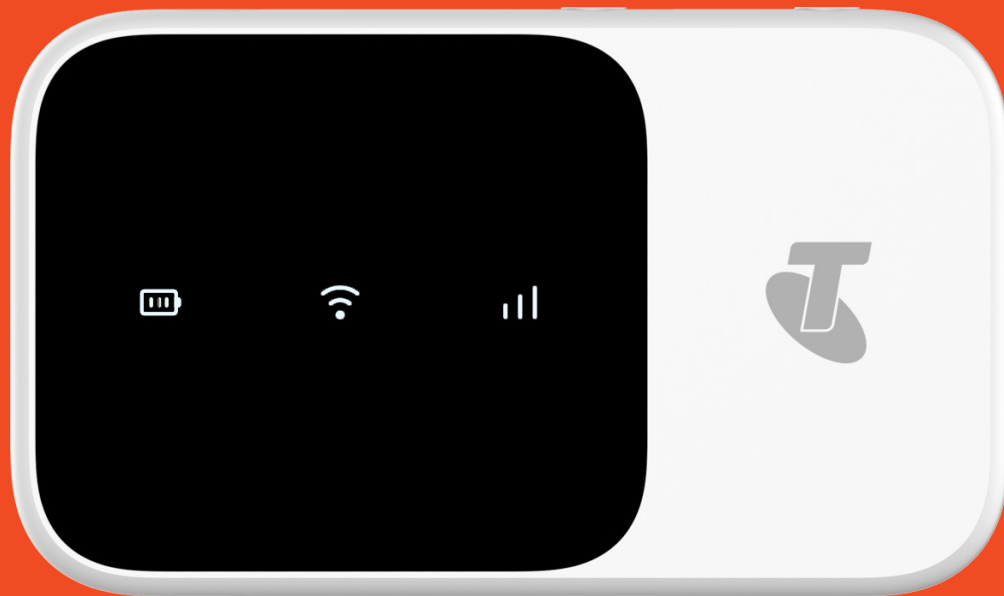




Telstra 4GX Wi-Fi Plus 2

User Manual

Software updates

We recommend that you have the latest software update installed on your hotspot - this will ensure that you have the latest features, most stable and secure experience while using this device.

Refer to section [Settings > Device settings > Software Update](#) (page 17) for additional information.

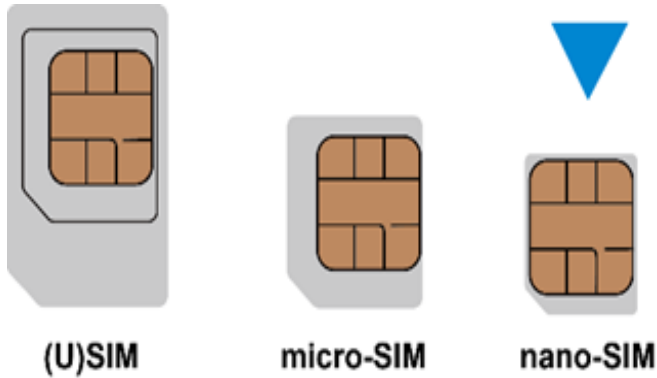
Device Overview



Setting up the Device

Step 1: SIM Type

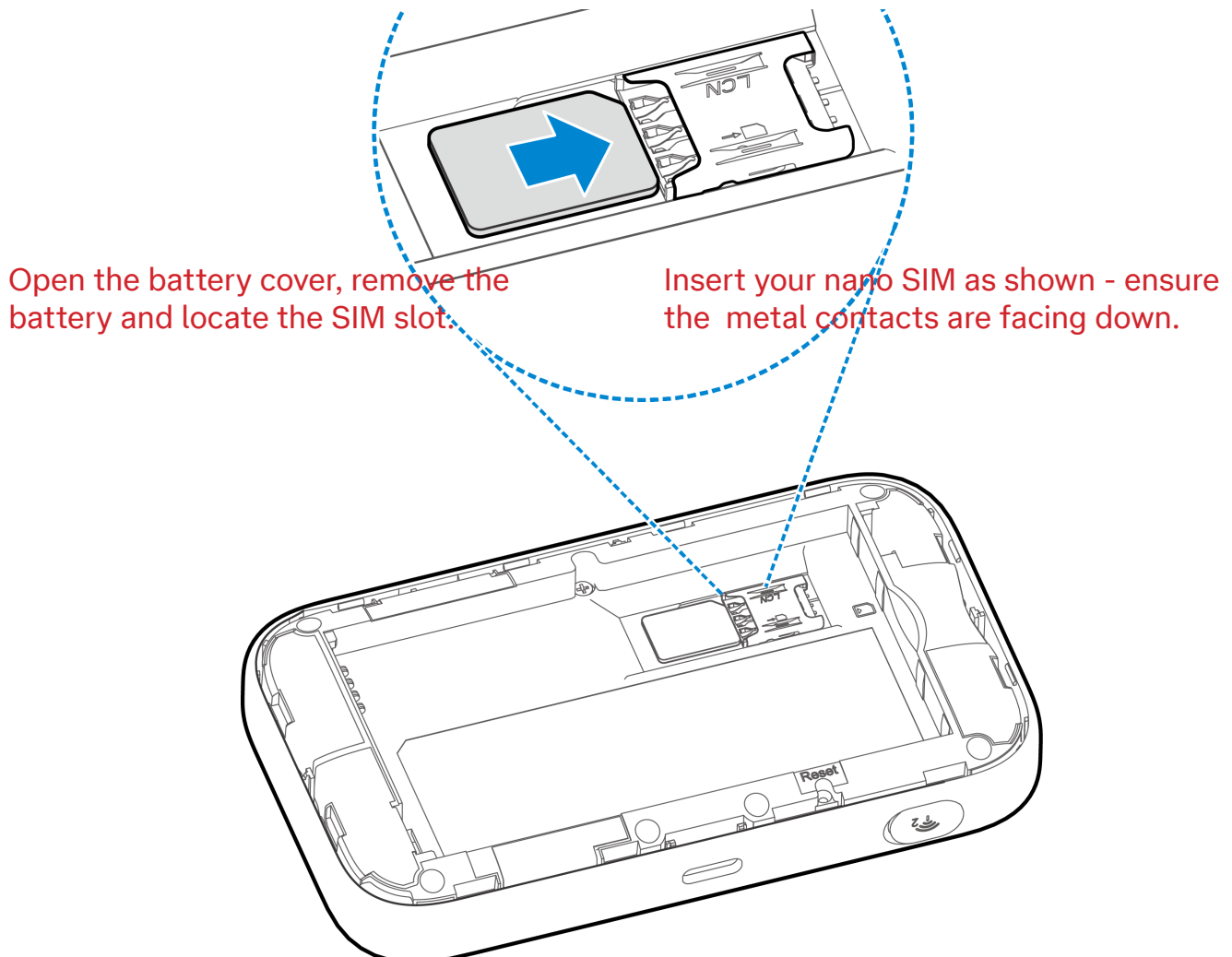
Make sure you are using a Telstra **nano-SIM** card:



Step 2: Activate SIM

If your SIM is not yet active visit telstra.com/activate
Follow the prompts to activate your SIM.

Step 3: Insert your SIM card



Connecting to Your PC

Connect the modem to your computer's USB port or connect using Wi-Fi. The operating system automatically detects and identifies your modem and creates a new connection.

Connect using Wi-Fi

With reference to the sticker on the back of your 5G Wi-Fi, search for the Wi-Fi network name then enter the Wi-Fi password.

Access the Internet

After the modem is connected to your computer successfully you can now access the Internet.

Check the modem homepage to make any configuration changes.

When you connect via USB it automatically will open your default web browser at the modem's configuration homepage.

You can make any changes to the settings through this homepage.

You can access this configuration homepage by entering either **m.home** or **192.168.0.1** in the web browsers address bar.

International Roaming

- The Roaming icon indicates you are connected to a foreign network.
- If Roaming is enabled on your data plan then roaming data charges will apply when connected via a roaming network.
- Contact Telstra to discuss your data charges and roaming options.

Software Installation / Uninstall

Windows users :

The modem will auto install and launch your browser when the USB is plugged in. To Uninstall go to: Start > All Programs > TELSTRA 5G Wi-Fi > Uninstall

MAC users :

Depending on your Mac OS, this device may work without installing any additional software. Driver Software is provided on the modem. To install, simply trigger the

contained Telstra 5G Wi-Fi app and follow the presented prompts

If required to uninstall the driver, navigate to System > Applications and run Uninstall TELSTRA 5G Wi-Fi app (you will be prompted to remove the USB if connected)

Important Note :

If your MAC device switches to sleep mode, the modem may no longer be recognised by your mac, simply remove and re-insert the modem to restore the device connection.

For any further trouble shooting tips - refer to the rear of this manual.

Built-in Web Interface

Connect the modem to any device via a vacant USB-A port and open your default web browser.

Enter **m.home** or **192.168.0.1** in the browser address bar to the device homepage.

- The home page shows a brief summary of the device status and your remaining data from Telstra.
- Software update notifications (if applicable) will be shown on this page
- The home page password is unique to each device and is printed on the label on the back of your modem. Use the device Password to log in.

Using the External Antenna ports

Your modem has 2 external TS9 antenna connectors.

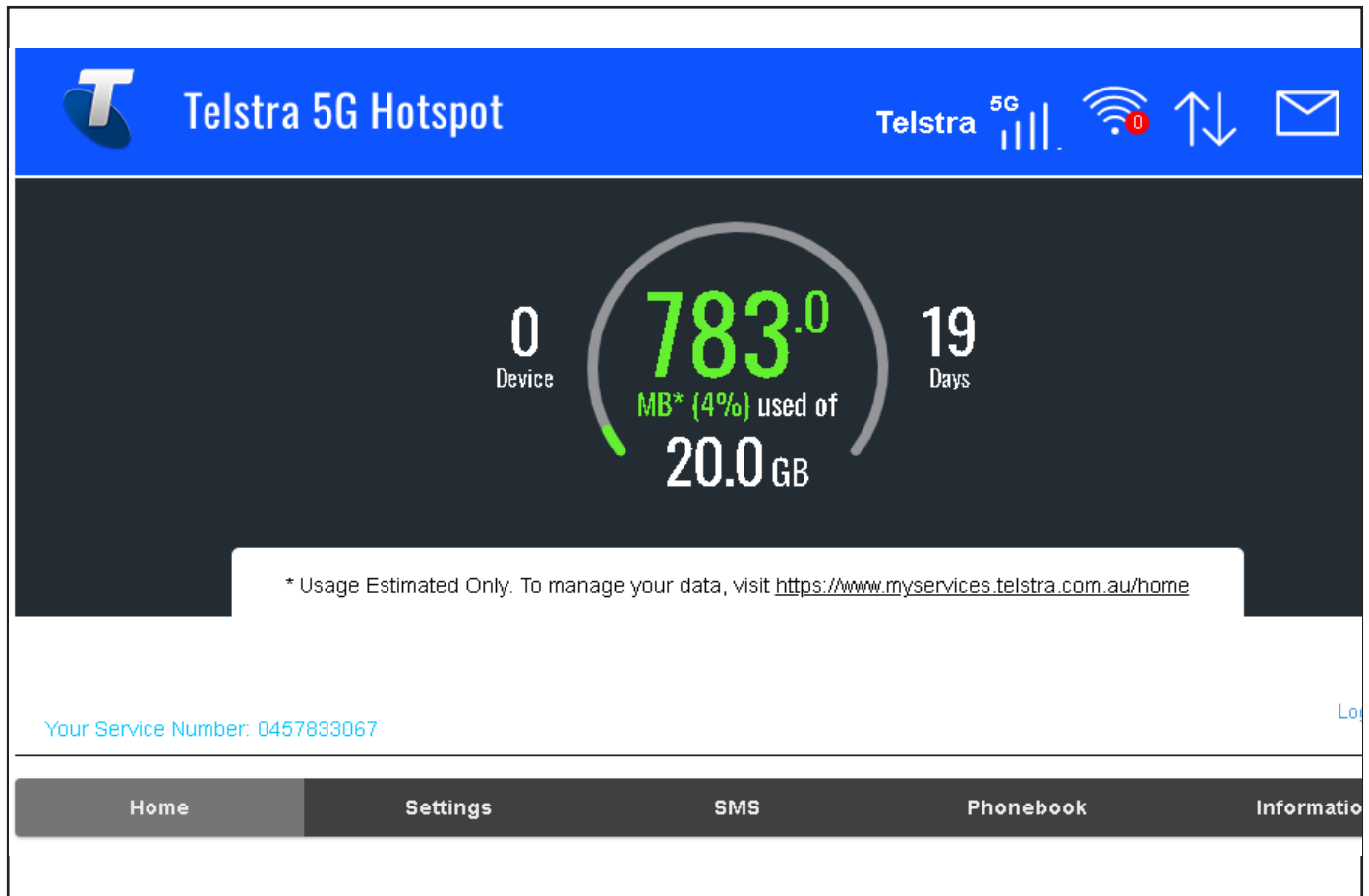
Using an external antenna will improve your device coverage and data rates. The antennas are for the Telstra network connection only and do not affect the device Wi-Fi performance.

- Antenna port 1 is used for 4G bands B7, B38, B40, B41, B42, B43
- Antenna port 2 is used for 4G Bands B1, B2, B3, B4, B5, B8, B20, B26, B28

Always insert the antenna leads with care. The connector is very small and delicate and can be easily damaged by rough treatment or harsh pulling or bending on the connector.

Screens Overview

Lock-screen



Overview :

On the initial loading of the WEB GUI, you will be presented the login screen.

The factory set default password is printed on the label on the back of your modem (Caps sensitive). To increase security, we highly recommend changing this default set password.

Instructions :

To change the default set password:

- > Navigate to Settings > Device Settings > Password Settings
- > Enter the current password from the back of your device
- > Enter your new password, confirm and press Apply

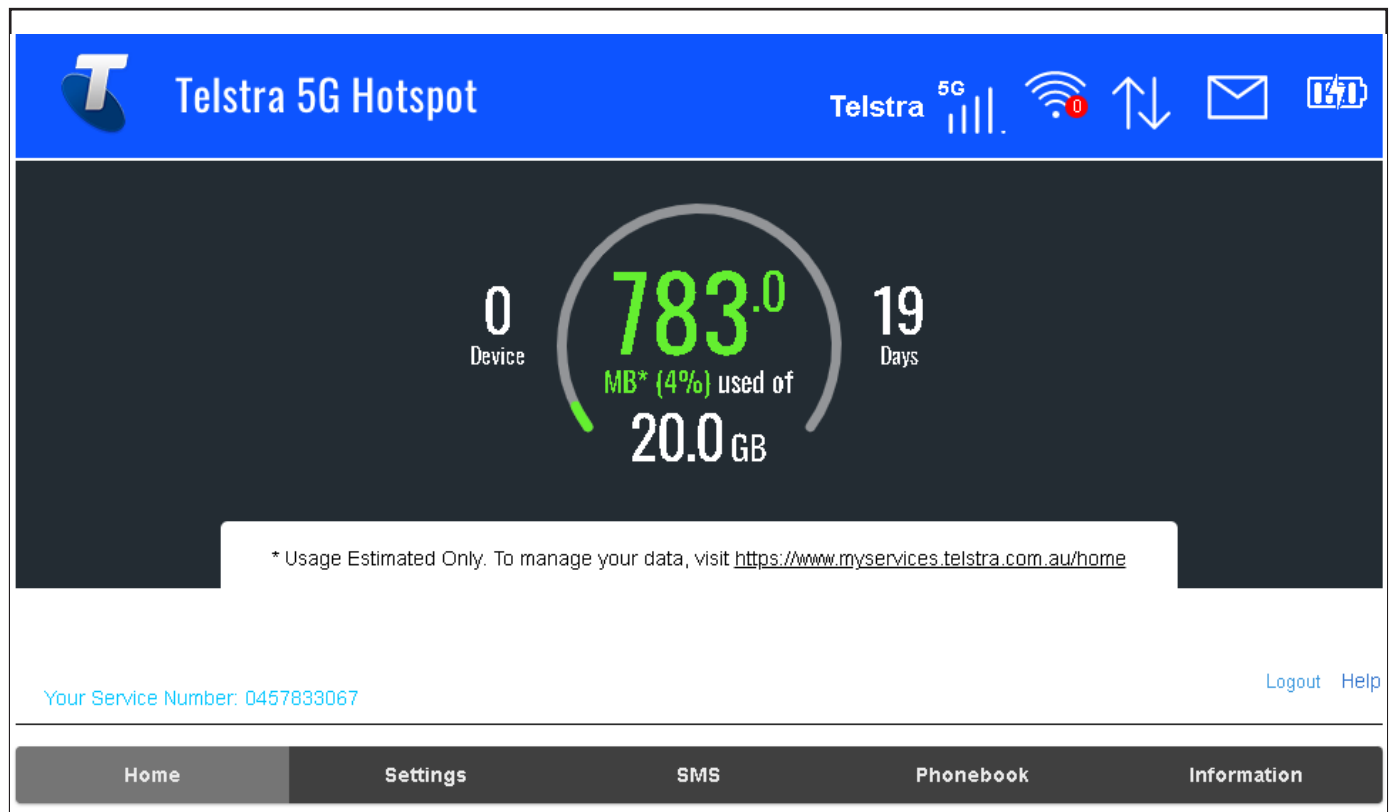
TIP: The device password is set under Device Settings. The Wi-Fi password is set under Wi-Fi Settings

Important Note :

To reset your modem settings and /or password at any stage, navigate to Device Settings > Reset and follow the set prompts or press the Reset button located under the battery cover.

After reset the password will be restored to the factory default password printed on the back of your device.

Home Tab



Overview :

The Home page is the default landing page that presents a quick summary of your devices network connection status, data usage summary, received SMS messages, service number and site navigation.

This device will automatically connect to the Telstra 5G or 4G network.
(Some device settings can only be changed when the device is disconnected from the network).

Instructions : To change to manual connection

Disconnect or Connect your devices mobile connection:

- > Click on Connect or Disconnect
- > The Device & connection status (Disconnect, 4G Connected or 5G Connected) will update on this page to its current state.

Quick access to change your SIM PIN page:

- > Navigate to Settings > Home
- > Under the PIN status, select the Change option.
- > You will be redirected to the USIM PIN Management (See USIM PIN Management for further instructions).

Important :

Changing the SIM PIN should be carried out with caution. When choosing a new SIM PIN, it is **recommended to use** a unique combination of numbers that is not easily guessable or shared with others.

Settings > Quick Setup (wizard)

The screenshot shows the 'Quick Setup' wizard in the Settings app. The top navigation bar includes 'Home', 'Settings', 'SMS', 'Phonebook', and 'Information'. The left sidebar lists various settings: 'Quick Setup' (selected), 'Network Settings', 'Wi-Fi Settings', 'Device Settings', 'Firewall', 'Router Settings', 'DDNS', 'NFC', and 'Power Save'. The main content area is titled 'Quick Setup' and shows a progress bar with five steps: '1. Password Settings', '2', '3', '4', and '5'. A 'Next' button is visible. Below the progress bar, a message states: 'This setup wizard will let you configure the device settings. Click Next to continue.' The section is titled 'Password Settings' and contains three input fields: 'Current Password *', 'New Password *', and 'Confirm New Password *'. Below these fields is a 'Password Strength' indicator with three options: 'Low', 'Middle', and 'High'. A blue question mark icon is located at the bottom left of the main content area.

Overview :

The Quick Settings page allows you to configure your device in 5 simple steps to quickly setup your device to your preference.

Instructions :

Accessing the Quick Settings Wizard for setting up your device:

- > Navigate to Settings > Quick Settings
- > Click Next to proceed to the PPP Profile Configuration
- > Click Next to proceed to the PPP Authentication
- > Click Next to proceed to configure Automatic Update preference.
- > Select Disable if you wish Click Next to proceed to the Summary page
- > Click Finish

Advanced Settings

Settings > Network Settings > WAN Connection Mode

Home

Settings

SMS

Phonebook

Information

Quick Setup

Network Settings

> WAN Connection Mode

> Network Selection

> APN

Wi-Fi Settings

Device Settings

Firewall

Router Settings

DDNS

NFC

Power Save

WAN Connection Mode

WAN Connection Mode ☒ Automatic

☐ Check here to connect to the internet while roaming.
Note: Telstra customers travelling outside Australia may incur additional data charges whilst roaming.

☐ Manual

Disconnect

Apply

The setting can only be changed when the modem is disconnected.

?

- To change current setting, please disconnect from network.
- Automatic: The device will automatically connect to network when it is powered on.
- Manual: The device will connect to network manually.

Overview :

Your device has been configured to be Plug and Play, so it will automatically connect to the mobile network once it is switched on. You may prefer to change the WAN Connection Mode so the device will only connect to the mobile network once you have accessed the Homepage and clicked to connect.

Instructions :

To change WAN connection mode or enable International Roaming:

- > Click the Disconnect button to change the WAN Connection Mode, select Manual or Automatic.
- > Click on the check box to enable International Roaming.
- > If you make any changes, Select Apply to save the changes.

Important :

The device will need to be Disconnected if you wish to make any modifications in the WAN Connection Mode page.

Click on the Help icon to get context tips.

Settings > Network Settings > Network selection

Overview :

Network Selection provides the option to select the preferred network technology type for your device to connect to. This device can connect to 5G, 4G or 3G technology.

Instructions :

To modify the network selection:

- > Navigate to Settings > Network Settings > Network Selection
- > Select Disconnect to modify the Network Selection.
- > Select the Manual or Automatic option.
- > Press Search to see available networks
- > If you choose an alternate network operator you will need to set the APN

Important :

The device will need to be Disconnected if you wish to make any modifications in the Network Selection page.

Click on the Help icon to get context tips.

Settings > Network Settings > APN

Home	Settings	SMS	Phonebook	Information
Quick Setup	APN			
Network Settings				
> WAN Connection Mode				
> Network Selection				
> APN				
Wi-Fi Settings				
Device Settings				
Firewall				
Router Settings				
DDNS				
NFC				
Power Save				

Current APN: Telstra Internet

Profile:

IP Type:

IP Type for Roaming:

Profile Name *:

APN *:

DNS Mode: ☒ Auto ☐ Manual

Authentication:

User Name:

Password:

Overview :

The APN settings allows users to configure the Access Point Name (APN) for the device to connect to the internet on the mobile network.

Instructions :

Adding a new APN:

- > Navigate to Settings > Network Settings > APN
- > Select Disconnect first
- > Click on the Add New button.
- > Enter in the Profile name, APN and modify other settings as appropriate.
- > Click on the Save button to confirm the new profile.

Selecting the newly created APN:

- > Navigate to Settings > Network Settings > APN
- > Click on the Disconnect button
- > Select the preferred APN Profile from the drop-down menu.
- > Click on Connect (You may want to set it as default by clicking the Set as Default button).

Deleting an APN:

- > Navigate to Settings > Network Settings > APN
- > Select an APN that you created.
- > Click on Delete
- > Click on Yes to confirm the changes.

Settings > Wi-Fi Settings > MAIN SSID

Home

Settings

SMS

Phonebook

Information

Quick Setup

Network Settings

Wi-Fi Settings

> Main SSID

> Guest SSID

> Advanced Settings

> WPS

Device Settings

Firewall

Router Settings

DDNS

Power Save

Wi-Fi Settings

Wi-Fi ☒ 2.4GHz Only ☐ 5.0GHz Only ☐ OFF

Apply

2.4GHz Basic Settings

Wi-Fi Name (SSID) *

TPW4G_7A4212

☒ Broadcast SSID

Security Mode

WPA2 (AES)-PSK

Wi-Fi Password *

.....

☐ Display Password

Max Station Number

32

Overview :

The Main SSID setting allows you to set the name and functionality for the primary Wi-Fi network. You can select 2.4GHz or 5GHz Wi-Fi or switch off Wi-Fi. You can rename the network to be more personal. All your common devices will connect to the Main SSID so make sure you keep your network secure with a password.

Instructions :

- Configure your home Wi-Fi network
- > Navigate to Settings > Wi-Fi Settings > Main SSID
 - > Select 2.4 or 5 as your main Wi-Fi frequency. (5Ghz is faster but only supports newer devices. For older devices you might have to set 2.4GHz)
 - > Change the Wi-Fi name if required. This your Wi-Fi network name which would normally be broadcast so your devices can ‘see’ it. If you prefer to hide your network then unselect Broadcast SSID.
 - > Most devices support WPA2 so it is preferred to leave this setting in place.
 - > You can check, change and display your Wi-Fi network password. This is the password that is entered into each device that you wish to connect.

Settings > Wi-Fi Settings > Guest SSID

Home	Settings	SMS	Phonebook	Information
Quick Setup	Multi SSID Switch ☒ Enable ☐ Disable			
Network Settings	☐ Allow the clients with guest SSID access to the Web UI			
Wi-Fi Settings	Time Limits For Network Access Free			
> Main SSID	Apply			
> Guest SSID				
> Advanced Settings				
> WPS				
Device Settings				
Firewall				
Router Settings				
DDNS				
Power Save				

2.4GHz Guest SSID

Wi-Fi Name (SSID) *	TPW4G_7A4212_Guest
	☒ Broadcast SSID
Security Mode	WPA2 (AES)-PSK
Wi-Fi Password *	
	☐ Display Password
Max Station Number	16
Number Of Users:	0

Overview :

The Guest SSID setting allows you to create a separate network with the ability to set restrictions.

Instructions :

Enable your guest Wi-Fi network

- > Navigate to Settings > Wi-Fi Settings > Guest SSID
- > Select the Enable button.
- > Allow or deny access to the web User Interface (UI).
- > Limit the time your guest can connect to the network.
- > Check, change and display your Guest Wi-Fi network password. This is the password that allows users to connect to the Guest network.

Settings > Wi-Fi Settings > Advanced Settings

These settings are for advanced users. Wi-Fi networks work on different channels and if your network is slow or subject to interference or drop outs you can manually select alternate channels.

Settings > Wi-Fi Settings > WPS

Overview :

WPS (Wi-Fi Protected Setup) allows you to quickly connect devices without having to enter the Wi-Fi password. You can choose a PIN code or PBC (Push Button Configuration) to connect other devices to your network.

Instructions :

- > Navigate to Settings > Wi-Fi Settings > WPS
- > Select your main or guest network
- > Select PIN or PBC
- > Enter a PIN code to be used by the other devices or
- > Press the WPS button on the side of the modem to turn on WPS.
- > The wi-fi LED will flash for 2 minutes while you can connect other devices.

To connect other devices using WPS-PBC they need to have a WPS function key otherwise use PIN and enter the same PIN on the connecting device.

Settings > Device settings > Password Settings

Overview :

Device Settings > Password sets the password for the web login.

Instructions :

Navigate to Settings > Device Settings > Password Settings

- > Enter your current password (default password is printed on the battery label)
- > Enter your new password x 2 and press Apply to set.

Settings > Device settings > USIM PIN Management

Home Settings SMS Phonebook Information

Quick Setup
Network Settings
Wi-Fi Settings
Device Settings
 > Password Settings
 > USIM PIN Management
 > Reset
 > Restart
 > Low Current Mode
 > Backup & Restore

USIM PIN Management

USIM PIN Status ☐ Enable ☒ Disable Change PIN

Current PIN *

Attempts Left: 3

Apply

[?](#)

Overview :

USIM PIN management allows you to enable or disable and change the SIM PIN on this device. By default, the SIM PIN is disabled for ease of use. If the SIM PIN feature is enabled, you will be prompted to enter the SIM PIN each time the device is turned on to use the device.

Instructions :

Enabling your devices SIM PIN:

- > Navigate to Settings > Device Settings > USIM PIN Management
- > Select Enable and enter the current SIM PIN.
- > Click on Apply to confirm the changes.

Disabling your devices SIM PIN:

- > Navigate to Settings > Device Settings > USIM PIN Management
- > Select Disable and enter the current SIM PIN.

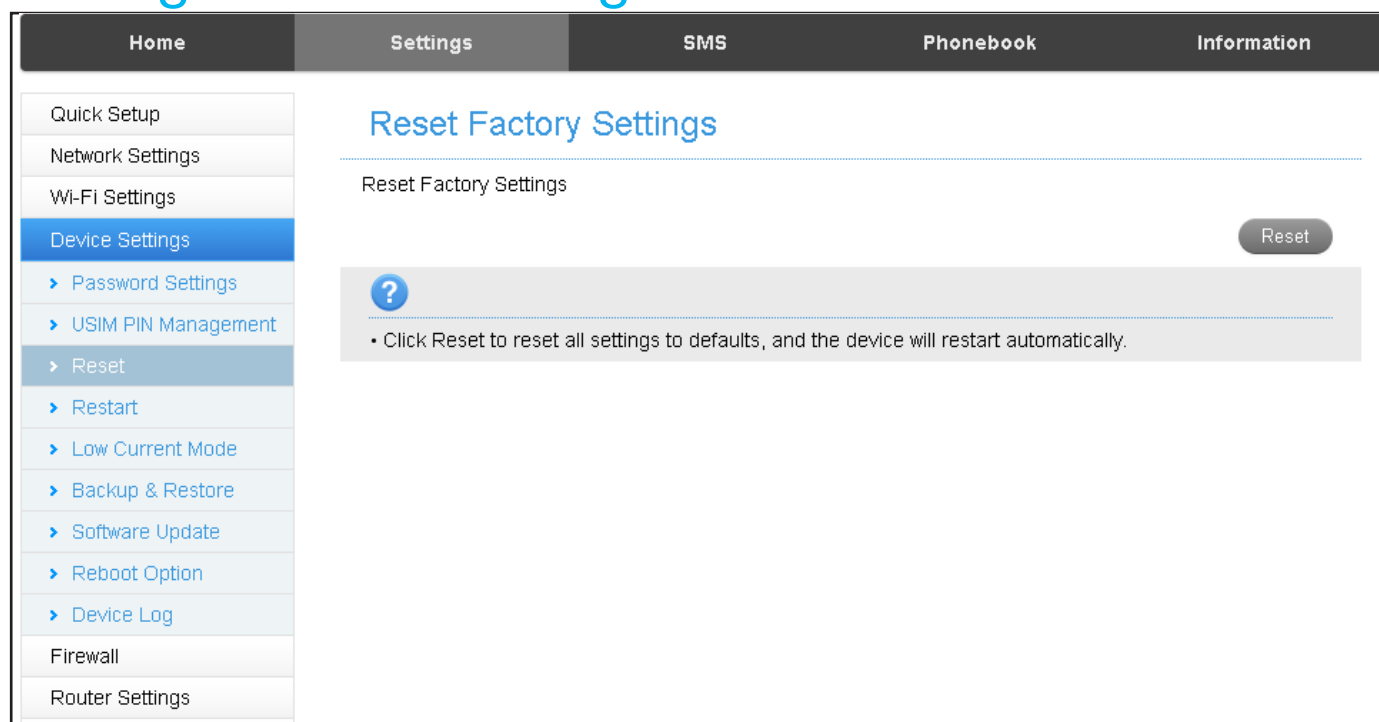
Important:

You will need to contact your Service Provider for the SIM PIN code if you do not have the default SIM PIN.

If you incorrectly enter the SIM PIN more than 3 times your SIM will be PUK locked, in this situation you will be prompted to enter the PUK code to unlock to SIM, you will need to contact your Service Provider for an PUK code to continue to use your SIM in the device.

Click on the Help icon to get context tips.

Settings > Device settings > Reset



Overview :

The Reset function enables you to reset your device to its original factory default settings and will revert any custom changes that have been made on the device.

Instructions :

Factory Reset your device:

- > Navigate to Settings > Device Settings > Reset
- > Click on Reset to restore your device to factory settings.
- > Click on Yes to confirm the changes.
- > Your device will restart to factory settings.

If you wish to Restart your device without a factory reset then choose Settings > Device Settings > Restart

Factory Reset button

You can restore the unit to factory settings by pressing the Reset button located under the battery cover.

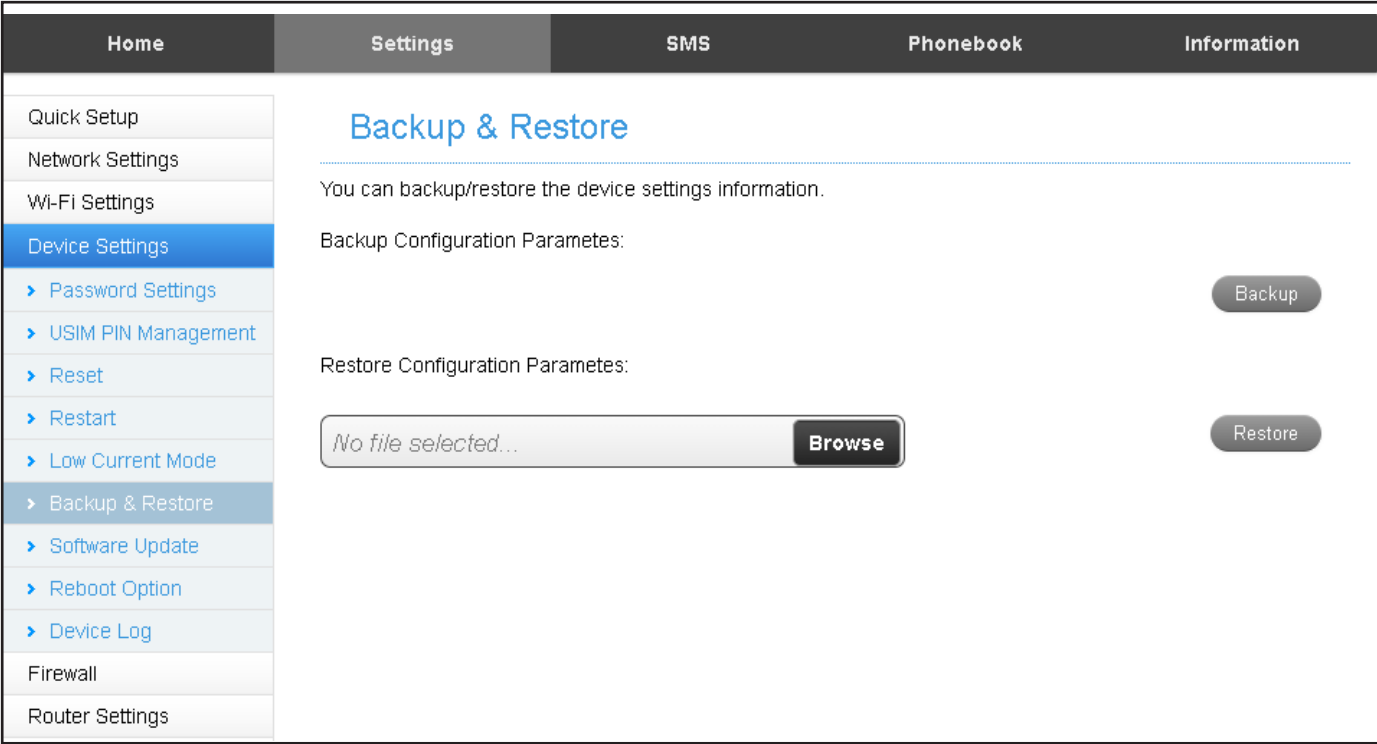
Open the battery cover and locate the Reset button. Insert a small pin and hold the button for 4-5 seconds until the LED's flash and the device restarts. The unit will reset to factory defaults and all personal settings, passwords, and messages will be reset.

Reset button under battery cover



Important :
It is important to note that all changes made to the device settings will be reset.

Settings > Device settings > Backup & Restore



Overview :

Backup and Restore allows you to save a config file to keep all your current settings and passwords.

Instructions :

- > Navigate to Settings > Device Settings > Backup & Restore
- > Press Backup to create a Backup file and Save at your chosen location.
- > To Restore a previously saved file press Browse to locate your file then press Restore to load that configuration file.

Settings > Device settings > Software Update

Overview :

The Software Update page allows you to modify the preference in enabling or disabling automatic updates when they become available. Software updates often include new features, improved performance, and bug fixes, which can enhance the device’s overall functionality and user experience.

The automatic software update function provides a convenient and hassle-free way to keep the device up-to-date with the latest software releases.

Home

Settings

SMS

Phonebook

Information

Quick Setup

Network Settings

Wi-Fi Settings

Device Settings

> Password Settings

> USIM PIN Management

> Reset

> Restart

> Low Current Mode

> Backup & Restore

> Software Update

> Reboot Option

> Device Log

Firewall

Router Settings

DDNS

NFC

Power Save

Automatic Updates

Automatic Updates ☒ Enable ☐ Disable

Software update package will be downloaded and installed automatically when Automatic Update is turned on and update is available. Additional data charge may incur (especially if device is roaming overseas).

Apply

Check for New Updates

Click the 'Update Now' button to see if a new version is available.

Update Now

Roaming Settings

☐ Check here to connect to the internet while roaming.

Note: Telstra customers travelling outside of Australia may incur additional data charges whilst roaming.

Apply

Instructions :

Modifying your devices software update preference:

- > Navigate to Settings > Device Settings > Software Update
- > Select Enable or Disable for Automatic Updates
- > Select Apply

Manually checking for new software updates:

- > Navigate to Settings > Device Settings > Software Update
- > Click on Update Now to check for available software updates.

Modifying your devices roaming settings:

- > Navigate to Settings > Device Settings > Software Update
- > Click on the checkbox to enable or disable roaming
- > Click on Apply to confirm the changes.

Settings > Device settings > Reboot Option

Overview :

You can set your device to Reboot every 24 hours at a set time. The device operation might be improved by setting a daily reboot to keep your device running at optimum.

Instructions:

To enable Reboot option:

- > Navigate to Settings > Device Settings > Reboot Option
- > Select Enable and enter a valid time to reboot the device
- > Click on Apply to confirm.

Settings > Device settings > Device Log

Overview :

You can review the device activity using the Device Log function.

Instructions:

- > Navigate to Settings > Device Settings > Device Log
- > Review the device logs presented or select an option from Display Type to review different logging data.

Settings > Firewall > Port Filtering

Overview :

Port filtering is considered an expert setting and is generally only used by network administrators. Port Filtering allows you to block unused ports in your network which can reduce the risk of external attack.

Instructions:

- > Navigate to Settings > Firewall > Port Filtering
- > Select Enable then Apply to see available settings.

Settings > Firewall > Port Forwarding

Overview :

Port Forwarding is considered an expert setting and is generally only used by network administrators. Port Forwarding allows remote servers and devices on the internet to access devices on your private internal network.

Port Forwarding can be used to set up web servers, email servers or other specialised Internet applications. When users send this type of request to your network via the internet then the router will forward these to the appropriate destination.

Instructions:

- > Navigate to Settings > Firewall > Port Forwarding
- > Select Enable then Apply to see available settings.

Settings > Firewall > Port Mapping

Overview :

Port Mapping is considered an expert setting and is generally only used by network administrators. Port Mapping allows you to map a port of the IP address of an external host on the internet to a machine on the internal side of your network.

Instructions:

- > Navigate to Settings > Firewall > Port Mapping
- > Select Enable then Apply to see available settings.

Settings > Firewall > Domain Filtering

Overview :

Domain Filtering allows you to block the modem from accessing specified Domains or websites. You can block all access to a website or domain based on the Domain Naming System (DNS) of the destination. Example if you put Youtube.com and press Apply then no one on your network can access Youtube.

Instructions:

- > Navigate to Settings > Firewall > Domain Filtering
- > Select Enable then Apply to see available settings.

Settings > Firewall > UPnP

Overview :

UPnP allows network devices to discover each other on your network. It is considered risky to deploy UPnP so should only be used by experienced network administrators who are familiar with the risks.

Settings > Firewall > DMZ

The screenshot shows the 'DMZ Settings' page in a modem's web interface. The top navigation bar includes 'Home', 'Settings', 'SMS', 'Phonebook', and 'Information'. The left sidebar lists various settings categories, with 'Firewall' selected and 'DMZ' highlighted. The main content area is titled 'DMZ Settings' and features a toggle switch for 'DMZ Settings' set to 'Disable'. An 'Apply' button is located in the top right corner. A help box with a question mark icon contains the following text:

- The DMZ function is considered an Expert function as you will need to configure an Static IP address for a LAN side device and understand what you are doing and the risks involved. You would also need to have a Public IP Address for the WAN connection enabled on your SIM and most likely use a specific APN as well.
- DMZ stands for "DeMilitarized Zone". In networking terms a DMZ typically allows all ports from the WAN side of a device to a IP address on the LAN side of the device.
- If you are having problems running network applications that are hosted on a PC or other device connected via LAN / USB / W-Fi through this device, you could use the DMZ function to allow access directly without having to create multiple Port Forwarding rules.
- You can Enable / Disable and configure DMZ on this page.

Overview :

Firewall DMZ (Demilitarized Zone) is a networking term that refers to a specific

zone on a network that is isolated from the rest of the network, but still accessible from the internet.

Instructions:

To enable DMZ on your device:

- > Navigate to Settings > Firewall > DMZ:
- > Select Enable and enter a valid IPv4 address
- > Click on Apply to confirm the changes.

To disable DMZ on your device:

- > Navigate to Settings > Firewall > DMZ:
- > Select Disable to disable DMZ
- > Click on Apply to confirm the changes.

Important:

Enabling DMZ mode may increase the device's exposure to potential security risks, and therefore should only be done if necessary and with caution.
Click on the Help icon to get context tips.

Settings > Firewall > SIP ALG

Overview :

The SIP ALG function is for experienced network administrators. If you are using a SIP terminal for voice over IP using this device then the SIP ALG function will help that device or app connect through the Firewall Network Address Translation. Generally you would need to have a public IP address enabled on your SIM service for this function to work as intended.

Settings > Firewall > System Tools

Overview :

You can enable or disable PING from WAN, which determines whether external apps or devices can Ping your modem IP address. External PING enabled will increase incoming traffic and may make you vulnerable to DOS attacks.

Settings > Router Settings

Overview :

You can set the DHCP range and whether DHCP is enabled or disabled. IP Passthrough is also known as Bridge Mode. All incoming data is passed directly the USB connected device. If you enable this option then you can no longer access the router's web pages. After setting IP Passthrough the device passes all traffic and can no longer be accessed via the web interface. Use the Factory Default

button to restore from this function.

Network Address Translation (NAT) allows the LAN side to communicate with the WAN side. It should not be switched OFF (Enable State).

Settings > DDNS

Overview :

Dynamic DNS allows you to register an account with a DDNS provider and set a Domain name for the device. This service needs a public IP address on your SIM card and is considered an advanced function for network administrators.

Settings > Power Save

Overview :

Power save will reduce power consumption by turning off the Wi-Fi when there is no network traffic. The sleep time can be adjusted or set to Never to prevent the device entering low power mode.

Instructions:

Navigate to Settings > Power Save and set the required Sleep time.

SMS

Overview :

You can manage the SMS (text messaging) feature in this setting and can view or delete received SMS messages and make changes to the SMS configuration.

Instructions :

To access SMS stored on the device:

- > Navigate to SMS > Device SMS

To delete SMS stored on the device:

- > Navigate to SMS > Device SMS
- > Click the checkbox next the SMS (or multiple SMS) you wish to remove.
- > Click on Delete to remove the SMS
- > Confirm the action by selecting Yes to delete the SMS (or multiple SMS).

To access the SMS stored on the SIM:

- > Navigate to SMS > USIM SMS

To delete SMS stored on the SIM:

- > Navigate to SMS > USIM SMS
- > Click the checkbox next the SMS (or multiple SMS) you wish to remove.
- > Click on Delete to remove the SMS
- > Confirm the action by selecting Yes to delete the SMS (or multiple SMS).

To modify the SMS Settings:

- > Navigate to SMS > SMS Settings
- > Select the Validity drop-down menu for outgoing SMS messages expiration

Phonebook

Overview :

All device Contacts are stored in the phone book.

Information > Device Information

Overview :

Navigate to the Information tab to check your device IMEI number, software version and quick change the SSID names.

Information > Network Information

Overview :

Network Information shows your current network signal technology (5G, 4G) and all related connected bands and signal strength. It is useful for troubleshooting network signal issues.

Technical Specifications

Network Compatibility	4GX LTE, Bands 1, 3, 7, 26, 28
Chipset	Qualcomm Snapdragon SDX12-2
Wi-Fi	Wi-Fi 802.11 b/g/n/ac 2.4GHz and 5GHz
Dimensions	107 x 63 x 14mm, 118g
Battery	3000mAh battery, user replaceable
Operating time	Active battery up to 8 hours.
Connectivity	USB 3.1 type C charging connection
Operating systems	Any Wi-Fi enabled device, Windows 10, 8, MAC OS X 10.7, Linux (3.10 kernel upwards).
SIM Card	Nano SIM, 4FF
Display	3 x LED indicators
Temperature	-5°C to +40°C

Troubleshooting

Issue	Possible cause	Possible Solution
No Network Access	A missing, faulty or incorrectly inserted SIM.	Check you have inserted your SIM card the right way and pushed inside the slot until it clicks into place.
No Network Access	A Non-Telstra SIM card.	If you use an alternative Mobile Network Providers SIM card, you may need to set a new APN for your carrier. See - Settings > Network Settings > APN : for more details.
No Network Access	PIN locked SIM card.	Log into the USB web interface (Home > Settings > Device settings > USIM PIN Management - page 16) then enter the PIN code for your SIM card.
No Network Access	PUK locked SIM	You may have entered the wrong SIM PIN code too many times, your SIM will be PUK locked. Please contact Telstra (on 13 22 00 and follow the voice prompts) to obtain your 8-digit Personal Unlocking Key (PUK) code. Log into the web interface (Home > Settings > Device settings > USIM PIN Management - page 16) to enter the provided PUK code.
No Network Access	PUK blocked SIM card.	When you enter the PUK code incorrectly too many times, your SIM card will be PUK blocked. You will need to contact Telstra (on 13 22 00 and follow the voice prompts) to replace your physical SIM.
The user interface doesn't start after the modem is plugged in.	PC configuration is not correct. (No autorun)	Start the program manually by going Start > Program Files or use the shortcut on the desktop.
The modem has no signal.	You have no network coverage.	Try moving location until you get good reception. Move the modem to a higher position or different orientation.

Technical examples for more advanced functions

Introduction

The Telstra 4G Hotspot / ZTE MF986C has many functions that are usually never touched by users as the out of the box experience is all that they need or will ever use. Then there are a small subset of users that are highly technical or have a specific technical requirement for configuring their communications solutions a very specific way.

Sometimes this is for gaming or security systems with older IP cameras. At other times they are business users that have a need to be mobile but need to have all the access that they have when they are in their office. The Telstra 4G Hotspot / ZTE MF986C has the functionality required to fulfil all these scenarios and it is recommended that only users with previous experience in the following Expert Class functions use them.

It is important to remember that some of these functions, if used, will require a Factory Default from the LCD interface to get control back of the device resulting in all your configured settings being removed. So plan ahead and try things out but be prepared for starting again from the start. Also check with your carrier if you are able to get a Public IP address on the SIM / service you are using with the Telstra 4G Hotspot as several of these functions require a Public IP Address.

So starting out with this new device we will go through the most logical and typically required configuration elements to obtain the most from these specific functions. Again it is important to mention again that these functions are not something that a normal user would normally touch or would be suggested to “play” with as they could cause themselves issues and would need to Factory Default the device using the LCD menus to get back to a working device.

Also it is important to point out that some of the requirements depend on what functionality your carrier provides you with or what provisioning they allow. Public IP Address allocation for SIM services typically requires you to be a Business or Enterprise customer before you can access them. There are also other Business or Enterprise offerings like Framed Routes for mobile office network linking that are part of SDN products that carriers have that normal users wouldn't qualify for. This is why some of the following settings are considered Expert Class functions.

First Steps

Why and How to get a Public IP Address for SIM based WAN connection

Normal Mobile data services are provided with private IP Addresses using Carrier Grade NAT (called CGNAT) that basically allows you to get to the internet but without an outgoing IP packet request from you the internet can't reach you or your modem.

This is perfectly fine for normal home use in most cases, but if you are hosting other devices that you need to reach remotely, typically for business or security use, then you would need a Public IP Address that is reachable from the internet.

To obtain a Public IP Address from a carrier you will need to speak with the carriers support team and find out what they offer. Typically this is an option for a business account user and could require both special provisioning of your SIM card that is used in your modem and a specific APN that has access to Public IP Addresses usually via DHCP but could be a true static Allocated IP Address with additional cost.

If you are a Telstra Business or Enterprise customer then Googling will show you that you will need to speak with Telstra Support and ask to add the data code GP-TEXB3 to your SIM. After this code has been added, connect with the APN "telstra.extranet" to get assigned a public IP address.

Remember that this requires you to be a Telstra Business or Enterprise user. Speak with your carriers support team or google "how to get Public IP Address on xxxxx SIM service" or such to learn more. But you will need this working before moving forward with most of the following functionality.

New APN Configuration

Most likely you will need to configure a specific APN to access a Public IP Address, so you will need to do the following.

1. Login to your modem WebGUI and go to the following menu:
Settings Tab / Network Settings / APN
2. Click on the “Disconnect” button as you need the device to not be active on-line to change APN settings.
3. Click on the “Add New” button that is located in the top right of this menu page.
<insert menu image here>
4. Fill in the Profile Name, APN and set the IP Type as IPv4v6. If required fill in the other fields before clicking on “Save”.
5. Next you need to select the new APN you have created from the available Profile drop down box and then click on the “Set as Default” button
6. Finally you need to press the “Connect” button to connect using your new APN..

Static IP Address Configuration

You may need to set aside IP Addresses for devices on your LAN side of your device so you can know exactly the IP Address of a specific device on your internal network and not worry about it changing every time the DHCP lease expires. You will have to configure your devices that need to have Static IP Addresses manually and change the DHCP IP Pool Range from the default setting to only serve a smaller Pool of IP Addresses allowing you to have IP Addresses to use and allocate manually as required.

The configuration for this is covered in detail later in this document following its location / position with the device menus. To learn more see that section.

DDNS Configuration

Now that you have a Public IP Address you can configure DDNS / Dynamic Domain Name Service. This module will allow the modem to communicate with DDNS service providers DynDNS or NoIP which you can have free or paid for accounts whenever your Public IP Address on the modem WAN connection changes.

Your DDNS service provider will allow you to create a domain name that you can easily remember that will always take you to your current Public IP Address. (ie ipcam.ddns.net instead of 150.157.172.88)

DDNS configuration is covered in detail later in this document following its location / position within the device menus. To learn more see that section.

Expert Class Settings

The settings below need you to know what you are doing otherwise you will be either getting very frustrated or Factory Defaulting your device via the LCD touch screen menu very often. These settings in some cases are very straight forward and only have been included here due to their presence in the menu structure (ie Domain filtering). Settings that are more complex are detailed as being Expert Class due to the potential complexity of the function and what is required for it to work in your network.

Firewall Settings Menu - Port Filtering

Enabling Port Filtering is considered an Expert function since you are taking responsibility for the security policies that are protecting your connected devices from malicious activities.

If you understand the risks involved you can proceed by Enabling Port Filtering which will then display the Filtering Policy creation interface. The Default Policy for how to handle packets is also able to set at this time. If the Default Policy setting is set as “Dropped” which means that any traffic or packet that doesn’t match a rule set is dropped into the bin or thrown away and never gets through to your connected devices.

If the Default Policy is set as “Accepted”, then all packets are allowed and it will be the following Port Filtering Rules that will do the dropping of packets. Due to this structure, Port Filtering has to be planned before you start entering the rules as the order that they are created could effect the outcome of what you are filtering. Port Filtering also requires that the LAN / Wi-Fi connected device is using a Static IP address, otherwise the Port Filtering Rule would fail after every reboot or reconnection.

You should also avoid configuring any rules that could interfere with being able to access or communicate with your own device. So port 80 (http) should never be forwarded or filtered. The rules can be set to match against a MAC address, Source / Destination IP address, Protocol and / or Source / Destination Port(s). When one of these set conditions is matched then the defined Action is performed on that packet. This would either be to Drop or Accept the packet, thus filtering the traffic flowing through your device.

If there is no match then the packet is passed to the next Rule. And if there is no next Rule then the Default Policy is applied. As Dropped is the usual Default Policy for security reasons, then everything else will be dropped / blocked. As the device only allows 10 rules to be set respectively for IPv4 and IPv6 you need to plan it all out logically or risk packet loss that you intended to support. The rules that have been configured are listed below the setting interface and can be selected for deletion.

Quick Setup

Network Settings

Wi-Fi Settings

Device Settings

Firewall

> Port Filtering

> Port Forwarding

> Port Mapping

> Domain Filtering

> UPnP

> DMZ

> SIP ALG

> System Tools

Router Settings

DDNS

NFC

Power Save

Port Filtering

MAC/IP/Port Filtering ☒ Enable ☐ Disable

Default Policy ☒ Accepted ☐ Dropped

Apply

?

MAC/IP/Port Filtering Settings

IP Settings ☒ IPv4 ☐ IPv6

MAC Address (e.g., 00:1E:90:FF:FF:FF)

Source IP Address

Destination IP Address

Protocol

Action ☒ Accept ☐ Drop

Comment *

Apply

?

Current MAC/IP/Port Filtering Rules in System

	MAC Address	IP Type	Source IP Address	Destination IP Address	Protocol	Sou
--	-------------	---------	-------------------	------------------------	----------	-----

- MAC Address: Set MAC address to be filtered.
- Source IP Address: Set source IP address to be filtered.
- Destination IP Address: Set destination IP address to be filtered.
- Protocol: Set protocol to be used for filtering.
- Source Port Range: Set source port numbers to be filtered.
- Destination Port Range: Set destination port numbers to be filtered.
- Action: Set to handle the packet if it matches with the rule.
- Comment: Free text comment field for your notes.

Port Forwarding

Enabling Port Forwarding is considered an Expert function since you are taking responsibility for the security policies that are protecting your connected devices from exposure to the internet and malicious activities. If you understand the risks involved you can proceed by Enabling Port Forwarding which will then display the Port Forwarding interface for creating Virtual Server access through your device to Wi-Fi / USB / LAN connected devices.

Port forwarding as an expert function, has other requirements that you need to configure and setup both on this device and on the device you are going to be forwarding too. Port Forwarding requires that the LAN / Wi-Fi connected device is using a Static IP address, otherwise the Port Forwarding Rule would fail after every reboot or reconnection.

For example, if you are going to Port Forward port 8080 to a device using the IP address 192.169.0.100, you will need to set that IP address to be assigned and used by that device only and on that device itself you would need to either set the assigned IP address and install a web server or application to handle the port 8080 traffic.

You should also avoid configuring any rules that could interfere with being able to access or communicate with your own device. So port 80 (http) should never be forwarded or filtered, otherwise you will need to factory default your device to change any settings, which means you will need to redo all your settings from scratch again. A maximum of 10 Rules can be set and can be seen listed below and they can be selected for deletion.

IP Address: Specify a computer located at LAN to provide services.

Port Range: Set port numbers to be forwarded.

Protocol: Protocols applied by services.

Comment: Free text comment field.

The maximum number of rules is 10.

Port Mapping

Port Mapping is very similar to Port Forwarding, except you can now alter the source port and destination port numbers. For instance you could make traffic coming to port 80 on the WAN connection of your device map to port 8000 on an internally connected device using this function.

As this is an Expert function and requires an understanding of many IT elements, you should understand also that you are responsible for the security of your devices and network if you use this function. For instance, you need to setup static IP addresses for the internally connected server / device that the Port Mapping will be directed towards.

A maximum of 10 Rules can be set and can be seen listed below and they can be selected for deletion.

This is an Expert function and is only used for single ports and NOT ranges of ports.

- Source Port/Destination Port: The port of the computer that provides services.
- Destination IP Address: Specify a computer located at LAN to provide services.
- Protocol: Protocols applied by services.
- Comment: Free text comment field.
- The maximum number of rules is 10.

Domain Filtering

Domain Filtering is simply a function that allows you to define domains that you wish to block from being able to be accessed by any other device connected to your hotspot device. You just enter the domain into the Domain Name field and click on Apply. The filtered domains are listed below this interface and can be selected for deletion.

UPNP

Universal Plug and Play (UPnP) is a set of networking protocols that allows networked devices, such as PC, printers, Internet gateways, Wi-Fi access points and mobile devices, to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and entertainment.

Today it is considered a risk to enable so do so only after considering the potential risks and benefits. The setting is only a choice between enabled or disabled.

DMZ

The DMZ function is considered an Expert function as you will need to configure a Static IP address for a LAN side device and understand what you are doing and the risks involved. You might also need to have a Public IP Address for the WAN connection enabled on your SIM and most likely use a specific APN as well if you are hosting a server / service that you need to access remotely.

DMZ stands for "DeMilitarized Zone". In networking terms a DMZ typically allows all ports from the WAN side of a device to an IP address on the LAN side of the device. If you are having problems running network applications that are hosted on a PC or other device connected via LAN / USB / W-Fi through this device, you could use the DMZ function to allow access directly without having to create multiple Port Forwarding rules. You can Enable / Disable and configure the internal (static) IP Address for the device that you require to receive ALL incoming traffic.

SIP ALG

The SIP ALG (Application Layer Gateway) function is considered an Expert function as you may need to have a Public IP enabled SIM configured depending on your SIP service requirements. If you are using a SIP terminal or application for voice calls over IP using this device, then the SIP ALG function could help that device / app to connect through the NAT (Network Address Translation) Firewall to perform normal data interaction with a SIP softswitch on the Internet / WAN connected network.

The SIP ALG interface is simply an Enable / Disable setting.

System Tools - Ping from WAN

This is an important function for testing only once you are setting up a Public IP Address on the WAN side of your device. This can be enabled while confirming that the Public IP address is indeed allowing access from the internet. It shouldn't be left enabled unless it is something that you need to remote monitoring (heart-beat ping) to check that the connection and device are live and accessible.

Router Menu Settings - Device IP Address Settings

This Device is set as a Dynamic Host Configuration Protocol (DHCP) server by default, providing IP address from DHCP IP Pool for all PC connections to LAN. By default, almost the entire internal IP Address range is allocated in the DHCP Pool. This is fine for most users, but if you are wanting to configure any of these functions that are defined as Expert Class functions, then the internal IP Addresses need to be reconfigured so that you can manually define static IP addresses to devices internally that you never want to change their IP Address.

To change the IP Address range or Pool you will need to firstly Disconnect the device from the mobile network connection. This will then allow you to change the internal IP address range and / or Pool range. Once you have made your changes and clicked on Apply the device will notify you that it will require a restart and once it has restarted the DHCP settings will have been updated and the mobile connection restored.

A Factory Default will restore the DHCP settings back to how they were so remember this if you are changing Expert Classed functions as several of them can only be stopped by performing a Factory default from the LCD interface.

- IP Address: IP address for LAN interface.
- Subnet Mask: Subnet mask for IP address.
- DHCP Server: Enable or Disable DHCP Server.
- DHCP IP Pool: Allocate start and end IP address for IP pool.
- DHCP Lease Time: Define validity of the leased IP address; and new IP address will be relocated.
- Your settings will take effect after restarting your device.

IP Address & DHCP Configuration

1. First login to your device and go to the Home tab on the WebGUI and scroll down until you see the “Disconnect” button and click it, as you need to be offline before you can change the devices IP address configuration.
2. Next go to the following menu in the WebGUI of your device:
Settings Tab / Router Settings / Device IP Address Settings
3. Now as long as your device is “Disconnected”, you will be able to alter the IP address settings shown in this menu including the device IP Address, Subnet Mask, DHCP Server On/Off, DHCP IP Pool Range and DHCP Lease Time settings.
4. Once you have made your IP address configuration changes click on the “Apply” button and a confirmation pop-up box will appear asking for you to confirm the change and that the device will need to perform a restart to apply these setting changes. Click Yes to continue.
5. Now wait for the device to restart and then login and check that your settings are now applied.

IP Passthrough

IP Passthrough is an Expert function as you need to understand all the risks and implications of enabling it. The IP Passthrough function will basically turn this device into an electrical interface only and pass all WAN traffic / packets as they come to the configured IP address connected preferably using the USB port.

The reason for this is a static IP Address is required and the IP Passthrough function also is mapped usually to a particular Port. Normally this is a LAN / Ethernet port, but as this device doesn't have an Ethernet port, the USB port has been defined as the port to use. Wi-Fi is not recommended for connections that require secure and reliable connectivity for critical communications especially when the device is basically now just an electrical modem and passing all traffic to a single device to handle. You will also likely require that the WAN side of the device (Mobile network connection), has a Public IP Address so it is accessible from the internet directly. It is recommended that you don't allow any other devices access via Wi-Fi to negate the risk of network connection confusion. The only way to stop this function is to Factory Default the device from the LCD interface.

Also note that IP Passthrough as that function passes ALL traffic through the device and any other local functions on the Hotspot device will have no effect. So functions like DDNS on the device itself will not work since they get no traffic. You would need to setup a DDNS client on the LAN side device that all traffic is being sent to.

- All other functionality on this device will no longer be available until you factory default the device to regain WebGUI access again.
- This function will deliver the WAN side traffic / packets directly to the FIRST device that connects to this device via either LAN / USB or Wi-Fi.
- Remember to only allow the one device that is configured to service the WAN connection to access this device, otherwise nothing will work until you Factory Default to regain full control.

NAT Off

The NAT Off function is considered an Expert function since you are taking responsibility for how your device will function and your security. NAT stands for Network Address Translation and is the functionality that allows the internal private IP address range used on the LAN side of the device to be able to communicate with the WAN side of it. It should never be turned off as there is no benefit and real risks for your network and security.

No reason for disabling NAT could be thought of during this device's designed normal use. It would only be used when the WAN connection is a private network service that is secured by carrier supplied firewalls or service (enterprise grade service typically) where the NAT function is not required as the device would be required to act as a Router only. The carrier service would then be providing a private routed service connection between multiple devices and networks under your control and you would need more device configuration than just disabling NAT.

DDNS Menu Settings

The DDNS function is considered an Expert function as you will need to understand the configuration requirements of much more than just DDNS on this device. DDNS stands for Dynamic Domain Name Service and it uses Internet based providers to provide a DDNS service that maintains a Domain Name mapping to the (Public) WAN IP address of this device and this will update every time your WAN IP changes.

Another reason this is considered an Expert function is that to work you will need a Public IP address on your SIM card service that can be accessed from the Internet and this typically requires a business or enterprise account to obtain. You will also likely require to configure a new APN on your device to be able to access the Public IP address service from your carrier.

The advantage that DDNS provides is that every time the Public IP Address updates on the WAN interface you can have it set to Automatically update the DDNS provider of the new Public IP Address and know that the Domain that you set should always be able to bring up your device WAN IP. DDNS is used typically with other Expert class functions like DMZ, Port Forwarding but NOT with IP Passthrough as that function passes ALL traffic through the device and the local functions have no effect, so you would need to setup a DDNS client on the LAN side device that all traffic is being sent to via the IP Passthrough function.

- DDNS function: User can register an account on DDNS provider and set a domain name for the device.
- DDNS Mode:
- Automatic: the IP address change will be updated to the DDNS server automatically (best option)
- Manual: the IP address change will be updated to the DDNS server by the user manually
- Dynamic DNS Provider: DDNS server
- Account: The account that register on DDNS server
- Password: The password of the account
- Domain Name: The domain name that is registered on DDNS server
- Provider – Select either DynDNS or NoIP

DDNS Configuration

1. Go to the DNS WebGUI menu page using the following path:
Settings / Modem Settings / DNS Setting Tab
2. Click on the Dynamic DNS Client Enable switch button and set it to “ON”,
3. Select your DDNS provider from the two options supported by the modem. If you haven't set up an account on one of these DDNS service providers then go do that now and come back once you have all the required account details that are required to be filled in on your modem DDNS configuration.
4. If you have all the required DDNS settings information for your account on either DynDNS or NoIP then enter them now into the following fields:

Username – Fill in your Account username for the DDNS service you are using,

Password – Fill in your Account password for the DDNS service you are using,

Hostname – Fill in the full hostname and domain you have selected on your DDNS service.

5. Now click the “Apply” button and the modem will contact the DDNS service and update it with your Public IP Address used on your modem WAN connection.

Defined Responses for DDNS Connection

Successfully: IP address update successful

Login error: Account validate on DDNS server is failed

Network error: The network is abnormal

Updating: IP address is updating

Not registered: The account is not registered on DDNS server

Error registering: other error for this function.

Precautions & Safety Information

1. The modem is a transmitting device and may cause interference to sensitive electronic equipment such as audio systems, vehicle systems and medical equipment. Please consult the manufacturer of the other device before using the modem.
2. Operating of laptop or desktop PCs with the modem may interfere with medical devices like hearing aids and pacemakers. Please keep the modem more than 20 centimetres away from such medical devices. Turn the modem off if necessary. Consult a physician or the manufacturer of the medical device before using the modem near such devices.
3. Be aware of regulations when using the modem at places such as oil refineries or chemical factories, where there are explosive gases or explosive products being processed. Turn off your modem as instructed.
4. Do not leave the modem in direct sun. Don't cover the modem or leave on soft furnishings or surfaces that retain heat. It is normal for the unit to run warm but do not allow to overheat. If the unit is above 40C it will not charge the battery. Higher temperatures increase the risk of failure or the battery being damaged.
5. Store the modem out of reach of children. This device may contain button cells which can be fatal if swallowed.
6. The modem contains sensitive electronic circuitry. Do not expose the modem to any liquids, high temperatures or shock.
7. Only use original accessories or accessories that are authorised by the manufacturer. Using unauthorised accessories may affect your modem's performance or damage your modem.
8. Avoid using the modem in areas that emit electromagnetic waves or in enclosed metallic structures e.g. lifts.
9. The modem is not waterproof. Please keep it dry and store in dry conditions.
10. Always handle the modem with care. Be careful not to drop or bend the modem.
11. There are no user serviceable parts inside the modem. Unauthorised dismantling or repair will void the warranty.
12. Do not dispose of the unit in a fire, the battery may explode.
13. At the end of life of the equipment, return the product to a suitable recycling agent such as Mobile Muster.

RF Safety Information

For optimum performance with minimum power consumption do not shield the device or cover with any object. Covering the antenna affects signal quality and may cause the modem to operate at a higher power level than needed.

Radio Frequency Energy

The hotspot is a low-power radio transmitter and receiver. When switched on it intermittently transmits radio frequency (RF) energy (radio waves).

The transmit power level is optimized for best performance and automatically reduces when there is good quality reception.

Maximum power is only used at the edge of network coverage so under most circumstances the power output is very low.

Under poor network conditions the modem transmits at a higher power level and may get hot.

Declaration of Conformity : Specific Absorption Rate (SAR)

The hotspot is designed to be used in close proximity to the body. We declare that the product detailed in this manual, and in combination with our accessories, conform with the essential requirements of The Radio Communications Standard (Electromagnetic Radiation Human Exposure) 2003 and the Australian Communications and Media Authority Section 376 of the Telecommunications Act 1997 when used at a distance of not less than 5mm from the body. The worst case simultaneous RF SAR result for this device is published on **ztemobiles.com.au**

* Download speeds will vary due to distance from the cell, local conditions, user numbers, file source, hardware, software and other factors.

** Operation and Standby times depend on a number of conditions and are measured in ideal conditions.

Telstra Copyright © 2024. All rights reserved.

Telstra SIM required.

ZTE Copyright © 2024. All rights reserved.



The manual is published by ZTE Corporation. We reserve the right to make modifications on errors or update specifications without prior notice.