USER GUIDE

inseego 5G

5G FX2000

Indoor Router

INSEEGO COPYRIGHT STATEMENT

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 Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp.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: 90027212 Rev E

Contents

1

Introduction and Getting Started

Overview

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

Inside the box you will find a 5G FX2000 Indoor Router, a Quick Start Guide, three AA batteries, an Ethernet cable, and an AC wall adapter power supply (in two pieces).

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.

Ports and Buttons

Indicator LEDs

The top of the 5G Indoor Router 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 Blinking	Strong 5G connection (3 – 5 bars) Weak 5G connection (1 – 2 bars)
Green	Solid Blinking	Strong 4G connection (3 – 5 bars) Weak 4G connection (1 – 2 bars)
White	Solid	Internet is available only on Ethernet WAN
Yellow	Solid	Software update is in progress
Red	Solid Blinking	Router is booting up No service, SIM error, or locked SIM card

The WAN/LAN connector ports also have 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 FX2000 Indoor Router up and running, as well as reset and support information.

Installing a SIM Card

Your SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The 5G Indoor Router supports only Nano SIM cards. If the device SIM is **NOT** already inserted into this device, 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 install a SIM card:

1. Remove the cover from the SIM slot on the right side of the device.
2. If necessary, remove the SIM card from the outer card, being careful not to touch the gold colored contacts.
3. Insert the SIM card into the slot with the gold-colored contact points facing the back of the device.
4. Replace the cover.

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

Installing Batteries

Your 5G Indoor Router uses AA batteries in the bottom of the router for the initial process of identifying a location.

NOTE: You cannot run your FX2000 on batteries alone for Internet use, they are only used for identifying the best location for your Indoor Router with the Inseego Connect App.

To install the batteries:

1. Slide the battery cover to the left and insert a fingernail at the edge to lift it out of place.

2. Insert three AA batteries following the diagrams on the router.

3. Replace the cover by pressing down and sliding it to the right.

4. Press the Power button on the router to turn it on for the location survey below.

Identifying a Location

Use the Inseego Connect App to identify the optimal location for your 5G Indoor Router.

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

2. Follow instructions within the Inseego Connect App to connect to your 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.

Powering On

Once you have identified a location for your 5G Indoor Router, turn it on with the AC wall adapter power supply:

1. Attach the power cord to the charger (power cord comes in two pieces).

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 router to overheat or catch fire, resulting in serious bodily injury, death, or property damage.

2. Plug the power cord into the power port on the back of the router.
3. Plug the power adapter into an AC wall outlet.
4. Press the Power button on the device to turn it on.

The indicator LED will turn on while the 5G Indoor Router powers on. Once the unit is fully on, the LED should turn solid blue, indicating a strong 5G connection.

Connecting to the Router

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 router:

1. Make sure the 5G Indoor Router is powered on, and the indicator LED is blue, green, or white.
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 network name (or SSID). **NOTE:** The default SSID is on the bottom of the router.

3. Click **Connect** or otherwise select the network name.

4. When prompted, enter the password. **NOTE:** The default password is on the bottom of the router.

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

Connecting Devices with WPS

Wi-Fi Protected Setup (WPS) allows compatible devices to connect to a Wi-Fi network on your 5G Indoor Router without having to manually enter the password.

To connect a device using WPS:

1. Push the WPS button on the router.
2. Follow the guidelines for the device you want connect.

NOTE: WPS is enabled by default on the 5G Indoor Router. You can find more information about enabling or disabling WPS under Managing Wi-Fi Settings on page 21.

Connecting Devices with Ethernet

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

To connect Ethernet devices:

1. Plug one end of an Ethernet cable into one of the Ethernet ports on the router.

   NOTE: To connect wired devices for Internet connection, use the LAN1, LAN2, or 5Gbps LAN ports (5Gbps LAN provides Internet throughput to up to 5Gbps, depending on the maximum throughput of the device you are connecting to). To connect to a fiber router or modem, use the WAN port and connect to the LAN port of the router/modem.

3. Plug the other end of the cable into the Ethernet port of the device you wish to connect.

Devices plugged into the FX2000 via Ethernet have instant access to the Internet.

Connecting to the Web UI

Once your 5G Indoor Router is connected to a device that supports Web browsing, you can use the Web User Interface to customize settings, change your password, and access information.

On a device connected to the 5G Indoor Router, open any Web browser and go to http://192.168.1.1 .

Select Sign In (in the top-right corner of the screen), and enter the Admin password printed on the bottom of the 5G Indoor Router.

Caring for your Router

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

Resetting your Router

You can reset your 5G Indoor Router to factory settings using the RESET button on the router or from the Admin Web UI.

CAUTION! Resetting returns your 5G FX2000 Indoor Router to factory settings, including resetting the Wi-Fi name and password. This disconnects all devices.

Resetting with the RESET button

The master reset button is in a small hole located in the battery compartment on the bottom of the 5G Indoor Router. This button returns the device to factory settings, including resetting the Wi-Fi name (SSID) and password and admin password.

To reset the 5G Indoor Router:

1. Slide the battery cover to the left and insert a fingernail at the edge to lift it out of place.
2. Place one end of an unfolded paper clip into the master reset button hole.
3. Press the paper clip on the button for about five to six seconds, then your 5G Indoor Router will restart.

Resetting from the Admin Web UI

To reset the router from the Admin Web UI, select **Settings > Backup and Restore** and select **Restore factory defaults**.

Care Tips

Inseego recommends the following care guidelines:

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

2

Software Configuration

Overview

Use the 5G FX2000 Indoor Router Admin Web User Interface to manage your router experience. With it, you can:

- Change your SSID and/or passwords (both admin and user).
- View connected devices.
- Check router status and data usage.
- Set up a guest network.
- View all currently connected devices.
- Control access by device.

On a computer or device connected to your FX2000, open any Web browser and go to http://192.168.1.1.

Home Page

The Home page is the local gateway to configuring and managing your FX2000. It displays the current Wi-Fi networks and passwords and lists all currently connected devices. It also shows Internet status, setting information, and provides access to help topics.

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

Side Menu

Each subscreen in the 5G Indoor Router 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.

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

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

The next time you sign in to the 5G Indoor Router Web User Interface, use the new Admin password. If you cannot remember the password, click **I forgot the Admin password**. After you correctly answer the security question you set up, the current password is displayed.

Managing Cellular Data Usage

You can monitor and manage cellular data usage on your 5G Indoor Router using the Cellular Data Usage page. To manage or view cellular data usage, select from any Home page panel and then select **Cellular Data Usage** from the Web UI side menu. The Cellular Data Usage page appears.

Cellular Data Usage Page

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

Usage alert level: Specify an alerting threshold for data usage (from 20 MB to 20 GB, or None).

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

Disable cellular on reaching max limit: Enter a data limit.

Tx: The amount of data transmitted during the current cycle.

Rx: The amount of data received during the current cycle.

Total usage: An estimation of the amount of data used during the current cycle.

Use the **Reset data usage counter** button to restart the data usage shown on this page to zero.

Select **Save 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 Web UI Home page, the Wi-Fi panel shows the current name (SSID) 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 Web UI 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.

Wi-Fi

Use the **Allow Wi-Fi devices to connect to this router** 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.

WPS

Wi-Fi Protected Setup (WPS) allows compatible devices to connect to a Wi-Fi network without having to manually enter the password. To enable WPS, turn the **Enable WPS** slider to on and check the box next to the networks on which you want to allow WPS.

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.

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

Settings

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.

Options

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.

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.

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**.

Settings

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.

Options

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.

Select **Save changes**.

Managing Connected Devices

On the 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.

To manage connected devices, select from the Home page Connected Devices panel (or select **Connected Devices** from the Web UI 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 Web UI. You can also block or unblock a device from Internet access.

Connected

This table lists all devices connected to the 5G Indoor Router:

Connection: An icon indicates the connection type (Wi-Fi or Ethernet) 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.

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.

To view details on a device or change the name of the device as it appears in this Web UI, click the **plus icon** (+) on the right to expand the device row. The following information appears:

- **Name:** To change how the device name appears in this Web UI, enter a different name. **NOTE:** This only changes the device name in the FX2000 Web UI.
- **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 **minus icon** (-) 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, click the **Unblock** button and select **Save changes**. The device is removed from the **Blocked** list and appears in the **Connected** list above.

Managing Settings

On the Web UI Home page, the Settings panel shows Port Filtering and the date and time of the last system update.

To configure more system settings, select from the Home page Settings panel (or select **Settings** from the Web UI side menu).

The Settings page includes five tabs:

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

Preferences Tab

This tab allows you to change how dates, time, and numbers are displayed in the FX2000 Web UI.
NOTE: These preferences affect packets sent to remote servers. For example, if you select a 24 hour time format, the Web UI, and any packets reporting time somewhere else, will display time in 24 hour format.

Language: Select a language for the Web UI.

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

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

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

Use the **Enable Device Installation** slider to enable or disable installing and connecting devices such as smartphones through Bluetooth applications.

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

Software Update Tab

Software updates are delivered to the 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 New Software Update

Checked for update: The date and time the FX2000 last checked to see if an update was available.

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

Check for Update: Click this button to manually check for available software updates. If a new software update is available, it is automatically downloaded.

Last Software Update

This section displays details about the last software update.

Software Update History

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

Backup and Restore Tab

Use this tab to back up current 5G Indoor Router settings to a file on your computer, restore (upload) a previously-saved configuration file, reset the router to factory defaults, or restart the router.

Backup

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

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

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 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 router and disconnecting you from the Web UI.

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

In the **Select a file** field, click **Browse** and choose a backup settings file to restore.

NOTE: You can only restore a file that was created for this model of 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 router and disconnecting you from the Web UI.

Restart Router

Restart: This button turns your 5G Indoor Router off and on again.

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.

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.

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 53.

Managing VPN

The 5G Indoor Router allows you to establish secure connections to remote networks over a public network using VPN. You can either create IPSec VPNs or enable OpenVPN.

To set up VPN, select **>** from any Home page panel and then select **VPN** from the Web UI side menu. The VPN page includes two tabs:

- IPSec VPN
- OpenVPN

IPSec VPN Tab

The 5G Indoor Router allows you to create IPSec VPNs to establish secure connections to remote networks over a public network.

VPN Service

Enable IPSec VPN service enables or disables IPSec VPN service on your device. When the **ON/OFF** slider is **ON**, VPN is enabled. When **OFF**, VPN service is not available.

VPN Tunnel Configurations

Once a tunnel is added, the page displays the list of tunnel configurations. You can delete, edit, view, change priorities of the tunnel configurations.

Add new VPN tunnel: Use this button to add a new VPN tunnel. The Add New VPN Tunnel Dialog appears.

Add New VPN Tunnel: Step 1 out of 5

General Settings

- **Start tunnel** — Select whether to start the tunnel automatically upon start up or manually.
- **Enable tunnel** —Check this box to enable the tunnel.
- **Tunnel name** — Enter a unique name to identify this VPN.
- **Local identity** — Enter a unique name to identify the local point of the tunnel.
- **Remote identity** — Enter a unique name to identify the remote point of the tunnel.
- **Local authentication** — Select an authentication type from the drop-down list. You will be prompted for further information based on your selection.
- **Remote authentication** — Select an authentication type from the drop-down list. You will be prompted for further information based on your selection.

Add New VPN Tunnel: Step 2 out of 5

Local Network

- **Local IP** — Enter the WAN IP address of local device. **NOTE:** This should be a static IP that you are able to reach from remote device (no NAT).
- **Local subnet mask** — Enter the subnet mask of the local device, for example: If your local IP is 192.168.0.100 and your subnet mask is 255.255.255.0 this should be **192.168.0.0/24**. **NOTE:** This should mirror what the subnet displays in the local device, for example: 192.168.0.0 / 255.255.255.0. **NOTE:** The local device should be on a different subnet from remote, for example: If the Remote Subnet Mask is **192.168.1.0/24**, the Local Subnet Mask might be **192.168.0.0/24**. This is usually based off the DHCP settings of the devices.

Remote Network

- **Remote IP** — Enter the WAN IP address of remote device. **NOTE:** This should be a static IP that you are able to reach from local device (no NAT).
- **Remote subnet mask** — Enter the subnet mask of the remote device, for example: If your remote IP is 192.168.1.100 and your subnet mask is 255.255.255.0 this should be **192.168.1.0/24**. **NOTE:** This should mirror what the subnet displays in the local device, for example: 192.168.1.0 / 255.255.255.0. **NOTE:** The remote device should be on a different subnet from local, for example: If the Local Subnet Mask is **192.168.0.0/24**, the Remote Subnet Mask might be **192.168.1.0/24**. This is usually based off the DHCP settings of the devices.

Add New VPN Tunnel: Step 3 out of 5

IKE Phase 1

Key lifetime: The lifetime of the phase 1 key, in seconds.

Select desired items from each column. **NOTE:** Each phase should support at least one matching option in each column. For example, if Phase 1 on this page is configured to support Hash SHA2 512, SHA2 384, and SHA2 256, then at least one of those selections must be selected in Phase 2 on the next page in order to be a common Hash.

Add New VPN Tunnel: Step 4 out of 5

IKE Phase 2

Key lifetime: The lifetime of the phase 2 key, in seconds.

Select desired items from each column. **NOTE:** Each phase should support at least one matching option in each column. For example, if Phase 1 on the previous page is configured to support Hash SHA2 512, SHA2 384, and SHA2 256, then at least one of those selections must be selected in Phase 2 on the this page in order to be a common Hash.

Add New VPN Tunnel: Step 5 out of 5

Dead Peer Detection (DPD) is a keep-alive method that ensures the tunnel is up and will take action if it is not able to reach the remote side of the tunnel, depending on what DPD action you select. You can use the default values, if desired.

Dead Peer Detection

Enable: Check this box to enable DPD.

DPD action: Use the drop-down to select a DPD action.

DPD delay: The number of seconds between DPD packets.

DPD timeout: The number of seconds the router will allow an IPSec session to be idle before beginning to send DPD packets to the peer machine.

Click **Finish and save** to implement your settings. You return to the VPN page. The new VPN tunnel is now listed.

OpenVPN Tab

You can configure and enable OpenVPN with your 5G Indoor Router. If OpenVPN is connected, there is no need for devices connected to the router to use their own OpenVPN client.

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

Auto-connect VPN: Use the **ON/OFF** slider to enable or disable auto-connect for the OpenVPN connection.

VPN Connection

Connection status: Indicates the status of the OpenVPN connection.

Connect: Use this button to connect the OpenVPN.

View log: Use this button to view OpenVPN log files.

Connection time: The duration of the current OpenVPN connection.

VPN Settings

Set configuration file: Click **Browse** to navigate to a setup file.

Username: Enter a username.

Password: Enter a password.

Use the **Clear all VPN settings** or **Save changes** buttons to clear or save your settings.

Managing Parental Control

Parental controls in the 5G FX2000 Indoor Router Web UI allow you to control Internet access to specific devices and view search history.

To manage parental controls, select  from the Home page Parental Control panel (or select **Parental Control** from the Web UI side menu).

The Parental Control page includes three tabs:

- Profile
- Profile Assignment
- Search History

Profile Tab

Parental controls in the FX2000 Web UI allow you to control Internet access to specific devices. You can set up multiple profiles for Internet access on the Profile tab and assign them to individual connected devices on the Profile Assignment tab. You can view search history on the Search History tab.

Use the Profile tab to create and manage profiles that determine when devices can access the Internet through your 5G Indoor Router.

Add New Profile: Select this button to create a new profile. The Add New Profile dialog box appears.

Profile Name: Enter a name for the profile.

Block URL: Enter a URL you want to block for this profile and click **Add**. Repeat for additional URLs.

Block PORT: Enter a port number you want to block for this profile and click **Add**. Repeat for additional ports.

URL Search History: Check the box if you want search history during this profile available for display on the Search History tab.

Internet Accessible Time: Set the start and end times for the days you want to allow Internet access for this profile.

Select **Save Profile** to close the dialog box and return to the Profile page. The new profile is now listed.

Use the **Edit** and **Delete** buttons to edit or delete (unassigned profiles only) listed profiles.

Use the **Assigned Profiles** tab to apply profiles to devices.

Profile Assignment Tab

Use this tab to assign profiles created on the Profile tab to individual connected devices, allowing you to determine when specific devices can access the Internet through your 5G Indoor Router.

NOTE: You must first create a profile on the **Profile** tab.

Add profile assignment: Select this button to assign a profile to devices. The Add profile assignment dialog box appears.

Profile: Use the drop-down to select a profile.

Devices: Use the drop-down to select a device you want the profile assigned to. **NOTE:** The drop-down lists devices that have been connected to the FX2000 in the past seven days.

Select **Save** to close the dialog box and return to the Profile Assignment page. The profile is now listed with the assigned device.

Use the **Edit** and **Delete** buttons to edit or delete profile assignments.

Search History Tab

Use this tab to view Internet search history for devices connected through your 5G Indoor Router.

NOTE: You must first create a profile on the **Profile** tab and check the **URL Search History** check box. Then you must assign the profile to a device on the **Profile Assignment** tab.

You can view all the URLs the selected device visited and the number of visits for each URL for the past 15 days.

Select **Clear history** to clear the displayed search history.

Viewing Info About the Router

On the Web UI Home page, the About panel shows current connection status, the amount of time connected, and the amount of data transmitted and received.

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 Web UI side menu).

The About page includes four tabs:

- General Status
- System Status
- Ethernet WAN
- Cellular WAN

General Status Tab

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

General

Connection status: The current status of the 5G Indoor Router connection.

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

Active interface: The interface that is active (Ethernet WAN, Cellular WAN, or None).

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

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

Software Components

Manufacturer: The manufacturer of the 5G Indoor Router (Inseego).

Model name: The model name of the 5G Indoor Router.

Model number: The model number of the 5G Indoor Router.

Modem version: The version number of the modem firmware.

IPQ Version: The version of Qualcomm® Internet Processor (IPQ).

System Status Tab

Use this tab to view details about your system status.

General

Ethernet clients: The number of client devices connected by Ethernet.

2.4 GHz clients: The number of client devices connected at 2.4 GHz band.

5 GHz clients: The number of client devices connected at 5 GHz band.

Ethernet WAN Tab

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

IP4

IPv4 address: The Internet IP address assigned to the 5G Indoor Router.

IPv4 subnet mask: The network mask associated with the IPv4 address.

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

IPv4 DNS: The Domain Name Server currently used by this device.

IPv6

IPv6 Address: The IPv6 address assigned to the 5G Indoor Router.

Cellular WAN Tab

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

General

Radio Access Technology: Indicates the current cellular data connection, for example, LTE.

IMEI: The International Mobile Equipment Identity (IMEI) for this device. This is a 15 digit code used to uniquely identify an individual mobile device on a cellular network. The IMEI does not change when the SIM is changed.

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

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

General

IPv4 Address: The IPv4 address assigned to the router.

IPv6 Address: The IPv6 address assigned to the router.

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

Getting Help

On the Web UI Home page, the Help panel provides links to introductory help and support.

To view more detailed help information, select from the Home page Help panel (or select **Help** from the Web UI side menu).

The Help page includes two tabs:

- Help
- Customer Support

Help Tab

This page provides links to help topics for every page of the Admin Web UI and general topics useful for getting started with your 5G Indoor Router.

Customer Support Tab

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

3

Advanced Settings

Overview

The Advanced Settings pages on the 5G Indoor Router Admin website are intended for users with technical expertise in the area of telecommunication and networking.

WARNING! Changing the Advanced settings may be harmful to the stability, performance, and security of the 5G FX2000 Indoor Router.

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.

The Advanced Settings page includes eight tabs:

- LAN
- WAN
- SIM
- Cellular
- Firewall
- MAC Filter
- Port Filtering
- Port Forwarding

LAN Tab

This tab provides settings and information about the 5G Indoor Router's local area network (LAN). The LAN consists of the router and all Wi-Fi and Ethernet connected devices.

IPv4

IP address: The IP address for your 5G Indoor Router, as seen from the local network. Normally, you can use the default value.

Subnet mask: The subnet mask network setting for the 5G FX2000 Indoor Router. The default value 255.255.255.0 is standard for small (class "C") networks. If you change the LAN IP Address, make sure to use the correct Subnet mask for the IP address range of the LAN IP address.

MAC address: (read-only) The Media Access Controller (MAC) Address for the Wi-Fi interface on your 5G Indoor Router. 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

Enable IPv6: Move the slider to ON if any of your connected devices support IPv6. This enables IPv6 connected devices to make IPv6 connections to the Internet.

DNS

Enable manual DNS: Move the slider to ON to manually assign up to two DNS IP addresses.

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** to activate and save new settings.

WAN Tab

Use this tab to configure and set the priority of each available WAN interface.

Active WAN Interface: The current active WAN interface.

Set WAN Interface Priority

First Priority: Use the drop-down to select the WAN interface to have first priority (Cellular WAN or Ethernet WAN).

WAN Interface Configuration

You can defined up to three IP address to check if Internet WAN is active.

Track IP 1 — The IP address of the host. This must be a stable Internet address.

Track IP 2 — The IP address of the host. This must be a stable Internet address.

Track IP 3 — The IP address of the host. This must be a stable Internet address.

Reliability — Sets the number of Track IPs that must respond to ping tests in order for the WAN interface to be considered active:

- **3** — If there is no response from any of the Track IPs, WAN interface is considered inactive.
- **2** — If there is no response from just one of the Track IPs, WAN interface is considered active.
- **1** — Only one of the Track IPs can be configured.

Ping Count — Number of ping packets to send for each ping test.

Ping Intervals — Time between two ping tests.

Ping Timeout — The amount of time the router waits between verification attempts, in minutes, before determining the verification has failed. **NOTE:** A shorter amount of time may create false positive results, while a longer amount of time may delay detection of issues.

Click **Save changes** to save any 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.

SIM PIN

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

- **Ready** – No SIM PIN is needed.
- **PIN Locked** - SIM PIN must be entered before you can use the mobile network.
- **PUK Locked** - PUK (personal unblocking key) for the SIM must be entered in order to continue. The PUK can be obtained from your service provider. Enter the PUK. Enter and confirm a new PIN and click **Unlock**.
- **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.

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

Change SIM PIN: Use this button to change the SIM PIN. You must enter the current PIN, then enter the new PIN and confirm it. Click **Save changes**.

Turn on SIM PIN Lock: Use this button to set the SIM so that entry of a PIN is required upon startup to connect to the mobile network. Enter the current PIN and click **Save changes**. The button will now display **Turn off SIM PIN Lock**.

Turn off SIM PIN Lock: Use this button to turn 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. Enter the current PIN and click **Save changes**. The button will now display **Turn on SIM PIN Lock**.

Cellular Tab

In most configurations, the 5G Indoor Router is used with a dynamic IP and SIM and the Access Point Name (APN) is available from the network, for example: *internet*. However, if you are on a private network, you may need to set the APN on this tab for the network to communicate with the router.

Network Selection

Allow device to connect to the mobile networks: 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 5G Indoor Router's mobile data plan. For normal operation, this setting must be left on.

Preferred Network Mode: Use the drop-down to select a mode (5G, 4G LTE, or Auto). If you select Auto, your router automatically selects the best available network.

APN Setting

Internet APN: Enter the APN for your private network.

CAUTION! Changing the APN may cause a loss of data connectivity and disconnect you from the Web UI.

Roaming

Allow domestic data roaming: Use the check boxes to allow or disallow access to the mobile network when roaming.

Firewall Tab

The 5G Indoor Router firewall determines which Internet traffic is allowed to pass between the router and connected devices and protects your connected devices from malicious incoming traffic from the Internet. The firewall cannot be turned off. Use the Firewall tab to adjust the general security level of the firewall, designate a specific device to receive all traffic, and set up specific firewall rules.

Security Level

You can select from three general security levels to block traffic into and through the 5G FX2000 Indoor Router. The default Security Level is Medium.

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

DMZ

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

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

Allow DMZ: Check this box to allow DMZ.

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

Click **Save changes**.

Firewall Rules

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

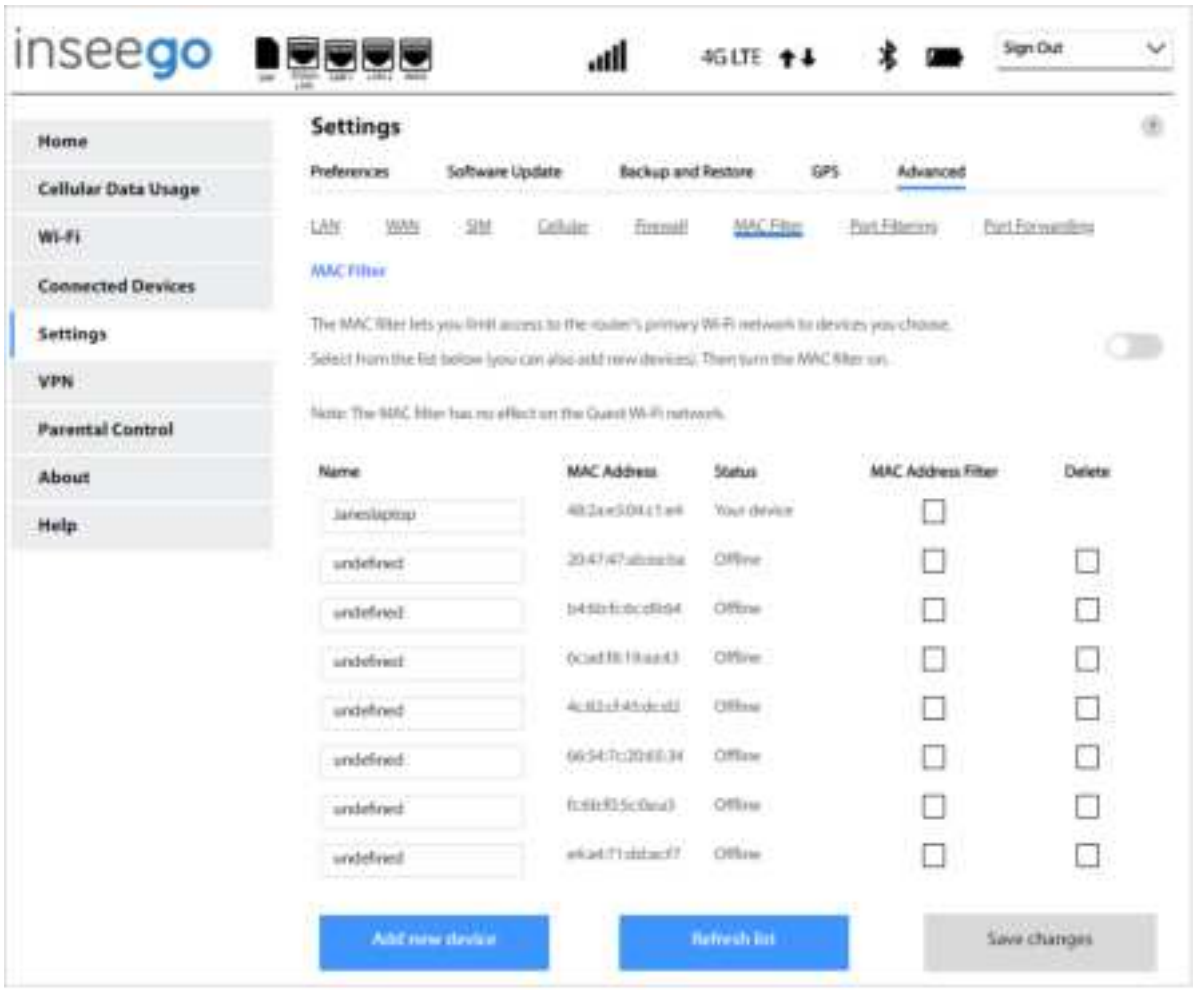
NOTE: For **Src. IP** and **Dest. IP**, enter a specific IP address or the keyword **any**.

Click **Save changes**.

MAC Filter Tab

The MAC filter allows only selected devices to access the 5G Indoor Router primary Wi-Fi network. By default, MAC filter is turned off.

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



NOTE: The MAC filter has no effect on devices connected to the guest Wi-Fi network or devices connected via Ethernet.

MAC Filter

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

Device List

This list includes all devices currently connected to the router, except those connected via Ethernet.

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

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

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

Notes on Blocking Devices

There are two ways to block devices from connecting to the 5G Indoor Router:

- **Temporarily block a device from connecting to the router via the primary and guest networks and via Ethernet.**
  To use this method, go to the **Connected Devices** page and click the **Block** button next to the device.
- **Permanently block a device from connecting to your FX2000 primary network only.** Use the **MAC Filter**.

When blocking devices, the following information applies:

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

Port Filtering Tab

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

NOTE: You can also view the current Port Filtering setting (ON/OFF) in the Settings panel on the Web UI Home page.

Port Filtering

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

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

Applications

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

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

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

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

Custom Applications

You can define up to ten custom applications.

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

- **On:** Check this box if you want the new application to be able to access the Internet.
- **Application Name**: Enter a name for the custom application.
- **Start Port:** Enter the beginning of the range of port numbers used by outgoing traffic for the custom application being added.
- **End Port:** Enter the end of the range of port numbers used by the application.

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

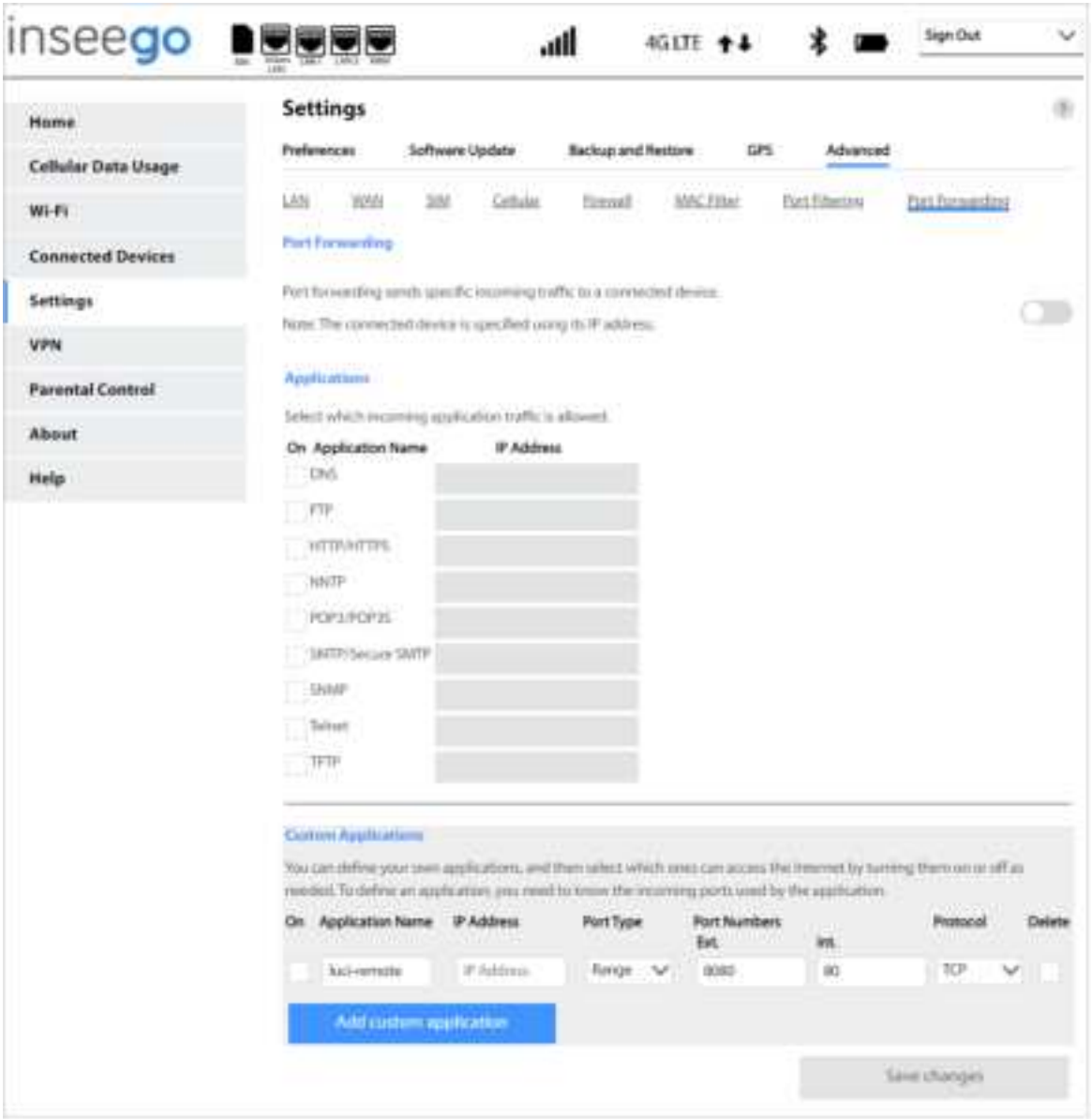
Click **Save changes** to save any changes made to the custom applications.

Port Forwarding Tab

Port Forwarding allows incoming traffic from the Internet to be forwarded to a particular device connected to your Wi-Fi network. Normally, the built-in firewall blocks incoming traffic from the Internet. Port forwarding allows Internet users to access any server you are running on your computer, such as a Web, FTP, or Email server. For some online games, port forwarding must be used in order for the games to function correctly.

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

Some mobile networks provide you with an IP address on their own network rather than an Internet IP address. In this case, Port Forwarding cannot be used, because Internet users cannot reach your IP address.



Port Forwarding

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

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

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.

Click **Save changes**.

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

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

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

Custom Applications

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

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

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

4

Troubleshooting and Support

Overview

When properly installed, the 5G Indoor Router is a highly reliable product. Most problems are caused by phones[†] or Ethernet devices connected to incorrect ports. Please refer to the labels next to the ports for proper connections.

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.

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 FX2000 Indoor Router 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

Device

Name:	FX20003
Model:	FX20003
Regulatory:	FCC, CE, GCF, PTCRB
Device Testing:	WEEE, RoHS, REACH
Dimensions:	6.3" x 2.8" x 2.4"
Weight:	59 oz (1675 g)
Ports:	1x 1 Gbps 1x WAN
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 Sub6 mmWave* or Sub6 only
LTE CAT 22

Wi-Fi

802.11 a/b/g/n/ac/ax
Wi-Fi 6 with 4x4 MU-MIMO
Real Simultaneous Dual-Band Wi-Fi
Multiple SSID/Guest Wi-Fi Support
Supports up to 128 simultaneous Wi-Fi Enabled Devices

Security

Secure Boot	
Admin Security	AES 256 Encryption, • Security Hardened Web Interface • Password Hash • Session Timeout • Wi-Fi On/Off Control • Incorrect Password Lockout • Block factory reset

* Optional feature

† Data plan required. Coverage subject to network availability.

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	
IPSec VPN	

External Antenna: This device employs hardware that may support an external antenna in the future. The external antenna hardware is disables via software and cannot be enabled by the end user. Prior to enabling the external antenna hardware this device will be reevaluated for compliance against all regulatory requirements

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.

CE

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

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

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

RF Radiation Exposure Guidance Statement

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

Radio Frequency and Transmitted Output Power Information

Band	Max Power	Frequency
WCDMA BAND I	24 dBm	1920-1980 MHz
WCDMA BAND II	24 dBm	1850-1910 MHz
WCDMA BAND IV	24 dBm	1710-1755 MHz
WCDMA BAND V	24 dBm	824-849 MHz
WCDMA BAND VIII	24 dBm	880-915 MHz
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 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

Band	Max Power	Frequency
LTE BAND B20	24 dBm	832-862 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 B30	24 dBm	2305–2315 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 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
n5	24 dBm	824–849 MHz
n7	24 dBm	2500-2570 MHz
n8	24 dBm	880-915 MHz
n12	24 dBm	699–716 MHz
n28	24 dBm	703-748 MHz
n40	24 dBm	2300-2400 MHz
n41	24 dBm	2496–2690 MHz
n66	24 dBm	1710–1780 MHz
n71	24 dBm	663–698 MHz
n78	24 dBm	3300–3800 MHz
WLAN ISM	17 dBm	2.4 GHz
WLAN UNII-1	17 dBm	5.2 GHz
WLAN UNII-3	10 dBm	5.8 GHz
n25	24 dBm	1850–1915 MHz

The device is restricted to indoor use only when operating in the 5150 to 5250 MHz 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)

Please make sure the temperature for device will be 0° C to 45° C (32° F to 113° F).

Product Certifications and Supplier's Declarations of Conformity

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

Wireless Communications

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

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

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

Inseego Corp. or its partners will not be held responsible for damages of any kind resulting from the delays or errors in data transmitted or received with the 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.

Proper Battery Use and Disposal

IMPORTANT: In the event of a battery leak:

- Do not allow the liquid to come in contact with the skin or the eyes. If contact has been made, wash the affected area with large amounts of water and seek medical advice.
- Seek medical advice immediately if a battery has been swallowed.
- Communicate the appropriate steps to be taken if a hazard occurs. Due to the transmission and reception properties of wireless communications, data occasionally can be lost or delayed.

Please review the following guidelines for safe and responsible battery use:

- Do not disassemble or open, crush, bend or deform, puncture, or shred.
- Do not modify or remanufacture, attempt to insert a foreign object into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.
- Only use the battery for the system for which it was specified.
- Do not short circuit a battery or allow a metallic or conductive object to contact the battery terminals.
- Promptly dispose of used batteries in accordance with local regulations.
- Battery usage by children should be supervised.

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.
- **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.