USER GUIDE

inseego

Inseego Wavemaker™
5G indoor router FX3100

INSEEGO COPYRIGHT STATEMENT

© 2023 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 Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp.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: 14965414 Rev 1

Contents

Introduction and getting started 5
Overview 6
System requirements 6
Ports and buttons 7
Indicator LED 8
Getting started 9
Installing a SIM card 9
Powering on 10
Identifying a location 10
Connecting to the FX3100 11
Monitoring and managing your FX3100 12
Caring for your FX3100 15
Replacing a SIM card 15
Resetting your FX3100 16
Care tips 17
Configuration 18
Overview 19
Home page 20
Side menu 20
Getting help 21
Admin password 21
Changing the Admin password 21
Managing data usage 22
Data Usage page 23
Managing Wi-Fi settings 25
Settings tab 26
Primary Network tab 28
Guest Network tab 30
Managing connected devices 32
Connected Devices page 33
Managing settings 35
Preferences tab 36
Software Update tab 38
Backup and Restore tab 40
ZTP tab 42
SIM 43
VPN tab 46
GPS tab 48
APN tab 50
Advanced tab 51
Viewing info about the FX3100 52
Internet Status tab 53
Internet Sessions tab 55
Diagnostics tab 56
Device Info tab 58
Logs Tab 59
Getting support 60
Help tab 60
Customer Support tab 61
Advanced settings 63

Overview....64
Using advanced settings....64
Cellular tab....65
DNS....66
Firewall tab....68
MAC Filter tab....70
LAN tab....71
WAN tab....74
Port Filtering tab....76
Port Forwarding tab....78
Inseego Connect tab....81
Heartbeat timer (Inseego Connect)....82
Troubleshooting and support....83
Overview....84
Troubleshooting....84
Will I always get 5G? Can I use the FX3100 outside of 5G coverage?....84
The FX3100 LED is switching from blue to green and sometimes dropping service....84
Can I set my FX3100 to use a specific band?....84
I cannot access the Admin web UI....84
The FX3100 LED is blinking red....85
My older device cannot connect....85
My FX3100 is “Waiting for Connection” on the Inseego Mobile app....87
My FX3100 is getting slow speeds/low throughput....87
My connecting device is not obtaining a valid IP address....88
I cannot get streaming platforms to work with my FX3100....88
Do I need a signal amplifier or booster?....89
Does the USB port support RNDIS?....89
Does the USB port support USB-C to Ethernet adapters?....89
Technical support....89
Product specifications and regulatory information....90
Product specifications....91
Device....91
Environmental....91
Network connectivity....91
Wi-Fi....92
Security....92
Networking....92
Regulatory information....93
Product certifications and supplier’s declarations of conformity....94
Energy efficiency....95
Wireless communications....95
Limited warranty and liability....96
Safety hazards....97
Glossary....98
Glossary....99

1

Introduction and getting started

Overview

Ports and buttons

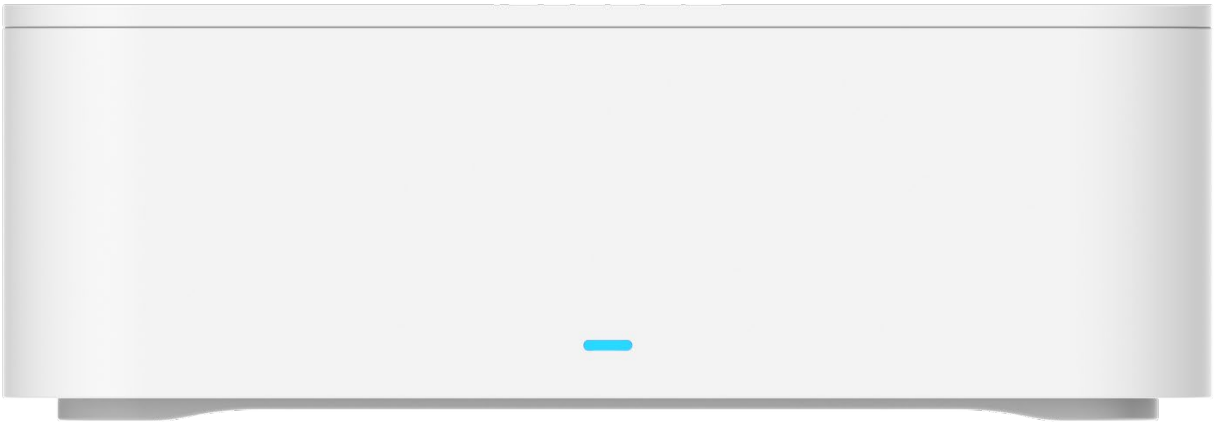
Indicator LEDs

Getting started

Caring for your FX3100

Overview

The FX3100 provides gigabit-class wireless broadband internet capabilities. With dual-band Wi-Fi 6, the FX3100 supports up to 64 connected devices, two Ethernet LAN/WAN ports, and a USB-C port for tethering. Connect laptops, tablets, e-readers, gaming consoles and more.



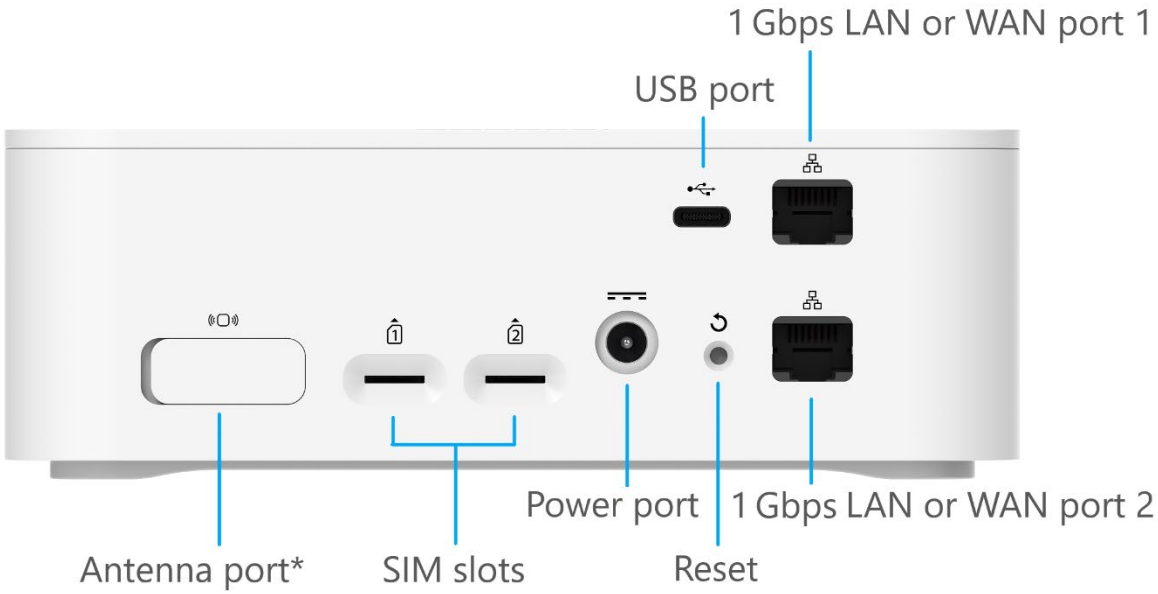
Inside the box you will find a FX3100, a Get started card, and an AC wall adapter power supply.

System requirements

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

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

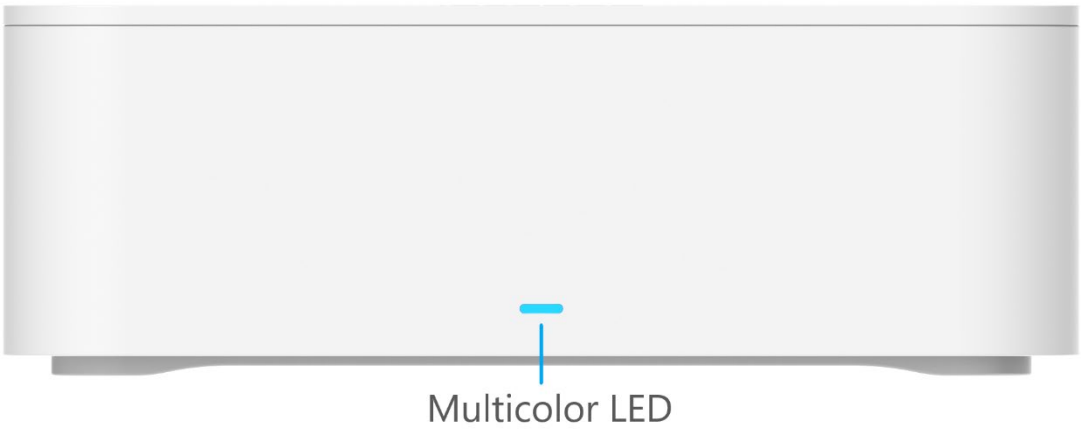
Ports and buttons



* The antenna port is for an optional external antenna and provides support for mobile frequency bands within either a 1700-2700 MHz or 3300-4200 MHz range. To activate the external antenna port, enable it from **Settings** > **Preferences** in the Admin web UI.

Indicator LED

The front of the FX3100 has an indicator LED. It changes colors and either blinks or glows solid to communicate current states for the device.



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

The LAN/WAN ports 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

Getting started

This section provides instructions for getting your FX3100 up and running, as well as reset and support information.

Installing a SIM card

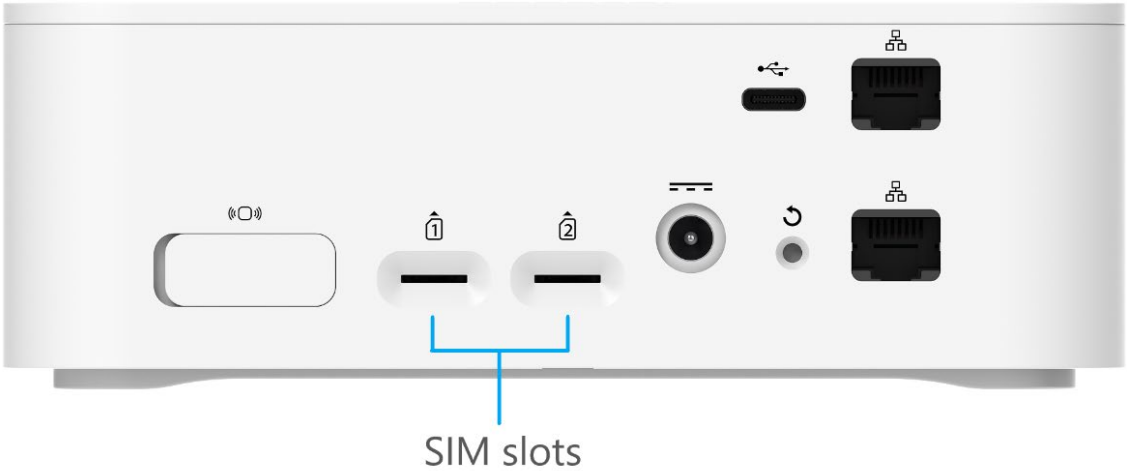
A SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The FX3100 supports only Nano SIM cards.

NOTE: If you received the FX3100 from your service provider, the device manufacturer may have pre-installed a SIM card. Please inspect the SIM slots on the back of the device to confirm.

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

To install a SIM card:

1. If necessary, remove the SIM card from the protective sleeve, being careful not to touch the gold-colored contacts.
2. Insert the SIM card into the SIM slot, ***notch first, with the gold-colored contact points facing down***. **NOTE:** It is best to use SIM slot 1 first.



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

Powering on

Turn on your FX3100 with the AC wall adapter power supply:

1. Plug the power cord into the power port on the back of the FX3100.
2. Plug the power adapter into an AC wall outlet.

WARNING! Use only the AC wall adapter power supply that came with the FX3100. Unapproved wall adapter power supplies could cause the FX3100 to overheat or catch fire, resulting in serious bodily injury, death, or property damage.

Identifying a location

Use the Inseego Mobile™ app to identify the optimal location for your FX3100.

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 FX3100 and perform a location survey to identify the ideal location for your FX3100.

NOTE: Once you have completed the location survey, you are prompted to set up a free Inseego Connect account that allows you to remotely monitor and configure your device from the Inseego Mobile app. After you create an account, you are asked to register your device using the current device password. Enter the current Admin password (the default Admin password is on the bottom label of the FX3100). Then restart the device.

Location suggestions:

- Near a window but not in direct sunlight
- On an 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

Connecting to the FX3100

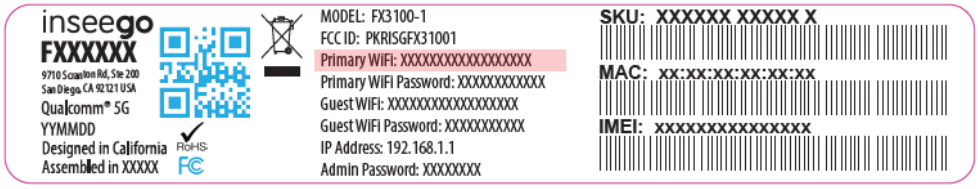
With the FX3100, Wi-Fi devices and wired devices can connect to the mobile broadband network simultaneously.

Connecting devices wirelessly

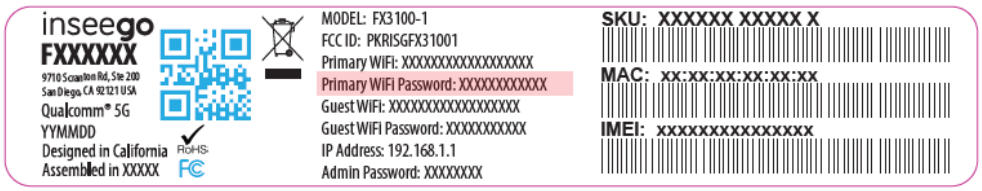
You can connect to your FX3100 with your computer, tablet or other wireless devices that have Wi-Fi and internet browser software.

To connect a Wi-Fi capable device to your FX3100:

1. Make sure the FX3100 is powered on, and the indicator LED is blue or green.
2. On the device you want to connect to the internet, open the Wi-Fi settings or application and in the displayed list of available networks, find the **Primary Wi-Fi network name** printed on the bottom of your FX3100.



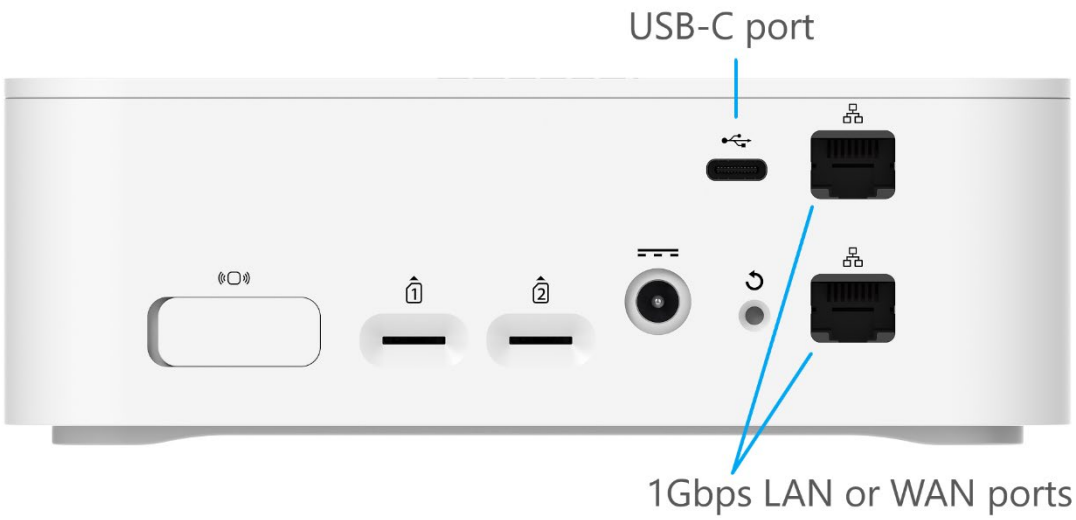
3. Click **Connect** or otherwise select the network name.
4. When prompted, enter the **Primary Wi-Fi password** printed on the bottom of the FX3100.



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 LAN/WAN port on the FX3100.
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 FX3100.
2. Plug the other end of the cable into the USB port of the device you wish to connect.

Devices plugged into the FX3100 via Ethernet and USB have instant access to the internet.

Monitoring and managing your FX3100

You can use the following options to monitor and manage your FX3100.

Inseego Mobile app

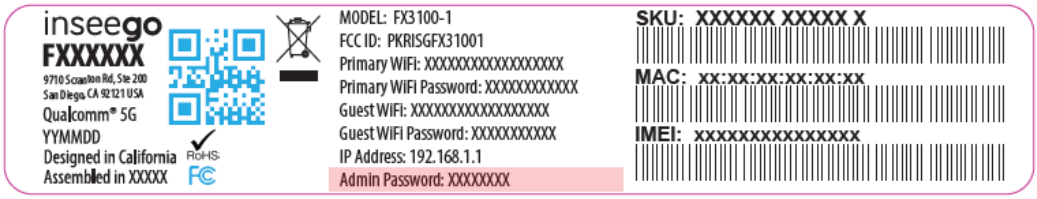
You can use the same mobile app you used to find a location for your FX3100 to perform basic device monitoring and management.

Admin web UI

Once your FX3100 is connected to a device that supports web browsing, you can use the Admin web UI to customize settings, change your password, and access information.

On a device connected to the FX3100, open any web browser, and go to http://192.168.1.1, http://Inseego.local*, or http://fx3100.com*.

Select **Sign In** (in the top-right corner of the screen) and enter the **Admin Password** printed on the bottom of the FX3100.



Inseego Connect™

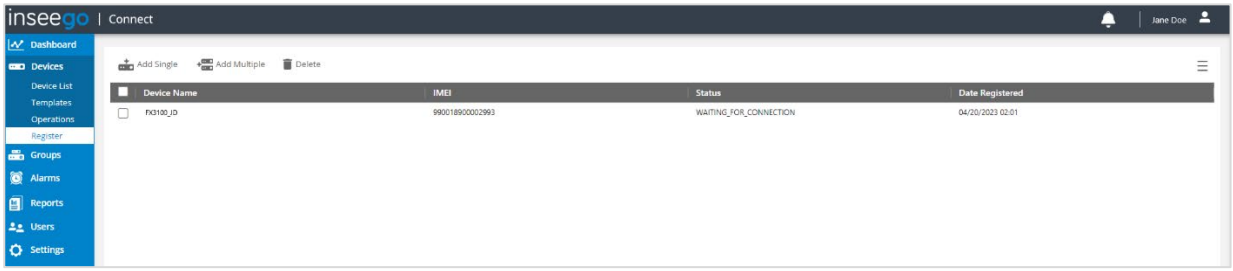
Inseego Connect is a multi-tiered device management platform that allows you to deploy, monitor, and manage Inseego IoT devices remotely from the cloud. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free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

NOTE: If you used the Inseego Mobile app to find a location for your device, it may have added your device to Inseego Connect. When logging in to Inseego Connect, check to see if your device is on the Device List or on Devices > Register. Restart your device to hasten the registration process.

Adding a device to Inseego Connect

To add a device or multiple devices to Inseego Connect:

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



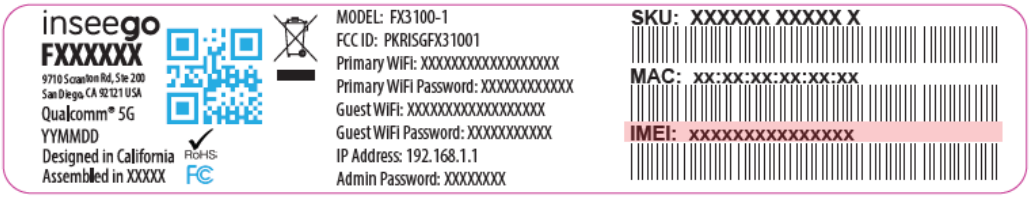
3. Use the tools along the top of the table to add devices.

   NOTE: When adding a device, make sure the device is powered on and connected to the internet.

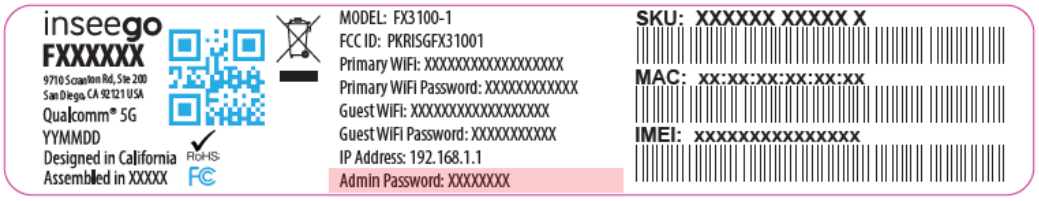
* The Inseego.local and fx3100.com web UI addresses rely on having IPv6 enabled on your connecting device.

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

- Enter a **Device Name** (optional).
- Enter the **Device IMEI** printed on the bottom of the device.



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



- Click **Register**. The device enters a Waiting for Connection state while waiting to connect to the Inseego cloud.

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

- Click the **Download sample template (.xlsx)** link.
- Open the .xlsx file and enter a **Name** (optional), **IMEI**, and **Password** for each device you wish to register.
- Click **Upload**. The devices enter a Waiting for Connection state while waiting to connect to the Inseego cloud.

IMPORTANT: After adding a device, restart the device immediately. This allows the device to check in and process the registration request.

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

Caring for your FX3100

This section provides information on general care and restoring your FX3100 to factory default settings.

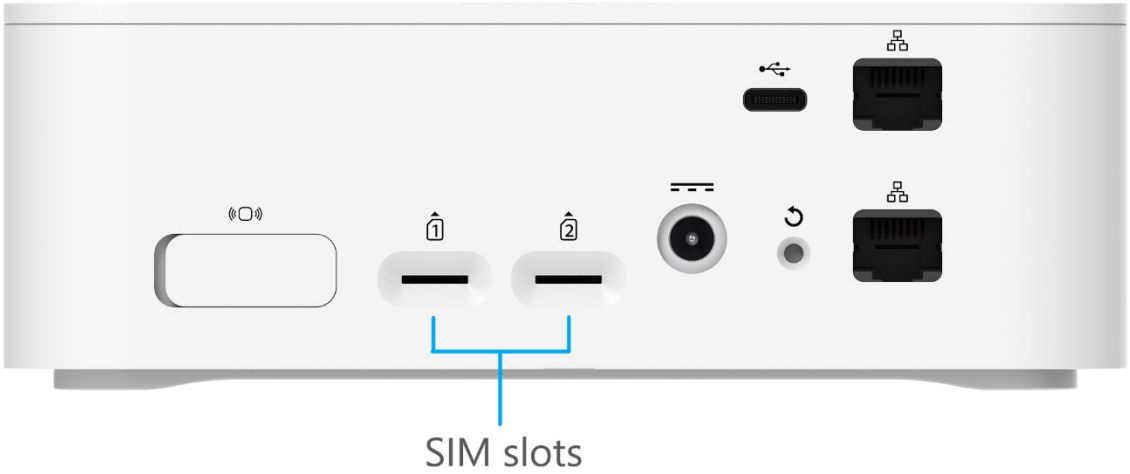
Replacing a SIM card

Your SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The FX3100 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 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 network operator.

Resetting your FX3100

You can reset your FX3100 to factory settings from the Admin web UI, Inseego Mobile app, Inseego Connect or by using the reset button on the FX3100.

CAUTION! Resetting returns your FX3100 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 FX3100 from the Admin web UI, select **Settings > Backup and Restore** and select **Restore factory defaults**.

Resetting from the Inseego Mobile app

To reset the FX3100 from the Inseego Mobile app, select **Mobile Options**, then select **Factory Reset.**

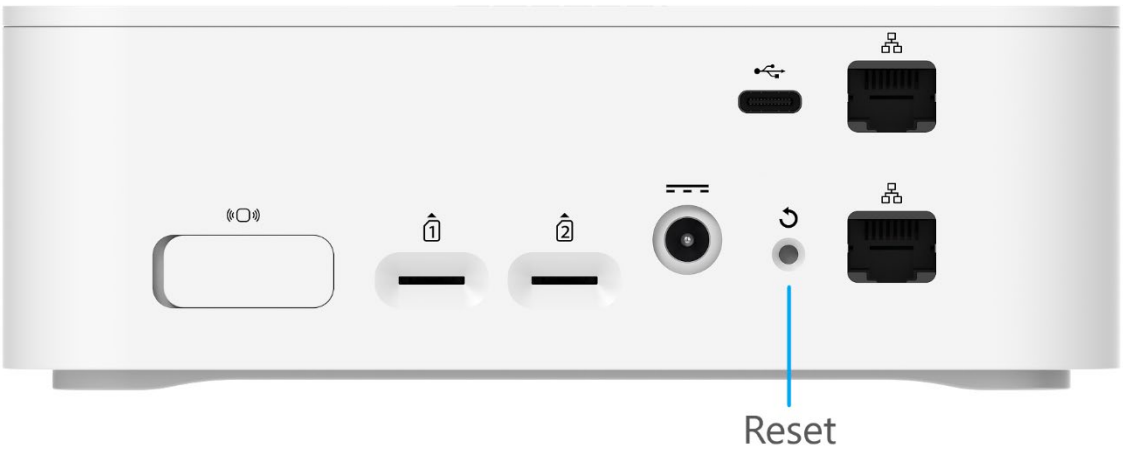
Resetting from Inseego Connect

To reset the FX3100 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 in a small hole located on the back of the FX3100.

1. Verify that your FX3100 is powered on.
2. Locate the reset opening ↺ on the back of your router.



3. Press the recessed button for about five seconds until the device resets. The LED blinks white, then turns red. When it is green or blue, your FX3100 is ready.

   NOTE: The first time you perform a factory reset, it may take over two minutes for your FX3100 to restart.

Care tips

Inseego recommends the following care guidelines:

- Avoid locating the FX3100 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 FX3100 from liquids, dust, and excessive temperatures.
- Do not apply adhesive labels to the FX3100 as they may cause the router to potentially overheat or alter the performance of the internal antenna.
- Store the FX3100 in dry and secure location when not in use.

2

Configuration

Overview

Admin password

Managing data usage

Managing Wi-Fi settings

Managing connected devices

Managing settings

Viewing info about the FX3100

Getting support

Overview

You can configure your FX3100 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 FX3100:

- **Inseego Mobile app** – Allows you to perform basic device monitoring and management. This is the same app you used to identify a location for your FX3100.
- **Admin web UI** – Provides a local gateway to configure and manage your FX3100. On a device connected to the FX3100, open any web browser, and go to http://192.168.1.1, http://Inseego.local*, or http://fx3100.com*. Select **Sign In** (in the top-right corner of the screen) and enter the **Admin Password** printed on the bottom of the FX3100.
- **Inseego Connect** – Enables you to monitor and configure an entire deployment of devices remotely from the cloud. You can group devices together to push widespread configurations, troubleshoot individual devices, set alarms, and run reports. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free Inseego Connect account at connect.inseego.

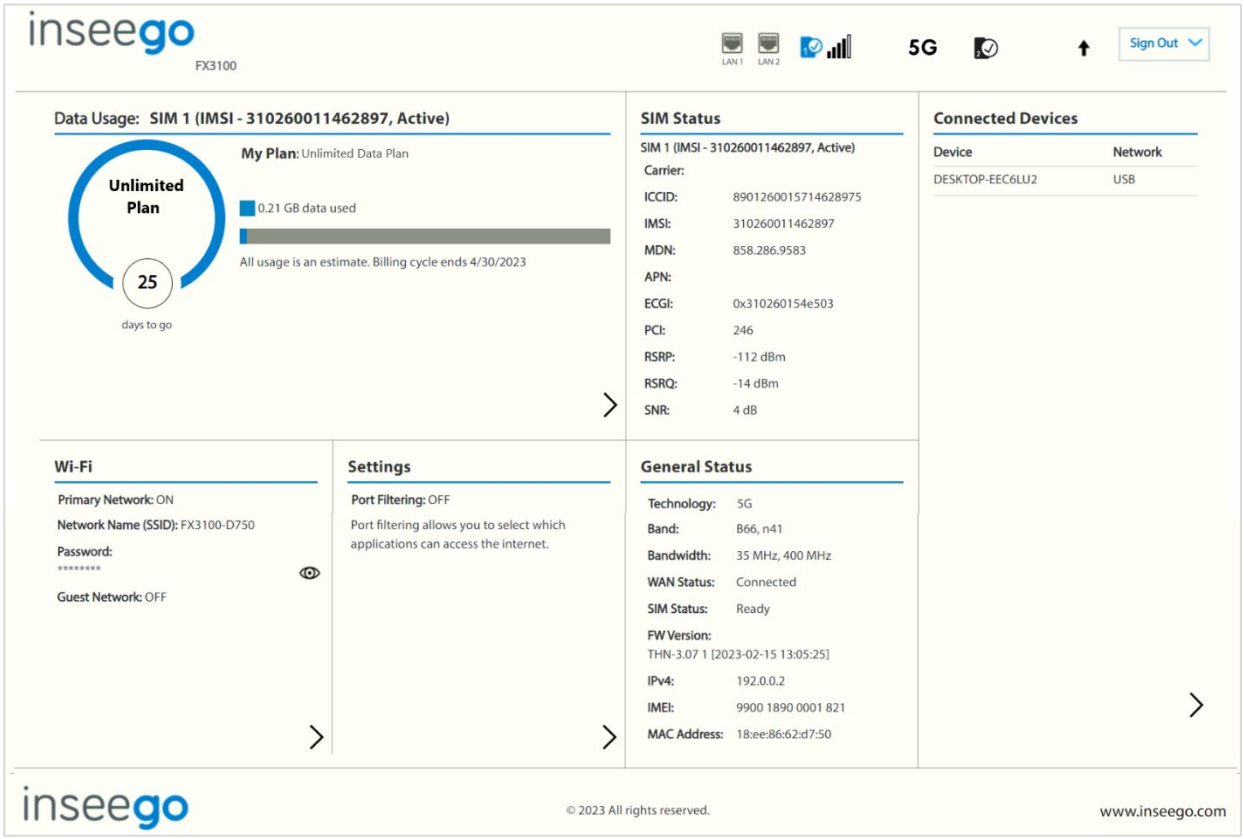
This chapter provides the configuration options available for your FX3100 devices. The configurations shown are from the Admin web UI, unless otherwise noted. Many of these options are also available with Inseego Mobile app and Inseego Connect. Some configurations are available only with Inseego Connect and are marked as such.

* The Inseego.local and fx3100.com web UI addresses rely on having IPv6 enabled on your connecting device.

Home page

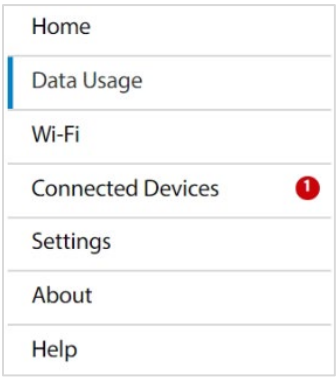
The home page of the Admin web UI is the local gateway to configuring and managing your FX3100. It displays the current Wi-Fi networks and passwords and lists all currently connected devices. It also shows data usage, SIM status, general status, and setting information.

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



Side menu

Each sub screen in the FX3100 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.

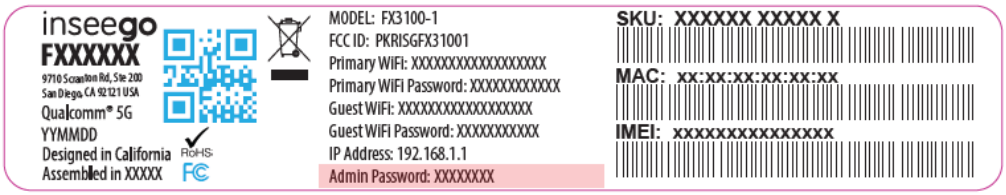


Getting help

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 FX3100 Admin web UI. A default Admin password is assigned to each individual device and is printed on the bottom of the device.



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:

Important: If you are in the process of adding your FX3100 to Inseego Connect, wait to change your Admin password until the registration process is complete and your FX3100 is listed on the Inseego Connect Device List page.

1. **From the Admin web UI:** Click the down arrow next to **Sign Out** in the top-right corner of any Admin web UI page and select **Change Password.**

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

2. Enter your current Admin password, then click **Continue**.

3. Enter your current Admin password again, then enter a new password and confirm it.

4. Select a security question from the drop-down list and type an answer to the question.
   NOTE: Answers are case-sensitive.

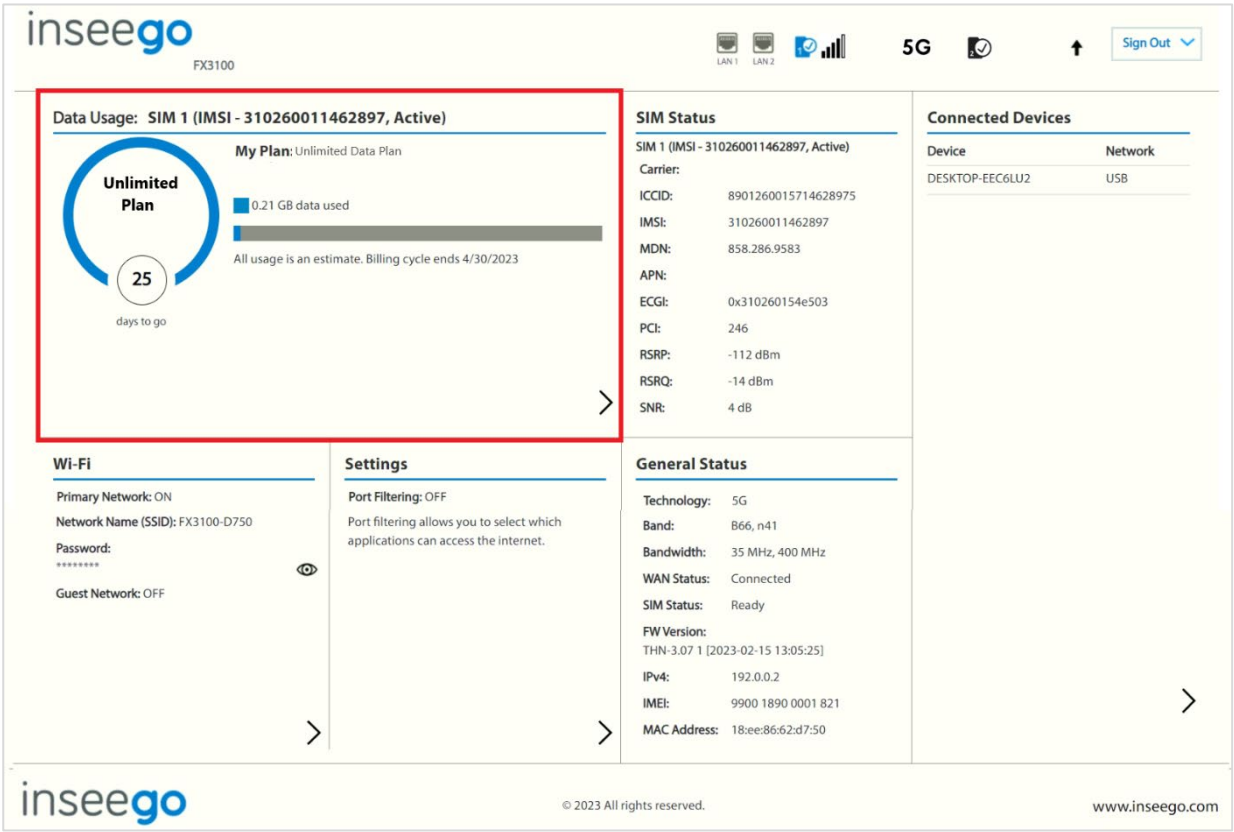
5. Click **Save Changes**.

The next time you sign in to the FX3100 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 FX3100 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.

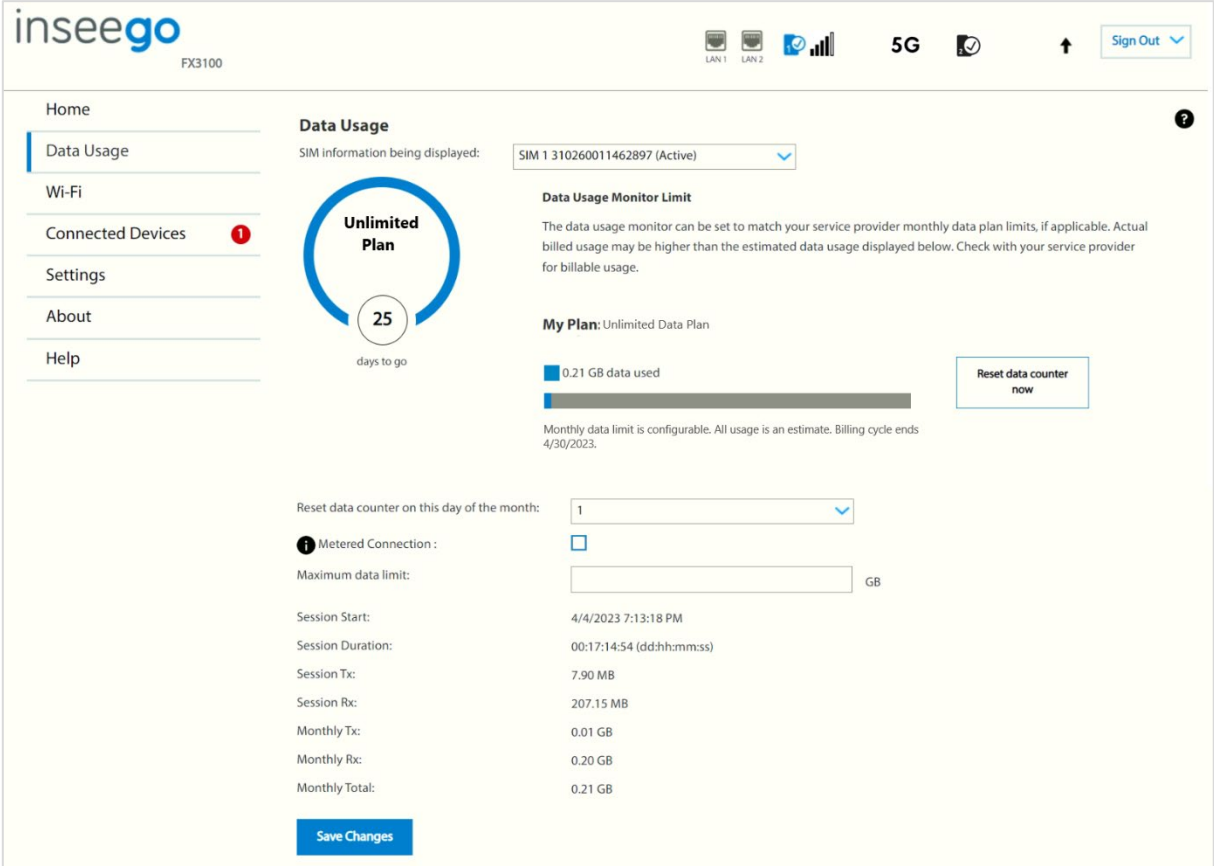


To manage or view data usage, select > from the home page Data Usage panel or select **Data Usage** from the side menu. The Data Usage page appears.

Data Usage page

Use the Data Usage page to view details and manage your FX3100 data usage.

NOTE: Your FX3100 provides only a rough estimate of data usage. Always check with your service provider for exact usage.



SIM information being displayed: Use the drop-down to change the SIM on which data usage is displayed.

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

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

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

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

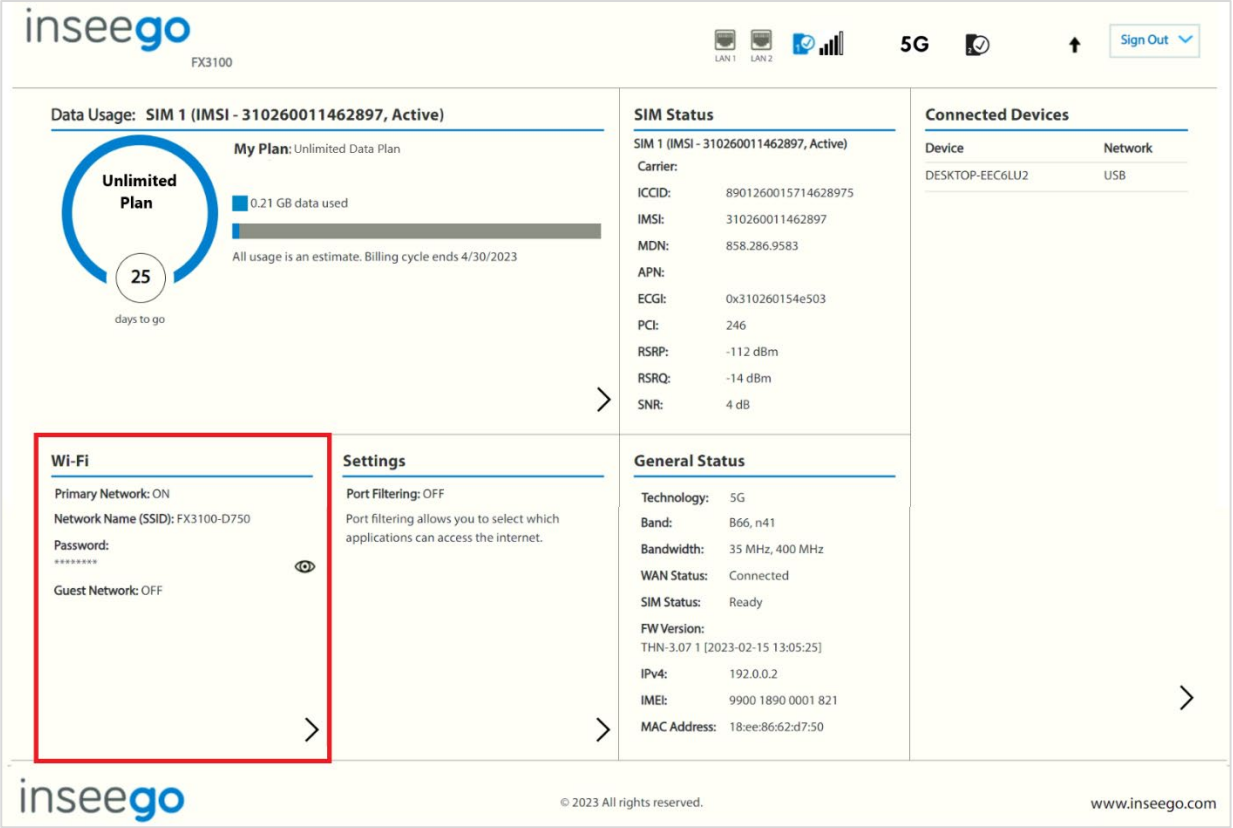
Monthly Total: The total amount of data for the current billing cycle.

Select **Save Changes** to enact changes.

Managing Wi-Fi settings

Your FX3100 offers primary and guest networks for accessing the internet over Wi-Fi. Each network can be accessed over two bands: 2.4 GHz and 5 GHz.

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



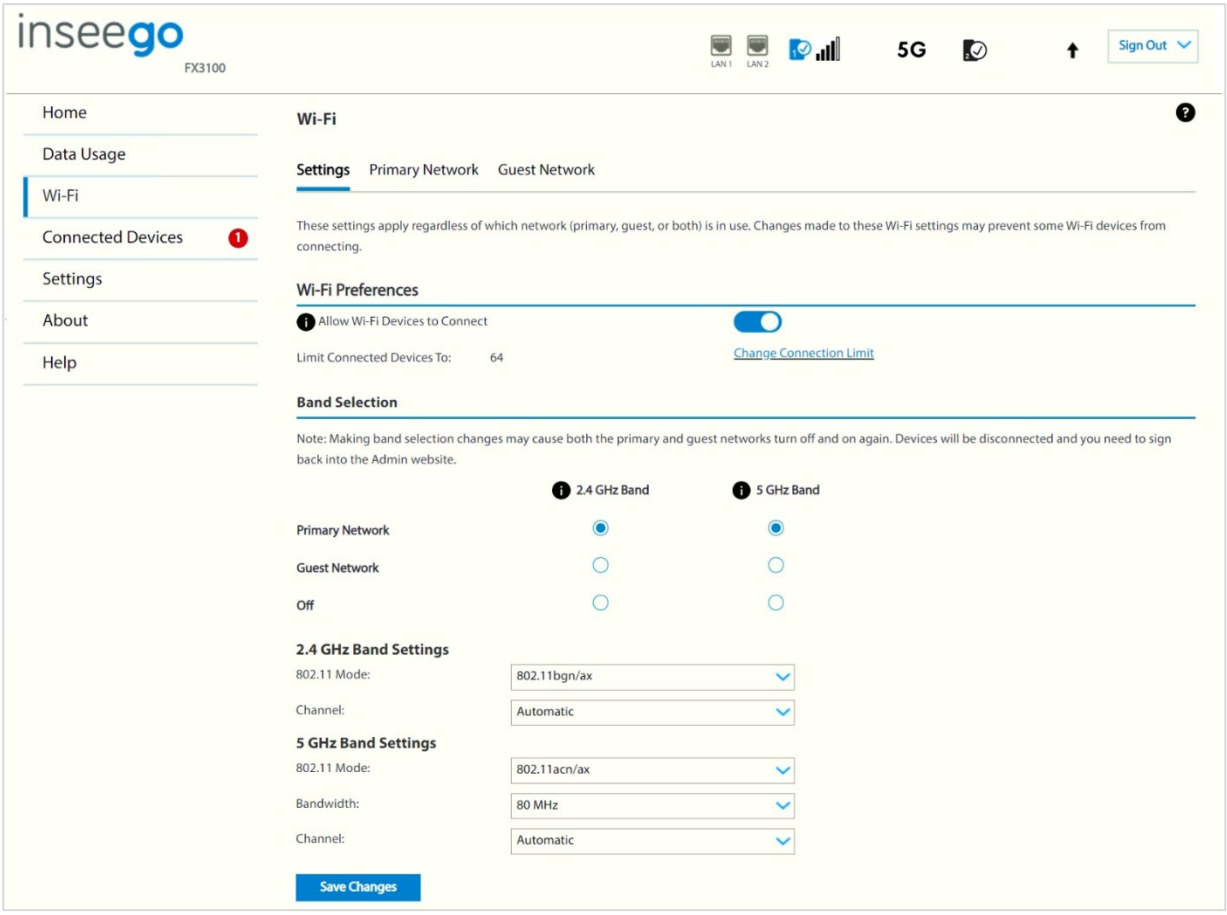
To manage settings for these networks, select > from the home page Wi-Fi panel or select **Wi-Fi** from the side menu.

The Wi-Fi page includes three tabs:

- Settings
- Primary Network
- Guest Network

Settings tab

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



Wi-Fi Preferences

Use the **Allow Wi-Fi Devices to Connect** slider to turn Wi-Fi on or off. This selection affects primary and guest networks. **NOTE:** If Wi-Fi is off, the only way to connect devices to the FX3100 is with an Ethernet cable or USB.

Select **Change Connection Limit** to change the maximum number of devices allowed to connect to your FX3100. The maximum number of connected devices is 64. Select a number and click **Save Changes**.

Band Selection

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

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

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

2.4 GHz Band Settings

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

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

5 GHz Band Settings

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

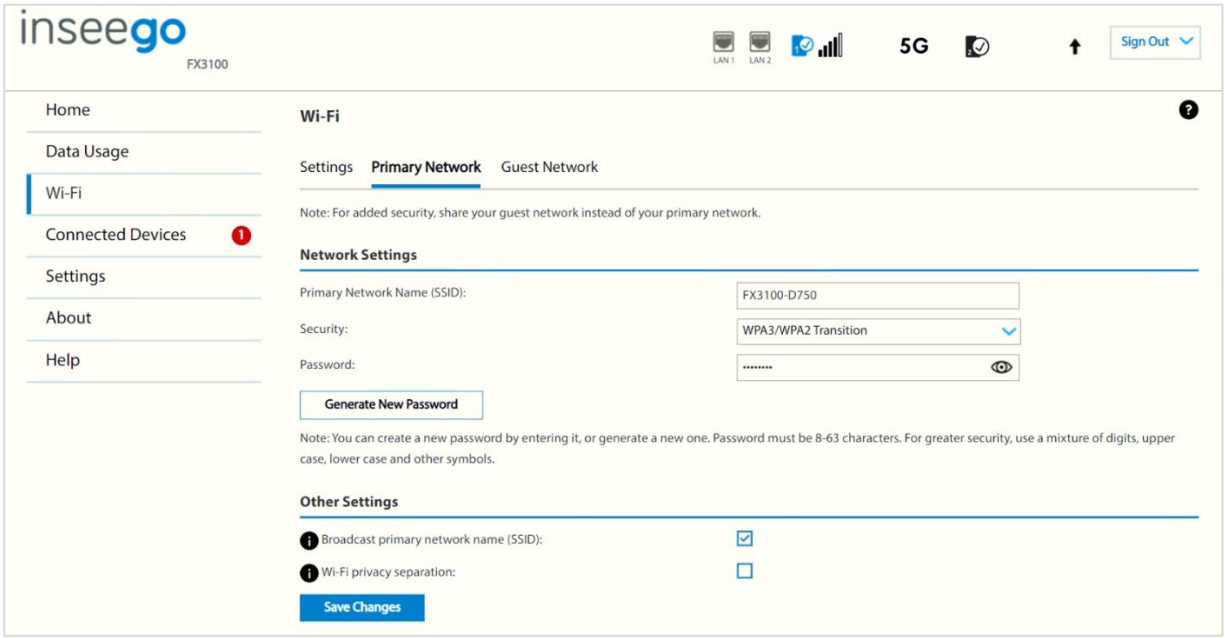
Bandwidth: Leave bandwidth at the default setting unless you experience interference with other Wi-Fi devices. If you experience interference, try lowering the setting to reduce the interference.

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

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

Primary Network tab

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



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

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

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

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

You can click the eye icon to view the password.

Other Settings

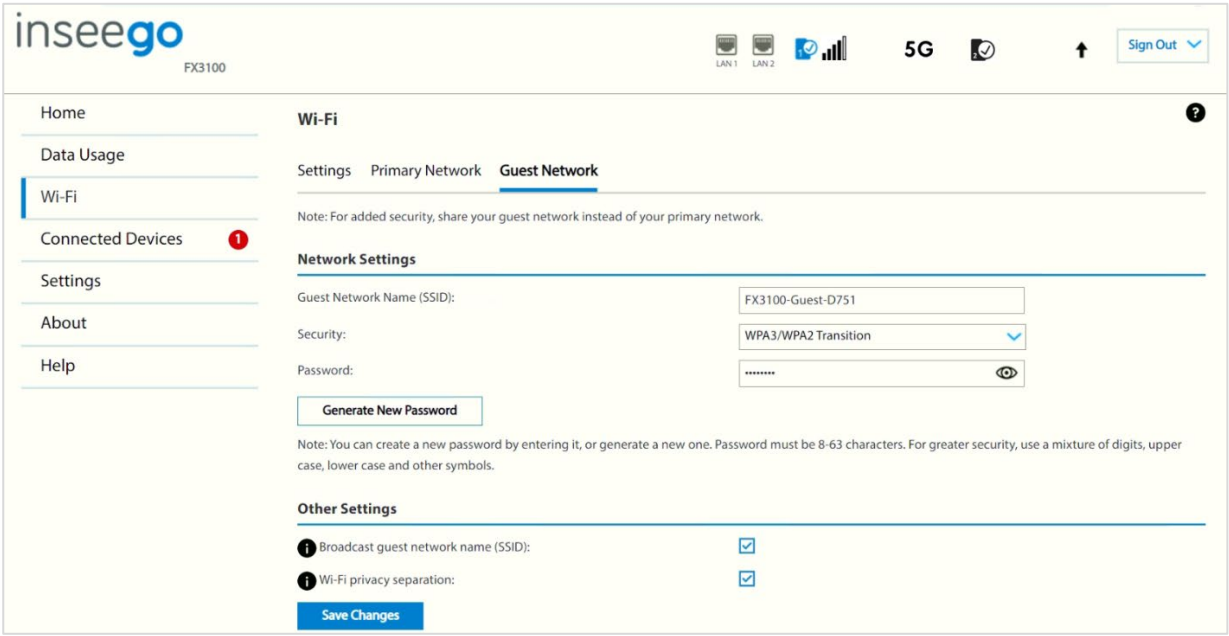
Broadcast primary network name (SSID): When checked, this allows the Wi-Fi primary network to be displayed in the list of available Wi-Fi networks on your connected devices. If unchecked, this network is not visible to connected devices.

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 FX3100 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 PSK** can be used for WPA3 devices.
- **WPA 3 Open Enhanced** provides encryption and privacy on open networks that are not password-protected and can be used for WPA3 devices.
- **WPA/WPA2 Mixed Mode** can be used if some of your older devices do not support WPA2.
- **WPA2 AES PSK** can be used for WPA2 devices.
- **Open** allows others to monitor your Wi-Fi traffic and use your data plan to access the internet. **NOTE:** Avoid using this option.

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

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

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

You can click the eye icon to view the password.

Other Settings

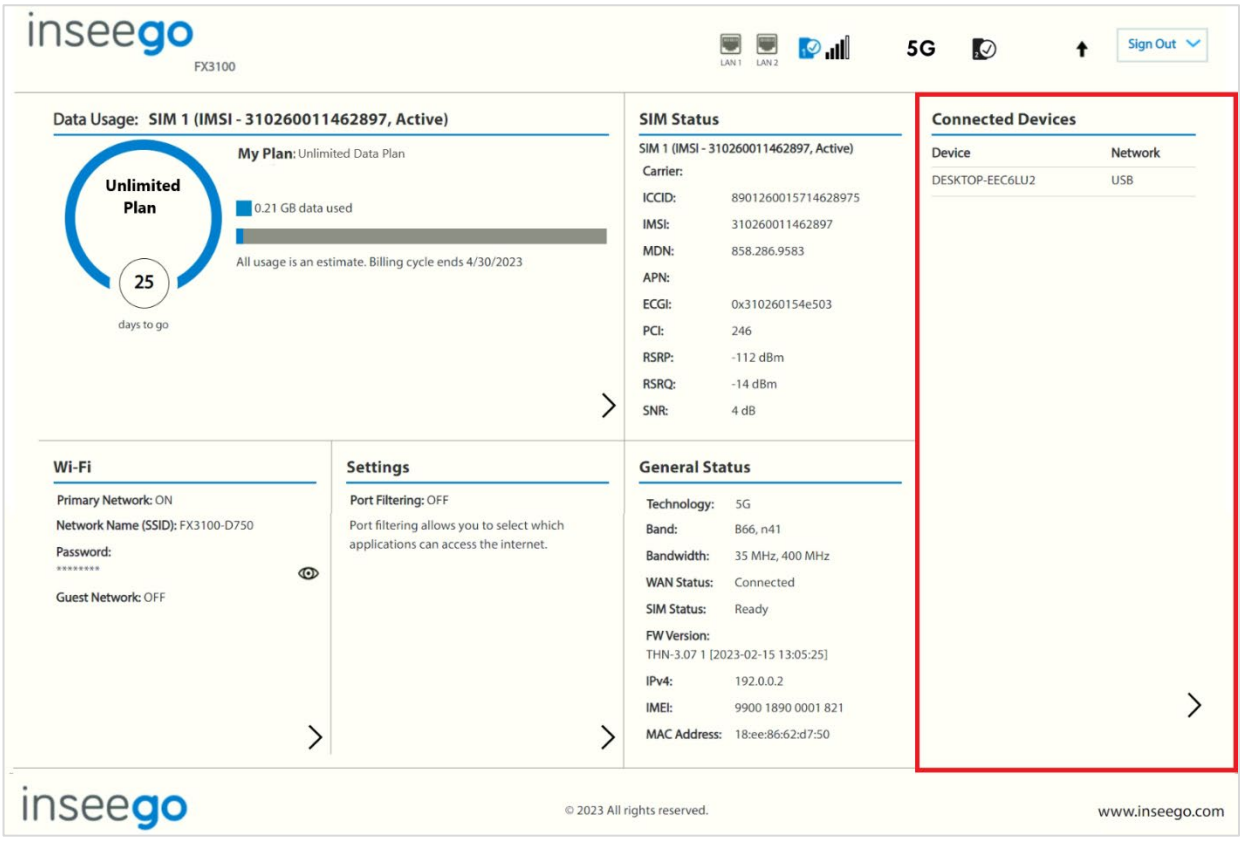
Broadcast guest network name (SSID): When checked, this allows the Wi-Fi guest network to be displayed in the list of available Wi-Fi networks on your connected devices. If unchecked, this network is not visible to connected devices.

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**.

Managing connected devices

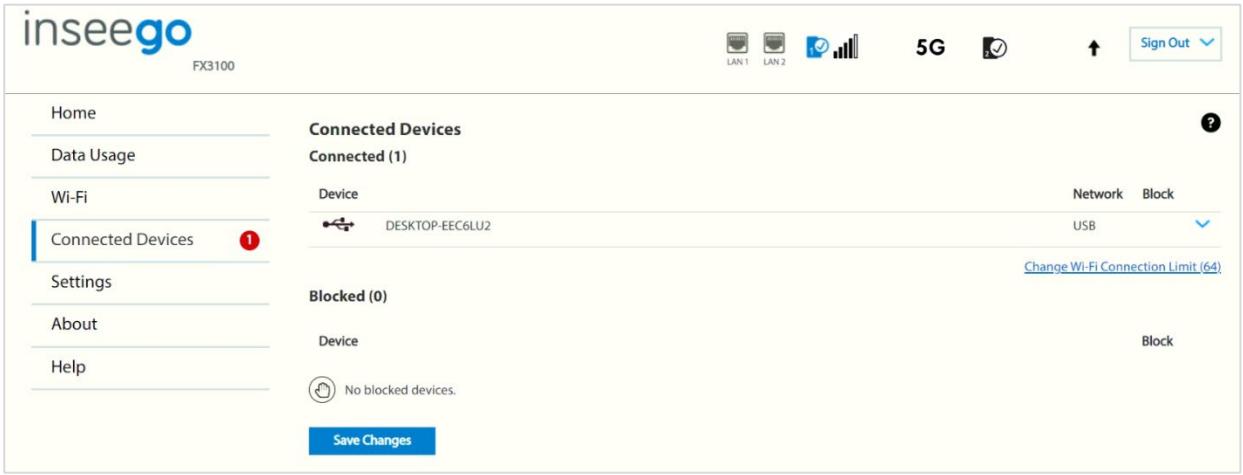
On the Admin web UI home page, the Connected Devices panel lists the networks currently connected to your FX3100 along with the number of connected devices for each network.



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 FX3100 and allows you to edit how device names appear in the UI. You can also block or unblock a device from internet access.



Connected Devices

Connected: The number of devices currently connected to your FX3100.

The table lists all devices connected to the FX3100:

> **Connection:** An icon indicates the connection type for each device. (You can hover over the icon to read the type of connection.)
>
> **Device:** The name of the connected device is usually the hostname set on the connected device. In rare cases, the hostname may be unavailable.
>
> **Network:** Indicates whether the device is connected to the primary or guest network, or through Ethernet or USB.
>
> **Block:** Select this box to disconnect a device and prevent it from reconnecting. Select **Save Changes**. The device is removed from the **Connected** list and appears in the **Blocked** list below. **NOTE:** This option is available for each device connected through Wi-Fi but is not available for your own device or devices connected via Ethernet or USB.

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

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

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

Blocked

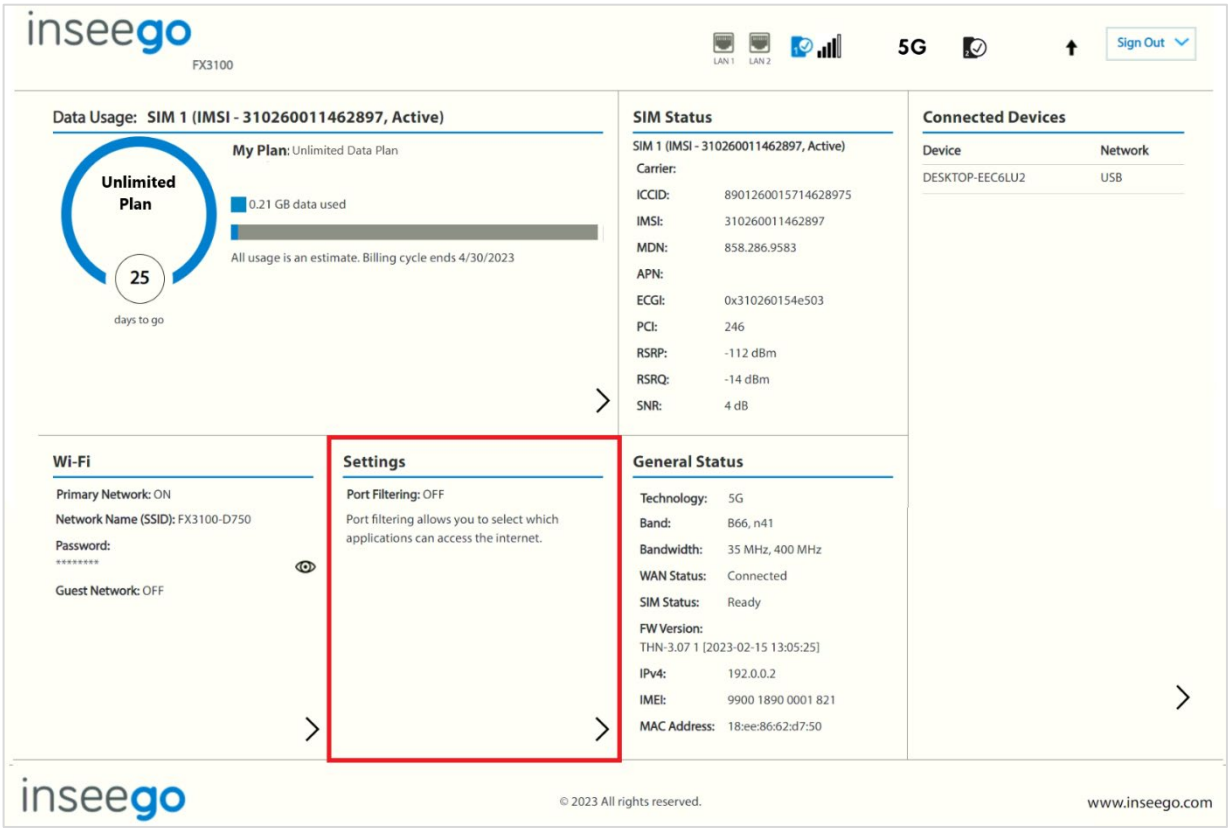
This section lists all devices blocked from connecting to the FX3100.

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

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

Managing settings

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



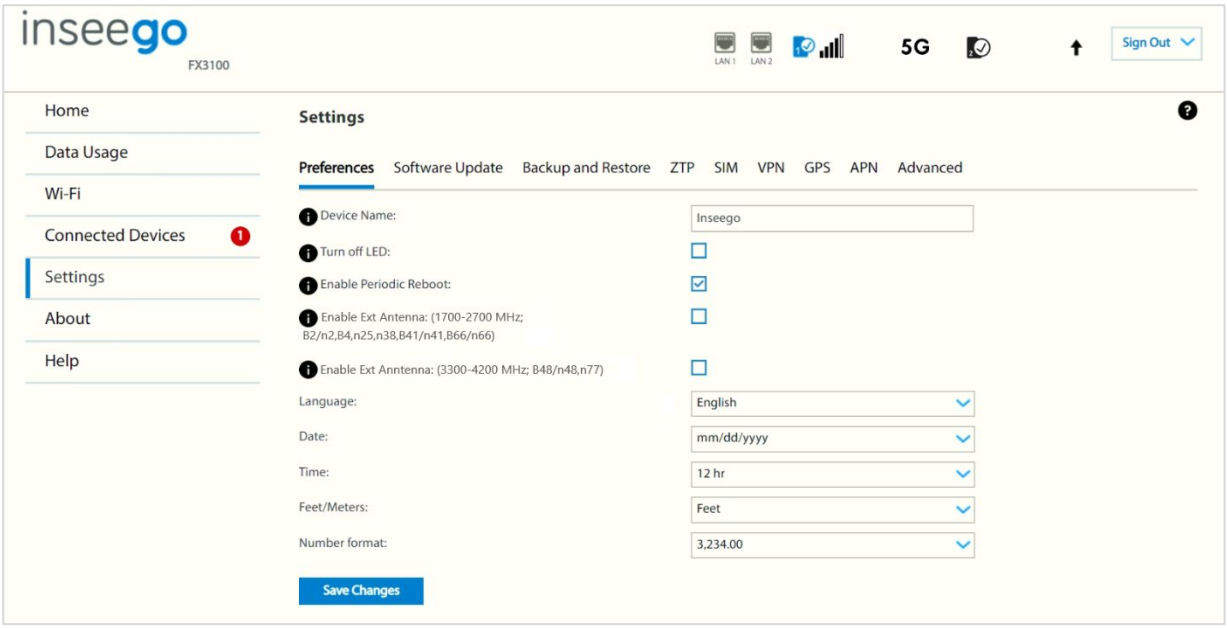
To configure more system settings, select > from the home page Settings panel or select **Settings** from the side menu.

The Settings page includes the following tabs:

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

Preferences tab

You can use this tab to change the FX3100 name visible to connecting devices, turn off the LED light, enable periodic reboot, and activate the external antenna port on your FX3100. You can also change the language and how dates, time, distance, and numbers are displayed in the web UI.



Device Name: To change how the FX3100 appears when connecting other devices, enter a different name.

Turn off LED: Check the checkbox to turn off the LED display light on your FX3100.

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.

Enable Ext Antenna: (1700-2700 MHz; B2/n2,B4,n25,n38,B41/n41,B66/n66)
Check the checkbox to activate the external antenna port on your FX3100 to support mobile frequency bands within the 1700-2700 MHz range. **NOTE:** Please contact your service provider for available bands at your location.

Enable Ext Antenna: (3300-4200 MHz; B48/n48,n77)
Check the checkbox to activate the external antenna port on your FX3100 to support mobile frequency bands within the 3300-4200 MHz range. **NOTE:** Please contact your service provider for available bands at your location.

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).

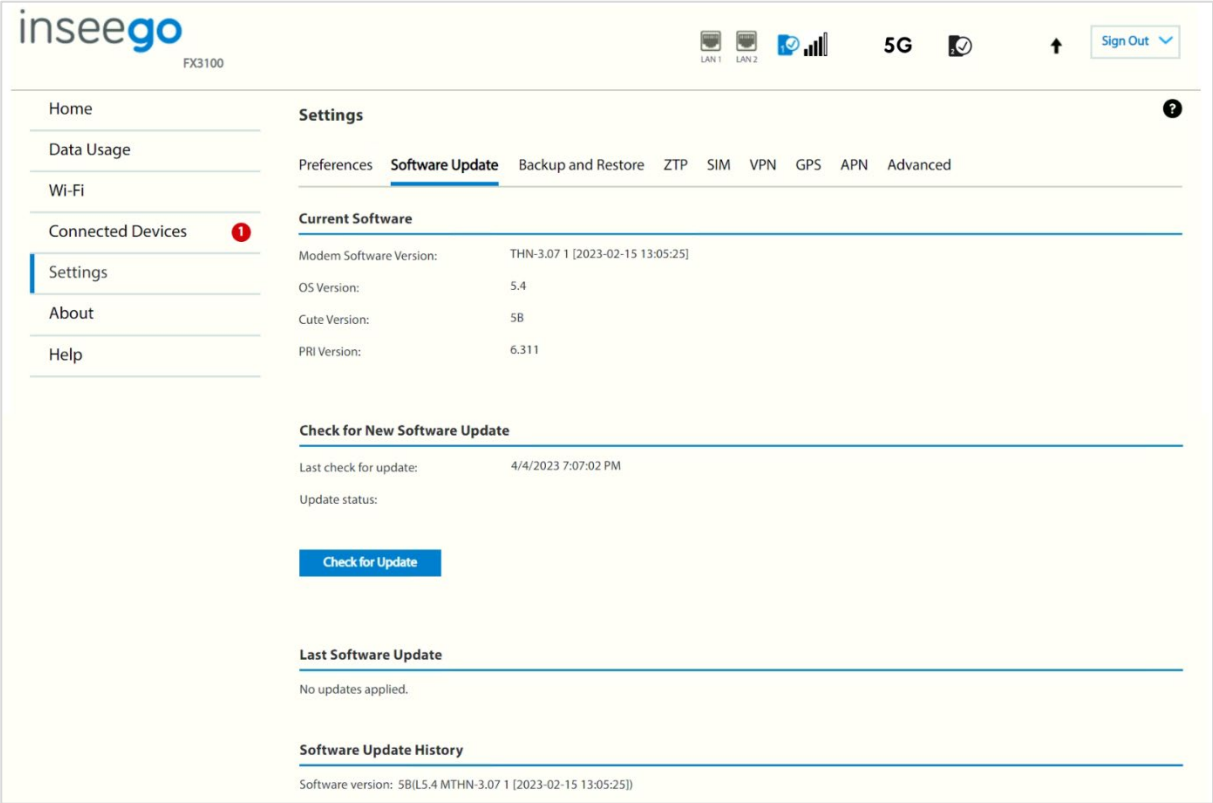
Number format: Choose the format for decimal numbers displayed in the web UI (using a period or comma as the decimal point).

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

Software Update tab

Software updates are delivered to the FX3100 automatically over the mobile network. This tab displays your current software version, last system update information, software update history, and allows you to check for new software updates.

NOTE: You can opt out of software updates using Inseego Connect.



Current Software

Modem Software Version: The version of software currently installed for the modem 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 FX3100.

PRI Version: The configuration version currently applied to your FX3100.

Check for New Software Update

Last check for update: The date and time the FX3100 last checked to see if an update was available.

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

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

Last Software Update

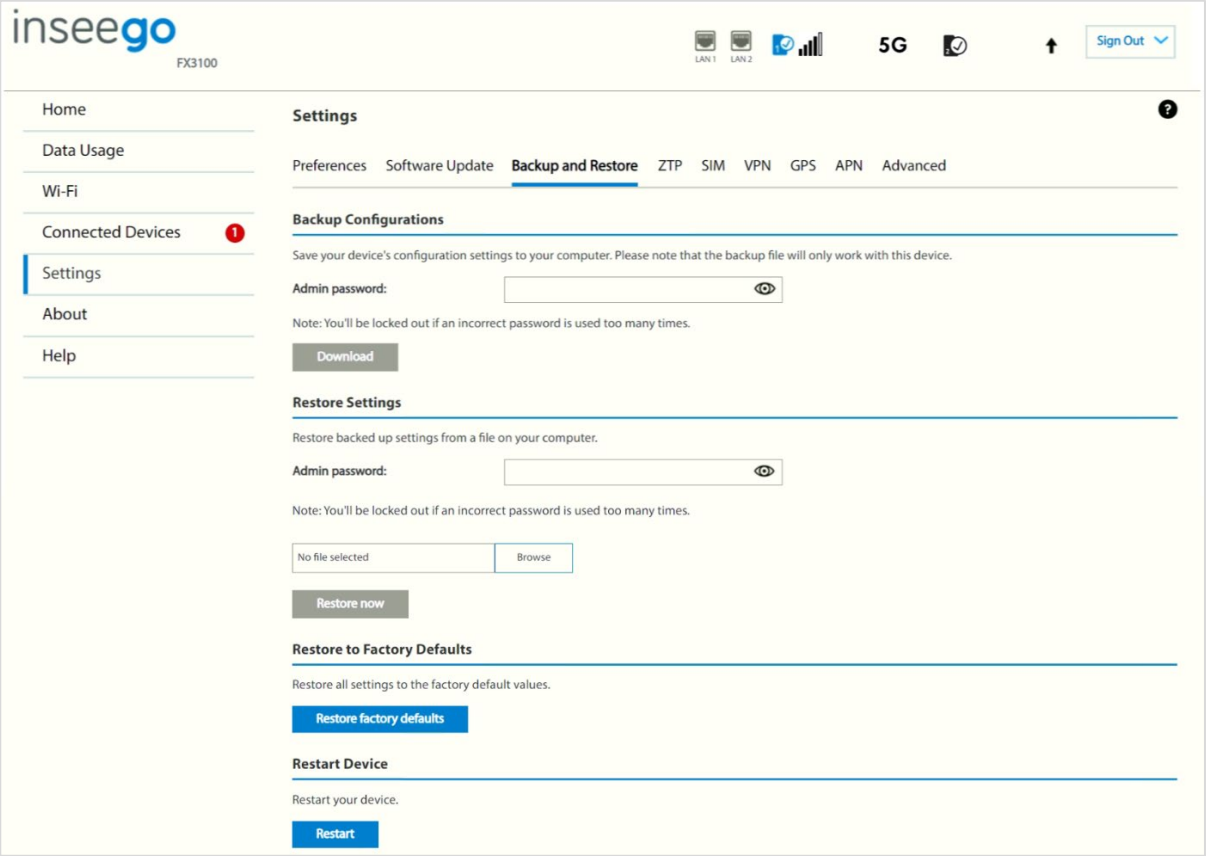
This section displays details about the last software update.

Software Update History

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

Backup and Restore tab

Use this tab to back up current FX3100 settings to a file on your computer, restore (upload) a previously saved configuration file, reset the FX3100 to factory defaults, or restart the FX3100.



Backup Configurations

To back up current FX3100 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 FX3100. 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 FX3100 and use the Admin password printed on the bottom of your FX3100.

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 FX3100.

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 FX3100, 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 FX3100 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 FX3100.

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 FX3100 and disconnecting you from the Admin web UI.

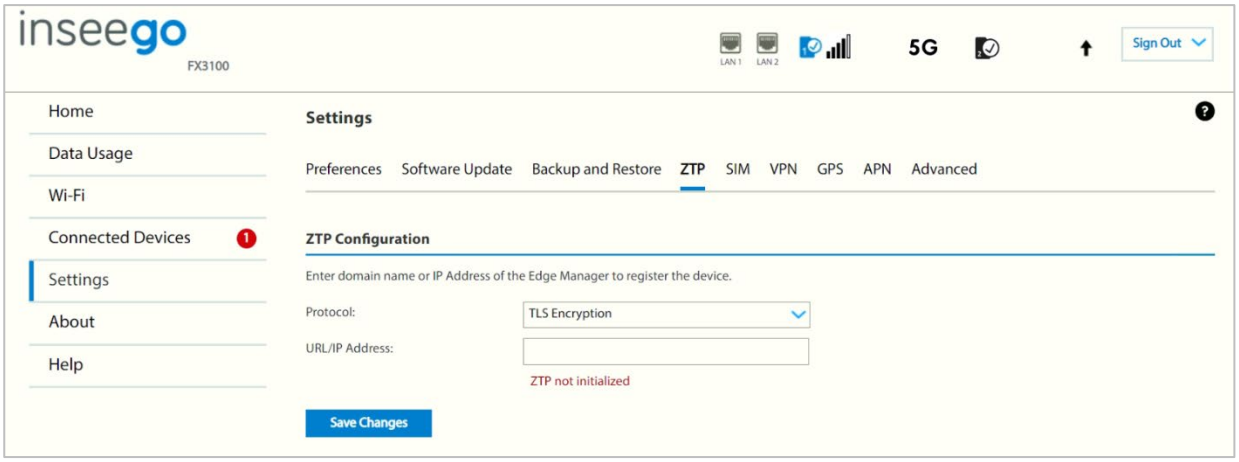
Restart Device

Restart: This button turns your FX3100 off and on again.

ZTP tab

Use this tab to initiate Zero Touch Provisioning (ZTP) when onboarding devices to Inseego 5G SD EDGE™ Manager.

Inseego SD Edge is a cloud-based management system that provides remote monitoring and comprehensive worksite network security. It provides IT teams with real-time visibility, control, and management of critical network infrastructure in a secure manner with advanced authentication, authorization, and encryption. To learn more about Inseego's SD Edge offering go to https://inseego.com/products/cloud-management/inseego-sd-edge/.



ZTP Configuration

Protocol: Use TLS Encryption as the protocol.

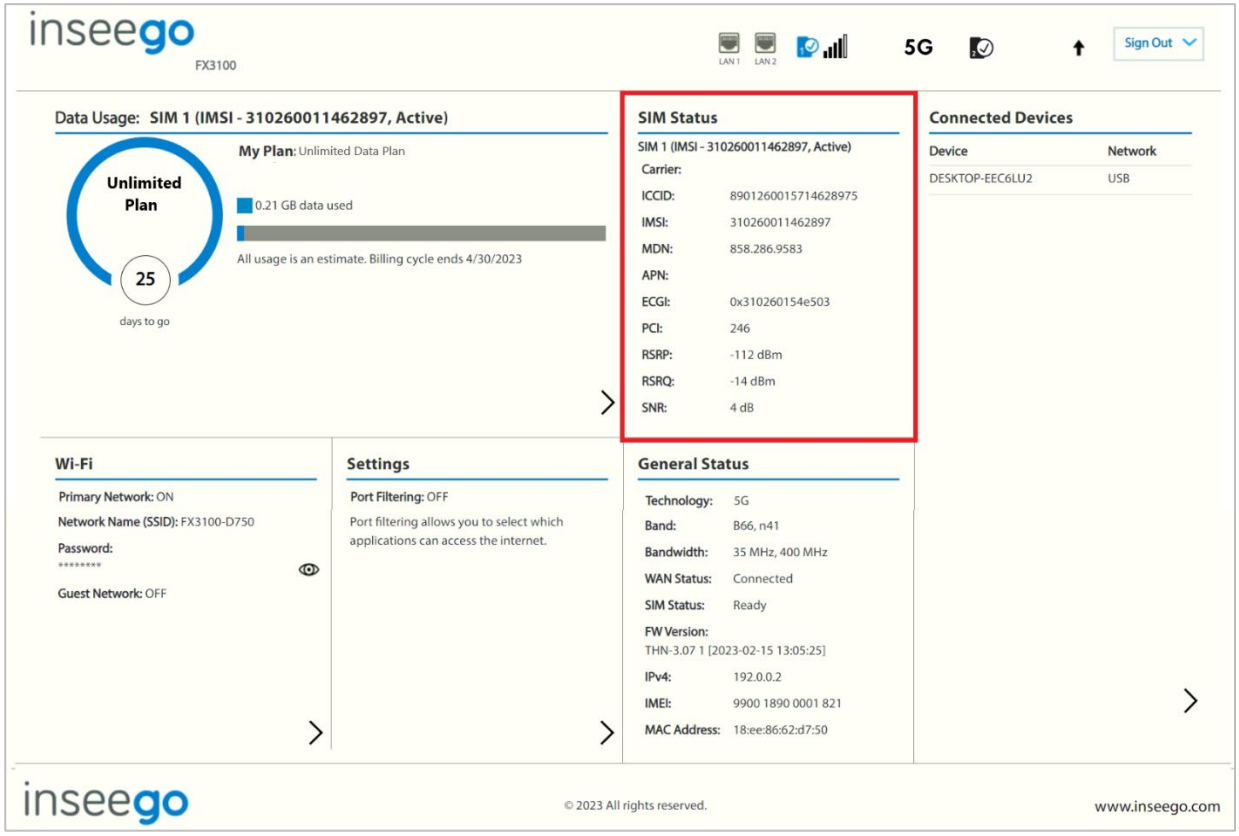
WARNING! **TLS Encryption** is strongly recommended. **Test** is plaintext for testing purposed only and may compromise the security of your network if used for deployment.

URL/IP Address: Enter the domain used for your EDGE Manager instance.

Click **Save Changes** to initiate ZTP.

SIM

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



SIM: The active SIM on which data is displayed.

Carrier: The name of the Mobile Network Operator.

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

IMSI: The International Mobile Subscriber Identity (IMSI) for your FX3100. This is a unique number, usually fifteen digits, that identifies a Global System for Mobile Communications (GSM) subscriber.

MDN: The phone number of your FX3100.

APN: The access point name for your FX3100.

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.

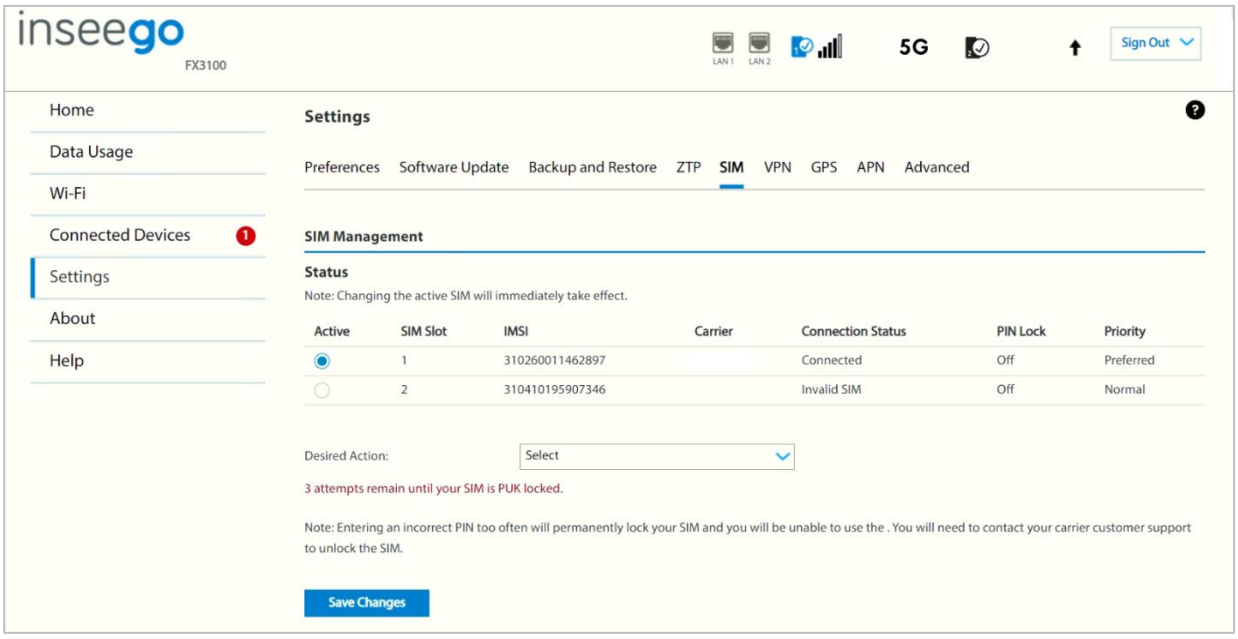
SNR: Signal to Noise Ratio. A ratio of signal power to noise power expressed in decibels. SNR is a positive value, and higher numbers are better.

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

SIM tab

The SIM card in your FX3100 can be locked using a PIN. If the SIM card is locked, you must enter the PIN before connecting to the mobile network. Once entered, the PIN is remembered until the next shutdown. You may also need to provide the existing PIN to change a SIM. The default PIN is available from your service provider.

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



SIM Management

Status

Active: Select the SIM you want to be active. **NOTE:** The change will take effect immediately.

SIM Slot: The SIM slot number.

IMSI: The International Mobile Subscriber Identity (IMSI) for your FX3100. This is a unique number, usually fifteen digits, that identifies a Global System for Mobile Communications (GSM) subscriber.

Carrier: The cellular carrier associated with the SIM.

Connection Status: The current status of the SIM.

PIN Lock: 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.

Priority: Indicates whether the SIM is Normal or Preferred priority.

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

Turn on PIN Lock - Sets the SIM so that entry of a PIN is required upon startup to connect to the mobile network. To perform this operation, you must enter the current PIN.

Turn off PIN Lock - Turns off a PIN lock that was previously turned on so that entry of a PIN is no longer required to connect to the mobile network. To perform this operation, you must enter the current PIN.

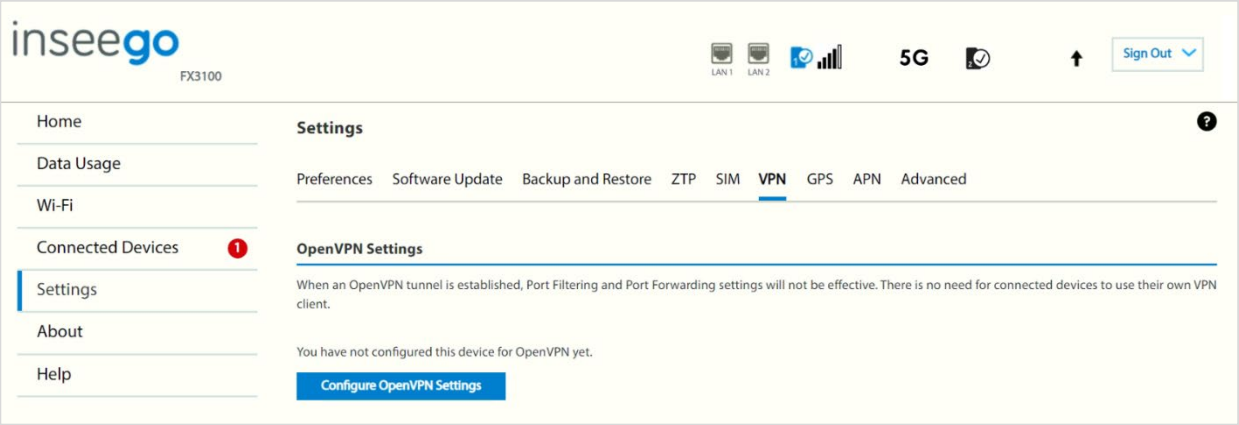
Change PIN - Allows you to change the SIM PIN. You must enter the current PIN, then enter the new PIN and confirm it.

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

Click **Save Changes**.

VPN tab

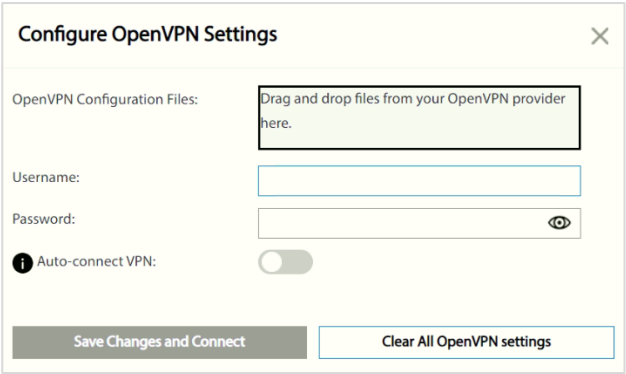
The FX3100 allows you to establish secure connections to remote networks over a public network using OpenVPN.



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 FX3100 for OpenVPN.

Connection status: Indicates the status of the OpenVPN connection.

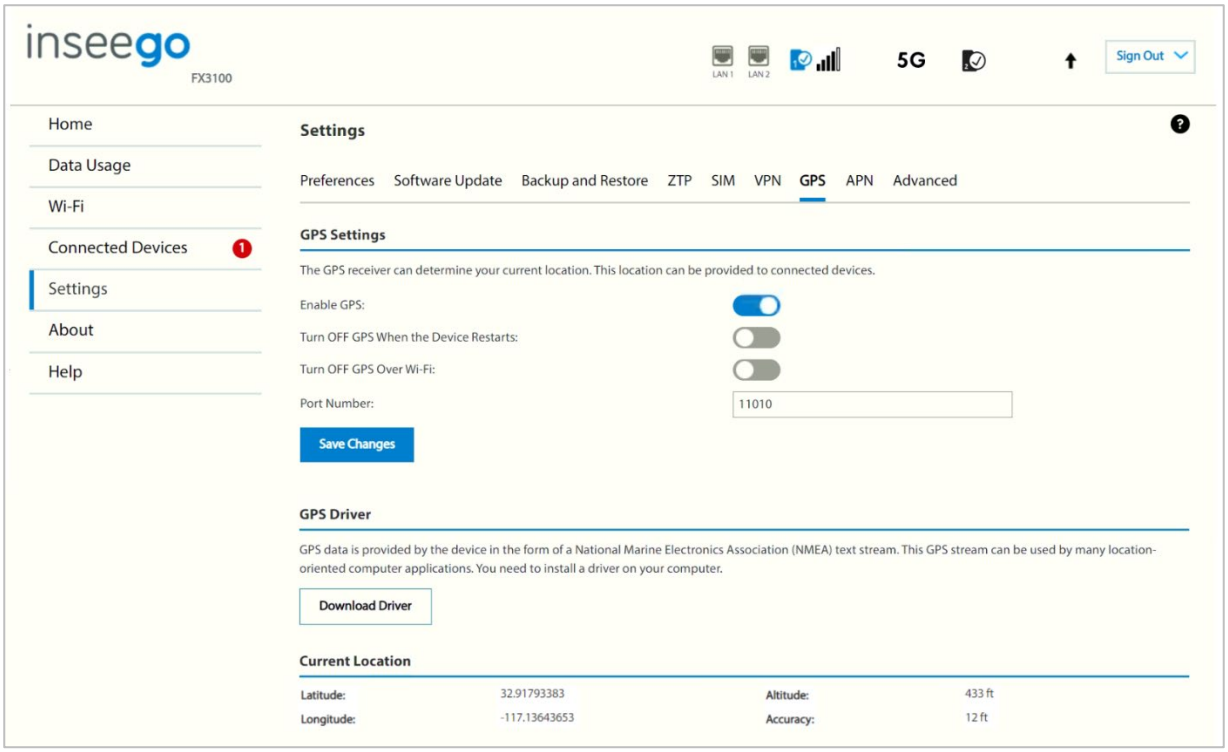
Connection time: The duration of the current OpenVPN connection.

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

Connect: Use this button to connect the OpenVPN.

GPS tab

The FX3100 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 FX3100. 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 FX3100is shut down. You will need to turn it on again the next time the GPS receiver is needed.

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

Port Number: The TCP port number used to establish a connection to the FX3100 and obtain raw GPS data for the GPS over Wi-Fi feature. Unless there is a good reason to do so, you should not change the port number. Acceptable port values are between 1024 and 65535.

Click **Save Changes** to update settings.

GPS Driver

For the GPS over Wi-Fi feature, if you want to access the GPS data stream from a virtual COM port instead of the TCP port (above), use the **Download Driver** button to download and install a GPS driver for your Windows platform. This driver creates a virtual NMEA port, obtains GPS data from the FX3100, and makes this GPS data available to NMEA-aware third-party applications.

Current Location

Latitude: Latitude for the last location fix.

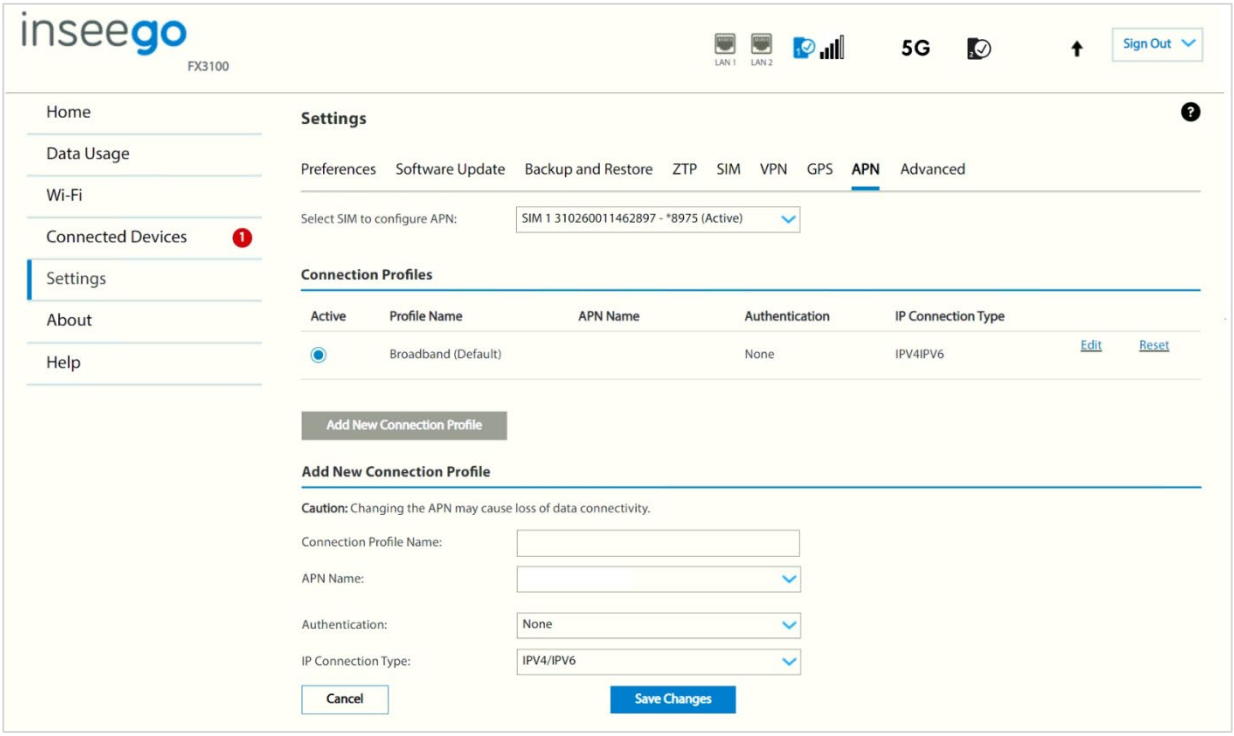
Longitude: Longitude for the last location fix.

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 FX3100 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 FX3100.



Select SIM to configure APN: Use the drop-down to select the SIM on which you want to configure the APN.

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 entered 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).

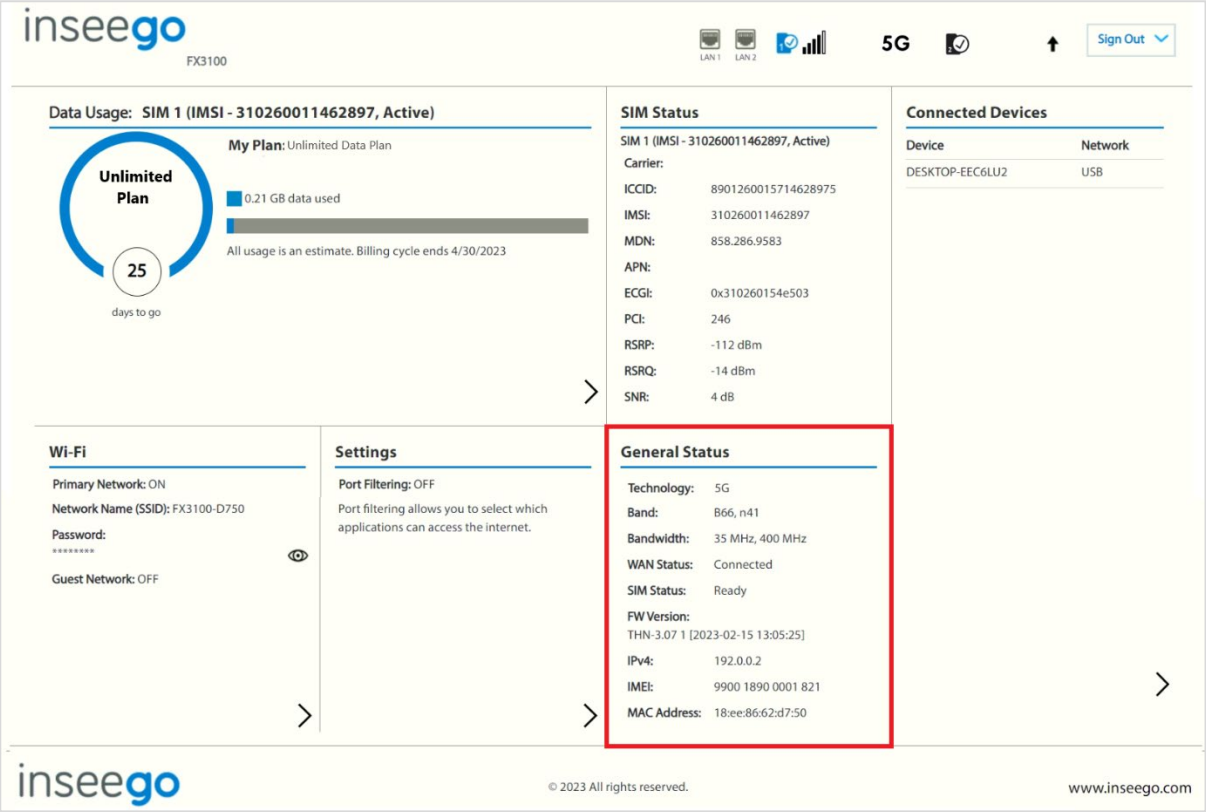
Click **Save Changes**.

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 64.

Viewing info about the FX3100

On the Admin web UI home page, the General Status panel provides an overview of the current FX3100 status.



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 FX3100.

IPv4: The internet IP address assigned to the FX3100.

IMEI: The International Mobile Equipment Identity (IMEI) for your FX3100. 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 FX3100. The MAC address is a unique network identifier assigned when a network device is manufactured.

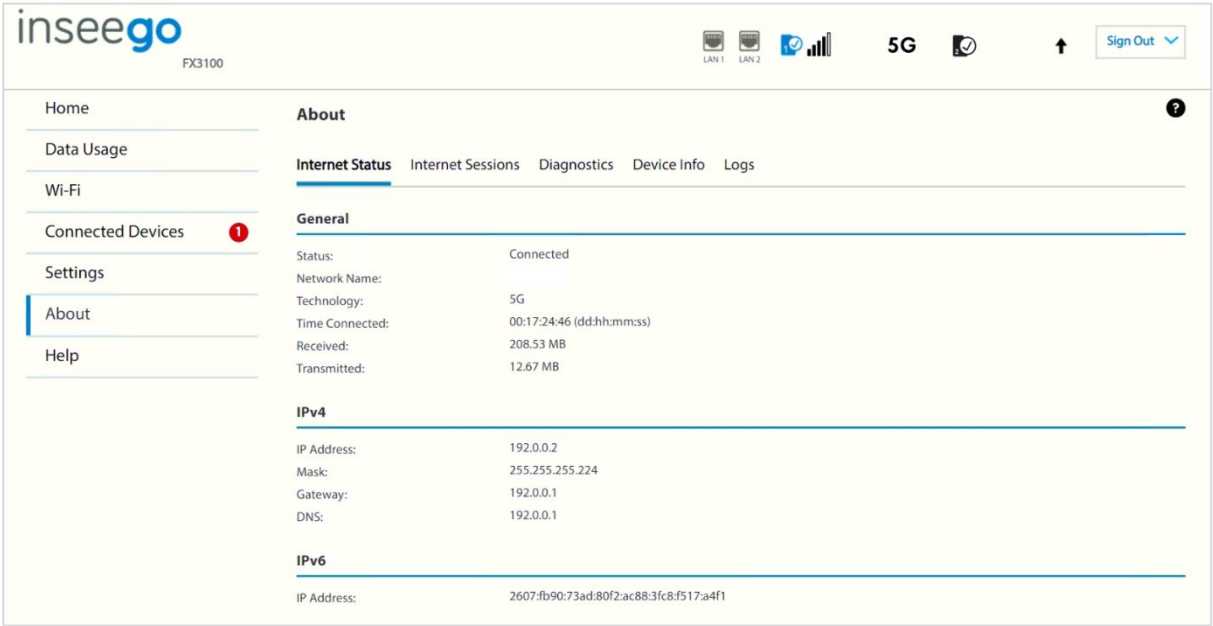
To view more detailed information about your FX3100 and its use, select > from the home page About panel or select **About** from the side menu.

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 FX3100 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 FX3100.

Mask: The network mask associated with the IPv4 address.

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

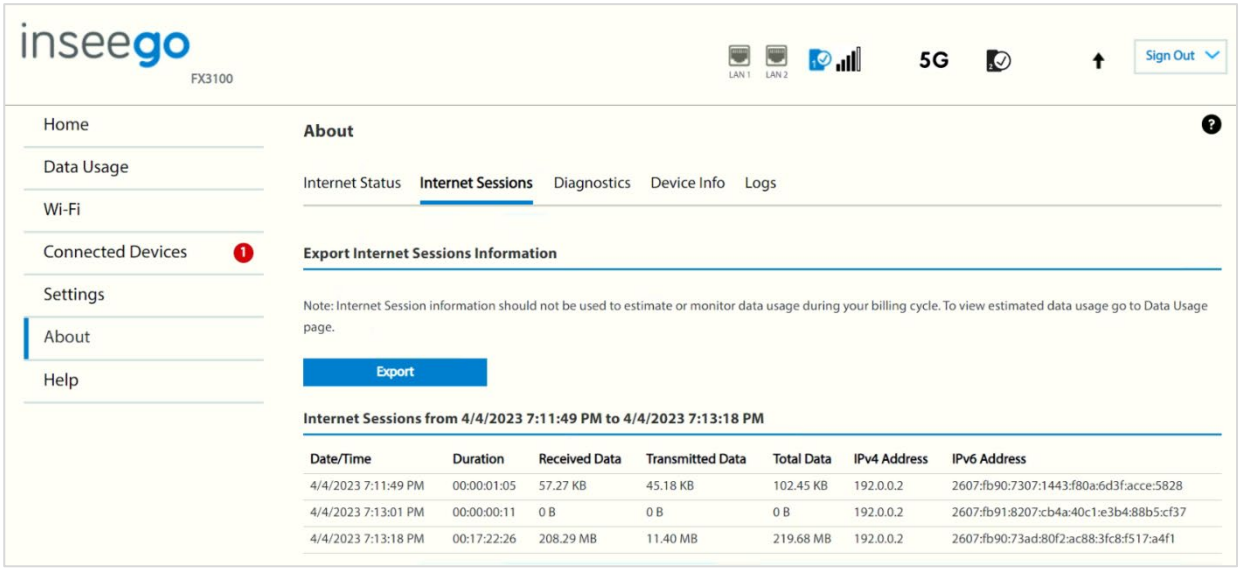
DNS: The Domain Name Server currently used by the FX3100.

IPv6

IP Address: The global IPv6 address for the FX3100 (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.

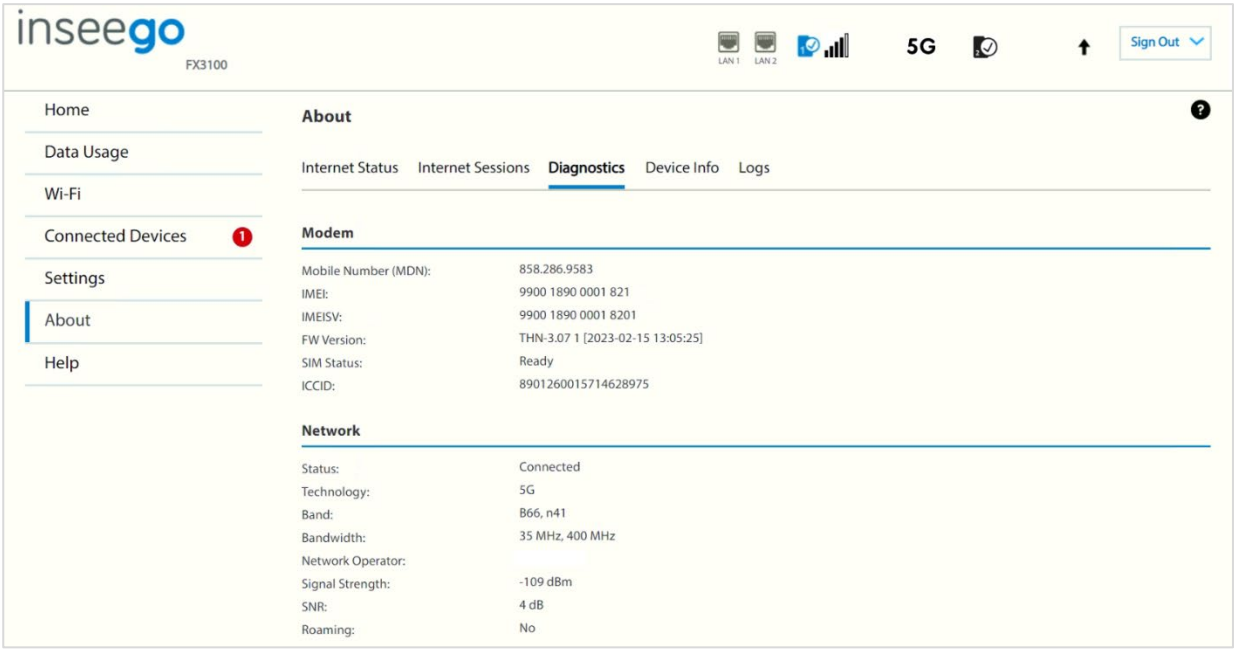
Total Data: The total amount of data for the internet session. This is the sum of Received Data and Transmitted Data.

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 FX3100.

IMEI: The International Mobile Equipment Identity (IMEI) for your FX3100. This is a 15-digit code used to uniquely identify an individual mobile station. The IMEI does not change when the SIM is changed.

IMEISI: 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 FX3100.

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

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

Network

Status: The status of the network.

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

Band: The band in use for the current connection.

Bandwidth: The bandwidth in use for the current connection.

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

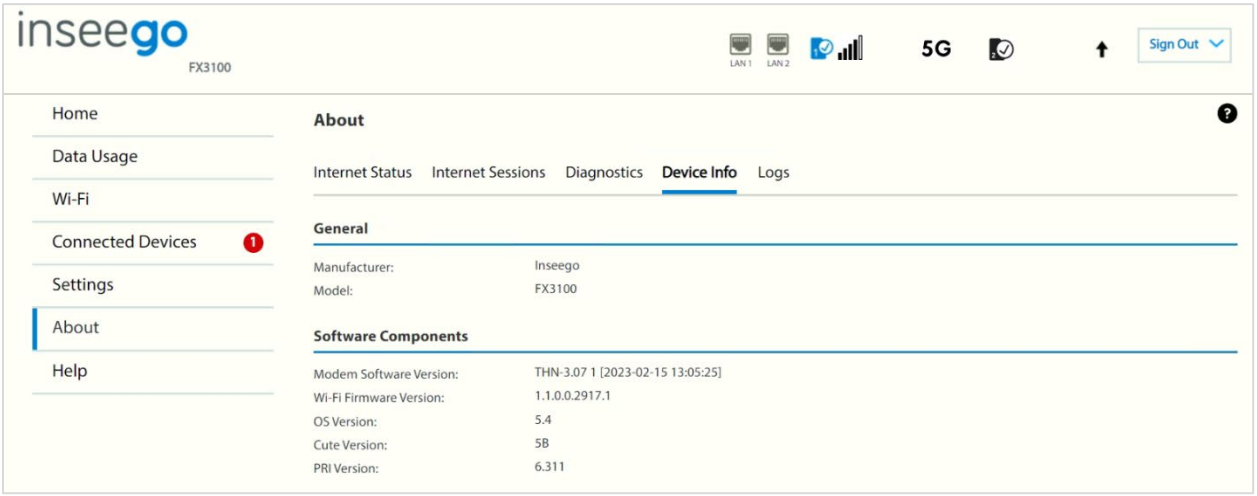
Signal Strength: The strength of the cellular signal (RSRP), measured in dBm. Higher absolute values indicate a stronger signal, for example: -80 dBm is a stronger signal than -90 dBm.

SNR: Signal to Noise Ratio. A 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 FX3100.



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.

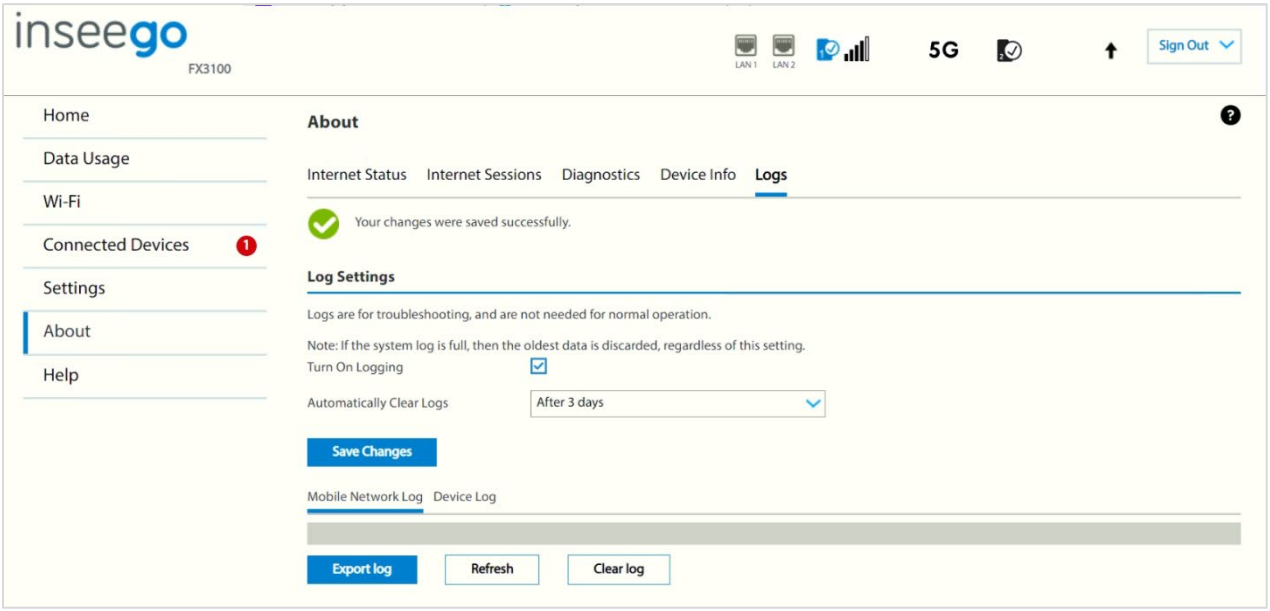
OS Version: The version number for the Operating System and its components.

Cute Version: The cute version of the software currently installed on your FX3100.

PRI Version: The configuration version currently applied to the FX3100.

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** for log data of connections to the mobile network.

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

Refresh: Updates the displayed log data.

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

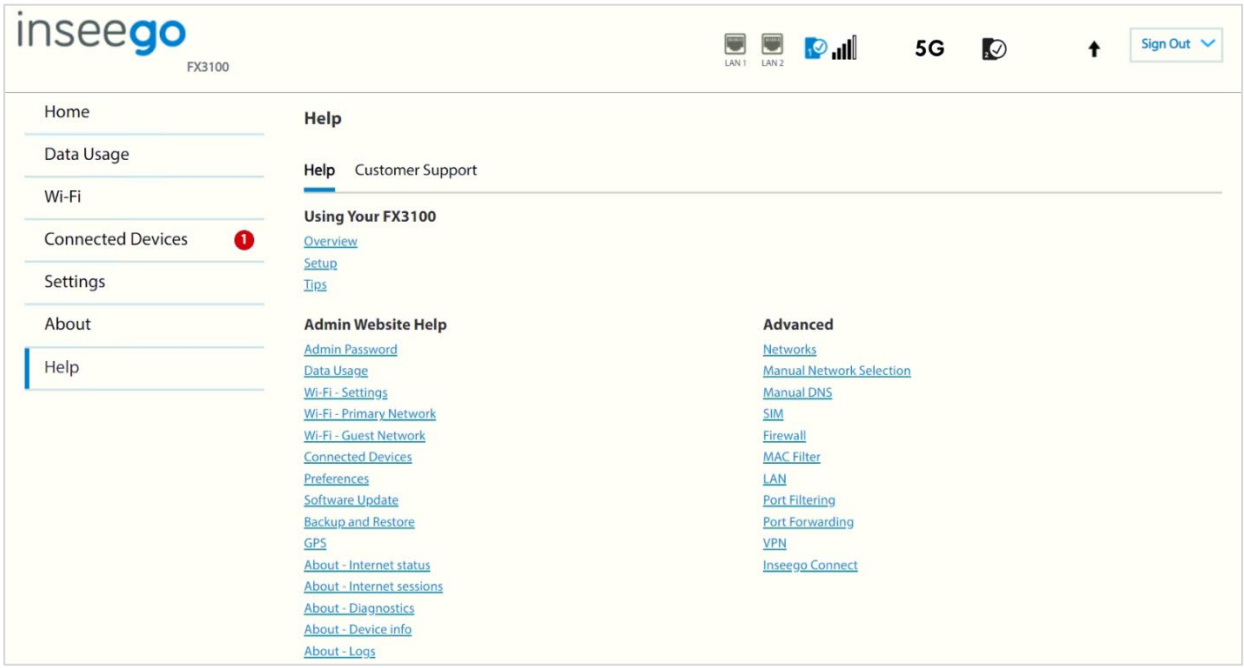
Export Logs: Allows you to export log data.

Getting support

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

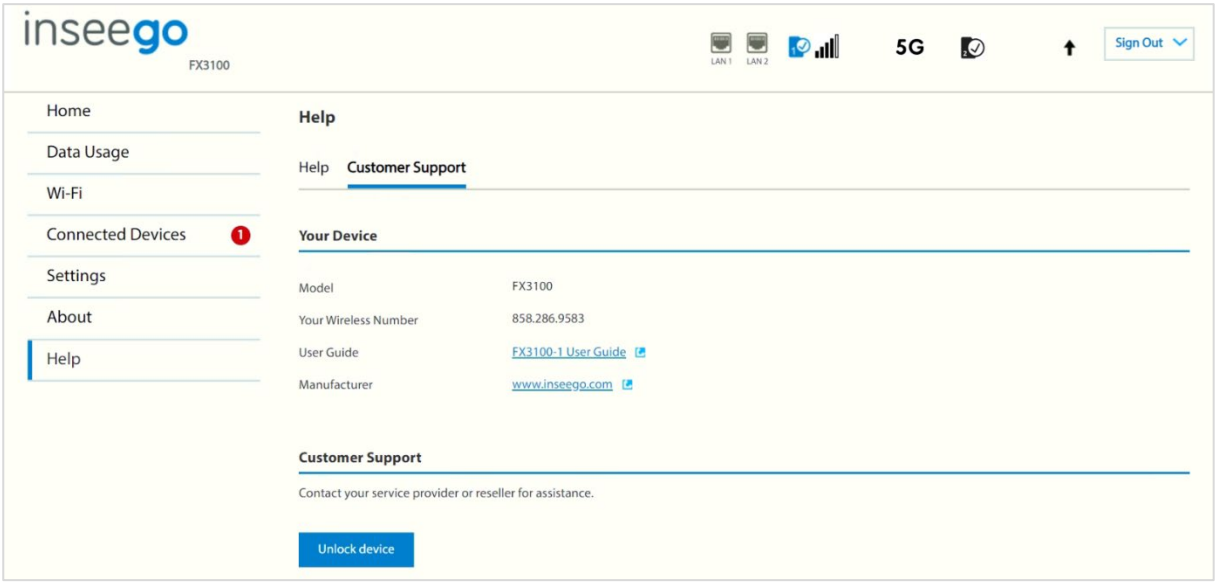
Help tab

This page provides links to help topics for every page of the Admin web UI and general topics useful for getting started with your FX3100.



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 FX3100.

User Guide: A link to this guide.

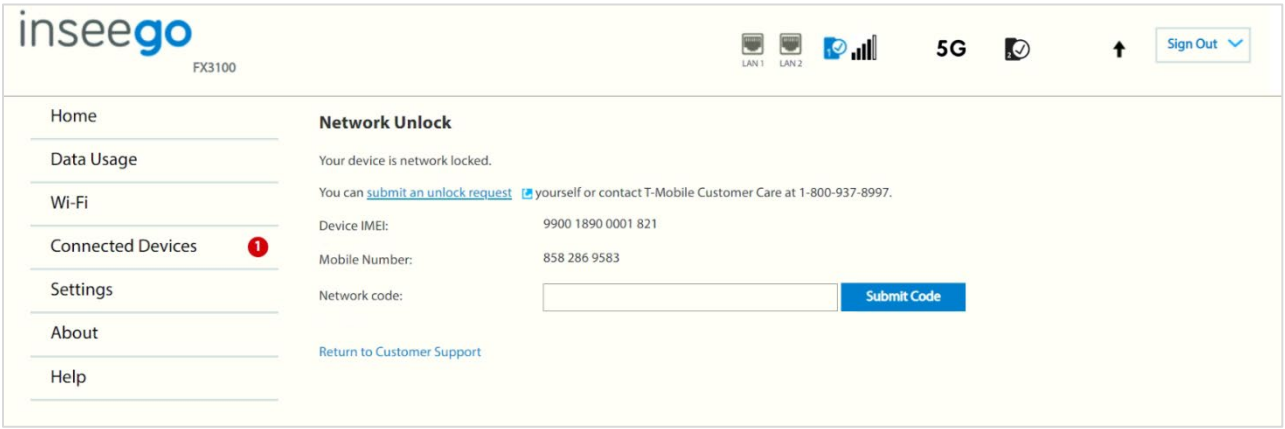
Manufacturer: A link to the Inseego website.

Customer Support

Contact your service provider for customer support.

Unlock/Lock device: To unlock a locked device, click **Unlock device**. The Network Unlock page appears.

NOTE: This button may not be visible, depending on your service provider.



To obtain a network code, click the **submit an unlock request** link, or follow the directions to contact your service provider.

Enter the code in the **Network code** text box and click **Submit Code**.

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

3

Advanced settings

Overview

Using advanced settings

Overview

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

WARNING! Changing the Advanced settings may be harmful to the stability, performance, and security of the FX3100.

Using advanced settings

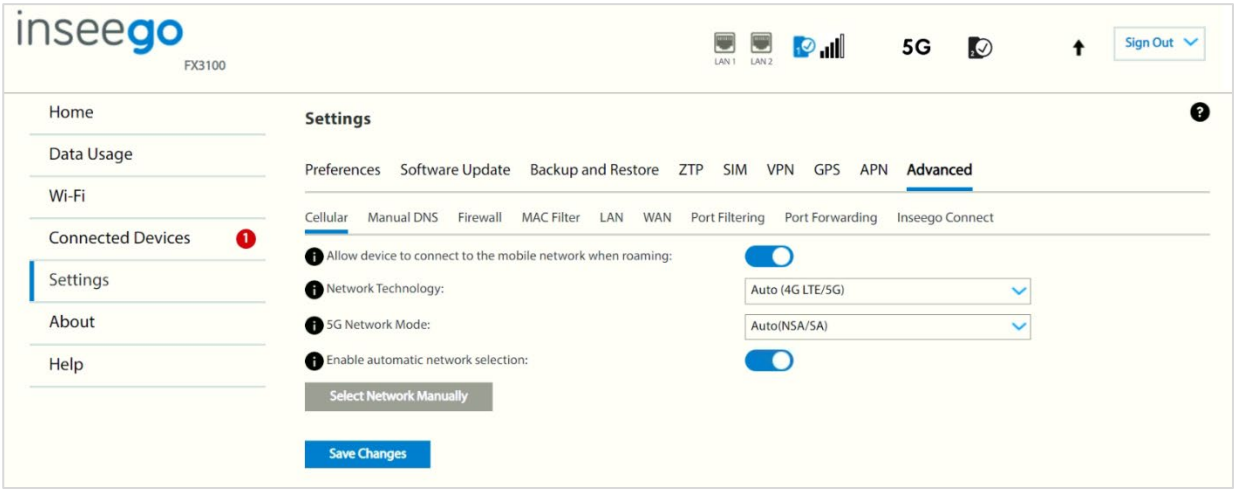
When you select the **Advanced** tab on the Settings page, a warning message appears. If you click **Continue**, the Network tab of the Advanced Settings page appears.

Advanced settings include:

- Cellular
- Manual DNS
- 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.



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 FX3100 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/UMTS or 5G from the drop-down, your FX3100 is restricted from connecting to networks not using that technology, for example: if you select 4G LTE/UMTS, your FX3100 will be unable to connect to 5G networks.

5G Network Mode: Your FX3100 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 FX3100 automatically selects the best 5G available 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**.

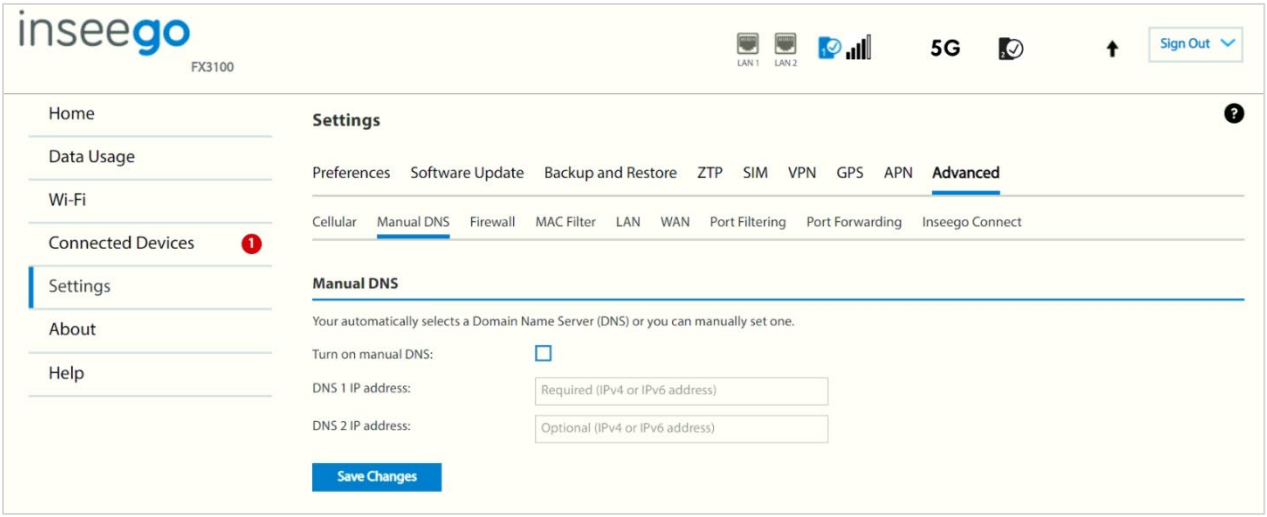
DNS

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 FX3100 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.

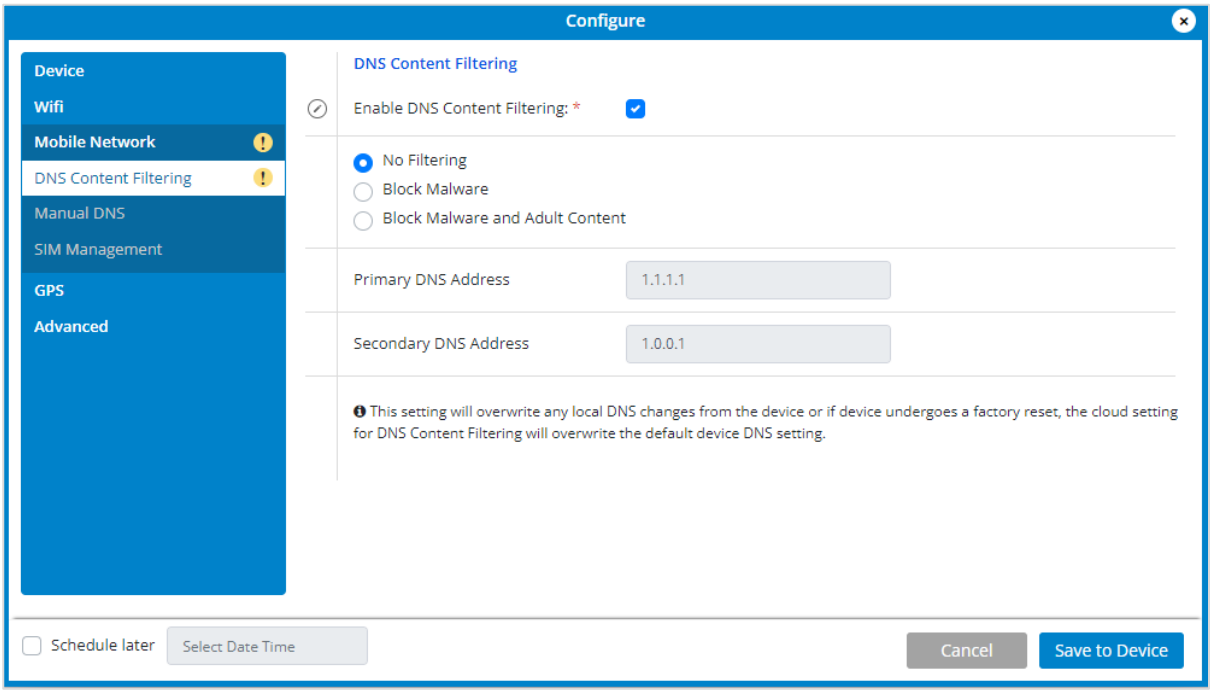
Click **Save Changes**.

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

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).



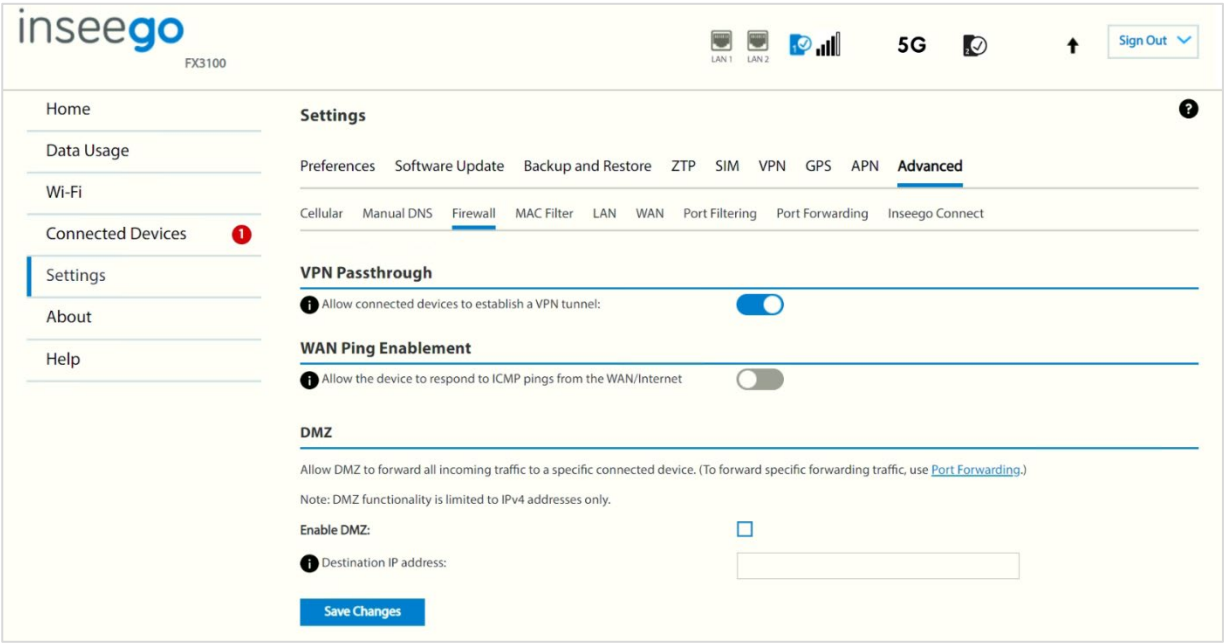
Enable DNS Content Filtering: Check this box to enable DNS content filtering.

Select the filter level (Block Malware, or Block Malware and Adult Content).

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

Firewall tab

The FX3100 firewall determines which internet traffic is allowed to pass between the FX3100 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 FX3100 will ignore ping requests received on the WAN interface. To enable your FX3100 to respond to the ping requests received on the WAN interface, 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.

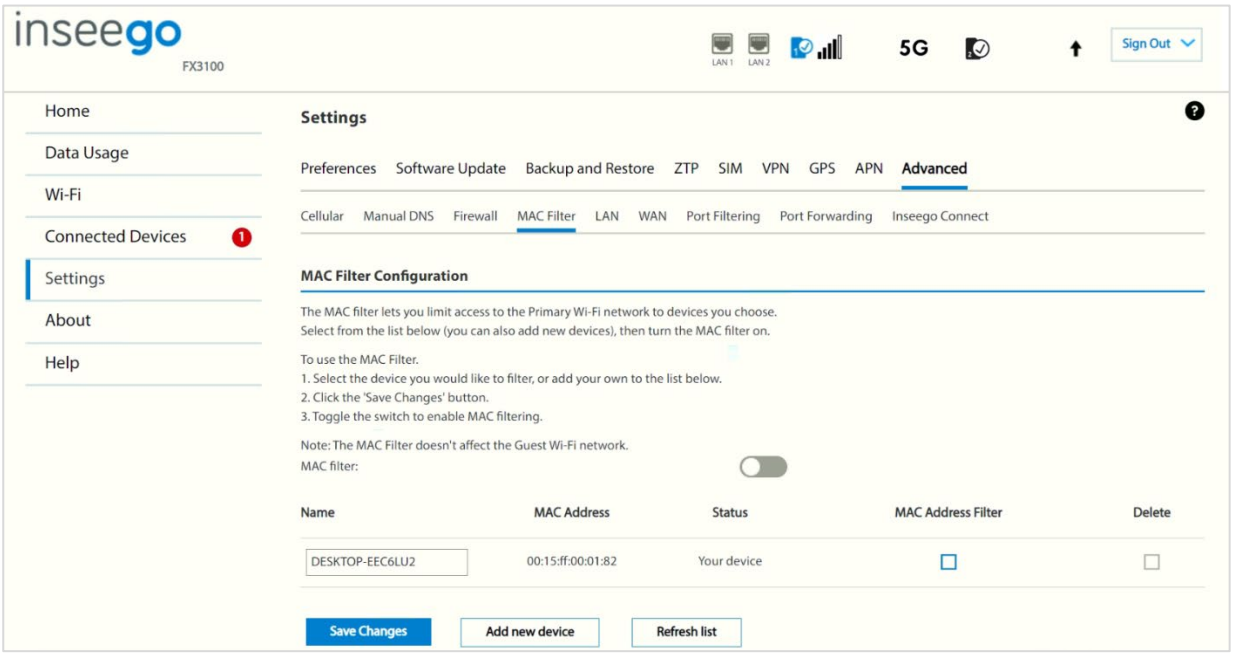
Destination IP address: Enter the IP address of the connected device you wish to become the DMZ device (the DMZ destination). **NOTE:** You can check the IP address of each connected device on the Connected Devices screen.

Click **Save Changes**.

MAC Filter tab

The MAC filter allows only selected devices to access the FX3100 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 FX3100.

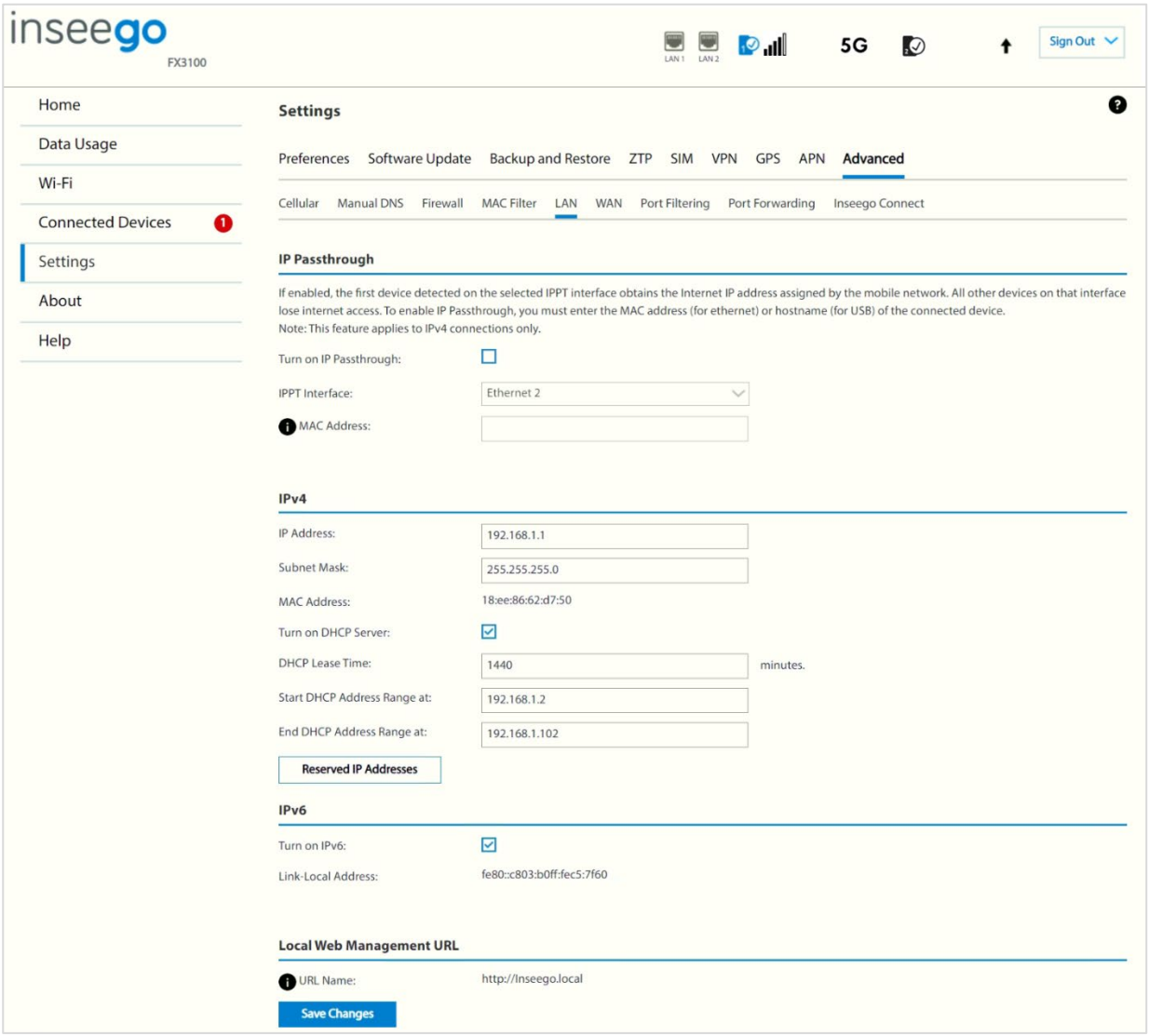
Add new device: Use this button to add a device to the device list, then enter the device name, MAC address, and choose whether to select the **MAC Address Filter** checkbox.

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 FX3100 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 LAN port to obtain the IP address assigned by the mobile network. IPPT allows you to enable a one-to-one connection to a host routing system. **NOTE:** When IP Passthrough is on, devices on other interfaces function normally. However, when IPPT is enabled, the following capabilities are set through the host routing system and web UI settings are not available:

- DMZ (Firewall)
- Port Filtering
- Port Forwarding

Turn on IP Passthrough: Check the box to enable IP Passthrough. **NOTE:** When Ethernet WAN is active, IP Passthrough cannot be enabled. You can change Ethernet WAN to LAN on **Settings > Advanced > WAN**.

IPPT Interface: Select an interface from the drop-down (Ethernet1, Ethernet2, or USB).

Hostname: When enabling IPPT on the USB interface, enter the hostname of the device connected for IP Passthrough. 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. 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 FX3100, as seen from the local network. Normally, you can use the default value.

Subnet Mask: The subnet mask network setting for the FX3100. 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 FX3100. The MAC address is a unique network identifier assigned when a network device is manufactured.

Turn on DHCP server: This checkbox turns the DHCP Server feature on or off. This should be left checked. The DHCP server allocates an IP address to each connected device. **NOTE:** If the DHCP Server is turned off, each connected device must be assigned a fixed IP address.

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

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

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

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.

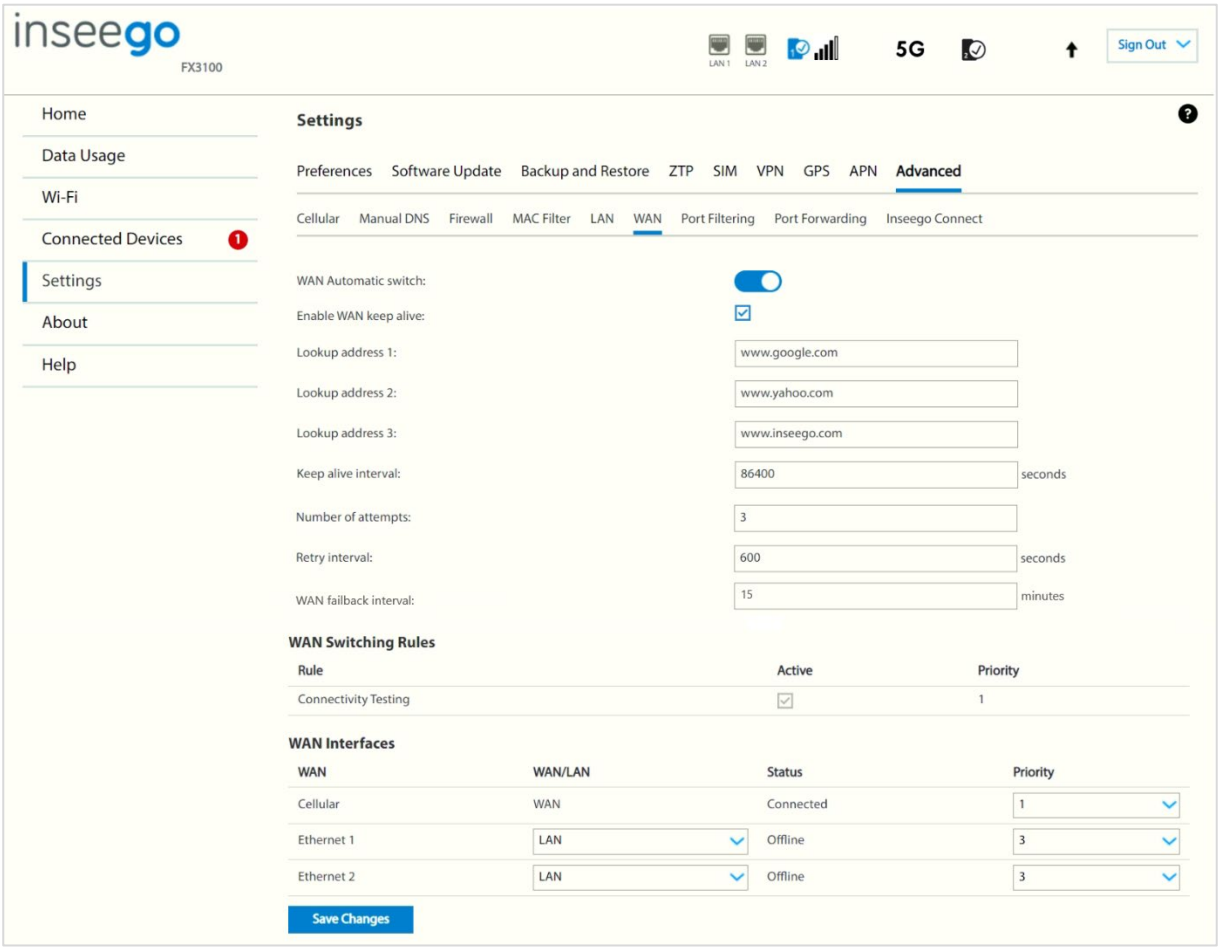
Local Web Management URL

URL Name: The URL name used to access the FX3100 local web UI**.**

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

WAN tab

Use this tab to select an active WAN interface, set WAN priorities, and configure keep alive. Keepalive allows for a persistent WAN connection.



WAN Automatic switch: Use the ON/OFF slider to enable/disable the automatic selection of WAN interfaces.

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 without receiving a valid packet before the first keep alive verification occurs. 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 re-activate 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, Ethernet1, or Ethernet2).

WAN/LAN: Use the drop-down to select WAN or LAN for your Ethernet interfaces.
NOTE: Although Ethernet ports are labeled as WAN or LAN on the device, you can configure them to be either WAN or LAN.

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

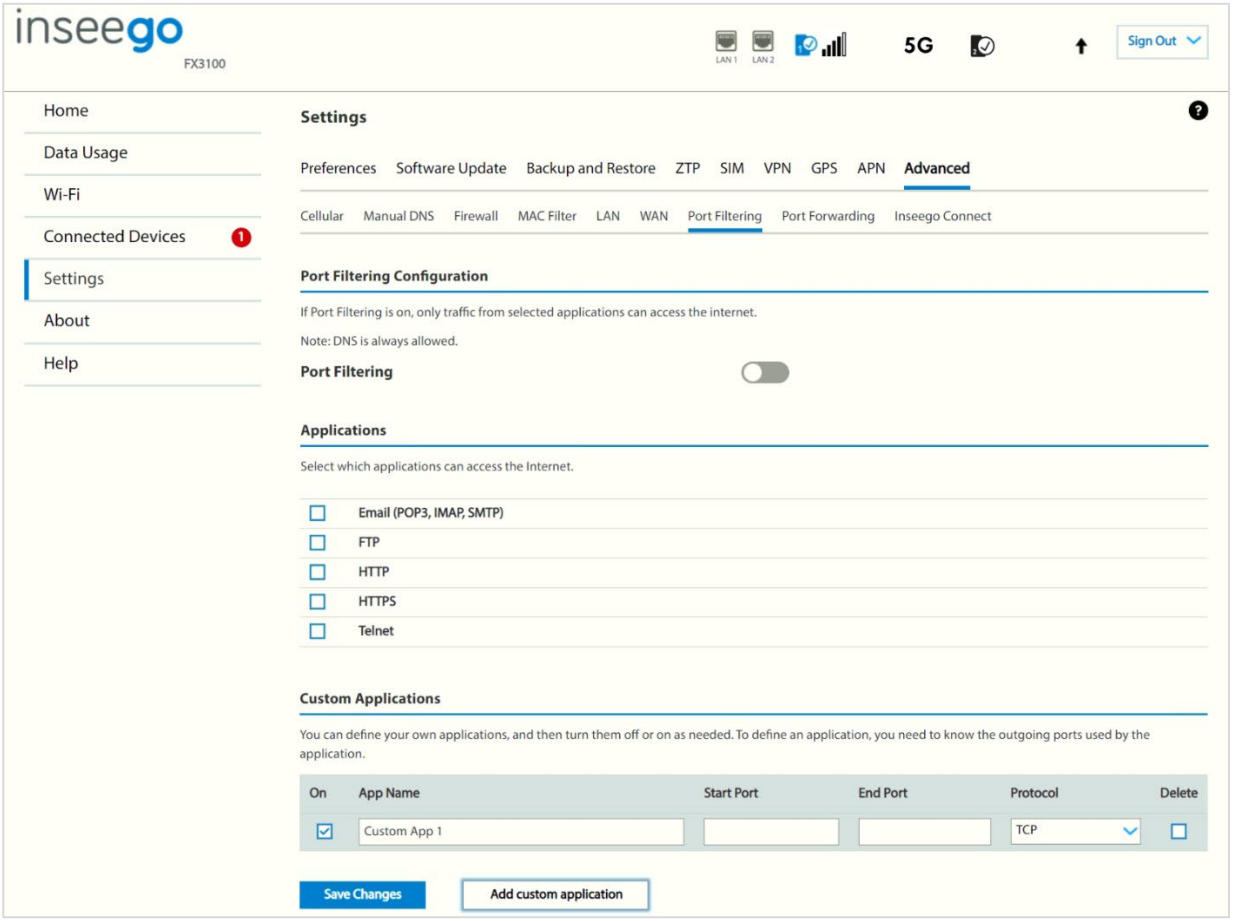
Priority: Use the drop-down to set a priority for each WAN interface.

Click **Save changes** to save new settings. A pop-up appears alerting you that your FX3100 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	110	Yes	No	Assigned
POP3S	995	Yes	No	Yes
IMAP	143	Yes	No	Assigned
IMAPS	993	Yes	No	Assigned
SMTP	25	Yes	No	Assigned
SecureSMTP	465	Yes	No	No
FTP control (command)	21	Yes	Yes	Assigned
FTP data transfer	20	Yes	Yes	Assigned
HTTP	80	Yes	Yes	Assigned
HTTPS	443	Yes	Yes	Assigned
Telnet	23	Yes	No	Assigned

Custom Applications

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

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

App Name: Enter a name for the custom application.

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

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

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

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

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

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

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

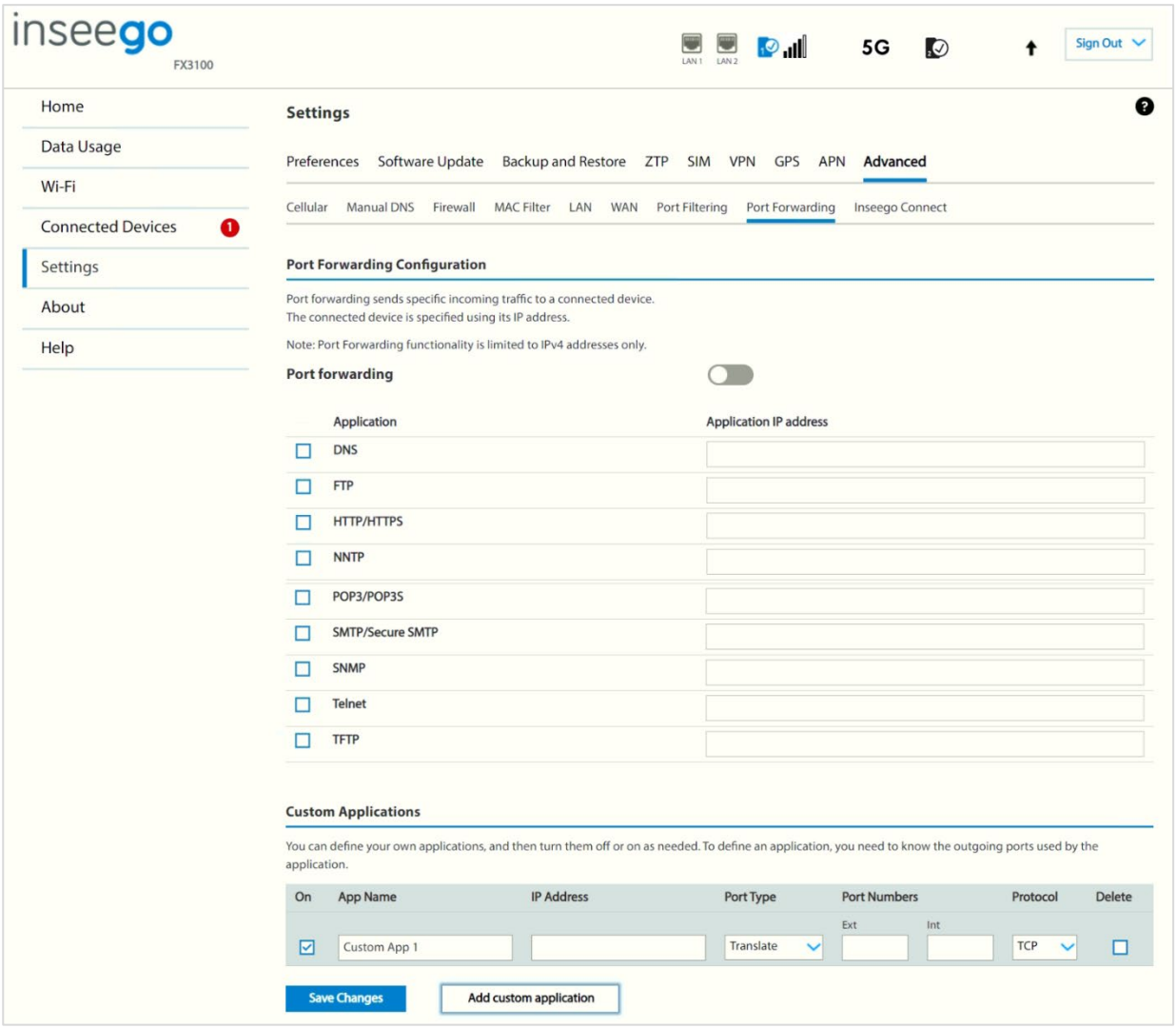
Port Forwarding tab

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

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

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

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



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: Select Range or Translate from the drop-down list.

Port Numbers: Use the **From** and **To** fields to specify the range of port numbers to be forwarded. **NOTE:** If the application uses a single port instead of a range, type the same value in both the **From** and **To** fields.

For translate ports, use the **Ext.** and **Int.** to specify ports. **NOTE:** Forwarding takes inbound traffic on a port to the same port on a client device. Use translate ports to send traffic to a different port on the client device. For example, instead of having inbound traffic on port 1234 forward to port 1234 of the client device, you can have it forward to port 5678.

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

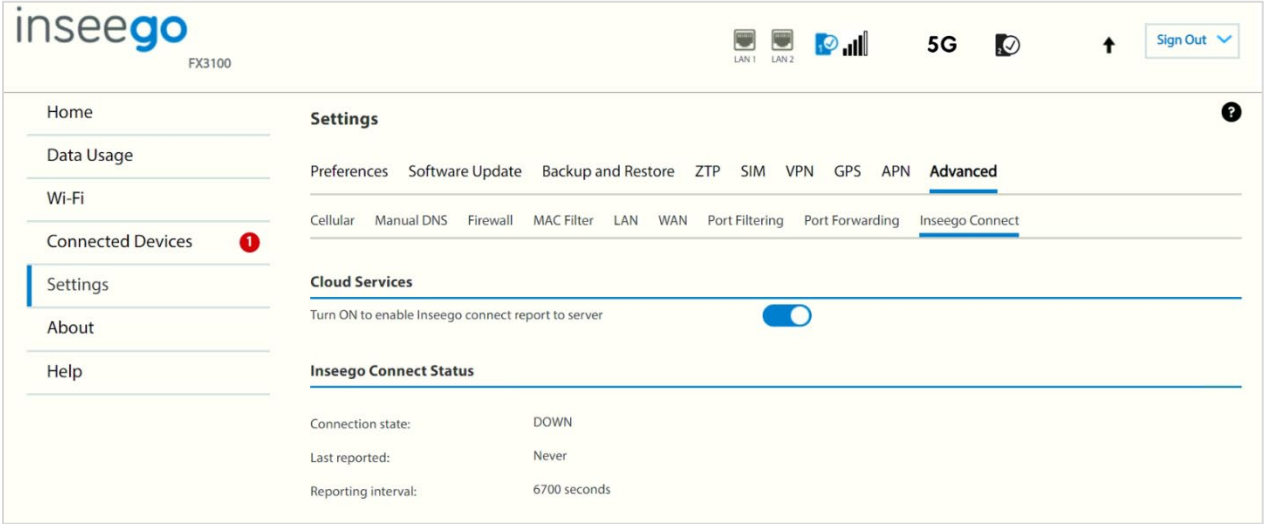
Delete: Check this box to delete a custom application. **NOTE:** Click on the Port Forwarding tab again to remove deleted custom applications from view on the screen.

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

Inseego Connect tab

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

IMPORTANT: After adding a device to Inseego Connect, restart the device immediately. This allows the device to check in and process the registration request.



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** – FX3100 is communicating with Inseego Connect servers.
- **DOWN** – FX3100 is NOT communicating with Inseego Connect servers.

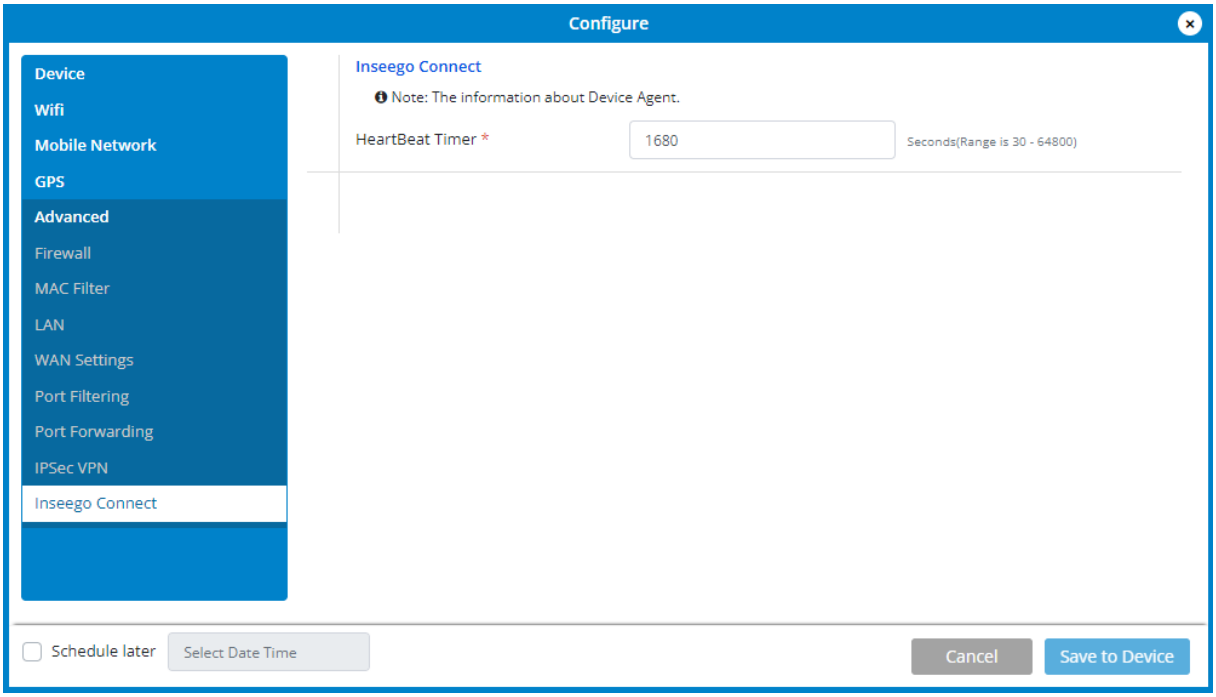
Last Reported: The time when FX3100 last sent a packet to Inseego Connect servers.

Reporting Interval: This is the interval at which your FX3100 will send packets to the Inseego Connect server. **NOTE:** A shorter interval means more data usage.

Heartbeat timer (Inseego Connect)

Your FX3100 sends a lightweight heartbeat packet to Inseego connect at a regular interval to indicate that the device is online. The default interval is 1680 seconds (28 minutes).

You can adjust the frequency of the heartbeat timer in Inseego Connect on the Inseego Connect configuration screen. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free Inseego Connect account at connect.inseego.



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

Click **Save to Device**.

4

Troubleshooting and support

Overview

Common problems and solutions

Technical support

Overview

When properly installed, the FX3100 is a highly reliable product.

The following tips can help solve many common problems encountered while using the FX3100:

- Make sure you are using the FX3100 in the correct geographic region.
- Ensure that your wireless coverage extends to your current location.
- If you do not receive a strong data signal, move the device to a different location.
- Ensure that you have an active subscription plan.
- You can resolve many issues by restarting your connected device and your FX3100.

Troubleshooting

This section can help solve many common problems and answer questions encountered while using the FX3100.

Will I always get 5G? Can I use the FX3100 outside of 5G coverage?

While this router is marketed as a 5G indoor 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 FX3100 LED is switching from blue to green and sometimes dropping service

- **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/UMTS**.

Can I set my FX3100 to use a specific band?

No, the FX3100 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 primary network, by USB or Ethernet.

The FX3100 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:
    - Turn off the FX3100, 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 FX3100.
    - Ask your service provider:
      - Is your SIM active and on a plan compatible with the FX3100.
      - 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 **Home** page, check the **SIM status**. 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.
      - 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 > SIM**, check for a locked SIM.

My older device cannot connect

If you can see other networks, but not the network name for your FX3100:

- **Reason:** The default multi-mode settings on your FX3100 work for most Wi-Fi clients, however, some older devices require that you set one of the Wi-Fi bands to support older BGN standards.

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

  1. Access the FX3100 Admin web UI and navigate to **Wi-Fi > Settings**. Under **2.4 GHz Band Settings**, use the drop-down to change the 802.11 mode to **802.11 bgn**.
     NOTE: This allows older devices to connect on the 2.4 GHz band but leaves the 5 GHz band in multi-mode to allow newer devices the fastest available connection.
  2. Click **Save Changes**. Your FX3100 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 FX3100:

- **Reason:** The default network security settings on your FX3100 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 FX3100 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 FX3100 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 special characters or long passwords.

  Solution: Change your Wi-Fi password.

  1. Access the FX3100 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 8 and 16 characters, using only numbers, uppercase letters, and lowercase letters.
  2. Click **Save Changes** and **Confirm**. Your FX3100 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 FX3100 Admin web UI and navigate to **Wi-Fi > Settings**. Uncheck **5 GHz** and use only **2.4 GHz**.
  2. Click **Save Changes**. Your FX3100 will reboot, and your device should be able to connect.

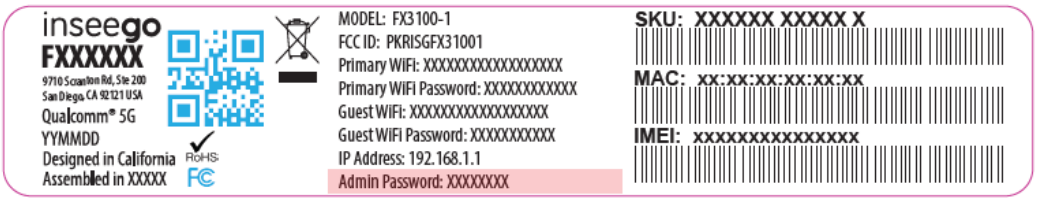
My FX3100 is “Waiting for Connection” on the Inseego Mobile app

- **Reason:** The registration request is still processing.

  Solution: Restart the device. This allows the device to check in and process the registration request.

- **Reason:** You entered an incorrect password for the device or changed the Admin password before Inseego Connect fully processed the registration request.

  - **Solution:** From the Inseego Mobile app or Inseego Connect, delete the device from the Device List and add it again using the current Admin password. If you have already logged into the device’s Admin web UI and changed the Admin password, use the new password. If you have not changed the Admin password, the default is printed on the bottom of the device.



  Restart the device. This allows the device to check in and process the registration request.

My FX3100 is getting slow speeds/low throughput

- **Reason:** Signal strength and quality are the most likely cause of slow speeds/low throughput. **NOTE:** The FX3100 is configured by default to use the best connection available, so low throughput is rarely related to configuration.

  Solution: Check the signal strength and quality reported by your FX3100:

  1. Access the FX3100 Admin web UI and navigate to **About > Diagnostics** to check the values for **Signal Strength (RSRP)** and **SNR.**

  2. **If the signal is poor**, relocate your FX3100 to improve signal conditions.

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

My connecting device is not obtaining a valid IP address

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

- **Reason:** IPPT is enabled, and you have connected a second device to your FX3100 without restarting.
  When IP Passthrough (IPPT) is enabled, only the first device detected can obtain the IP address assigned by the mobile network.

  Solution: When IPPT is enabled, any time you switch the device you are connecting to the FX3100, you must first disconnect the existing connected device and power cycle the FX3100before connecting the new device.

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

  Solutions:
  Reset your FX3100 to factory settings, see “Resetting your FX3100” on page 16.
  or
  Use Inseego Mobile 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 FX3100, but if you have connected a succession of devices to your FX3100 in a short period of time, you may have used up all the IP address available.

  Solution: Disconnect your connected device and power cycle the FX3100 before reconnecting a device.

- **Reason:** There is an issue with your FX3100.

  Solution: Contact your service provider for assistance.

I cannot get streaming platforms to work with my FX3100

- **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?

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

Cellular signal amplifiers/boosters typically work by receiving and re-transmitting specific frequencies. This can increase the amount of signal noise, which has a negative effect on connectivity. In addition, when specific frequencies are targeted, other frequencies can be effectively filtered or blocked. If not all 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 FX3100 to provide a network connection via Remote Network Driver Interface Specification (RNDIS). Most major operating systems support RNDIS. There are no device-specific drivers for the USB port, so any drivers needed are related to the PC operating system.

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

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

Technical support

IMPORTANT: Before reaching out for support, be sure to restart both your connected device and your FX3100 and ensure that your SIM card is inserted correctly.

Customer Service and Troubleshooting
Contact your service provider for assistance.

More Information
Documentation for your FX3100 is available online. Go to https://inseego.com/resources/product-documentation. Or, from the Admin website, select **Help > Customer Support**.

5

Product specifications and regulatory information

Product specifications

Regulatory information

Product certifications and supplier's declarations of conformity

Wireless communications

Limited warranty and liability

Safety hazards

Product specifications

Device

Name:	FX3100
Model:	FX3100-1
Regulatory:	FCC(US)
Certifications:	GCF, PTCRB REACH, RoHS, WEEE
Dimensions:	160 mm x 76 mm x 52 mm (6.3” x 3” x 2”)
Weight:	350 g (12 oz)
Ports:	2x LAN/WAN 1 Gbps 1x USB 3.1 Type C (data and tethering) 1x external antenna (2 TS-9)
SIM:	Dual SIM, (2) 4FF Nano SIM slots
Chipset:	Qualcomm® Snapdragon™ SDX62
LED:	Status

Environmental

Operating temperature:	0° C to 40° C (32°F to 104°F)
Storage temperature:	-30° C to +70° C (-22°F to 158° F)

Network connectivity*

5G NR with SA/NSA
5G sub-6 GHz
4G LTE Cat 19
4x4 MIMO sub-6 GHz
256 QAM sub-6 GHz
CBRS

* Data plan required. Coverage subject to network availability.

Wi-Fi

802.11 a/b/g/n/ac/ax	
Wi-Fi 6 with 2x2 MU-MIMO	
Simultaneous dual-band Wi-Fi	
Multiple SSID/guest Wi-Fi support	
Supports up to 64 simultaneous Wi-Fi enabled devices	

Security

Secure boot	
Admin security:	AES 256 encryption • Security hardened web interface • Password hash • Session timeout • Wi-Fi on/off control • Incorrect password lockout
Encrypted configuration backup/restore	
Advanced firewall	
Wi-Fi security:	Wi-Fi security (WPA/WPA2/WPA3) • Wi-Fi privacy separation
Anti CSRF (OWASP)	
OpenVPN	
Static IP	

Networking

Configurable DNS	
MAC address filtering	
NAT firewall	
Port forwarding	
Port filtering	
Auto and custom APN	
MTU configuration	
Network selection and band lock	
Inseego Connect and Inseego 5G SD EDGE	

Regulatory information

Federal Communications Commission Notice (FCC – United States)

FCC ID: PKRISGFX31001

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:

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

WWAN band	Antenna gain (dBi)
4G-LTE: B48 5G-FR1: n48, n77	≤ 1.5
4G-LTE: B2 5G-FR1: n2, n25	≤ 1.6
4G-LTE: B66 5G-FR1: n66	≤ 1.8
4G-LTE: B4	≤ 1.9
4G-LTE: B41 5G-FR1: n38, n41	≤ 2.8

Product certifications and supplier's declarations of conformity

Product certifications and supplier's declarations of conformity documentation may be consulted at Inseego Corp., 9710 Scranton Road Suite 200, San Diego CA 92121, USA. https://www.inseego.com/support/.

Energy efficiency

Efficiency performance is based on the U.S. Department of Energy Federal Energy Conservation Standards for Battery Chargers.

Energy efficiency terms - the energy efficiency values are based on the following conditions:

- **Power adapter, no-load:** Condition in which the FX3100 power adapter is connected to AC power, but not connected to device.
- **Power adapter efficiency:** Average of the FX3100 power adapter with the measured efficiency when tested at 100 percent, 75 percent, 50 percent, and 25 percent of the power adapter's rated output current.

Mode	Power consumption for FX3100	
	115V	230V
Power adapter, no load	0.03W	0.065W
Power adapter efficiency	87.03%	87.39%

Wireless communications

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

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

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

Inseego Corp. or its partners will not be held responsible for damages of any kind resulting from the delays or errors in data transmitted or received with the FX3100 device, or failure of the FX3100 device to transmit or receive such data.

Limited warranty and liability

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

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

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

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

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

Safety hazards

Do not operate the FX3100 in an environment that might be susceptible to radio interference resulting in danger, specifically:

Areas where prohibited by the law

Follow any special rules and regulations and obey all signs and notices. Always turn off the host device when instructed to do so, or when you suspect that it might cause interference or danger.

Where explosive atmospheres might be present

Do not operate your device in any area where a potentially explosive atmosphere might exist. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Be aware and comply with all signs and instructions.

Users are advised not to operate the device while at a refueling point or service station. Users are reminded to observe restrictions on the use of radio equipment in fuel depots (fuel storage and distribution areas), chemical plants or where blasting operations are in progress.

Areas with a potentially explosive atmosphere are often but not always clearly marked. Potential locations can include gas stations, below deck on boats, chemical transfer or storage facilities, vehicles using liquefied petroleum gas (such as propane or butane), areas where the air contains chemicals or particles, such as grain, dust or metal powders, and any other area where you would normally be advised to turn off your vehicle engine.

Near medical and life support equipment

Do not operate your device in any area where medical equipment, life support equipment, or near any equipment that might be susceptible to any form of radio interference. In such areas, the host communications device must be turned off. The device can transmit signals that could interfere with this equipment.

On an aircraft, either on the ground or airborne

In addition to FAA requirements, many airline regulations state that you must suspend wireless operations before boarding an airplane. Please ensure that the modem is turned off prior to boarding aircraft in order to comply with these regulations. The modem can transmit signals that could interfere with various onboard systems and controls.

While operating a vehicle

The driver or operator of any vehicle should not operate a wireless data device while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some countries, operating such communications devices while in control of a vehicle is an offense.

Electrostatic Discharge (ESD)

Electrical and electronic devices are sensitive to electrostatic discharge (ESD). Macintosh native connection software might attempt to reinitialize the device should a substantial electrostatic discharge reset the device. If the software is not operational after an ESD occurrence, then restart your computer.

6

Glossary

Glossary

- **4G LTE** —Fourth Generation Long Term Evolution. LTE is a standard for wireless data communications technology and an evolution of the GSM/UMTS standards. The goal of LTE is to increase the capacity and speed of wireless data networks using new DSP (digital signal processing) techniques and modulations that were developed around the turn of the millennium. A further goal is the redesign and simplification of the network architecture to an IP-based system with significantly reduced transfer latency compared to the 3G architecture. The LTE wireless interface is incompatible with 2G and 3G networks, so that it must be operated on a separate wireless spectrum

- **5G**—Fifth Generation. The successor to 4GLTE technology, offering greater bandwidth and higher download speeds. In addition to serving cellular networks, 5G networks can be used as internet service providers, competing with other ISPs. 5G also opens up new IoT and M2M possibilities. Wireless devices must be 5G enabled to use 5G networks.

- **802.11 (a, b, g, n, ax)** — A set of WLAN Wi-Fi communication standards in the 2.4 and 5 GHz frequency bands.

- **APN** — Access Point Name. The name of a gateway between a mobile network and another computer network, often the internet.

- **bps** — Bits per second. The rate of data flow.

- **Broadband** — High-capacity high-speed transmission channel with a wider bandwidth than conventional modem lines. Broadband channels can carry video, voice, and data simultaneously.

- **DHCP** — Dynamic Host Configuration Protocol. Software found in servers and routers that automatically assigns IP addresses and other configuration data to computers, tablets, printers, and other devices connection to the IP network.

- **DHCP Server** — A server or service with a server that assigns IP addresses.

- **DMZ** — DeMilitarized Zone. A sub-network that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the internet.

- **DNS** — Domain Name System. A system for converting host names and domain names into IP addresses on the internet or on local networks that use the TCP/IP protocol.

- **Firmware** — A computer program embedded in an electronic device. Firmware usually contains operating code for the device.

- **FTP** — File Transfer Protocol. A standard network protocol used to transfer computer files between a client and server.

- **GB** — Gigabyte. A multiple of the unit byte for digital information storage. Usage depends on context. When referring to disk capacities it usually means 10^9 bytes. It also applies to data transmission quantities over telecommunication circuits.

- **Gbps** — Gigabits per second. The rate of data flow.
- **HTTP**—Hypertext Transfer Protocol. An application-level protocol for accessing the World Wide web over the internet.
- **IEEE** — Institute of Electrical and Electronics Engineers. An international technical/professional society that promotes standardization in technical disciplines.
- **IMAP** — Internet Message Access Protocol. An internet standard protocol for accessing email from a remote server from email clients. IMAP allows access from multiple client devices.
- **IMEI**—International Mobile Equipment Identity. Used in LTE networks to identify the device. It is usually printed on the device and can often be retrieved using a USSD code.
- **IP** — Internet Protocol. The mechanism by which packets are routed between computers on a network.
- **IP type** — The type of service provided over a network.
- **IP address**—Internet Protocol address. The address of a device attached to an IP network (TCP/IP network).
- **ISP**—Internet Service Provider. Also referred to as the service carrier, an ISP provides internet connection service (*See* Network Operator).
- **Kbps** — Kilobits per second. The rate of data flow.
- **LAN**—Local Area Network. A type of network that lets a group of computers, all in close proximity (such as inside an office building), communicate with one another. It does not use common carrier circuits though it can have gateways or bridges to other public or private networks.
- **MAC Address**—Media Access Control. A number that uniquely identifies each network hardware device. MAC addresses are 12-digit hexadecimal numbers. This is also known as the physical or hardware address.
- **Mbps** — Megabits per second. The rate of data flow.
- **Network Operator**—The vendor that provides your wireless access. Known by different names in different regions, some examples are wireless provider, network provider, or cellular carrier.
- **Network Technology**—The technology on which a particular network provider's system is built, such as LTE or GSM.
- **NNTP** — Network News Transfer Protocol. The primary protocol used to connect to Usenet servers and transfer news articles between systems over the internet.
- **POP3** — Post Office Protocol 3. A protocol in which email is received and held for you by your internet server until you download it.
- **Port** — A virtual data connection used by programs to exchange data. It is the endpoint in a logical connection. The port is specified by the port number.

- **Port Forwarding** — A process that allows remote devices to connect to a specific computer within a private LAN.
- **Port Number** — A 16-bit number used by the TCP and UDP protocols to direct traffic on a TCP/IP host. Certain port numbers are standard for common applications.
- **Protocol** — A standard that enables connection, communication, and data transfer between computing endpoints.
- **Proxy** — A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it.
- **Router** — A device that directs traffic from one network to another.
- **RSSI** — Received Signal Strength Indicator. An estimated measure of how well a device can hear a signal from an access point or router. RSSI value is pulled from the device's Wi-Fi card (hence "received" signal strength), so it is not the same as transmit power from an access point or router.
- **SIM** — Subscriber Identification Module. Found in LTE and GSM network technology, the SIM is a card containing identification information for the subscriber and their account. The SIM card can be moved to different devices.
- **SMTP** — Simple Mail Transfer Protocol. The standard protocol for sending emails across the internet.
- **SNMP** — Simple Network Management Protocol. An internet protocol used to manage and monitor network devices and their functions.
- **SNR** — Signal to Noise Ratio. A ratio of signal power to noise power expressed in decibels. SNR is a positive value, and higher numbers are better.
- **SSID** — Service Set IDentifier. The name assigned to a Wi-Fi network.
- **TCP/IP** — Transmission Control Protocol/Internet Protocol. The set of communications protocols used for the internet and other similar networks.
- **TFTP** — Trivial File Transfer Protocol. An internet software utility for transferring files that is simpler to use than FTP but does not provide user authentication and directory visibility supported by FTP.
- **Telnet** — A user command and underlying TCP/IP protocol that allows a user on one computer to log into another computer that is part of the same network.
- **TTY** — Text Telephones (TTY), also known as Telecommunications Device for the Deaf (TDD), are used by the deaf, hard–of–hearing, and individuals with speech impairments to communicate.
- **UDP** — User Datagram Protocol (UDP) is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses

the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.

- **USSD** — Unstructured Supplementary Service Data (USSD), also known as “Quick code” or “Feature code”, is a communications protocol used to send data between a mobile device and network service provider.
- **VPN** — Virtual Private Network. A secure private network that runs over the public internet. Commonly used to connect to an office network from elsewhere.
- **Wi-Fi** — Any system that uses the 802.11 standard developed and released in 1997 by the IEEE.
- **Wi-Fi 5** — The fifth generation of Wireless Fidelity, using 802.11ac on 5 GHz. This standard was developed and released in 2013.
- **Wi-Fi 6** — The sixth generation of Wireless Fidelity, using 802.11ax on licensed exempt bands between 1 and 6 GHz. This standard was developed in 2020.
- **Wi-Fi Client** — A wireless device that connects to the internet via Wi-Fi
- **WPA/WPA2** — Wi-Fi Protected Access. A security protocol for wireless 802.11 networks from the Wi-Fi Alliance.
- **WPA3** — The next generation of Wi-Fi Protected Access. WPA3 simplifies security, provides more robust authentication, increased cryptographic strength, and offers additional capabilities for personal and enterprise networks. WPA3 retains interoperability with WPA2 devices.