USER GUIDE

inseego

Inseego Wavemaker™ PRO
5G Outdoor CPE FW2000e

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 Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp.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: 14945406 Rev 1

Contents

Introduction and Getting Started 5
Overview 6
Key Features 6
System Requirements 6
Getting Started 7
Configuration 8
Overview 9
Home Page 10
Side Menu 10
Header Icons 11
Getting Help 11
Admin Password 12
Changing the Admin Password 12
Managing Data Usage 13
Data Usage Page 14
Managing Settings 16
Preferences Tab 16
Software Update Tab 17
Backup and Restore Tab 18
SIM Tab 20
Advanced Tab 23
Viewing Info About the FW2000e 39
Internet Status Tab 40
Internet Sessions Tab 41
Diagnostics Tab 42
Device Info Tab 43
GPS Tab 44
Logs Tab 45
Getting Support 46
Customer Support Page 46
Troubleshooting and Support 47
Overview 48
Replacing your SIM Card 48
Indicator LED 50
Resetting your Device 51
Resetting with the RESET Button 51
Resetting from the Inseego Mobile App 52
Resetting from the Admin Web UI 52
Resetting from Inseego Connect 52
Technical Support 52
Product Specifications and Regulatory Information 53
Product Specifications 54
Device 54
Environmental 54
Network Connectivity 55
Security 55
Regulatory Information 56
Product Certifications and Supplier's Declarations of Conformity 59
Energy Efficiency 59
Wireless Communications 59
Limited Warranty and Liability 61

Safety Hazards 62
Glossary 63
Glossary 64

1

Introduction and Getting Started

Overview

Getting Started

Overview

The Inseego Wavemaker PRO 5G Outdoor CPE FW2000e is the next-gen CPE solution that brings wireless 5G data speeds to urban, suburban, and rural customers alike. The FW2000e delivers high-speed data over both 5G and 4G LTE networks using a proprietary high-gain antenna array. The FW2000e connects to the best cellular network and provides data connectivity to the existing in-building network.

Your FW2000e is installed by professional technicians to assure optimal performance.

Key Features

- Sophisticated antenna array delivers up to 14dbi gain to achieve longer range and higher all-around data throughput at all distances*.
- Designed to operate in extreme temperatures from -30°C to 70°C (-22 to 158°F) and has an environmental rating of IP67 for water and dust ingress.
- Enterprise-grade device security, encryption, content filtering, and more. Plus, enterprise customers can subscribe to Inseego Secure™ for an additional layer of end-to-end security features, threat identification, monitoring and alerts
- Remote management with the Inseego Connect™ platform enables remote device management, diagnostics, performance monitoring, alerts, and much more.
- Inseego Mobile App, available on Apple and GooglePlay App stores, guides installers to find the best location for performance, and enables consumers to manage device settings with their smartphone.
- Support for up to two carrier SIMs and auto switching between carriers. Multi-carrier firmware allows the FW2000e to be used on most major global carriers.

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

* Data plan required. Coverage and speeds subject to network availability.

Getting Started

To turn on your FW2000e and connect a device:

1. Check that the PoE cable from the FW2000e 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.

WARNING! Use only the PoE power injector supplied with the FW2000e. 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.

2

Configuration

Overview

Admin Password

Managing Data Usage

Managing Settings

Viewing Info About the FW2000e

Getting Support

Overview

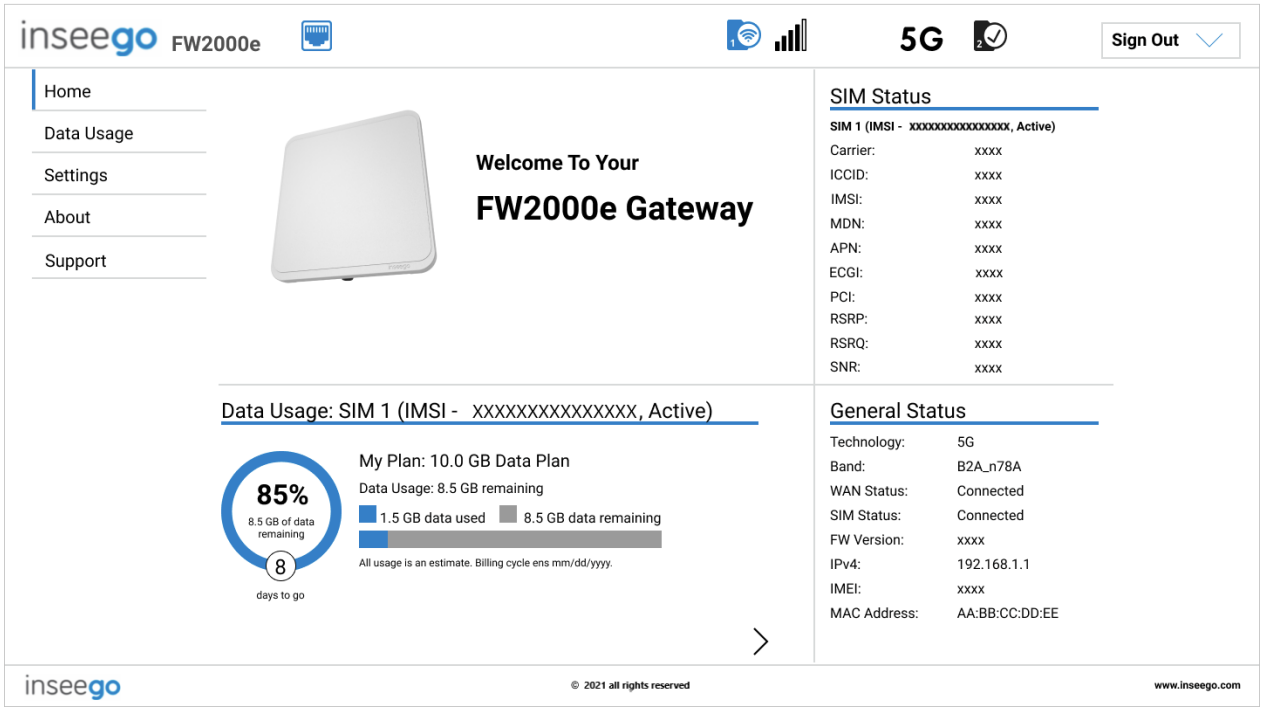
You can use multiple tools to configure and troubleshoot your FW2000e:

- **Admin Web UI** – Provides a local gateway to configure and manage your FW2000e. On a device connected to your FW2000e, 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** (see Admin Password on page 12).
- **Inseego Connect** – Enables you to monitor and configure an entire deployment of devices. You can group devices together to push widespread configurations, troubleshoot individual devices, set alarms, and run reports. Go to **connect.inseego.com** to sign up for a free Inseego Connect account.
- **Inseego Mobile App** – Allows you to perform basic device monitoring and management. Scan the QR code to install the Inseego Mobile App from AppStore or Google Play, or visit https://inseego.com/inseego-connect-get-app to download the App.

This chapter provides the configuration options available for your FW2000e devices. The configurations shown are from the Admin Web UI, unless otherwise noted. Many options are also available with Inseego Mobile App and Inseego Connect. Some configurations are available only with Inseego Connect, and are marked as such.

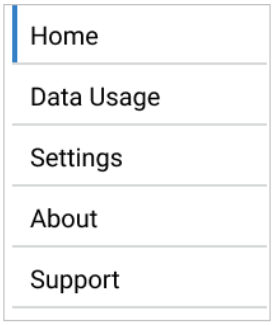
Home Page

The Home page of the Admin Web UI is the local gateway to configuring and managing your FW2000e. It displays data usage and general status information.



Side Menu

The Home page and each subscreen in the FW2000e Admin Web UI 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. A similar side menu is available when configuring devices with Inseego Connect.



Header Icons

The top of each FW2000e Admin 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
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 an Admin Web UI page to go to the Customer Support page where you can access this User Guide and other information for the FW2000e.

Admin Password

The Admin password is what you use to sign into the FW2000e 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:

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 enter a new password and confirm it.

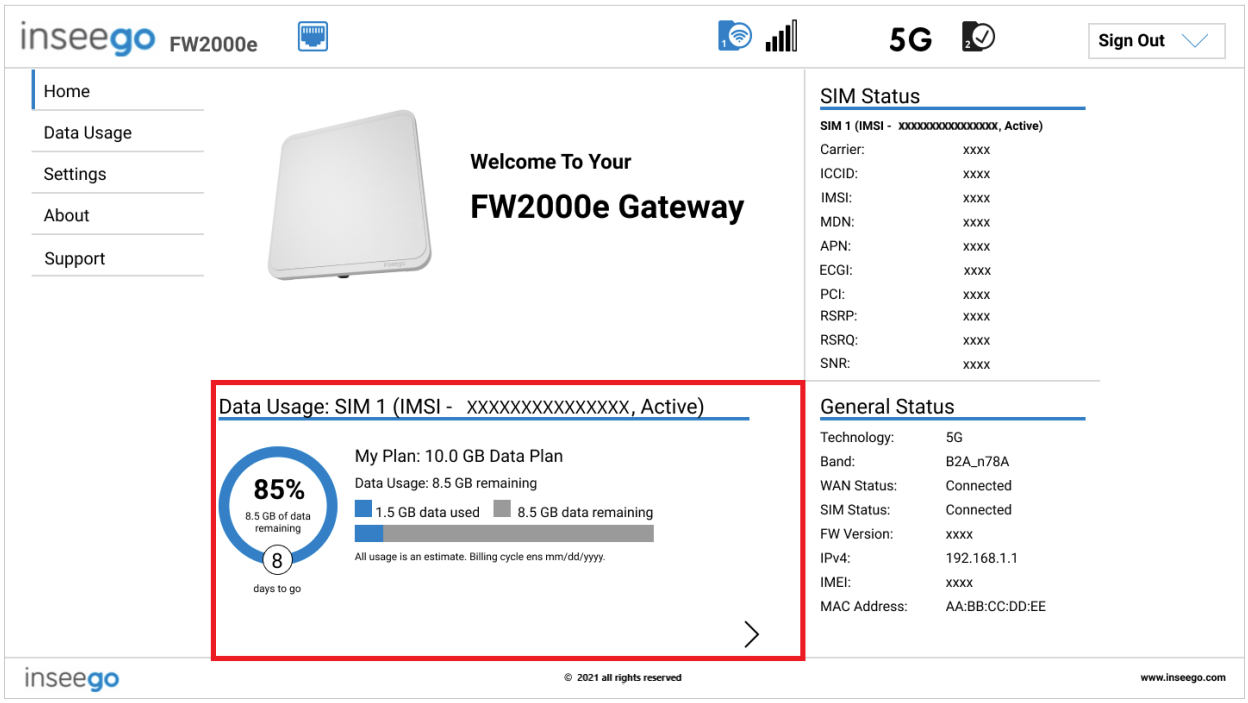
3. Select a security question from the drop-down list and type an answer to question in the **Answer** field. **NOTE:** Answers are case-sensitive.

4. Click **Save Changes**.

The next time you sign in to the FW2000e Admin Web UI, 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

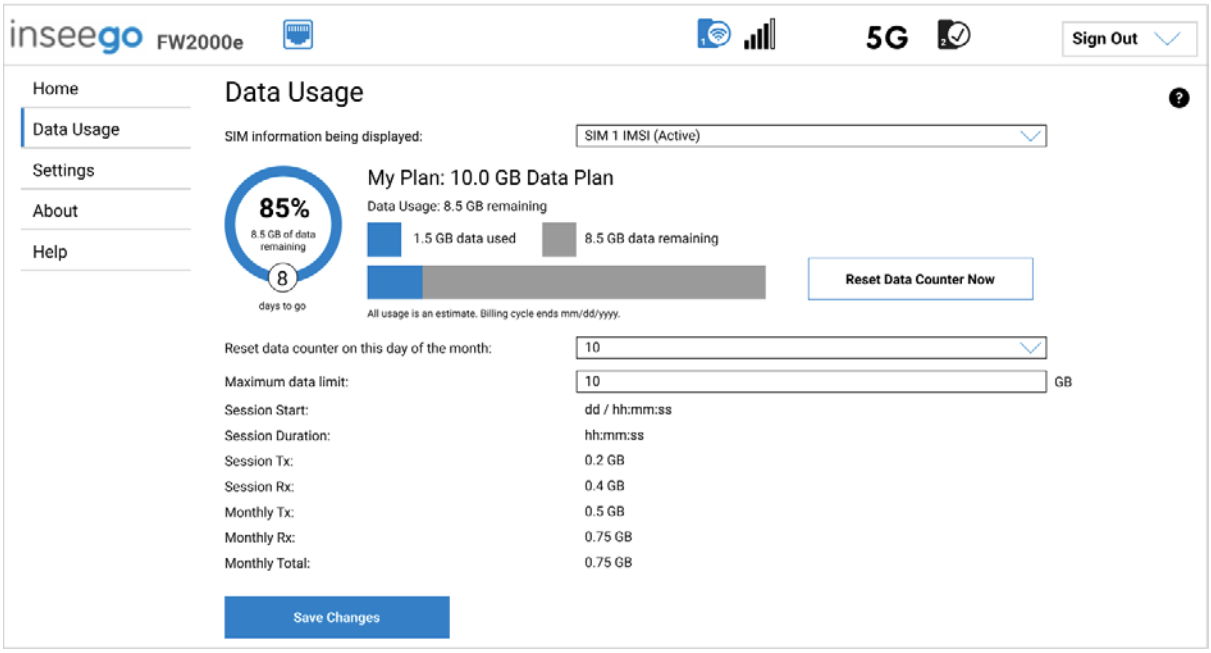
On the Admin Web UI Home page, the Data Usage panel displays graphs of your FW2000e data usage for the current billing cycle.



To view the Data Usage page, 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 about your FW2000e 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.

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

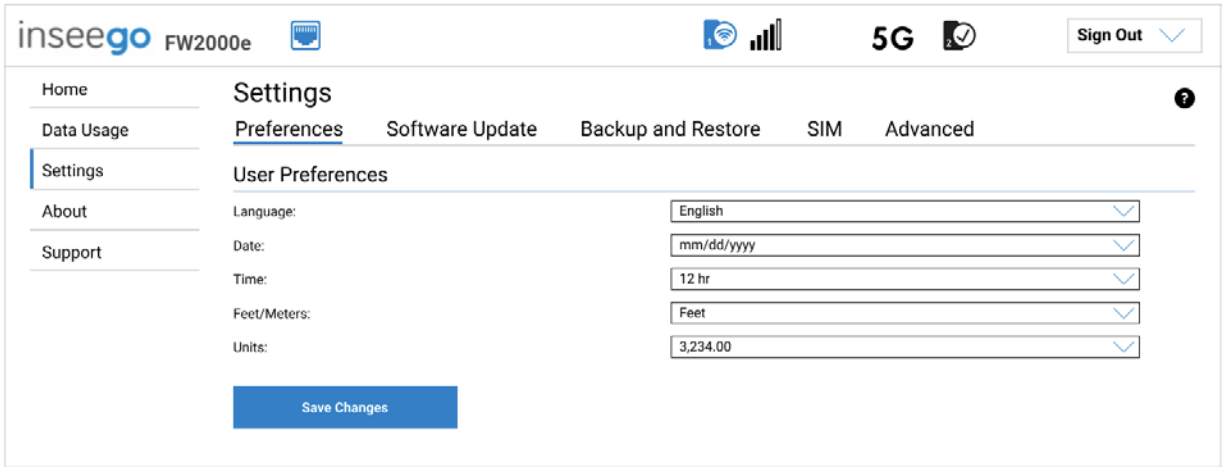
You can view and configure system settings for your FW2000e. To change system settings, select **Settings** from the side menu.

The Settings page includes four tabs:

- Preferences
- Software Update
- Backup and Restore
- Advanced

Preferences Tab

This tab allows you to change how dates, time, and numbers are displayed in the FW2000e Admin Web UI. **NOTE:** These preferences 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.



User Preferences

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).

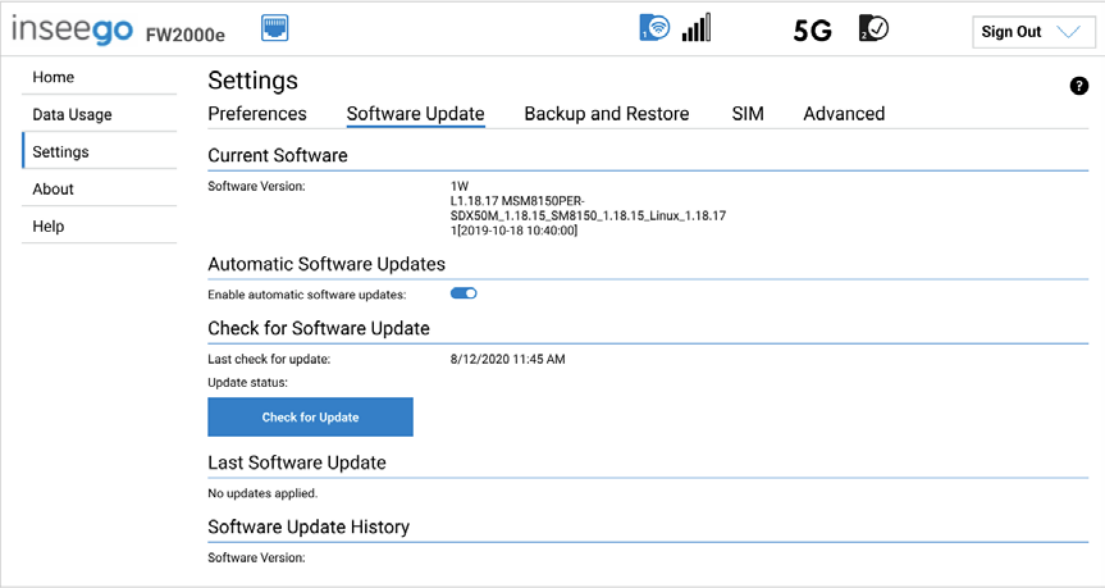
Feet/Meters: Select the distance format to be used for the Web UI when marking GPS altitude and accuracy (Feet or Meters).

Units: 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 FW2000e 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.



Current Software

Software Version: The version of the software currently installed on your FW2000e.

Automatic Software Update

By default, software updates are automatically delivered to your FW2000e. This setting allows you to turn off automatic software updates. If you do not want software updates automatically delivered, move the **ON/OFF** slider to **OFF**.

Check for Software Update

Last check for update: The date and time the FW2000e last checked to see if an update was available.

Update status: This is 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

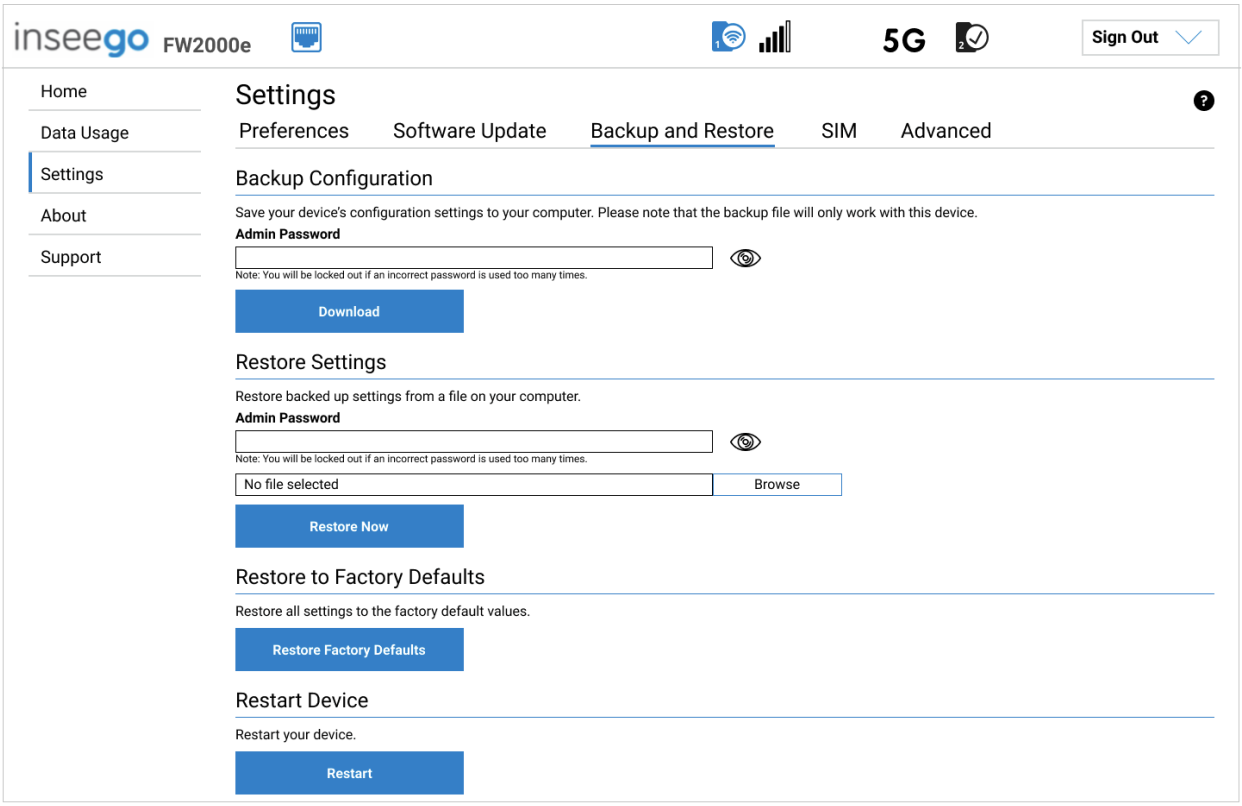
This section displays details about the last software update.

Software Update History

This section 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 FW2000e settings to a file on your computer, restore (upload) a previously-saved configuration file, reset the device to factory defaults, or restart the device.



Backup Configuration

To back up current FW2000e settings to a file on your computer, enter your Admin password in the **Admin Password** field.

The default Admin password is **Fast5G!** and should have been changed upon first login. If you don't remember your Admin password, 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 Admin Web UI. To unlock it, restart your FW2000e by disconnecting the PoE cable from the PoE Injector **Data & Power Out** port for 10 seconds and reconnecting it.

Click the **Download** button. The file is automatically downloaded to your Downloads folder. This configuration file contains all settings for your FW2000e.

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 FW2000e, and settings can only be viewed or changed using the Admin 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, 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 FW2000e.

Click the **Restore Now** button.

Restore to Factory Defaults

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

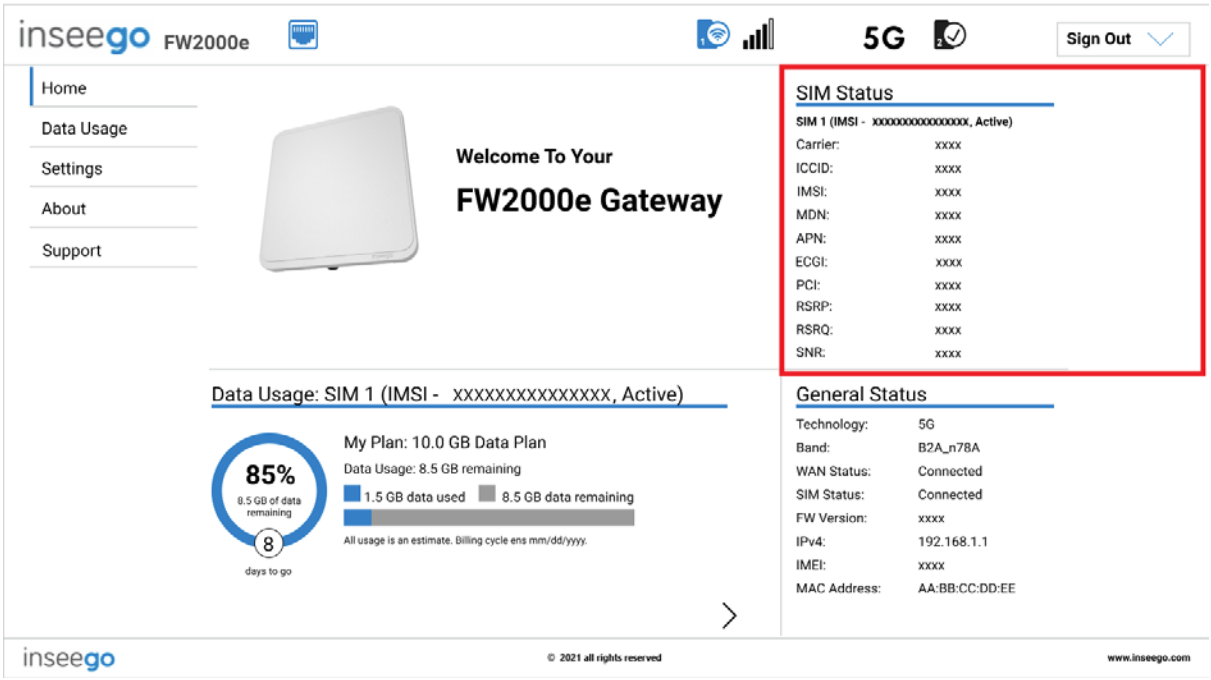
CAUTION! This resets all settings to their factory default values, including the Admin password.

Restart Device

Restart: This button turns your FW2000e off and on again.

SIM Tab

On the Admin 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 FW2000e. This is a unique number, usually fifteen digits, that identifies a Global System for Mobile Communications (GSM) subscriber.

MDN: The phone number of your FW2000e.

APN: The access point name for your FW2000e.

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

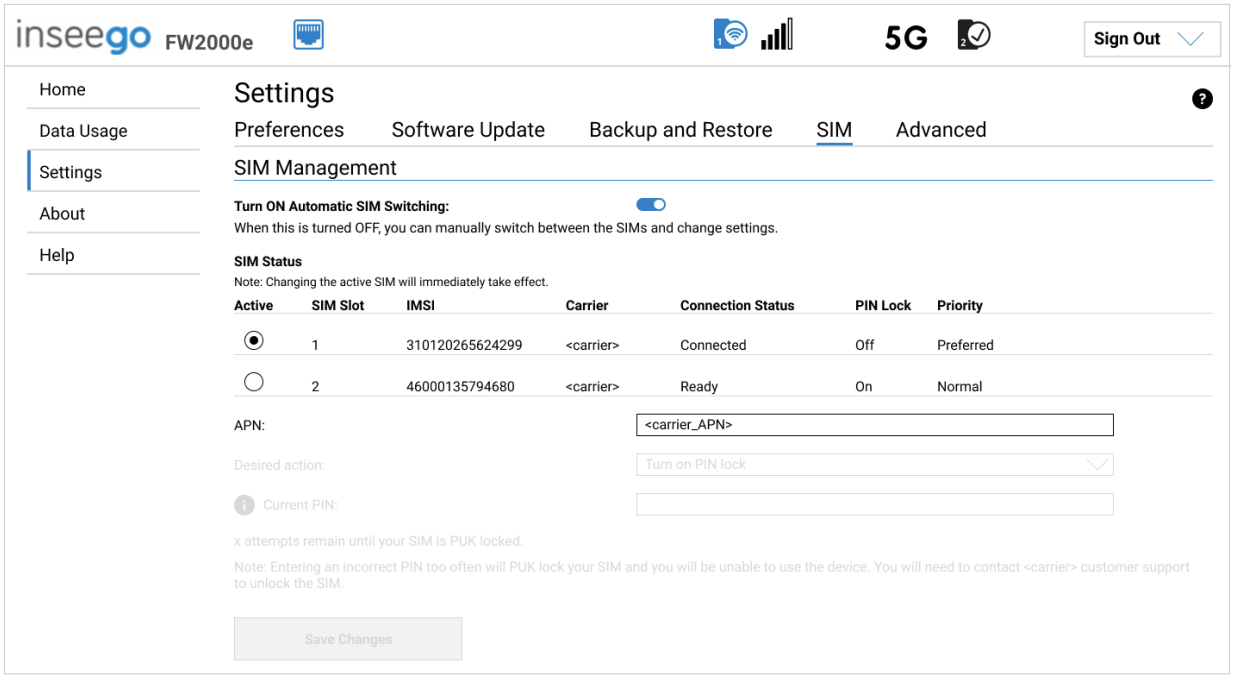
PCI: The Physical Cell ID.

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. A ratio of signal power to noise power expressed in decibels. SNR is a positive value, and higher numbers are better.

To turn on automatic SIM switching or enter a SIM PIN, select **Settings** from the side menu. Then select **SIM**.



NOTE: The SIM card in your FW2000e 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 FW2000e. 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**.

Advanced Tab

Advanced settings 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 FW2000e.

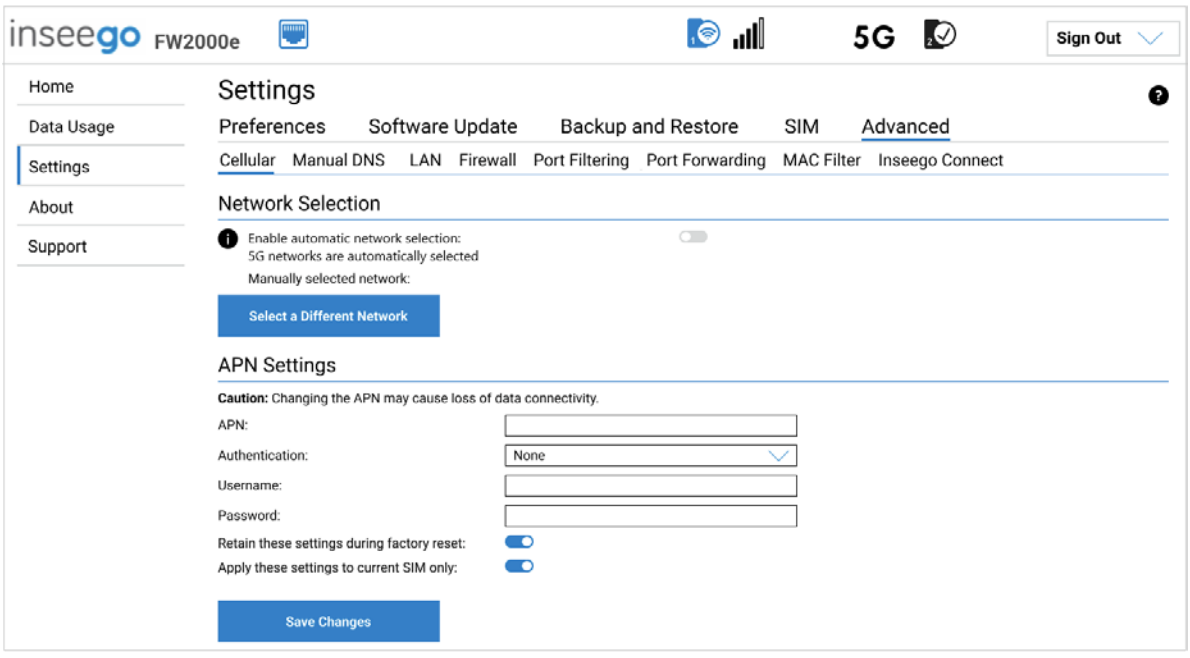
When you select the **Advanced** tab on the Settings page, a warning message appears. If you click **Continue**, the Cellular tab of the Advanced Settings page appears.

Advanced Settings include:

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

Cellular Sub Tab

In most configurations, the FW2000e 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 FW2000e.



Network Selection

Enable automatic network selection: When the **ON/OFF** slider is **ON**, your FW2000e automatically selects the best 5G available network and you cannot use the **Select a Different Network** button below.

Select a Different Network: 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.

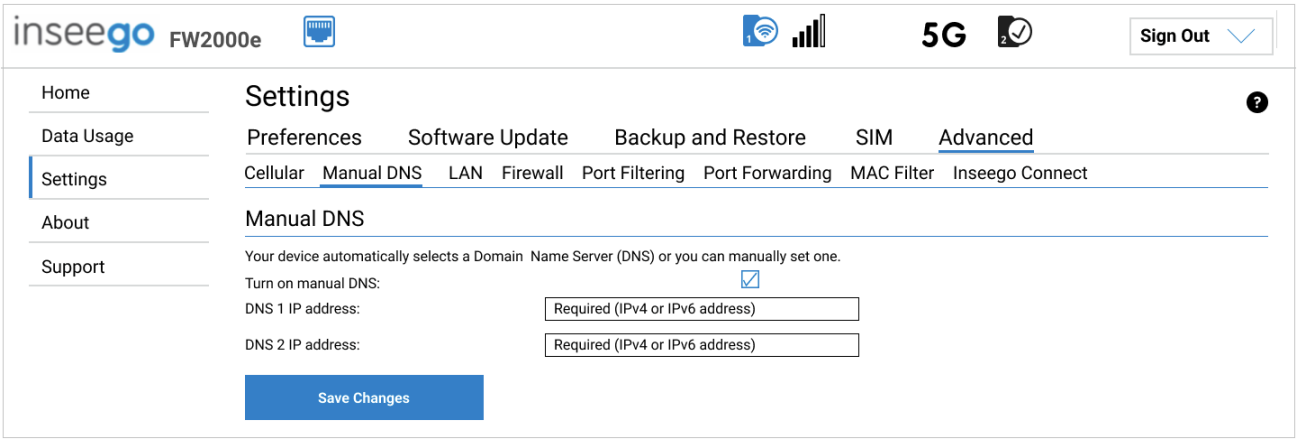
Retain these settings during factory reset: When the **ON/OFF** slider is **ON**, your FW2000e will keep these APN settings after a factory reset.

Apply these settings to current SIM only: When the **ON/OFF** slider is **ON**, your FW2000e will only apply these APN settings to the current SIM.

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

Manual DNS Sub Tab

The FW2000e 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.

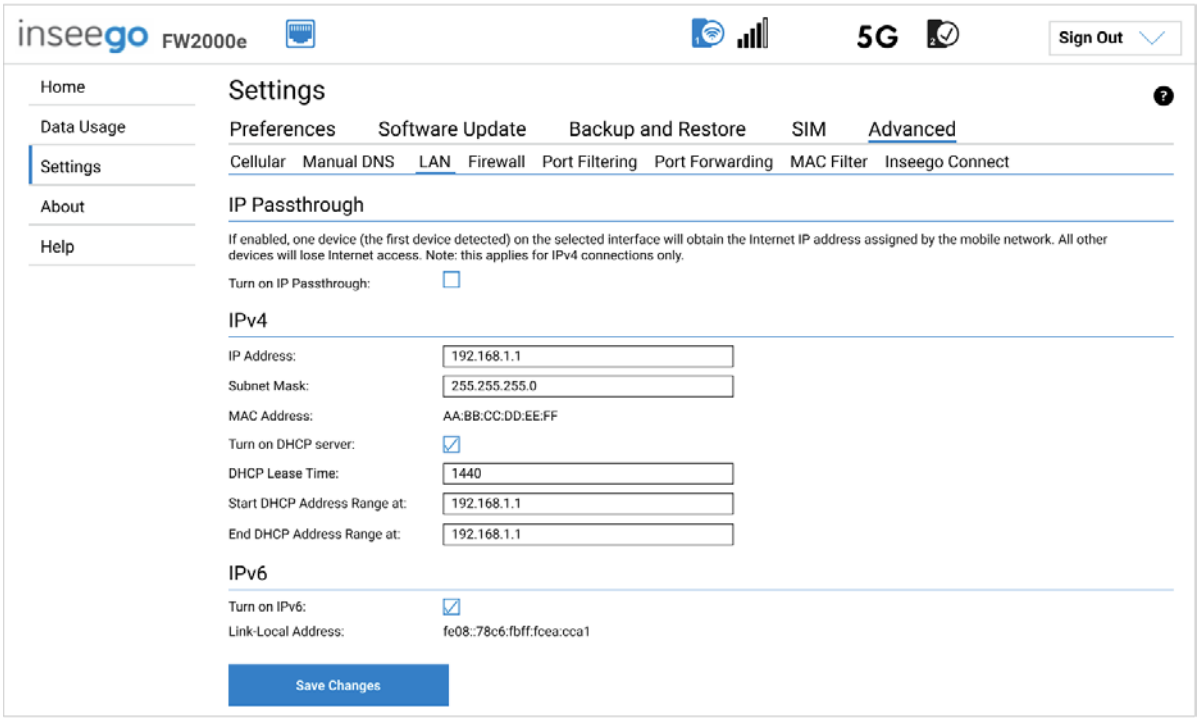
DNS 1 IP address: Enter the IP address for the primary DNS. This address is required to use the Manual DNS feature.

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**.

LAN Sub Tab

This page provides settings and information about the FW2000e's 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 IP Passthrough is turned on, all other devices will lose Internet access. In addition, you will not be able to make changes to the Firewall, Port Filtering, or Port Forwarding settings.

IPv4

IP Address: The IP address for your FW2000e, as seen from the local network. Normally, you can use the default value.

Subnet Mask: The subnet mask network setting for the FW2000e. 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 FW2000e. 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.

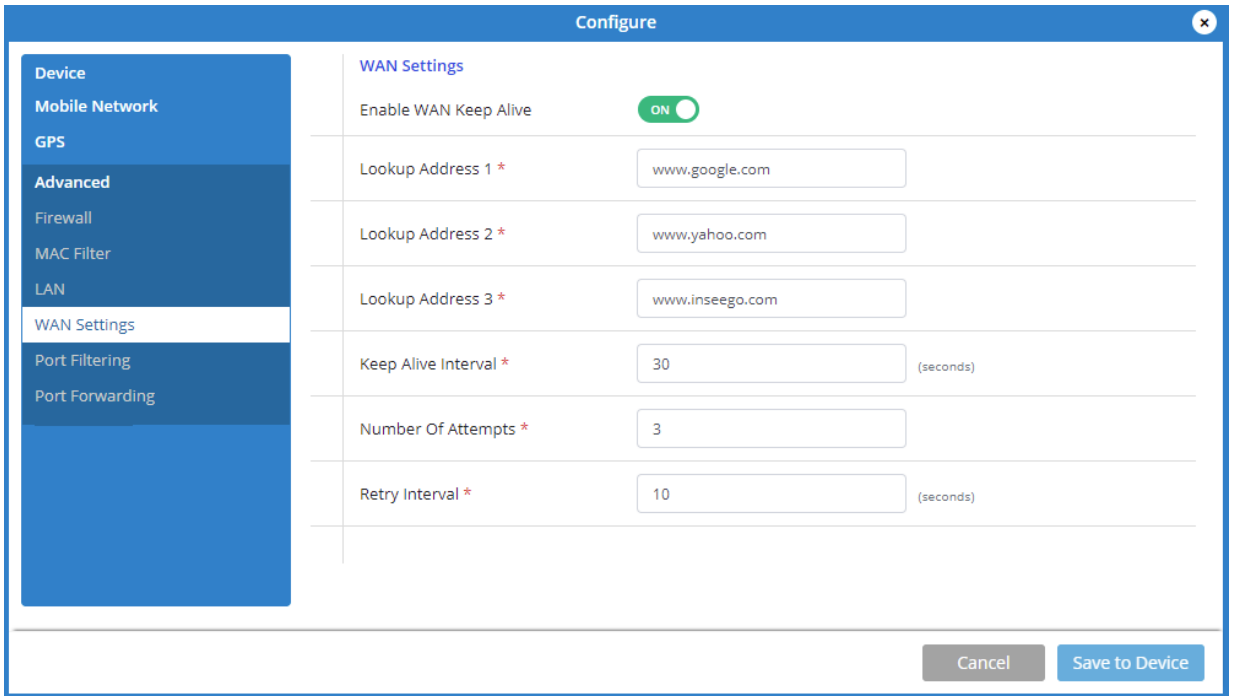
Link-Local Address: The Link-Local IPv6 address if the connected device supports IPv6.

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

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 Settings

Enable WAN Keep Alive: If ON, keep alive pings lookup addresses to verify cellular connectivity.

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

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

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

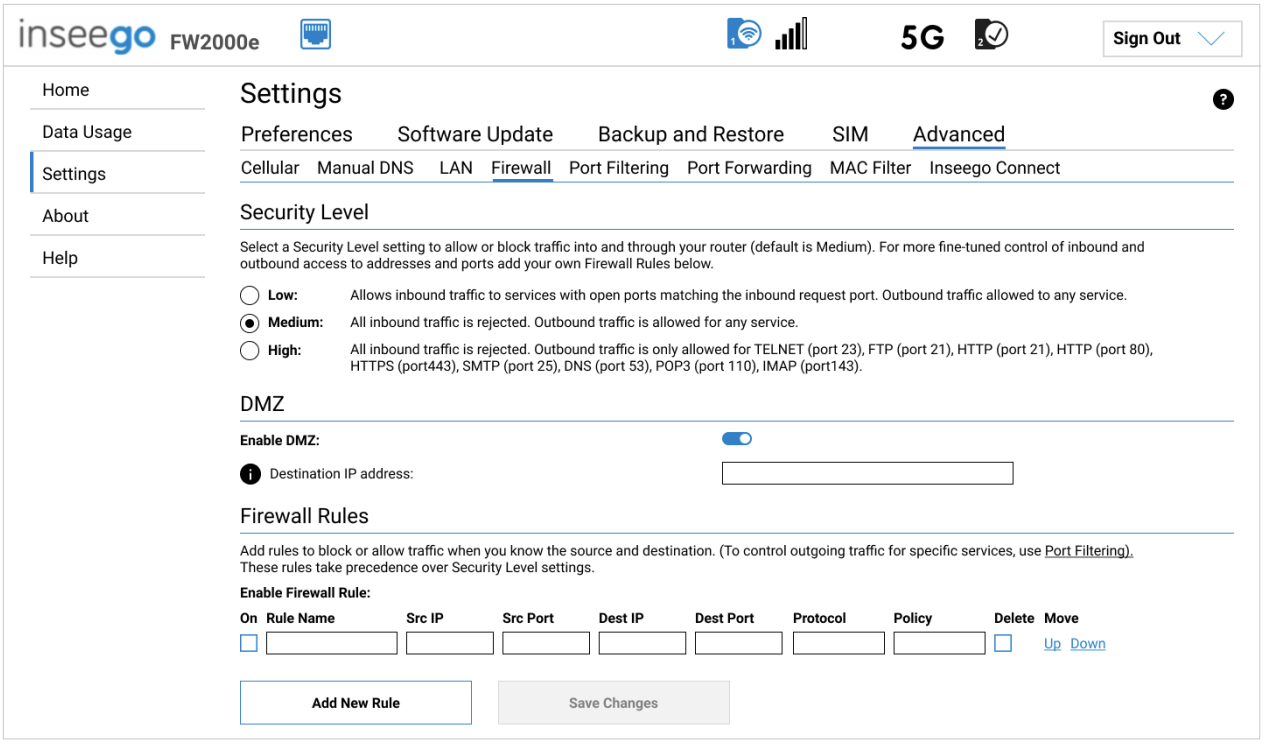
Keep Alive Interval: Enter the desired number of seconds without receiving a valid packet before the first keep alive ping is sent.

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

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

Firewall Sub Tab

The FW2000e firewall determines which Internet traffic is allowed to pass between the CPE 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.



NOTE: When IP Passthrough is turned on, you will not be able to make changes to the Firewall settings. Go to **Advanced > LAN** and turn IP Passthrough off.

Security Level

You can select from three general security levels to block traffic into and through the FW2000. The default Security Level is Medium.

- **Low** — allows inbound traffic to services with open ports matching the inbound request port. Outbound traffic is allowed for any service.
- **Medium** — Rejects inbound traffic. Outbound traffic is allowed for any service.
- **High** — Rejects inbound traffic. Outbound traffic is allowed only for TELNET (port 23), FTP (port 21), HTTP (port 21), HTTP (port 80), HTTPS (port 443), SMTP (port 25), DNS (port 53), POP3 (port 110), and IMAP (port 143).

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.

Enable DMZ: Check this box to allow DMZ.

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

Firewall Rules

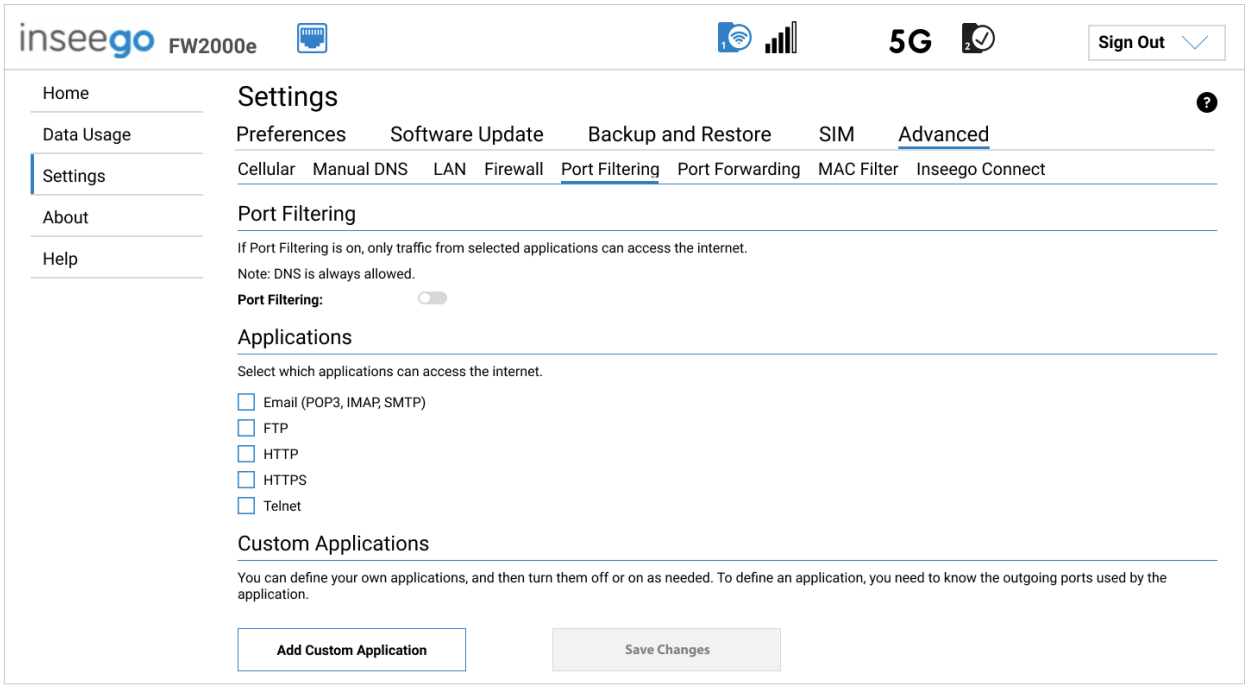
You can define one or more specific rules for the firewall to follow. Use the fields to set up a rule, and click **Add New Rule**. New rules are added to the bottom of the list. Use **Up** and **Down** to reposition rules on the list.

NOTE: For **Src. IP** and **Dest. IP**, enter a specific IP address or the keyword **any**.

Click **Save Changes**.

Port Filtering Sub 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, you will not be able to make changes to the Port Filtering settings. Go to **Advanced > LAN** and turn IP Passthrough off.

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.

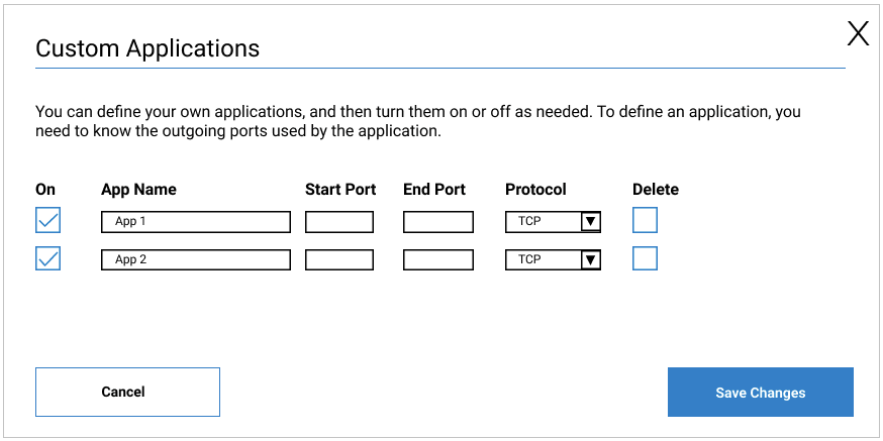
The following table provides port numbers and protocol information for each port filtering application listed.

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

* **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

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.
- **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.

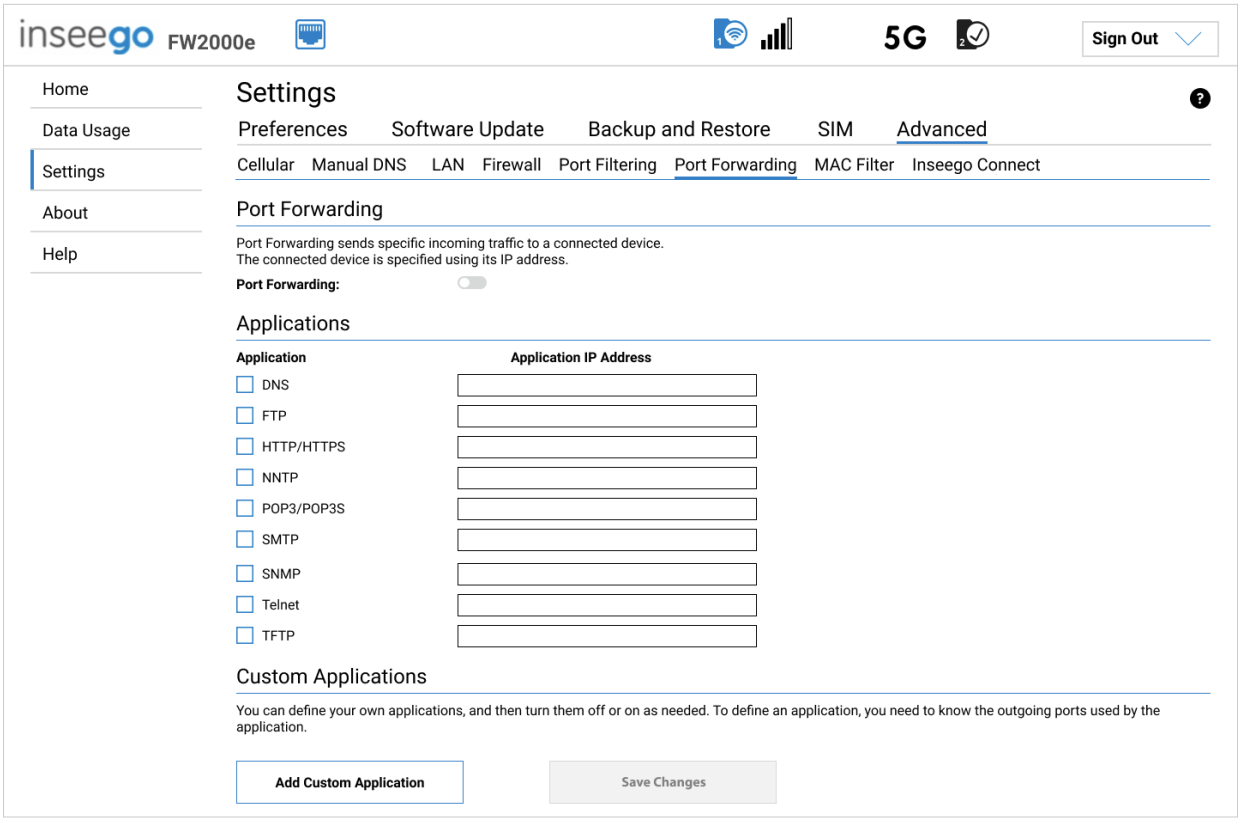
Click **Save Changes** to save any changes made to the custom applications.

Port Forwarding Sub 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.



NOTE: When IP Passthrough is turned on, you will not be able to make changes to the Port Forwarding settings. Go to **Advanced > LAN** and turn IP Passthrough off.

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.

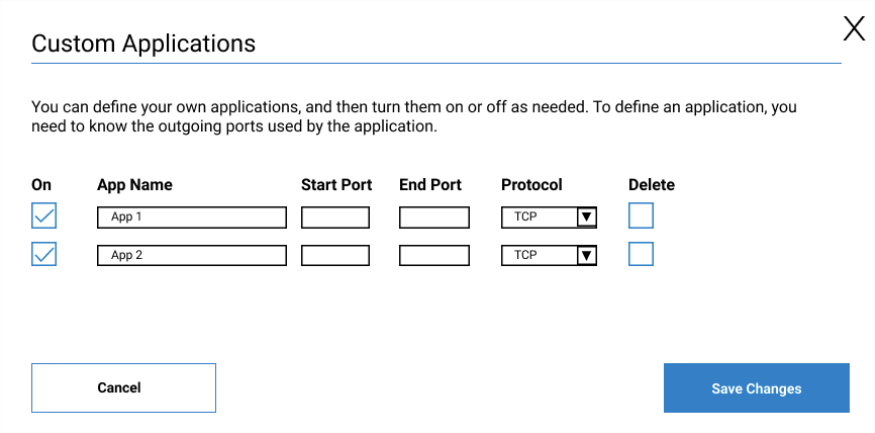
The following table provides port numbers and protocol information for each port forwarding application listed.

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**.**

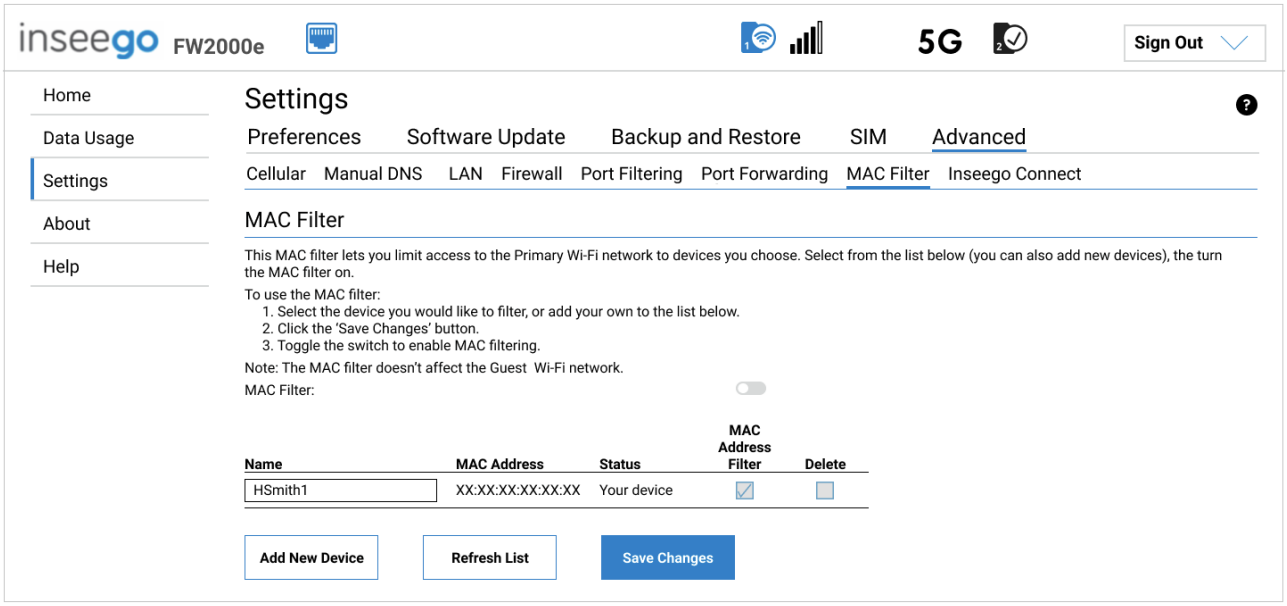
  NOTE: If the application uses a single port instead of a range, type the same value for both the **Start Port** and the **End Port**.
- **Protocol:** Select the protocol used by the port range from the drop-down list (TCP, UDP, or both).
- **Delete:** Check this box to delete a custom application. **NOTE:** 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.

MAC Filter Sub Tab

The MAC filter allows only selected devices to access the FW2000e 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 FW2000e.

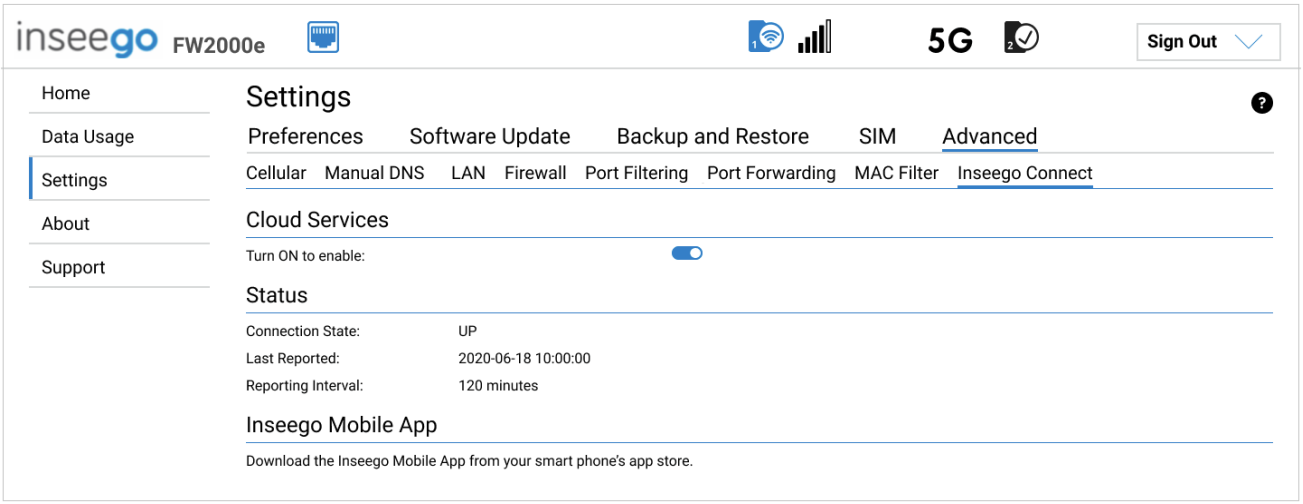
Add New Device: Use this button to add a device to the device list, then enter the device name, MAC address, choose whether to select the MAC Address Filter checkbox, and click **Save Changes**.

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**.

Inseego Connect Sub 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 **ON**. Slide the ON/OFF slider to **OFF** if you wish to disable the connection.

Status

Connection state: The status of the Inseego Connect connection.

- **UP** – FW2000e is communicating with Inseego Connect servers.
- **DOWN** – FW2000e is NOT communicating with Inseego Connect servers.

Last reported: The time when FW2000e last sent a packet to Inseego Connect servers.

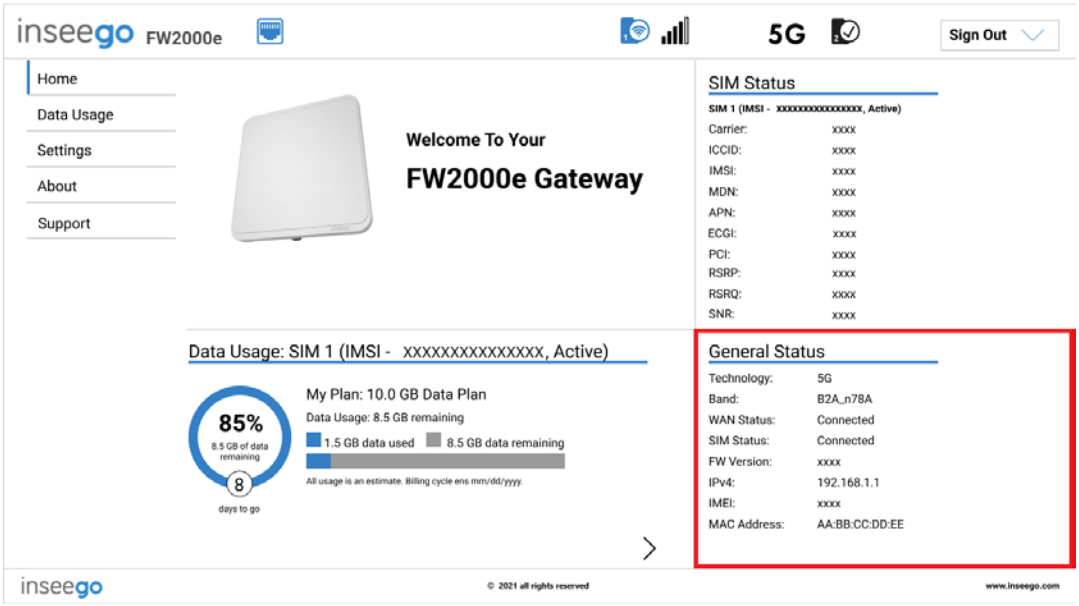
Reporting interval: This is the interval at which your FW2000e will send packets into the Inseego Connect server. **NOTE:** A shorter interval means more data usage.

Inseego Mobile App

You can download the Inseego Mobile App from your device's app store.

Viewing Info About the FW2000e

On the Admin Web UI Home page, the General Status panel shows general system information.



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 FW2000e.

IPv4: The network IP address assigned to your computer, not your FW2000e device.

IMEI: The International Mobile Equipment Identity (IMEI) for your FW2000e. 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 FW2000e. The MAC address is a unique network identifier assigned when a network device is manufactured.

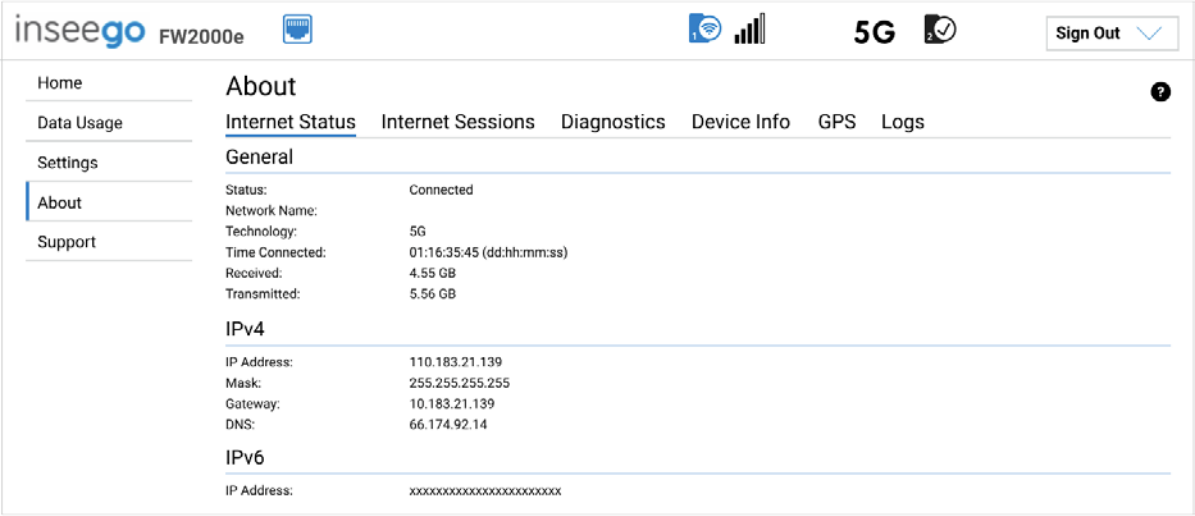
To view more information about your FW2000e and its use, select **About** from the side menu.

The About page includes the following tabs:

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

Internet Status Tab

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



General

Status: The current status of the FW2000e Internet 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

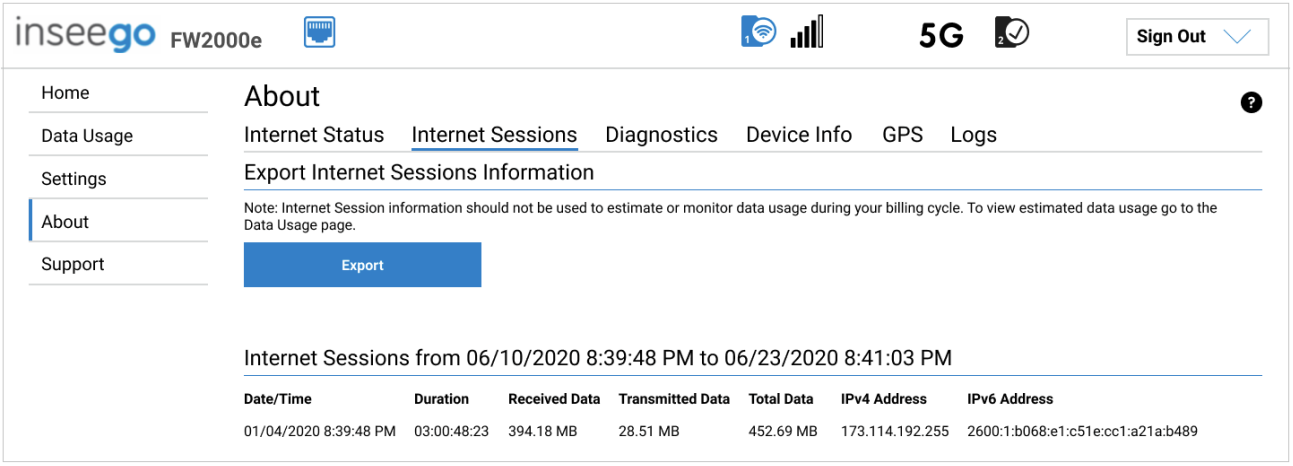
- **IP Address:** The Internet IP address assigned to the FW2000e.
- **Mask:** The network mask associated with the IPv4 address.
- **Gateway:** The gateway IP address associated with the IPv4 address.
- **DNS:** The Domain Name Server currently used by the FW2000e.

IPv6

- **IP Address:** The global IPv6 address for the FW2000e (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 display 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.

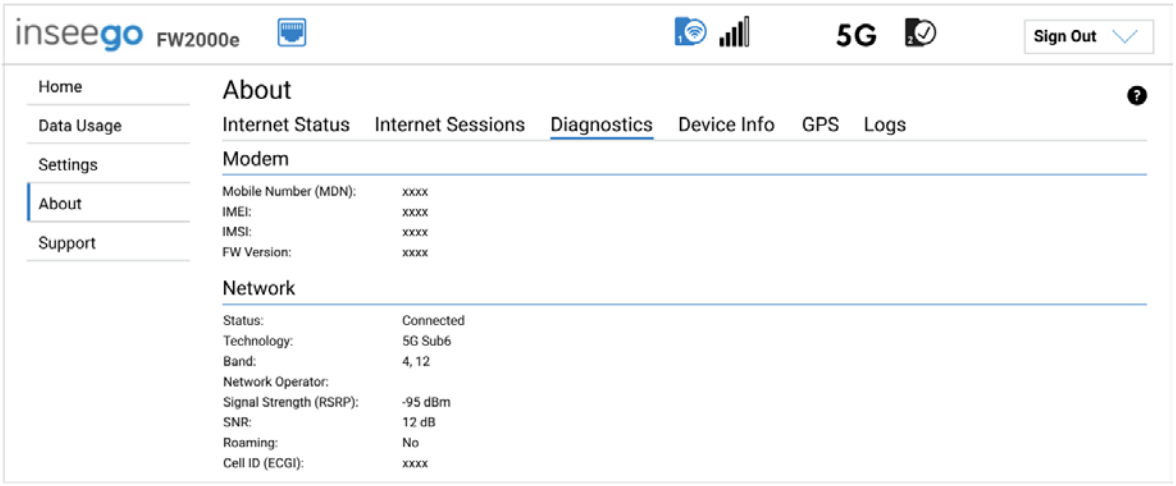
Total Data: The total amount of data for the Internet session. This is the sum of Received Data and Transmitted Data.

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 FW2000e.

IMEI: The International Mobile Equipment Identity (IMEI) for your FW2000e. 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 FW2000e. 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 FW2000e.

Network

Status: The status of the network.

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

Band: The band in use for the current connection.

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.

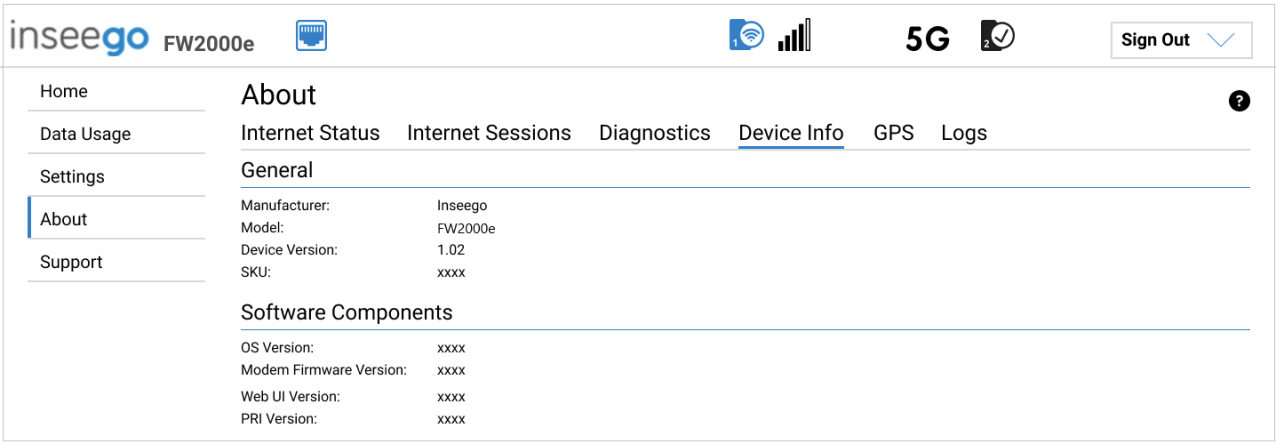
SNR: Signal to Noise Ratio. A ratio of signal power to noise power expressed in decibels. SNR is a positive value, and higher numbers are better.

Roaming: Indicates whether roaming is on.

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

Device Info Tab

Use this tab to view details about your internal WAN connection.



General

Manufacturer: Inseego.

Model: FW2000e.

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

SKU: The SKU for your FW2000e.

Software Components

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

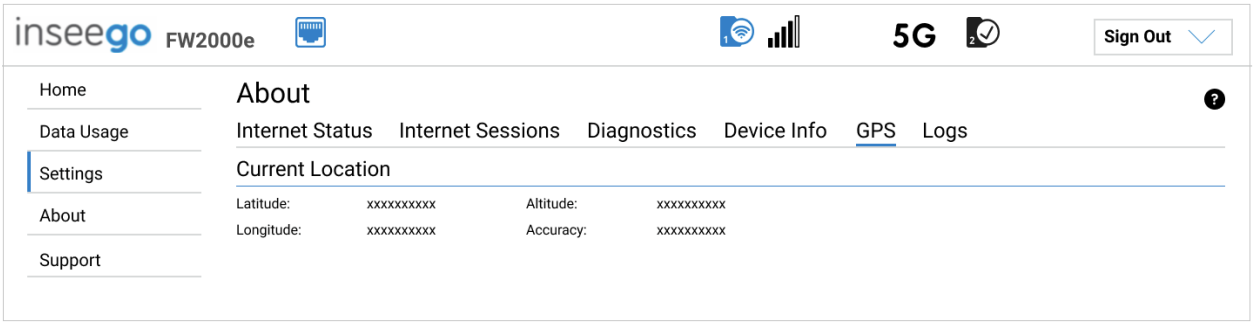
Modem Firmware Version: The version of firmware (software) currently installed for the modem component.

Web UI Version: The version number for the FW2000e Admin Web UI.

PRI Version: The configuration version currently applied to the FW2000e.

GPS Tab

The FW2000e incorporates a GPS receiver. The GPS receiver can determine your current location. Use this tab to view current location information.



Current Location

Latitude: Latitude for the last location fix.

Longitude: Longitude for the last location fix.

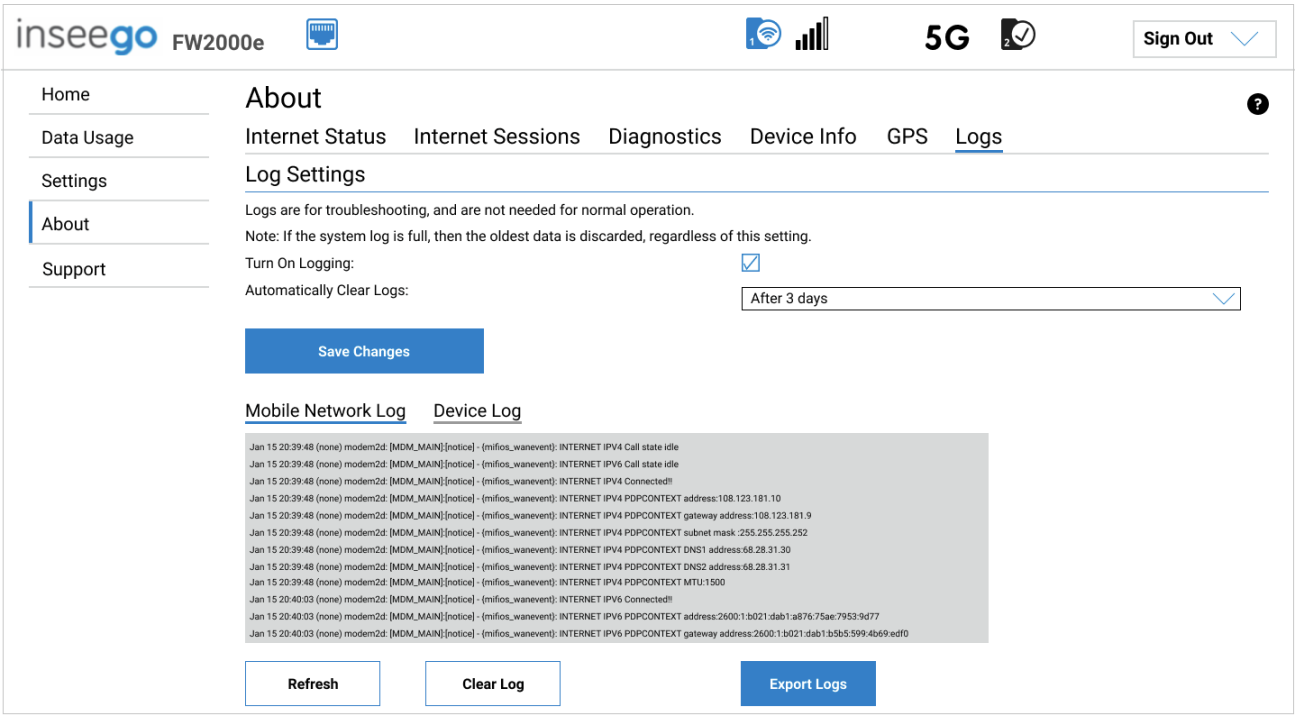
Altitude: Altitude for the last location fix.

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

NOTE: You can change the format of measurement (Feet or Meters) in **Settings > Preferences > User Preferences**.

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.

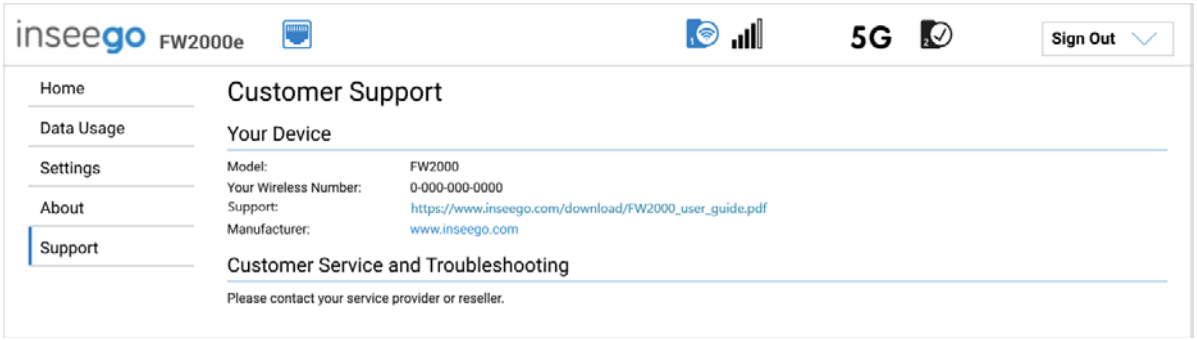
Export Logs: Allows you to export log data.

Getting Support

To view the Customer Support page, select **Support** from the side menu. The Customer Support page appears.

Customer Support Page

Use the Customer Support page to access documentation and support information for your FW2000e.



3

Troubleshooting and Support

Overview

Replacing your SIM Card

Indicator LED

Resetting your Device

Technical Support

Overview

This chapter provides troubleshooting and support information, including instructions on replacing a SIM card, information on the indicator LED, and how to reset your device.

Replacing your SIM Card

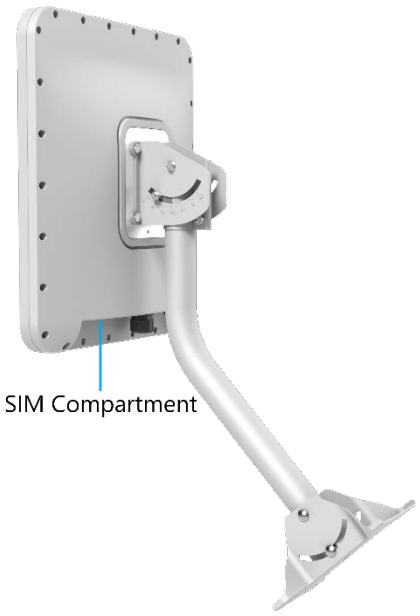
A SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. A SIM card is installed in your FW2000e during the technician installation process. These instructions are for replacing your SIM card.

The FW2000e supports only Nano SIM cards.

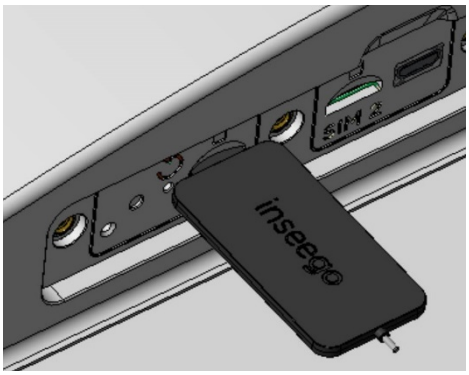
CAUTION! Always use a factory-made SIM card supplied by the service provider. Do not bend or scratch your SIM card. Avoid exposing your SIM card to static electricity, water, or dirt.

To replace the SIM card:

1. Disconnect the PoE cable to the FW2000e from the **Data & Power Out** port on the PoE power injector.
2. Unscrew the protective shield over the SIM slots using a Phillips-head screwdriver.



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

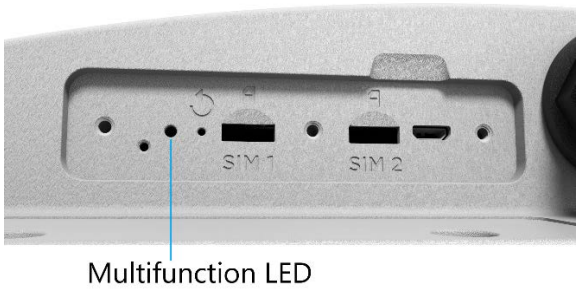


4. If necessary, remove the new SIM card from the protective sleeve, being careful not to touch the gold colored contacts.
5. Use the SIM end of the provided SIM tool to insert the SIM card into the appropriate SIM slot with the gold-colored contact points facing the front of the device.
6. Reattach the protective shield cover to a torque of 1.2Nm (0.885 ft/lb).
7. Insert the PoE cable to the FW2000e back into the **Data & Power Out** port on the PoE power injector.

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

Indicator LED

There is a multifunction LED located on the FW2000e device in the SIM compartment (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	CPE is booting up, acquiring signal No service, SIM error, or locked SIM card

Resetting your Device

You can reset your FW2000e to factory settings using the RESET button on the device or from the Mobile App, Admin Web UI, or Inseego Connect.

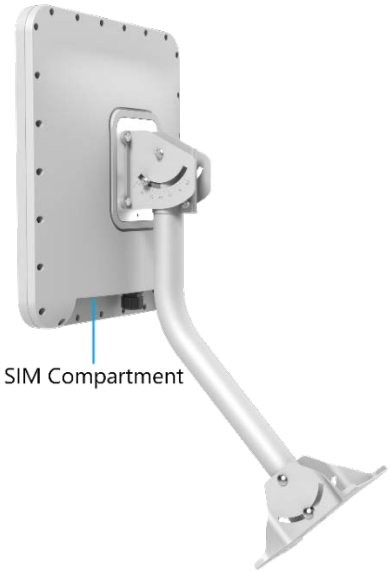
CAUTION! Resetting returns your FW2000e to factory settings, including the Admin password.

Resetting with the RESET Button

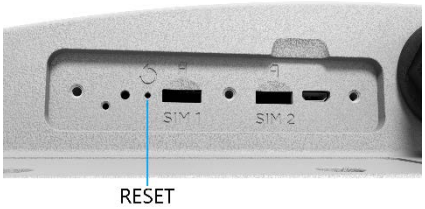
The master reset button is in a small hole located in the SIM compartment on the bottom of the FW2000e device. This button returns the device to factory settings, including resetting the Admin password.

To reset the FW2000e from the RESET button:

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



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



2. Press for five to six seconds, then your FW2000e will restart.
3. Check the indicator LED (see Indicator LED on the previous page) to make sure the FW2000e is working correctly.
4. Reattach the protective shield cover to a torque of 1.2Nm (0.885 ft/lb).

Resetting from the Inseego Mobile App

To reset the FW2000e from the Inseego Mobile App, select **Mobile Options**, then select **Factory Reset.**

Resetting from the Admin Web UI

To reset the FW2000e from the Admin Web UI, select **Settings > Backup and Restore** and select **Restore Factory Defaults**.

Resetting from Inseego Connect

To reset the FW2000e from Inseego Connect, on the Devices page, check the box next to the device and select **Factory Reset.**

Technical Support

IMPORTANT: Before contacting Support, be sure to restart both your computer and your FW2000e device.

Customer Service and Troubleshooting
Contact your reseller for assistance.

More Information
Documentation for your FW2000e is available online. Go to www.inseego.com/support-documentation. Or, from the Admin Web UI, select **Support**.

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

Product Specifications

Device

Name:	5G Outdoor CPE
Model:	FW2000
Standards/Approvals/Certifications:	FCC, GCF, PTCRB CE/ISED/MIC/RCM-ACMA* Bluetooth SIG
Device Testing:	WEEE, RoHS, REACH
Dimensions:	430mm x 400mm x 71.7mm (16.9" x 15.75" x 2.8")
Weight:	4.22 kg (9.3 lbs)
Ports:	1 x 5Gbps Ethernet LAN Port
SIM:	Dual SIM, 2 x 4FF Nano SIM Slots Multi-carrier support with automatic switching
Chipset:	Qualcomm® Snapdragon™ SDX55
LED:	Power and Status
Power:	Power over Ethernet (PoE)
Web UI OS Support:	Windows 10 and later MacOS 10.14 and later Linux® Ubuntu 18.04 LTS and later
High-Gain Antennas:	14dBi: 3.3GHz - 4.2GHz 12dBi: 1.7GHz - 2.7GHz 5dBi: 1.5GHz 0-4dBi: 600MHz - 1.0GHz

Environmental

Operating Temperature:	-30°C to 70°C (-22 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).	

* Certification schedules dependent on customer launch requirements.

Network Connectivity*

5G NR Sub6
4G LTE CAT 22
4x4 MIMO Sub6
256 QAM Sub6

Security

Inseego Secure™ Compatible
3rd Party Cybersecurity Penetration Testing Verified
Security Hardened Web Interface
Password Hash
Session Timeout
Incorrect Password Lockout
Anti CSRF
MACsec Encryption

* Data plan required. Coverage subject to network availability.

Regulatory Information

Federal Communications Commission Notice (FCC – United States)

FCC ID: PKRISGFW2000

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-FW2000

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 RF Exposure Guidance Statement

In order to comply with FCC RF Exposure requirements, this device must be installed to provide at least 35cm 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 35cm de séparation du corps humain en tout temps.

CE

Inseego Corp. declares that FW2000 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 35 cm separation from the human body at all times.

Radio Frequency and Transmitted Output Power Information

Band	Max Power	Frequency
BAND 1	24 dBm	1920-1980 MHz
BAND 3	24 dBm	1710-1785 MHz
BAND 7	24 dBm	2500-2570 MHz
BAND 8	24 dBm	880-915 MHz
BAND 20	24 dBm	832-862 MHz
BAND 28	24 dBm	703–748 MHz
BAND 38	24 dBm	2570–2620 MHz
BAND 40	24 dBm	2300–2400 MHz
BAND 41	24 dBm	2496–2690 MHz
BAND 42	24 dBm	3400–3600 MHz
BAND 43	24 dBm	3600–3800 MHz
FR1 n1	24 dBm	1920-1980 MHz
FR1 n3	24 dBm	1710-1785 MHz
FR1 n7	24 dBm	2500-2570 MHz
FR1 n8	24 dBm	880-915 MHz
FR1 n20	24 dBm	832–862 MHz
FR1 n28	24 dBm	703-748 MHz
FR1 n38	24 dBm	2570–2620 MHz
FR1 n40	24 dBm	2300-2400 MHz
FR1 n41	24 dBm	2496–2690 MHz
FR1 n77	24 dBm	3300–4200 MHz
FR1 n78	24 dBm	3300–3800 MHz
Bluetooth	3 dBm	2400-2483.5 MHz

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/.

Energy Efficiency

Efficiency performance is based on the U.S. Department of Energy Federal Energy Conservation Standards for Battery Chargers.

Energy efficiency terms - the energy efficiency values are based on the following conditions:

- **Power adapter, no-load:** Condition in which the FW2000e power adapter is connected to AC power, but not connected to device.
- **Power adapter efficiency:** Average of the FW2000e power adapter with the measured efficiency when tested at 100 percent, 75 percent, 50 percent, and 25 percent of the power adapter's rated output current.

Mode	Power Consumption for FW2000e	
	115V	230V
Power adapter, no load	<0.21W	<0.21W
Power adapter efficiency	>88%	>88%

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 FW2000e device, or failure of the FW2000e device to transmit or receive such data.

SURGE WARNING: If the FW2000e endures significant interference from the environment, disconnection may occur on the cellular network or Bluetooth. This is due to a circuit-protection design feature that reboots the device to avoid potential damage. If you experience this disruption, please ensure all wireless links are re-established.

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 FW2000e 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 CPE is turned off prior to boarding aircraft in order to comply with these regulations. The CPE 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.

- **CHAP** — Challenge Handshake Authentication Protocol. Protocol used in conjunction with Point to Point Protocol (PPP) to provide security and authentication to users of remote resources. CHAP does not use username/password, but uses a challenge method for authentication. Initiator sends a logon request to the server. The server sends back a challenge to the client. The challenge is encrypted and sent back to the server. The server compares the value from the client, and if it matches, allows the session. If the compare fails, the session is denied and the request restarts.

- **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.

- **ECGI** —E-UTRAN Cell Global Identifier. A 15-digit code used to identify cells globally. It is constructed from the Mobile Country Code (MCC), Mobile Network Code (MNC), and the E-UTRAN Cell Identifier (ECI).
- **Firmware** — A computer program embedded in an electronic device. Firmware usually contains operating code for the device.
- **FTP** — File Transfer Protocol. A standard network protocol used to transfer computer files between a client and server.
- **GB** — Gigabyte. A multiple of the unit byte for digital information storage. Usage depends on context. When referring to disk capacities it usually means 10^9 bytes. It also applies to data transmission quantities over telecommunication circuits.
- **Gbps** — Gigabits per second. The rate of data flow.
- **Hotspot** — A Wi-Fi (802.11) access point or the area covered by an access point. Used for connecting to the Internet.
- **HTTP**—Hypertext Transfer Protocol. An application-level protocol for accessing the World Wide Web over the Internet.
- **IEEE** — Institute of Electrical and Electronics Engineers. An international technical/professional society that promotes standardization in technical disciplines.
- **IMAP** — Internet Message Access Protocol. An Internet standard protocol for accessing email from a remote server from email clients. IMAP allows access from multiple client devices.
- **IMEI** — International Mobile Equipment Identity. Used in LTE networks to identify the device. It is usually printed on the device and can often be retrieved using a USSD code.
- **IMSI** —International Mobile Subscriber Identity. A unique number, usually fifteen digits, that identifies a Global System for Mobile Communications (GSM) subscriber.
- **IoT**—Internet of things. An expansion of the internet and network connections to sensors and devices (things) allowing simple objects, such as light fixtures and locks, a higher degree of computing and analytical capabilities. IoT enables connected devices (things) to gather and share data from their environment with other devices and networks with the need for little or no human interaction.
- **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.
- **M2M**— Machine to machine. Direct communication between devices. This may include wired or wireless communication.
- **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.
- **MNO** —Mobile 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.
- **MSID** — Mobile Station IDentifier. A number for a mobile phone that identifies that phone to the network.
- **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.
- **NMEA port** — National Marine Electronics Association port. The port through which applications can access a GPS data stream.
- **NNTP** — Network News Transfer Protocol. The primary protocol used to connect to Usenet servers and transfer news articles between systems over the Internet.
- **PAP** — Password Authentication Protocol. A protocol used by Point to Point Protocol (PPP) to validate users. PAP does not encrypt data and sends the password and username to the authentication server as plain text. Most network operating system remote servers support PAP.
- **PCI** — Physical Cell ID. Each PCI corresponds to one 5G NR cell or LTE cell and consists of two parts: PSS Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS).
- **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.
- **PRL** — Preferred Roaming List. A list that your wireless phone or device uses to determine which networks to connect with when you are roaming (Network operator specific).
- **Protocol** — A standard that enables connection, communication, and data transfer between computing endpoints.
- **Proxy** — A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.
- **Router** — A device that directs traffic from one network to another.
- **RSRP** – Reference Signal Receive Power. An LTE-specific measure of signal strength, similar to RSSI, but RSRP measures lower than RSSI due to the method of calculation.
- **RSRQ** – Reference Signal Received Quality. A calculated value from RSRP and RSSI that provides a measure of signal and interference.
- **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.
- **SNR** — Signal to Noise Ratio. A ratio of signal power to noise power expressed in decibels. SNR is a positive value, and higher numbers are better.
- **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.
- **SNR** — Signal to Noise Ratio. A ratio of signal power to noise power expressed in decibels. SNR is a positive value, and higher numbers are better.
- **SSID** — Service Set IDentifier. The name assigned to a Wi-Fi network.
- **TCP/IP** — Transmission Control Protocol/Internet Protocol. The set of communications protocols used for the Internet and other similar networks.
- **TFTP** — Trivial File Transfer Protocol. An Internet software utility for transferring files that is simpler to use than FTP, but does not provide user authentication and directory visibility supported by FTP.

- **Telnet** — A user command and underlying TCP/IP protocol that allows a user on one computer to log into another computer that is part of the same network.
- **TTY** — Text Telephones (TTY), also known as Telecommunications Device for the Deaf (TDD), are used by the deaf, hard–of–hearing, and individuals with speech impairments to communicate.
- **UDP** — User Datagram Protocol (UDP) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.
- **USB** — Universal Serial Bus. A connection type for computing device peripherals such as a printer, mobile modem, etc.
- **USB Port Types** —USB ports on computers and hubs have a rectangular Type A port, and peripheral devices have a cable with a Type A connector. Peripheral devices that do not have an attached cable typically have a Type C port on the device and a separate Type A to C cable. Type B connectors have been replaced by Type C. Mini-USB connectors have largely been superseded by Micro-USB, but are still used with some cameras, music players, etc. Micro-USB connectors are used with portable devices, such as phones and battery packs, although USB-C is being adopted by most manufacturers.
- **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.