User Guide

inseego

Inseego Wavemaker™

5G Cellular Router FX4200

INSEEGO COPYRIGHT STATEMENT

SOFTWARE LICENSE

Proprietary Rights Provisions:
Any software drivers provided with this product are copyrighted by Inseego Corp. and/or Inseego Corp.'s suppliers. Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp. and/or Inseego Corp. suppliers. The disassembly, decompilation, and/or Reverse Engineering of the software drivers for any purpose is strictly prohibited by international law. The copying of the software drivers, except for a reasonable number of back-up copies is strictly prohibited by international law. It is forbidden by international law to provide access to the software drivers to any person for any purpose other than processing the internal data for the intended use of the software drivers.

U.S. Government Restricted Rights Clause:
The software drivers are classified as "Commercial Computing device Software" and the U.S. Government is acquiring only "Restricted Rights" in the software drivers and their Documentation.

U.S. Government Export Administration Act Compliance Clause:
It is forbidden by US law to export, license or otherwise transfer the software drivers or Derivative Works to any country where such transfer is prohibited by the United States Export Administration Act, or any successor legislation, or in violation of the laws of any other country.

TRADEMARKS AND SERVICE MARKS

Inseego Corp. is a trademark of Inseego Corp., and the other trademarks, logos, and service marks (collectively the "Trademarks") used in this user manual are the property of Inseego Corp. or their respective owners. Nothing contained in this user manual should be construed as granting by implication, estoppel, or otherwise, a license or right of use of Inseego Corp. or any other Trademark displayed in this user manual without the written permission of Inseego Corp. or its respective owners.

- MiFi® and the MiFi logo are registered trademarks of Inseego Corp.
- Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.
- Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

The names of actual companies and products mentioned in this user manual may be the trademarks of their respective owners.

Document Number PRT-14965465 Rev 1

Contents

1

Introduction and getting started

Overview

The FX4200 cellular router provides reliable, high-speed connectivity wherever you need it, making it the ultimate broadband solution.

You'll find the following Inside the box:

- 5G Cellular Router FX4200
- Rechargeable 5050 mAh LI-ion backup battery
- Get Started Card
- USB-C cable
- AC wall adapter power supply

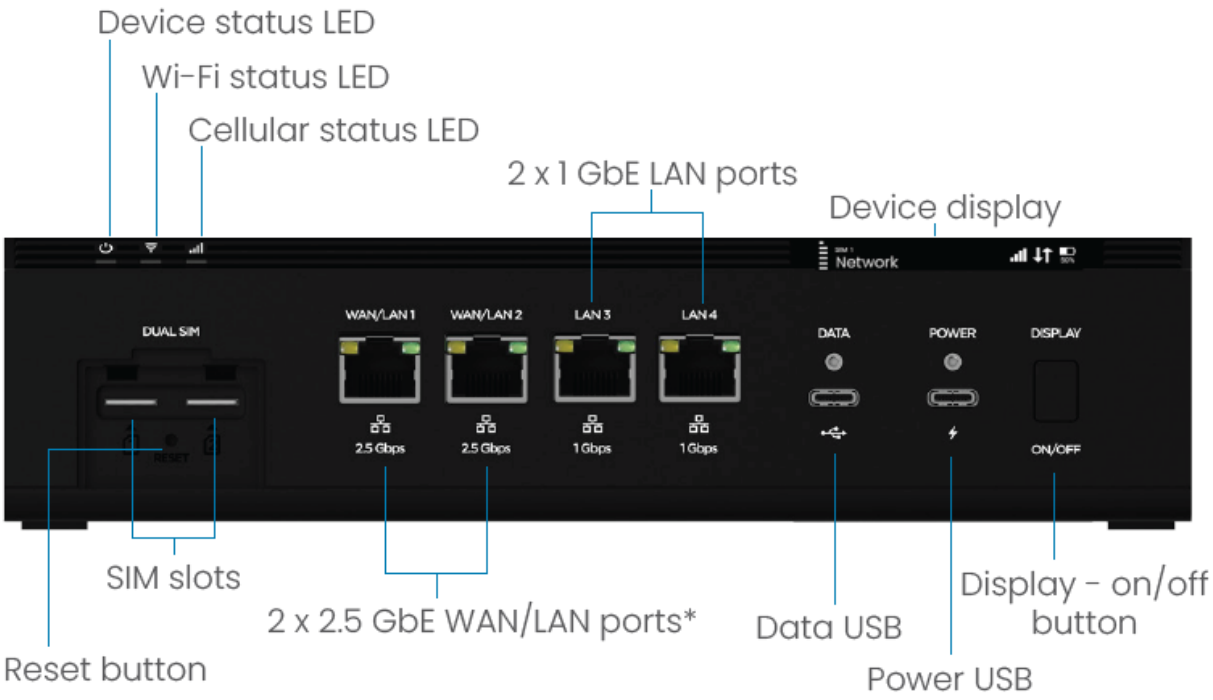
Key features

- With 5G NR, Wi-Fi 7, a quad-core processor, integrated antennas, and automatic failover, the FX4200 delivers fast, reliable wireless broadband.
- Deploys in minutes with plug and play setup and instant high-speed connectivity right out of the box.
- The FX4200 simplifies configuration with integrated antennas, built-in diagnostics, intelligent carrier selection, and automatic cloud integration through Inseego Connect™.
- Supports up to 256 connected client devices on Wi-Fi, two Ethernet WAN/LAN 2.5 GbE ports, two 1 GbE Ethernet LAN ports, and USB-C ports for power and data.
- 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.
- Enables remote and hybrid teams to work securely from anywhere. It supports secure edge networking with split or full tunnel VPNs, ensuring encrypted, high-uptime connections between headquarters and remote locations.
- Optional Inseego Mesh Wi-Fi X700 expands coverage without sacrificing performance, ensuring seamless connectivity and eliminating dead zones.

System requirements

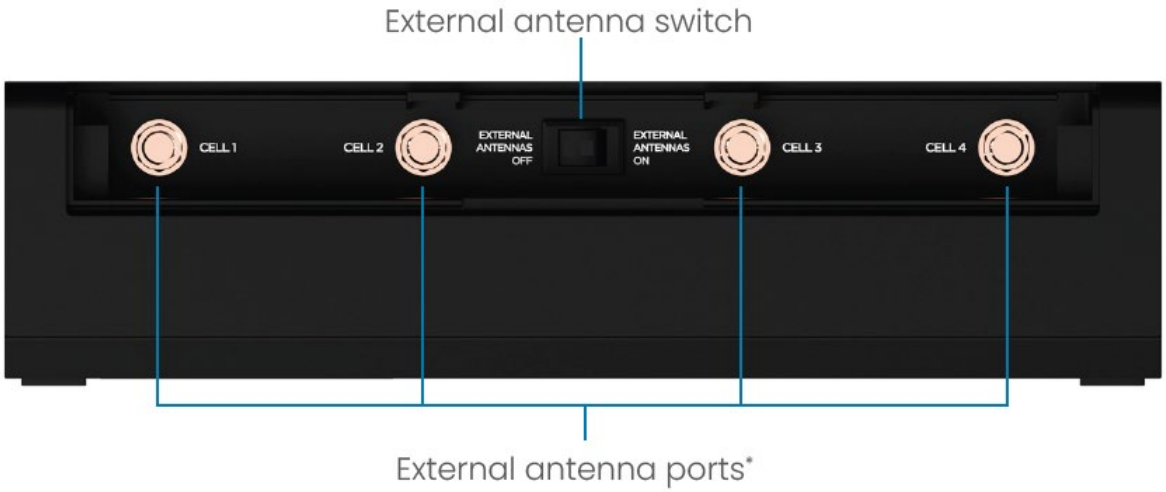
- Compatible with all major operating systems.
- Works with the latest versions of browsers.
- To use Wi-Fi, connecting devices need Wi-Fi capability. You can also connect via Ethernet or USB.

Device front



* 2.5 GbE Ethernet ports can be configured as WAN or LAN in the admin web UI **Network > Ethernet** tab, or with Inseego Connect **WAN Settings**.

Device back



* When enabled, each external antenna 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 Wi-Fi status LED, and a cellular 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 **Administration > 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
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
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

The Ethernet ports on the front of the router also have indicator LEDs.

LED Color	Operation	Meaning
Green		Indicates Ethernet connection speed
	Solid	1000 Mbps (Gigabit)
	Blinking	Data is being transferred
	Off	10/100 Mbps
Amber		Indicates port status
	Solid	Port is being connected, but no data is being transferred
	Off	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 turn the display on or off and 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:

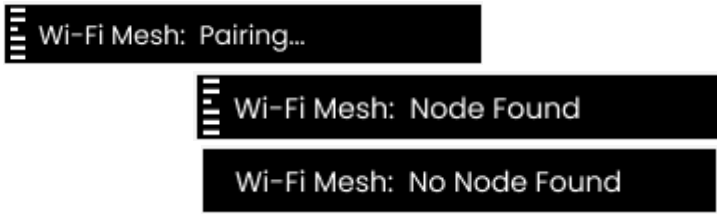
 The menu icon on the left shows you where you are in the main menu.

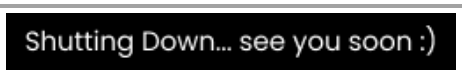
 The scroll icon on the bottom of a submenu shows you where you are in the submenu.

 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
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	
	

Main menu	Submenu
	
	       
	    
	 

Getting started

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

Installing a SIM card

Your SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The FX4200 supports only Nano SIM cards. To install 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 install a SIM card:

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

2. If necessary, remove the SIM card from the protective sleeve, being careful not to touch the metallic contacts.

3. Insert the SIM card into the SIM slot ***notch first, with the metallic contact points facing down.*** Press the card in until it clicks into place.

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 (maintain at least 2" from metal objects or electronic equipment)
- 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)

The FX4200 is equipped with nine internal antennas, providing an average 4 dBi peak gain across all frequency ranges. In addition, the device has four external full spectrum cell SMA ports (0.6-6 GHz each) to support up to four external antennas.

NOTE: If you are getting 3-5 bars signal strength, external antennas are most likely not necessary to improve performance. Adding the wrong external antennas (less than 4 dBi, including cable loss) will decrease performance.

Cases where external antennas are needed are rare and include:

- Poor signal quality
- Challenging location (basement, thick building walls, scenarios where there is a strong 5G signal outside, but only 4G inside, etc.)
- Need to boost higher frequency bands

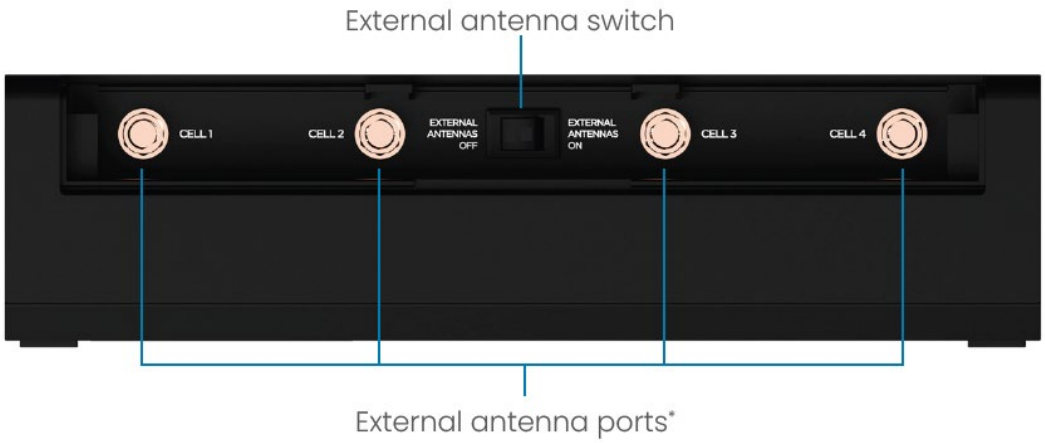
If you are using external antennas:

- You must connect an antenna to all four external antenna ports with full-spectrum antenna elements (0.6-6 GHz each.). You can use four separate antennas or a multi-element antenna from a reputable vendor with four leads.
- When the External Antennas switch is on, the six internal WWAN antennas are disabled – leaving the two Wi-Fi and one GPS internal antenna enabled.
- External antennas must provide at least 4 dBi (with cable loss factored in) and reasonable efficiency (~ greater than 50%), or they will decrease performance.
- When purchasing antennas, consider the reliability of the manufacturer - specs should show gain per frequency range rather than a singular gain number, correct connectors, bands/frequencies, and cable loss.

To use external antennas:

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

2. Tighten external antennas to the external antenna ports to 5 in-lbs. You must attach four discrete antennas or a multi-element antenna from a reputable vendor with four leads.

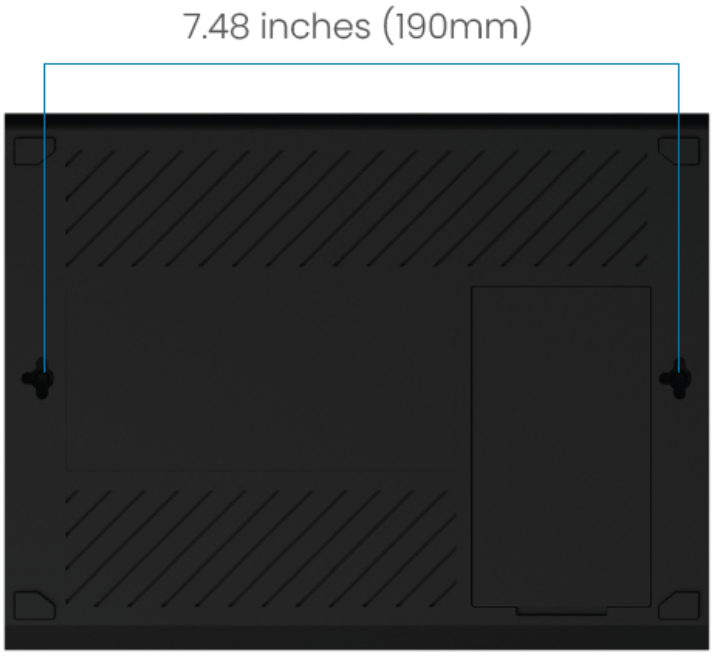


3. Flip the switch to **EXTERNAL ANTENNAS ON**. When enabled, each external port supports the full cellular frequency range of 0.6-6 GHz. An antenna icon appears on the main screen of the device display and in the admin web UI.

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

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.

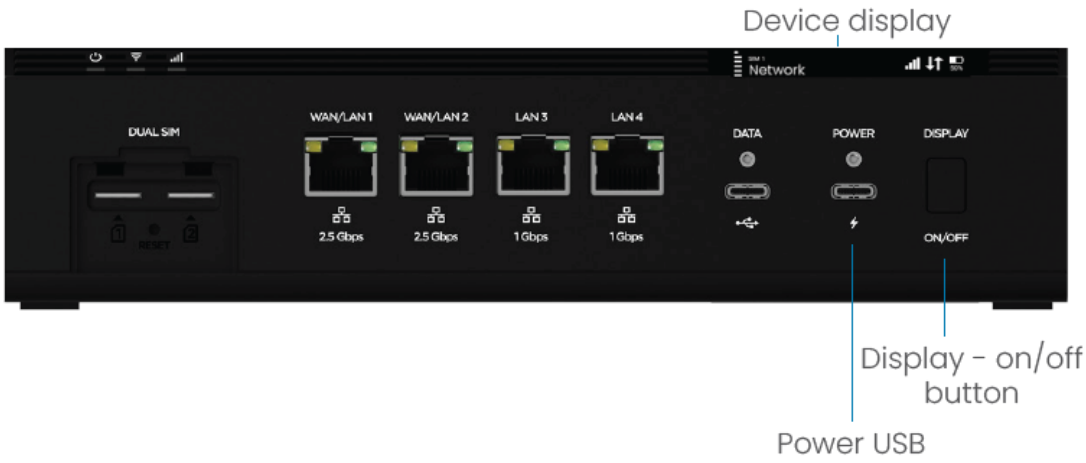
Inseego recommends professional installation to assure safety when drilling near electrical lines, plumbing, or other hazards.

Powering on

To turn on your router, follow these steps:

1. Press the ON/off button to power on with the battery.
   OR
   Plug the USB C cable into the router power port and plug the other end into any of the following:
   - 24W (12V, 2A) AC power adapter (provided)
   - USB-powered hub
   - USB power delivery (PD) host equipment

   WARNING! Use only the AC wall adapter power supply and cable that are packaged with the FX4200. 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 cellular network name and arrows indicating traffic is active.

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

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).

Powering off

To turn your router off:

1. Press the device display – on/off button until you are at the bottom of the side menu at the shutdown screen.

2. Press and hold the button until you see a message that the device is shutting down.

Connecting devices to the router

With your FX4200, 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 mesh is enabled).

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.

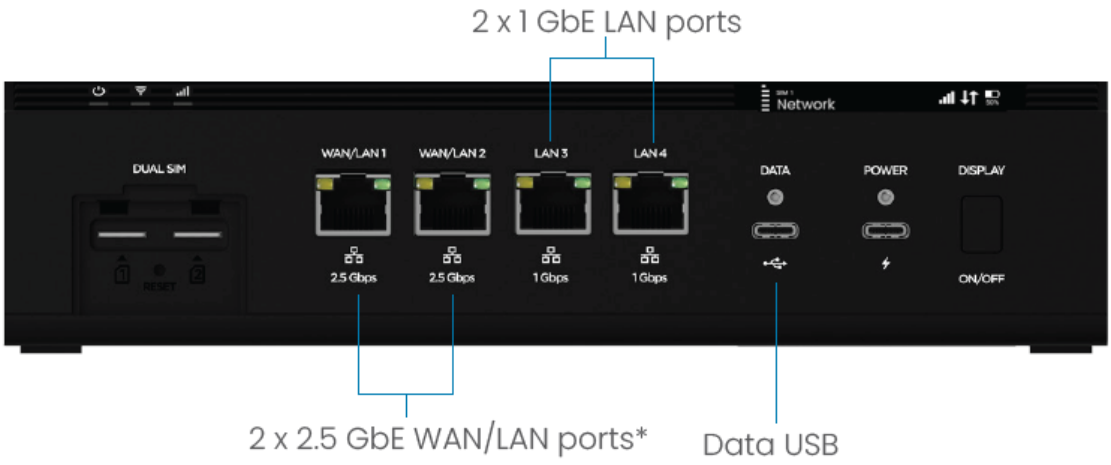
4. When prompted, enter the **Primary Wi-Fi Password** printed on the bottom of the router.

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

NOTE: See Primary Network on page 53 for instructions on changing your primary Wi-Fi network name and/or password. See Guest Network on page 55 for information on setting up a guest network.

Connecting devices with Ethernet or USB

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



To connect Ethernet devices:

1. Plug one end of an Ethernet cable into a WAN or 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 **Data** 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.

* 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 > Ethernet**, or with Inseego Connect: **WAN Settings**.

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 **Log 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 34.

Inseego Mobile app

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

Inseego Connect

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

NOTE: If you used the Inseego Mobile app to set up your router, it may have added it to Inseego Connect. When logging in to Inseego Connect, check to see if your router is already registered and appears on the **Device List** page. If it is not, check **Devices › Register**. If the router is listed there, restart your router to hasten the registration process.

---

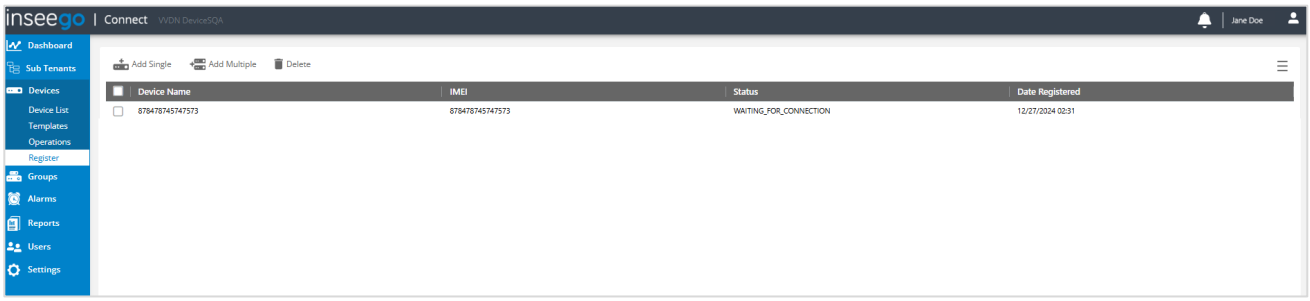
* The Inseego.local web UI address relies on having IPv6 enabled on your connecting device.
NOTE: Connected devices using IPv6 are not compatible with Fortinet VPN. Disable IPv6 on the connected device to use Fortinet.

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

Adding a device with Inseego Connect

To add a device or multiple devices to Inseego Connect:

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

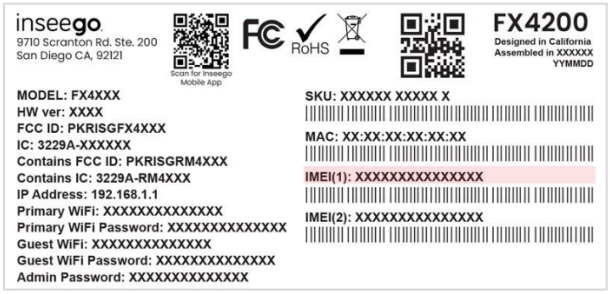


3. Use the tools along the top of the table to add devices.

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

   a. Enter a **Device Name** (optional).

   b. Enter **IMEI(1)** printed on the device label.



   c. For **Device Password**, enter the current Admin web UI password. If you have already logged into the device's Admin web UI and changed the Admin password, use the new password. If you have not changed the Admin password, the default is printed on the label.

   d. Click **Register**. The device enters the WAITING_FOR_CONNECTION state while waiting to connect to the Inseego cloud.

   e. Restart the device.

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

   a. Click the Download sample template (.xlsx) link.

b. Open the .xlsx file and enter a **Name** (optional), **IMEI**, and **Password** for each device you wish to register.
c. Click **Upload**. The devices enter the WAITING_FOR_CONNECTION state while waiting to connect to the Inseego cloud.
d. Restart the devices.

IMPORTANT: Restart the device(s) immediately after adding. This allows the device(s) to check in and process the registration request.

Once the registration process is complete, devices appear on the **Device List** page and no longer appear on the **Register** page.

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 is compatible with the Inseego Wavemaker X700 Mesh Wi-Fi. Refer to the X700 Mesh Wi-Fi documentation at go.inseego.com/x700 for more information.

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 within 10 to 50 feet of each other when connecting via Wi-Fi. You'll position the mesh node after connecting.
- 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:

1. Power on the FX4200. When the FX4200 Wi-Fi status LED is **solid green** or **blue**, it is ready to pair.
2. On a device connected to the router, open any web browser, and log in to the admin web UI at http://192.168.1.1 or http://Inseego.local *.
3. Navigate to **Network > Wi-Fi** and ensure that **Enable Mesh Network** slider is **on**.

* 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.

4. Power on the X700. You can use the provided AC adapter, a USB-powered hub, or USB power delivery (PD) host equipment.

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

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

Pair 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

- Ensure the router and mesh node are within 10 to 50 feet of one another. You can position the mesh node after pairing.
- 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**.
- **Wait** – pairing takes 2 – 3 minutes. The light on the X700 and the Wi-Fi status LED  on the router blink blue while pairing.
- 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:

- Ensure the router and mesh node are within 10 to 50 feet of one another. You can position the mesh node after pairing.
- 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.
- **Wait** – pairing takes 2 – 3 minutes. The light on the X700 and the Wi-Fi status LED  on the router blink blue while pairing.
- 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.

Pair with Ethernet

- Connect an Ethernet cable from the X700 to a LAN port on the FX4200.
  NOTE: The router and mesh node must be within 300 feet of each other.
- 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.

Caring for your router

This section provides information on replacing a SIM card, restoring your FX4200 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 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 cover on the front of the router.

2. Remove the existing SIM card you want to replace.

2. If necessary, remove the SIM card from the protective sleeve, being careful not to touch the metallic contacts.

3. Insert the SIM card into the SIM slot ***notch first, with the metallic contact points facing down***. Press the card in until it clicks into place.

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

Battery tips

Before operating your FX4200 on a battery:

- Ensure the battery is fully charged.
- Find a location with optimal signal strength.

WARNING! Always use official OEM approved batteries and chargers with your router. The warranty does not cover damage caused by non-approved batteries and/or chargers.

- Do not use sharp objects or use excessive force to remove the battery or to access the battery well, this may damage the router and the battery.
- The battery discharges more rapidly as additional devices access your router.
- Battery life depends on the network, signal strength, temperature, features, and accessories you use.
- New batteries or batteries that have been stored for a long time may take more time to charge.
- When storing your battery, keep it uncharged in a cool, dark, dry place.
- When charging your battery, keep it near room temperature.
- Never expose batteries to temperatures below -30°C (-22°F) or above 70°C (158°F).
- Never leave the router in an unattended vehicle where it can get too hot or too cold.
- Some batteries perform best after several full charge/discharge cycles.
- It is normal for batteries to gradually wear down and require longer charging times. If you notice a change in your battery life, it is probably time to purchase a new battery.

Replacing the battery

CAUTION: Whenever you remove or insert the battery, ensure your router is not connected to any device or power source. Never use tools, knives, keys, pens or any type of object to force the door open or to remove the battery. Using any of these types of objects could result in puncturing the battery.

To remove and replace the battery:

1. Insert a fingernail at the edge of the battery cover on the bottom of the router and lift and remove it. Set the cover aside.
2. Insert your finger into the battery removal divot and lift the battery out of the battery compartment.
3. Align the gold contacts on the new battery with the gold contacts on the router and gently slide the battery into place.
4. Replace the cover, ensuring it clicks into place and is flat across the entire bottom surface.

Resetting your router

You can restart or reset your FX4200 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 connected devices.

Resetting from the admin web UI

To reset the router from the admin web UI, select **Administration > Software**, then select **Restarting your router** or **Restoring to 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 device status LED blinks white, then turns red. When the LED is solid white, 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

You can configure your FX4200 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:

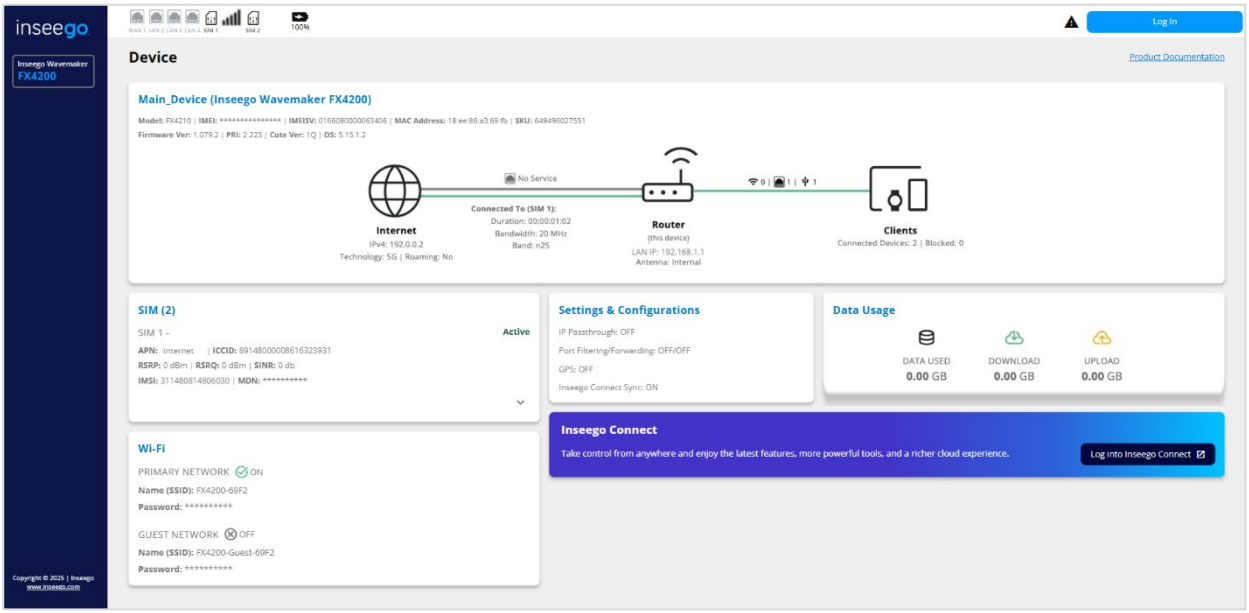
- **Admin web UI** – Provides local access to configure and manage your router. On a device connected to the router, open any web browser, and go to http://192.168.1.1 or http://Inseego.local [*]. Select **Log In** (in the top-right corner of the screen) and enter the **Admin Password** printed on the bottom of the router.
- **Inseego Connect** – Enables you to deploy, monitor, and manage Inseego IoT devices remotely from the cloud. You can group devices together to push widespread configurations, troubleshoot individual devices, set alarms, and run reports. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free Inseego Connect account at connect.inseego.com.
- **Inseego Mobile app** – Use the mobile app to perform basic device monitoring and management.

This chapter provides the configuration options available for your 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, 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 35.



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 white highlight. 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.
- Click on the alert icon in the upper right to view alert messages.

Getting help

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

You can also click on Product Documentation in the upper right-hand corner of any page to jump to the full set of online documentation for the FX4200.

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.

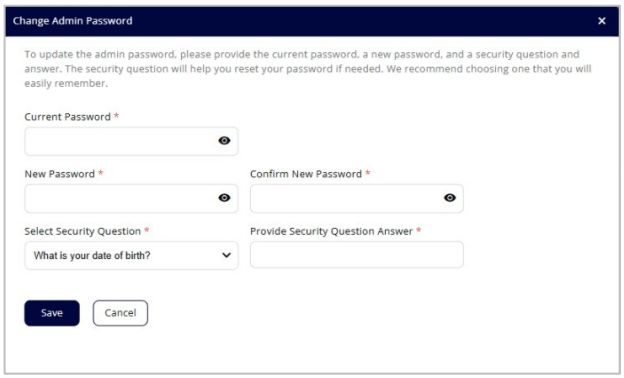
NOTE: You can set up separate Wi-Fi passwords for both primary and guest networks in **Wi-Fi**, but these are different from the admin password, which is for this web user interface.

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.



   Or,

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

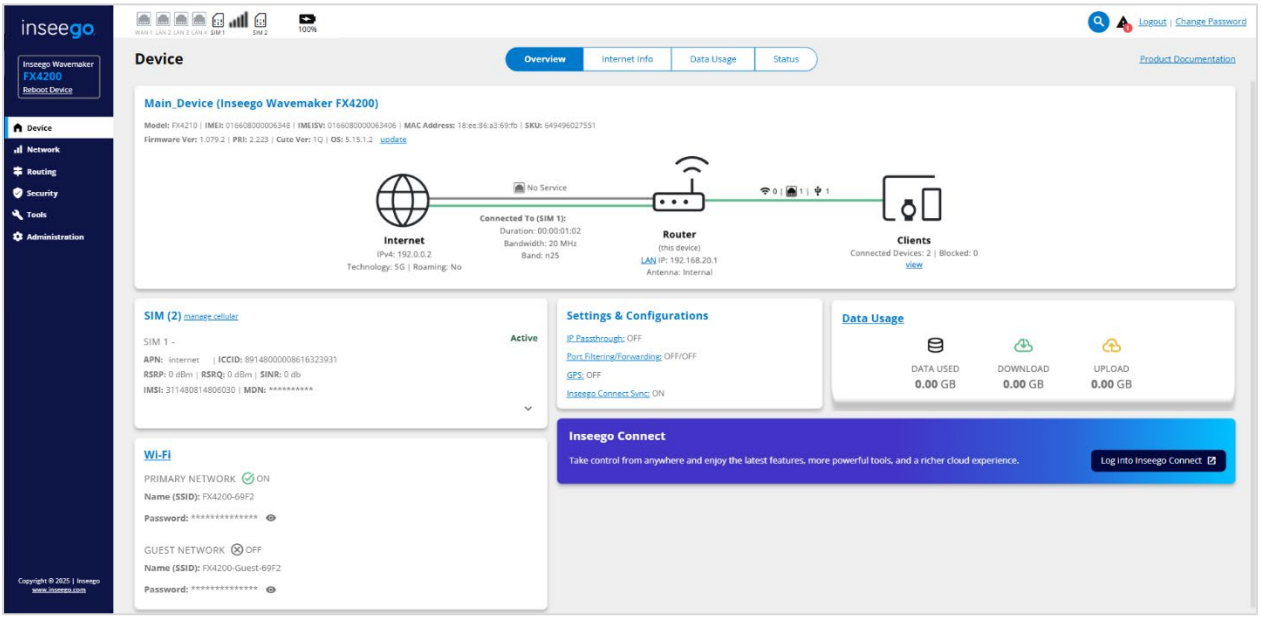
Managing devices

The Device page includes the following tabs:

- Overview
- Internet Info
- Data Usage
- Status

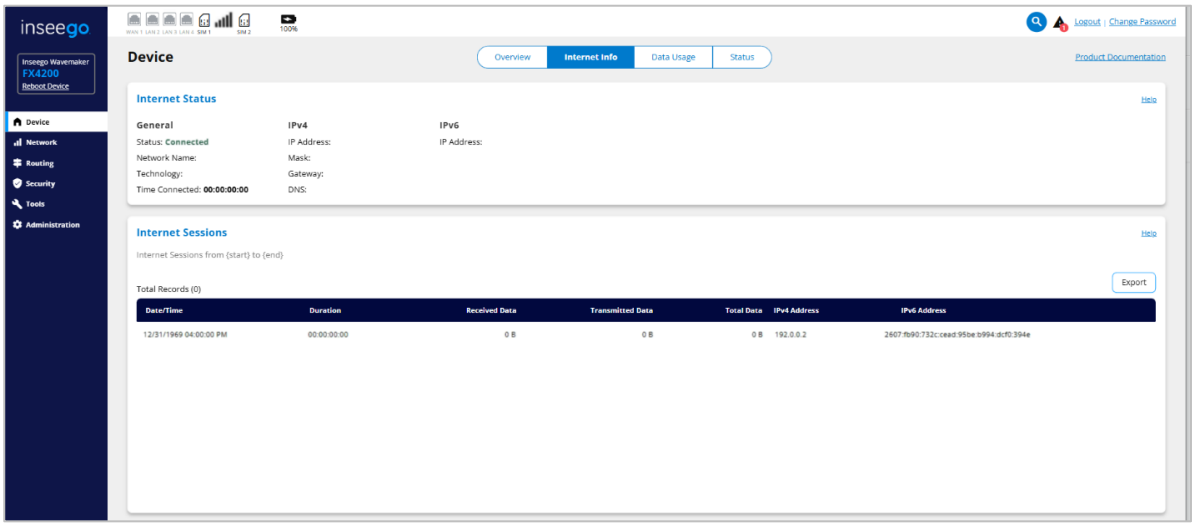
Overview tab

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, common settings, data usage stats, and current Wi-Fi networks and passwords. Use the links to jump to a specific topic for more details and configuration options or navigate using the side menu.



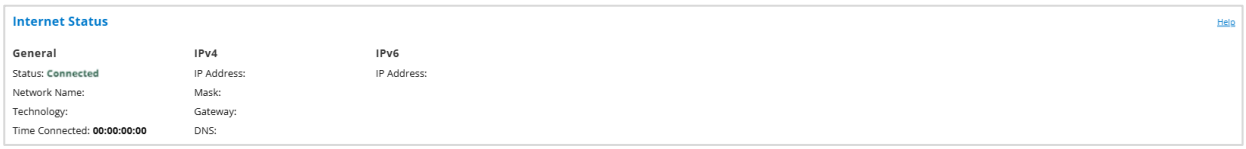
Internet Info tab

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



Internet Status

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



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.

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.

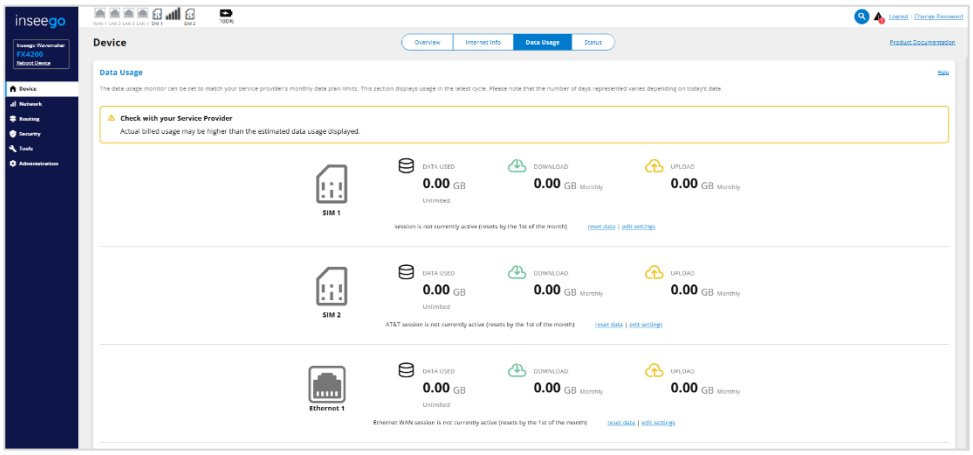
IPv6 Address: The global IPv6 address for the session (blank if IPv6 is turned off or is not supported by the current network connection or service provider).

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.

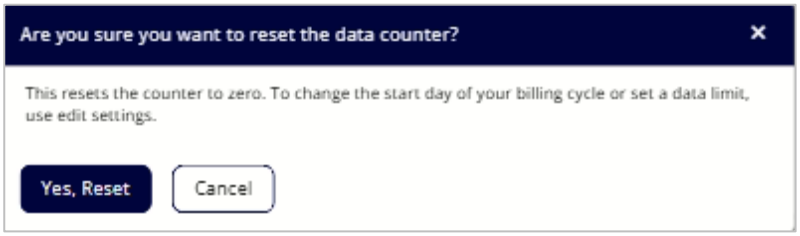
NOTE: Your FX4200 provides only a rough estimate of data usage. Always check with your service provider for exact usage.



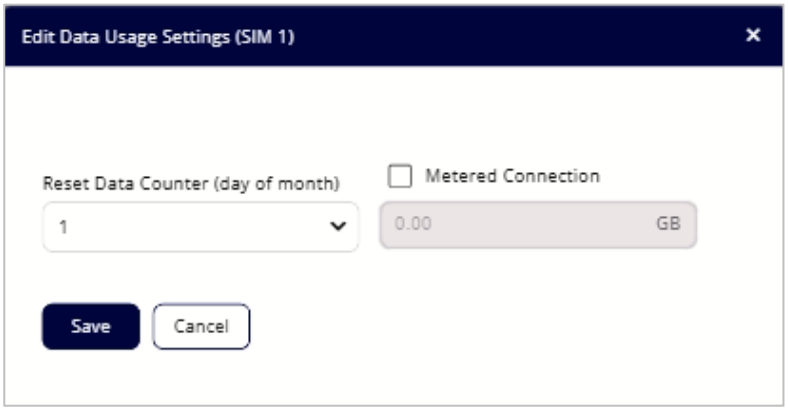
The data usage tab displays the following information for your SIM(s) and WAN Ethernet connection:

- **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.



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

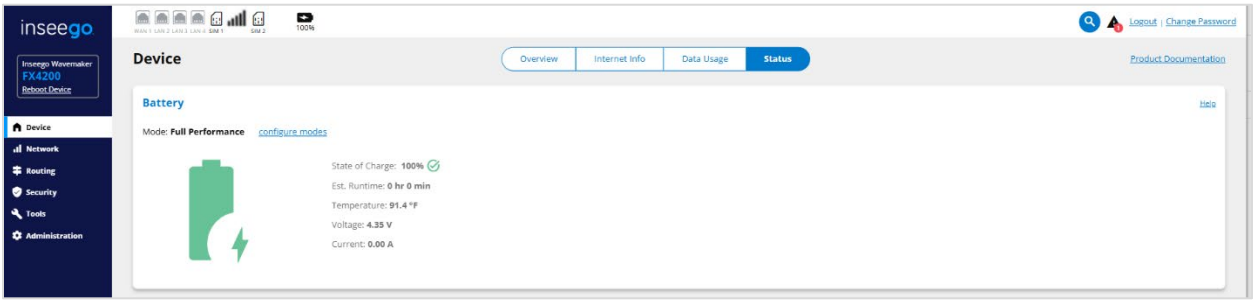
Metered Connection: Check this box if there is a data limit on your plan, then enter a maximum data limit in the box below.

Click **Save** to enact changes.

Status tab

The FX4200 has a rechargeable 5050 mAh LI-ion backup battery that is accessible from a compartment on the bottom of the router. Use the Status tab to view information on the status of the battery.

NOTE: When running on a battery that has 30% or less charge, automatic firmware updates are disabled.



Mode: The mode the battery is currently in.

Click **battery management** to configure and enable/disable battery modes to meet your needs. Refer to Battery Management on page 96.

State of Charge: The current charge of the battery. The color is green when in Full Performance mode, yellow when in Mission Critical mode (if enabled), and red when in Low Power mode.

Est. Runtime: The approximate amount of charging time for the battery to be at full power.

Temperature: The current temperature of the battery.

Voltage: The current charging voltage of the battery.

Current: The current discharge rate of the battery.

Managing your network

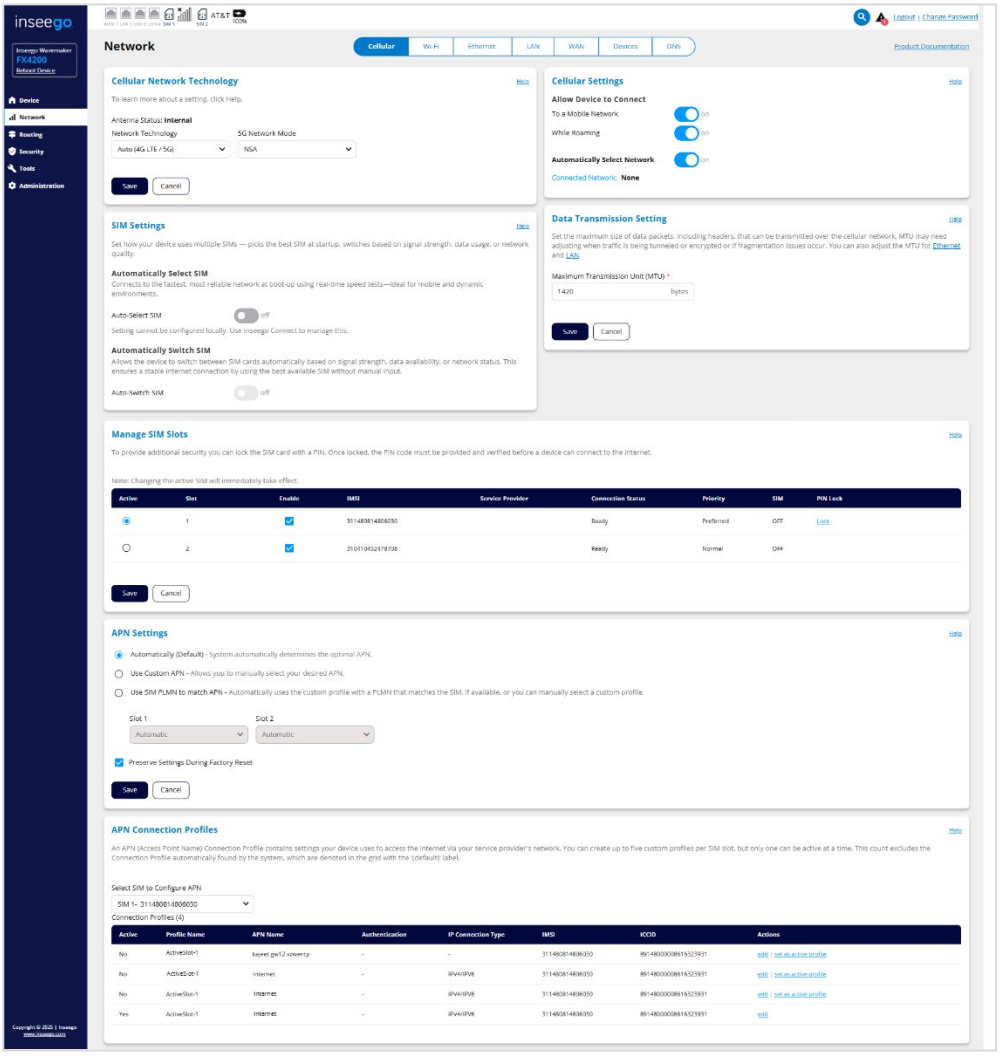
Use Network tabs to view and configure settings for your router's network.

The Network page includes the following tabs:

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

Cellular tab

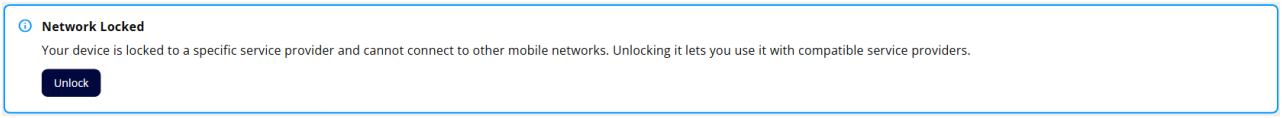
Use this tab to set options for the cellular network.



Network Locked

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

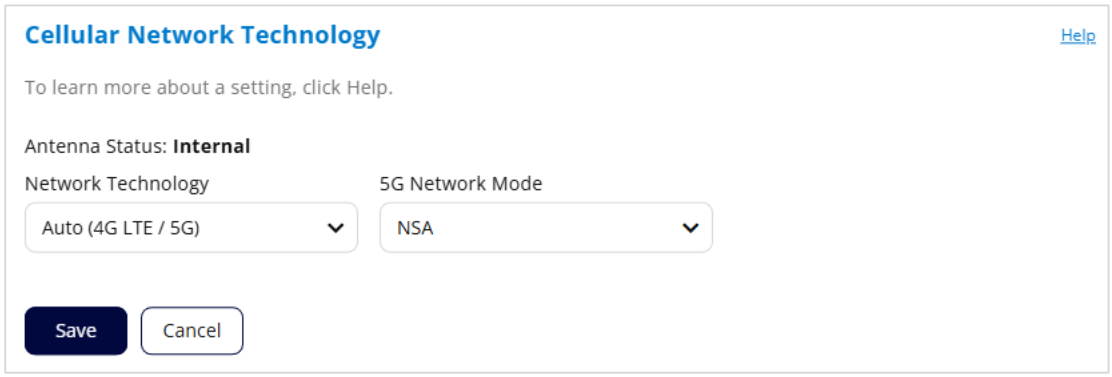
Locked devices can only use the network currently provided by the service provider. Use this section if you want to unlock your router to use with a different service provider.



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

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.



Antenna State: Internal indicates the external antenna switch is set to **EXTERNAL ANTENNAS OFF** and all nine internal antennas are enabled. **External** indicates the switch is set to **EXTERNAL ANTENNAS ON**.

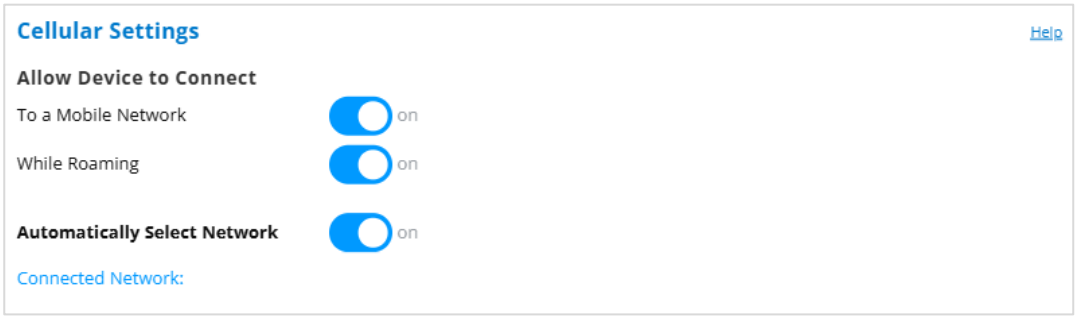
Network Technology: Your router is set to Auto (4G LTE/5G) by default, which prioritizes 5G but allows 4G and other non-5G technologies to be used. If you select 4G LTE or 5G from the dropdown, your router is restricted from connecting to networks not using that technology, for example, if you select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



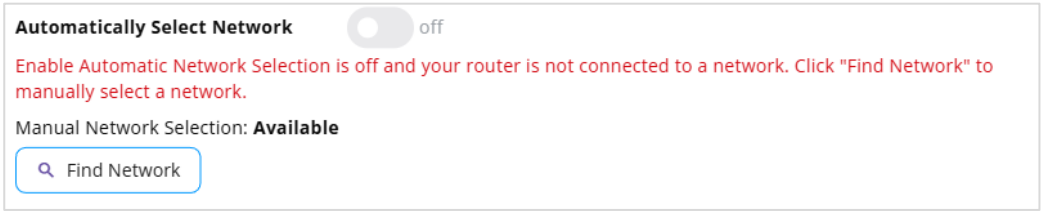
Allow Device to Connect

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.



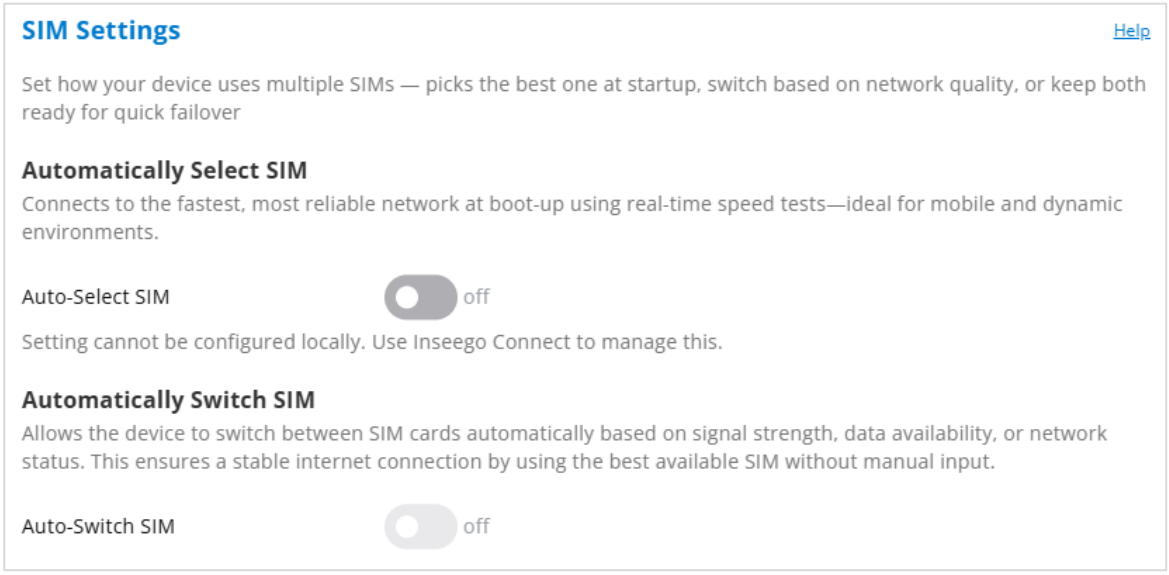
Find Network: You may wish to manually select a network if multiple networks are available and you have a preference. Click the button to scan for available networks, then choose the preferred network and click **Select Network**.
NOTE: This option is available only if **Automatically Select Network** is **off**.

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

SIM Settings

Use this section to view and configure how your device uses multiple SIMs.

NOTE: Inseego Connect offers more selections for these settings.



Automatically Select SIM

Auto-Select SIM: When **on**, speed tests determine the best SIM to use when powering on the device.

Automatically Switch SIM

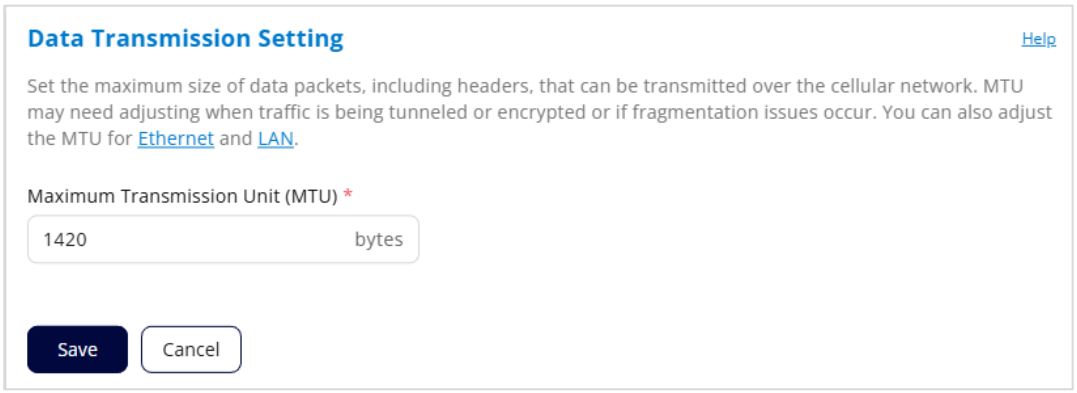
Auto-Switch SIM:

- When **on**, the device switches between SIM cards automatically, based on signal strength, data availability, and network connection status.
- When **off**, you can manually switch between SIMs in **Manage SIM Slots** below.

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.

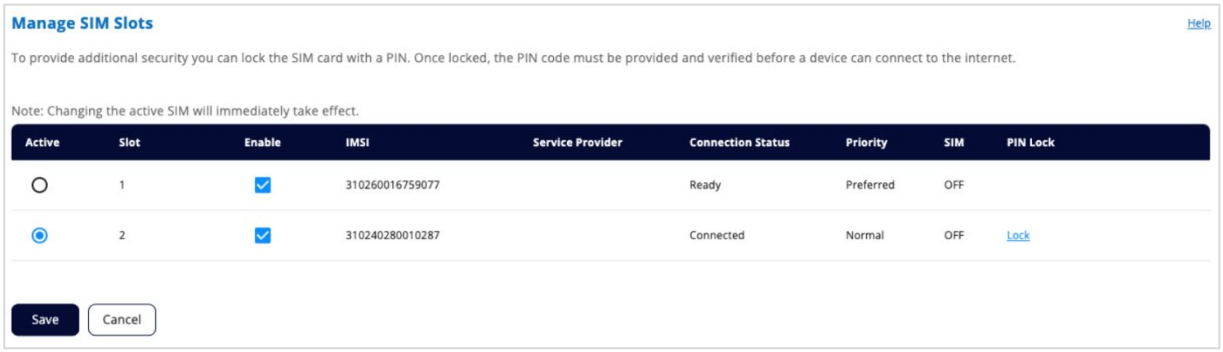
NOTE: You can also adjust the MTU for your WAN Ethernet connection on the Ethernet tab, and for your LAN network on the LAN tab.



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.

Manage SIM Slots

Use this section to manually switch between SIMs and lock or unlock SIMs. 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.



Active: If **Auto-Switch SIM** is not enabled in **SIM Settings** above, select the SIM(s) you want to be active.

Slot: The SIM slot number.

Enable: When selected, the system runs a speed test on the SIM whenever the router boots up.

IMSI: The International Mobile Subscriber Identity (IMSI) for your router. This is a unique number, usually fifteen digits, that identifies a Global System for Mobile Communications (GSM) subscriber.

Service Provider: The service provider associated with the SIM.

Connection Status: The current connection status of the SIM.

Priority: Indicates whether the priority of the SIM (Preferred or Normal).

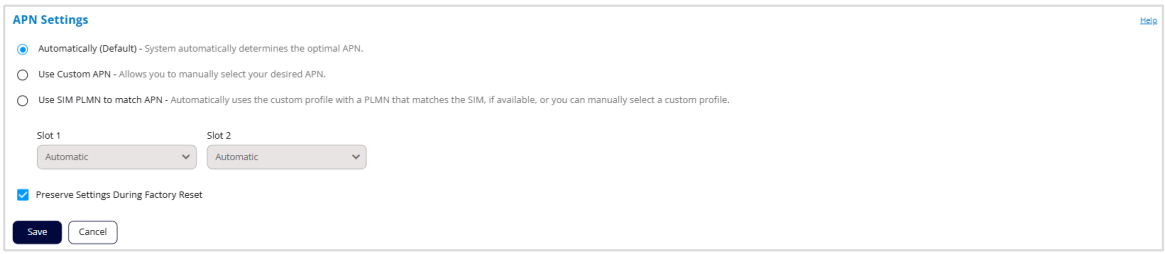
SIM: The current state of the SIM lock.

PIN Lock:

- **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.
- **Unlock** - 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.

APN Settings

By default, the system automatically determines the connection profile and APN for each SIM. Use this section to change how APNs are selected.



Automatically (Default) – The system automatically determines the optimal APN for each SIM.

Use Custom APN – You can manually assign a connection profile for each SIM from the custom connection profiles in the **APN Connection Profiles** section below.

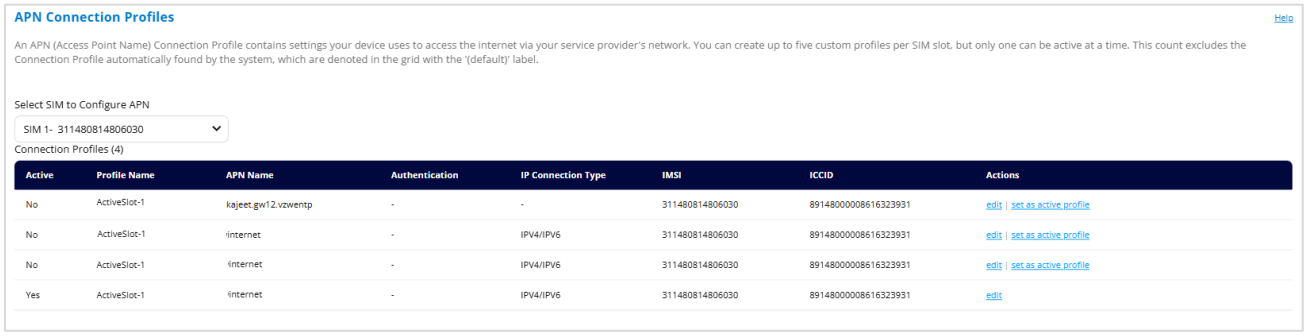
Use SIM PLMN to match APN –The system automatically sets the profile for each SIM based on a PLMN match between the SIM and the custom connection profiles in the **APN Connection Profiles** section below. If there is no PLMN match, the system selects a profile without a PLMN. You can also manually select profiles for a SIM.

Preserve Settings During Factory Reset: When this box is checked, your APN settings will remain even after a factory reset of the device.

Click **Save**.

APN Connection Profiles

In most configurations, the FX4200 is used with dynamic IP and SIMs, and Access Point Names (APNs) are available from the network, for example: *internet*. However, if you are on a private network, you may need to configure connection profiles for your APNs in this section for the network to communicate with the router.



Select SIM to Configure APN: Use the dropdown to select the SIM for which you are configuring APN.

Connection Profiles

This table lists all the APN connection profiles that have been defined. The number of profiles appears next to the title.
NOTE: Initially, the default APN profile is displayed. You cannot delete this profile, but you can edit it and/or add additional profiles.

Priority: The order in which the profile logic checks the connection profiles. **NOTE:** This column is not available when Automatically (Default) is selected in APN Settings.

Active: Indicates whether a profile is currently set as the active profile. **NOTE:** Click on **set as active profile** on the right to select the connection profile you want to be active.

Profile Name: The name that identifies the connection profile.

APN Name: The access point name.

Authentication: The authentication method for the connection profile.

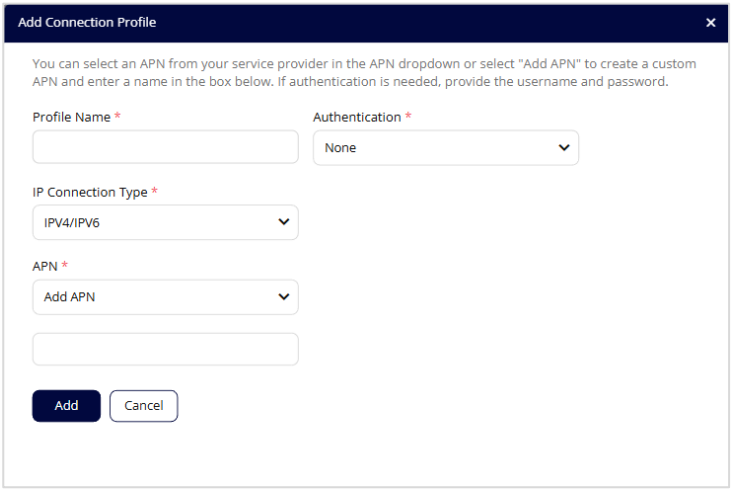
IP Connection Type: The IP connection type for the connection profile.

PLMN: The Public Land Mobile Network(PLMN) for the connection profile. **NOTE:** This column is only available if you have selected **Use SIM PLMN to Match APN** in APN Settings.

Actions:

- Click **edit** to edit a profile.
- Click **delete** to delete a profile.
- Click **set as active** to set a profile as the active profile.
  CAUTION! Changing the APN may cause a loss of data connectivity.

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

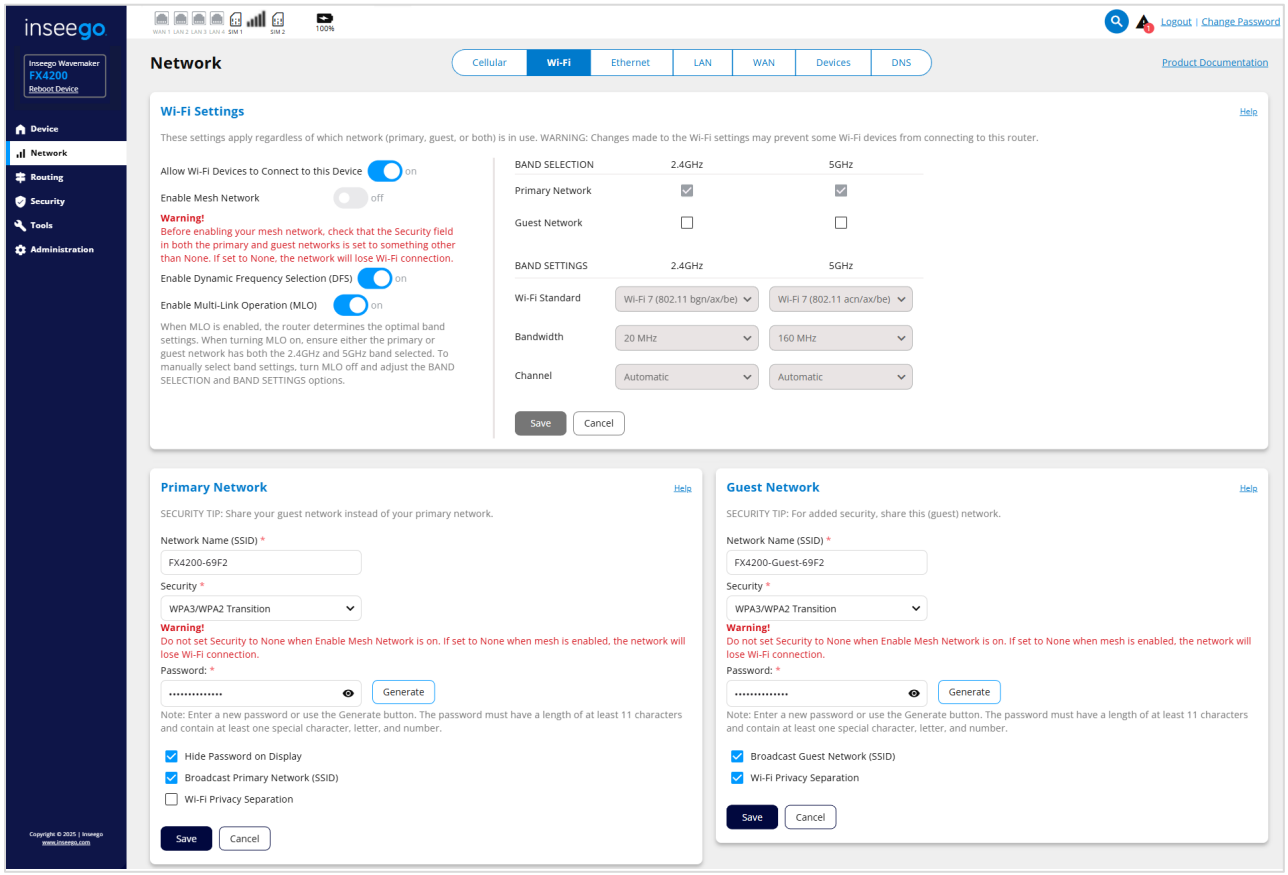


- **Profile Name:** Enter a name to identify this connection profile.
- **IP Connection Type:** Select an IP connection type from the dropdown (IPv4, IPv6, or IPv4/IPv6).
- **APN:** Select an APN supplied by your service provider from the dropdown or select **Add APN** and enter the APN for your private network in the text box that appears below.
- **PLMN:** The Public Land Mobile Network(PLMN) for the connection profile. **NOTE:** This column is only available if you have selected **Use SIM PLMN to Match APN** in APN Settings.
- **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**.

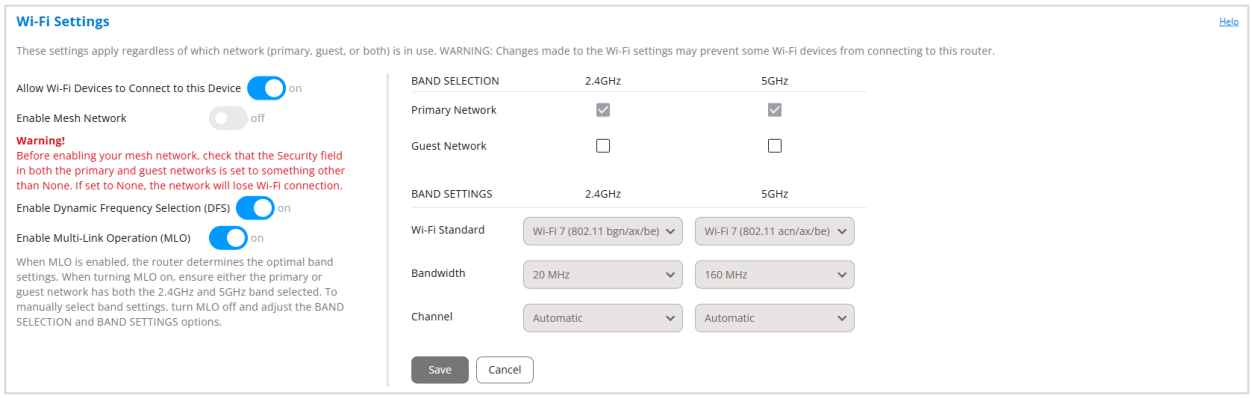
Wi-Fi tab

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



Wi-Fi Settings

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



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 FX4200 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 **off** by default. Turn it **on** to use mesh nodes to expand your network coverage.
NOTES:

- Both the **2.4GHz and 5GHz band must be selected** for your Primary Network in **BAND SELECTION** to enable mesh.
- Make sure the **Security** field in both your primary and guest networks is set to something **other than None** before enabling your mesh network. If Security is set to None, the network will lose Wi-Fi connection.
- If you disable this setting after it has been enabled, 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.
- Use the **Mesh Network** section below to add and manage mesh nodes.

Enable Dynamic Frequency Selection (DFS): DFS is **off** 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 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.

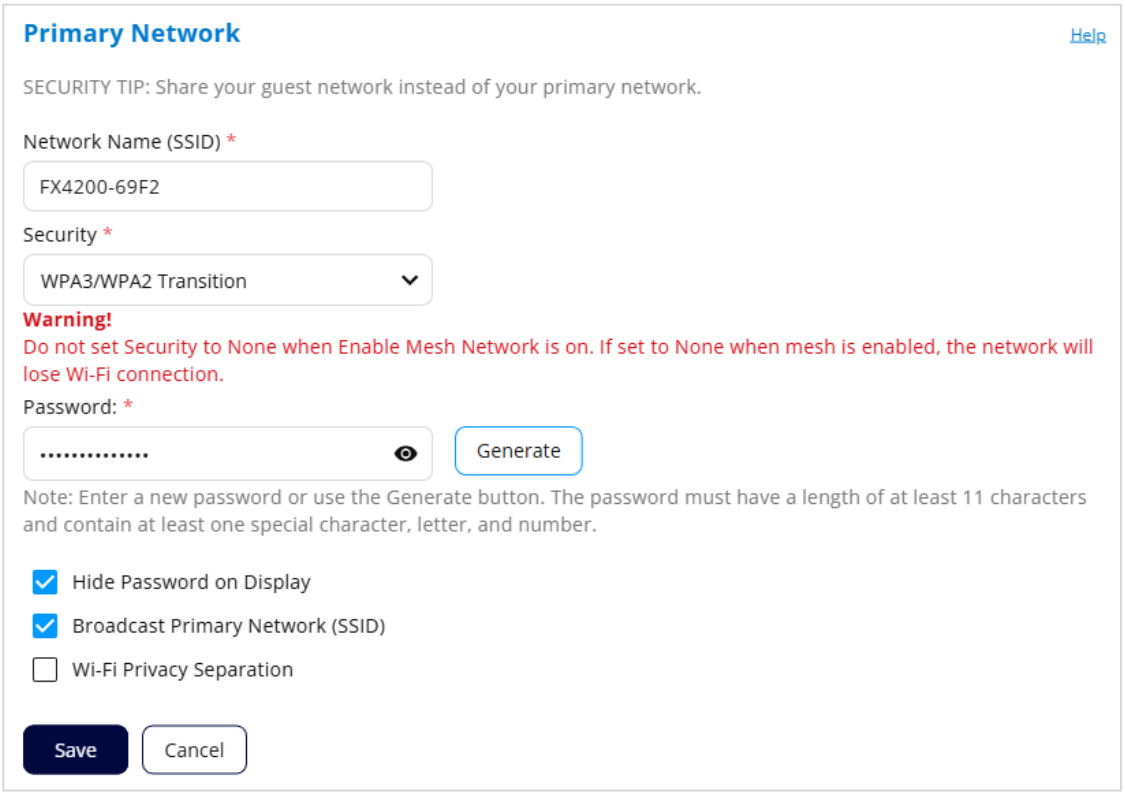
Bandwidth: Leave bandwidth at the default setting unless you experience interference with other Wi-Fi devices.

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.



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, and at least one number and/or 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 primary Wi-Fi 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 Device display on page 11).

Broadcast Primary Network (SSID): This option is checked by default, allowing the primary Wi-Fi 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.

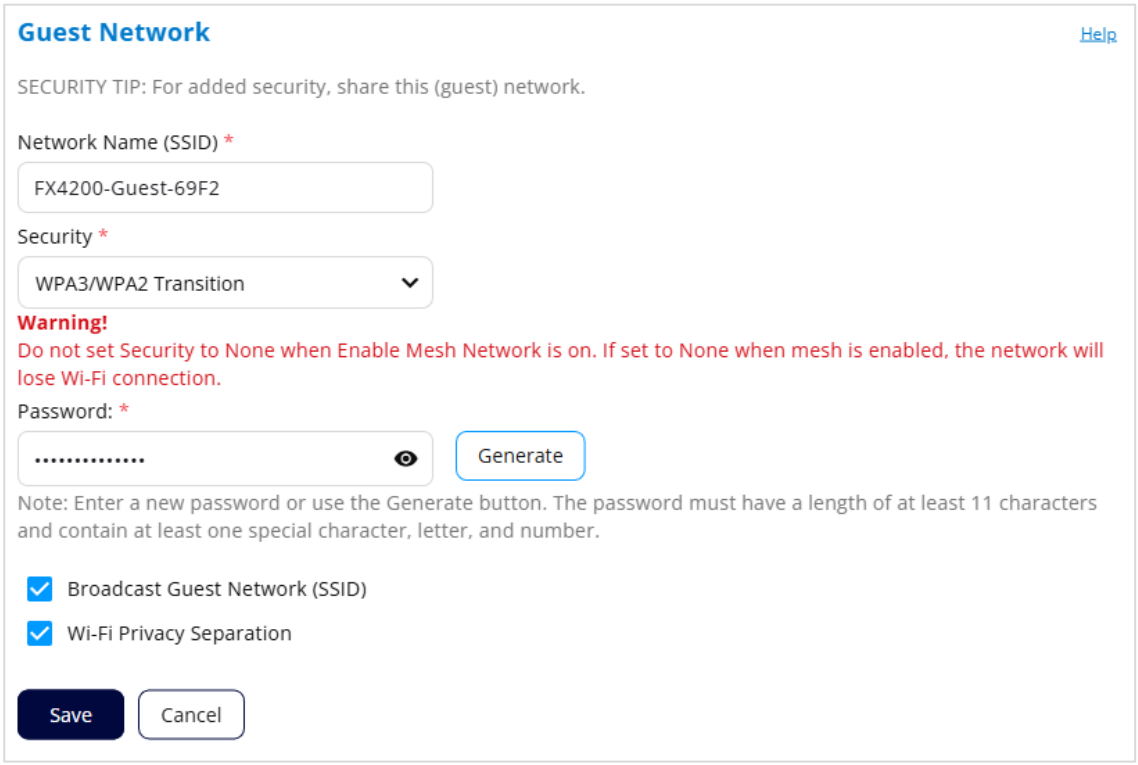
Wi-Fi Privacy Separation: Check this box to keep each connected client device on this network isolated from all other connected client devices. This provides additional security if some connected client devices are unknown or not completely trusted.
NOTE: For normal operation, this should be unchecked.

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 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**.



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, and at least one number and/or 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 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.

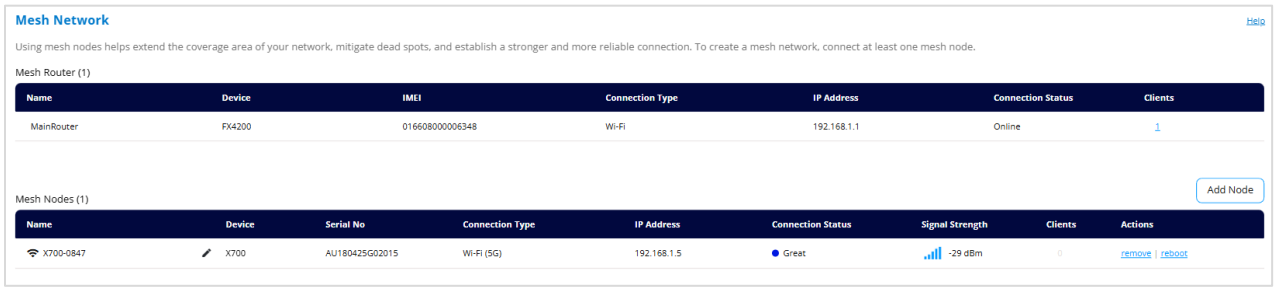
Wi-Fi Privacy Separation: Check this box to keep each connected client device on this network isolated from all other connected client devices. This provides additional security if some connected client devices are unknown or not completely trusted.
NOTE: For normal operation, this should be unchecked.

Select **Save**.

Mesh Network

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

NOTE: This section is only visible when **Enable Mesh Network** in Wi-Fi Settings above is **on**.



Mesh Router

This table provides information on your FX4200(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. To change the name as it appears to connecting client devices, use the **Administration > Preferences** tab.)

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:

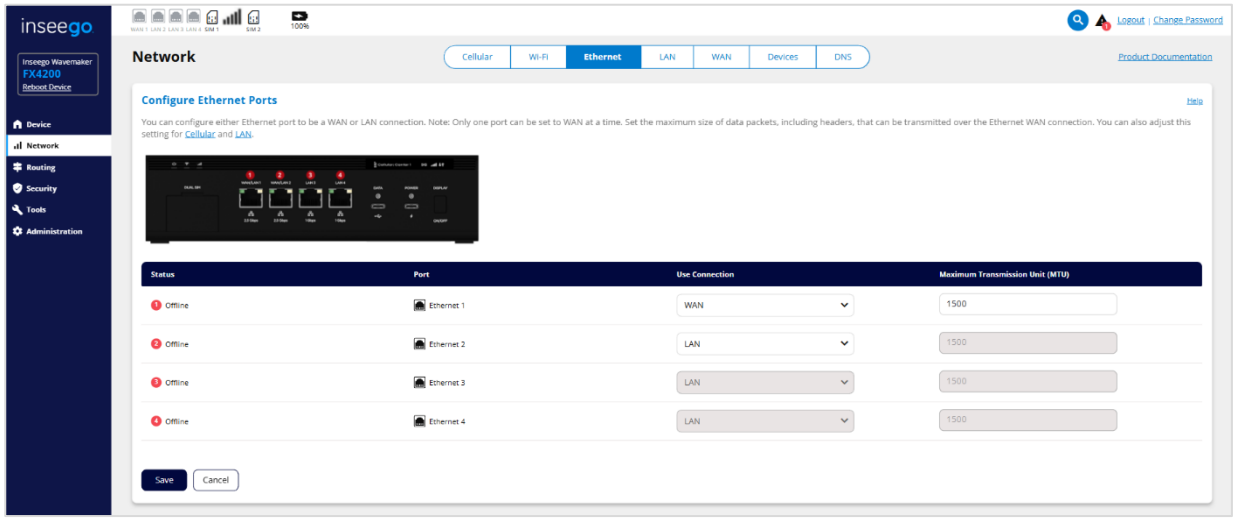
1. Ensure the router and mesh node are within 10 to 50 feet of one another. You can position the mesh node after pairing.
2. Ensure **Enable Mesh Network** in Wi-Fi Settings above is **on**.
3. Power on the X700. You can use the provided AC adapter, a USB-powered hub, or USB powered delivery (PD) host equipment.

   When the X700 LED is blinking green, it is ready to pair.
4. Click the **Add Node button** on the **Network > Wi-Fi** web UI page.
5. Within 30 seconds, press the **Mesh button** on the back of the X700.
6. **Wait** – pairing takes 2 – 3 minutes. The light on the X700 and the Wi-Fi status LED on the router blink blue while pairing.
7. 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 FX4200, or by connecting to the mesh node via Ethernet. See Pairing mesh nodes (optional) on page 23 for more information.

Ethernet tab

Use this tab to configure Ethernet ports. The two ports on the left are labeled as WAN/LAN on the FX4200, and 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.



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

Port: The ports are numbered 1 – 4, from left to right on your router.

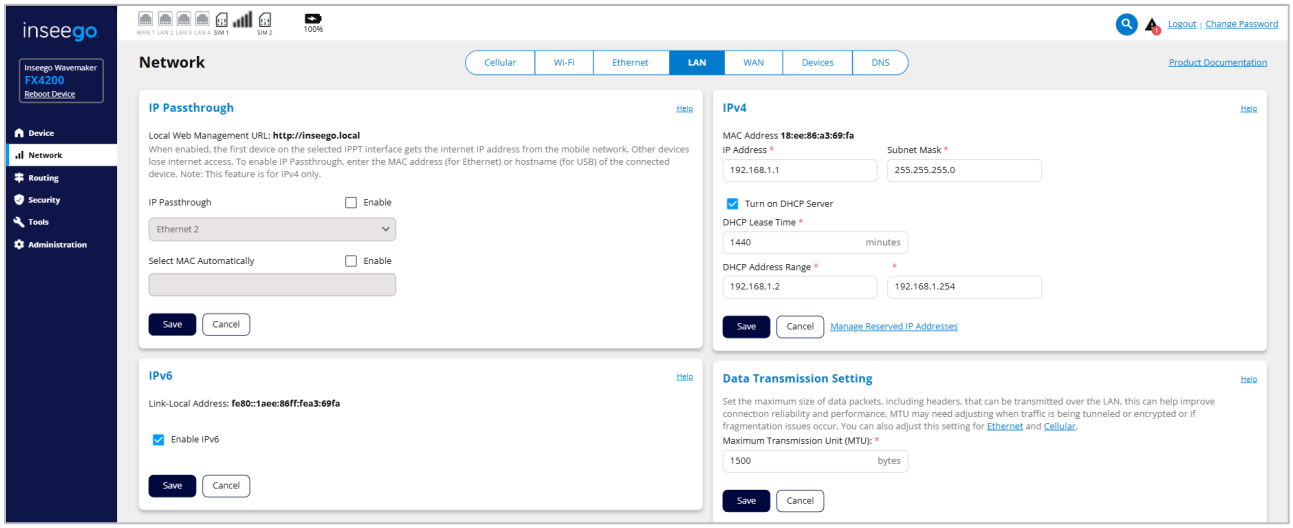
Use Connection: Use the dropdown to select WAN or LAN for the type of Ethernet connection you want on each of the WAN/LAN ports.
NOTE: When IP Passthrough is turned on, you cannot configure Ethernet ports as WAN. Go to **Network > LAN** to turn IP Passthrough off.

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 FX4200 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.

Click **Save**.

LAN tab

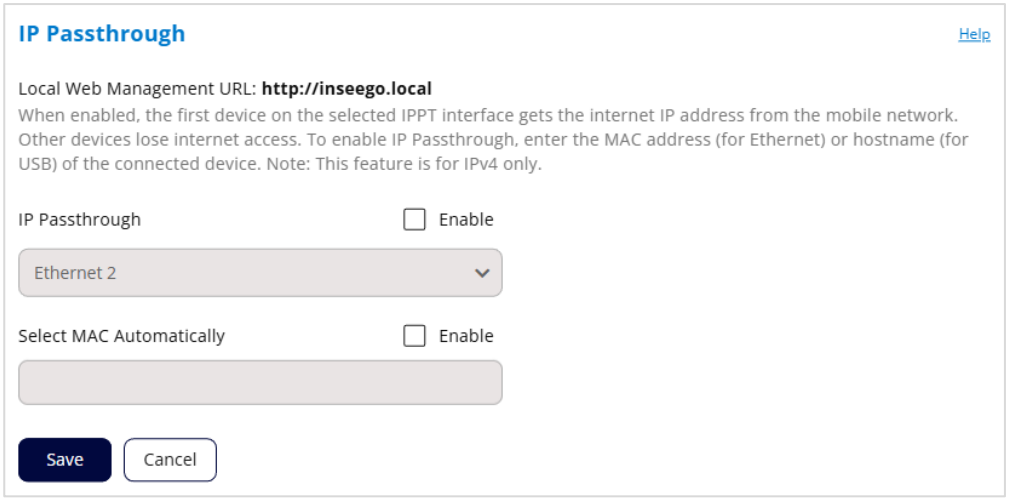
This tab provides settings and information about the FX4200 local area network (LAN). The LAN consists of the device and all connected devices.



IP Passthrough

IP Passthrough (IPPT) enables the first device detected on the specified 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



Local Web Management URL: The URL name used to access the FX4200 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.

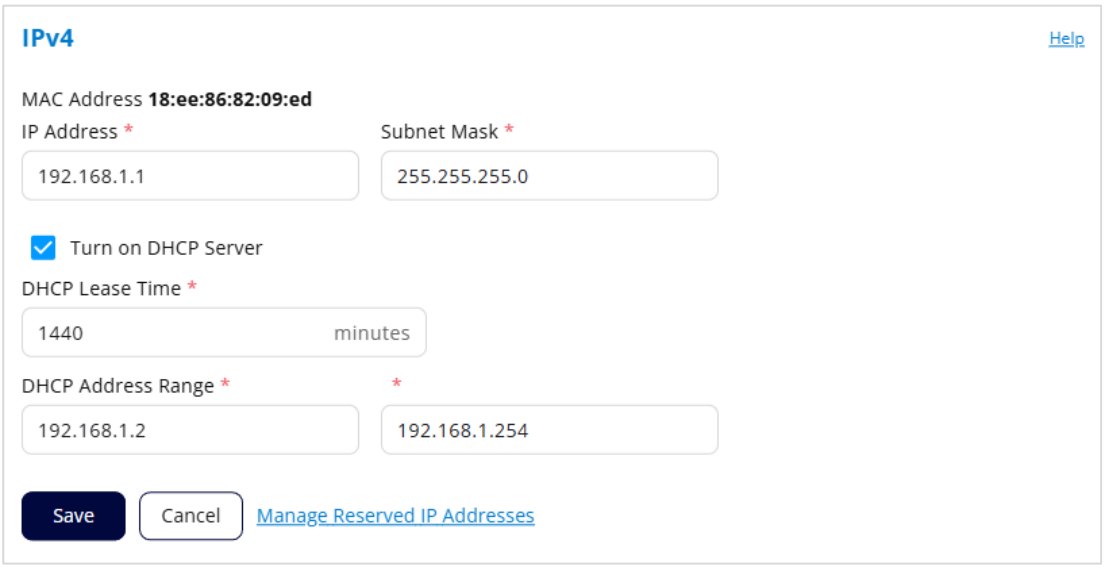
Select MAC Automatically: (visible If you select an Ethernet interface for IPPT). You can either enter the MAC address of the device connected for IPPT or check the **Enable** box to find the MAC address automatically. This is the MAC address of the only device connected to the selected Ethernet port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



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.

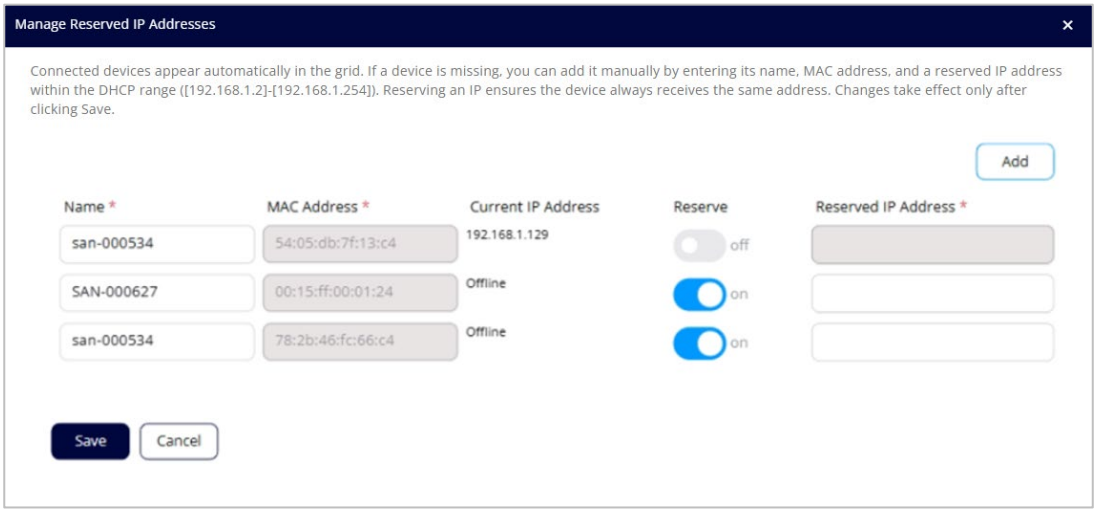
DHCP Address Range: The start and end of the IP address range used by the DHCP server. If the IP address is set on the client device, use an IP address outside of this DHCP range; if the IP address is set using an IP reservation, it will usually be inside this range. **NOTE:** Only expert users should 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.



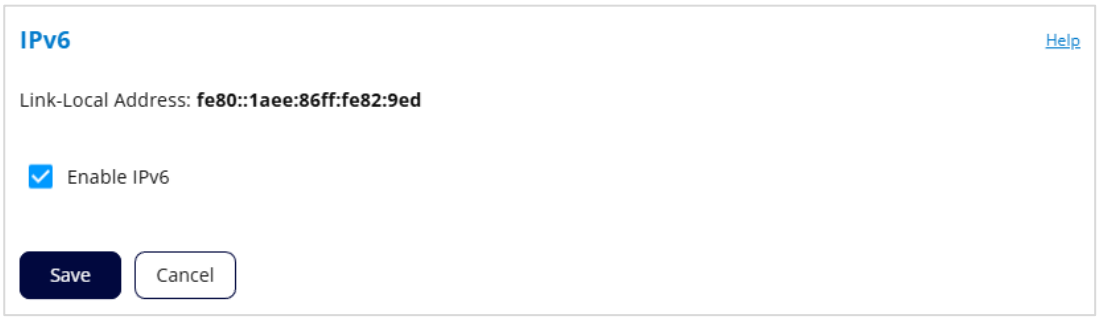
Connected devices display automatically. To manually add a device:

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.



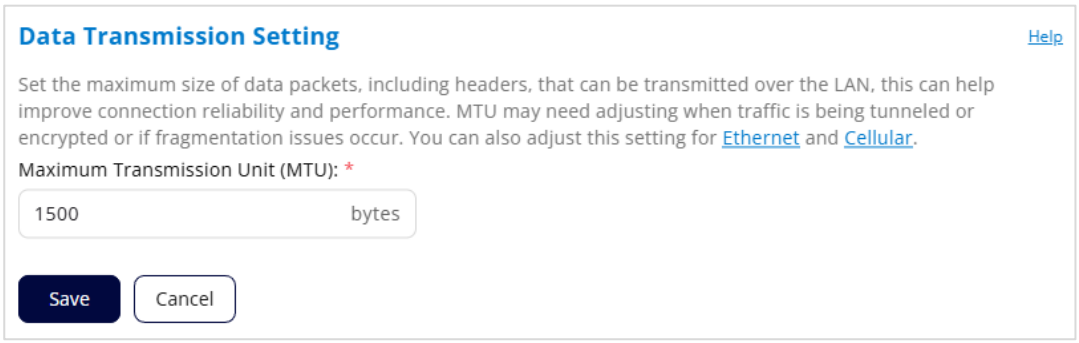
Link-Local Address: The Link-Local IPv6 address if the connected device supports IPv6 (read-only).

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.



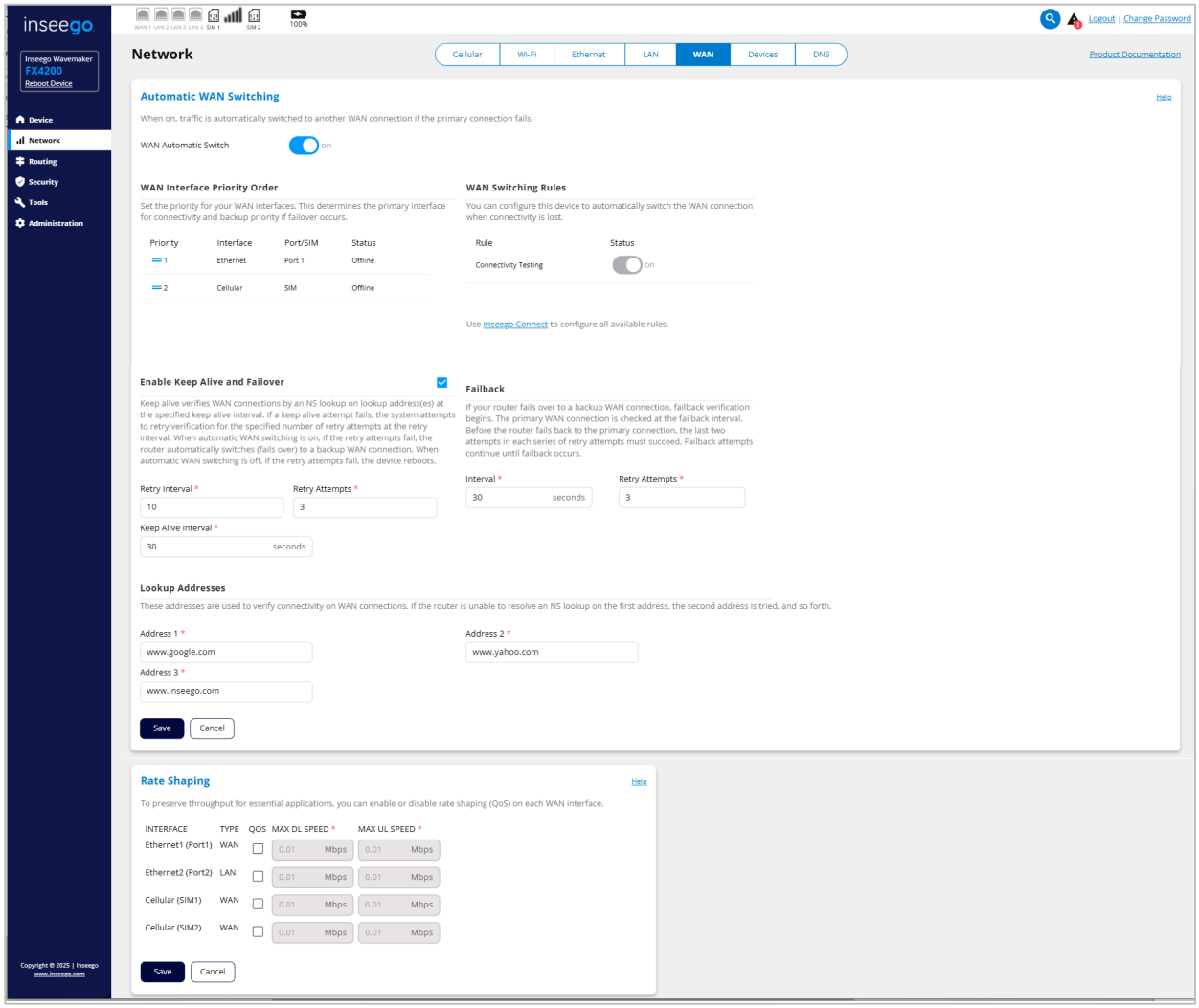
Maximum Transition Unit (MTU): The default (1500 bytes) is the recommended MTU for your FX4200 LAN network. You can enter a different value between 1280 and 1500 bytes

Click **Save**.

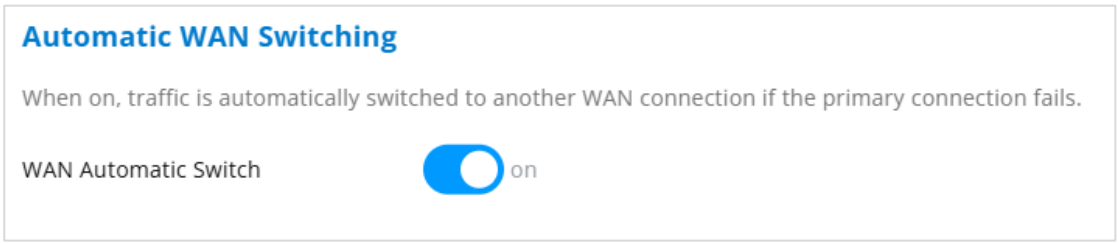
[*] Connected devices using IPv6 are not compatible with Fortinet VPN. Disable IPv6 on the connected device to use Fortinet.

WAN tab

Use this tab to enable WAN automatic switching, set WAN priorities, configure health checks (keep alive, failover, failback, and lookup addresses), and enable rate shaping on WAN interfaces.



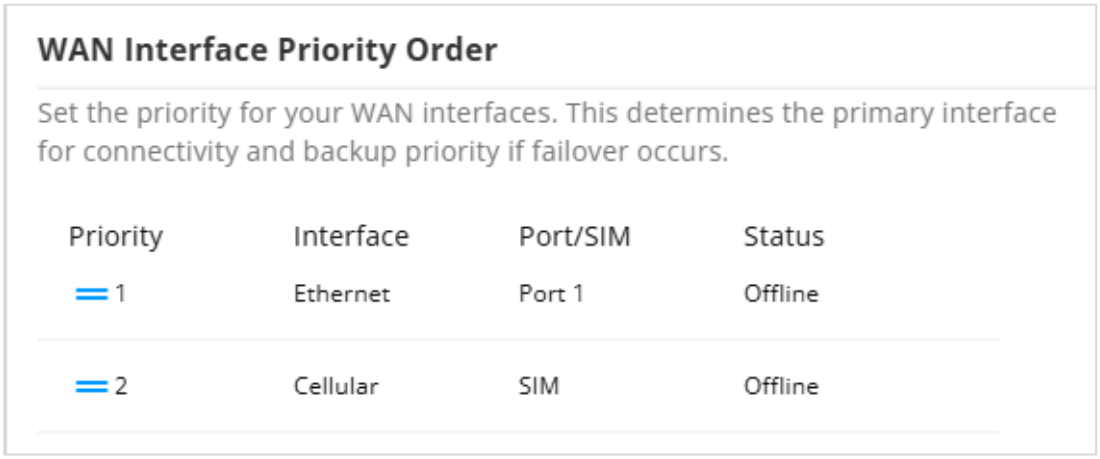
Automatic WAN Switching



WAN Automatic Switch: Automatic WAN switching is **on** by default. This allows rerouting of network traffic to your backup connection if the 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, if connectivity is lost on the priority 1 connection, the connection switches (fails over) to the priority 2 interface, and switches back (fails back) to the priority 1 connection when connectivity is restored.



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

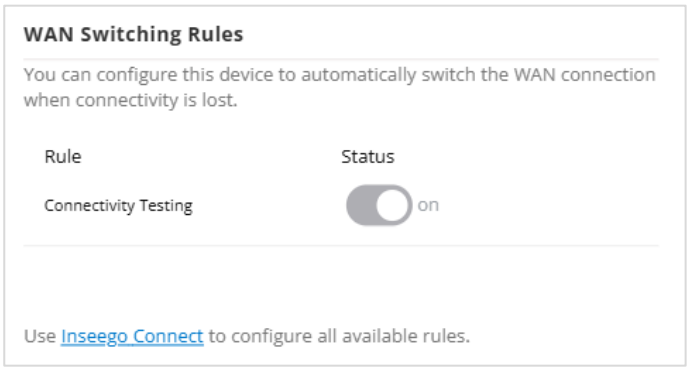
Interface: The type of interface (Cellular or Ethernet).

Port/SIM: For Ethernet interfaces, this is Port 1 or Port 2, whichever WAN/LAN port you have set for WAN on the Ethernet tab.

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

WAN Switching Rules

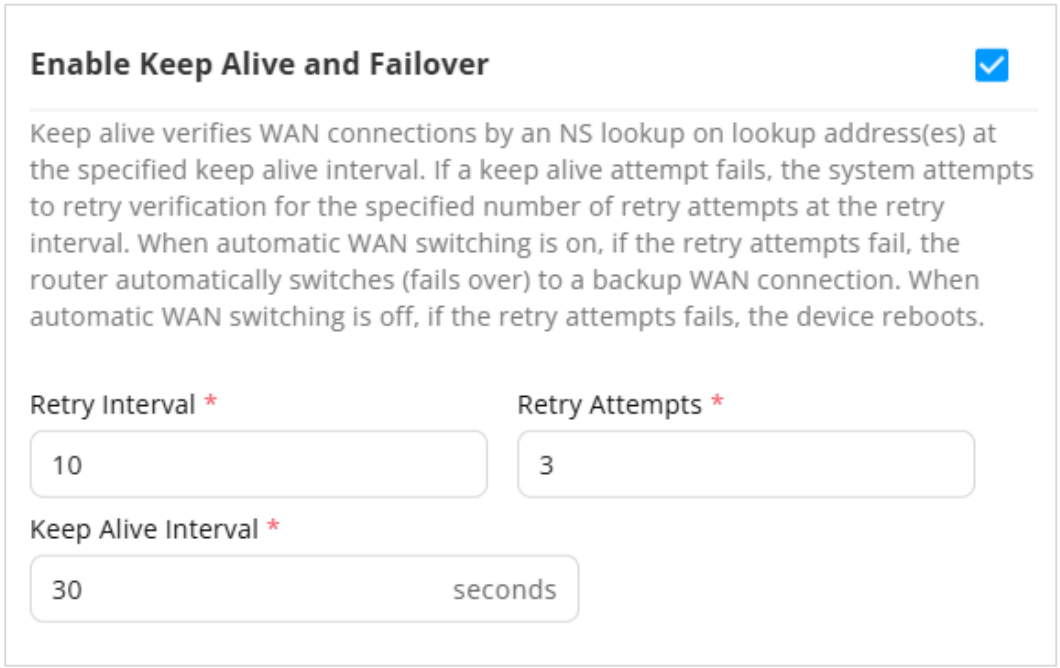
Connectivity testing is on by default and cannot be adjusted. To turn connectivity testing off, disable keep alive below.



Enable Keep Alive and Failover

Keep alive verifies your WAN connections by performing an NS lookup on lookup address(es) at the keep alive interval. If a keep alive attempt fails (the router is unable to resolve an NS lookup on any of the three lookup addresses), the system retries the connection at the retry interval for the set number of retry attempts.

When automatic WAN switching is **on**, if the retry attempts fail, the connection fails over to your backup WAN connection. When automatic WAN switching is **off** and the retry attempts fail, the router reboots.



Enable: Keep alive/failover health checks are **on** by default.

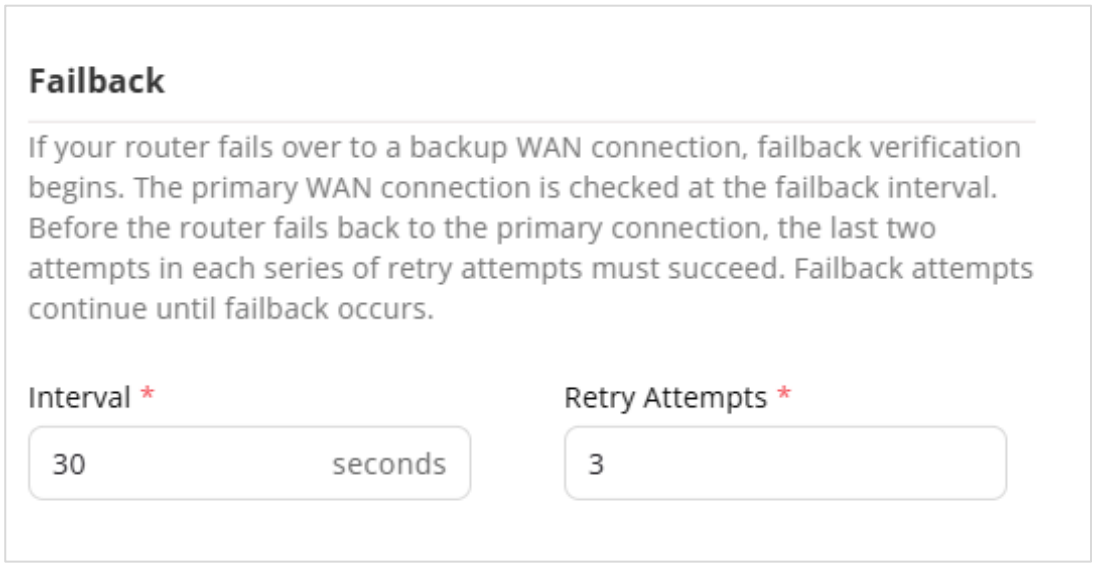
Retry Interval: The number of seconds between retry attempts to verify your WAN connection. Retry attempts occur after the router is unable to resolve an NS lookup on any of the three lookup addresses during a regular keep alive attempt.

Retry Attempts: The number of times to retry verification of your WAN connection after a regular keep alive attempt has failed. If all of the retry attempts fail, the WAN either switches over to the backup WAN (when automatic WAN switching is enabled), or the router reboots (when automatic WAN switching is not enabled).

Keep Alive Interval: The number of seconds between regular keep alive checks on your WAN connection. Keep alive verifies your WAN connections by performing an NS lookup on lookup addresses at this interval.

Failback

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

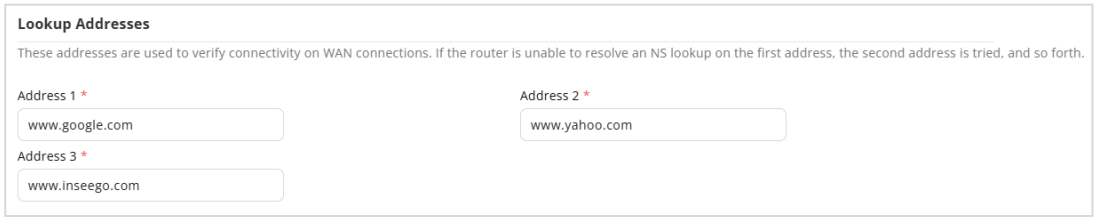
NOTES:

- For failback to the primary WAN connection to occur, the ***last two*** attempts in this number of attempts must succeed. For example, if set to 5 and attempts 1-4 succeed, but attempt 5 fails, failback does not occur.

- Failback attempts continue until failback occurs. This setting determines how many attempts to try in a series of attempts, the last two of which must succeed for failback to occur.

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.



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

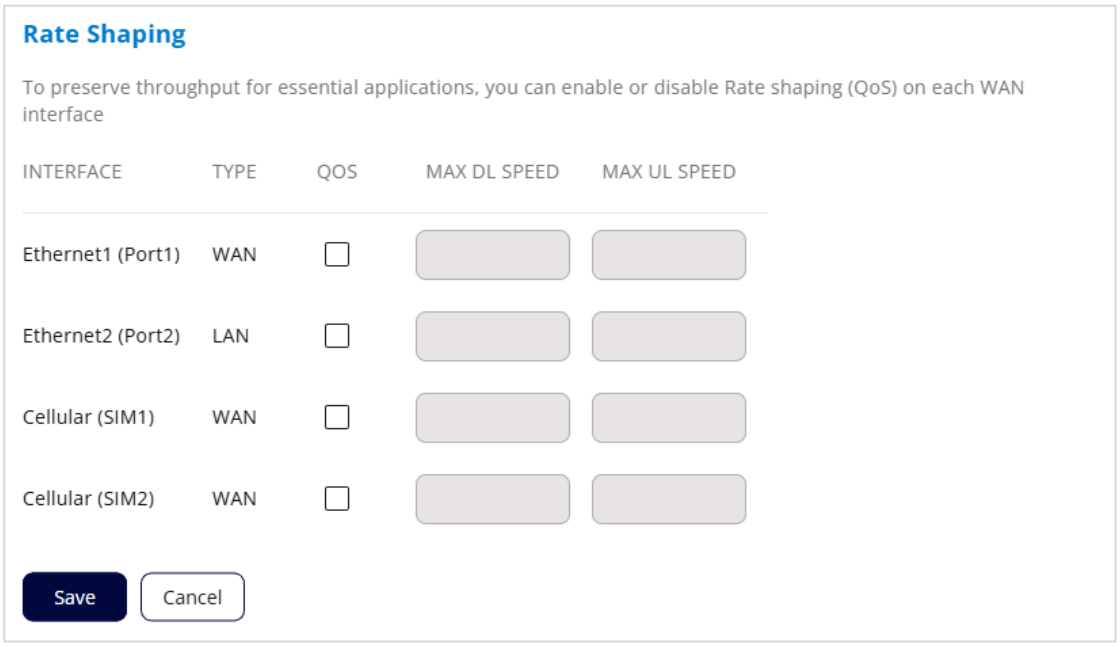
Address 2: The second IP address to verify if Address 1 does not respond.

Lookup Address 3: Enter the third IP address to verify if Address 2 does not respond.

Click **Save** to save your configurations.

Rate Shaping

Use this section to configure rate shaping on your interfaces.



Interface: The WAN interface - Ethernet1 (Port1), Ethernet2 (Port2), Cellular (SIM1), Cellular (SIM2).

Type: The type of connection currently set for the interface (WAN or LAN).
NOTE: Rate shaping only works on WAN connections. However, you can configure both WAN/LAN Ethernet ports so that rate shaping will apply if you change your Ethernet WAN interface.

QOS: (Quality of Service) Check this box to enable QOS rate shaping on the interface.

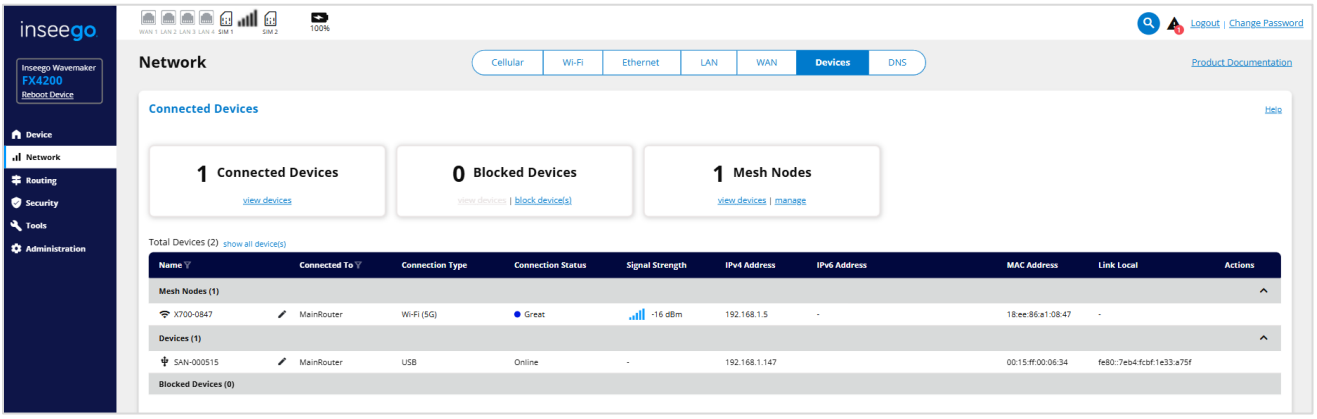
Max DL Speed: Enter the maximum download speed you want allowed on the interface.

Max UL Speed: Enter the maximum upload speed you want allowed on the interface.

Click **Save**.

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. To change the name of the router as it appears to connecting client devices, use the **Administration > Preferences** tab)

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.

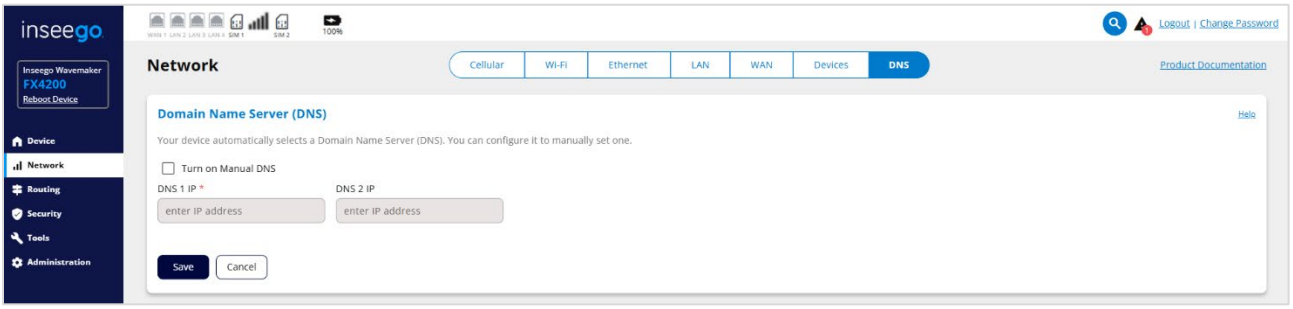
DNS

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

- DNS tab (admin web UI and Inseego Connect)
- DNS Content Filtering (Inseego Connect)

DNS tab (admin web UI and Inseego Connect

The FX4200 automatically selects a Domain Name Server (DNS). This page allows you to manually assign up to two DNS IP addresses.



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.

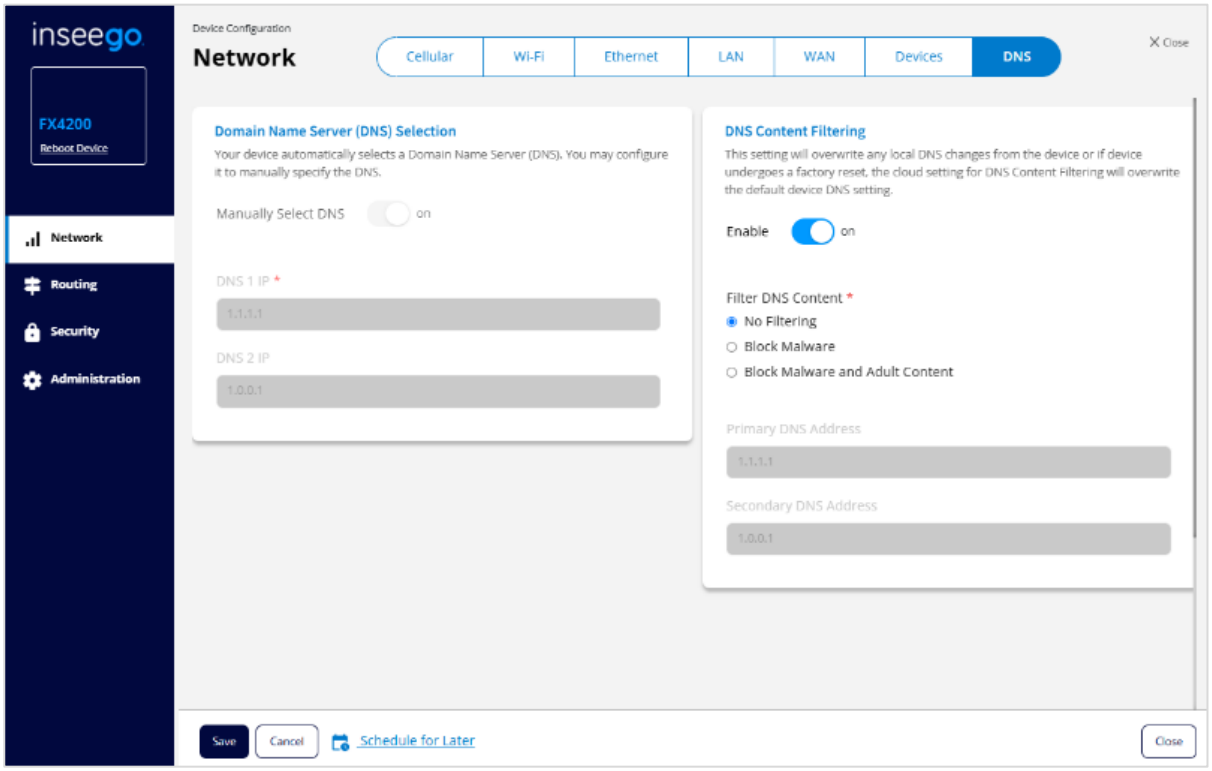
Click **Save**.

DNS Content Filtering (Inseego Connect)

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

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

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



DNS Content Filtering

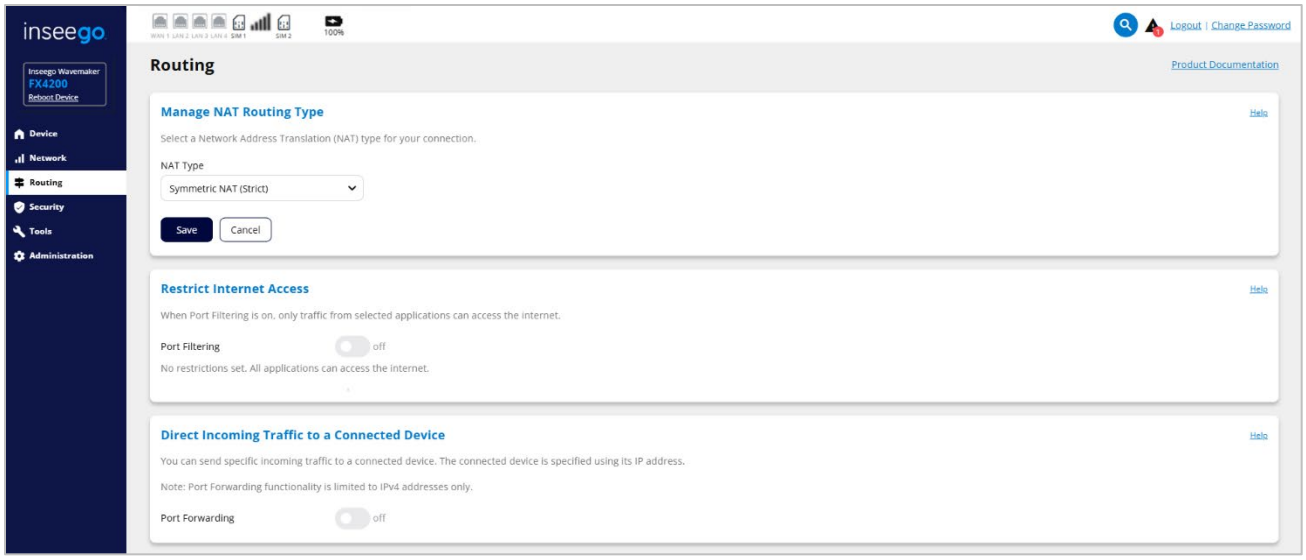
Enable: Check this box to enable DNS content filtering.

Select the filter level (No Filtering, Block Malware, or Block Malware and Adult Content).

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**.

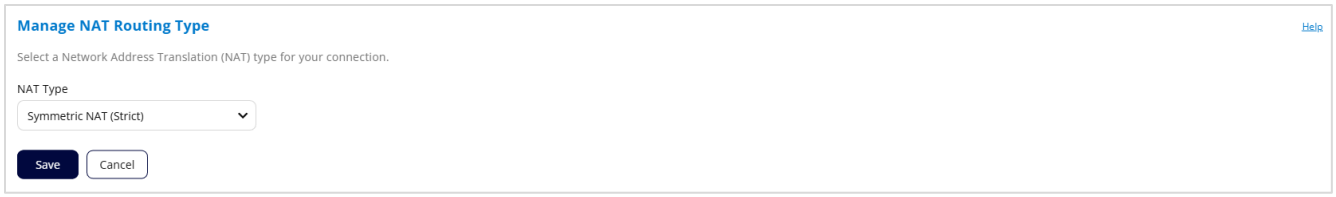
Managing routing

Use this page to set routing options.



Manage NAT Routing Type

Your FX4200 uses Symmetric Network Address Translation (NAT) routing by default. Use this section to select the type of NAT for your connection.



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

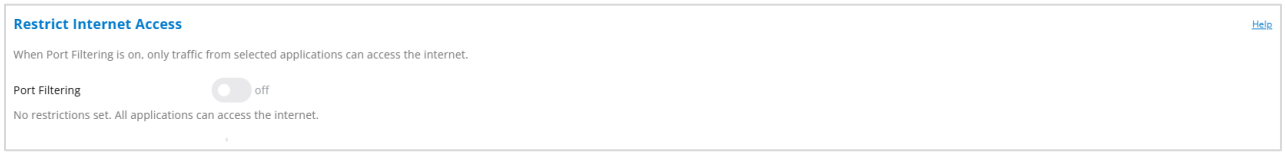
- **Symmetric NAT** (default) is more restrictive. It maps requests with the same source IP address and port number to a unique external IP and port, based on the destination IP and port of the outgoing connection.
- **PRC NAT** (port restricted cone) maps all requests from the same source IP address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

Click **Save**.

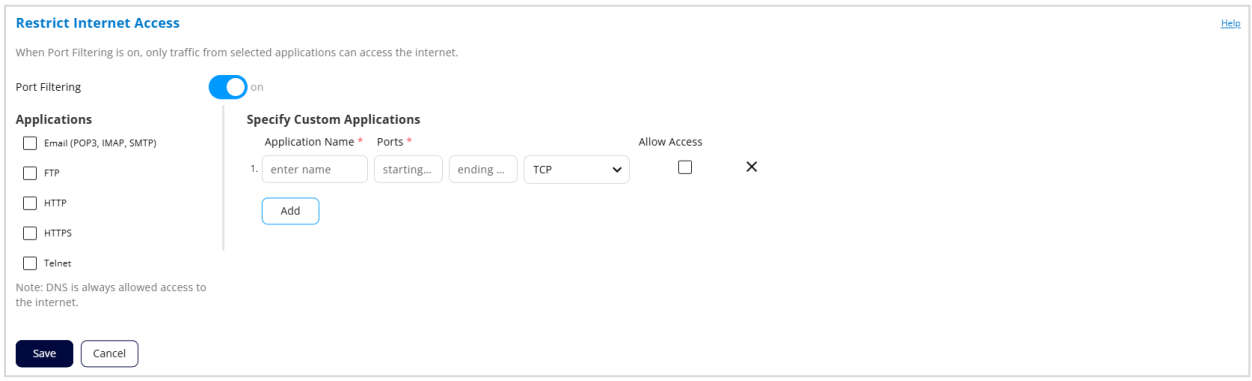
Restrict Internet Access For Applications

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, and you cannot enable port filtering. Go to **Network > LAN** to turn IP Passthrough off.



Port Filtering: To enable port filtering and select which applications can access the internet, move the slider to **on**.



Applications

Only traffic from applications you select can access the internet. Some applications are pre-defined. Select the applications you want to be able to access the internet.

The following table provides port numbers and protocol information for each pre-defined application listed.

Application Name	Port	TCP *	STCP*	UDP*
Email				
POP3 POP3S	110 995	Yes Yes	No No	Assigned Yes
IMAP IMAPS	143 993	Yes Yes	No No	Assigned Assigned
SMTP	25	Yes	No	Assigned

* **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.

Application Name	Port	TCP *	STCP*	UDP*
SecureSMTP	465	Yes	No	No
FTP control (command) FTP data transfer	21 20	Yes Yes	Yes Yes	Assigned 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.

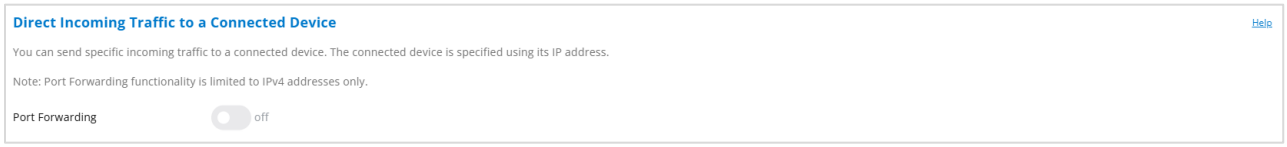
Direct Incoming Traffic to a Connected Device

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.

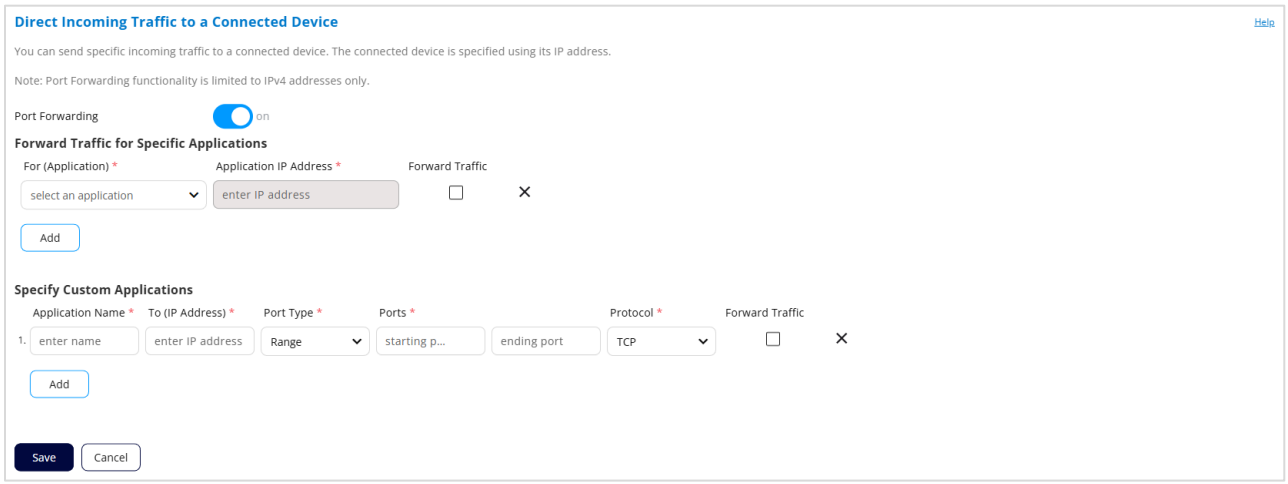
IMPORTANT: Port forwarding creates a security risk and should not be turned on unless it is required.

NOTES:

- 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.
- 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 direct incoming traffic to a connected device, enable port forwarding.



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.

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

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

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) FTP data transfer	21 20	Yes Yes	Yes Yes	Assigned Assigned
HTTP HTTPS	80 443	Yes Yes	Yes Yes	Assigned Assigned
NNTP	119	Yes	No	Assigned
POP3 POP3S	110 995	Yes Yes	No No	Assigned Yes
SMTP SecureSMTP	25 465	Yes Yes	No No	Assigned No
SNMP	161	Assigned	No	Yes
Telnet	23	Yes	No	Assigned
TFTP	69	Assigned	No	Yes

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

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.

Ports:

For Range 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.

For Translate ports -

- Use **external port** and **internal port** 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 **external port** and **internal port**.
- 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

Use Security tabs to view and configure settings for your router's security.

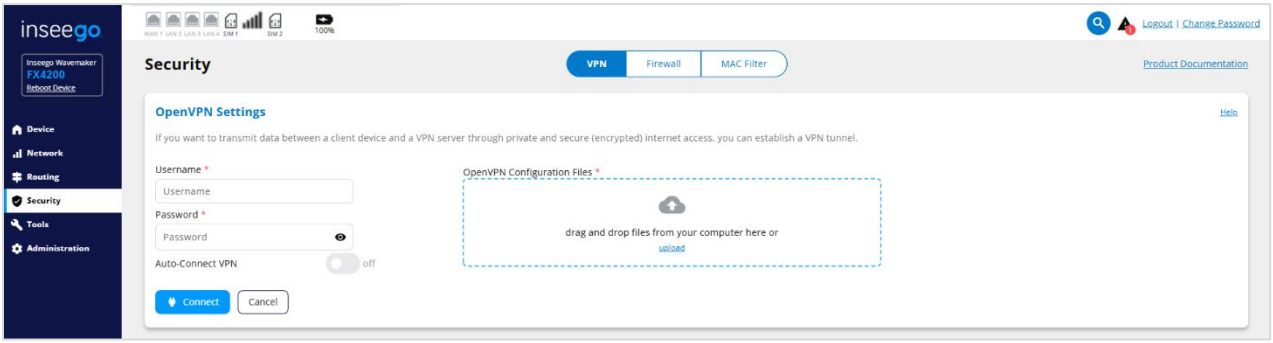
The Security page includes the following tabs:

- OpenVPN
- Firewall
- MAC Filter

VPN tab

Your FX4200 allows you to establish secure connections to remote networks over a public network using OpenVPN.

NOTE: You can configure IPSec VPN with Inseego Connect.



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.

To configure a VPN connection:

1. Drag and drop the OpenVPN configuration files from your OpenVPN provider in the file upload area or click **upload** to browse for the files.
2. Enter your OpenVPN connection **username**.
3. Enter your OpenVPN connection **password**.
4. If you want the VPN tunnel to automatically be established whenever an internet connection is made, move the Auto-Connect VPN slider to on.
5. 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.

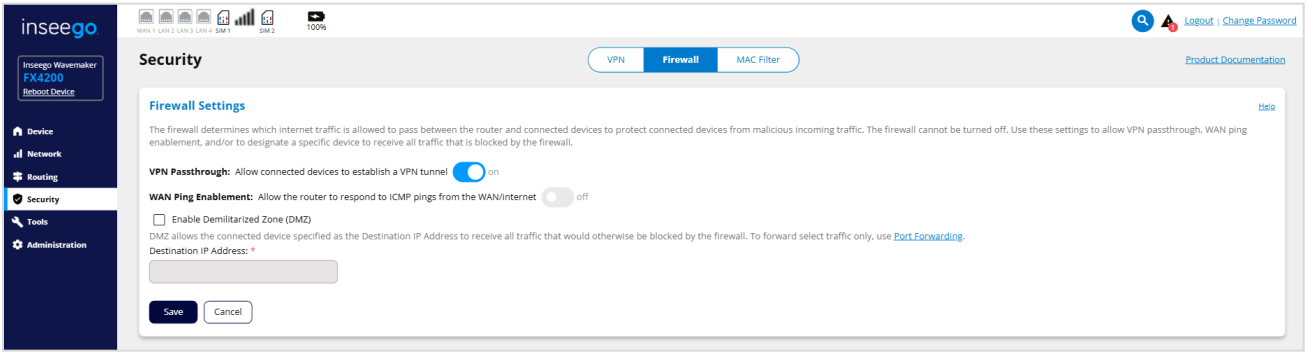
Connection time: The duration of the current OpenVPN connection.

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

Connect: Use this button to connect the OpenVPN.

Firewall tab

The FX4200 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, enable WAN ping requests, 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

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

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.
- Allowing DMZ may assist some troublesome network applications to function properly, but the DMZ device should have its own firewall to protect itself against malicious traffic.
- **Enable Demilitarized Zone (DMZ):** Check the checkbox to enable 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.

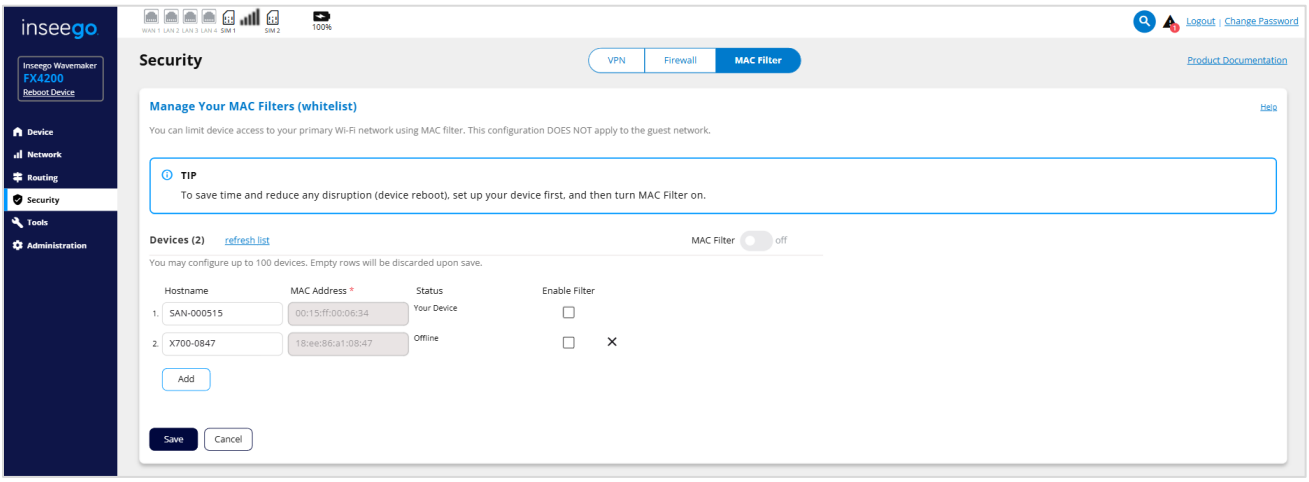
Destination IP Address: Enter the IP address of the connected device you wish to become the DMZ device (the DMZ destination). **NOTE:** You can see the IP address of each connected device on the Network > Devices tab.

Click **Save**.

MAC Filter tab

The MAC filter only allows selected devices to access the FX4200 network through DHCP. By default, MAC filter is turned off.

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



The devices list includes all client 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

Use the Tools tabs to view or run speed tests and view logs.

The Tools page includes the following tabs:

- Speed Test
- Logs

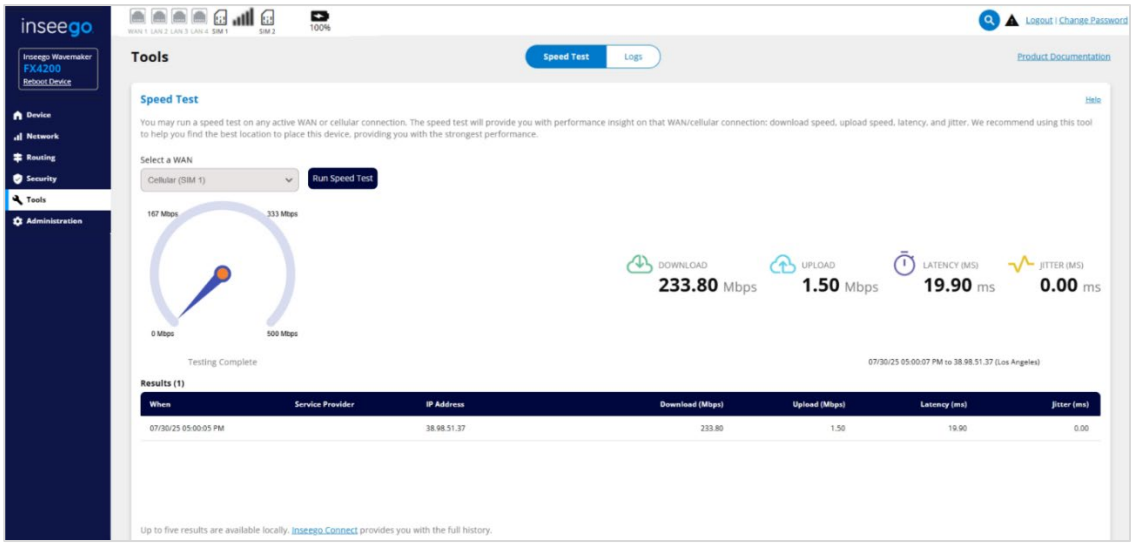
NOTE: In addition to the web UI tools, Inseego Connect allows you to launch a terminal window and securely run basic network diagnostic tools on your FX4200 remotely without exposing the full device Command Line Interface (CLI) or compromising system security. Allowed commands include: ping, traceroute, nslookup, and tcpdump.

Speed Test tab

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

NOTES:

- You can run up to 20 speed tests on a device within a 30-minute period, and up to 40 speed tests on a device within a 12-hour period. These numbers reflect the combined number of speed tests initiated from the web UI and Inseego Connect on a single device.
- You can also run speed tests with Inseego Connect and view a graphical display of results over time.
- If you're concerned about your speed, contact your service provider to confirm the typical speeds for your account type and location.



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

Run Speed Test: Click the button to start the speed test. When the test is complete, the results of the current speed test are displayed on the right and added to the table below.

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.

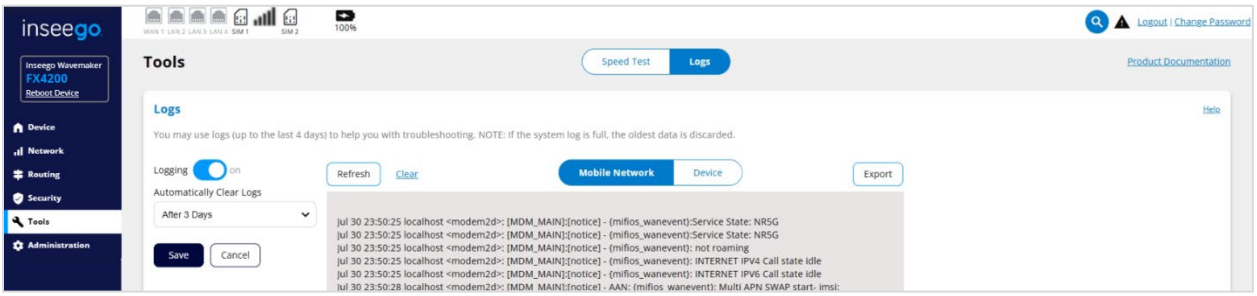
Jitter (ms): The amount that latency fluctuates over time, measured in milliseconds.

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.



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:

Mobile Network: Displays log data of connections to the mobile network.

Device: Displays log data of events that occurred on this device other than mobile data connections.

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 administration options

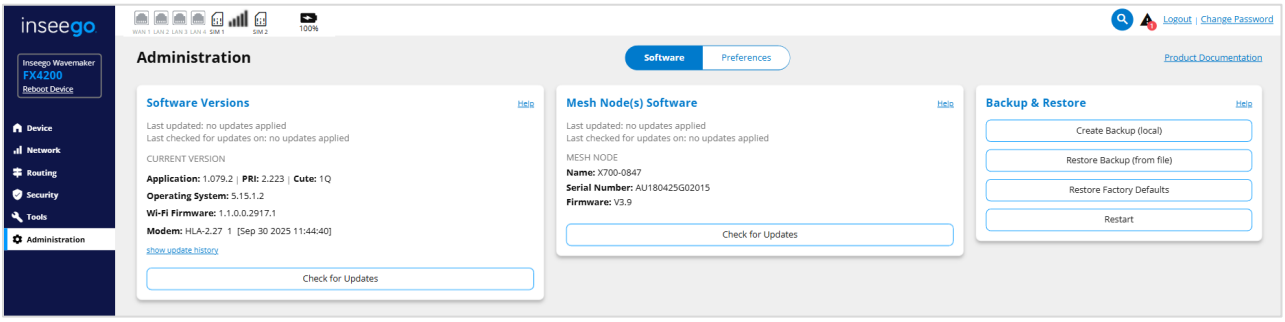
Use the Administration tabs to manage your router's software and device preferences.

The Administration page includes the following tabs:

- Software
- Preferences

Software tab

Use this tab to check or update software for your router or mesh nodes in your network, and to backup and/or restore settings.

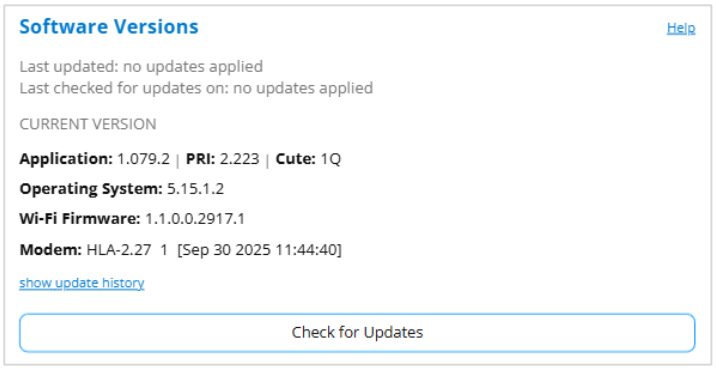


Software Versions

Software updates are delivered to your FX4200 automatically over the mobile network. This section displays current software version information, software update history, and allows you to check for new software updates for your router.

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).

NOTE: When running on a battery, if the batter has 30% or less charge, automatic firmware updates are disabled.



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 Version

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 the history of previous software updates.

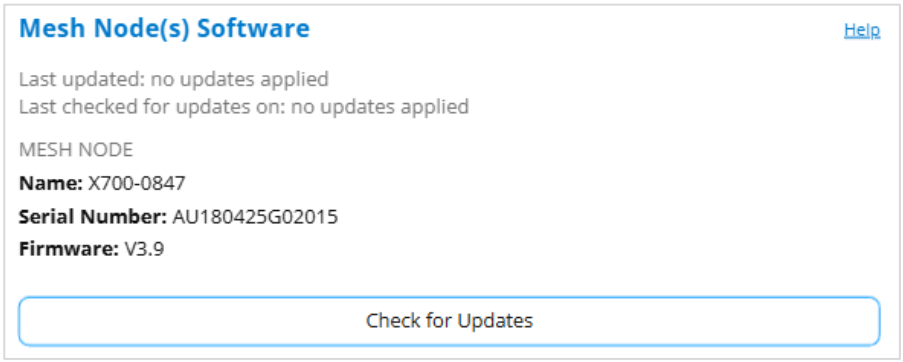
Check for Updates: Click this button to manually check for available software updates. If a new software update is available, it is automatically downloaded. You are prompted to install with a message that your router will be unavailable for about 18 minutes during the update.

Mesh Node(s) Software

Software updates are delivered to your X700 Mesh Wi-Fi nodes automatically over the mobile network. This section displays current software version information and allows you to check for new software updates for the mesh nodes in your network.

NOTE: This section is not visible unless **Enable Mesh Network** on **Network > Wi-Fi** is on.

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).



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 of the mesh node.

Firmware: The version of firmware currently installed.

Check for Updates: 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.

Notes on software updates

Software updates are delivered to your FX4200 automatically over the mobile network. You can also initiate updates through the web UI or Inseego Connect. This section provides details on the different types of updates.

Automatic updates (device initiated)

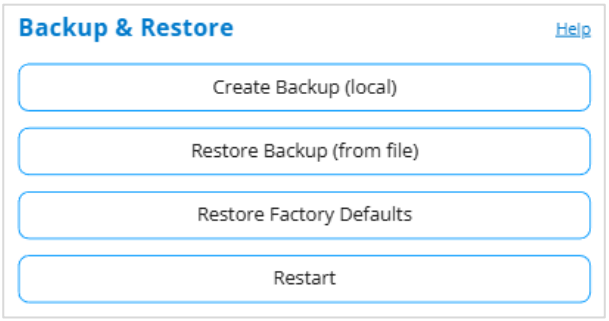
- The device looks for updates once every 24 hours.
- If an update is available, it is downloaded to the device.
- The update is installed on the device within 48 hours of being downloaded, between 2 - 4 AM local time, or immediately upon reboot.

User-initiated updates

- **From admin web UI**
  - Check for updates from the **Administration > Software** tab.
  - If an update is available, it is downloaded to the device.
  - Choose to install the update immediately, or it will be installed within 48 hours of being downloaded, between 2 - 4 AM local time (or immediately upon reboot).
- **From Inseego Connect**
  - Update a single device, multiple devices or groups of devices using the **Update Firmware** button.
  - If an update is available, choose whether to install it immediately or use **Schedule Later** to select a time.
  - Track updates on the **Operations** page.

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 backup file

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 from a backup file

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.

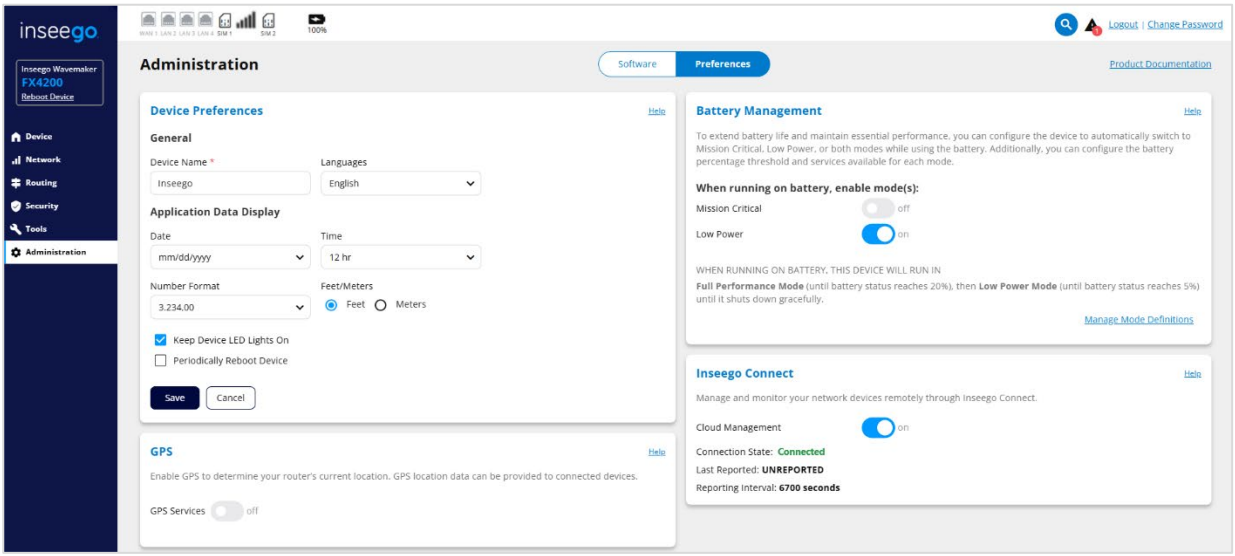
To reset all settings to their factory default values, click the **Restore Factory Defaults** button, then confirm by clicking **Yes, Restore Factory Defaults**.

Restarting your router

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

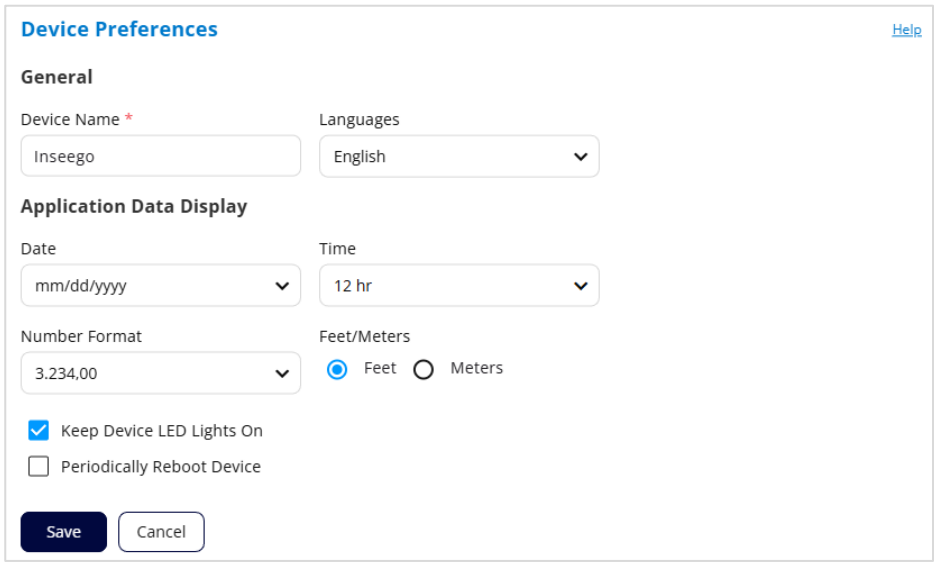
Preferences tab

Use this tab to set device preferences such as language, enable/disable Inseego Connect, to enable GPS to view current device location information, to configure battery modes, and to enable/disable connection with Inseego Connect.



Device Preferences

Use this section to change preferences for your router. You can change the name of the router that is visible to connecting devices and change the language displayed. You can change how dates, time, distance, and numbers are displayed in the web UI. You can also turn off the LED lights on the router and enable a periodic reboot feature.



General

Device Name: The name of the FX4200 that appears when connecting with client devices. If desired, enter a different name.

Languages: Select a language for the admin web UI.

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).

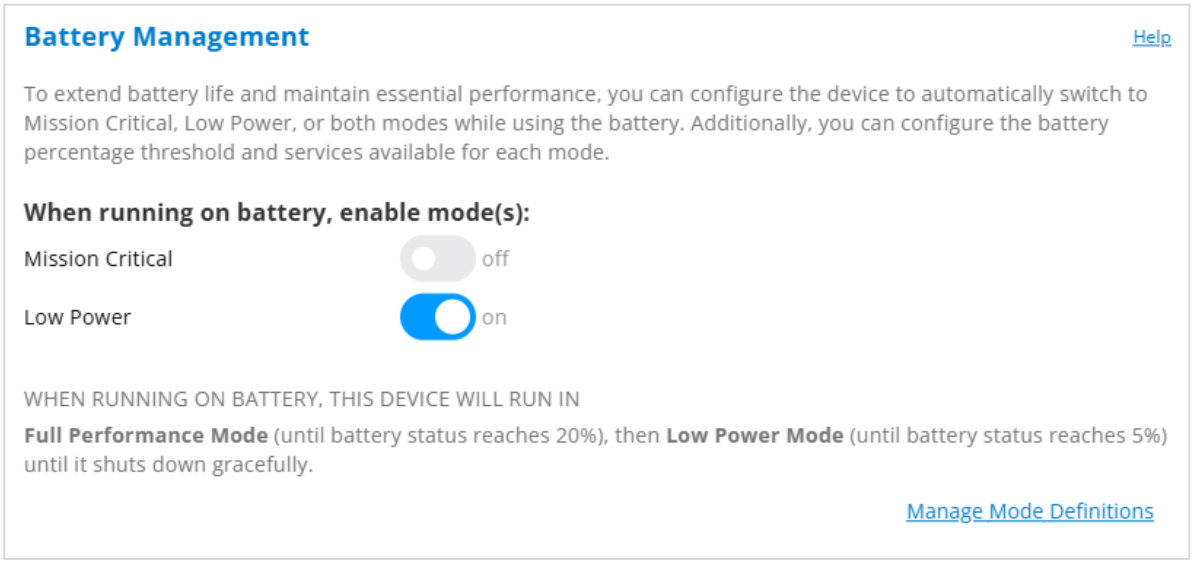
Keep Device LED Light On: When checked the LED lights on the front left of your router remain on. To turn these lights off, uncheck the box.
NOTE: This does not affect the device display on the front right of the router, which you can turn off with the Display button, and which times out after 60 seconds.

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.

Click **Save**.

Battery Management

The FX4200 has a rechargeable 5050 mAh LI-ion backup battery that is accessible from a compartment on the bottom of the router. Use this section to configure battery thresholds and modes to extend battery life and maintain essential performance when using the battery.

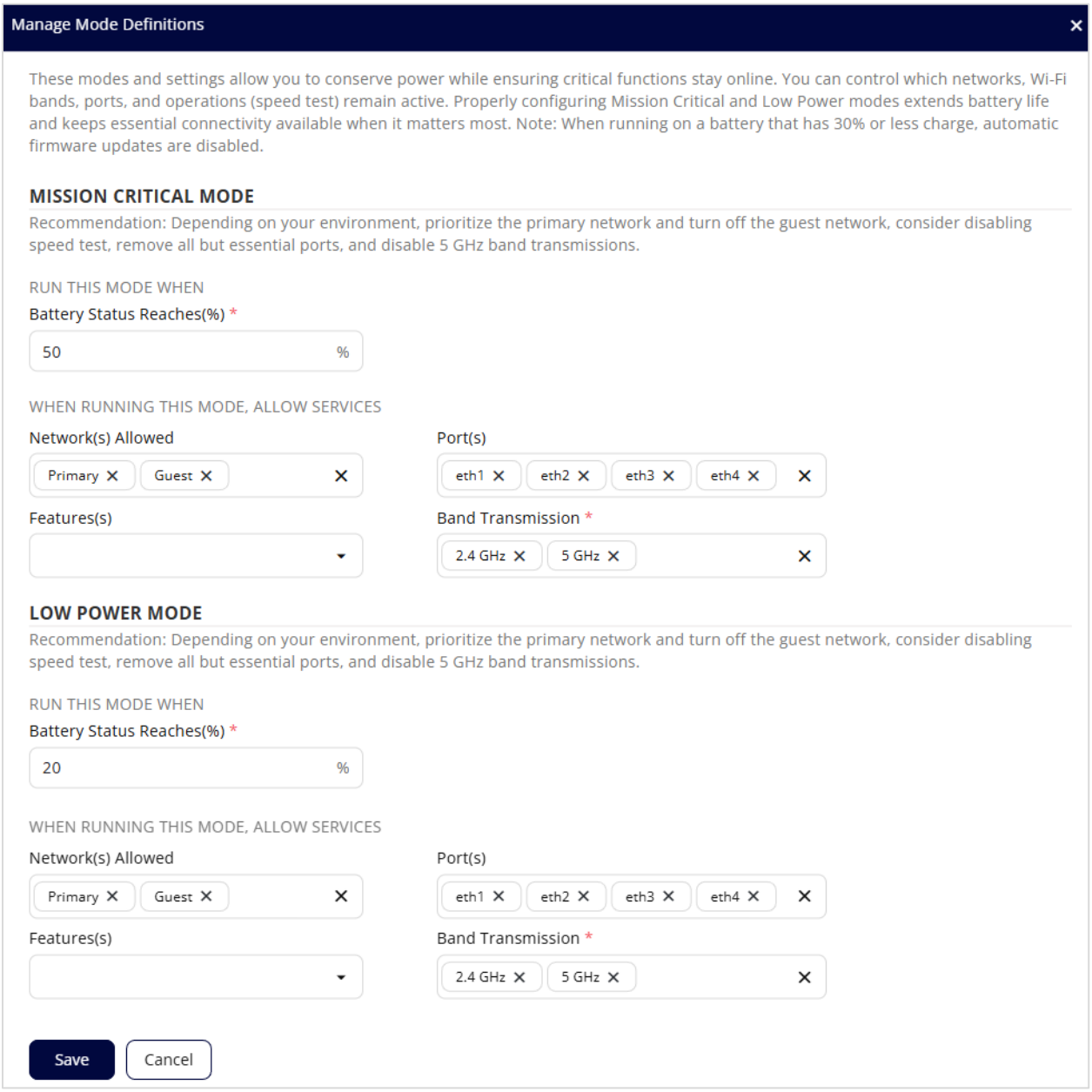


When running on battery, enable mode(s):

Mission Critical: This mode is **off** by default. When **on**, it provides an intermediary mode between Full Performance and Low Power modes.

Low Power: This mode is **on** by default.

Click **Manage Mode Definitions** to select which services you want to remain active and set thresholds for battery modes.



Configure battery modes to help preserve battery life when running your router on battery. Depending on your environment, consider turning off your guest and/or mesh network, restricting ports to only those that are essential, disabling the 5GHz band, and disabling speed tests.

NOTES:

- When running on a battery that has 30% or less charge, automatic firmware updates are disabled.
- When running on a battery that has only 5% charge, the router begins graceful shutdown.

MISSION CRITICAL MODE

When enabled, Mission Critical mode can serve as an intermediary mode between Full Performance and Low Power mode. When in this mode, your battery status is yellow on the **Device > Status** tab.

LOW POWER MODE

Lower Power mode is enabled by default. Adjust settings to best fit your environment to conserve battery life when your battery is running low. When in this mode, your battery status is red on the **Device > Status** tab.

Configure each mode you want enabled:

RUN THIS MODE WHEN

Battery Status Reaches(%): Enter the battery percentage at which you want the router to enter this mode (required).

WHEN RUNNING THIS MODE, ALLOW SERVICES

Network(s) Allowed: Select or deselect networks (Primary, Guest, or Mesh). The networks displayed remain running when the battery is in this mode.

Port(s): Select or deselect Ethernet ports. The ports displayed remain running when the battery is in this mode.

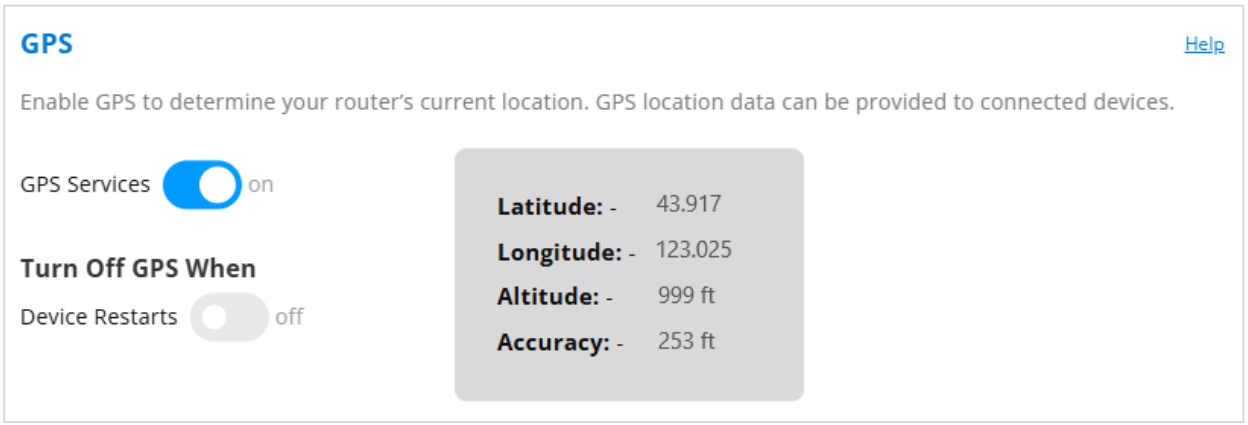
Features(s): Select or deselect features (speed test). The features displayed remain active when the battery is in this mode.

Band Transmission: Select or deselect band transmissions (2.4 GHz, 5 GHz). The bands displayed remain active when the battery is in this mode.

Click **Save**.

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 turned **on**, a GPS Agreement appears, click **Yes, Enable GPS** to proceed. The FX4200 acquires GPS and makes GPS location data available.

Latitude: Latitude for the last location fix.

Longitude: Longitude for the last location fix.

Altitude: Altitude for the last location fix.

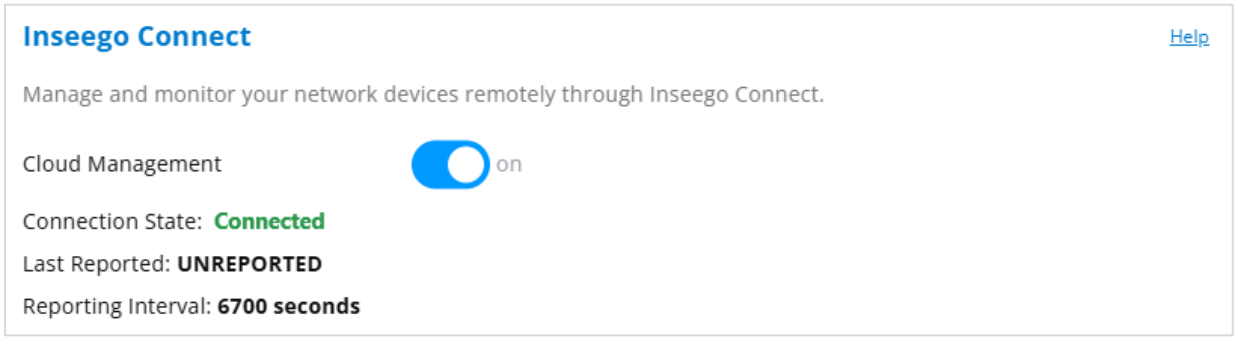
Accuracy: A measure of the accuracy of the horizontal position obtained by the GPS receiver.

Turn Off GPS When

Device Restarts: When GPS is **on**, the GPS receiver turns off when the router turns off and does not automatically restart when the router restarts - you will need to enable GPS again.

Inseego Connect

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



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.

3

Troubleshooting and support

Overview

When properly installed, the FX4200 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 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 **Network > Cellular** and change **Network Technology** to **4G LTE**.

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

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

My router is not booting up

- **Issue:** The FX4200 is not booting up (the device display does not show your service provider's name, even after pushing the button next to the display).

  Solution: Power cycle the router by unplugging and plugging it back in.

- **Issue:** The router is on, and the Wi-Fi status LED  is green or blue, but you can't see a Wi-Fi name (SSID) to connect to.

  Solution: Power cycle the router by unplugging and plugging it back in.

- **Issue:** The router is on, but the Wi-Fi LED  indicates no Wi-Fi

  Solution: Press the reset button on the back of the device until the device resets (approximately five seconds.) The device status LED on the far left blinks white, then turns red. When the LED is solid white, 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.

If you are still having issues, contact your service provider for assistance.

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.

The cellular status LED is blinking red

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

  Solutions:

  Try the following:

  - Unplug the router, then remove and reinsert the SIM card(s). Do not touch the metallic contacts. Make sure each card is inserted with the contacts facing down, notch facing in, and that it clicks into place. Restart your router.
  - Ask your service provider:
    - Are your SIM cards active and on a plan compatible with your 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 **Device > Overview** (home) screen, check if there are any values in the SIM section. If SIM cards are 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 **Device > Overview** (home) screen, 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(s) and rebooting the device with a SIM from a different service provider. The SIM does NOT need to be active. Reinsert the original SIM(s) 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 **Network > Cellular**, check for a locked SIM.

My older device cannot connect

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

- **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 **Network >Wi-Fi** . Disable **MLO**, and under **2.4 GHz Band Settings**, use the dropdown 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**. 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:

- **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 **WPA2 Personal PSK (AES)**:

  1. Access the admin web UI and navigate to **Network > Wi-Fi > Primary Network**. In the **Security** dropdown, select **WPA2 Personal PSK (AES)**.
  2. Click **Save** 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 **Network > Wi-Fi > Primary Network**, or **Network > 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** 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 **Network > Wi-Fi > Settings**. Disable MLO and in BAND SELECTION, uncheck **5 GHz** and use only **2.4 GHz**. **NOTE:** If you have a mesh network, both 5GHz and 2.4 GHz must be selected.
  2. Click **Save**. 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 27.
  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, 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 **Network > 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: **Network > 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.

My router is getting slow speeds/low throughput

- **Reason:** Signal strength is the most likely cause of slow speeds/low throughput. **NOTE:** The FX4200 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.

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 external antennas?

In most cases, external antennas are not needed with the FX4200. The integrated internal antennas provide an average 4 dBi peak gain across all frequency ranges. If you are getting 3-5 bars signal strength, external antennas are most likely not necessary to improve performance. In fact, adding the wrong external antennas (less than 4 dBi, including cable loss) could decrease your router's performance.

Situations where external antennas are needed are rare, and may include:

- Poor signal quality
- Challenging location (basement, thick building walls, scenarios where there is a strong 5G signal outside, but only 4G inside, etc.)
- The need to boost higher frequency bands

When using external antennas, consider the reliability of the manufacturer, correct connectors, bands/frequencies, and cable loss.

Contact your Account team for more information about external antennas.

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 a data USB port, which can 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.

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 or reseller for assistance.

More information
Documentation for your FX4200 cellular router is available online. Go to go.inseego.com/FX4200.

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

Product specifications

Regulatory information

Product certifications and supplier's declarations of conformity

Wireless communications

Limited warranty and liability

Safety hazards

Proper battery use and disposal

Product specifications

Device

Name:	5G Cellular Router FX4200
Model:	FX4210
Regulatory:	FCC (US), ISED (Can)
Certifications:	GCF, PTCRB, FIPS-3*, Wi-Fi Alliance, REACH, RoHS, UL 2710†
Battery:	Rechargeable 5050 mAh LI-ion backup battery
Dimensions:	8.3" x 5.5" x 2.1" (210 mm x 140 mm x 54 mm)
Weight:	51.9 oz (1.47 kg)
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/what-is-fips-140-3-and-how-does-it-secure-sensitive-data/

† 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

Operating system features

Seamless WAN failover and failback
WAN prioritization
Firewall
VPN passthrough
IP Passthrough
Network slicing
On-device speed test
IPv4 and IPv6 with XLAT support
WPA2/3 personal and enterprise
Secure local user interface
Data usage monitoring
FIPS 140-3 OpenSSL
Wired and wireless Wi-Fi mesh support

* Data plan required. Coverage subject to network availability.

Software solutions

Inseego Connect remote management
Inseego Mobile app
Inseego Connect API support
Firmware management and scheduling
Automatic carrier selection
Remote troubleshooting and diagnostics
Zero-touch deployment
Network slicing
On-device speed test
Notifications and alerts
GPS with map location
IPsec VPN and OpenVPN
VPN passthrough
Data usage monitoring
Inseego Mobile™ app

Accessories (sold separately)

External antennas
Inseego Wavemaker Mesh Wi-Fi X700

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.

Innovation, Science and Economic Development Notice (ISED – Canada)

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 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.

Proper battery use and disposal

IMPORTANT: In the event of a battery leak:

- Do not allow the liquid to come in contact with the skin or the eyes. If contact has been made,
  wash the affected area with large amounts of water and seek medical advice.

- Seek medical advice immediately if a battery has been swallowed.

- Communicate the appropriate steps to be taken if a hazard occurs. Due to the transmission
  and reception properties of wireless communications, data occasionally can be lost or delayed.

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

- Do not disassemble or open, crush, bend or deform, puncture, or shred.
- Do not modify or remanufacture, attempt to insert a foreign object into the battery, immerse or expose to water or other liquids, or expose to fire, explosion, or other hazard.
- Only use the battery for the system for which it was specified.
- Only use the battery with a charging system that has been qualified with the system per IEEE 1725. Use of an unqualified battery or charger may present a risk of fire, explosion, leakage, or other hazard.
- Do not short circuit a battery or allow a metallic or conductive object to contact the battery terminals.
- Replace the battery only with another battery that has been qualified with the system per IEEE 1725. Use of an unqualified battery may present a risk of fire, explosion, leakage, or other hazard.
- Promptly dispose of used batteries in accordance with local regulations.
- Battery usage by children should be supervised.
- Avoid dropping the MiFi or battery. If the MiFi or the battery is dropped, especially on a hard surface, and the user suspects damage, take it to a service center for inspection.
- Improper battery use may result in a fire, explosion, or other hazard.