Predator Connect X5 5G CPE
User Guide
Version 0.1.18

Contents

1. Overview

The Predator Connect X5 5G CPE is designed to feature 5G and Wi-Fi 6 technology. This guide provides an overview of Predator Connect X5's features, and description of the user interface and ports of the device.

The Predator Connect X5 delivers gigabit transfer speed along with gaming features and user experience tuned for demands of PC gamers and media streamers. The Predator Connect X5 can be used to provide internet access through 5G or 4G cellular data (SIM and Data Plan not included) over WiFi 6 or Cat. Paired with Web UI, Predator Connect X5 5G CPE provides a simple and secure user experience for connecting and gaming on the internet.

1.1. Package Contents
- The box should include the following items:
- Predator Connect X5
- Power Adapter
- Quick Start Guide
- Warranty
- Declaration of Conformity

1.2 System Requirements
- This Predator Connect X5 is compatible with WiFi devices which support 2.4GHz (802.11 b/g/n/ax) or 5GHz (802.11 a/n/ac/ax) and have a web browser.
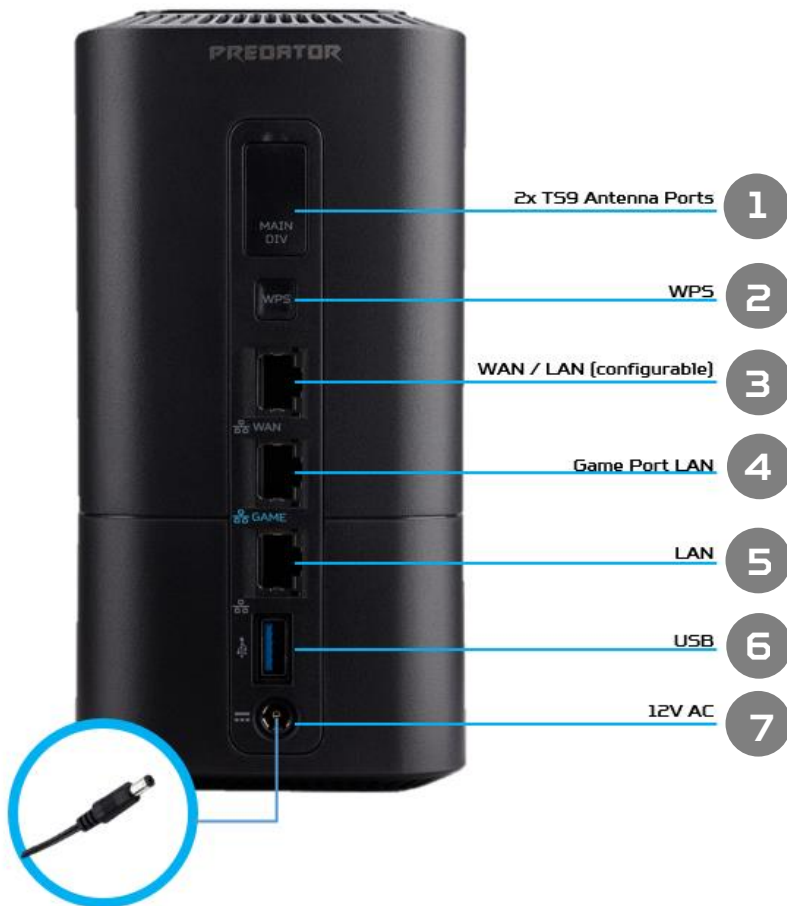
1.3 LED Behaviors

Device Operation LED Behavior				
LED Indicator & Status	5G LED Status	4G LED Status	WiFi / WPS LED Status	Power LED Status
5G Signal	Flashing Blue	Off	Static	Solid Green
4G Signal		Flashing Green	Static	Solid Green
Booting	Flashing Green	Flashing Green	Static	Solid Green
No Coverage or No SIM	Solid Red	Solid Red	Static	Solid Green
5G Data Connection (Connected)	Solid Blue	Off	Static	Solid Green
4G Data Connection (Connected)	Off	Solid Green	Static	Solid Green
WiFi is	Static	Static	Solid Green	Solid Green

Enabled				
WiFi is Disabled	Static	Static	Off	Solid Green

Reset and Update LED Behavior				
LED Indicator & Status	5G LED Status	4G LED Status	WiFi / WPS LED Status	Power LED Status
Factory Reset	Static then Flashing Blue	Static then Off	Static then Off	Static then Off
Firmware Update	Static then Flashing Blue	Static then Off	Static then Off	Static then Off
Device Shutdown	Static then Off	Static then Off	Static then Off	Static then Solid Green then Off

1.4 Rear View (Ports)

2x TS9 Antenna Ports	1
WPS	2
WAN / LAN (configurable)	3
Game Port LAN	4
LAN	5
USB	6
12V AC	7

1.5 Bottom View

Reset Button 1

SIM card Port 2
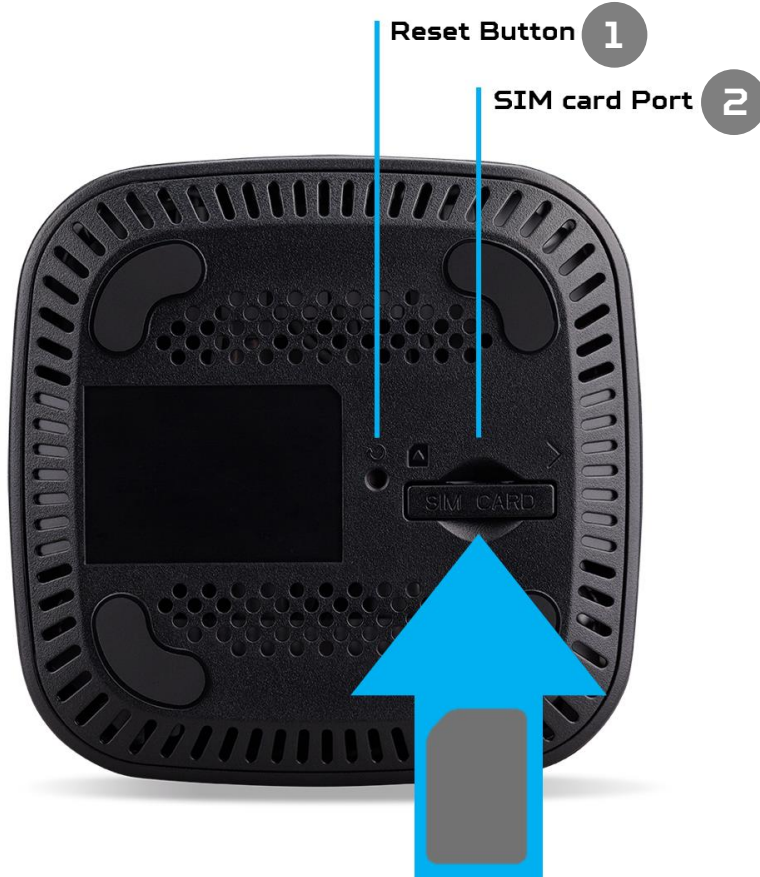
1.6 Environmental
- Operating temperature: -0 °C to 43 °C (0 °F to 95 °F) RH 90% Humidity
- Storage temperature: 0 °C to 45 °C (0 °F to 113 °F) RH 0% to 90% Humidity

1.3.5 Power Management
- Your Predator Connect X5 5G CPE comes with a 12v, 2.0A Max 24.0W power adapter. The included power adapter has an AC Input rating of 100-240V~, 0.85A, 50-60Hz.

- Note: To ensure your Predator Connect X5 works as intended, it is recommended you only use the accessories provided with your device.

2. Installation / First-time setup

2.1 Setup location
- Please choose a sturdy and open space for your Predator Connect X5 5G CPE.
- To ensure the best performance, be sure the area around your Predator Connect X5 is clear of miscellaneous items and debris. To ensure the best thermal performance and safe operations, please ensure that the thermal vents are not be blocked.

2.2 Setting up
- Locate the bottom of the Device
- Insert the SIM Card
- Lift the SIM door.
- Insert the SIM card into the slot with the gold contacts facing downwards.

- Fully insert the SIM card until it clicks into place.

- Note: Follow the notch direction on the top left of the SIM card slot. Also push the SIM into the slot smoothly all the way in with your finger tip and nail. Do not use any tool, as it may damage the SIM.

- Power to the device
- To power your device, connect it to your power adapter.
- Connect the power supply to the wall plug socket.

- Powering on the Predator Connect X5.
- Power on: Press the power button for 3 seconds. All LEDs will show solid green at the same time when the device has been switched on.
- To switch off your device: Press the power button for 3 seconds, until the LEDs power off.

2.3 Getting online

- Ensure your Predator Connect X5 is switched on and connected to the network.
    - A. You can refer to the LED Behavior table for more information.
- Connect your Computer to the internet using WiFi
    - A. Connect your computer or device to Predator Connect X5 via WiFi:
    - B. Search Predator Connect X5 wireless network name (SSID) on your device.
    - C. 2.4GHz wireless network name: PredatorConnect-X5-XXXX-2.4GHz
    - D. 5GHz wireless network name: PredatorConnect-X5-XXXX-5GHz
    - E. Connect to your preferred SSID.
    - F. Enter your WiFi password.
        - i. Note: You can find your default WiFi password on the label located on the underside of the Predator Connect X5.
- Connect your Computer to Predator Connect X5 via Ethernet cable:
    - A. Connect your Ethernet cable to Game port (Blue Icon) or LAN port (Gray Icon). You will see a LAN port connection on your laptop
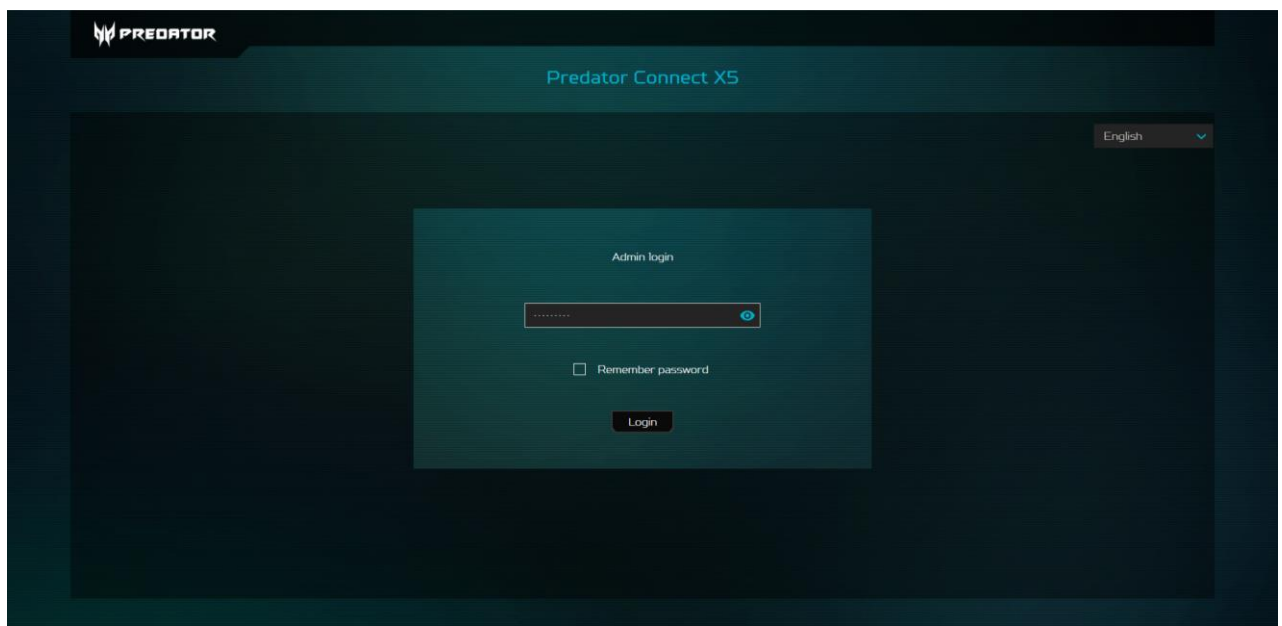
3. Predator Connect X5 Home Page

3.1 Predator Connect X5 Home Page Compatibility
- The Predator Connect X5 Home Page is compatible with the following browsers:
  - A. Google Chrome
  - B. Mozilla Firefox
  - C. Safari
  - D. Microsoft Edge

3.2 Logging into the Predator Connect X5 Home Page
- Open your web browser.
- Type http://connect.acer   or http://192.168.76.1:8080 into the address bar and press enter. The Home page will then load, as shown in the screenshot below.

- On the Home page, enter the password as found on device label on the bottom of the Predator Connect X5 and click Login.
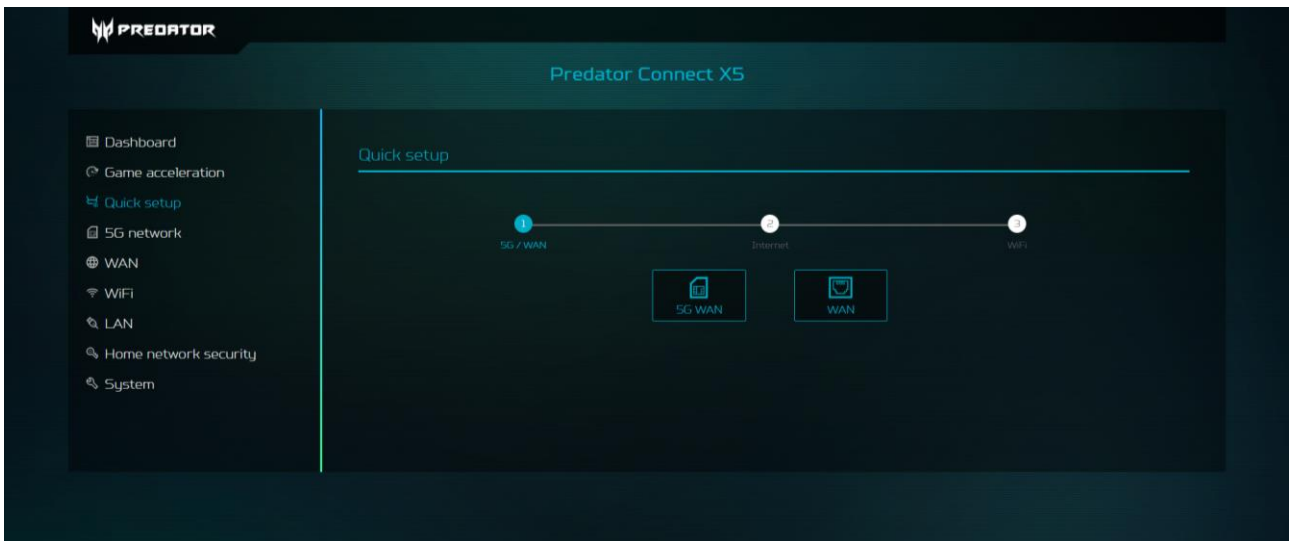
- Note: You will need to change your password at first time you login.
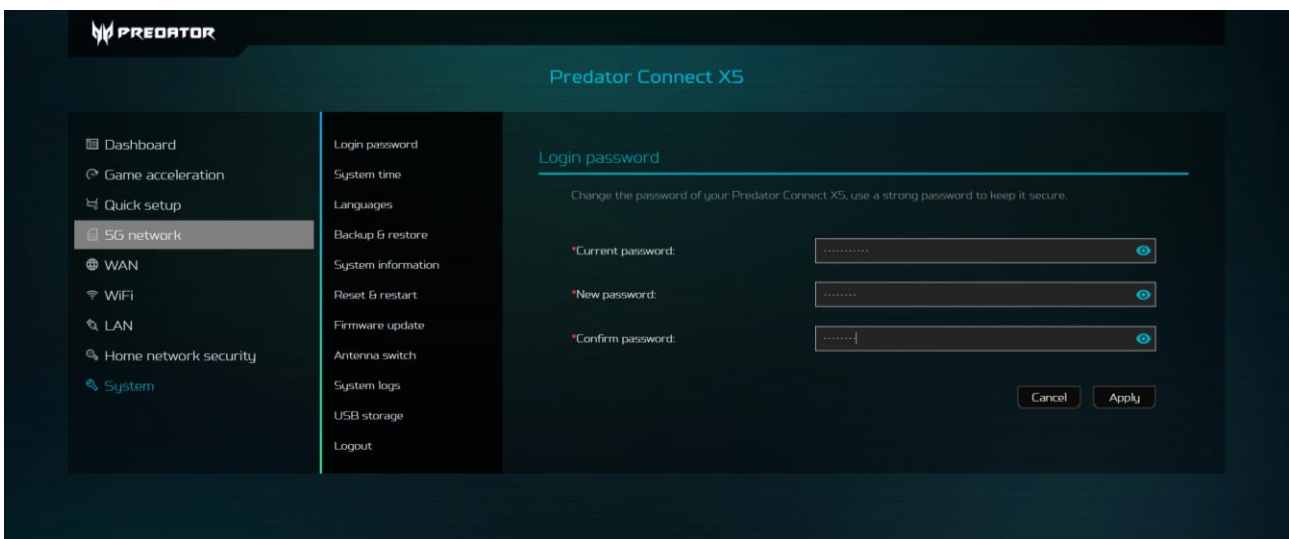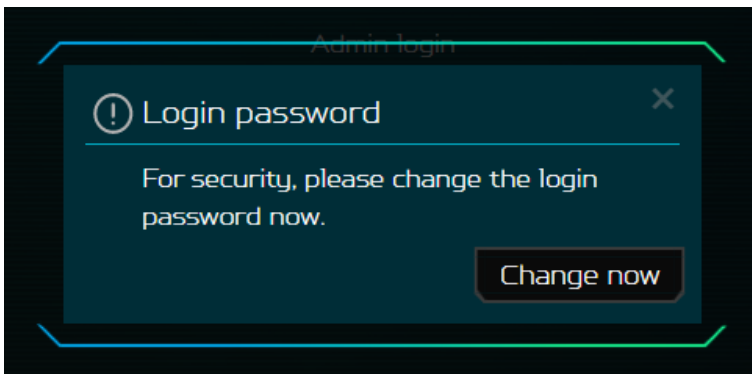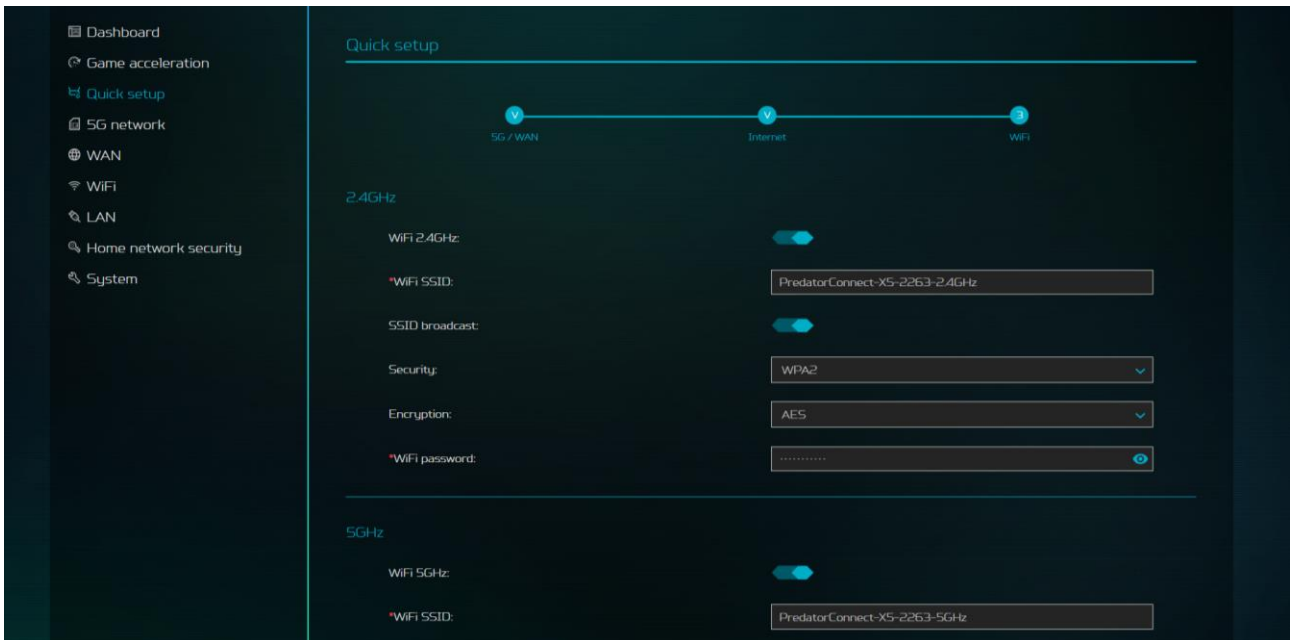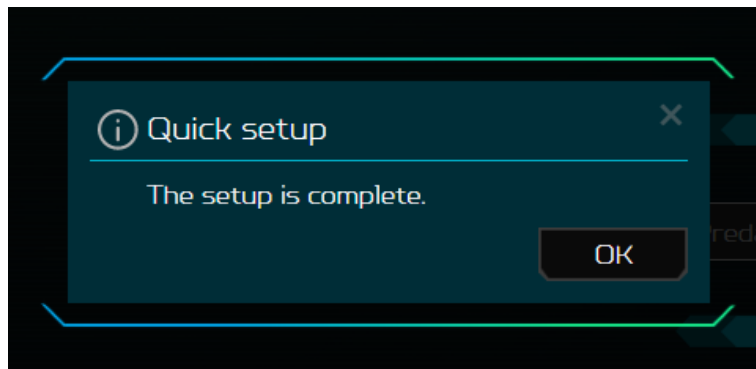
4. Quick Setup

4.1 First boot up

- You will need to proceed with your Predator Connect X5's Quick setup. This process will take only a few steps to complete. To connect to the internet. Please choose your preferred WAN to set first.
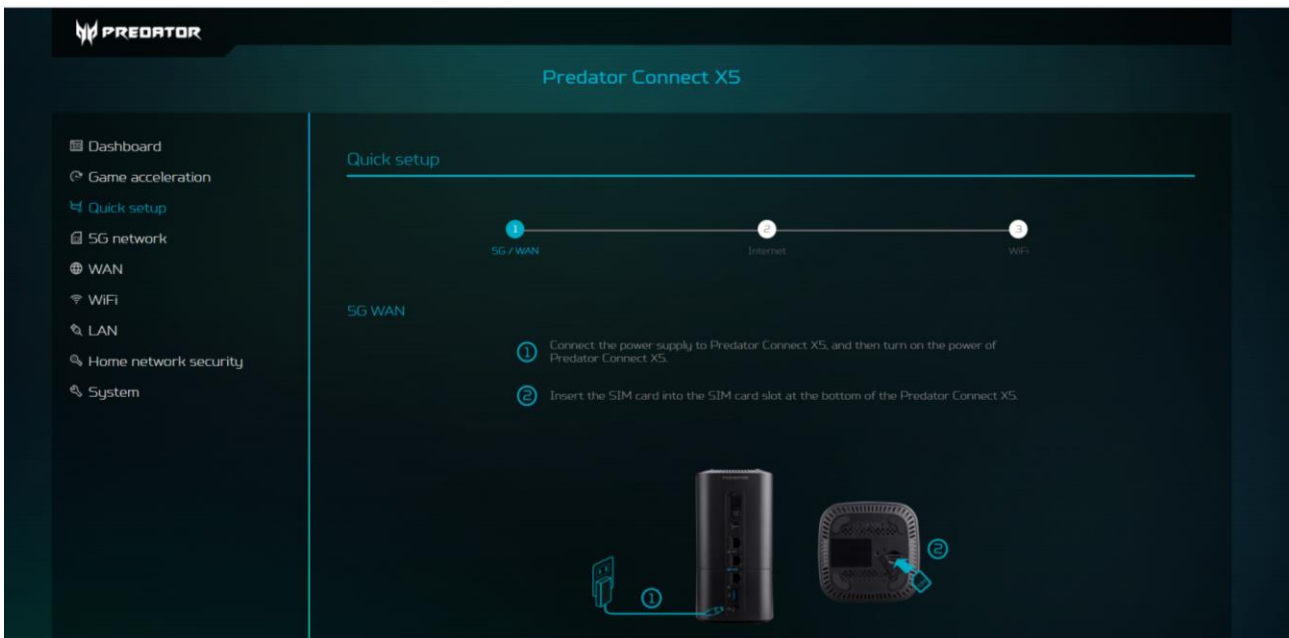
- You may modifying your WiFi SSID for both 2.4GHz and 5GHz.

4.2 Status Icons

Description	Icon displayed on Dashboard	
Signal indicator	From full signal bar to no signal	
Connection status	Disconnected	Connected
LAN status	LAN is disconnected	LAN is connected
WiFi status	WiFi is disabled	WiFi is enabled
Connected devices	Connected devices	
Data usage	Data usage	

5. Dashboard

5.1 Command Center

- The first available option on the menu tree is the Dashboard. You will also firstly arrive at The Predator Connect X5's dashboard once successfully logged in. You can check and view basic information about your device here

.
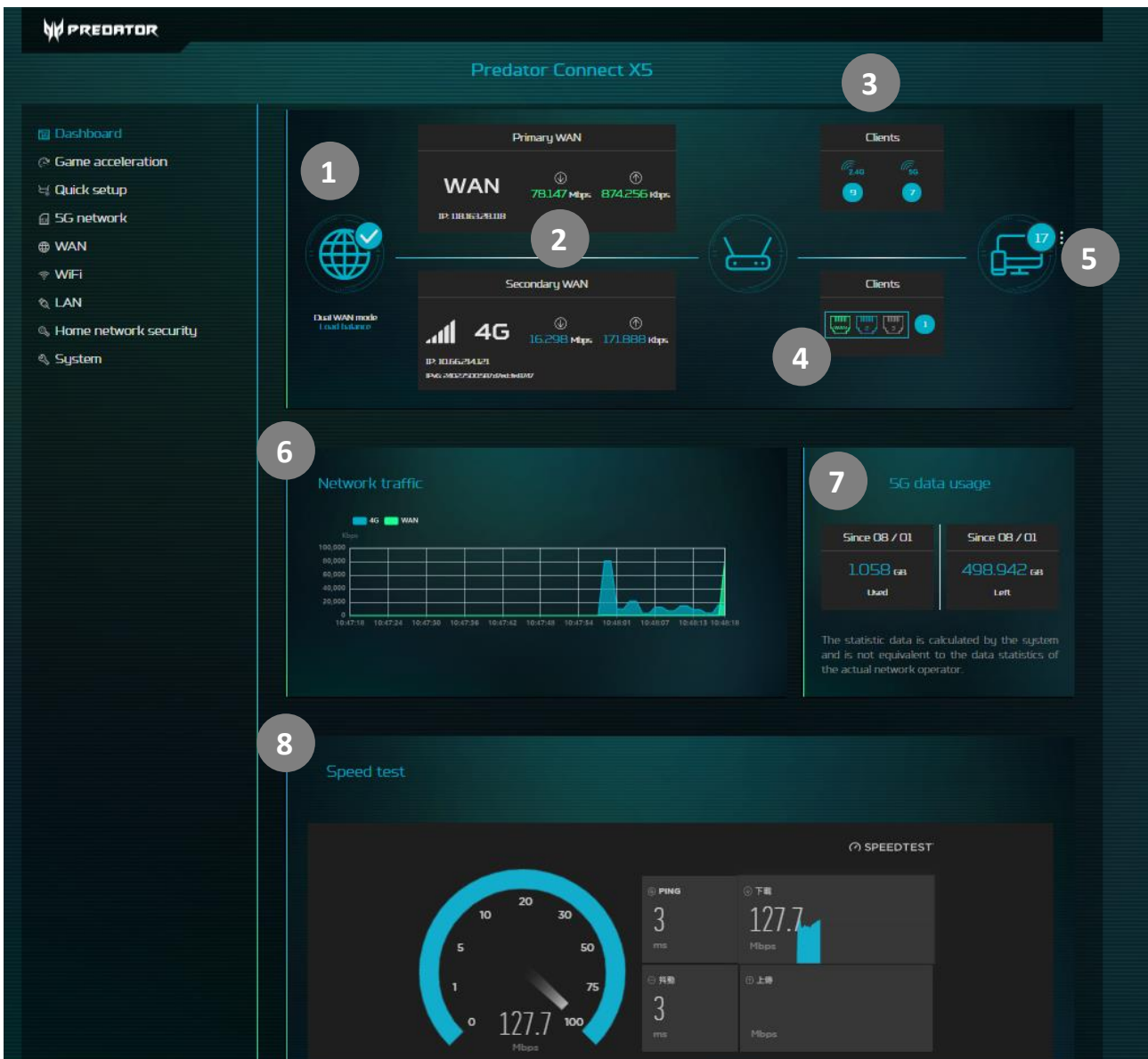
1. **Internet Status**: shows the current connection status to the internet.
2. **Dual WAN Status**: it shows dual WAN status include primary WAN and second WAN source. User can decide which of the Cellular or Ethernet WAN connection will be assigned the primary WAN or second WAN. Dual WAN supports two modes:
   A. Load balance is also a feature of Dual WAN mode. User can assign each client device to connect to internet through primary WAN or secondary WAN to make overall processing more efficient.
   B. Failover mode by default utilizes primary WAN. If the primary WAN is disconnected, the secondary WAN will switch over seamlessly.

3. **WiFi Status** quickly indicate the status of 2.4GHz and 5GHz WiFi, in easily distinguishable on-or-off indicator.
4. **LAN Status** quickly indicate the status of LAN ports 1,2, and 3. LAN1 can be set as a WAN port.
5. **Connected Devices** shows how many client devices are connected to your Predator Connect X5's WiFi or LAN.
   There is also a Device List where you further review or execute actionable tasks such as renaming or blocking devices.

-

6. **Network Traffic** help indicate real time status of the Download (DL) and Upload (UL) Speeds across the Primary and Secondary WAN.
7. **5G Data Usage** can indicate the total data used this month. User can set start date of each month.
8. **Network Speed Test** powered by OOKLA. With a single push of the "GO" button to test the speed for the Primary WAN.

6. Game Acceleration

Designed for Gaming

The Predator Connect X5 5G CPE is designed with awesome gaming capabilities to ensure you to have the best online gaming experience. Predator Connect X5 supports two types of QoS modes (Quality of Service) for game acceleration.
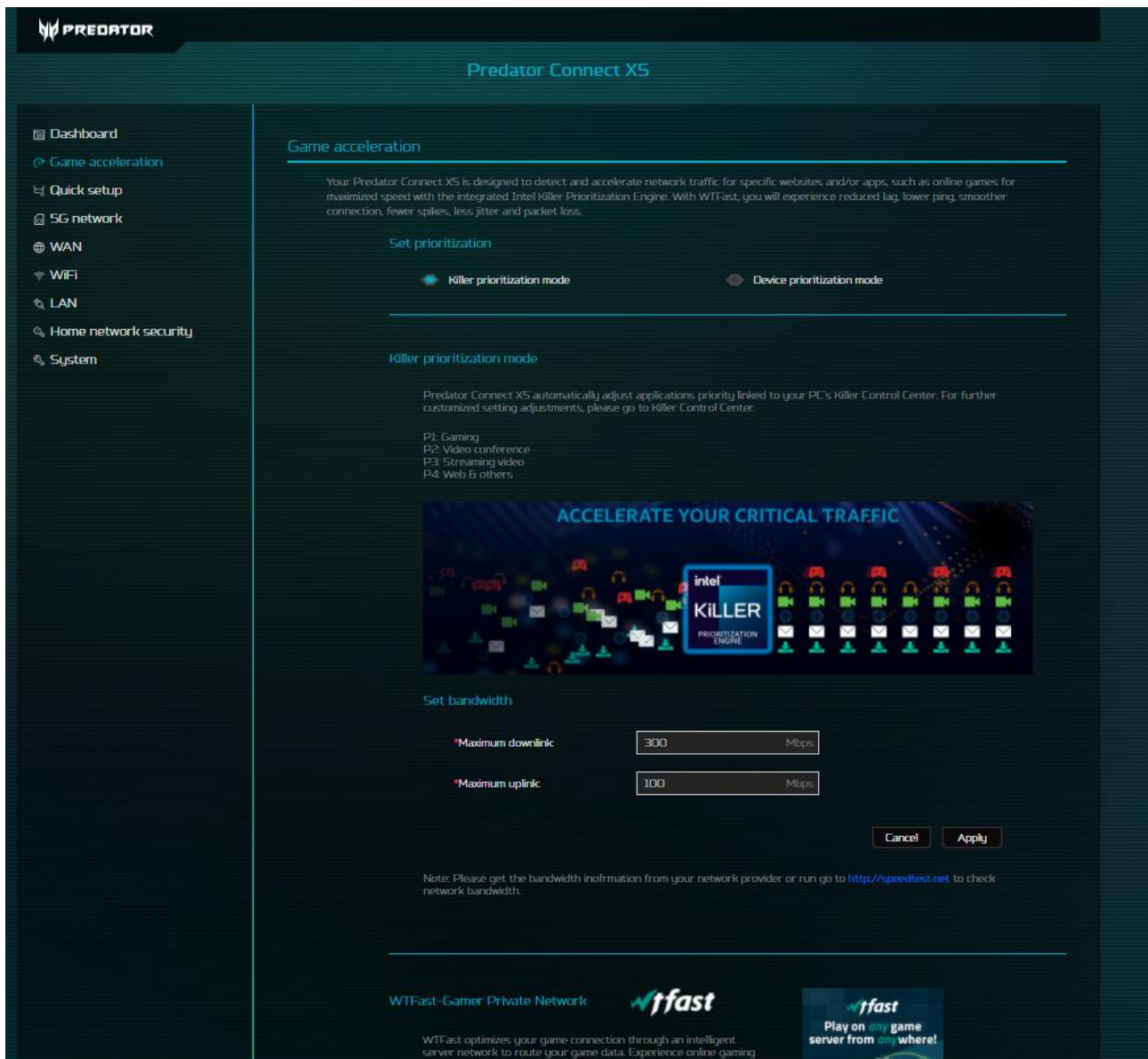
6.1 Killer prioritization mode
The Intel® Killer™ Prioritization Engine

- Offers advanced network data detection and prioritization. It offers new intelligent network capabilities that detect and accelerate network traffic for specific websites in addition to the gaming or creative applications running on your computer. By prioritizing network traffic for key websites above lower-priority websites and apps, the Intel Killer Prioritization Engine provides a more enjoyable and uninterrupted online entertainment experience. Watch a game, stream your game, play web-based games, and watch online videos all at the same time with a new level of confidence. The engine enables default prioritization automatically, but you can also customize settings and bandwidth levels. With 4 levels of prioritization, you can take full advantage of the extra network data detection capabilities that are part of the Intel Killer Prioritization Engine to get the best online experience possible on your system.

-
  Note: Please set to single WAN or Dual WAN with failover mode. Killer prioritization mode can only be used in Single WAN configuration.

  Killer prioritization mode is compatible with Killer enabled PC or devices. If your PC doesn't support killer, you can select Device Prioritization mode.

6.2 Device Prioritization Mode

- Enables you to manage priorities of the devices connected to your router. Easily and permanently set your devices as main priority to ensure your bandwidth is not throttled or affected by others.

-
  Game Port
- Devices connected to this port will always be set to high priority.
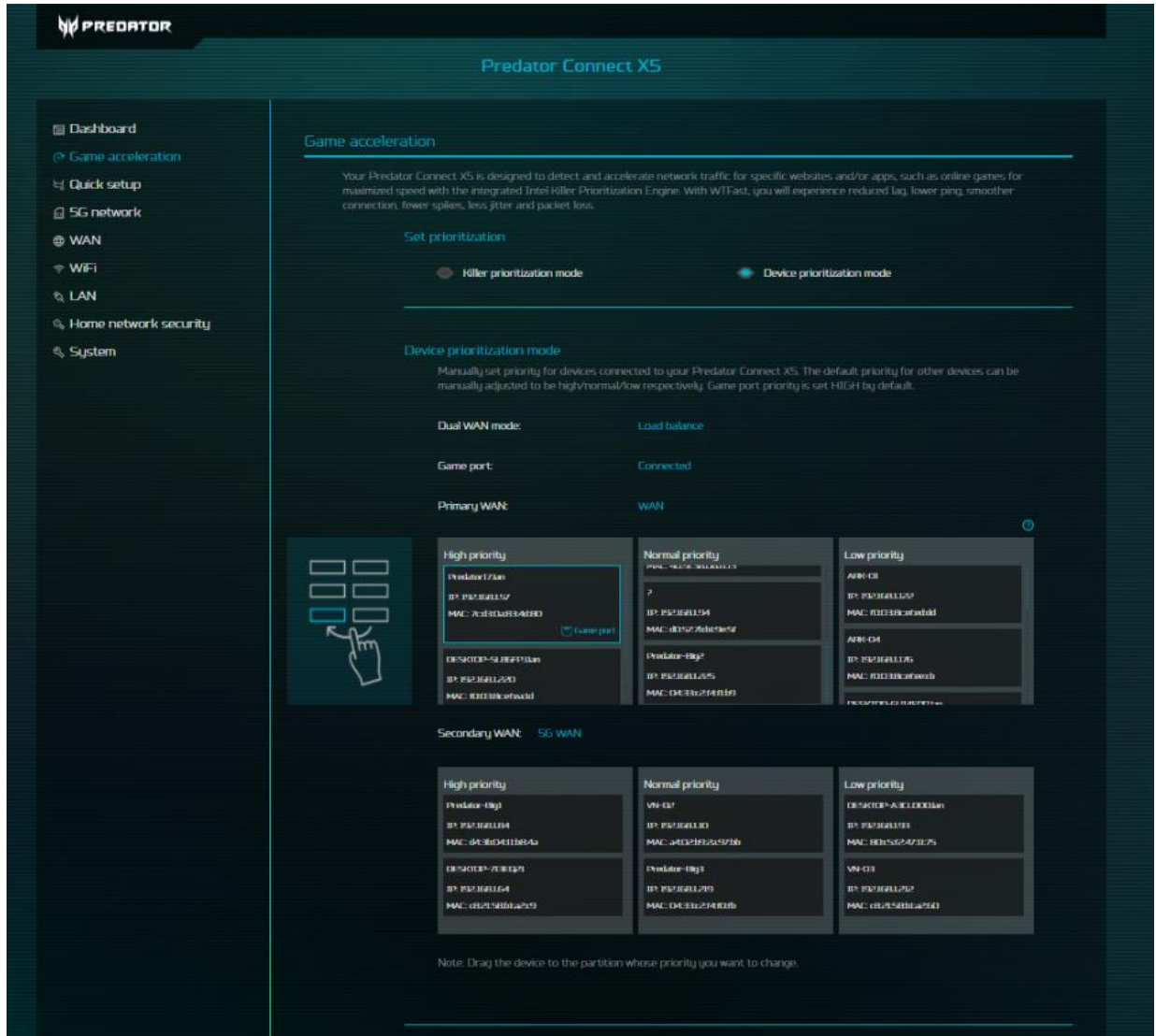
  Manual Prioritization
- Enables a finer grain control of your device priority and management within the network. Manually set priority for devices connected to your Predator Connect X5. It can be manually adjusted to be high/normal/low respectively.

Please refer to the below screen captures for routing options for your connected devices.
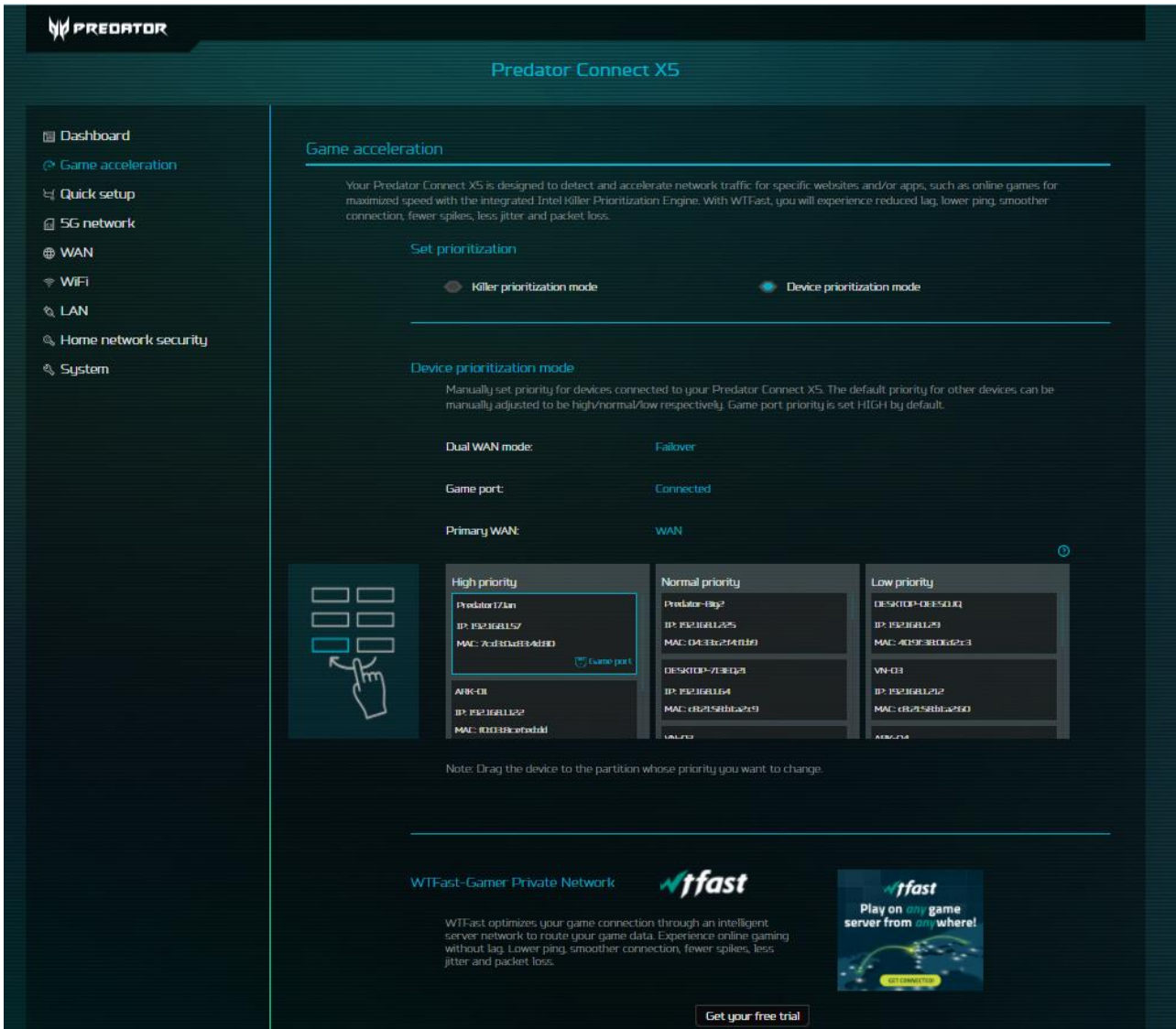
Single WAN

-

Dual WAN Mode

- **Figure. Dual WAN with Load Balance**

■   Figure. Dual WAN with Failover

Note: all client devices will set to normal priority as default. User can adjust
the preferred priority manually.

7. 5GNR / 4GLTE Cellular Network

7.1 Your 5G network status
- This section displays key fine-grain information regarding your connection status. You may find information such as connection status, network type, network name, bands, IP address and more. Furthermore, you may even disconnect by pressing the disconnect button
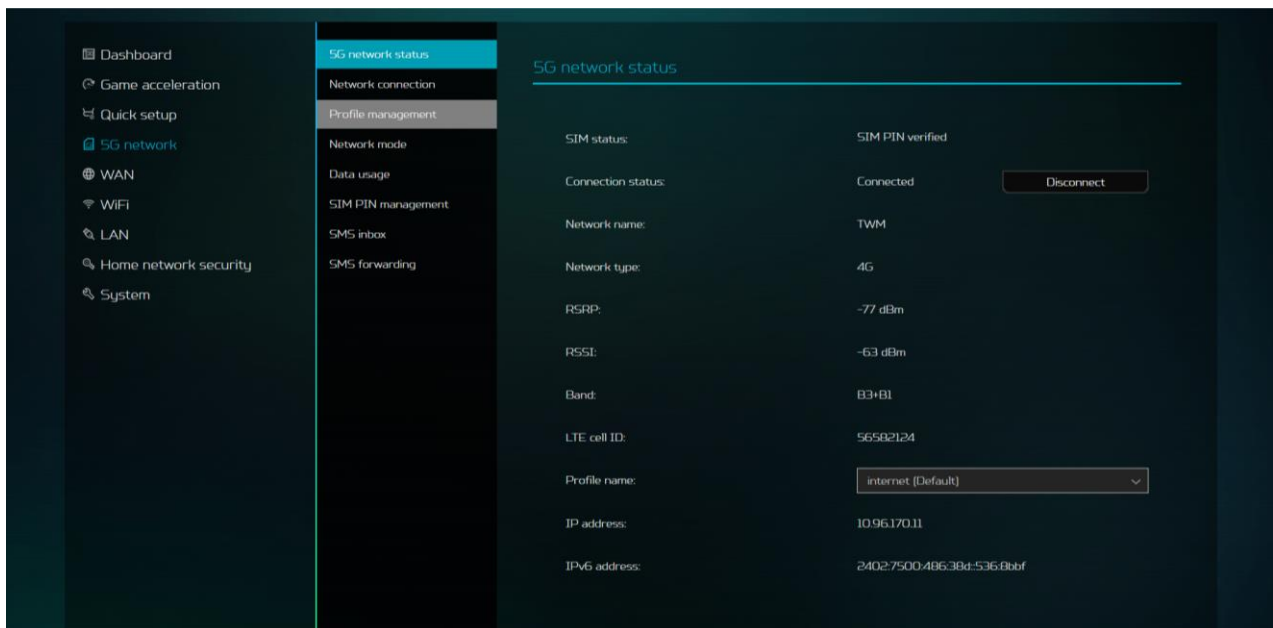
7.2 Network Connection modes
- Can be selectable between Auto and Manual.
- Auto : Every time router boot up, the router will connect to the 4G/5G network automatically by default.
- Manual : Every time router boot up, user is required to press "Connect" button to connect to the 4G/5G network.
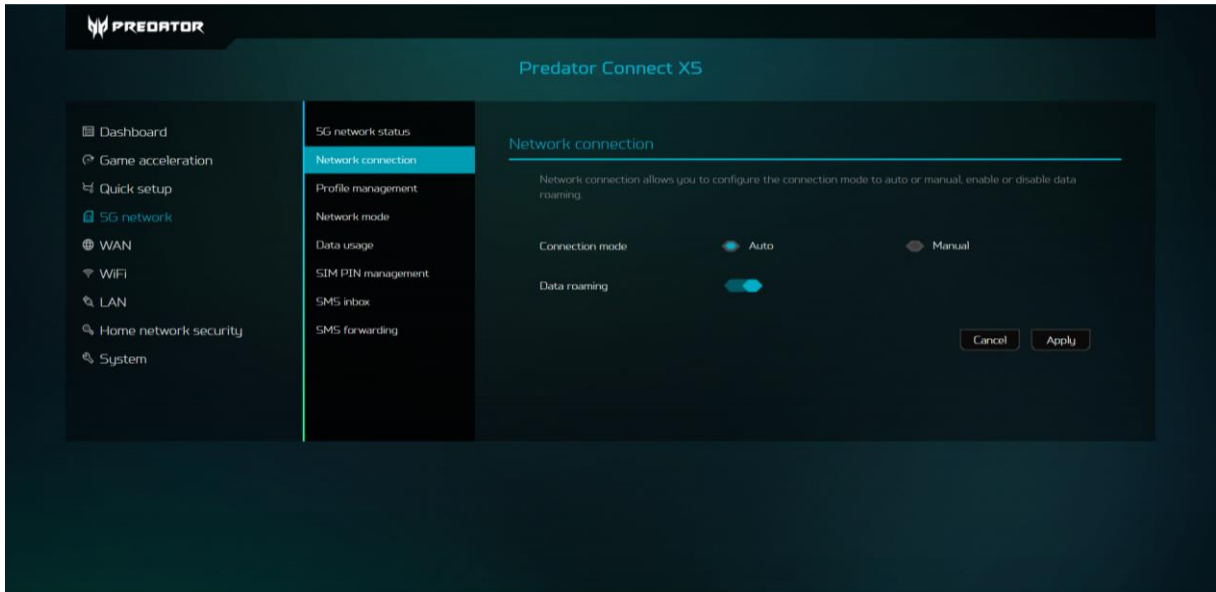
7.3 Data Roaming

*   Occurs whenever your device disconnects from your carrier's network and hops on another network. This functionality is by default disabled. Data Roaming can be turned on by navigating to the 5G

7.4 Profile Management

*   Predator Connect X5 will detect your SIM and set APN(Access Point Name) for 4G/5G data connection as the default configuration. But some carriers maybe not be automatically configured by Predator Connect X5. In those cases, user need to manually create a new profile and setup the SIM's APN.
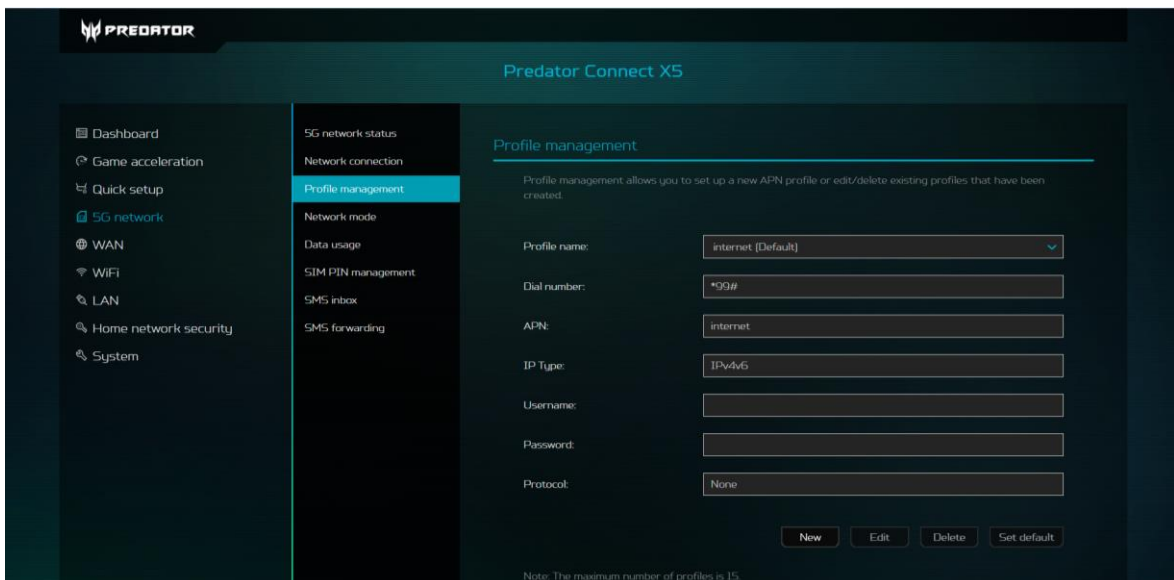
7.5 Network search mode

*   Network search can be set to Auto or Manual.
*   There are 4 network modes that can be selected.
*   1. 5G NSA -> 4G
*   2. 5G SA -> 5G NSA -> 4G

- 3. 5G SA only
- 4. 4G only
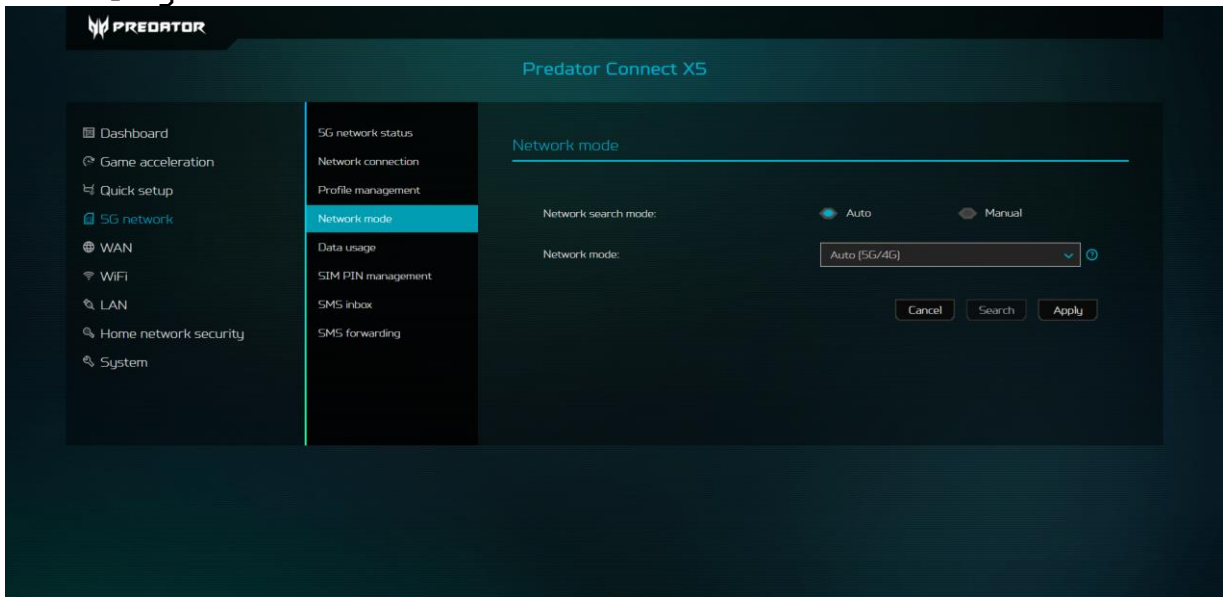
7.6 Data usage

- Enables you to understand how you are using your data. You can designate the start date for each month, limitation, and even data limit warnings.

  Note: The data limitation is base on your data plan and network operator. The router will not limit data usage. Please contact your data plan provider for more details about your data plan and how it may affect your online experience.
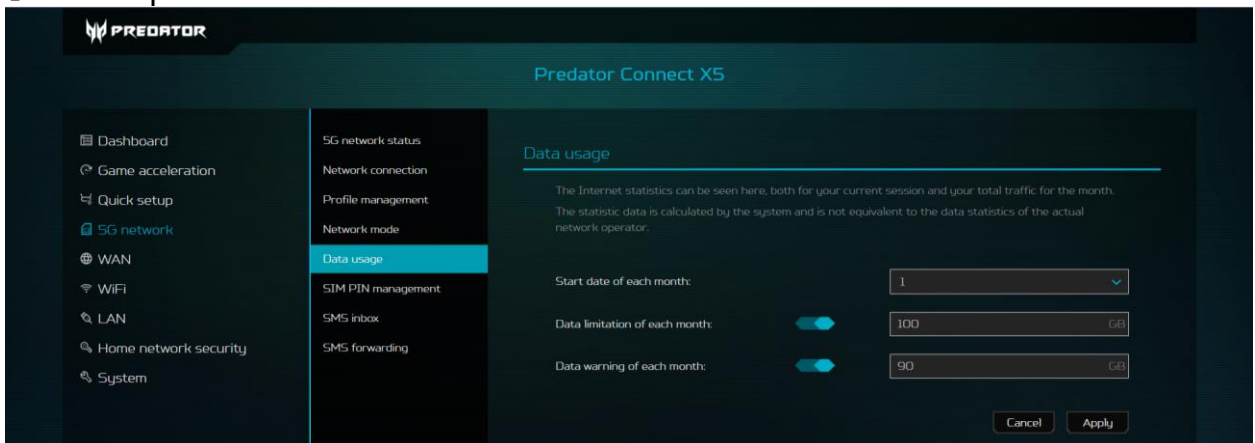
There will be statistical chart that will be available where as you will be able to set your data period and also how your view your data. Please note that 3 months is the limit for the stored data consumption.

7.7 SIM PIN Management.

- SIM PIN is a password used to control the rights of using a SIM card, and prevent unauthorized users from using it. You may also change the SIM PIN by clicking the Change SIM PIN button. Do note that if you fail to enter the correct SIM PIN code 3 times in succession, the SIM card will be locked. You can unlocked the SIM card by entering the PUK code. If you do not have the PUK Code, please contact your 5G / 4G cellular provider. Please be advised, if you fail to enter the correct PUK code 10 times in succession, the SIM card will be locked permanently.
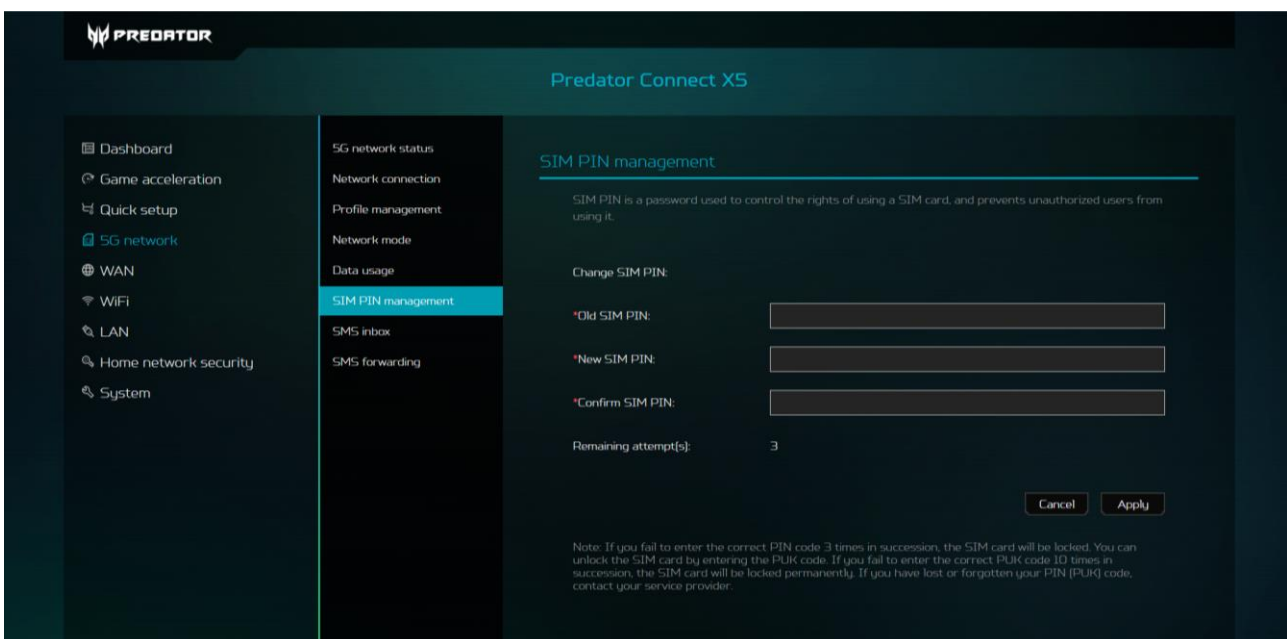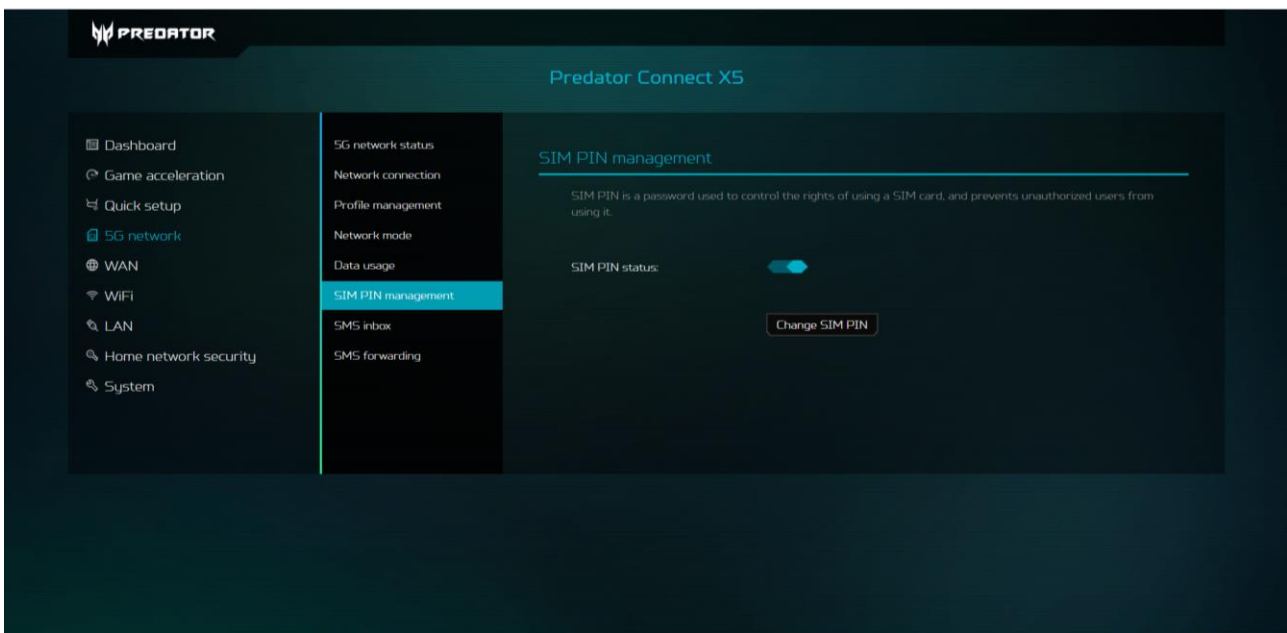
Note: if user enables SIM PIN. The router will not connect to 4G/5G network automatically until user enter PIN code when every time router boot up.

7.8 SIM Inbox
- Allows you to view SMS messages that is received in the installed SIM card of your Predator Connect X5. You are able to individually delete unwanted SMS from here.
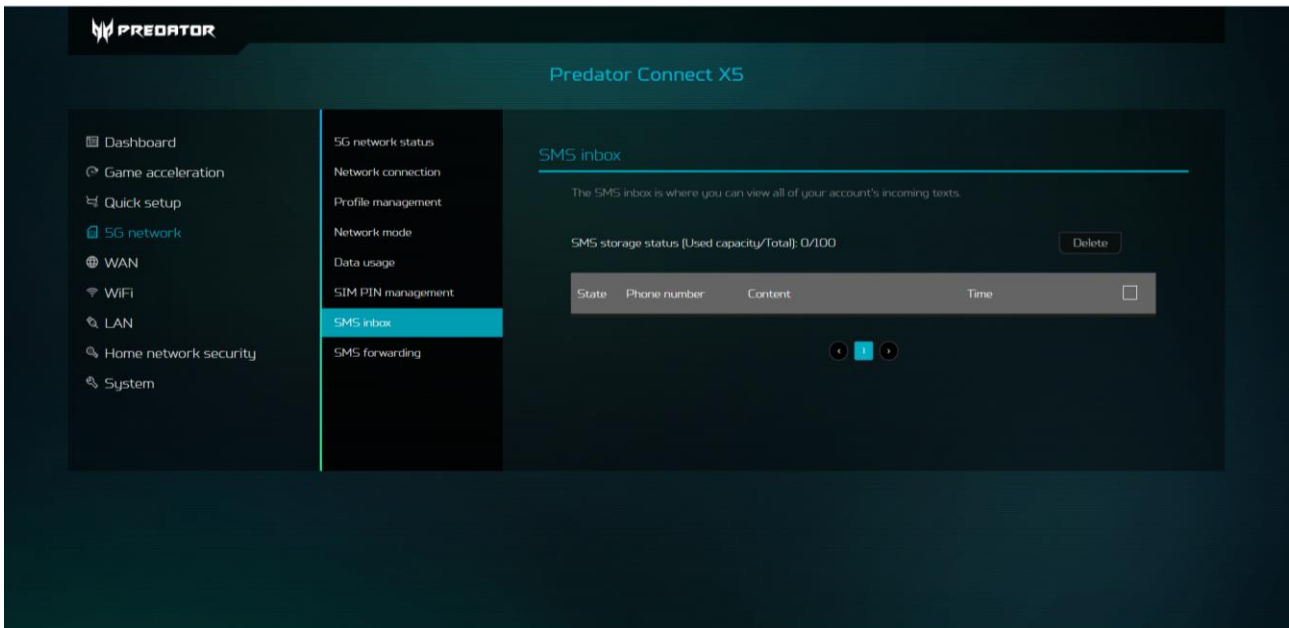
7.9 SMS Forwarding function
- Allows SMS messages that is received by the installed SIM card of your Predator Connect X5 to be forward to another phone number; such as the phone number of your personal Smartphone.

7.10 Reading SMS
A. Left-click the content of the message you wish to read.
B. You may delete your SMS messages by clicking the delete button.
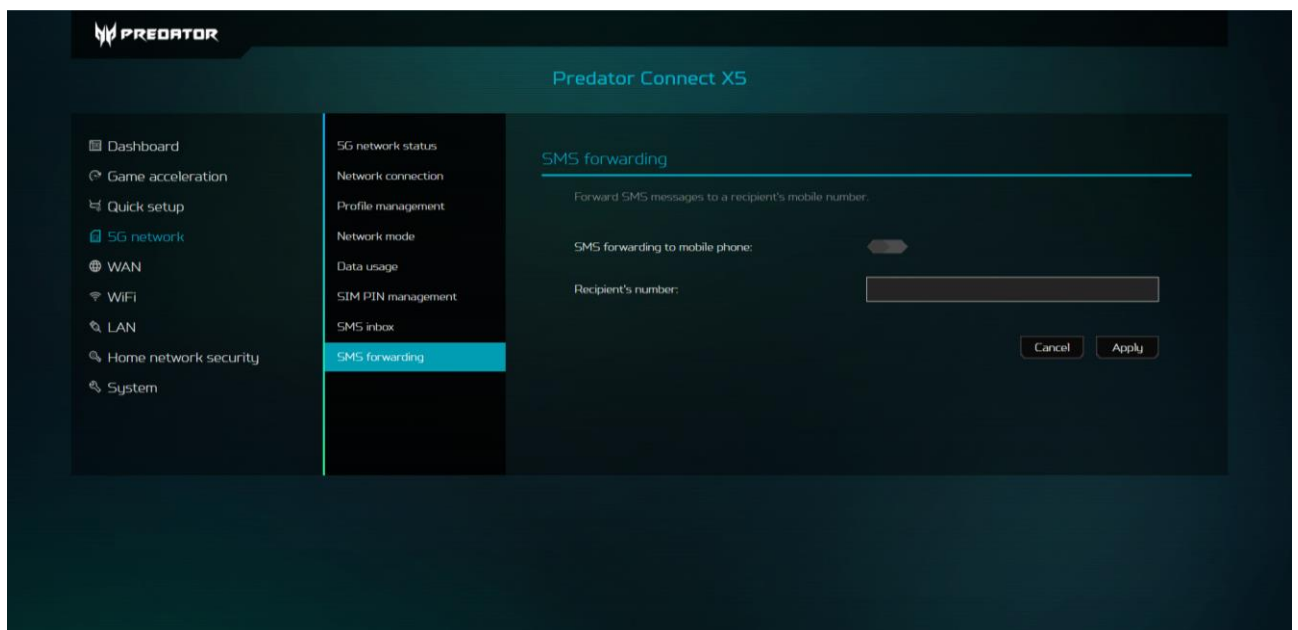
8. WAN

8.1 WAN Status.

- Displays the different operating status regarding the functions and features of your Predator Connect X5's WAN capabilities.
  - A. Duration
  - B. Connection Status: displays Connected or Disconnected
  - C. MAC address
  - D. Connection Mode: DHCP, Static IP, PPPoE, and Switch WAN port to LAN1. You may change the connection mode in WAN Setting.
  - E. IP address
  - F. Subnet mask
  - G. Default gateway
  - H. Primary DNS sever
  - I. Secondary DNS server
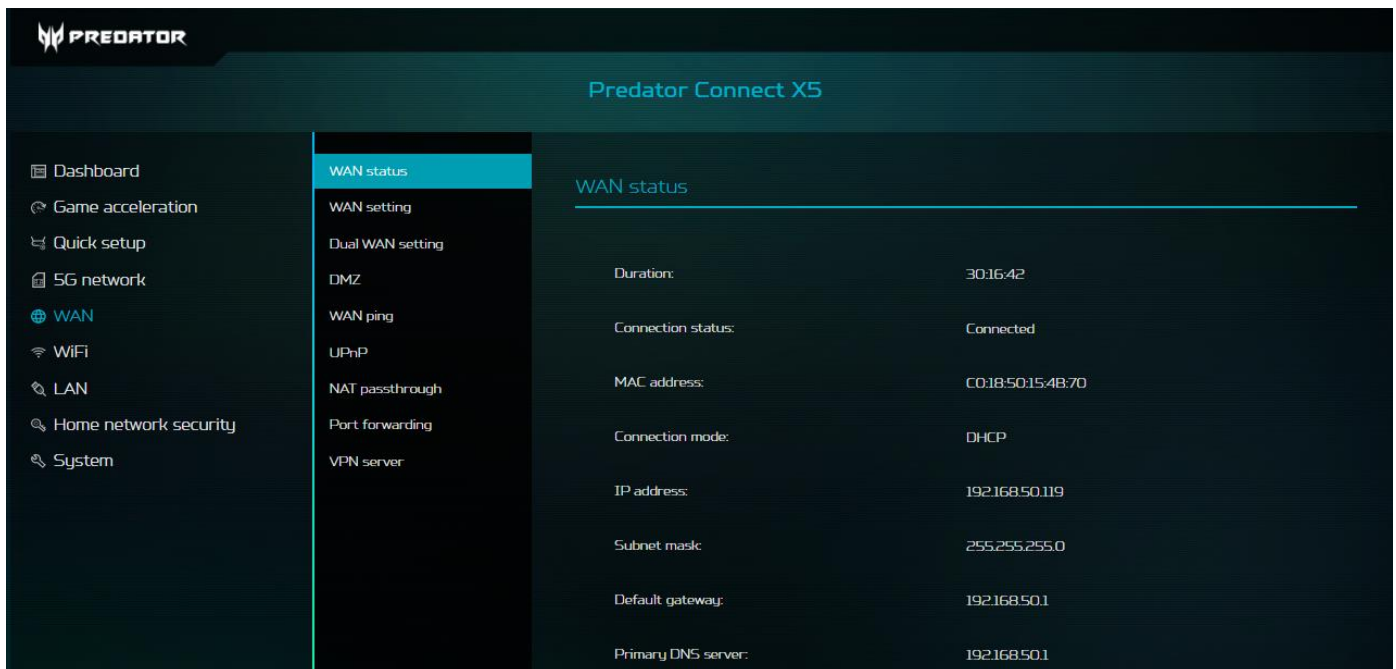
8.2 WAN Setting
* Set Ethernet WAN connection mode. It can be dynamic IP static IP, or PPPoE. It is possible to set this port as LAN port. Just use the down arrow to reveal the drop down menu to select your preferred WAN setting.
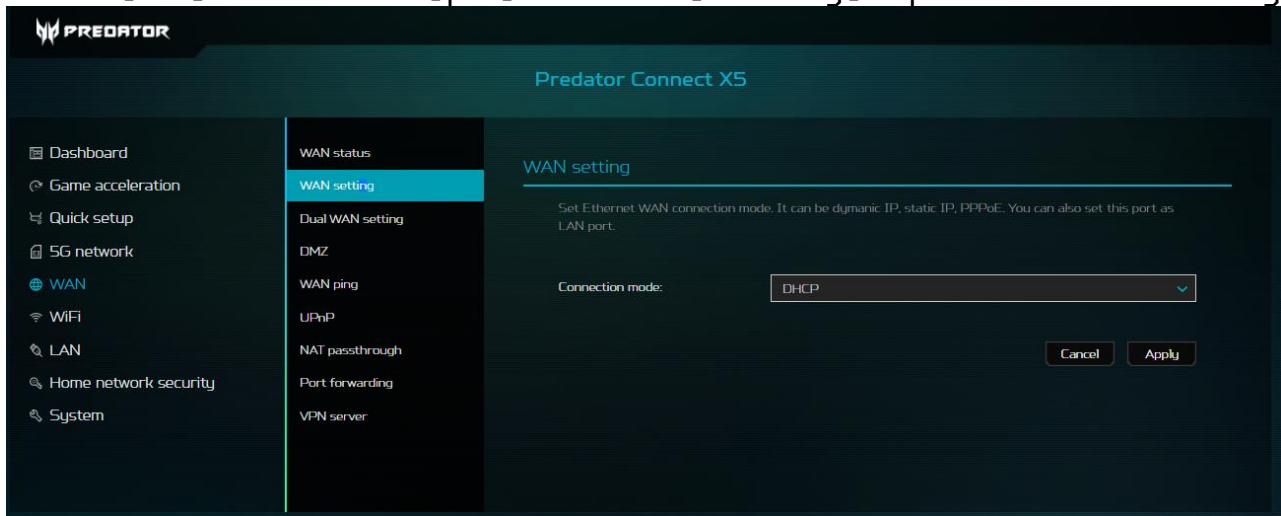
8.3 Dual WAN Setting
* Predator Connect X5 has two WAN connections, 5G NR and Ethernet WAN. User can select primary WAN and secondary WAN. User can also select dual WAN mode with failover or load balance function applied.
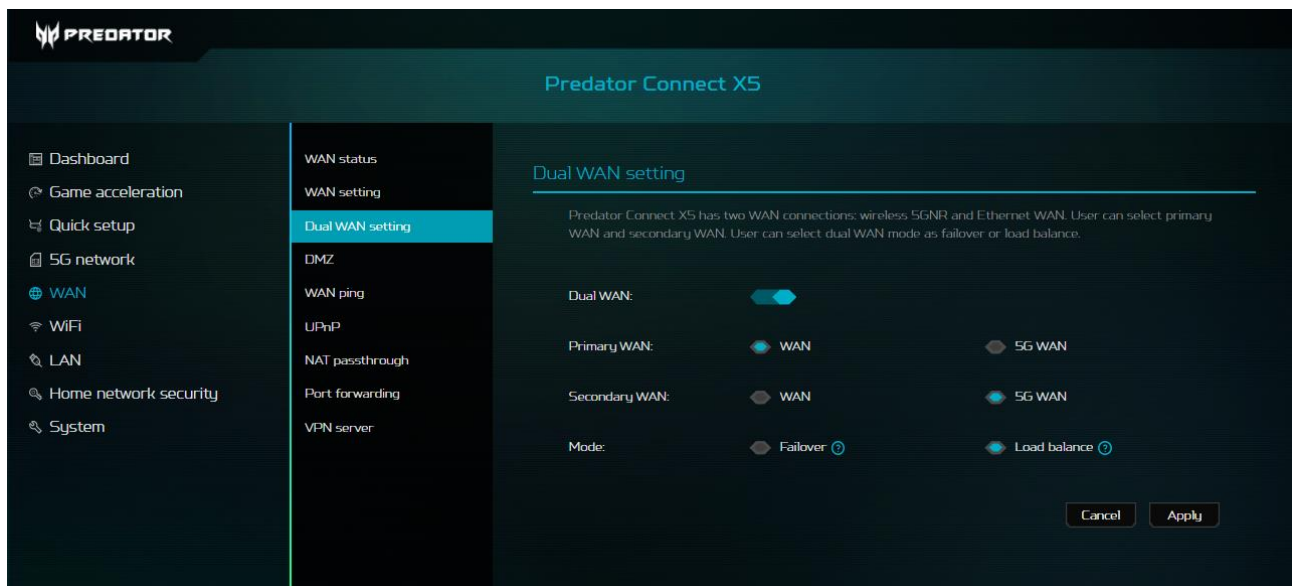
8.4 DMZ

- If external users can't access certain network services provided by the Local Area Network (LAN), use the DMZ function to set the client that provides the required network services as the DMZ host. External users will then have access to all the services. Note that clients in the DMZ will be exposed to WAN traffic. Apply DMZ host IP address in the provided field and click "apply" to instate the function.
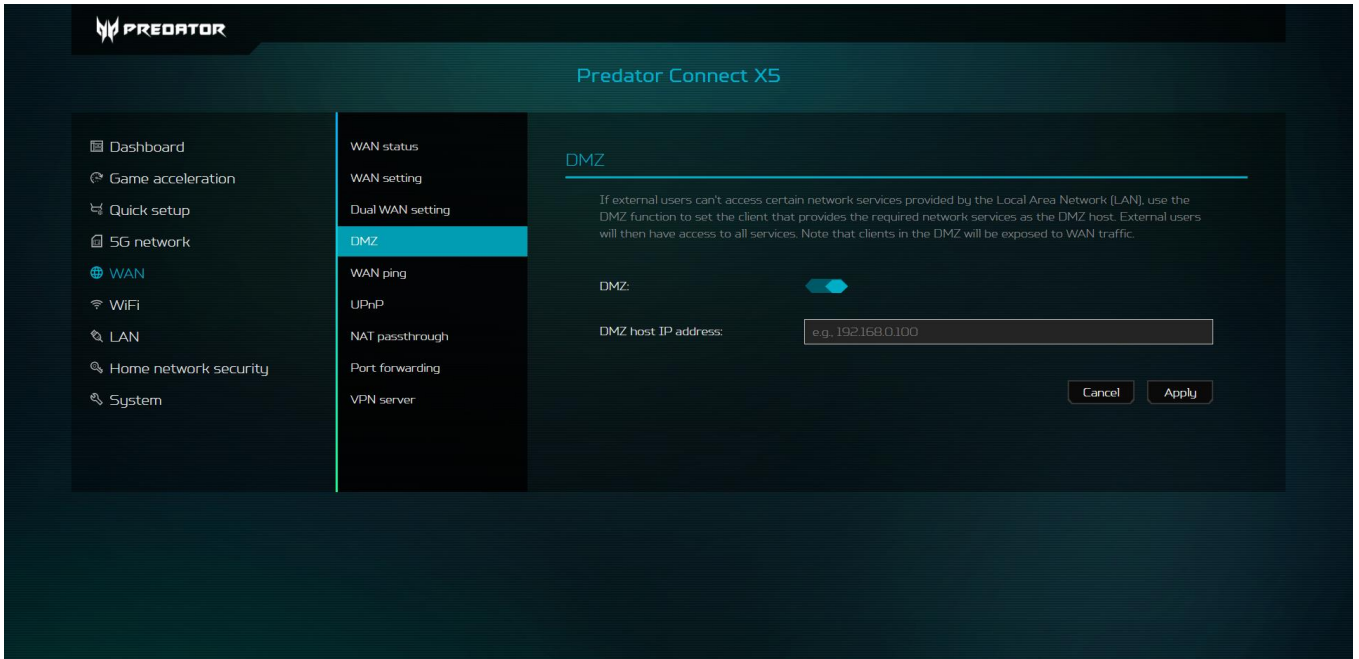
8.5 WAN Ping

- The WAN port of Predator Connect X5 will respond to ping requests from the Internet that are sent to the WAN IP address. By switching WAN port ping, your device will respond to ping. For improved security, switch off the WAN ping when not in use.
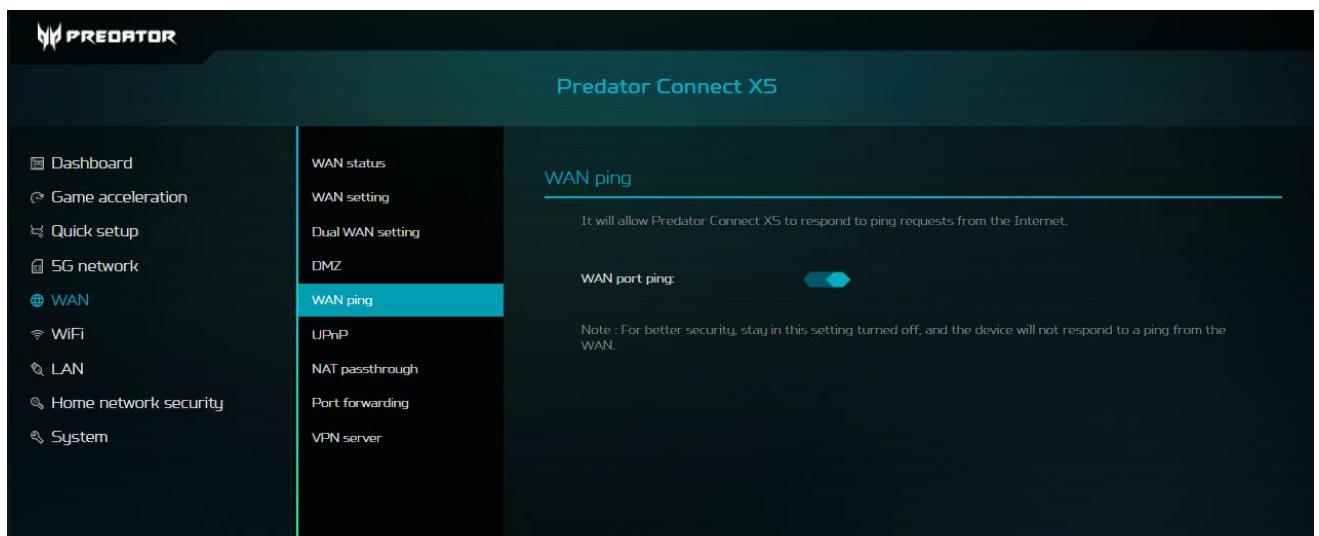
8.6 UPnP

- Also known as Universal Plug and Play, is a set of networking protocol that permits devices connected to your Predator Connect X5 to discover each other and establish functional network services for data sharing, communications, and entertainment.
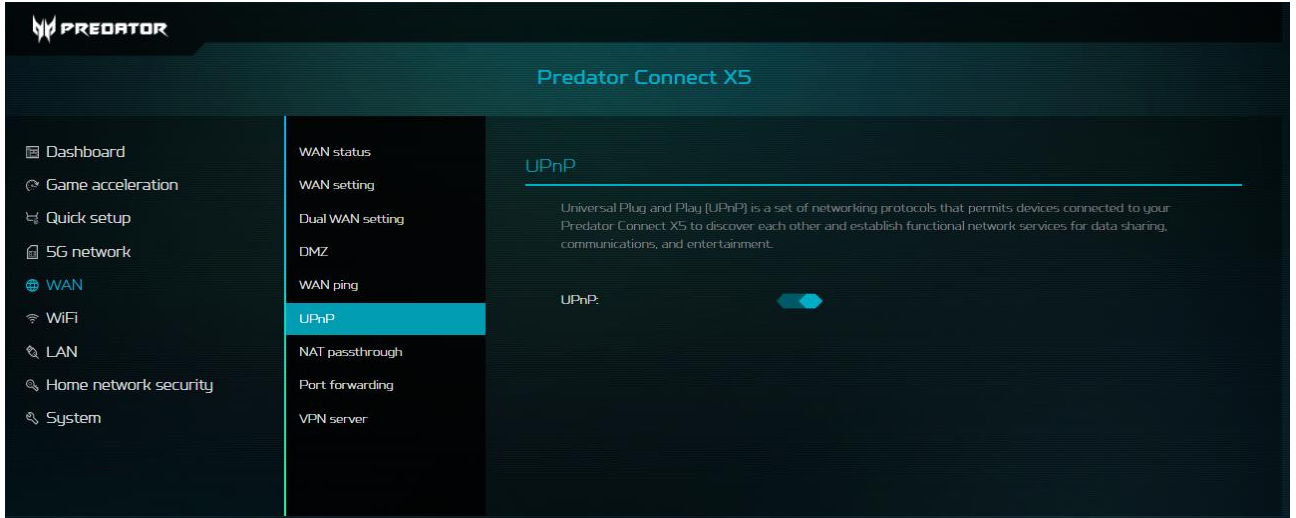
8.7 NAT Passthrough

- Allows a VPN, or virtual private network connection to pass through the router to the network client(s).
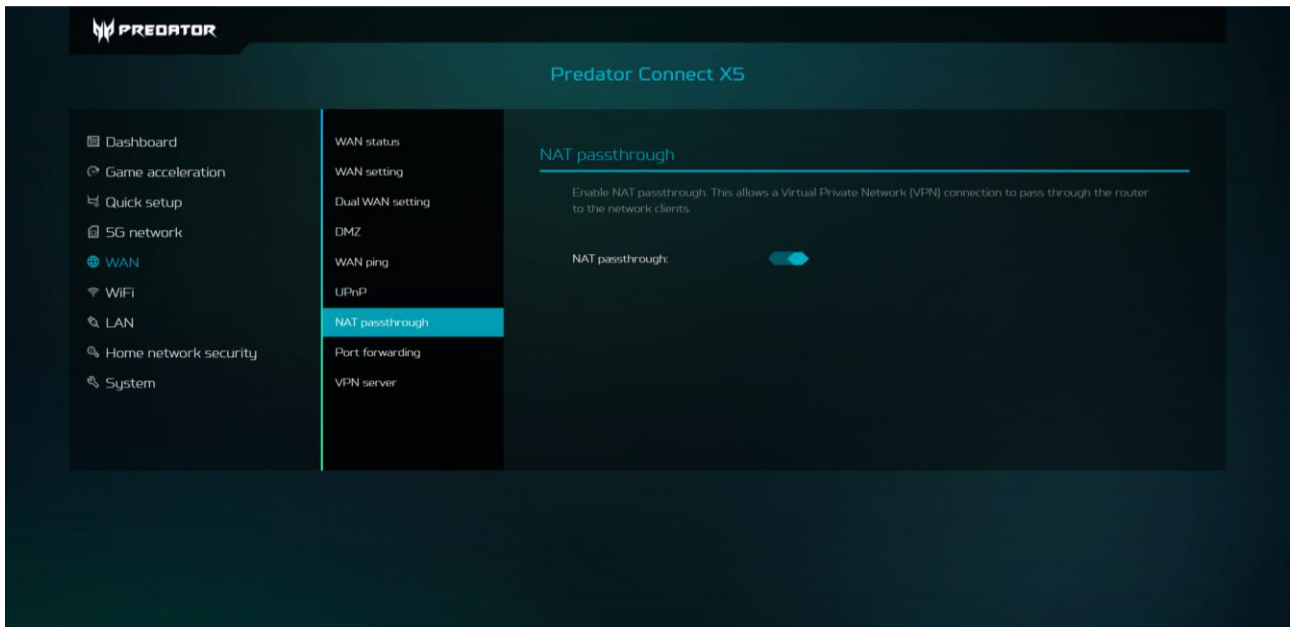
8.8 Port forwarding

- This feature allows external users to connect to Local Area Network (LAN) services using Hypertext Transfer Protocol (HTTP), File Transfer Protocols (FTP), and other protocols.
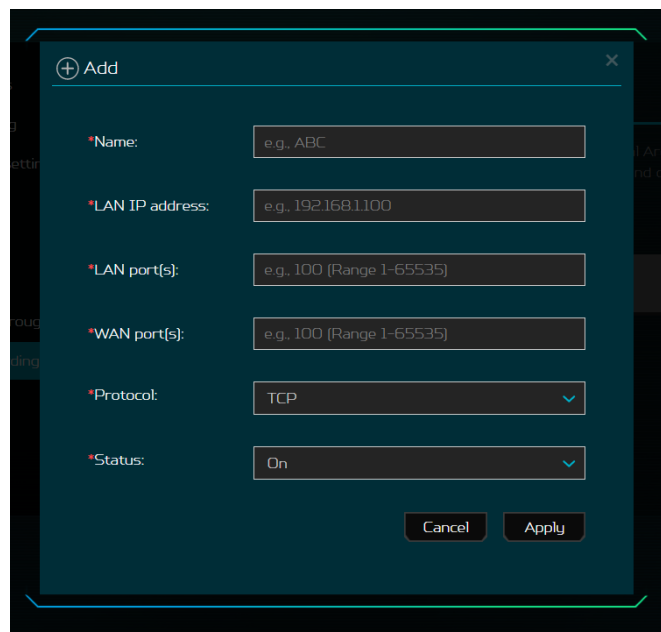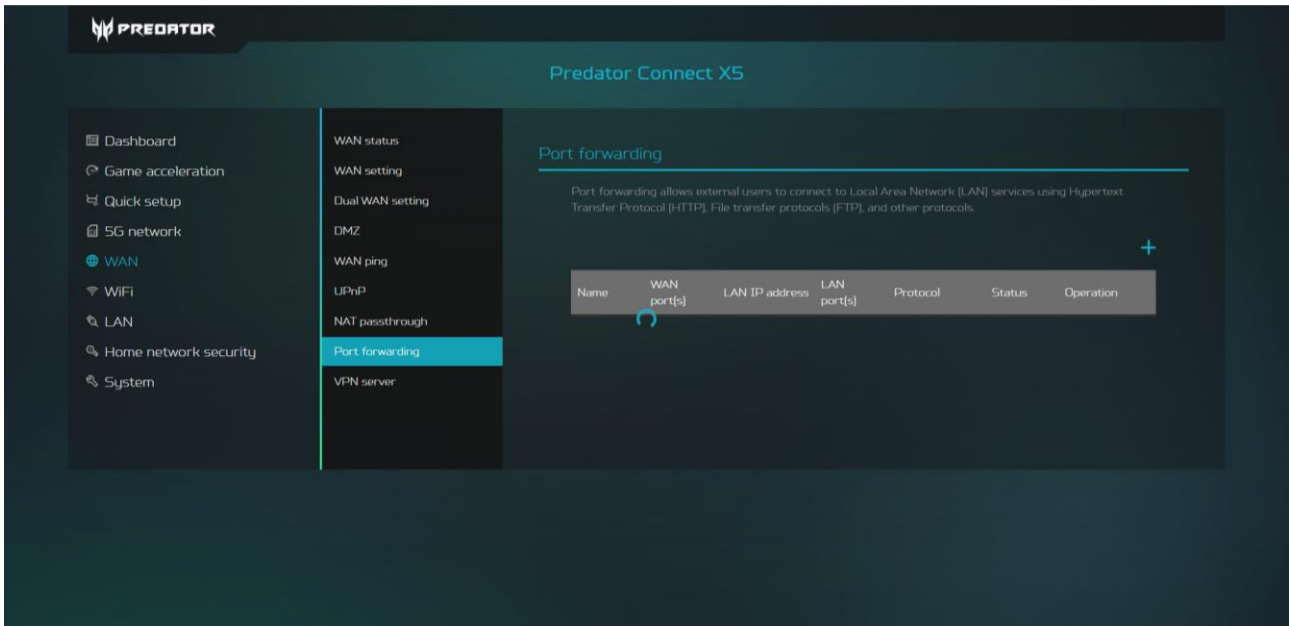
8.9 VPN server

• Setup VPN server on Predator Connect X5 for remote VPN connection from the internet. By switching on this function, further adjust your requirement by selecting between UDP and TCP. Designate Service port, VPN subnet, VPN netmask. Further client access control can be created by limiting user to Hone network only, or Internet and home network. You may export your configuration file and also generate new certificates.
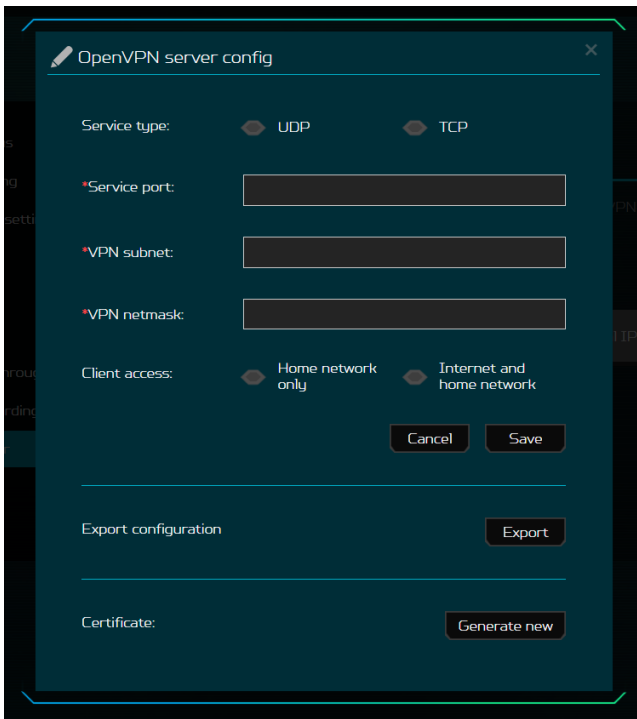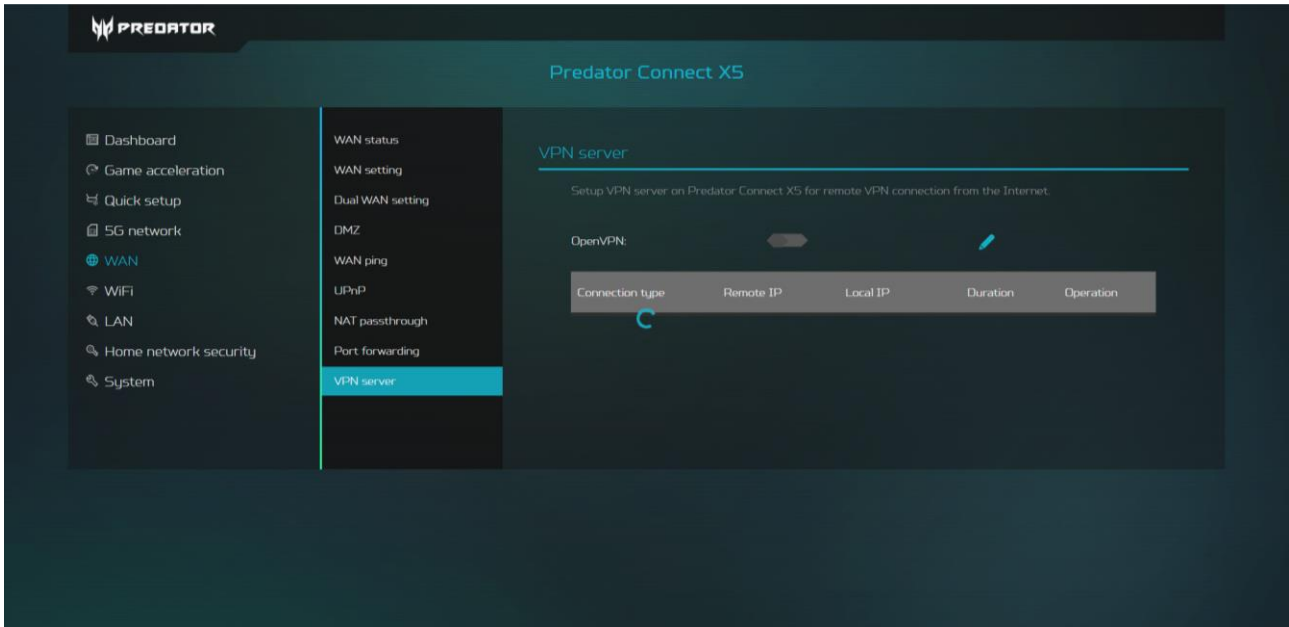
9. WiFi

9.1 WiFi Status

- Displays key information such as WiFi SSID, Security, Connected devices, Gateway address, and Mac address. You can freely change your WiFi SSID for both 2.4GHz and 5GHz bands.
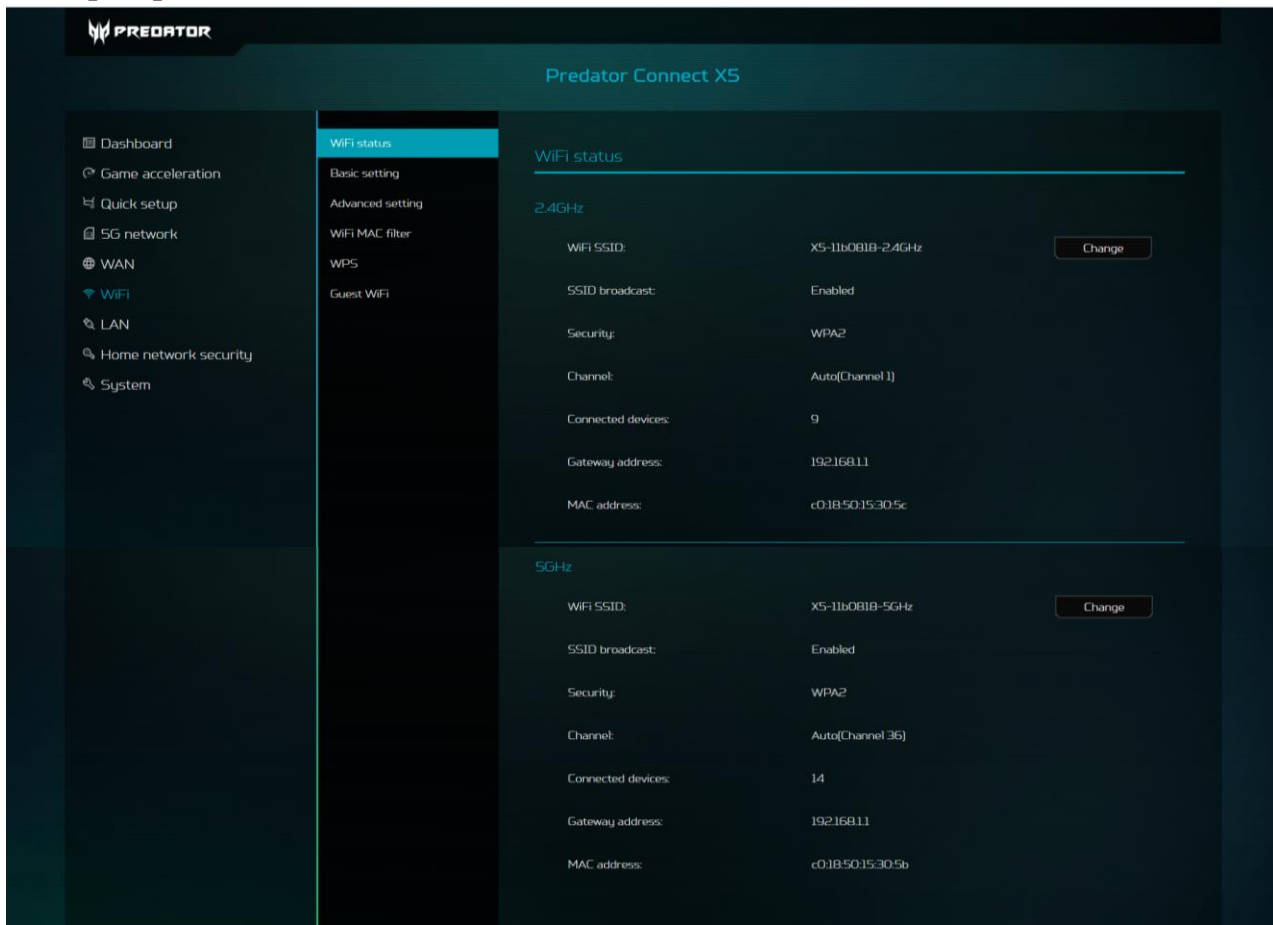
9.2 Basic Setting

- Displays key information such as WiFi SSID, Security, Connected devices, Gateway address, and Mac address. You can freely change your WiFi SSID for both 2.4GHz and 5GHz bands.
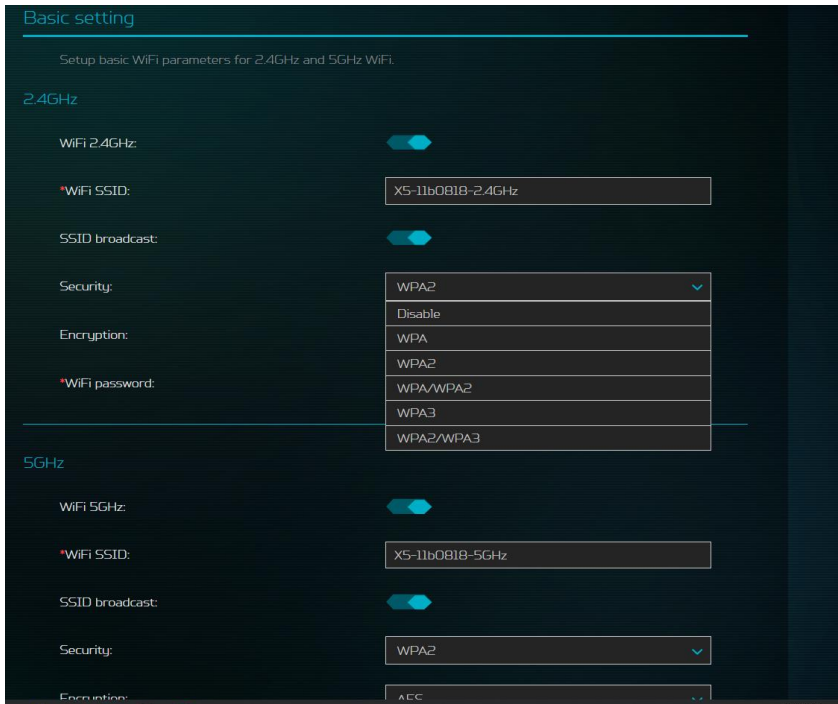
When changing the SSID name, there will be additional options made available for modification. Such as in the security field. You may be able to disable, or use the following security functions: WPA, WPA2, WPA/WPA2, WPA3, and WPA2/WPA3.
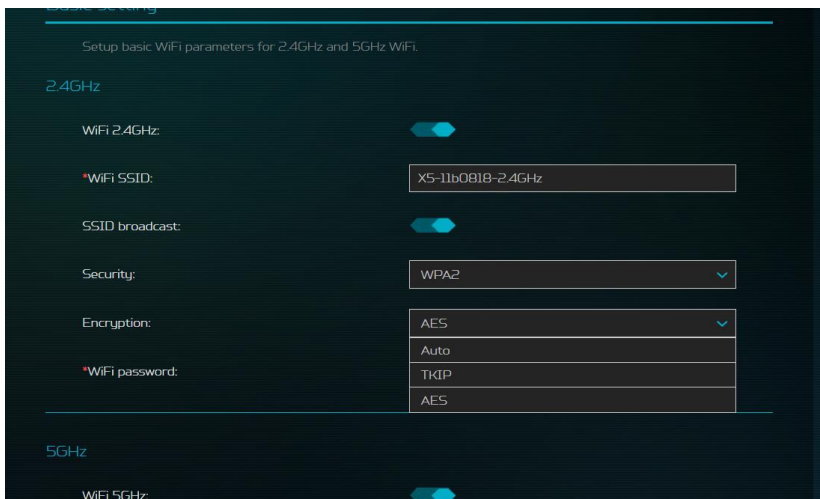
- Encryption options are AES, Auto, and TKIP.

9.3 Advance Settings

- When you first click the Advance setting button, you will be presented with a warning. It is important to note that any changes in the advanced setting could affect your connection and overall experience using the Predator Connect X5 5G CPE.
- Please click OK if you are sure to proceed to adjusting parameters within the advanced settings submenu.
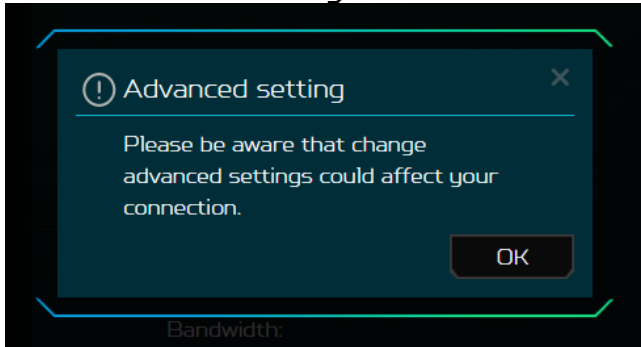
- When you arrive at the Advanced Setting submenu, you will be provided various options to configure which channels you would like to be in, your 802.11 modes, AP isolation, and lastly configure what bandwidth you would prefer.
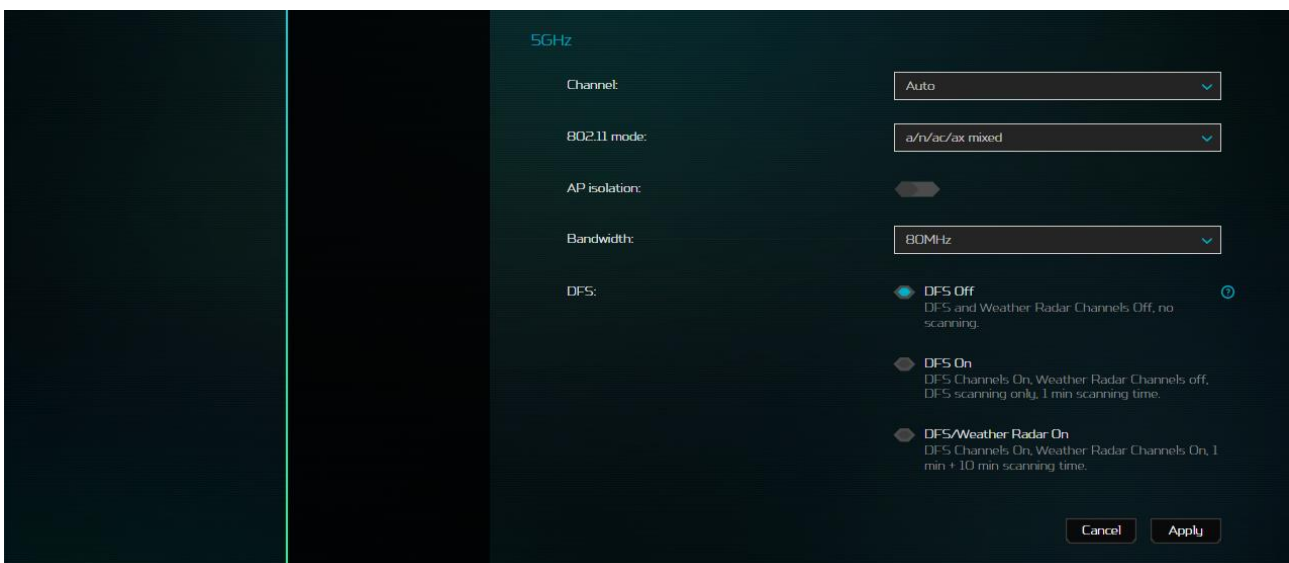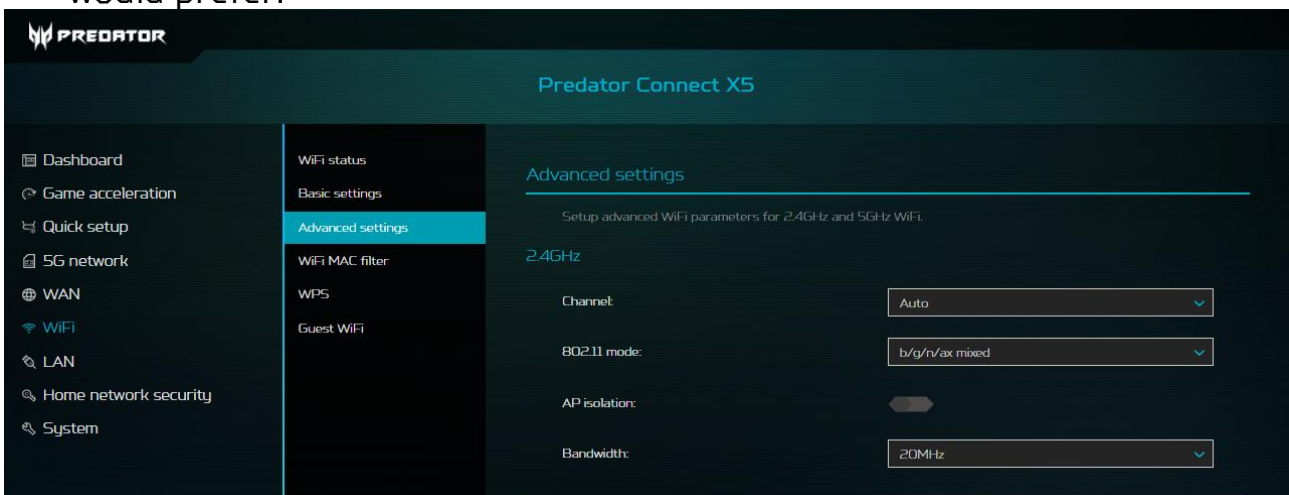
- After you have configured your custom selections, please click apply.

9.4 WiFi MAC filter

- Devices will be blocked from accessing the Internet once they are added in the MAC filter list. Up to 32 devices can be added to this list.
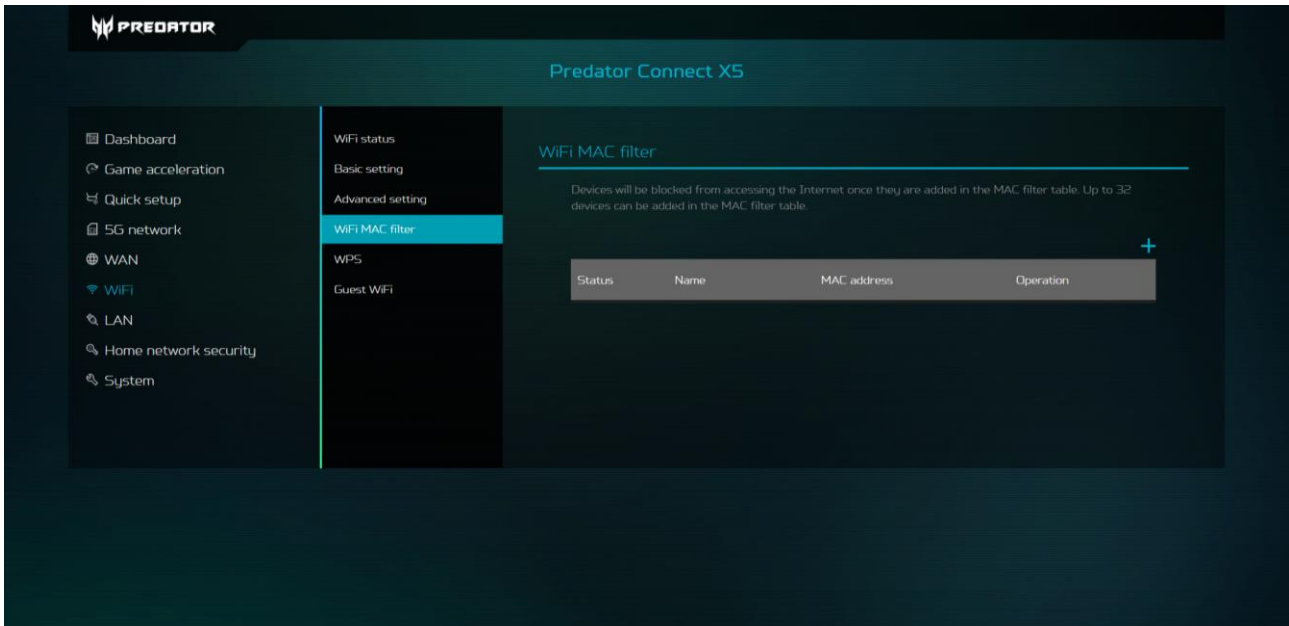
- When you have completed inputting the name and MAC address you would like to filter, please click apply.

9.5 WPS

- WPS or WiFi Protected Setup provides an easy way to connect your device to the network via pushing the WPS button or entering a PIN code.
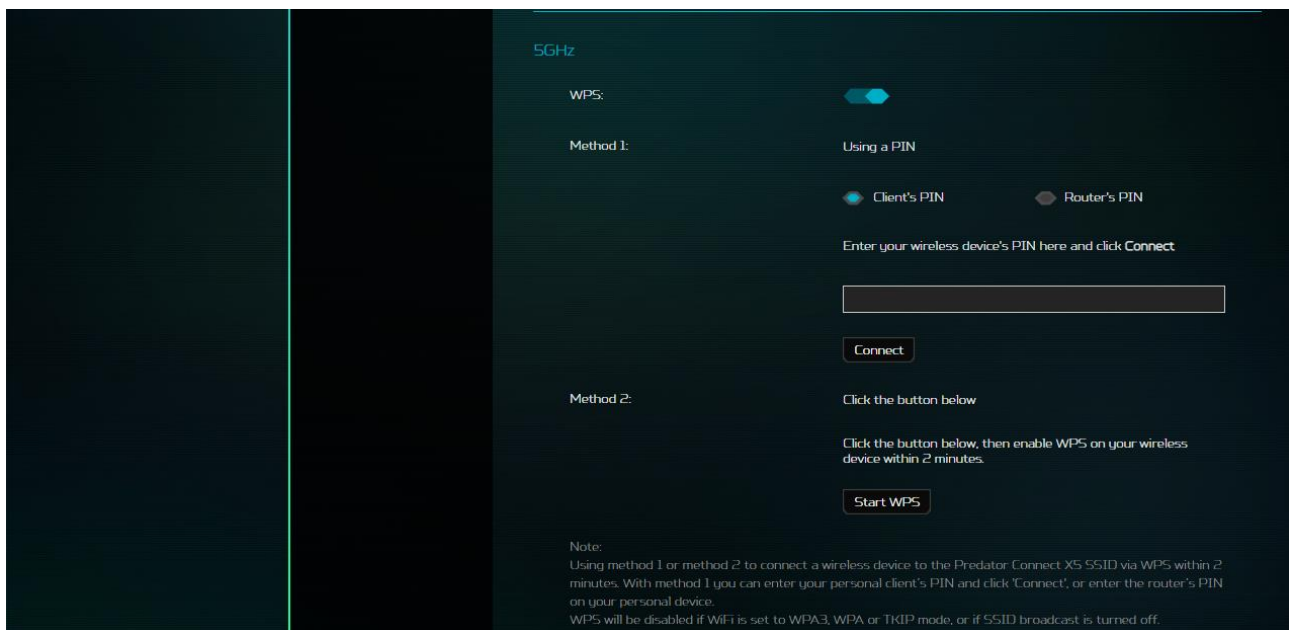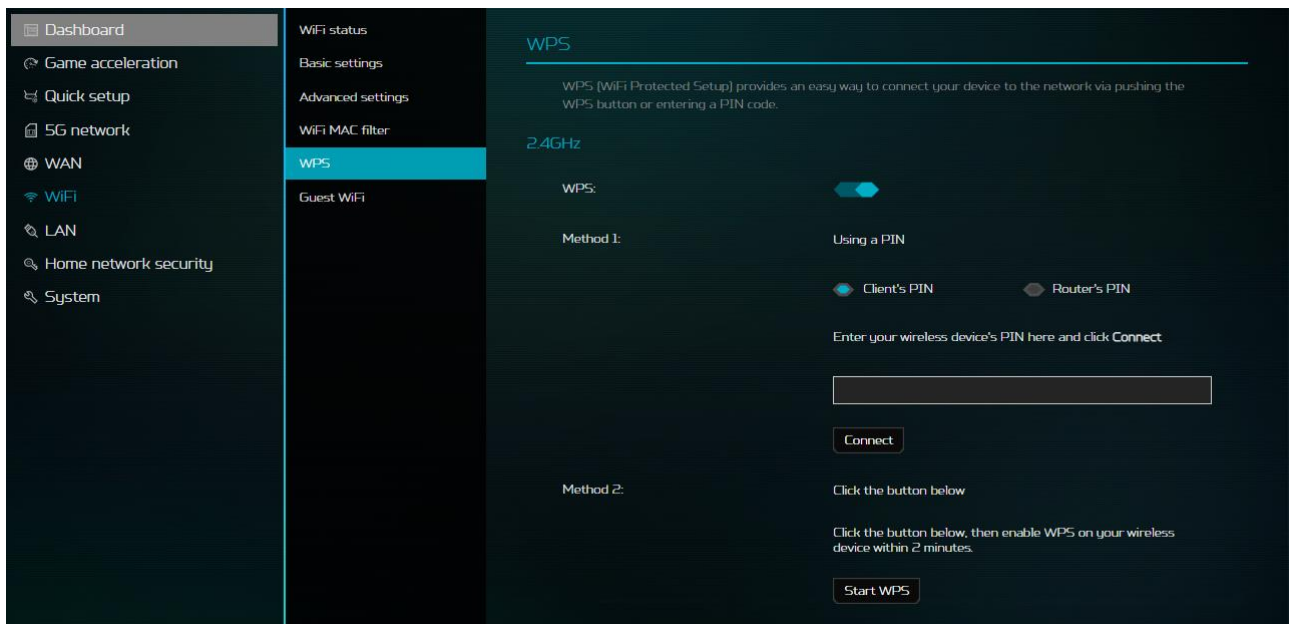
- Using method 1 or method 2 to connect a wireless device to the Predator Connect X5 SSID via WPS within 2 minutes. With method 1 you can enter your personal client's PIN and click 'Connect', or enter the router's PIN on your personal device.
WPS will be disabled if WiFi is set to WPA3 or TKIP mode, or if SSID broadcast is turned off.

9.6 Guest WiFi

- You may also provide Internet Connection for guests, but access to devices on your network. Choose to enable between 2.4GHz and 5GHz bands for your guests.

-
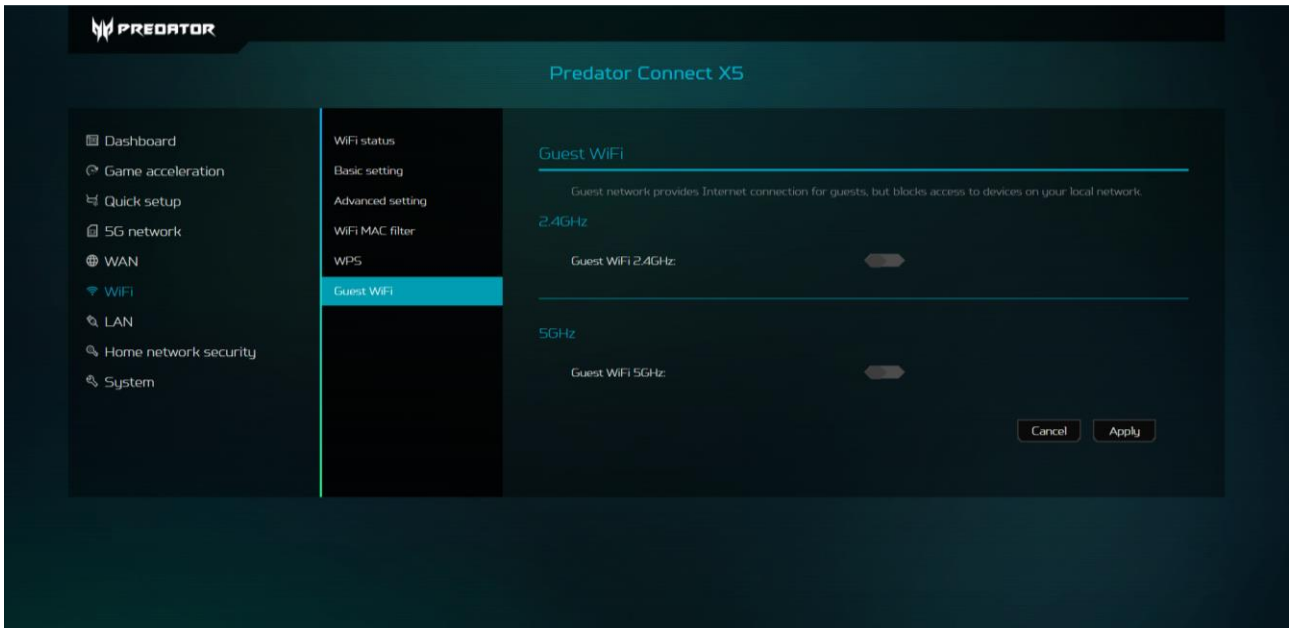
10 LAN Status

10.1 Here, you can easily see your connected status, IP address, MAC address and DHCP server. The Predator Connect X5 has 3 possible LAN ports. LAN3 is usually designated as WAN.
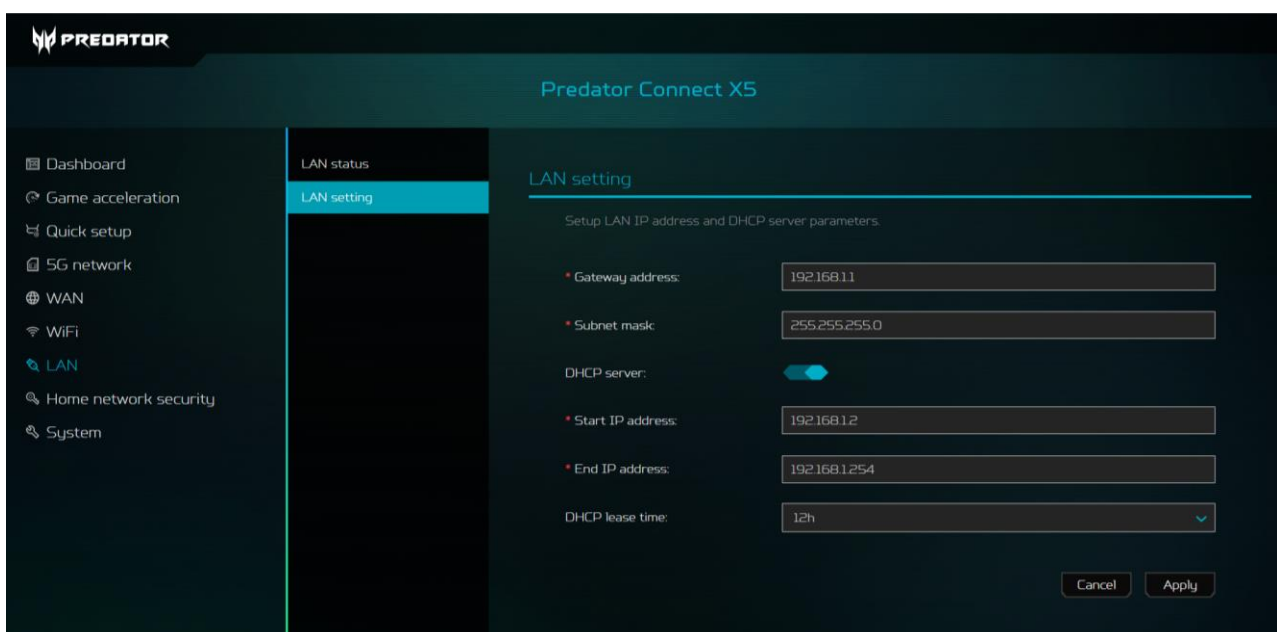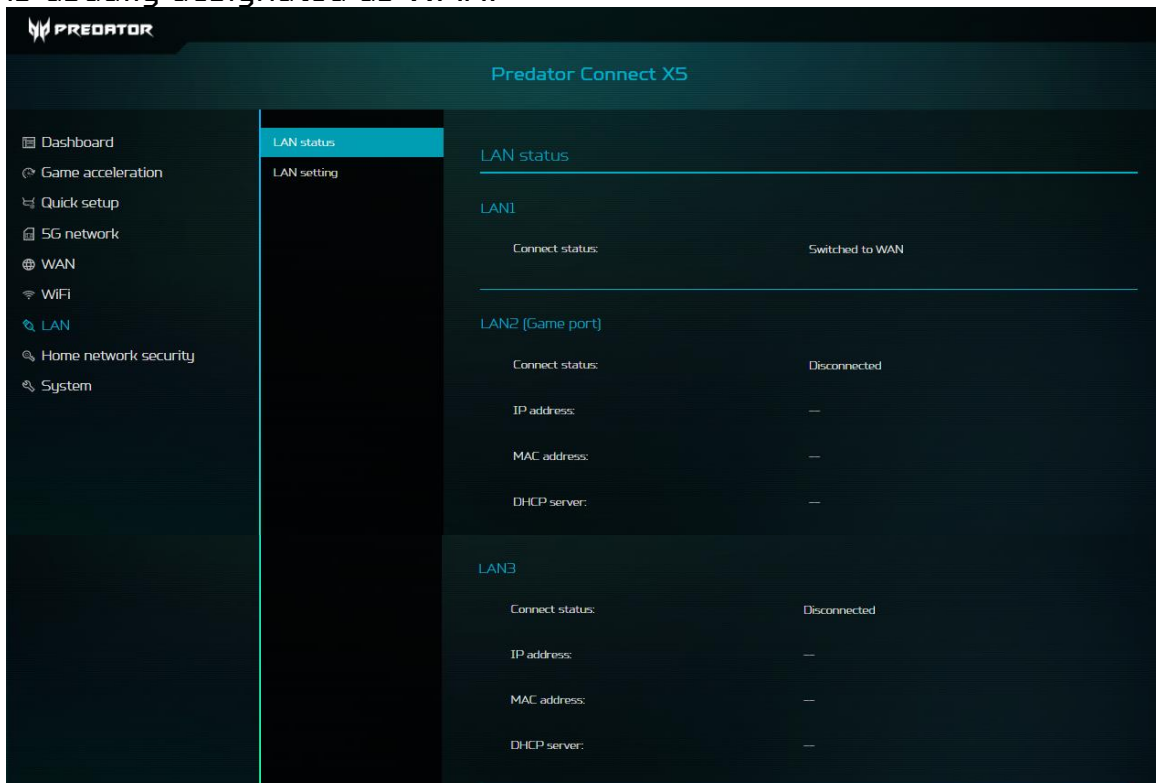
10.2 In the LAN Setting, further configuration can be done here.

11. Home Network Security

11.1

Powered by TrendMicro, Malicious website blocking can prevent you from visiting malicious websites thereby protecting your computers from being infected with Trojans or being exploited unknowingly. Trend Micro's Web Reputation Services (WRS) can helps you identify malicious URLs.
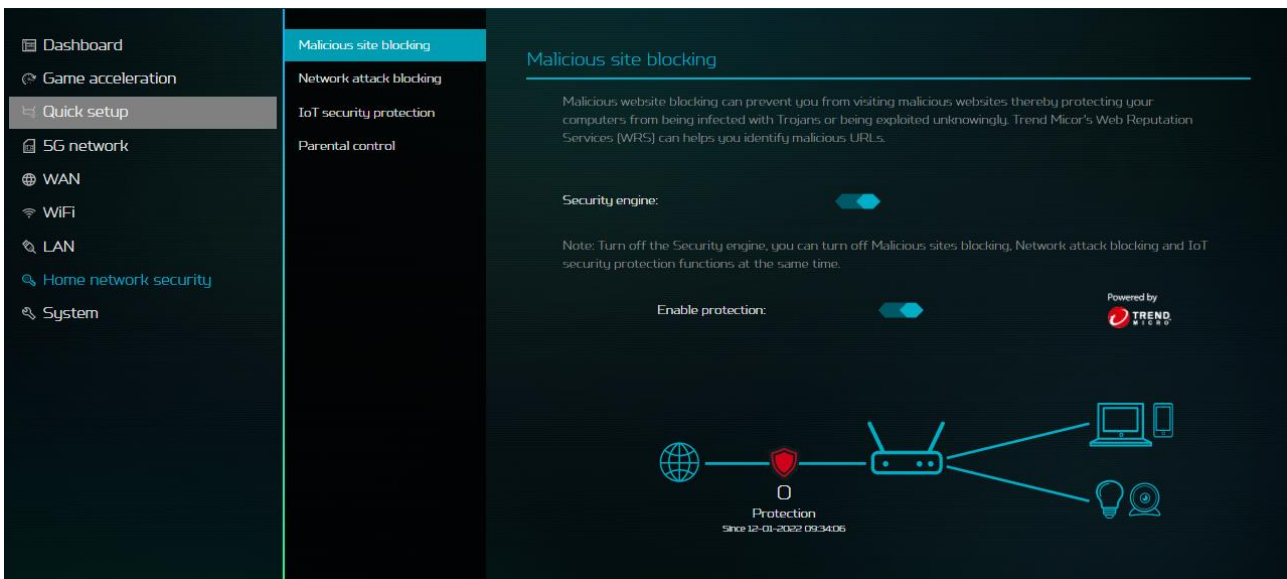
11.2

Network attack blocking can help prevent the exploitation of a known vulnerability even when the vulnerable systems/devices have not yet been installed with security patches. It can also detect the infected device and block its network behavior to prevent infection to other devices.
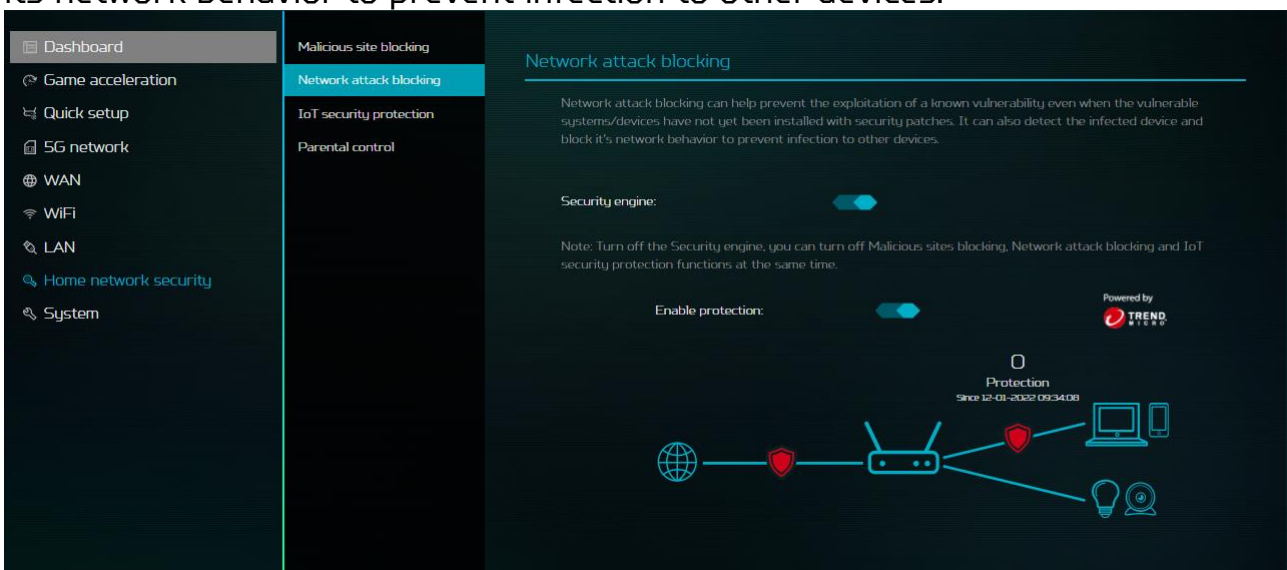
11.3
IoT security protection can detect and block harmful connections from compromised IoT devices by using Trend Micro's Smart Protection Network, a continuously updated IoT device reputation database.
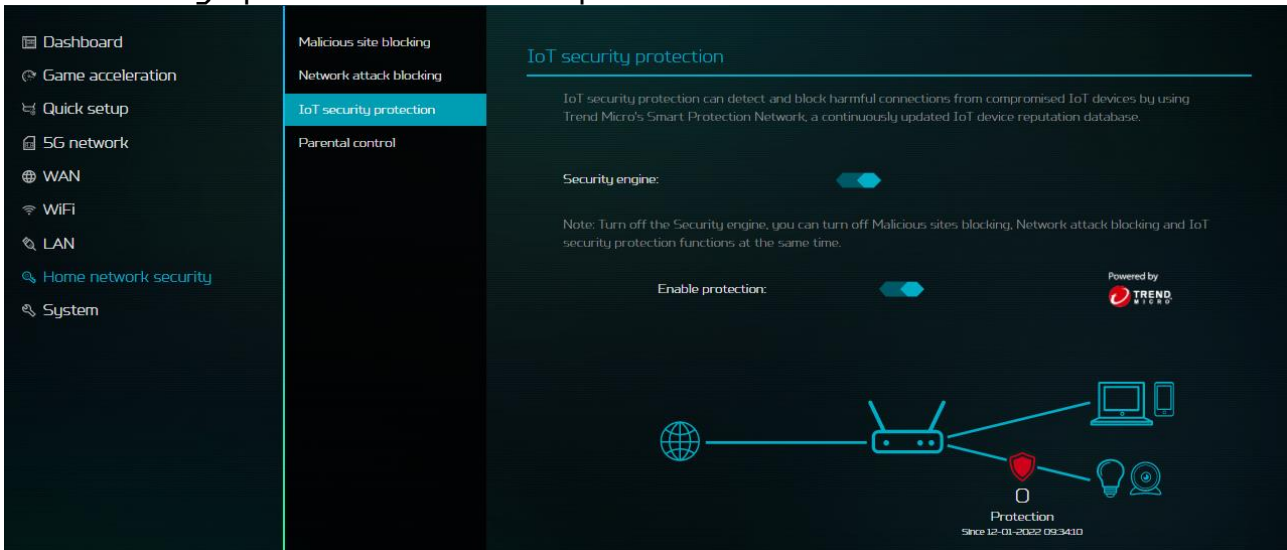
11.4 Parental Control allows you to block unwanted websites on specifically devices.
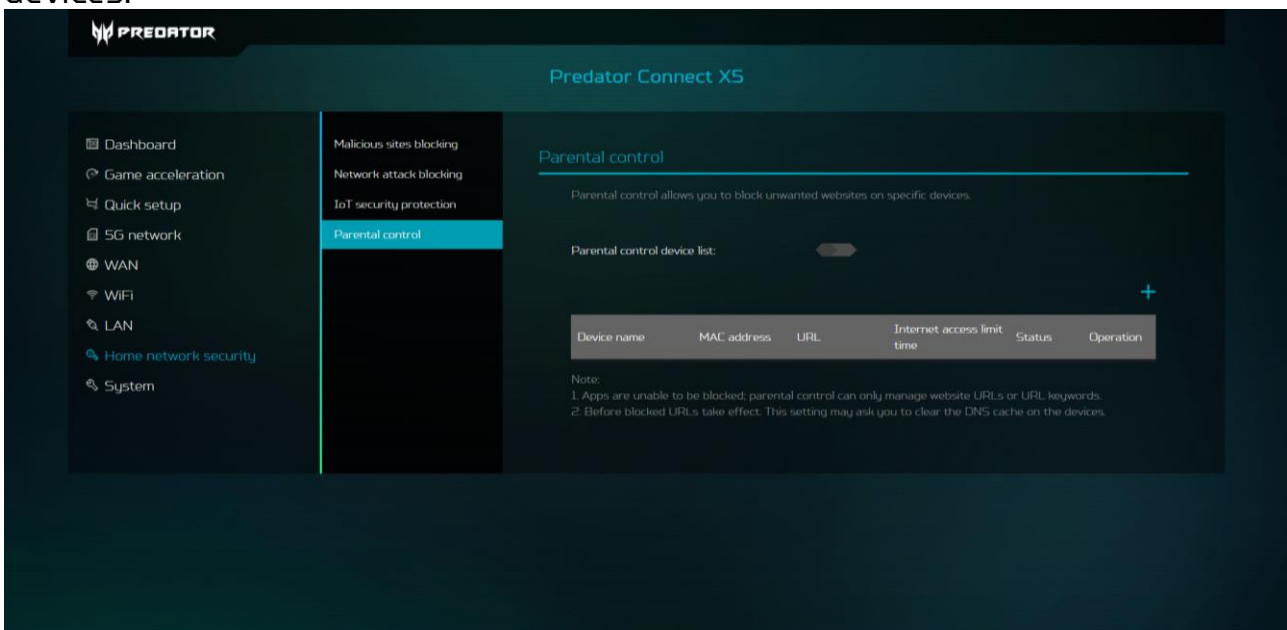
12. Setting

12.1 Login Password

- Change the password of your Predator Connect X5, use a strong password to keep it secure.
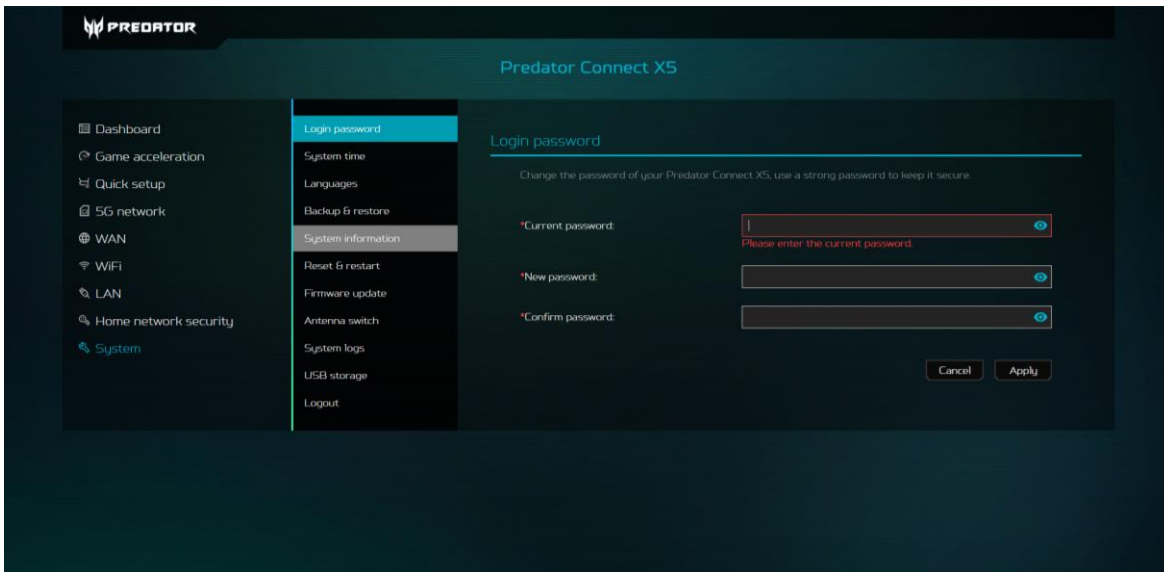
12.2 System Time

- This allows device to synchronize the system time to the time zone selected. When daylight savings time setting is ON, device will automatically adjust the daylight saving system time according to the time zone.
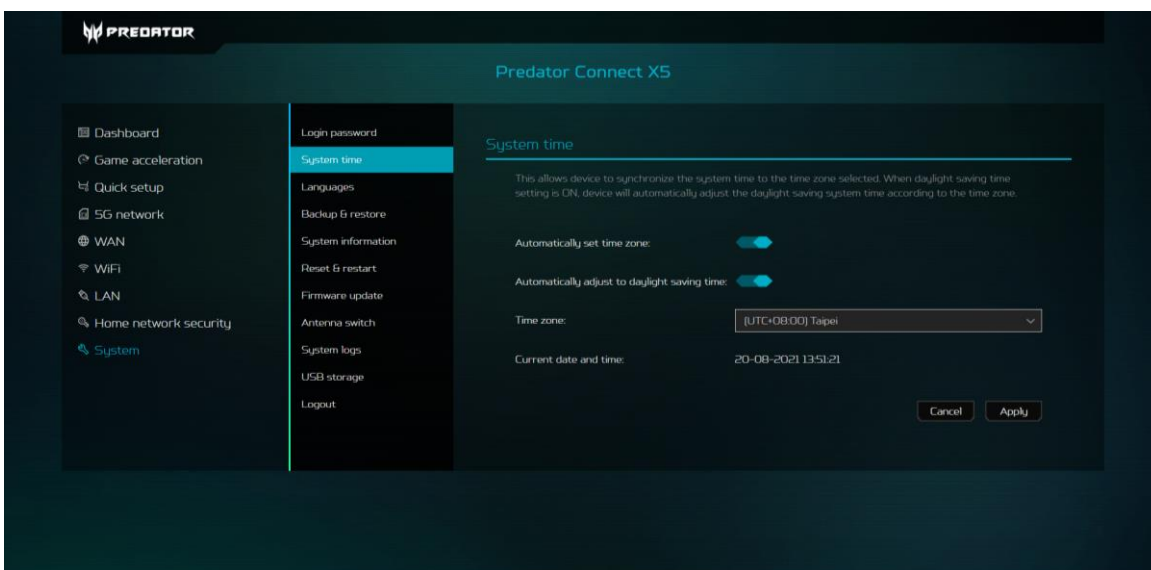
12.3Language

- Set the language of your Predator Connect X5.
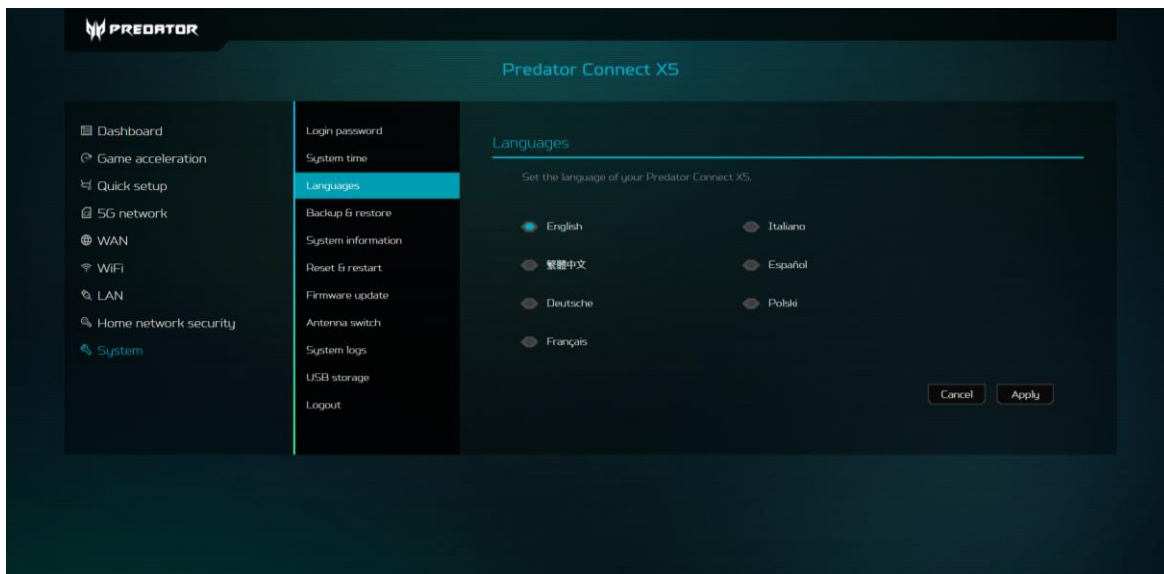
12.4 Backup and restore
- Backup your custom device settings.
- Reverts your device to original factory settings.
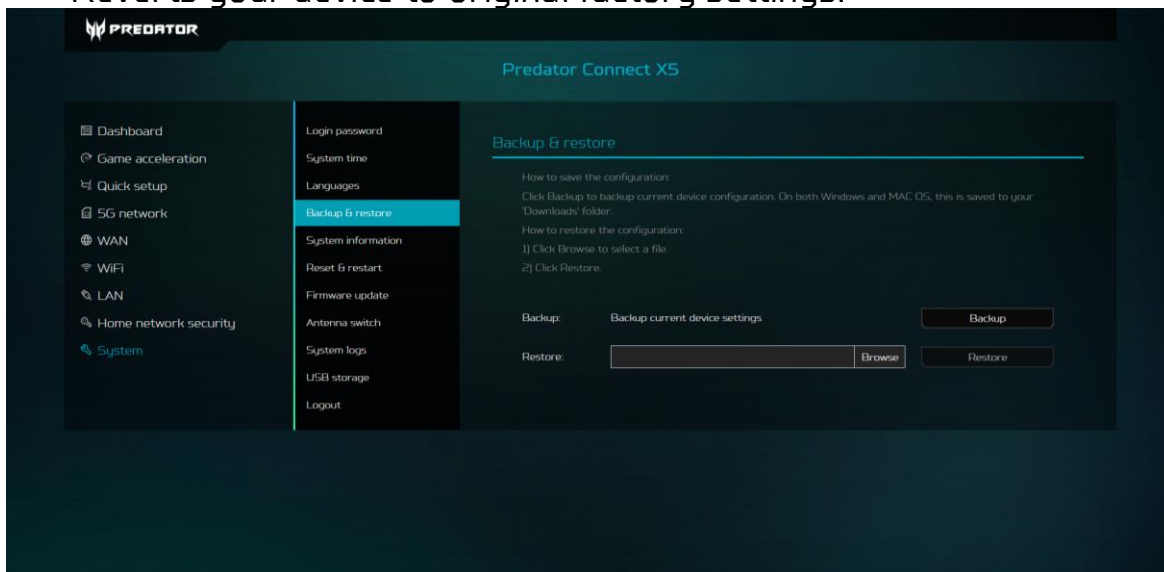
12.5 System Information

- Shows key device information such as
  - A. Device Name
  - B. IMEI
  - C. Serial Number
  - D. Software Version
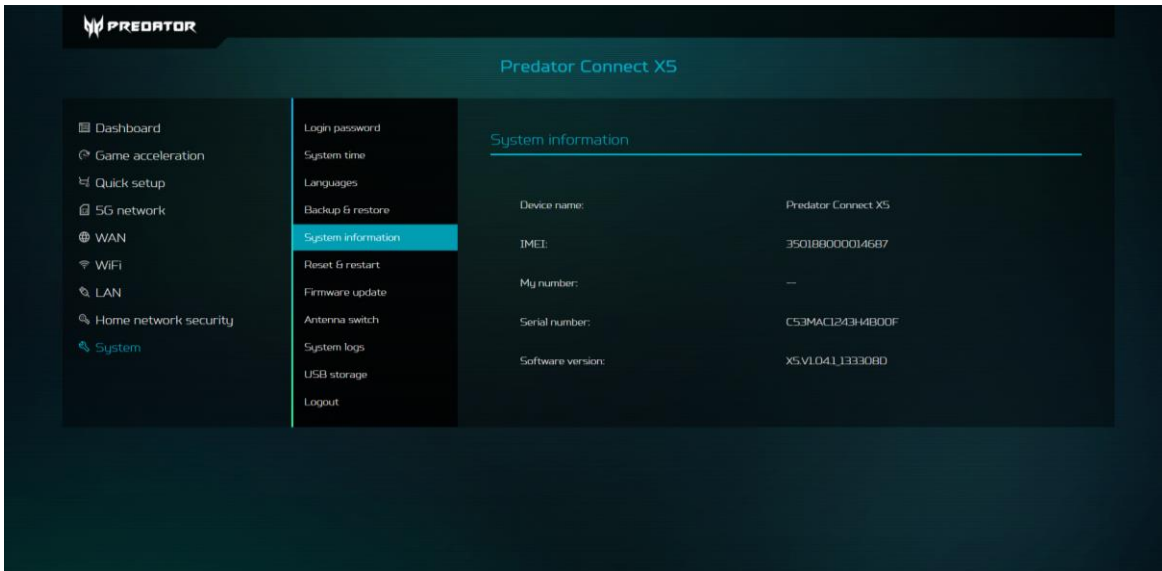
12.6 Reset & restart

- Click Restart to reboot the device and click Reset to restore factory default settings.
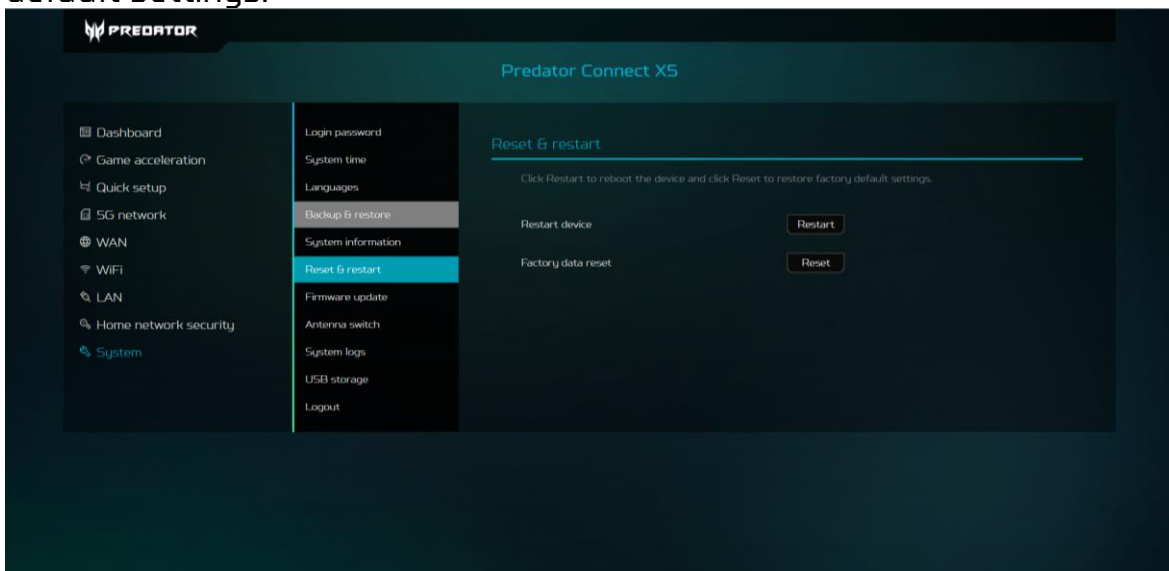
12.7 Firmware update

- Click Check new for updates. Your router will check if there is an update available. If one is found, you may click Download. Once the file has downloaded successfully you will be able to click Update.
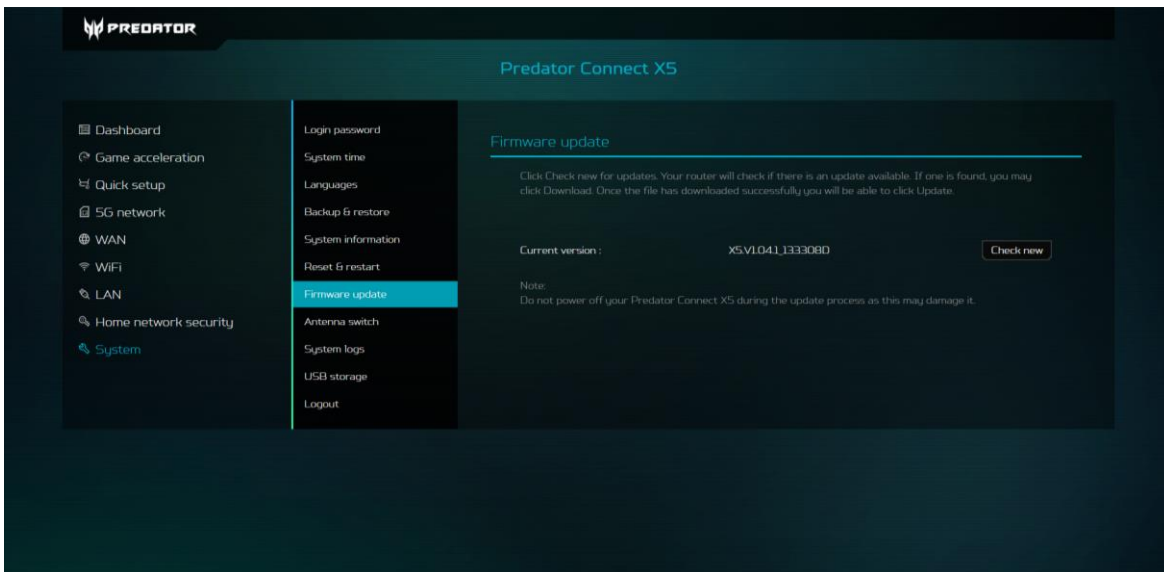
12.8 Antenna switch

- Set to Internal to use the inbuilt antenna. Set to External to connect a compatible external antenna to Predator Connect X5 via the LTE TS9 connectors.
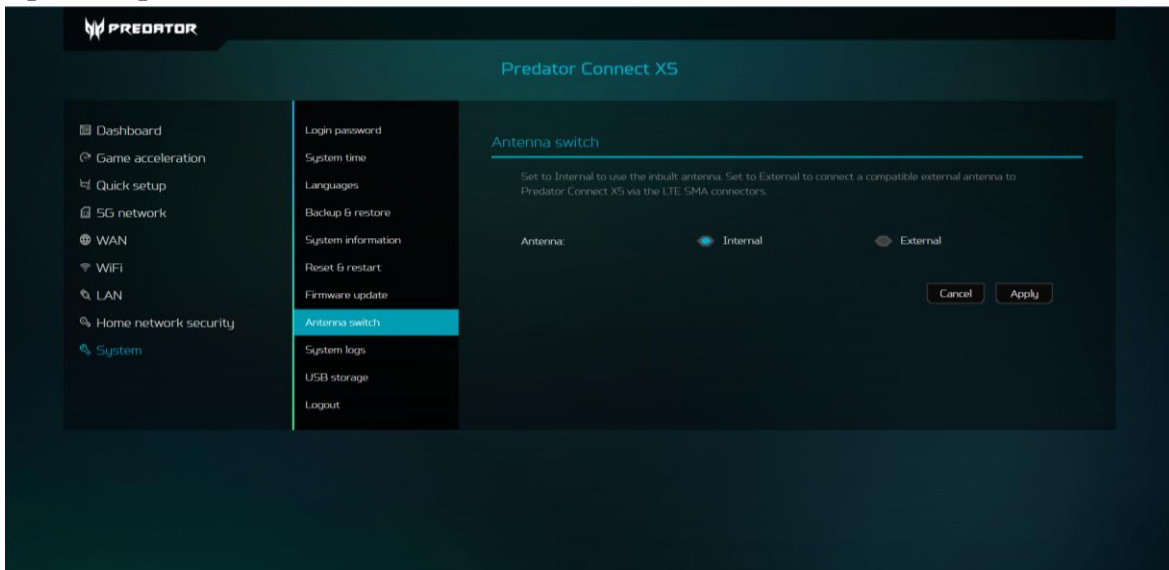
12.9 System logs

The system log will save the last 100 activities.
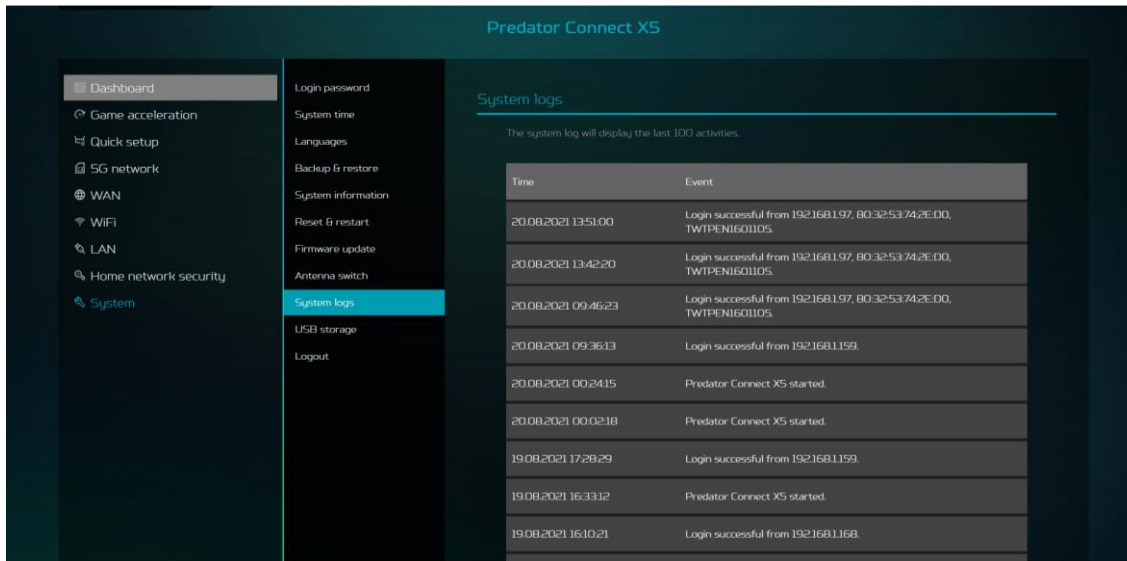
12.10 USB storage

- Plug in USB dongle on Predator Connect X5 and allow all users connected to your network access rights to the file folders in your USB Dongle.
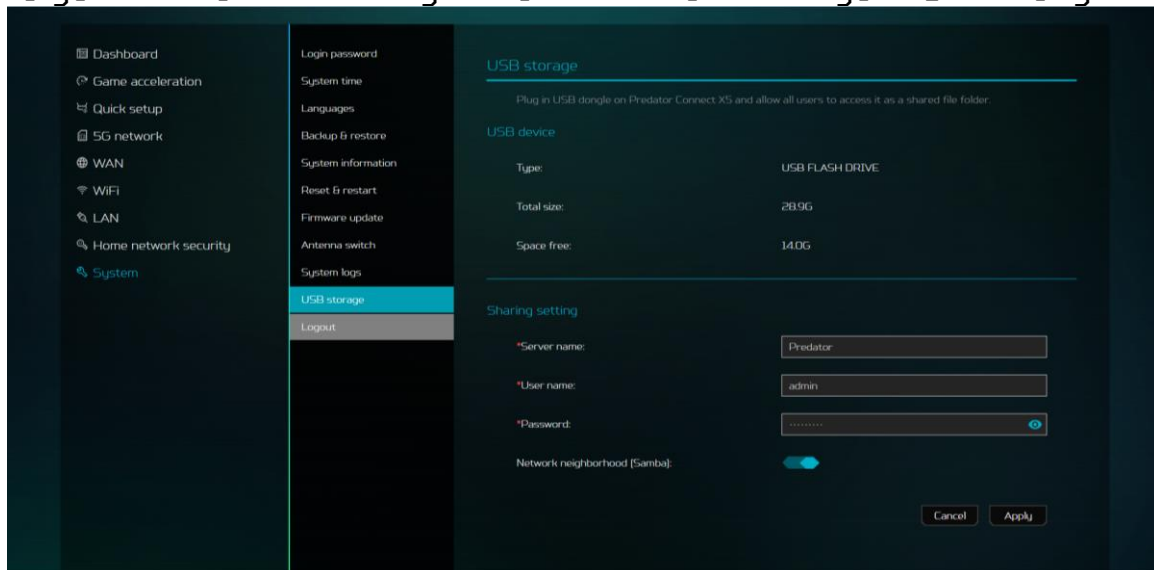
To access the USB storage from PC, you can type \\192.168.76.1\ into the address column of the file manager.
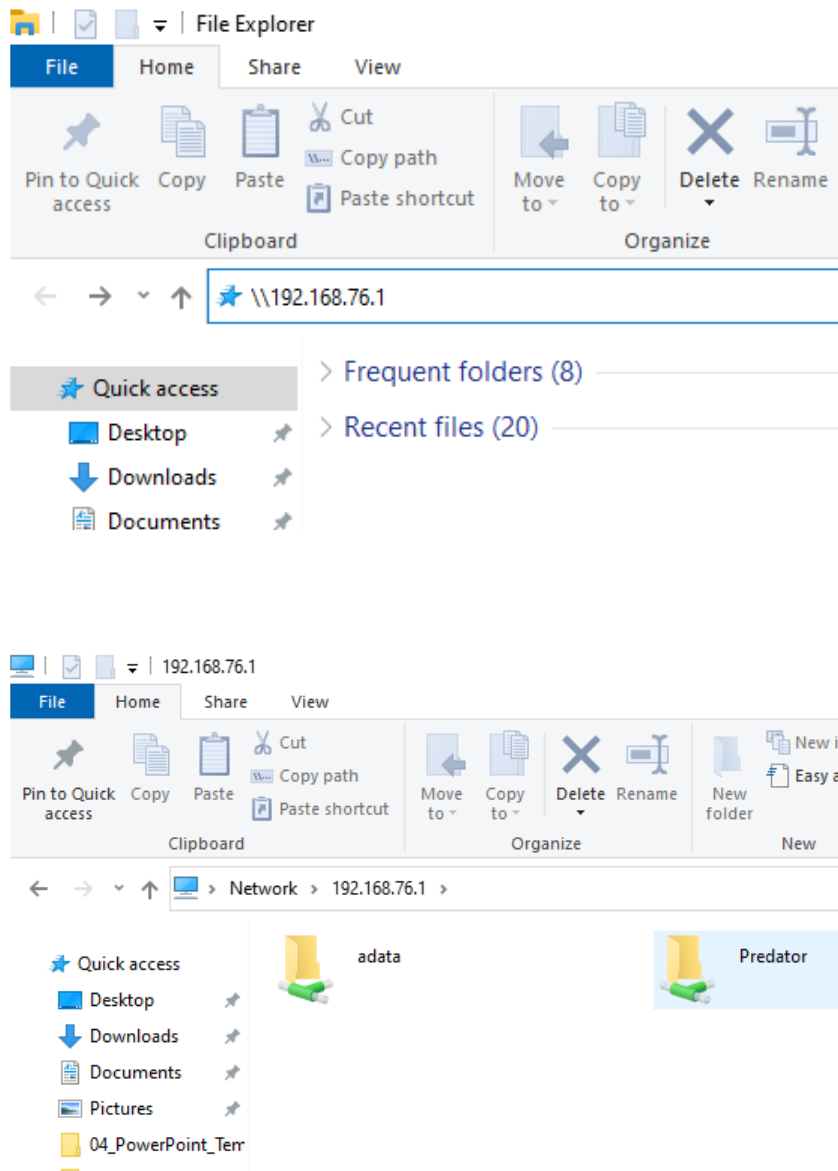
12.11 Logout
- Once you push this button, you will be instantly logged out. To reenter the Predator Connect Webpage, you will need to input login credentials and password.

13. Predator Connect APP

13.1 Download Predator App from App store or Google Play

13.2 Register account
    New users will need to register new accounts if this is their first time logging into the Predator Connect App.

13.3 Quick setup
    Run quick setup to help the X5 connect to internet. Follow the quick setup instructions you see on the Predator Connect App. Scan the QR code to quickly apply your X5's unique WiFi SSID, WiFi password and Admin password.

13.4 Device Binding
- After quick setup, you will need to bind your device to your Predator APP's linked email account.
- The App allow user to bind multiple devices to an account. In the Predator APP, you can check "Bind List" to see the devices in your account.
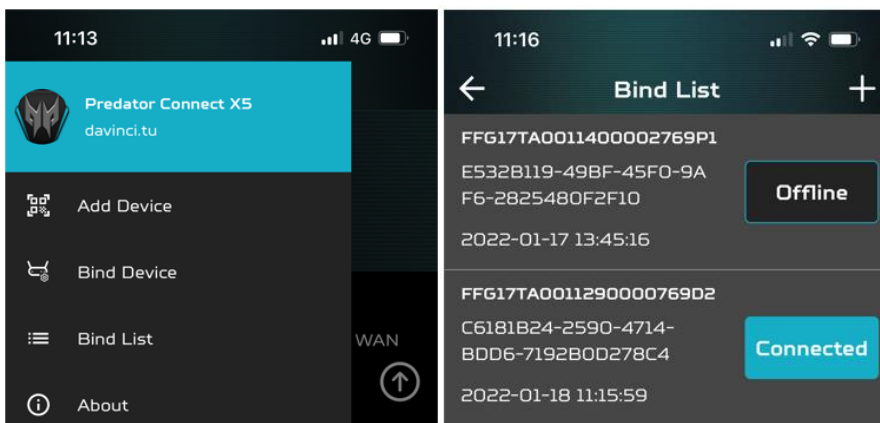
14. Regulatory Information

14.1 Important Safety Precaution
Your Predator Connect X5 5G CPE device is manufactured to comply with European safety standards. This section outlines the safety precautions associated with using the device. Please read the safety and operation instructions before using your device and other accessories. Keep these instructions safe for future reference.

14.2 Condition of Use
The device is not water-resistant. Please protect the device from water or moisture and do not touch the device with wet hands. Otherwise short-circuit and malfunction of the product or electric shock may occur.
Keep the device and accessories in a cool, well- ventilated area and away from direct sunlight. Do not place the device in a container with poor heat dissipation. Do not enclose or cover your device with clothes, towels, or other objects.
Put your device in places beyond the reach of children. Do not allow children to use the wireless device without guidance.
Do not use your device at places for medical treatment (in an operating room, intensive care unit, or coronary care unit, etc.) where wireless device use is prohibited.
To reduce the risk of accidents, do not use your device while driving.
RF signals may affect the electronic systems of motor vehicles. For more information, consult the vehicle manufacturer.
Acer recommends using the charger supplied with your device. Use of another type of charger may result in malfunction and/or danger.

14.3 Cleaning and Maintenance
Do not attempt to dry your device with an external heat source, such as a microwave oven or hair dryer.
Use a clean, soft, and dry cloth to clean the device and accessories.

14.4 Disposal Instructions
Do not throw this electronic device into the trash when discarding. To minimize pollution and ensure utmost protection of the global environment, please recycle. For more information on the Waste from Electrical and Electronics Equipment (WEEE) regulations, visit
www.acer-group.com/public/Sustainability

14.5 Ethernet Cable Line Safety

Disconnect all Ethernet cable lines from the equipment when not in use and/or before servicing.

To avoid the remote risk of electric shock from lightning, do not connect the Ethernet cable line to this equipment during lightning or thunderstorms.

14.6 Medical Devices

Operation of any radio transmitting equipment, including wireless phones, may interfere with the functionality of inadequately protected medical devices. Consult a physician or the manufacturer of the medical device to determine if they are adequately shielded from external RF energy or if you have any questions. Switch off your device in health care facilities when any regulations posted in these areas instruct you to do so. Hospitals or health care facilities may be using equipment that could be sensitive to external RF transmissions. Pacemakers. Pacemaker manufacturers recommend that a minimum separation of 15.3 centimeters (6 inches) be maintained between wireless devices and a pacemaker to avoid potential interference with the pacemaker. These recommendations are consistent with the independent research by and recommendations of Wireless Technology Research. Persons with pacemakers should do the following:

Always keep the device more than 15.3 centimeters (6 inches) from the pacemaker

Not carry the device near you pacemaker when the device is switched on. If you suspect interference, switch off your device, and move it.

Hearing aids. Some digital wireless devices may interfere with some hearing aids. If interference occurs, consult your service provider.

14.7 Vehicles

RF signals may affect improperly installed or inadequately shielded electronic systems in motor vehicles such as electronic fuel injection systems, electronic antiskid (anti-lock) braking systems, electronic speed control systems, and air bag systems. For more information, check with the manufacturer, or its representative, of your vehicle or any equipment that has been added. Only qualified personnel should service the device, or install the device in a vehicle. Faulty installation or service may be dangerous and may invalidate any warranty that may apply to the device. Check regularly that all wireless equipment in your vehicle is mounted and operating properly. Do not store or carry flammable liquids, gases, or explosive materials in the same compartment as the device, its parts, or enhancements. For vehicles equipped with an air bag, remember that air bags inflate with great force. Do not place objects, including installed or portable wireless equipment in the area over the air bag or in the air bag deployment area. If in-vehicle wireless equipment is

improperly installed, and the air bag inflates, serious injury could result. Using your device while flying in aircraft is prohibited. Switch off your device before boarding an aircraft. The use of wireless devices in an aircraft may be dangerous to the operation of the aircraft, disrupt the wireless telephone network, and may be illegal.

14.8 Warning
Do not attempt to open the device by yourself. Disassembling may result in damage to the device. Small parts may also present a choking hazard.
When this device is switched on, it should be kept at least 15 cm from any medical device such as a pacemaker, a hearing aid or insulin pump, etc. Switch this device off when you are near gas or flammable liquids. Strictly obey all signs and instructions posted in any potentially explosive atmosphere.

14.9 Explosive Device Proximity Warning
Switch off your device when in any area with a potentially explosive atmosphere and obey all signs and instructions. Potentially explosive atmospheres include areas where you would normally be advised to turn off your vehicle engine. Sparks in such areas could cause an explosion or fire resulting in bodily injury or even death. Switch off the device at refueling points such as near gas pumps at service stations. Observe restrictions on the use of radio equipment in fuel depots, 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. They include below deck on boats, chemical transfer or storage facilities, vehicles using liquefied petroleum gas (such as propane or butane), and areas where the air contains chemicals or particles such as grain, dust or metal powders. Do not switch the notebook on when wireless phone use is prohibited or when it may cause interference or danger.
Warning: Do not operate a portable transmitter (including this wireless adapter device) near unshielded blasting caps or in an explosive environment unless the transmitter has been modified to be qualifies for such use.
Warning: The wireless adapter is not designed for use with high-gain directional antennas

14.10 Wireless adapter regulatory information
Warning: For safety reasons, turn off all wireless or radio transmitting devices when using your device under the following conditions.
Remember to follow any special regulations in force in any area, and always switch off your device when its use is prohibited or when it may cause interference or danger. Use the device only in its normal operating positions. This device meets RF exposure guidelines when used normally. To successfully transmit data files or messages, this device requires a good quality connection to the network. In some cases, transmission of data files or messages may be delayed until such a connection is available. Parts of the device are magnetic. Metallic materials may be attracted to the device, and persons with hearing aids should not hold the device to the ear with the hearing aid. Do not place credit cards or other magnetic storage media near the device, because information stored on them may be erased.

Aircraft
Warning FCC and FAA regulations may prohibit airborne operation of radio-frequency wireless devices (wireless adapters) because their signals could interfere with critical aircraft instruments. Ask the airport staff and cabin crew before turning on your device's wireless adapter whilst on board.
The wireless adapter and your health
The wireless adapter, like other radio devices, emits radio frequency electromagnetic energy. The level of energy emitted by the wireless adapter, however, is less than the electromagnetic energy emitted by other wireless devices such as mobile phones. The wireless adapter operates within the guidelines found in radio frequency safety standards and recommendations. These standards and recommendations reflect the consensus of the scientific community and result from deliberations of panels and committees of scientists who continually review and interpret the extensive research literature. In some situations or environments, the use of the wireless adapter may be restricted by the proprietor of the building or responsible representatives of the applicable organization. Examples of such situations may include:
· Using the wireless adapter on board airplanes, or
· Using the wireless adapter in any other environment where the risk of interference with other devices or services is perceived or identified as being harmful.
If you are uncertain of the policy that applies to the use of wireless adapters in a specific organization or environment (an airport, for example), you are encouraged to ask for authorization to use the adapter before you turn it on.

14.11 EU Regulatory Conformance

List of applicable countries

This product must be used in strict accordance with the regulations and constraints in the country of use. For further information, contact the local office in the country of use. Please see https://europa.eu/ european-union/about-eu/countries_en for the latest country list.

Specific absorption rate information
This device meets the EU requirements on the limitation of exposure of the general public to electromagnetic fields by way of health protection. The limits are part of extensive recommendations for the protection of the general public. These recommendations have been developed and checked by independent scientific organizations through regular and thorough evaluations of scientific studies. The unit of measurement for the European Council's recommended limit for mobile devices is the "Specific Absorption Rate" (SAR), and the SAR limit is 2.0 W/kg averaged over 10 grams of body tissue. The MPE was calculated at 20 CM to show compliance with the power density limit. It meets the requirements of the International Commission on Non-Ionizing Radiation Protection (ICNIRP). For body worn operation, this device has been tested and meets the ICNIRP exposure guidelines and the European Standard, for use with dedicated accessories. Use of other accessories which contain metals may not ensure compliance with ICNIRP exposure guidelines.

Hereby, Acer Inc. declares that the radio equipment type XXXXXX is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available: Please search for Predator Connect X5 5G CPE at www.acer.com

14.12 Duty Cycle Attestation
5G MiFi UE (User Equipment) will operate on its 5G network with a configuration of 1:1 DL:UL ratio, i.e. The highest uplink duty cycle is 50% for NR n78 band for the lifetime of this device.

14.13 Restrictions
Operations in the 5.15–5.35GHz band are restricted to indoor usage only.

AT	BE	BG	HR	CY	CZ	DK
EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL
PT	RO	SK	SI	ES	SE	UK (NI)
IS	LI	NO	CH	TR		

14.14 EU Regulatory Compliance – Radio

Frequency range (MHz)	Max power in the range (dBm)
B1 (1920 – 1980)	25
B3 (1710 – 1785)	25
B5 (824 – 849)	25
B7 (2500 – 2570)	25
B8 (880– 915)	25
B20 (832– 862)	25
B28 (703 – 748)	25
B38 (2570 – 2620)	25
B39 (1880 – 1920)	25
B40 (2300 – 2400)	25
B41 (2496 – 2690)	27
B42 (3400 – 3600)	25
B46 (5150 – 5925)	25
n1 (1920 – 1980)	25
n3 (1710 – 1785)	25
n7 (2500 – 2570)	25
n8 (880– 915)	25
n20 (832– 862)	25
n28 (703 – 748)	25
n38 (2570 – 2620)	25
n39 (1880 – 1920)	25
n40 (2300 – 2400)	25
n41 (2496 – 2690)	27
n77 (3300 – 4200)	25
n78 (3300 – 3800)	27
n79 (4400 – 5000)	27
Wi-Fi 2.4G (E.I.R.P)	20
Wi-Fi 5G (E.I.R.P)	27

14.15 Power Supply Unit Information

Model Identifier	Predator X5 Adaptor
Input Voltage	AC 100 – 240V
Input AC Frequency	50/60Hz
Output Voltage	DC 12V
Output Current	2.0A
Output Power	24.0W

15. Limited Warranty

The product is covered by a limited warranty. Please check the warranty booklet inside the product package for details.