USER GUIDE

inseego

Inseego Wavemaker™

5G cellular router FX4100

INSEEGO COPYRIGHT STATEMENT

© 2025 Inseego Corp. All rights reserved. Complying with all copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose without the expressed written permission of Inseego Corp.

SOFTWARE LICENSE

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 Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp.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

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

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

TRADEMARKS AND SERVICE MARKS

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

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

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

Document Number PRT-14965443 Rev 2

Contents

1

Introduction and getting started

Overview

The FX4100 cellular router provides reliable, high-speed connectivity wherever you need it, making it the ultimate broadband solution.

Inside the box you will find an FX4100 cellular router, a Get started card, a USB-C cable and AC wall adapter power supply.

Key features

- With 5G NR technology, Wi-Fi 7 capability, and simplified device management, the compact FX4100 cellular router provides reliable, high-speed connectivity wherever you need it.
- The FX4100 ensures seamless, day-one connectivity and easy setup. You can get online instantly without waiting for wireline installations. The digital display shows network status, initiates mesh pairing, and more for maximum performance.
- Supports up to 128 connected devices, two Ethernet WAN/LAN ports, and a USB-C port for data and tethering.
- Offers the flexibility to function as a dependable primary 5G wireless connection with full Wi-Fi 7 access point; or enhance your network's resiliency by seamlessly transitioning to a failover solution for wired networks, delivering consistent performance and reliability.
- Enterprise-grade management with Inseego Connect allows you to remotely manage thousands of devices and mesh networks from one central interface. Ideal for scaling enterprise networks, ensuring uptime, and reducing complexity.

System requirements

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

Device front

Device back

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

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

Indicator LEDs

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

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

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

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

LED Color	Operation	Meaning
Green		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 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:

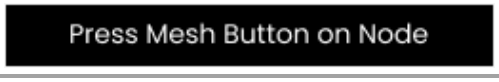

The menu icon on the left shows you where you are in the main menu.


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

Getting started

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

Powering on

To turn on your router, plug the USB C cable into the router power port. Plug the other end into any of the following:

- 24W (12V, 2A) AC power adapter (provided)
- USB-powered hub
- USB-powered delivery device (laptop, computing station, another router, etc.)

WARNING! Use only the AC wall adapter power supply that is packaged with the FX4100 cellular router. Using an unapproved wall adapter or cable are done at the risk of the user.

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

Connecting external antennas (optional)

Your FX4100 cellular router is equipped with four internal antennas. In addition, the device has two external full spectrum cell SMA ports (0.6-6 GHz each) to support two external antennas.

To use external antennas:

1. Remove the SIM/EXTERNAL ANTENNAS cover on the back of the router.

2. Finger tighten your external antennas to the CELL1 and CELL2 external antenna ports.

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

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

Identifying a location

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

1. Scan the QR code to install the Inseego Mobile app from AppStore or Google Play.

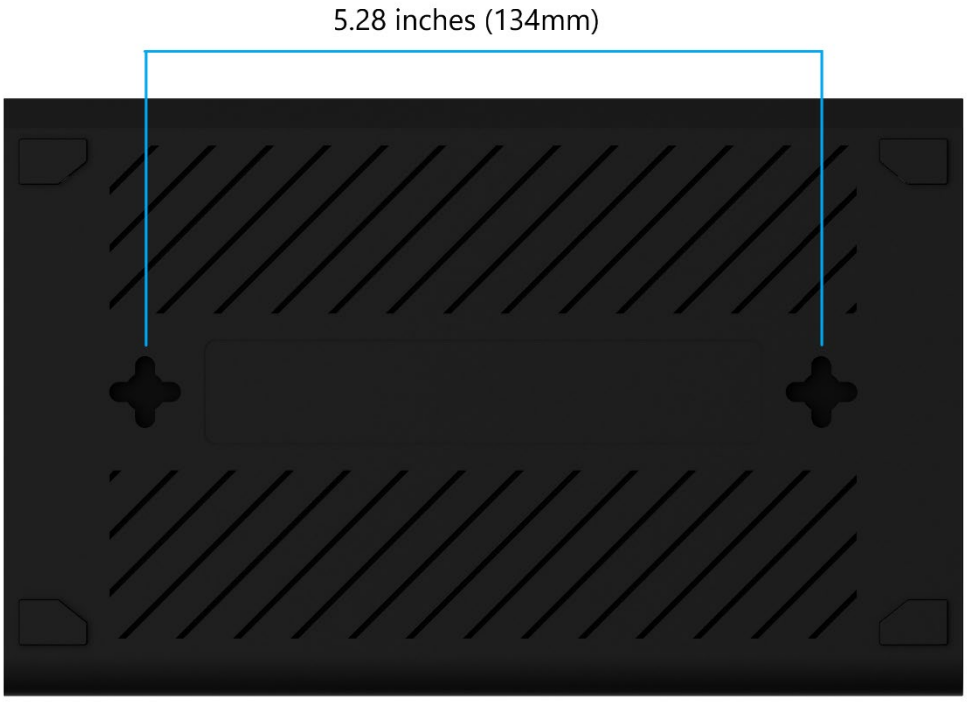
2. Follow instructions within the Inseego Mobile app to connect to your FX4100 and perform a location survey to identify the ideal location for your router.

Location suggestions:

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

Mounting your FX4100 (optional)

The FX4100 has two multi-directional keyhole mounting points on the bottom of the device for wall or rack mounting.



Mounting suggestions:

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

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

Pairing mesh nodes (optional)

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

Your FX4100 cellular router is compatible with the Inseego Wavemaker mesh Wi-Fi X700. See Using Inseego Wavemaker mesh Wi-Fi X700 on page 100 for more information.

To pair an X700 mesh node to your FX4100 cellular router:

1. Power on the FX4100.
2. Power on the X700 by plugging the USB-C cable into the USB power port. Plug the other end into any of the following:
   - AC adapter (provided)
   - USB-powered hub
   - USB host device

   When the X700 LED is blinking green, it is ready to pair.
3. Pair the X700. You can pair your X700 with an Inseego FX4100 cellular router using Wi-Fi or Ethernet.

   Pairing with Wi-Fi

   To initiate Wi-Fi pairing, use the Admin web UI or the interactive device display on the FX4100.

   Using the FX4100 device display

   - Press the **device display button** repeatedly until you see **Wi-Fi Mesh: Hold button to add**.
   - Press and hold the **device display button**.
   - When prompted by the display, press the **Mesh button** on the X700.

   Using the Admin web UI:

   - Go to http://192.168.1.1 to access the Admin web UI for the FX4100. Navigate to **Wi-Fi > Mesh**.
   - Press the **Mesh button** on the X700.
   - Within 30 seconds, click **Add Node** on the UI Mesh page.

   The LED on the X700 and the router blink blue while pairing. When the LEDs are solid, pairing is complete.

   Pairing with Ethernet

   - Connect an Ethernet cable from the X700 to the FX4100.
   - Pairing is automatic. The LED on the X700 blinks blue while pairing. When pairing is complete the LED is solid.
   - When you disconnect the Ethernet cable, the X700 remains paired via Wi-Fi.

Connecting devices to the router

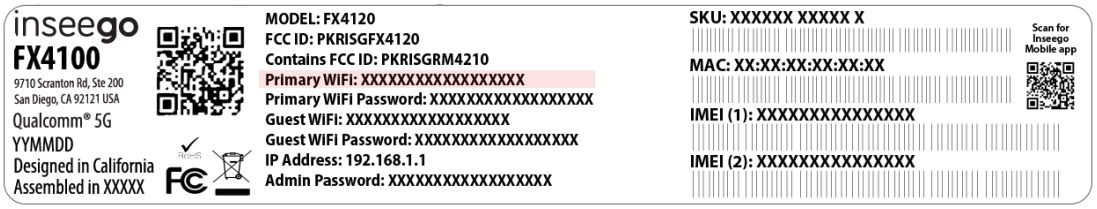
With your FX4100 cellular router, Wi-Fi devices and wired devices can connect to the mobile broadband network simultaneously.

Connecting devices wirelessly

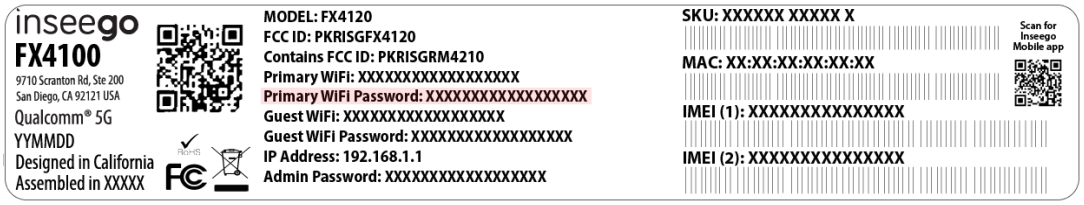
You can connect to your router with your computer, tablet or other wireless devices that have Wi-Fi and internet browser software.

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

1. Make sure the router is powered on, and the Device status LED is blue or green.
2. On the device you want to connect to the internet, open the Wi-Fi settings or application and in the displayed list of available networks. You can find the **Primary Wi-Fi** network name printed on the bottom of your router.



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



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

Connecting devices with Ethernet or USB

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

To connect Ethernet devices:

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

To connect USB devices:

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

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

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

Monitoring and managing your router

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

Inseego Connect™

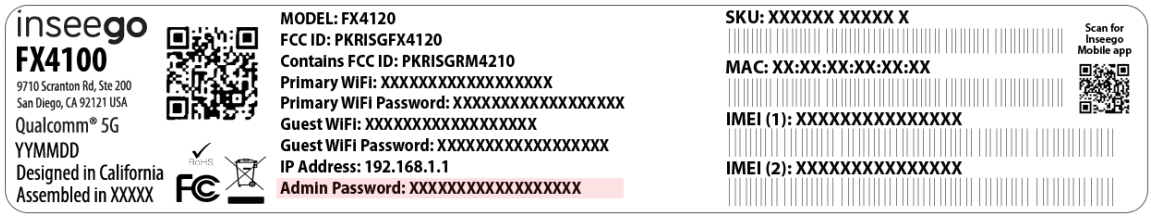
Inseego Connect lets you configure settings, monitor status, and update the firmware on your device remotely from the cloud*. All T-Mobile owned Inseego FX devices come with the option of purchasing the Inseego Connect Add-on. Please work with your Account team to order the Inseego Connect Add-on, which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

Admin web UI

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

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

Select **Sign In** (in the top-right corner of the screen) and enter the **Admin Password** printed on the bottom of the router. In order to securely set up the device, you are prompted to change the password upon login, see Changing the Admin password on page 28.



Inseego Mobile app

You can use the same mobile app you used to find a location for your FX4100 to perform basic device monitoring and management.

---

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

† 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.

Caring for your router

This section provides information on replacing a SIM card, restoring your FX4100 cellular router to factory default settings, and general care tips.

Replacing a SIM card

Your SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The FX4100 cellular router supports only Nano SIM cards. To replace a SIM card, select the correct SIM for this device.

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

To replace a SIM card:

1. Remove the SIM/EXTERNAL ANTENNAS cover on the back of the router.

2. Remove the existing SIM card.

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

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

Resetting your router

You can restart or reset your FX4100 cellular router to factory settings from the Admin web UI, Inseego Mobile app, Inseego Connect or by using the reset button on the router.

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

CAUTION! Factory reset returns your router to factory settings, including resetting the Wi-Fi name and password and Admin password to the defaults shown on the label. This disconnects all devices.

Resetting from the Admin web UI

To reset the router from the Admin web UI, select **Settings > Backup and Restore**, then select **Restart** or **Restore factory defaults**.

Resetting from the Inseego Mobile app

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

Resetting from Inseego Connect

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

Resetting with the reset button

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

1. Verify that your router is powered on.
2. Locate the reset button on the back of your router.

3. **To reboot the router:**
   Press the reset button for one second.

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

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

Care tips

Inseego recommends the following care guidelines:

- Avoid locating the router in areas that can get excessively hot, such as in direct sunlight or in a small, enclosed cabinet without ventilation. Excessive heat may impact performance.
- Protect the router from liquids, dust, and excessive temperatures.
- Do not apply adhesive labels to the router as they may cause the router to potentially overheat or alter the performance of the internal antenna.
- Store the router in a dry and secure location when not in use.

2

Configuration

Overview

You can configure your FX4100 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:

- **Inseego Connect** – Inseego Connect lets you configure settings, monitor status, and update the firmware on your device remotely from the cloud. All T-Mobile owned Inseego FX devices come with the option of purchasing the Inseego Connect Add-on. Please work with your Account team to order the Inseego Connect Add-on, which provides Manager access.
- **Admin web UI** – Provides local access to configure and manage your router. On a device connected to the router, open any web browser, and go to http://192.168.1.1 or http://Inseego.local*. Select **Sign In** (in the top-right corner of the screen) and enter the **Admin Password** printed on the bottom of the router.
- **Inseego Mobile app** – You can use the same mobile app you used to find a location for your FX4100 to perform basic device monitoring and management.

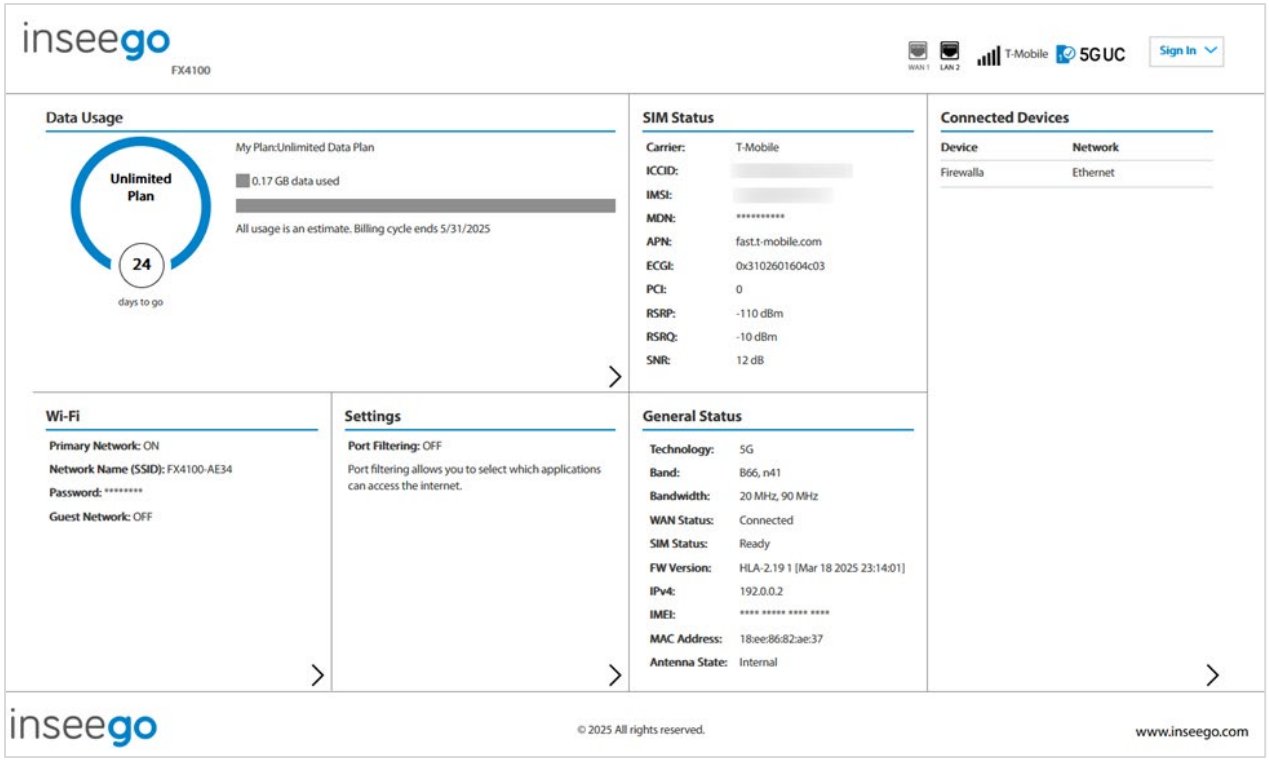
This chapter provides the configuration options available for your FX4100 cellular router. The configurations shown are from the Admin web UI, unless otherwise noted. Many of these options are also available with Inseego Mobile app and Inseego Connect. Some configurations are available only with Inseego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

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

Home page

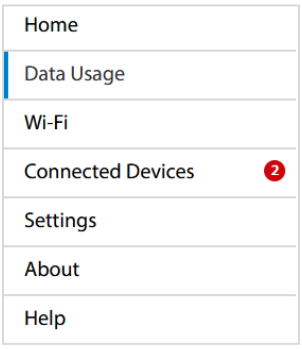
The home page of the Admin web UI is the local gateway to configuring and managing your FX4100 cellular router. It displays the current Wi-Fi networks and passwords and lists all currently connected devices. It also shows data usage, SIM status, general status, and setting information.

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



Side menu

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

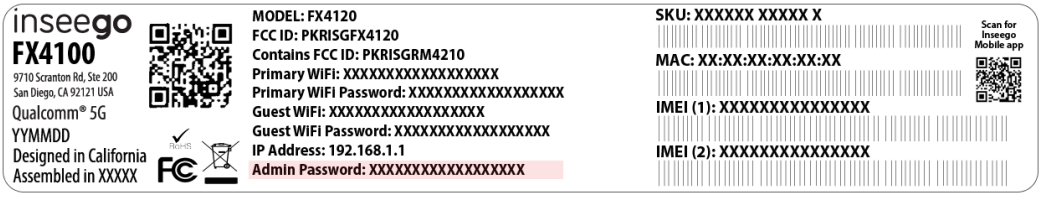


Getting help

Select the question mark (?) in the upper right-hand corner of a page to view help on that topic.

Admin password

The Admin password is what you use to sign into the 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 the down arrow next to **Sign Out** in the top-right corner of any Admin web UI page and select **Change Password.**

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

2. Enter your current Admin password, then enter a new password and confirm it.
   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 drop-down list and type an answer to the question.
   NOTE: Answers are case-sensitive.

4. Click **Save Changes**. A confirmation appears.

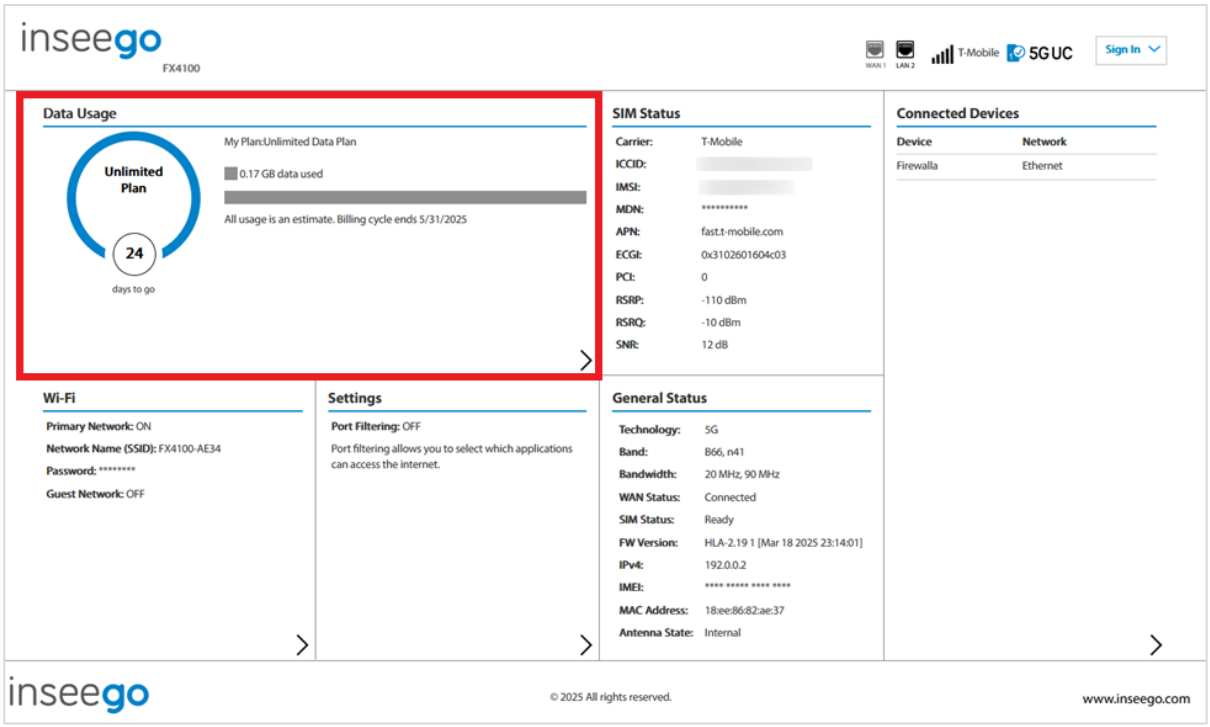
5. Click **OK**.

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

Managing data usage

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

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

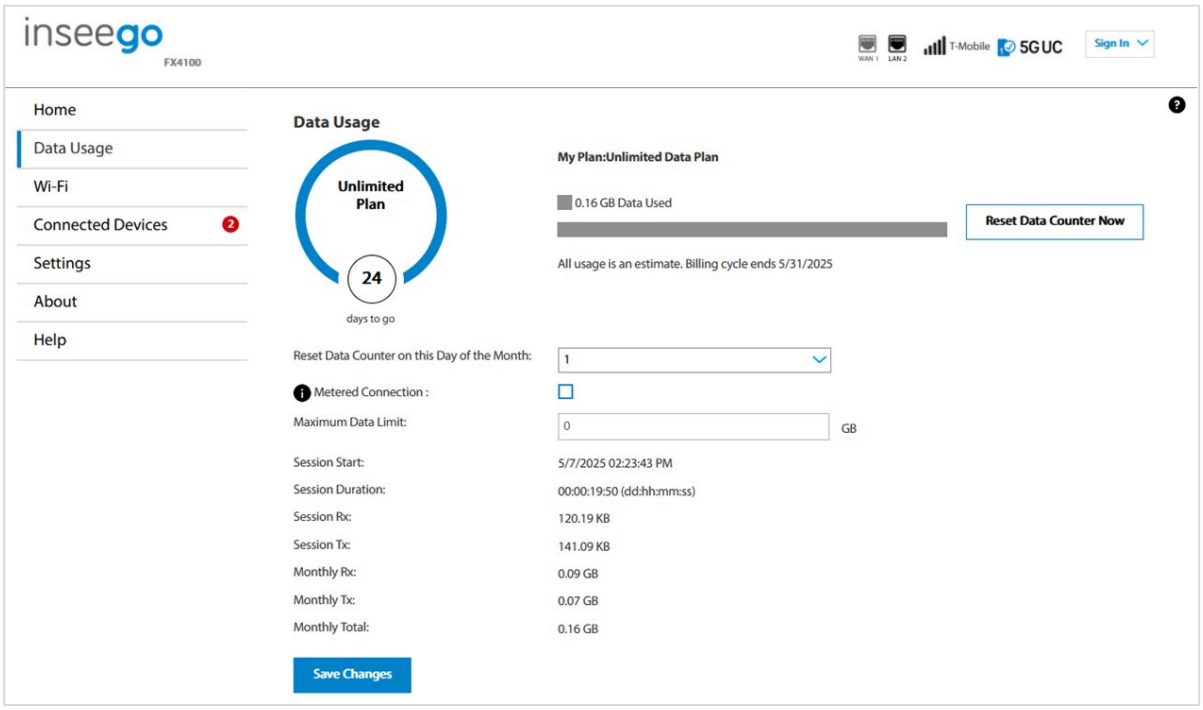


To manage or view data usage, select › from the home page Data Usage panel or select **Data Usage** from the side menu. The Data Usage page appears.

Data Usage page

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

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



The data usage displays vary according to plan, but generally include:

- Estimated amount of data used in the current billing cycle
- Number of days left in the billing cycle
- Date the billing cycle ends

You can configure settings to reflect your monthly data plan.

Use the **Reset Data Counter Now** button to restart the data usage shown on this page to zero.

Reset data Counter on this Day of the Month: Use the drop-down to select a day of the month for the counter displayed on this page to reset.

Metered Connection: Check this box if there is a data limit on your plan.

Maximum Data Limit: Enter a maximum data limit, if applicable.

Session Start: The date and time the current internet session began.

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

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

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

Monthly Rx: The amount of data downloaded for the current billing cycle.

Monthly Tx: The amount of data uploaded for the current billing cycle.

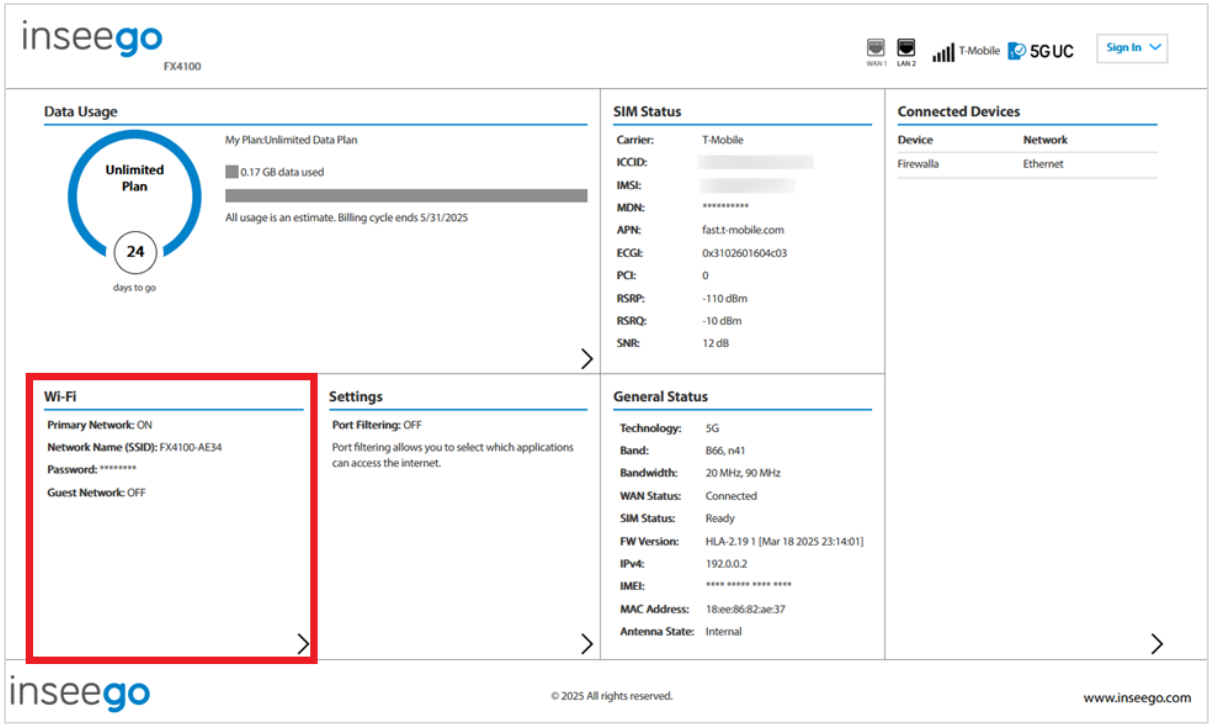
Monthly Total: The total amount of data for the current billing cycle.

Select **Save Changes** to enact changes.

Managing Wi-Fi settings

Your FX4100 cellular router offers primary and guest networks for accessing the internet over Wi-Fi. Each network can be accessed over two bands: 2.4 GHz and 5 GHz.

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



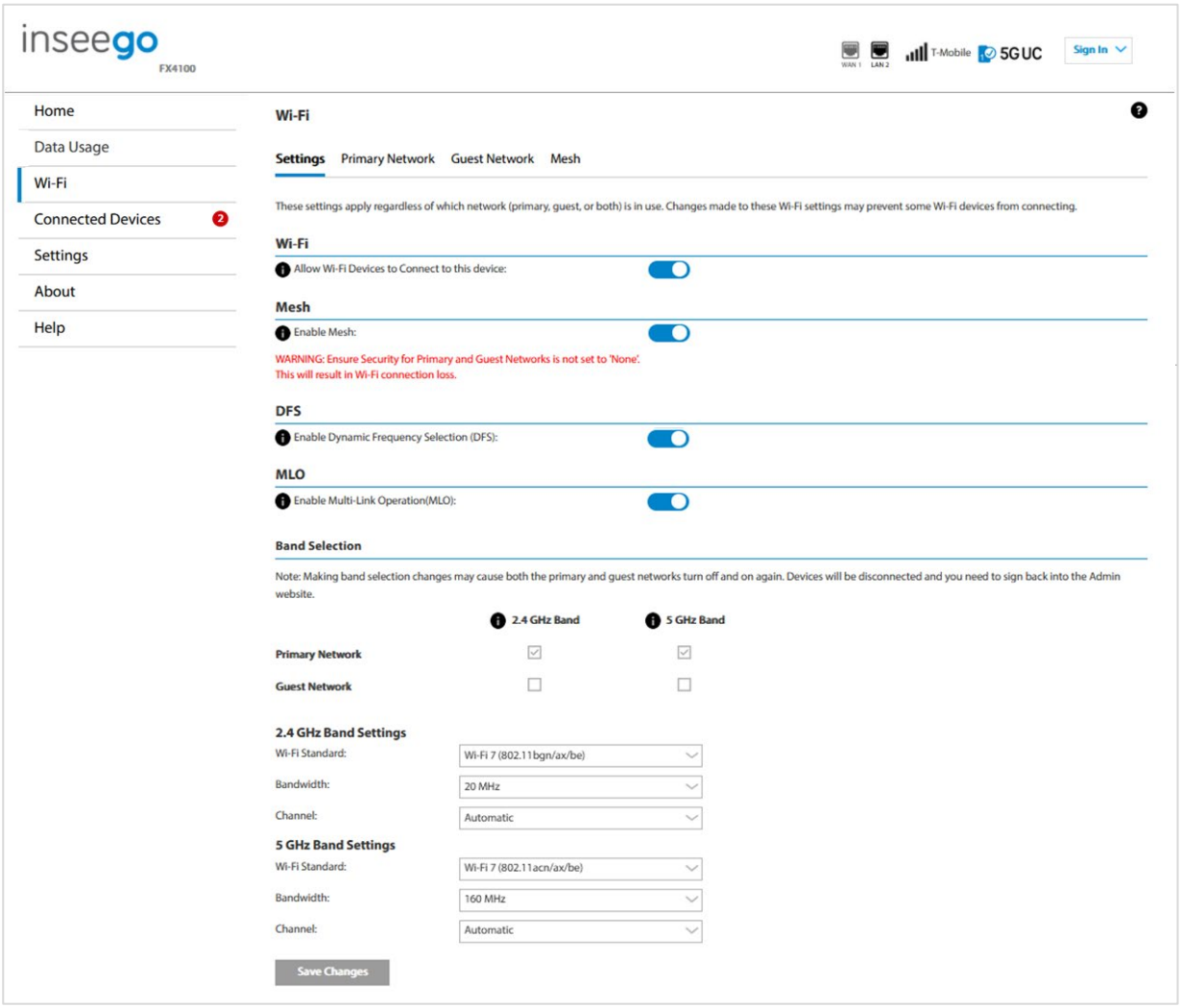
To manage settings for these networks, select › from the home page Wi-Fi panel or select **Wi-Fi** from the side menu.

The Wi-Fi page includes four tabs:

- Settings
- Primary Network
- Guest Network
- Mesh

Settings tab

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



Wi-Fi

Use the **Allow Wi-Fi Devices to Connect to this device** slider to turn Wi-Fi on or off. This selection affects primary and guest networks.

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

Mesh

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

NOTE: Use the **Wi-Fi > Mesh** tab to add and manage mesh nodes.

DFS

Use the **Enable Dynamic Frequency Selection (DFS)** slider to turn DFS on or off. 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.

MLO

Use the **Enable Multi-Link Operation (MLO)** slider to turn MLO on or off. MLO allows the device to simultaneously utilize multiple frequency bands, ensuring seamless data flow. When enabled, the system automatically determines the best band and settings, and the Band Selection section below is read-only.

NOTE: Before enabling MLO, ensure that either the Primary and/or Guest network has both bands (2.4 GHz and 5 GHz) enabled.

Band Selection

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

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

NOTES:

- The Enable Multi-Link Operation (MLO) slider must be off to select bands.
- The guest network must be assigned at least one band before it can be turned on.

2.4 GHz Band Settings

Wi-Fi Standard: Use the drop-down to select a Wi-Fi standard: Wi-Fi 7 802.11bgn/ax/be (default), Wi-Fi 6 802.11bgn/ax, or Wi-Fi 4 802.11bgn.

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.

5 GHz Band Settings

Wi-Fi Standard: Use the drop-down to select a Wi-Fi standard: Wi-Fi 7 802.11bgn/ax/be (default), Wi-Fi 6 802.11acn/ax, Wi-Fi 5 802.11acn, or Wi-Fi 4 802.11n.

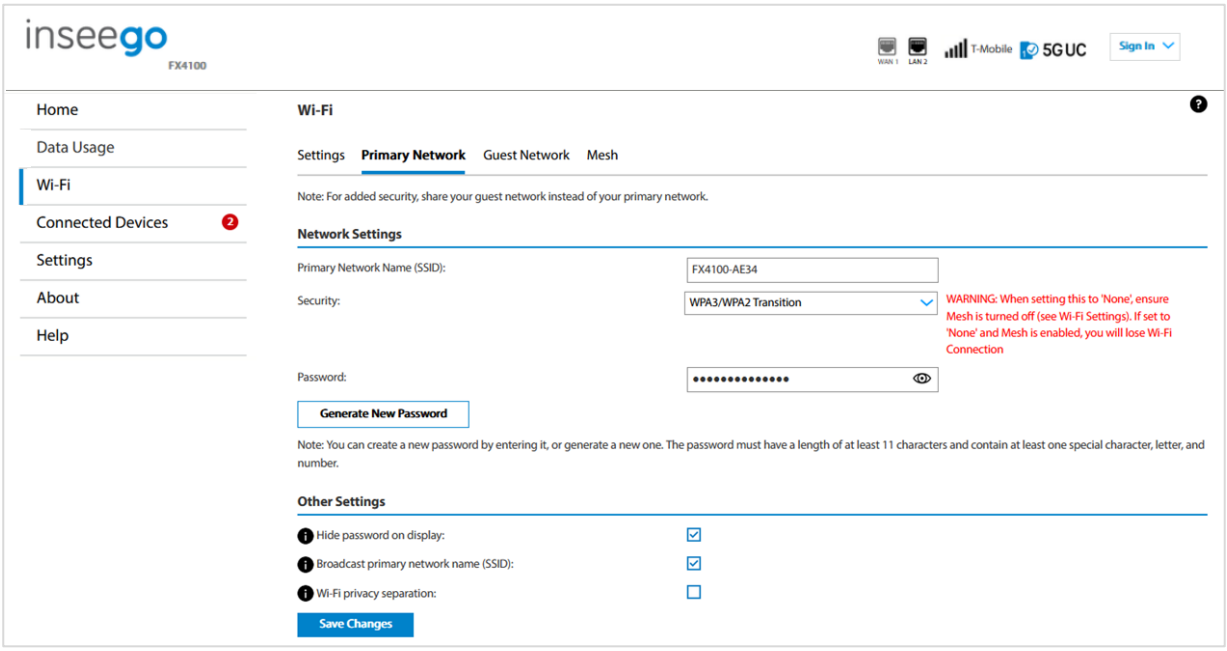
Bandwidth: Leave bandwidth at the default setting unless you experience interference with other Wi-Fi devices.

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

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

Primary Network tab

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



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

Network Settings

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

Security: Select an option for Wi-Fi security:

- **WPA3/WPA2 Transition** is the most secure method of Wi-Fi Protected Access and should be used, if possible, for WPA2 and WPA3 compliant devices.
- **WPA3 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:** Avoid using this option.

Password: Enter a Wi-Fi password, ***or*** you can use the Generate New Password button. **NOTE:** The password must have a length of at least 11 characters and contain at least one special character, letter, and number. 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 and use a different password from your Admin password to keep the device and your network secure.

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

Other Settings

Hide password display: Check this box to hide the Wi-Fi primary network password on the device display. If unchecked, the primary network password is visible on the device display.

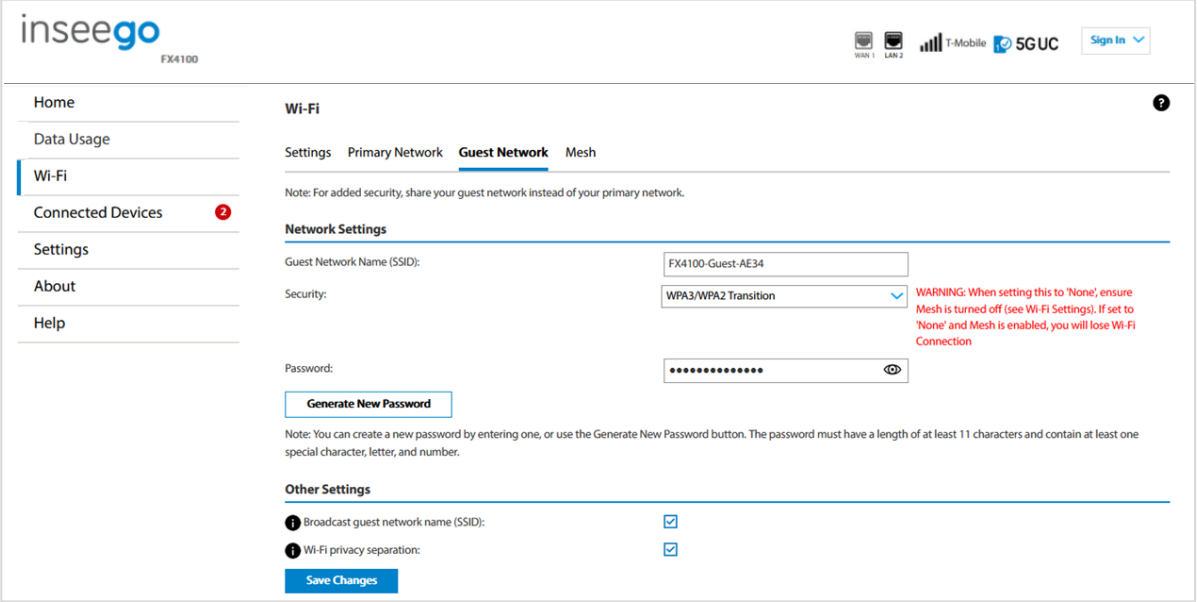
Broadcast primary network name (SSID): When checked, this allows the Wi-Fi primary network to be displayed in the list of available Wi-Fi networks on your connected devices. If unchecked, this network is not visible to connected devices.

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

Select **Save Changes**.

Guest Network tab

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



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

Network Settings

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

Security: Select an option for Wi-Fi security:

- **WPA3/WPA2 Transition** is the most secure method of Wi-Fi Protected Access and should be used, if possible, for WPA2 and WPA3 compliant devices.
- **WPA3 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:** Avoid using this option.

Password: Enter a Wi-Fi password, ***or*** you can use the Generate New Password button. **NOTE:** The password must have a length of at least 11 characters and contain

at least one special character, letter, and number. 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 and use a different password from your Admin and primary network password to keep the device and your network secure.

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

Other Settings

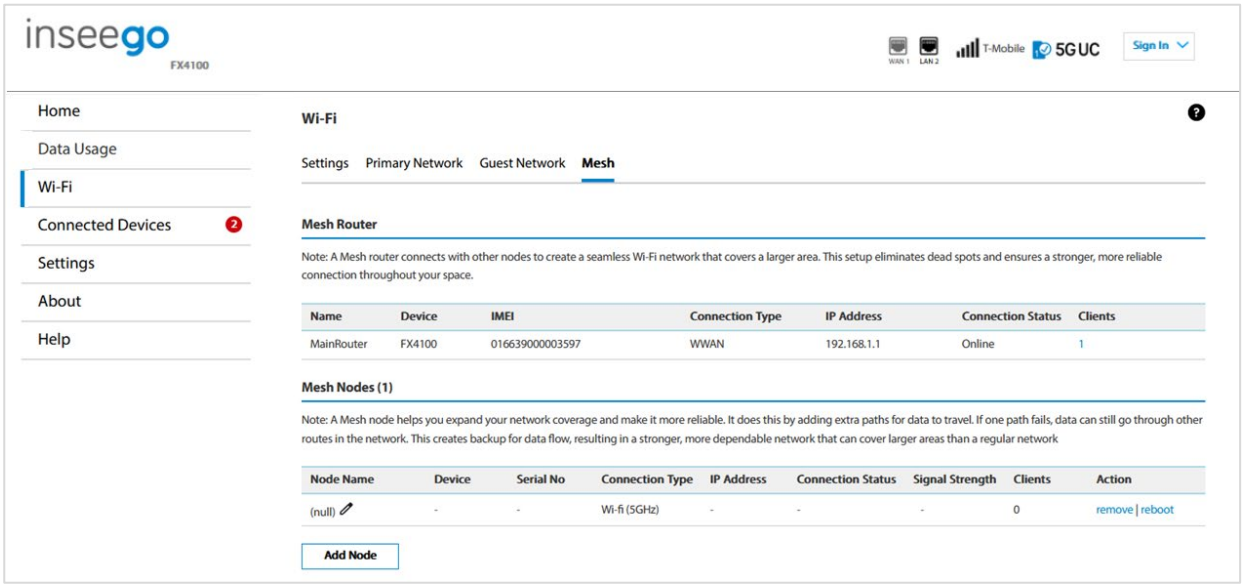
Broadcast guest network name (SSID): When checked, this allows the Wi-Fi guest network to be displayed in the list of available Wi-Fi networks on your connected devices. If unchecked, this network is not visible to connected devices.

Wi-Fi privacy separation: When checked, each connected device on this network is isolated from all other connected devices. This provides additional security if some connected devices are unknown or not completely trusted.

Select **Save Changes**.

Mesh tab

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



Mesh Router

The section provides information on your FX4100.

Name: The name of your router. You can edit the name using the pencil icon ✎.

Device: The model of the device.

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

The table provides information on mesh nodes in your network.

Node Name: The name of the mesh node. You can edit the name using the pencil icon ✎.

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 to the router. Click on the number to view detailed information on connected client devices.

Action: 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 on this page. Alternately, you can also add a mesh node using the device display button on the FX4100, or by connecting to the mesh node via Ethernet.

NOTE: To pair, make sure both the FX4100 and X700 are powered on and the LED on the X700 is blinking green and ready to pair.

Using this web UI page

You can use the Add Node button to pair a mesh node and add it to your network:

1. Press the **Mesh button** on the mesh node.
2. Within 30 seconds, click the **Add Node** button on the Admin web UI Mesh page.

The LED on the mesh node and the router blink blue while pairing. When the LEDs are solid, pairing is complete.

Using the device display

1. Press the **device display button** repeatedly until you see **Wi-Fi Mesh: Hold button to add**.
2. Press and hold the **device display button**.
3. When prompted by the display, press the **Mesh button** on the mesh node.

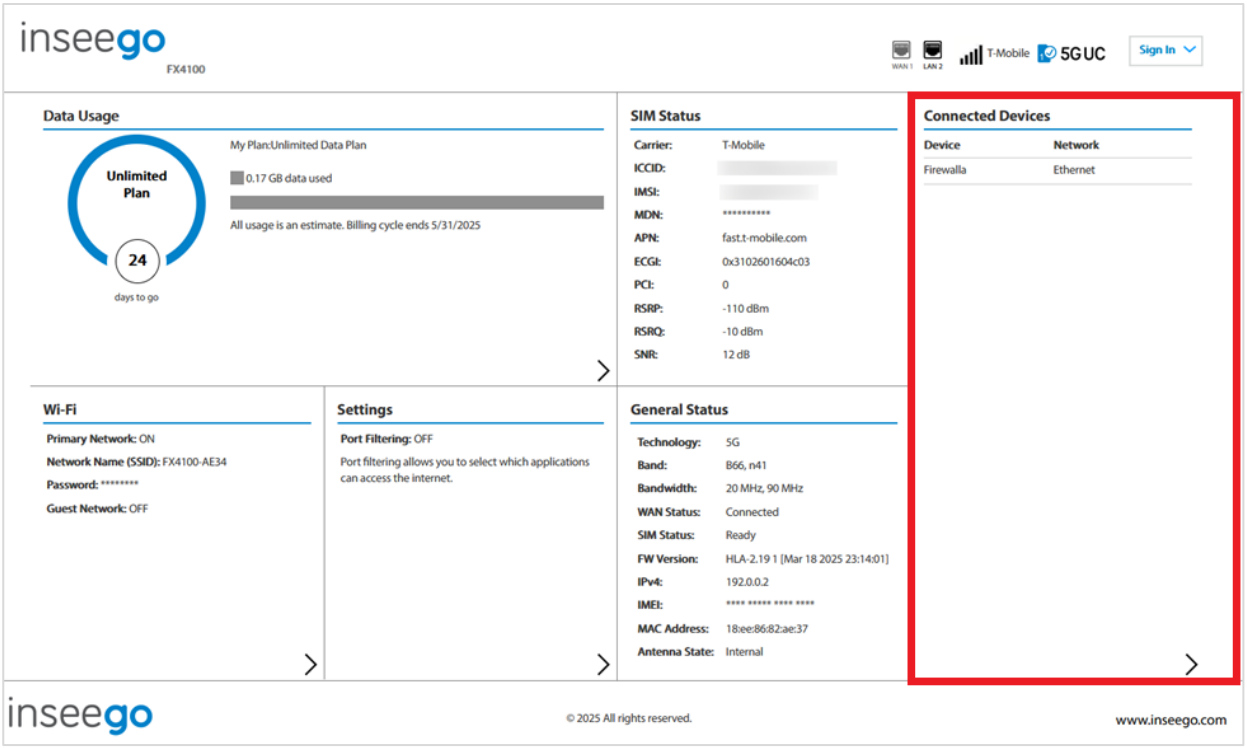
The LED on the mesh node and the router blink blue while pairing. When the LEDs are solid, pairing is complete.

Using Ethernet

1. Connect an Ethernet cable from the router to the mesh node.
2. Pairing is automatic. The LED on the X700 blinks blue while pairing. When pairing is complete the LED is solid.
3. When you disconnect the Ethernet cable, the mesh node remains paired via Wi-Fi.

Managing connected devices

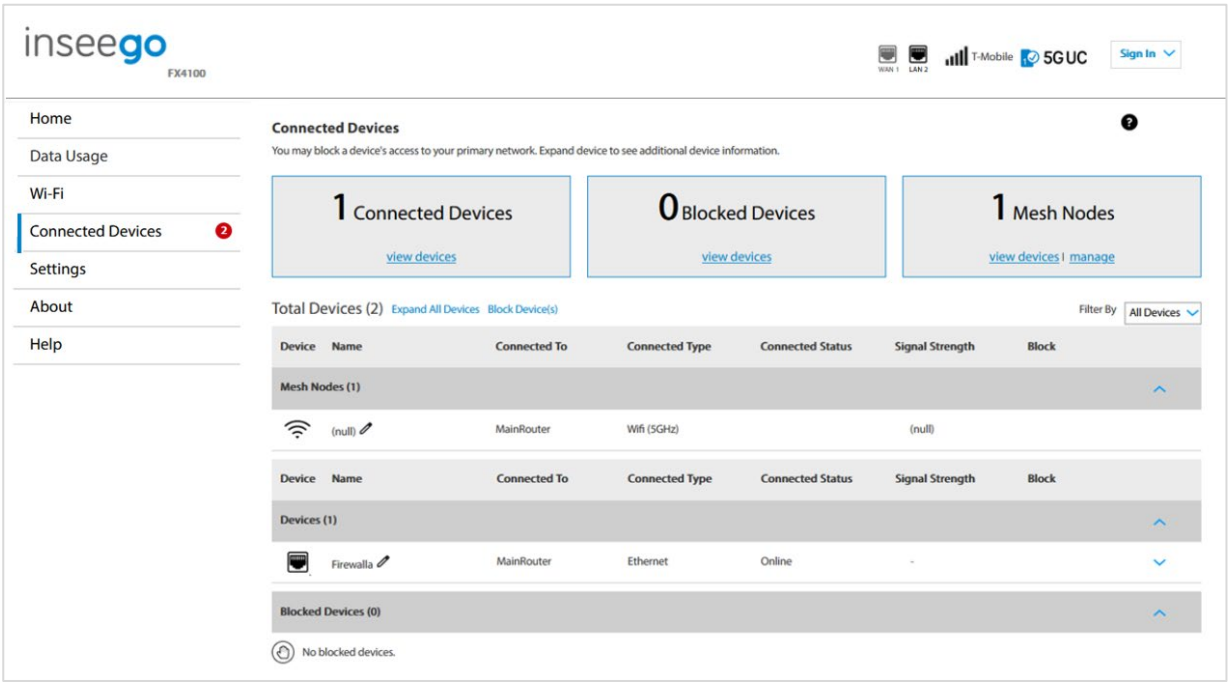
On the Admin web UI home page, the Connected Devices panel lists the networks currently connected to your FX4100 cellular router along with the number of connected devices for each network.



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

Connected Devices page

This page provides details about each device connected to the FX4100 cellular 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.



Connected Devices

This section shows the number of connected devices, blocked devices and mesh nodes. Click **view devices** to see details for that topic. Click **manage** under Mesh Nodes to go to the Wi-Fi Mesh tab to manage mesh nodes.

Total Devices

This table displays details for all connected devices, mesh nodes, and blocked devices, and allow you to block or unblock devices from internet access.

Use the **Filter By** dropdown in the upper right to filter the display.

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

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

Connection Type: Indicates whether the device is connected to the primary or guest network, or through 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.

Block: Click **Block** next to a device to disconnect it from accessing your network and prevent it from reconnecting. Click **Block Device** 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.

To view details on a device, click the **down arrow** on the right to expand the device row. The following information appears:

- **IPv4**: The IPv4 address of the connected device.
- **IPv6**: 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.

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

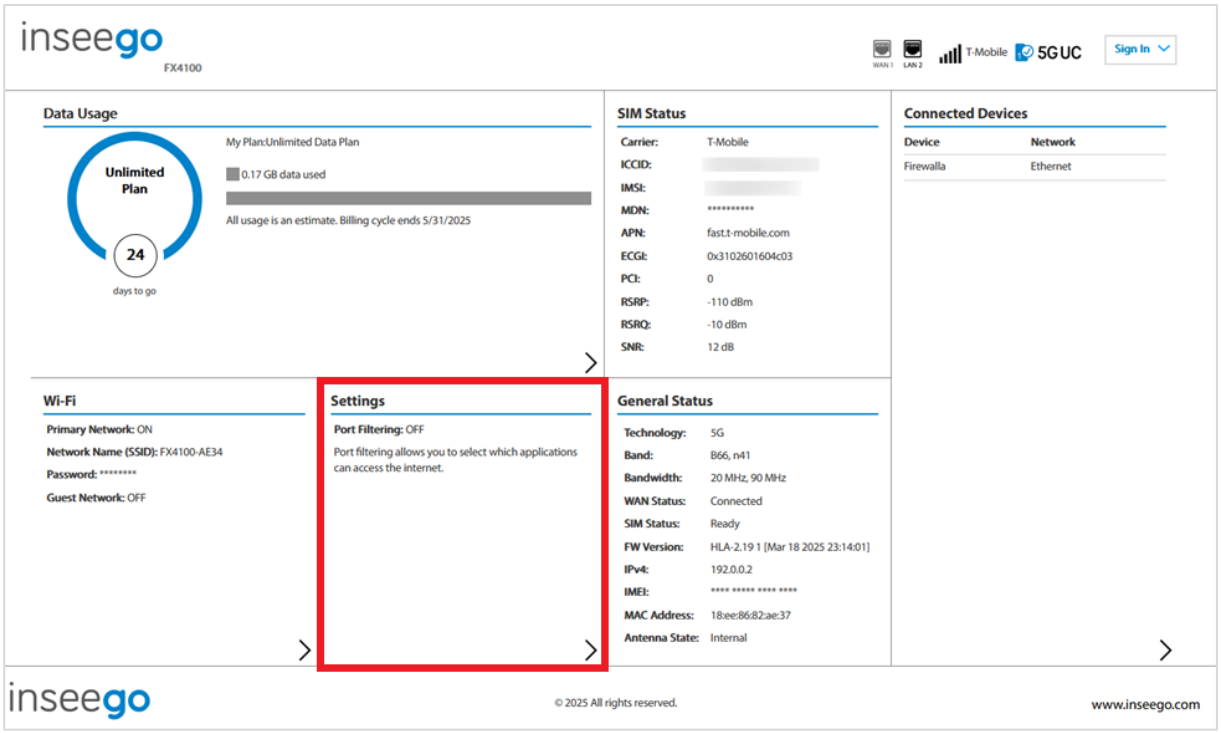
Blocked Devices

This section lists all devices blocked from connecting to your router.

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.

Managing settings

On the Admin web UI home page, the Settings panel shows Port Filtering information.



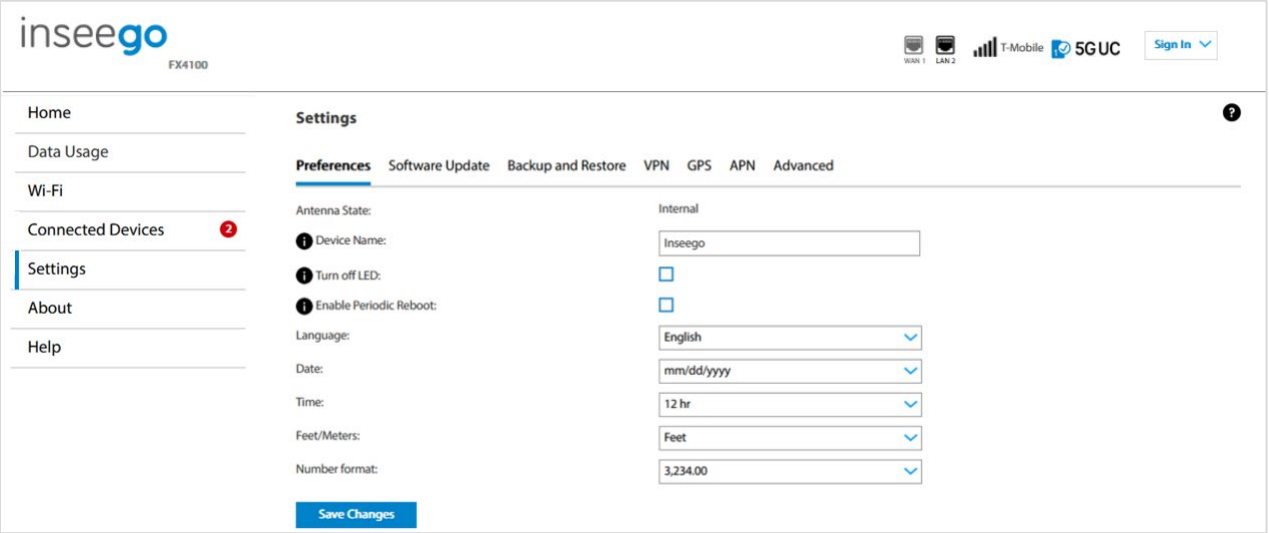
To configure more system settings, select ›from the home page Settings panel or select **Settings** from the side menu.

The Settings page includes the following tabs:

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

Preferences tab

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



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

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

Turn off LED: Check the checkbox to turn off the LED lights on the front left of your router. **NOTE:** This does not affect the device display on the front right of the router, which times out after 60 seconds.

Enable Periodic Reboot: 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.

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.

Language: Select a language for the Admin web UI.

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

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

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

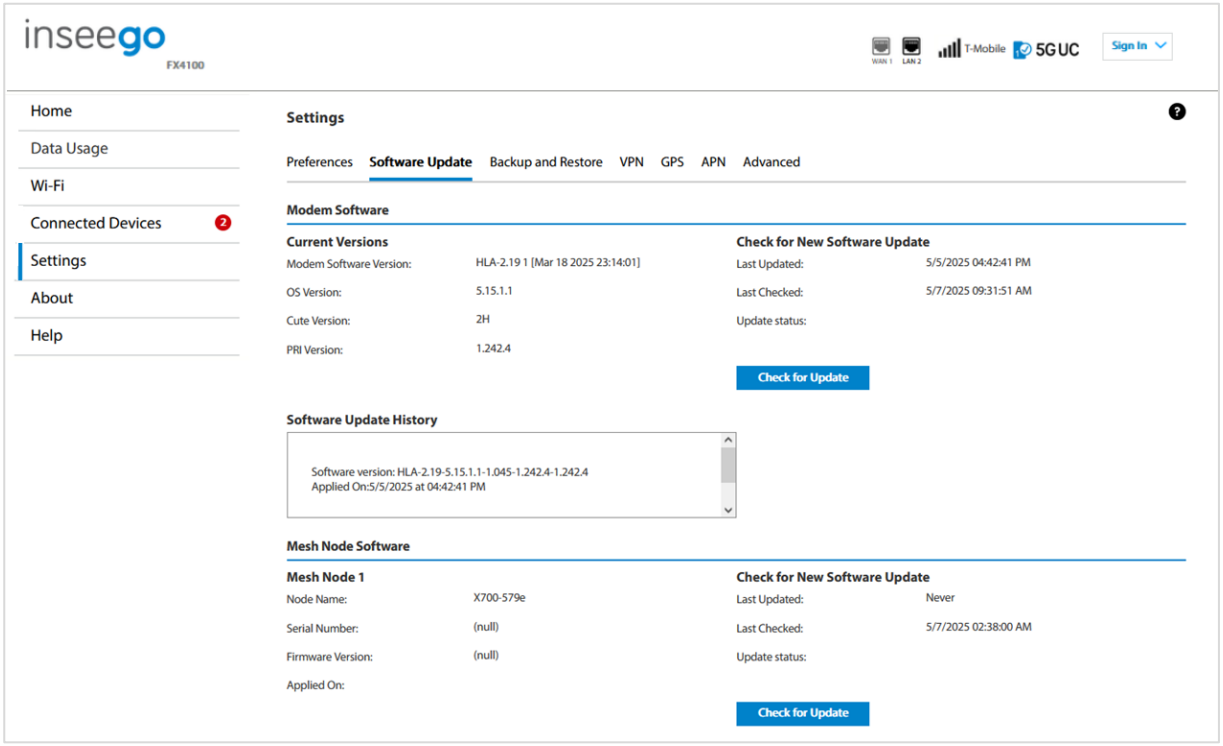
Number format: Choose the format for decimal numbers displayed in the web UI (using a period or comma as the decimal point).

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

Software Update tab

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

If your router is used on a private APN or cellular network, or if access is limited to specific sites, you must include the following URL in the access list so that automatic software updates can be delivered and you can check for updates: https://fota.production.nvtl.mifiupdates.com (TCP 443).



Modem Software

Current Versions

Modem Software Version: The version of software currently installed.

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

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

PRI Version: The configuration version currently applied to your router.

Software Update History

A history of previous software updates.

Check for New Software Update

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

Update status: This area is usually blank. If you check for an update, the results display.

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

Mesh Node Software

Mesh Node

Node Name: The name of the mesh node.

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

Firmware Version: The version of firmware currently installed.

Check for New Software Update

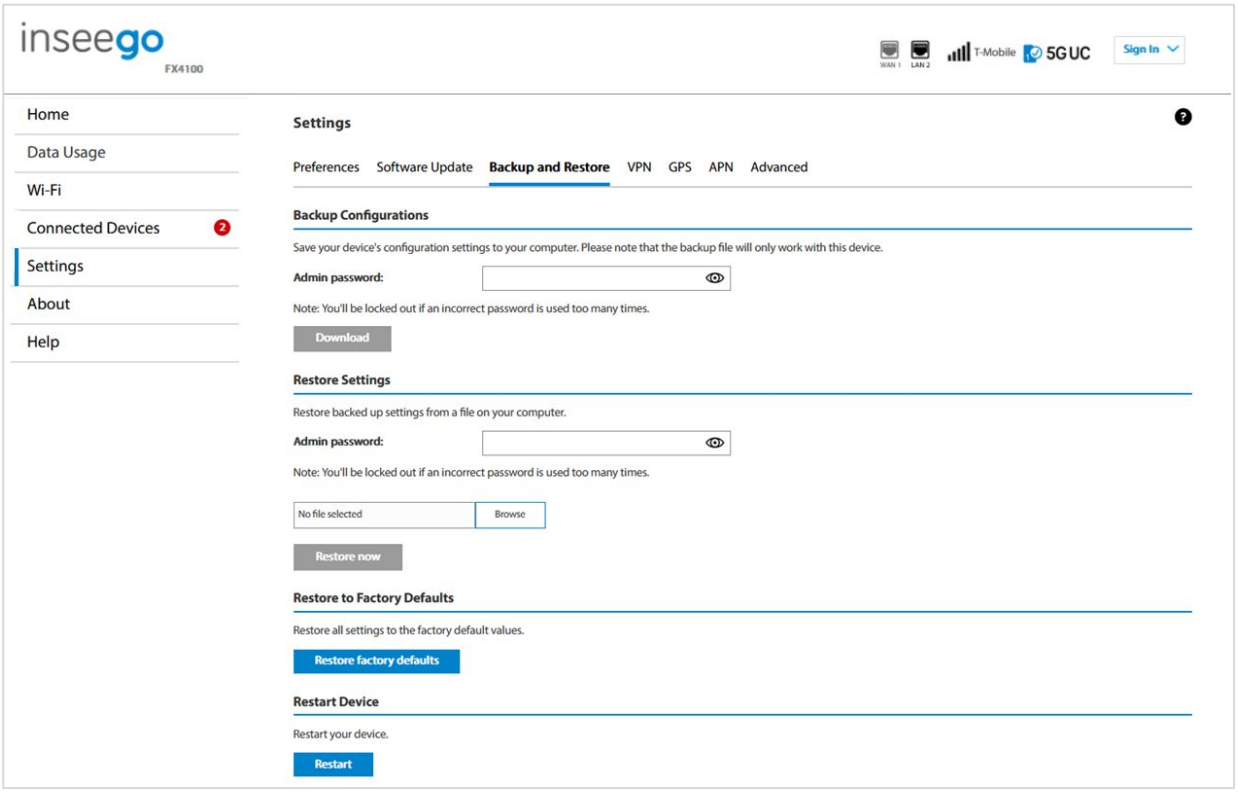
Last check for update: The date and time the router last checked to see if an update was available.

Update status: This area is usually blank. If you check for an update, the results display.

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

Backup and Restore tab

Use this tab to back up your current FX4100 cellular router settings to a file on your computer, restore (upload) a previously saved configuration file, reset the router to factory defaults, or restart the router.



Backup Configurations

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

The default Admin password is printed on the bottom of the router. If you have changed the Admin password and don't remember it, select **Sign In** in the top-right corner, click **Forgot Admin Password**, and answer the displayed security question. The current Admin password is displayed.

NOTE: If you enter an incorrect password five times in a row, you will be locked out of the Admin web UI. To unlock it, restart your router and use the Admin password printed on the bottom label.

Click the **Download** button. The file is automatically downloaded to the default Downloads folder on the device connected to the Admin web UI. This configuration file contains all settings for your 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 FX4100 cellular router, and settings can only be viewed or changed using the Admin web UI.

Restore Settings

CAUTION! Restoring settings (uploading a configuration file) changes ALL 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, enter your Admin password in the **Admin password** field.

Click **Browse** and choose a backup settings file to restore.

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

Click the **Restore now** button.

Restore to Factory Defaults

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

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

Restart Device

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

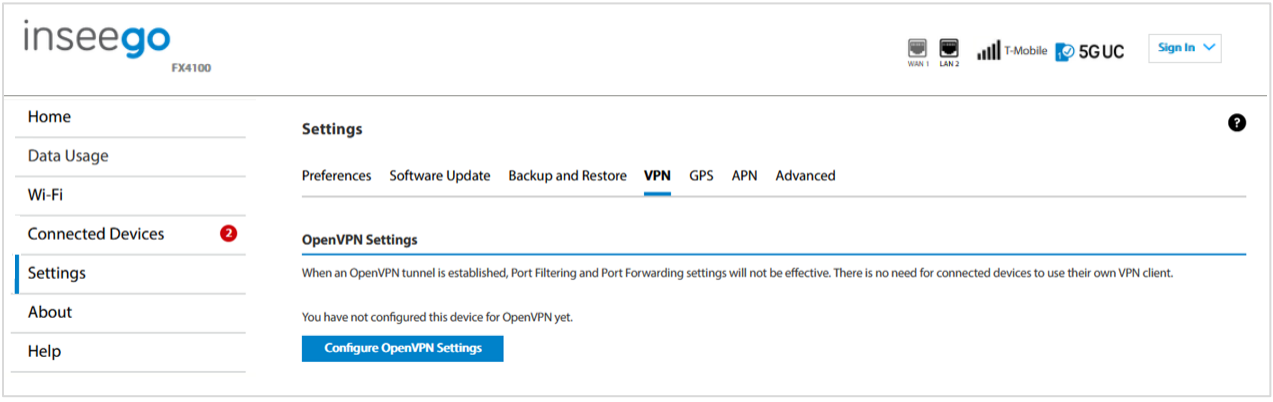
VPN

You can configure OpenVPN through the Admin web UI. IPSec VPN is available with Inseego Connect.

- VPN tab (OpenVPN) - Admin web UI
- IPSec VPN (Inseego Connect)

VPN tab (OpenVPN)

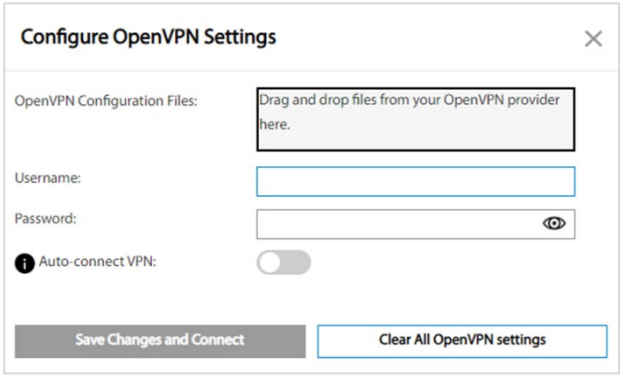
Your FX4100 cellular router allows you to establish secure connections to remote networks over a public network using OpenVPN.



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

OpenVPN Settings

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



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

Username: Enter your OpenVPN connection username here.

Password: Enter your OpenVPN connection password here.

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

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

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

VPN Connection

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

Connection status: Indicates the status of the OpenVPN connection.

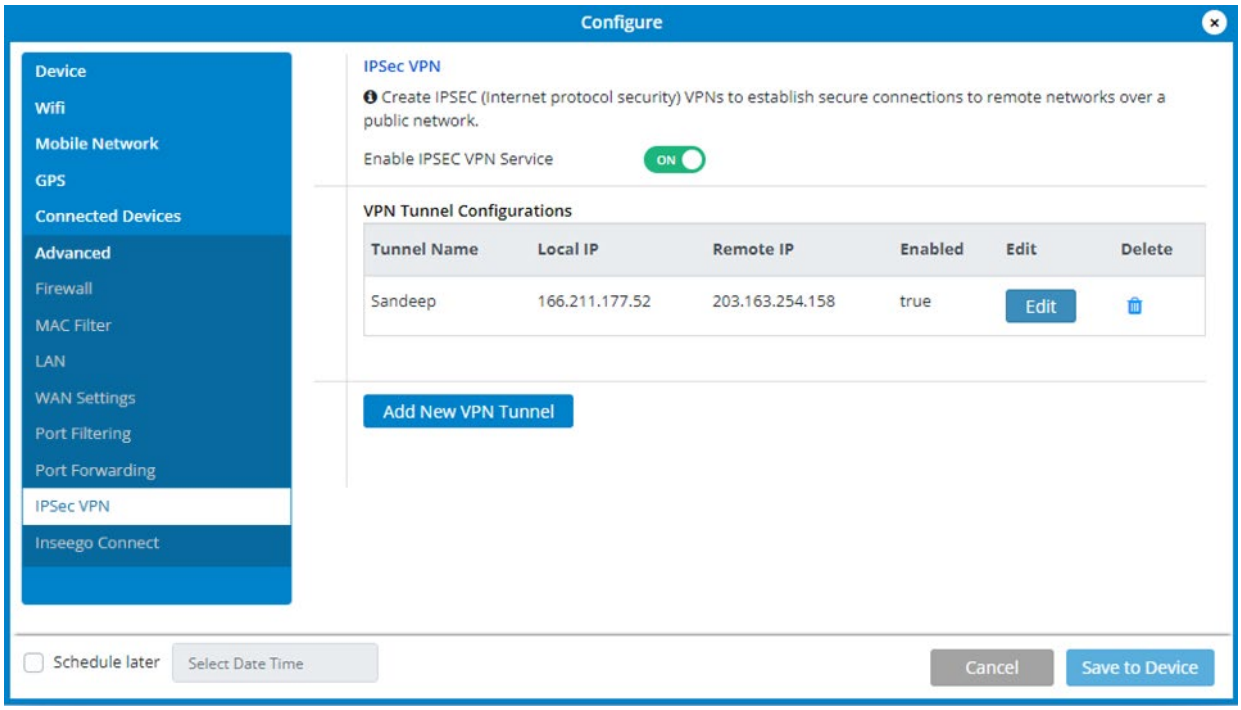
Connection time: The duration of the current OpenVPN connection.

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

Connect: Use this button to connect the OpenVPN.

IPSec VPN (Inseego Connect)

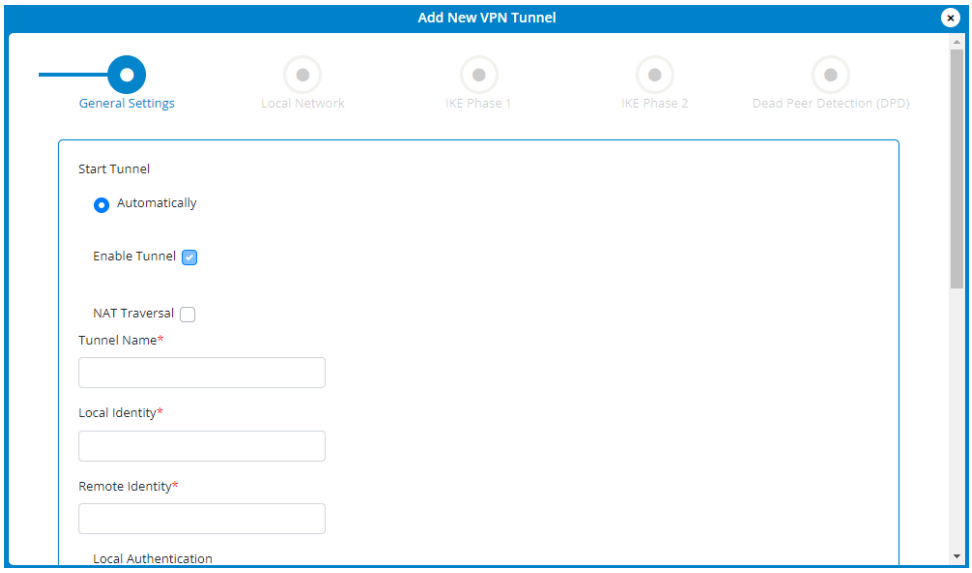
You can create IPSec VPNs using Inseego Connect. All T-Mobile owned Inseego FX devices come with the option of purchasing the Inseego Connect Add-on. Please work with your Account team to order the Inseego Connect Add-on, which provides Manager access.



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

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

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



General Settings

- **Start Tunnel** — Select whether to start the tunnel automatically upon start up or manually.
- **Enable Tunnel** — Check this box to enable the tunnel.
- **NAT Traversal** — Check this box if you want NAT traversal to automatically detect if network address translation (NAT) is being performed between the two VPN tunnel endpoints.
- **Tunnel Name** — Enter a unique name to identify this VPN.
- **Local Identity** — Enter a unique name to identify the local point of the tunnel.
- **Remote Identity** — Enter a unique name to identify the remote point of the tunnel.
- **Local Authentication** — Select a type of authentication from the drop-down list. You are prompted for further information based on your selection.
- **Remote Authentication** — Select a type of authentication from the drop-down list. You are prompted for further information based on your selection.

Click **Next**.

Local Network

- **Local IP** — Enter the WAN IP address of local device. **NOTE:** This should be a static IP that you are able to reach from remote device (no NAT).
- **Local Subnet Mask** — Enter the subnet mask of the local device, for example: If your local IP is 192.168.0.100 and your subnet mask is 255.255.255.0 this should

be **192.168.0.0/24**. **NOTE:** This should mirror what the subnet displays in the local device, for example: 192.168.0.0 / 255.255.255.0. **NOTE:** The local device should be on a different subnet from remote, for example: If the Remote Subnet Mask is **192.168.1.0/24**, the Local Subnet Mask might be **192.168.0.0/24**. This is usually based off the DHCP settings of the devices.

Remote Network

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

Click **Next**.

IKE Phase 1

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

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

Click **Next**.

IKE Phase 2

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

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

Click **Next**.

Dead Peer Detection (DPD)

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

Enable: Check this box to enable DPD.

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

DPD Delay: The number of seconds between DPD packets.

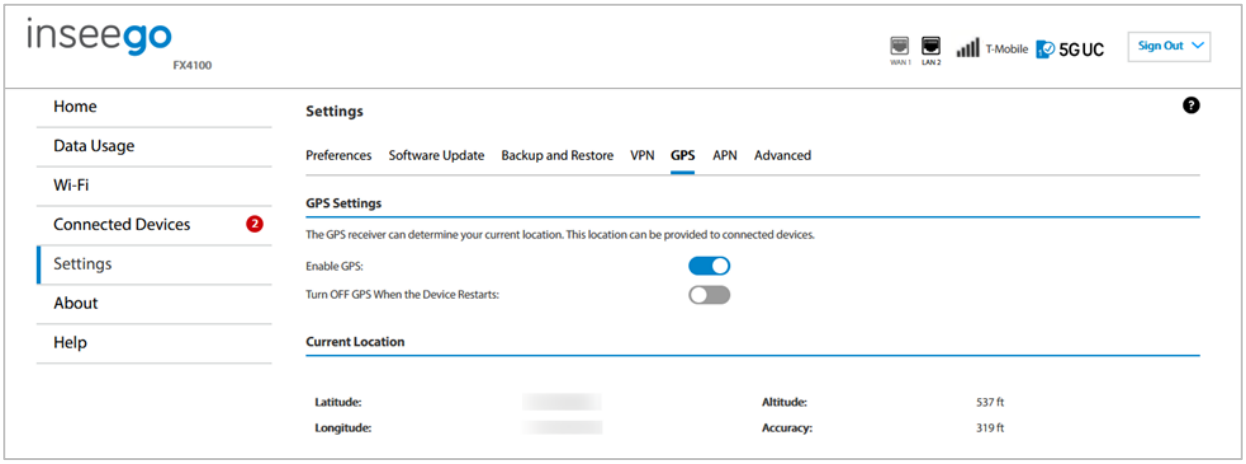
DPD Timeout: The number of seconds the router will allow an IPSec session to be idle before beginning to send DPD packets to the peer machine.

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

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

GPS tab

Your FX4100 cellular router incorporates a GPS receiver. The GPS receiver can determine your current location. Use this tab to enable GPS, view current location information, and to enable GPS streaming to devices with the GPS over Wi-Fi feature.



GPS Settings

Enable GPS: This setting enables or disables the GPS radio on your router. When the ON/OFF slider is **ON**, the device acquires GPS and makes GPS location data available on this page. A GPS Agreement appears, click **Confirm** to proceed. When **OFF**, no GPS data is available.

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

Current Location

Latitude: Latitude for the last location fix.

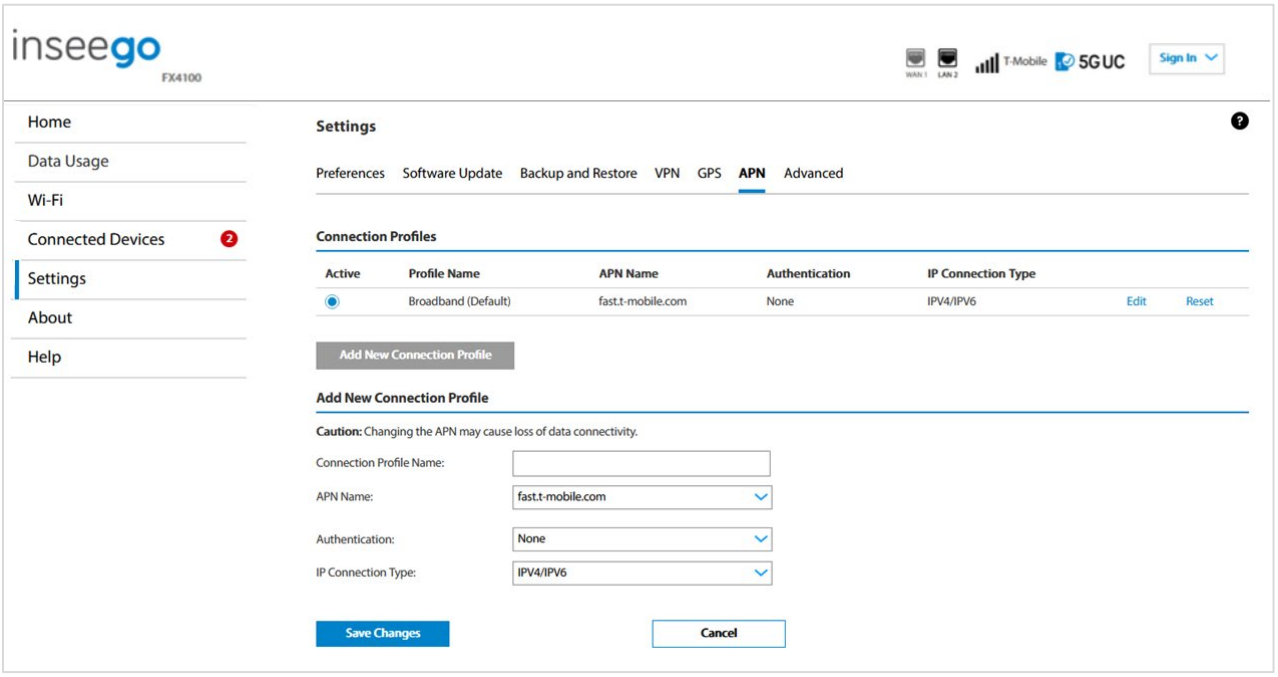
Longitude: Longitude for the last location fix.

Altitude: Altitude for the last location fix.

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

APN tab

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



Connection Profiles

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

Active: 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.

Click **Edit** to edit a profile.

Click **Reset** to reset a profile to default values.

Click the **Add New Connection Profile** button to add an additional APN connection profile.

Add New Connection Profile

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

Connection Profile Name: Enter a name to identify this connection profile.

APN Name: Select an APN supplied by your service provider from the drop-down or select **Add APN** and enter the APN for your private network in the text box that appears below.

NOTE: Information in the following fields should come from your service provider based on network requirements.

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

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.

IP Connection Type: Select an IP connection type from the drop-down (IPv4, IPv6, or IPv4/IPv6).

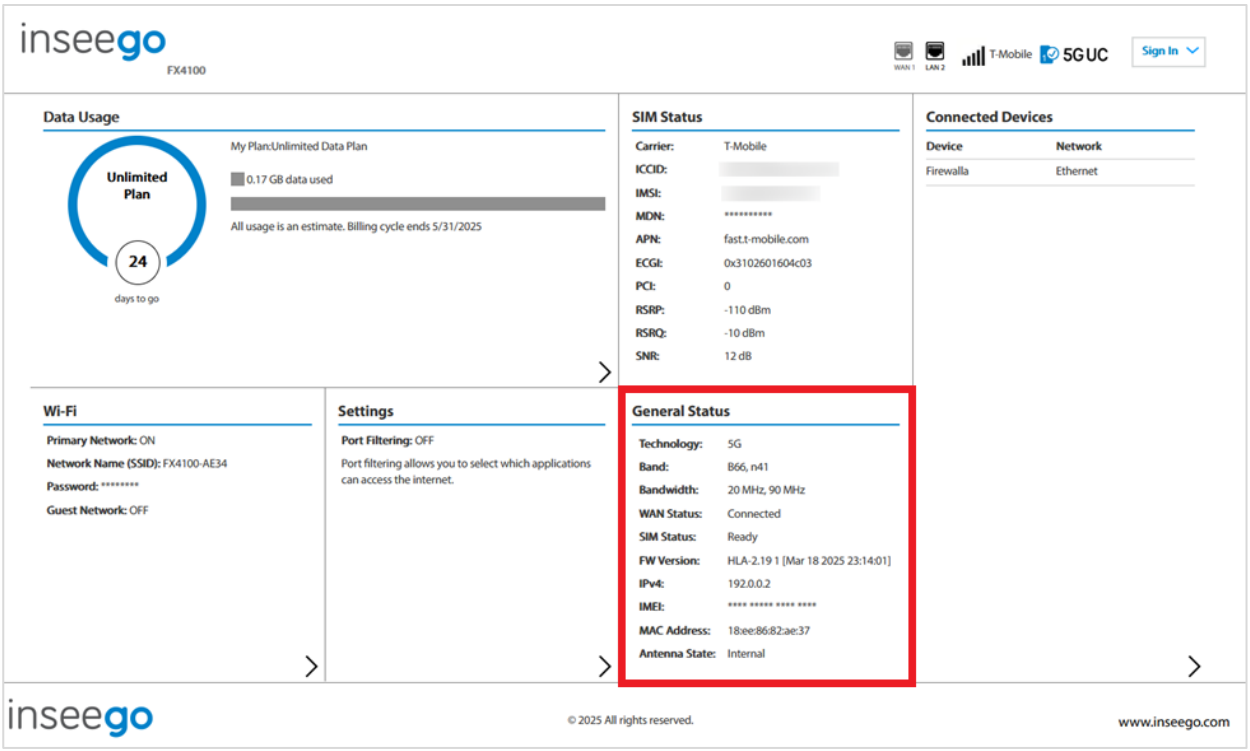
Click **Save Changes**.

Advanced tab

Advanced settings are intended only for users with advanced technical knowledge. For information about the Advanced Settings page, go to Chapter 4, Advanced Settings on page 75.

Viewing info about your router

On the Admin web UI home page, the General Status panel provides an overview of the current status of your router.



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

Band: The band in use for the current connection.

Bandwidth: The bandwidth in use for the current connection.

WAN Status: The status of the WAN.

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

FW Version: The version of the firmware (software) currently installed on your router.

IPv4: The internet IP address assigned to your router.

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

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

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

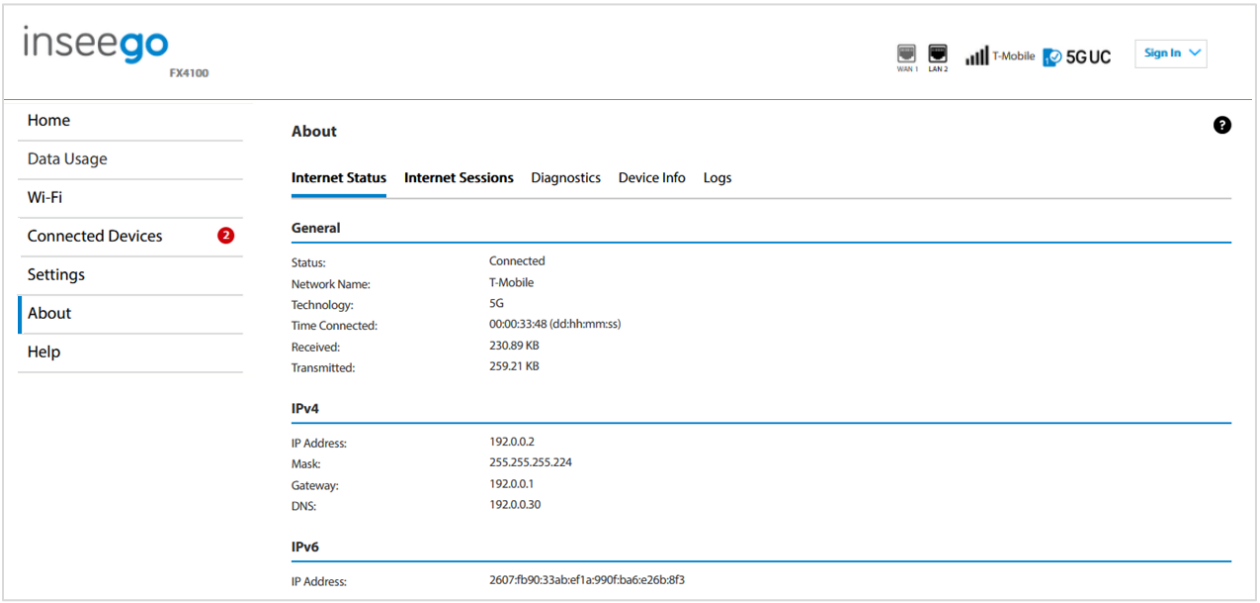
To view more detailed information about your router and its use, select > from the home page About panel or select **About** from the side menu.

The About page includes the following tabs:

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

Internet Status tab

Use the Internet Status tab 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 cellular data connection, for example, 5G.

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

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

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

IPv4

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

Mask: The network mask associated with the IPv4 address.

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

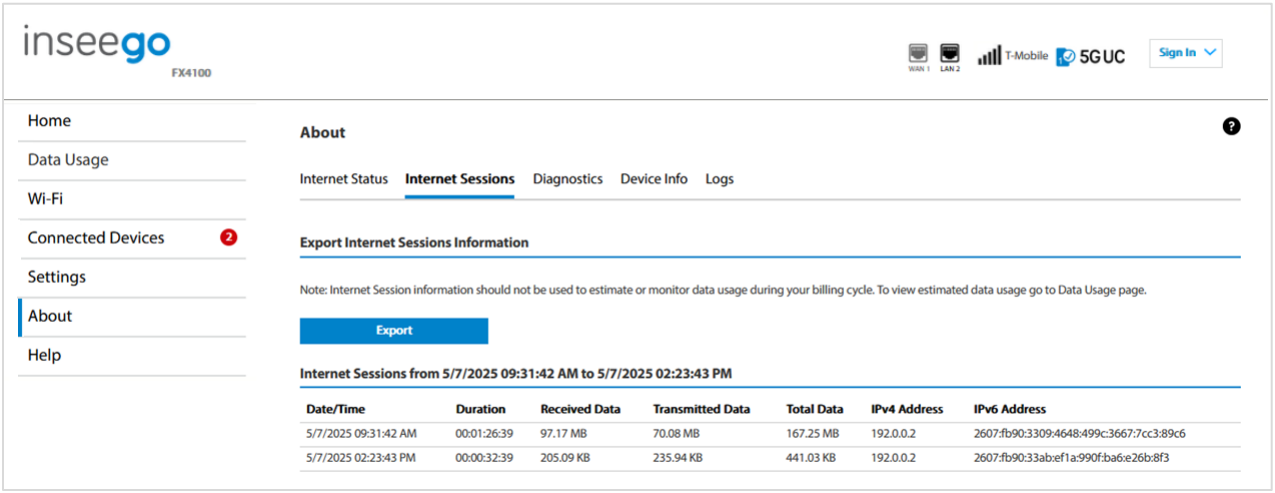
DNS: The Domain Name Server currently used by the router.

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 tab

Use the Internet Sessions tab to export and view internet session data.



Export Internet Sessions Information

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

Internet Sessions

NOTE: Internet sessions are presented in date order.

Date/Time: The date and time the internet session began.

Duration: The total amount of time for the internet session.

Received Data: The amount of data received for the internet session. This counter starts at zero when the connection is established.

Transmitted Data: The amount of data transmitted for the internet session. This counter starts at zero when the connection is established.

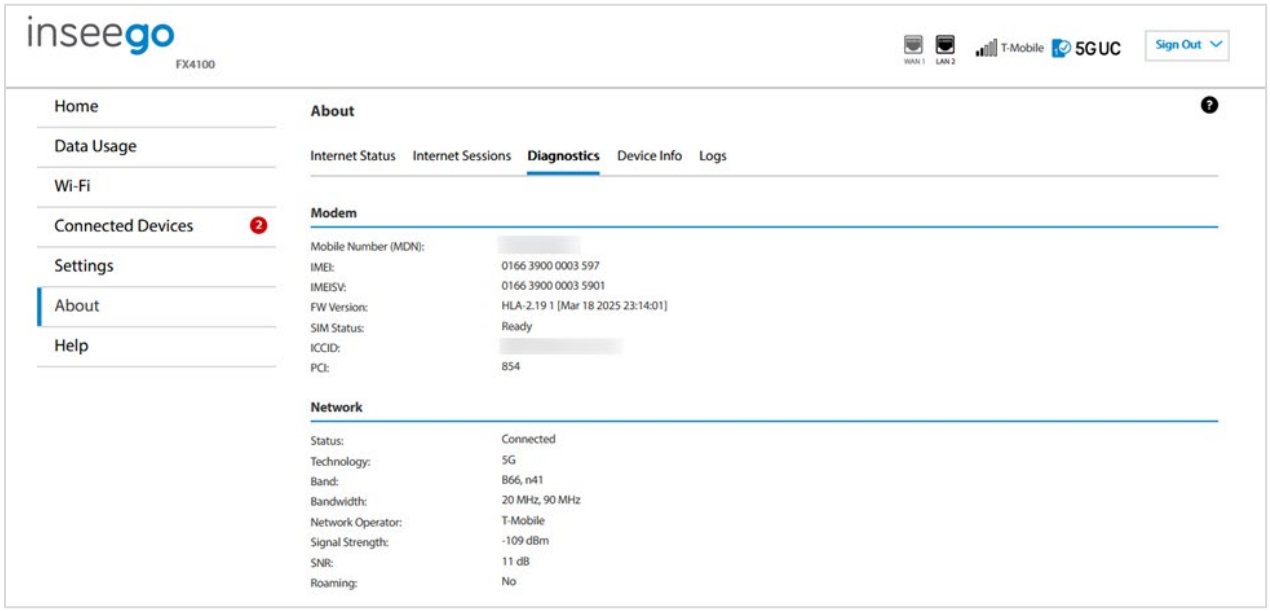
Total Data: The total amount of data for the internet session. This is the sum of Received Data and Transmitted Data.

IPv4 Address: The IP address for the session.

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

Diagnostics tab

This tab displays detailed information used solely for troubleshooting or technical support.



Modem

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

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

IMEISV: A combination of the IMEI and an approval number for this type of device.

FW Version: The version of the firmware (software) currently installed on your router.

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

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

PCI: The physical cell ID.

Network

Status: The status of the network.

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

Band: The band in use for the current connection.

Bandwidth: The bandwidth in use for the current connection.

Network Operator: The name of the Mobile Network Operator (MNO).

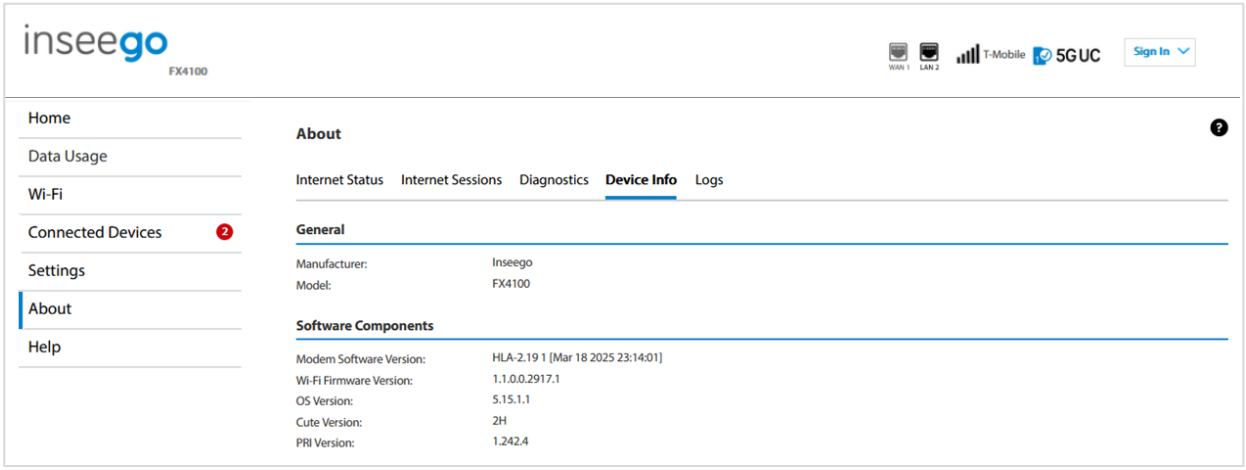
Signal Strength: The strength of the cellular signal (RSRP), measured in dBm. Higher absolute values indicate a stronger signal, for example: -80 dBm is a stronger signal than -90 dBm.

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

Roaming: Indicates whether roaming is on.

Device Info tab

Use this tab to view details about your FX4100 cellular router.



General

Manufacturer: Inseego.

Model: The model of this device.

Software Components

Modem Software Version: The version of software currently installed for the modem component.

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

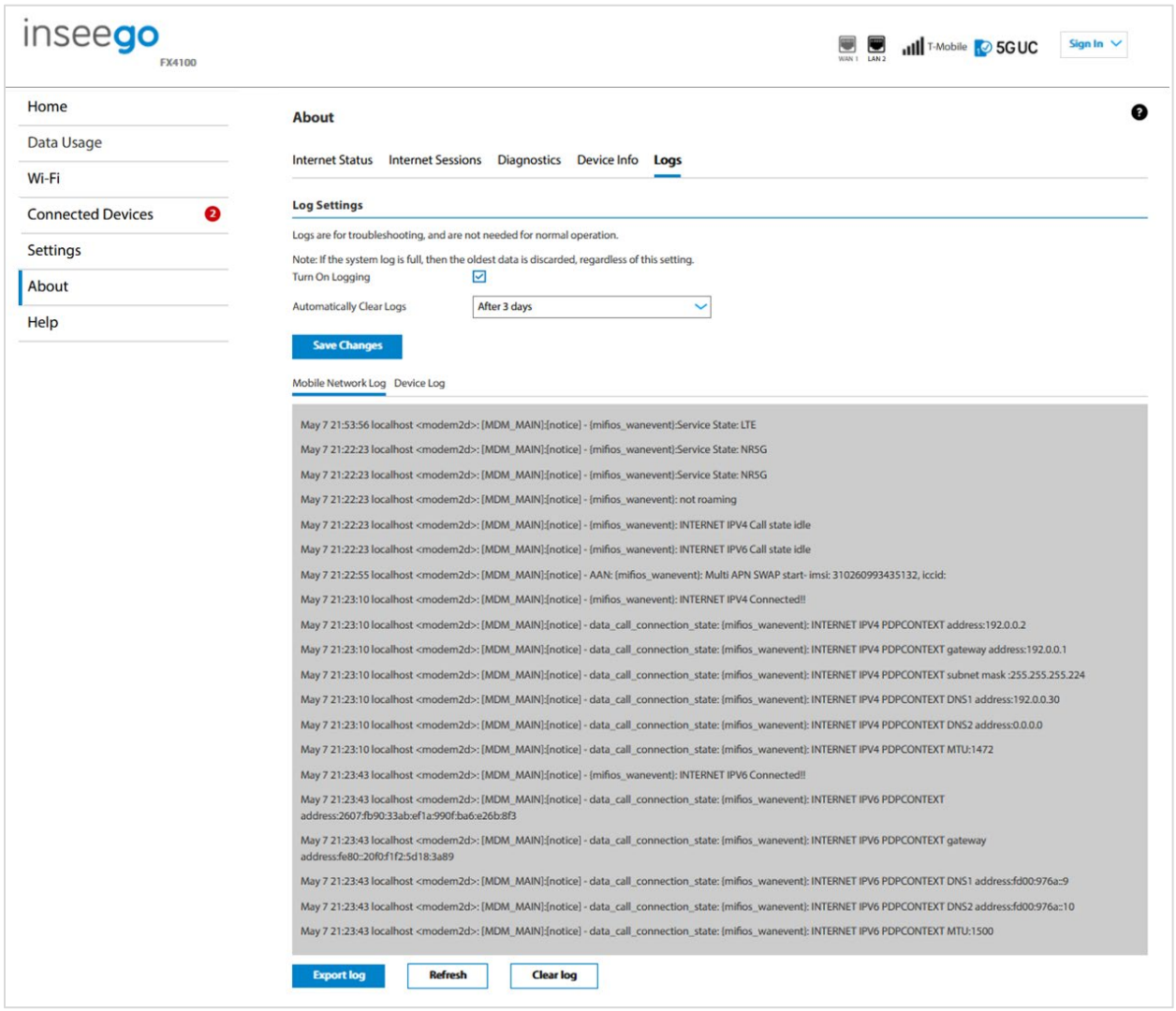
OS Version: The version number for the Operating System and its components.

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

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

Logs tab

Use this tab to view log information for troubleshooting.



Log Settings

Turn On Logging: Check this box to turn on logs as needed.

Automatically Clear Logs: Use the drop-down list to select when logs are cleared.
NOTE: If the log is full, the oldest data is deleted regardless of this setting.

Click **Save Changes** to enact changes.

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

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

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

Export log: Allows you to export log data.

Refresh: Updates the displayed log data.

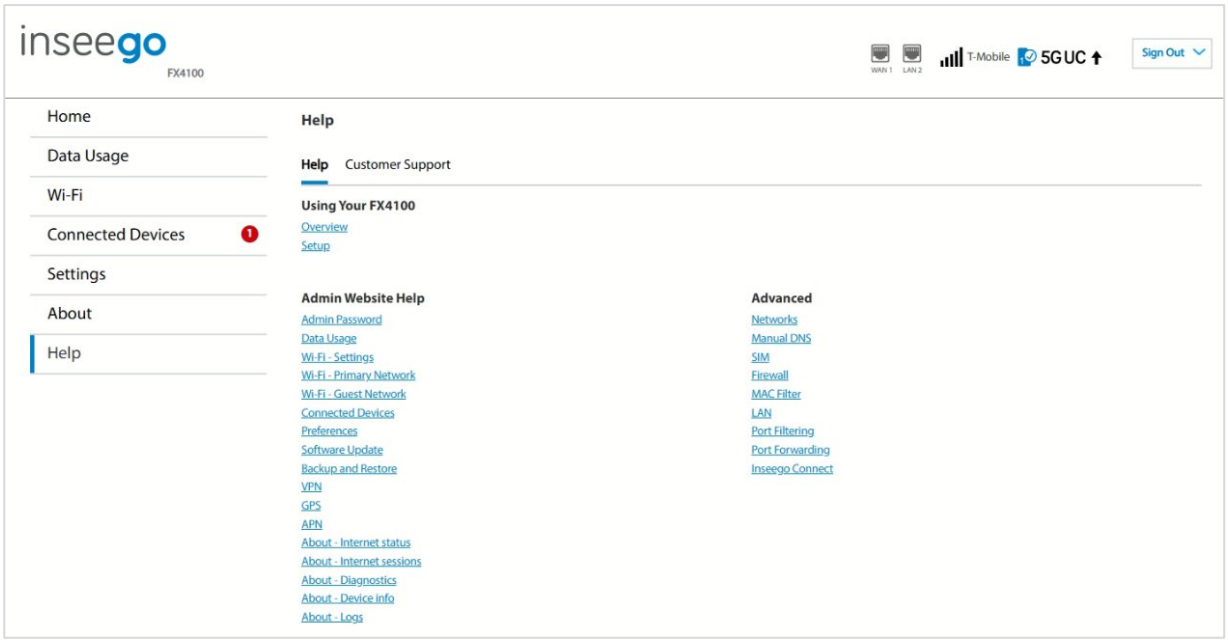
Clear log: Deletes all existing log data. This makes new data easier to read.

Getting support

For support, select Help from the Admin web UI side menu.

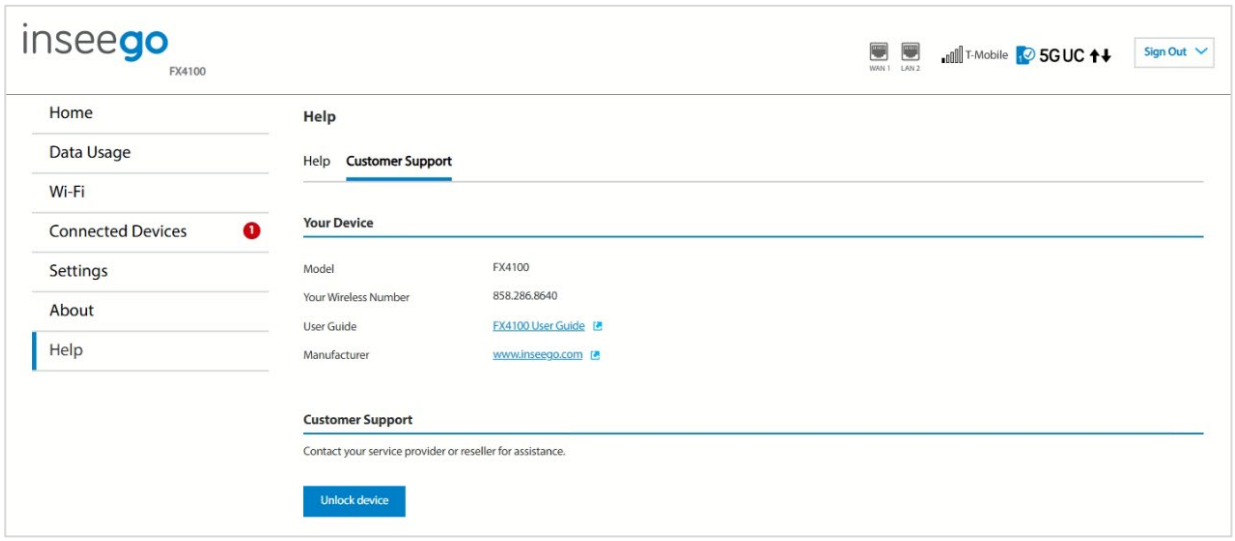
Help tab

This page provides links to help topics for every page of the Admin web UI and general topics useful for getting started with your router.



Customer Support tab

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



Your Device

Model: Model of the device.

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

User Guide: A link to this guide.

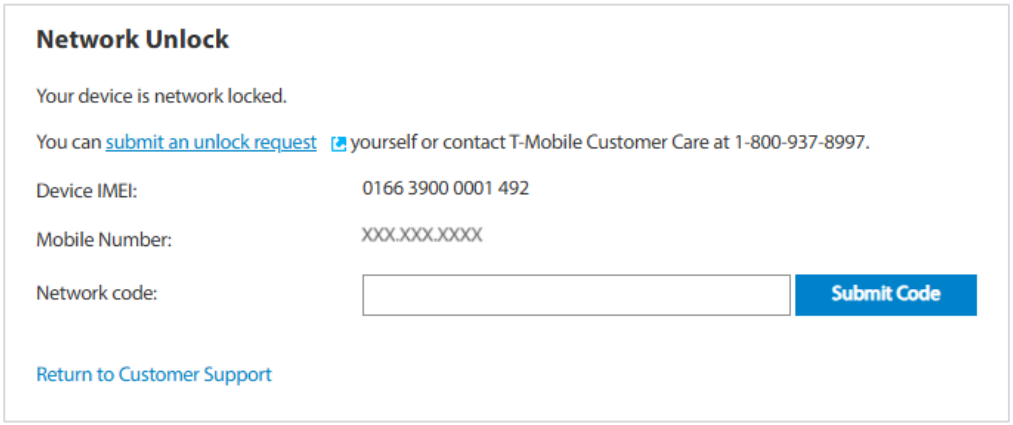
Manufacturer: A link to the Inseego website.

Customer Support

Contact your service provider or Account team for customer support.

Unlock/Lock device

Locked devices can only use the network currently provided by the service provider. To unlock a locked device, click **Unlock device**. The Network Unlock page appears:



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

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

3

Advanced settings

Overview

Advanced settings are intended for users with technical expertise in telecommunications and networking.

WARNING! Changing the Advanced settings may be harmful to the stability, performance, and security of the router.

Using advanced settings

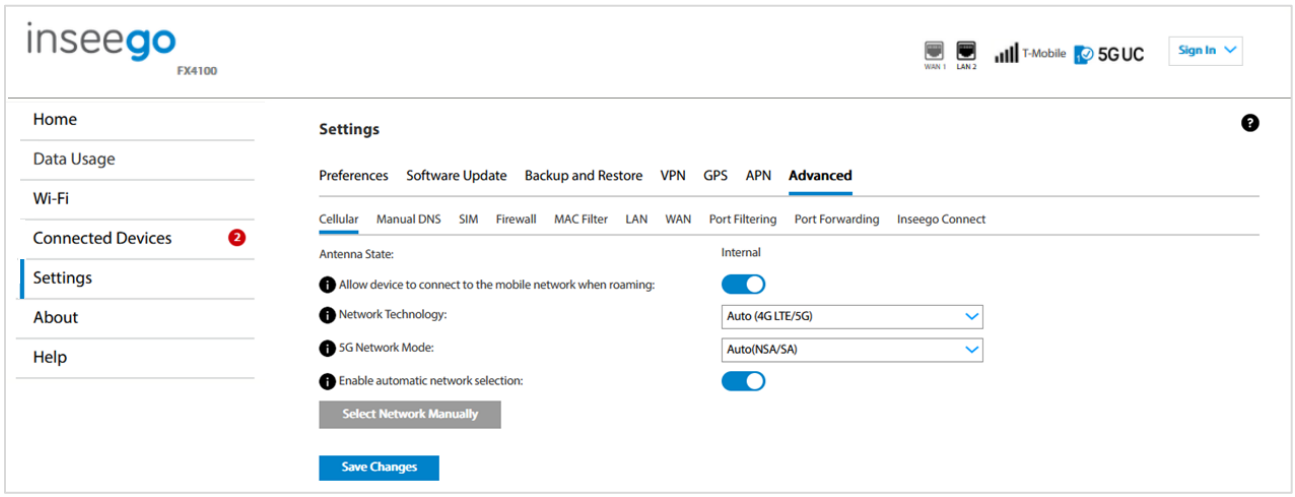
When you select the **Advanced** tab on the Settings page, a warning message appears. If you click **Continue**, the Network tab of the Advanced Settings page appears.

Advanced settings include:

- Cellular
- Manual DNS
- SIM
- Firewall
- MAC Filter
- LAN
- WAN
- Port Filtering
- Port Forwarding
- Inseego Connect
- HeartBeat Timer (Inseego Connect)

Cellular tab

Use this tab to set options for the cellular network.



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

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

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 drop-down to select standalone (SA) or non-standalone (NSA) 5G network modes.

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

Select Network Manually: You may wish to use this option if multiple networks are available, and you have a preference. Click the button to scan for available networks, then choose the preferred network. **NOTE:** This option is available only if **Enable automatic network selection** is off.

Click **Save Changes**.

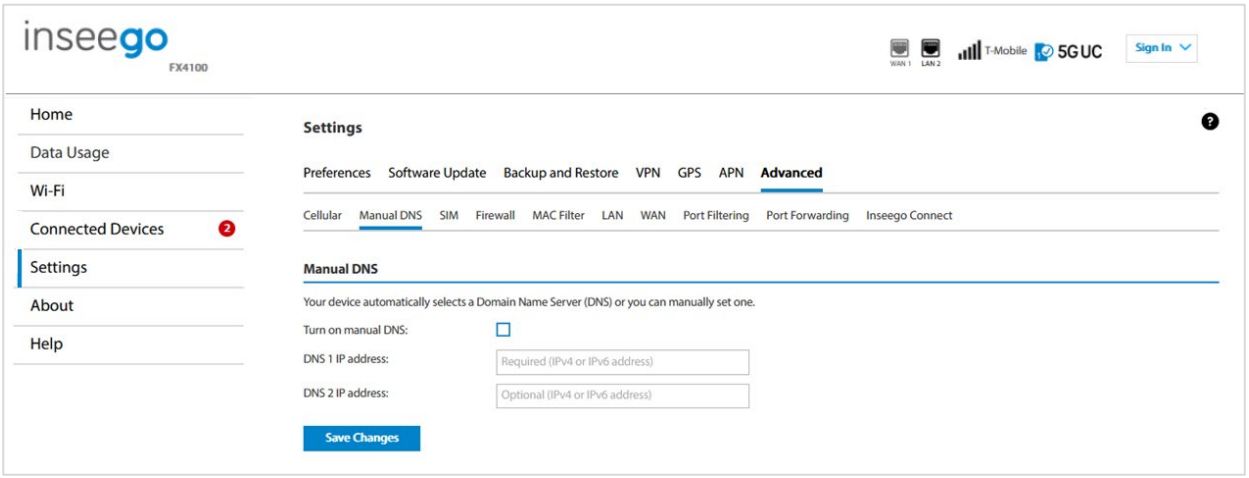
Manual DNS

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

- Manual DNS tab (Admin web UI)
- DNS Content Filtering (Inseego Connect)

Manual DNS tab

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



Manual DNS

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

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

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

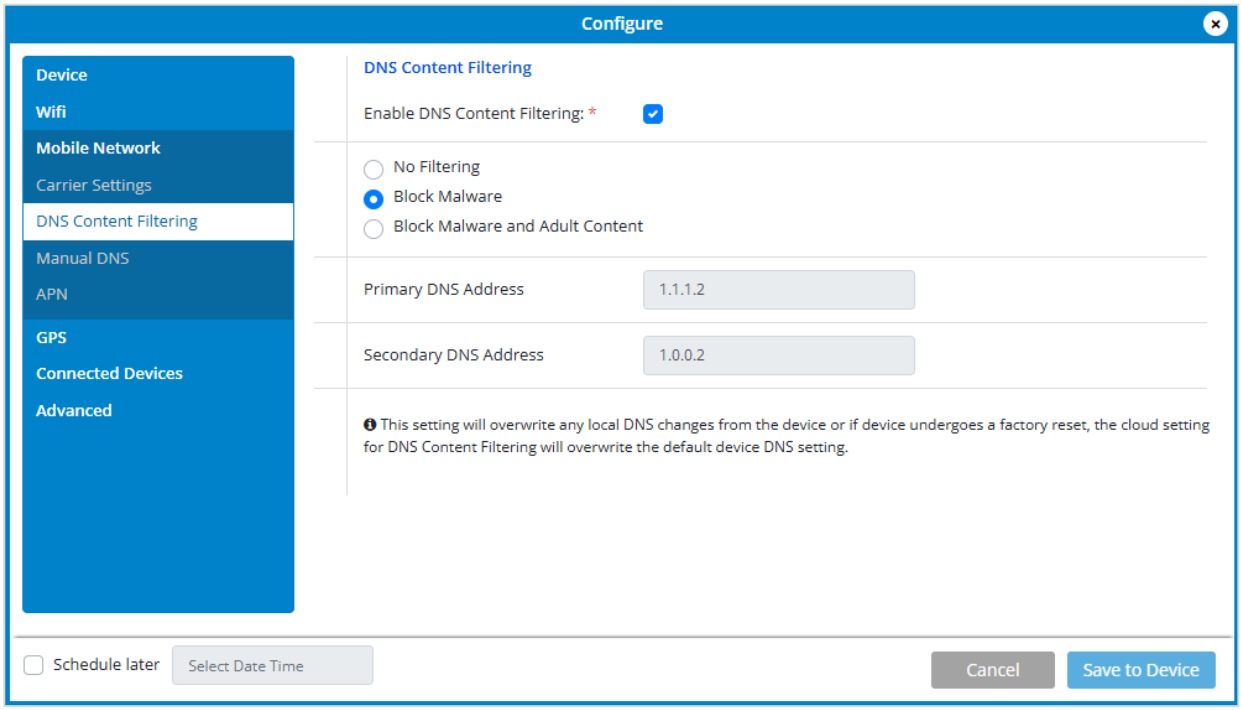
Click **Save Changes**.

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

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



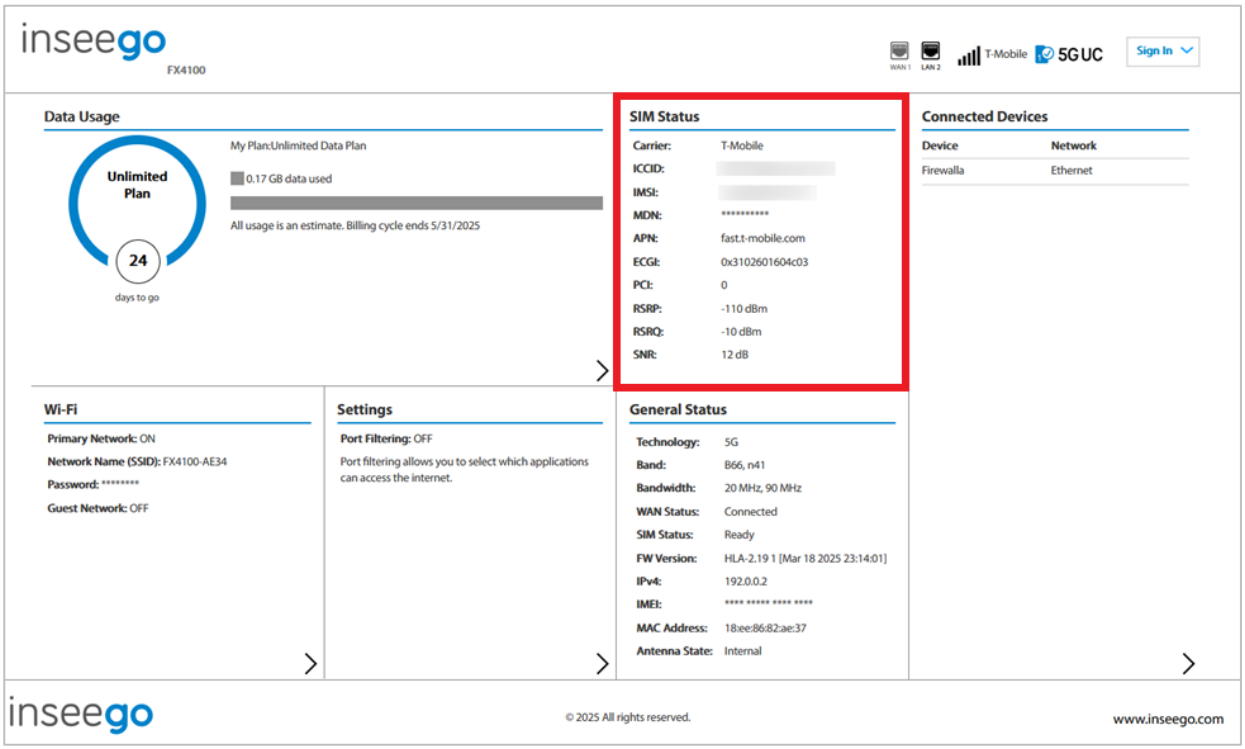
Enable DNS Content Filtering: Check this box to enable DNS content filtering.

Select the filter level (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 to Device**.

SIM

On the Admin Web UI Home page, the SIM Status panel shows SIM status information.



Carrier: The name of the service provider.

ICCID: The unique ID number assigned to the SIM card.

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

MDN: The phone number of your router.

APN: The access point name for your router.

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

PCI: The physical cell ID.

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

RSRQ: Reference Signal Received Quality. A calculated value from RSRP and RSSI that provides a measure of signal and interference.

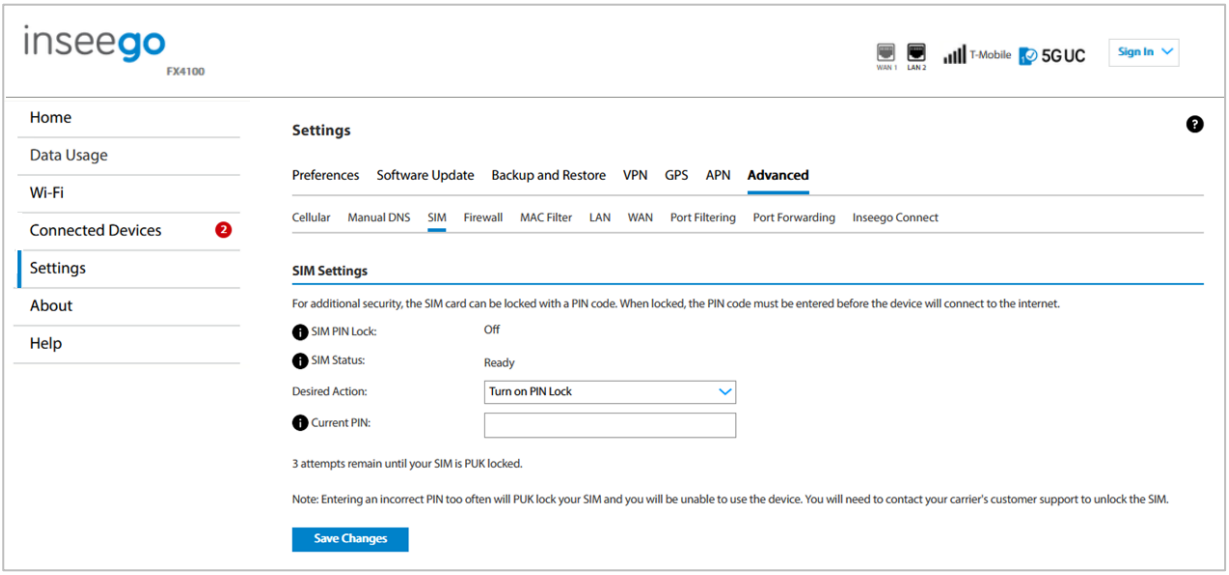
SNR: Signal to Noise Ratio. The ratio of signal power to noise power expressed in decibels. SNR is a positive value, and higher numbers are better.

To configure more system settings, select ›from a panel on the home page and then select **Settings** from the side menu and click the SIM tab.

SIM tab

The SIM card in your router can be locked using a PIN. If the SIM card is locked, you must enter the PIN before connecting to the mobile network. Once entered, the PIN is remembered until the next shutdown. You may also need to provide the existing PIN to change a SIM. The default PIN is available from your service provider.

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



SIM PIN Lock: Indicates whether the PIN lock feature is in use. If **ON**, the PIN lock has been turned on, and the SIM PIN must be entered to connect to the mobile network. If **OFF**, the PIN lock feature is not turned on and the SIM PIN is not required.

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

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

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

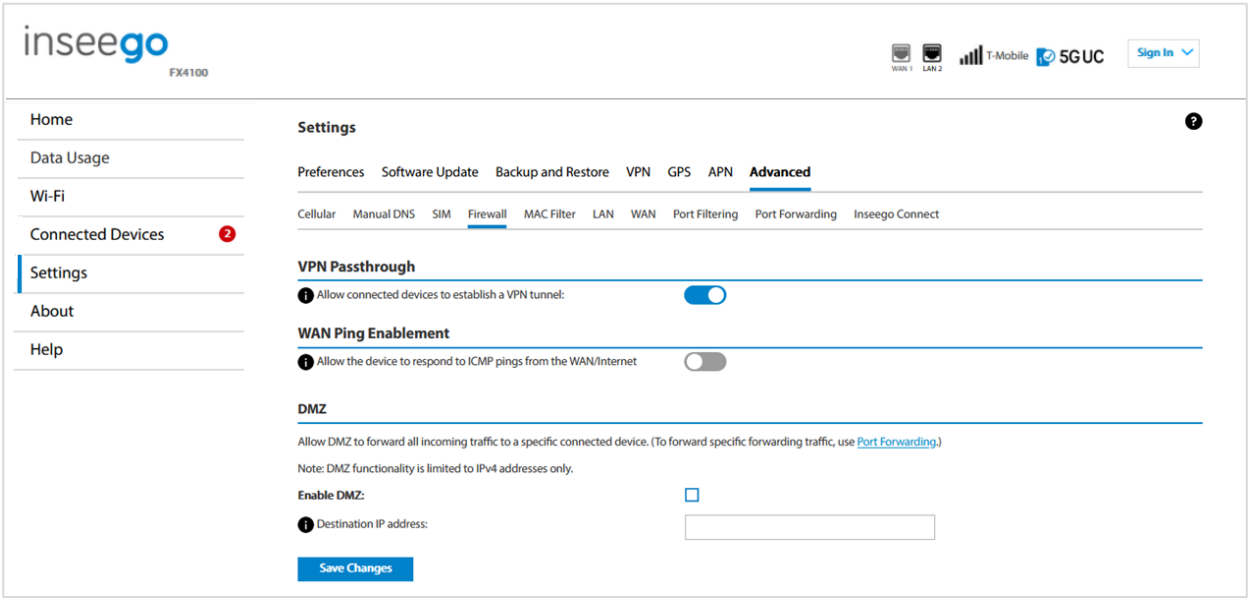
- **PIN Lock** - If the SIM is currently PIN locked, you are prompted to enter the PIN. **NOTE:** If an incorrect PIN is entered too many times, the SIM becomes PUK locked. A counter indicates how many incorrect entries will cause PUK lock. Once PUK locked, the PUK must be obtained from your service provider.
- **PUK Lock** - If the SIM is currently PUK locked, the only operation possible is to enter the PUK. **NOTE:** If an incorrect PUK is entered too many times, the SIM becomes permanently unusable. You will need to obtain a new SIM. A counter indicates how many entry attempts remain.
- **Turn on PIN Lock** - Sets the SIM so that entry of a PIN is required upon startup to connect to the mobile network. To perform this operation, you must enter the current PIN.
- **Turn off PIN Lock** - Turns off a PIN lock that was previously turned on so that entry of a PIN is no longer required to connect to the mobile network. To perform this operation, you must enter the current PIN.

Current PIN: Enter the current PIN.

Click **Save Changes**.

Firewall tab

The FX4100 cellular router firewall determines which internet traffic is allowed to pass between your router and connected devices and protects your connected devices from malicious incoming traffic from the internet. The firewall cannot be turned off. Use the Firewall tab to allow VPN Passthrough and/or designate a specific device to receive all traffic.



VPN Passthrough

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

WAN Ping Enablement

By default, the router will ignore 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 ON/OFF slider to **ON**.

DMZ

NOTE: 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 **Advanced > 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.

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

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

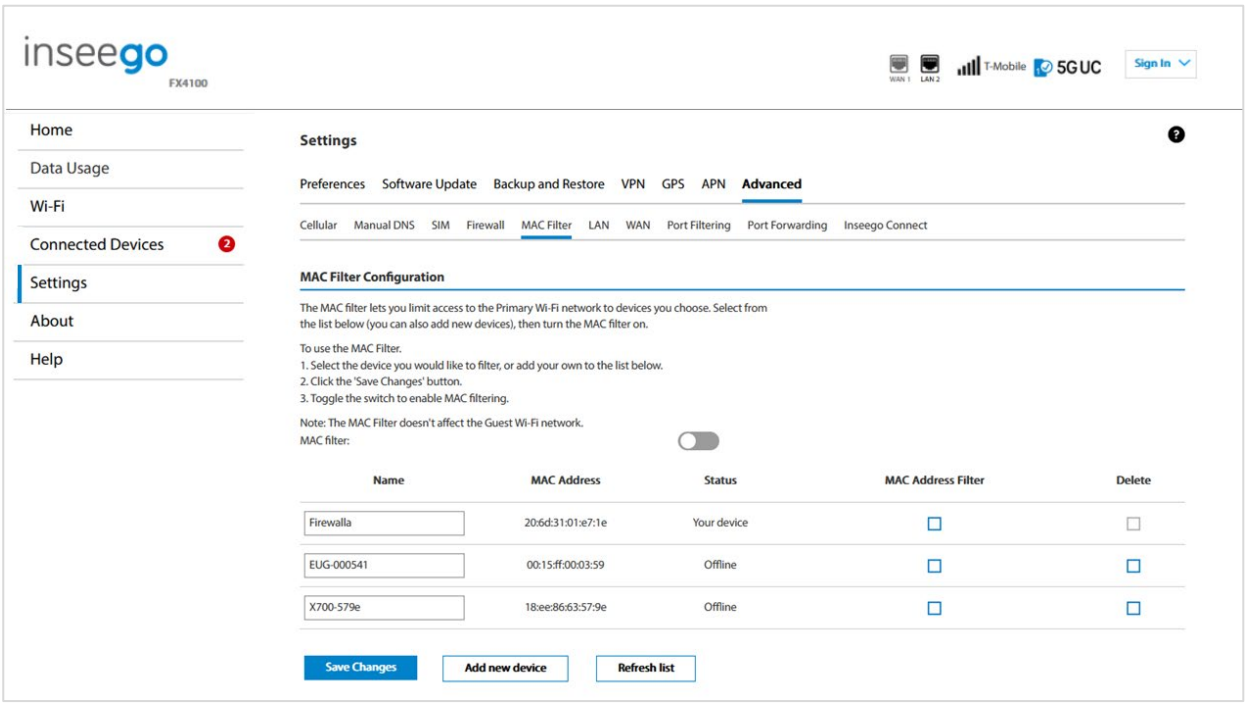
Destination IP address: Enter the IP address of the connected device you wish to become the DMZ device (the DMZ destination). **NOTE:** You can check the IP address of each connected device on the Connected Devices screen.

Click **Save Changes**.

MAC Filter tab

The MAC filter allows only selected devices to access the FX4100 cellular router network through DHCP. By default, MAC filter is turned off.

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



MAC Filter Configuration

To use the MAC filter, select the device(s) from the device list that you want to be allowed to connect to the network through DHCP and move the **MAC filter** ON/OFF slider to **ON**. Click **Save Changes**.

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

This list includes all devices currently connected to the router.

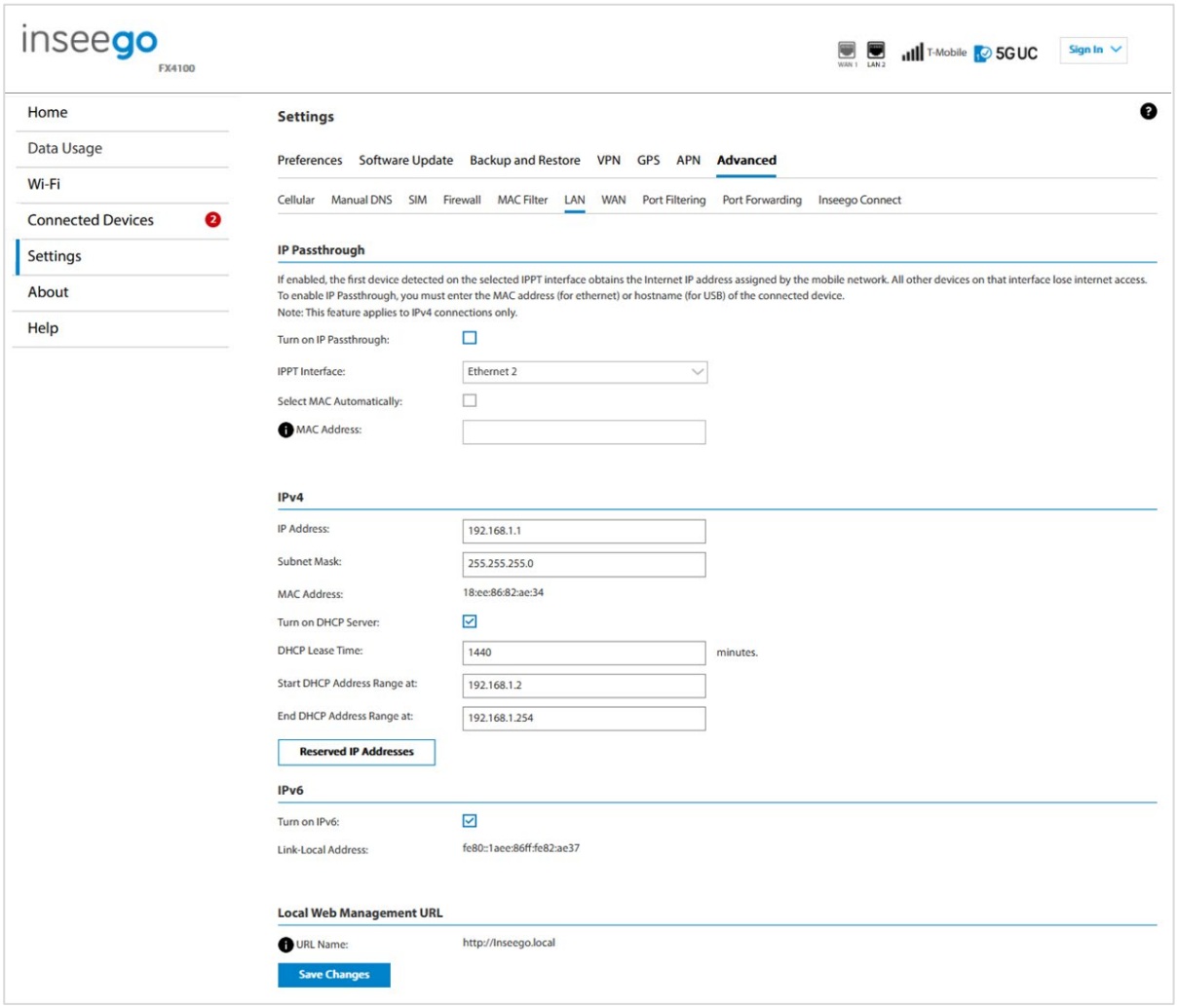
Add new device: Use this button to add a device to the device list, then enter the device name, MAC address, and choose whether to select the **MAC Address Filter** checkbox.

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

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

LAN tab

This page provides settings and information about the FX4100 cellular router 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 port to obtain the IP address assigned by the mobile network. IPPT allows you to enable a one-to-one connection to a host routing system. **NOTE:** When IP Passthrough is on, only one device 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

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

NOTES:

- Enabling IPPT will disable Wi-Fi from the router and disconnect 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 **Advanced > WAN** and change Ethernet WAN to LAN, or set Ethernet WAN to a lower priority than Priority 1.

IPPT Interface: Select an interface from the drop-down (Ethernet 1, Ethernet 2, or USB).

Hostname: When enabling IPPT on the USB interface, enter the hostname of the device connected for IP Passthrough or use **Select Hostname automatically**. This is the only USB-connected device that can obtain the IP address assigned to the mobile network. You can view the hostname on the Home or Connected Devices page.

MAC Address: When enabling IPPT on an Ethernet interface, enter the MAC address of the device connected for IP Passthrough or use **Select MAC automatically**. This is the only device connected to the selected Ethernet port that can obtain the IP address assigned to the mobile network.

IPv4

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, make sure to use the correct Subnet mask for the IP address range of the LAN IP address*.

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

Turn on DHCP server: This checkbox turns the DHCP Server feature on or off. This should be left checked. The DHCP server allocates an IP address to each connected

* 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).

device. **NOTE:** If the DHCP Server is turned off, each connected device must be assigned a fixed IP address.

DHCP Lease Time: The number of minutes in which connected devices must renew the IP address assigned to them by the DHCP server. Normally, this can be left at the default value, but if you have special requirements, you can change this value.

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

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

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.

IPv6

Turn on IPv6: Check the box if the connected device supports IPv6*. This enables IPv6 connected devices to make IPv6 connections to the internet.

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

Local Web Management URL

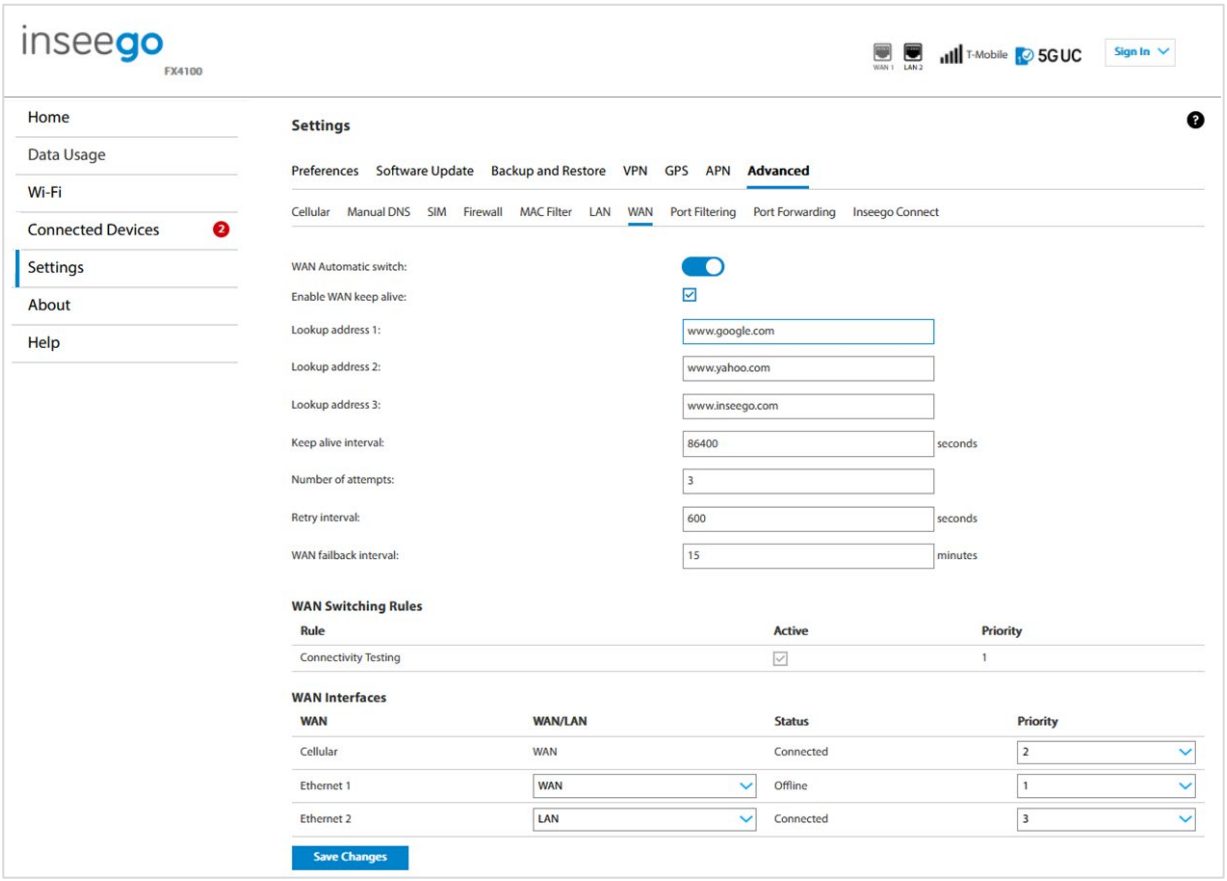
URL Name: The URL name used to access the FX4100 cellular router local web UI**.**

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

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

WAN tab

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



WAN Automatic switch: By default, automatic switching for WAN is enabled, which allows rerouting of network traffic to another connection if your primary connection fails.

Enable WAN keep alive: When this box is checked, keep alive verifies lookup addresses to check the internet connectivity on the WAN connection.

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

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

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

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

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

Retry interval: The number of seconds between verification retries. The default is 600 seconds.

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

WAN Switching Rules

When WAN automatic switching is enabled, WAN switching is determined by connectivity testing. To turn connectivity testing off, uncheck the Active box.

WAN Interfaces

Use this table to configure Ethernet WAN ports as WAN or LAN and to set a priority for your WAN interfaces.

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

WAN/LAN: Although Ethernet ports are labeled as WAN or LAN on the device, you can configure them to be either WAN or LAN. Use the drop-down to select WAN or LAN for your Ethernet interfaces. **NOTE:** When IP Passthrough is turned on, you cannot configure Ethernet ports as WAN.

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

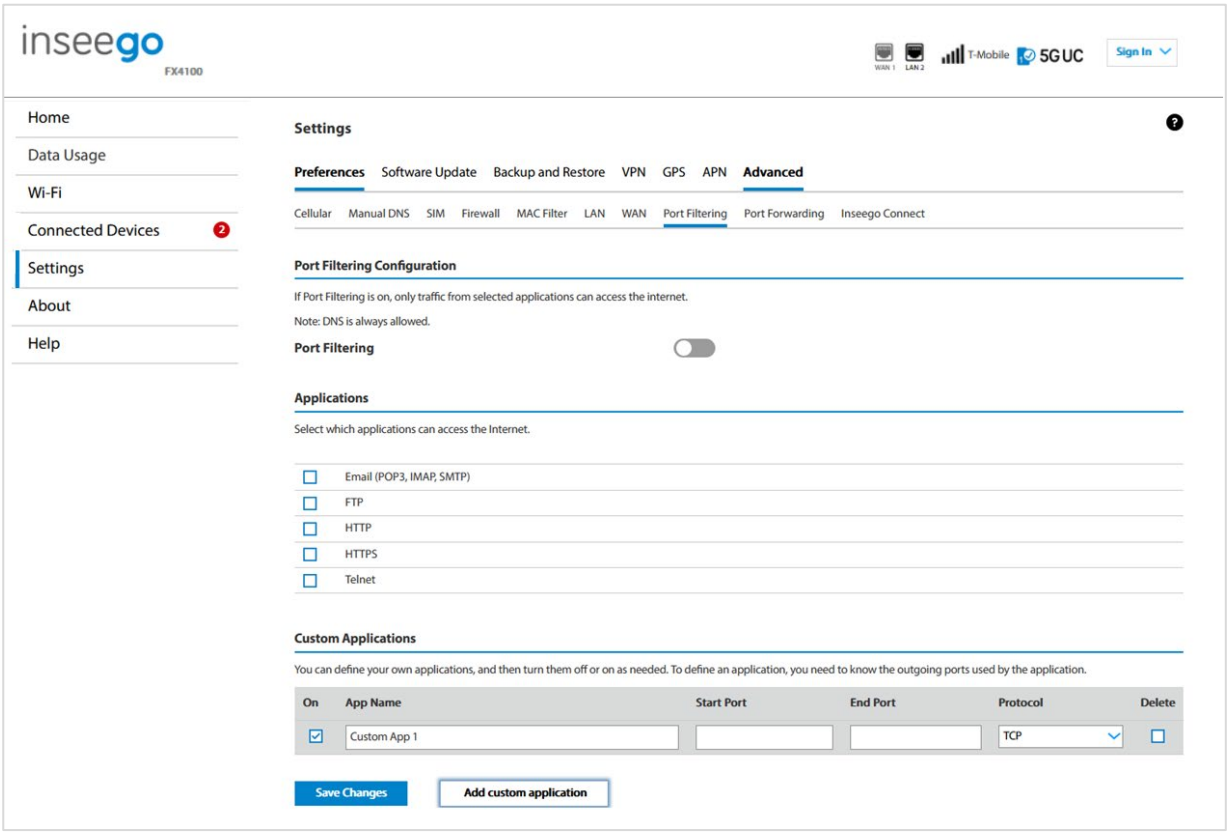
Priority: Use the drop-down to set a priority for each WAN interface.

Click **Save changes** to save new settings. A pop-up appears alerting you that your router will reboot.

Click **OK** to restart the device.

Port Filtering tab

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



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

Port Filtering Configuration

Port Filtering: To turn on port filtering, move the ON/OFF slider to **ON**. To turn off port filtering, so that any application can connect to the internet, move the slider to **OFF**.

Applications

Select the applications you want to be able to access the internet.

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

Application Name	Port	TCP*	STCP*	UDP*
Email				
POP3 POP3S	110 995	Yes Yes	No No	Assigned Yes
IMAP IMAPS	143 993	Yes Yes	No No	Assigned Assigned
SMTP SecureSMTP	25 465	Yes Yes	No No	Assigned 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

Custom Applications

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

On: Check this box if you want the new application to be able to access the internet.

App Name: Enter a name for the custom application.

Start Port: Enter the beginning of the range of port numbers used by outgoing traffic for the custom application being added.

End Port: Enter the end of the range of port numbers used by the application.

NOTE: If the application uses a single port instead of a range, type the same value for both the **Start Port** and the **End Port**.

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

Delete: Check this box to delete a custom application. **NOTE:** Click on the Port Filtering tab again to remove deleted custom applications from view on the screen.

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

---

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

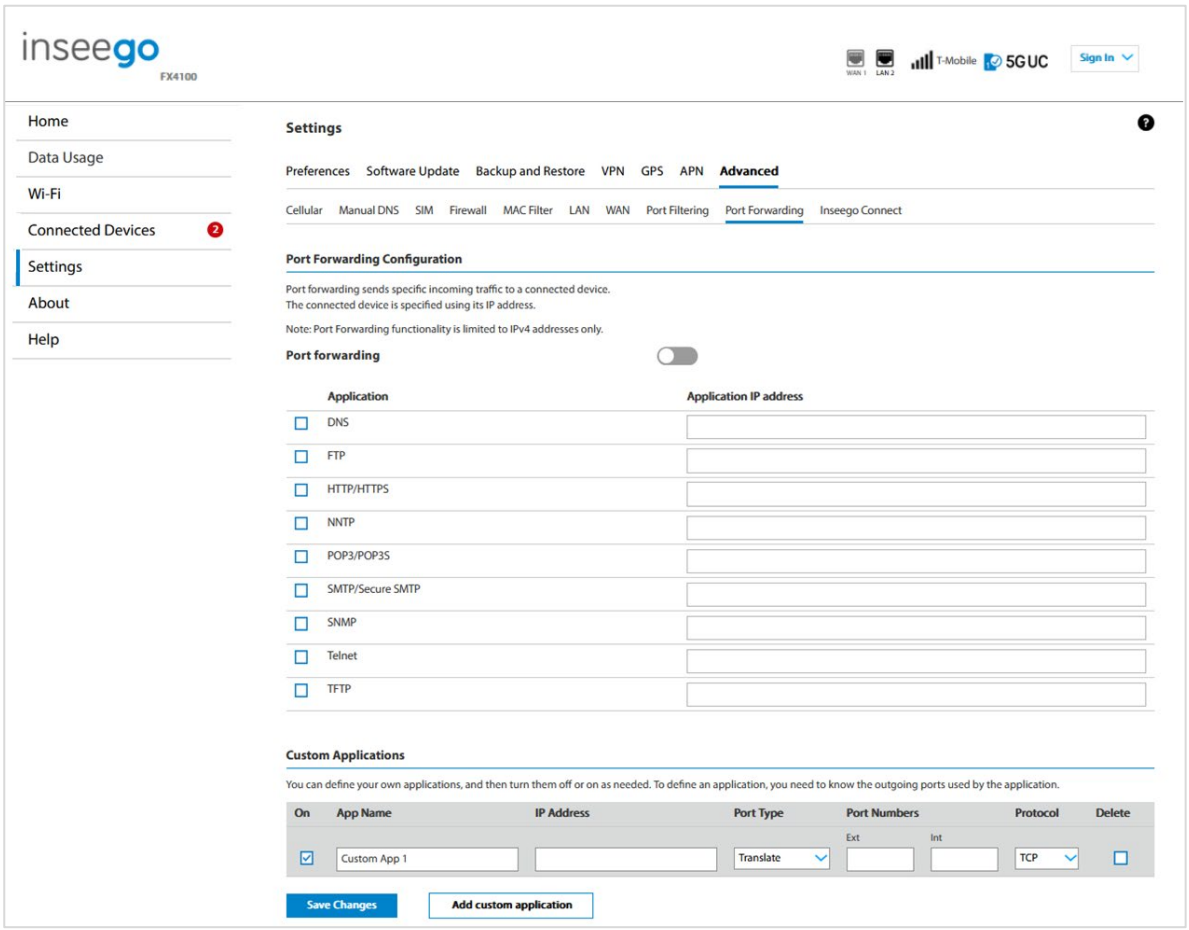
Port Forwarding tab

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

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

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

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



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

Port Forwarding Configuration

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

Applications

Check the box next to each Port Forwarding application that you want to allow.

To forward all inbound WAN traffic on a specific port to a single LAN client, enter the IP address of the target device in the **Application IP address** field.

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

Application Name	Port	TCP*	STCP*	UDP*
DNS	53	Yes	No	Yes
FTP control (command) 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.

Custom Applications

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

On: Check this box if you want the new application to be able to access the internet (enabling port forwarding).

App Name: Enter a name for the custom application.

IP Address: If you want to limit service for the application to a single connected device, enter the IP address of the target device. To find the IP address of a device, go to the Connected Devices page. **NOTE:** To ensure the device you are forwarding to does not have a different IP address after a reboot, either statically assign the IP address on the client device or set up a DHCP reservation.

Port Type: Use **Translate** as the port type.

Port Numbers: Use **Ext.** and **Int.** to specify ports to be forwarded. **NOTE:** To forward inbound traffic to the same port on a client device, enter the same port number in both **Ext.** and **Int.** You can also use translate ports to send traffic to a different port on the client device. For example, instead of having inbound traffic on port 1234 forward to port 1234 of the client device, you can have it forward to port 5678.

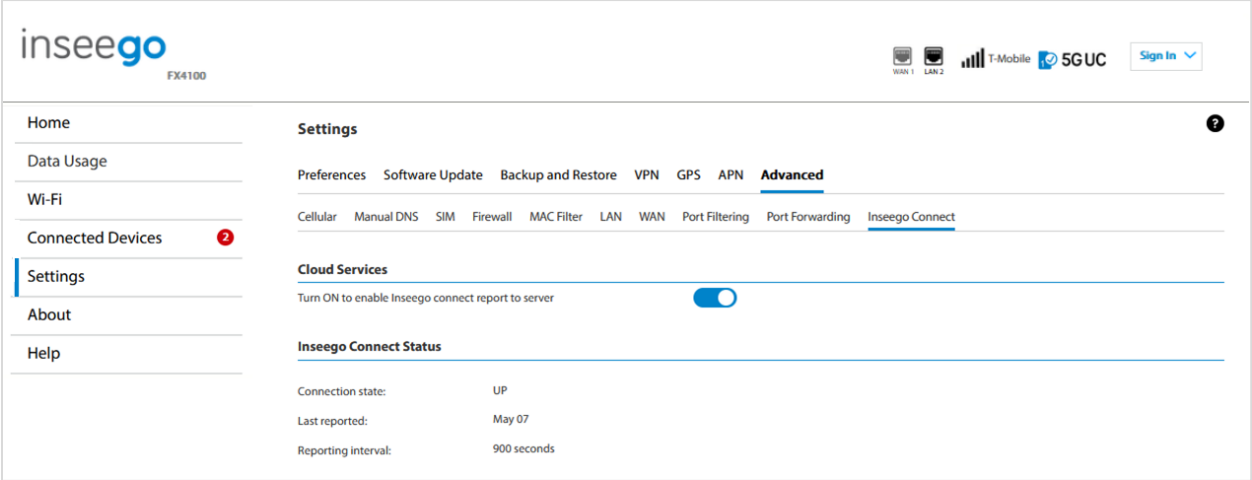
Protocol: Select the protocol used by the port range from the drop-down list (TCP, UDP, or both).

Delete: Check this box to delete a custom application. **NOTE:** Click on the Port Forwarding tab again to remove deleted custom applications from view on the screen.

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

Inseego Connect tab

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



Cloud Services

By default, the connection to Inseego Connect is **ON**. Slide the ON/OFF slider to **OFF** if you wish to disable the connection.

Inseego Connect Status

Connection State: The status of the Inseego Connect connection.

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

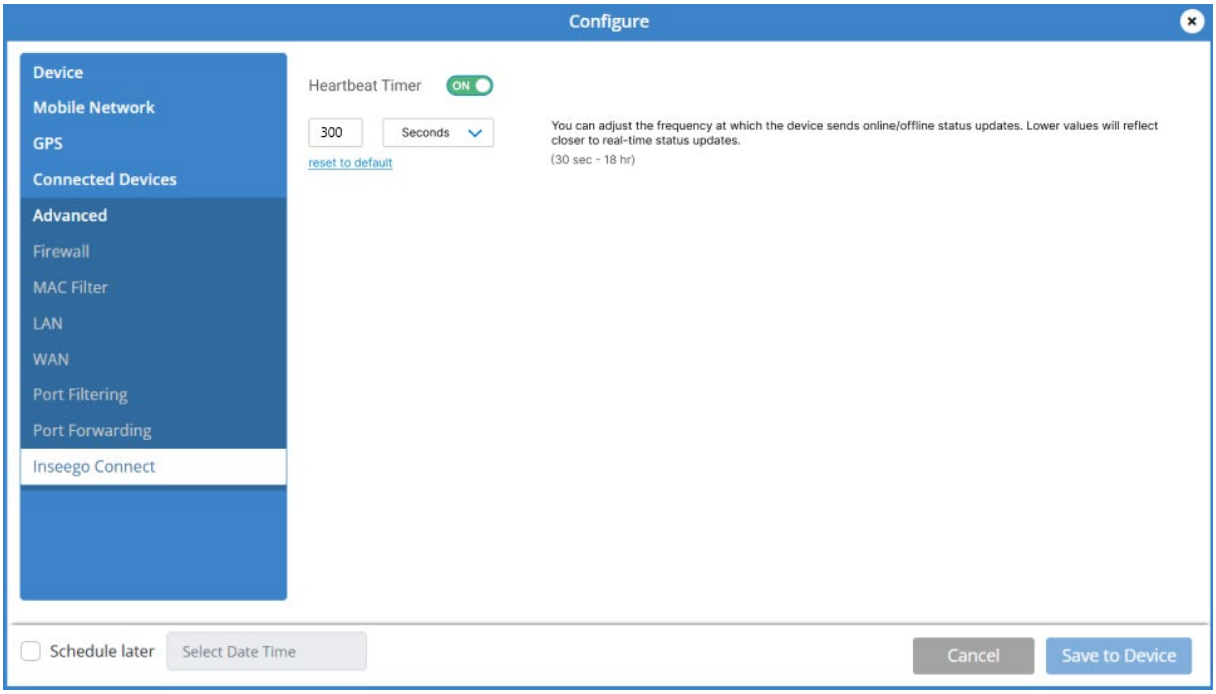
Last Reported: The time when the router last sent a packet to Inseego Connect servers.

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.

Heartbeat timer (Inseego Connect)

Your FX4100 cellular router sends a lightweight heartbeat packet to Inseego Connect at a regular interval to indicate that the device is online. The default interval is 300 seconds (5 minutes).

You can adjust the frequency of the heartbeat timer in Inseego Connect on the Advanced > Inseego Connect configuration screen. All T-Mobile owned Inseego FX devices come with the option of purchasing the Inseego Connect Add-on. Please work with your Account team to order the Inseego Connect Add-on, which provides Manager access.



HeartBeat Timer: By default, the heartbeat timer is **ON**.

Select the amount of time desired for the heartbeat timer interval.

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

4

Accessories

Overview

The following accessories are available for use with your FX4100 cellular router. Contact your reseller for more information about accessories.

- External antennas
- External power bank
- PoE to USB-C adapter
- Inseego Wavemaker mesh Wi-Fi X700

Using external antennas

Your FX4100 cellular router is equipped with four internal antennas. In addition, the device has two external full spectrum cell SMA ports (0.6-6 GHz each) to support two external antennas. **NOTE:** Contact your Account team for more information about external antennas.

Connecting external antennas (optional)

To use external antennas:

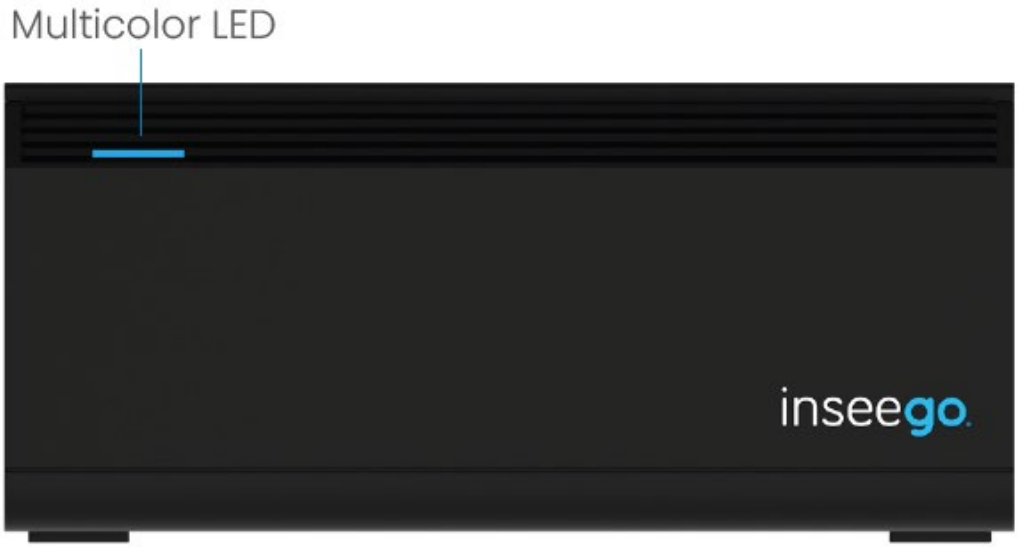
1. Remove the SIM/EXTERNAL ANTENNAS cover on the back of the router.

2. Finger tighten your external antennas to the CELL1 and CELL2 external antenna ports.
3. Set the switch to **EXT.ANT.ON**. When enabled, each external port supports the full cellular frequency range of 0.6-6 GHz. Two of the internal antennas are disabled. The other two internal antennas remain active. An antenna icon appears on the main screen of the device display.

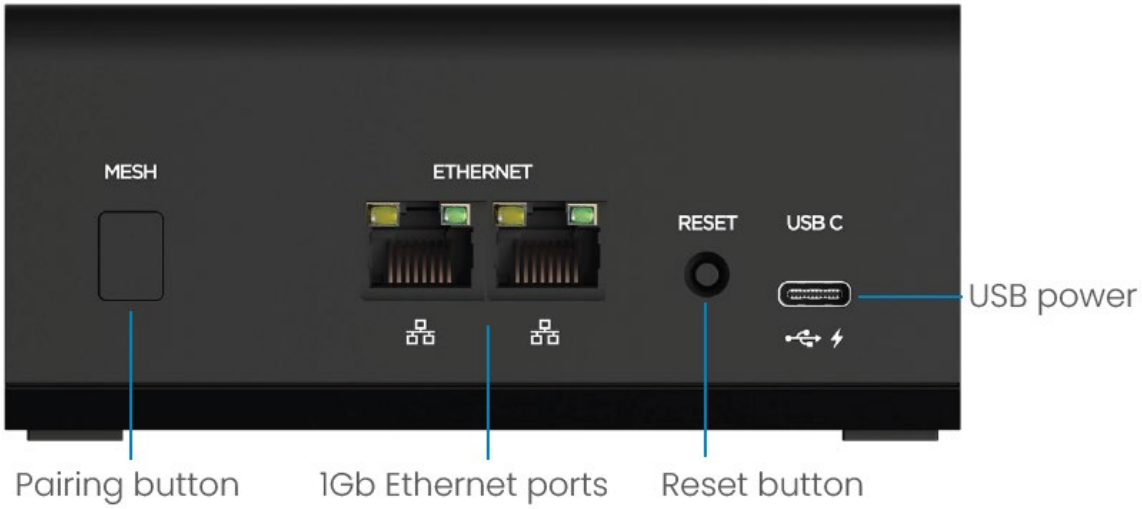
Using Inseego Wavemaker mesh Wi-Fi X700

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 FX4100 cellular router is compatible with Inseego Wavemaker mesh Wi-Fi X700. You can connect up to three mesh nodes to one FX4100.

Device front



Device back



Indicator LEDs

The front of the mesh Wi-Fi X700 has a device status LED that changes colors and blinks or glows solid to communicate current states for the mesh node.

LED color	Operation	Meaning
Blue	Solid Blinking	Mesh on, great signal Pairing
Green	Solid Blinking	Mesh on, good signal Ready to pair
Yellow	Solid	Mesh on, poor signal
White	Solid Blinking	Firmware update is in progress Mesh is booting up
Red	Solid Blinking	Mesh issue/not connected Firmware update failed

The Ethernet ports on the back of the mesh node also have indicator LEDs.

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

Pairing your X700 mesh node

To pair an X700 mesh node to your FX4100 cellular router:

1. Power on the FX4100.
2. Power on the X700 by plugging the USB-C cable into the USB power port. Plug the other end into any of the following:
   - AC adapter (provided)
   - USB-powered hub
   - USB host device

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

3. Pair the X700. You can pair your X700 with an Inseego FX4100 cellular router using Wi-Fi or Ethernet.

   Pairing with Wi-Fi

   To initiate Wi-Fi pairing, use the Admin web UI or the interactive device display on the FX4100.

   Using the FX4100 device display

   - Press the **device display button** repeatedly until you see **Wi-Fi Mesh: Hold button to add**.
   - Press and hold the **device display button**.
   - When prompted by the display, press the **Mesh button** on the X700.
   - The LED on the X700 and the router blink blue while pairing. When the LEDs are solid, pairing is complete.

   Using the Admin web UI:

   - Go to http://192.168.1.1 to access the Admin web UI for the FX4100. Navigate to **Wi-Fi > Mesh**.
   - Press the **Mesh button** on the X700.
   - Within 30 seconds, click **Add Node** on the UI Mesh page.
   - The LED on the X700 and the router blink blue while pairing. When the LEDs are solid, pairing is complete.

   Pairing with Ethernet

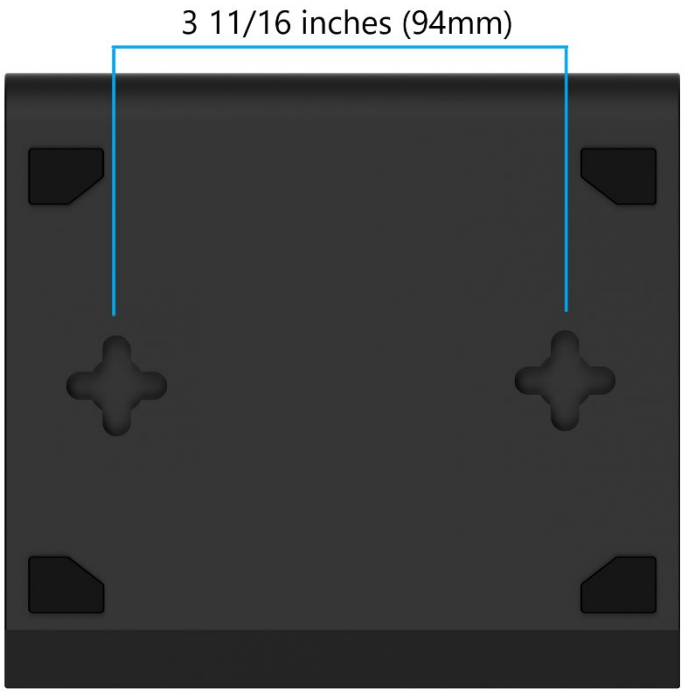
   - Connect an Ethernet cable from the X700 to the FX4100.
   - Pairing is automatic. The LED on the X700 blinks blue while pairing. When pairing is complete the LED is solid.
   - When you disconnect the Ethernet cable, the X700 remains paired via Wi-Fi.

Find a location for your X700 mesh node

Adjust the location of the X700 using the LED color as a guide. Solid blue indicates a great signal. Solid green indicates a good signal.

Mounting your X700 (optional)

The X700 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 of 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.

Connecting wireless devices

Connecting wireless devices to your FX4100 cellular router through the mesh Wi-Fi X700 node looks and feels the same as connecting directly to the router. Follow the instructions for connecting a device for the first time on page 18.

Managing your X700 mesh node

You can manage your X700 mesh node(s) through the FX4100's Admin web UI or Inseego Connect settings.

Use **Wi-Fi Settings > Mesh** to view all mesh nodes paired with your FX4100, add or remove a mesh node, or reboot a mesh node. You can also see the connected devices for each mesh node.

Use the **Connected Devices** page to edit how the mesh node name appears in the UI and view more details on connected devices. You can also block or unblock devices from internet access.

You can monitor mesh nodes with the Inseego Mobile app.

Resetting your X700 mesh node

To **reboot** your X700:

- Press the **reset** button for one second.

To perform a **factory reset** (removes pairing):

- Press and hold the **reset** button for five seconds.

5

Troubleshooting and support

Overview

When properly installed, the FX4100 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 FX4100 cellular router.

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

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

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

The device status LED is switching from blue to green

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

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

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

No, the FX4100 cellular router is designed to connect to the strongest signal available. You can set the network technology and 5G network mode using **Settings > Advanced > Cellular**.

I cannot access the Admin web UI

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

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

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

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

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

  Solution: Use the http://192.168.1.1 URL.

My router is getting slow speeds/low throughput

- **Reason:** Signal strength is the most likely cause of slow speeds/low throughput. **NOTE:** The FX4100 cellular router is configured by default to use the best connection available, so low throughput is rarely related to configuration.

  Solution: Check the signal strength reported by your router:

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

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

The device status LED is blinking red

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

  Solutions:

  Try the following:

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

My older device cannot connect

If you can see other networks, but not the network name for your FX4100 cellular router:

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

  Solution: Set your 2.4 GHz band to **Wi-Fi 4 802.11 bgn**:

  1. Access the Admin web UI and navigate to **Wi-Fi > Settings**. Under **2.4 GHz Band Settings**, use the drop-down to change the **Wi-Fi Standard** to **Wi-Fi 4 802.11 bgn**.
     NOTE: This allows older devices to connect on the 2.4 GHz band but leaves the 5 GHz band in multi-mode to allow newer devices the fastest available connection.
  2. Click **Save Changes**. Your router will reboot, and the network name should be visible on all devices.

If you can see the network name, but cannot connect a device to your FX4100 cellular router:

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

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

  1. Access the Admin web UI and navigate to **Wi-Fi > Primary Network**. In the **Security** drop-down, select **WPA/WPA2 Mixed Mode**.
  2. Click **Save Changes** and **Confirm**. Your router will reboot, and all devices should be able to connect.

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

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

  Solution: Change your Wi-Fi password.

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

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

- **Reason:** In rare cases, a Wi-Fi device may have issues with the same SSID being used on both 5GHz and 2.4 GHz bands.

  Solution: Disable the 5 GHz band.

  1. Access the Admin web UI and navigate to **Wi-Fi > Settings**. Uncheck **5 GHz** and use only **2.4 GHz**.
  2. Click **Save Changes**. Your router will reboot, and your device should be able to connect.

My connecting device is not obtaining a valid IP address

There are several possible reasons your connecting device is not obtaining a valid IP address:

- **Reason:** The DHCP server has been turned off.
  If IPPT is not enabled, the DHCP server provides IP addresses. If the DHCP server is turned off, no IP addresses can be provided.

  Solutions:

  Reset your router to factory settings, see “Resetting your router” on page 22.
  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 FX4100 cellular router, but if you have connected a succession of devices to your router in a short period of time, you may have used up all the IP addresses available.

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

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

  Solution: Contact your service provider for assistance.

My connected device cannot connect to Fortinet VPN

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

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

I cannot get streaming platforms to work with my router

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

  Solution: Contact your service provider for assistance.

Do I need a signal amplifier or booster?

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

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

Does the USB port support RNDIS?

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

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

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

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

Technical support

IMPORTANT: Before reaching out for support, be sure to restart both your connected device and your router and ensure that your SIM card is inserted correctly.

Customer service and troubleshooting
Contact your service provider for assistance.

More information
Documentation for your FX4100 cellular router is available online. Go to go.inseego.com/fx4100. Or, from the Admin website, select **Help > Customer Support**.

Vulnerability disclosure policy

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

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

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

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

6

Product specifications and regulatory information

FX4100 product specifications

X700 product specifications

Regulatory information

Product certifications and supplier's declarations of conformity

Wireless communications

Limited warranty and liability

Safety hazards

FX4100 Product specifications

Device

Name:	5G cellular router FX4100
Model:	FX4120
Regulatory:	FCC (US)
Certifications:	GCF, PTCRB, FIPS-2*, Wi-Fi Alliance, REACH, RoHS, UL 2710†
Power:	- 24W (12V, 2A) AC power adapter (provided) - USB-powered hub - USB-powered delivery device
Dimensions:	6.6" x 4.1" x 2.0" (167mm x 104mm x 52mm)
Weight:	23oz (650g)
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 LAN/WAN (1 GbE) 1x USB 3.1 Type C (data and power) 2x external full spectrum cell SMA ports (0.6-6 GHz each)
SIM:	1x 4FF Nano SIM
Module:	Inseego RM4210
Chipset:	Qualcomm® Snapdragon™ SDX72
Location:	Standalone GPS Internal antenna
Indicator LEDs:	Device status Cellular status Wi-Fi status
Device display:	Interactive device display for info, alerts, mesh pairing, and FOTA

* See https://inseego.com/resources/blog/what-is-fips-140-2-why-is-it-important/.

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

Network connectivity*

5G NR with SA/NSA	
5G sub-6 GHz	
4x4 MIMO 5G sub-6 GHz	
4G LTE Cat 20	
4x4 MIMO 4G LTE	
256 QAM sub-6 GHz	
Bands	**5G sub-6:** n2, n5, n12, n25, n26, n41, n48, n66, n71, n77 **4G LTE Cat 20:** 2, 4, 5, 12, 25, 26, 41, 48, 66, 71

Wi-Fi

Wi-Fi 7 with 2x2 MU-MIMO
802.11be with EasyMesh & EasyConnect standards
Simultaneous dual-band Wi-Fi
Full power AP Wi-Fi (~30dBm) with mesh
Primary and guest networks
Supports up to 128 simultaneous Wi-Fi enabled devices

Remote management

Inseego Mobile app (when registered with Inseego Connect)
Inseego Connect device management
Cloud API support through Inseego Connect Advanced
FOTA management and scheduling

* Data plan required. Coverage subject to network availability.

Software and security

IPv4 and IPv6
IPsec VPN and OpenVPN
VPN passthrough
IPPT and NAT mode
Port forwarding and filtering
MAC filtering
Content filtering
Periodic reboot
Seamless failover
WAN management
Secure boot/root of trust
WPA2/WPA3 authentication
Encrypted configuration backup/restore
Advanced firewall
Anti CSRF (OWASP)
Multi-link operation (MLO)
Wireless and wired mesh pairing
Wireless and wired mesh backhaul

X700 Product specifications

Device

Name:	Mesh Wi-Fi X700
Model:	X702
Regulatory:	FCC (US)
Certifications:	GCF, PTCRB, Wi-Fi Alliance, REACH, RoHS
Power:	12V@2.5A (+/- 5%)
Dimensions:	4.6" x 4.1" x 2.0" (117 x 104 x 52 mm)
Weight:	16.4oz (465g)
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)
Processor:	Multi-core processor with 1GB RAM + 1GB Flash or more
Ports:	2x LAN/WAN (1 GbE) 1x USB 3 Type C (data and power)
Indicator LED:	Device/signal status

Wi-Fi

2 x 2 dual-band Wi-Fi 6
2 x 2 2GHz 2 x 2 5GHz
Full power AP Wi-Fi (~30dBm, including antenna gain)
160 MHz bandwidth for 5GHz radio (80 MHz for router link and 80 MHz for client link)
Options for shared or different SSIDs with primary router
Support for 64 clients per radio

Regulatory information

Federal Communications Commission Notice (FCC – United States)

FCC ID: PKRISGFX4120, Contains FCC ID: PKRISGRM4210
FCC ID: PKRISGX702

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.

Cellular external antenna considerations for FX4120:

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

External antenna port	4G band	5G band	Max allowable antenna gain (dBi)
CELL1	B71	n71	6.9
CELL1	B12	n12	7.6
CELL1	B17	-	7.6
CELL1	B5	n5	8.4
CELL1	B26	n26	8.4
CELL1, CELL2	B4	-	4.5
CELL1, CELL2	B66	n66	4.5
CELL1, CELL2	B2 B25	n2 n25	6.5
CELL1, CELL2	B38	n38	8.0
CELL1, CELL2	B41	n41	5.5
CELL1, CELL2	-	n77	3.0
CELL1, CELL2	-	n78	3.0
CELL1, CELL2	B48	n48	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 FX4100 device, or failure of the FX4100 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 FX4100 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.