USER GUIDE

inseego

MiFi® X PRO 5G

Global Mobile Hotspot

INSEEGO COPYRIGHT STATEMENT

© 2024 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 Although copyrighted, the software drivers are unpublished and embody valuable trade secrets proprietary to Inseego Corp.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: 14964508 Rev 3

Contents

Introduction and getting started 6
Overview 7
Key features 7
Description 7
Display view 8
Side view 8
Status indicators and icons 9
Getting started 10
Setting up with the Inseego Mobile app 10
Installing a SIM card 11
Turning on and off 12
System requirements 13
Finding your Wi-Fi name and password 13
Connecting devices to your MiFi 13
Caring for your MiFi 15
Charging 15
Battery Preservation Mode 17
Battery tips 19
Replacing the battery 20
Replacing the SIM card 21
Unlocking the SIM card 22
Resetting your MiFi 23
Care tips 24
Touchscreen 25
Overview 26
Home screen 26
Navigation tips 27
Managing Wi-Fi settings 27
Wi-Fi 27
Band Selection 28
Wi-Fi Name/Password 28
Wi-Fi Protected Setup (WPS)[1] 29
Managing connected devices 30
Connected devices (details and blocking) 30
Blocked devices (unblocking) 30
Viewing data usage 31
Managing settings 31
Charging other devices 32
Viewing software update info 33
Viewing messages 33
Viewing info about your MiFi 34
Viewing help 35
Admin web UI 36
Overview 37
Home page 37
Side menu 37
Admin password 38
Changing the Admin password 38
Hiding the Admin password on the touchscreen 38
Managing data usage 39

Data Usage page....40
Managing Wi-Fi settings....42
Settings tab....43
Primary Network tab....45
Guest Network tab....47
Managing connected devices....49
Connected Devices page....50
Managing settings....52
Preferences tab....52
Software Update tab....58
Backup and Restore tab....60
GPS tab....62
Advanced tab....63
Initiating ZTP for SD EDGE....64
ZTP tab....64
Viewing info about your MiFi....66
Internet Status tab....67
Internet Sessions tab....68
Diagnostics tab....69
Device Info tab....71
Logs tab....72
Getting help....73
Help tab....74
Customer Support tab....75
Advanced settings....76
Overview....77
Using advanced settings....77
Cellular tab....78
Manual DNS....80
SIM tab....82
Firewall tab....84
MAC Filter tab....86
LAN tab....88
Port Filtering tab....90
Port Forwarding tab....92
VPN....95
Inseego Connect tab....100
Heartbeat timer (Inseego Connect)....101
Troubleshooting and support....102
Overview....103
First troubleshooting steps....103
Common problems and solutions....103
My MiFi powered off without pressing the Power button....103
No service is available....104
My MiFi has no power/touchscreen doesn't display when I press the Power button....104
I forgot my Wi-Fi password....104
I forgot my MiFi Admin web UI password....104
I cannot connect a device to my MiFi....104
I see other networks, but not the network name for my MiFi....105
I see the network name, but cannot connect a device to my MiFi....105
I want to see how many devices are connected....106
I want to see the firmware (software) version installed on my MiFi....106

I want to see the phone number for my MiFi 106
I want to see the battery level of my MiFi 106
I want to turn my MiFi off 106
I want to know if my MiFi is still on when the touchscreen is dark 107
Technical support 107
Product specifications and regulatory information 108
Product specifications 109
Device 109
Environmental 109
Power 110
Wi-Fi 110
Software 110
Connectivity, approvals, bands, chipset, and languages by SKU 111
Warranty and services 112
Regulatory information 112
Federal Communications Commission Notice (FCC – United States) 112
Innovation, Science and Economic Development Notice (ISED – Canada) 113
ISED Canada ICES-003 Compliance 113
FCC and ISED RF Exposure Guidance Statement 113
Product Certifications and Supplier's Declarations of Conformity 114
Wireless communications 114
Limited warranty and liability 114
Safety hazards 115
Proper battery use and disposal 116
Glossary 117
Glossary 118

1

Introduction and getting started

Overview

Description

Status indicators and icons

Getting started

Caring for your MiFi

Overview

MiFi X PRO 5G is Inseego's 5G mobile hotspot, providing groundbreaking speeds wherever you go with dual-band Wi-Fi 6 and 5G, including mid-band spectrum, which provides more coverage and versatility. You can connect up to 32 Wi-Fi devices simultaneously, use the USB Type-C charging port, or connect directly to the internet with the 1 Gbps Ethernet port.

Key features

- Robust 5G band option support (sub-6, and C-band) and 5G band combinations provide strong performance, speed, and low latency.
- Dual-band Wi-Fi 6 supporting up to 32 connected devices, as well as a USB Type-C charging port and RJ452 Ethernet port for direct internet connection.
- WPA3 Wi-Fi security support, advanced encryption, VPN passthrough, and remote connectivity to office networks.
- Rechargeable 5050 mAh battery to last through the day[1] and the ability to charge other devices.
- Inseego Mobile™ app provides step-by-step setup instructions and remote device management.

Description

The Inseego MiFi X PRO 5G package includes:

- 5G MiFi X PRO 5G
- Pre-installed 5050 mAh Li-Ion battery
- 18W Qualcomm® Quick Charge™ 3.0 charger
- USB 3.1 Gen 1, type A to C cable
- Get Started card

[1] Battery life and activity may vary depending on the number of connected devices and activity, including use of Ethernet.

Display view

Press and hold the Power button for three seconds to turn your MiFi X PRO 5G on and off. Press and release the Power button to wake up the display.

The touchscreen displays and allows you to view Wi-Fi name and password, connected devices, data usage, and more. Swipe through screens and tap the arrows, buttons, and icons to access available menu options.

Side view

Connect to the Quick Charge charger or tether to a device with the USB-C port.

Use the Ethernet port to connect a device directly to the internet.

Status indicators and icons

The MiFi X PRO 5G uses the following status indicators and display icons[1].

Display Icon		Description
No icons		MiFi is powered off or not receiving power, or the screen is in power-saving mode.
Home		Home
Network signal strength		More bars indicate more signal strength.
Activity indicator		Data is transferring between cellular network and the MiFi.
Roaming[2]		Indicates roaming.
Messages		You have unread messages.
Wi-Fi		MiFi Wi-Fi network is on.
Connected devices		Displays number of Wi-Fi devices connected to your MiFi.
Information		Tap to view more information (on Home screen tap to view Wi-Fi network names and passwords).
Multiple screens		Indicates you can swipe left/right to view more screens.
Battery charged		Battery is fully charged.
Battery needs charge		Battery is critically low. The MiFi will shut down unless the battery is connected to the charger.
Battery on AC charge		MiFi is connected to the AC charger and charging.
Battery on USB charge		MiFi is connected via USB and is either being charged or charging a connected device.
Battery Preservation Mode		MiFi battery level is maintained at 70% – 80%[3] until the charger is disconnected or the MiFi is power cycled.
No SIM		No SIM card is detected.
Locked SIM		SIM card is locked. The data usage meter will not display.
SIM error		SIM card error. Check that your SIM card is properly installed.
USB tethered		A device is connected to the MiFi via USB.
Ethernet		Ethernet port is activated.
No Ethernet		Ethernet port is deactivated.

[1] Icons may appear slightly different, depending on service provider.
[2] This icon may not be available on some devices.
[3] On some devices, Battery Preservation Mode maintains battery level at 50% - 60% instead of 70% - 80%.

Getting started

Important: Before you use your MiFi, charge the battery for at least four hours to ensure a full initial charge. When fully charged, the battery has all day life[1].

Setting up with the Inseego Mobile app

You can set up and manage your MiFi with the Inseego Mobile app:

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

2. Follow the in-app instructions to set up your MiFi.

3. Use the app to configure and customize your MiFi.

[1] Battery life and activity may vary depending on the number of connected devices and activity, including use of Ethernet.

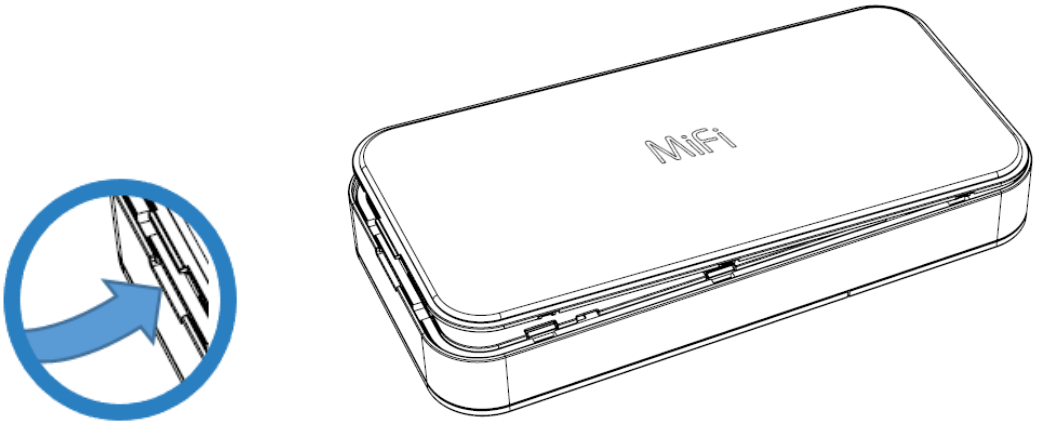
Installing a SIM card

Your SIM card is a small rectangular plastic card that stores your phone number and important information about your wireless service. The MiFi X PRO 5G supports only Nano SIM cards. To prevent damage to the SIM slot, please select the correct SIM for this device.

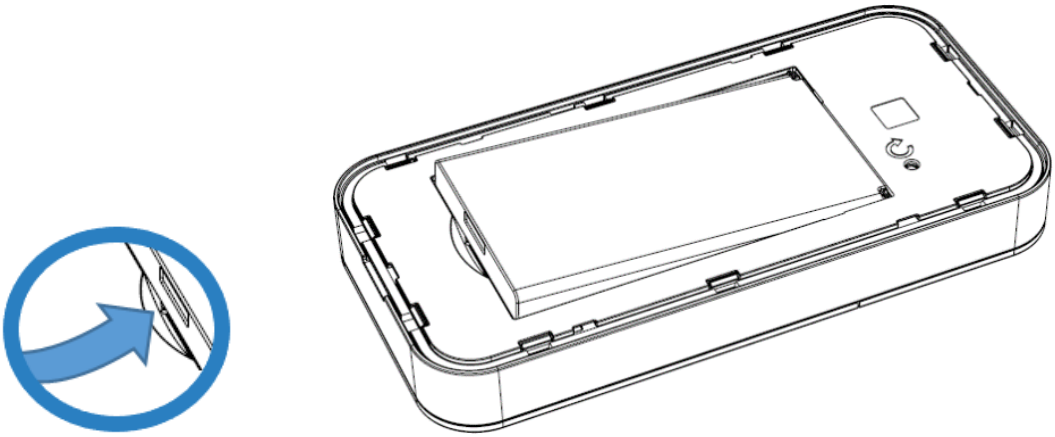
CAUTION: Always use a factory-made SIM card supplied by the service provider. Do not bend or scratch your SIM card. Avoid exposing your SIM card to static electricity, water, or dirt.

To install a SIM card:

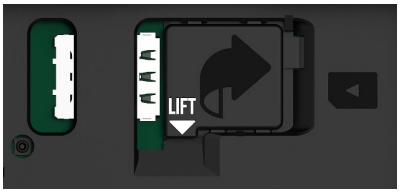
1. Insert a fingernail at the edge of the battery cover and lift and remove the battery cover. Set the cover aside.



2. Remove the battery from the battery compartment.



3. Lift the SIM access tab by placing a fingernail underneath the white arrow and lifting the tab up and to the right.



4. If necessary, remove the SIM card from the outer card, being careful not to touch the gold-colored contacts.

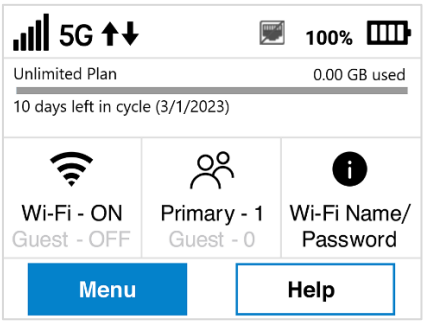
5. Slide the SIM card into the slot **notch first, with the contact points facing down**.

6. Close the SIM access tab, place the battery in the battery compartment and replace the cover. The SIM card MUST remain in the SIM card slot when in use.

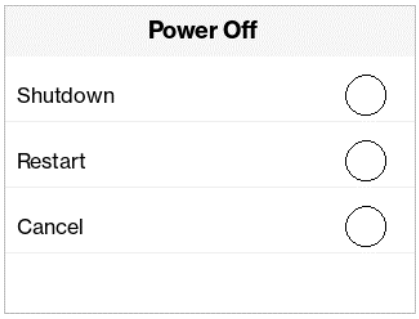
Turning on and off

To turn your MiFi on, press and hold the Power button for three seconds.

The Home screen appears.



To turn your MiFi off, press and hold the Power button for three seconds until you see the Power Off screen.



Then select **Shutdown**.

To wake up the display, press and release the Power button.

System requirements

Any device with Wi-Fi capability can connect to your MiFi. You can also connect via USB or Ethernet.

The MiFi must have proper data service to function and is compatible with all major operating systems and the latest versions of browsers.

Finding your Wi-Fi name and password

Tap **Wi-Fi Name/Password** on the Home screen. The name and password for your MiFi primary network is displayed. Swipe left to see the credentials for the guest network.

Important: The default Admin password is the same as the primary network's default. To change either password, sign into the MiFi Admin web UI.

Connecting devices to your MiFi

Connecting devices wirelessly

Your MiFi has two Wi-Fi networks, primary and guest, and lets you connect up to 32 Wi-Fi capable devices. For added security, share your guest network instead of your primary network. The guest network is off by default. You can turn it on from either the MiFi touchscreen (see page 28) or the Admin web UI (see page 47).

To connect devices to your MiFi:

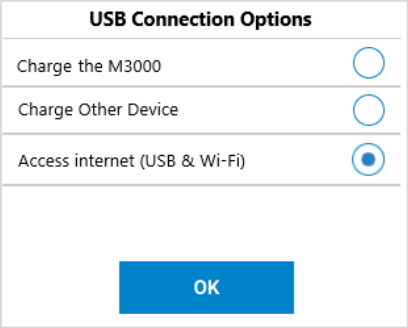
1. Turn on the device you want to connect. The MiFi will broadcast its own wireless network and name.
2. On the device, open the list of available Wi-Fi networks. Select the MiFi primary or guest network and enter the password. Once connected to the internet, the MiFi Home screen displays the connected device.

NOTE: You can view or change MiFi settings on the MiFi touchscreen or by connecting to the Admin web UI from the primary network at http://my.MIFI/ or http://192.168.1.1.

Connecting devices with USB

You can tether to a device using the USB-C port:

1. Connect the USB-C end of a USB cable into the USB-C port on your MiFi.
2. Connect the USB-A end of a USB cable into the device you wish to connect. The USB Connection Options touchscreen appears.



3. Select **Access internet (USB & Wi-Fi)** and tap **OK**.

Connecting devices with Ethernet

NOTE: The Ethernet port is disabled by default to optimize battery life. You can enable it from the touchscreen (**Menu > Settings**), or from the Admin web UI (**Settings > Preferences**).

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

1. Plug one end of an Ethernet cable into the Ethernet port on your MiFi.
2. Plug the other end of the cable into the Ethernet port of the device you wish to connect.

Devices plugged into the MiFi via Ethernet have direct access to the internet.

Caring for your MiFi

This section provides information on charging, battery tips and replacement, replacing and unlocking the SIM card, restoring your MiFi to factory default settings, and general care.

Charging

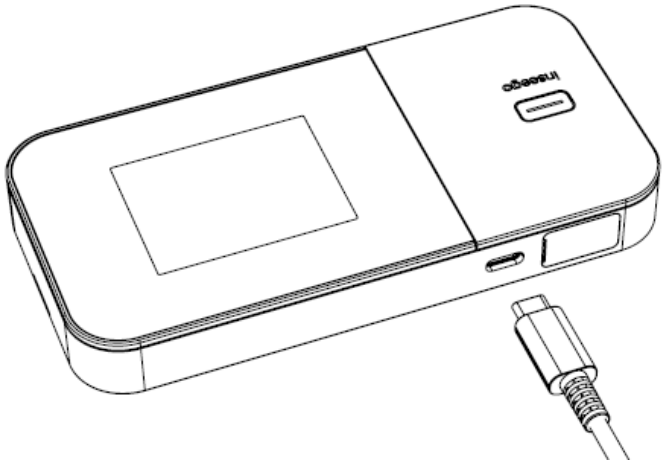
You can check the battery level and charging status of your MiFi from the Home screen.

Important: Before using your MiFi, charge the battery for at least four hours to ensure a full initial charge. When fully charged, the battery has all day life[1].

Charging with Quick Charge Charger

To charge the battery with the Quick Charge charger:

1. Connect the USB-C end of the USB cable into the charging port of the MiFi.



2. Connect the other end of the USB cable into the Quick Charge charger and plug the charger into an appropriate electrical outlet.

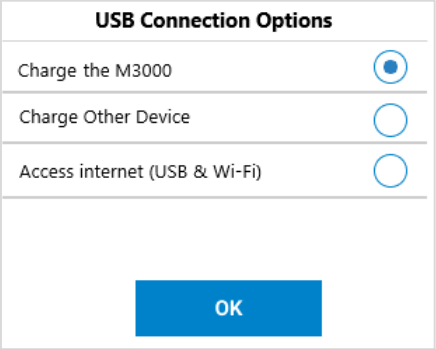
Charging with the USB cable

Your MiFi X PRO 5G comes with a USB charging/data cable that can be used to charge your MiFi. You can use this cable to charge directly from a variety of USB-powered ports (laptops, computers, hubs, etc.).

To charge your MiFi from a powered USB port:

1. Connect the USB-C end of the USB cable into the USB-C port of the MiFi.
2. Connect the USB-A end of the USB cable into another device, such as a laptop. The USB Connection Options touchscreen appears.

[1] Battery life and activity may vary depending on the number of connected devices and activity, including use of Ethernet.



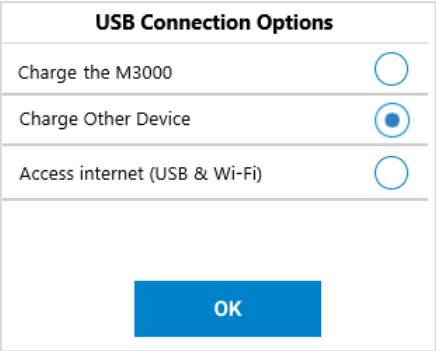
3. Select **Charge the M3000** and tap **OK**.

Charging other devices

You can use the USB-C port on your MiFi to charge other devices, like a cell phone or tablet.

To charge another device:

1. Connect the USB-C end of a USB cable into the USB-C port of the MiFi.
2. Connect the other end of the USB cable into the device you wish to charge. The USB Connection Options touchscreen appears.



3. Select **Charge Other Device** and tap **OK**.

NOTE: Do not use the Charge Other Device feature if you want to use the battery for a full day.

Charging best practices

For optimum battery health and life, Inseego does not recommend keeping the battery fully charged for an extended period of time. To support this, your MiFi includes the Battery Preservation Mode (BPM) feature, which helps prevent overcharging and preserves the integrity of your battery.

Inseego recommends the following best practices to ensure optimal battery performance and life:

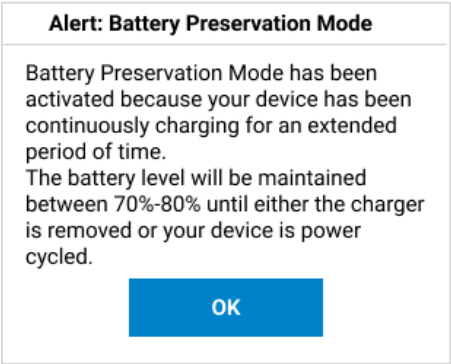
- Minimize the amount of time the battery stays at 0% or 100%.
- Charge, operate, and store the device as close to normal room temperature as possible (60° to 80°).
- Store your MiFi with a battery strength between 30% - 80%.
- Best results are achieved by allowing Battery Preservation Mode to activate if you keep your MiFi continuously powered.

Before using your MiFi, read the Battery Preservation Mode and Battery Tips sections that follow and the battery safety information in the Safety Hazards and Proper Battery Use and Disposal sections at the end of this guide.

CAUTION: Always use official OEM batteries and chargers that have been approved by Inseego for optimal performance and safe operation of your MiFi.

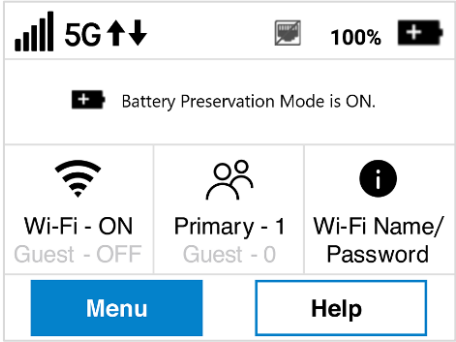
Battery Preservation Mode

Battery Preservation Mode is designed for users that typically keep their MiFi plugged in for extended periods (over 24 hours at a time). Batteries that continuously hold a full charge have been shown to lose charge capacity over time and have reduced longevity. To avoid any loss of battery integrity, Battery Preservation Mode activates on your MiFi when it has charged for more than 16 hours straight. With Battery Preservation Mode, the battery level is allowed to fall to 70%[1] and then your MiFi maintains a charge of 70% - 80%[1] until you power cycle or remove it from charging. When Battery Preservation Mode is activated, the following message appears:

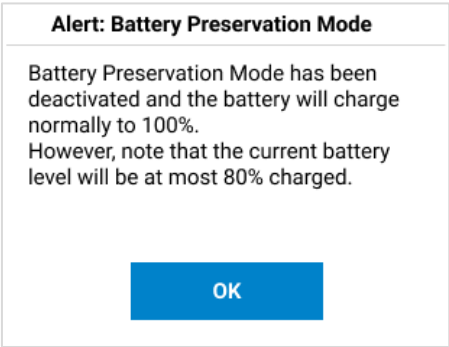


[1] On some devices, Battery Preservation Mode maintains battery level at 50% - 60% instead of 70% - 80%.

Click **OK**. The Battery Preservation Mode icon on the Home screen and a message on the InfoPanel indicate that Battery Preservation Mode is on.



Battery Preservation Mode automatically deactivates when you unplug the charger or power cycle your MiFi.



Click **OK**.

Once Battery Preservation Mode has been activated, your MiFi no longer charges to 100%. Initially, the charge level is between 70%[1] and 99% and eventually, 70% to 80%[1]. If this is not desired, you can disable Battery Preservation Mode on the touchscreen (**Menu > Settings**), or on the Admin web UI (**Settings > Preferences**).

[1] On some devices, Battery Preservation Mode maintains battery level at 50% - 60% instead of 70% - 80%.

Battery tips

Before operating for a full day:

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

NOTE: Do not use the Charge Other Device feature if you want to use the battery for a full day.

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

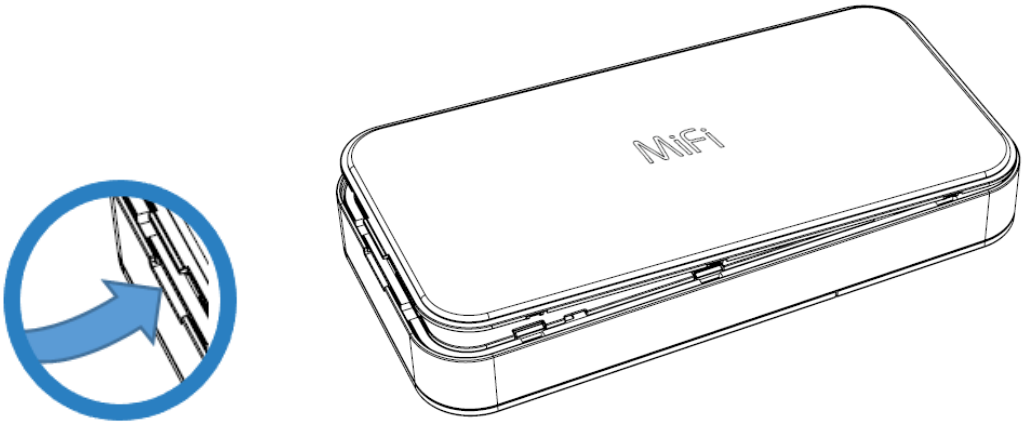
- Do not use sharp objects or use excessive force to remove the battery or to access the battery well, this may damage the MiFi and the battery.
- The battery discharges more rapidly as additional devices access your MiFi.
- Battery life depends on the network, signal strength, temperature, features, and accessories you use.
- New batteries or batteries that have been stored for a long time may take more time to charge.
- When storing your battery, keep it uncharged in a cool, dark, dry place.
- When charging your battery, keep it near room temperature.
- Never expose batteries to temperatures below -20°C (4°F) or above 60°C (140°F).
- Never leave the MiFi in an unattended vehicle where it can get too hot or too cold.
- Some batteries perform best after several full charge/discharge cycles.
- It is normal for batteries to gradually wear down and require longer charging times. If you notice a change in your battery life, it is probably time to purchase a new battery.

Replacing the battery

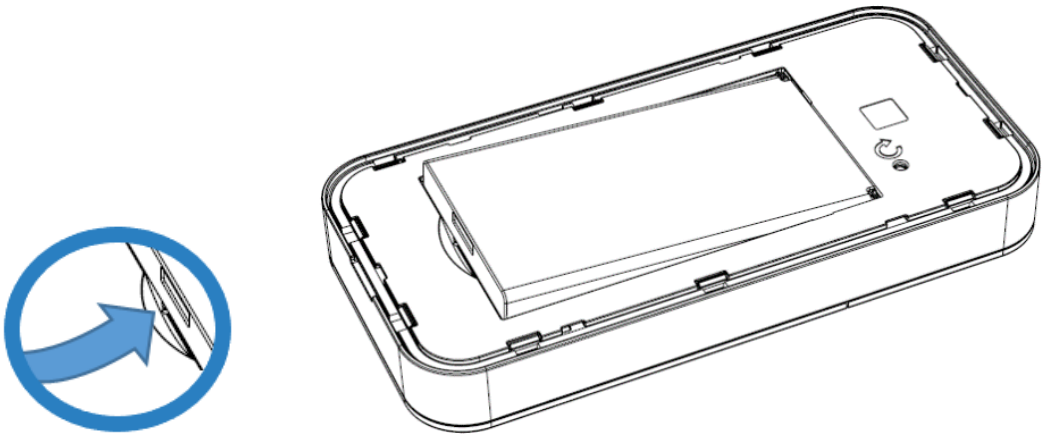
CAUTION: Whenever you remove or insert the battery, ensure your MiFi is not connected to any device or power source. Never use tools, knives, keys, pens, or any type of object to force the door open or to remove the battery. Using any of these types of objects could result in puncturing the battery.

To remove and replace the battery:

1. Insert a fingernail at the edge of the battery cover and lift and remove the battery cover. Set the cover aside.



2. Insert your finger into the battery removal divot and lift the battery out of the battery compartment.



3. Align the gold contacts on the new battery with the gold contacts on the MiFi and gently slide the battery into place.

4. Replace the cover by setting it on the MiFi where the notches align, then press on the cover until it clicks into place and is flat across the entire bottom surface.

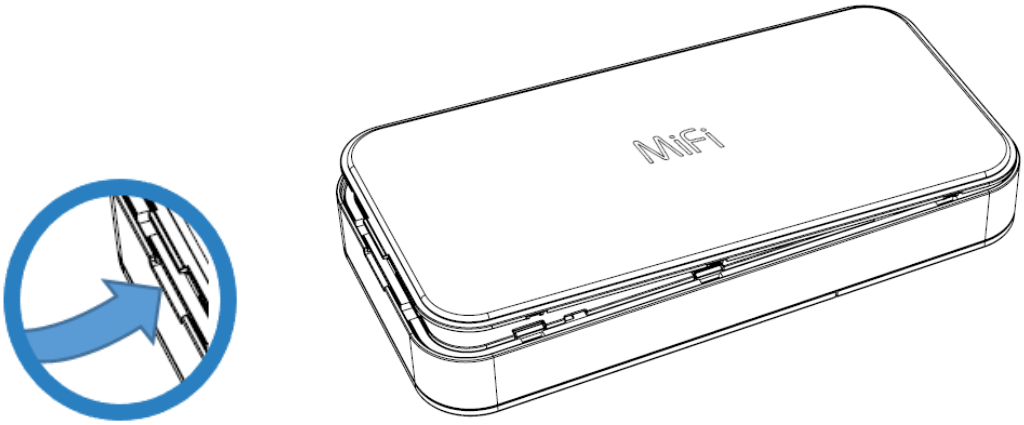
Replacing the SIM card

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

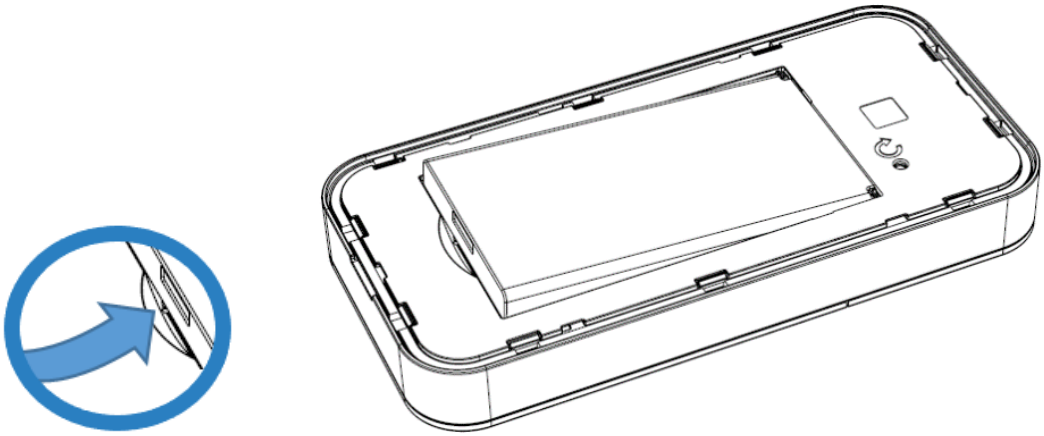
NOTE: Should your SIM card be lost or damaged, contact your network operator.

To remove the SIM card:

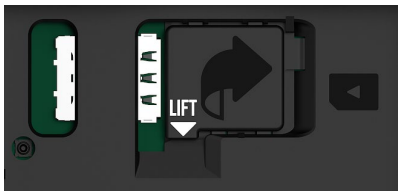
1. Insert a fingernail at the edge of the battery cover and lift and remove the battery cover. Set the cover aside.

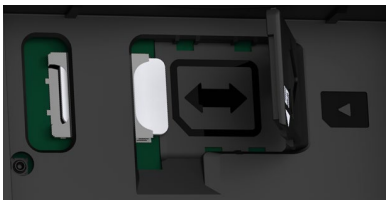


2. Remove the battery from the battery well.



3. Lift the SIM access tab by placing a fingernail underneath the white arrow and lifting the tab up and to the right.





4. Carefully slide the SIM card out of the SIM card slot.

To place a new SIM card:

1. If necessary, remove the SIM card from the outer card, being careful not to touch the gold-colored contacts.

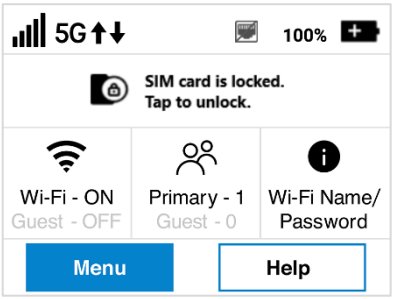
2. Slide the SIM card into the slot **notch first, with the contact points facing down**.

3. Close the SIM access tab, place the battery in the battery well and replace the cover. The SIM card MUST remain in the SIM card slot when in use.

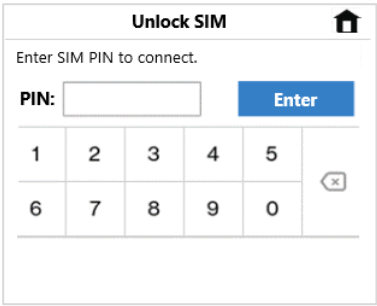
CAUTION: Do not bend or scratch your SIM card. Avoid exposing your SIM card to static electricity, water, or dirt.

Unlocking the SIM card

You can create a PIN code to lock your MiFi SIM card on the Admin web UI (Settings > Advanced > SIM). When the SIM is locked, your MiFi will not have access to the internet. A display appears in the InfoPanel of the Home screen.



Tap the message to unlock the SIM card.
Or you can tap Unlock SIM from the Help menu.



Enter the PIN and tap Enter.

CAUTION: If you run out of PIN attempts, your SIM is PUK (personal unblocking key) locked and you must contact your network operator for the PUK code. You must enter the PUK code in the Admin web UI. If you enter the wrong PUK code, your SIM card will be permanently locked.

Resetting your MiFi

You can reset your MiFi to factory settings using the Reset button on the MiFi, from the MiFi touchscreen, or from the Admin web UI.

CAUTION: Resetting returns your MiFi to factory settings, including resetting the Wi-Fi name and password. This disconnects all devices.

Resetting with the Reset button

To reset using the Reset button on the MiFi:

1. Insert a fingernail at the edge of the battery cover and lift and remove the battery cover. Set the cover aside.

   The Reset button is in a small hole located on the bottom of the MiFi.

2. Place one end of an unfolded paper clip into the **Reset hole** and press until the screen displays **MiFi Resetting** (about five to six seconds). Your MiFi restarts with factory settings.

NOTE: This option may be disallowed from the Admin web UI (Settings > Preferences > Device Preferences).

Resetting from the MiFi touchscreen

To reset from the MiFi touchscreen, tap **Menu > Settings > Factory Reset**.

NOTE: This option may be disallowed from the Admin web UI (Settings > Preferences > Device Preferences).

Resetting from the Admin web UI

To reset the MiFi from the Admin web UI, select **Settings > Backup and Restore** and click **Restore factory defaults**.

Care tips

Inseego recommends the following care guidelines:

- Protect your MiFi from liquids, dust, and excessive temperatures.
- Do not apply adhesive labels to your MiFi; they might cause the device to potentially overheat or alter the performance of the antenna.
- Store the MiFi in a safe place when not in use.

2

Touchscreen

Overview

Managing Wi-Fi settings

Managing connected devices

Viewing data usage

Managing settings

Charging other devices

Viewing software update info

Viewing messages

Viewing info about your MiFi

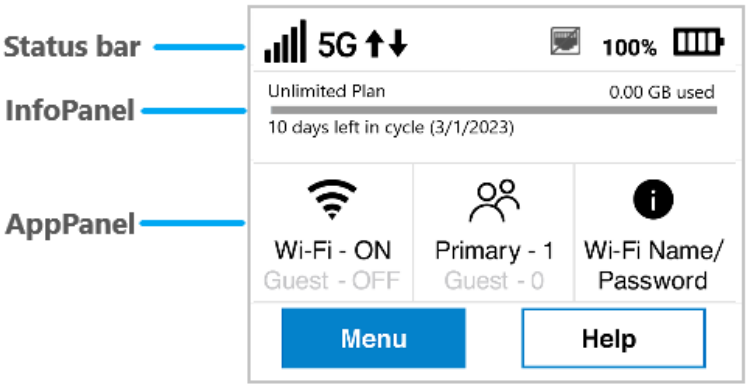
Viewing help

Overview

You can manage, monitor, and customize your MiFi settings directly on the MiFi touchscreen, or by using the MiFi Admin web UI. This chapter explains the features available with the touchscreen[1].

Home screen

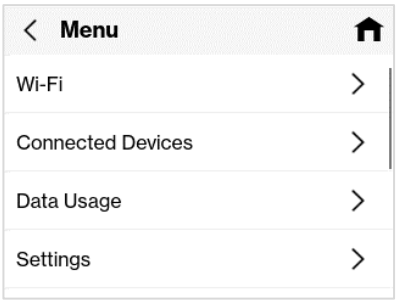
The Home screen lets you see what your MiFi is doing at a glance.



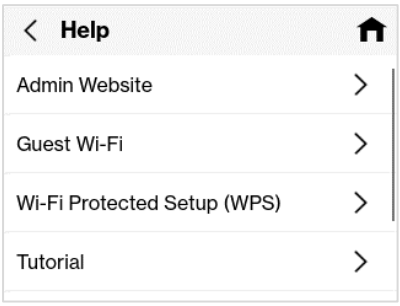
Status bar: The top of the screen displays status indicators, which may include: network signal strength , network type (for example, **5G**), data traffic activity , unread system messages , battery 100% , USB tethered , or Ethernet disabled .

InfoPanel: This panel presents a carousel display of current information on your MiFi. It initially displays data usage but may also display other information, such as when Airplane mode is on, or if there is a SIM card error. Swipe left/right through the displays.

AppPanel: Displays whether Wi-Fi is on or off (tap to access the Wi-Fi menu). Displays how many devices are connected to your MiFi Wi-Fi primary and guest network (tap to access the Connected Devices menu). Tap to view the name and password for your primary and guest networks.



Menu provides access to all menu options



Help provides access to info screens and tutorial

Swipe up/down to scroll through options

[1] Touchscreen images and options may differ different, depending on service provider.

Navigation tips

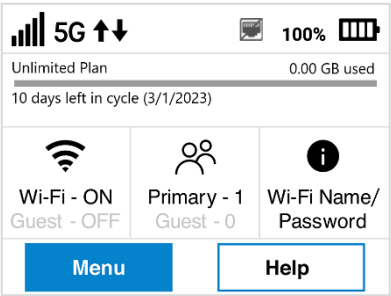
- Tap on the arrows > to navigate through topics.
- Use to return to the Home screen.
- A multiple screen icon indicates there are multiple screens on that topic. Swipe left and right through screens.
- If there is a scroll bar visible on the right, swipe up or down to scroll.

Managing Wi-Fi settings

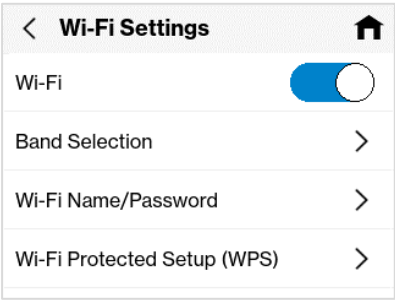
The Wi-Fi Settings screen allows you to turn Wi-Fi on/off and select primary and guest network settings.

NOTE: Wi-Fi settings can be locked from the Admin web UI. If they are locked, they must be unlocked from the Admin web UI Wi-Fi Settings page.

To manage Wi-Fi settings, tap the Wi-Fi icon on the Home screen (or tap **Menu** > **Wi-Fi Settings**).



Tap

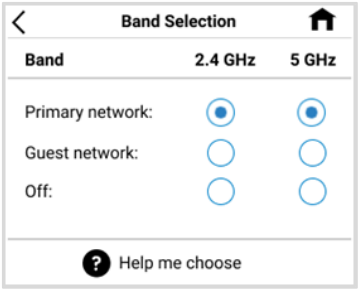


Make selections

Wi-Fi

Use the **Wi-Fi** on/off 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 MiFi is by tethering with the USB cable or connecting via Ethernet.

Band Selection



Use the default values as they appear or adjust them for your environment.

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.

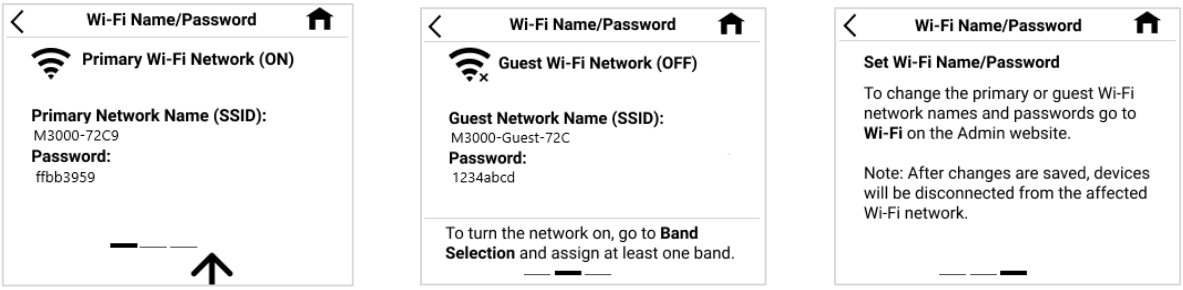
NOTE: You must assign at least one band for the guest network before it can be turned on.

When you make a selection, your MiFi notifies you that it is applying changes and returns to the screen when finished.

Tap **Help me choose** for more information.

Wi-Fi Name/Password

Use the Wi-Fi Name/Password screens to view information on your primary and guest network and to find your passwords. (You can also access these screens by tapping the icon on the Home screen.)



Swipe left to view the Guest Wi-Fi Network screen and left again to view information.

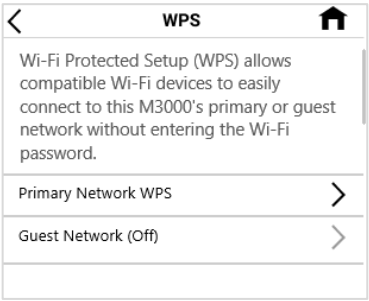
To turn on your guest network, assign it at least one band in **Wi-Fi Settings > Band Selection**.

NOTE: You can change or hide the network name and password information shown on these screens using the Admin web UI Wi-Fi pages.

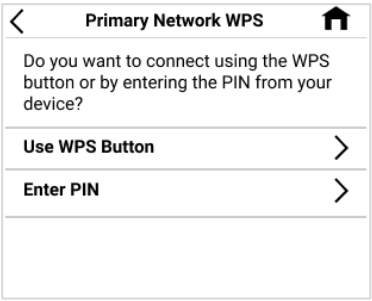
Wi-Fi Protected Setup (WPS)[1]

Enabling Wi-Fi Protected Setup (WPS) allows compatible Wi-Fi devices to easily connect to your MiFi primary or guest network.

NOTE: If WPS is off, you can turn it on using the Admin web UI Wi-Fi pages.

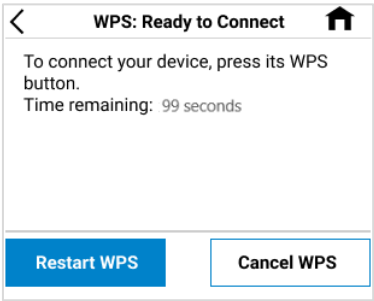


Tap a network



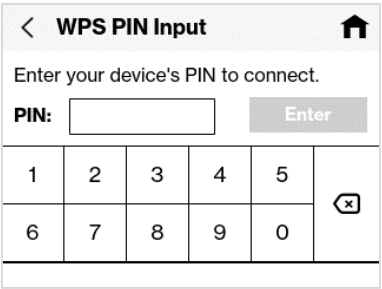
Select a connection option

Use WPS Button



Press the WPS button on the connecting device. A notification appears when successful. If unsuccessful, tap Restart WPS to try again.

Enter PIN



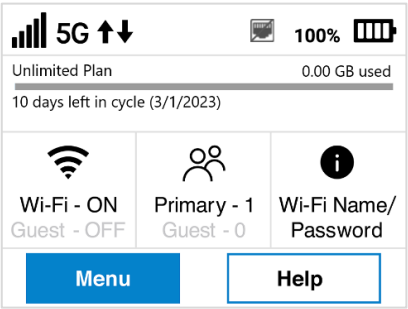
If connecting device has a WPS PIN, enter it and tap Enter.

[1] Availability of WPS is subject to device model.

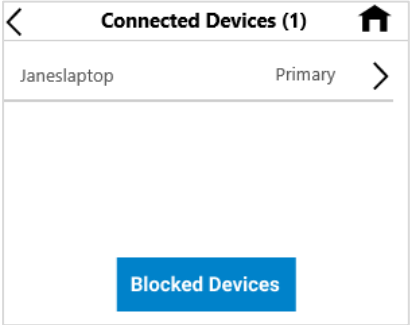
Managing connected devices

The Connected Devices screen lists all devices currently connected to your MiFi, along with the network they are using. You can view device details and block or unblock devices from internet access.

To manage connected devices, tap the connected devices icon on the Home screen (or tap **Menu** > **Connected Devices**).



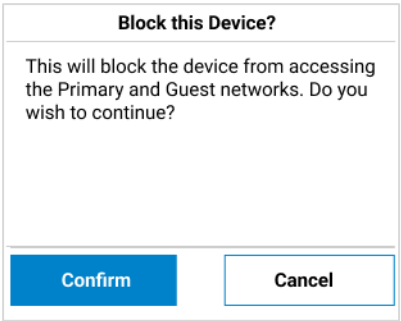
Tap



Tap a device for more details or to block devices
Tap Blocked Devices to unblock devices

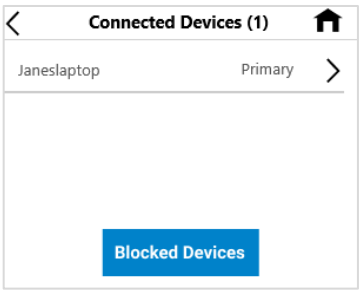
Connected devices (details and blocking)

Tap Block to block
Swipe left/right for a different device

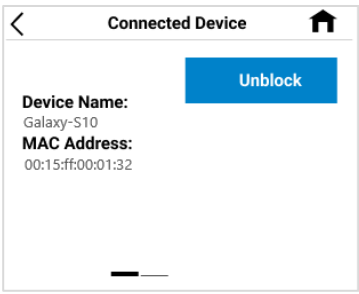


Tap Confirm to block the device

Blocked devices (unblocking)



Tap Blocked Devices to unblock

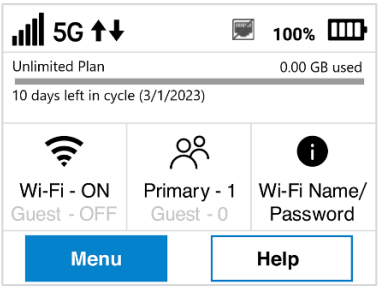


Tap Unblock. The device is removed from Blocked Devices and added to Connected Devices.
Swipe left/right for a different blocked device.

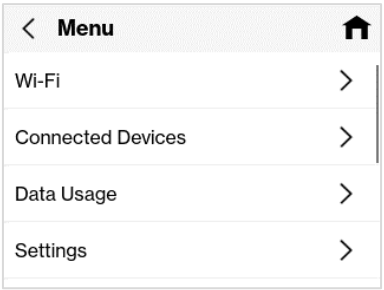
Viewing data usage

You can view data usage on the Home screen or tap **Menu** > **Data Usage**.

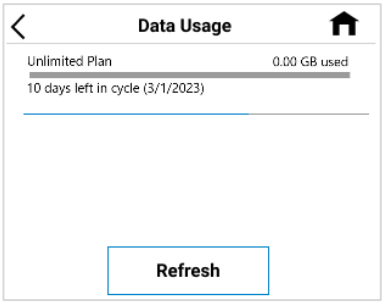
NOTE: The data usage information displayed is an estimate and may differ from your service provider's data usage numbers. Always refer to your service provider account for precise data usage information.



Tap Menu



Tap Data Usage



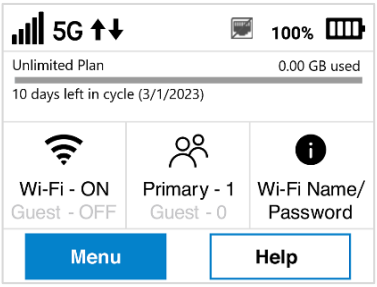
View estimated usage and plan info

NOTE: Data usage estimates may not include roaming. If roaming is on, an informational screen appears. Tap **Continue** for the Data Usage screen.

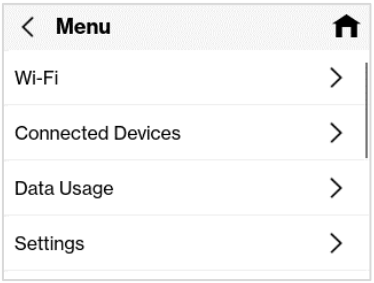
Managing settings

Use the Settings screen to change various MiFi settings or reset your MiFi to the original factory settings.

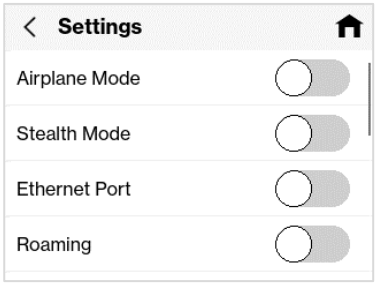
NOTE: Settings can be locked from the Admin web UI. If they are locked, you will receive an error message and they must be unlocked from the Admin web UI (Settings > Preferences).



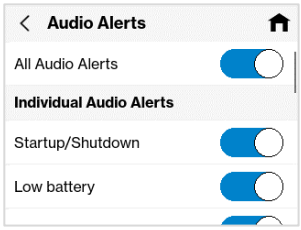
Tap Menu



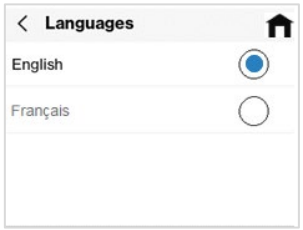
Tap Settings



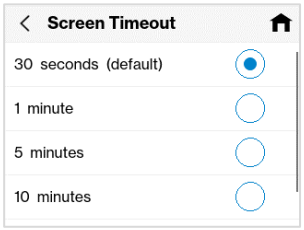
Set on/off slider or tap a setting



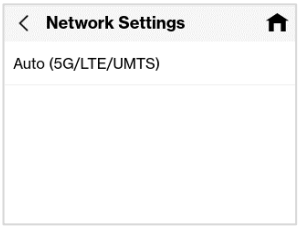
Slide desired alerts on/off



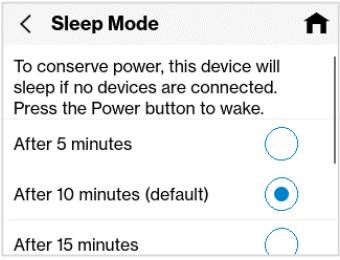
Set touchscreen language



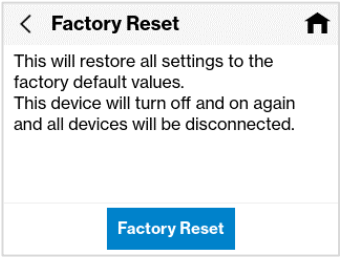
Set touchscreen timeout



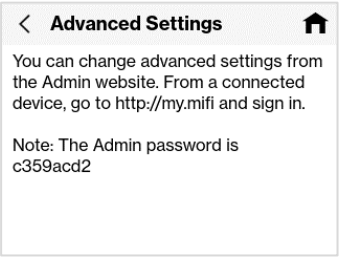
Select a network



Set timer for sleep mode



Tap Factory Reset to restore all settings to the factory default values. Your MiFi will turn off and then on again and all connected devices will be disconnected.



Use the Admin web UI

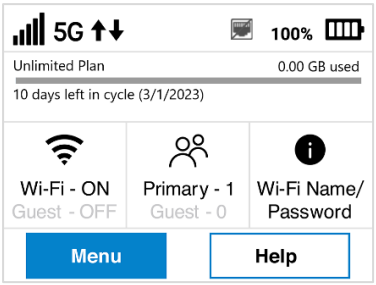
NOTE: Factory Reset can be locked from the Admin web UI. If it is locked, you will receive an error message and it must be unlocked from the Admin web UI (Settings > Preferences).

CAUTION: Factory Reset returns your MiFi to factory settings, including resetting the Wi-Fi name and password and Admin password. This disconnects all devices.

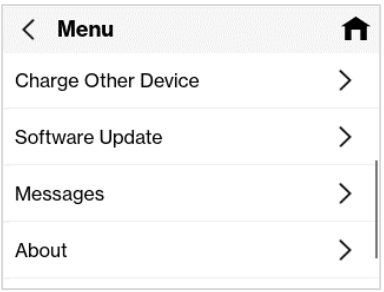
Charging other devices

You can use the USB-C port on your MiFi to charge other devices, like a cell phone or tablet. The Charge Other Device touchscreen provides battery and charging information.

NOTE: Do not use the Charge Other Device feature if you want to use the battery for a full day.



Tap Menu

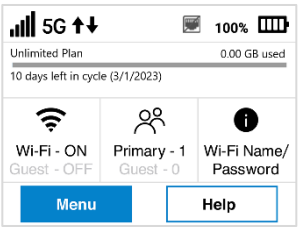


Swipe up and tap Charge Other Device

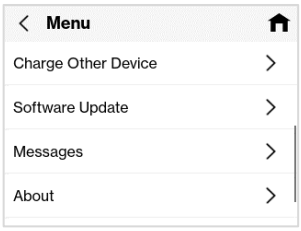
View charging capability
Tap ? for more info

Viewing software update info

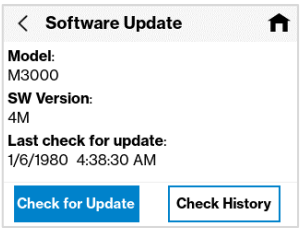
Software updates are delivered to the MiFi automatically over the mobile network. Use the Software Update screen to view the current software version, the last check for updates, update history, and to check for a new update.



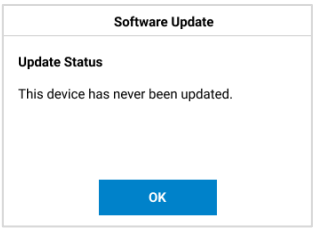
Tap Menu



Swipe up and tap Software Update



Tap Check History



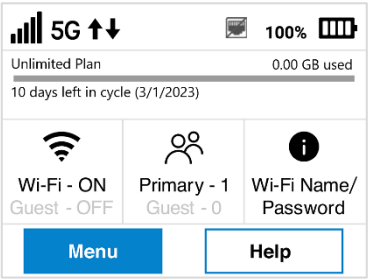
View history

Check for Update: Use this button to check for new software updates.

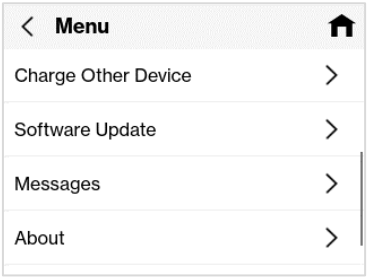
NOTE: Software updates are delivered to the MiFi automatically over the network, so this is usually not necessary.

Viewing messages

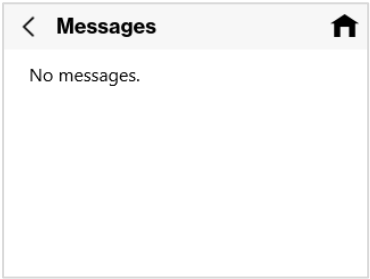
You can check messages on your MiFi with the Messages screen.



Tap Menu



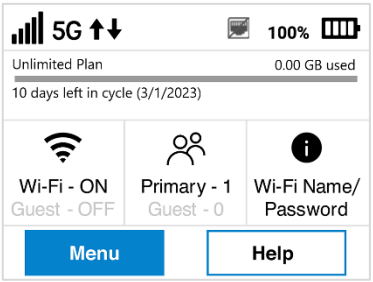
Swipe up and tap Messages



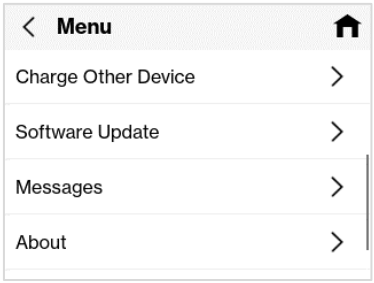
View and manage messages

Viewing info about your MiFi

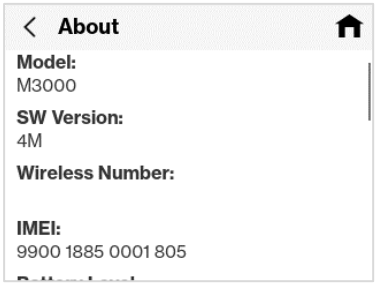
You can view detailed information about your MiFi on the About screen.



Tap Menu



Swipe up and tap About



View details about your MiFi

The About touchscreen provides the following information:

Model: The model of your MiFi.

SW Version: The version of the software currently installed on your MiFi.

Wireless Number: The phone number stored in the SIM card for your MiFi.

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

Battery Level: The percentage of charge currently on the battery.

Internet Status: The current internet status.

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

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

Signal Strength: 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.

SNR: Signal to Noise Ratio. A measure of the ratio between signal strength and noise level. SNR values are positive, and higher numbers are better.

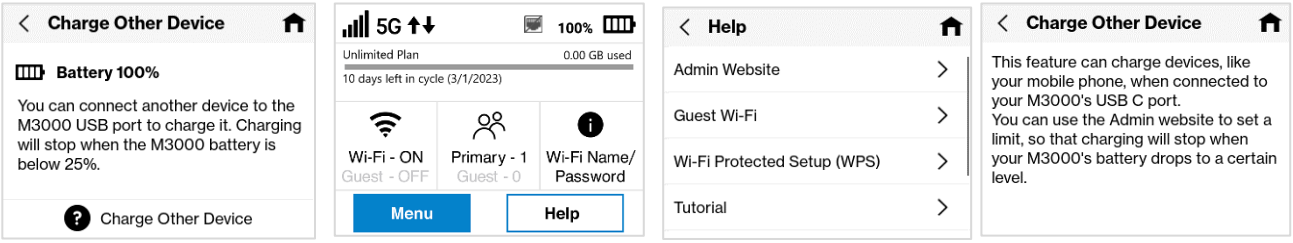
Roaming: Indicates whether roaming is on.

APN: The Access Point Name (APN) available from the network.

IP Address: The internet IP address assigned to your MiFi.

Viewing help

When you see ? on a screen, tap it for more information on that topic, or use the Help menu. The Help screen provides all the help topics and a tutorial for your MiFi.



Tap ? or Tap Help and then Select a topic View help topic

3

Admin web UI

Overview

Admin password

Managing data usage

Managing Wi-Fi settings

Managing connected devices

Managing settings

Viewing info about your MiFi

Getting help

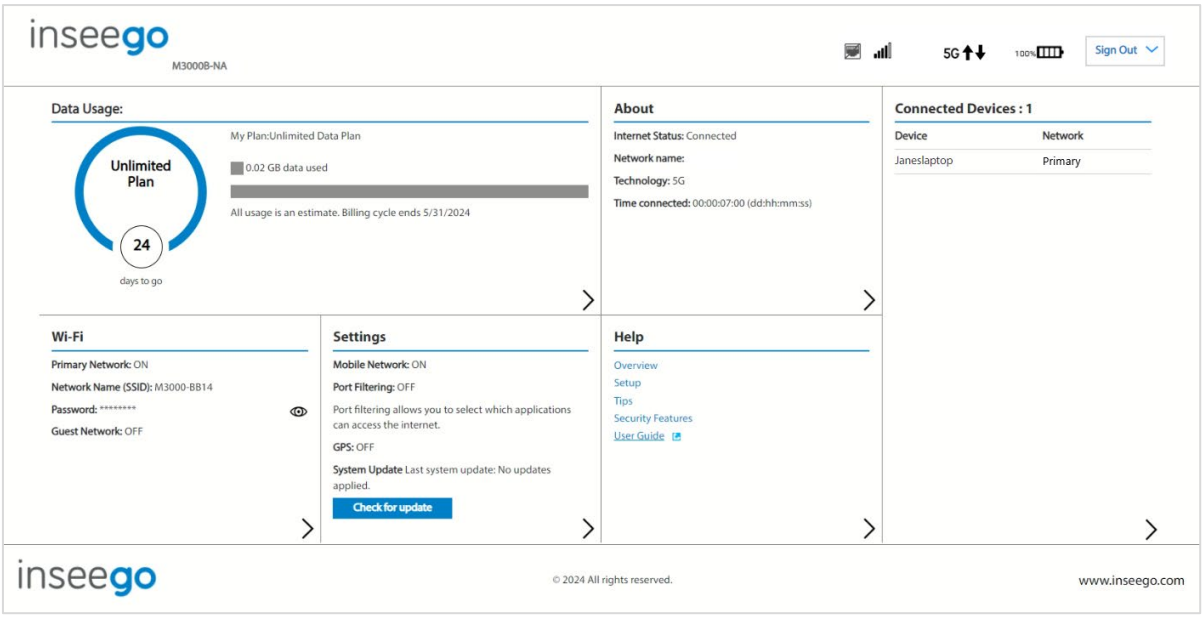
Overview

On a computer or device connected to your MiFi, open any web browser, and go to http://my.MIFI/ or http://192.168.1.1.

Home page

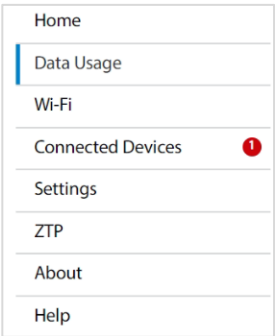
The Home page is the local gateway to configuring and managing your MiFi. It displays current data usage and Wi-Fi status, lists currently connected devices, and offers links to other pages with option settings and help.

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



Side menu

Each sub screen in the MiFi Admin web user interface (UI) includes a menu on the left, which you can use to return to the Home page or jump to other pages. The current page is indicated by a red bar.
NOTE: Menu options may differ depending on service provider.



Admin password

The Admin password is what you use to sign into the MiFi Admin web UI. Initially, it is the same as the default password for your MiFi primary network. Tap **Wi-Fi Name/Password** on the Home touchscreen of your MiFi to view the initial default password.

You are prompted to change the Admin password upon first login. Change the password to something easy to remember and set up a security question.

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 UI.

Changing the Admin password

To change the Admin password:

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

The next time you sign in to the Admin web UI, use the new Admin password. If you cannot remember the password, click **Forgot Admin password?**. After you correctly answer the security question you set up, the current password is displayed. Alternately, you can view the Admin password on the MiFi touchscreen by tapping **Help** > **Admin Website** or **Menu** > **Settings** > **Advanced Settings**.

Hiding the Admin password on the touchscreen

The Admin password can be viewed on the MiFi touchscreen by tapping **Help** > **Admin Website** or **Menu** > **Settings** > **Advanced Settings**.

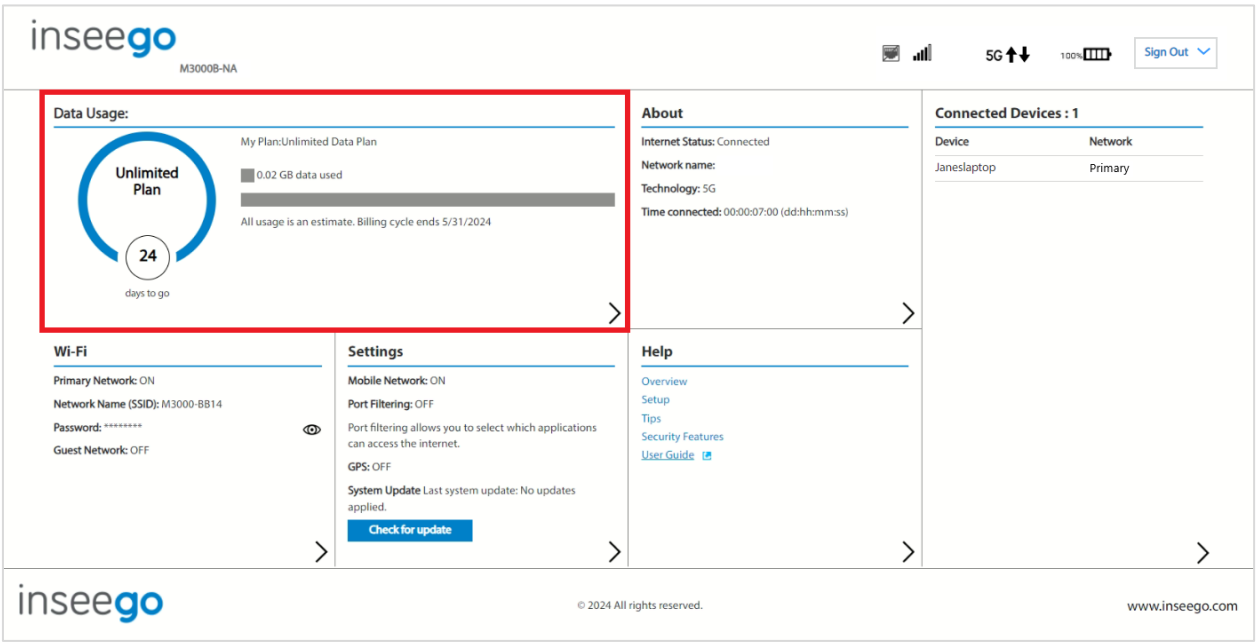
To hide the Admin password:

1. Click the down arrow next to **Sign Out** in the top-right corner of any web UI page and select **Change Password**.
2. Move the **Hide Admin Password on the Device Screen** on/off slider to the right to hide the Admin password on the MiFi touchscreen. The Admin password is no longer visible on the touchscreen.

Managing data usage

On the web UI Home page, the Data Usage panel displays graphs of your MiFi data usage for the current billing cycle.

NOTE: The data usage information displayed is an estimate and may differ from your service provider's data usage numbers. Always refer to your service provider account for precise data usage information.

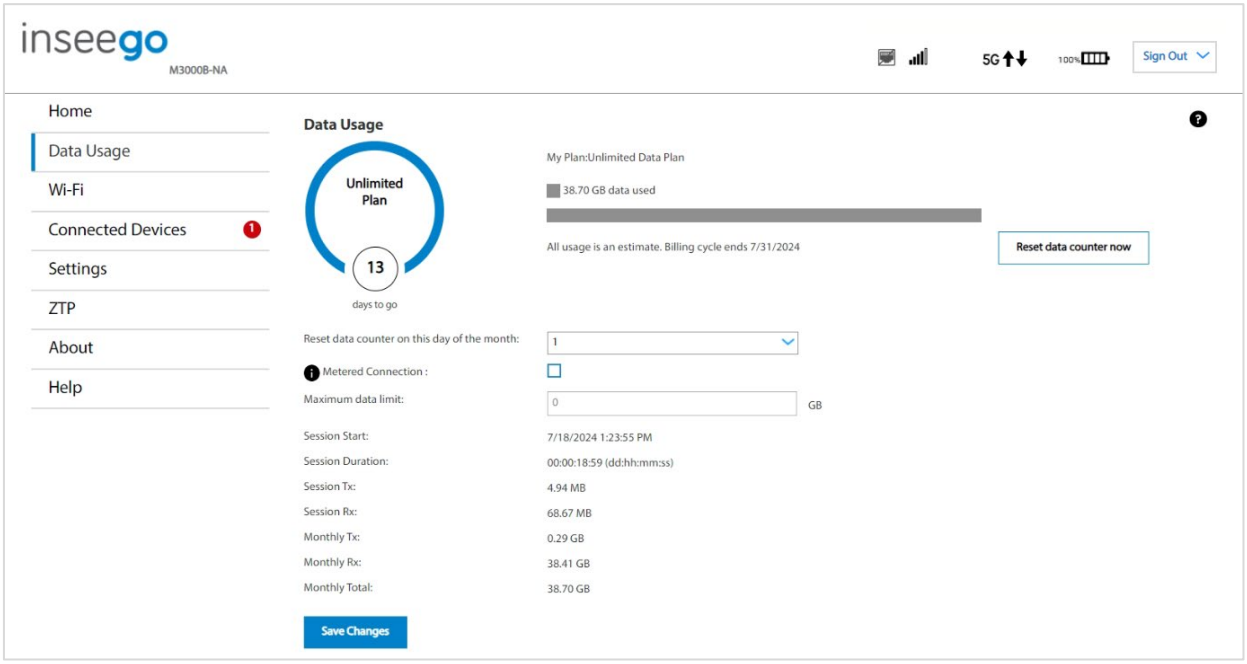


To view the Data Usage page, select ❯ from the Home page Data Usage panel or select **Data Usage** from the web UI side menu. The Data Usage page appears.

Data Usage page

Use the Data Usage page to view details about your MiFi data usage and billing plan.

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



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

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

You can configure settings to reflect your monthly data plan.

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

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

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

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

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

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

Session 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.

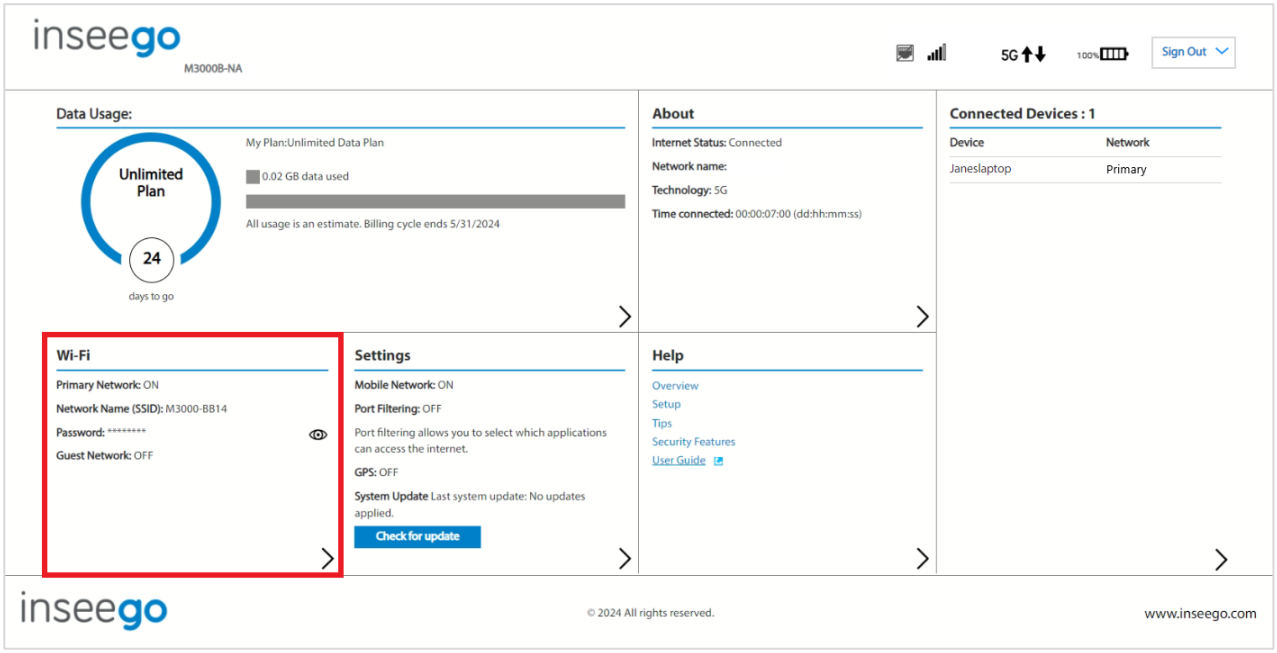
Monthly Total: The total amount of data for the current billing cycle.

Select **Save Changes** to enact changes.

Managing Wi-Fi settings

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

On the web UI Home page, the Wi-Fi panel shows the current name (SSID) and state of primary and guest networks. Click the eye icon to view the current passwords for each.



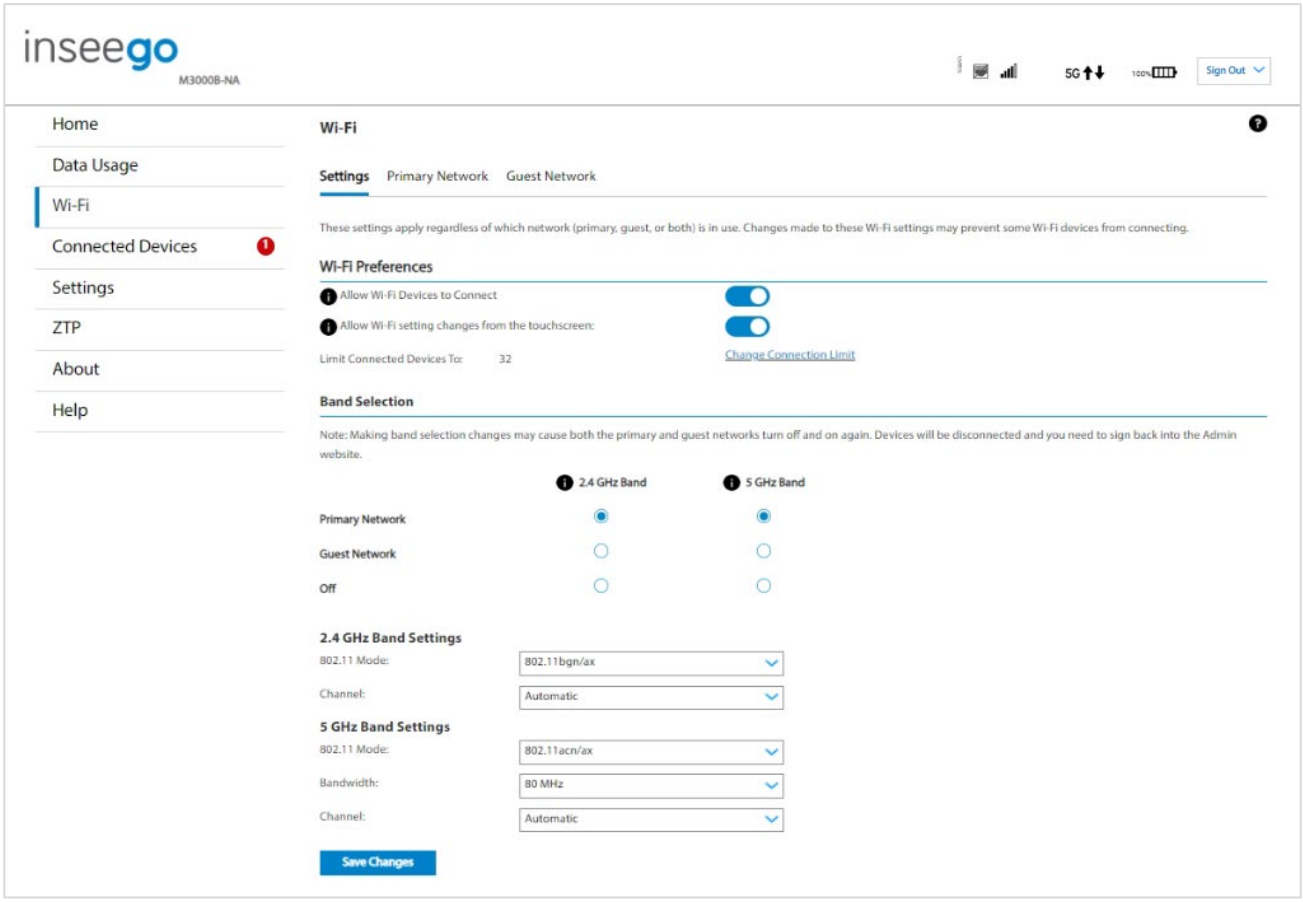
To manage settings for these networks, select > from the Home page Wi-Fi panel or select **Wi-Fi** from the web UI side menu.

The Wi-Fi page includes three tabs:

- Settings
- Primary Network
- Guest Network

Settings tab

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



Wi-Fi Preferences

Use the **Allow Wi-Fi Devices to Connect** on/off 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 MiFi is by tethering with a USB cable or via Ethernet if the Ethernet port is enabled.

Use the **Allow Wi-Fi setting changes from the touchscreen** on/off slider to allow or disallow setting Wi-Fi options on the MiFi touchscreen.

Select **Change connection limit** to change the maximum number of devices allowed to connect to your MiFi Wi-Fi. Use the slider to select a number and click **Save Changes**. The maximum number of connected devices is 32.

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.

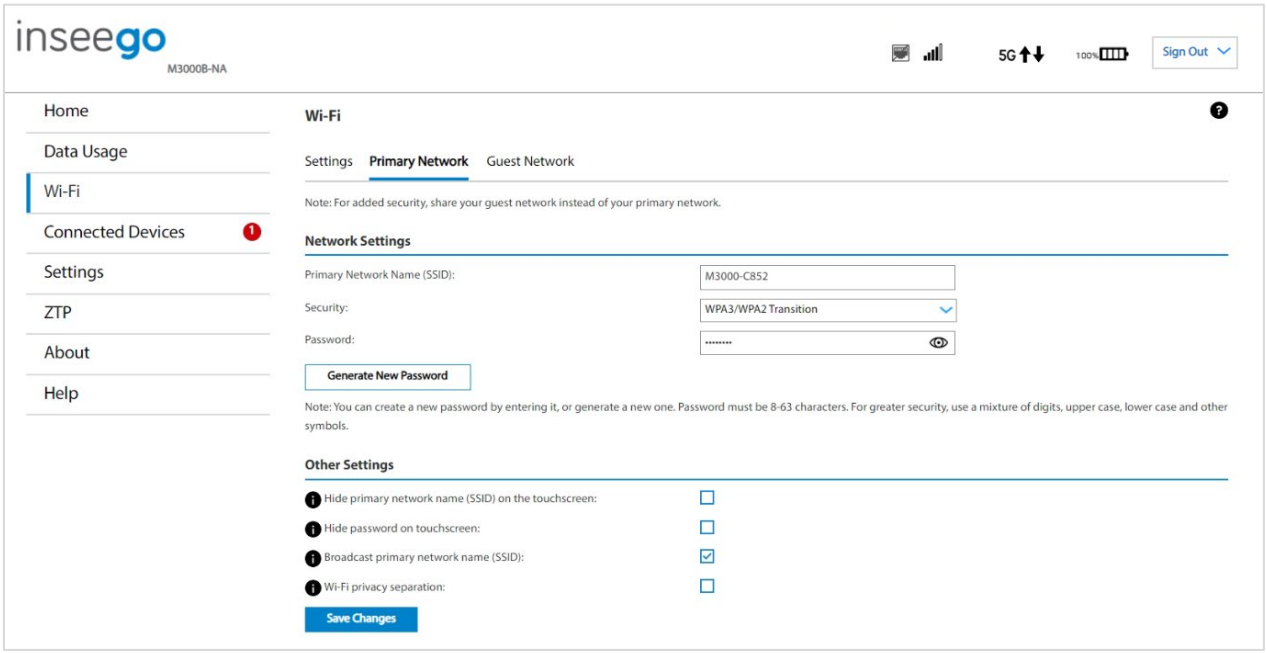
Bandwidth: Leave bandwidth at the default setting unless you experience interference with other Wi-Fi devices. If you experience interference, try lowering the setting to reduce the interference.

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.



Network Settings

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

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.
- **WPA2 Personal PSK (AES)** can be used for WPA2 devices.
- **WPA/WPA2 Mixed Mode** can be used if some of your older devices do not support WPA2.
- **None** allows anyone to connect and access Wi-Fi network and use your data plan to access the internet. **NOTE:** This setting is not recommended.

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

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

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

You can click the eye icon to view the password.

Other Settings

Hide primary network name (SSID) on the touchscreen: Check this box to hide the Wi-Fi primary network name on the MiFi touchscreen. If unchecked, the primary network name is visible on the touchscreen.

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

Broadcast primary network name (SSID): Check this box to display the Wi-Fi primary network in the list of available Wi-Fi networks on your connected devices. If unchecked, this network is not visible to connected devices.

WPS:[1] Check this box to use Wi-Fi Protected Setup (WPS) for the primary network. WPS allows compatible devices to connect to a Wi-Fi network without having to manually enter the password.

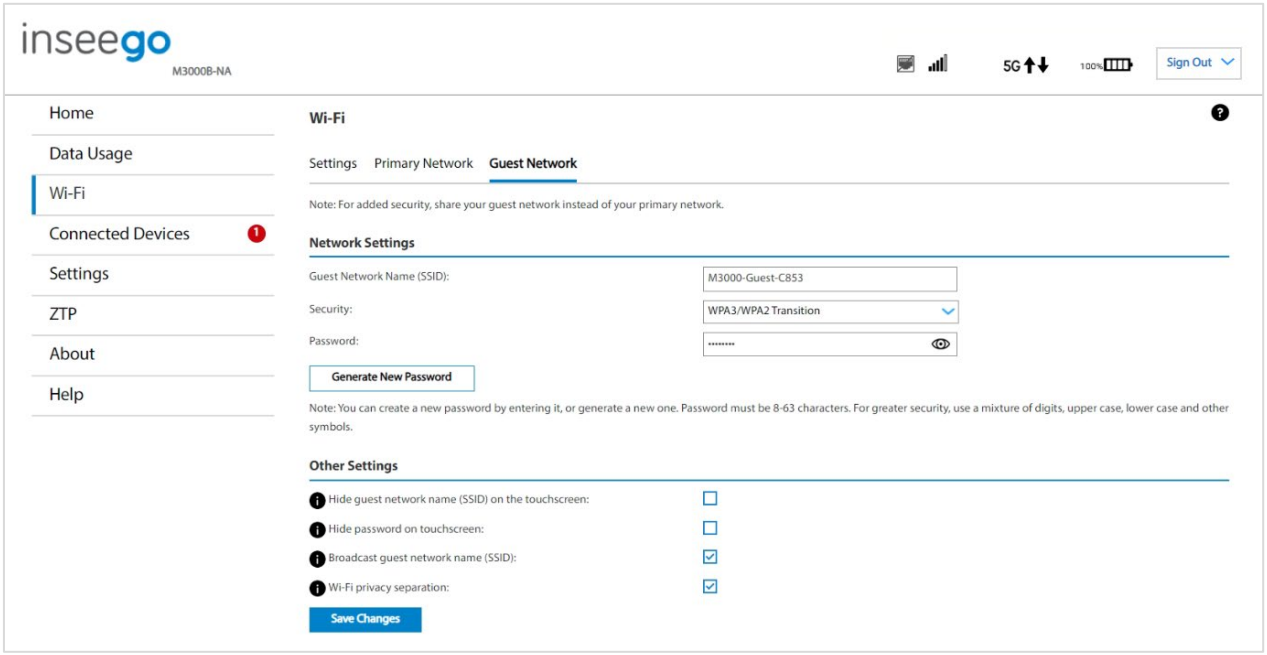
Wi-Fi privacy separation: Check this box to keep each connected device on this network isolated from all other connected devices. This provides additional security if some connected devices are unknown or not completely trusted.
NOTE: For normal operation, this should be unchecked.

Select **Save Changes**.

[1] This option may not be available on some devices.

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 MiFi 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.
- **WPA2 Personal PSK (AES)** can be used for WPA2 devices.
- **WPA/WPA2 Mixed Mode** can be used if some of your older devices do not support WPA2.
- **None** allows anyone to connect and access Wi-Fi network and use your data plan to access the internet. **NOTE:** This setting is not recommended.

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

Important: It is recommended 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

Hide guest network name (SSID) on the touchscreen: Check this box to hide the Wi-Fi guest network name on the MiFi touchscreen. If unchecked, the guest network name is visible on the touchscreen.

Hide password on touchscreen: Check this box to hide the Wi-Fi guest network password on the MiFi touchscreen. If unchecked, the guest network password is visible on the touchscreen.

Broadcast guest network name (SSID): Check this box to display the Wi-Fi guest network in the list of available Wi-Fi networks on your connected devices. If unchecked, this network is not visible to connected devices.

WPS:[1] Check this box to use Wi-Fi Protected Setup (WPS) for the guest network. WPS allows compatible devices to connect to a Wi-Fi network without having to manually enter the password.

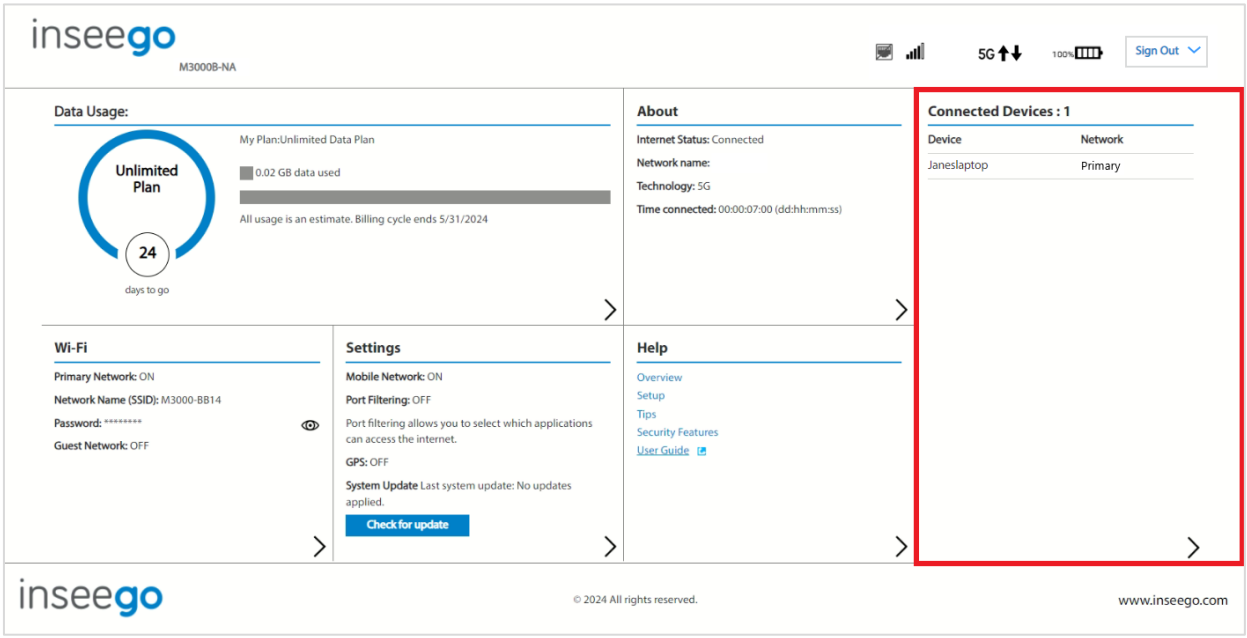
Wi-Fi privacy separation: Check this box to keep each connected device on this network isolated from all other connected devices. This provides additional security if some connected devices are unknown or not completely trusted.
NOTE: For normal operation, this should be unchecked.

Select **Save Changes**.

[1] This option may not be available on some devices.

Managing connected devices

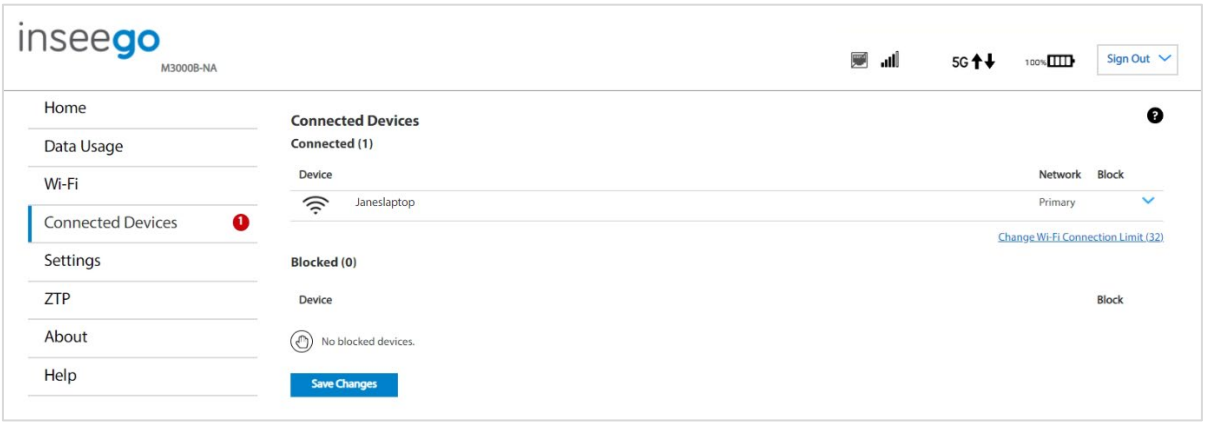
On the web UI Home page, the Connected Devices panel lists all devices currently connected to your MiFi, along with the network they are using.



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

Connected Devices page

This page provides details about each device connected to the MiFi and allows you to edit how device names appear in the web UI. You can also block or unblock a device from internet access.



Connected Devices

This table lists all devices connected to the MiFi:

Device: An icon indicates the connection type (Wi-Fi, USB, or Ethernet) for each device. (You can hover over the icon to read the type of connection.) 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.

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: The Block option is available only for devices connected through Wi-Fi.

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

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

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

Select **Change Wi-Fi connection limit** to change the maximum number of devices allowed to connect to your MiFi Wi-Fi. Use the slider to select a number and click **Save Changes**. The maximum number of connected devices is 32.

Blocked

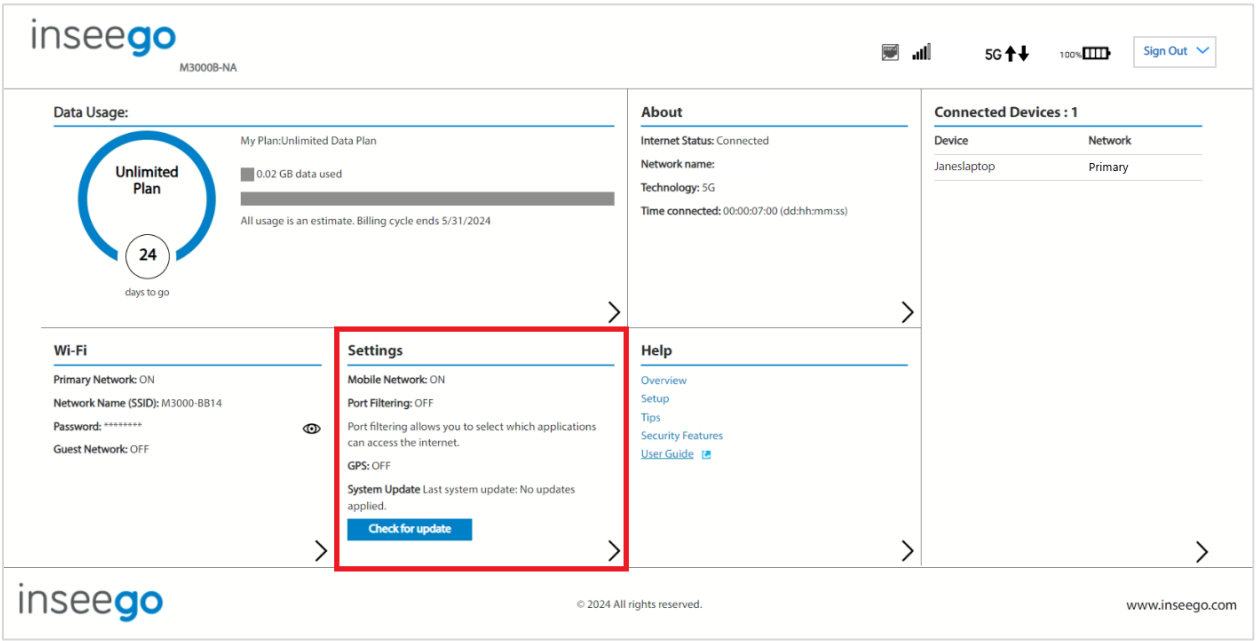
This section lists all devices blocked from connecting to the MiFi.

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

To unblock a blocked device, click the **Unblock** button and select **Save Changes**. The device is removed from the **Blocked** list and appears in the **Connected Devices** list above.

Managing settings

On the web UI Home page, the Settings panel shows the current Mobile Network, Port Filtering and GPS settings (on/off), and the date and time of the last system update.



To change system settings, select > from the Home page Settings panel or select **Settings** from the web UI side menu.

The Settings page includes the following tabs:

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

Preferences tab

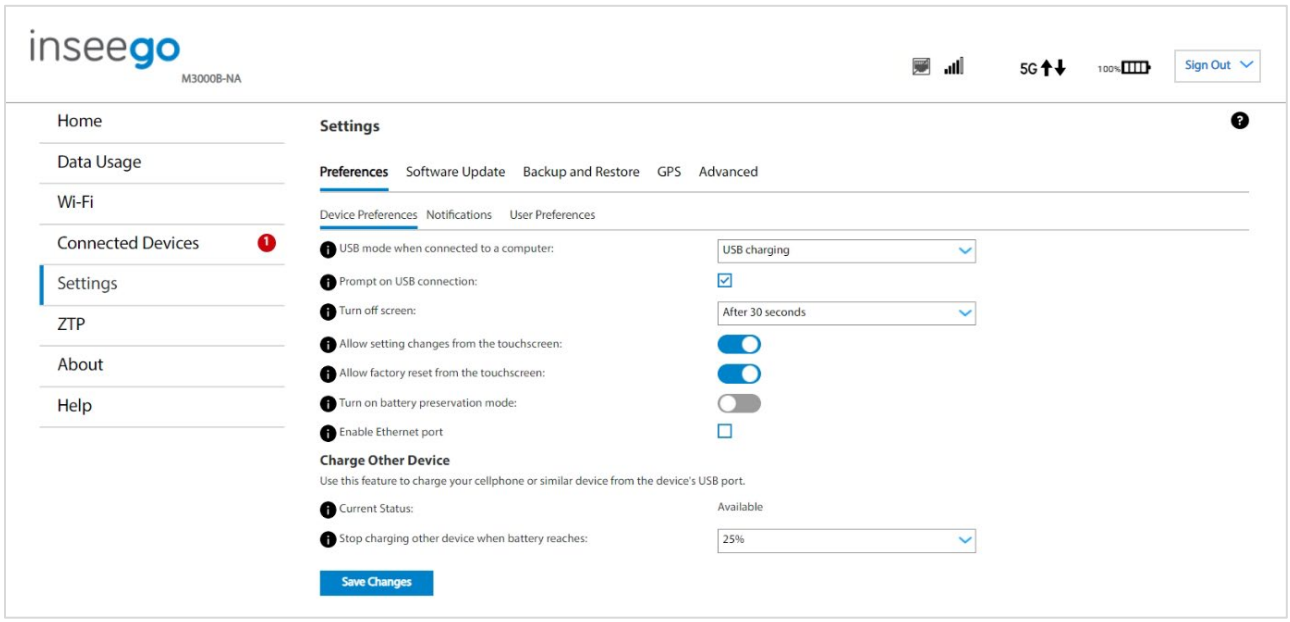
This tab allows you to configure options for the MiFi touchscreen, notification settings, and web UI display settings.

The Preference tab includes three sub tabs:

- Device Preferences
- Notifications
- User Preferences

Device Preferences sub tab

Use this page to set options for the MiFi touchscreen.



USB mode when connected to a computer: Use the drop-down list to select the type of connection you want for devices connecting to the MiFi USB-C port: USB charging, internet access via USB and Wi-Fi, or internet access via USB only.

Prompt on USB connection: Check this box for a prompt to display on the MiFi screen when a device connects via USB. The prompt allows selection of the USB mode of connection.
NOTE: A USB mode selection made on the MiFi touchscreen does not change the setting above. The setting above acts as a default, and the choice on the MiFi touchscreen sets the mode for the current USB session only.

Turn off screen: Use the drop-down list to select how long you want the MiFi to be inactive before the touchscreen turns off.

Sleep[1]: Use the drop-down list to select how long you want the MiFi to be inactive before entering sleep mode.

Shutdown[1]: Use the drop-down list to select how long you want the MiFi to be inactive before shutting down.

Allow settings changes from the touchscreen: Use the on/off slider to allow or disallow configuration of settings on the MiFi touchscreen.
NOTE: If on, settings can be configured on the MiFi touchscreen, including Factory Reset, which resets all settings to factory default settings and disconnects all connected devices.

Allow factory reset from the touchscreen: Use the on/off slider to allow or disallow factory reset from the MiFi Reset button and touchscreen (Settings > Factory Reset). If on, factory reset is allowed from the MiFi Reset button and touchscreen. Factory reset resets all settings to factory default

[1] This option may not be available on some devices.

settings and disconnects all connected devices.
NOTE: If **Allow settings changes from the touchscreen** (above) is off, Settings > Factory Reset is not available on the touchscreen, even when this slider is on.

Turn on battery preservation mode:[1] Battery Preservation Mode is enabled by default. When enabled, Battery Preservation Mode is automatically activated after an extended period of approximately 16 hours of continuous power charge and maintains a battery charge level between 70% and 80%[2]. This helps prevent overcharging and aids in preserving the integrity of your battery. This mode is strongly recommended if you frequently charge your device for extended periods of time.

Enable Ethernet port: Check this box to enable the Ethernet port.
NOTE: The Ethernet port is disabled by default to optimize battery life.

Charge Other Device

You can charge devices such as your phone or Bluetooth headset from the MiFi by connecting the device's USB cable to the MiFi's USB-C port.

Current Status: The current status of Charge Other Device:

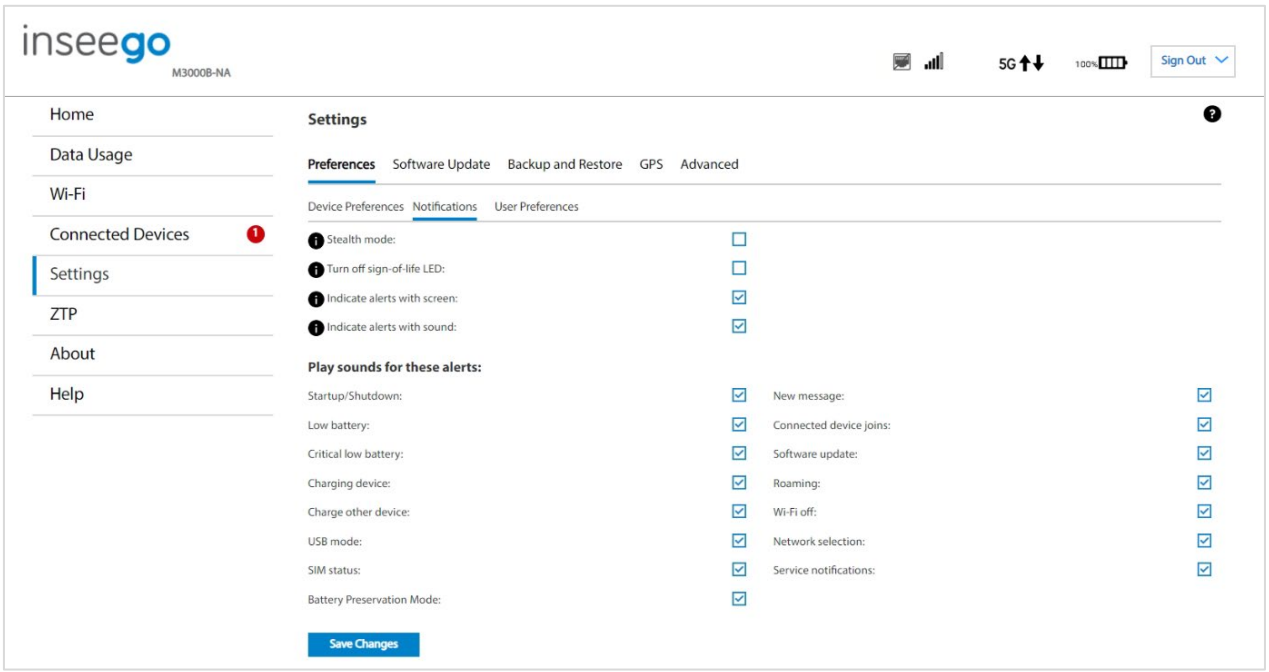
> **Charging** – A device is being charged from the MiFi battery.
> **Available** – If a device connects to the MiFi USB-C port, it will be charged.
> **Not available (low battery)** – The MiFi battery is too low to charge a device.

Stop charging other device when battery reaches: Use the drop-down list to select a battery percentage for the MiFi at which you want to stop charging other devices in order to reserve MiFi battery power.
NOTE: Do not use the Charge Other Device feature if you want to use the battery for a full day.

[1] This option may not be available on some devices.
[2] On some devices, Battery Preservation Mode maintains battery level at 50% to 60%.

Notifications sub tab

Use this page to set options for notifications on your MiFi.



Stealth mode: Check this box to turn off the LED and audio capabilities of your MiFi.
NOTE: If checked, other than the startup process, the MiFi touchscreen turns on only when the Power button is pushed.

Turn off sign-of-life LED: Check this box to turn off the LED status light. When unchecked, the LED blinks slowly as a "sign of life." This option is grayed out if Stealth mode is on.

Indicate alerts with screen: Check this box to turn on your MiFi touchscreen when an alert message displays. This setting is enabled by default.

Indicate alerts with sound: Check this box to have your MiFi make sounds upon startup, shutdown, and other various events. This setting is enabled by default. This option is grayed out if Stealth mode is on.

Play sounds for these alerts:

Check the boxes for the events you want to trigger an audio alert:

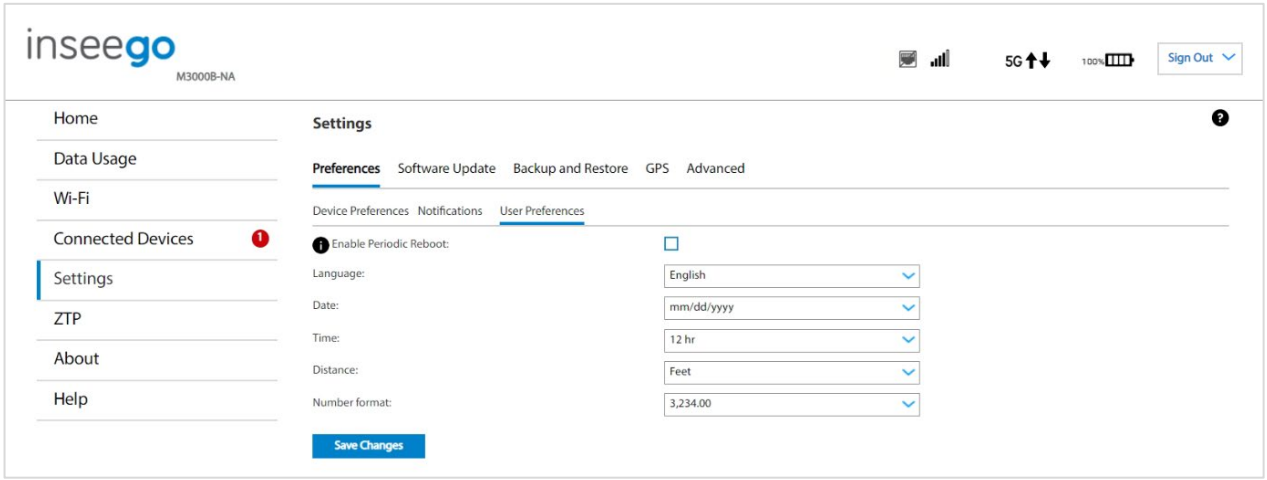
- **Startup/Shutdown**
- **Low battery**
- **Critical low battery**
- **Charging device**
- **Charge other device**
- **USB mode**
- **SIM status**
- **Battery Preservation Mode**
- **New message**
- **Connected device joins**
- **Software update**
- **Roaming**
- **Wi-Fi off**
- **Network selection**[1]

NOTE: This section is grayed out if the Stealth mode setting above is checked or Indicate alerts with sound setting is unchecked.

[1] This option may not be available on some devices.

User Preferences sub tab

Use this page to change how dates, time, distance, and numbers are displayed in the Admin web UI.



Enable Periodic Reboot[1]**:** 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.

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).

Distance: Select the distance format to be used for the web UI when marking GPS altitude and accuracy (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).

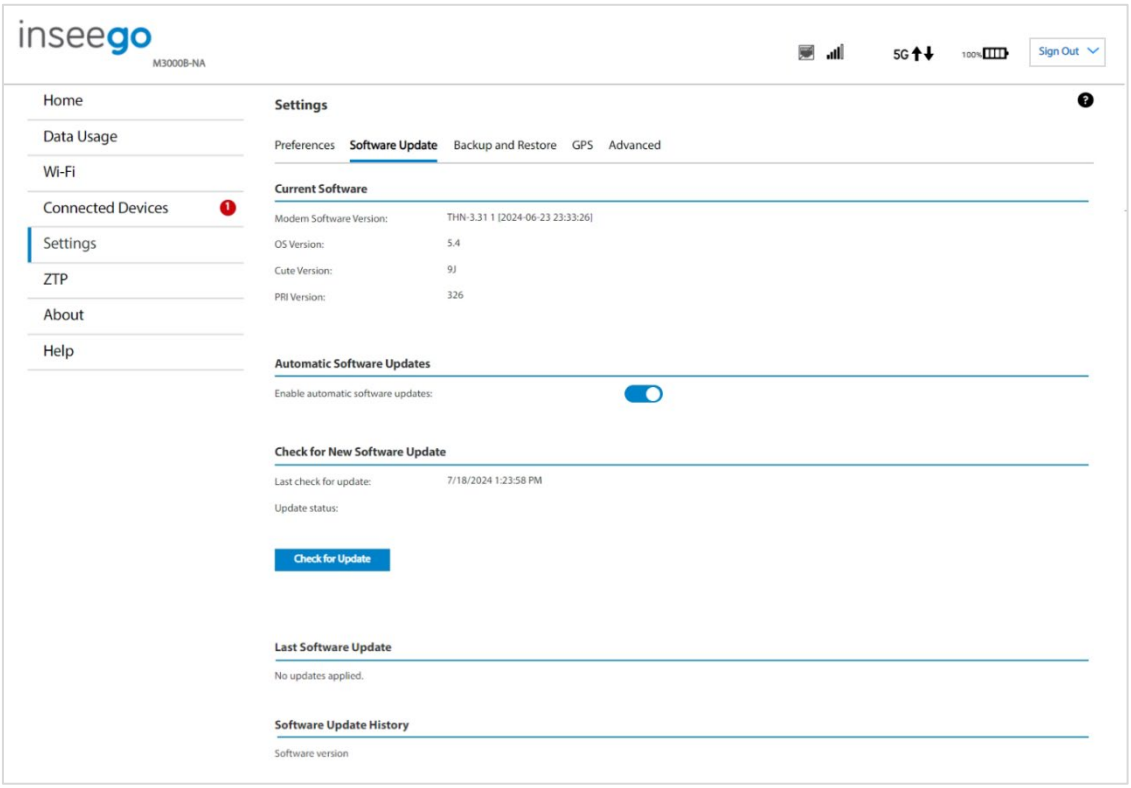
Select your display choices from the drop-down menus and click **Save Changes** to update settings.

[1] This option may not be available on some devices.

Software Update tab

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



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 MiFi.

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

Check for New Software Update

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

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

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

Last Software Update

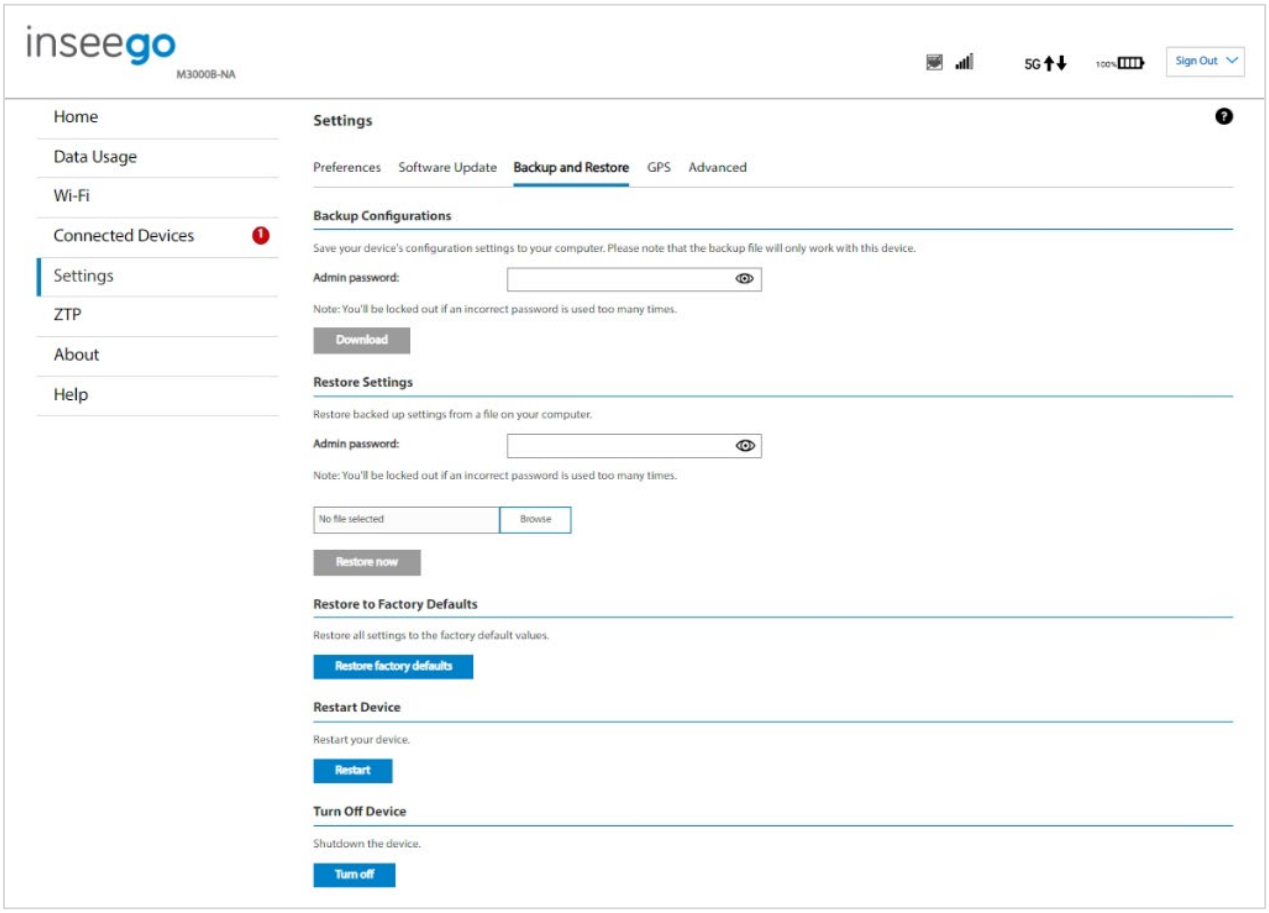
This section displays details about the last software update.

Software Update History

This section displays details of the last updates that have been downloaded and installed to this device. If no updates have been installed, this section displays the current software version.

Backup and Restore tab

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



Backup Configurations

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

If you don't remember the Admin password, click the down arrow next to **Sign Out** in the top-right corner of any web UI page and click **Change Password,** then **Forgot Admin password?**. Answer the displayed security question. The current Admin password will be displayed. Alternately, you can view the Admin password on the MiFi touchscreen by tapping **Help** > **Admin Website** or **Menu** > **Settings** > **Advanced Settings**.

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

Click the **Download** button. The file is automatically downloaded to your Downloads folder. This configuration file contains all settings for your MiFi.

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 MiFi.

Restore Settings

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

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

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

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

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 MiFi and disconnecting you from the web UI.

Restart Device

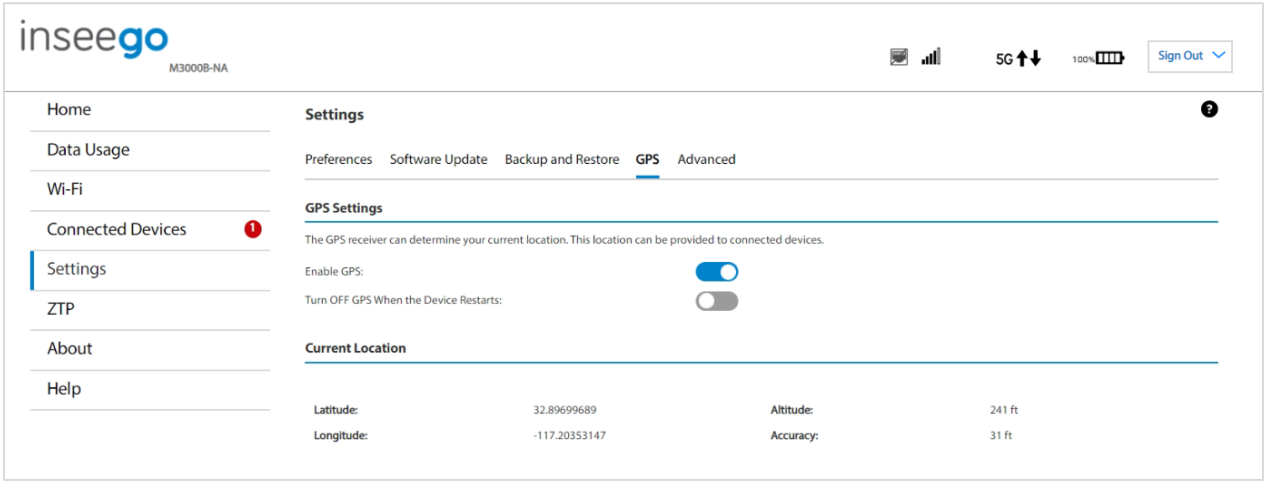
Restart: This button turns your MiFi off and on again.

Turn off Device

Turn Off: This button turns your MiFi off.

GPS tab

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

Turn OFF GPS Over Wi-Fi[1]: This setting determines whether location information can be shared with connected devices. When the on/off slider is on, location information can be shared. 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.

Port Number[1]**:** The TCP port number used to establish a connection to the MiFi 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**[2] to update settings.

[1] This option may not be available on some devices.
[2] The **Save Changes** button may not be available on some devices. Changes will occur when made.

GPS Driver[1]

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 MiFi, 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.

NOTE: You can change the format of measurement (Feet or Meters) in **Settings > Preferences > User Preferences**.

Advanced tab

Advanced settings are intended only for users with advanced technical knowledge. For information about the advanced settings, go to Chapter 4, Advanced settings on page 77.

[1] This option may not be available on some devices.

Initiating ZTP for SD EDGE

Inseego 5G 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 5G SD EDGE offering go to https://inseego.com/products/cloud-management/inseego-sd-edge/.

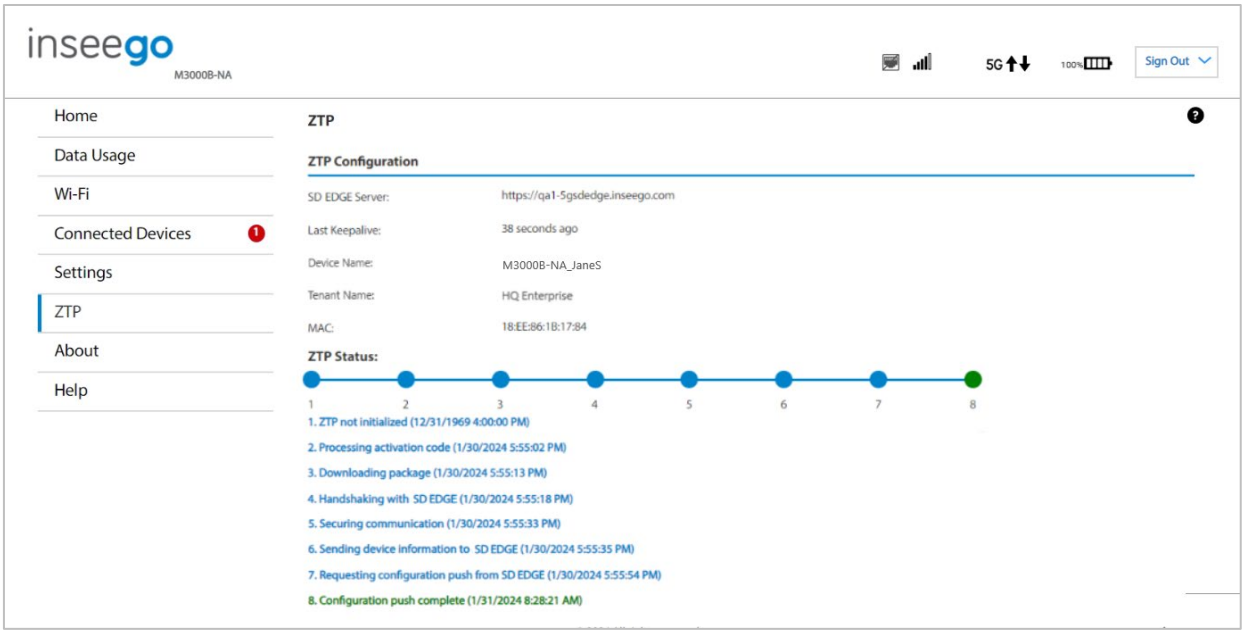
NOTE: This tab may not be available, or may be located under **Settings**, depending on your device model or service provider.

ZTP tab

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

When registering or configuring a device with SD EDGE, you will receive an activation email with instructions and an activation URL. Connect to the device network and click the provided activation link to begin the activation process. The ZTP page displays the configuration parameters and progress of the activation.

NOTE: Once a device is registered with SD EDGE, all configurations are managed by EDGE Manager and are no longer available through the Admin web UI, Inseego Mobile app, or Inseego Connect.



ZTP Configuration

SD EDGE Server: The URL of the SD EDGE server.

Last Keepalive: The last amount of time since that last WireGuard tunnel handshake with SD EDGE. This is used for debugging.

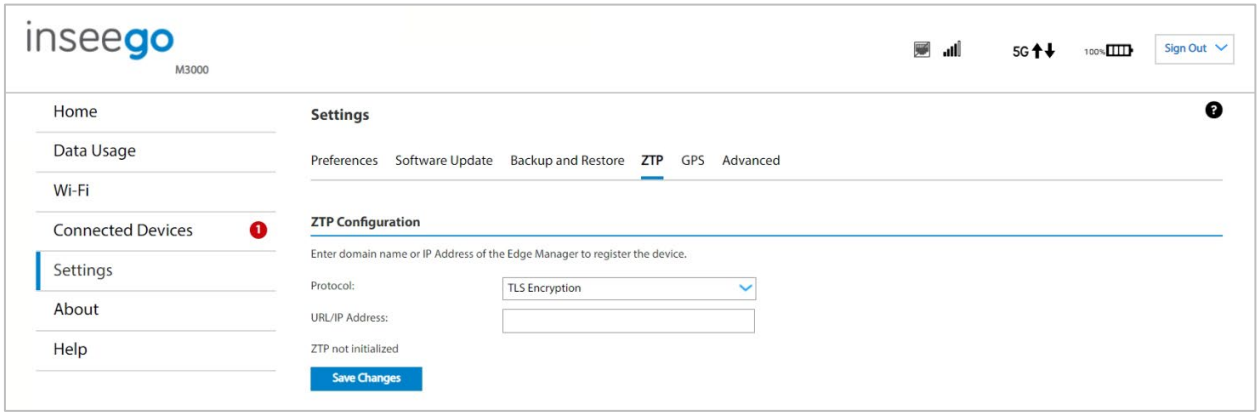
Device Name: The name of the device.

Tenant Name: The name of the tenant on which the device is registered.

MAC: The Media Access Controller (MAC) address for the bridge interface.

ZTP Status: The activation process displays in eight steps. When a step is in progress, the step text displays blue with fade-in/fade-out animation and a timestamp. When a step is successfully completed, the animation stops, and the text is solid blue. When Step 8 displays as green, the activation is complete.

NOTE: If the ZTP tab on your web UI is located under **Settings**, it is configured as follows.



ZTP Configuration

Protocol: Use TLS Encryption[1] as the protocol.

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

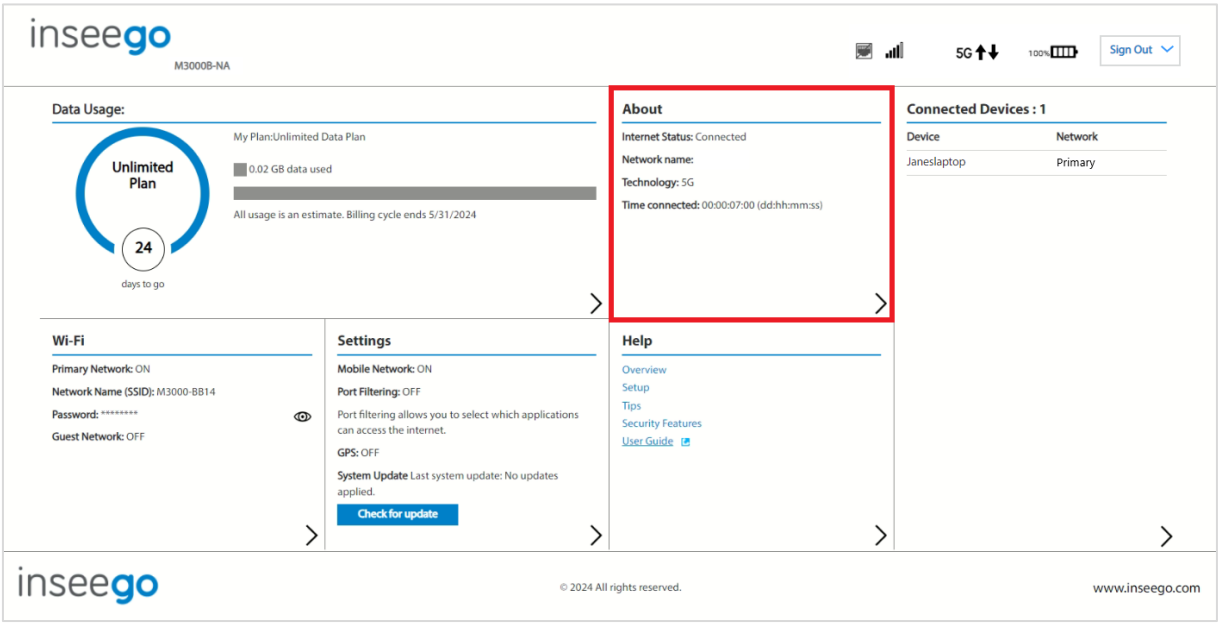
URL/IP Address: Enter the domain used for your EDGE Manager instance.

Click **Save Changes** to initiate ZTP.

[1] The protocol choices may appear as **SSL** or **No SSL** on some devices. Use **SSL**.

Viewing info about your MiFi

On the web UI Home page, the About panel shows current internet status, the name of the network to which the MiFi is connected, technology, and amount of time connected.



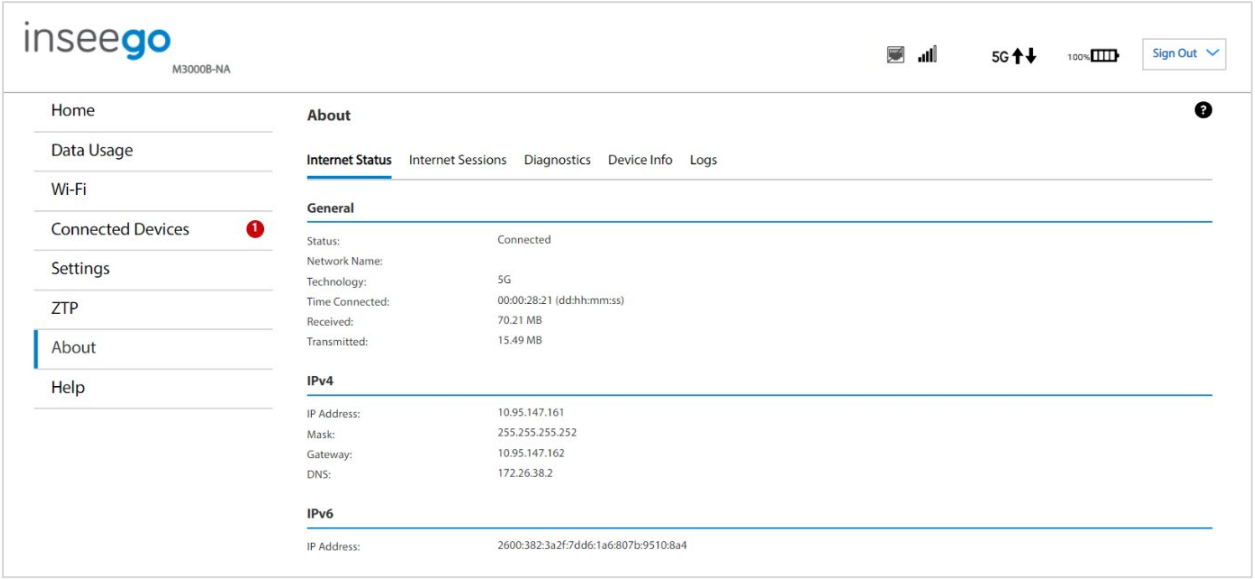
To view more detailed information about your MiFi and its use, select > from the Home page About panel (or select **About** from the web UI side menu).

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 MiFi internet connection.

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

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 MiFi.

Mask: The network mask associated with the IPv4 address.

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

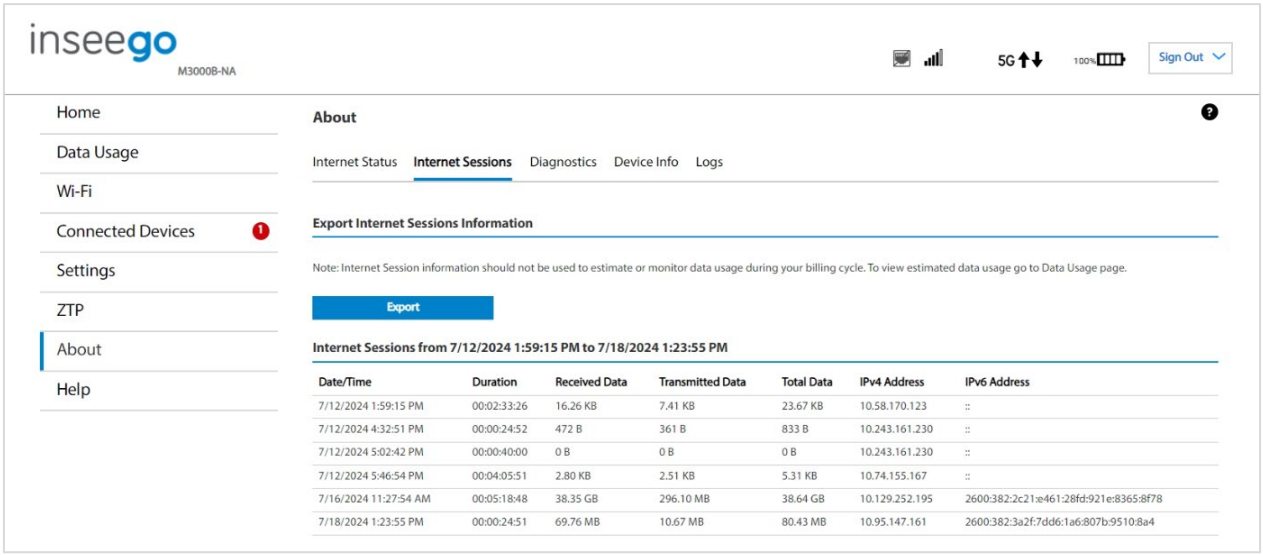
DNS: The Domain Name Server currently used by the MiFi.

IPv6

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



Date/Time	Duration	Received Data	Transmitted Data	Total Data	IPv4 Address	IPv6 Address
7/12/2024 1:59:15 PM	00:02:33:26	16.26 KB	7.41 KB	23.67 KB	10.58.170.123	::
7/12/2024 4:32:51 PM	00:00:24:52	472 B	361 B	833 B	10.243.161.230	::
7/12/2024 5:02:42 PM	00:00:40:00	0 B	0 B	0 B	10.243.161.230	::
7/12/2024 5:46:54 PM	00:04:05:51	2.80 KB	2.51 KB	5.31 KB	10.74.155.167	::
7/16/2024 11:27:54 AM	00:05:18:48	38.35 GB	296.10 MB	38.64 GB	10.129.252.195	2600:382:2c21:e461:28fd:921e:8365:8f78
7/18/2024 1:23:55 PM	00:00:24:51	69.76 MB	10.67 MB	80.43 MB	10.95.147.161	2600:382:3a2f:7dd6:1a6:807b:9510:8a4

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.

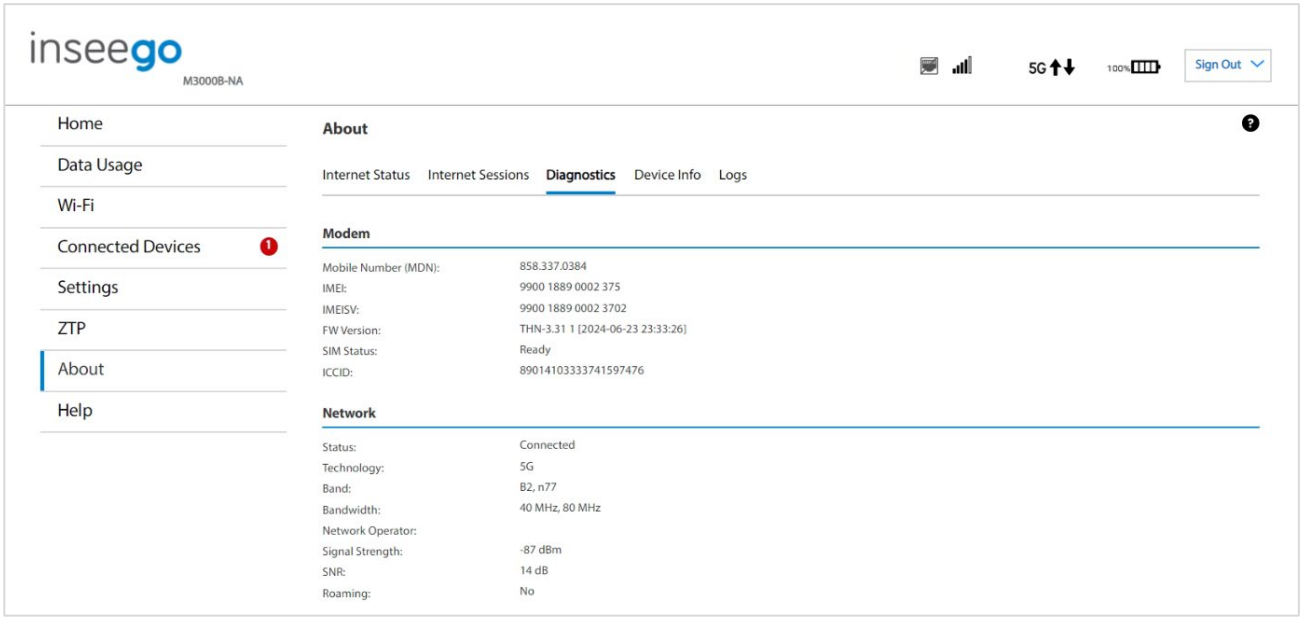
Total Data: The total amount of data for the internet session. This is the sum of Received Data and Transmitted Data.

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 carrier).

Diagnostics tab

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



Modem

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

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

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

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

SIM Status: Indicates 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: Not available or Available.

Technology: 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).

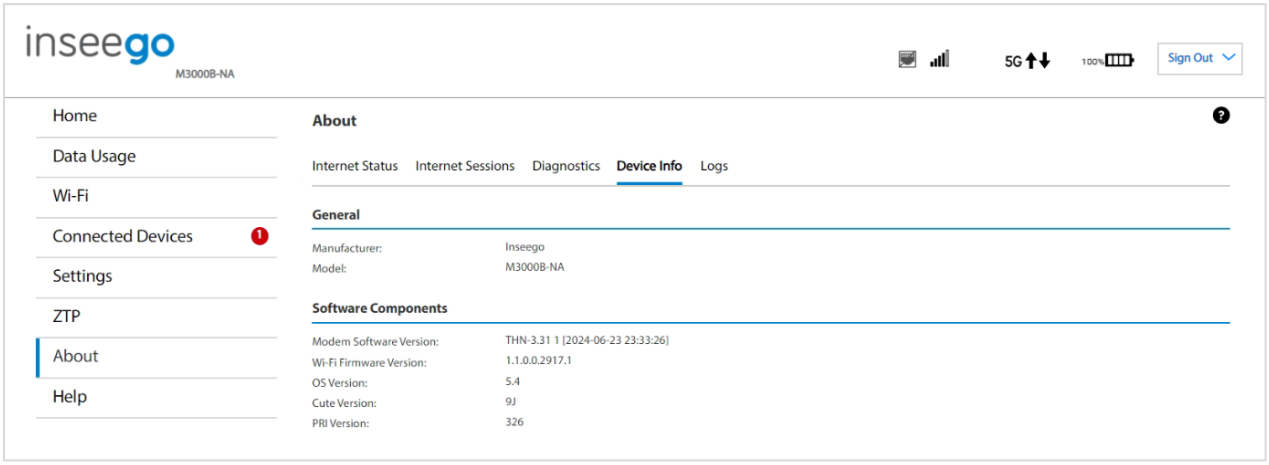
Signal Strength: The strength of the cellular signal, measured in dBm. Higher absolute values indicate a stronger signal, for example: -80 dBm is a stronger signal than -90 dBm.

SNR: Signal to Noise Ratio. A measure of the ratio between signal strength and noise level. SNR values are positive, and higher numbers are better.

Roaming: Indicates whether roaming is on.

Device Info tab

Use this tab to view details about your MiFi.



General

Manufacturer: Inseego.

Model: The model of your MiFi.

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.

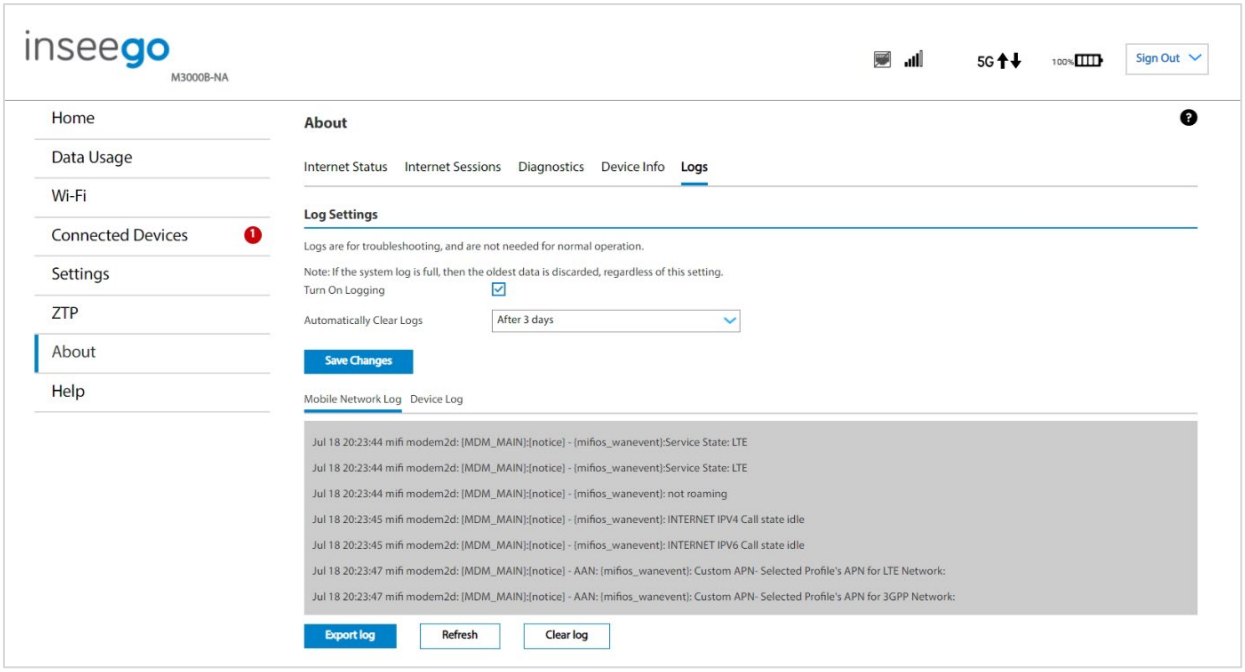
OS Version: The version number for the operating system and its components.

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

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

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

Click **Save Changes** to enact changes.

If logs are turned on, the following are visible:

Mobile Network Log: This tab displays the log data of connections to the mobile network.

Device Log: This tab displays the log data of events other than mobile data connections that occurred on this device.

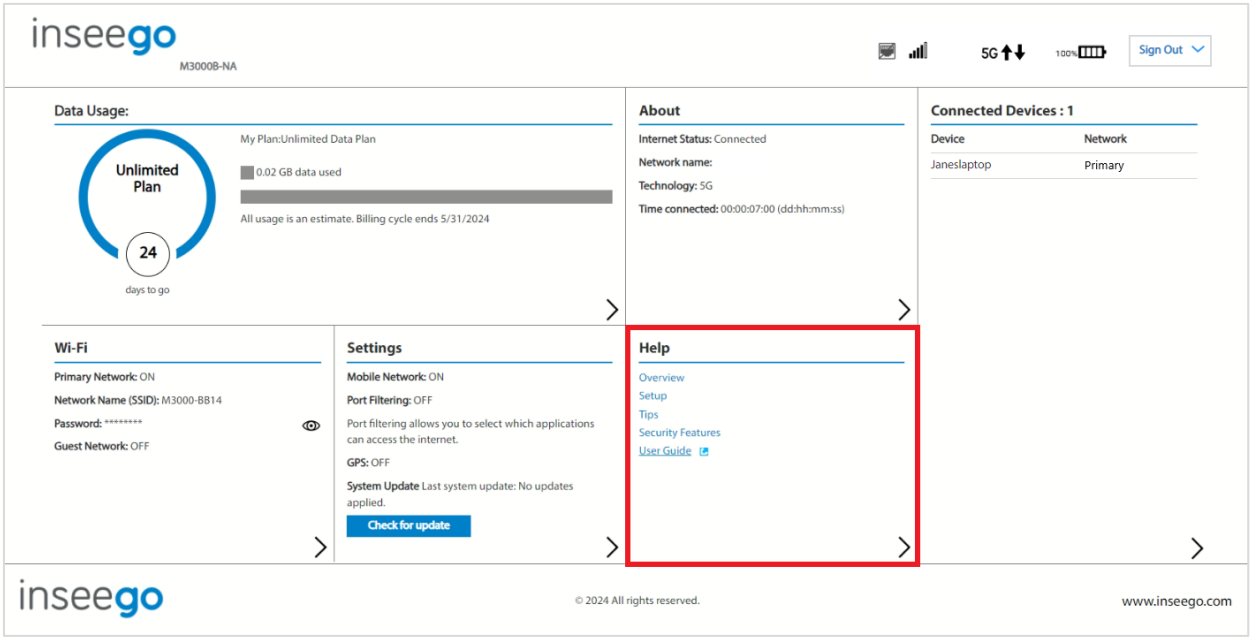
Export Log: Allows you to download log data.

Refresh: Updates the displayed log data.

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

Getting help

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



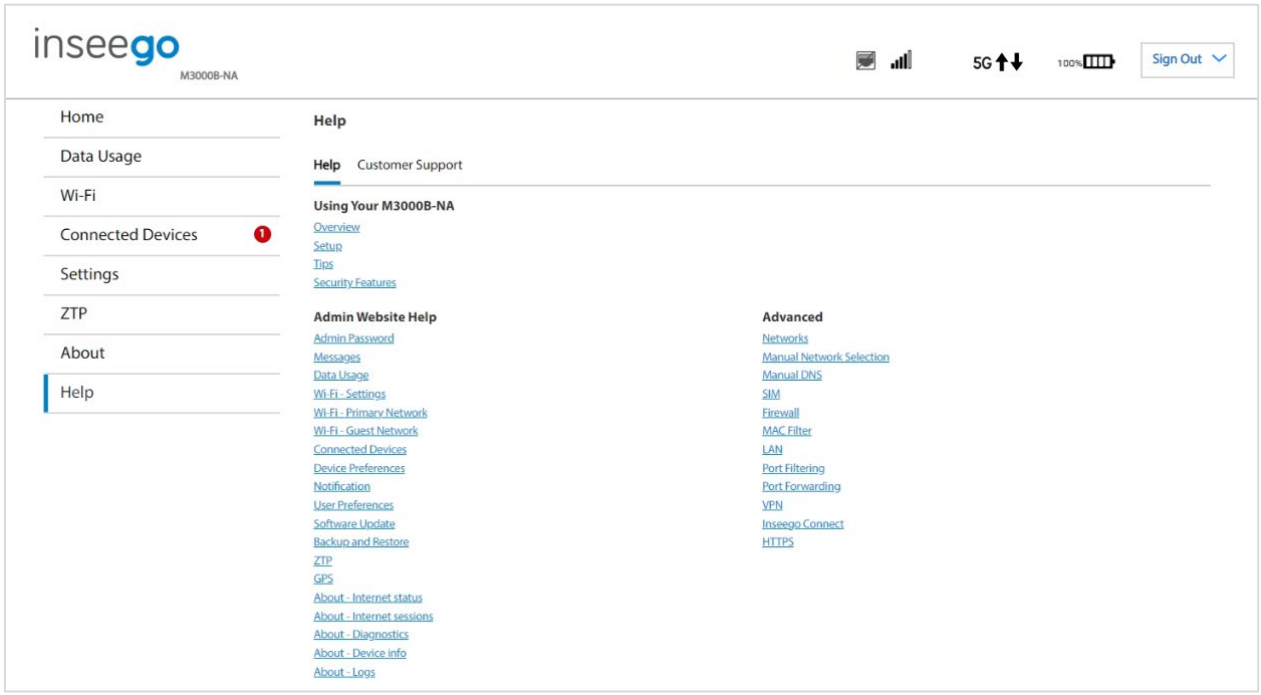
To view more detailed help information, select > from the Home page Help panel (or select **Help** from the web UI side menu).

The Help page includes two tabs:

- Help
- Customer Support

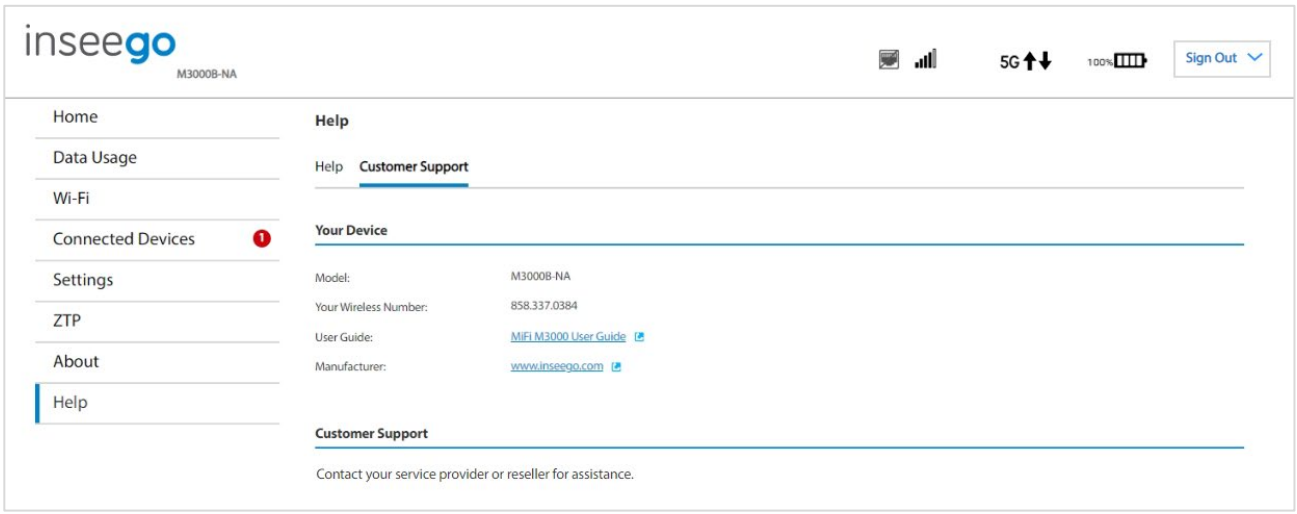
Help tab

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



Customer Support tab

Use the Customer Support tab for support information.



Your MiFi

Model: The model of your MiFi.

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

Customer Support

Contact your service provider or reseller for customer support.

4

Advanced settings

Overview

Using advanced settings

Overview

The Advanced pages on the MiFi Admin web UI are intended for users with technical expertise in the area of telecommunication and networking.

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

Using advanced settings

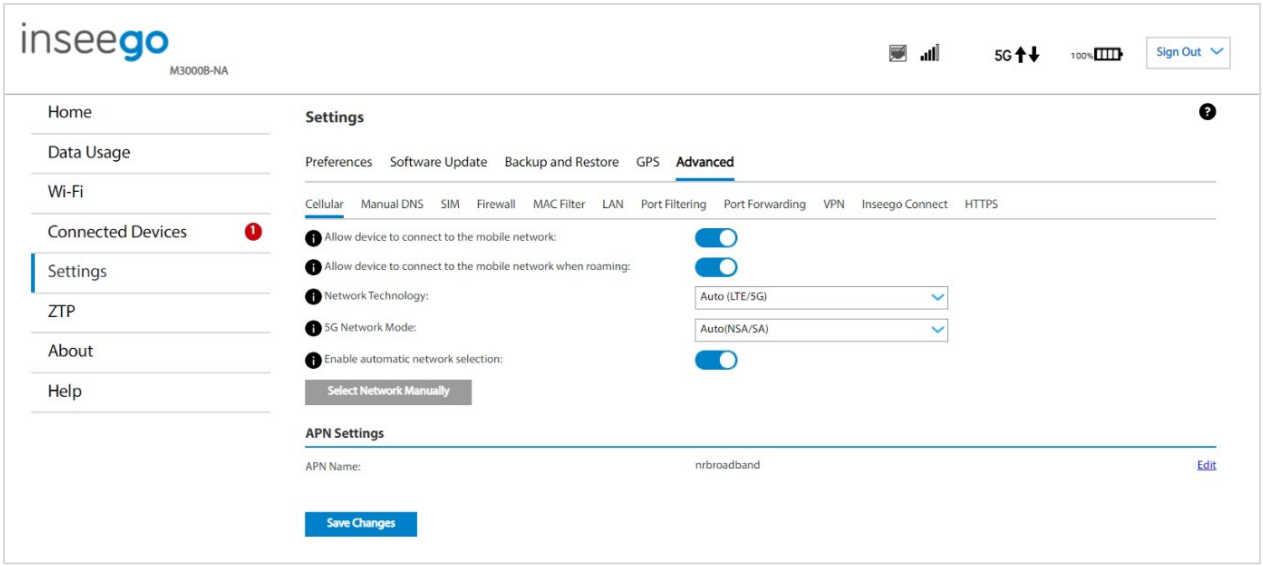
When you select the **Advanced** tab on the Settings page, a warning message appears. If you click **Continue**, the Cellular tab of the Advanced page appears.

The Advanced page includes the following tabs:

- Cellular
- Manual DNS
- SIM
- Firewall
- MAC Filter
- LAN
- Port Filtering
- Port Forwarding
- VPN
- Inseego Connect
- Heartbeat timer (Inseego Connect)

Cellular tab

In most configurations, the MiFi is used with a dynamic IP and SIM, and the Access Point Name (APN) is available from the network. However, if you are on a private network, you may need to set the APN on this tab for the network to communicate with the MiFi.



Allow device to connect to the mobile network:[1] Use the on/off slider when necessary to turn off cellular data and prevent access to the mobile network. This prevents connected devices from connecting to the internet and using your MiFi's mobile data plan. For normal operation, this setting must be left on.

Allow device to connect to the mobile network when roaming: Use the on/off slider when necessary to turn international and domestic roaming on or off as needed. Additional data charges may apply when roaming.

Network Technology:[1] Use the drop-down to select the type of cellular data connection (Auto (LTE/5G), LTE/UMTS, or 5G).

5G Network Mode:[1] Use the drop-down to select the network mode (Auto(NSA/SA), SA, or NSA). **NOTE:** NSA (Non-Standalone) uses 4G anchor bands. SA (Standalone) uses only 5G bands.

Enable automatic network selection: When the on/off slider is on, your MiFi automatically selects the best available network, and you cannot use the **Select Network Manually** button.

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

[1] This option may not be available on some devices.

APN Settings

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

APN: Use the drop-down to choose the APN for your MiFi.

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

NOTE: Sub settings may appear, depending on your APN selection. These settings cannot be modified and saved, for example: **PDP Type** cannot be changed on an already defined APN profile. To modify sub settings for an APN, you must add a new APN profile by selecting **Add APN** from the APN drop-down and configuring the desired settings.

To set up your MiFi for static IP, please contact your service provider to set up a line of service for static IP and for steps to configure your MiFi for static IP functionality.

Click **Save Changes**. The MiFi will reboot for changes to take effect.

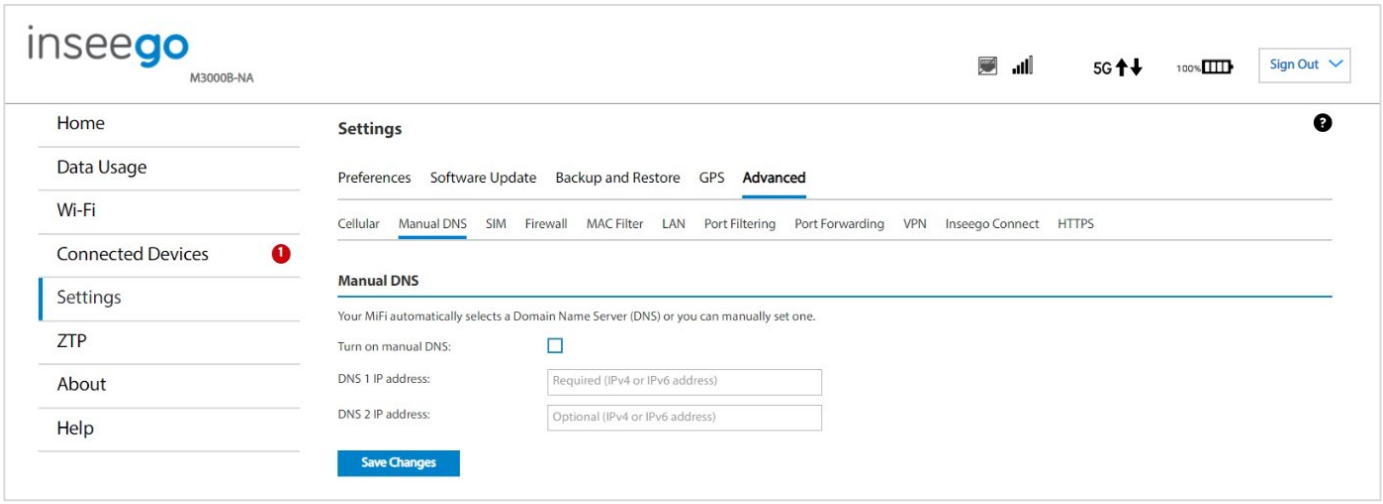
Manual DNS

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

- Manual DNS tab (Admin web UI)
- DNS Content Filtering (Inseego Connect) [1]

Manual DNS tab

The MiFi automatically selects a Domain Name Server (DNS). This tab 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**.

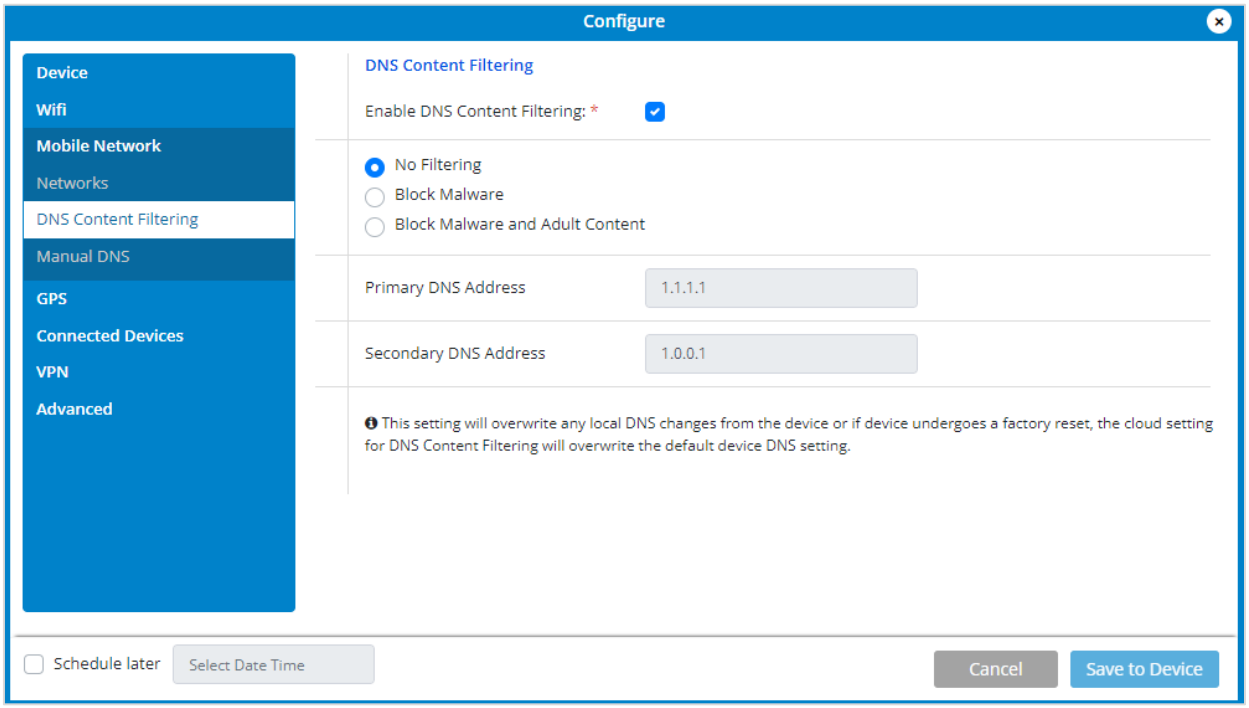
[1] This option may not be available on some devices.

DNS Content Filtering (Inseego Connect)

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

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

NOTE: Settings on this page override any settings 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.

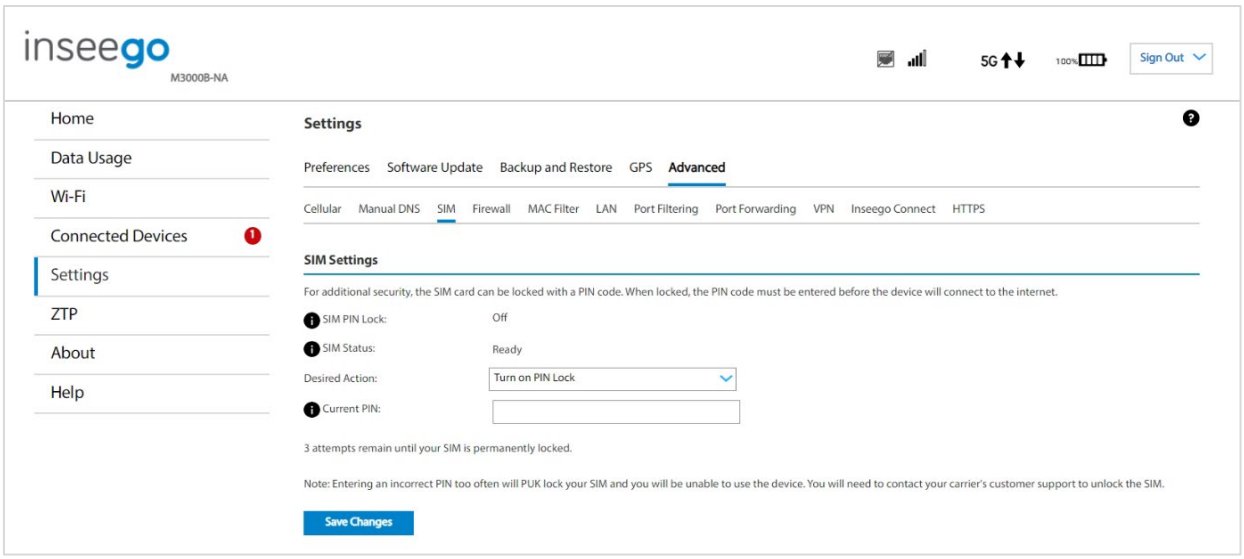
Select the filter level (Block Malware, or Block Malware and Adult Content).

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**.

SIM tab

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

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



SIM Settings

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

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

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

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

- **PIN Lock** - If the SIM is currently PIN locked, you are prompted to enter the PIN.
  NOTE: If an incorrect PIN is entered too many times, the SIM becomes PUK locked. A counter indicates how many incorrect entries will cause PUK lock. Once PUK locked, the PUK must be obtained from your service provider.

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

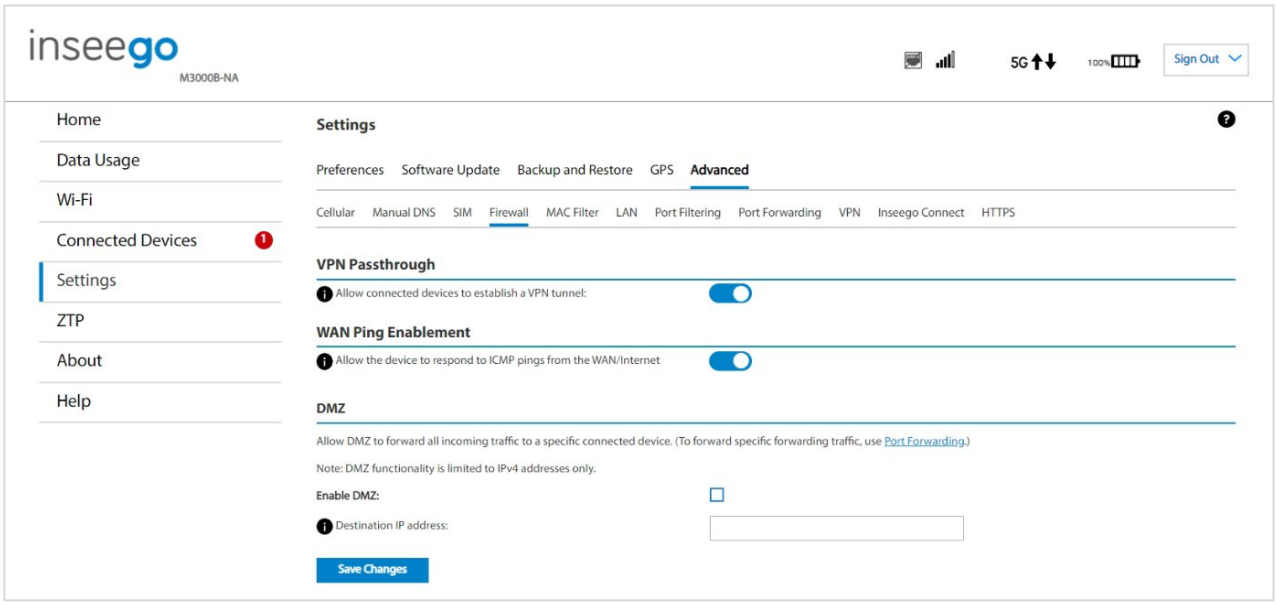
Current PIN: Enter the current PIN.

Click **Save Changes**.

Firewall tab

The MiFi firewall determines which internet traffic is allowed to pass between the MiFi and connected devices and protects your connected devices from malicious incoming traffic from the internet. The firewall cannot be turned off.

Use this tab to allow VPN passthrough and to designate a specific device to receive all traffic.



VPN Passthrough

Allow connected devices to establish a VPN tunnel: To use the **VPN Passthrough**, ensure the on/off slider is on. This allows you to establish a VPN tunnel while using your MiFi.

WAN Ping Enablement[1]

By default, the device will ignore ping requests received from the WAN/internet. To enable your MiFi to respond to the ping requests received, 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 and settings in this section are not available.

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

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

Enable DMZ: Check this box to allow DMZ.

[1] This option may not be available on some devices.

Destination IP address: Enter the IP address of the connected device you wish to become the DMZ device (the DMZ destination).

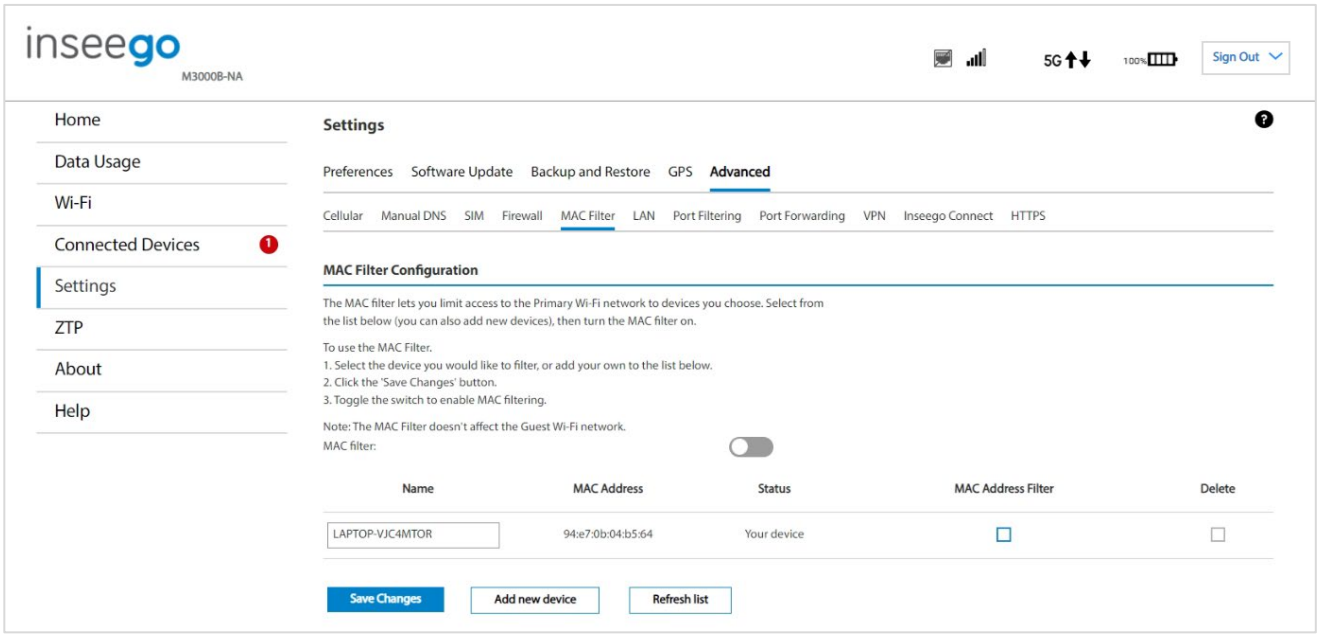
NOTE: You can check the IP address of each connected device on the Connected Devices tab.

Click **Save Changes**.

MAC Filter tab

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

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



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

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 primary network and move the on/off slider to on. Click **Save Changes**.

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

A device list displays all devices currently connected to the MiFi.

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

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

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

Notes on Blocking Devices

There are two ways to block devices from connecting to the MiFi:

- **Temporarily block a device from connecting to the MiFi via the primary and guest networks and via USB or Ethernet.**

  To use this method, go to the **Connected Devices** page and click the **Block** button next to the device.

- **Permanently block a device from connecting to your MiFi primary network only.**

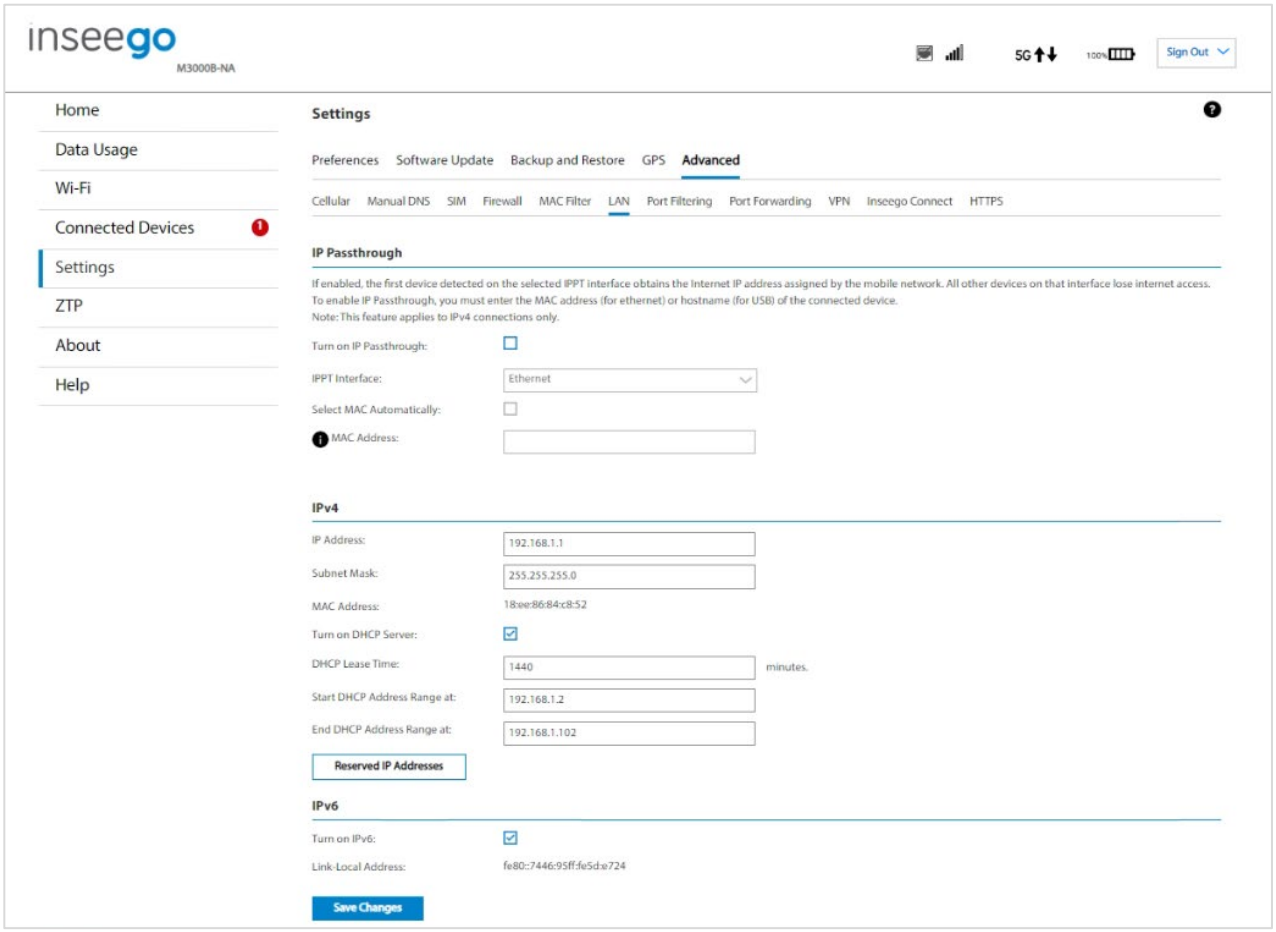
  Use the **MAC Filter**.

When blocking devices, the following information applies:

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

LAN tab

This tab provides settings and information about the MiFi local area network (LAN). The LAN consists of the MiFi and all Wi-Fi, USB, and Ethernet connected devices.



IP Passthrough

IP Passthrough (IPPT) enables the first device detected on the specified interface to obtain the IP address assigned by the mobile network. IPPT allows you to enable a one-to-one connection to a host routing system. **NOTE:** When IP Passthrough is on, 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:

- Port Forwarding
- Port Filtering
- DMZ (Firewall)

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

IPPT Interface: Select the interface used by the network device you wish to become the IP Passthrough device.
NOTE: The Ethernet port is disabled by default. You can enable it on **Settings > Preferences**.

Hostname: When enabling IPPT on the USB interface, enter the hostname of the device connected for IP Passthrough or click the **Select Hostname Automatically** checkbox[1].. 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 the Ethernet interface, enter the MAC address of the device connected for IP Passthrough or click the **Select MAC Automatically** checkbox[1]. This is the only Ethernet-connected device that can obtain the IP address assigned to the mobile network.

IPv4

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

Subnet Mask: The subnet mask network setting for the MiFi. 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 MiFi. 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 this box if any of your connected devices support 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.

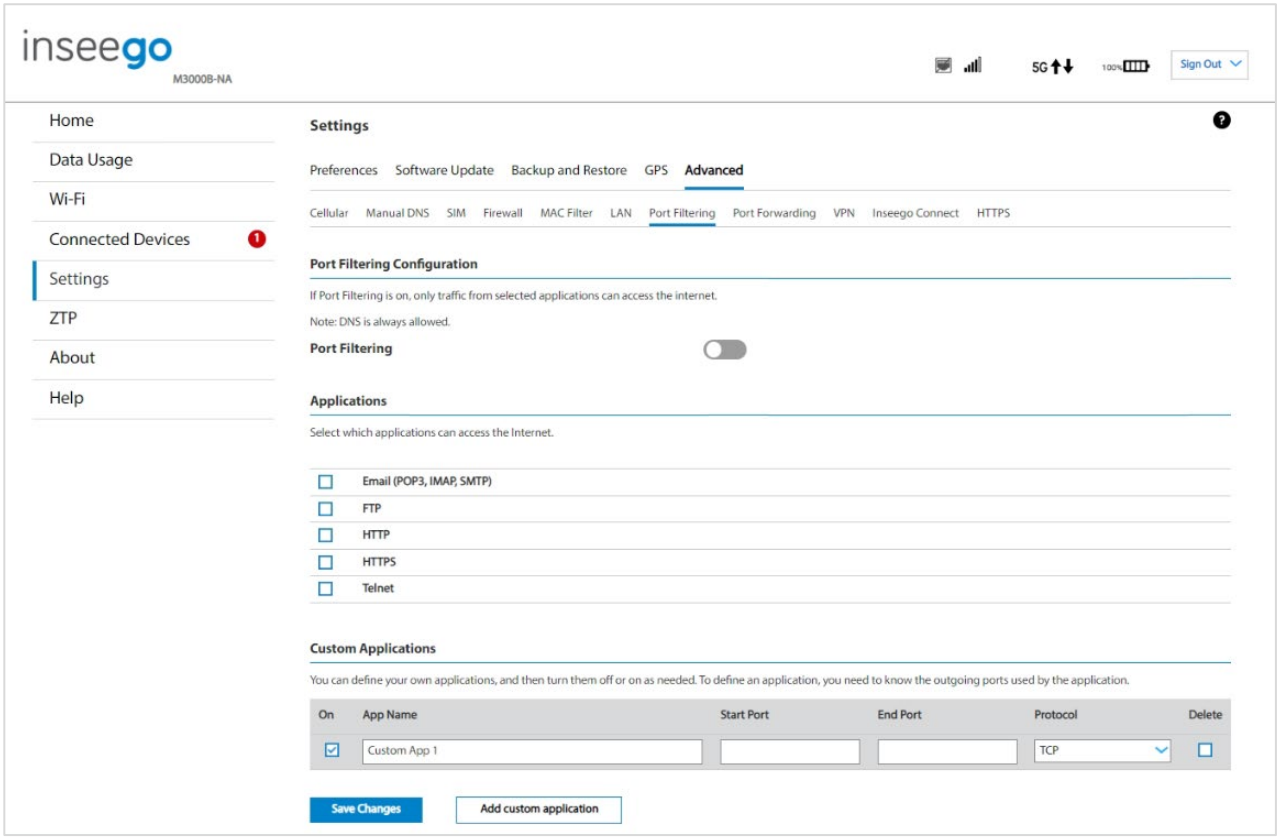
Click **Save Changes** to activate and save new settings.

[1] This option may not be available on some devices.

Port Filtering tab

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

NOTE: You can view whether port filtering is on or off in the Settings panel on the web UI Home page.



NOTE: When IP Passthrough is turned on, port filtering capabilities are set through the connected host routing system and settings on this page are not available.

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 and click **Save Changes**.

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

Application	Port	TCP[1]	STCP[1]	UDP[1]
Email				
POP3 **POP3S**	110 995	Yes Yes	No No	Assigned Yes
IMAP **IMAPS**	143 993	Yes Yes	No No	Assigned Assigned
SMTP **SecureSMTP**	25 465	Yes Yes	No No	Assigned No
FTP control (command) **FTP data transfer**	21 20	Yes Yes	Yes Yes	Assigned Assigned
HTTP	80	Yes	Yes	Assigned
HTTPS	443	Yes	Yes	Assigned
Telnet	23	Yes	No	Assigned

Custom Applications

You can define up to ten custom applications.

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

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

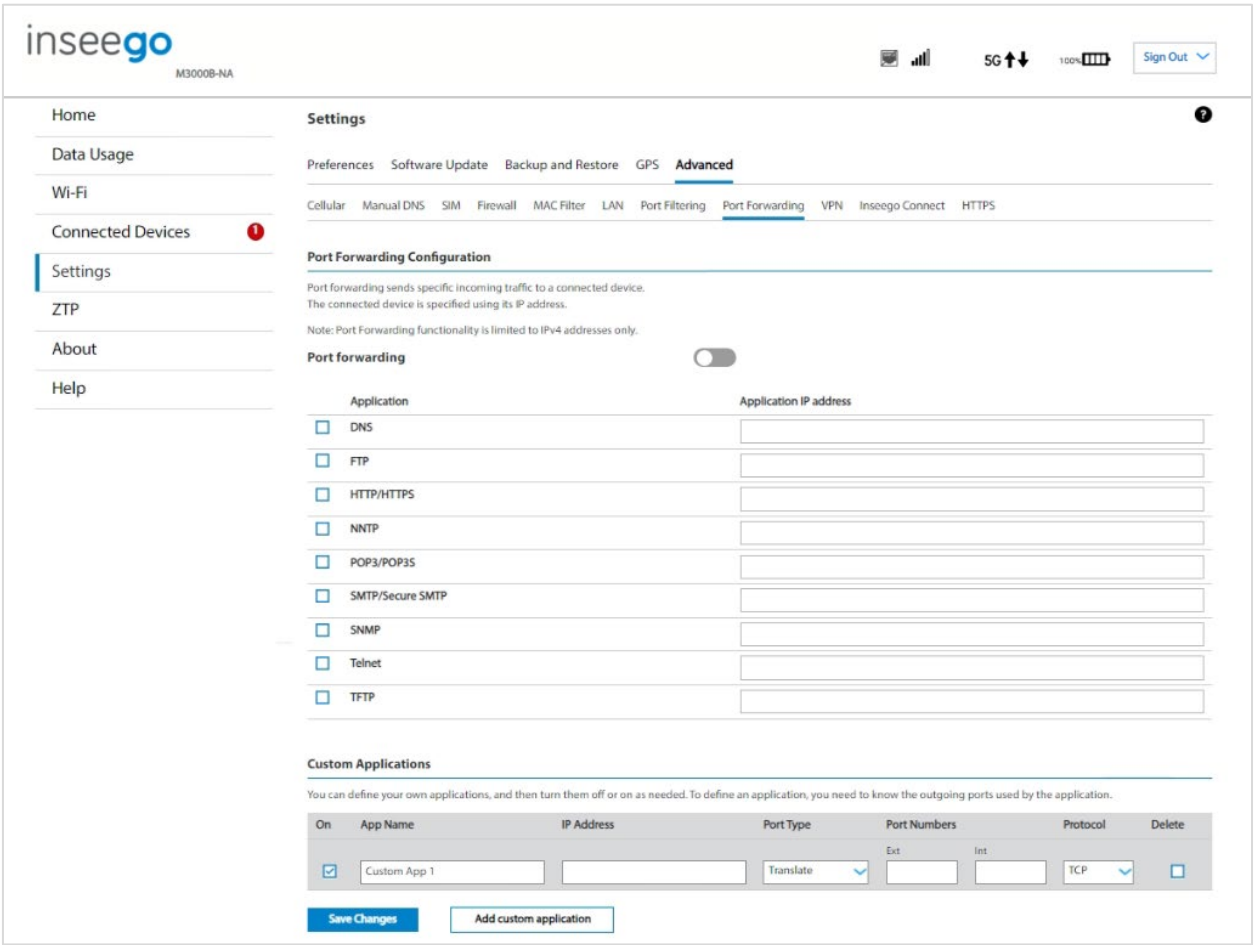
[1] **Yes** indicates the protocol is standardized for the port number.
No indicates the protocol is not standardized for the port number.
Assigned indicates the port number is assigned by IANA (Internet Assigned Numbers Authority) for protocol use but may not be standardized.

Port Forwarding tab

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

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

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



NOTE: When IP Passthrough is turned on, port forwarding capabilities are set through the connected host routing system and settings on this page are not available.

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.

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 for the application.

Click **Save Changes**.

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

Application	Port	TCP[1]	STCP[1]	UDP[1]
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

[1] **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

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

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

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

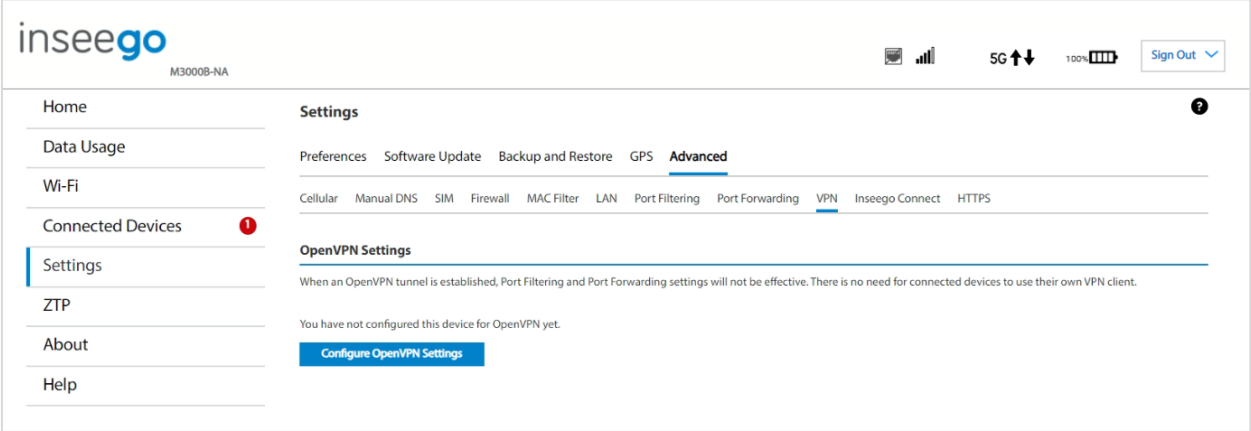
VPN

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

- VPN tab (OpenVPN) - Admin web UI
- IPSec VPN (Inseego Connect)[1]

VPN tab (OpenVPN)

Use this page to establish a tunnel connection to an OpenVPN server and route all traffic on connected devices through the tunnel.



OpenVPN Settings

This section is visible once you have configured your MiFi for OpenVPN using the **Configure OpenVPN Settings** button.

Connection status: The status of the VPN connection.

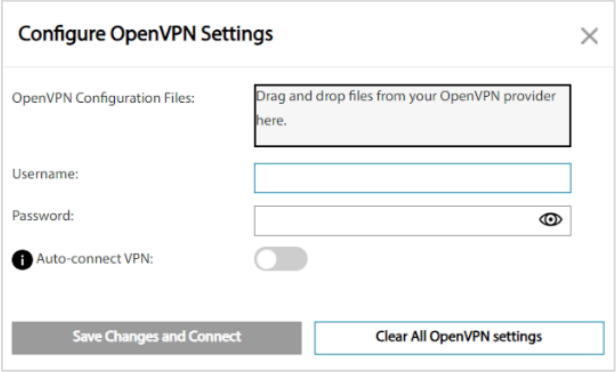
Connection time: The amount of time the VPN connection has been established.

Connect: Connects to the VPN server.

View log: Displays the VPN connection log.

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

[1] This option may not be available on some devices.



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.

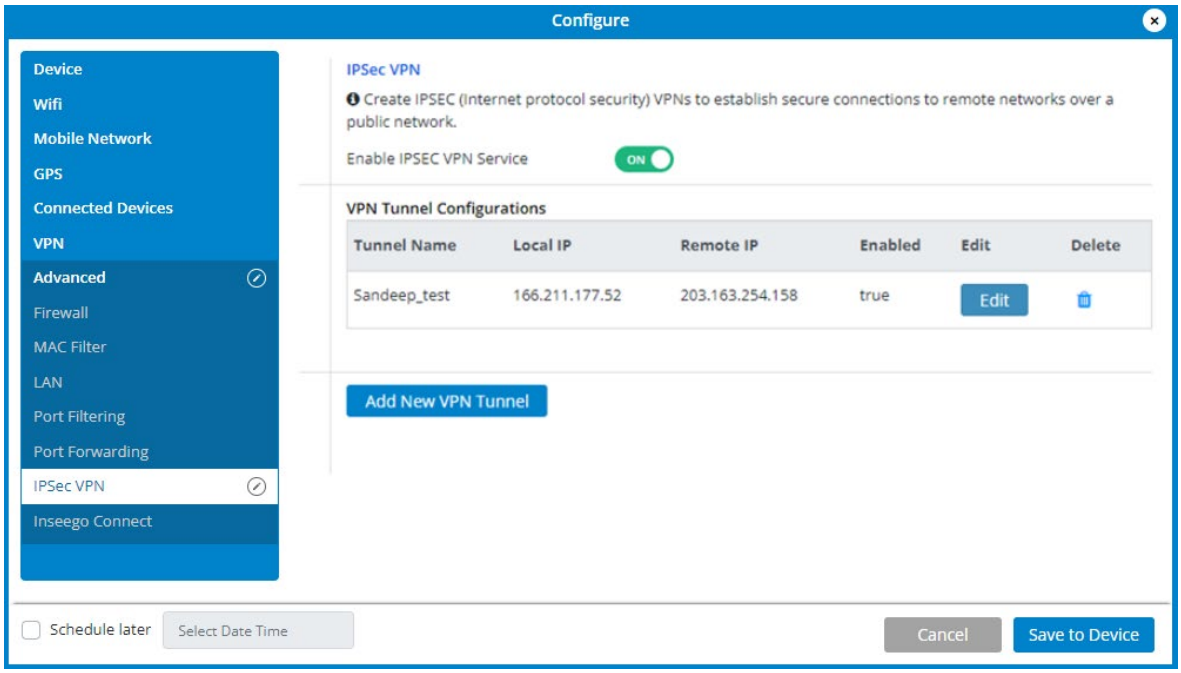
Auto-connect VPN: When the Auto-connect VPN on/off slider is on, the VPN tunnel will automatically be established whenever an internet connection is made. When off, the VPN connection must be established manually.

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

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

IPSec VPN (Inseego Connect)[1]

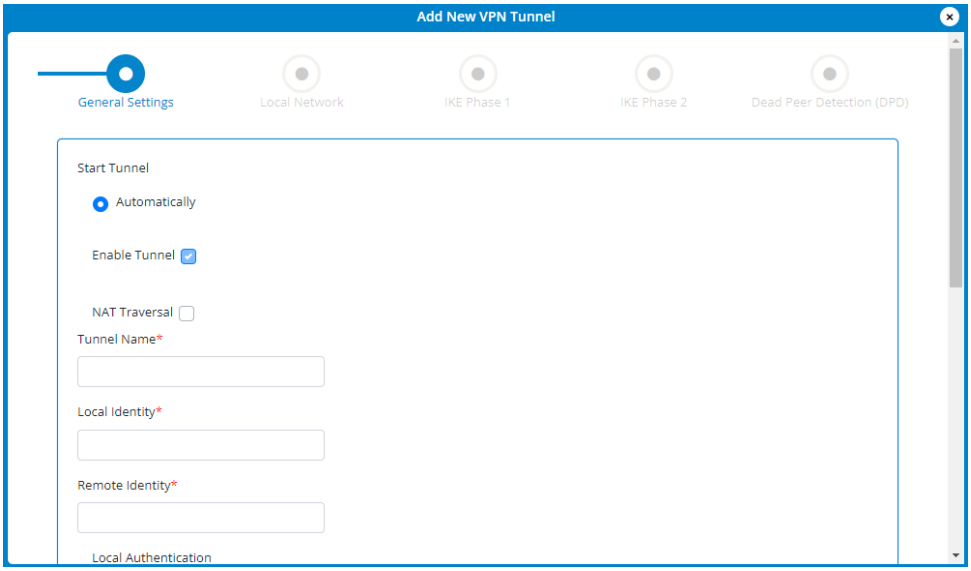
You can create IPSec VPNs using Inseego Connect. To learn more about the benefits of Inseego Connect, go to https://inseego.com/products/cloud-management/inseego-connect/. You can sign up for a free Inseego Connect account at connect.inseego.com.



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

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

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



[1] This option may not be available on some devices.

General Settings

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

Click **Next**.

Local Network

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

Remote Network

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

Click **Next**.

IKE Phase 1

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

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

Click **Next**.

IKE Phase 2

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

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

Click **Next**.

Dead Peer Detection (DPD)

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

Enable: Check this box to enable DPD.

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

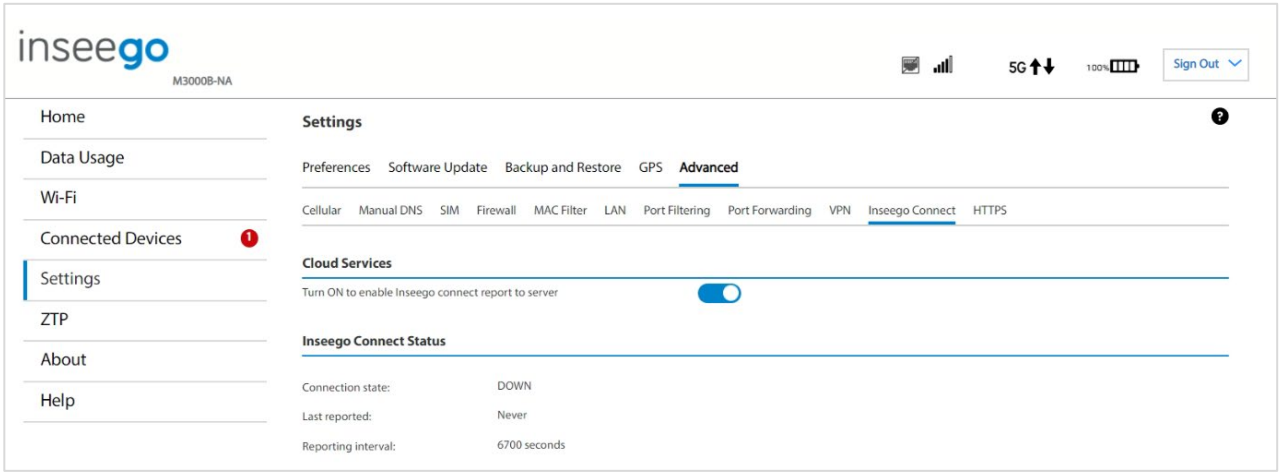
DPD Delay: The number of seconds between DPD packets.

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

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

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.com.



Cloud Services

Use the on/off slider to turn the connection to Inseego Connect on or off.

Inseego Connect Status

Connection state: The status of the Inseego Connect connection.

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

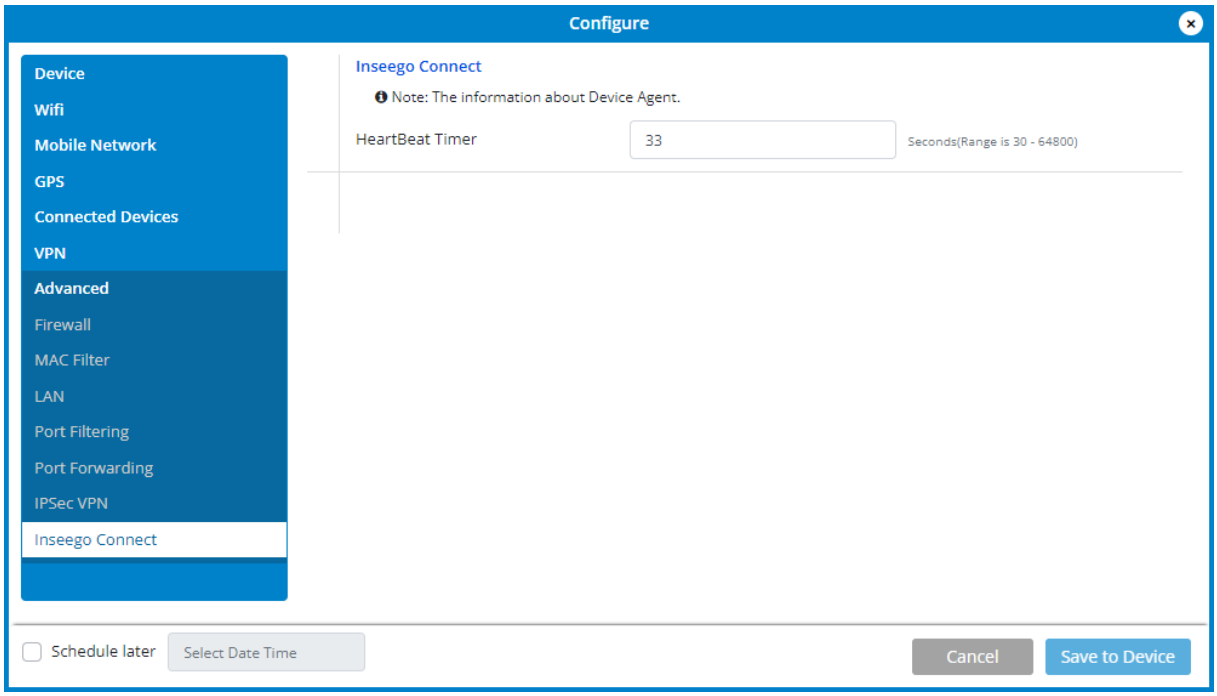
Last reported: The time when your MiFi last sent a packet to Inseego Connect servers.

Reporting interval: This is the interval at which your MiFi will send packets into the Inseego Connect server.
NOTE: A shorter interval means more data usage.

Heartbeat timer (Inseego Connect)

Your MiFi 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.com.



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

Click **Save to Device**.

5

Troubleshooting and support

Overview

Common problems and solutions

Technical support

Overview

The MiFi is a highly reliable product. Most problems are caused by one of these issues:

- System resources required by the MiFi are being used by other devices.
- Network coverage is unavailable due to coverage area, an account problem, or a network problem.

First troubleshooting steps

- Make sure you are using the MiFi in the correct geographic region.
- Ensure that your wireless coverage extends to your current location.
- Ensure you have an active data plan.
- For MiFi optimum radio performance, DO NOT place your MiFi on metal surfaces.

IMPORTANT: Before contacting Support, be sure to restart both your connected device and your MiFi and ensure that your SIM card is inserted correctly.

Common problems and solutions

The solutions in this section can help solve many common problems encountered while using the MiFi.

My MiFi powered off without pressing the Power button

This may occur under any of the following circumstances:

- Pressing the Reset button or Restore Factory Settings on the touchscreen or Admin web UI
- MiFi automatically restarting after configuration changes
- Switching profiles
- Restoring the configuration settings
- Battery depletion

To restore power, follow these steps:

1. Manually press and hold the MiFi Power button for three seconds to turn it back on.
2. If the battery is depleted, charge the MiFi with the wall charger.

No service is available

- Reorient your device. If you are inside a building or near a structure that may be blocking the signal, change the position or location of the device. For example, try moving your device close to a window.
- You are outside your coverage area, or there may be a problem with your account. Check with your network operator.

My MiFi has no power/touchscreen doesn't display when I press the Power button

- Make sure the battery is properly seated in the device.
- Check that the battery is fully charged.

I forgot my Wi-Fi password

Tap **Wi-Fi Name/Password** to see your Wi-Fi name (SSID) and Wi-Fi password.

I forgot my MiFi Admin web UI password

- Your initial MiFi Admin web UI password is the same as your Wi-Fi password. **NOTE:** If you reset your MiFi to factory settings, use the default password.
- If you have changed your Admin password, click the down arrow next to **Sign Out** in the top-right corner of any web UI page and click **Change Password,** then **Forgot Admin password?**. Answer the displayed security question. The current Admin password will be displayed. Alternately, you can view the Admin password on the MiFi touchscreen by tapping **Help > Admin Website** or **Menu > Settings > Advanced Settings**.

I cannot connect a device to my MiFi

On your MiFi: Make sure the Network Signal Strength indicator displays at least one bar and that the type of network is displayed on the Home screen (for example, 5G).

On the device you want to connect: Make sure Wi-Fi is turned on. The MiFi will broadcast its own wireless network and name. Open the list of available Wi-Fi networks. Select the MiFi primary or guest network and enter the password.

NOTE: You can find the primary network name and password by tapping **Wi-Fi Name/Password** on your MiFi – swipe left to see the guest network name and password.

Once connected to the internet, the MiFi Home screen displays the connected device.

I see other networks, but not the network name for my MiFi

The default multi-mode settings on your MiFi 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:

1. Access the MiFi Admin web UI. Tether your device to the MiFi with the USB-C cable. On the MiFi touchscreen, select **Access Internet (USB & Wi-Fi)** and click **OK**. Open any web browser and go to http://my.MIFI/ or http://192.168.1.1.
   NOTE: If you have another device that can connect to your MiFi, you can use it to access the Admin web UI.

2. 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.

3. Click **Save Changes**. Your MiFi will reboot, and the network name should be visible on all devices.

I see the network name, but cannot connect a device to my MiFi

Tap **Wi-Fi Name/Password** on the MiFi Home screen to make sure you are using the correct Wi-Fi password. Swipe left to view the guest network credentials if you are connecting to the guest network.

The default network security settings on your MiFi work for most Wi-Fi clients, however, some older devices may not have access. 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 MiFi Admin web UI by tethering the device to the MiFi with the USB-C cable. On the MiFi touchscreen, select **Access Internet (USB & Wi-Fi)** and click **OK**. Open any web browser and go to http://my.MIFI/ or http://192.168.1.1.
   NOTE: If you have another device that can connect to your MiFi, you can use it to access the Admin web UI.

2. Navigate to **Wi-Fi > Primary Network**. In the **Security** drop-down, select **WPA/WPA2 Mixed Mode**.

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

I want to see how many devices are connected

On the MiFi touchscreen: Look below the **Connected Devices** icon on the Home screen for the number of connected devices. Tap the icon for details on the connected devices.

On the MiFi Admin web UI: The **Connected Devices** panel on the Home page lists the number of connected devices to the right of **Connected Devices**. Click › in the bottom-right corner of the panel for details on connected devices.

I want to see the firmware (software) version installed on my MiFi

NOTE: Software updates are delivered to the MiFi automatically over the mobile network.

On the MiFi touchscreen: Tap **Menu** and then swipe up and tap **Software Update**.

On the MiFi Admin web UI: Click › in the bottom-right corner of the **Settings** panel and select the **Software Updates** tab.

I want to see the phone number for my MiFi

On the MiFi touchscreen: Tap **Menu** and then swipe up and tap **About**. Your MiFi phone number is listed as **Wireless Number**.

On the MiFi Admin web UI: Click › in the bottom-right corner of the **About** panel and select the **Diagnostics** tab. Your MiFi phone number is listed as **Mobile number (MDN)**.

I want to see the battery level of my MiFi

On the MiFi touchscreen: You can view the battery icon and percentage 100% on the top right of the Home screen.

On the MiFi Admin web UI: You can view the battery icon and percentage on the top right of the Home page.

I want to turn my MiFi off

Press and hold the Power button on the MiFi for three seconds until you see the Power Off screen. Then select **Shutdown** and tap **OK**.

I want to know if my MiFi is still on when the touchscreen is dark

- When the MiFi is on, the LED status light blinks slowly as a “sign of life.”

- You can press and release the Power button to wake up the touchscreen.

Technical support

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

Customer service and troubleshooting
Contact your service provider for assistance.

More information
Documentation for your MiFi is available online. Go to https://go.inseego.com/mifixpro. Or click **User Guide** on the Admin web UI Home page.

6

Product specifications and regulatory information

Product specifications

Regulatory information

Product Certifications and Supplier's Declarations of Conformity

Wireless communications

Limited warranty and liability

Safety hazards

Proper battery use and disposal

Product specifications

Device

Name:	MiFi X PRO 5G	
Model:	M3000A, M3000B, M3000B-NA, M3000D, M3100	
Regulatory:	M3000A	FCC, ISED
	M3000B	FCC
	M3000B-NA	FCC
	M3000D	FCC, ISED
	M3100	FCC
Certifications:	FIPS 140-2	
Location services:	GNSS: GPS/GLONASS/Galileo/Beidou	
Dimensions:	5.9" x 2.91" x 0.74" (150mm x 74mm x 18.9mm)	
Weight:	8.6 oz (245 g)	
Operating Temperature:	14° to 131°F (-10°C to 55°C)	
Ports:	USB-C Port – charging, tethering, charging of other external devices 1 Gbps RJ45 Ethernet port - tethering	
SIM:	4FF Nano SIM	
Display:	2.4" (60.96mm) IPS color touchscreen Power and status LED	

Environmental

Operating Temperature:	14° to 131°F (-10°C to 55°C)
Storage Temperature:	-22° to 158°F (-30° C to 70° C)
Battery Charging Temperature:	32° to 104°F (0° C to 40° C)
Relative Humidity:	The device shall be fully operational up to a maximum of 93% relative humidity (non-condensing).
Drop:	The device accessories (battery and charger) shall withstand drop from 1.5m onto hard surface (stone, concrete, metal) without mechanical, electrical, or functional damage, except for slight scratches or mars. The housing will withstand drop from 1.25m onto hard surface stone, concrete, metal) without mechanical, electrical, or functional damage, except for slight scratches or mars.
Electrostatic Discharge:	The device shall be able to withstand the following ESD: 8kV contact / 15kV air discharge.
Vibration Stability:	The device shall be able to withstand the following vibration profile: 10-2000Hz, 1.5G acceleration, 3 axes.

Power

Charging:	18W Qualcomm Quick Charge 3.0 charger USB 3.1 Gen 1, type A to C cable
Time for Full Charge:	3 hours (when not in use)
Battery:	5050 mAh Li-Ion battery (Included)
Battery Life:	All day

Wi-Fi

Wi-Fi 6: 802.11 a/b/g/n/ac/ax (2.4GHz/5.0GHz)
2x2 SU-MIMO
Real simultaneous dual-band Wi-Fi
Primary and guest Wi-Fi networks
Connect up to 32 Wi-Fi enabled devices

Software

Systems supported:	Windows® 10 or higher Mac OS® X 10.10 or higher Linux® Ubuntu 14.04 or higher Chrome OS™ v79 or higher
Security:	Administration portal Security hardened web interface Password hash Session timeout Incorrect password lockout 3rd party penetration testing Anti-CSRF
Wi-Fi features:	Wi-Fi on/off control Wi-Fi security (WPA/WPA2/WPA3) Wi-Fi protected setup (WPS 2.0) Wi-Fi privacy separation AES encryption
Advanced networking:	MAC address filtering NAT firewall Port forwarding Port filtering VPN passthrough OpenVPN support DMZ Manual DNS IP Passthrough Static IP

Connectivity, approvals, bands, chipset, and languages by SKU

SKU	Approval	Connectivity[1]	Bands	Chipset	Language
649496 02661 5	Bell Canada	- 5G sub-6 GHz - NSA, SA, NR-CA, DSS supported - 4x4 MIMO sub-6 GHz - LTE Cat 20 - 4X4 MIMO LTE - 3G HSPA+/UMTS	**5G sub-6:** n1, n2, n3, n5, n7, n12, n20, n25, n38, n40, n41, n48, n66, n70, n71, n77, n78 **LTE:** B1, B2, B3, B4, B5, B7, B12, B13, B20, B25, B26, B30, B38, B41B48, B66, B71 **3G HSPA+/UMTS:** 1, 2, 4, 5, 8	Qualcomm SDX65	English French
649496 02743 8	Cellcom	- 5G sub-6 GHz - NSA, SA, NR-CA, DSS supported - 4x4 MIMO sub-6 GHz - LTE Cat 20 - 4X4 MIMO LTE - 3G HSPA+/UMTS	**5G sub-6:** n1, n2, n3, n5, n7, n12, n20, n25, n38, n40, n41, n48, n66, n70, n71, n77, n78 **LTE:** B1, B2, B3, B4, B5, B7, B12, B13, B20, B25, B26, B30, B38, B41B48, B66, B71 **3G HSPA+/UMTS:** 1, 2, 4, 5, 8	Qualcomm SDX65	English Spanish
649496 02752 0	North America Multi-carrier Inseego Ignite[2] - AT&T - T-Mobile - Verizon	- 5G sub-6 GHz - NSA, SA, NR-CA, DSS supported - SRS antenna switching - 4x4 MIMO sub-6 GHz - LTE Cat 20 - 4X4 MIMO LTE - 3G HSPA+/UMTS	**5G sub-6:** n2, n5, n7, n12, n25, n30, n41, n48, n66, n71, n77 **LTE:** B2, B4, B5, B7, B12, B13, B17, B25, B26, B30, B41, B46, B48, B66, B71 **3G HSPA+/UMTS:** 1, 2, 4, 5, 8	Qualcomm SDX62	English Spanish
649496 02739 1	Rogers	- 5G sub-6 GHz - NSA, SA, NR-CA DSS supported - 4x4 MIMO sub-6 GHz - LTE Cat 20 - 4X4 MIMO LTE - 3G HSPA+/UMTS	**5G sub-6:** n1, n2, n3, n5, n7, n12, n20, n25, n38, n40, n41, n48, n66, n70, n71, n77, n78 **LTE:** B1, B2, B3, B4, B5, B7, B12, B13, B20, B25, B26, B30, B38, B41B48, B66, B71 **3G HSPA+/UMTS:** 1, 2, 4, 5, 8	Qualcomm SDX65	English French
649496 02688 2 649496 02746 9	T-Mobile® Inseego Ignite[2] (T-Mobile)	- 5G sub-6 GHz - NSA, SA, NR-CA, DSS supported - SRS Antenna switching - 4x4 MIMO sub-6 GHz - LTE Cat 20 - 4X4 MIMO LTE - 3G HSPA+/UMTS	**5G sub-6:** n1, n2, n3, n5, n7, n20, n25, n28, n40, n41, n48, n66, n71, n77, n78 **LTE:** B1, B2, B3, B4, B5, B7, B8, B12, B13, B20, B25, B26, B28, B38, B39, B, 40, B41, B46, B48, B66, B71 **3G HSPA+/UMTS:** 1, 2, 4, 5, 8	Qualcomm SDX62	English Spanish
649496 02650 9 649496 02745 2	Verizon Inseego Ignite[2] (Verizon)	- 5G mmW - 2X2 MIMO mmW - 5G sub-6 GHz - 4x4 MIMO sub-6 GHz - LTE Cat 20 - 4X4 MIMO LTE - 3G HSPA+/UMTS	**5G mmW:** n257, n260, n261 **5G sub-6:** n2, n5, n48, n66, n77, n78 **LTE Cat 20:** B1, B2, B3, B4, B5, B7, B12, B13, B17, B20, B28, B46, B48, B66 **3G HSPA+/UMTS:** 1, 2, 4, 5, 8	Qualcomm SDX65	English Spanish

[1] Data plan required. Actual results may vary. Coverage and data speeds subject to network availability.
[2] Go to https://inseego.com/company/partners/.

Warranty and services

Industry leading warranty
Inseego Care Support and Advanced Replacement options available
MiFi provisioning available to apply custom templates and verify device activation prior to shipment

Regulatory information

Federal Communications Commission Notice (FCC – United States)

FCC ID: PKRISGM3000A
FCC ID: PKRISGM3000B
FCC ID: PKRISGM3000D
FCC ID: PKRISGM3100

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.

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

IC: 3229A-M3000A
IC: 3229A-M3000D

ISED RSS-Gen Notice

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

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

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

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

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Les dispositifs fonctionnant dans la bande de 5 150 à 5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

ISED Canada ICES-003 Compliance

CAN ICES-3 (B)/NMB-3(B)

FCC and ISED RF Exposure Guidance Statement

In order to comply with FCC RF Exposure requirements, this device must be installed to provide at least 10 mm separation from the human body at all times.

Afin de se conformer aux exigences d'exposition RF FCC / ISED, cet appareil doit être installé pour fournir au moins 10 mm de séparation du corps humain en tout temps.

Product Certifications and Supplier's Declarations of Conformity

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

Wireless communications

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

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

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

Inseego Corp. or its partners will not be held responsible for damages of any kind resulting from the delays or errors in data transmitted or received with the M3000 device, or failure of the M3000 device to transmit or receive such data.

Limited warranty and liability

Inseego Corp. warrants for the 12-month period immediately following receipt of the Product by Purchaser that the Product will be free from defects in material and workmanship under normal use. 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's option, of defective or non-conforming materials, parts or components. 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'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's specifications or authorized by Inseego, (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, (VII) products designated by Inseego 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.

Safety hazards

Do not operate the 5G MiFi X PRO 5G 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.

S-23841

Proper battery use and disposal

IMPORTANT: In the event of a battery leak:

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

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

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

7

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.
- **Hotspot** — A Wi-Fi (802.11) access point or the area covered by an access point. Used for connecting to the internet.
- **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.
- **MNO** — Mobile 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.
- **MSID** — Mobile Station IDentifier. A number for a mobile phone that identifies that phone to the network.
- **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.

- **NMEA port** — National Marine Electronics Association port. The port through which applications can access a GPS data stream.
- **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.
- **PRL** — Preferred Roaming List. A list that your wireless phone or device uses to determine which networks to connect with when you are roaming (Network operator specific).
- **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 measure of the ratio between signal strength and noise level. SNR values are positive, 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.
- **USB**—Universal Serial Bus. A connection type for computing device peripherals such as a printer, mobile modem, etc.
- **USB Port Types**—USB ports on computers and hubs have a rectangular Type A port, and peripheral devices have a cable with a Type A connector. Peripheral devices that do not have an attached cable typically have a Type C port on the device and a separate Type A to C cable. Type B connectors have been replaced by Type C. Mini-USB connectors have largely been superseded by Micro-USB, but are still used with some cameras, music players, etc. Micro-USB connectors are used with portable devices, such as phones and battery packs, although USB-C is being adopted by most manufacturers.
- **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.