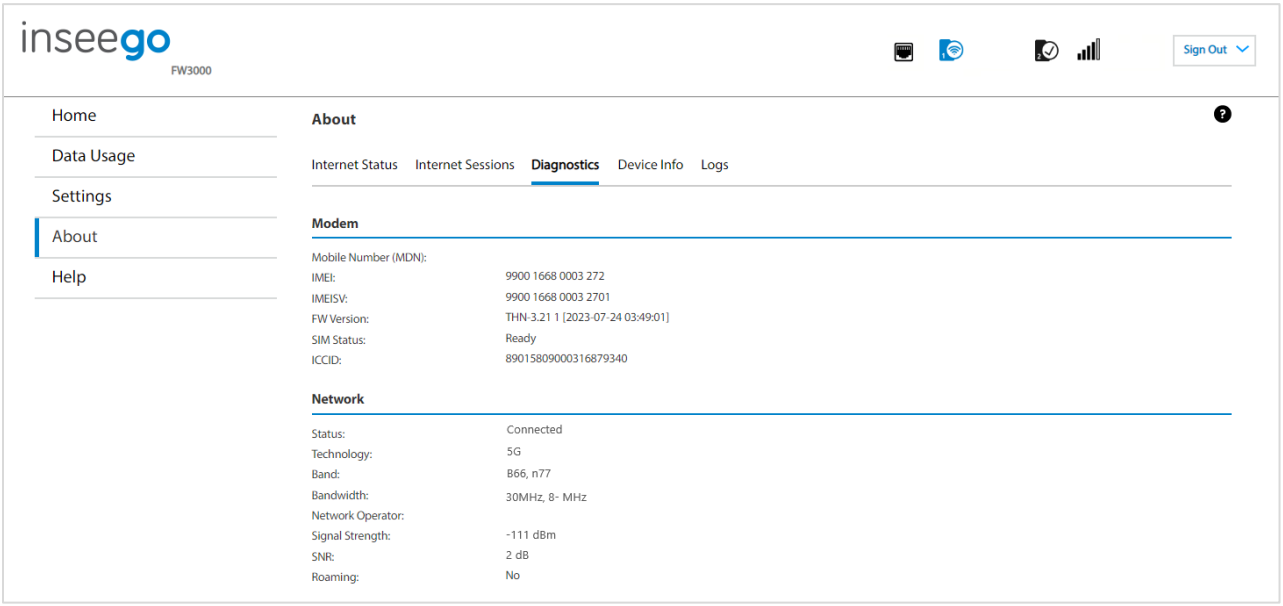
Total Data: The total amount of data for the internet session. This is the sum of Received Data and Transmitted Data.

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 service provider).

Diagnostics tab

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



Modem

Mobile Number (MDN): The phone number of your FW3000.

IMEI: The International Mobile Equipment Identity (IMEI) for your FW3000. This is a 15-digit code used to uniquely identify an individual mobile station. The IMEI does not change when the SIM is changed.

IMEISI: A combination of the IMEI and an approval number for this type of device.

FW Version: The version of the firmware (software) currently installed on your FW3000.

SIM Status: The status of the SIM card. If the SIM card is missing, or there is some form of SIM error, connection to the mobile network is not possible.

ICCID: The unique ID number assigned to the SIM card. This field is blank if there is no SIM card installed, or a SIM error condition exists.

Network

Status: The status of the network.

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

Band: The band in use for the current connection.

Bandwidth: The bandwidth in use for the current connection.

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

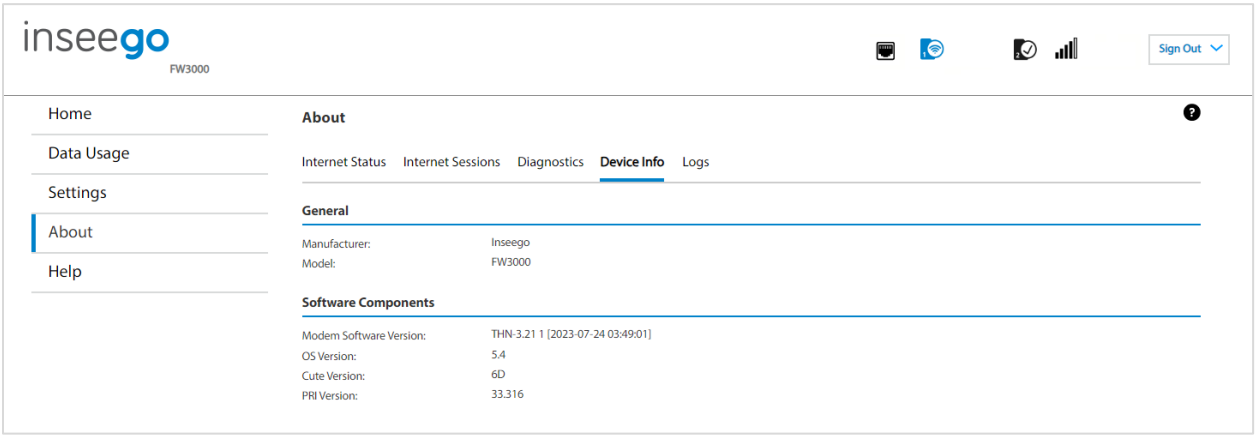
Signal Strength: The strength of the cellular signal (RSRP), measured in dBm. Higher absolute values indicate a stronger signal, for example: -80 dBm is a stronger signal than -90 dBm.

SNR: Signal to Noise Ratio. The ratio of signal power to noise power expressed in decibels. SNR is a positive value, and higher numbers are better.

Roaming: Indicates whether roaming is on.

Device Info tab

Use this tab to view details about your FW3000.



General

Manufacturer: Inseego.

Model: The model of this device.

Software Components

Modem Software Version: The version of software currently installed for the modem component.

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

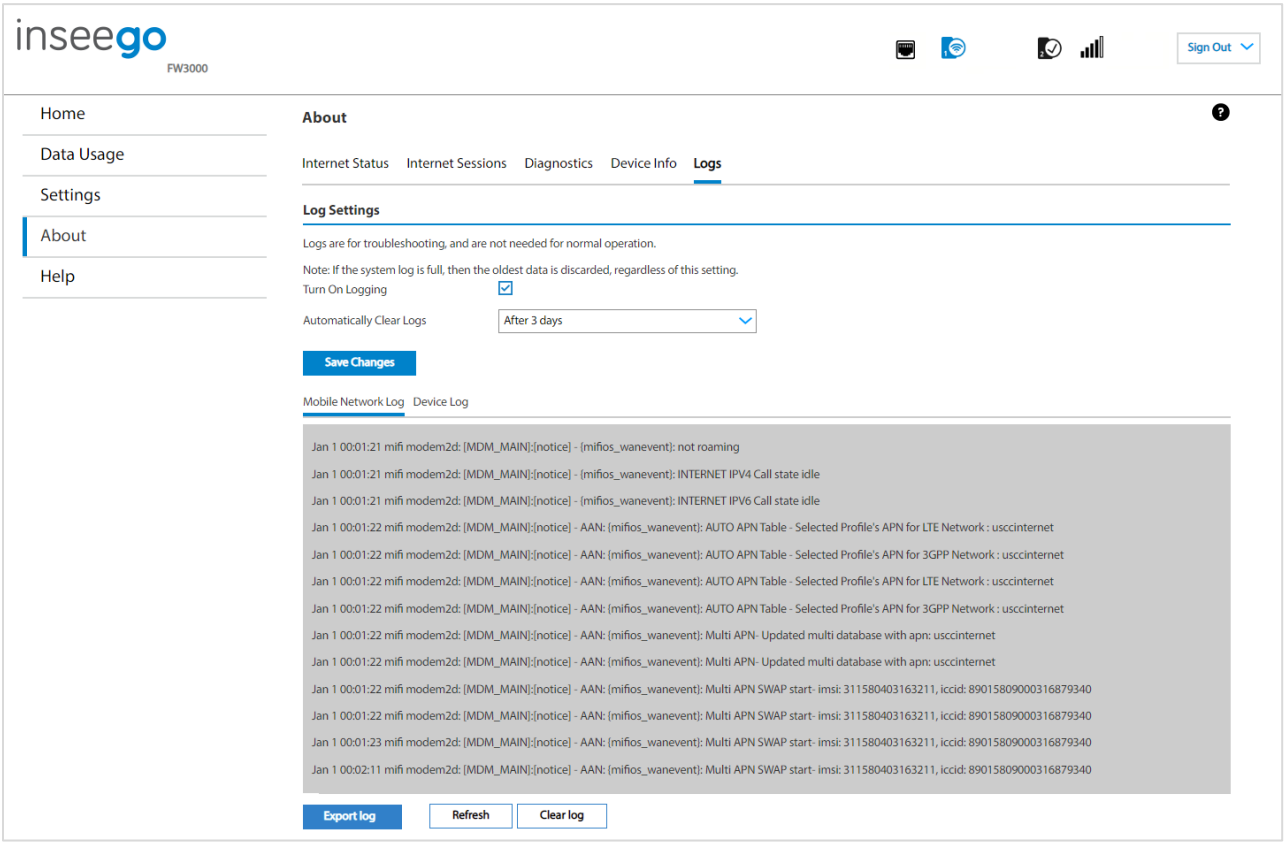
OS Version: The version number for the Operating System and its components.

Cute Version: The cute version of the software currently installed on your FW3000.

PRI Version: The configuration version currently applied to the FW3000.

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.

When logs are turned on, a list of logs is visible:

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

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

Export Logs: Allows you to export log data.

Refresh: Updates the displayed log data.

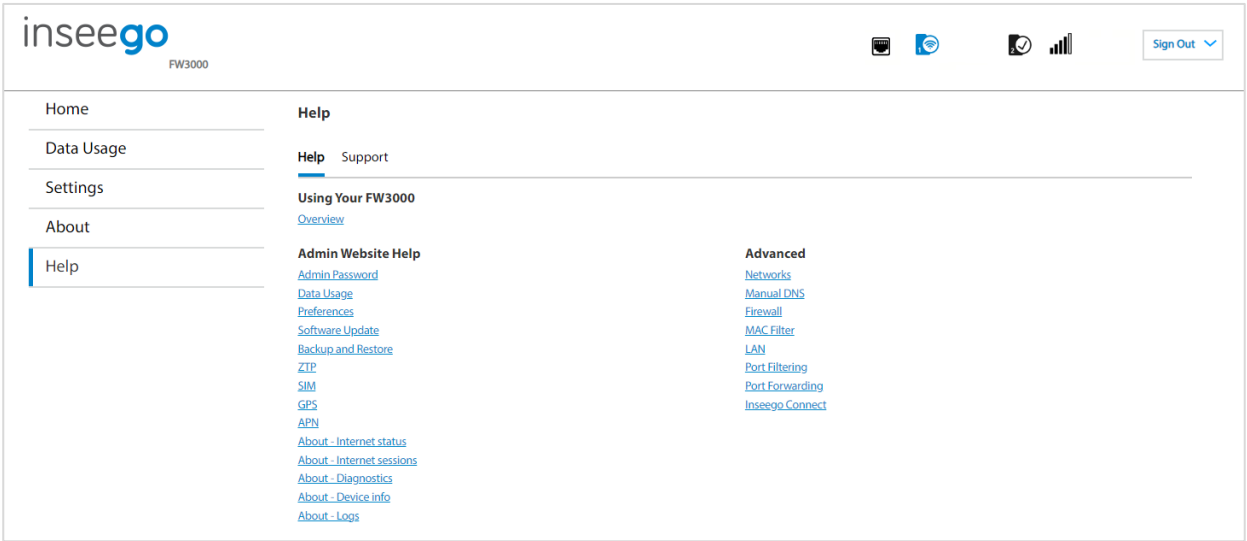
Clear Log: Deletes all existing log data. This makes new data easier to read.

Getting support

For support, select Help from the Admin web UI side menu.

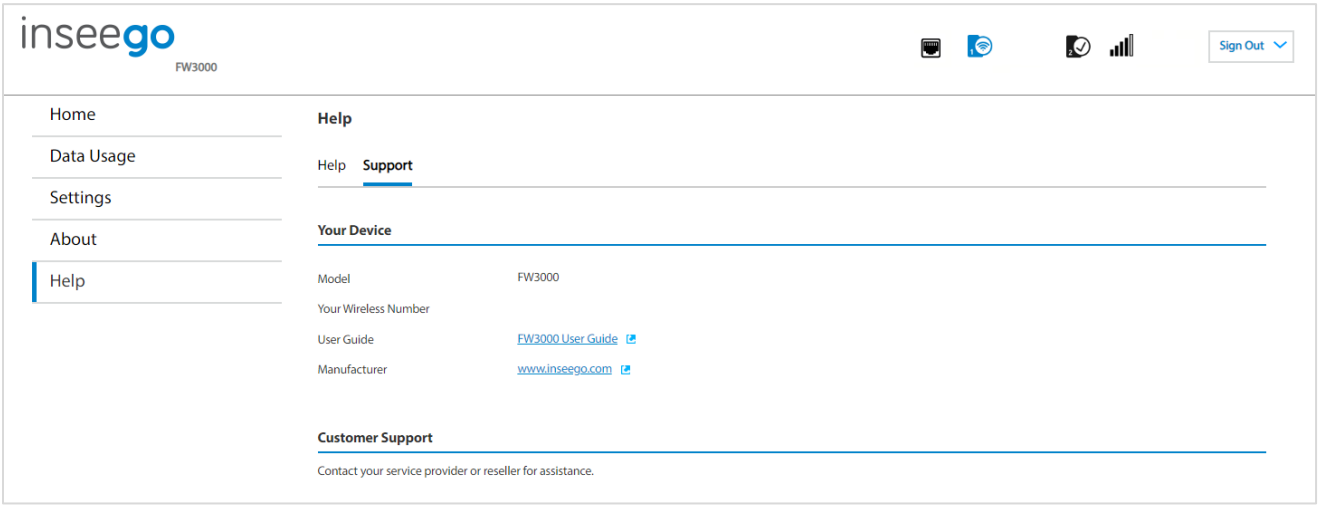
Help tab

This page provides links to help topics for every page of the Admin web UI and general topics useful for getting started with your FW3000.



Support tab

Use the Support tab for useful links and support information.



Your Device

Model: Model of the device.

Your Wireless Number: The phone number associated with your FW3000.

User Guide: A link to this guide.

Manufacturer: A link to the Inseego website.

Customer Support

Contact your service provider for customer support.

3

Advanced settings

Overview

Using advanced settings

Overview

Advanced settings are intended for users with technical expertise in telecommunications and networking.

WARNING! Changing the Advanced settings may be harmful to the stability, performance, and security of the FW3000.

Using advanced settings

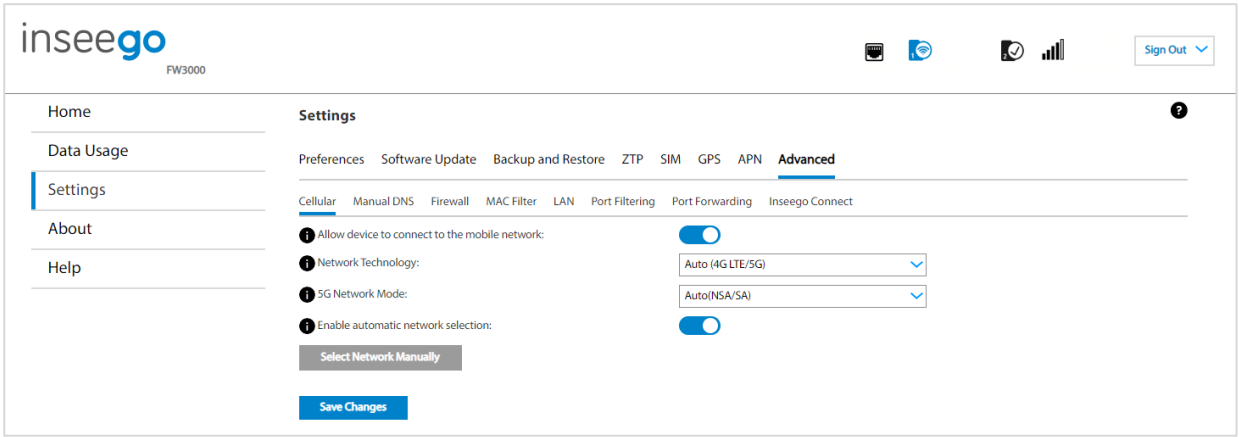
When you select the **Advanced** tab on the Settings page, a warning message appears. If you click **Continue**, the Network tab of the Advanced Settings page appears.

Advanced settings include:

- Cellular
- Manual DNS
- Firewall
- MAC Filter
- LAN
- WAN (Inseego Connect)
- Port Filtering
- Port Forwarding
- Inseego Connect
- HeartBeat Timer (Inseego Connect)

Cellular tab

Use this tab to set options for the cellular network.



Allow device to connect to the mobile network: Use the ON/OFF slider when necessary to turn off cellular data and prevent access to the mobile network. For normal operation, this setting must be left on.

Network Technology: Your FW3000 is set to Auto (4G LTE/5G) by default, which prioritizes 5G but allows 4G and other non-5G technologies to be used. If you select 4G LTE or 5G from the drop-down, your FW3000 is restricted from connecting to networks not using that technology, for example: if you select 4G LTE, your FW3000 will be unable to connect to 5G networks.

5G Network Mode: Your FW3000 is set to Auto (NSA/SA) by default, allowing it to use both standalone 5G and non-standalone 5G, which utilizes 4G anchor bands. You can use the drop-down to select standalone (SA) or non-standalone (NSA) 5G network modes.

Enable automatic network selection: When the ON/OFF slider is **ON**, your FW3000 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. Click the button to scan for available networks, then choose the preferred network. **NOTE:** This option is available only if **Enable automatic network selection** is off.

Click **Save Changes**.

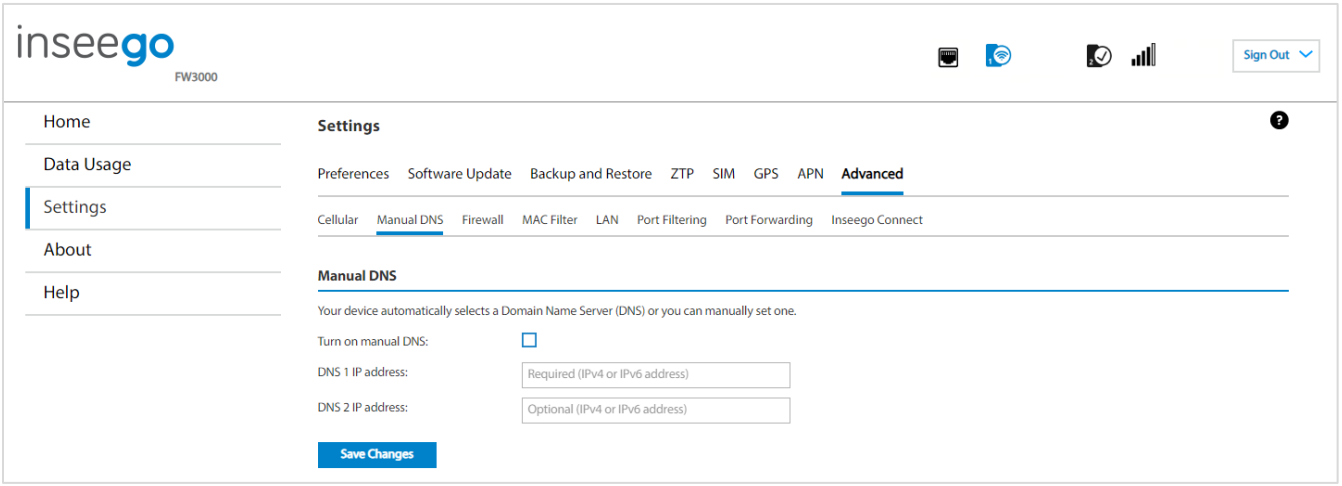
Manual DNS

Manual DNS configuration is available through the Admin web UI and Inseego Connect. You can enable DNS content filtering through Inseego Connect.

- Manual DNS tab (Admin web UI)
- DNS Content Filtering (Inseego Connect)

Manual DNS tab

The FW3000 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.

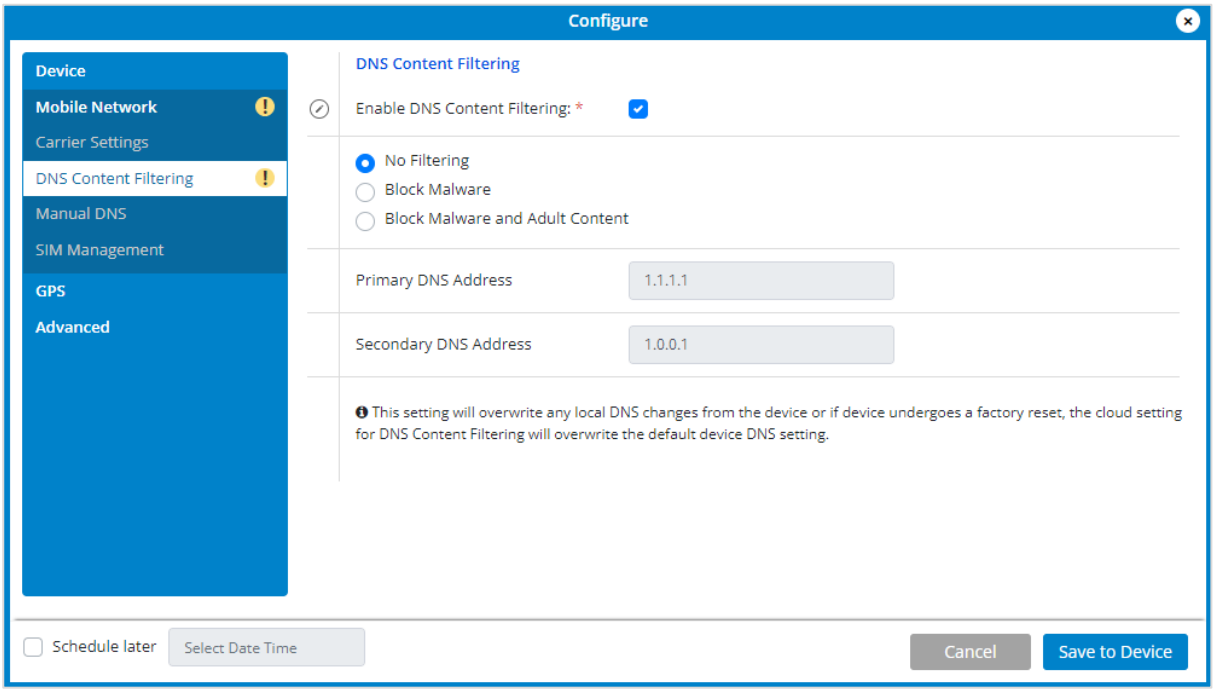
Click **Save Changes**.

DNS Content Filtering (Inseego Connect)

DNS content filtering uses DNS (Domain Name System) to block harmful malware inappropriate content.

You can configure DNS content filtering with Inseego Connect. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free Inseego Connect account at connect.inseego.

NOTE: Settings on this page override any settings on the device Admin web UI and default device settings (when device is reset to factory defaults).



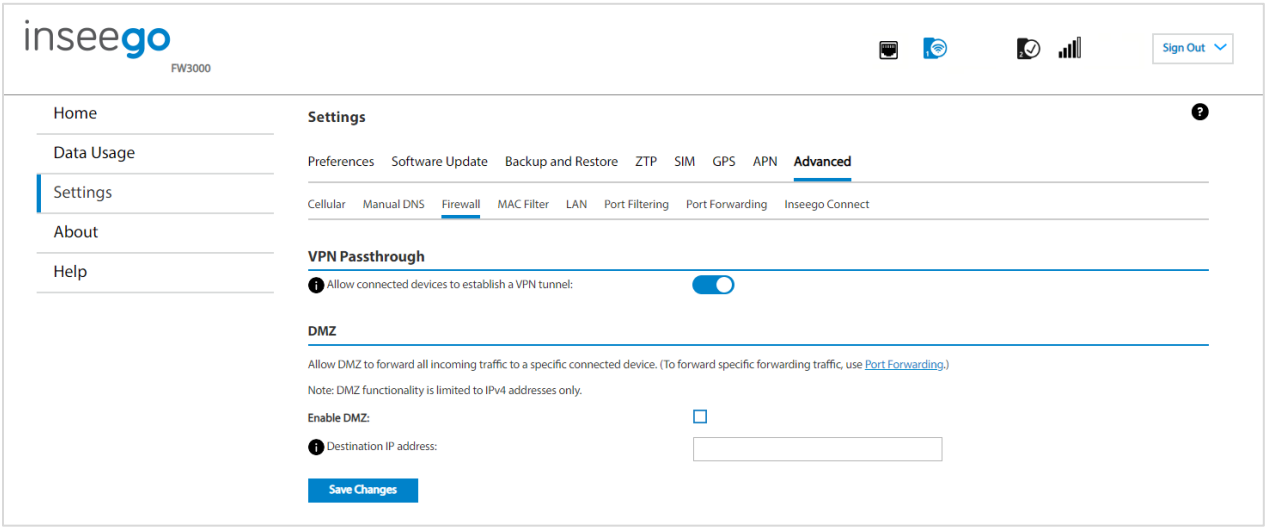
Enable DNS Content Filtering: Check this box to enable DNS content filtering.

Select the filter level (Block Malware, or Block Malware and Adult Content).

If you want the changes enacted at a later time, check the **Schedule later** box (bottom left) and select a date and time from the calendar. Once all your changes are made, select **Save to Device**.

Firewall tab

The FW3000 firewall determines which internet traffic is allowed to pass between the FW3000 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 allow VPN Passthrough and/or designate a specific device to receive all traffic.



VPN Passthrough

To allow a connected device to establish a VPN tunnel, ensure the ON/OFF slider is **ON**.

DMZ

NOTE: When IP Passthrough is turned on, DMZ capabilities are set through the connected host routing system. Settings in this section are not available. Go to **Advanced** > **LAN** to turn IP Passthrough off.

To allow DMZ, you need a static IP address assigned to your line of service. Contact your service provider to set up a line of service for static IP.

Enable 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.

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.

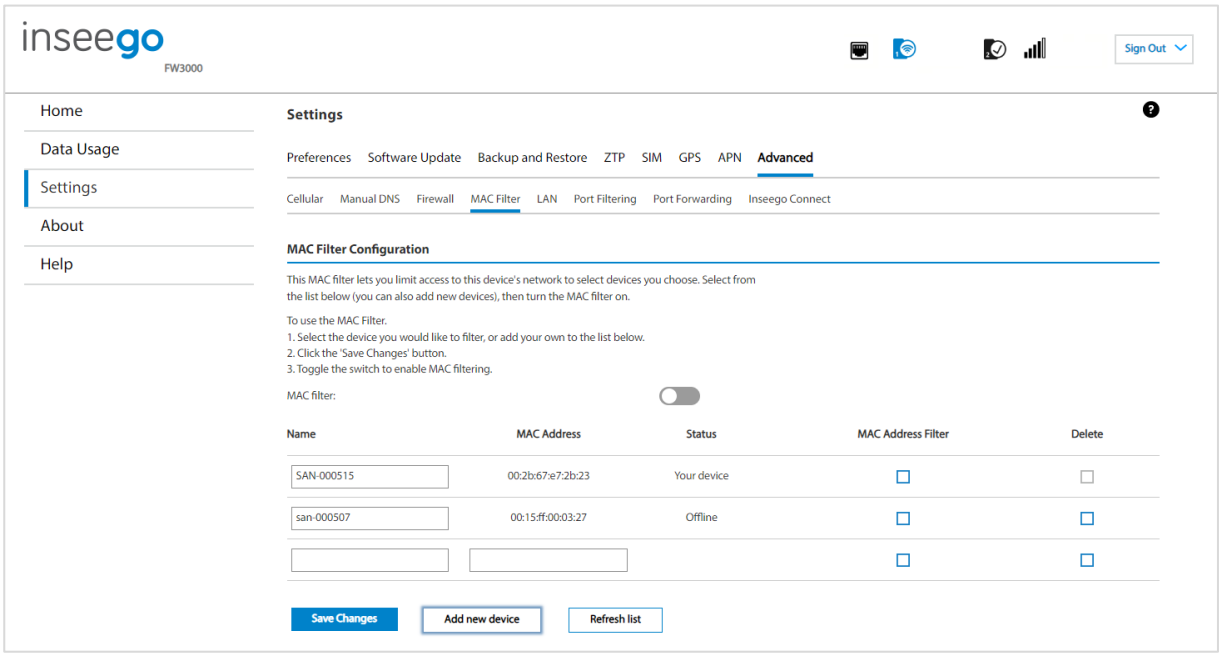
Destination IP address: Enter the IP address of the connected device you wish to become the DMZ device (the DMZ destination).

Click **Save Changes**.

MAC Filter tab

The MAC filter allows only selected devices to access the FW3000 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 Configuration

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.

This list includes all devices currently connected to the FW3000.

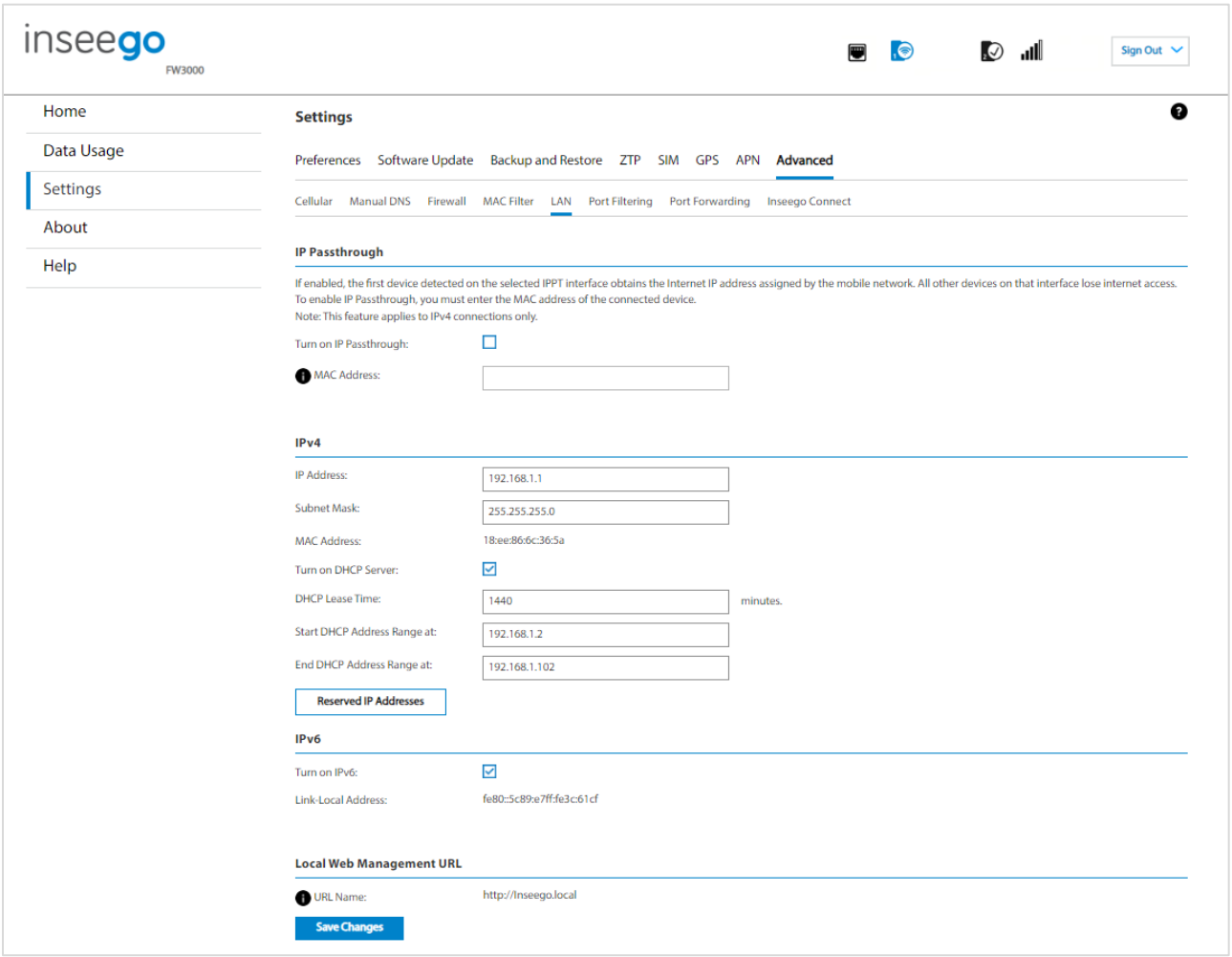
Add new device: Use this button to add a device to the device list, then enter the device name, MAC address, and choose whether to select the **MAC Address Filter** checkbox.

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**.

LAN tab

This page provides settings and information about the FW3000 local area network (LAN). The LAN consists of the device and all connected devices.



IP Passthrough

IP Passthrough (IPPT) enables the first device detected on the specified LAN port to obtain the IP address assigned by the mobile network. IPPT allows you to enable a one-to-one connection to a host routing system. **NOTE:** When IP Passthrough is on, the following capabilities are set through the host routing system and web UI settings are not available:

- DMZ (Firewall)
- Port Filtering
- Port Forwarding

Turn on IP Passthrough: Check the box to enable IP Passthrough**.**

MAC Address: Enter the MAC address of the device connected for IP Passthrough. This is the only device connected to the selected Ethernet port that can obtain the IP address assigned to the mobile network.

IPv4

NOTE: When IP Passthrough is turned on, you will not be able to configure IPv4.

IP Address: The IP address for your FW3000, as seen from the local network. Normally, you can use the default value.

Subnet Mask: The subnet mask network setting for the FW3000. The default value 255.255.255.0 is standard for small (class "C") networks. If you change the LAN IP Address, make sure to use the correct Subnet mask for the IP address range of the LAN IP address.

MAC Address: (read-only) The Media Access Controller (MAC) Address for the Wi-Fi interface on your FW3000. 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.

Reserved IP Addresses: Use this button to set up reserved IP addresses. Reserved IP addresses ensure that a connected device will always be allocated the same IP Address.

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.

Local Web Management URL

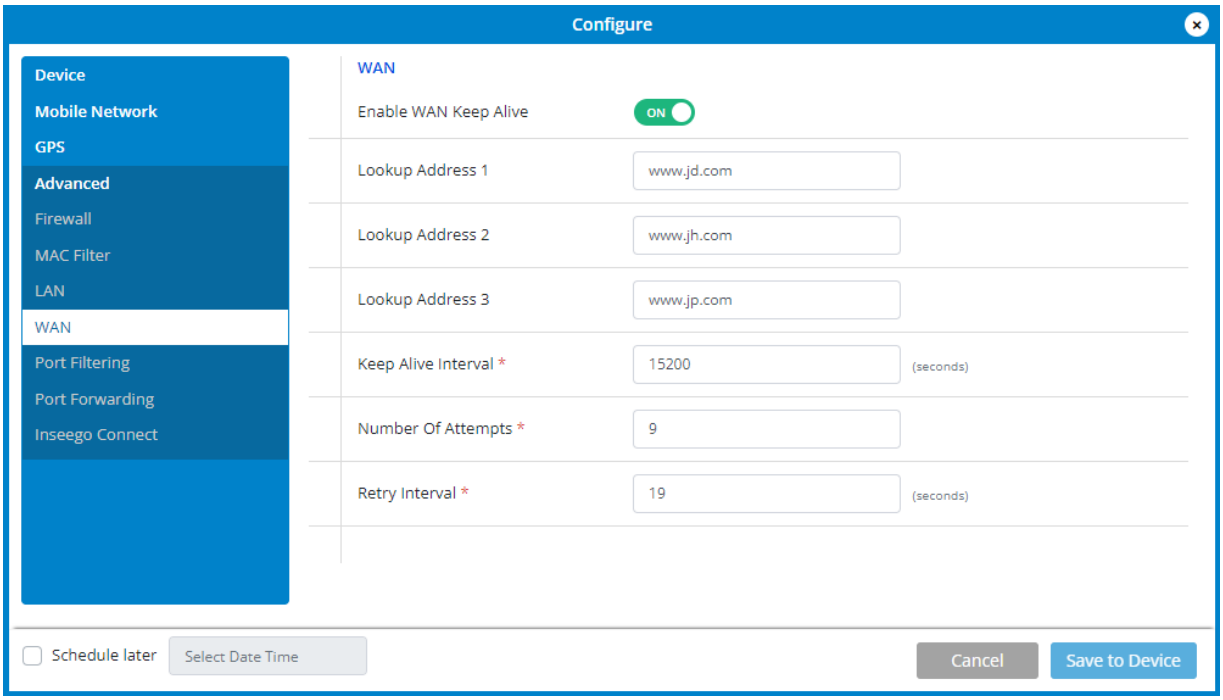
URL Name: The URL name used to access the FW3000 local web UI**.**

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

WAN settings

NOTE: WAN settings are available only with Inseego Connect.

Use this page to enable and configure WAN keep alive. Keep alive allows for a persistent WAN connection.



WAN

Enable WAN Keep Alive: If ON, keep alive verifies lookup addresses to check the Internet connectivity on the WAN connection.

Lookup Address 1: Enter the first IP address to verify the WAN connection.

Lookup Address 2: Enter the second IP address to verify (if Lookup Address 1 does not respond with keep alive acknowledgement (ACK)).

Lookup Address 3: Enter the third IP address to verify (if Lookup Address 2 does not respond with keep alive ACK).

Keep Alive Interval: Enter the desired number of seconds without receiving a valid packet before the first keep alive verification occurs.

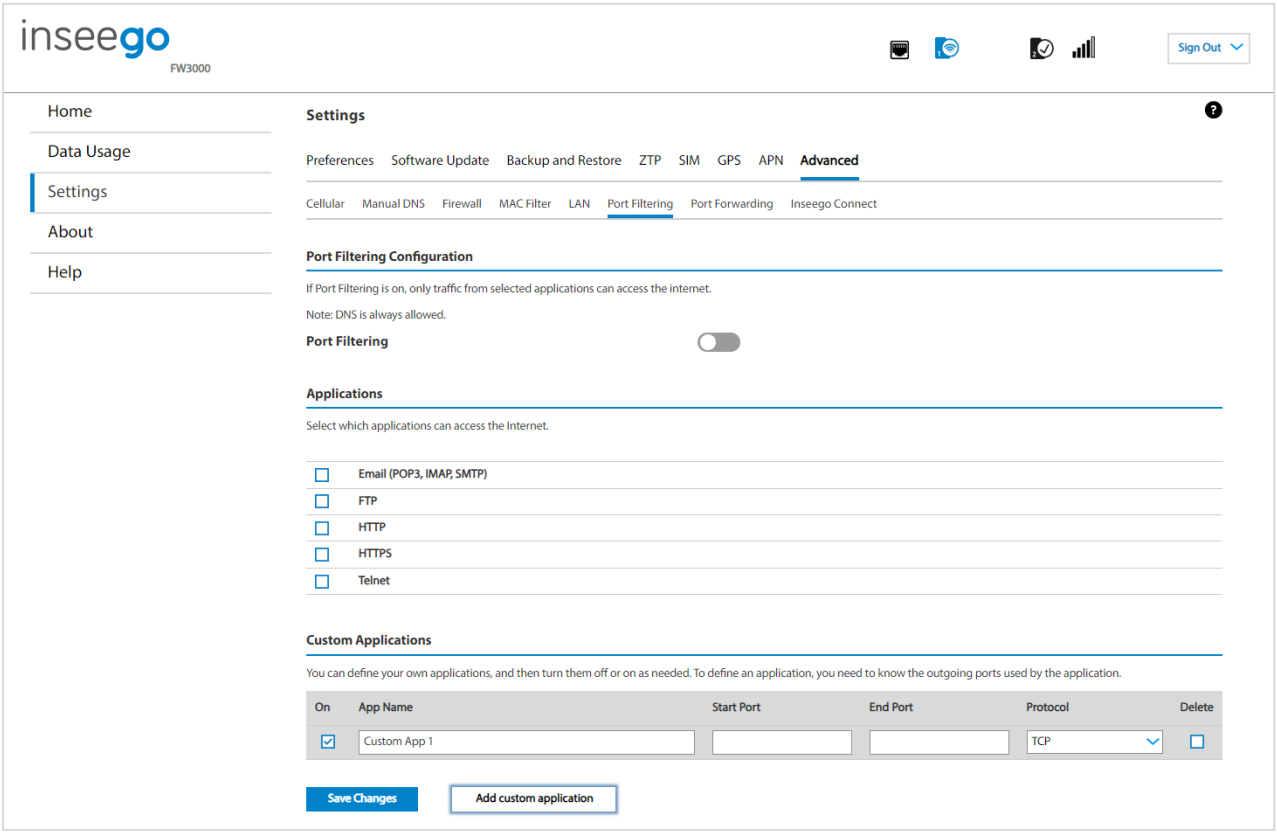
Number of Attempts: Enter the number of times to retry after verification failure for all three lookup addresses.

Retry Interval: Enter the number of seconds between verification retries.

Click **Save to Device** to save new settings.

Port Filtering tab

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



NOTE: When IP Passthrough is turned on, port filtering capabilities are set through the connected host routing system. Settings on this page are not available. Go to **Advanced** > **LAN** to turn IP Passthrough off.

Port Filtering Configuration

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

Use the **Add custom application** button to add a new row to the custom application list.

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

App Name: Enter a name for the custom application.

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

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

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.

* **Yes** indicates the protocol is standardized for the port number.
No indicates the protocol is not 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.

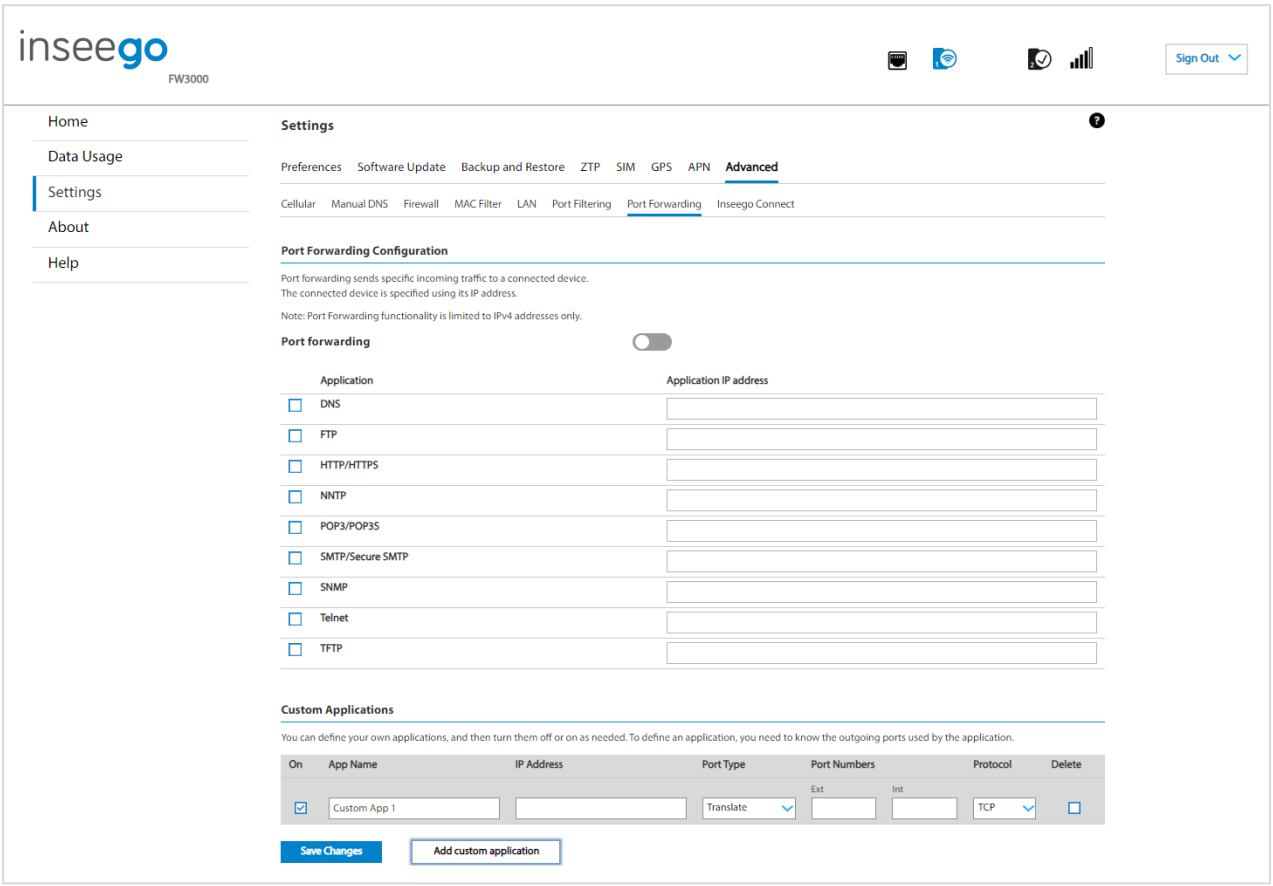
Port Forwarding tab

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.

NOTE: To configure Port Forwarding, you need a static IP address assigned to your line of service. Contact your service provider to set up a line of service for static IP.

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.



NOTE: When IP Passthrough is turned on, port forwarding capabilities are set through the connected host routing system. Settings on this page are not available. Go to **Advanced > LAN** to turn IP Passthrough off.

Port Forwarding Configuration

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) **FTP data transfer**	21 20	Yes Yes	Yes Yes	Assigned Assigned
HTTP **HTTPS**	80 443	Yes Yes	Yes Yes	Assigned Assigned
NNTP	119	Yes	No	Assigned
POP3 **POP3S**	110 995	Yes Yes	No No	Assigned Yes
SMTP **SecureSMTP**	25 465	Yes Yes	No No	Assigned 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 not 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

Use the **Add custom application** button to add a new row to the custom application list. 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.

IP Address: If you want to limit service for the application to a single connected device, enter the IP address of the target device. To find the IP address of a device, go to the Connected Devices page. **NOTE:** To ensure the device you are forwarding to does not have a different IP address after a reboot, either statically assign the IP address on the client device or set up a DHCP reservation.

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

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

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

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

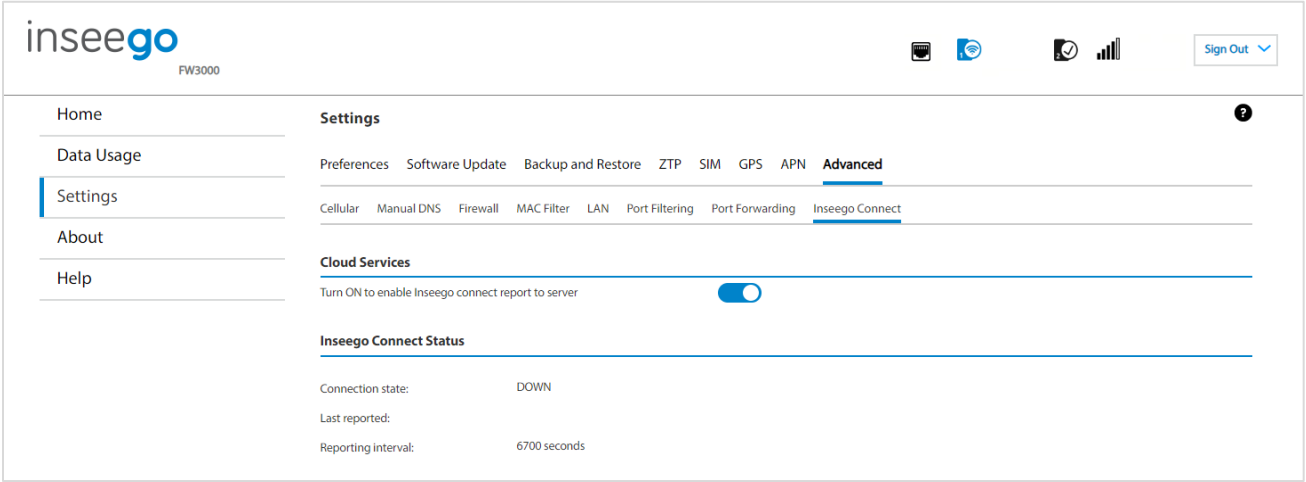
Delete: Check this box to delete a custom application. **NOTE:** Click on the Port Forwarding tab again to remove deleted custom applications from view on the screen.

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

Inseego Connect tab

Inseego Connect is a multi-tiered device management platform that allows you to deploy, monitor, and manage Inseego IoT devices remotely from the cloud. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free Inseego Connect account at connect.inseego.

IMPORTANT: After adding a device to Inseego Connect, restart the device immediately. This allows the device to check in and process the registration request.



Cloud Services

By default, the connection to Inseego Connect is **ON**. Slide the ON/OFF slider to **OFF** if you wish to disable the connection.

Inseego Connect Status

Connection state: The status of the Inseego Connect connection.

- **UP** – FW3000 is communicating with Inseego Connect servers.
- **DOWN** – FW3000 is NOT communicating with Inseego Connect servers.

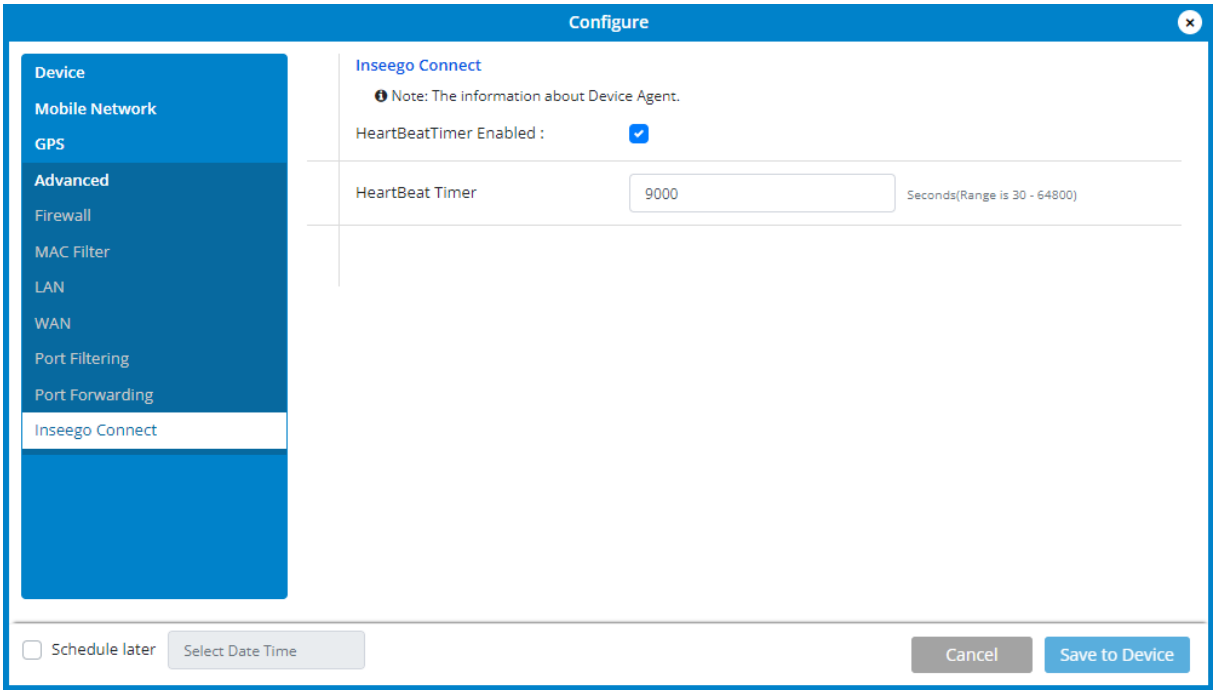
Last reported: The time when FW3000 last sent a packet to Inseego Connect servers.

Reporting interval: This is the interval at which your FW3000 will send packets to the Inseego Connect server. **NOTE:** A shorter interval means more data usage.

Heartbeat timer (Inseego Connect)

Your FW3000 sends a lightweight heartbeat packet to Inseego connect at a regular interval to indicate that the device is online. The default interval is 1680 seconds (28 minutes).

You can adjust the frequency of the heartbeat timer in Inseego Connect on the Inseego Connect configuration screen. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free Inseego Connect account at connect.inseego.



HeartBeatTimer Enabled: By default, the heartbeat time is enabled and your FW3000 sends a heartbeat packet to Inseego Connect. Slide the ON/OFF slider to **OFF** if you wish to disable this feature.

HeartBeat Timer: Select the number of seconds desired for the heartbeat timer interval.

Click **Save to Device**.

4

Troubleshooting and support

Overview

Troubleshooting

Technical support

Overview

When properly installed, the FW3000 is a highly reliable product.

The following tips can help solve many common problems encountered while using the FW3000:

- Make sure you are using the FW3000 in the correct geographic region.
- Ensure that your wireless coverage extends to your location.
- Ensure that you have an active subscription plan.
- You can resolve many issues by restarting your connected device and your FW3000.

Troubleshooting

This section can help solve many common problems and answer questions encountered while using the FW3000.

Will I always get 5G? Can I use the FW3000 outside of 5G coverage?

While this router is marketed as a 5G indoor router, it supports both 5G and 4G and connects to the strongest signal available.

Check your service provider's coverage map to see what type of signal you can expect.

The FW3000 LED is switching from blue to green and sometimes dropping service

- **Reason:** In rare cases when the device is near the edge of 5G coverage and frequently switching from 4G to 5G coverage, it may temporarily drop service.

  Solution: If this is an ongoing issue, go to **Settings** > **Advanced** > **Cellular** and change **Network Technology** to **4G LTE**.

Indicator LED is blue or green/SIM appears active, but I cannot browse the internet

- **Reason:** When there is a SIM or APN issue, some service providers let you connect and provide an IP address, but you are not able to browse the internet.

  Solution: Contact your service provider to check the status of the SIM and troubleshoot any APN issues.

Can I set my FW3000 to use a specific band?

No, the FW3000 is designed to connect to the strongest signal available. You can set the network technology and 5G network mode using **Settings** > **Advanced** > **Cellular**.

I cannot access the Admin web UI

- **Reason:** It is not possible to connect to the web UI through a router.

  Solution: Your computer must be directly connected by Ethernet cable to the Data In port on the FW3000 PoE power injector.

- **Reason:** You need a valid connection to access the web UI using http://192.168.1.1.

  Solution: If you are unable to connect to http://192.168.1.1, use http://Inseego.local*, or http://fw3000.com*.

My FW3000 is "Waiting for Connection" on the Inseego Mobile app

- **Reason:** The registration request is still being processed.

  Solution: Restart the device. This allows the device to check in and process the registration request.

- **Reason:** You entered an incorrect password for the device or changed the Admin password before Inseego Connect fully processed the registration request.

  - **Solution:** From the Inseego Mobile app or Inseego Connect, delete the device from the Device List and add it again using the current Admin password. If you have already logged into the device's Admin web UI and changed the Admin password, use the new password. If you have not changed the Admin password, the default is "Fast5G!".

    Restart the device. This allows the device to check in and process the registration request.

My FW3000 is getting slow speeds/low throughput

- **Reason:** Signal strength and quality are the most likely cause of slow speeds/low throughput. **NOTE:** The FW3000 is configured by default to use the best connection available, so low throughput is rarely related to configuration.

  Solution: Check the signal strength and quality reported by your FW3000:

  1. Access the FW3000 Admin web UI and navigate to **About > Diagnostics** to check the values for **Signal Strength (RSRP)** and **SNR.**
  2. **If the signal is good, but throughput is slow**, check your service provider's network conditions for outages and expected performance.

* The Inseego.local and fw3000.com web UI addresses rely on having IPv6 enabled on your connecting device.

My connecting device is not obtaining a valid IP address

There are several possible reasons your connecting device is not obtaining a valid IP address:

- **Reason:** IPPT is enabled, and you have switched the device connected to your FW3000 without restarting.
  When IP Passthrough (IPPT) is enabled, only the first device detected can obtain the IP address assigned by the mobile network.

  Solution: When IPPT is enabled, any time you switch the device you are connecting to the FW3000, you must first disconnect the existing connected device and power cycle the FW3000 before connecting the new device.

- **Reason:** The DHCP server has been turned off.
  If IPPT is not enabled, the DHCP server provides IP addresses. If the DHCP server is turned off, no IP addresses can be provided.

  Solutions:
  Reset your FW3000 to factory settings, see “Resetting your FW3000” on page 11.
  or
  Use Inseego Mobile app LAN settings to turn the DHCP server on.

- **Reason:** The DHCP server has used all its IP addresses.
  This is unlikely to happen with the FW3000, but if you have connected a succession of devices to your FW3000 in a short period of time, you may have used up all the IP addresses available.

  Solution: Disconnect your connected device and power cycle the FW3000 before reconnecting the device.

- **Reason:** There is an issue with your FW3000.

  Solution: Contact your service provider for assistance.

I cannot get streaming platforms to work with my FW3000

- **Reason:** Some service provider plans include content filtering that prevents streaming over the internet connection.

  Solution: Contact your service provider for assistance.

Technical support

IMPORTANT: Before reaching out for support, be sure to restart both your connected device and your FW3000 and ensure that your SIM card is inserted correctly.

Customer service and troubleshooting

Contact your service provider or reseller for assistance.

More information

Documentation for your FW3000 is available online. Go to go.inseego.com/fw3000. Or, from the Admin website, select **Help > Support**.

5

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

Product specifications

Device

Name:	FW3000
Model:	FW3000
Regulatory:	FCC(US)
Certifications:	GCF Prop 65
Dimensions:	11.8" x 7.87" x 2.36"(300 mm x 200 mm x 60 mm)
Weight:	5.60 lbs (2540 g)
Ports:	(1) 2.5Gbps Ethernet LAN port
SIM:	Dual SIM, (2) 4FF Nano SIM slots
Chipset:	Qualcomm® Snapdragon™ SDX65
LED:	(1) Power and status LED
Power:	Power over Ethernet (PoE):
Power class:	PC1.5 n77 PC2 on B41, n41 PC3 on all other bands
Web UI OS support:	Windows 10 and later MacOS 10.14 and later Linux® Ubuntu 18.04 LTS and later
SRS antenna switching:	n41/n77
Accessories:	PoE injector (included) SIM tool (included) Mounting options (optional) J-Arm mount Wall mount Pole mount

Environmental

Operating temperature:	-30°C to 70°C (-22°F to 158°F)
IP67 rating for water and dust ingress protection	
Internal heating element for startup and operation in cold environments	
NOTE: The PoE injector is an indoor device and considered support equipment. It can operate at a maximum temperature of 35°C (95°F).	

Network connectivity*

NSA, SA, and DSS supported
5G sub-6 GHz
4G LTE Cat 22
4x4 MIMO sub-6 GHz
4x4 MIMO LTE

Security

Security hardened web interface
Password hash
Session timeout
Incorrect password lockout
Anti CSRF

* Data plan required. Coverage subject to network availability.

Regulatory information

Federal Communications Commission Notice (FCC – United States)

FCC ID: PKRISGFW3000

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.

FCC RF EXPOSURE GUIDANCE STATEMENT: This device complies with FCC Radio Frequency Radiation Exposure Limits set forth for Uncontrolled Environment. To ensure compliance with the FCC Radio Frequency Exposure Guidelines, this device must be installed to provide at least 28.5 cm separation from the human body at all times.

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 FW3000 device, or failure of the FW3000 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 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 FW3000 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.