

Inseego Wavemaker™ 5G indoor router FX2000



INSEEGO COPYRIGHT STATEMENT

© 2022 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 Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp.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: 14965420 Rev 2

Contents

| | |
|---|----|
| Introduction and getting started | 5 |
| Overview | 6 |
| System requirements | 6 |
| Ports and buttons..... | 7 |
| Indicator LEDs..... | 8 |
| Getting started | 9 |
| Installing a SIM card | 9 |
| Powering on..... | 10 |
| Identifying a location | 10 |
| Connecting to the FX2000 | 10 |
| Monitoring and managing your 5G indoor router | 12 |
| Caring for your FX2000 | 13 |
| Replacing a SIM card..... | 13 |
| Resetting your FX2000..... | 14 |
| Care tips | 15 |
| Configuration..... | 16 |
| Overview | 17 |
| Home page | 18 |
| Side menu..... | 18 |
| Getting help | 19 |
| Admin password..... | 19 |
| Changing the Admin password..... | 19 |
| Managing data usage..... | 20 |
| Data Usage page | 21 |
| Managing Wi-Fi settings | 23 |
| Settings tab..... | 24 |
| Primary Network tab | 26 |
| Guest Network tab | 28 |
| Managing connected devices..... | 30 |
| Connected Devices page | 31 |
| Managing settings | 33 |
| Preferences tab..... | 34 |
| Software Update tab | 35 |
| Backup and Restore tab | 36 |
| VPN tab | 38 |
| GPS tab..... | 40 |
| Advanced tab | 41 |
| Viewing info about the FX2000..... | 42 |
| Internet Status tab..... | 43 |
| Internet Sessions tab | 44 |
| Diagnostics tab..... | 45 |
| Device Info tab..... | 46 |
| Getting support..... | 47 |
| Customer Support tab | 48 |
| Advanced settings | 50 |

| | |
|--|----|
| Overview | 51 |
| Using advanced settings..... | 51 |
| Cellular tab | 52 |
| Manual DNS tab..... | 54 |
| SIM tab | 55 |
| Firewall tab..... | 57 |
| MAC Filter tab..... | 58 |
| LAN tab..... | 59 |
| WAN | 61 |
| Port Filtering tab | 62 |
| Port Forwarding tab..... | 64 |
| Inseego Connect tab | 67 |
| Inseego Connect | 68 |
| Troubleshooting and support | 69 |
| Overview | 70 |
| Troubleshooting | 70 |
| I cannot access the Admin web UI..... | 70 |
| My connecting device is not obtaining a valid IP address..... | 70 |
| I see other networks, but not the network name for my FX2000 | 71 |
| I see the network name, but cannot connect a device to my FX2000..... | 71 |
| I cannot register my FX2000 with Inseego Connect or Inseego Mobile app | 72 |
| I cannot get streaming platforms to work with my FX2000..... | 72 |
| My FX2000 is getting slow speeds/low throughput | 72 |
| Do I need an external antenna? | 73 |
| Do I need a signal amplifier or booster? | 73 |
| Does the USB port support RNDIS? | 73 |
| Does the USB port support USB-C to Ethernet adapters? | 73 |
| Technical Support | 74 |
| Product specifications and regulatory information | 75 |
| Product specifications..... | 76 |
| Device..... | 76 |
| Environmental..... | 76 |
| Network connectivity | 76 |
| Wi-Fi | 77 |
| External antenna port bands | 77 |
| Security | 77 |
| Regulatory information..... | 78 |
| Product certifications and supplier's declarations of conformity | 83 |
| Energy efficiency..... | 84 |
| Wireless communications | 84 |
| Limited warranty and liability | 85 |
| Safety hazards..... | 86 |
| Glossary..... | 87 |
| Glossary..... | 88 |

1

Introduction and getting started

Overview

Ports and buttons

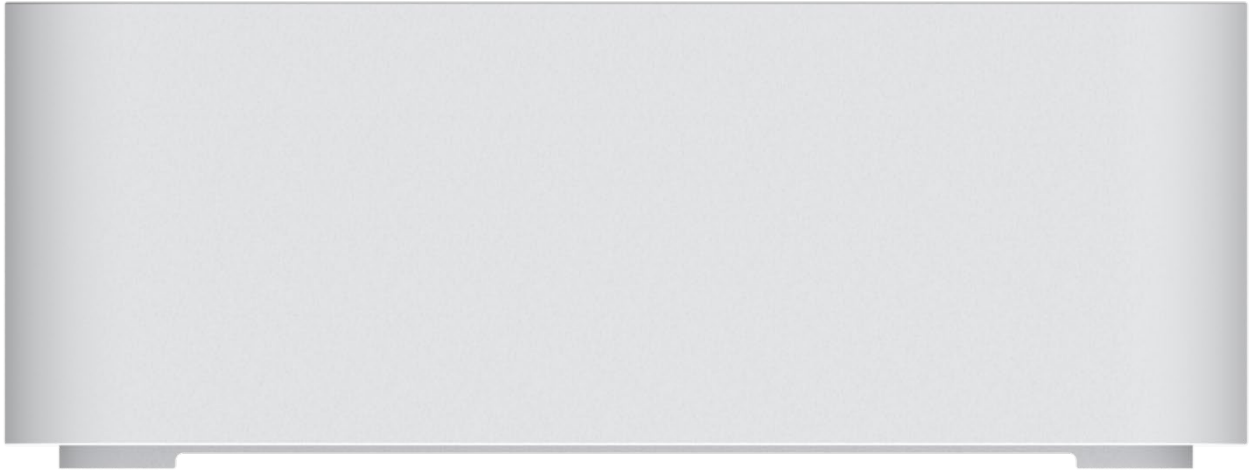
Indicator LEDs

Getting started

Caring for your FX2000

Overview

The 5G indoor router FX2000 is a wireless device that delivers Internet service. The FX2000 provides network and Internet connectivity via Wi-Fi, Ethernet, and USB. Connect laptops, tablets, e-readers, gaming consoles and more.



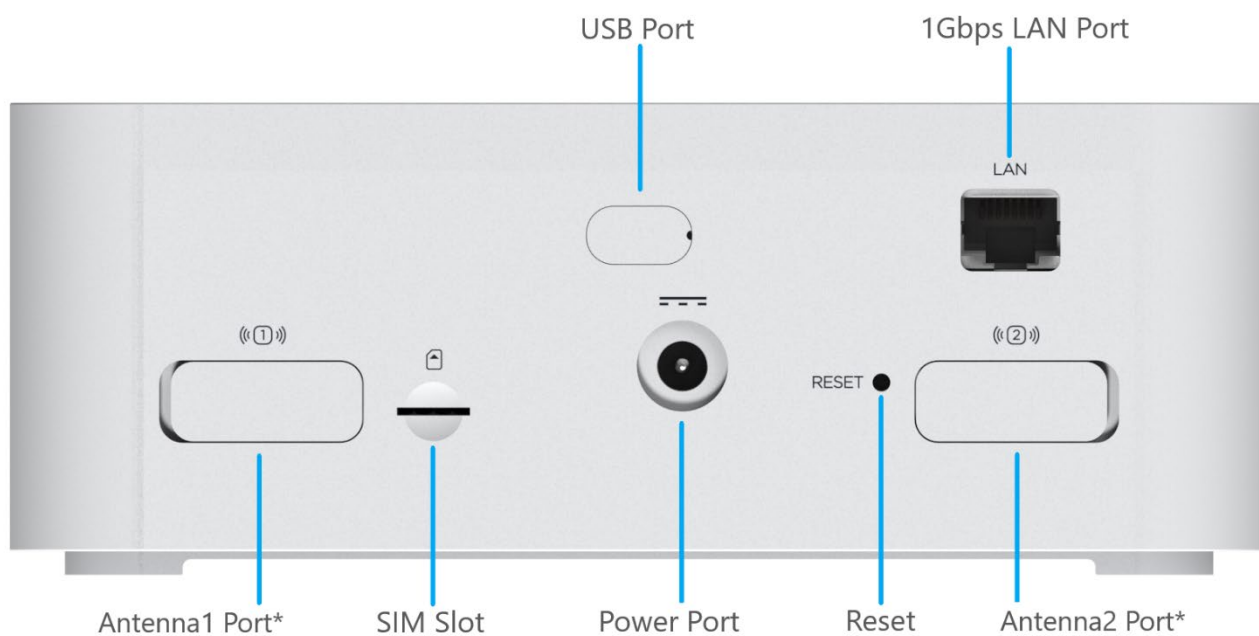
Inside the box you will find a 5G indoor router FX2000, a Welcome card, an Ethernet cable, and an AC wall adapter power supply.

System requirements

- Compatible with all major operating systems.
- Works with the latest versions of browsers.

To use Wi-Fi mode, connecting devices need Wi-Fi capability. You can also connect via Ethernet or USB.

Ports and buttons








* Antenna ports are for external 3.4-5GHz antennas supporting high sub-6 bands (CBRS and C-band). For most users, there is no benefit to attaching external antennas. For specific bands supported, see page 77.

NOTE: When connecting only one antenna, use the Antenna1 port.



Indicator LEDs

The top of the FX2000 has an indicator LED. It changes colors and either blinks or glows solid to communicate current states for the device.



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

The LAN port also has indicator LEDs.

| LED color | Operation | Meaning |
|--|--------------------------|---|
| Green  | Solid Blinking Off | Indicates Ethernet connection speed |
| | | 1000 Mbps (Gigabit) |
| | | Data is being transferred |
| | | 10/100 Mbps |
| Amber  | Solid Off | Indicates port status |
| | | Port is being connected, but no data is being transferred |
| | | Port is being disconnected |

Getting started

This section provides instructions for getting your 5G indoor router FX2000 up and running, as well as reset and support information.

Installing a SIM card

A SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The 5G indoor router supports only Nano SIM cards.

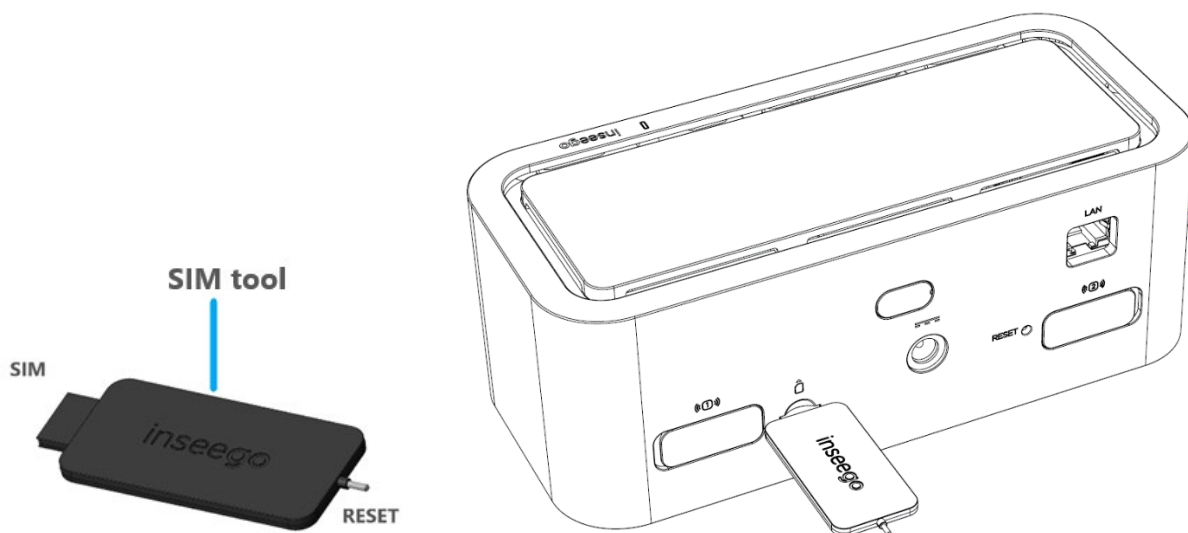
NOTE: If you received the FX2000 from your service provider, the device manufacturer may have pre-installed the SIM card. Please inspect the SIM slot on the back of the device to confirm.



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

To install a SIM card:

1. If necessary, remove the SIM card from the protective sleeve, being careful not to touch the gold-colored contacts.
2. Use the included SIM tool to insert the SIM card into the SIM slot, ***notch first, with the gold-colored contact points facing down.***



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

Powering on

Turn on your FX2000 with the AC wall adapter power supply:

1. Plug the power cord into the power port on the back of the FX2000.
2. Plug the power adapter into an AC wall outlet.

WARNING! Use only the AC wall adapter power supply that came with the 5G indoor router. Unapproved AC wall adapter power supplies could cause the FX2000 to overheat or catch fire, resulting in serious bodily injury, death, or property damage.

Identifying a location

Use the Inseego Mobile™ app to identify the optimal location for your 5G indoor router.

1. 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.



2. Follow instructions within the Inseego Mobile app to connect to your 5G indoor router and perform a location survey to identify the ideal location for your 5G indoor router.

NOTE: Make sure to place your 5G indoor router on a sturdy surface.

Connecting to the FX2000

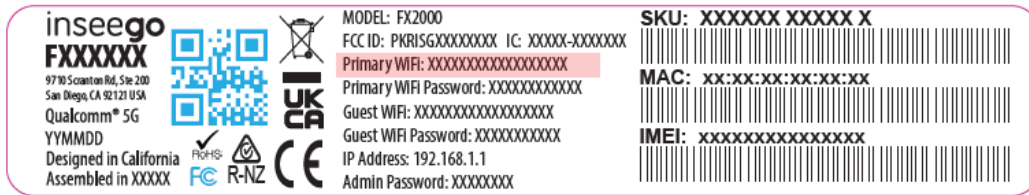
With the 5G indoor router, Wi-Fi devices and wired devices can connect to the mobile broadband network simultaneously.

Connecting devices wirelessly

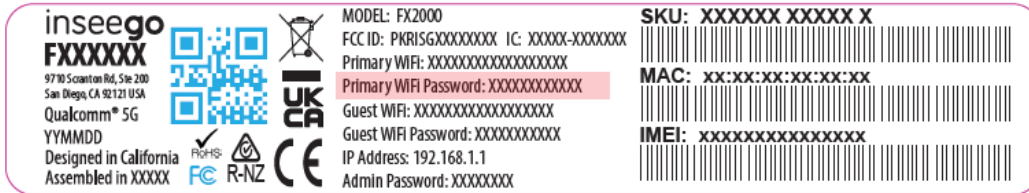
You can connect to your 5G indoor router with your computer, tablet or other wireless devices that have Wi-Fi and Internet browser software.

To connect a Wi-Fi capable device to your FX2000:

1. Make sure the 5G indoor router is powered on, and the indicator LED is blue or green.
2. On the device you want to connect to the Internet, open the Wi-Fi settings or application and in the displayed list of available networks, find the **Primary Wi-Fi network name** printed on the bottom of your FX2000.



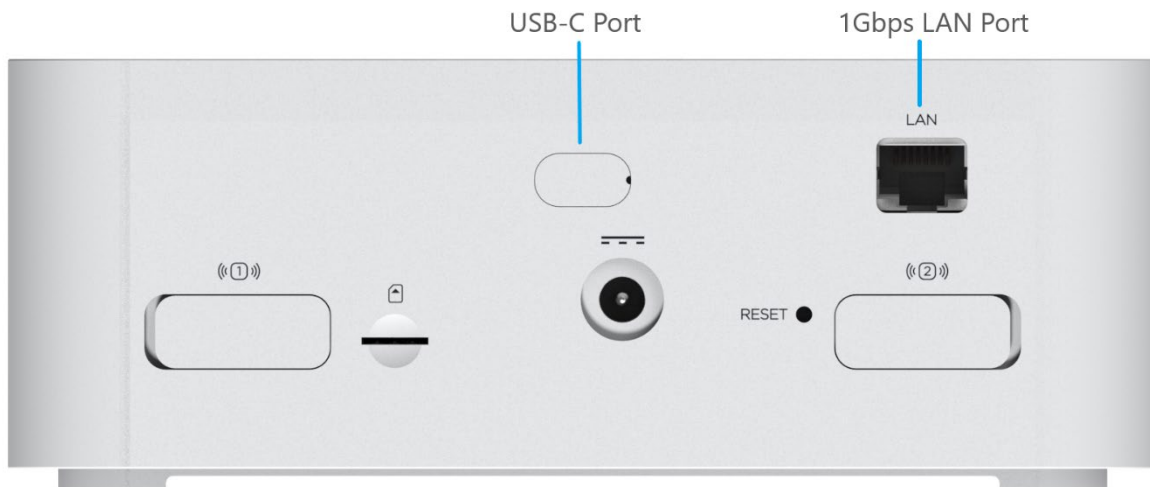
3. Click **Connect** or otherwise select the network name.
4. When prompted, enter the **Primary Wi-Fi password** printed on the bottom of the FX2000.



Your Wi-Fi capable device is now connected to the Internet.

Connecting devices with Ethernet or USB

You can connect wired devices such as laptops, printers, and gaming consoles via Ethernet or USB.



To connect Ethernet devices:

1. Plug one end of an Ethernet cable into the LAN port on the FX2000.
2. Plug the other end of the cable into the Ethernet port of the device you wish to connect.

To connect USB devices:

1. Plug the USB-C end of a USB cable into the USB port on the FX2000.
2. Plug the other end of the cable into the USB port of the device you wish to connect.

Devices plugged into the FX2000 via Ethernet and USB have instant access to the internet.

Monitoring and managing your 5G indoor router

You can use multiple options to monitor and manage your 5G indoor router.

Inseego Mobile app

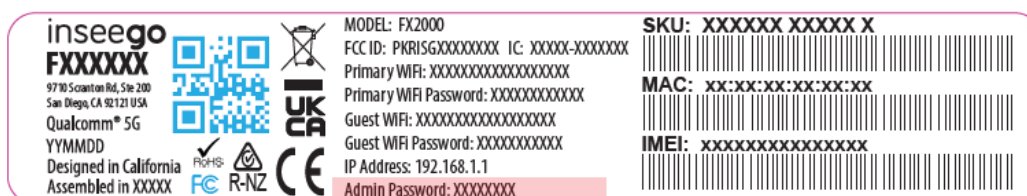
You can use the same mobile app you used to find a location for your FX2000 to perform basic device monitoring and management.

Admin web UI

Once your 5G indoor router 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 5G indoor router, open any web browser and go to <http://192.168.1.1> or <http://inseego.local/> *.

Select **Sign In** (in the top-right corner of the screen) and enter the **Admin Password** printed on the bottom of the FX2000.



Inseego Connect

Go to **connect.inseego.com** to sign up for a free Inseego Connect™ account, which provides the fullest experience for monitoring and managing FX2000 devices from virtually anywhere in the world with access to a web browser.

* The Inseego.local web UI address relies on having IPv6 enabled on your connecting device.

Caring for your FX2000

This section provides information on general care and restoring your 5G indoor router to factory default settings.

Replacing a SIM card

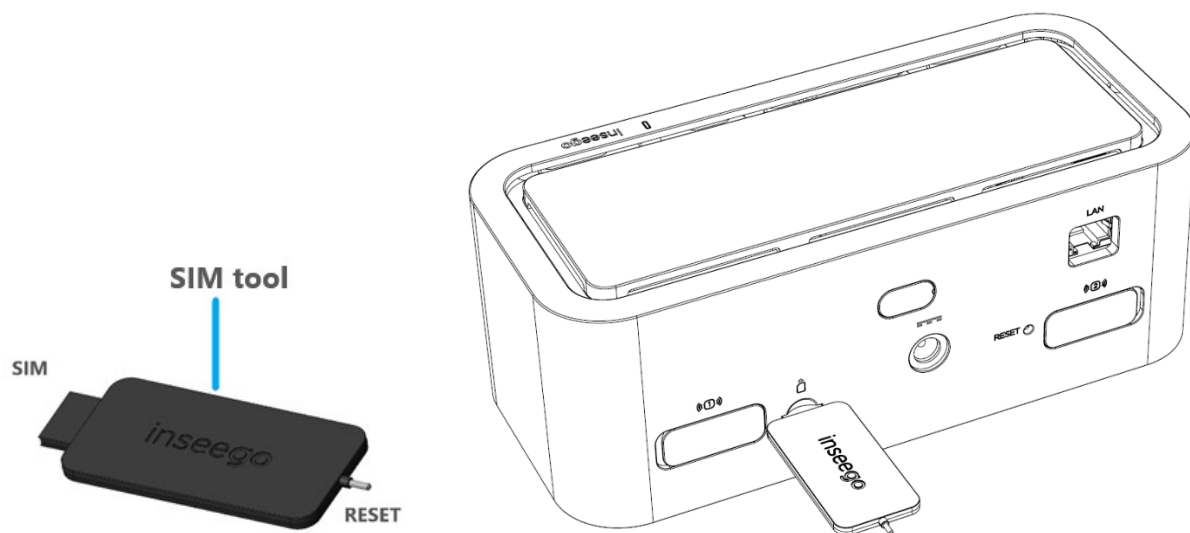
Your SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The 5G indoor router supports only Nano SIM cards. To replace a SIM card, select the correct SIM for this device.



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 a SIM card:

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



2. If necessary, remove the SIM card from the protective sleeve, being careful not to touch the gold-colored contacts.
3. Use the included SIM tool to insert the SIM card into the SIM slot, **notch first, with the gold-colored contact points facing down.**

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

Resetting your FX2000

You can reset your 5G indoor router to factory settings from the Admin web UI, Inseego Connect, Inseego Mobile app, or by using the RESET button on the FX2000

CAUTION! Resetting returns your FX2000 to factory settings, including resetting the Wi-Fi name and password and admin password to the defaults shown on the label. This disconnects all devices.

Resetting from the Admin web UI

To reset the FX2000 from the Admin web UI, select **Settings > Backup and Restore** and select **Restore Factory Defaults**.

Resetting from Inseego Connect

To reset the FX2000 from Inseego Connect, on the Devices page, check the box next to the device and select **Factory Reset**.

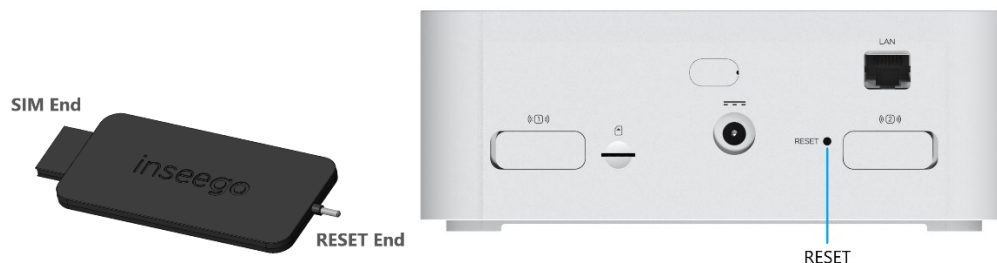
Resetting from the Inseego Mobile app

To reset the FX2000 from the Inseego Mobile app, select **Mobile Options**, then select **Factory Reset**.

Resetting with the RESET button

The master reset button is in a small hole located on the back of the 5G indoor router.

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



2. Press the SIM tool on the button for about five to six seconds, then your 5G indoor router will restart.

Care tips

Inseego recommends the following care guidelines:

- Protect the FX2000 from liquids, dust, and excessive temperatures.
- Do not apply adhesive labels to the FX2000 as they may cause the router to potentially overheat or alter the performance of the internal antenna.
- Store the FX2000 in dry and secure location when not in use.

2

Configuration

Overview

Admin password

Managing data usage

Managing Wi-Fi settings

Managing connected devices

Managing settings

Viewing info about the FX2000

Getting support

Overview

You can configure your FX2000 to best suit your needs, including: changing your network name and/or passwords, setting up a guest network, viewing all currently connected devices, and setting device preferences.

There are multiple tools for configuring your 5G indoor router:

- **Inseego Mobile app** – Allows you to perform basic device monitoring and management. This is the same app you used to identify a location for your FX2000.
- **Admin web UI** – Provides a local gateway to configure and manage your FX2000. On a device connected to your FX2000, open any web browser and go to <http://192.168.1.1> or <http://inseego.local/> *. Select **Sign In** (in the top-right corner of the screen) and enter the **Admin Password** printed on the bottom of the FX2000.
- **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.

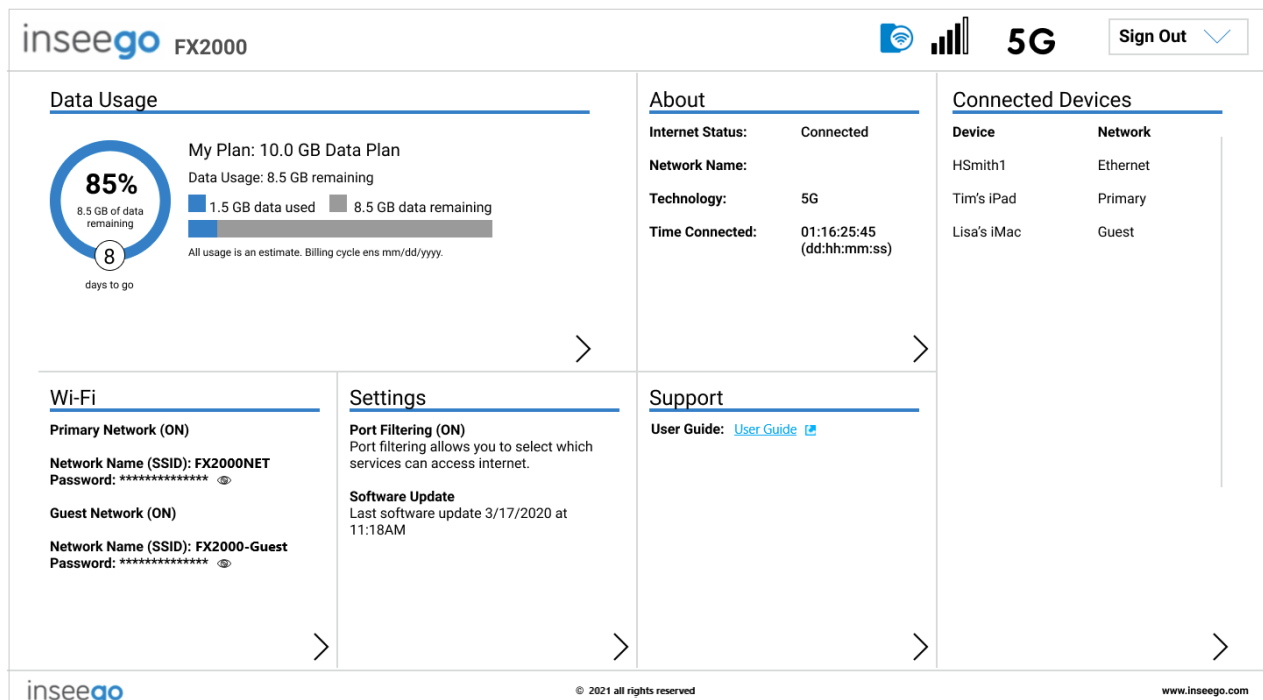
This chapter provides the configuration options available for your FX2000 devices. The configurations shown are from the Admin web UI, unless otherwise noted. Many of these options are also available with Inseego Mobile app and Inseego Connect. Some configurations are available only with Inseego Connect and are marked as such.

* The Inseego.local web UI address relies 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 FX2000. It displays the current Wi-Fi networks and passwords and lists all currently connected devices. It also shows data usage, Internet status, setting information, and provides access to support.

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



Side menu

Each sub screen in the 5G indoor router Admin web User Interface 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 Inseeego Connect.

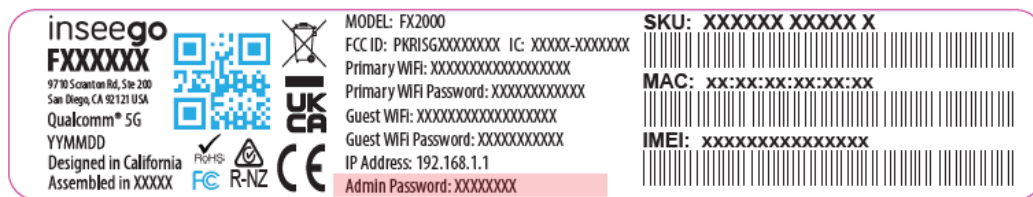
| |
|-------------------|
| Home |
| Data Usage |
| Wi-Fi |
| Connected Devices |
| Settings |
| About |
| Support |

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 5G indoor router Admin web UI. A default Admin password is assigned to each individual device and is printed on the bottom of the FX2000.



You can change the Admin password to something easier to remember and set up a security question that will help you securely recover your password if you forget it.

NOTE: You can set up separate Wi-Fi passwords for both primary and guest networks in **Wi-Fi**, but these are different from the Admin password, which is for this web User Interface.

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.

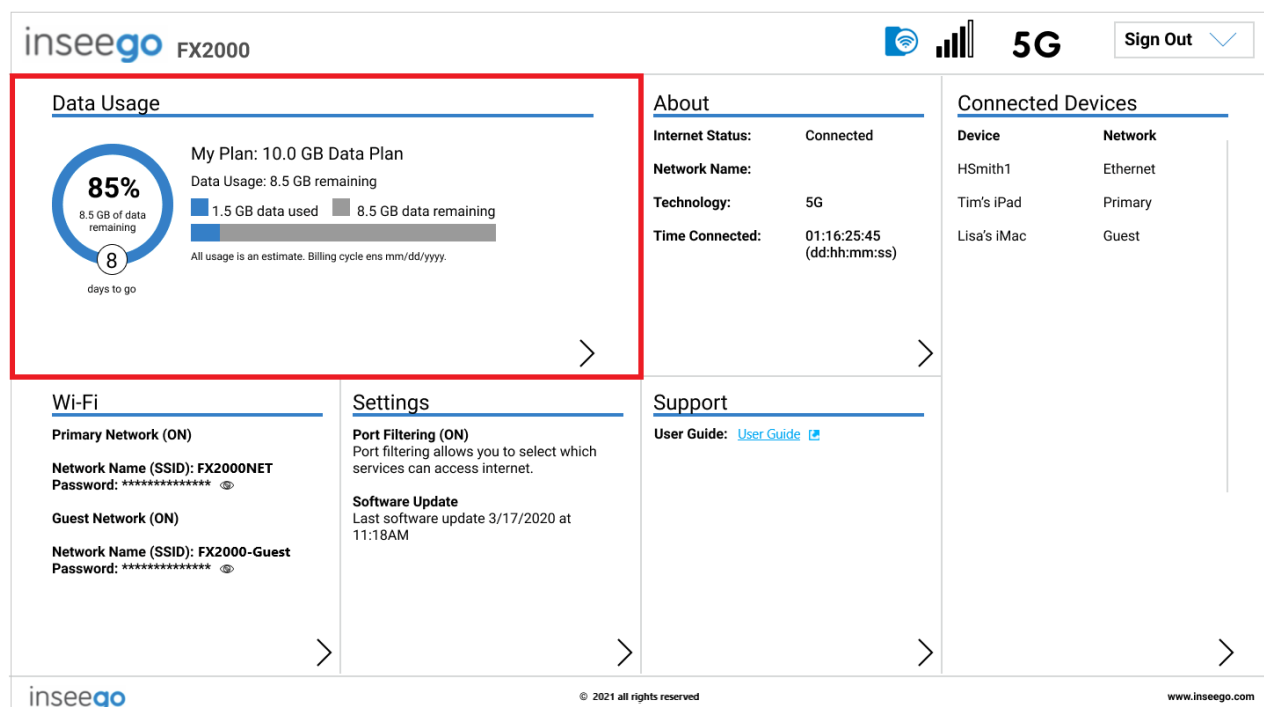
2. Enter your current Admin password, then click **Continue**.
3. Enter your current Admin password again, then enter a new password and confirm it.
4. Select a security question from the drop-down list and type an answer to the question.
NOTE: Answers are case-sensitive.
5. Click **Save Changes**.

The next time you sign in to the 5G indoor router web User Interface, 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

You can monitor and manage data usage on your FX2000 using the Data Usage page.

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

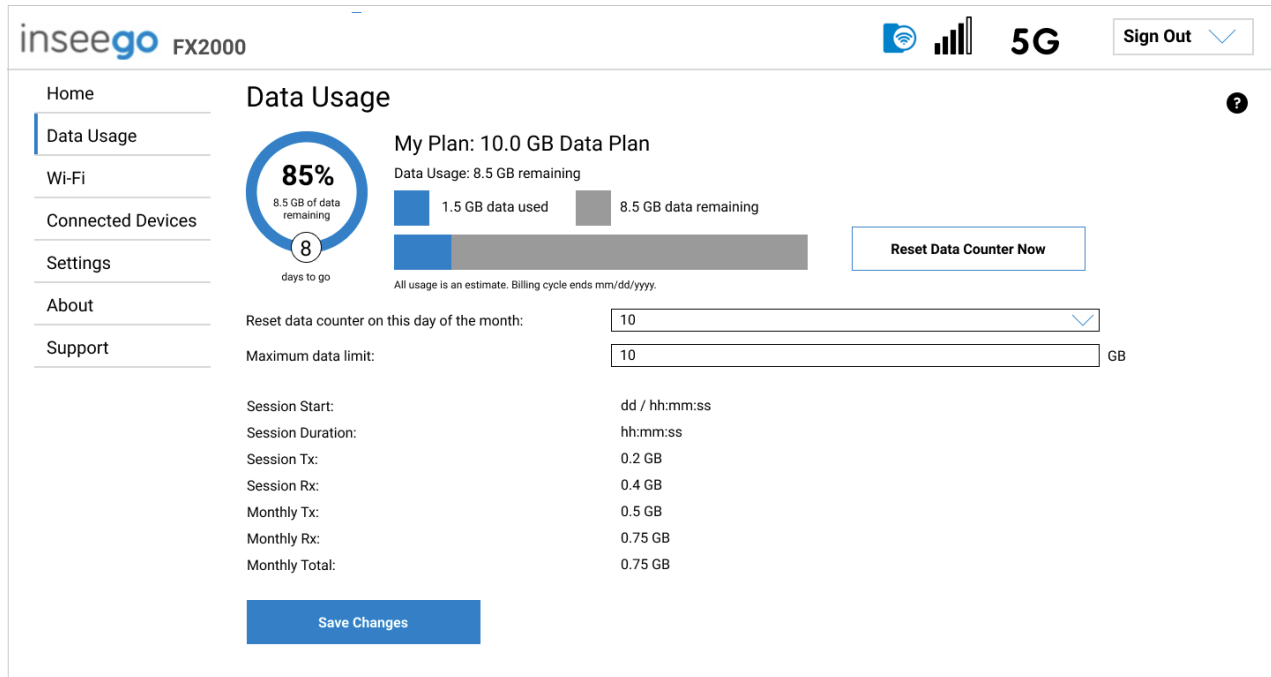


To manage or view data usage, select ➤ from the home page Data Usage panel or select **Data Usage** from the side menu. The Data Usage page appears.

Data Usage page

Use the Data Usage page to view details and manage your FX2000 data usage.

NOTE: Your FX2000 provides only a rough estimate of data usage. Always check with your service provider for exact usage.



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.

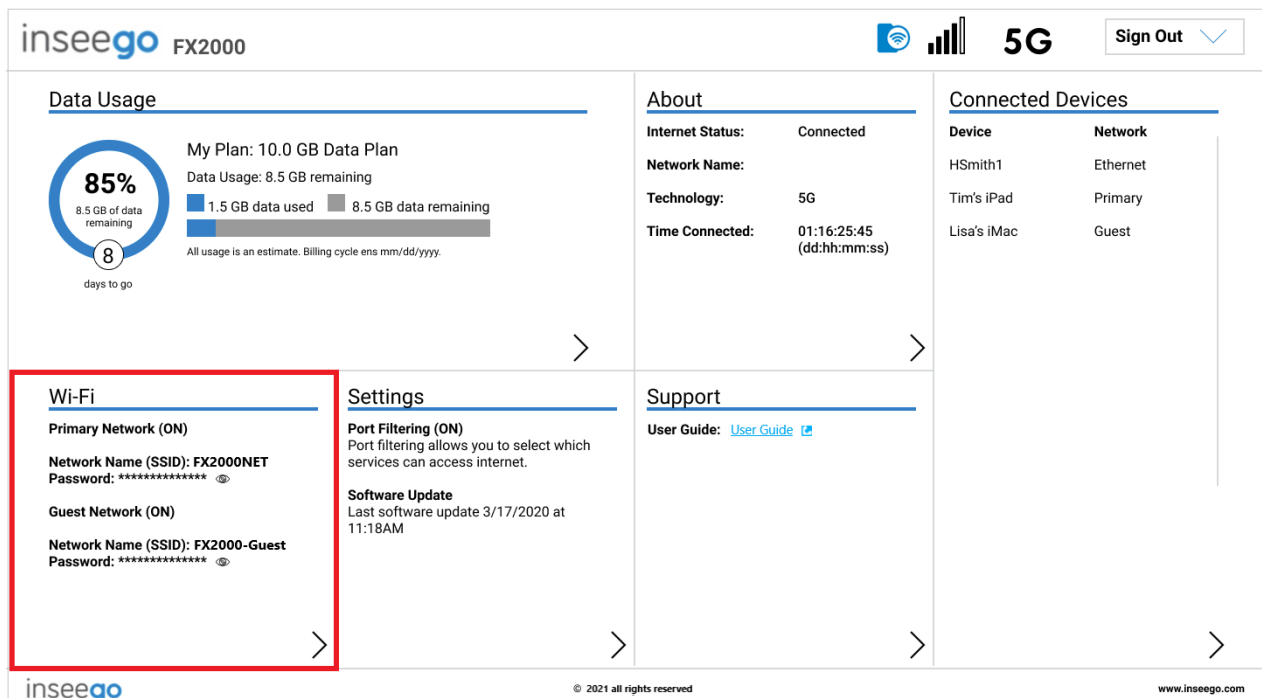
Monthly Total: The total amount of data for the current billing cycle.

Select **Save Changes** to enact changes.

Managing Wi-Fi settings

Your 5G indoor router offers primary and guest networks for accessing the Internet over Wi-Fi. Each network can be accessed over two bands: 2.4 GHz and 5 GHz.

On the Admin web UI home page, the Wi-Fi panel shows the current name and password of the primary and guest networks.



To manage settings for these networks, select > from the home page Wi-Fi panel or select **Wi-Fi** from the side menu.

The Wi-Fi page includes three tabs:

- Settings
- Primary Network
- Guest Network

Settings tab

You can use the default values as they appear on this tab or can adjust them for your environment.

The screenshot shows the 'insee.go FX2000' web interface. The top navigation bar includes a 'Sign Out' button. The left sidebar lists 'Home', 'Data Usage', 'Wi-Fi' (selected), 'Connected Devices', 'Settings', 'About', and 'Support'. The main content area is titled 'Wi-Fi' and has tabs for 'Settings', 'Primary Network', and 'Guest Network'. A note states: 'These settings apply regardless of which network (primary, guest or both) is in use. Changes made to these Wi-Fi settings may prevent some Wi-Fi devices from connecting.' The 'Wi-Fi' section includes a toggle for 'Allow Wi-Fi devices to connect' (currently on), a 'Limit connected devices to: 30' with a link to 'Change connection limit', and a 'Band Selection' section. The 'Band Selection' section has a note: 'Note: Making band selection changes may cause both the primary and guest networks to run off and on again. Devices will be disconnected and you may need to sign back into the Admin website.' It features two columns for '2.4 GHz Band' and '5 GHz Band'. Under '2.4 GHz Band', 'Primary Network' is selected, 'Guest Network' is unselected, and 'Off' is unselected. Under '5 GHz Band', 'Primary Network' is selected, 'Guest Network' is unselected, and 'Off' is unselected. Below these are '2.4 GHz Band Settings' and '5 GHz Band Settings'. The '2.4 GHz Band Settings' include '802.11 Mode' (802.11bgn/ax) and 'Channel' (Automatic). The '5 GHz Band Settings' include '802.11 Mode' (802.11acn/ax), 'Bandwidth' (80 MHz), and 'Channel' (Automatic). A 'Save Changes' button is at the bottom.

NOTE: When IP Passthrough is turned on, Wi-Fi networking 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.

Wi-Fi

Use the **Allow Wi-Fi devices to connect** slider to turn Wi-Fi on or off. This selection affects primary and guest networks. **NOTE:** If Wi-Fi is off, the only way to connect devices to the 5G indoor router is with an Ethernet cable or USB.

Select **Change connection limit** to change the maximum number of devices allowed to connect to your 5G indoor router. Select a number and click **Save Changes**. The maximum number of connected devices is 30.

Band Selection

Each network can be accessed over two bands: 2.4 GHz and 5 GHz:

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

NOTE: The guest network must be assigned at least one band before it can be turned on.

2.4 GHz Band Settings

This section displays the 802.11 Mode in use when the 2.4 GHz band is active and allows you to select a Channel.

NOTE: Leave the Channel set to **Automatic** unless you need to choose a particular channel for your environment.

5 GHz Band Settings

This section displays the 802.11 Mode in use when the 5 GHz band is active and allows you to select a Bandwidth and Channel.

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

NOTE: Leave the **Channel** set to **Automatic** unless you need to choose a particular channel for your environment.

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

Primary Network tab

Use these settings to connect initially to the primary Wi-Fi network or change primary network information. Connected devices must use the Wi-Fi settings shown on this screen.

The screenshot shows the 'Primary Network' tab in the inseeo FX2000 web interface. The left sidebar contains links for Home, Data Usage, Wi-Fi (selected), Connected Devices, Settings, About, and Support. The main content area is titled 'Wi-Fi' and has sub-tabs for 'Settings', 'Primary Network' (selected), and 'Guest Network'. A note states: 'Note: For added security, share your guest network instead of your primary network.' The settings include: 'Primary Network Name (SSID)' with a text input field containing '<primary-ssid>', 'Security' with a dropdown menu showing 'WPA3/WPA2 Transition', and 'Password' with a text input field containing 'SecretCode123' and a toggle for visibility. Below these is a 'Generate New Password' button. A second note explains: 'Note: You can create a new password by entering it, or generate a new one. Password must be 8-63 characters. For greater security, use a mixture of digits, upper case, lower case and other symbols.' At the bottom are two checkboxes: 'Broadcast primary network name (SSID):' and 'Wi-Fi privacy separation:', both currently unchecked. A blue 'Save Changes' button is at the very bottom.

NOTE: When IP Passthrough is turned on, Wi-Fi networking 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.

WARNING! If you change these settings, existing connected devices may lose their connection.

Primary network name (SSID): Enter a primary network name (SSID) to set up or change the primary network name. The name can be up to 32 characters long.

Security: Select an option for Wi-Fi security:

- **WPA3/WPA2 Transition** is the most secure method of Wi-Fi Protected Access and should be used, if possible, for WPA2 and WPA3 compliant devices.
- **WPA3 PSK** can be used for WPA3 devices.
- **WPA 3 Open Enhanced** provides encryption and privacy on open networks that are not password-protected and can be used for WPA3 devices.
- **WPA/WPA2 Mixed Mode** can be used if some of your older devices do not support WPA2.
- **WPA2 AES PSK** can be used for WPA2 devices.
- **Open** allows others to monitor your Wi-Fi traffic and use your data plan to access the Internet. **NOTE:** Avoid using this option.

Password: Enter a Wi-Fi password, **or** you can use the Generate New Password button.

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

Generate New Password: This button inserts a strong random password in the Password field.

You can click the eye icon to view the password.

Broadcast primary network name (SSID): Check this box to display the Wi-Fi primary network in the list of available Wi-Fi networks on your connected devices. If unchecked, this network is not visible to connected devices.

Wi-Fi privacy separation: Check this box to keep each connected device on this network isolated from all other connected devices. This provides additional security if some connected devices are unknown or not completely trusted. **NOTE:** For normal operation, this should be unchecked.

Select **Save Changes**.

Guest Network tab

The Wi-Fi guest network allows you to segregate traffic to a separate network rather than share access to your Wi-Fi primary network. Use settings on this tab to set up or change Wi-Fi guest network information. Connected devices must use the Wi-Fi settings shown on this screen to connect to the guest 5G indoor router Wi-Fi network.

The screenshot shows the 'inseeego FX2000' web interface. The top navigation bar includes a 'Sign Out' button. The left sidebar lists 'Home', 'Data Usage', 'Wi-Fi', 'Connected Devices', 'Settings', 'About', and 'Support'. The main content area is titled 'Wi-Fi' and has tabs for 'Settings', 'Primary Network', and 'Guest Network'. The 'Guest Network' tab is active. A note states: 'Note: For added security, share your guest network instead of your primary network.' Below this are three input fields: 'Guest Network Name (SSID)' with the placeholder '<guest-ssid>', 'Security' set to 'WPA3/WPA2 Transition', and 'Password' set to 'SecretCode123'. A 'Generate New Password' button is located below the password field. Another note explains: 'Note: You can create a new password by entering it, or generate a new one. Password must be 8-63 characters. For greater security, use a mixture of digits, upper case, lower case and other symbols.' At the bottom, there are two checkboxes: 'Broadcast guest network name (SSID)' and 'Wi-Fi privacy separation', both currently unchecked. A blue 'Save Changes' button is at the very bottom.

NOTE: When IP Passthrough is turned on, Wi-Fi networking 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.

NOTE: To turn the Wi-Fi guest network on, you must select at least one band for Guest Network under **Band Selection** on the **Wi-Fi Settings** tab and then select **Save Changes**.

Guest Network Name (SSID): Enter a guest network name (SSID) to set up or change the guest network name. The name can be up to 32 characters long.

Security: Select an option for Wi-Fi security:

- **WPA3/WPA2 Transition** is the most secure method of Wi-Fi Protected Access and should be used, if possible, for WPA2 and WPA3 compliant devices.
- **WPA3 PSK** can be used for WPA3 devices.
- **WPA 3 Open Enhanced** provides encryption and privacy on open networks that are not password-protected and can be used for WPA3 devices.
- **WPA/WPA2 Mixed Mode** can be used if some of your older devices do not support WPA2.
- **WPA2 AES PSK** can be used for WPA2 devices.
- **Open** allows others to monitor your Wi-Fi traffic and use your data plan to access the Internet. **NOTE:** Avoid using this option.

Password: Enter a Wi-Fi password, **or** you can use the Generate New Password button.

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

Generate New Password: This button inserts a strong random password in the Password field.

You can click the eye icon to view the password.

Broadcast guest network name (SSID): Check this box to display the Wi-Fi guest network in the list of available Wi-Fi networks on your connected devices. If unchecked, this network is not visible to connected devices.

Wi-Fi privacy separation: Check this box to keep each connected device on this network isolated from all other connected devices. This provides additional security if some connected devices are unknown or not completely trusted. **NOTE:** For normal operation, this should be unchecked.

Select **Save Changes**.

Managing connected devices

On the Admin web UI home page, the Connected Devices panel lists the networks currently connected to your 5G indoor router along with the number of connected devices for each network.

The screenshot displays the inseeFX2000 Admin web UI. The top navigation bar includes the inseeFX2000 logo, a 5G signal indicator, and a 'Sign Out' button. The main content area is divided into several panels:

- Data Usage:** Shows a circular progress indicator at 85% remaining, with 8.5 GB of data remaining and 1.5 GB used. It also displays 'My Plan: 10.0 GB Data Plan' and 'Data Usage: 8.5 GB remaining'.
- About:** Displays 'Internet Status: Connected', 'Network Name', 'Technology: 5G', and 'Time Connected: 01:16:25:45 (dd:hh:mm:ss)'.
- Connected Devices:** A table listing connected devices and their networks. The table has two columns: 'Device' and 'Network'. The data is as follows:

| Device | Network |
|-------------|----------|
| HSmith1 | Ethernet |
| Tim's iPad | Primary |
| Lisa's iMac | Guest |
- Wi-Fi:** Shows settings for 'Primary Network (ON)' and 'Guest Network (ON)', including Network Name (SSID) and Password.
- Settings:** Includes 'Port Filtering (ON)' and 'Software Update' information.
- Support:** Provides a link to the 'User Guide'.

To manage connected devices, select ➤ from the home page Connected Devices panel or select **Connected Devices** from the side menu.

Connected Devices page

This page provides details about each device connected to the 5G indoor router and allows you to edit how device names appear in the UI. You can also block or unblock a device from Internet access.

The screenshot shows the 'inseeFX2000' web interface. The top right has a 'Sign Out' button. The left sidebar lists navigation options. The main section is 'Connected Devices' with a sub-header 'Connected (3)'. It contains two tables. The first table lists connected devices with columns for Device, Network, and Block. The second table lists blocked devices with columns for Device and Block. A 'Save Changes' button is at the bottom.

| Device | Network | Block |
|-------------|----------|--------------------------|
| HSmith1 | Ethernet | <input type="checkbox"/> |
| Tim's iMac | Primary | <input type="checkbox"/> |
| Lisa's iMac | Guest | <input type="checkbox"/> |

| Device | Block |
|--|-------------------------------------|
| Sue's iPhone MAC Address: XX:XX:XX:XX:XX:XX | <input checked="" type="checkbox"/> |
| Jim's iPhone MAC Address: XX:XX:XX:XX:XX:XX | <input checked="" type="checkbox"/> |

Connected Devices

Connected: The number of devices currently connected to your FX2000.

The table lists all devices connected to the 5G indoor router:

Connection: An icon indicates the connection type for each device. (You can hover over the icon to read the type of connection.)

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

Network: Indicates whether the device is connected to the primary or guest network, or through Ethernet or USB.

Block: Select this box to disconnect a device and prevent it from reconnecting. Select **Save Changes**. The device is removed from the **Connected** list and appears in the **Blocked** list below. **NOTE:** This option is available for each device connected through Wi-Fi but is not available for your own device or devices connected via Ethernet or USB.

To view details on a device or change the name of the device as it appears in this web UI, click the **down arrow** on the right to expand the device row. The following information appears:

- **Name:** To change how the device name appears in this UI, enter a different name.
NOTE: This only changes the device name in the UI in which it is changed.
- **IPv4:** The IP address of the connected device.
- **MAC Address:** The MAC Address (unique network identifier for this connected device).
- **Link Local:** The Link-Local IPv6 address if the connected device supports IPv6.

Click the **up arrow** to collapse the row.

Blocked

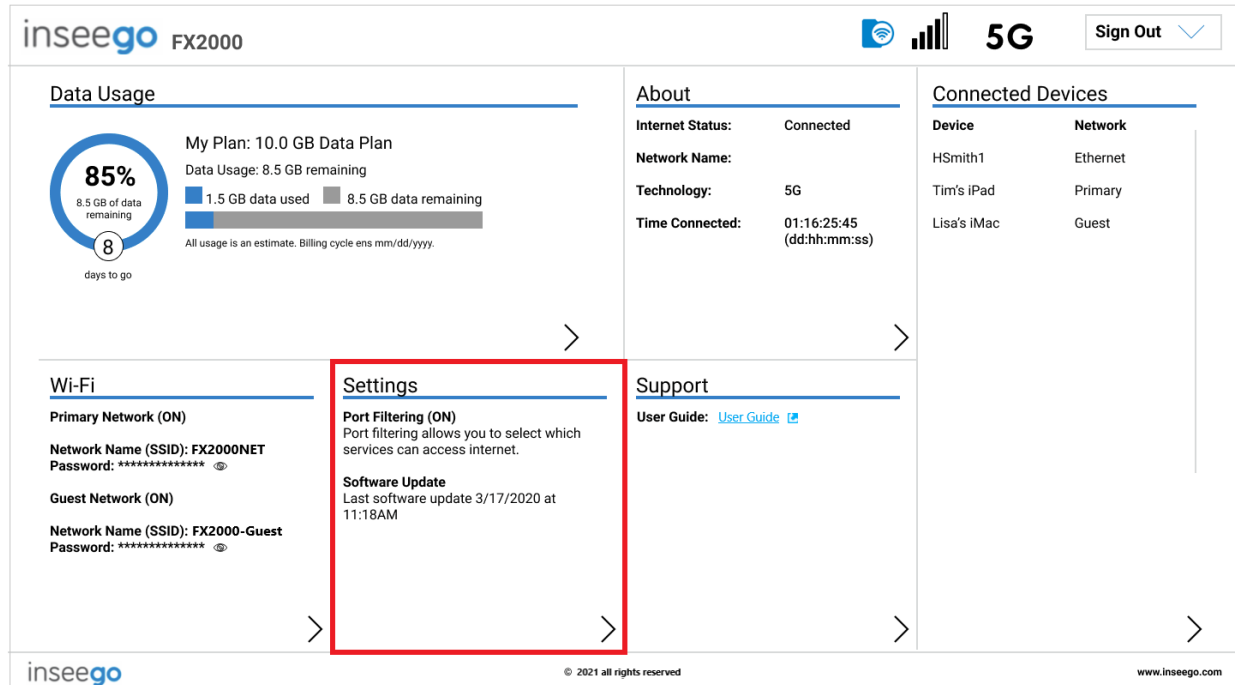
This section lists all devices blocked from connecting to the 5G indoor router.

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

To unblock a blocked device, uncheck the **Block** checkbox and select **Save Changes**. The device is removed from the **Blocked** list and appears in the **Connected** list above.

Managing settings

On the Admin web UI home page, the Settings panel shows Port Filtering and the date and time of the last software update.



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
- VPN
- GPS
- Advanced

Preferences tab

This tab allows you to disable Ethernet on your FX2000 and change how dates, time, and numbers are displayed in the FX2000 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.

The screenshot shows the 'inseeo FX2000' web interface. At the top, there's a status bar with a Wi-Fi icon, signal strength bars, '5G', and a 'Sign Out' button. The main navigation menu on the left includes 'Home', 'Data Usage', 'Wi-Fi', 'Connected Devices', 'Settings' (highlighted), 'About', and 'Support'. The 'Settings' section has tabs for 'Preferences', 'Software Update', 'Backup and Restore', 'VPN', 'GPS', and 'Advanced'. The 'Preferences' tab is active, showing the following settings:

- Device Name:** A text input field containing 'inseeo'.
- Enable Ethernet:** A checkbox that is checked.
- Enable Reboot:** A checkbox that is checked.
- Language:** A dropdown menu set to 'English'.
- Date:** A dropdown menu set to 'mm/dd/yy'.
- Time:** A dropdown menu set to '12 hr'.
- Distance:** A dropdown menu set to 'ft (US)'.
- Number format:** A dropdown menu set to '3,234.00'.

A blue 'Save Changes' button is located at the bottom of the settings list.

Device Name: The device name that defines the device network and URL to access the FX2000 local web UI. **NOTE:** Depending on your service provider, this selection may be read-only.

Enable Ethernet: Ethernet is enabled by default. Uncheck the checkbox if you want to disable connection to your FX2000 via Ethernet.

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

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).

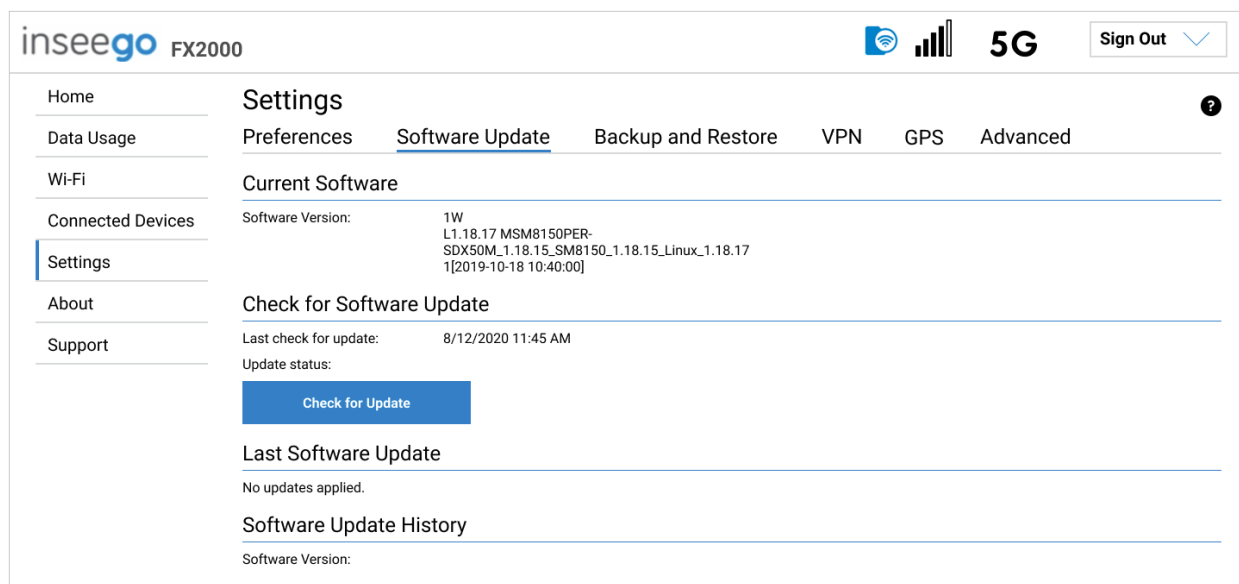
Distance: Select the format for distance displayed in the web UI (feet or meters).

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

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

Software Update tab

Software updates are delivered to the 5G indoor router 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 5G indoor router.

Check for Software Update

Last check for update: The date and time the FX2000 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 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 5G indoor router settings to a file on your computer, restore (upload) a previously saved configuration file, reset the FX2000 to factory defaults, or restart the FX2000.

The screenshot shows the 'inseeego FX2000' web interface. The top navigation bar includes the logo, 'FX2000', signal strength indicators, '5G', and a 'Sign Out' button. A left sidebar lists navigation options: Home, Data Usage, Wi-Fi, Connected Devices, Settings (highlighted), About, and Support. The main content area is titled 'Settings' and has sub-tabs: Preferences, Software Update, Backup and Restore (active), VPN, GPS, and Advanced. The 'Backup and Restore' section is divided into three parts: 1. 'Backup Configurations' with instructions to save settings, an 'Admin Password' field with a note about lockouts, and a blue 'Download' button. 2. 'Restore Settings' with instructions to restore from a file, an 'Admin Password' field, a file selection area showing 'No file selected' and a 'Browse' button, and a blue 'Restore Now' button. 3. 'Restore to Factory Defaults' with instructions to reset to defaults and a blue 'Restore Factory Defaults' button. 4. 'Restart Device' with instructions to restart and a blue 'Restart' button.

Backup Configurations

To back up current 5G indoor router settings to a file on your computer, enter your Admin password in the **Admin Password** field.

The default Admin password is printed on the bottom of the FX2000. 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 FX2000.

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 5G indoor router.

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 5G indoor router, 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. This may change the current Wi-Fi settings, breaking all existing connections to the FX2000 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 5G indoor router.

Click the **Restore Now** button.

Restore to Factory Defaults

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

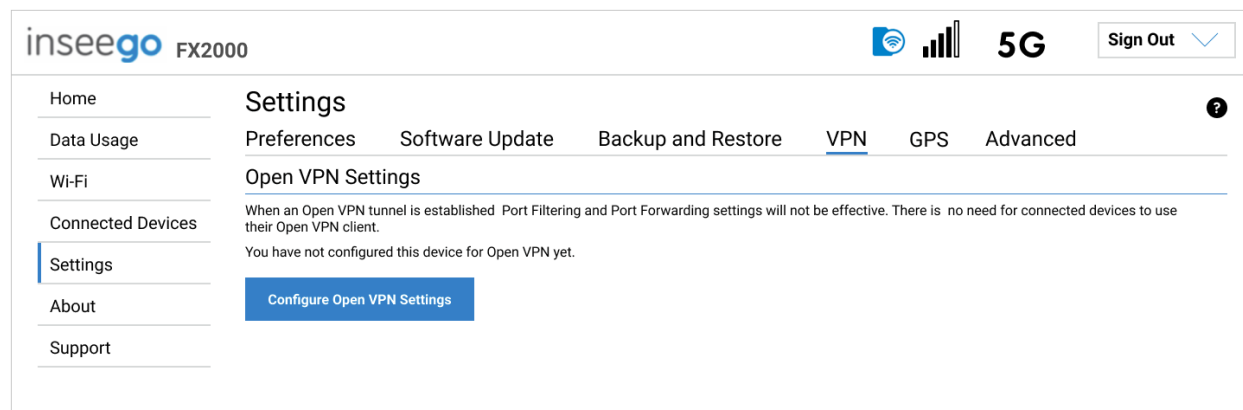
CAUTION! This initiates a restart and may change the current Wi-Fi settings, breaking all existing connections to your FX2000 and disconnecting you from the Admin web UI.

Restart Device

Restart: This button turns your 5G indoor router off and on again.

VPN tab

The 5G indoor router allows you to establish secure connections to remote networks over a public network using Open VPN.



NOTE: When an Open VPN connection is established, Port Filtering and Port Forwarding settings are not effective, as traffic from all connected devices goes through the Open VPN tunnel.

To configure a VPN connection, click **Configure Open VPN Settings**.

The screenshot shows a 'Configure Open VPN Settings' dialog box with a close button (X) in the top right corner. Inside the dialog, there are several fields and controls: 'Open VPN Configuration Files:' with a text box containing the instruction 'Drag and drop files from your Open VPN provider here.'; 'Username:' with a text input field; 'Password:' with a text input field; and 'Auto-connected VPN:' with an information icon (i) and a toggle switch currently in the 'OFF' position. At the bottom of the dialog, there are two buttons: 'Clear all Open VPN Settings' and 'Save Changes and Connect'.

Open VPN Configuration Files: Drag and drop the Open VPN configuration files from your Open VPN provider in the file upload area.

Username: Enter your Open VPN connection username here.

Password: Enter your Open VPN connection password here.

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

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

Click **Save Changes and Connect** to save your configurations and connect to the VPN server.

VPN Connection

This section is visible once you have configured your FX2000 for Open VPN.

Connection status: Indicates the status of the Open VPN connection.

Connection time: The duration of the current Open VPN connection.

View Logs: Use this button to view Open VPN log files.

Connect: Use this button to connect the Open VPN.

GPS tab

The 5G indoor router incorporates a GPS receiver. The GPS receiver can determine your current location. Use this tab to enable GPS, view current location information, and to enable GPS streaming to devices with the GPS over Wi-Fi feature.

The screenshot shows the inseeo FX2000 web interface. At the top, there's a header with the inseeo logo, 'FX2000', and status icons for Wi-Fi, signal strength, and 5G, along with a 'Sign Out' button. A left sidebar contains navigation links: Home, Data Usage, Wi-Fi, Connected Devices, Settings (highlighted), About, and Support. The main content area is titled 'Settings' and has sub-tabs: Preferences, Software Update, Backup and Restore, VPN, GPS (selected), and Advanced. Under the 'GPS Settings' section, there's a description: 'The GPS receiver can determine your current location. This location can be provided to connected devices.' Below this are three toggle switches: 'Enable GPS:' (turned ON), 'Turn off GPS when the device restarts:' (turned OFF), and 'Turn off GPS over Wi-Fi:' (turned OFF). There's a text input field for 'Port Number:' with the value '11010'. A blue 'Save Changes' button is below these settings. At the bottom, the 'Current Location' section displays four fields: Latitude (xxxxxxx), Altitude (xxxxxxx), Longitude (xxxxxxx), and Accuracy (xxxxxxx).

GPS Settings

Enable GPS: This setting enables or disables the GPS radio on your 5G indoor router. 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 FX2000 is shut down. You will need to turn it on again the next time the GPS receiver is needed.

Turn off GPS over Wi-Fi: GPS over Wi-Fi allows you to share location information with connected devices. Raw GPS data is provided in the form of a National Marine Electronics Association (NMEA) text stream. You can use third-party applications to utilize or forward the GPS data to a remote server. When the **ON/OFF** slider is **ON**, location information is **NOT** shared.

Port Number: The TCP port number used to establish a connection to the FX2000 and obtain raw GPS data for the GPS over Wi-Fi feature. Unless there is a good reason to do so, you should not change the port number. Acceptable port values are between 1024 and 65535.

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.

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 51.

Viewing info about the FX2000

On the Admin web UI home page, the About panel shows current Internet status, the network name, technology used, and the amount of time connected.

The screenshot displays the inseeo FX2000 Admin web UI. The top navigation bar includes the inseeo logo, 'FX2000', a 5G signal indicator, and a 'Sign Out' button. The main content area is divided into several panels:

- Data Usage:** Shows a circular progress indicator at 85% (8.5 GB of data remaining). Text indicates 'My Plan: 10.0 GB Data Plan', 'Data Usage: 8.5 GB remaining', and '1.5 GB data used / 8.5 GB data remaining'. A note states 'All usage is an estimate. Billing cycle ends mm/dd/yyyy.' and '8 days to go'.
- About (highlighted with a red box):** Displays the following information:
 - Internet Status: Connected
 - Network Name:
 - Technology: 5G
 - Time Connected: 01:16:25:45 (dd:hh:mm:ss)
- Connected Devices:** A table listing connected devices and their network types:

| Device | Network |
|-------------|----------|
| HSmith1 | Ethernet |
| Tim's iPad | Primary |
| Lisa's iMac | Guest |
- Wi-Fi:** Shows settings for Primary Network (ON) and Guest Network (ON), including Network Name (SSID) and Password.
- Settings:** Includes Port Filtering (ON) and Software Update information (Last software update 3/17/2020 at 11:18AM).
- Support:** Provides a link to the User Guide.

The footer contains the inseeo logo, copyright notice '© 2021 all rights reserved', and the website 'www.inseeo.com'.

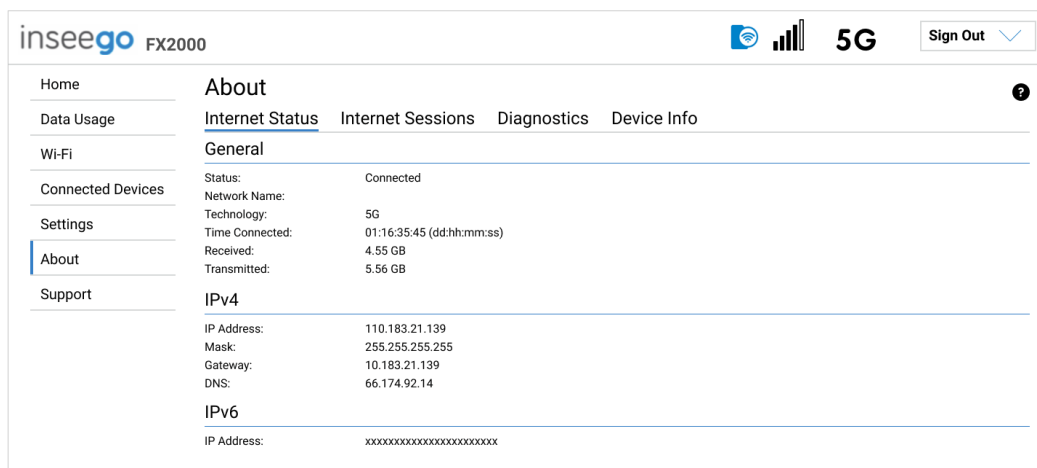
To view more detailed information about your 5G indoor router and its use, select ➤ from the home page About panel or select **About** from the side menu.

The About page includes the following tabs:

- Internet Status
- Internet Sessions
- Diagnostics
- Device Info

Internet Status tab

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



General

Status: The current status of the FX2000 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 FX2000.

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 FX2000.

IPv6

IP Address: The global IPv6 address for the FX2000 (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.

The screenshot shows the inseeo FX2000 web interface. At the top, there's a header with the inseeo logo, 'FX2000', and icons for Wi-Fi, cellular signal, and 5G. A 'Sign Out' button is in the top right. A left sidebar contains navigation links: Home, Data Usage, Wi-Fi, Connected Devices, Settings, About (highlighted), and Support. The main content area is titled 'About' and has sub-tabs: Internet Status, Internet Sessions (selected), Diagnostics, and Device Info. Below these is the heading 'Export Internet Sessions Information' and a blue 'Export' button. A note states: 'Note: Internet Session information should not be used to estimate or monitor data usage during your billing cycle. To view estimated data usage go to the Data Usage page.' Below the note, it says 'Internet Sessions from 06/10/2020 8:39:48 PM to 06/23/2020 8:41:03 PM'. A table follows with the following data:

| Date/Time | Duration | Received Data | Transmitted Data | Total Data | IPv4 Address | IPv6 Address |
|-----------------------|-------------|---------------|------------------|------------|-----------------|-----------------------------------|
| 01/04/2020 8:39:48 PM | 03:00:48:23 | 394.18 MB | 28.51 MB | 452.69 MB | 173.114.192.255 | 2600:1:b068:e1:c51e:cc1:a21a:b489 |

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.

The screenshot shows the insee FX2000 web interface. At the top, there's a header with the insee logo, 'FX2000', and a 'Sign Out' button. Below the header is a navigation menu with 'Home', 'Data Usage', 'Wi-Fi', 'Connected Devices', 'Settings', 'About', and 'Support'. The 'About' section is expanded, showing 'Internet Status', 'Internet Sessions', 'Diagnostics' (selected), and 'Device Info'. The 'Diagnostics' tab is active, displaying 'Modem' and 'Network' information. The 'Modem' section lists: Mobile Number (MDM): xxxx, IMEI: xxxx, IMEISV: xxxx, FW Version: xxxx, SIM Status: xxxx, and ICCID: xxxx. The 'Network' section lists: Status: Connected, Technology: 5G, Band: B66, n71, Bandwidth: 35MHz, 20MHz, Network Operator: (blank), Signal Strength (RSRP): -95 dBm, and SNR: 12 dB.

| Modem | |
|----------------------|------|
| Mobile Number (MDM): | xxxx |
| IMEI: | xxxx |
| IMEISV: | xxxx |
| FW Version: | xxxx |
| SIM Status: | xxxx |
| ICCID: | xxxx |

| Network | |
|-------------------------|--------------|
| Status: | Connected |
| Technology: | 5G |
| Band: | B66, n71 |
| Bandwidth: | 35MHz, 20MHz |
| Network Operator: | |
| Signal Strength (RSRP): | -95 dBm |
| SNR: | 12 dB |

Modem

Mobile Number (MDN): The phone number of your FX2000.

IMEI: The International Mobile Equipment Identity (IMEI) for your FX2000. This is a 15-digit code used to uniquely identify an individual mobile station. The IMEI does not change when the SIM is changed.

IMEISV: 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 FX2000.

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 (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.

Device Info tab

Use this tab to view details about your FX2000.

The screenshot shows the Inseego FX2000 web interface. At the top, there's a header with the Inseego logo, 'FX2000', and status icons for Wi-Fi, cellular signal, and 5G. A 'Sign Out' button is in the top right. A left sidebar contains navigation links: Home, Data Usage, Wi-Fi, Connected Devices, Settings, About (highlighted), and Support. The main content area is titled 'About' and has sub-tabs: Internet Status, Internet Sessions, Diagnostics, and Device Info (selected). Under 'Device Info', there are two sections: 'General' and 'Software Components'. The 'General' section lists: Manufacturer: Inseego, Model: FX2000-3, Hardware Version: 4, and Device Version: 25. The 'Software Components' section lists: OS Version: 2.501, Modem Firmware Version: SDX55MDR-2.54.1 [2022-01-08 01:16:09], Wi-Fi Firmware Version: 1.0.1.2.193.0, Web UI Version: 2.501, and PRI Version: 182.

| General | |
|------------------|----------|
| Manufacturer: | Inseego |
| Model: | FX2000-3 |
| Hardware Version | 4 |
| Device Version: | 25 |

| Software Components | |
|-------------------------|---------------------------------------|
| OS Version: | 2.501 |
| Modem Firmware Version: | SDX55MDR-2.54.1 [2022-01-08 01:16:09] |
| Wi-Fi Firmware Version: | 1.0.1.2.193.0 |
| Web UI Version: | 2.501 |
| PRI Version: | 182 |

General

Manufacturer: Inseego.

Model: Model of the device.

Hardware Version: The version of hardware for your device.

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

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.

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

web UI Version: The version number for the FX2000 Admin web UI.

PRI Version: The configuration version currently applied to the FX2000.

Getting support

On the Admin web UI home page, the Support panel provides a link to this user guide and basic support information.

The screenshot displays the insee FX2000 Admin web UI. At the top, the 'insee' logo and 'FX2000' model name are on the left, while signal strength, '5G' connectivity, and a 'Sign Out' button are on the right. The main content area is divided into several panels:

- Data Usage:** Shows a circular progress indicator at 85% (8.5 GB of data remaining), a bar chart for 1.5 GB data used and 8.5 GB data remaining, and a 'My Plan: 10.0 GB Data Plan' summary.
- About:** Displays 'Internet Status: Connected', 'Network Name', 'Technology: 5G', and 'Time Connected: 01:16:25:45 (dd:hh:mm:ss)'.
- Connected Devices:** A table listing devices and their network types.
- Wi-Fi:** Shows 'Primary Network (ON)' and 'Guest Network (ON)' with their respective SSIDs and passwords.
- Settings:** Includes 'Port Filtering (ON)' and 'Software Update' status.
- Support:** Highlighted with a red border, it contains a 'User Guide' link.

| Device | Network |
|-------------|----------|
| HSmith1 | Ethernet |
| Tim's iPad | Primary |
| Lisa's iMac | Guest |

| |
|--|
| User Guide: User Guide |
|--|

To view more support information, select ➤ from the home page Support panel or select **Support** from the Admin web UI side menu.

Customer Support tab

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

The screenshot shows the inseeo FX2000 web interface. At the top, there's a header with the inseeo logo, 'FX2000', signal strength bars, '5G', and a 'Sign Out' button. On the left is a navigation menu with links: Home, Data Usage, Wi-Fi, Connected Devices, Settings, About, and Support (which is highlighted). The main content area is titled 'Customer Support'. Under 'Your Device', it lists: Model: FX2000, Your Wireless Number: 0-000-000-0000, User Guide: FX2000 User Guide, and Manufacturer: www.inseeo.com. Below this is a section titled 'Customer Support' with the text 'Please contact your service provider or reseller.' and a blue 'Unlock Device' button.

Your Device

Model: Model of the device.

Your Wireless Number: The phone number associated with your FX2000.

User Guide: A link to this User Guide.

Manufacturer: A link to the Inseeo website.

Customer Support

Contact your service provider or reseller for customer support.

The **Unlock/Lock Device** button is available on some devices, depending on service provider. Locked devices can only use the network currently provided by the service provider.

To unlock a locked device, click **Unlock Device**.

The screenshot shows the inseeo FX2000 web interface for the 'Network Unlock' page. The header is identical to the previous screenshot. The navigation menu is the same, with 'Support' highlighted. The main content area is titled 'Network Unlock'. It states 'Your device is network locked.' and provides instructions: 'You can [submit an unlock request](#) yourself or contact Customer Care at 1-800-000-0000'. It also displays: Device IMEI: 9900 1310 0005 888, Mobile Number: 858 337 5121, and Network Code: [input field]. There is a blue 'Submit Code' button. At the bottom, there is a link 'Return to Customer Support'.

To obtain a network code, click the **submit an unlock request** link, or follow the directions to contact your service provider. Enter the code in the **Network Code** text box and click **Submit Code**.

To lock a device so that it can only use the current network, click **Lock Device** and then **Okay**.

3

Advanced settings

Overview

Using advanced settings

Overview

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 5G indoor router FX2000.

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
- SIM
- Firewall
- MAC Filter
- LAN
- WAN Settings (Inseego Connect only)
- Port Filtering
- Port Forwarding
- Inseego Connect

Cellular tab

In most configurations, the FX2000 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 FX2000.

The screenshot shows the inseeego FX2000 web interface. At the top, there's a header with the inseeego logo, 'FX2000', a signal strength indicator, '5G', and a 'Sign Out' button. A left sidebar contains navigation links: Home, Data Usage, Wi-Fi, Connected Devices, Settings (highlighted), About, and Support. The main content area is titled 'Settings' and has several tabs: Preferences, Software Update, Backup and Restore, VPN, GPS, and Advanced (selected). Under the 'Advanced' tab, there are sub-tabs: Cellular, Manual DNS, SIM, Firewall, MAC Filter, LAN, Port Filtering, Port Forwarding, and Inseeego Connect. The 'Cellular' sub-tab is active, showing 'Cellular Network Technology' settings. These include: 'Allow device to connect to the mobile network' (ON), 'Allow device to connect to the mobile network when roaming' (ON), 'Network Technology' (Auto (4G LTE/5G)), '5G Network Mode' (NSA), and 'Enable automatic network selection' (ON). A 'Select a Different Network' button is below. The 'APN Settings' section includes fields for APN (Add APN), Add APN (fbb.home), Authentication (None), and PDP (IPv6v4). A caution note states: 'Caution: Changing the APN may cause loss of data connectivity.' A 'Save Changes' button is at the bottom.

Cellular Network Technology

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. This prevents connected devices from connecting to the Internet and using your FX2000 mobile data plan. For normal operation, this setting must be left on.

Allow device to connect to the mobile network while roaming: Use the **ON/OFF** slider to turn off cellular data and prevent access to the mobile network when roaming.

Network Technology: Your FX2000 is set to Auto (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 FX2000 is restricted from connecting to networks not using that technology, for example: if you select 4G LTE, your FX2000 will be unable to connect to 5G networks.

5G Network Mode: Your FX2000 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 non-standalone (NSA) or standalone (SA) 5G network modes.

Enable automatic network selection: When the **ON/OFF** slider is **ON**, your FX2000 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. 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.

APN Settings

APN: 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.

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

NOTE: The following APN fields are optional. Information entered in these fields should come from your service provider based on network requirements.

Username: Enter the username for your private network.

Password: Enter the password for your private network.

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

PDP: Select a type of Packet Data Protocol (PDP) from the drop-down (IPv4, IPv6, or IPv4/IPv6).

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

Manual DNS tab

The FX2000 automatically selects a Domain Name Server (DNS). This page allows you to manually assign up to two DNS IP addresses.

The screenshot shows the inseeogo FX2000 web interface. At the top, there's a header with the inseeogo logo, 'FX2000', and status icons for Wi-Fi, cellular signal, and 5G. A 'Sign Out' button is in the top right. A left sidebar contains navigation links: Home, Data Usage, Wi-Fi, Connected Devices, Settings (highlighted), About, and Support. The main content area is titled 'Settings' and has sub-tabs: Preferences, Software Update, Backup and Restore, VPN, GPS, and Advanced (selected). Under the 'Advanced' tab, there are more sub-tabs: Cellular, Manual DNS (selected), SIM, Firewall, MAC Filter, LAN, Port Filtering, Port Forwarding, and Inseeogo Connect. The 'Manual DNS' section is titled 'Manual DNS' and includes the text: 'Your device automatically selects a Domain Name Server (DNS) or you can manually set one.' Below this, there's a checkbox for 'Turn on manual DNS:' which is checked. Two input fields follow: 'DNS 1 IP address:' and 'DNS 2 IP address:', both with placeholder text 'Required (IPv4 or IPv6 address)'. A blue 'Save Changes' button is at the bottom.

Manual DNS

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

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

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

Click **Save Changes**.

SIM tab

The SIM card in your 5G indoor router 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.

Use this page to unlock your SIM or enter a SIM PIN.

inseeo FX2000

Sign Out

Home

Data Usage

Wi-Fi

Connected Devices

Settings

About

Support

Settings

Preferences Software Update Backup and Restore VPN GPS Advanced

Cellular Manual DNS SIM Firewall MAC Filter LAN Port Filtering Port Forwarding Inseeo Connect

For additional security, the SIM card can be locked with a PIN code. When locked, the PIN code must be entered before the device will connect to the internet.

• SIM PIN lock: Off

• SIM status: Ready

Desired action: Turn on PIN lock

• Current PIN:

x attempts remain until your SIM is PUK locked.

Note: Entering an incorrect PIN too often will PUK lock your SIM and you will be unable to use the device. You will need to contact <carrier> customer support to unlock the SIM.

Save Changes

SIM PIN lock: The status of the SIM PIN lock.

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

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

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

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.

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

Click **Save Changes**.

Firewall tab

The FX2000 firewall determines which Internet traffic is allowed to pass between the FX2000 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.

The screenshot shows the inseeogo FX2000 web interface. At the top, there's a header with the logo, 'FX2000', and status icons for Wi-Fi, cellular signal, and 5G, along with a 'Sign Out' button. A left sidebar contains navigation links: Home, Data Usage, Wi-Fi, Connected Devices, Settings (highlighted), About, and Support. The main content area is titled 'Settings' and has sub-tabs: Preferences, Software Update, Backup and Restore, VPN, GPS, and Advanced (selected). Under the 'Advanced' tab, there are sub-sections: Cellular, Manual DNS, SIM, Firewall (selected), MAC Filter, LAN, Port Filtering, Port Forwarding, and Inseeo Connect. The 'Firewall' section includes three main settings: 'VPN Passthrough' with a toggle switch turned ON, 'WAN Ping Enablement' with a toggle switch turned OFF, and 'DMZ' with an unchecked checkbox and a 'Destination IP address' input field. A blue 'Save Changes' button is located at the bottom of the settings area.

NOTE: When IP Passthrough is turned on, firewall 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.

VPN Passthrough

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

WAN Ping Enablement

By default, the FX2000 will ignore ping requests received on the WAN interface. To enable your FX2000 to respond to the ping requests received on the WAN interface, move the ON/OFF slider to **ON**.

DMZ

NOTE: 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.

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

Allowing DMZ may assist some troublesome network applications to function properly, but the DMZ device should have its own firewall to protect itself against malicious traffic.

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

Click **Save Changes**.

MAC Filter tab

The MAC filter allows only selected devices to access the FX2000 network through DHCP. By default, MAC filter is turned off.

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

inseeego FX2000

Home Data Usage Wi-Fi Connected Devices **Settings** About Support

Settings Preferences Software Update Backup and Restore VPN GPS **Advanced**

Cellular Manual DNS SIM Firewall **MAC Filter** LAN Port Filtering Port Forwarding Inseeego Connect

This MAC filter lets you limit access to the Primary Wi-Fi network to devices you choose. Select from the list below (you can also add new devices), then turn the MAC filter on.

To use the MAC filter:

1. Select the device you would like to filter, or add your own to the list below.
2. Click the 'Save Changes' button.
3. Toggle the switch to enable MAC filtering.

Note: The MAC filter doesn't affect the Guest Wi-Fi network.

MAC Filter: ☐

| Name | MAC Address | Status | MAC Address Filter | Delete |
|---------|-------------------|--------|-------------------------------------|--------------------------|
| HSmith1 | XX:XX:XX:XX:XX:XX | | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Add New Device Refresh List Save Changes

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 FX2000.

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**.

LAN tab

This page provides settings and information about the FX2000 local area network (LAN). The LAN consists of the device and all connected devices.

inseeo FX2000

Home Data Usage Wi-Fi Connected Devices **Settings** About Help

Settings

Preferences Software Update Backup and Restore VPN GPS Advanced

Cellular Manual DNS SIM Firewall MAC Filter LAN Port Filtering Port Forwarding Inseeo Connect

IP Passthrough

If enabled, one device (the first device detected) on the selected interface will obtain the Internet IP address assigned by the mobile network. All other devices will lose Internet access. Note: this applies for IPv4 connections only.

Turn on IP Passthrough: ☐

IPPT Interface: Ethernet

IPv4

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

MAC Address: 28:80:a2:f2:9d:d3

Turn on DHCP Server: ☒

DHCP Lease Time: 1440 minutes

Start DHCP Address Range at: 192.168.1.2

End DHCP Address Range at: 192.168.1.102

IPv6

Turn on IPv6: ☒

Link-Local Address: fe80:f883:9bff:fe68:2702

Local Web Management URL

URL Name: http://inseeo.local

Save Changes

IP Passthrough

NOTE: IP Passthrough may not be visible/available, depending on your service provider.

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, only one device will have internet access. All other connected devices will be disconnected and lose internet access. The following capabilities are set through the host routing system and web UI settings are not available:

- Primary and Guest Wi-Fi networks
- Firewall
- Port Filtering
- Port Forwarding

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

IPPT Interface: Select an interface from the drop-down (Ethernet or USB). Make sure a cable is only connected to the interface you select. **NOTE:** When IPPT is enabled on an interface, all other interfaces are disabled.

IPv4

IP Address: The IP address for your FX2000, as seen from the local network. Normally, you can use the default value.

Subnet Mask: The subnet mask network setting for the FX2000. 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 FX2000. 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.

Local Web Management URL

URL Name: The URL name used to access the FX2000 local web UI.

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

WAN

NOTE: WAN settings are available only with Inseego Connect.

Use this page to enable and configure WAN keepalive. Keepalive allows for a persistent WAN connection.

| Configure | |
|-----------------------|--|
| WAN | |
| Enable WAN Keep Alive | <input checked="" type="checkbox"/> |
| Lookup Address 1 * | <input type="text" value="www.google.com"/> |
| Lookup Address 2 * | <input type="text" value="www.yahoo.com"/> |
| Lookup Address 3 * | <input type="text" value="www.inseego.com"/> |
| Keep Alive Interval * | <input type="text" value="86400"/> (seconds) |
| Number Of Attempts * | <input type="text" value="3"/> |
| Retry Interval * | <input type="text" value="10"/> (seconds) |

☐ Schedule later

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

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

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

Lookup Address 3: Enter the third DNS IP address to verify (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 keepalive 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.

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.

inseeego FX2000

5G Sign Out

Home Settings

Data Usage Preferences Software Update Backup and Restore VPN GPS Advanced

Wi-Fi Cellular Manual DNS SIM Firewall MAC Filter LAN Port Filtering Port Forwarding Inseego Connect

Connected Devices

Settings

About

Support

Port Filtering Configuration

If Port Filtering is on, only traffic from selected applications can access the internet.
Note: DNS is always allowed.

Port Filtering: ☐

Applications

Select which applications can access the internet.

- ☐ Email (POP3, IMAP, SMTP)
- ☐ FTP
- ☐ HTTP
- ☐ HTTPS
- ☐ Telnet

Custom Applications

You can define your own applications, and then turn them off or on as needed. To define an application, you need to know the outgoing ports used by the application.

| On | App Name | Start Port | End Port | Protocol | Delete |
|-------------------------------------|----------|------------|----------|----------|--------------------------|
| <input checked="" type="checkbox"/> | App 1 | | | TCP | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | App 1 | | | TCP | <input type="checkbox"/> |

Add Custom Application Save Changes

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

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.

The screenshot shows the 'inseeego FX2000' web interface. The top navigation bar includes 'Sign Out' and a '5G' signal indicator. The left sidebar lists navigation options: Home, Data Usage, Wi-Fi, Connected Devices, Settings (selected), About, and Support. The main content area is titled 'Settings' and contains tabs for 'Preferences', 'Software Update', 'Backup and Restore', 'VPN', 'GPS', and 'Advanced'. The 'Advanced' tab is active, showing 'Port Forwarding Configuration'. A toggle for 'Port Forwarding' is currently off. Below this, a list of applications (DNS, FTP, HTTP/HTTPS, NNTP, POP3/POP3S, SMTP, SNMP, Telnet, TFTP) is shown, each with an 'Application IP Address' field. The 'Custom Applications' section allows defining new applications with columns for 'On', 'App Name', 'IP Address', 'Port Type', 'Port Numbers', 'Protocol', and 'Delete'. Two custom applications are listed, both with 'App 1' as the name and 'TCP' as the protocol. The 'Add Custom Application' button is visible at the bottom.

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) | 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

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.

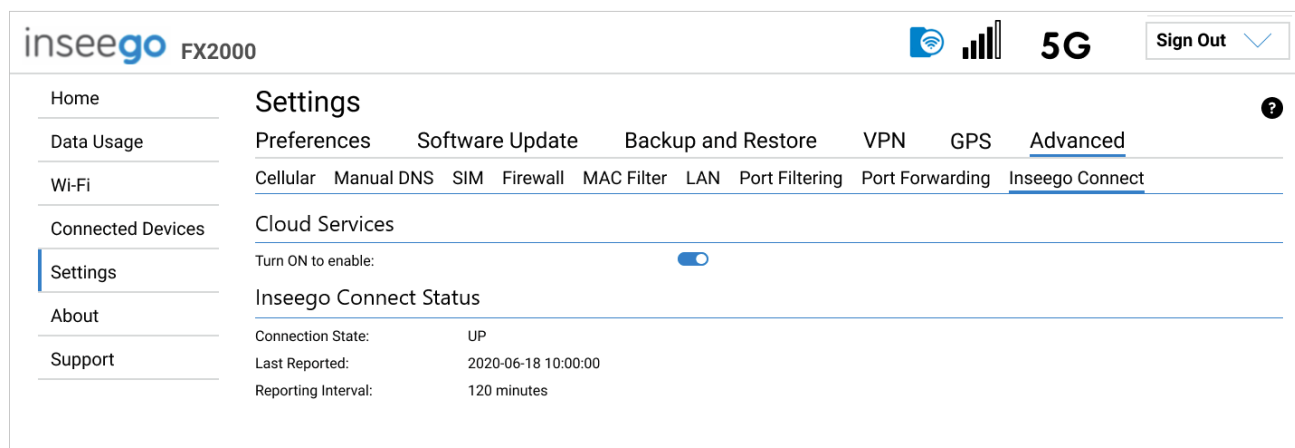
Protocol: Select the protocol used by the port range from the drop-down list (TCP, UDP, or both).

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

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 cloud services 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** – FX2000 is communicating with Inseego Connect servers.
- **DOWN** – FX2000 is NOT communicating with Inseego Connect servers.

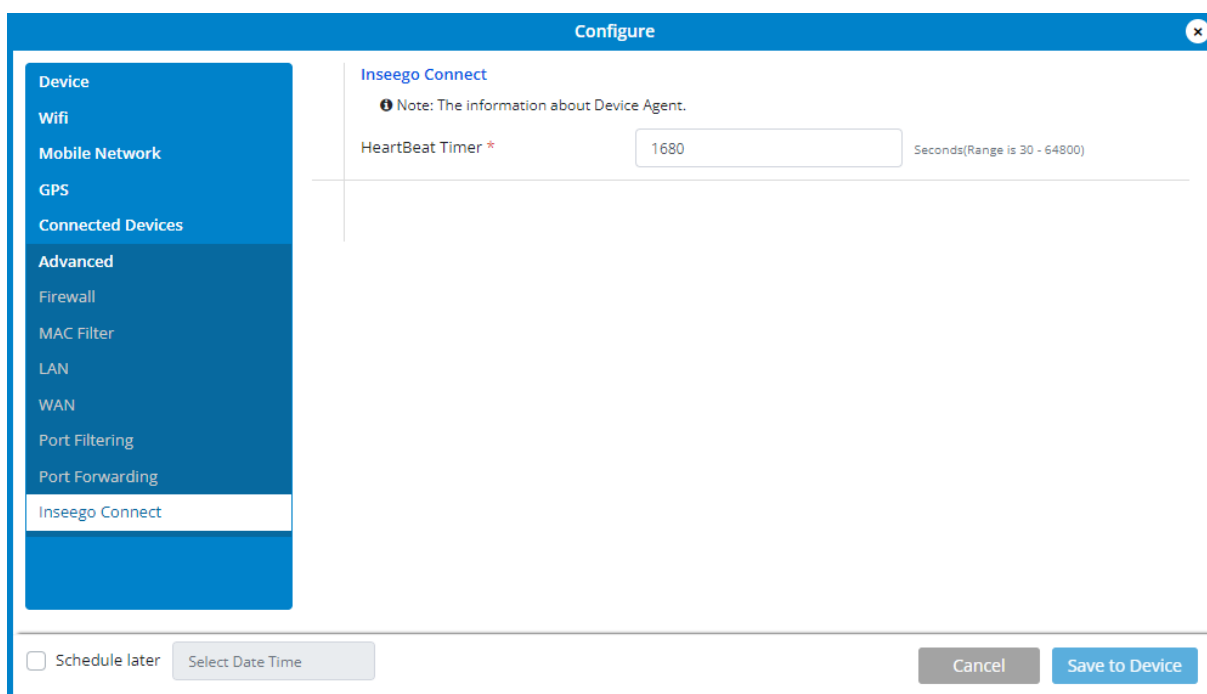
Last Reported: The time when FX2000 last sent a packet to Inseego Connect servers.

Reporting Interval: This is the interval at which your FX2000 will send packets to the Inseego Connect server. **NOTE:** A shorter interval means more data usage.

Inseego Connect

Your FX2000 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.



The screenshot shows a web-based configuration interface for a device. The title bar at the top is blue and says "Configure" with a close button (X) on the right. On the left is a blue sidebar menu with the following items: "Device", "Wifi", "Mobile Network", "GPS", "Connected Devices", "Advanced", "Firewall", "MAC Filter", "LAN", "WAN", "Port Filtering", "Port Forwarding", and "Inseego Connect" (which is highlighted in white). The main content area has a blue header "Inseego Connect". Below it is a note: "Note: The information about Device Agent." followed by a "HeartBeat Timer *" field containing the value "1680". To the right of the field is the text "Seconds(Range is 30 - 64800)". At the bottom of the main area, there is a checkbox labeled "Schedule later" next to a "Select Date Time" button. On the far right are two buttons: "Cancel" and "Save to Device".

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

Click **Save to Device**.

4

Troubleshooting and support

Overview

Common problems and solutions

Technical support

Overview

When properly installed, the 5G indoor router is a highly reliable product.

The following tips can help solve many common problems encountered while using the 5G indoor router:

- Make sure you are using the 5G indoor router in the correct geographic region.
- Ensure that your wireless coverage extends to your current location.
- If you do not receive a strong data signal, move the device to a different location.
- Ensure that you have an active subscription plan.
- You can resolve many issues by restarting your connected device and your 5G indoor router.

Troubleshooting

This section can help solve many common problems and answer questions encountered while using the FX2000.

I cannot access the Admin web UI

- **Reason:** You are on the guest network. The web UI is not accessible from the guest Wi-Fi network by design.

Solution: Connect to the primary network, by USB or Ethernet.

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 connected a second device to your FX2000 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 FX2000, you must first disconnect the existing connected device and power cycle the FX2000 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 FX2000 to factory settings, see “Resetting your FX2000” on page 14.
or

Use Inseego Connect or Inseego Mobile LAN settings to turn the DHCP server on.

- **Reason:** The DHCP server has used all of its IP addresses.
This is unlikely to happen with the FX2000, but if you have connected a succession of devices to your FX2000 in a short period of time, you may have used up all of the IP address available.

Solution: Disconnect your connected device and power cycle the FX2000 before reconnecting a device.

- **Reason:** There is an issue with your FX2000.

Solution: Contact your service provider for assistance.

I see other networks, but not the network name for my FX2000

- **Reason:** The default multi-mode settings on your FX2000 work for most Wi-Fi clients, however, some older devices require that you set one of the Wi-Fi bands to support older BGN standards.

Solution: Set your 2.4 GHz band to **802.11 bgn**:

1. Access the FX2000 Admin web UI and navigate to **Wi-Fi > Settings**. Under **2.4 GHz Band Settings**, use the drop-down to change the 802.11 mode to **802.11 bgn**.
NOTE: This allows older devices to connect on the 2.4 GHz band but leaves the 5 GHz band in multi-mode to allow newer devices the fastest available connection.
2. Click **Save Changes**. Your FX2000 will reboot, and the network name should be visible on all devices.

I see the network name, but cannot connect a device to my FX2000

- **Reason:** The default network security settings on your FX2000 work for most Wi-Fi clients, however, some older devices may not have access.

Solution: Contact your service provider for assistance. If you are entering the correct password and still unable to connect, change the network security setting to **WPA/WPA2 Mixed Mode**:

1. Access the FX2000 Admin web UI and navigate to **Wi-Fi > Primary Network**. In the **Security** drop-down, select **WPA/WPA2 Mixed Mode**.

2. Click **Save Changes** and **Confirm**. Your FX2000 will reboot, and all devices should be able to connect.

I cannot register my FX2000 with Inseego Connect or Inseego Mobile app

- **Reason:** Some service providers sell the FX2000 already registered with Inseego Connect and/or Inseego Mobile.

Solution: Contact your service provider for assistance.

I cannot get streaming platforms to work with my FX2000

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

Solution: Contact your service provider for assistance.

My FX2000 is getting slow speeds/low throughput

- **Reason:** Signal strength and quality are the most likely cause of slow speeds/low throughput. **NOTE:** The FX2000 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 FX2000:

1. Access the FX2000 Admin web UI and navigate to **About > Diagnostics** to check the values for **Signal Strength (RSRP)** and **SNR**.
2. **If the signal is poor**, relocate your FX2000 to improve signal conditions.

If the signal is good, but throughput is slow, check your service provider's network conditions for outages and expected performance.

Do I need an external antenna?

The external TS9 antenna ports on your FX2000 are used for high sub-6 bands (3.4GHz-5GHz). These frequencies are used for CBRS or C-band, which are not often used. If you are not using these bands, there is no benefit to attaching external antennas to your FX2000.

The external antenna ports support the following bands:

- **B42** - 3550-3700 MHz (US and Canada)
- **B48** - 3550-3700 MHz (US)
- **n77** – 3700-3980 MHz (US)
- **n78** - 3450-3650 MHz (Canada)

Do I need a signal amplifier or booster?

Inseego does not recommend or support the use of cellular signal amplifiers or boosters.

Cellular signal amplifiers/boosters typically work by receiving and re-transmitting specific frequencies. This can increase the amount of signal noise, which has a negative effect on connectivity. In addition, when specific frequencies are targeted, other frequencies can be effectively filtered or blocked. If not all of your needed bands are supported, you may experience a worse connection.

Does the USB port support RNDIS?

You can use the USB port on the back of your FX200 to provide a network connection via Remote Network Driver Interface Specification (RNDIS). Most major operating systems support RNDIS. There are no device-specific drivers for the USB port, so any drivers needed are related to the PC operating system.

Does the USB port support USB-C to Ethernet adapters?

The USB port does not support USB-C to Ethernet adapters. If you require additional Ethernet ports, Inseego recommends using an Ethernet switch connected to the Ethernet port.

Technical Support

IMPORTANT: Before contacting Support, be sure to restart both your connected device and your 5G indoor router and ensure that your SIM card is inserted correctly.

Customer Service and Troubleshooting

Contact your service provider for assistance.

More Information

Documentation for your 5G indoor router FX2000 is available online. Go to www.inseego.com/support-documentation. Or, from the Admin website, select **Help >**

Customer 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: | 5G indoor router FX2000 | |
| Model: | FX2000-3 | |
| Regulatory: | FX2000-3 | FCC, ISSED, CE, UKCA, RCM, RSM, CITC, CITRA, ICT, TRA UAE, TRA Bahrain, TRA Oman |
| Standards, approvals, certifications: | GCF, PTCRB Wi-Fi Alliance REACH, RoHS, WEEE | |
| Dimensions: | 160 mm x 71.6 mm x 60 mm (6.3" x 2.8" x 2.4") | |
| Weight: | 350 g (12 oz) | |
| Ports: | 1x LAN 1 Gbps 1x USB 3.1 Type C 2x External antenna (2x2 TS-9) | |
| SIM: | 4FF Nano SIM | |
| Chipset: | Qualcomm® Snapdragon™ SDX55 | |
| LED: | Status | |

Environmental

| | |
|------------------------|------------------------------------|
| Operating temperature: | 0° C to 45° C (32° F to 113° F) |
| Storage temperature: | -30° C to +70° C (-22°F to 158° F) |

Network connectivity^{*}

| |
|--------------------|
| 5G Sub-6 GHz |
| 4G LTE Cat 22 |
| 4x4 MIMO sub-6 GHz |
| 256 QAM sub-6 GHz |
| HSPA+/UMTS |
| CBRS |

^{*} Data plan required. Coverage subject to network availability.

Wi-Fi

802.11 a/b/g/n/ac/ax

Wi-Fi 6 with 2x2 MU-MIMO

Real simultaneous dual-band Wi-Fi

Multiple SSID/guest Wi-Fi support

Supports up to 30 simultaneous Wi-Fi enabled devices

External antenna port bands

External antenna ports support the following bands:

| Band | Frequency range | Country |
|------|-----------------|---------------|
| B42 | 3550-3700 MHz | US and Canada |
| B48 | 3550-3700 MHz | US |
| n77 | 3700-3980 MHz | US |
| n78 | 3450-3650 MHz | Canada |

Security

Secure boot

Admin security AES 256 encryption • Security hardened web interface • Password hash • Session timeout • Wi-Fi on/off control • Incorrect password lockout

Encrypted configuration backup/restore

Advanced firewall

Wi-Fi security Wi-Fi security (WPA/WPA2/WPA3) • Wi-Fi protected setup (WPS 2.0) • Wi-Fi privacy separation • Configurable DNS • MAC address filtering • NAT firewall • Port forwarding • Port filtering

Anti CSRF (OWASP)

OpenVPN

Regulatory information

Federal Communications Commission Notice (FCC – United States)

FCC ID: PKRISGFX20003

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.

RF EXPOSURE INFORMATION: This device meets the government's requirements for RF exposure to radio waves. This device is designed and manufactured not to exceed the emissions

limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

This device complies with FCC radiation exposure limits set forth for uncontrolled environments. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal use.

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- FX20003

ISED Notice

This device complies with Innovation, Science and Economic Development Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

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

Le présent appareil est conforme aux CNR 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, et
2. L'utilisateur de 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)

ISED RF Exposure Statement

This device complies with ISED RSS-102 RF exposure limits set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the IC RSS-102 RF exposure

limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

Cet appareil est conforme aux limites d'exposition aux rayonnements de la CNR-102 définies pour un environnement non contrôlé. Afin d'éviter la possibilité de dépasser les limites d'exposition aux fréquences radio de la CNR-102, la proximité humaine à l'antenne ne doit pas être inférieure à 20 cm (8 pouces) pendant le fonctionnement normal.

Cellular external antenna considerations:

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

| Cellular band | Antenna gain (dBi) including cable loss |
|---------------------------------------|--|
| 4G-LTE: B42 (US/CAN) B48 (US only) | 3.5 |
| 5G-FR1: n77 (US only) | 5.5 |
| 5G-FR1: n78 (Canada only) | 11 |



Inseego Corp. declares that FX2000-3 is in Compliance with the Radio Equipment Directive 2014/53/EU, its essential requirements and other relevant provisions of the directive.

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

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

This device is restricted to indoor Use Only when operating in the 5.15-5.35GHz frequency range.

| | | | | | | | |
|--|----|----|----|----|----|----|--------|
| | AT | BE | BG | HR | CY | CZ | DK |
| | EE | FI | FR | DE | EL | HU | IE |
| | IT | LV | LT | LU | MT | NL | PL |
| | PT | RO | SK | SI | ES | SE | UK(NI) |
| | IS | LI | NO | CH | TR | | |

AU/NZ RF radiation exposure guidance statement

This device complies with the requirements of the relevant ACMA Standards made under the Radiocommunications Act 1992 and the Telecommunications Act 1997

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



Inseego Corp. declares that FX2000-3 is in conformity with the Radio Equipment Regulations 2017, its essential requirements and other relevant provisions of the regulation.

A full copy of the UK 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.

Restrictions or Requirements in the UK: 5.15-5.35GHz indoor-use only.

EU/UK RF radiation exposure guidance statement

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

Cellular external antenna considerations:

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

| Cellular band | Antenna gain (dBi) including cable loss |
|----------------------|--|
| 4G-LTE: B42 | 12.5 |
| 5G-FR1: n78 | 12.5 |

Radio frequency and transmitted output power information

| Band | Max power | Frequency |
|--------------|------------------|---------------------|
| LTE BAND B1 | 24 dBm | 1920-1980 MHz |
| LTE BAND B2 | 24 dBm | 1850-1910 MHz |
| LTE BAND B3 | 24 dBm | 1710-1785 MHz |
| LTE BAND B4 | 24 dBm | 1710-1785 MHz |
| LTE BAND B5 | 24 dBm | 824-849 MHz |
| LTE BAND B7 | 24 dBm | 2500-2570 MHz |
| LTE BAND B8 | 24 dBm | 880-915 MHz |
| LTE BAND B11 | 24 dBm | 1427.9 – 1452.9 MHz |
| LTE BAND B12 | 24 dBm | 698-716 MHz |
| LTE BAND B13 | 24 dBm | 777-787 MHz |
| LTE BAND B14 | 24 dBm | 788-798 MHz |
| LTE BAND B17 | 24 dBm | 704-716 MHz |
| LTE BAND B18 | 24 dBm | 815 – 830 MHz |
| LTE BAND B19 | 24 dBm | 830 – 845 MHz |
| LTE BAND B20 | 24 dBm | 832-862 MHz |
| LTE BAND B21 | 24 dBm | 1447.9 – 1462.9 MHz |
| LTE BAND B25 | 24 dBm | 1850-1915 MHz |
| LTE BAND B26 | 24 dBm | 814-849 MHz |
| LTE BAND B28 | 24 dBm | 703-748 MHz |
| LTE BAND B29 | 24 dBm | 717 – 728 MHz |
| LTE BAND B30 | 24 dBm | 2305-2315 MHz |
| LTE BAND B32 | 24 dBm | 1452 – 1496 MHz |
| LTE BAND B38 | 24 dBm | 2570-2620 MHz |
| LTE BAND B39 | 24 dBm | 1880-1920 MHz |
| LTE BAND B40 | 24 dBm | 2300-2400 MHz |
| LTE BAND B41 | 24 dBm | 2496-2690 MHz |
| LTE BAND B42 | 19.5 dBm | 3400-3600 MHz |
| LTE BAND B46 | NA | 5150 – 5925 MHz |
| LTE BAND B48 | 19.5 dBm | 3550-3700 MHz |
| LTE BAND B66 | 24 dBm | 1710-1780 MHz |
| LTE BAND B71 | 24 dBm | 663-698 MHz |
| n1 | 24 dBm | 1920-1980 MHz |
| n2 | 24 dBm | 1850-1910 MHz |
| n3 | 24 dBm | 1710-1785 MHz |

| Band | Max power | Frequency |
|------|-----------|-----------------|
| n5 | 24 dBm | 824–849 MHz |
| n7 | 24 dBm | 2500–2570 MHz |
| n8 | 24 dBm | 880–915 MHz |
| n12 | 24 dBm | 699–716 MHz |
| n25 | 24 dBm | 1850–1915 MHz |
| n28 | 24 dBm | 703–748 MHz |
| n38 | 24 dBm | 2570 – 2620 MHz |
| n40 | 24 dBm | 2300–2400 MHz |
| n41 | 24 dBm | 2496–2690 MHz |
| n46 | 24 dBm | 5150 – 5925 MHz |
| n48 | 24 dBm | 3550 – 3700 MHz |
| n66 | 24 dBm | 1710–1780 MHz |
| n71 | 24 dBm | 663–698 MHz |
| n77 | 24 dBm | 3300 – 4200 MHz |
| n78 | 24 dBm | 3300–3800 MHz |
| n79 | 24 dBm | 4400 – 5000 MHz |
| n83 | 24 dBm | 703 – 748 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 FX2000 power adapter is connected to AC power, but not connected to device.
- **Power adapter efficiency:** Average of the FX2000 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 FX2000 | |
|--------------------------|------------------------------|--------|
| | 115V | 230V |
| Power adapter, no load | 0.03W | 0.065W |
| Power adapter efficiency | 87.03% | 87.39% |

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 FX2000 device, or failure of the FX2000 device to transmit or receive such data.

Limited warranty and liability

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

INSEEGO CORP warrants for the 12-month period (or 24-month period if required by statute where you purchased the Product) immediately following your receipt of the Product that the Product will be free from defects in material and workmanship under normal use. TO THE EXTENT PERMITTED BY LAW, THESE WARRANTIES ARE EXPRESSLY IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The exclusive remedy for a claim under this warranty shall be limited to the repair or replacement, at INSEEGO CORP'S option, of defective or non-conforming materials, parts, components or the device. The foregoing warranties do not extend to (I) non conformities, defects or errors in the Products due to accident, abuse, misuse or negligent use of the Products or use in other than a normal and customary manner, environmental conditions not conforming to INSEEGO CORP'S specification, of failure to follow prescribed installation, operating and maintenance procedures, (II) defects, errors or nonconformities in the Product due to modifications, alterations, additions or changes not made in accordance with INSEEGO CORP'S specifications or authorized by INSEEGO CORP, (III) normal wear and tear, (IV) damage caused by force of nature or act of any third person, (V) shipping damage, (VI) service or repair of Product by the purchaser without prior written consent from INSEEGO CORP, (VII) products designated by INSEEGO CORP as beta site test samples, experimental, developmental, reproduction, sample, incomplete or out of specification Products, or (VIII) returned products if the original identification marks have been removed or altered. There is no warranty that information stored in the Product will be retained following any Product repair or replacement.

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

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

Safety hazards

Do not operate the 5G indoor router 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.

6

Glossary

Glossary

- **4G LTE**—Fourth Generation Long Term Evolution. LTE is a standard for wireless data communications technology and an evolution of the GSM/UMTS standards. The goal of LTE is to increase the capacity and speed of wireless data networks using new DSP (digital signal processing) techniques and modulations that were developed around the turn of the millennium. A further goal is the redesign and simplification of the network architecture to an IP-based system with significantly reduced transfer latency compared to the 3G architecture. The LTE wireless interface is incompatible with 2G and 3G networks, so that it must be operated on a separate wireless spectrum
- **5G**—Fifth Generation. The successor to 4GLTE technology, offering greater bandwidth and higher download speeds. In addition to serving cellular networks, 5G networks can be used as internet service providers, competing with other ISPs. 5G also opens up new IoT and M2M possibilities. Wireless devices must be 5G enabled to use 5G networks.
- **802.11 (a, b, g, n, ax)**—A set of WLAN Wi-Fi communication standards in the 2.4 and 5 GHz frequency bands.
- **APN** — Access Point Name. The name of a gateway between a mobile network and another computer network, often the Internet.
- **bps** — Bits per second. The rate of data flow.
- **Broadband** — High-capacity high-speed transmission channel with a wider bandwidth than conventional modem lines. Broadband channels can carry video, voice, and data simultaneously.
- **DHCP** — Dynamic Host Configuration Protocol. Software found in servers and routers that automatically assigns IP addresses and other configuration data to computers, tablets, printers, and other devices connection to the IP network.
- **DHCP Server** — A server or service with a server that assigns IP addresses.
- **DMZ** — DeMilitarized Zone. A sub-network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.
- **DNS**— Domain Name System. A system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol.
- **Firmware** — A computer program embedded in an electronic device. Firmware usually contains operating code for the device.

- **FTP** — File Transfer Protocol. A standard network protocol used to transfer computer files between a client and server.
- **GB**— Gigabyte. A multiple of the unit byte for digital information storage. Usage depends on context. When referring to disk capacities it usually means 10^9 bytes. It also applies to data transmission quantities over telecommunication circuits.
- **Gbps** — Gigabits per second. The rate of data flow.
- **HTTP**—Hypertext Transfer Protocol. An application-level protocol for accessing the World Wide web over the Internet.
- **IEEE** — Institute of Electrical and Electronics Engineers. An international technical/professional society that promotes standardization in technical disciplines.
- **IMAP** — Internet Message Access Protocol. An Internet standard protocol for accessing email from a remote server from email clients. IMAP allows access from multiple client devices.
- **IMEI**— International Mobile Equipment Identity. Used in LTE networks to identify the device. It is usually printed on the device and can often be retrieved using a USSD code.
- **IP** — Internet Protocol. The mechanism by which packets are routed between computers on a network.
- **IP type** — The type of service provided over a network.
- **IP address**—Internet Protocol address. The address of a device attached to an IP network (TCP/IP network).
- **ISP**— Internet Service Provider. Also referred to as the service carrier, an ISP provides Internet connection service (See Network Operator).
- **Kbps** — Kilobits per second. The rate of data flow.
- **LAN** — Local Area Network. A type of network that lets a group of computers, all in close proximity (such as inside an office building), communicate with one another. It does not use common carrier circuits though it can have gateways or bridges to other public or private networks.
- **MAC Address**— Media Access Control. A number that uniquely identifies each network hardware device. MAC addresses are 12-digit hexadecimal numbers. This is also known as the physical or hardware address.
- **Mbps** — Megabits per second. The rate of data flow.
- **Network Operator**— The vendor that provides your wireless access. Known by different names in different regions, some examples are: wireless provider, network provider, or cellular carrier.

- **Network Technology**—The technology on which a particular network provider’s system is built, such as LTE or GSM.
- **NNTP** — Network News Transfer Protocol. The primary protocol used to connect to Usenet servers and transfer news articles between systems over the Internet.
- **POP3** — Post Office Protocol 3. A protocol in which email is received and held for you by your Internet server until you download it.
- **Port** — A virtual data connection used by programs to exchange data. It is the endpoint in a logical connection. The port is specified by the port number.
- **Port Forwarding** — A process that allows remote devices to connect to a specific computer within a private LAN.
- **Port Number** — A 16-bit number used by the TCP and UDP protocols to direct traffic on a TCP/IP host. Certain port numbers are standard for common applications.
- **Protocol** — A standard that enables connection, communication, and data transfer between computing endpoints.
- **Proxy** — A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.
- **Router** — A device that directs traffic from one network to another.
- **RSSI** — Received Signal Strength Indicator. An estimated measure of how well a device can hear a signal from an access point or router. RSSI value is pulled from the device’s Wi-Fi card (hence “received” signal strength), so it is not the same as transmit power from an access point or router.
- **SIM** — Subscriber Identification Module. Found in LTE and GSM network technology, the SIM is a card containing identification information for the subscriber and their account. The SIM card can be moved to different devices.
- **SMTP** — Simple Mail Transfer Protocol. The standard protocol for sending emails across the Internet.
- **SNMP** — Simple Network Management Protocol. An Internet protocol used to manage and monitor network devices and their functions.
- **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.
- **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.