Acer Predator Connect X7 BE11000 Tri-band Wi-Fi 7 5G CPE

User Guide

V1.6

Important: This manual contains proprietary information that is protected by copyright laws. The information contained in this manual is subject to change without notice. Some features described in this manual may not be supported depending on the Operating System version. Images provided herein are for reference only and may contain information or features that do not apply to your device. Acer Group shall not be liable for technical or editorial errors or omissions contained in this manual.

Revision May, 2024

Contents

Contents

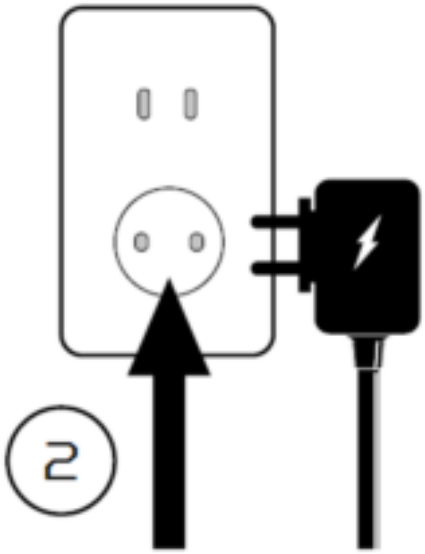
1. Overview

Acer Predator Connect Series X7 is a 5G CPE with a cutting-edge Wi-Fi 7 Tri-band (2.4GHz + 5GHz + 6GHz) simultaneously with BE11000 throughput, specifically optimized for gamers. It boasts dual WAN features and an easy 1-2-3 setup wizard for a hassle-free installation. Enjoy continuous connectivity with the seamless transition between your primary 5G NR and secondary Ethernet internet network. Our integrated load balancer and failover features ensure optimal network performance and robustness across your internet network. Unlock the ultimate gaming experience with Wi-Fi 7's groundbreaking technology, designed for peak data transmission and minimal latency. Wi-Fi 7's Multi-Link Operation (MLO) is a significant technical advancement, enhancing throughput, reducing latency, and improving network efficiency by allowing devices to connect to multiple links simultaneously. This CPE includes band steering, which ensures that each device uses the optimal frequency band for its conditions, resulting in a more efficient and reliable Wi-Fi experience. Trend Micro network security protection is built-in, with live updates keeping your network safe from malware and vulnerabilities around the clock. Automatic Channel Selection (ACS) dynamically selects the best channel to avoid interference from nearby networks. The X7 also includes port forwarding profiles for popular gaming consoles like PS5 and Xbox, facilitating seamless gameplay. Hybrid QoS prioritizes your gaming traffic and optimizes bandwidth utilization. Additionally, the VPN feature provides a secure connection for your device when browsing online.

2. Installation and Setup

2.1. Plug in the AC adapter

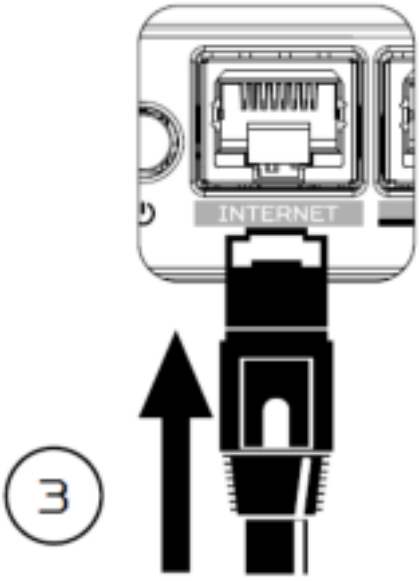
2.2. Plug into an outlet.

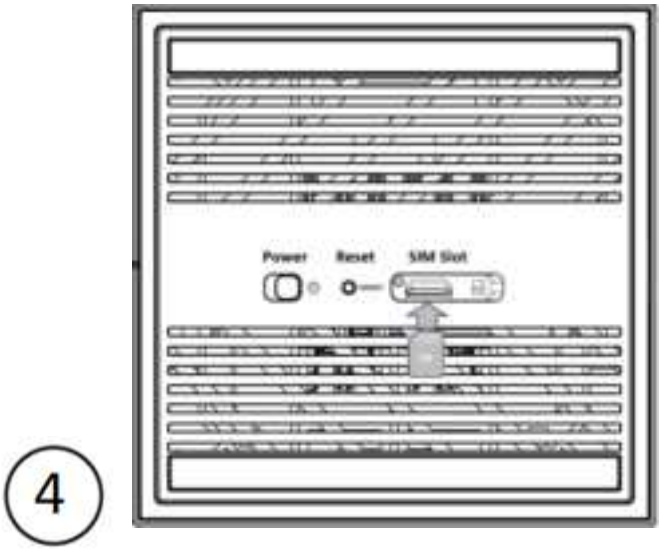


2.3. Plug in the Internet cable and power ON the device

AND/OR

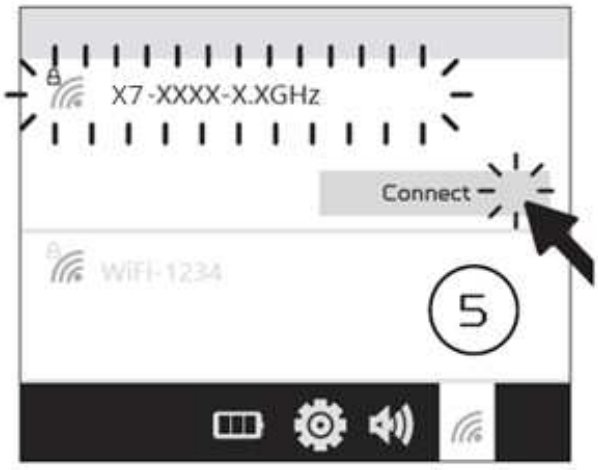
2.4 Insert 5G SIM into the SIM slot





2.5 Connect to Predator X7 Wi-Fi.

2.6 Important info is at the back of the device



2.6 The device can be either setup via Predator Connect mobile App or the browser web admin.

How to set up the CPE via **Predator Connect Mobile App**:

- Use a mobile device camera to scan the QR code below. Download the Predator Connect mobile App via Play Store or App Store.

Download APP

Available on the App Store

GET IT ON Google Play

- Open the Predator Connect Mobile App and follow the steps for registering an account. Go to your email inbox, review the registration email, and input the 4-digit registration code onto the mobile App. When the whole process is completed, you will be automatically signed in.
- Enable the mobile Wi-Fi function and scan the device QR-code printed on the back label. The default admin and Wi-Fi password will be automatically exported into the mobile app. (SSID: X7_YYYY)
- Device setup completed.

Set up the CPE via browser:

- Please make sure that the wireless function on your laptop is already enabled.
- Check the device's back label, find the CPE's default SSID (X7_YYYY_2.4GHz) and password and then connect.
- Open the browser on your laptop/desktop, input the device web admin URL: http://acer-connect.com or IP: http://192.168.76.1
- The device will automatically redirect to a quick setup wizard. Follow the easy 1-2-3 steps and get ready to access the internet.

  Note: The admin login password requires changing within the setup wizard for first-time use. Please create a strong password and keep it in a safe place. (The new password cannot be the same as the prior one.)

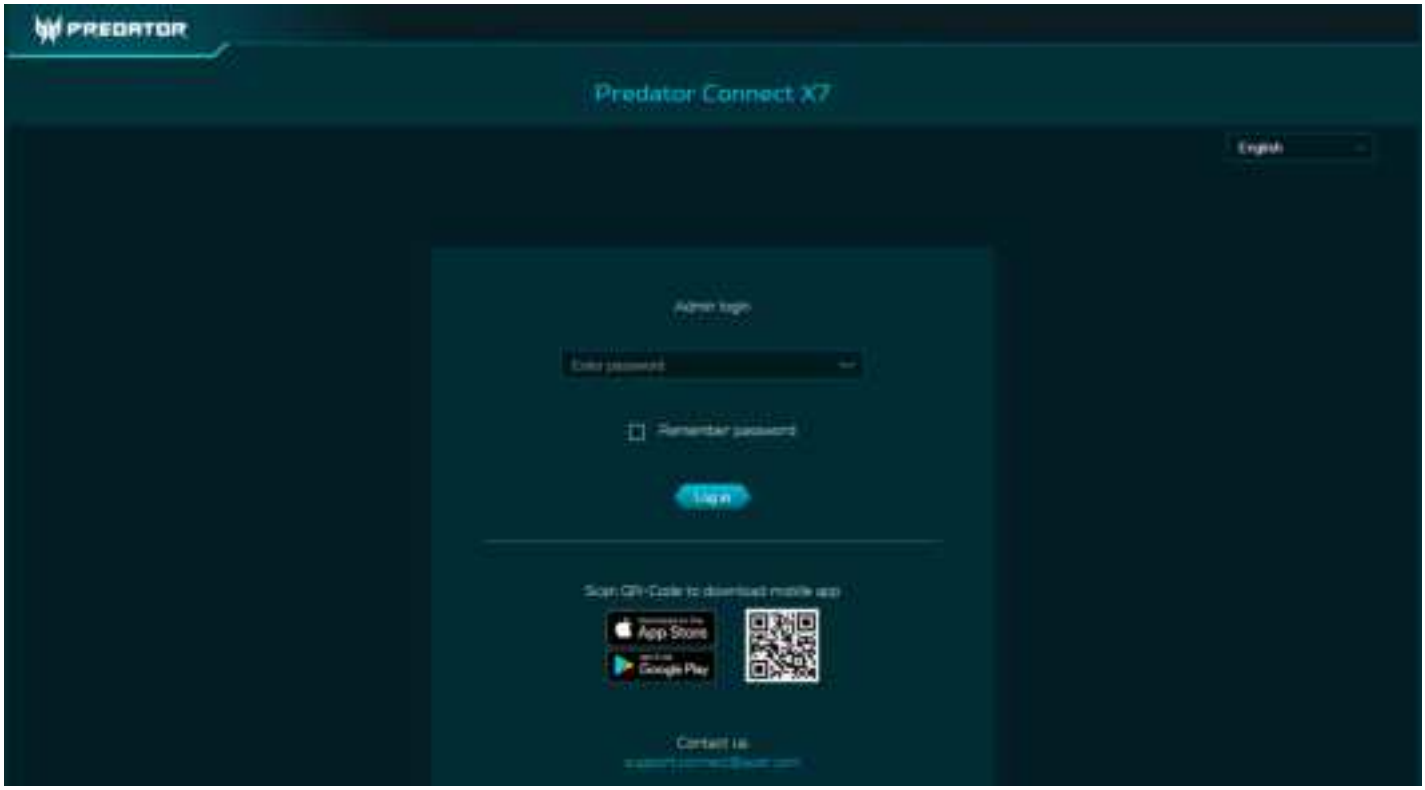
  Note: The CPE web admin portal will automatically lock after five consecutive incorrect attempts. You have to power cycle the CPE to unlock the web admin.

  Note: The SSID Wi-Fi password can't be the same as the admin login password.

  Both the App & browser can help the CPE to do a quick setup. Web UI can execute all functions and settings of the CPE. Mobile App allows the user to remotely control some functions of the CPE and receive notifications.

3. Initial Configuration

Please log in to the Predator Connect X7 Web Portal (http://acer-connect.com or IP: http://192.168.76.1) by using the current valid Admin password. You can select the language of Web UI by clicking on the drop-down box on the top right of the web portal.



Enter the login password to see the dashboard and other settings of your Predator Connect X7. The CPE will automatically guide you step by step on how to set up and configure internet access and basic network settings.

You can scan the QR code (on the login screen using your Android mobile or iPhone) to download the mobile app and manage your CPE remotely.

4. Dashboard

Once you have successfully logged in, the following key information will be displayed on the Predator Connect X7 dashboard.

Connection Status: shows the current connection status of Internet.

WAN Status: shows both the primary and secondary WAN connectivity, download/ upload speed and IPs.

Wi-Fi Status: shows the number of wireless client devices connected with 2.4GHz, 5GHz and 6GHz bands. By enabling band steering Wi-Fi, the CPE monitors and organizes the frequency band allocation within a Wi-Fi network.

LAN Status: quickly indicates the status of LAN ports. Predator Connect X7 has one WAN port, one Game port and one LAN port. The "icon" (at the far right) represents the number of devices connected to the X7 CPE. Clicking on this icon will display the table shown below.

Connected Devices: shows how many client devices are connected with your Predator Connect X7 through Wi-Fi or LAN. You can also modify the device name by clicking on the edit icon. This tab displays the client device name, the IP address allocated by the CPE, the MAC address, the mode of connection (whether the device is connected with the CPE through Ethernet or Wi-Fi), and the duration of device connectivity with the CPE. You can even block the device from accessing the Internet by clicking on the "block" button.

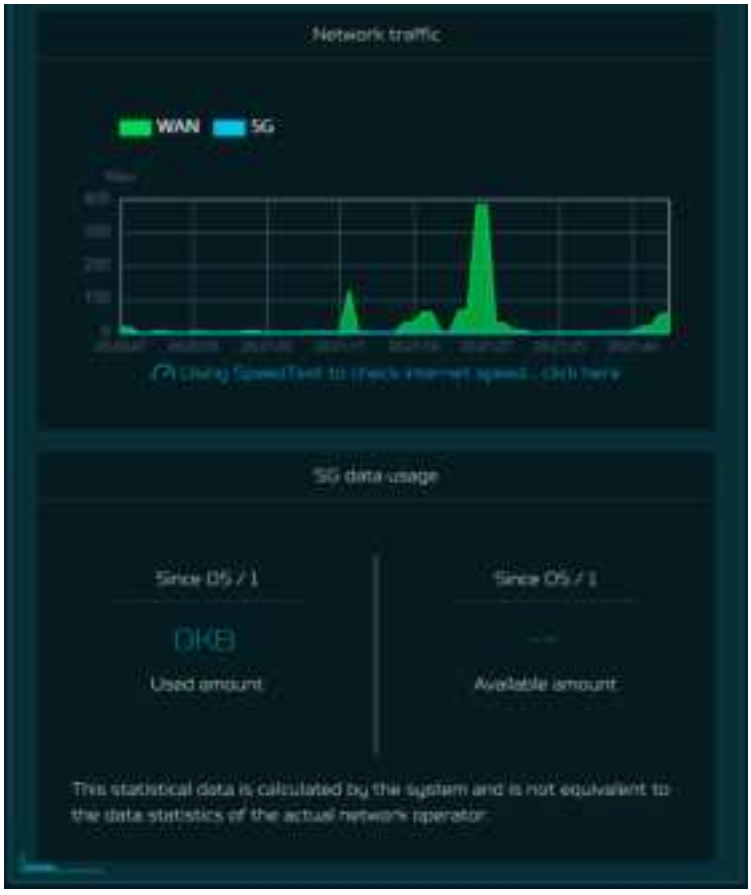
Network Traffic: helps indicate real time connectivity speed of Ethernet WAN & 5G.

You can even check the internet speed by clicking on the Speed Test, powered by Ookla.

This tab also displays the information about 5G data usage from when the data package was activated on the SIM.

You can easily track the amount of used and available 5G data through the X7 CPE's dashboard.

Note: The statistical data is calculated by the system and is not equivalent to the data statistics of the ISP (Internet Service Provider).



Network Speed Test:
Powered by Ookla. A push of the "Speed Test" button tests the speed of the WAN connectivity.

You can even manually select the server option. Click on the dropdown box and it will display the available servers.

It will test and clearly show the network download and upload speed in Mbps, ping rate, and jitter in milliseconds.

After getting the speed test results, you have the option to run the speed test again.

5. Hybrid QoS

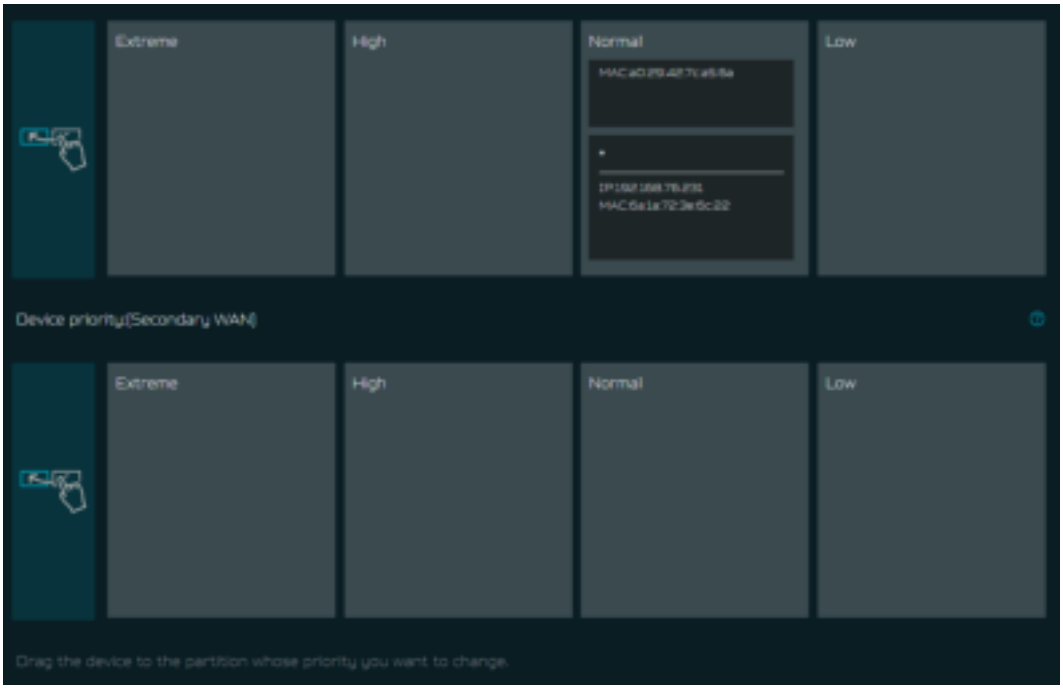
Hybrid QoS combines application priority and device priority. The Killer-Enabled PC can set applications priority and send packets with DSCP values to the Predator Connect X7 CPE, then the CPE will classify packets and set priority for all different applications based on the below definition.
For non-Killer-Enabled devices, Predator Connect X7 can identify game consoles, streaming devices, computers, smartphones, and IoT devices in the network and allocate them a priority group according to the default settings, or the user can manually set priority for devices connected to the CPE.

*Note: Device identification requires the network security engine option enabled.
Application-based QoS* priority: (Enabled by default)

*Note: Application Priority will use the DSCP value in the IP header for packet classification. Laptop/desktop with Killer™ embedded traffic priorities in four grades by application. I.e. Extreme (Games), High (Streaming), Normal (Browsing), Low (Download).

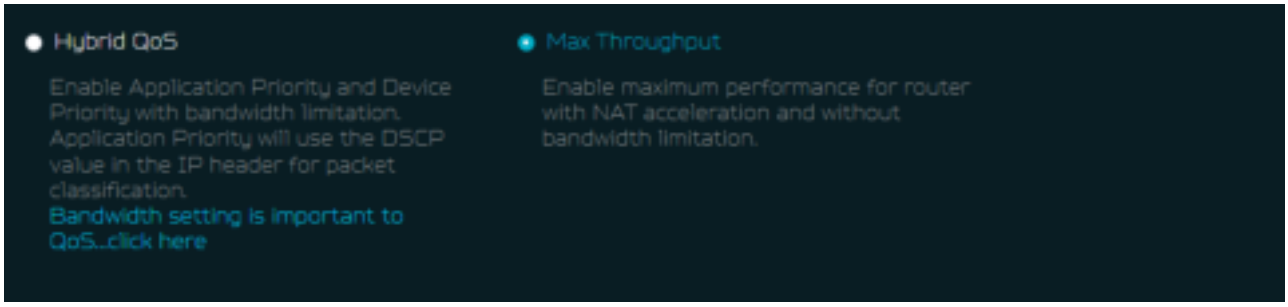
Priority	Extreme (Games)	High (Streaming)	Normal (Browsing)	Low (Download)
Applications (DSCP) Intel Killer Teams/Zoom, GT-Booster	· Killer Priority 1 (Games) · Killer Priority 2 (Real Time)	· Killer Priority 3 (Streaming)	· Killer Priority 4 (Browsing)	· Killer Priority 5 & 6 (Cloud Download)
	· Teams/Zoom Voice	· Teams/Zoom Video	· Teams Shared Screen	
Devices	· Game Port Connected · Game Console: PS, Xbox, Switch	· Chromecast, FireTV, Roku · SmartTV	· Computers, Smartphones · Other Devices	· IoT Devices, Wearable

Device priority (Primary WAN and Secondary WAN):
Note 1: Killer-Enabled PC is set to default extreme priority whether connected by wired Ethernet or by wireless.
Note 2: You may drag and drop connected clients into the desired priority level. The change is effective immediately.



For the upload and download **bandwidth** configuration, please contact your ISP to get the exact value of the upload and download bandwidth. Once the bandwidth is configured, QoS will reserve the bandwidth according to the weighting percentage of each priority queue.

You may select “use default configuration” and click on “Apply bandwidth”. You can select “setting Otherwise, manually” and enter the required upload and download bandwidth with priority weighting.



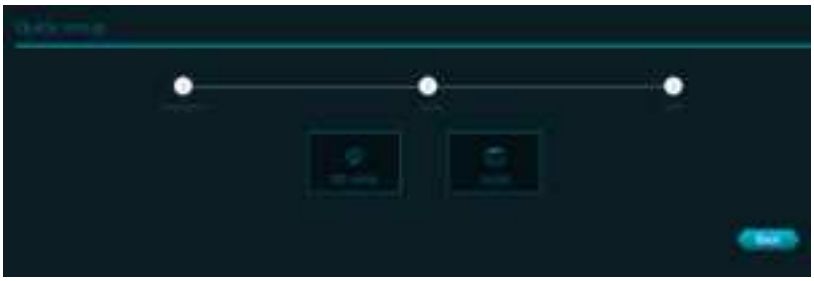
For enabling CPE maximum performance with NAT acceleration and without bandwidth limitation, please select the option “**Max Throughput**” in this case.

6. Quick Setup

The Predator Connect X7 can operate as a standalone Wi-Fi router or establish a Mesh network. Please select a mode which this device will operate in:

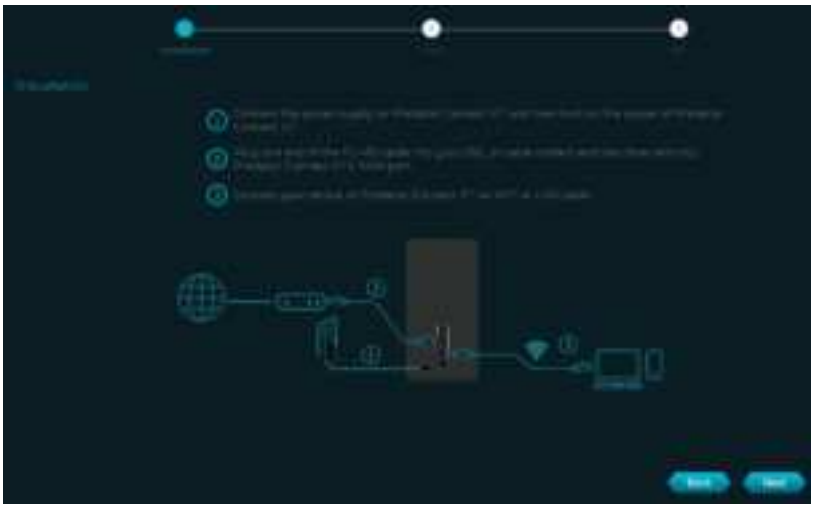
1) Router Mode
2) Mesh Controller

In the **Router mode/Mesh controller mode**, you will have two options; either select 5G WAN or Ethernet WAN connection.



In Ethernet WAN connection, plug one end of the RJ-45 cable into your DSL or cable modem and the other end into Predator Connect X7's WAN port.

Connect your device to Predator Connect X7 via Wi-Fi or LAN cable.



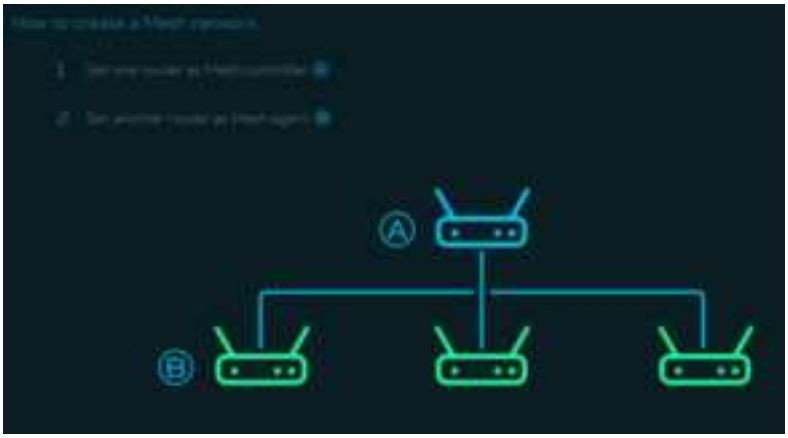
In 5G WAN connection, it will guide you to set up the CPE with a 5G SIM.

1) Connect the power supply to the Acer Connect X7.

2) Insert the SIM card into the SIM card slot at the bottom of the Acer Connect X7.

6.1 How to create a Mesh network

To create a mesh network, set X7 as a Mesh controller (A) and set another router (for example: Acer Connect T7) as a Mesh agent (B). Please note that the X7 can only be set as a Mesh controller.



To ensure better performance, it is recommended not to use wireless to connect more than 2 agents in series, but you can connect multiple agents behind the controller. Or you can use LAN cable to connect more than 2 agents in series.

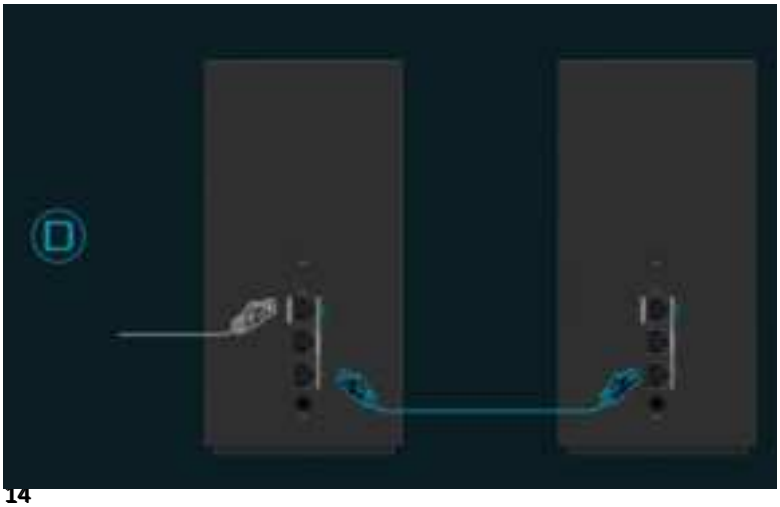
Following are the steps to create a Mesh network;

1. Go to quick setup and set the X7 as a Mesh controller.
2. Power on the other Predator router (for example: Acer Connect T7) and set it as a Mesh agent.
3. Place both the routers close to each other.

There are two ways to onboard an agent to a Mesh network.

I. Press the WPS button on both devices for 2 seconds at the same time.
II. Connect agent to the controller via LAN cable.

If the agent is successfully onboarded to the controller, the LED will be breathing blue, otherwise the LED will become a solid red color.



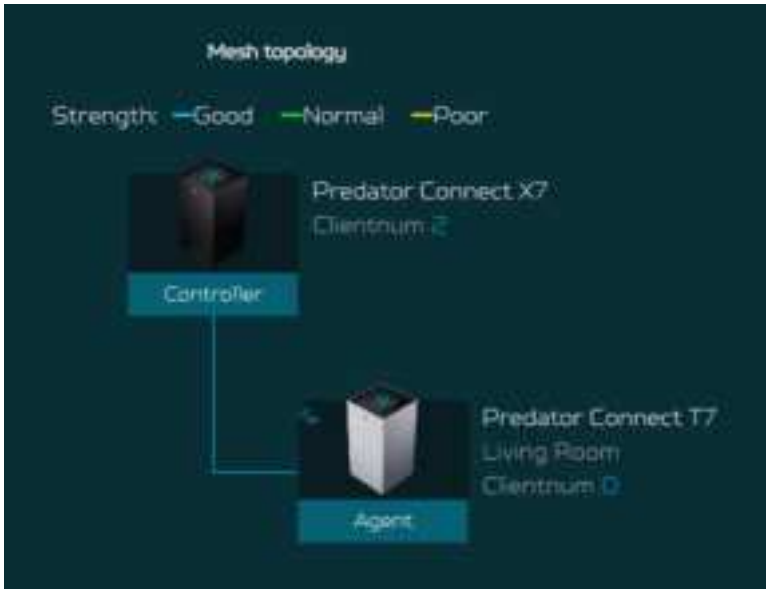
Power off the agent device, move it to another place, and then power ON. Then observe the agent's LED color. Agent's LED color shows RSSI indication between a controller and agent.

The Blue color means RSSI is good, Green color means RSSI is normal, Orange color means RSSI is poor, Red color means disconnected.

6.1.1 Mesh Topologies

Following are the mesh topologies:

- Topology – One agent
- Start topology – 3 agents
- Daisy chain topology – 2 agents
- Tree topology – 3 agents



Topology – One Agent

In one agent topology, a controller is connected with one agent, and the medium between a controller and the agent can be wireless or wired connectivity. Blue color line indicates the good signal strength between a controller and the agent, so it is always recommended to place an agent close to the controller.

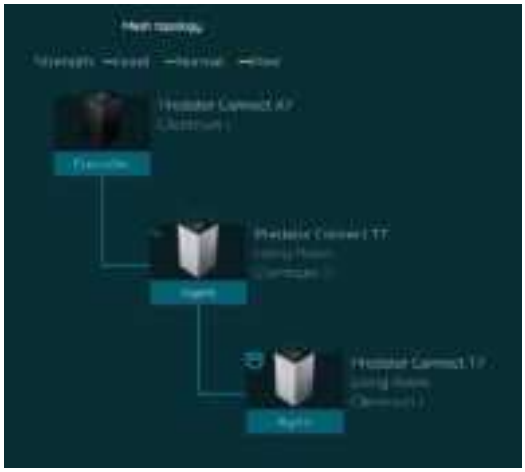
Star topology – 3 agents

In start topology of 3 agents, a controller is simultaneously connected with the three agents, and the medium between a controller and the agents can be wireless or wired connectivity.

Daisy Chain topology – 2 agents

In daisy chain topology of 2 agents, a controller is wirelessly connected with the first agent, and then an agent is connected with the second agent through Ethernet cable, making a chain topology.

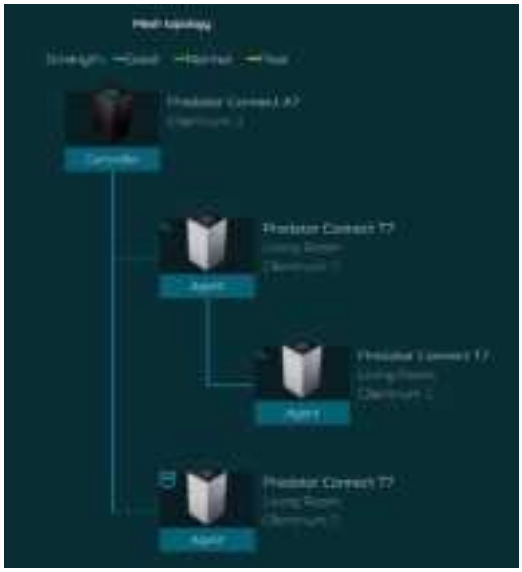
Blue line indicates a good signal strength.



Tree topology – 3 agents

In tree topology of 3 agents, a controller is connected with the two agents; whereas a third agent is connected with the first agent, making a tree topology.

Medium between a controller and the agents can be wireless or wired connectivity.



Agent information

From this tab, you can see the agent's information including:

1) Location
2) Model number
3) IP address
4) Serial number
5) Firmware version
6) Devices connected with the agent
7) Agent backhaul connectivity.

There are some limitations in our mesh which are listed below:

I. Due to the adoption of front-haul and backhaul sharing bandwidth to connect various nodes in the Mesh network, if the Mesh agent is in a daisy-chain configuration, each layer of connected nodes needs to simultaneously handle communication with both upper-layer nodes and lower-level devices. As a result, the available bandwidth speed will be halved and evenly distributed. Based on this limitation, we recommend that users assemble the Mesh network using Ethernet cables to connect the nodes. This will avoid rate loss due to shared bandwidth (achieving lossless conditions). If users must connect the nodes wirelessly, we suggest forming a star topology network to prevent significant rate reduction caused by multi-tiered connections.

II. All devices are factory-defaulted as CPEs. Users can change the device role (e.g., Mesh controller, Mesh agent) through Quick Setup.

III. Once a device has been set as a Mesh controller or Mesh agent, changing the device role requires restoring the device to its factory settings before the role change can be made. Note: When the current device is a CPE, it can be changed to other roles such as Mesh controller or agent (using GUI operation mode or Quick Setup).

IV. Mesh supports WPS Onboarding, but in cases where connection is hindered due to environmental interference, it's recommended to move the agent closer to the controller, or restore the device to its factory default settings and follow the Quick Setup process to reconfigure the agent. Alternatively, you can perform the setup steps via Ethernet connection.

V. If the Mesh Wi-Fi SSID or password is changed in an existing Mesh network, agents will apply the new configuration after the synchronization process is done. If the agent does not apply the new configuration successfully or the agent is in the offline status, it must go through the onboarding process with the controller again. This is necessary for the updated SSID or password to be applied to these agents.

7. 5G Network

7.1 5G Network Status

This tab displays key information about 5G NR/4G LTE networks such as:

• **SIM status:**
Shows verification status of your SIM.

• **Connection status:** You can reconnect X7 to the internet by pressing the connect button on the right if the connection status is disconnected.
• **My number:** Showing the phone number of your 5G NR/4G LTE SIM card.
• **Network name:** Showing the network name provided by the ISP (Internet Service Provider).
• **Network type:** Auto (5G SA/NSA/4G LTE) or Auto (5G NSA/4G LTE) or 5G SA only or 4G LTE only.
• **RSRP:** Reference Signal Received Power.
• **RSSI:** Received Signal Strength Indicator.
• **Band:** Current camped band for 4G LTE and 5G NR.
• **Cell ID:** Current camped cell ID for 4G LTE and 5G NR.
• **Configuration name:** APN configuration name.
• **IPv4 address**
• **IPv6 address**

7.2 Network Connection

Network Connection allows you to configure the connection mode to auto or manual and enable/disable the data roaming.

7.3 Connection Configuration Mgmt.

Connection configuration management allows you to set up a new APN profile or edit/delete existing profiles that have been created.

Note: The maximum number of configuration is 15.

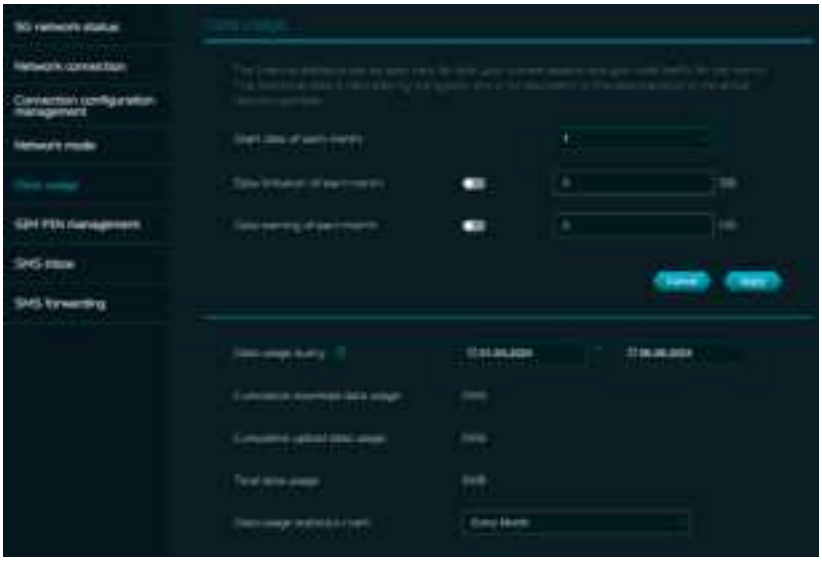
7.4 Network Mode

Click on the drop-down box to select the network mode among the following options: Auto (5G NSA/4G), Auto (5G SA/NSA/4G), 5G SA only, 4G only.

7.5 Data Usage

Internet statistics can be seen here for both your current and your total traffic for the whole month. This statistical data is calculated by the system and is not equivalent to the data statistics of the ISP (Internet Service Provider). You can select the start date of each month on your own, and limit and warn the monthly data usage in GBs.

You can even view the data usage from time to time, cumulative download and upload data usage, and total data usage in graphical representation.



7.6 SIM Pin Management

SIM pin is a password used to control the rights to use a SIM card, and prevents unauthorized users from using it.

Note: If you fail to enter the correct PIN code 3 times in a row, the SIM card will be locked. You can unlock the SIM card by entering the PUK code. If you fail to enter the correct PUK code 10 times in a row, the SIM card will be locked permanently. If you have lost or forgotten your PIN (PUK) code, contact your service provider.

7.7 SMS Inbox

The SMS inbox is where you can view all of your account's incoming texts.

A total of 100 SMS texts can be stored and viewed from this tab.

7.8 SMS Forwarding

Forward SMS messages to a recipient's mobile number by enabling this feature and enter the recipient's mobile number.

8. WAN

8.1 WAN Status

This tab provides information about WAN connectivity status and the following key information:

- Time duration (format HH:MM:SS)
- MAC address
- Connection Mode: DHCP, static IP, PPPoE, etc.
- IP address
- Subnet mask
- Default gateway
- Primary & Secondary DNS server

8.2 WAN Setting

On this page, you can set up Ethernet WAN connection mode to DHCP, Static IP or PPPoE.

8.3 Dual WAN setting

Predator Connect X7 has two WAN connections: 5G NR and Ethernet WAN. User can select primary and secondary WAN as per the priority. Users can select dual WAN mode as a failover or load balance.

Note: Please be aware that changes to the dual WAN mode could affect your network connection. Client devices may be disconnected and reconnected again.

8.4 DMZ

DMZ is physical or logical subnetwork that protects and adds an extra layer of security to an organizations internal local area network from untrusted traffic

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. The host IP address needs to be entered and then external users will have access to all services.

8.5 WAN Ping

By enabling this feature, WAN port ` of Predator Connect X7 will respond to ping requests that are sent to the WAN IP address from the Internet.

For better security, keep the feature turned OFF, and the device will not respond to a WAN ping.

8.6 Firewall

Set up firewall rule to accept or drop network requests from the Internet. To set up a firewall, click on (+) icon to enter the name, source and destination port, source and destination IP address, and protocol to get the status information.

8.7 NAT pass-through

NAT pass-through allows a Virtual Private Network (VPN) connection to pass through the CPE to the external network.

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. To add any application, click on (+) icon and select a required service.

You can select any service profile from common services tab and it will then automatically show its name, the port number and its protocol.
Enter the LAN IP address and select the status ON/OFF and click on the “Apply” button to activate the service.

We have added a new game console profile including:

- Xbox network
- Play Station 5
- Play Station 4
- Nintendo SWITCH
- Nvidia GeForce Now
- Steam

8.9 VPN Server

Set up the VPN server on Predator Connect X7 for remote VPN connection over the Internet. This CPE offers following VPN service:

7.9.1 OpenVPN

The user needs to generate a certificate before enabling the VPN server. Once you create a VPN server, the VPN connection link establishes and the status will be shown. It will display the connection type, remote & local IP address, and duration information.

Open VPN is SSL VPN and uses a chosen UDP or TCP port, allowing for flexible configuration choices. User access consists of two different options; Home network, Internet and home network. Users can also export OpenVPN configuration file (client.ovpn).

Enter the following information to configure Open VPN services.

1) WAN IP address
2) Service port
3) VPN subnet
4) VPN netmask

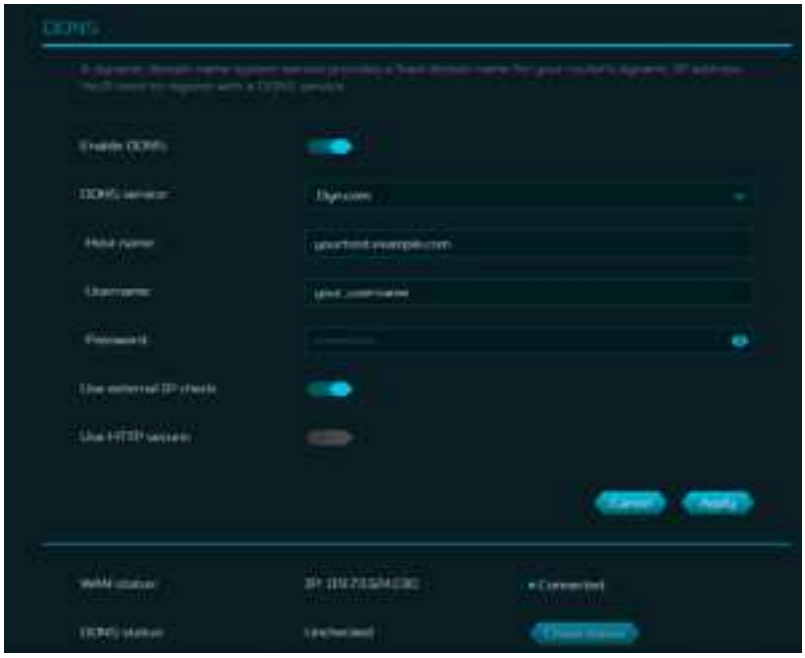
8.10 DDNS

A DDNS service provides a fixed domain name for your CPE's dynamic IP address. You will need to register with a DDNS service among the following ones.

1. Dyn.com
2. No IP
3. Google domain
4. Cloudflare.com

Once you select the DDNS service, enter the host name, username and password, and click on 'Apply' button to activate the DDNS service.

DDNS and WAN status will be shown once the DDNS information is entered.



9. Wi-Fi

9.1 Wi-Fi Status

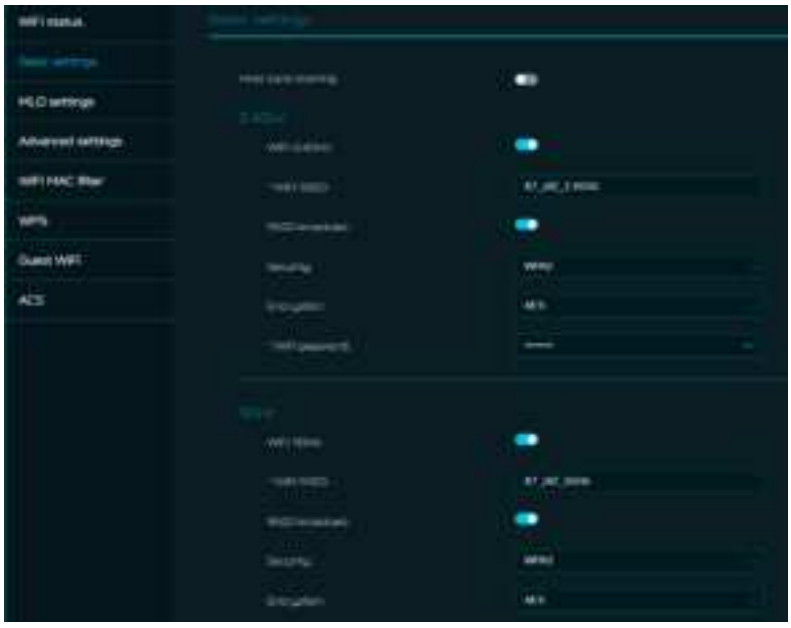
Displays the key information such as:

- Wi-Fi SSID
- SSID Broadcast
- Security
- Channel
- Connected devices
- Gateway address
- Mac addresses of 2.4GHz, 5GHz & 6GHz bands

9.2 Basic Settings

On this page, you can edit the basic Wi-Fi settings of 2.4/5/6GHz frequency bands. You can set the Wi-Fi SSID, security, encryption and Wi-Fi password.

Host band steering is disabled by default. By enabling band steering, it automatically connects your devices to the best available Wi-Fi frequency in the surroundings.



9.3 MLO Settings

Wi-Fi 7's MLO (Multi-Link Operation) is a major technical advancement. It enables devices to simultaneously send and receive data across different frequency bands and channels. It's the reason why the new standard can achieve and maintain 1ms latency, even for the most data-demanding, real time applications. Connecting to MLO network enhances throughput and improves network efficiency. When the mesh is activated, the backhaul settings between the controller and the agents are set to default MLO's 5+6G.

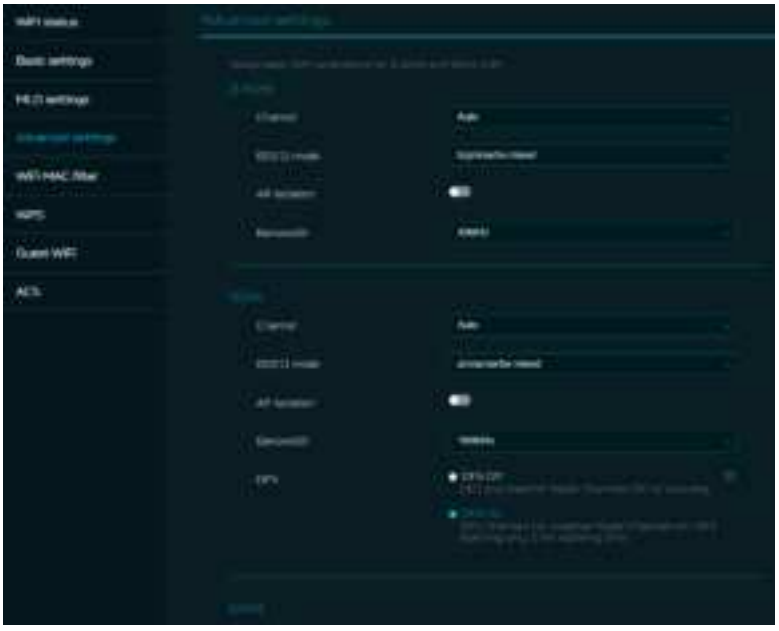
9.4 Mesh Wi-Fi (In Mesh Mode)

This tab provides information about Mesh Wi-Fi SSID and password.

Band steering is ON by default in mesh mode. It automatically connects your devices to the best available Wi-Fi frequency in the surroundings.

9.5 Advanced Settings

This tab will help you to set up advanced Wi-Fi parameters for 2.4GHz, 5GHz & 6GHz band.



AP isolation is a feature that enables you to create a separate virtual network preventing client communicating with each other and preventing unwanted hacking. This feature is disabled by default.

The full list of **PSCs** is:5, 21, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213 and 229.
802.11 mode will be “b/g/n/ax/be mixed” by default. 802.11be (Wi-Fi 7) standard aims to implement wireless communications at much faster speeds and larger capacities than the previous 802.11ax.

9.6 Wi-Fi MAC filter

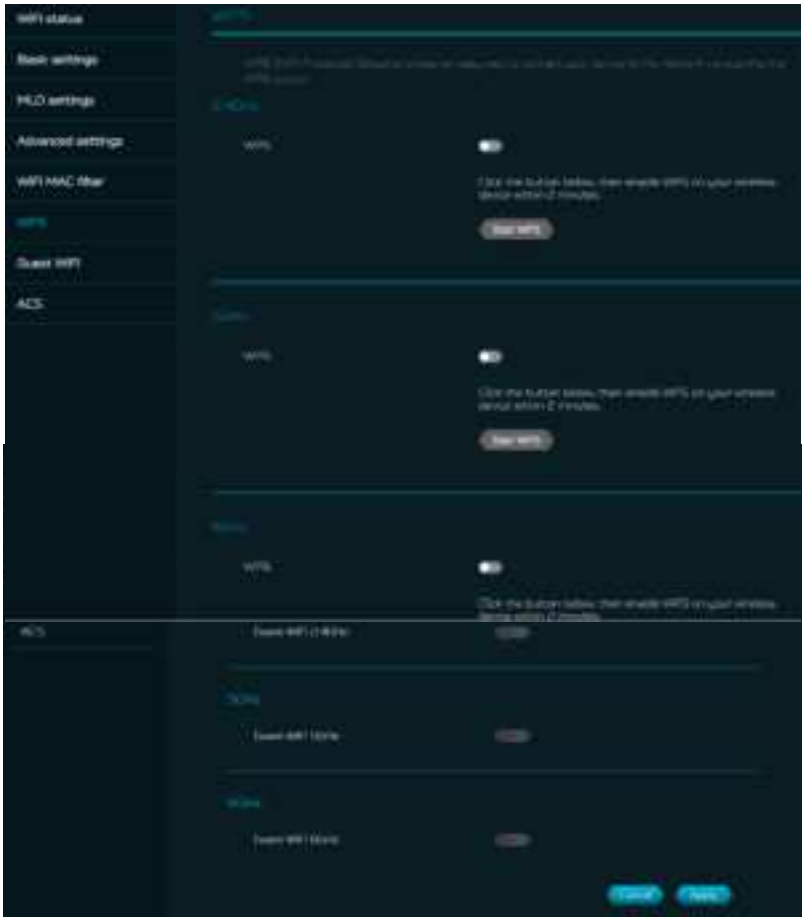
Devices that are added to the Wi-Fi MAC filter will be blocked from accessing the Internet.

Click on the (+) icon to add the device in the filter table by entering its name & MAC address. Up to 32 devices can be added to the MAC filter.

9.7 WPS

WPS (Wi-Fi Protected Setup) provides an easy way to connect your device to the network by pushing the WPS button or click “Start WPS” on UI, then enable WPS on your wireless device within two minutes.

WPS will be disabled, if Wi-Fi security is set to WPA3, WPA, or TKIP mode, or if the SSID broadcast is turned off.



9.8 Guest Wi-Fi

This tab provides information about the Internet connection for guests and their devices accessing your network.

Guest Wi-Fi password is set by default for all bands, so it is suggested changing the passwords for security reasons.

9.9 ACS (Automatic Channel Selection)

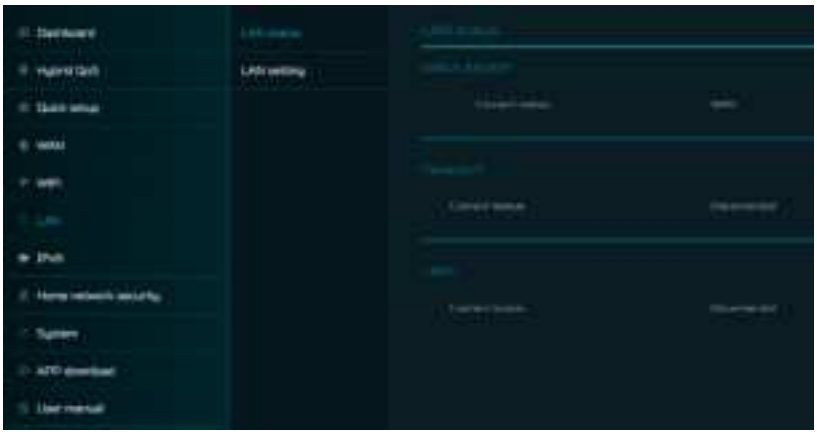
ACS is a mechanism to optimize the channel assignment. It selects the best working channel dynamically, one that is clear and has the least traffic.

Note 1: There will be a small delay, rescanning, and then cycling OFF and ON if the client is associated with the ACS enablement band. Please check your device’s wireless connection and select the best Wi-Fi X7 CPE SSID after the ACS process is completed.

Note 2: The ACS is not applicable if all three bands (2.4GHz, 5GHz, and 6GHz) are configured as fixed channels. ACS also works in a mesh mode and when the device is in mesh mode, this will trigger channel planning.

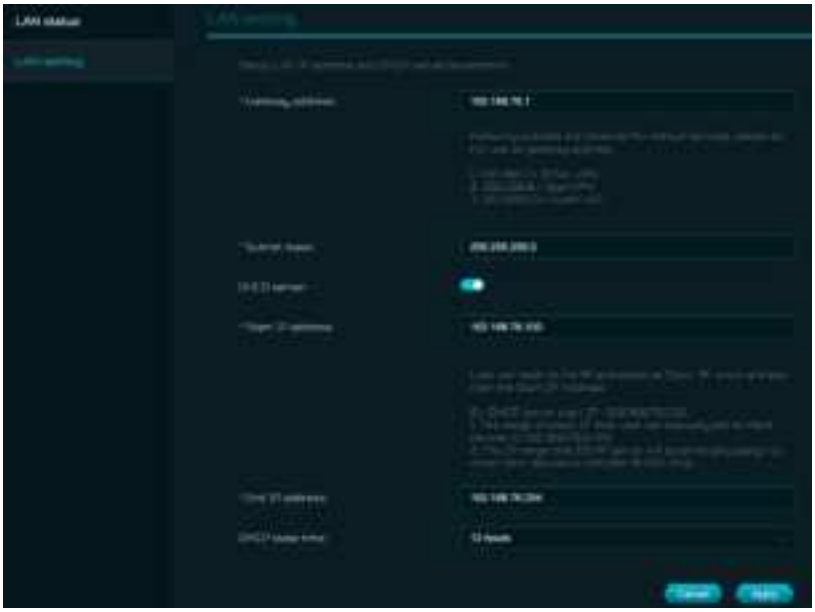
10. LAN

LAN status
On this page, you can view each LAN port status including its associated IP address, MAC address and DHCP server. The Predator Connect X7 has one Game port and two LAN ports, with one port configurable as WAN/LAN port.



LAN Setting
This tab allows you to set up LAN IP gateway address with an option to enable or disable the DHCP server feature. You can enter the gateway address and subnet mask. DHCP provides and assigns IP addresses, default gateways, and other network parameters to client devices. DHCP server can be enabled or disabled as per the network requirement.
The following subnets are reserved for default services. Please do not use it as a gateway address.

1. 192.168.7.x (IPsec VPN)
2. 192.168.8.x (Open VPN)
3. 192.168.10.x (Guest Wi-Fi)



11. IPv6

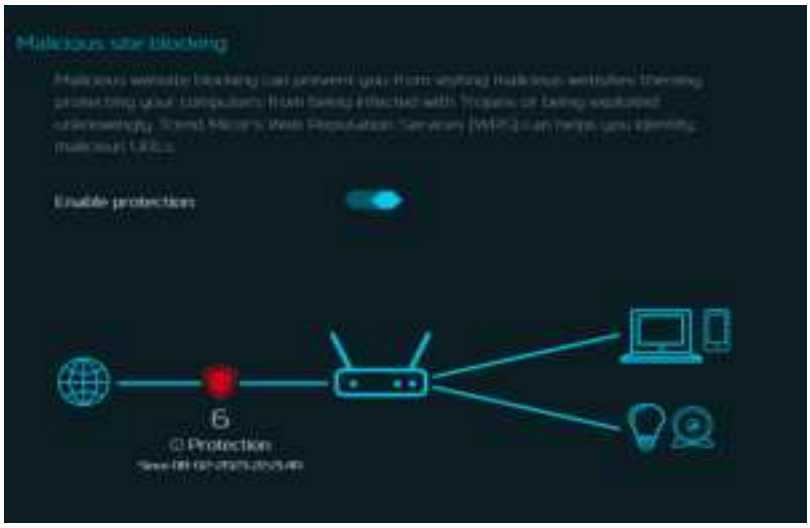
You can set up IPv6 settings from this tab. The Predator Connect X7 supports IPv6 mode below: DHCPv6, static IPv6, PPPoE, 464xlat, 6rd, DS-Lite. Connection mode will be disabled by default.
Please consult local Internet Service Provider before enabling and configuring this option.

12. Home Network Security

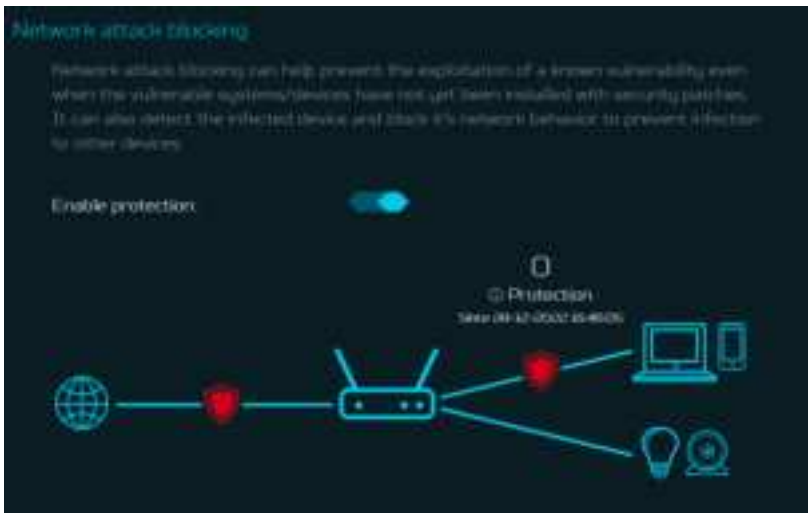
The home network security tab includes network security settings and web & app controller settings within the parental control feature. These two features must accept the Trend Micro license agreement before enablement.

12.1 Network Security Setting
This tab contains the network security-related information, powered by Trend Micro, where you can turn on/off the security engine and enable protection against malicious sites, network attacks and harmful connections coming from IoT devices.

Malicious site blocking prevents unwanted sites to open and hence protecting your computer from being infected with Trojans. There is a feature called “Trend Micro’s Web Reputation Service (WRS) that identifies malicious URLs and allow you to take action against infected URLs.

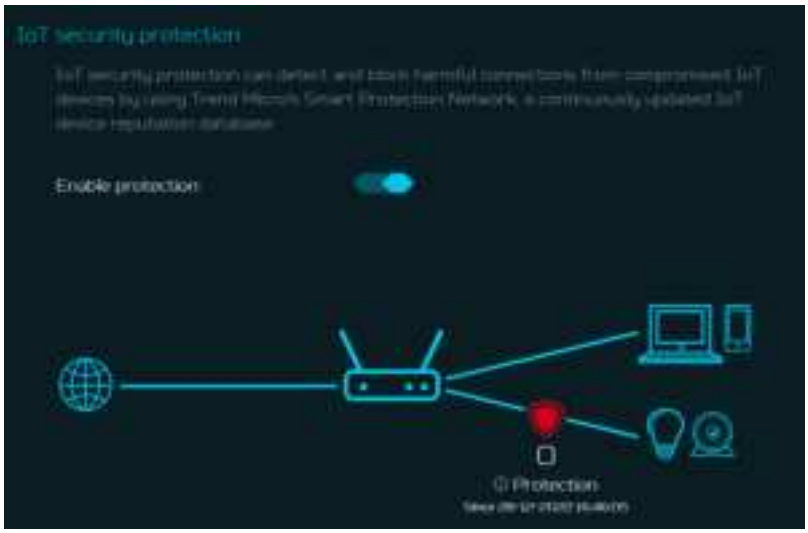


By enabling **Network attack blocking** feature, the CPE detects the infected devices and block its network behavior to prevent infection in other devices.



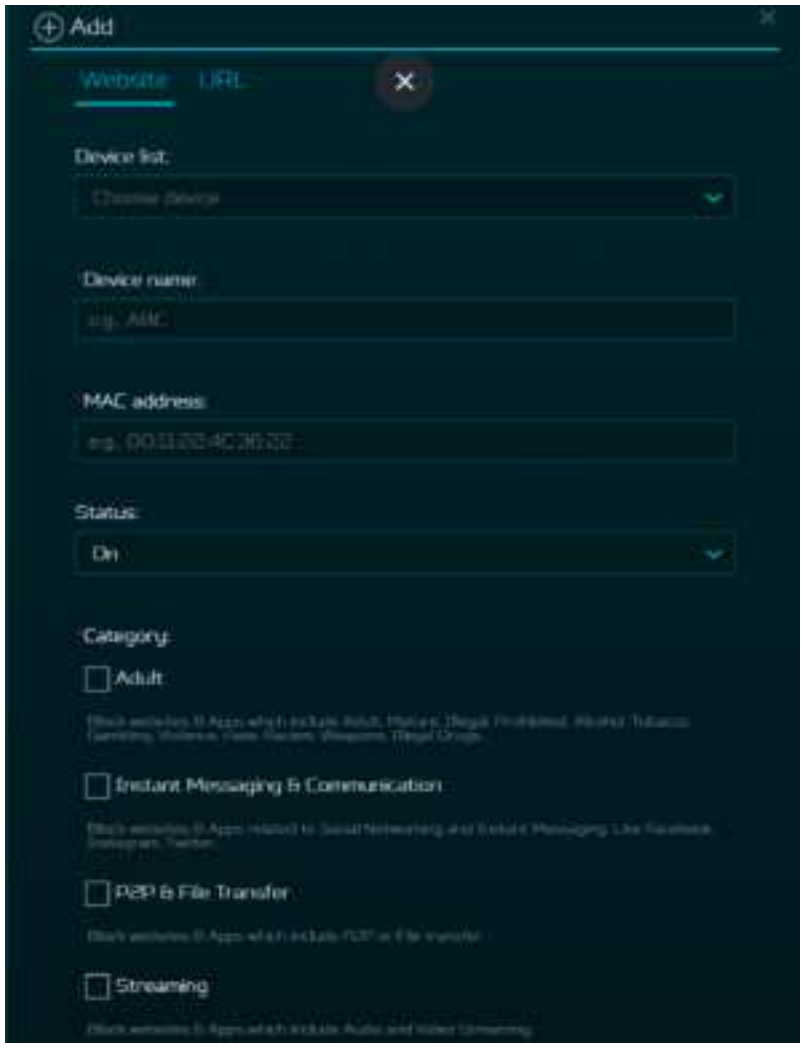
Enabling **IoT security protection** feature detects and blocks harmful connections from compromised IoT devices by using Trend Micro's smart protection network.

It's a continuously updated IoT device reputation database that prevents the network from false connections.



12.2 Parental Control
This feature allows you to control and block unwanted sites on specific devices. You can enable/disable Web & App controller and URL controller.

Once you click on (+) icon, the following window will appear and here you can enter the device list, device name, its MAC address, status and select the following categories for blocking the websites.



Adult
Block websites and Apps which include Adult, Mature, Illegal, Prohibited, Alcohol, Tobacco, Gambling, Violence, Hate, Racism, Weapons, Illegal Drugs related content.

Instant Messaging & Communication
Block websites and Apps related to Social Networking and Instant Messaging like Facebook, Instagram, Twitter etc.

P2P and File Transfer
Block websites and Apps which include P2P or File transfer.

Streaming
Block websites and Apps which include Audio and Video streaming.

Under the URL tab, you can enter the device list, device name, its MAC address and URL, which you want to forbid access to e.g. www.aaaa.com. Or you can add a keyword e.g. AAAA to forbid any URL containing the keyword.

You can also enter the Internet access time limit by setting the start time and end time.

Note: If the end time is earlier than the start time, the block time will cross to the next day. If the start time is the same as the end time, the block will be for a full day.

13. SYSTEM

13.1 Operation Mode

This Predator Connect X7 can operate as a standalone Wi-Fi router, Modem, or establish a Mesh network.

Please select a mode which this device will operate in.

13.2 Login Password

You can change the login password of your Predator Connect X7 from this page.

To create a new login password, you need to enter your current password first. Please use a strong login password to keep the device secured.

13.3 System Time

This tab allows you to synchronize the device time with the system time by enabling “Automatically set time zone”.

By enabling “daylight savings time”, the device will automatically adjust the time according to the time zone.

13.4 languages

You can select the web UI language of your Predator Connect X7 from this tab.

13.5 Backup and Restore

In this tab, you can check how to save the configuration:
Click on "Backup" to backup the current device configuration. On both Windows and MAC OS, this is saved to your 'Downloads' folder.

How to restore the configuration:
1) Click Browse to select a file
2) Click Restore

13.6 System Information

This tab displays key information of Predator Connect X7, such as:

- Device name
- IMEI
- Serial number
- Firmware version
- Web version

13.7 Restart and Reset Default

In this tab, you can click on "Restart device" to reboot the CPE and click on "Factory data reset" to restore the factory default settings.

Please check if you bind your device with Predator Connect Mobile App. After the factory reset, please don't forget to unbind the device from the mobile App.

13.8 Firmware Update

In this tab, you can check the existing firmware version. You can also click on "check new", to see if there is an update available.

13.9 System Log

The system logs consists of general logs and Wi-Fi logs. It will display here all the recent 100 activities you have done with the CPE.

You can save the system logs by clicking the “Save log” button at the bottom of the page. The main purpose of savings logs is to allow the logs to be saved and sent back to Acer for analysis, if there are issues encountered.

13.10 USB Storage

This CPE has a USB type-c port where you can plug in a USB drive and allow all authorized users to access the files on your USB drive. Once you plug in a USB drive, it will display device type, size and free space available.

Enter the server name and login credentials for shared access to the USB drive. In sharing setting, there is an option to enable/disable Network neighborhood (Samba).

13.11 Main LED

This tab displays information about CPE LED colors and its indication. These LED indicators will help you to know and understand the CPE behavior.

By enabling **LED night mode**, it only dims the device’s luminance. Please check if you have already set up the correct time zone (auto/manual), before enabling this option. You can set up the daily schedule as needed. Please refer to the following light definitions, as the X7 has two LEDs; mask and front.

X7	Mask LED	Blue flashing LED	The router is powering on.
	Mask LED	Solid Blue LED	The router is powered on.
	Mask LED	Blue breathing LED	WAN status is good.
	Mask LED	Green breathing LED	WAN status is normal.
	Mask LED	Orange breathing LED	WAN status is poor.
	Mask LED	Solid Red LED	WAN is disconnected. (No internet)
	Mask LED	Green flashing LED	WPS is active. Mesh on-borading
	Mask LED	Orange flashing LED	The firmware is being upgraded.
	Mask LED	White flashing LED	The router is performing a factory reset.
	Mask LED	PING Server	PING site: (default is Google server, user can add and edit PING Server) if 8.8.8.8 cannot be accessed then access the second one 8.8.4.4 . . .and so on 1.8.8.8.8 (default) 2.8.8.4.4 3.4.2.2.2 4.1.1.1.1 5.1.0.0.1 or Ping 2001:4860:4860::8888 (IPv6)
	Mask LED	LED status of internet	Blue : connection is good Green: connection is normal Orange: connection is Poor Red : disconnect
	Mask LED	PING Rule	send out 4 PING requests with interval 1 sec, in every 60 secs, If packet loss =0, the condition is good (LED flashing Blue); If packet loss <= 25%, the condition is not good(LED flashing Green) If packet loss > 25%, the condition is bad(LED flashing Orange)
	Front LED(Wi-Fi)	Blue flashing LED	The device is powering on.
	Front LED(Wi-Fi)	Solid Blue LED	The device is powered on and Wi-Fi AP is ready. (2.4GHz band or 5GHz band or 6GHz band)
	Front LED(Wi-Fi)	Solid Red LED	The device is powered on and Wi-Fi APs have a problem. (2.4GHz band and 5GHz band and 6GHz band)

14. APP Download

User can download the mobile App by scanning the QR code, available in “App download” tab, to control the following features:

1. Quick setup assistance
2. Control the CPE remotely
3. Get notifications of:

   i) CPE Internet disconnection
   ii) USB storage removal

15. Troubleshooting

15.1 Quick Tips

This section describes common issues which you can encounter.

Sequence to restart the device and network:

1. Turn off and unplug the CPE power plug.
2. Plug in the CPE power plug and then turn it on. Wait for two minutes till the CPE LED is steady as before.
3. Wait for the device's upper deck main LED to steady breathing.

15. 2 Frequently Asked Questions (FAQs)

15.2.1 What can I do if I forget my wireless password?

- Connect to the X7 CPE via Ethernet LAN cable.
- Visit device portal http://acer-connect.com and login admin.
- Go to Wi-Fi -> Basic settings/Retrieve or reset the Wi-Fi passwords.

15.2.2 What can I do if I forget the CPE's web portal admin password?

Reset the device by pressing and holding the reset key until the LED starts blinking white. After the device restores to factory default, please login web admin portal with admin PWD, label printed on the bottom of the device.

Note 1: The device web admin will be locked after 5 wrong password attempts. The user is required to reboot the device to disable the web admin.
Note 2: Remember to set up the device's internet connection after resetting. Remember to also change the admin password.
Note 3: If you ever bind the device via Predator Connect mobile App; remember to unbind it after the factory data reset.

15.2.3 What can I do if I can't log into the CPE's web admin portal?

Please follow the steps below to check on your client's device.

- Check whether the client-allocated IP and DNS server IPs both are with the same subnet and gateway.
- Clean the browser cookies or use private/Incognito mode to access the CPE admin page.

15.2.4 What can I do if I can't surf the internet even though the configuration is finished?

Please follow the step below to check on your X7 CPE:

- Login to the web admin portal dashboard to check Internet status.
- Continuingly, if the Internet status is up and connect. Go to the WAN setting, manually configure the DNS server using the below IP and apply:

  Primary DNS server: 8.8.8.8
  Secondary DNS server: 8.8.4.4

- If the issue is still there, please restart the modem and CPE accordingly.

16. Regulatory Information

Important Safety Precaution

Your 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.

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.

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.

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

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.

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.

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 storeor 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 52

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.

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.

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

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.53

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.

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.

The MPE (Maximum Permissible Exposure) 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 X7 is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available: Please search for Predator Connect X7 5G CPE at www.acer.com/support

17. Factory Default Settings

CPE web admin	
URL	http://acer-connect.com or http://192.168.76.1
Login Password (case-sensitive)	XXXXXXXX (XXXXXXXX is randomized variables. Please check the device's bottom label)
Local Network (LAN)	
Gateway address	192.168.76.1
Subnet mask	255.255.255.0
DHCP server	192.168.76.1
DHCP range	192.168.76.100 to 192.168.76.254
Time zone	Depends on the country or region you bought the CPE
DHCP starting IP address	192.168.76.100
DHCP ending IP address	192.168.76.254
Time adjusted for daylight save time	Enabled.
Wireless LAN (WLAN)	
Wi-Fi SSID (case-sensitive)	2.4GHz: X7_YYYY_2.4GHz 5GHz: X7_YYYY_5GHz 6GHz: X7_YYYY_6GHz (YYYY is randomized variables. Please check the device's bottom label)
Security	2.4GHz : WPA2/WPA3 5GHz : WPA2/WPA3 6GHz : WPA3
SSID Broadcast	Enabled.
RF channel	2.4GHz : Auto 5GHz : Auto 6GHz : Auto
Default operation mode (with BE enabled)	2.4GHz: 2x2 MIMO streams, 1024 QAM, 40MHz, 573MBps 5GHz: 2x2 MIMO streams, 4096 QAM, 240MHz, 4324Mbps 6GHz: 2x2 MIMO streams, 4096 QAM, 320MHz, 5764Mbps
Guest Wi-Fi	Disabled.
Home Network Security	Disabled.

18. CPE Basic Specification

Processor	System	Qualcomm proprietary BSP
	SOC	Qualcomm IPQ5322 + SDX62 + QCN6274
Memory	LPDDR4X	1GB
	Flash	512MB
SIM	Nano SIM	Nano SIM (push-push)
5G NR Band	Global	SA: n1/3/5/7/8/20/28/38/40/41/75/76/77/78, NSA:n1/3/5/7/8/20/28/38/40/77/78
	US	SA: n2/5/12/14/25/30/41/48/66/70/71/77, NAS: n2/5/12/25/30/41/66/71/77
4G LTE Band	Global	FDD: B1/3/5/7/8/20/28/32, TDD: B38/40/41/42/43
	US	FDD: Band 2/4/5/12/13/29/30/66/71, TDD: Band 41/48/46
Wireless LAN	IEEE standard	802.11 a/b/g/n/ac/ax/be
	Band	Tri-band (2.4GHz + 5GHz + 6GHz) simultaneously
	Max. connected devices	256
Ethernet	WAN	1 x 2.5GbE
	LAN	2 x 1GbE
Antennas	Antennas	Internal
Software Update	Firmware Upgrade	FOTA
USB	Port	USB 2.0 Type-C
	Storage	FTP, Samba
Buttons	Power, Reset, WPS	Yes
LED	LED	Mask LED and front LED
Form factor	Tower	Yes
	Dimension	109mm_109mm_212mm
	Weight	About 1020g
Temperature	Operating Temp.	0°C to 45°C (32 °F to 115 °F)
	Operating Humidity	20% - 80%
	Storage Temperature	-10°C to + 60°C (14 °F to 140 °F)
	Storage Humidity	20% - 60%
Power Adapter	DC	12V 4A, 48W
	AC	100 V -240 V 50 Hz / 60 Hz,
Additional Accessories	Accessories	12V 4A Adaptor and network cable