

Inseego Wavemaker[™]

FX4200 5G Cellular Router



INSEEGO COPYRIGHT STATEMENT

© 2025 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 Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp.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 PRT-14965465 Rev B



Contents

Introduction and getting started	6
Overview	7
Key features.....	7
System requirements.....	7
Device front	8
Device back.....	9
Indicator LEDs	10
Device display.....	11
Getting started	14
Inserting a SIM card	14
Placing your router.....	15
Connecting external antennas (optional)	15
Powering on	16
Mounting your FX4200 (optional)	17
Pairing mesh nodes (optional).....	17
Connecting devices to the router	19
Monitoring and managing your router	20
Caring for your router.....	22
Replacing a SIM card	22
Resetting your router.....	23
Care tips	24
Configuration.....	25
Overview	26
Home page.....	27
Navigation tips.....	27
Getting help	28
Admin password.....	28
Changing the admin password	28
Managing devices	30
Overview tab	30
Internet Info tab	30
Data Usage tab	33
Managing your network	35
Cellular tab.....	35
Wi-Fi tab.....	43
Ethernet tab.....	52
LAN tab	53
WAN tab	59
Devices tab.....	64

DNS tab	66
Managing routing	67
Managing security.....	73
VPN	73
Firewall tab	79
MAC Filter tab	80
Using Tools	82
Speed Test tab	82
Logs tab.....	83
Setting Administrative options.....	85
Software Update tab	85
Preferences tab	89
Troubleshooting and support	92
Overview	93
Troubleshooting	93
Will I always get 5G? Can I use the router outside of 5G coverage?.....	93
The device status LED is switching from blue to green	93
Can I set my router to use a specific cellular band?	93
I cannot access the Admin web UI	94
My router is getting slow speeds/low throughput	94
The device status LED is blinking red.....	95
My older device cannot connect.....	96
My connecting device is not obtaining a valid IP address	97
My connected device cannot connect to Fortinet VPN.....	98
Devices connected via Ethernet are not getting internet	98
I cannot get streaming platforms to work with my router	98
Do I need a signal amplifier or booster?.....	98
Does the USB port support RNDIS?	99
Does the USB port support USB-C to Ethernet adapters?.....	99
Technical support	99
Vulnerability disclosure policy	99
Product specifications and regulatory information	100
FX4200 product specifications	101
Device	101
Network connectivity.....	102
Wi-Fi	102
Remote management.....	102
Software and security.....	103
Accessories (sold separately).....	103
Regulatory information.....	104
Federal Communications Commission Notice (FCC – United States).....	104

Innovation, Science and Economic Development Notice (ISED – Canada)	106
Cellular external antenna considerations for FX4210	107
Product certifications and supplier’s declarations of conformity.....	109
Wireless communications.....	109
Limited warranty and liability	109
Safety hazards	110

1

Introduction and getting started

Overview

Device front

Device back

Indicator LEDs

Device display

Getting started

Caring for your router

Overview

The FX4200 5G Cellular Router provides reliable, high-speed connectivity wherever you need it, making it the ultimate broadband solution.

Inside the box you will find an FX4200 5G Cellular Router, a Get started card, a USB-C cable and AC wall adapter power supply.

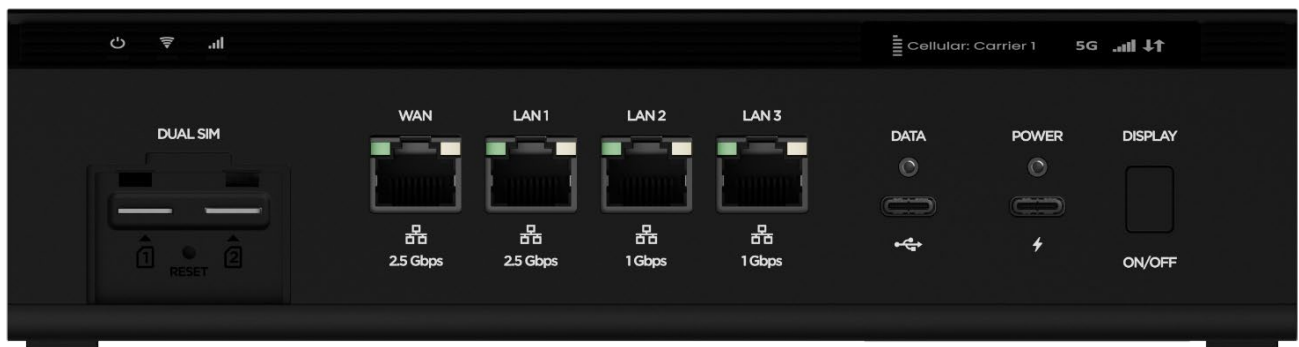
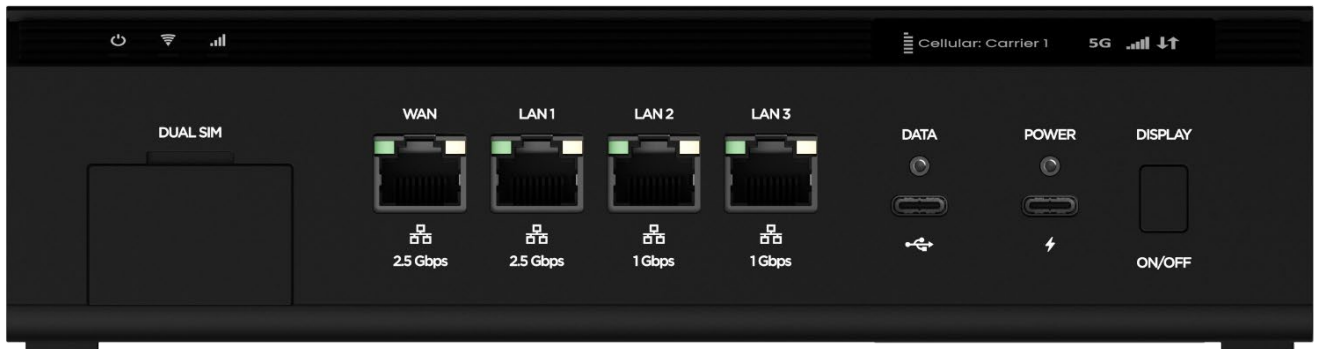
Key features

- With 5G NR technology, Wi-Fi 7 capability, and simplified device management, the compact FX4200 5G Cellular Router provides reliable, high-speed connectivity wherever you need it.
- The FX4200 ensures seamless, day-one connectivity and easy setup. You can get online instantly without waiting for wireline installations. The digital display shows network status, initiates mesh pairing, and more for maximum performance.
- Supports up to 128 connected devices, two Ethernet WAN/LAN ports, and a USB-C port for data and tethering.
- Offers the flexibility to function as a dependable primary 5G wireless connection with full Wi-Fi 7 access point; or enhance your network's resiliency by seamlessly transitioning to a failover solution for wired networks, delivering consistent performance and reliability.
- Enterprise-grade management with Inseego Connect allows you to remotely manage thousands of devices and mesh networks from one central interface. Ideal for scaling enterprise networks, ensuring uptime, and reducing complexity.

System requirements

- Compatible with all major operating systems.
- Works with the latest versions of browsers.
- To use Wi-Fi, connecting devices need Wi-Fi capability. You can also connect via Ethernet or USB.

Device front



* Ethernet ports are labeled with their default setting (WAN or LAN). You can configure any port to be WAN or LAN in the admin web UI: **Network > WAN**, or with Inseego Connect: **WAN Settings**.

Device back



* When enabled, each external port supports the full cellular frequency range of 0.6–6 GHz. To activate the external antenna ports, turn the switch to **EXTERNAL ANTENNAS ON**.

Indicator LEDs

The front of the router has a device status LED, a cellular status LED, and a Wi-Fi status LED. Each LED changes colors and blinks or glows solid to communicate current states for the device.

NOTE: You can turn off the indicator LEDs in the Admin web UI with **Settings > Preferences**.

LED	Color		Operation	Meaning
Device status 	Blue		Solid	Device on 5G
	Green		Solid	Device on LTE
	Yellow		Solid Blinking	Software update is available Software update is downloading/installing
	White		Solid Blinking	Device on, Ethernet WAN Device booting up
	Red		Solid Blinking	Device error Software update failed
Cellular status 	Blue		Solid	Great signal (5 bars)
	Cyan		Solid	Good signal (4 bars)
	Green		Solid	Fair signal (3 bars)
	Yellow		Solid	Poor signal (2 bars)
	Red		Solid Blinking	Very poor signal (1 bar) No signal/no network
	White		Blinking	Searching for signal
Wi-Fi status 	Blue		Solid Blinking	Wi-Fi on, mesh Mesh pairing mode
	Green		Solid	Wi-Fi on, no mesh
	White		Blinking	Wi-Fi initiating/rebooting
	Red		Solid	Wi-Fi error
	Off		Off	Wi-Fi off

The WAN/LAN ports on the back of the router also have indicator LEDs.

LED Color	Operation	Meaning
Green 	Solid Blinking Off	Indicates Ethernet connection speed 1 000 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

Device display

The device display provides device information, alerts, and allows you to perform actions, like pair with a mesh node or check for a firmware update.

NOTE: The device display times out after 60 seconds.

Use the display button to navigate through the display:

- **Short press (<1 second)** – cycles through the display menu or submenu options.
- **Long press (>3 seconds)** – initiates an action or accesses/exits a submenu.

TIPS:



The menu icon on the left shows you where you are in the main menu.



The scroll icon on the bottom of a submenu shows you where you are in the submenu.



An X appears over the signal strength icon when no network is found.



An X appears on the data arrows icon when there is no data traffic.



An antenna icon appears when the external antenna switch is on.

Main menu	Submenu
Cellular: T-Mobile 5G  	Cellular IMEI: 350077523237513 
	Cell SIM: 12345678912345689478 
	Cellular Number: (418) 154-1234 
	Cellular APN: fast.t-mobile.com 
	Cellular IP: 17.172.224.47.192.0 
	Cellular Band: B66_n77 
	Cellular Signal: -85 dBm 
	Exit Submenu: Hold button 3 2 1 
Ethernet WAN: Connected 	E MAC Address: 00:1A:2B:3C:4D:5E 
	Ethernet WAN IP: 123.123.123.123 
	Exit Submenu: Hold button 3 2 1 
Wi-Fi Name: FX4100-08AC	Wi-Fi Pwd: wwwwwwwwwwwwwww 
	Wi-Fi Clients: 20 
	Wi-Fi Mesh Nodes : 3 
	Exit Submenu: Hold button 3 2 1 
Wi-Fi Mesh: Hold Button To Add	Wi-Fi Mesh: Hold Button 3 2 1
	Wi-Fi Mesh: Searching
	Press Mesh Button on Node
	Wi-Fi Mesh: Pairing...
	Wi-Fi Mesh: Node Found
	Wi-Fi Mesh: No Node Found

Main menu	Submenu
	Wi-Fi Mesh: Paired! ✓
Firmware: IT	
Update: Hold Button to Check	Update: Hold Button 3 2 1 Update: Checking... 🔍 Update: 7L PRI v718 is available! Update: Downloading... ⬇ Update: Hold Button to Install Update: Hold Button 3 2 1 Update: Installing... ⚙️ Do Not Unplug the Device Update: Rebooting... Do Not Unplug the Device
Alerts (4): Hold Button to Review	Alert (1/4): Invalid SIM ■ □ □ □ Alert (2/4): No Service □ ■ □ □ Alert (3/4): Wi-Fi Is Off □ □ ■ □ Alert (4/4): Data Limit Hit, Fees Apply □ □ □ ■ Exit Submenu: Hold button 3 2 1 □ □ □ ■

Getting started

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

Inserting a SIM card

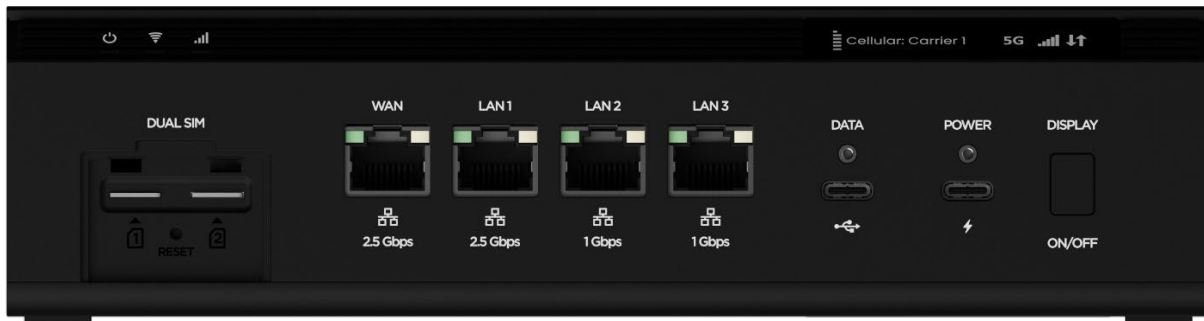
Your SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The FX4200 5G Cellular Router supports only Nano SIM cards. To insert a SIM card, select the correct SIM for this device.



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 insert a SIM card:

1. Remove the SIM cover on the front of the router.



3. If necessary, remove the SIM card from the protective sleeve, being careful not to touch the gold-colored contacts.
4. Insert the SIM card into one of the SIM slots ***notch first, with the gold-colored contact points facing down.***

NOTE: Should your SIM card be lost or damaged, contact your service provider.

Placing your router

The location of your router can directly affect performance. Follow these suggestions for placing your router:

- On or above ground level (not in a basement)
- Ideally on an exterior wall closest to the nearest cell tower
- Near a window but not in direct sunlight, with the back of the router facing out
- Clear from obstructions and interference from other electronic devices
- Outside of cabinets or locations that can get excessively hot

After your router is powered on, if necessary, you can adjust the placement using the device display and LEDs.

Connecting external antennas (optional)

Your FX4200 5G Cellular Router is equipped with four internal antennas. In addition, the device has four external full spectrum cell SMA ports (0.6–6 GHz each) to support four external antennas.

To use external antennas:

1. Remove the cover on the back of the router.



2. Finger tighten your external antennas to the external antenna ports.



3. Set the switch to **EXTERNAL ANTENNAS ON**. When enabled, each external port supports the full cellular frequency range of 0.6–6 GHz. Two of the internal antennas are disabled. The other two internal antennas remain active. An antenna icon  appears on the main screen of the device display.

NOTE: Contact your Account team for more information about external antennas.

Powering on

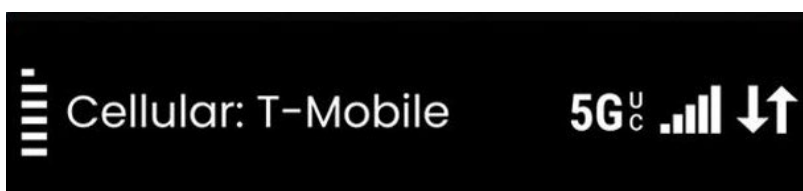
To power on your router, follow these steps:

1. Plug the USB C cable into the router power port. Plug the other end into any of the following:
 - 24W (12V, 2A) AC power adapter (provided)
 - USB-powered hub
 - USB-powered delivery device (laptop, computing station, another router, etc.)

WARNING! Use only the AC wall adapter power supply and cable that are packaged with the FX4200 5G Cellular Router. Using an unapproved wall adapter or cable are done at the risk of the user.

2. Wait for the router to power on. This can take up to three minutes. You'll know it's powered on when the device display shows your service provider and signal strength bars.

NOTE: The display times out after 60 seconds. If it is dark, press the button to the right.



3. If you have fewer than four bars, adjust the location of the router until you have four or five bars and the cellular status LED  is cyan (4 bars) or blue (5 bars).

NOTE: To power the router off, simply disconnect it from the power supply.

Mounting your FX4200 (optional)

The FX4200 has two multi-directional keyhole mounting points on the bottom of the device for wall or rack mounting.

Mounting suggestions:

- Use #4 or #6 (M3 or M3.5) screws or anchors.
- Use the appropriate type of screw or anchor:
 - For drywall, plaster, or masonry, use anchor screws.
 - For studs, use wood screws.
 - For metal, use metal screws.

Inseego recommends professional installation to assure safety when drilling near electrical lines, plumbing, or other hazards.

Pairing mesh nodes (optional)

Mesh nodes expand your network coverage and make it more reliable by adding extra paths for data to travel. This provides backups to data flow, creating a stronger, more dependable network that can cover larger areas.

Your FX4200 5G Cellular Router is compatible with the Inseego Wavemaker X700 Mesh Wi-Fi. For more information, visit go.inseego.com/.

Key things to know before connecting a mesh node with a router:

- Both the router and mesh node must be powered on and ready to pair.
- The router and mesh node should be close together to pair. You will place the mesh node after pairing.
- Pairing actions on the router and mesh node must occur within 30 seconds of one another when pairing via Wi-Fi.
- The multicolor LED on the X700, and the device display and Wi-Fi status LED on the FX4200 help guide the pairing process.

To pair an X700 mesh node to your FX4200 5G Cellular Router:

1. Power on the FX4200. When the **FX4200 Wi-Fi status LED**  **is solid green**, it is **ready to pair**.
2. Power on the X700. You can use the provided AC adapter, a USB-powered hub, or a USB-powered delivery device. **NOTE:** Using a USB-powered hub for setup allows you to find the best location without unplugging the router.

When the **X700 LED is blinking green**, it is **ready to pair**.

3. Pair the X700. You can pair your X700 with an Inseego FX4200 5G Cellular Router using Wi-Fi or Ethernet.

Pairing with Wi-Fi

To initiate Wi-Fi pairing, use the interactive device display on the FX4200 or the Admin web UI.

Pair using the FX4200 device display

- Press the **device display button** repeatedly until you see **Wi-Fi Mesh: Hold button to add**.
- Press and hold the **device display button**.
- When prompted by the display, press the **Mesh button** on the back of the X700 within 30 seconds.
- The LED on the X700 and the router blink blue while pairing. Pairing typically takes 2–3 minutes.
- When the display shows **Wi-Fi Mesh: Paired!** and the **LED on the mesh node is a solid color**, pairing is complete.

OR

Pair using the Admin web UI:

- Go to <http://192.168.1.1> to access the Admin web UI for the FX4200. Navigate to **Wi-Fi > Mesh**.
- Click **Add Node** on the UI Mesh tab.
- Within 30 seconds, press the **Mesh button** on the back of the X700.
- The LED on the X700 and the router blink blue while pairing. Pairing typically takes 2–3 minutes.
- When **Wi-Fi status LED on the router is solid blue** and the **LED on the mesh node is a solid color**, pairing is complete.

Pairing with Ethernet

- Connect an Ethernet cable from the X700 to the LAN port on the FX4200.
- Pairing is automatic. The LED on the X700 blinks blue while pairing. When pairing is complete the LED is solid.
- When you disconnect the Ethernet cable, the X700 remains paired via Wi-Fi.

Connecting devices to the router

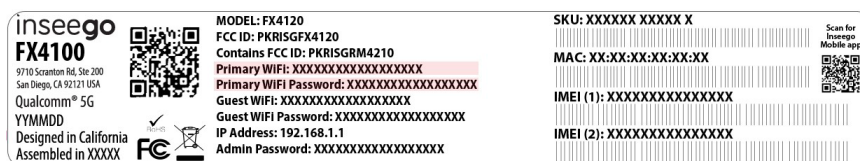
With your FX4200 5G Cellular Router, Wi-Fi devices and wired devices can connect to the mobile broadband network simultaneously.

Connecting devices wirelessly

You can connect to your 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 router is powered on, and the Wi-Fi status LED  is green (or blue if you have mesh).
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 router.



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

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.



* Ethernet ports are labeled with their default setting (WAN or LAN). You can configure either port to be WAN or LAN in the admin web UI: **Network > WAN**, or with Inseego Connect: **WAN Settings**.

To connect Ethernet devices:

1. Plug one end of an Ethernet cable into a WAN/LAN port on the router.
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 router.
2. Plug the other end of the cable into the USB port of the device you wish to connect.

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

Monitoring and managing your router

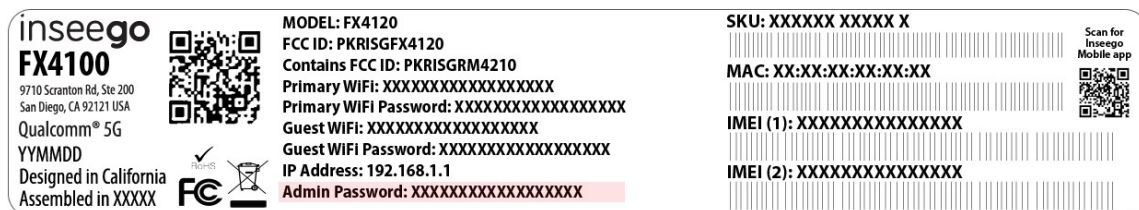
You can use the following options to monitor and manage your router.

Admin web UI

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

On a device connected to the 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 router. In order to securely set up the device, you are prompted to change the password upon login, see Changing the Admin password on page **Error! Bookmark not defined.**



Inseego Connect™

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

NOTE: Connected devices using IPv6 are not compatible with Fortinet VPN. Disable IPv6 on the connected device to use Fortinet.

Inseego Connect lets you configure settings, monitor status, and update the firmware on your device remotely from the cloud *. All T-Mobile owned Inseego FX devices come with the option of purchasing the Inseego Connect Add-on. Please work with your Account team to order the Inseego Connect Add-on, which provides Manager access.

Inseego Mobile app

You can use the same mobile app to perform basic device monitoring and management.

* When a device is deleted from Inseego Connect, all device-related information and user data associated with the device is removed from the system.

Caring for your router

This section provides information on replacing a SIM card, restoring your FX4200 5G Cellular Router to factory default settings, and general care tips.

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 FX4200 5G Cellular 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. Remove the SIM cover on the front of the router.



2. Remove the existing SIM card.
5. If necessary, remove the SIM card from the protective sleeve, being careful not to touch the gold-colored contacts.
6. 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 service provider.

Resetting your router

You can restart or reset your FX4200 5G Cellular Router to factory settings from the Admin web UI, Inseego Mobile app, Inseego Connect or by using the reset button on the router.

- **Restart** – reboots your router.
- **Factory Reset** – resets the router to factory settings

CAUTION! Factory reset returns your router 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 router from the Admin web UI, select **Settings > Backup and Restore**, then select **Restart** or **Restore factory defaults**.

Resetting from the Inseego Mobile app

To reset the router from the Inseego Mobile app, select **General Settings > Device Options**, then select **Restart** or **Factory Reset**.

Resetting from Inseego Connect

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

Resetting with the reset button

The reset button is located on the back of the router.

1. Verify that your router is powered on.
2. Locate the reset button on the back of your router.
3. **To reboot the router:**
Press the reset button for one second.

To reset the router to factory settings:

Press the reset button for five seconds until the device resets. The LED blinks white, then turns red. When it is green or blue, your router is ready.

NOTE: The first time you perform a factory reset, it may take over two minutes for your router to restart.

Care tips

Inseego recommends the following care guidelines:

- Avoid locating the router in areas that can get excessively hot, such as in direct sunlight or in a small, enclosed cabinet without ventilation. Excessive heat may impact performance.
- 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 a dry and secure location when not in use.

2

Configuration

Overview

Admin password

Managing devices

Managing your network

Managing routing

Managing security

Using tools

Setting administrative options

Overview

You can configure your FX4100 5G Cellular Router 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.

You can use the following tools for configuring your router:

- **Admin web UI** – Provides local access to configure and manage your router. On a device connected to the 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 router.
- **Inseego Connect** – Inseego Connect lets you configure settings, monitor status, and update the firmware on your device remotely from the cloud. All T-Mobile owned Inseego FX devices come with the option of purchasing the Inseego Connect Add-on. Please work with your Account team to order the Inseego Connect Add-on, which provides Manager access.
- **Inseego Mobile app** – Use the mobile app to perform basic device monitoring and management.

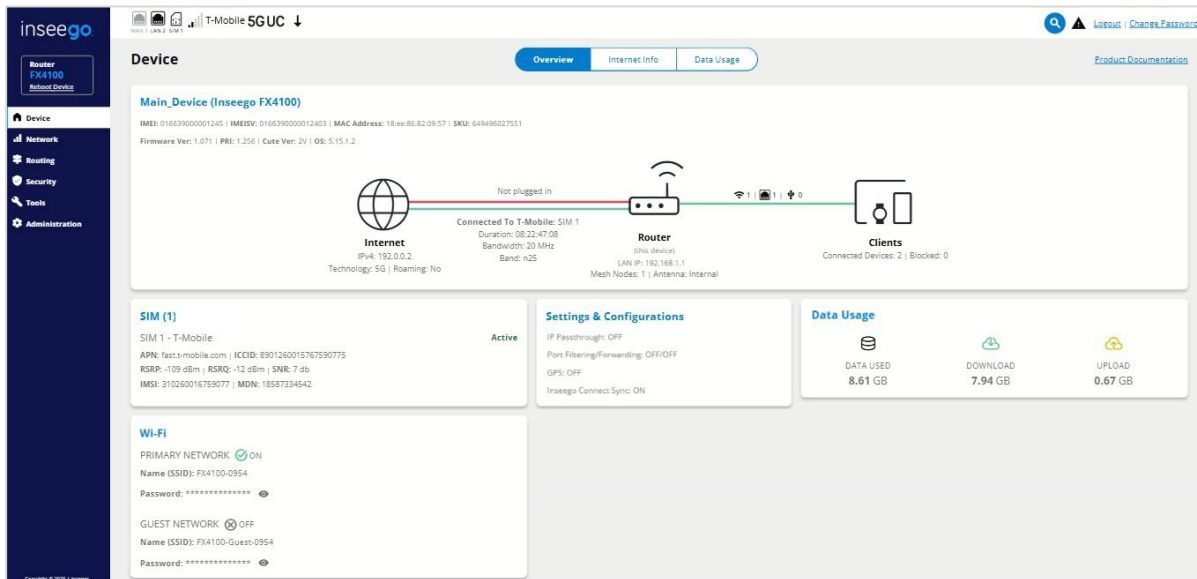
This chapter provides the configuration options available for your FX4100 5G Cellular Router. The configurations shown are from the admin web UI, unless otherwise noted. Many of these options are also available with Inseego Mobile app and Inseego Connect. Some configurations are available only with Inseego Connect and are marked as such.

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

NOTE: Connected devices using IPv6 are not compatible with Fortinet VPN. Disable IPv6 on the connected device to use Fortinet.

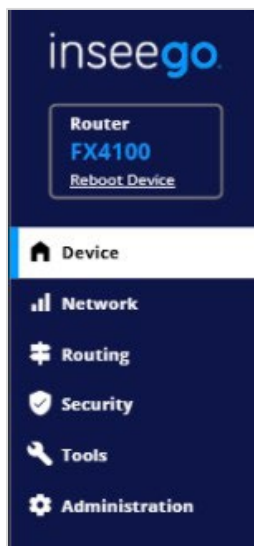
Home page

The home page of the admin web UI is the Device > Overview tab, which displays the device status, SIM information, some common settings, current Wi-Fi networks and passwords, and data usage information. Once you log in, links are available for more information and management options. See the Overview tab on page 30.



Navigation tips

- Each screen in the admin web UI includes a menu on the left that you can use to navigate to other pages. The current page is indicated by a blue bar. A similar side menu is available when configuring devices with Inseego Connect.



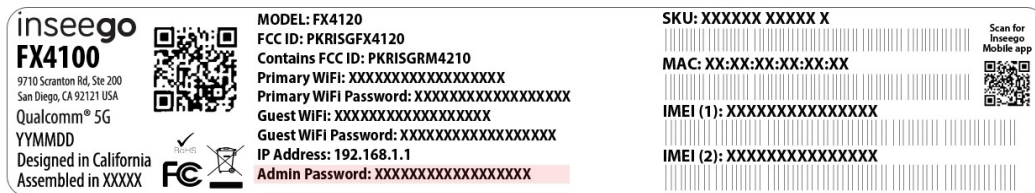
- You can search for a topic by clicking on the search icon  in the upper right of any page and selecting a topic from the dropdown list.

Getting help

Click on [Help](#) in the upper right-hand corner of a tab or section to view help on that topic.

Admin password

The admin password is what you use to sign into the admin web UI. A default admin password is assigned to each individual device and is printed on the bottom of the device.



In order to securely set up your router, you are prompted to change the admin password upon login. 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.

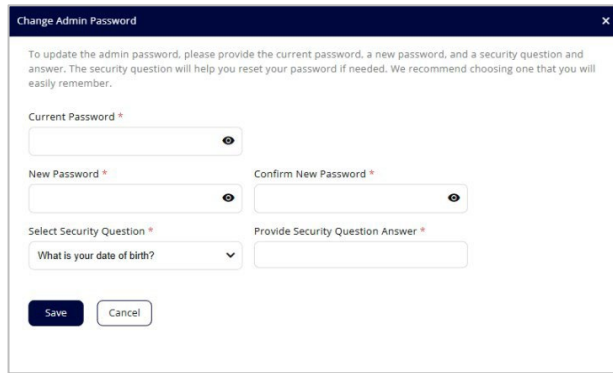
NOTE: You can set up separate Wi-Fi passwords for both primary and guest networks in **Wi-Fi**, but these are different from the admin password, which is for this web user interface.

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 **Change Password** in the upper right.

A screenshot of a web browser window titled "Change Admin Password". The window has a dark blue header bar with the title and a close button. Below the header, there is a paragraph of text: "To update the admin password, please provide the current password, a new password, and a security question and answer. The security question will help you reset your password if needed. We recommend choosing one that you will easily remember." Below this text are four input fields: "Current Password *" (a text box with a toggle icon), "New Password *" (a text box with a toggle icon), "Confirm New Password *" (a text box with a toggle icon), "Select Security Question *" (a dropdown menu), and "Provide Security Question Answer *" (a text box). The dropdown menu is currently set to "What is your date of birth?". At the bottom of the form are two buttons: "Save" (a dark blue button) and "Cancel" (a light blue button).

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

2. Enter your current admin password, then enter a new password and confirm it.
NOTE: The new password must have a length between 14 and 32 characters and contain at least one special character and number.
3. Select a security question from the dropdown and type an answer to the question.
NOTE: Answers are case-sensitive.
4. Click **Save**.

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

Managing devices

Overview tab

The Device Overview tab is the home page of the admin web UI. Use it to view information about your router at a glance. You can see an overview of your router and network, SIM information, some common settings, current Wi-Fi networks and passwords, and data usage stats. Use the links to jump to a specific topic for more details and configuration options, or navigate using the side menu

Device Overview

Main_Device (InseeGo FX4100)
IMEI: 01663900001245 | IMEIsv: 016639000012403 | MAC Address: 18:ee:86:82:09:57 | SKU: 649496027551
Firmware Ver: 1.071 | PB: 1.256 | Cate Ver: 2V | OS: 5.15.1.2 [update](#)

Internet
IPV4: 192.0.0.2
Technology: 5G | Roaming: No

Router
Connected To T-Mobile: SIM 1
Duration: 08:22:47:08
Bandwidth: 20 MHz
Band: n25
LAN IP: 192.168.1.1
Mesh Nodes: 1 | Antenna: Internal

Clients
Connected Devices: 2 | Blocked: 0 [view](#)

SIM (1) [view details](#)
SIM 1 - T-Mobile
APN: fast-t-mobile.com | ICCID: 8901260015767590775
RSRP: -109 dBm | RSRQ: -12 dBm | SNR: 7 db
IMSI: 31026016759077 | MDN: 18887334542

Settings & Configurations
IP Passthrough: OFF
Port Filtering/Forwarding: OFF/ON
GPS: OFF
InseeGo Connect Sync: ON

Data Usage
DATA USED: 8.61 GB
DOWNLOAD: 7.94 GB
UPLOAD: 0.67 GB

Wi-Fi
PRIMARY NETWORK: ON
Name (SSID): FX4100-0954
Password: *****
GUEST NETWORK: OFF
Name (SSID): FX4100-Guest-0954
Password: *****

Internet Info tab

The Internet Info tab provides internet status and internet session information.

Internet Info

Internet Status [info](#)

General

Status: Connected	IPv4 Address: 192.0.0.2	IPv6 Address: 2607:fb90:732c:cead:95be:b994:dcf0:394e
Network Name: T-Mobile	Mask: 255.255.255.224	
Technology: 5G	Gateway: 192.0.0.1	
Time Connected: 00:00:08:25	DNS: 192.0.0.30	

Internet Sessions [info](#)

Internet Sessions from 07/23/2025 03:46:12 PM to 07/23/2025 03:46:12 PM

Total Records (1) [Export](#)

Date/Time	Duration	Received Data	Transmitted Data	Total Data	IPv4 Address	IPv6 Address
12/31/1969 04:00:00 PM	00:00:00:00	0 B	0 B	0 B	192.0.0.2	2607:fb90:732c:cead:95be:b994:dcf0:394e

Internet Status

Use this section to view general internet connection and system information.

Internet Status			Help
General	IPv4	IPv6	
Status: Connected	IP Address: 192.0.0.2	IP Address: 2607:fb90:732c:cead:95be:b994:dcf0:394e	
Network Name: T-Mobile	Mask: 255.255.255.224		
Technology: 5G	Gateway: 192.0.0.1		
Time Connected: 00:00:08:25	DNS: 192.0.0.30		

General

Status: The current status of the router connection.

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

Technology: Indicates the current type of 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.

IPv4

IP Address: The internet IP address assigned to the router.

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 router.

IPv6

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

Internet Sessions

Use this section to export and view internet session data.

Internet Sessions						
Internet Sessions from 08/07/25 12:41:17 PM to 08/21/25 10:51:46 AM						
Total Records (26)						
Date/Time	Duration	Received Data	Transmitted Data	Total Data	IPv4 Address	IPv6 Address
08/07/25 12:41:17 PM	00:00:00:27	210.86 KB	128.87 KB	339.72 KB	192.0.0.2	2607:f090:7353:689:52d:6d4:a24f:2712
08/07/25 12:41:48 PM	00:01:01:05	45.68 MB	8.42 MB	54.10 MB	192.0.0.2	2607:f090:7353:689:52d:6d4:a24f:2712

Total Records

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.

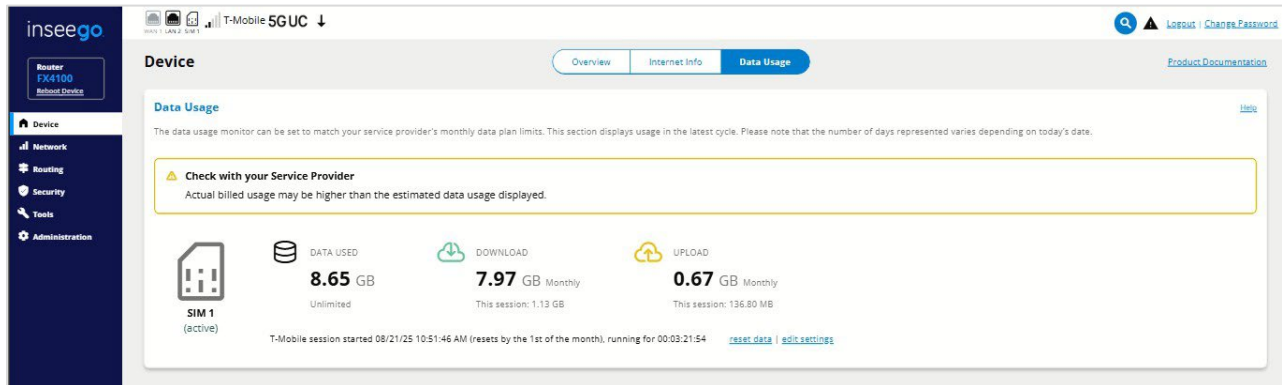
IPv6 Address: The global IPv6 address for the session (blank if IPv6 is turned off or is not supported by the current network connection or service provider).

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

Data Usage tab

Use the Data Usage tab to view details and manage your router's data usage.

NOTE: Your FX4100 provides only a rough estimate of data usage. Always check with your service provider for exact usage.



The data usage tab displays:

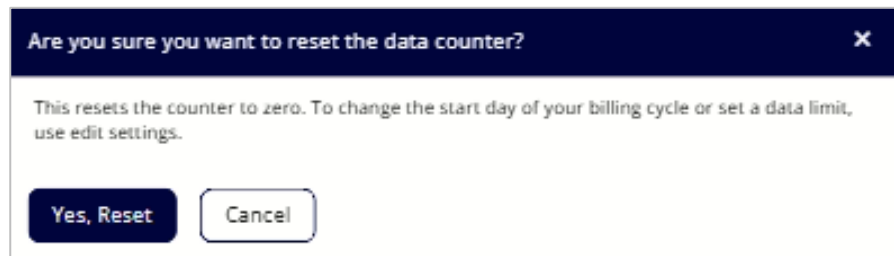
DATA USED: An estimate of the amount of data used in the current billing cycle.

DOWNLOAD: An estimate of the amount of data downloaded in the current billing cycle, as well as the amount of data downloaded during the current internet session.

UPLOAD: An estimate of the amount of data uploaded in the current billing cycle, as well as the amount of data uploaded during the current internet session.

A timestamp of when the current internet session started, how long it has been running, and when the data counter is set to restart.

Click **reset data** to restart the data counter. **NOTE:** This only resets the display; to change the start day of your billing cycle or set a data limit, use **edit settings**.



Click **edit settings** to configure settings to reflect your monthly data plan.

Edit Data Usage Settings (SIM 1) X

Reset Data Counter (day of month)

1 ▼

☐ Metered Connection

0.00 GB

Save Cancel

Reset Data Counter (day of the month): Use the dropdown to select a day of the month for the usage data to reset.

Metered Connection: Check this box if there is a data limit on your plan, then enter a maximum data limit in the box below.

Click **Save** to enact changes.

Managing your network

Use Network tabs to view and configure settings for your router's network.

The Network page includes the following tabs:

- Cellular
- Wi-Fi
- Ethernet
- WAN
- LAN
- Devices
- DNS

Cellular tab

Use this tab to set options for the cellular network.

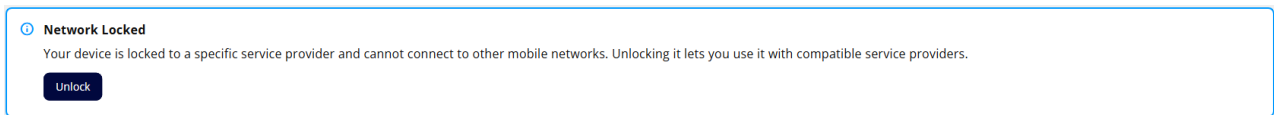
The screenshot shows the 'inseeGO' web interface for the 'Network' settings, specifically the 'Cellular' tab. The interface includes a sidebar with navigation options: Router, Device, Network (selected), Routing, Security, Tools, and Administration. The main content area is titled 'Network' and features tabs for Cellular, Wi-Fi, Ethernet, LAN, WAN, Devices, and DNS. The 'Cellular' tab is active, displaying several configuration sections:

- Network Locked:** A message stating 'Your device is locked to a specific service provider and cannot connect to other mobile networks. Unlocking it lets you use it with compatible service providers.' with an 'Unlock' button.
- Cellular Network Technology:** Includes 'Antenna Status: Internal', 'Network Technology' (set to 'Auto (4G LTE / 5G)'), and '5G Network Mode' (set to 'Auto (NSA / SA)'). There are 'Save' and 'Cancel' buttons.
- Cellular Settings:** Includes three toggle switches: 'Allow Device to Connect To a Mobile Network' (on), 'While Roaming' (on), and 'Automatically Select Network' (on). It also shows 'Connected Network: T-Mobile 5G'.
- SIM Lock Settings:** Includes a message 'No SIM Card' stating 'This device requires a SIM card to connect to the mobile network. Insert a SIM card or make sure the SIM card is properly positioned.'
- Data Transmission Setting:** Includes a text box for 'Maximum Transmission Unit (MTU)' set to '0' bytes, with 'Save' and 'Cancel' buttons.
- APN Connection Profiles:** Includes a description of APN profiles and a table for 'Connection Profiles (0)'. The table has columns for 'Active Profile', 'Profile Name', 'APN Name', 'Authentication', 'IP Connection Type', and 'Actions'. It currently shows 'No results found' and an 'Add Connection Profile' button.

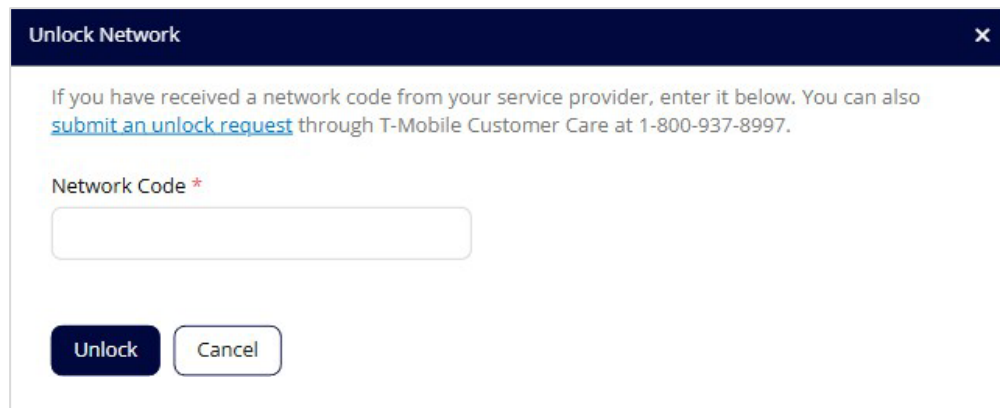
The footer of the interface includes 'Copyright © 2023 | inseeGO' and 'www.inseeGO.com'.

Network Locked

Locked devices can only use the network currently provided by the service provider. Use this section if you want to unlock your router to use with a different service provider.



To unlock a locked device, click **Unlock**. The Unlock Network popup appears:

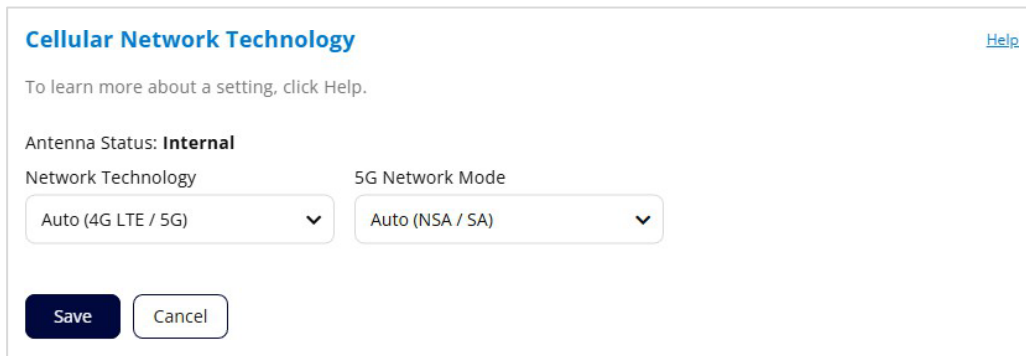
A dark blue header bar with the text "Unlock Network" and a white 'x' icon on the right. Below the header, the text reads: "If you have received a network code from your service provider, enter it below. You can also [submit an unlock request](#) through T-Mobile Customer Care at 1-800-937-8997." Below this text is a label "Network Code" followed by a red asterisk. Underneath the label is a white text input field. At the bottom of the form are two buttons: a dark blue "Unlock" button and a white "Cancel" button with a dark blue border.

To obtain a network code, click the **submit an unlock request** link, or follow the directions to contact T-Mobile Customer Care. Enter the code in the **Network Code** text box and click **Unlock**.

NOTE: if your device is unlocked, this section does not appear.

Cellular Network Technology

Use this section to configure the network technology and 5G network mode for your router. You can also view whether external antennas are enabled.



The screenshot shows a configuration page titled "Cellular Network Technology" with a "Help" link in the top right. Below the title is a note: "To learn more about a setting, click Help." The "Antenna Status" is set to "Internal". There are two dropdown menus: "Network Technology" set to "Auto (4G LTE / 5G)" and "5G Network Mode" set to "Auto (NSA / SA)". At the bottom are "Save" and "Cancel" buttons.

Antenna State: Internal indicates the external antenna switch is set to **EXT.ANT. OFF** and all four internal antennas are enabled. **External** indicates the switch is set to **EXT.ANT.ON**.

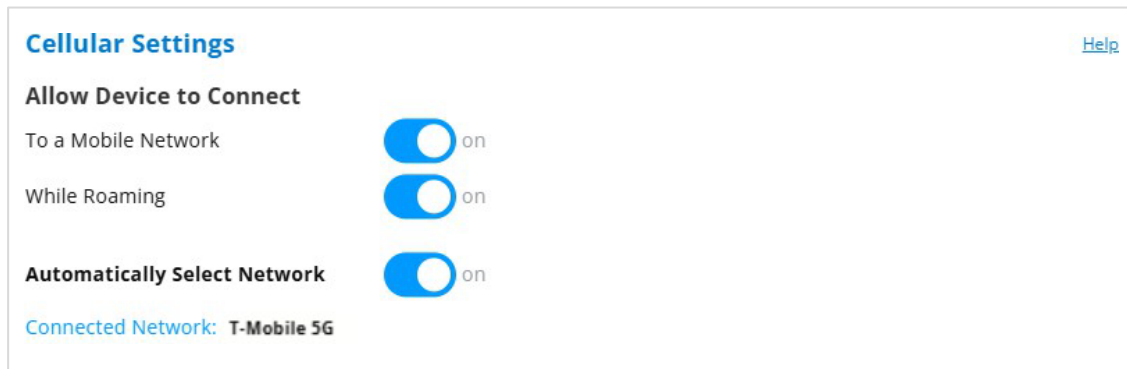
Network Technology: Your router is set to Auto (4G LTE/5G) by default, which prioritizes 5G but allows 4G and other non-5G technologies to be used. If you select 4G LTE or 5G from the dropdown, your router is restricted from connecting to networks not using that technology, for example, if you select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

5G Network Mode: Your router 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 dropdown to select standalone (SA) or non-standalone (NSA) 5G network modes.

Click **Save**.

Cellular Settings

Use this section if you want to temporarily turn off your network completely, or turn it off while roaming. You can also turn off automatic network selection to manually select a network.



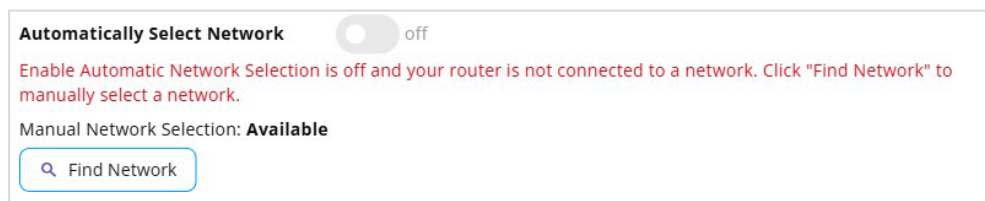
Allow Device to Connect

To a Mobile Network: Use the slider when necessary to turn off cellular data and prevent access to the mobile network. **NOTE:** This prevents connected devices from connecting to the internet and using your router's mobile data plan. **For normal operation, this setting must be left on.**

While Roaming: Use the slider to turn international and domestic roaming on or off as needed. Additional data charges may apply when roaming.

Automatically Select Network: When **on**, your router automatically selects the best available 5G network and you cannot manually select a network.

When **off**, you must manually select a network by clicking **Find Network** and choosing a network.



Find Network: You may wish to manually select a network if multiple networks are available and you have a preference. Click the button to scan for available networks, then choose the preferred network and click **Save**.

NOTE: This option is available only if **Automatically Select Network** is **off**.

Connected Network: The name of the network to which the router is currently connected.

SIM Lock Settings

The SIM card in your 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 section to lock or unlock your SIM or enter a SIM PIN.

SIM Lock Settings [Help](#)

To provide additional security you can lock the SIM card with a PIN. Once locked, PIN must be provided and verified before a device can connect to the internet.

Current PIN *

0 attempts remains until your SIM is PUK locked

Once the device is PUK locked, you will be unable to use the device and will need to contact [T-Mobile] customer support.

Turn On PIN Lock

Current PIN: Enter the current PIN.

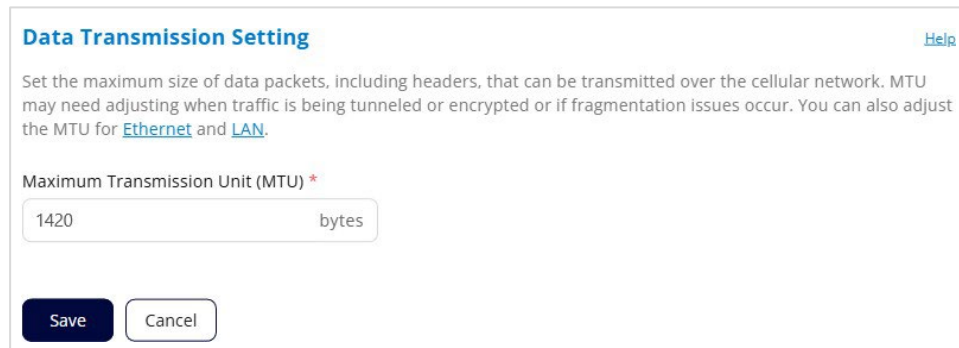
The button shows one of the following options.

- **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.
- **PIN Lock** – If the SIM is currently PIN locked, you are prompted to enter the PIN.
NOTE: If an incorrect PIN is entered too many times, the SIM becomes PUK locked. A counter indicates how many incorrect entries will cause PUK lock. Once PUK locked, the PUK must be obtained from your service provider.
- **PUK Lock** – If the SIM is currently PUK locked, the only possible operation is to enter the PUK. **NOTE:** If an incorrect PUK is entered too many times, the SIM becomes permanently unusable. You will need to obtain a new SIM.

Data Transmission Setting

Use this section to set the maximum transmission unit (MTU) for the cellular network. This is the maximum size of data packets, including headers, that can be transmitted. You might want to adjust the MTU when traffic is being tunneled or encrypted, or if you are noticing fragmentation issues.

NOTE: You can also adjust the MTU for your WAN Ethernet connection on the Ethernet tab, and for your LAN network on the LAN tab.



The screenshot shows a web interface titled "Data Transmission Setting" with a "Help" link in the top right. Below the title is a descriptive paragraph: "Set the maximum size of data packets, including headers, that can be transmitted over the cellular network. MTU may need adjusting when traffic is being tunneled or encrypted or if fragmentation issues occur. You can also adjust the MTU for [Ethernet](#) and [LAN](#)." Below this text is a label "Maximum Transmission Unit (MTU) *" followed by a text input field containing "1420" and a "bytes" unit selector. At the bottom are two buttons: "Save" and "Cancel".

Maximum Transition Unit (MTU): The default (1420 bytes) is the recommended MTU for your cellular network. You can enter a different value between 1280 and 1500 bytes.

APN Connection Profiles

In most configurations, the FX4100 is used with a dynamic IP and SIM and the Access Point Name (APN) is available from the network, for example: *internet*. However, if you are on a private network, you may need to configure connection profiles for your APN in this section for the network to communicate with the router.

APN Connection Profiles

An APN (Access Point Name) connection profile is a set of configurations that your device uses to connect to the internet and other services over your service provider's mobile network. You can define additional connection profiles, but only one can be used (i.e., active) at a time.

Connection Profiles (2) [Add Connection Profile](#)

Active Profile	Profile Name	APN Name	Authentication	IP Connection Type	Actions
☒	Broadband	fast.l-mobile.com	None	IPv4/IPv6	edit reset default
☐	Test	MikeTest	PAP	IPv4/IPv6	edit delete

Connection Profiles

This table lists all the APN connection profiles that have been defined. The number of profiles appears next to this title.

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

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

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

Profile Name: The name that identifies the connection profile.

APN Name: The access point name.

Authentication: The authentication method for the connection profile.

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

Actions: Click **edit** to edit a profile. Click **reset default** to reset a profile to default values.

Add Connection Profile: Click this button to add an additional APN connection profile.

Add Connection Profile

You can select an APN from your service provider in the APN dropdown or select "Add APN" to create a custom APN and enter a name in the box below. If authentication is needed, provide the username and password.

Profile Name *

Authentication * None

IP Connection Type * IPv4/IPv6

APN * Add APN

Add **Cancel**

- **Profile Name:** Enter a name to identify this connection profile.
- **IP Connection Type:** Select an IP connection type from the dropdown (IPv4, IPv6, or IPv4/IPv6).
- **APN:** Select an APN supplied by your service provider from the dropdown or select **Add APN** and enter the APN for your private network in the text box that appears below.
- **Authentication:** Select the authentication method for your private network from the dropdown (None, PAP, CHAP, or PAP and CHAP).
- **Username:** Enter the username for your private network.
NOTE: This option is not visible when **Authentication** is set to **None**.
- **Password:** Enter the password for your private network.
NOTE: This option is not visible when **Authentication** is set to **None**.

Click **Add**.

Wi-Fi tab

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

inseeGo Router FX4100 Reboot Device

Network

Cellular **Wi-Fi** Ethernet LAN WAN Devices DNS

Wi-Fi Settings

These settings apply regardless of which network (primary, guest, or both) is in use. WARNING: Changes made to the Wi-Fi settings may prevent some Wi-Fi devices from connecting to this router.

Allow Wi-Fi Devices to Connect to this Device ☒ on

Enable Mesh Network ☒ on

Warning!
Before enabling your mesh network, check that the Security field in both the primary and guest networks is set to something other than None. If set to None, the network will lose Wi-Fi connection.

Enable Dynamic Frequency Selection (DFS) ☒ on

Enable Multi-Link Operation (MLO) ☒ on

When MLO is enabled, the router determines the optimal band settings. When turning MLO on, ensure either the primary or guest network has both the 2.4GHz and 5GHz band selected. To manually select band settings, turn MLO off and adjust the BAND SELECTION and BAND SETTINGS options.

BAND SELECTION

	2.4GHz	5GHz
Primary Network	☒	☒
Guest Network	☐	☐

BAND SETTINGS

	2.4GHz	5GHz
Wi-Fi Standard	Wi-Fi 7 (802.11 bgn/ax/be)	Wi-Fi 7 (802.11 acn/ax/be)
Bandwidth	20 MHz	160 MHz
Channel	Automatic	Automatic

Save Cancel

Primary Network

SECURITY TIP: Share your guest network instead of your primary network.

Network Name (SSID) *

FX4100-09EA

Security *

WPA3/WPA2 Transition

Warning!
Do not set Security to None when Enable Mesh Network is on. If set to None when mesh is enabled, the network will lose Wi-Fi connection.

Password: *

..... Generate

Note: Enter a new password or use the Generate button. The password must have a length of at least 11 characters and contain at least one special character, letter, and number.

☒ Hide Password on Display

☒ Broadcast Primary Network (SSID)

☐ Wi-Fi Privacy Separation

Save Cancel

Guest Network

SECURITY TIP: For added security, share this (guest) network.

Network Name (SSID) *

FX4100-Guest-09EA

Security *

WPA3/WPA2 Transition

Warning!
Do not set Security to None when Enable Mesh Network is on. If set to None when mesh is enabled, the network will lose Wi-Fi connection.

Password: *

..... Generate

Note: Enter a new password or use the Generate button. The password must have a length of at least 11 characters and contain at least one special character, letter, and number.

☒ Broadcast Guest Network (SSID)

☒ Wi-Fi Privacy Separation

Save Cancel

Mesh Network

Using mesh nodes helps extend the coverage area of your network, mitigate dead spots, and establish a stronger and more reliable connection. To create a mesh network, connect at least one mesh node.

Mesh Router (1)

Name	Device	IMEI	Connection Type	IP Address	Connection Status	Clients
MainRouter	FX4100	016639000001492	Wi-Fi	192.168.1.1	Online	1

Mesh Nodes (0)

Add Node

Name	Device	Serial No	Connection Type	IP Address	Connection Status	Signal Strength	Clients	Actions
X700-559e	X700	AU100325G00069	Wi-Fi (2.4G)	192.168.1.187	Great	-3 dBm	1	Remove Add Node

Copyright © 2025 | inseeGo
www.inseeGo.com

Wi-Fi Settings

You can use this section to turn Wi-Fi off, disable a mesh network, turn off DFS, or disable MLO in order to select bands and band settings manually.

Wi-Fi Settings

These settings apply regardless of which network (primary, guest, or both) is in use. WARNING: Changes made to the Wi-Fi settings may prevent some Wi-Fi devices from connecting to this router.

Allow Wi-Fi Devices to Connect to this Device ☒ on

Enable Mesh Network ☒ on

Warning: Before enabling your mesh network, check that the Security field in both the primary and guest networks is set to something other than None. If set to None, the network will lose Wi-Fi connection.

Enable Dynamic Frequency Selection (DFS) ☒ on

Enable Multi-Link Operation (MLO) ☒ on

When MLO is enabled, the router determines the optimal band settings. When turning MLO on, ensure either the primary or guest network has both the 2.4GHz and 5GHz band selected. To manually select band settings, turn MLO off and adjust the BAND SELECTION and BAND SETTINGS options.

	2.4GHz	5GHz
BAND SELECTION		
Primary Network	☒	☒
Guest Network	☐	☐
BAND SETTINGS		
Wi-Fi Standard	Wi-Fi 7 (802.11 bgn/ax/be)	Wi-Fi 7 (802.11 acn/ax/be)
Bandwidth	20 MHz	160 MHz
Channel	Automatic	Automatic

Save Cancel

Allow Wi-Fi Devices to Connect to this Device: Wi-Fi is **on** by default. If it is turned **off**, all Wi-Fi connected devices, including mesh nodes, are disconnected from your FX4100 and all other setting options on this page disappear. The only way to connect devices will be with an Ethernet cable or USB. You will need to pair each node again once you turn Wi-Fi back on.

NOTE: This selection affects both the primary and guest network.

Enable Mesh Network: The mesh network is **on** by default, allowing you to use mesh nodes to expand your network coverage. If it is turned **off**, all mesh nodes are disconnected from the network, and you cannot add new nodes. Client devices should automatically reconnect directly to the router. You will need to pair each node again once you turn mesh back on.

NOTE: Use the **Mesh Network** section below to add and manage mesh nodes.

Enable Dynamic Frequency Selection (DFS): DFS is **on** by default. DFS enables wireless routers operating on 5GHz to monitor for, and detect, other radar systems, such as weather, military, or airport radars and switch to another channel automatically.

Enable Multi-Link Operation (MLO): MLO is **on** by default. MLO allows the device to simultaneously utilize multiple frequency bands, ensuring seamless data flow. When enabled, the system automatically determines the best bands and settings, and the BAND SELECTION and BAND SETTINGS sections to the right are read-only.

NOTE: When enabling MLO, ensure that either the primary and/or guest network has both bands (2.4 GHz and 5 GHz) enabled.

BAND SELECTION

NOTE: This section is read-only by default. To select bands, the **Enable Multi-Link Operation (MLO)** slider to the left must be **off**.

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.

BAND SETTINGS

Wi-Fi Standard: Use the dropdown to select a Wi-Fi standard.

Bandwidth: Leave bandwidth at the default setting unless you experience interference with other Wi-Fi devices.

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

Click **Save** to enact new settings.

Primary Network

Use this section to change settings for your primary Wi-Fi network, including changing the name and password. Connected devices use the settings shown in this section to connect to the primary Wi-Fi network.

Primary Network

[Help](#)

SECURITY TIP: Share your guest network instead of your primary network.

Network Name (SSID) *

Security *

WPA3/WPA2 Transition

Warning!
Do not set Security to None when Enable Mesh Network is on. If set to None when mesh is enabled, the network will lose Wi-Fi connection.

Password: *

Generate

Note: Enter a new password or use the Generate button. The password must have a length of at least 11 characters and contain at least one special character, letter, and number.

☒

 Hide Password on Display

☒

 Broadcast Primary Network (SSID)

☐

 Wi-Fi Privacy Separation

Save

Cancel

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

Network Name (SSID): To set up or change your primary network name, enter a name (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 Only** can be used for WPA3 devices.
- **WPA2 Personal PSK (AES)** can be used for WPA2 devices.
- **None** allows others to monitor your Wi-Fi traffic and use your data plan to access the internet. **NOTE: Do not** select None when **Enable Mesh Network** is on. **If you select None while mesh is enabled, the network will lose Wi-Fi connection.**

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

NOTE: The password must have a length of at least 11 characters and contain at least one letter, number, and special character. You can click the eye icon to view the password.

IMPORTANT: In order to securely set up your network, it is critical that you change the password from the default. Use a different password from your admin password to keep the device and your network secure.

Generate: This button inserts a strong random password in the Password field. You can click the eye icon to view the password.

Hide Password on Display: This option is checked by default, so that the Wi-Fi primary network password is not shown on the device display. If you choose to uncheck this option, the primary network password is visible on the device display (see **Error! Reference source not found.** on page **Error! Bookmark not defined.**).

Broadcast Primary Network (SSID): This option is checked by default, allowing the Wi-Fi primary network to be displayed in the list of available Wi-Fi networks on connecting client devices. If you choose to uncheck this option, this network is not visible to connecting client devices.

Wi-Fi Privacy Separation: Check this box to keep each connected client device on this network isolated from all other connected client devices. This provides additional security if some connected client devices are unknown or not completely trusted.

NOTE: For normal operation, this should be unchecked.

Select **Save**.

Guest Network

The guest Wi-Fi network allows you to segregate traffic to a separate network rather than share access to your primary Wi-Fi network. Use settings in this section to set up or change guest Wi-Fi network information. Connected devices must use the Wi-Fi settings shown in this section to connect to the guest Wi-Fi network.

NOTE: To turn the Wi-Fi guest network on, you must select at least one band for the guest network under **BAND SELECTION** in the **Wi-Fi Settings** section and then select **Save**.

Guest Network

[Help](#)

SECURITY TIP: For added security, share this (guest) network.

Network Name (SSID) *

Security *

WPA3/WPA2 Transition ▼

Warning!
Do not set Security to None when Enable Mesh Network is on. If set to None when mesh is enabled, the network will lose Wi-Fi connection.

Password: *



Generate

Note: Enter a new password or use the Generate button. The password must have a length of at least 11 characters and contain at least one special character, letter, and number.

☒ Broadcast Guest Network (SSID)

☒ Wi-Fi Privacy Separation

Save

Cancel

Network Name (SSID): To set up or change your guest network name, enter a name (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 Only** can be used for WPA3 devices.
- **WPA2 Personal PSK (AES)** can be used for WPA2 devices.
- **None** allows others to monitor your Wi-Fi traffic and use your data plan to access the internet. **NOTE: Do not** select None when **Enable Mesh Network** is on. **If you select None while mesh is enabled, the network will lose Wi-Fi connection.**

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

NOTE: The password must have a length of at least 11 characters and contain at least one letter, number, and special character. You can click the eye icon to view the password.

IMPORTANT: It is critical that you use a different password from your admin and primary Wi-Fi network password to keep the device and your network secure.

Generate: This button inserts a strong random password in the Password field. You can click the eye icon to view the password.

Broadcast Primary Network (SSID): This option is checked by default, allowing the Wi-Fi guest network to be displayed in the list of available Wi-Fi networks on connecting client devices. If you choose to uncheck this option, this network is not visible to connecting client devices.

Wi-Fi Privacy Separation: Check this box to keep each connected client device on this network isolated from all other connected client devices. This provides additional security if some connected client devices are unknown or not completely trusted.

NOTE: For normal operation, this should be unchecked.

Select **Save**.

Mesh Network

Use this section to pair with a mesh node and monitor the mesh nodes in your Wi-Fi network.

Mesh Network

Using mesh nodes helps extend the coverage area of your network, mitigate dead spots, and establish a stronger and more reliable connection. To create a mesh network, connect at least one mesh node.

Mesh Router (1)

Name	Device	IMEI	Connection Type	IP Address	Connection Status	Clients
MainRouter	FX4100	01663900001492	Wi-Fi	192.168.1.1	Online	1

Mesh Nodes (0)

Add Node

Name	Device	Serial No	Connection Type	IP Address	Connection Status	Signal Strength	Clients	Actions
X700-559e	X700	AU100325G00069	Wi-Fi (2.4G)	192.168.1.187	Great	-3 dBm	1	

Mesh Router

This table provides information on your FX4100(s).

Name: The name of the router and an icon for the type of connection. You can edit the name using the pencil icon . (This only changes the name in this UI.)

Device: The model of the router.

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

Connection Type: The type of connection the router is using to connect with the admin web UI.

IP Address: The internet IP address assigned to the router.

Connection Status: The connection status of the router.

Clients: The number of client devices connected to the router. Click on the number to view detailed information on connected client devices.

Mesh Nodes

This table provides information on the mesh nodes in your network.

Name: The name of the mesh node and an icon for the type of connection. You can edit the name using the pencil icon . (This only changes the name in this UI.)

Device: The model of the mesh node.

Serial No: The serial number of the mesh node.

Connection Type: The type of connection the mesh node is using to connect with the router.

IP Address: The internet IP address assigned to the mesh node.

Connection Status: The connection status of the mesh node.

Signal Strength: The strength of the network signal. **NOTE:** Ethernet and USB connections display a line instead of a value.

Clients: The number of client devices connected through the mesh node. Click on the number to view detailed information on connected client devices.

Actions: Click **remove** to remove the mesh node from your network. Click **reboot** to restart the mesh node.

Adding a mesh node

You can add a mesh node using the **Add Node** button in this section:

1. Power on the **X700**. You can use the provided AC adapter, a USB-powered hub, or a USB-powered delivery device.
2. When the **X700 LED is blinking green**, it is **ready to pair**. Make sure the router and mesh node are within 10 to 50 feet of each other and click the **Add Node** button on this web UI page.
3. Within 30 seconds, press the **Mesh button** on the back of the X700.
4. The LED on the X700 and the Wi-Fi status LED on the router blink blue while pairing. Pairing typically takes 2–3 minutes.
5. When the **Wi-Fi status LED  on the router is solid blue** and the **LED on the mesh node is a solid color**, pairing is complete.

NOTE: You can also add a mesh node using the device display button on the FX4100, or by connecting to the mesh node via Ethernet. See **Error! Reference source not found.** on page **Error! Bookmark not defined.** for more information.

Ethernet tab

Use this tab to configure Ethernet ports. Although Ethernet ports are labeled as WAN/LAN or LAN on the device, you can set either of them to be a WAN or LAN connection. **NOTE:** Only one port can be set to WAN at a time.

Configure Ethernet Ports

You can configure either Ethernet port to be a WAN or LAN connection. Note: Only one port can be set to WAN at a time. Set the maximum size of data packets, including headers, that can be transmitted over the Ethernet WAN connection. You can also adjust this setting for [Cellular](#) and [LAN](#).

Status	Port	Use Connection	Maximum Transmission Unit (MTU)
Offline	Ethernet 1	WAN	1500
Offline	Ethernet 2	LAN	1500

Save Cancel

Status: The status of the interface (Connected, Online, Offline).

Port: Ethernet 1 is the port on the left labeled WAN/LAN on the router; Ethernet 2 is the port on the right labeled LAN.

Use Connection: Use the dropdown to select WAN or LAN for the type of Ethernet connection you want on each port.

NOTE: When IP Passthrough is turned on, you cannot configure Ethernet ports as WAN.

Maximum Transition Unit (MTU): MTU is the maximum size of data packets, including headers, that can be transmitted. You might want to adjust the MTU when traffic is being tunneled or encrypted, or if you are noticing fragmentation issues. The default (1500 bytes) is the recommended MTU for your FX4100 WAN Ethernet connection. You can enter a different value between 1280 and 1500 bytes. You can set the MTU for your LAN network on the LAN tab, and for cellular on the Cellular tab.

LAN tab

This tab provides settings and information about the FX4100 local area network (LAN). The LAN consists of the device and all connected devices.

The screenshot shows the 'LAN' tab in the inseeGo router's web interface. The left sidebar contains navigation links: Device, Network (selected), Routing, Security, Tools, and Administration. The top navigation bar includes tabs for Cellular, Wi-Fi, Ethernet, LAN (selected), WAN, Devices, and DNS. The main content area is divided into four sections:

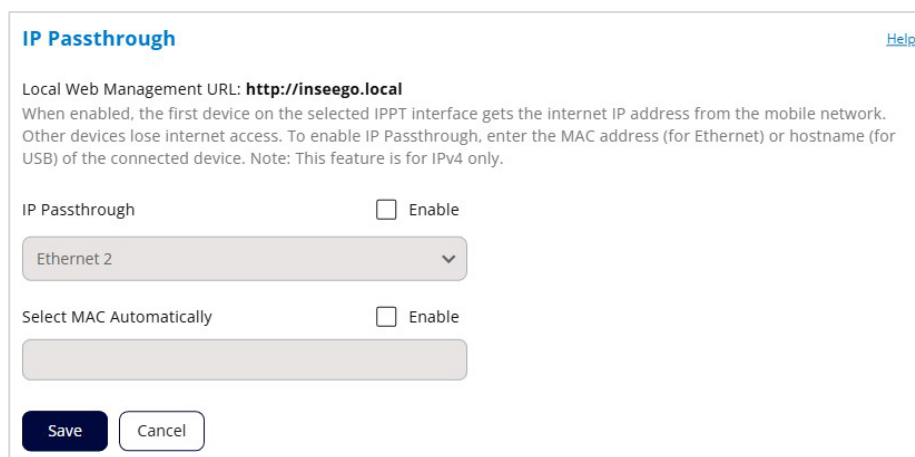
- IP Passthrough:** Local Web Management URL: <http://inseeGo.local>. A note explains that enabling this feature allows the first device on the selected IPPT interface to get the internet IP address from the mobile network, while other devices lose internet access. It requires entering a MAC address for Ethernet or a hostname for USB. The 'IP Passthrough' checkbox is unchecked. The 'Select MAC Automatically' checkbox is also unchecked. A dropdown menu shows 'Ethernet 2'. 'Save' and 'Cancel' buttons are at the bottom.
- IPv4:** MAC Address: 18:ee:86:82:09:ed. IP Address: 192.168.1.1. Subnet Mask: 255.255.255.0. The 'Turn on DHCP Server' checkbox is checked. DHCP Lease Time is 1440 minutes. DHCP Address Range is 192.168.1.2 to 192.168.1.254. 'Save' and 'Cancel' buttons are at the bottom, along with a link to 'Manage Reserved IP Addresses'.
- IPv6:** Link-Local Address: fe80::1aee:86ff:fe82:9ed. The 'Enable IPv6' checkbox is checked. 'Save' and 'Cancel' buttons are at the bottom.
- Data Transmission Setting:** A note explains that this setting sets the maximum size of data packets (MTU) that can be transmitted over the LAN, which can improve connection reliability and performance. The 'Maximum Transmission Unit (MTU)' is set to 1500 bytes. 'Save' and 'Cancel' buttons are at the bottom.

The top right corner of the interface includes a search icon, a user profile icon, and links for 'Logout' and 'Change Password'. A 'Product Documentation' link is also present in the top right.

IP Passthrough

IP Passthrough (IPPT) enables the first device detected on the specified interface 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 has internet access. All other connected devices are disconnected and lose internet access. The following capabilities are set through the host routing system and web UI settings are not available:

- Wi-Fi (including Mesh)
- DMZ (Firewall)
- Port Filtering
- Port Forwarding



The screenshot shows the 'IP Passthrough' configuration page. At the top, it says 'IP Passthrough' with a 'Help' link. Below that, it states 'Local Web Management URL: <http://inseego.local>'. A paragraph explains that when enabled, the first device on the selected IPPT interface gets the internet IP address from the mobile network, and other devices lose internet access. It also mentions that to enable IP Passthrough, the user must enter the MAC address (for Ethernet) or hostname (for USB) of the connected device, and that this feature is for IPv4 only. There are two checkboxes: 'IP Passthrough' and 'Select MAC Automatically', both with an 'Enable' label. Below the 'IP Passthrough' checkbox is a dropdown menu currently showing 'Ethernet 2'. Below the 'Select MAC Automatically' checkbox is a text input field. At the bottom, there are 'Save' and 'Cancel' buttons.

Local Web Management URL: The URL name used to access the FX4100 local web UI (read-only).

IP Passthrough: Check the **Enable** box to enable IP Passthrough and select the interface you want to use for IPPT from the dropdown.

NOTES:

- Enabling IPPT disables Wi-Fi from the router and disconnects all mesh nodes. You will need to pair each node again once you turn IPPT off.
- When Ethernet WAN is connected, IP Passthrough cannot be configured. To allow configuration, go to **Network > Ethernet** and change Ethernet WAN to LAN, or on **Network > WAN**, set Ethernet WAN to a lower priority than Priority 1.

Select MAC Automatically: (visible If you select an Ethernet interface for IPPT). You can either enter the MAC address of the device connected for IPPT or check the **Enable** box to find the MAC address automatically. This is the MAC address of the only device connected to the selected Ethernet port that can obtain the IP address assigned to the mobile network.

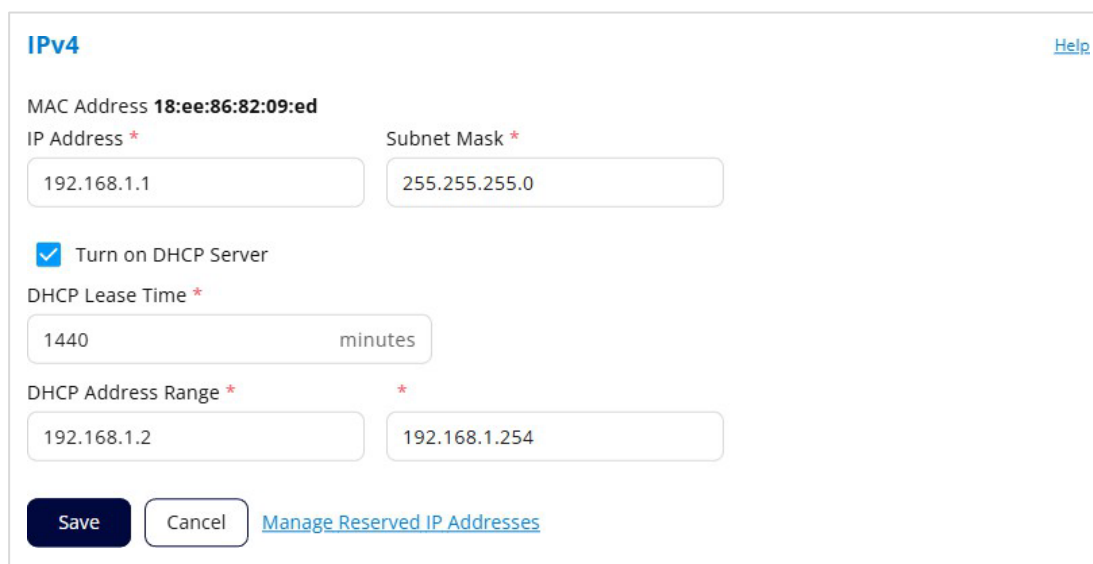
NOTE: You can find the MAC address of connected devices on the **Network > Devices** tab.

Select Hostname Automatically: (visible If you select USB as the interface for IPPT). You can either enter the hostname of the device connected for IPPT or check the Enable box to find the hostname automatically. This is the hostname of the only USB-connected device that can obtain the IP address assigned to the mobile network.

Click **Save**.

IPv4

Use this section if you need to make changes to your router's IPv4 address or subnet mask, or if you want to adjust DHCP server settings.



The screenshot shows the IPv4 configuration page. At the top left is the title "IPv4" and at the top right is a "Help" link. Below the title, the "MAC Address" is displayed as "18:ee:86:82:09:ed". The "IP Address" field contains "192.168.1.1" and the "Subnet Mask" field contains "255.255.255.0". There is a checkbox labeled "Turn on DHCP Server" which is checked. Below this, the "DHCP Lease Time" is set to "1440" minutes. The "DHCP Address Range" is shown with a start of "192.168.1.2" and an end of "192.168.1.254". At the bottom, there are "Save" and "Cancel" buttons, and a link to "Manage Reserved IP Addresses".

MAC Address: The Media Access Controller (MAC) Address for the Wi-Fi interface on your router (read-only). The MAC address is a unique network identifier assigned when a network device is manufactured.

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

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

Turn on DHCP server: The DHCP server is **on** by default. 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 Address Range: The start and end of the IP address range used by the DHCP server. If the IP address 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.

* If you are using a 255.0.0.0 (class "A"), or 255.255.0.0 (class "B") network, the 3rd octet of the IP address must be an even number (for example: x.x.2.x/10.5.2.1).

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 it.

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

Manage Reserved IP Addresses

Connected devices appear automatically in the grid. If a device is missing, you can add it manually by entering its name, MAC address, and a reserved IP address within the DHCP range ([192.168.1.2]-[192.168.1.254]). Reserving an IP ensures the device always receives the same address. Changes take effect only after clicking Save.

Name *	MAC Address *	Current IP Address	Reserve	Reserved IP Address *
san-000534	54:05:db:7f:13:c4	192.168.1.129	☐ off	
SAN-000627	00:15:ff:00:01:24	Offline	☒ on	
san-000534	78:2b:46:fc:66:c4	Offline	☒ on	

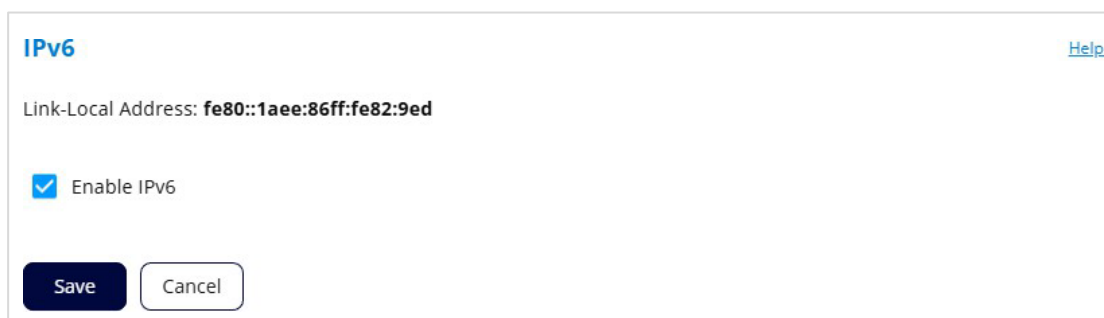
Connected devices display automatically. To manually add a device:

1. Click the **Add** button to start a new row.
2. Enter a name, MAC address and a reserved IP address that falls between the values set in **DHCP Address Range**.
3. Use the **Reserve** slider if you want to reserve the address.
4. Click **Save**.

Click **Save** to activate and save IPv4 settings.

IPv6

Use this section to enable IPv6 so that IPv6 connected devices can make IPv6 connections to the internet.



IPv6 [Help](#)

Link-Local Address: **fe80::1aee:86ff:fe82:9ed**

☒ Enable IPv6

Save **Cancel**

Link-Local Address: The Link-Local IPv6 address if the connected device supports IPv6 (read-only).

Enable IPv6: Check the box if the connected device supports IPv6*.

Click **Save**.

Data Transmission Setting

Use this section to set the maximum transmission unit (MTU) for your LAN network. This is the maximum size of data packets, including headers, that can be transmitted. You might want to adjust the MTU when traffic is being tunneled or encrypted, or if you are noticing fragmentation issues.

NOTE: You can also adjust the MTU for Cellular on the Cellular tab and for the WAN Ethernet connection on the Ethernet tab.

Maximum Transition Unit (MTU): The default (1 500 bytes) is the recommended MTU for your FX4100 LAN network. You can enter a different value between 1280 and 1500 bytes

Click **Save**.

* Connected devices using IPv6 are not compatible with Fortinet VPN. Disable IPv6 on the connected device to use Fortinet.

WAN tab

Use this tab to enable WAN automatic switching, set WAN priorities, and configure keep alive, failover, fallback, and lookup addresses.

The screenshot displays the WAN configuration interface for the inseeo Router FX4100. The interface is divided into several sections:

- Automatic WAN Switching:** A toggle switch is set to "on". Below it, a table lists WAN Interface Priority Order.
- WAN Interface Priority Order:** A table with columns: Priority, Interface, Port/SIM, and Status.
- WAN Switching Rules:** A section for configuring rules for automatic switching.
- Enable Keep Alive and Failover:** A checkbox is checked. Below it, fields for Retry Interval (600), Retry Attempts (3), Keep Alive Interval (86400), and seconds are visible.
- Failback:** A section for configuring failback settings.
- Lookup Addresses:** Fields for Address 1 (www.google.com), Address 2 (www.yahoo.com), and Address 3 (www.inseeo.com).

At the bottom, there are "Save" and "Cancel" buttons.

WAN Automatic Switch the WAN: Automatic Wan switching is **on** by default. This allows rerouting of network traffic to another connection if your primary WAN connection fails.

WAN Interface Priority Order

Use this section to set the priority for your WAN interfaces. Priority 1 is your primary connection. When automatic WAN switching is enabled, the connection switches to the priority 2 interface (fails over) if connectivity is lost on the priority 1 connection, and switches back to the priority 1 connection (fails back) when connectivity is restored.

WAN Interface Priority Order

Set the priority for your WAN interfaces. This determines the primary interface for connectivity and backup priority if failover occurs.

Priority	Interface	Port/SIM	Status
 1	Ethernet	Port 1	Offline
 2	Cellular	SIM	Offline

Priority: Drag the two blue lines up and down to change the priority of the interfaces.

Interface: The type of interface (Cellular or Ethernet 1 or 2).

Port/SIM: For Ethernet interfaces, this is Port 1 or Port 2 (Port 1 is labeled WAN/LAN and is on the left on the router, Port 2 is labeled LAN.).

Status: The status of the interface (Connected, Online, Offline).

WAN Switching Rules

Connectivity testing is on by default and cannot be adjusted. This allows for keep alive to verify your WAN connections.

WAN Switching Rules

You can configure this device to automatically switch the WAN connection when connectivity is lost.

Rule	Status
Connectivity Testing	 on

Enable Keep Alive and Failover

Keep alive verifies your WAN connections by performing a DNS lookup on lookup address(es) at a specified interval. When automatic WAN switching is **on**, if a keep alive attempt fails (the router is unable to resolve an NS lookup on any of the three lookup addresses), failover verification is initiated, and if the failover attempts and the connection may fail over to a backup connection. When automatic WAN switching is **off**, if retry attempts fail, the router reboots.

Enable Keep Alive and Failover

Keep alive verifies WAN connections by an NS lookup on lookup address(es) at the specified keep alive interval. If a keep alive attempt fails, the system attempts to retry verification for the specified number of retry attempts at the retry interval. When automatic WAN switching is on, if the retry attempts fail, the router automatically switches (fails over) to a backup WAN connection. When automatic WAN switching is off, if the retry attempts fails, the device reboots.

Retry Interval *

600

Retry Attempts *

3

Keep Alive Interval *

86400

seconds

Enable: Keep alive and failover are **on** by default. Keep alive checks the internet connectivity on your WAN connections using the lookup addresses at the specified interval. If a check detects an issue with your priority 1 WAN connection, it continues to check at the retry interval for the number of attempts set in Retry Attempts, and if those attempt fails (the router is unable to resolve an NS lookup on any of the three lookup addresses), failover verification is initiated, and if the failover attempts and the connection may fail over to a backup connection. When automatic WAN switching is **off**, if retry attempts fail, the router reboots.

When keep alive detects an issue with your priority 1 WAN connection, failover verification is initiated. The connection is checked using lookup addresses at the specified interval for the number of retry attempts. If any attempt fails, the router automatically switches (fails over) to a backup WAN connection.

Interval: The number of seconds between failover verification attempts.

Retry Attempts: The of times to retry failover verification.

Keep Alive Interval: Keep alive verifies your WAN connections by performing a DNS lookup on lookup address(es) at a specified interval. When automatic WAN switching Switch is **on**, if a keep alive attempt fails (the router is unable to resolve a DNS lookup on any of the three lookup addresses) , failover verification starts and the connection may fail over to a backup connection. When automatic WAN switching is **off**, if a keep alive attempt fails, the router reboots.

Retry Interval: The number of seconds between keep alive verification attempts.

Lookup Addresses

Lookup addresses are used to verify connectivity on WAN connections. If the router is unable to resolve a DNS lookup on the first address, the second address is tried, and so forth. You can use the default addresses or enter new ones.

Failback

If your router has automatically switched (failed over) from your priority 1 WAN connection to a backup connection, failback verification is initiated. This checks connectivity on your priority 1 connection at the specified interval. Failback verification continues until connectivity is verified and the router automatically switches (fails back) to the priority 1 connection.

Interval: The number of seconds between failback verification attempts.

Retry Attempts: The number of times to retry failback verification in a series of attempts. For failback to occur, the last two attempts in the series must succeed. For example, if set to 5 and the first four attempts succeed, but the last attempt fails, failback does not occur. **NOTE:** Failback attempts continue until failback occurs. This setting only determines how many attempts to try in a series, where the last two attempts must succeed.

(Failover Number of attempts: Enter the number of times to retry after verification failure for all three lookup addresses. The default is 3 attempts.

Keep alive interval: Enter the desired number of seconds between keep alive verifications. The default is 86400 seconds.

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

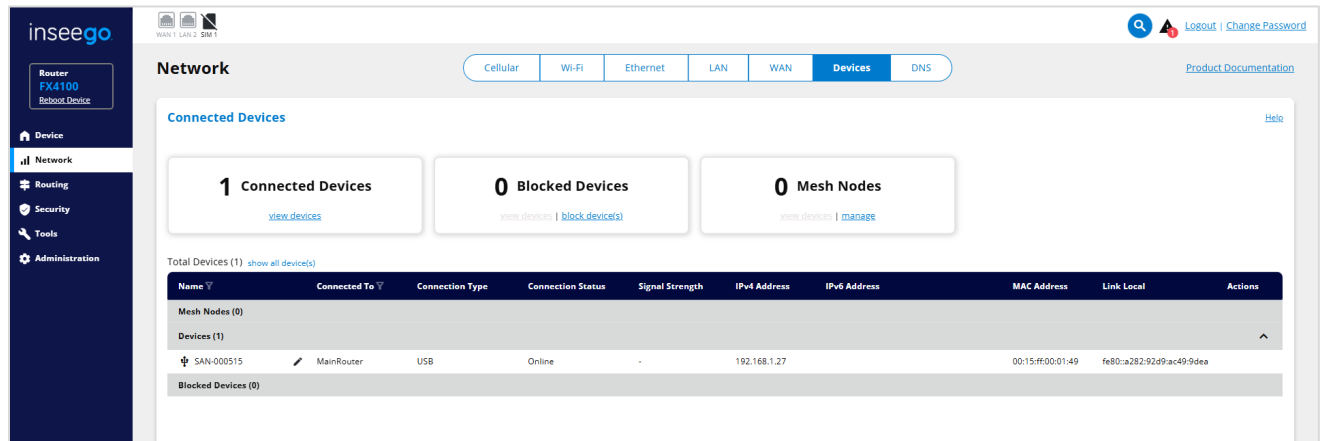
Lookup Address 2: Enter the second IP address to verify (if Lookup Address 1 does not respond with keep alive acknowledgement (ACK)).

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

WAN failback interval: The interval used to reactivate the priority WAN interface after the device has failed over to a backup WAN interface. For example, if cellular WAN is your priority WAN interface, this interval allows the device to resume use of a cellular WAN connection after it has failed over to an Ethernet WAN interface. The interval begins when the active WAN interface has failed over to a backup WAN interface. Once the interval expires, the device re-establishes the priority WAN interface as the active connection. The default interval is 15 minutes.

Devices tab

This tab provides details about each device connected to your router and any mesh nodes in your network. It allows you to edit how device names appear in the UI. You can also block or unblock devices from internet access.



The top section shows the number of connected client devices, blocked devices and mesh nodes.

- Click **view devices** in each section for details on that topic.
- Click **block devices** under **Blocked Devices** to disconnect client devices from accessing your network and prevent them from reconnecting. Blocked devices are removed from the **Devices** section of the table below and appear in the **Blocked Devices** section.
NOTE: This option is available for each client device connected through Wi-Fi but is not available for your own device or devices connected via Ethernet or USB.
- Click **manage** under **Mesh Nodes** to go to the Wi-Fi tab where you can add nodes.

The Total Devices table displays details for all mesh nodes, connected client devices, and blocked devices.

Name: The name of the device or mesh node. You can edit the name using the pencil icon . (This only changes the name in this UI.)

Connected To: The mesh node or router the device is connected to.

Connection Type: Indicates whether the device is connected through Wi-Fi, Ethernet, or USB.

Connection Status: The status of the connection.

Signal Strength: The strength of the network signal. **NOTE:** Ethernet and USB connections display a line instead of a value.

IPv4 Address: The IPv4 address of the connected device.

IPv6 Address: The IPv6 address of the connected device.

MAC Address: The MAC Address (unique network identifier for the device).

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

Actions:

- **block** – Click **block** next to a device to disconnect it from accessing your network and prevent it from reconnecting. Click **Block Device(s)** when asked. The device is removed from the **Devices** list and appears in the **Blocked Devices** 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.
- **unblock** – To unblock a blocked device, click **unblock** and confirm. The device is removed from the **Blocked Devices** list and appears in the **Devices** list above.

Tips:

- Use the **Filter** icon in the **Name** or **Connected To** columns to filter the table data.
- ✓ Click the **down arrow** on the right to expand a section. Click the up arrow to collapse.

DNS tab

The FX4100 automatically selects a Domain Name Server (DNS). This page allows you to manually assign up to two DNS IP addresses.

The screenshot shows the inseeGO web interface for the FX4100 router. The left sidebar contains navigation links: Device, Network (selected), Routing, Security, Tools, and Administration. The top navigation bar includes tabs for Cellular, Wi-Fi, Ethernet, LAN, WAN, Devices, and DNS (selected). The main content area is titled 'Domain Name Server (DNS)' and includes a 'Help' link. Below the title, a message states: 'Your device automatically selects a Domain Name Server (DNS). You can configure it to manually set one.' There is a toggle switch for 'Turn on Manual DNS' currently set to 'off'. Below this are two input fields: 'DNS 1 IP *' with the value '8.8.8.8' and 'DNS 2 IP' with the value '8.8.4.4'. At the bottom are 'Save' and 'Cancel' buttons.

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

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

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

Click **Save**.

Managing routing

Use this tab to set routing options.

The screenshot displays the inseeGO web interface for the Router FX4100. The top navigation bar includes the inseeGO logo, status icons (Wi-Fi, Ethernet, T-Mobile 5GUC), and user options (Logout, Change Password). The left sidebar contains a menu with the following items: Router FX4100, Device, Network, Routing (highlighted), Security, Tools, and Administration. The main content area is titled "Routing" and contains three configuration sections:

- Manage NAT Routing Type**: A section titled "Select a Network Address Translation (NAT) type for your connection." It features a "NAT Type" dropdown menu currently set to "Symmetric NAT (Strict)" and "Save" and "Cancel" buttons.
- Restrict Internet Access For Applications**: A section titled "You can restrict internet access for specific applications. When Port Filtering is off, all applications can access the Internet. To restrict access, turn on Port Filtering and specify the applications that should not have Internet access." It includes a "Port Filtering" toggle switch set to "off" and a message: "No restrictions set. All applications can access the internet."
- Direct Incoming Traffic To a Connected Device**: A section titled "You can send incoming traffic to a specific device." It includes a "Port Forwarding" toggle switch set to "off" and a note: "Note: Port Forwarding functionality is limited to IPv4 addresses only."

Managing NAT Routing Type

NAT Type: Use the dropdown to select the type of Network Address Translation (NAT) for your connection.

- **Symmetric NAT** is more restrictive. It maps requests with the same source IP address and port number to a unique external IP and port, based on the destination IP and port of the outgoing connection.
- **PRC NAT** maps all requests from the same source IP address and port to the same public IP address and port, regardless of destination.

Click **Save**.

Restrict Internet Access For Applications

This section allows you to block outgoing internet connections and permit only selected applications to access the internet using port filtering.

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

Port Filtering: When **on**, only traffic from the selected applications can access the internet. Some applications are pre-defined. You can define additional applications if you know the details of the traffic used and generated by the applications.

Restrict Internet Access For Applications

You can restrict internet access for specific applications. When Port Filtering is off, all applications can access the internet. To restrict access, turn on Port Filtering and specify the applications that should not have internet access.

Port Filtering ☒ on

Restrict Internet Access For

Email (POP3, IMAP, SMTP)	☒ restricted
FTP	☒ restricted
HTTP	☒ restricted
HTTPS	☒ restricted
Telnet	☒ restricted

NOTE: DNS is always allowed access to the internet.

Specify Custom Applications

Application Name *	Ports *	Restricted
1. enter name	starting... ending...	TCP ☒ off

Add

Save Cancel

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

Specify Custom Applications

You can define your own applications (up to 25) and then turn them on or off as needed.

Application Name: Enter a name for the custom application.

Ports:

- **starting** - Enter the beginning of the range of port numbers used by outgoing traffic for the custom application being added.
- **ending** - 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 in both the **starting** and **ending** text boxes.

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

Allow Access: Check the box if you want the new application to be able to access the internet.

Click the **X** to delete a custom application.

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

Click **Save** to save your changes.

* **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.

Direct Incoming Traffic to a Connected Device

You can allow specific applications to be forwarded to a particular device connected to your network by enabling port forwarding. Normally, the built-in firewall blocks incoming traffic from the internet. Port forwarding allows internet users to access any server you are running on your computer, such as a web, FTP, or Email server.

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

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

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

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

Port Forwarding: To turn on port forwarding, move the on/off slider to **on**.

Direct Incoming Traffic to a Connected Device

You can send incoming traffic to a specific device.

Note: Port Forwarding functionality is limited to IPv4 addresses only.

Port Forwarding ☒ on

Forward Traffic for Specific Applications

For (Application) *	Application IP address *	Status
select an application	enter IP Address	☐ off X

Specify Custom Applications

Application Name *	To (IP Address) *	Port Type *	Ports *	Protocol *	Restricted
1. enter name	enter IP Address	Range	starting port ending port	TCP	☐ off X

Forward Traffic for Specific Applications

For (Application): Select an application from the dropdown that you want to be forwarded.

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.

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

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

Forward Traffic: Check this box if you want the application to be forwarded.

Click the **X** to delete an application.

Specify Custom Applications

Use the **Add** button to add a new row to the custom application list. You can add up to 26 custom applications. Once defined, these applications can be turned on and off the same way as pre-defined applications.

Application Name: Enter a name for the custom application.

To (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, refer to the Devices tab. **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: You can use the dropdown to select **Range** if you want to enable a range of one or more ports for forwarding, or select **Translate** for single port forwarding.

* **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.

Ports:

- **starting** - Enter the beginning of the range of port numbers for the custom application being added.
- **ending** - 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 in both the **starting** and **ending** text boxes.

Port Numbers: Use **Ext.** and **Int.** to specify ports to be forwarded. **NOTE:** To forward inbound traffic to the same port on a client device, enter the same port number in both **Ext.** and **Int.** You can also 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 dropdown list (TCP, UDP, or both).

Forward Traffic: Check this box if you want the custom application to be forwarded.

Click the **X** to delete a custom application.

Click **Save**.

Managing security

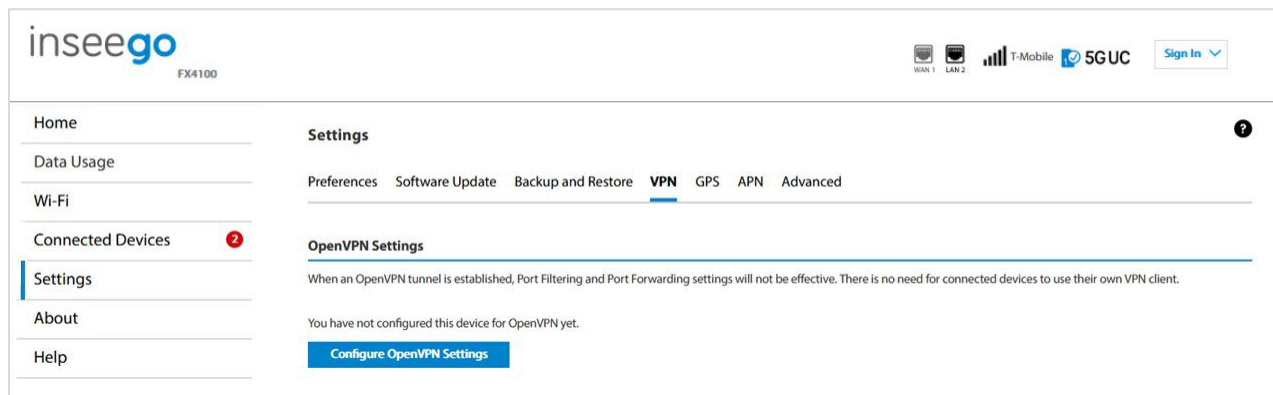
VPN

You can configure OpenVPN through the admin web UI. IPsec VPN is available with Inseego Connect.

- VPN tab (OpenVPN) – admin web UI
- IPsec VPN (Inseego Connect)

VPN tab (OpenVPN)

Your FX4100 5G Cellular Router allows you to establish secure connections to remote networks over a public network using OpenVPN.



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.

OpenVPN Settings

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

The screenshot shows a 'Configure OpenVPN Settings' dialog box with a close button (X) in the top right corner. It contains the following fields and controls:

- 'OpenVPN Configuration Files:' with a text area that says 'Drag and drop files from your OpenVPN provider here.'
- 'Username:' with a text input field.
- 'Password:' with a text input field and an eye icon for toggling visibility.
- 'Auto-connect VPN:' with an information icon (i) and a toggle switch.
- At the bottom, there are two buttons: 'Save Changes and Connect' (grey) and 'Clear All OpenVPN settings' (blue).

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

Username: Enter your OpenVPN connection username here.

Password: Enter your OpenVPN connection password here.

Auto-connect 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 OpenVPN settings: This button deletes all VPN files, logs, and resets all VPN settings.

Click **Connect** to connect to the VPN server.

VPN Connection

This section is visible once you have configured your router for OpenVPN.

Connection status: Indicates the status of the OpenVPN connection.

Connection time: The duration of the current OpenVPN connection.

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

Connect: Use this button to connect the OpenVPN.

IPSec VPN (Inseego Connect)

You can create IPSec VPNs using Inseego Connect. All T-Mobile owned Inseego FX devices come with the option of purchasing the Inseego Connect Add-on. Please work with your Account team to order the Inseego Connect Add-on, which provides Manager access.

The screenshot shows the 'Configure' window for IPSec VPN. On the left is a sidebar menu with options: Device, Wifi, Mobile Network, GPS, Connected Devices, Advanced (selected), Firewall, MAC Filter, LAN, WAN Settings, Port Filtering, Port Forwarding, IPSec VPN, and Inseego Connect. The main panel is titled 'IPSec VPN' and contains the following elements:

- A help icon and text: 'Create IPSEC (Internet protocol security) VPNs to establish secure connections to remote networks over a public network.'
- A toggle switch for 'Enable IPSEC VPN Service' set to 'ON'.
- A section titled 'VPN Tunnel Configurations' containing a table:

Tunnel Name	Local IP	Remote IP	Enabled	Edit	Delete
Sandeep	166.211.177.52	203.163.254.158	true	<button>Edit</button>	

Below the table is a blue button labeled 'Add New VPN Tunnel'.

At the bottom of the window, there is a checkbox for 'Schedule later' with a 'Select Date Time' button next to it, and two buttons on the right: 'Cancel' and 'Save to Device'.

Move the **Enable IPSEC VPN Service** slider to **ON** to enable IPSec VPN service.

When IPSec VPN service is enabled, established tunnel information displays. You edit or delete existing tunnels.

Click **Add New VPN Tunnel** to add a new VPN tunnel. The Add New VPN Tunnel Dialog appears.

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.
- **NAT Traversal** — Check this box if you want NAT traversal to automatically detect if network address translation (NAT) is being performed between the two VPN tunnel endpoints.
- **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 a type of authentication from the dropdown list. You are prompted for further information based on your selection.
- **Remote Authentication** — Select a type of authentication from the dropdown list. You are prompted for further information based on your selection.

Click **Next**.

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 a 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.

Click **Next**.

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.

Click **Next**.

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 on this page to be a common Hash.

Click **Next**.

Dead Peer Detection (DPD)

Dead Peer Detection (DPD) is a keep-alive method that ensures the tunnel is up and takes 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.

Enable: Check this box to enable DPD.

DPD Action: Use the dropdown to select a DPD action.

DPD Delay: The number of seconds between DPD packets.

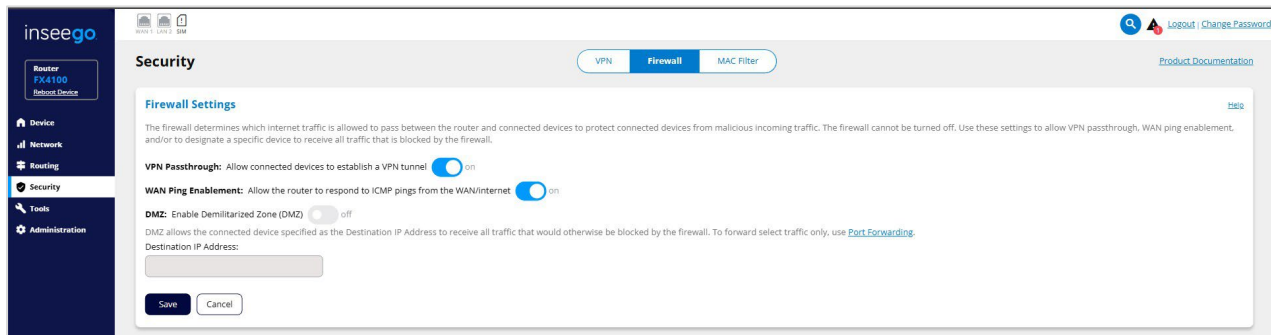
DPD Timeout: The number of seconds the router will allow an IPSec session to be idle before beginning to send DPD packets to the peer machine.

Click **Next** and implement your settings. The new VPN tunnel is displayed on the IPSec VPN page.

If you want changes to go into effect at a later time, check the **Schedule later** box and select a date and time from the calendar. Once all your changes are made, select **Save to Device**.

Firewall tab

The FX4100 5G Cellular Router firewall determines which internet traffic is allowed to pass between your 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 allow VPN Passthrough and/or designate a specific device to receive all traffic.



VPN Passthrough

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

WAN Ping Enablement

By default, the router ignores ping requests received on the WAN interface. To enable your router to respond to ping requests received on the WAN interface (IPv4 only), move the slider to **on**.

DMZ

Turn on 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.

NOTES:

- When IP Passthrough is turned on, DMZ capabilities are set through the connected host routing system. Settings in this section are not available. Go to **Network > LAN** to turn IP Passthrough off.
- To allow DMZ, you need a static IP address assigned to your line of service. Contact your service provider to set up a line of service for static IP.

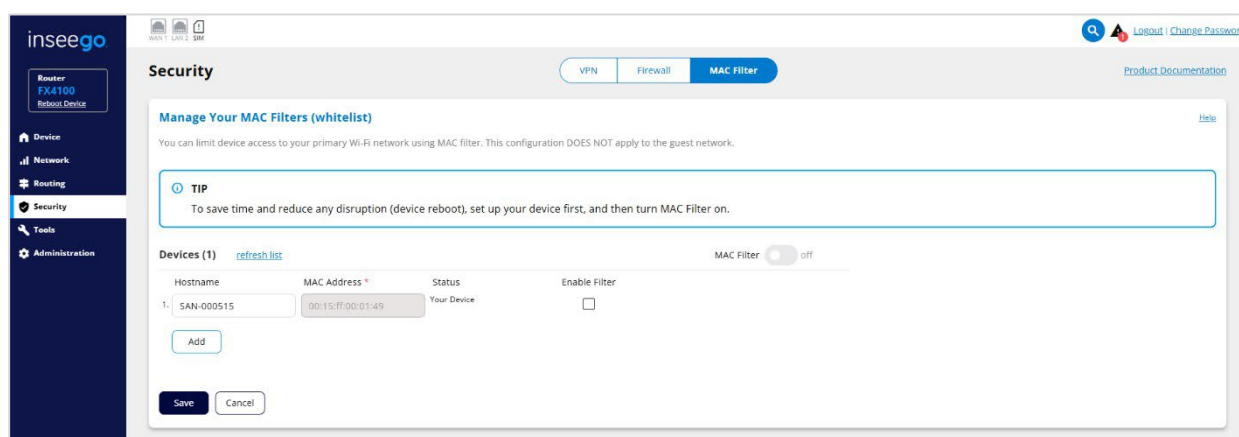
Destination IP Address: Enter the IP address of the connected device you wish to become the DMZ device (the DMZ destination). **NOTE:** You can check the IP address of each connected device on the Network > Devices tab.

Click **Save**.

MAC Filter tab

The MAC filter allows only selected devices to access the FX4100 5G Cellular Router network through DHCP. By default, MAC filter is turned off.

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



Manage Your MAC Filters (whitelist)

Devices

This list includes all devices currently connected to the router.

To use the MAC filter:

1. Check **Enable Filter** for the device(s) in the device list that you want to be allowed to connect to the network through DHCP.
2. Turn **MAC Filter** on.
3. Click **Save**.

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

To add devices to the Devices list:

1. Click the **Add** button.
2. Enter the device hostname and MAC address.
3. You can choose whether to enable MAC filter for the device.

4. Click **Save**.

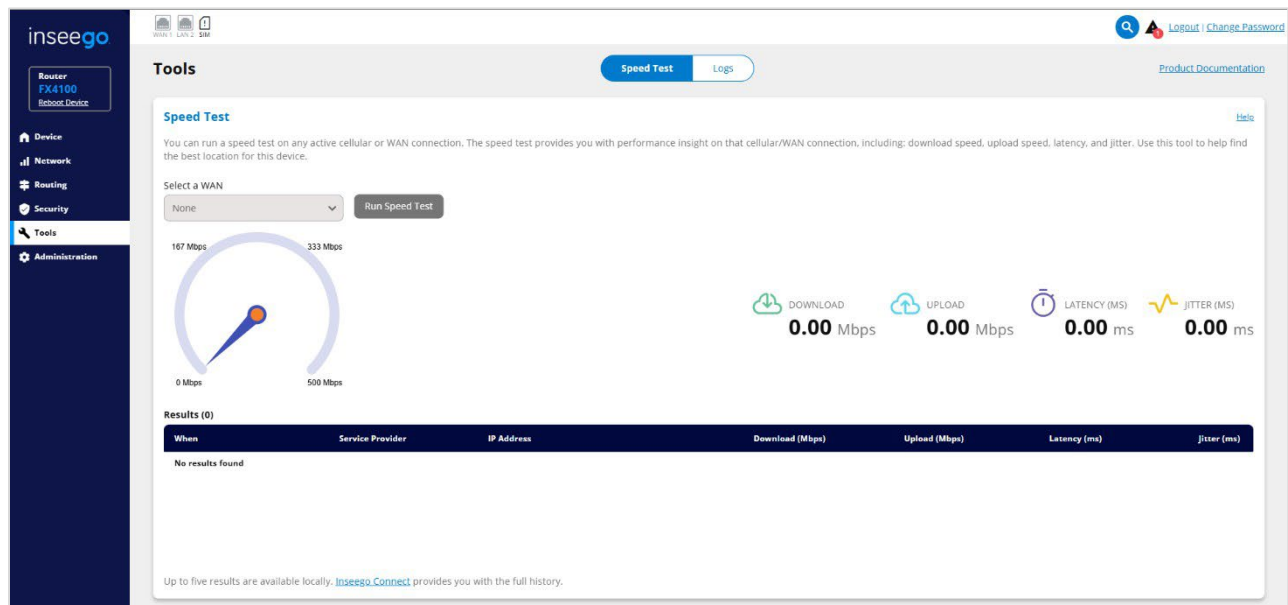
To discard any unsaved changes and refresh the list, click **refresh list**

Click the **X** next to a device to delete it from the list.

Using Tools

Speed Test tab

You can run a speed test on any active cellular or WAN connection. The speed test provides you with performance insight on that cellular/WAN connection, including: download speed, upload speed, latency, and jitter. You can use this tool to help find the best location for your router.



Speed Test

Select a WAN: Use the dropdown to select a WAN connection to test.

Click the **Run Speed Test** button to start the speed test. The results of the current speed test are displayed on the right.

Results: A row in this table displays for each speed test.

- **When:** The date and time of the test.
- **Service Provider:** The service provider associated with the connection.
- **IP Address:** The IP address of the connection.
- **Download (Mbps):** The number of megabits the connection can download from the internet to your router per second.
- **Upload (Mbps):** The number of megabits the connection can upload from your router to the internet per second.

- **Latency (ms):** The number of milliseconds it takes a data packet to travel from the router to a server and back on the connection.
- **Jitter (ms):** The amount that latency fluctuates over time, measured in milliseconds.

Logs tab

Use this tab to view log information for troubleshooting.

inseeGO FX4100

Home
Data Usage
Wi-Fi
Connected Devices **2**
Settings
About
Help

About

Internet Status Internet Sessions Diagnostics Device Info **Logs**

Log Settings

Logs are for troubleshooting, and are not needed for normal operation.

Note: If the system log is full, then the oldest data is discarded, regardless of this setting.

Turn On Logging ☒

Automatically Clear Logs After 3 days

Save Changes

Mobile Network Log Device Log

```

May 7 21:53:56 localhost <modem2d>: [MDM_MAIN]:[notice] - (mifios_wanevent):Service State: LTE
May 7 21:22:23 localhost <modem2d>: [MDM_MAIN]:[notice] - (mifios_wanevent):Service State: NR5G
May 7 21:22:23 localhost <modem2d>: [MDM_MAIN]:[notice] - (mifios_wanevent):Service State: NR5G
May 7 21:22:23 localhost <modem2d>: [MDM_MAIN]:[notice] - (mifios_wanevent): not roaming
May 7 21:22:23 localhost <modem2d>: [MDM_MAIN]:[notice] - (mifios_wanevent): INTERNET IPV4 Call state idle
May 7 21:22:23 localhost <modem2d>: [MDM_MAIN]:[notice] - (mifios_wanevent): INTERNET IPV6 Call state idle
May 7 21:22:55 localhost <modem2d>: [MDM_MAIN]:[notice] - AAN: (mifios_wanevent): Multi APN SWAP start- lmsi: 310260993435132, iccid:
May 7 21:23:10 localhost <modem2d>: [MDM_MAIN]:[notice] - (mifios_wanevent): INTERNET IPV4 Connected!!
May 7 21:23:10 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV4 PDPCONTEXT address:192.0.0.2
May 7 21:23:10 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV4 PDPCONTEXT gateway address:192.0.0.1
May 7 21:23:10 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV4 PDPCONTEXT subnet mask :255.255.255.224
May 7 21:23:10 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV4 PDPCONTEXT DNS1 address:192.0.0.30
May 7 21:23:10 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV4 PDPCONTEXT DNS2 address:0.0.0.0
May 7 21:23:10 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV4 PDPCONTEXT MTU:1472
May 7 21:23:43 localhost <modem2d>: [MDM_MAIN]:[notice] - (mifios_wanevent): INTERNET IPV6 Connected!!
May 7 21:23:43 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV6 PDPCONTEXT
address:2607:fb90:33ab:f1a:990f:ba6:a26b:8f3
May 7 21:23:43 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV6 PDPCONTEXT gateway
address:fe80:20f0:f1f2:5d18:3a89
May 7 21:23:43 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV6 PDPCONTEXT DNS1 address:fd00:976a:9
May 7 21:23:43 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV6 PDPCONTEXT DNS2 address:fd00:976a:10
May 7 21:23:43 localhost <modem2d>: [MDM_MAIN]:[notice] - data_call_connection_state: (mifios_wanevent): INTERNET IPV6 PDPCONTEXT MTU:1500

```

Export log **Refresh** **Clear log**

Log Settings

Logging: Turn on when logs are needed.

Automatically Clear Logs: Use the dropdown list to select when logs are cleared.

NOTE: If the log is full, the oldest data is deleted regardless of this setting.

Click **Save**.

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

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

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

Refresh: Updates the displayed log data.

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

Click **Export** to export log data.

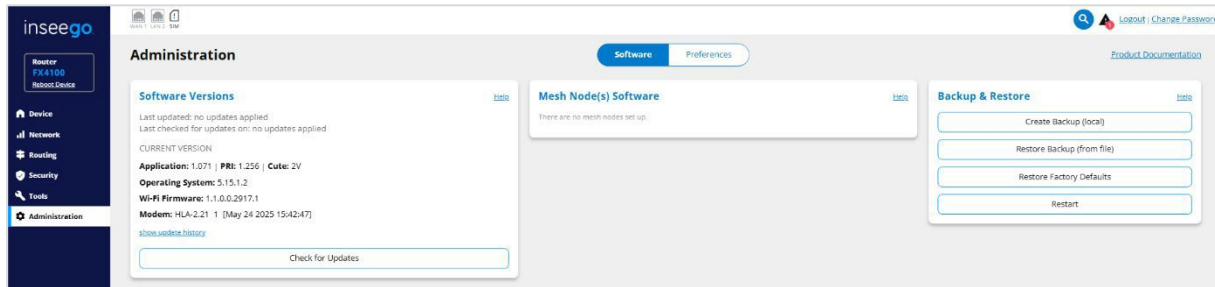
Setting Administrative options

Software Update tab

Software updates are delivered to your FX4100 5G Cellular Router and X700 Mesh Wi-Fi automatically over the mobile network. This tab displays current software version information, software update history, and allows you to check for new software updates for your router and any mesh nodes in your network.

If your router is used on a private APN or cellular network, or if access is limited to specific sites, you must include the following URL in the access list so that automatic software updates can be delivered and you can check for updates:

<https://fota.production.nvtl.mifiupdates.com> (TCP 443).



Software Versions

Last updated: The date and time the software was last updated.

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

Current Versions

Application: The configuration version currently applied to your router.

PRI: The configuration version currently applied to your router.

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

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

Wi-Fi Firmware: The version of Wi-Fi firmware currently installed.

Modem: The version of modem software currently installed.

Click **show update history** to view a history of previous software updates.

Check for Update: Click this button to manually check for available software updates. If a new software update is available, it is automatically downloaded. You are prompted to install with a message that your router will be unavailable for about 18 minutes during the update.

Mesh Node(s) Software

Last updated: The date and time the software was last updated.

Last checked for updates: The most recent date and time mesh nodes were last checked for an update.

Mesh Node

Name: The name of the mesh node.

Serial Number: The serial number on the label of the mesh node.

Firmware: The version of firmware currently installed.

Applied On: The date and time the mesh node firmware was last updated.

Check for Update: Click this button to manually check for available software updates. If a new software update is available, it is automatically downloaded. You are prompted to install with a message that your mesh node will be unavailable for about 18 minutes during the update.

Backup and Restore

Use this section to back up your current 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.

Creating a local backup

To create a local backup of current router settings to a file on your computer:

1. Click the **Create Backup (local)** button.
2. 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 **Log In** in the top-right corner, click **Forgot 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 router and use the admin password printed on the bottom label.

3. Click the **Create Backup File** 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 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 router, and settings can only be viewed or changed using the admin web UI.

Restoring a backup

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

To restore system settings from a backup settings file:

1. Click the **Restore Backup (from file)** button
2. Enter your admin password in the **Admin Password** field.
3. Drag and drop a backup settings file to restore or click **upload** to browse for the file.

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

4. Click the **Yes, Restore Settings** button.

Restoring to factory defaults

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 admin web UI.

To reset all settings to their factory default values, click the **Restore Factory Defaults** button, then confirm by clicking **Yes, Restore Factory Defaults**.

Restarting your router

To restart your router (turn it off and on again), click the **Restart** button: then confirm by clicking **Yes, Reboot Device**.

Preferences tab

You can use this section to change the router name visible to connecting devices, turn off the LED lights, and enable periodic reboot. You can also change the language and how dates, time, distance, and numbers are displayed in the web UI.

The screenshot displays the Inseego router's web interface, specifically the 'Preferences' tab under the 'Administration' section. The left sidebar shows navigation options: Device, Network, Routing, Security, Tools, and Administration (selected). The main content area is titled 'Device Preferences' and includes a 'Help' link. It is divided into two columns: 'General' and 'Application Data Display'. The 'General' column contains fields for 'Device Name' (set to 'Inseego'), 'Languages' (set to 'English'), and checkboxes for 'Keep Device LED Light On' (checked) and 'Periodically Reboot Device' (unchecked). The 'Application Data Display' column contains dropdowns for 'Date' (set to 'mm/dd/yyyy'), 'Time' (set to '12 hr'), and 'Number Format' (set to '3.234.00'), along with radio buttons for 'Feet/Meters' (set to 'Feet'). Below these columns are 'Save' and 'Cancel' buttons. At the bottom, there are two additional sections: 'Inseego Connect' and 'GPS'. The 'Inseego Connect' section shows 'Cloud Management' as 'on', 'Connection State' as 'Disconnected', 'Last Reported' as 'UNREPOR', and 'Reporting Interval' as '6700 seconds'. The 'GPS' section shows 'GPS Services' as 'on', 'Turn Off GPS When Device Restarts' as 'on', and a box for location data (Latitude, Longitude, Altitude, Accuracy) which is currently empty.

Device Preferences

You can use this section to change the router name visible to connecting devices, turn off the LED lights, and enable periodic reboot. You can also change the language and how dates, time, distance, and numbers are displayed in the web UI.

General

Device Name: To change how the router appears when connecting other devices, enter a different name.

Languages: Select a language for the admin web UI.

Keep Device LED Light On: When checked, the LED lights on the front left of your router remain on. To turn these lights off, uncheck the box. **NOTE:** This does not affect the device display on the front right of the router, which times out after 60 seconds.

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

Application Data Display

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

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).

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

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

Click **Save**.

Inseego Connect

Inseego Connect enables you to configure settings, monitor status, and update the firmware on your device remotely from the cloud.

Cloud Management: By default, the connection to Inseego Connect is **on**.

Connection State: The status of the Inseego Connect connection.

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

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

GPS

Your router incorporates a GPS receiver. The GPS receiver can determine your current location. Use this feature to enable GPS and view current location information.

GPS Services: This setting enables or disables the GPS radio on your router. When the slider is **on**, the device acquires GPS and makes GPS location data available. A GPS Agreement appears, click **Yes, Enable GPS** to proceed. When **off**, no GPS data is available.

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

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.

3

Troubleshooting and support

Overview

Troubleshooting

Technical support

Overview

When properly installed, the FX4200 5G Cellular Router is a highly reliable product.

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

- 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 plan with your service provider.
- You can resolve many issues by restarting your connected device and your router.

Troubleshooting

This section can help solve many common problems and answer questions encountered while using the FX4200 5G Cellular Router.

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

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

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

The device status LED is switching from blue to green

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

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

Can I set my router to use a specific cellular band?

No, the FX4200 5G Cellular Router is designed to connect to the strongest signal available. You can set the network technology and 5G network mode using **Settings > Advanced > Cellular**.

I cannot access the Admin web UI

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

Solution: Connect to the web UI through the primary Wi-Fi network, USB, or Ethernet.

- **Reason:** You are not accessing the correct URL.

Solution: On a device connected to the router, open any web browser, and go to <http://192.168.1.1> or <http://Inseego.local>.

- **Reason:** You are trying to connect to <http://Inseego.local>, and have Fortinet VPN on your connecting device. The Inseego.local web UI address relies on having IPv6 enabled on your connecting device, but devices using IPv6 are not compatible with Fortinet VPN.

Solution: Use the <http://192.168.1.1> URL.

My router is getting slow speeds/low throughput

- **Reason:** Signal strength is the most likely cause of slow speeds/low throughput.
NOTE: The FX4200 5G Cellular Router is configured by default to use the best connection available, so low throughput is rarely related to configuration.

Solution: Check the signal strength reported by your router:

- Check the **Cellular Signal LED** on the device and/or **number of bars** on the device display.

If the signal is poor (LED is yellow, white, or red, or there are less than three bars), relocate your router to improve signal conditions.

The device status LED is blinking red

- **Reason:** The status LED blinks red when there is a SIM error, no service, or in rare cases, the SIM card is locked.

Solutions:

Try the following:

- Unplug the router, then remove and reinsert the SIM card. Do not touch the gold-colored contacts. Make sure the card is inserted with the contacts facing down, notch facing in, and that it clicks into place. Restart your router.
- Ask your service provider:
 - Is your SIM active and on a plan compatible with the router.
 - Are there any service outages in your area.
- Perform a factory reset.
- Log in to the Admin web UI and check the following:
 - On the **device display**, check if there is a SIM error message, or on the web UI **Home** screen, check if there are any values in the SIM Status section. If the SIM card is properly inserted and the device does not recognize the SIM, the SIM slot may be defective. Contact your service provider to replace the device.
 - On the **Home** page, check that the **APN** is correct. Check with your service provider if you are unsure.
 - In the **top banner** of any page, check the **signal strength**. If you see, “No service,” the device cannot see any towers or is in a hung state.
If you know you are in range, try removing the SIM and rebooting the device with a SIM from a different service provider. The SIM does NOT need to be active. Reinsert the original SIM and restart the device. This prompts the device to reload modem configuration details and should resolve the hung state. If this does not work or another SIM is not available, contact your service provider to replace the device.
 - On **Settings > Advanced > SIM**, check for a locked SIM.

My older device cannot connect

If you can see other networks, but not the network name for your FX4200 5G Cellular Router:

- **Reason:** The default multi-mode settings on your router 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 **Wi-Fi 4 802.11 bgn**:

1. Access the Admin web UI and navigate to **Wi-Fi > Settings**. Under **2.4 GHz Band Settings**, use the drop-down to change the **Wi-Fi Standard** to **Wi-Fi 4 802.11 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 router will reboot, and the network name should be visible on all devices.

If you can see the network name, but cannot connect a device to your FX4200 5G Cellular Router:

- **Reason:** The default network security settings on your router 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 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 router will reboot, and all devices should be able to connect.

If the solutions above do not resolve the issue, try the following:

- **Reason:** Some Wi-Fi devices cannot properly store long passwords.

Solution: Change your Wi-Fi password.

1. Access the Admin web UI and navigate to **Wi-Fi > Primary Network**, or **Wi-Fi > Guest Network**, depending on the network to which you are trying to connect. Change the Wi-Fi password to between 11 and 16 characters.

2. Click **Save Changes** and **Confirm**. Your router will reboot, and all devices should be able to connect.
- **Reason:** In rare cases, a Wi-Fi device may have issues with the same SSID being used on both 5GHz and 2.4 GHz bands.
Solution: Disable the 5 GHz band.
 1. Access the Admin web UI and navigate to **Wi-Fi > Settings**. Uncheck **5 GHz** and use only **2.4 GHz**.
 2. Click **Save Changes**. Your router will reboot, and your device should be able to connect.

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:** 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 router to factory settings, see “Resetting your router” on page 23.
or

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

- **Reason:** The DHCP server has used all its IP addresses.
This is unlikely to happen with the FX4200 5G Cellular Router, but if you have connected a succession of devices to your router in a short period of time, you may have used up all the IP addresses available.

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

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

Solution: Contact your service provider for assistance.

My connected device cannot connect to Fortinet VPN

- **Reason:** Connected devices using IPv6 are not compatible with Fortinet VPN.

Solution: Disable IPv6 on the connected device to use Fortinet.

Devices connected via Ethernet are not getting internet

- **Reason:** If your FX4200 router has been connected to another router (such as in a backup configuration), the routers may be using the same IP address.

Solution: Ensure that the IP address of the FX4200 and the IP address of the other router are different. In the FX4200 Admin web UI, go to **Settings >**

Advanced > LAN and change the IP address to something other than 192.168.1.1, for example: 192.168.3.1.

- **Reason:** You are not plugged into the correct Ethernet port. By default, the Ethernet ports on the back of the FX4200 are configured as labeled (WAN on the left, LAN on the right). However, both Ethernet ports can be configured to LAN or WAN in the FX4200 Admin web UI: **Settings > Advanced > WAN**.

Solution: When using the FX4200 to provide internet connectivity to a wired client or to your network through a router or switch, use a port configured for LAN. When connecting the FX4200 to a wired WAN/internet connection for failover, use a port configured for WAN.

I cannot get streaming platforms to work with my router

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

Solution: Contact your service provider for assistance.

Do I need a signal amplifier or booster?

Signal amplifiers or boosters are used at the user's risk and may not provide improved coverage, signal, or performance.

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 your needed bands are supported, you may experience a worse connection.

Does the USB port support RNDIS?

The FX4200 has one USB port, which is used for power. You can use a USB hub or splitter that supports USB 3.1 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. PCs with Thunderbolt Networking can expect speeds up to 2.5Gbps.

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 an Ethernet port.

NOTE: The USB-C port does not support charging of other devices.

Technical support

IMPORTANT: Before reaching out for support, be sure to restart both your connected device and your 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 FX4200 5G Cellular Router is available online. Go to go.inseego.com/fx4200. Or, from the Admin website, select **Help > Customer Support**.

Vulnerability disclosure policy

Inseego is committed to acting on reported vulnerabilities in a timely manner, and to prioritize critical issues appropriately.

Inseego is able to send Firmware Over-the-Air (FOTA) updates to resolve most issues.

To submit a vulnerability issue, email: technicalsupportus@inseego.com.

- Inseego will respond within five business days to acknowledge receipt of the suspected vulnerability.
- Inseego will provide a status update within a reasonable time based on severity and impact, after an assessment is made.

4

Product specifications and regulatory information

FX4200 product specifications

X700 product specifications

Regulatory information

Product certifications and supplier's declarations of conformity

Wireless communications

Limited warranty and liability

Safety hazards

FX4200 product specifications

Device	
Name:	FX4200 5G Cellular Router
Model:	FX4210
Regulatory:	FCC (US), ISED (Can)
Certifications:	GCF, PTCRB, FIPS-3, Wi-Fi Alliance, REACH, RoHS, UL 2710 *
Battery:	Rechargeable LI-ion backup battery
Dimensions:	8.3" x 5.5" x 2.1" (210 mm x 140 mm x 54 mm)
Weight:	30 oz (850g)
Operating temperature:	32°F to 104°F (0°C to +40°C)
Operating temperature with limitations:	14°F to 122°F (-10°C to +50°C)
Storage temperature:	-22°F to 158°F (-30°C to +70°C)
Ports:	2x 2.5 GbE RJ45 2x 1 GbE RJ45 1x USB 3.1 Type C (data) 1x USB PD Type-C (power) 4x external full spectrum SMA cellular antenna
SIM:	2x 4FF Nano SIM
Module:	Inseego RM4210
Chipset:	Qualcomm® Dragonwing™ FWA Gen 3 Platform Qualcomm Snapdragon SDX72 Modem-RF System
Location:	Standalone GNSS Internal antenna
Device display:	3x indicator LEDs(device, Wi-Fi, and cell status) Single line LCD display for status, Wi-Fi and cell details, mesh pairing, and FOTA updates

* See <https://inseego.com/resources/blog/ecologo-and-ul-2710-certified-devices/>.

Network connectivity*

5G NR (SA/NSA) with 3x downlink CA and 2x uplink CA

4x4 MIMO 5G sub-6 GHz

4G LTE Cat 20 fallback

4x4 MIMO 4G LTE

Bands **5G sub-6:** n2, n5, n7, n12, n13, n14, n25, n26, n29, n30, n38, n41, n48, n66, n70, n71, n77 (ext 2A), n78 (ext 2A),
 4G LTE Cat 20: 2, 4, 5, 7, 12, 13, 14, 17, 25, 26, 29, 30, 38, 41, 42, 43, 46, 48, 66, 70, 71

Wi-Fi

Wi-Fi 7 with 2x2 MU-MIMO

802.11be with EasyConnect standards

Simultaneous dual-band Wi-Fi

Full power AP Wi-Fi (30dBm) with mesh

Primary and guest networks

Connects up to 256 simultaneous Wi-Fi enabled devices

Remote management

Inseego Mobile app (when registered with Inseego Connect)

Inseego Connect device management

Cloud API support through Inseego Connect Advanced

Cloud AI messaging

FOTA management and scheduling

* Data plan required. Coverage subject to network availability.

Software and security

Seamless WAN failover and failback

Full routing stack

Policy-based routing

Static and dynamic routing

Network slicing

Virtual LANs

IPv4 and IPv6 with XLAT support

Anti-CSRF (OWASP)

VPN passthrough

IPsec VPN and OpenVPN

Speed test

FIPS 140-3 OpenSSL

Secure boot

Encrypted configuration backup/restore

WPA2/3 personal and enterprise

Wired and wireless mesh pairing

Wired and wireless mesh fronthaul and backhaul

Secure HTTPS web UI

Accessories (sold separately)

External antennas

Inseego Wavemaker mesh Wi-Fi X700

PoE to USB-C adapter

Regulatory information

Federal Communications Commission Notice (FCC – United States)

FCC ID: PKRISGFX4210, Contains FCC ID: PKRISGRM4210

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

This equipment has been tested to, and found to be within, the acceptable limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment.

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

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

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

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

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

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

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

FCC RF EXPOSURE GUIDANCE STATEMENT

This device complies with FCC Radiation Exposure Limits set forth for Uncontrolled Environment. To ensure compliance with the FCC Radio Frequency Exposure Guidelines, this device must be installed to provide at least 20cm separation from the human body at all times.

IC: 3229A-FX4210, Contains IC: 3229A-RM4210

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

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

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

1. L'appareil ne doit pas produire de brouillage.
2. L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This device complies with the Canadian ICES-003 Class B specifications. CAN ICES-003(B)/ NMB-003(B)

Cet appareil est conforme aux spécifications canadiennes ICES-003 Classe B. CAN ICES-003(B)/ NMB-003(B)

Any devices capable of operating in the band 5150–5250 MHz shall only be used indoors to reduce the potential for harmful interference to co-channel mobile satellite systems.

Tout dispositif capable de fonctionner dans la bande de 5150 à 5250 MHz ne doit être utilisé qu'à l'intérieur des bâtiments afin de réduire les risques d'interférences nuisibles avec les systèmes mobiles par satellite à canaux multiples.

ISED RF Exposure Guidance 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 23cm 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 23cm pendant le fonctionnement normal

Cellular external antenna considerations for FX4210

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

FCC (US) Authorized Frequency Bands

External antenna port	4G band	5G band	UL/Tx Frequency (MHz)	Max allowable antenna gain (dBi)
CELL1, CELL4	B71	n71	663~698	6.9
CELL1	B12	n12	699~716	7.6
CELL1	B17	–	704~716	7.6
CELL1	B13	–	777~787	8.1
CELL1	B14	n14	788~798	8.1
CELL1	B5	n5	824~849	8.4
CELL1	B26	n26	814~849	
CELL1	B70	n70	1695~1710	4.5
CELL1	B4	–	1710~1755	4.5
CELL1, CELL3	B66	n66	1710~1780	4.5
CELL1, CELL3	B2 B25	n2 n25	1850~1910 1850~1915	6.5
CELL1, CELL3	B30	n30	2305~2315	1.9
CELL1, CELL3	B38	n38	2570~2620	8.0
CELL1, CELL3	B7	n7	2500~2570	5.5
CELL1, CELL3	B41	n41	2496~2690	
CELL2, CELL3	–	n77	3450~3550 3700~3980	3.0
CELL2, CELL3	–	n78	3450~3550 3700~3800	3.0
CELL2, CELL3	B48	n48	3550~3700	3.0

ISED (CAN) Authorized Frequency Bands

External antenna port	4G band	5G band	UL/Tx Frequency (MHz)	Max allowable antenna gain (dBi)
CELL1, CELL4	B71	n71	663~698	3.9
CELL1	B12	n12	699~716	4.6
CELL1	B17	–	704~716	4.6
CELL1	B13	–	777~787	4.9
CELL1	B14	n14	788~798	4.9
CELL1	B5	n5	824~849	5.1
CELL1	B26	n26	814~849	
CELL1	B4	–	1710~1755	4.5
CELL1, CELL3	B66	n66	1710~1780	3.5
CELL1, CELL3	B2 B25	n2 n25	1850~1910 1850~1915	6.5
CELL1, CELL3	B30	n30	2305~2315	1.9
CELL1, CELL3	B38	n38	2570~2620	8.0
CELL1, CELL3	B7	n7	2500~2570	5.5
CELL1, CELL3	B41	n41	2496~2690	5.5
CELL2, CELL3	–	n77	3450~3550 3700~3980	3.0
CELL2, CELL3	–	n78	3450~3550 3700~3800	3.0
CELL3	B42	–	3400~3600	5.0
CELL3	B43	–	3600~3800	5.0
CELL2, CELL3	B48	n48	3550~3700	3.0

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 FX4200 device, or failure of the FX4200 device to transmit or receive such data.

Limited warranty and liability

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

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

The exclusive remedy for a claim under this warranty shall be limited to the repair or replacement, at INSEEGO CORP'S option, of defective or non-conforming materials,

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

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

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

Safety hazards

Do not operate the FX4200 5G Cellular 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.