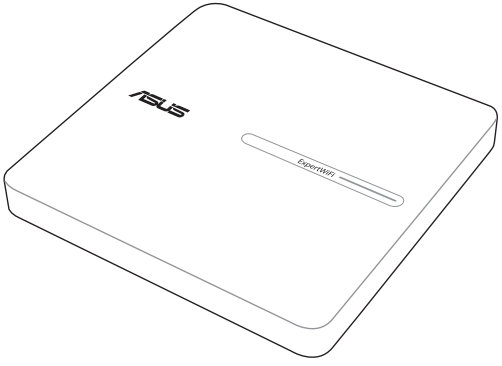
User Guide

ASUS ExpertWiFi EBA63

AX3000 PoE Access Point

Model: EBA63



IN SEARCH OF INCREDIBLE

E23207
First Edition
January 2024

Table of contents

Table of contents

1 Getting to know your EBA63

1.1 Welcome!

Thank you for purchasing an ASUS ExpertWiFi EBA63!

The ultra-thin and stylish EBA63 features a 2.4GHz and 5GHz dual bands for an unmatched concurrent wireless HD streaming and the ASUS Green Network Technology, which provides up to 70% power-saving solution.

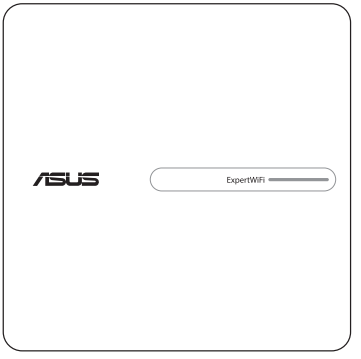
1.2 Package contents

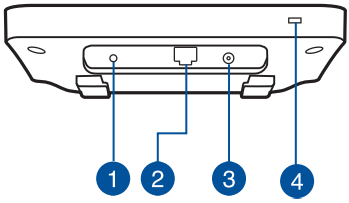
- ☑ ExpertWiFi EBA63
- ☑ Power adapter
- ☑ Warranty card
- ☑ Network cable (RJ-45)
- ☑ Quick Start Guide
- ☑ Mounting kit

NOTES:

- If any of the items are damaged or missing, contact ASUS for technical inquiries and support. Refer to **Service and Support** at the back of this user manual.
- Keep the original packaging material in case you would need future warranty services such as repair or replacement.

1.3 Your wireless access point





1	**Reset button** This button resets or restores the system to its factory default settings.
2	**PoE IN port** Connect a PoE cable to this port for your Power Over Ethernet network.
3	**Power (DCIN) port** Insert the bundled AC adapter into this port and connect your access point to a power source.
4	**Kensington® lock slot** The Kensington® lock slot allows the product to be secured using Kensington® compatible security cable.

NOTES:

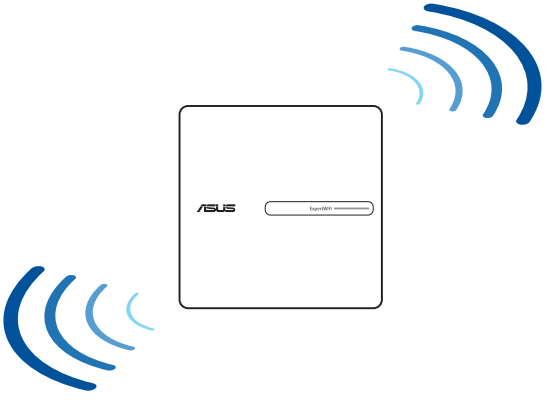
- Use only the adapter that came with your package. Using other adapters may damage the device.
- **Specifications:**

DC Power adapter	DC Output: +12V with max 1.5A current		
Operating Temperature	0~40°C	Storage	0~60°C
Operating Humidity	50~90%	Storage	20~90%

1.4 Positioning your access point

For the best wireless signal transmission between the wireless access point and the network devices connected to it, ensure that you:

- Place the wireless access point in a centralized area for a maximum wireless coverage for the network devices.
- Keep the device away from metal obstructions and away from direct sunlight.
- Keep the device away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.
- Always update to the latest firmware. Visit the ASUS website at **http://www.asus.com** to get the latest firmware updates.



1.5 Setup Requirements

To set up your wireless network, you need a computer that meets the following system requirements:

- Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/ 1000BaseTX)
- IEEE 802.11a/b/g/n/ac/ax wireless capability
- An installed TCP/IP service
- Web browser such as Microsoft Edge, Safari, or Google Chrome

---

NOTES:

- If your computer does not have built-in wireless capabilities, you may install an IEEE 802.11a/b/g/n/ac/ax WLAN adapter to your computer to connect to the network.
- With its dual band technology, your wireless access point supports 2.4GHz and 5GHz wireless signals simultaneously. This allows you to do Internet-related activities such as Internet surfing or reading/ writing e-mail messages using the 2.4GHz band while simultaneously streaming high-definition audio/video files such as movies or music using the 5GHz band.
- Some IEEE 802.11n devices that you want to connect to your network may or may not support 5GHz band. Refer to the device's manual for specifications.
- The Ethernet RJ-45 cables that will be used to connect the network devices should not exceed 100 meters.

1.6 Access Point Setup

IMPORTANT!

- Use a wired connection when setting up your wireless access point to avoid possible setup problems.
- Before setting up your ASUS wireless access point, do the following:
  - If you are replacing an existing access point, disconnect it from your network.
  - Disconnect the cables/wires from your existing modem setup. If your modem has a backup battery, remove it as well.
  - Reboot your cable modem and computer (recommended).

WARNING!

- The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground. Connect the equipment only to a nearby socket outlet that is easily accessible.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- DO NOT use damaged power cords, accessories, or other peripherals.
- DO NOT mount this equipment higher than 2 meters.
- Use this product in environments with ambient temperatures between 0°C (32°F) and 40°C (104°F).

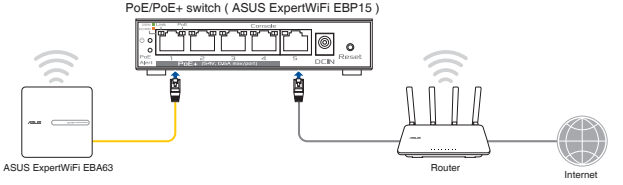
EBA63 LED indications

- Solid green: Your EBA63 is starting up
- Solid blue: Your EBA63 is ready for setup
- Blinking blue: Your EBA63 is syncing with AiMesh node
- Solid white: Your EBA63 is online and works well
- Solid yellow: The signal on your EBA63 is weak

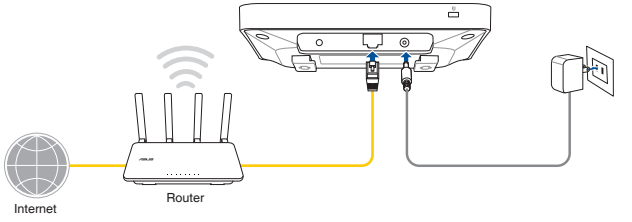
To set up your ExpertWiFi EBA63:

1. Connect ExpertWiFi EBA63 (select either of the options):

   1)Power up EBA63 by connecting the PoE IN port to a PoE switch or PoE gateway.



   2)Connect EBA63 to a router and a socket outlet.



2. Join an existing WiFi network.

   - **Connect to an ASUS router** (ExpertWiFi series / AiMesh compatible router)

     Access ASUS router's web or app (ASUS ExpertWiFi app or ASUS router app) management interface to add EBA63 to your existing AiMesh system with just one click.
   - **Connect to a non-ASUS router**

     Connect your device (mobile device or laptop) to EBA63 using the default network name (SSID) shown on the product rating label.

   [App] Scan the code and download ASUS ExpertWiFi app for setup.

[Web] • Open a web browser and navigate to http://expertwifi.net for web setup.

• Once QIS (Quick Installation Setup) is finished, you can connect to the new SSID and go to http://expertwifi_eba63-XXXX.local for advanced settings.

* XXXX refers to the last four digits of the MAC address shown on the product rating label.

2 Getting started

2.1 Logging into the Web GUI

Your ASUS Wireless Access Point comes with an intuitive web graphical user interface (GUI) that allows you to easily configure its various features through a web browser such as Microsoft Edge, Safari, or Google Chrome.

NOTE: The features may vary with different firmware versions.

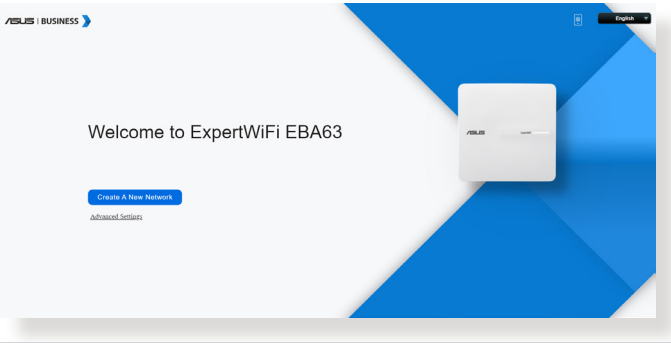
Connecting to your network wirelessly:

1. On your computer, click the network icon in the notification area to display the available wireless networks.
2. Select the wireless network of EBA63, then click **Connect**.
3. Key in the network security key that is shown on the rating label of EBA63, then click **OK**.
4. Wait while your computer establishes connection to the wireless network successfully. The connection status is displayed and the network icon displays the connected status.

Connecting to your network wiredly:

To log into the web GUI:

1. On your web browser, enter http://expertwifi.net.
2. Follow the instructions for setup.

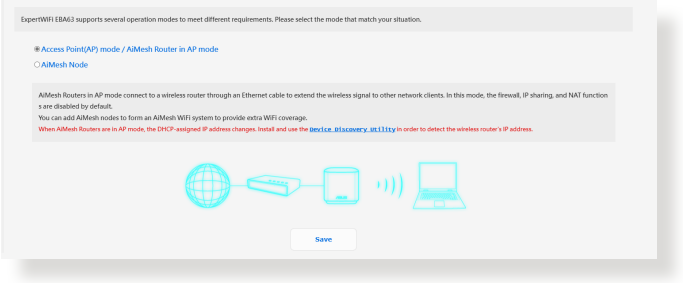


3 Configuring EBA63

3.1 Administration

3.1.1 Operation Mode

The Operation Mode page allows you to select the appropriate mode for your network.



To set up the operating mode:

1. From the navigation panel, go to **Settings** > **Administration** > **Operation Mode**.
2. Select any of these operation modes:
   - **AiMesh mode:** You can add AiMesh nodes to establish an AiMesh WiFi system to provide extra WiFi coverage.
   - **Access Point mode**: In this mode, the access point creates a new wireless network on an existing network.
3. Click **Save**.

NOTE: The access point will reboot when you change the modes.

3.1.2 System

The **System** page allows you to configure your wireless access point settings.

To set up the System settings:

1. From the navigation panel, go to **Settings** > **Administration** > **System**.
2. You can configure the following settings:
   - **Change access point login password**: You can change the password and login name for the wireless access point by entering a new name and password.
   - **USB setting**: You can Enable HDD Hibernation and change USB mode.
   - **Time Zone**: Select the time zone for your network.
   - **NTP Server**: The wireless access point can access a NTP (Network time Protocol) server in order to synchronize the time.
   - **Network Monitoring**: You can enable DNS Query to check Resolve Hostname and Resolved IP Addresses, or enable Ping, then check your Ping Target.
   - **Auto Logout**: You can set the time of auto-logout.
   - **Enable WAN down browser redirect notice:** This feature allows the browser to display a warning page when the access point is disconnected from Internet. When disabled, the warning page will not appear.
   - **Enable Telnet**: Click **Yes** to enable Telnet services on the network. Click **No** to disable Telnet.
   - **Authentication Method**: You can select HTTP, HTTPS, or both protocols to secure access point access.
   - **Enable Reboot Scheduler:** When enabled, you can set the Date to Reboot and Time of Day to Reboot.
   - **Enable Web Access from WAN**: Select **Yes** to allow devices outside the network to access the wireless access point GUI settings. Select **No** to prevent access.
   - **Enable Access Restrictions**: Click **Yes** if you want to specify the IP addresses of devices that are allowed to access to the wireless access point GUI settings from WAN/LAN.

- **Service**: This feature allows you to configure Enable Telnet/ Enable SSH/SSH Port/Allow Password Login/Authorized Keys/Idle Timeout.

3. Click **Apply**.

3.1.3 Firmware Upgrade

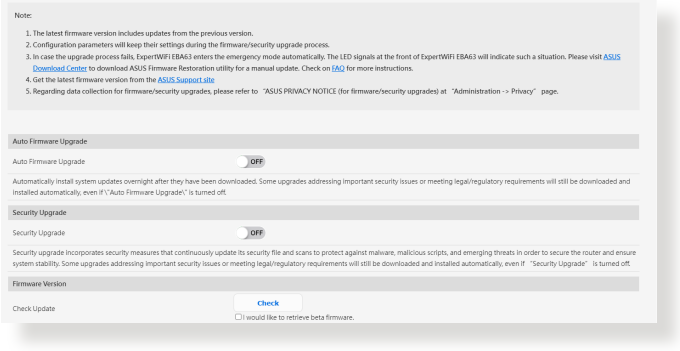
NOTE: Download the latest firmware from the ASUS website at **http://www.asus.com**.

To upgrade the firmware:

1. From the navigation panel, go to **Settings** > **Administration** > **Firmware Upgrade**.
2. In the **New Firmware File** field, click **Browse** to locate the downloaded file.
3. Click **Upload**.

NOTES:

- When the upgrade process is complete, wait for some time for the system to reboot.
- If the upgrade process fails, the wireless access point automatically enters rescue mode and the power LED indicator on the front panel starts flashing slowly. To recover or restore the system, refer to section **4.2 Firmware Restoration**.

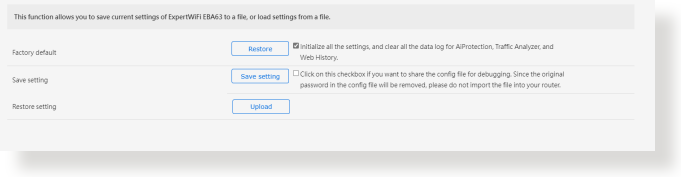


3.1.4 Restore/Save/Upload Setting

To restore/save/upload wireless access point settings:

1. From the navigation panel, go to **Settings** > **Administration** > **Restore/Save/Upload Setting**.
2. Select the tasks that you want to do:
   - **Factory default**: Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer and Web History.
   - **Save setting**: Click on this checkbox if you want to share the configuration file for debugging. Since the original password in the configuration file will be removed, please do not import the file into your access point.
   - **Restore setting**: Upload the restoration settings you want to apply.

IMPORTANT! If issues occur, upload the latest firmware version and configure new settings. Do not restore the access point to its default settings.



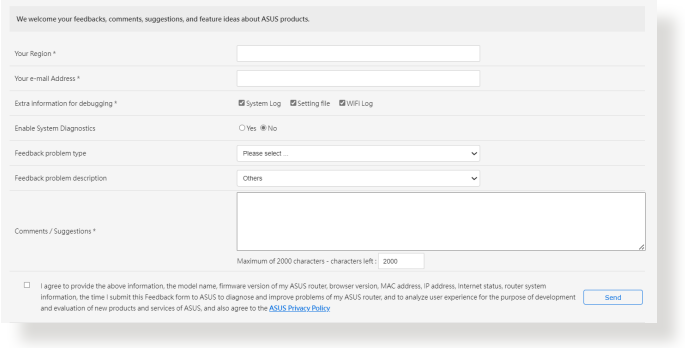
3.1.5 Feedback

To use Feedback:

1. From the navigation panel, go to **Settings** > **Administration** > **Feedback**.
2. Enter your region, e-mail address, extra information for debugging, comments and suggestions, and send your access point log back for troubleshooting.

IMPORTANT!

- Describe your comments on the situation in details to get a quick response.
- Please agree with the ASUS Privacy Policy.



3.1.6 Privacy

1. For account binding, DDNS and Remote connection (ASUS Router app/Lyra app/AiCloud/AiDisk):

Please note that your information, including your product model name, firmware version, Internet status, IP Address, MAC address and DDNS name, will be collected by ASUS through the above functions.

If you want to disable sharing your information with ASUS through the above functions, please click **Withdraw** below. However, please note that these features/functions may not work if you stop sharing your information with ASUS.

IMPORTANT!

- After you click **Withdraw**, there will be some changes as listed below:
  - The DDNS name you are currently using will not be kept in your access point.
  - ASUS Router app, Lyra app, AiCloud, AiDisk can be used only when your device is in the same LAN with the access point.

---

2. ASUS PRIVACY Notice (for firmware/security upgrade):

Please note that your information will be collected by ASUS access point for firmware/security upgrade purposes. If you want to disable sharing your information with ASUS access point, please click **Withdraw** below.

IMPORTANT! Clicking **Withdraw** here may result in the failure of upgrading to the latest firmware and getting the most up-to-date protection on your ASUS access point. However, to protect the security of your access point and ensure the compliance with laws, upgrades addressing important security issues or meeting legal/regulatory requirements will still be downloaded and installed automatically.

3.2 AiMesh

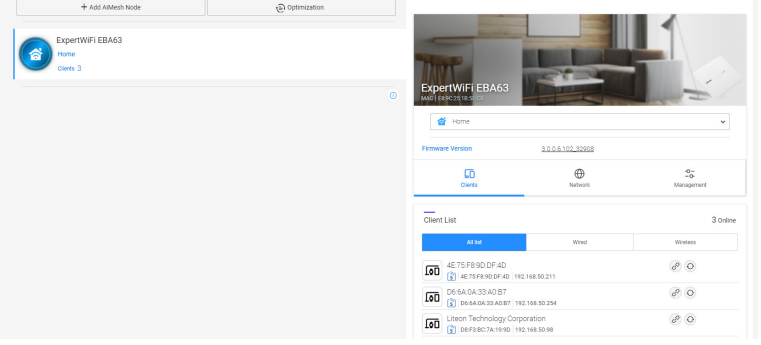
3.2.1 Setting up the wireless settings

To protect your wireless network from unauthorized access, you need to configure its security settings.

To set up the wireless settings:

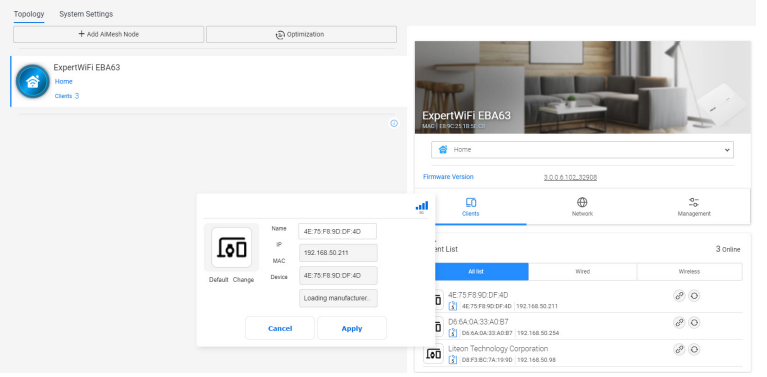
1. From the navigation panel, go to **AiMesh** > **Topology**.
2. You can configure the wired and wireless connection, manage the network status and the LED status.

NOTE: You can set up different wireless security settings for your 2.4GHz and 5GHz wireless connection.



3. Go to **AiMesh** > **System Settings** to enable or disable Ethernet Backhaul Mode, configure Roaming Block List, reset the system settings to factory defaults or reboot the system.

3.2.2 Managing your network clients

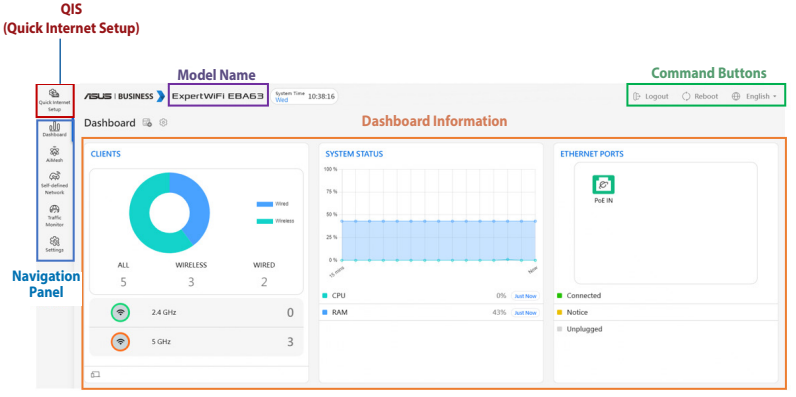


To manage your network clients:

1. From the navigation panel, go to **AiMesh** > **Topology**.
2. Select the **Clients** icon to display your network client's information such as the client's name, MAC and IP address.
3. You can block the client's access to your network, disable its time scheduling or disable its MAC and IP binding by moving the slider to **OFF**.
4. Click **Apply** when done.

3.3 Dashboard

Dashboard allows you to manage your network such as internet connection, client connection, DNS benchmark, system status, ethernet port, and traffic monitor.

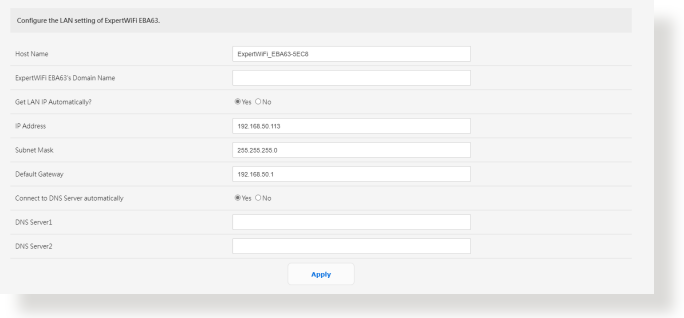


3.4 LAN

3.4.1 LAN IP

The LAN IP screen allows you to modify the LAN IP settings of your wireless access point.

NOTE: Any changes to the LAN IP address will be reflected on your DHCP settings.



To modify the LAN IP settings:

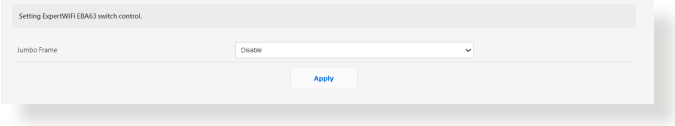
1. From the navigation panel, go to **Settings** > **LAN** > **LAN IP**.
2. Modify the **IP Address** and **Subnet Mask**.
3. When done, click **Apply**.

3.4.2 Switch Control

Allows you to set up the access point for the function of switch control. You can combine two 1Gbps LAN ports to deliver up to 2Gbps wired speeds via bonding to your compatible NAS or other high-bandwidth network device.

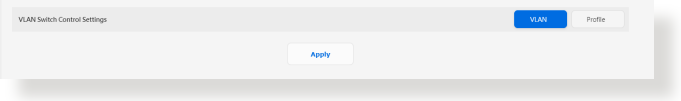
NOTES:

- To use the Link Aggregation Control Protocol (LACP) function, the devices must support IEEE 802.3ad protocol.
- The LAN aggregation function can be operated by pairing the LAN3 port with the LAN2 port.



3.4.3 VLAN

A VLAN (Virtual Local Area Network) is a logical network created within a larger physical network. VLANs allow you to segment a network into smaller, virtual sub-networks, which can be used to isolate traffic and improve network performance.



To set up VLAN:

1. From the navigation panel, go to **Settings** > **LAN** > **VLAN**.
2. Click the **Profile** tab and then ⊕ to create a VLAN profile. You can assign your own VLAN ID.
3. **Port isolation** restricts the access right of different devices in the same VLAN. You are now creating a "VLAN-only-Network", which means a network with VID but without DHCP.
4. Click **VLAN** tab to select a port with specific profile and mode (**Trunk** / **Access**).

NOTE: You can select one of the following default modes:

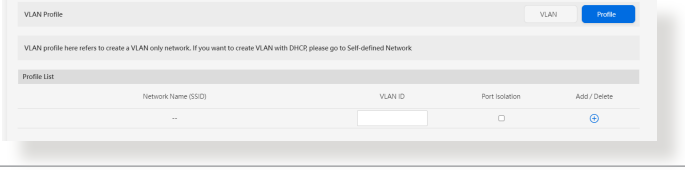
All (Default) allows all tagged and untagged packets to access.

Access mode allows a selected SDN(VLAN) to access. You can select profiles created by Guest Network pro or by VLAN.

Trunk mode:

- **Allow all tagged:** Only tagged packets are allowed to access.
- **With selected SDN(VLAN):** Only selected SDN or VLAN is allowed to access.

5. When done, click **Apply**.



NOTE: For more information, please visit https://www.asus.com/support/FAQ/1049415/.

3.5 Network Tools

To use network tools, from the navigation panel, go to **Settings** > **Network Tools**.

3.5.1 Network Analysis

Send ICMP ECHO_REQUEST packets to network hosts.

3.5.2 Netstat

Display the network details.

3.5.3 Wake on LAN

The WOL (Wake-On-LAN) feature lets you wake up a computer from any device in the network.

3.5.4 Smart Connect Rule

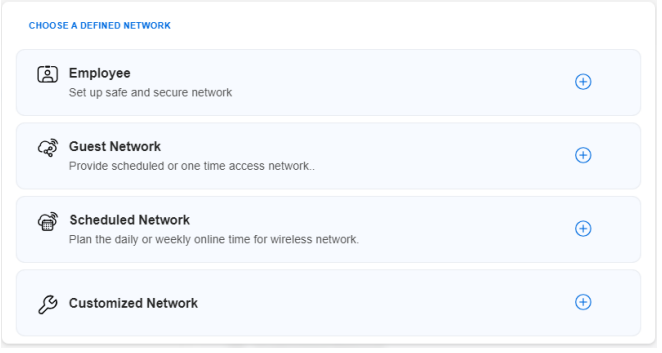
Set up the Smart Connect related information.

3.6 Self-Defined Network

A Self-Defined Network (SDN) provides up to five SSIDs to separate and prioritize devices for different business uses and network alternatives, creating network segments for employees, guest portals, guest networks, scheduled networks, IoT networks and VPN networks.

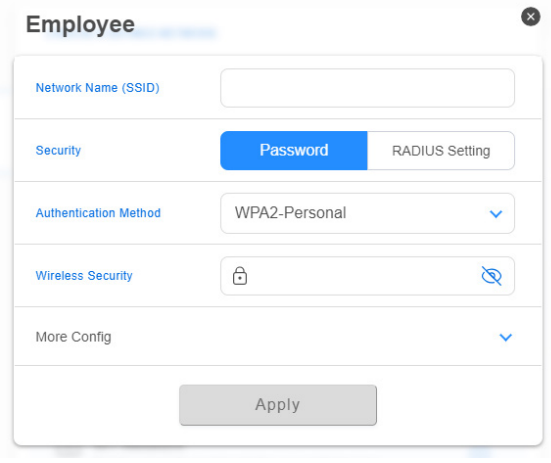
To create a Self-Defined Network:

1. From the navigation panel, go to **Self-Defined Network**.
2. Choose a defined network that fits your specific scenario.



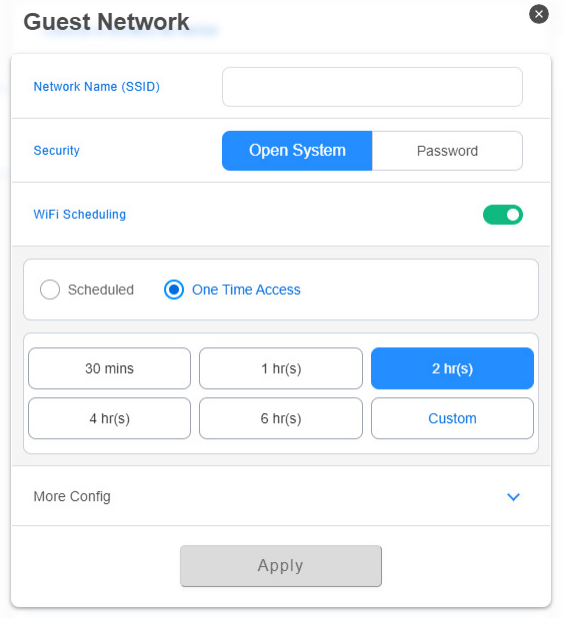
3.6.1 Employee

Allows you to set up access level for different uses to enhance network security. Recommended for offices that assign permissions to different departments.



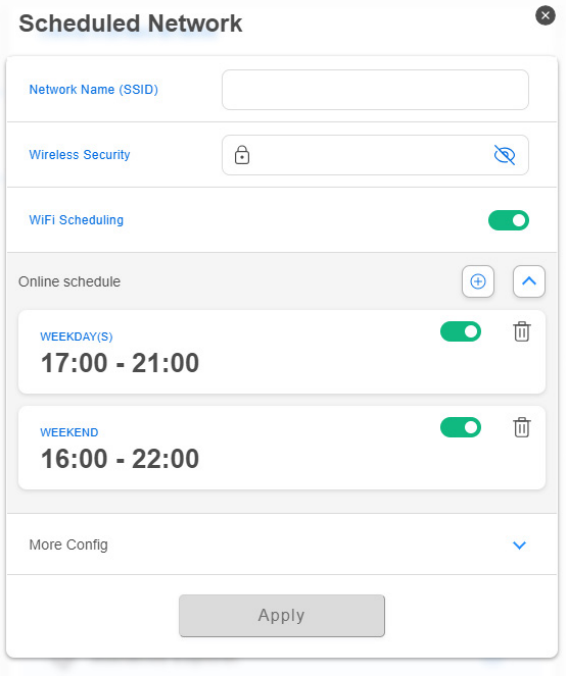
3.6.2 Guest Network

Provides temporary visitors with scheduled or one time access to the network. Recommended for use in shopping malls, gyms or for visitors.



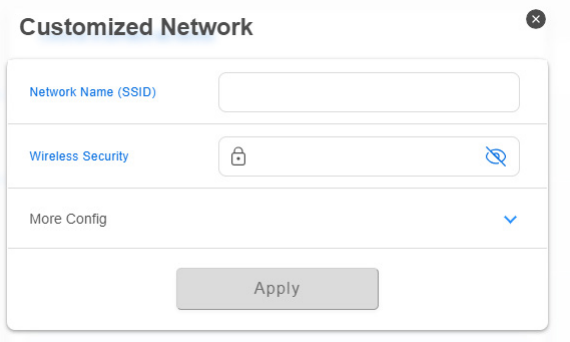
3.6.3 Scheduled Network

Plans the daily or weekly online time for the wireless network. Recommended for distance learning, classroom or children's use.



3.6.4 Customized Network

Allows you to select the option of a personalized network.



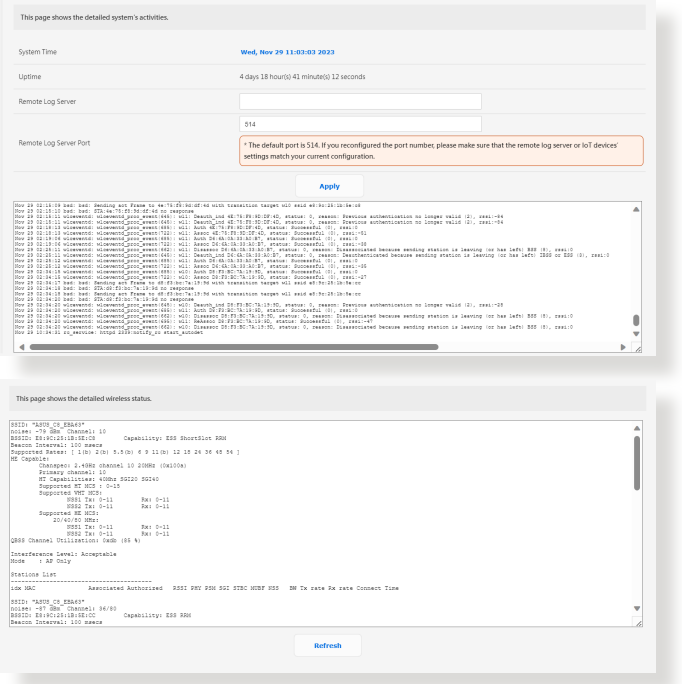
3.7 System Log

System Log contains your recorded network activities.

NOTE: System log resets when the access point is rebooted or powered off.

To view your system log:

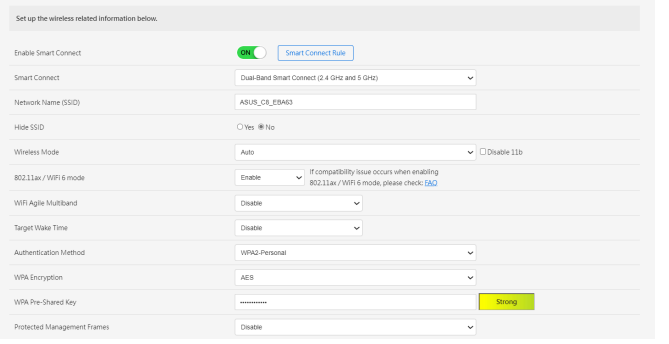
1. From the navigation panel, go to **Settings** > **System Log**.
2. You can view your network activities in any of these tabs:
   - General Log
   - DHCP Leases
   - Wireless Log
   - Port Forwarding
   - Routing Table
   - IPv6
   - Connections



3.8 Wireless

3.8.1 General

The **General** tab allows you to configure the basic wireless settings.



To configure the basic wireless settings:

1. From the navigation panel, go to **Settings** > **Wireless** > **General**.
2. Select 2.4GHz or 5GHz as the frequency band for your wireless network.
3. Assign a unique name for your SSID (Service Set Identifier) or network name to identify your wireless network. Wi-Fi devices can identify and connect to the wireless network via your assigned SSID. The SSIDs on the information banner are updated once new SSIDs are saved to the settings.

NOTE: You can assign unique SSIDs for the 2.4 GHz and 5GHz frequency bands.

4. In the **Hide SSID** field, select **Yes** to prevent wireless devices from detecting your SSID. When this function is enabled, you would need to enter the SSID manually on the wireless device to access the wireless network.
5. Select any of these wireless mode options to determine the types of wireless devices that can connect to your wireless access point:

- **Auto**: Select **Auto** to allow 802.11ax, 802.11ac, 802.11n, 802.11g, and 802.11b devices to connect to the wireless access point.

6. Select any of these channel bandwidth to accommodate higher transmission speeds:

   2.4GHz: Select between 40MHz and 20MHz for wireless throughput.

   5GHz: Select among 160MHz, 80MHz, 40MHz and 20MHz for wireless throughput.

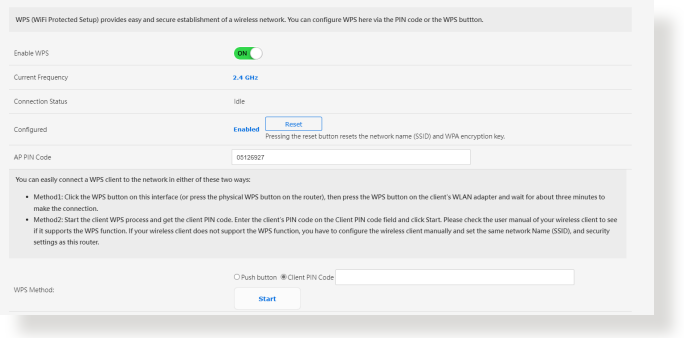
7. Select the operating channel for your wireless access point. Select **Auto** to allow the wireless access point to automatically select the channel that has the least amount of interference.

8. Select any of these authentication methods:
   - **Open System**: This option provides no security.
   - **WPA/WPA2/WPA3-Personal**: This option provides strong security. You can use either WPA (with TKIP) or WPA2 (with AES). If you select this option, you must use TKIP + AES encryption and enter the WPA passphrase (network key).
   - **WPA/WPA2/WPA3-Enterprise**: This option provides very strong security. It is with integrated EAP server or an external RADIUS back-end authentication server.

3.8.2 WPS

WPS (Wi-Fi Protected Setup) is a wireless security standard that allows you to easily connect devices to a wireless network. You can configure the WPS function via the PIN code or WPS button.

NOTE: Ensure that the devices support WPS.



To enable WPS on your wireless network:

1. From the navigation panel, go to **Settings** > **Wireless** > **WPS**.
2. In the **Enable WPS** field, move the slider to **ON**.
3. WPS uses 2.4GHz by default. If you want to change the frequency to 5GHz, turn **OFF** the WPS function, click **Switch Frequency** in the **Current Frequency** field, and turn WPS **ON** again.

NOTE: WPS supports authentication using Open System, WPA-Personal, and WPA2-Personal. WPS does not support a wireless network that uses a Shared Key, WPA-Enterprise, WPA2-Enterprise, and RADIUS encryption method.

3. In the **WPS Method** field, select **Push button** or **Client PIN Code**. If you select **Push button**, go to step 4. If you select **Client PIN Code**, go to step 5.
4. To set up WPS using the WPS button on the interface, follow these steps:

a. Click **Start**.

b. The wireless access point will scan for any available WPS devices. If the wireless access point does not find any WPS devices, it will switch to standby mode.

5. To set up WPS using the client's PIN code, follow these steps:

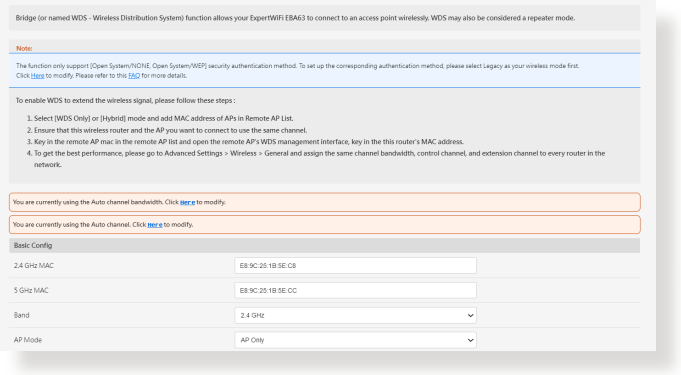
   a. Locate the WPS PIN code on your wireless device's user manual or on the device itself.

   b. Key in the Client PIN code on the text box.

   c. Click **Start** to put your wireless access point into WPS survey mode. The access point's LED indicators quickly flash three times until the WPS setup is completed.

3.8.3 WDS (Bridge)

Bridge or WDS (Wireless Distribution System) allows your ASUS wireless access point to connect to another wireless access point exclusively, preventing other wireless devices or stations to access your ASUS wireless access point. It can also be considered as a wireless repeater where your ASUS wireless access point communicates with another access point and other wireless devices.

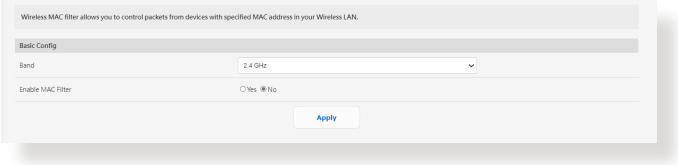


To set up the wireless bridge:

1. From the navigation panel, go to **Settings** > **Wireless** > **WDS**.
2. Select **WDS Only** or **Hybrid** mode and add the MAC addresses of APs in **Remote AP List (Max Limit:4)**.
3. Ensure that this wireless access point and the AP you want to connect to use the same channel.
4. Key in the remote AP MAC address in the **Remote AP List** field, open the remote AP's WDS management interface, and key in this access point's MAC address.
5. To get the best performance, go to **Settings** > **Wireless** > **General** and assign the same channel bandwidth, control channel, and extension channel to every access point in the network.

3.8.4 Wireless MAC Filter

Wireless MAC filter provides control over packets transmitted to a specified MAC (Media Access Control) address on your wireless network.

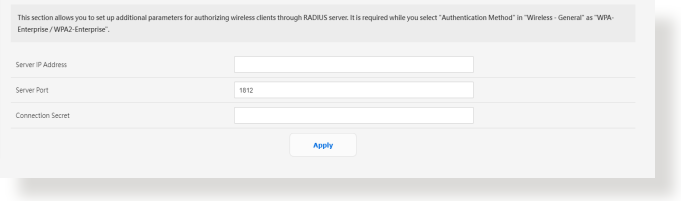


To set up the Wireless MAC filter:

1. From the navigation panel, go to **Settings** > **Wireless** > **Wireless MAC Filter**.
2. Tick **Yes** in the **Enable Mac Filter** field.
3. In the **MAC Filter Mode** dropdown list, select either **Accept** or **Reject**.
   - Select **Accept** to allow devices in the MAC filter list to access to the wireless network.
   - Select **Reject** to prevent devices in the MAC filter list to access to the wireless network.
4. On the MAC filter list, click ⊕ and key in the MAC address of the wireless device.
5. Click **Apply**.

3.8.5 RADIUS Setting

RADIUS (Remote Authentication Dial In User Service) allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required when you select **Authentication Method** in **Wireless - General** as **WPA-Enterprise / WPA2-Enterprise**.



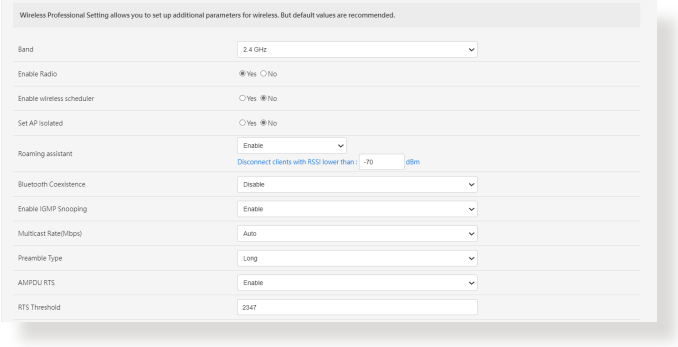
To set up wireless RADIUS settings:

1. Ensure that the wireless access point's authentication mode is set to WPA-Enterprise, WPA2-Enterprise.
2. From the navigation panel, go to **Settings** > **Wireless** > **RADIUS Setting**.
3. Select the frequency band.
4. In the **Server IP Address** field, key in your RADIUS server's IP Address.
5. In the **Connection Secret** field, assign the password to access your RADIUS server.
6. Click **Apply**.

3.8.6 Professional

The Professional settings allows you to set up additional parameters for wireless connection.

NOTE: We recommend that you use the default values on this page.



In the **Professional** settings screen, you can configure the following:

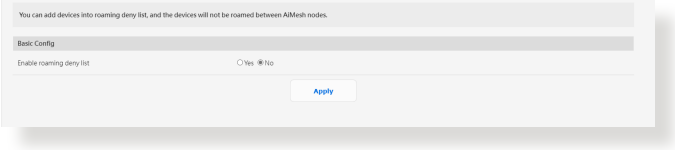
- **Band**: Select the frequency band that the professional settings will be applied to.
- **Enable Radio**: Select **Yes** to enable wireless networking. Select **No** to disable wireless networking.
- **Enable wireless scheduler**: You can choose clock format as 24-hour or 12-hour. The color in the table indicates Allow or Deny. Click each frame to change the settings of the hour of the weekdays and click **OK** when done.

- **Set AP isolated**: The Set AP isolated item prevents wireless devices on your network from communicating with each other. This feature is useful if many guests frequently join or leave your network. Select **Yes** to enable this feature or select **No** to disable.
- **Roaming assistant**: In network configurations that involve multiple Access Points or wireless repeater, wireless clients sometimes cannot connect automatically to thefts available AP because they are still connected to the main wireless router. Enable this setting so that the client will disconnect from the main wireless router if the signal strength is under a specific threshold and connect to a stronger signal.
- **Enable IGMP Snooping**: Enable this function allows the IGMP (Internet Group Management Protocol) to be monitored among devices and optimizes wireless multicast traffic.
- **Multicast rate (Mbps)**: Select the multicast transmission rate or click **Disable** to switch off simultaneous single transmission.
- **Preamble Type**: Preamble Type defines the length of time that the access point spent for CRC (Cyclic Redundancy Check). CRC is a method of detecting errors during data transmission. Select **Short** for a busy wireless network with high network traffic. Select **Long** if your wireless network is composed of older or legacy wireless devices.
- **AMPDU RTS**: Enable this function allows to build a group of frames before they are transmitted and use RTS for every AMPDU for communication among 802.11g and 802.11b devices.
- **RTS Threshold**: Select a lower value for RTS (Request to Send) Threshold to improve wireless communication in a busy or noisy wireless network with high network traffic and numerous wireless devices.
- **DTIM Interval**: DTIM (Delivery Traffic Indication Message) Interval or Data Beacon Rate is the time interval before a signal is sent to a wireless device in sleep mode indicating that a data packet is awaiting delivery. The default value is three milliseconds.

- **Beacon Interval**: Beacon Interval is the time between one DTIM and the next. The default value is 100 milliseconds. Lower the Beacon Interval value for an unstable wireless connection or for roaming devices.
- **Enable TX Bursting**: Enable TX Bursting improves transmission speed between the wireless access point and 802.11g devices.
- **Enable WMM APSD**: Enable WMM APSD (Wi-Fi Multimedia Automatic Power Save Delivery) to improve power management between wireless devices. Select **Disable** to switch off WMM APSD.

3.8.7 Roaming Block List

The feature allows you to add devices to the roaming block list and prevent them from roaming between AiMesh nodes.



4 Utilities

NOTES:

- Download and install the wireless access point's utilities from the ASUS website:
  - Device Discovery v1.4.7.1 at http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Discovery.zip
  - Firmware Restoration v1.9.0.4 at http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Rescue.zip
  - Windows Printer Utility v1.0.5.5 at http://dlcdnet.asus.com/pub/ASUS/LiveUpdate/Release/Wireless/Printer.zip
- The utilities are not supported on MAC OS.

4.1 Device Discovery

Device Discovery is an ASUS WLAN utility that detects an ASUS wireless access point device, and allows you to configure the wireless networking settings.

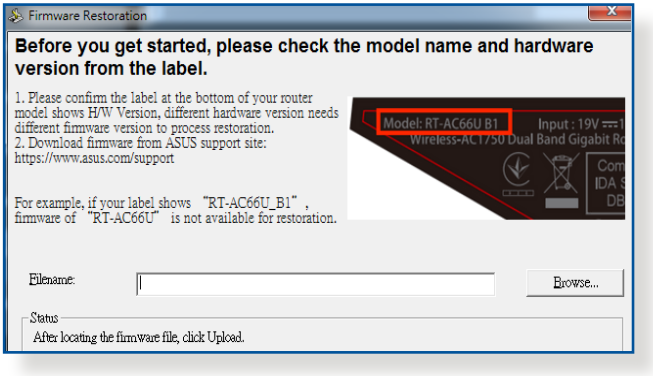
To launch the Device Discovery utility:

- From your computer's desktop, click **Start** > **All Programs** > **ASUS Utility** > **Wireless Router** > **Device Discovery**.

NOTE: When you set the router to Access Point mode, you need to use Device Discovery to get the router's IP address.

4.2 Firmware Restoration

Firmware Restoration is used on an ASUS Wireless Access Point that failed during its firmware upgrading process. It uploads the firmware that you specify. The process takes about three to four minutes.



IMPORTANT! Launch the rescue mode on the access point before using the Firmware Restoration utility.

NOTE: This feature is not supported on MAC OS.

To launch the rescue mode and use the Firmware Restoration utility:

1. Unplug the wireless access point from the power source.
2. Hold the Reset button at the rear panel and simultaneously replug the wireless access point into the power source. Release the Reset button when the Power LED at the front panel flashes slowly, which indicates that the wireless access point is in the rescue mode.
3. Set a static IP on your computer and use the following to set up your TCP/IP settings:

   IP address: 192.168.1.x

   Subnet mask: 255.255.255.0

4. From your computer's desktop, click **Start** > **All Programs** > **ASUS Utility** > **Wireless Router** > **Firmware Restoration**.
5. Specify a firmware file, then click **Upload**.

NOTE: This is not a firmware upgrade utility and cannot be used on a working ASUS Wireless Access Point. Normal firmware upgrades must be done through the web interface. Refer to **Chapter 3: Configuring EBA63** for more details.

5 Troubleshooting

This chapter provides solutions for issues you may encounter with your access point. If you encounter problems that are not mentioned in this chapter, visit the ASUS support site at: https://www.asus.com/support/ for more product information and contact details of ASUS Technical Support.

5.1 Basic Troubleshooting

If you are having problems with your access point, try these basic steps in this section before looking for further solutions.

Upgrade Firmware to the latest version.

1. From the navigation panel, go to **Settings** > **Administration** > **Firmware Upgrade**. Click **Check** to verify if the latest firmware is available.
2. If the latest firmware is available, visit the ASUS global website to download the latest firmware.
3. From the **Firmware Upgrade** page, click **Browse** to upload the firmware file.
4. Click **Upload** to upgrade the firmware.

Restart your network in the following sequence:

1. Turn off the modem.
2. Unplug the modem.
3. Turn off the access point and computers.
4. Plug in the modem.
5. Turn on the modem and then wait for 2 minutes.
6. Turn on the access point and then wait for 2 minutes.
7. Turn on computers.

Check if your Ethernet cables are plugged properly.

- When the Ethernet cable connecting the access point with the modem is plugged in properly, the WAN LED will be on.
- When the Ethernet cable connecting your powered-on computer with the access point is plugged in properly, the corresponding LAN LED will be on.

Check if the wireless setting on your computer matches that of your access point.

- When you connect your computer to the access point wirelessly, ensure that the SSID (wireless network name), encryption method, and password are correct.

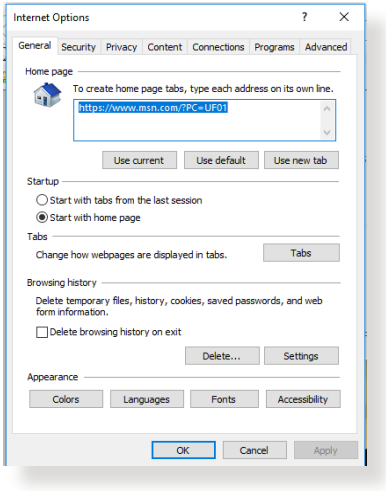
Check if your network settings are correct.

- Each client on the network should have a valid IP address. ASUS recommends that you use the wireless access point's DHCP server to assign IP addresses to computers on your network.
- Some cable modem service providers require you to use the MAC address of the computer initially registered on the account. You can view the MAC address in the web GUI, **Dashboard** > **Clients**.

5.2 Frequently Asked Questions (FAQs)

I cannot access the access point GUI using a web browser

- If your computer is wired, check the Ethernet cable connection and LED status as described in the previous section.
- Ensure that you are using the correct login information. The default factory login name and password can be found on the label at the bottom of EBA63. Ensure that the Caps Lock key is disabled when you enter the login information.
- Delete the cookies and files in your web browser. For Internet Explorer, follow these steps:
  1. Launch Internet Explorer, then click **Tools** > **Internet Options**.
  2. In the **General** tab, under **Browsing history**, click **Delete…**, select **Temporary Internet files and website files** and **Cookies and website data** then click **Delete**.



NOTES:

- The commands for deleting cookies and files vary with web browsers.
- Disable proxy server settings, cancel the dial-up connection, and set the TCP/IP settings to obtain IP addresses automatically. For more details, refer to Chapter 1 of this user manual.
- Ensure that you use CAT5e or CAT6 ethernet cables.

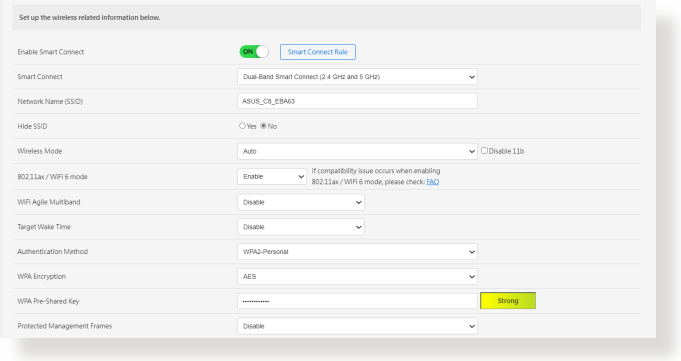
The client cannot establish a wireless connection with the access point.

NOTE: If you are having issues connecting to 5GHz network, make sure that your wireless device supports 5GHz or features dual band capabilities.

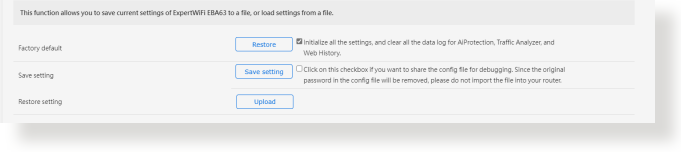
- **Out of Range:**

  Move the access point closer to the wireless client.

- SSID has been hidden. If your device can find SSIDs from other access points but cannot find your access point's SSID, go to **Settings** > **Wireless** > **General**, select **NO** on **Hide SSID**, and select **Auto** on **Wireless Mode**.



- If you are using a wireless LAN adapter, check if the wireless channel in use conforms to the channels available in your country/area. If not, adjust the channel, channel bandwidth, and wireless mode.
- If you still cannot connect to the access point wirelessly, you can reset your access point to factory default settings. In the access point GUI, click **Settings** > **Administration** > **Restore/ Save/Upload Setting** and click **Restore**.



Internet is not accessible.

- Check if your access point can connect to your ISP's WAN IP address. To do this, launch the web GUI and go to **Dashboard**, and check the Internet status.
- If your access point cannot connect to your ISP's WAN IP address, try restarting your network as described in the section **Restart your network in following sequence** under **Basic Troubleshooting**.
- If there is still no Internet access, try to reboot your computer and verify the network's IP address and gateway address.
- Check the status indicators on the ADSL modem and the wireless access point. If the WAN LED on the wireless access point is not ON, check if all cables are plugged properly.

You forgot the SSID (network name) or network password

- Setup a new SSID and encryption key via a wired connection (Ethernet cable). Launch the web GUI, go to **Dashboard**, click the access point icon, enter a new SSID and encryption key, and then click **Apply**.
- Reset your access point to the default settings. Launch the web GUI, go to **Settings** >**Administration** > **Restore/Save/Upload Setting**, and click **Restore**. The default login account and password can be found on the label at the bottom of EBA63.

How to restore the system to its default settings?

- Go to **Setting**s > **Administration** > **Restore/Save/Upload Setting**, and click **Restore**.

Firmware upgrade failed.

Launch the rescue mode and run the Firmware Restoration utility. Refer to section **4.2 Firmware Restoration** on how to use the Firmware Restoration utility.

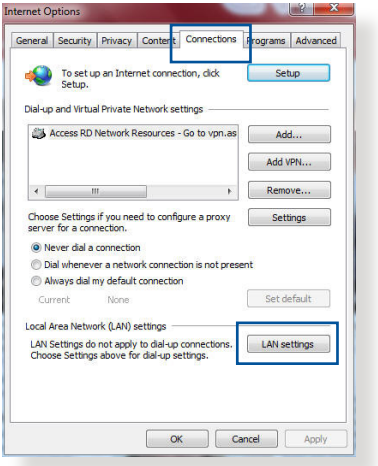
Cannot access Web GUI

Before configuring your wireless access point, do the steps described in this section for your host computer and network clients.

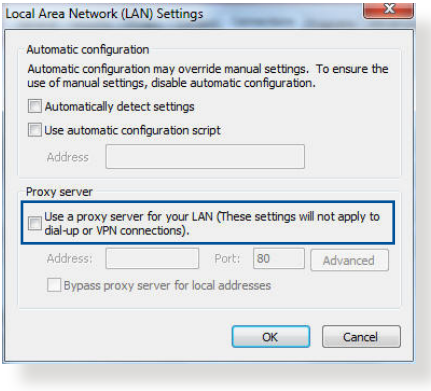
A. Disable the proxy server, if enabled.

Windows®

1. Click **Start > Internet Explorer** to launch the browser.
2. Click **Tools** > **Internet options** > **Connections** > **LAN settings**.

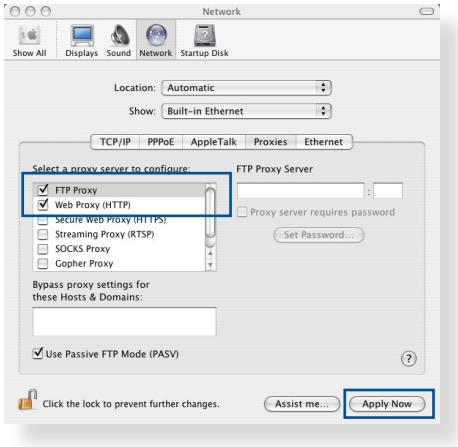


3. From the Local Area Network (LAN) Settings screen, untick **Use a proxy server for your LAN**.
4. Click **OK** when done.



MAC OS

1. From your Safari browser, click **Safari** > **Preferences** > **Advanced** > **Change Settings...**
2. From the Network screen, deselect **FTP Proxy** and **Web Proxy (HTTP)**.
3. Click **Apply Now** when done.

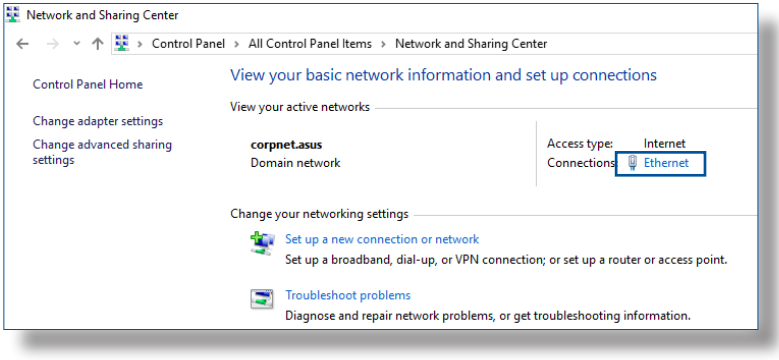


NOTE: Refer to your browser's help feature for details on disabling the proxy server.

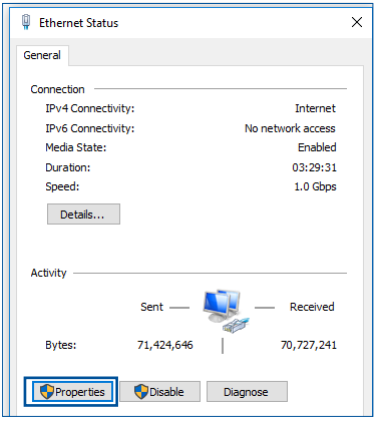
B. Set the TCP/IP settings to automatically obtain an IP address.

Windows®

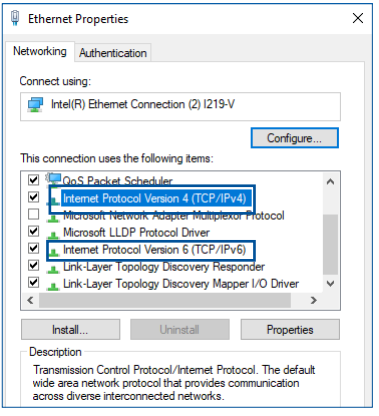
1. Click **Start** > **Control Panel** > **Network and Sharing Center,** then click the network connection to display its status window.



2. Click **Properties** to display the Ethernet Properties window.



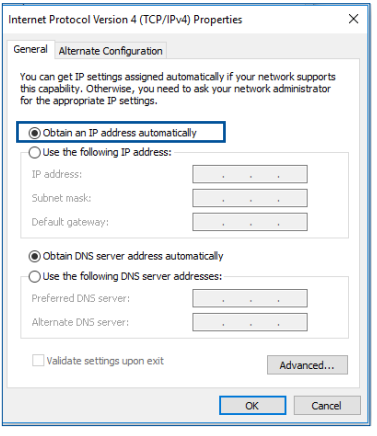
3. Select **Internet Protocol Version 4 (TCP/IPv4)** or **Internet Protocol Version 6 (TCP/IPv6)**, then click **Properties**.



4. To obtain the IPv4 IP settings automatically, tick **Obtain an IP address automatically**.

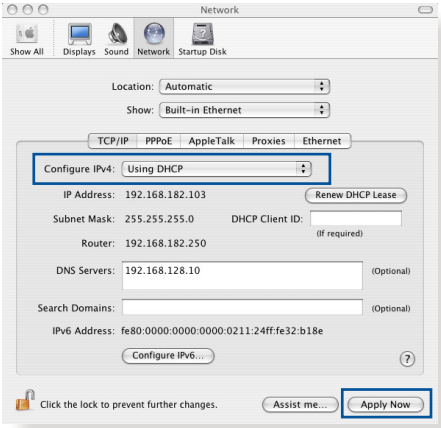
   To obtain the IPv6 IP settings automatically, tick **Obtain an IPv6 address automatically**.

5. Click **OK** when done.



MAC OS

1. Click the Apple icon located on the top left of your screen.
2. Click **System Preferences** > **Network** > **Configure...**
3. From the **TCP/IP** tab, select **Using DHCP** in the **Configure IPv4** dropdown list.
4. Click **Apply Now** when done.

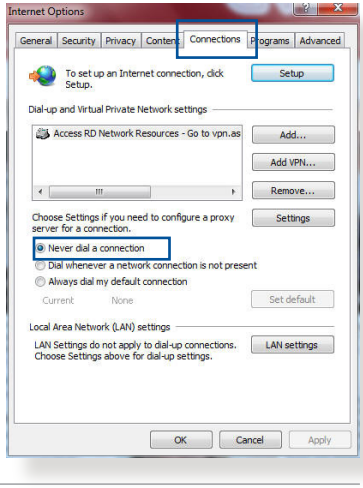


NOTE: Refer to your operating system's help and support feature for details on configuring your computer's TCP/IP settings.

C. Disable the dial-up connection, if enabled.

Windows®

1. Click **Start** > **Internet Explorer** to launch the browser.
2. Click **Tools** > **Internet options** > **Connections**.
3. Tick **Never dial a connection**.
4. Click **OK** when done.



NOTE: Refer to your browser's help feature for details on disabling the dial-up connection.

Appendices

GNU General Public License

Licensing information

This product includes copyrighted third-party software licensed under the terms of the GNU General Public License. Please see The GNU General Public License for the exact terms and conditions of this license. All future firmware updates will also be accompanied with their respective source code. Please visit our web site for updated information. Note that we do not offer direct support for the distribution.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

Terms & conditions for copying, distribution, & modification

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License.

Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance

on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission.

    For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12 IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Safety Notices

When using this product, always follow the fundamental safety precautions, including, but not limited to the following:

WARNING!

- The power supply cord(s) must be plugged into socket-outlet(s) that is /are provided with a suitable earth ground. Connect the equipment only to a nearby socket outlet that is easily accessible.
- If the Adapter is broken, do not try to fix it by yourself. Contact a qualified service technician or your retailer.
- DO NOT use damaged power cords, accessories, or other peripherals.
- DO NOT mount this equipment higher than 2 meters.
- Use this product in environments with ambient temperatures between 0°C (32°F) and 40°C (104°F).
- Read the operational guidelines and the temperature range provided before using the product.
- Pay particular attention to the personal safety when using this device in airports, hospitals, gas stations and professional garages.
- Medical device interference: Maintain a minimum distance of at least 15 cm (6 inches) between implanted medical devices and ASUS products to reduce the risk of interference.
- Kindly use ASUS products in good reception conditions to minimize the radiation's level.
- Keep the device away from pregnant women and the lower abdomen of the teenager.
- DO NOT use this product if visible defects can be observed or it has been wet or damaged or modified. Seek servicing for assistance.

WARNING!

- DO NOT place on uneven or unstable work surfaces.
- DO NOT place or drop objects on the top of the product. Avoid exposing the product to mechanical shock such as crushing, bending, puncturing or shredding.
- DO NOT disassemble, open, microwave, incinerate, paint, or shove any foreign objects into this product.
- Refer to the rating label on the bottom of your product and ensure your power adapter complies with this rating.
- Keep the product away from fire and heat sources.
- DO NOT expose to or use near liquids, rain, or moisture. DO NOT use the product during electrical storms.
- Connect the PoE output circuits of this product exclusively to PoE networks, without routing to external facilities.
- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- Only use accessories that have been approved by the device manufacturer to work with this model. The use of other types of accessories may invalidate the warranty or violate local regulations and laws, and may pose safety risks. Contact your local retailer for the availablity of authorized accessories.
- Use of this product in a way not recommended in the provided instructions may result in a risk of fire or personal injury.

Service and Support

Visit our multi-language website at https://www.asus.com/support.