E20552

REPUBLIC OF GAMERS

USER MANUAL

GT-AX5400

ROG Rapture Dual-band Gaming Router

ASUS

E20552

First Edition

February 2023

Product warranty or service will not be extended if: (1) the product is repaired, modified or altered, unless such repair, modification of alteration is authorized in writing by ASUS; or (2) the serial number of the product is defaced or missing.

ASUS PROVIDES THIS MANUAL "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL ASUS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES (INCLUDING DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INTERRUPTION OF BUSINESS AND THE LIKE), EVEN IF ASUS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES ARISING FROM ANY DEFECT OR ERROR IN THIS MANUAL OR PRODUCT.

SPECIFICATIONS AND INFORMATION CONTAINED IN THIS MANUAL ARE FURNISHED FOR INFORMATIONAL USE ONLY, AND ARE SUBJECT TO CHANGE AT ANY TIME WITHOUT NOTICE, AND SHOULD NOT BE CONSTRUED AS A COMMITMENT BY ASUS. ASUS ASSUMES NO RESPONSIBILITY OR LIABILITY FOR ANY ERRORS OR INACCURACIES THAT MAY APPEAR IN THIS MANUAL, INCLUDING THE PRODUCTS AND SOFTWARE DESCRIBED IN IT.

Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Table of contents

1 Getting to know your wireless router

2 Getting started

3 Configuring the General Settings of ROG Gaming Center

Table of contents

4 Configuring the Advanced Settings

Table of contents

5 Utilities

6 Troubleshooting

Appendices

1 Getting to know your wireless router

1.1 Welcome!

Thank you for purchasing ROG STRIX Wireless Router!

The stylish router features 2.4GHz and 5GHz dual bands for an unmatched concurrent wireless HD streaming; SMB server, UPnP AV server, and FTP server for 24/7 file sharing; a capability to handle 300,000 sessions; and the ASUS Green Network Technology, which provides up to 70% power-saving solution.

1.2 Package contents

☑ ROG STRIX gaming router

☑ Network cable (RJ-45)

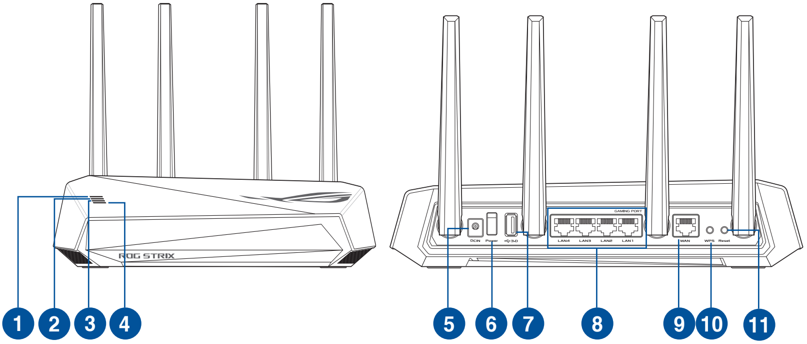
☑ AC adapter

☑ Quick Start Guide

NOTES:

- If any of the items is damaged or missing, contact ASUS for technical inquiries and support, Refer to the ASUS Support Hotline list 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 router



1 **WAN (Internet) LED**

Red: No IP or no physical connection.

On: Has physical connection to a wide area network (WAN).

2 **5GHz LED**

Off: No 5GHz signal.

On: Wireless system is ready.

Flashing: Transmitting or receiving data via wireless connection.

3 **2.4GHz LED**

Off: No 2.4GHz signal.

On: Wireless system is ready.

Flashing: Transmitting or receiving data via wireless connection.

4 **Power LED**

Off: No power.

On: Device is ready.

Flashing slow: Rescue mode.

5 **Power (DCIN) port**

Insert the bundled AC adapter into this port and connect your router to a power source.

6 **Power switch**

Press this switch to power on or off the system.

7 **USB 3.2 Gen 1 port**

Insert a USB 3.2 Gen 1 device such as a USB hard disk or USB flash drive into this port. Insert your Ipad's USB cable into this port to charge your iPad.

8 **LAN 1~4 ports**

Connect network cables into these ports to establish LAN connection.

9 **WAN (Internet) port**

Connect a network cable into this port to establish WAN connection.

10	**WPS button** This button launches the WPS Wizard.
11	**Reset button** This button resets or restores the system to its factory default settings.

NOTES:

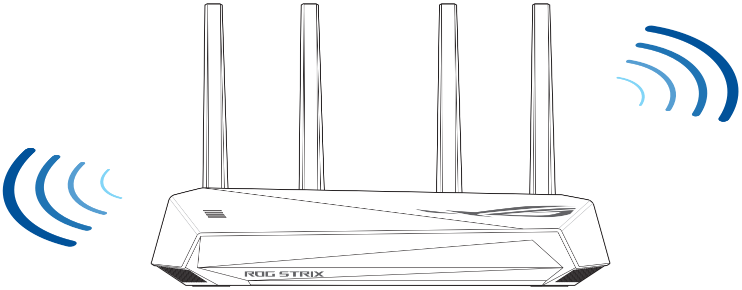
- Use only the adapter that came with your package. Using other adapters may damage the device.
- **Specifications:**

DC Power adapter	DC Output: +19V with max 1.75A current		
Operating Temperature	0~40°C	Storage	0~70°C
Operating Humidity	50~90%	Storage	20~90%

1.4 Positioning your router

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

- Place the wireless router 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.
- To ensure the best wireless signal, orient the four detachable antennas as shown in the drawing below.



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 Internet Explorer, Firefox, 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 triple band technology, your wireless router 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.

IMPORTANT!

- Some wireless adapters might have connectivity issues to 802.11ax WiFi APs.
- If you’re experiencing such issue, please ensure you update the driver to the latest version. Check your manufacturer's official support site where software drivers, updates, and other related information can be obtained.
  - Realtek: https://www.realtek.com/en/downloads
  - Mediatek: https://www.mediatek.com/products/connectivity-and-networking/broadband-wifi
  - Intel: https://downloadcenter.intel.com/

2 Getting started

2.1 Router Setup

IMPORTANT!

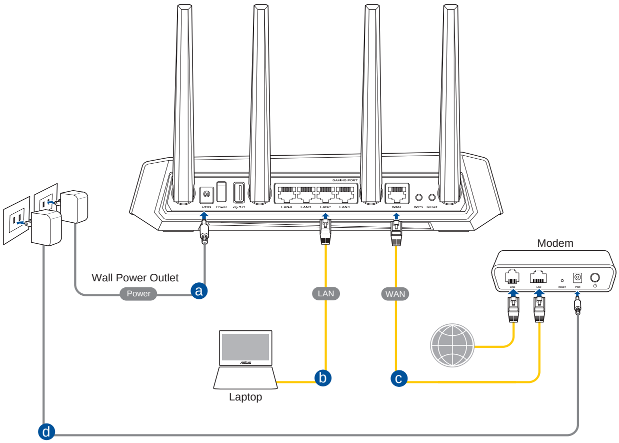
- Use a wired connection when setting up your wireless router to avoid possible setup problems.
- Before setting up your ASUS wireless router, do the following:
- If you are replacing an existing router, disconnect it from your network.
- Disconnect the cables/wires from your existing modem setup. If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

A. Wired connection

NOTE: You can use either a straight-through cable or a crossover cable for wired connection.

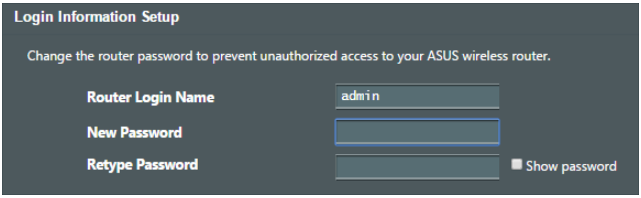
To set up your wireless router via wired connection:

1. Plug your router into a power outlet and power it on. Connect the network cable from your computer to a LAN port on your router.



2. The web GUI launches automatically when you open a web browser. If it does not auto-launch, enter http://www.asusrouter.com

3. Set up a password for your router to prevent unauthorized access.



Login Information Setup

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name: admin

New Password:

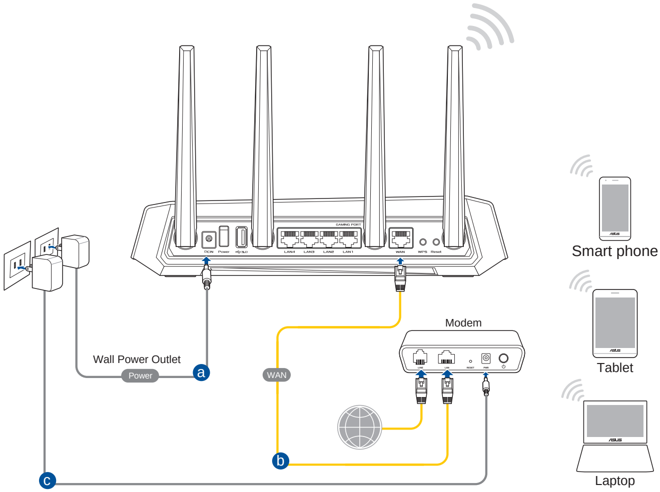
Retype Password:

□ Show password

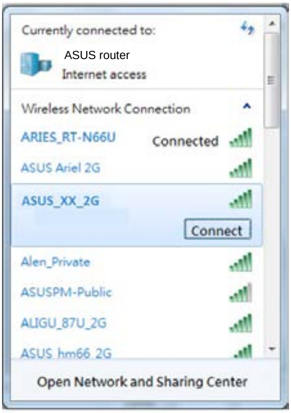
B. Wireless connection

To set up your wireless router via wireless connection:

1. Plug your router into a power outlet and power it on.



2. Connect to the network name(SSID) shown on the product label on the back side of the router. For better network security, change to a unique SSID and assign a password.



2.4G Wi-Fi Name (SSID):	ASUS_XX_2G
5G Wi-Fi Name (SSID):	ASUS_XX_5G

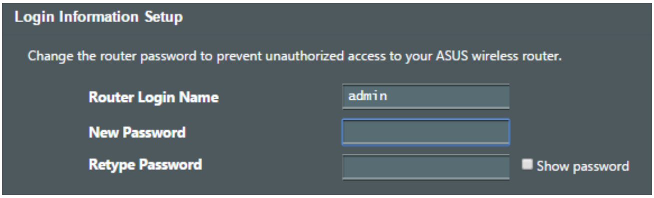
* **XX** refers to the last two digits of 2.4GHz MAC address. You can find it on the label on the back of your ROG router.

3. Once connected, the web GUI launches automatically when you open a web browser. If it does not auto-launch, enter http://www.asusrouter.com.

4. Set up a password for your router to prevent unauthorized access.

NOTES:

- For details on connecting to a wireless network, refer to the WLAN adapter's user manual.
- To set up the security settings for your network, refer to the section **Setting up the wireless security settings** in Chapter 3 of this user manual.



Login Information Setup

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name	admin
New Password	
Retype Password	

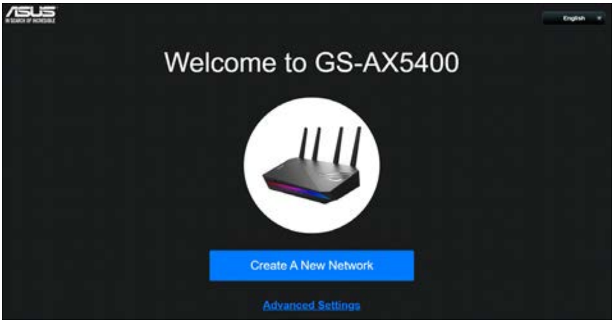
2.2 Quick Internet Setup (QIS) with Auto-detection

The Quick Internet Setup (QIS) function guides you in quickly setting up your Internet connection.

NOTE: When setting the Internet connection for the first time, press the Reset button on your wireless router to reset it to its factory default settings.

To use QIS with auto-detection:

1. Launch a web browser. You will be redirected to the ASUS Setup Wizard (Quick Internet Setup). If not, key in http://www.asusrouter.com manually.

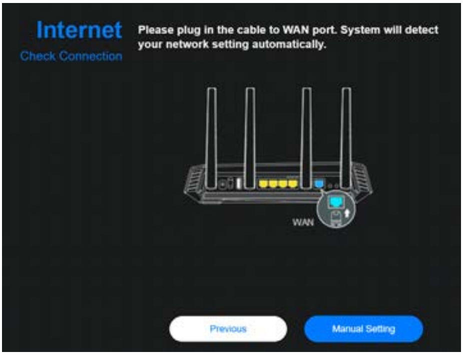


2. The wireless router automatically detects if your ISP connection type is **Dynamic IP**, **PPPoE**, **PPTP** and **L2TP**. Key in the necessary information for your ISP connection type.

IMPORTANT! Obtain the necessary information from your ISP about the Internet connection type.

NOTES:

- The auto-detection of your ISP connection type takes place when you configure the wireless router for the first time or when your wireless router is reset to its default settings.
- If QIS failed to detect your Internet connection type, click **Skip to manual setting** and manually configure your connection settings.

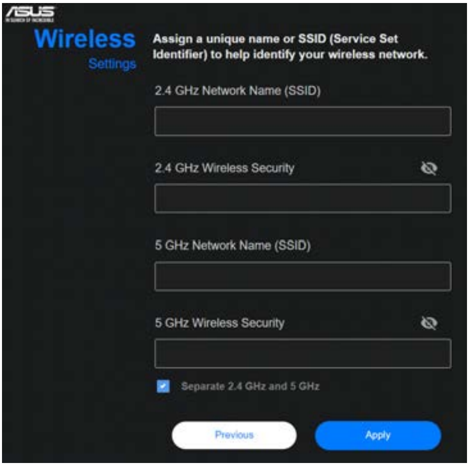


Internet

Check Connection

Please plug in the cable to WAN port. System will detect your network setting automatically.

3. Assign the wireless network name (SSID) and security key for your 2.4GHz and 5 GHz wireless connection. Click **Apply** when done.



Wireless

Settings

Assign a unique name or SSID (Service Set Identifier) to help identify your wireless network.

2.4 GHz Network Name (SSID)

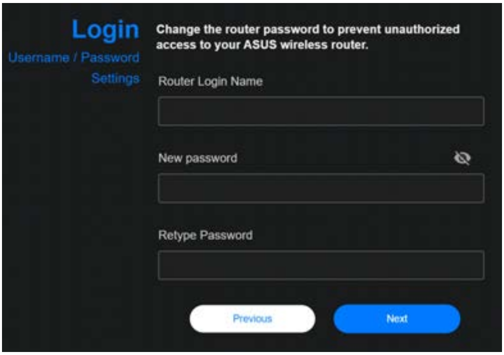
2.4 GHz Wireless Security

5 GHz Network Name (SSID)

5 GHz Wireless Security

☑ Separate 2.4 GHz and 5 GHz

4. On the **Login Information Setup** page, change the router’s login password to prevent unauthorized access to your wireless router.



Login

Username / Password

Settings

Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name

New password

Retype Password

NOTE: The wireless router's login username and password is different from the 2.4GHz/5GHz network name (SSID) and security key. The wireless router's login username and password allows you to log into your wireless router's Web GUI to configure your wireless router's settings. The 2.4GHz/5GHz network name (SSID) and security key allows Wi-Fi devices to log in and connect to your 2.4GHz/5GHz network.

2.3 Connecting to your wireless network

After setting up your wireless router via QIS, you can connect your computer or other smart devices to your wireless network.

To connect to your network:

1. On your computer, click the network icon 📶 in the notification area to display the available wireless networks.
2. Select the wireless network that you want to connect to, then click **Connect**.
3. You may need to key in the network security key for a secured wireless network, 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.

NOTES:

- Refer to the next chapters for more details on configuring your wireless network's settings.
- Refer to your device's user manual for more details on connecting it to your wireless network.

3 Configuring the General Settings of ROG Gaming Center

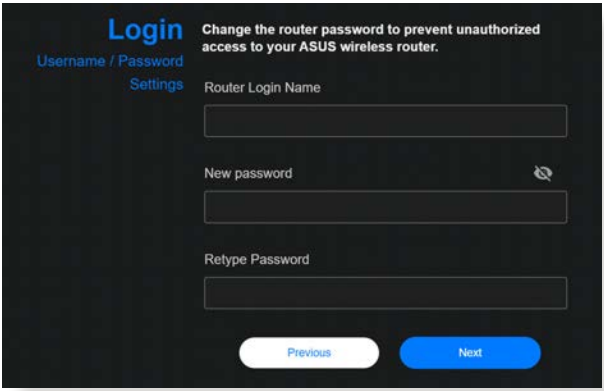
3.1 Logging into the Web GUI

Your ROG STRIX gaming router comes with an intuitive web graphical user interface (GUI) - ROG Gaming Center, which gives you total network control, with need-to-know information such as connected device status and worldwide game-server ping values, and instant access to all the amazing gaming features.

NOTE: The features may vary with different firmware versions.

To log into the web GUI:

1. On your web browser, manually key in the wireless router's default IP address: http://www.asusrouter.com.
2. On the login page, key in the default user name (**admin**) and the password that you have set in **2.2 Quick Internet Setup (QIS) with Auto-dection**.



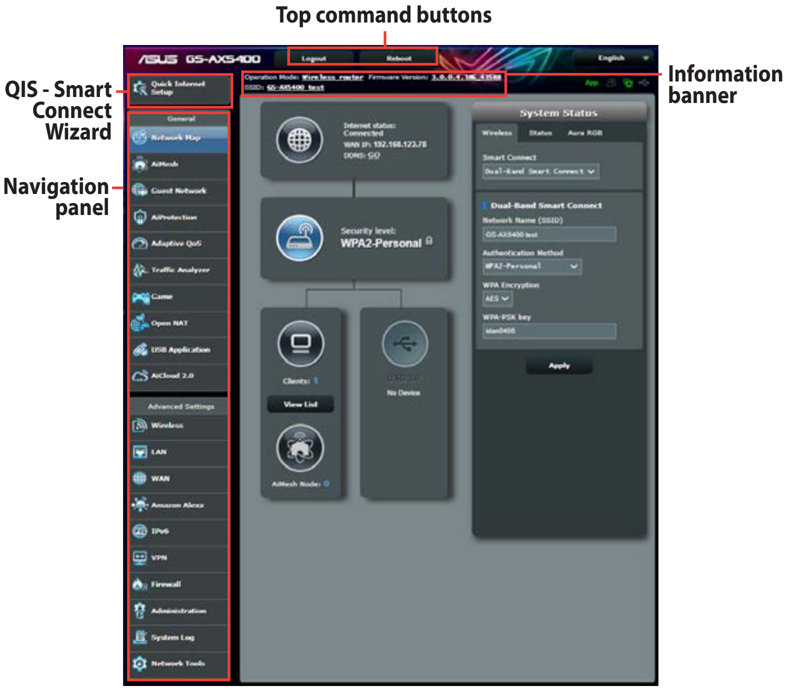
Change the router password to prevent unauthorized access to your ASUS wireless router.

Router Login Name

New password

Retype Password

3. You can now use the Web GUI to configure various settings of your ASUS Wireless Router.



Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_43588
SSID: GS-AX5400_test

Internet status: Connected
WAN IP: 192.168.123.78
DDNS: GO

Security level: WPA2-Personal

Clients: 1

No Device

AiMesh Node: 0

Smart Connect: Dual-Band Smart Connect

Dual-Band Smart Connect

Network Name (SSID): GS-AX5400 test

Authentication Method: WPA2-Personal

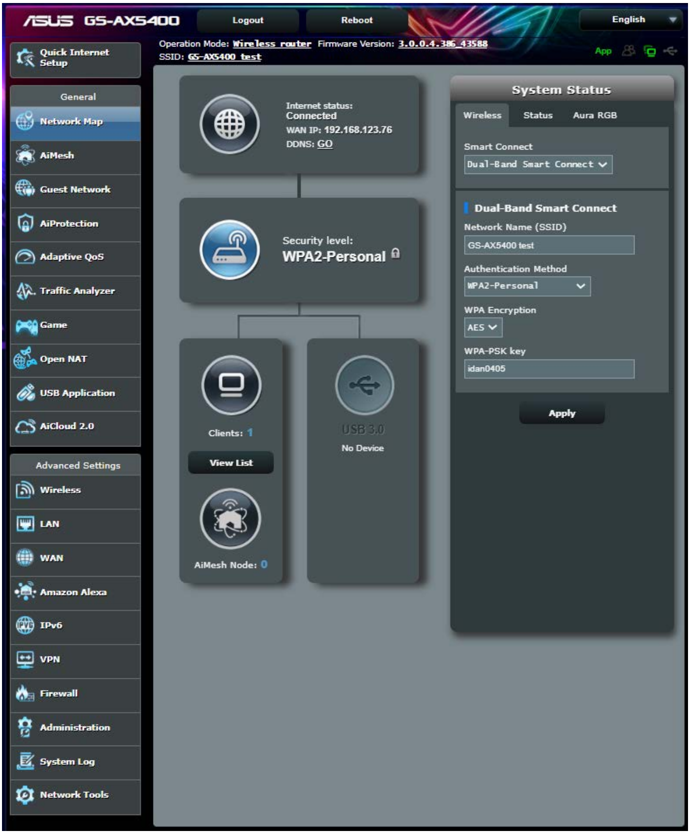
WPA Encryption: AES

WPA-PSK key: idan0405

NOTE: If you are logging into the Web GUI for the first time, you will be directed to the Quick Internet Setup (QIS) page automatically.

3.2 Using the Network Map

Network Map allows you to configure your network's security settings, manage your network clients, and monitor your USB device.



Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_43588
SSID: GS-AX5400_test

Internet status:
Connected
WAN IP: 192.168.123.76
DDNS: GO

Security level:
WPA2-Personal

Clients: 1

AiMesh Node: 0

USB 3.0
No Device

Smart Connect
Dual-Band Smart Connect

Dual-Band Smart Connect
Network Name (SSID)
GS-AX5400 test
Authentication Method
WPA2-Personal
WPA Encryption
AES
WPA-PSK key
idan0405

3.2.1 Setting up the wireless security settings

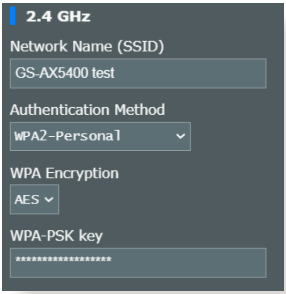
To protect your wireless network from unauthorized access, you need to configure its security settings.

To set up the wireless security settings:

1. From the navigation panel, go to **General** > **Network Map**.
2. On the Network Map screen and under **System Status**, you can configure the wireless security settings such as SSID, security level, and encryption settings.

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

2.4GHz security settings



2.4 GHz

Network Name (SSID)

GS-AX5400 test

Authentication Method

WPA2-Personal

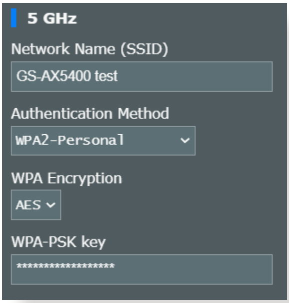
WPA Encryption

AES

WPA-PSK key

****

5GHz security settings



5 GHz

Network Name (SSID)

GS-AX5400 test

Authentication Method

WPA2-Personal

WPA Encryption

AES

WPA-PSK key

****

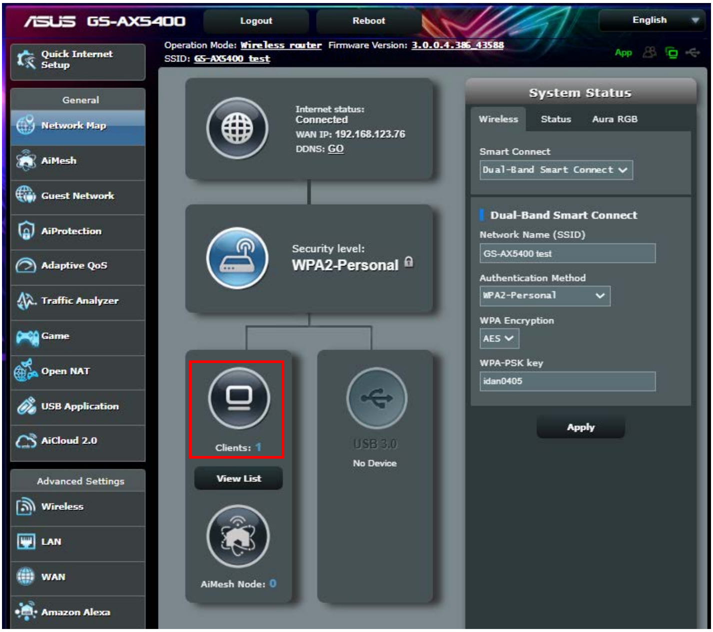
3. On the **Network Name (SSID)** field, key in a unique name for your wireless network.
4. From the **Authentication Method** dropdown list, select the authentication method for your wireless network.

   If you select WPA-Personal or WPA-2 Personal as the authentication method, key in the WPA-PSK key or security passkey.

   IMPORTANT! The IEEE 802.11n/ac standard prohibits using High Throughput with WEP or WPA-TKIP as the unicast cipher. If you use these encryption methods, your data rate will drop to IEEE 802.11g 54Mbps connection.

5 Click **Apply** when done.

3.2.2 Managing your network clients



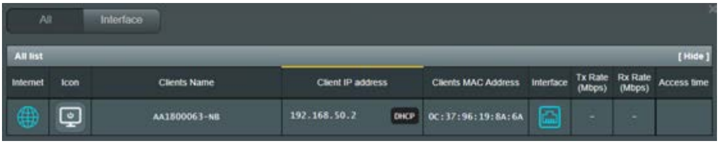
Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_43588
SSID: GS-AX5400_test

Internet status: Connected
WAN IP: 192.168.123.76
DDNS: GO

Security level: WPA2-Personal

Smart Connect: Dual-Band Smart Connect

Dual-Band Smart Connect
Network Name (SSID): GS-AX5400 test
Authentication Method: WPA2-Personal
WPA Encryption: AES
WPA-PSK key: idan0405



All list

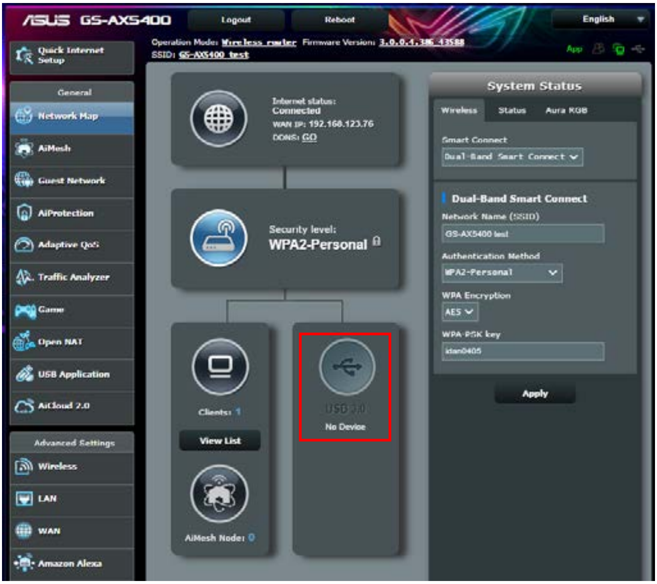
Internet	Icon	Clients Name	Client IP address	Clients MAC Address	Interface	Tx Rate (Mbps)	Rx Rate (Mbps)	Access time
		AA1800063-NB	192.168.50.2 DHCP	0C:37:96:19:8A:6A		-	-	

To manage your network clients:

1. From the navigation panel, go to **General** > **Network Map**.
2. On the **Network Map** screen, select the **Clients** icon to display your network client's information.
3. Click View List below the **Clients** icon to display all the clients.
4. To block a client's access to your network, select the client and click the open lock icon.

3.2.3 Monitoring your USB device

The ASUS wireless router provides a USB port for connecting a USB device or USB printer to allow you to share files or printer with clients in your network.



Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_43588
SSID: GS-AX5400_test

Internet status:
Connected
WAN IP: 192.168.123.76
DDNS: GO

Security level:
WPA2-Personal

Clients: 1

AiMesh Node: 0

USB 3.0
No Device

Smart Connect: Dual-Band Smart Connect

Dual-Band Smart Connect
Network Name (SSID): GS-AX5400 test
Authentication Method: WPA2-Personal
WPA Encryption: AES
WPA-PSK key: idan0405

NOTES:

- To use this feature, you need to plug a USB storage device, such as a USB hard disk or USB flash drive, to the USB 3.0/2.0 port on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the Plug-n-Share Disk Support List at **http://event.asus.com/networks/disksupport**
- The USB port supports a USB drive or a printer.

IMPORTANT! You first need to create a share account and its permission /access rights to allow other network clients to access the USB device via an FTP site/third-party FTP client utility, Servers Center, Samba, or AiCloud. For more details, refer to the section **3.10 Using the USB Application** and **3.11 Using AiCloud 2.0** in this user manual.

To monitor your USB device:

1. From the navigation panel, go to **General** > **Network Map**.
2. On the Network Map screen, select the **USB Disk Status** icon to display your USB device's information.
3. On the AiDisk Wizard field, click **GO** to set up an FTP server for Internet file sharing.

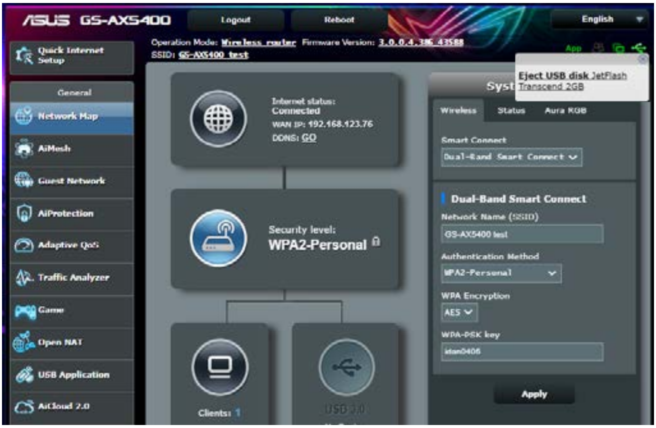
> **NOTES:**
>
> - For more details, refer to the section **3.10.2 Using Servers Center** in this user manual.
> - The wireless router works with most USB HDDs/Flash disks (up to 4TB size) and supports read-write access for FAT16, FAT32, NTFS, and HFS+.

Safely removing the USB disk

> **IMPORTANT!** Incorrect removal of the USB disk may cause data corruption.

To safely remove the USB disk:

1. From the navigation panel, go to **General** > **Network Map**.
2. In the upper right corner, click ⭠ > **Eject USB disk**. When the USB disk is ejected successfully, the USB status shows **Unmounted**.



Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_43588
SSID: GS-AX5400_test

Eject USB disk JetFlash Transcend 2GB

Internet status: Connected
WAN IP: 192.168.123.76
DDNS: GO

Security level: WPA2-Personal

Clients: 1

Smart Connect: Dual-Band Smart Connect

Dual-Band Smart Connect
Network Name (SSID): GS-AX5400 test
Authentication Method: WPA2-Personal
WPA Encryption: AES
WPA-PSK key: idan0406

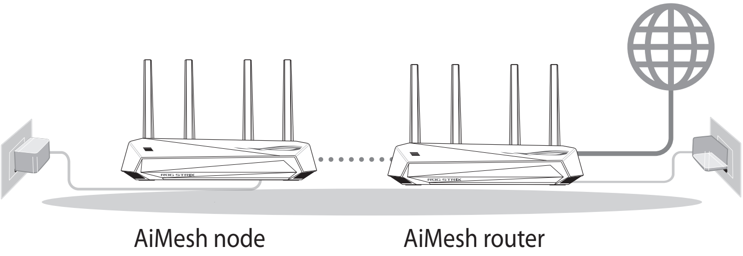
3.3 AiMesh

3.3.1 Before setting

Preparing to setup an AiMesh Wi-Fi system

1. Two (2) ASUS routers (models supporting AiMesh: https://www.asus.com/AiMesh/).
2. Assign one as AiMesh router, and another one as AiMesh node.

NOTE: If you have multiple AiMesh routers, we recommend using the router with the highest specifications as your AiMesh router and the others as AiMesh nodes.



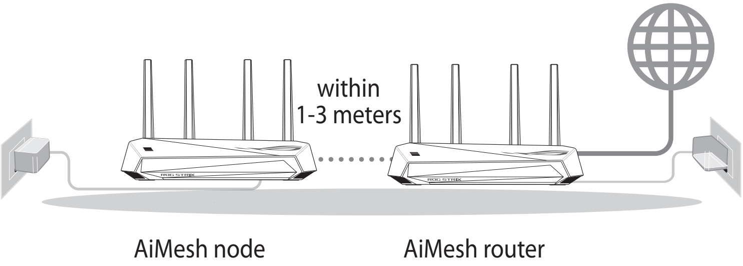
3.3.2 AiMesh Setup steps

Prepare

Place your AiMesh router and node within 1-3 meters of each other during the setup process.

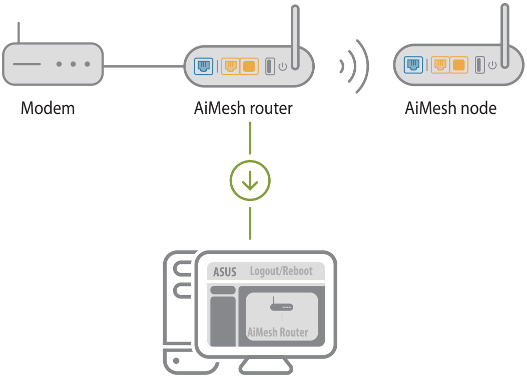
AiMesh node

Factory default status. Keep power on and standby for AiMesh system settings.



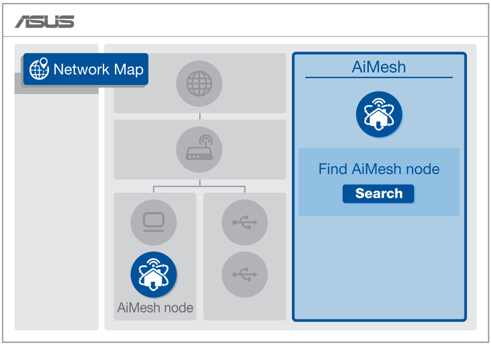
AiMesh router

1) Refer to the other router **Quick Start Guide** to connect your AiMesh router to your PC and modem, and then log in into the web GUI.



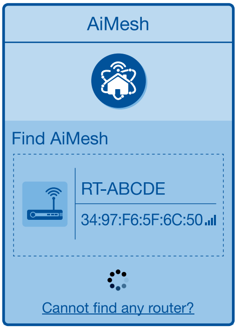
2) Go to Network Map page, click AiMesh icon and then Search for your extending AiMesh node.

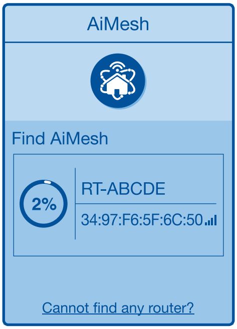
NOTE: If you cannot find the AiMesh icon here, click on firmware version and update the firmware.



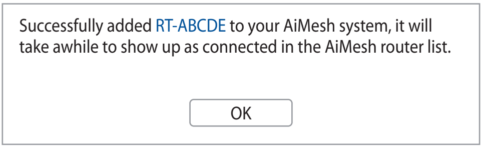
3) Click **Search**, it will automatically search for your AiMesh node. When the AiMesh node shows on this page, click it to add it into the AiMesh system.

NOTE: If you cannot find any AiMesh node, please go to **TROUBLE SHOOTING**.

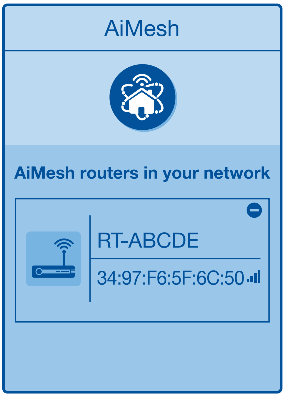




4) A message is displayed when synchronization is completed.


Successfully added RT-ABCDE to your AiMesh system, it will take awhile to show up as connected in the AiMesh router list.

5) Congratulations! You will find the pages below show up when an AiMesh node has been successfully added to the AiMesh network.



3.3.3 Troubleshooting

If your AiMesh router cannot find any AiMesh node nearby or synchronization fails, please check followings and try again.

1) Move your AiMesh node closer to the AiMesh router ideally. Ensure it is within 1-3 meters.

2) Your AiMesh node is powered on.

3) Your AiMesh node is upgraded to AiMesh supported firmware.

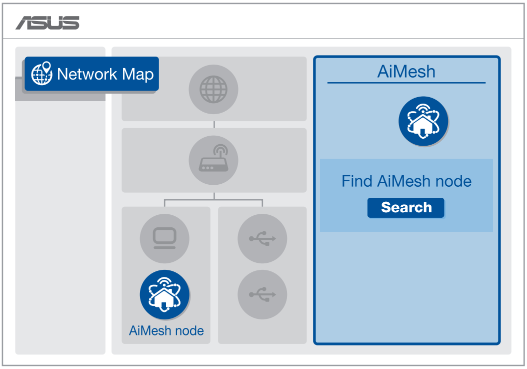
   i. Download AiMesh - supported fireware at: https://www.asus.com/AiMesh/

   ii. Power on your AiMesh node and connect it to your PC via a network cable.

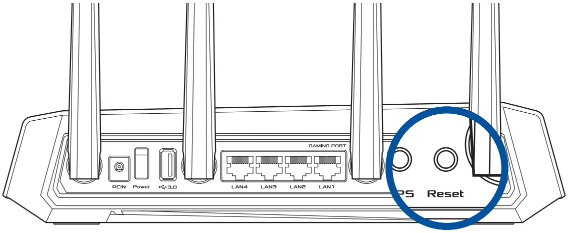
   iii. Launch a web GUI. You will be redirected to the ASUS Setup Wizard. If not, navigate to http://www.asusrouter.com

   iv. Go to **Administration** > **Firmware Upgrade**. Click on **Choose File**, and upload the AiMesh-supported firmware.

   v. After firmware uploaded, please go to Network Map page to confirm whether AiMesh icon showed up.



   vi. Press the reset button on your AiMesh node for at least 5 seconds. Release the reset button when the power LED is flashing slowly.



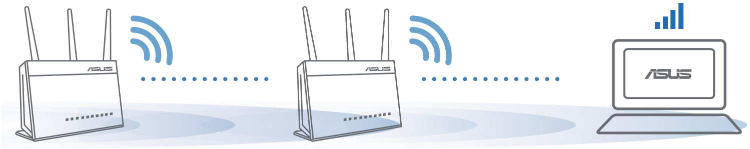
3.3.4 Relocation

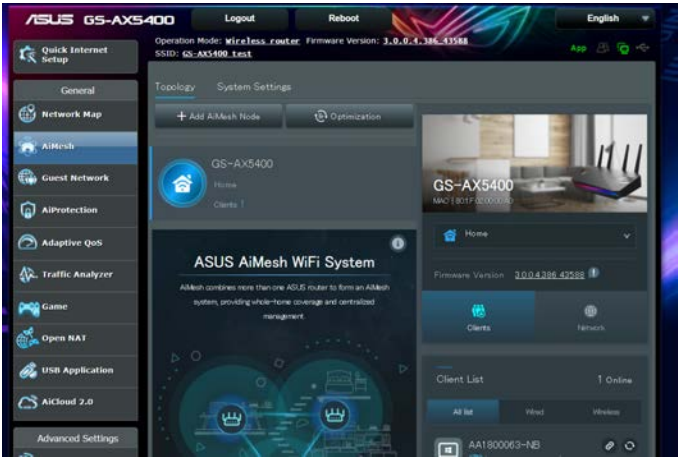
The best performance:

Locate your AiMesh node and router at the best place.

NOTES:

- To minimize interference, keep the routers away from devices like cordless phones, Bluetooth devices and microwave ovens.
- We recommend that you place the routers in an open or spacious location.





Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_43588
SSID: GS-AX5400_test

GS-AX5400
Home
Clients 1

ASUS AiMesh WiFi System

AiMesh combines more than one ASUS router to form an AiMesh system, providing whole-home coverage and centralized management.

GS-AX5400
MAC | 80:1F:02:00:00:AD

Firmware Version 3.0.0.4.386_43588

Client List 1 Online

AA1800063-NB

3.3.5 FAQs (Frequently Asked Questions)

Q1: Does the AiMesh router support Access Point mode?

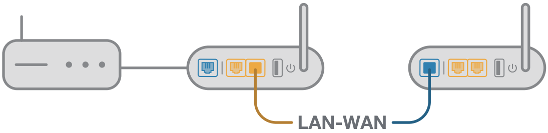
A: Yes. You can choose to set the AiMesh router as router mode or access point mode. Please go to web GUI (http://www.asusrouter.com), and go to the page **Administration** > **Operation Mode**.

Q2: Could I setup wired connection between AiMesh routers (Ethernet backhaul)?

A: Yes. AiMesh system supports both wireless and wired connection between AiMesh router and node to maximize throughput and stability. AiMesh analyzes the wireless signal strength for each frequency band available, and then determines automatically whether a wireless or wired connection is best to serve as the inter-router connection backbone.

1) Follow the setup steps to establish a connection between the AiMesh router and node via Wi-Fi first.

2) Place the node in the ideal locations for best coverage. Run an Ethernet cable from the LAN port of the AiMesh router to the WAN port of AiMesh node.



3) AiMesh system will auto-select the best path for data transmission, whether wired or wireless.

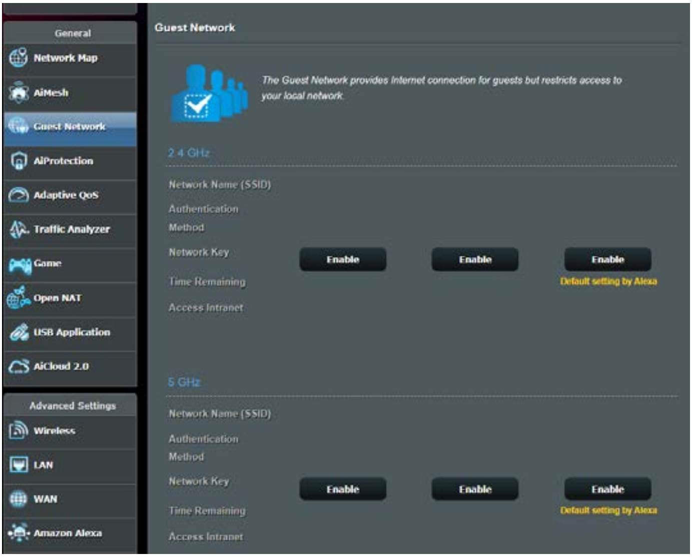
3.4 Creating a Guest Network

The Guest Network provides temporary visitors with Internet connectivity via access to separate SSIDs or networks without providing access to your private network.

NOTE: GS-AX5400 supports up to six SSIDs (three 2.4GHz and three 5GHz).

To create a guest network:

1. From the navigation panel, go to **General** > **Guest Network**.
2. On the Guest Network screen, select 2.4GHz or 5GHz frequency band for the guest network that you want to create.
3. Click **Enable**.



Guest Network

The Guest Network provides Internet connection for guests but restricts access to your local network.

2.4 GHz

Network Name (SSID)

Authentication Method

Network Key

Time Remaining

Access Intranet

Default setting by Alexa

5 GHz

Network Name (SSID)

Authentication Method

Network Key

Time Remaining

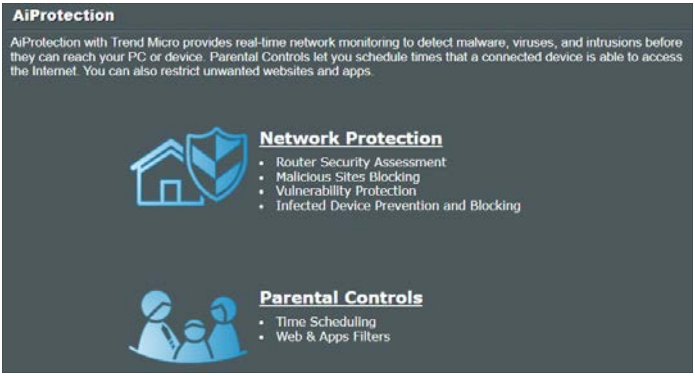
Access Intranet

Default setting by Alexa

4. To change a guest's settings, click the guest settings you want to modify. Click **Remove** to delete the guest's settings.
5. Assign a wireless name for your temporary network on the Network Name (SSID) field.
6. Select an Authentication Method.
7. If you select a WPA authentication method, select a WPA Encryption.
8. Specify the Access time or choose **Limitless**.
9. Select **Disable** or **Enable** on the Access Intranet item.
10. When done, click **Apply**.

3.5 AiProtection

AiProtection provides real-time monitoring that detects malware, spyware, and unwanted access. It also filters unwanted websites and apps and allows you to schedule Internet access time for a connected device.



AiProtection

AiProtection with Trend Micro provides real-time network monitoring to detect malware, viruses, and intrusions before they can reach your PC or device. Parental Controls let you schedule times that a connected device is able to access the Internet. You can also restrict unwanted websites and apps.

Network Protection

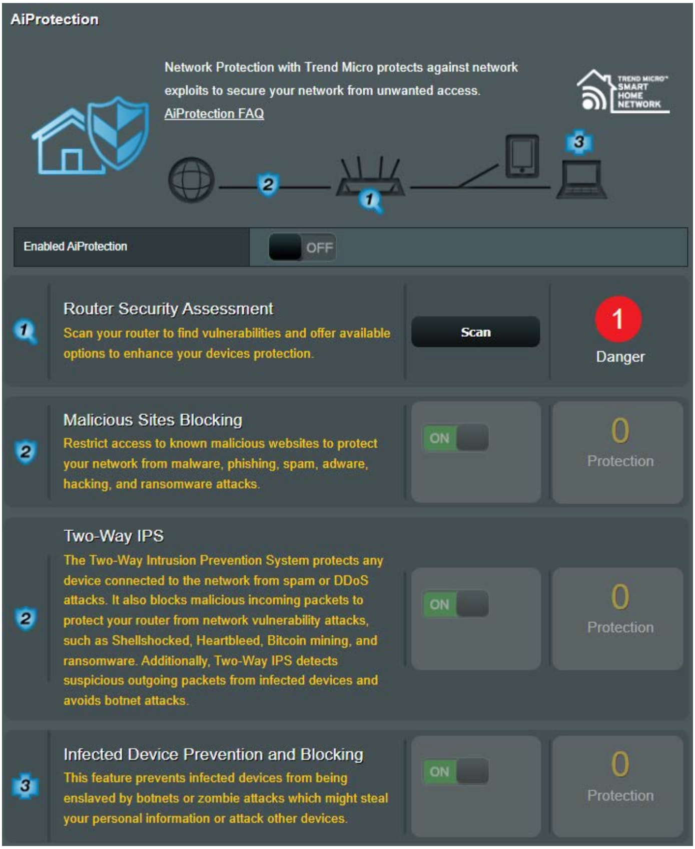
- Router Security Assessment
- Malicious Sites Blocking
- Vulnerability Protection
- Infected Device Prevention and Blocking

Parental Controls

- Time Scheduling
- Web & Apps Filters

3.5.1 Configuring AiProtection

AiProtection prevents network exploits and secures your network from unwanted access.



AiProtection

Network Protection with Trend Micro protects against network exploits to secure your network from unwanted access.

AiProtection FAQ

Enabled AiProtection — OFF

1 Router Security Assessment — Scan your router to find vulnerabilities and offer available options to enhance your devices protection. — Scan — 1 Danger

2 Malicious Sites Blocking — Restrict access to known malicious websites to protect your network from malware, phishing, spam, adware, hacking, and ransomware attacks. — ON — 0 Protection

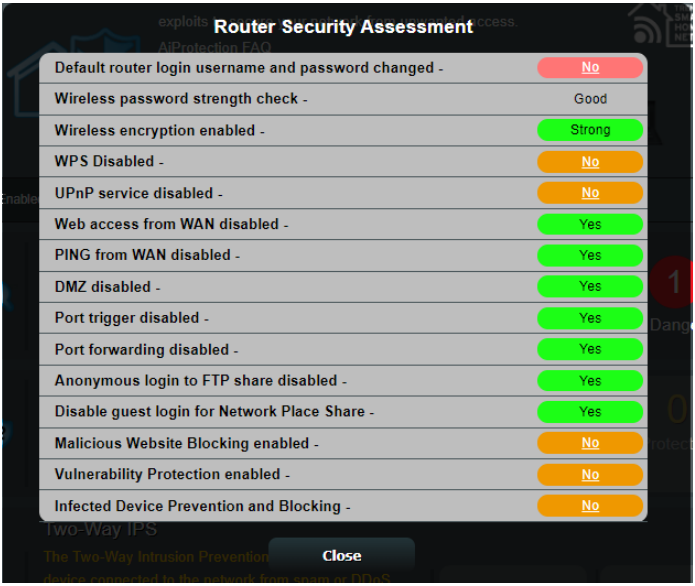
2 Two-Way IPS — The Two-Way Intrusion Prevention System protects any device connected to the network from spam or DDoS attacks. It also blocks malicious incoming packets to protect your router from network vulnerability attacks, such as Shellshocked, Heartbleed, Bitcoin mining, and ransomware. Additionally, Two-Way IPS detects suspicious outgoing packets from infected devices and avoids botnet attacks. — ON — 0 Protection

3 Infected Device Prevention and Blocking — This feature prevents infected devices from being enslaved by botnets or zombie attacks which might steal your personal information or attack other devices. — ON — 0 Protection

To Configure AiProtection:

1. From the navigation panel, go to **General** > **AiProtection**.
2. From the AiProtection main page, click **Network Protection**.
3. From the Network Protection pane, click **Scan**.

The search results are displayed on the **Router Security Assessment** page.



Router Security Assessment

Default router login username and password changed -	No
Wireless password strength check -	Good
Wireless encryption enabled -	Strong
WPS Disabled -	No
UPnP service disabled -	No
Web access from WAN disabled -	Yes
PING from WAN disabled -	Yes
DMZ disabled -	Yes
Port trigger disabled -	Yes
Port forwarding disabled -	Yes
Anonymous login to FTP share disabled -	Yes
Disable guest login for Network Place Share -	Yes
Malicious Website Blocking enabled -	No
Vulnerability Protection enabled -	No
Infected Device Prevention and Blocking -	No

IMPORTANT! Items marked with **Yes** on the **Router Security Assessment** page are considered to be safe.

4. (Optional) From the **Router Security Assessment** page, manually configure the items marked as **No**, **Weak**, or **Very Weak**. To do this:

    a. Click an item to go to the item's setting page.

    b. From the item's security settings page, configure and make the necessary changes and click **Apply** when done.

    c. Go back to the **Router Security Assessment** page and click **Close** to exit the page.

5. Click **OK** on the confirmation message.

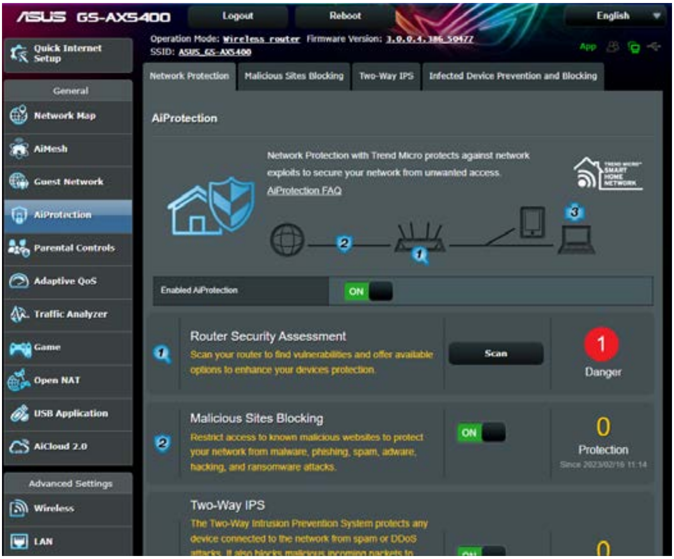
3.5.2 Blocking Malicious Sites

This feature restricts access to known malicious websites in the cloud database for an always-up-to-date protection.

> **NOTE:** This function is automatically enabled if you run the Router Weakness Scan.

To enable Malicious Sites Blocking:

1. From the navigation panel, go to **General** > **AiProtection**.
2. From the AiProtection main page, click **Network Protection**.
3. From the Malicious Sites Blocking pane, click **ON**.



Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_50477
SSID: ASUS_GS-AX5400

AiProtection

Network Protection with Trend Micro protects against network exploits to secure your network from unwanted access.
AiProtection FAQ

Enabled AiProtection ON

1 Router Security Assessment
Scan your router to find vulnerabilities and offer available options to enhance your devices protection.
1 Danger

2 Malicious Sites Blocking
Restrict access to known malicious websites to protect your network from malware, phishing, spam, adware, hacking, and ransomware attacks.
0 Protection
Since 2023/02/16 11:14

Two-Way IPS
The Two-Way Intrusion Prevention System protects any device connected to the network from spam or DDoS attacks. It also blocks malicious incoming packets to
0

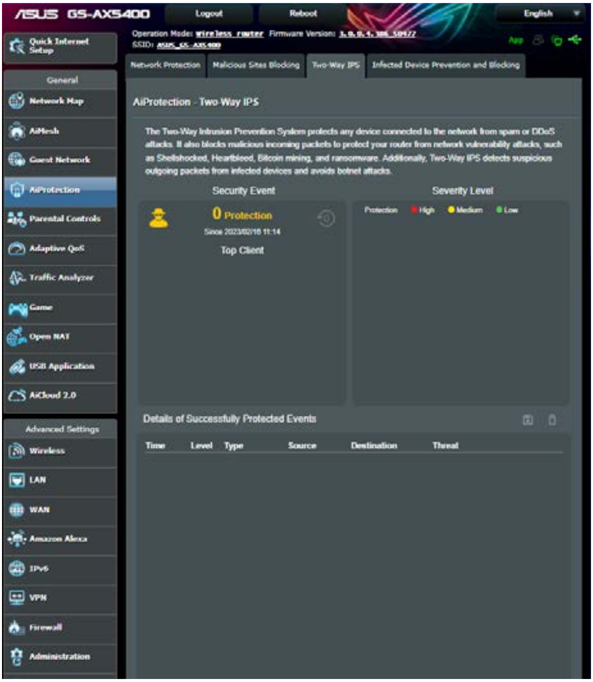
3.5.3 Two-Way IPS

This feature resolves common exploits within the router configuration.

NOTE: This function is automatically enabled if you run the Router Weakness Scan.

To enable Two-Way IPS:

1. From the navigation panel, go to **General** > **AiProtection**.
2. From the AiProtection main page, click **Network Protection**.
3. From the Two-Way IPS pane, click **ON**.



Operation Mode: wireless router Firmware Version: 3.0.0.4.386_50477
SSID: ASUS_GS-AX5400

AiProtection - Two-Way IPS

The Two-Way Intrusion Prevention System protects any device connected to the network from spam or DDoS attacks. It also blocks malicious incoming packets to protect your router from network vulnerability attacks, such as Shellshocked, Heartbleed, Bitcoin mining, and ransomware. Additionally, Two-Way IPS detects suspicious outgoing packets from infected devices and avoids botnet attacks.

0 Protection
Since 2023/02/16 11:14

Details of Successfully Protected Events

Time	Level	Type	Source	Destination	Threat

3.5.4 Infected Device Prevention and Blocking

This feature prevents infected devices from communicating personal information or infected status to external parties.

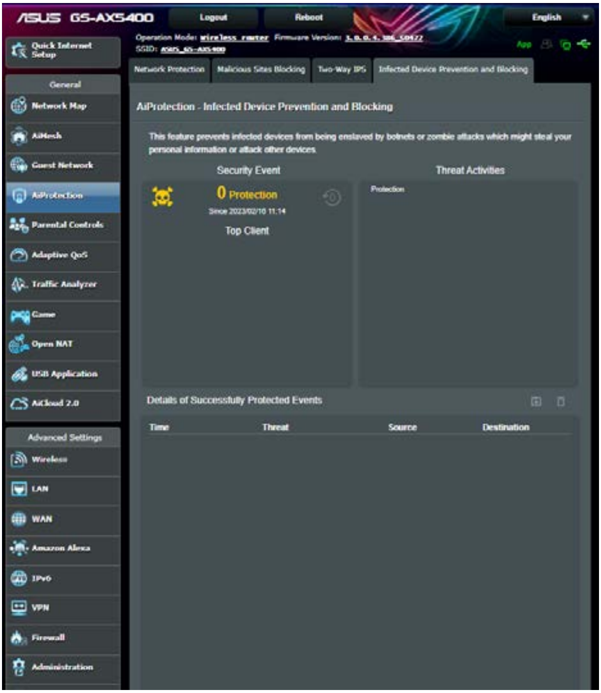
> **NOTE:** This function is automatically enabled if you run the Router Weakness Scan.

To enable infected device prevention and blocking:

1. From the navigation panel, go to **General** > **AiProtection**.
2. From the AiProtection main page, click **Network Protection**.
3. From the Infected Device Prevention and Blocking pane, click **ON**.

To configure Alert Preference:

1. From the Infected Device Prevention and Blocking pane, click **Alert Preference**.
2. Select or key in the e-mail provider, e-mail account, and password then click **Apply**.



Operation Mode: wireless router Firmware Version: 3.0.0.4.386_50477
SSID: ASUS_GS-AX5400

AiProtection - Infected Device Prevention and Blocking

This feature prevents infected devices from being enslaved by botnets or zombie attacks which might steal your personal information or attack other devices.

Security Event

0 Protection
Since 2023/02/10 11:14

Top Client

Threat Activities

Protection

Details of Successfully Protected Events

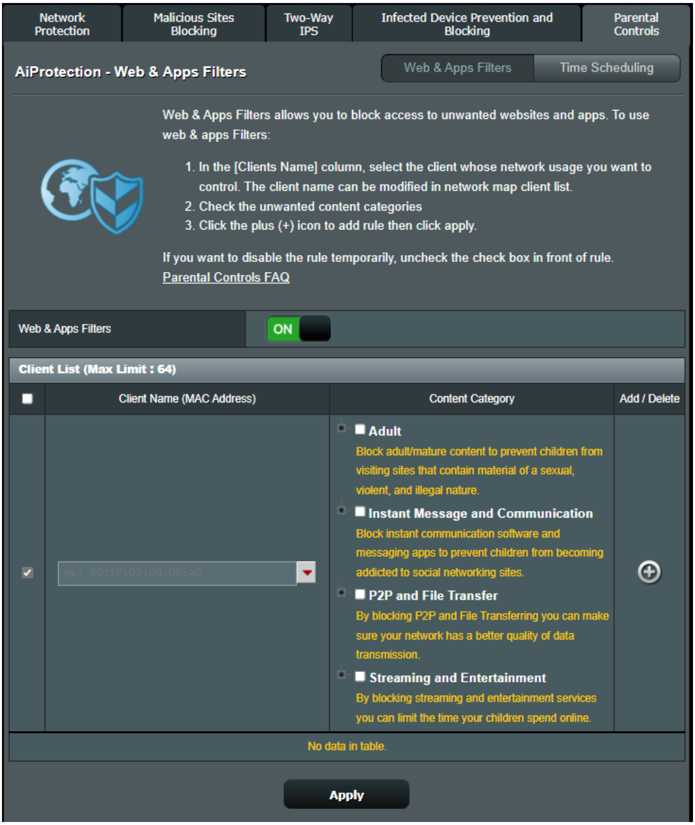
Time	Threat	Source	Destination

3.5.5 Setting up Parental Control

Parental Control allows you to control the Internet access time or set the time limit for a client's network usage.

To enable Two-Way IPS:

1. From the navigation panel, go to **General** > **AiProtection**.
2. From the AiProtection main page, click **Parental Controls**.



AiProtection - Web & Apps Filters

Web & Apps Filters allows you to block access to unwanted websites and apps. To use web & apps Filters:

1. In the [Clients Name] column, select the client whose network usage you want to control. The client name can be modified in network map client list.
2. Check the unwanted content categories
3. Click the plus (+) icon to add rule then click apply.

If you want to disable the rule temporarily, uncheck the check box in front of rule.
Parental Controls FAQ

Web & Apps Filters: ON

Client List (Max Limit : 64)

□	Client Name (MAC Address)	Content Category	Add / Delete
☑	ex: 80:1F:02:00:00:A0	□ **Adult** Block adult/mature content to prevent children from visiting sites that contain material of a sexual, violent, and illegal nature. □ **Instant Message and Communication** Block instant communication software and messaging apps to prevent children from becoming addicted to social networking sites. □ **P2P and File Transfer** By blocking P2P and File Transferring you can make sure your network has a better quality of data transmission. □ **Streaming and Entertainment** By blocking streaming and entertainment services you can limit the time your children spend online.	⊕

No data in table.

Web & Apps Filters

Web & Apps Filters is a feature of Parental Controls that allows you to block access to unwanted web sites or applications.

To configure Web & Apps Filters:

1. From the navigation panel, go to **General** > **AiProtection**.
2. From the AiProtection main page, click **Parental Controls** icon to go to the Parental Controls tab.
3. From the **Web & Apps Filters** pane, click **ON**.

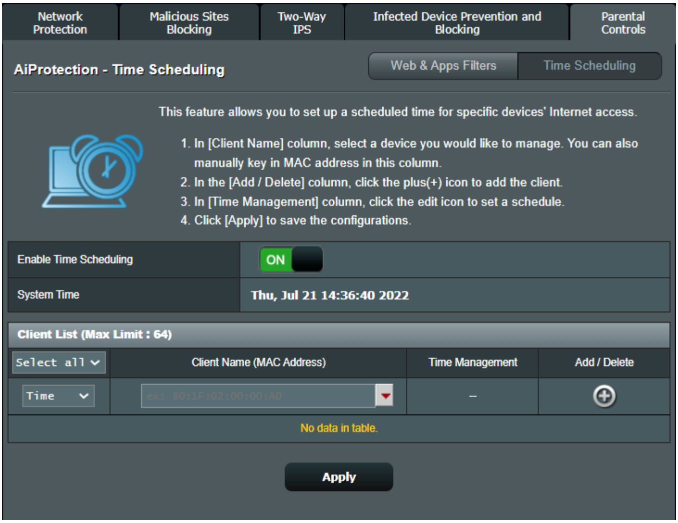
4 When the End Users License Agreement (EULA) message prompt appears, click **I agree** to continue.

5. From the **Client List** column, select or key in the client's name from the dropdown list box.
6. From the **Content Category** column, select the filters from the four main categories: **Adult**, **Instant Message and Communication**, **P2P and File Transfer**, and **Streaming and Entertainment**.
7. Click ⊕ to add the client's profile.
8. Click **Apply** to save the settings.

Time Scheduling

Time Scheduling allows you to set the time limit for a client's network usage.

NOTE: Ensure that your system time is synchronized with the NTP server.



AiProtection - Time Scheduling

This feature allows you to set up a scheduled time for specific devices' Internet access.

1. In [Client Name] column, select a device you would like to manage. You can also manually key in MAC address in this column.
2. In the [Add / Delete] column, click the plus(+) icon to add the client.
3. In [Time Management] column, click the edit icon to set a schedule.
4. Click [Apply] to save the configurations.

Enable Time Scheduling	ON
System Time	Thu, Jul 21 14:36:40 2022

Client List (Max Limit : 64)

Select all	Client Name (MAC Address)	Time Management	Add / Delete
Time	ex: 80:1F:02:00:00:A0	–	⊕
No data in table.			

To configure Time Scheduling:

1. From the navigation panel, go to **General** >**AiProtection** > **Parental Controls** > **Time Scheduling**.
2. From the **Enable Time Scheduling** pane, click **ON**.
3. From the **Client Name** column, select or key in the client's name from the dropdown list box.

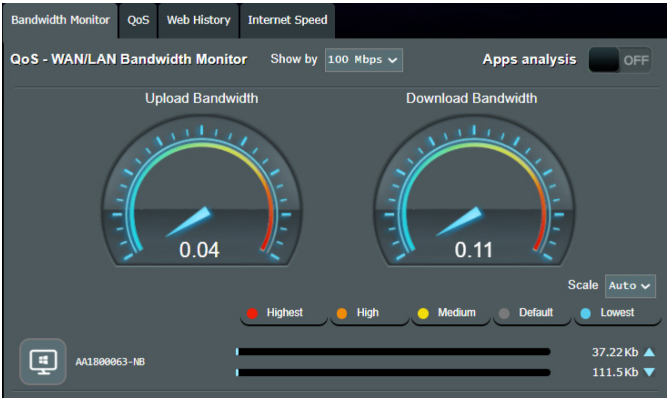
NOTE: You may also key in the client's MAC address in the Client MAC Address column. Ensure that the client name does not contain special characters or spaces as these may cause the router to function abnormally.

4. Click ⊕ to add the client's profile.
5. Click **Apply** to save the settings.

3.6 Adaptive QoS

3.6.1 Bandwidth Monitor

This feature allows you to monitor the bandwidth of WAN/LAN and displays the upload and download speed of your connection.



Show by 100 Mbps

Apps analysis OFF

Scale Auto

37.22 Kb ▲

111.5 Kb ▼

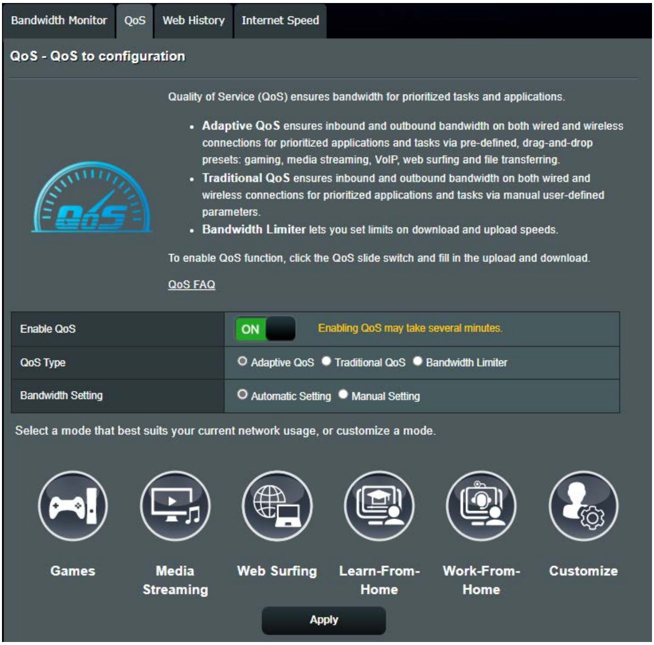
Apps analysis

To enable Apps analysis function:

1. From the navigation panel, go to **General** > **Adaptive QoS**> **Bandwidth Monitor** tab.
2. From the **Apps analysis** pane, click **ON**.

3.6.2 QoS

This feature ensures bandwidth for prioritized tasks and applications.



QoS - QoS to configuration

Quality of Service (QoS) ensures bandwidth for prioritized tasks and applications.

- **Adaptive QoS** ensures inbound and outbound bandwidth on both wired and wireless connections for prioritized applications and tasks via pre-defined, drag-and-drop presets: gaming, media streaming, VoIP, web surfing and file transferring.
- **Traditional QoS** ensures inbound and outbound bandwidth on both wired and wireless connections for prioritized applications and tasks via manual user-defined parameters.
- **Bandwidth Limiter** lets you set limits on download and upload speeds.

To enable QoS function, click the QoS slide switch and fill in the upload and download.

QoS FAQ

Enable QoS	ON Enabling QoS may take several minutes.
QoS Type	○ Adaptive QoS ● Traditional QoS ● Bandwidth Limiter
Bandwidth Setting	○ Automatic Setting ● Manual Setting

Select a mode that best suits your current network usage, or customize a mode.

To enable the QoS function:

1. From the navigation panel, go to **General** > **Adaptive QoS**> **QoS** tab.
2. From the **Enable QoS** pane, click **ON**.
3. Fill in the upload and download bandwidth fields.

> **NOTE:** Get the bandwidth information from your ISP. You can also go to http://speedtest.net to check and get your bandwidth.

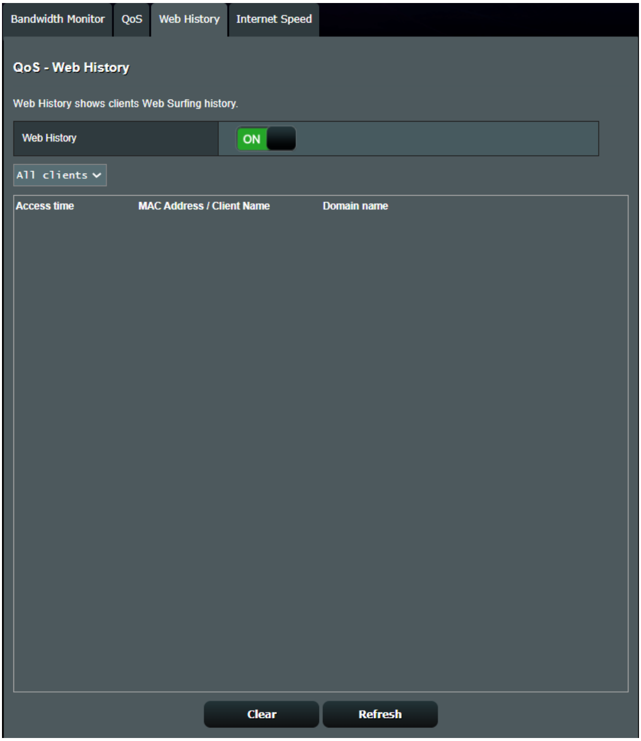
4. Select the QoS Type (Adaptive or Traditional) for your configuration.

> **NOTE:** The definition of the QoS Type is displayed on the QoS tab for your reference.

5. Click **Apply**.

3.6.3 Web History

This feature displays the history and details of the sites or URLs that the client visited.



QoS - Web History

Web History shows clients Web Surfing history.

Web History: ON

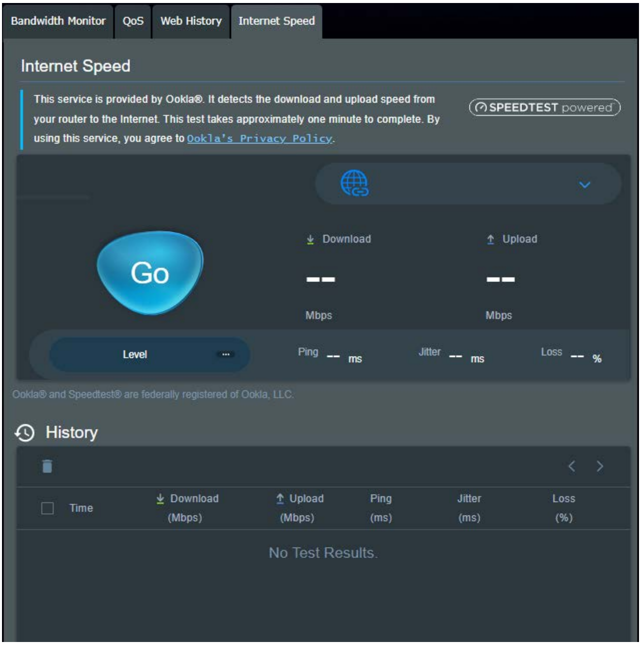
Access time	MAC Address / Client Name	Domain name

To view the Web History:

1. From the navigation panel, go to **General** > **Adaptive QoS**> **Web History** tab.
2. (Optional) Click **Refresh** to clear the list.

3.6.4 Internet Speed

This feature detects the download and upload speed from you router to the Internet.



Internet Speed

This service is provided by Ookla®. It detects the download and upload speed from your router to the Internet. This test takes approximately one minute to complete. By using this service, you agree to Ookla's Privacy Policy.

Ookla® and Speedtest® are federally registered of Ookla, LLC.

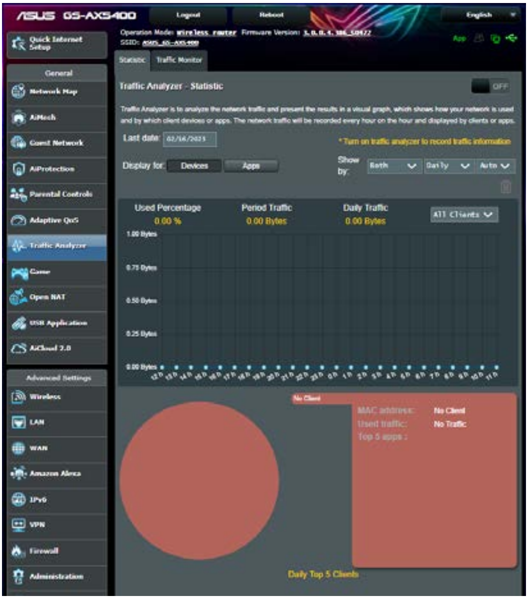
History

□ Time	Download (Mbps)	Upload (Mbps)	Ping (ms)	Jitter (ms)	Loss (%)

No Test Results.

3.7 Traffic Analyzer

Traffic Analyzer gives you an at-a-glance view of what's happening on your network on a daily, weekly, or monthly basis. It lets you to quickly see each user's bandwidth usage or the device or app used, helping you reduce the bottlenecks in your Internet connection. It's also a great way to monitor the users' Internet usage or activities.



Operation Mode: wireless router Firmware Version: 3.0.0.4.386_50472
SSID: ASUS_GS-AX5400

Traffic Analyzer - Statistic

Traffic Analyzer is to analyze the network traffic and present the results in a visual graph, which shows how your network is used and by which client devices or apps. The network traffic will be recorded every hour on the hour and displayed by clients or apps.

Last date: 02/16/2021

*Turn on traffic analyzer to record traffic information

Display for: Devices Apps

Show by: Both Daily Auto

Used Percentage 0.00 %

Period Traffic 0.00 Bytes

Daily Traffic 0.00 Bytes

MAC address: No Client

Used traffic: No Traffic

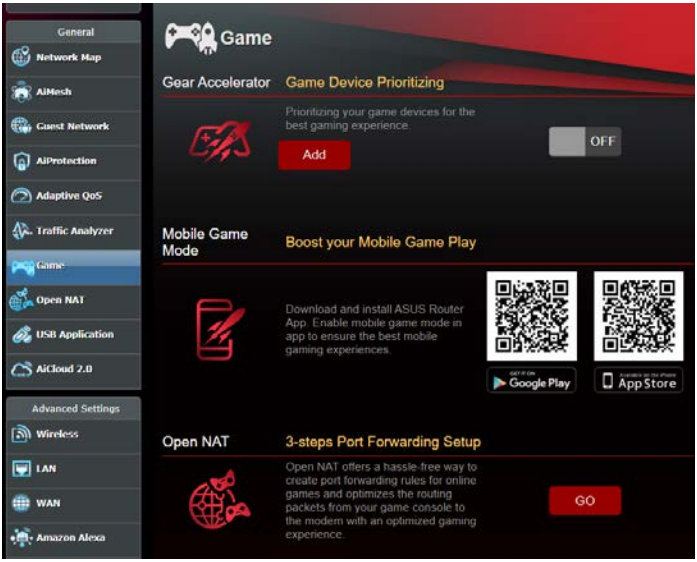
Top 5 apps :

To configure the Traffic analyzer:

1. From the navigation panel, go to **General** > **Traffic Analyzer**.
2. From the **Traffic Analyzer** main page, turn on traffic analyzer statistic.
3. Select the date whose chart you want to display.
4. On the **Display for** field, select Router or Apps to display the traffic information.
5. On the Show by field, select how you want to display the traffic information.

3.8 Game

ROG STRIX gaming router puts the gaming packet as the top priority to provide you with the best gaming experience.



Prioritizing your game devices for the best gaming experience.

Download and install ASUS Router App. Enable mobile game mode in app to ensure the best mobile gaming experiences.

Open NAT offers a hassle-free way to create port forwarding rules for online games and optimizes the routing packets from your game console to the modem with an optimized gaming experience.

Gear Accelerator

Gear Accelerator allows you to prioritize game devices wirelessly via online control panel for the best gaming experience.

To configure Gear Accelerator:

1. From the navigation panel, go to **General > Game**.
2. From the **Gear Accelerator** pane, click **ON**.
3. After applying setting, click **Add** to choose the client name.
4. Click ⊕ to add the client's profile.
5. Click **Apply** to save the settings

NOTE: If you want delete the client profile, click ⊖ .

Mobile Game Mode

Download and install ASUS Router App. Enable mobile game mode in the app to ensure the best mobile game experiences.

GET IT ON Google Play

Download on the App Store

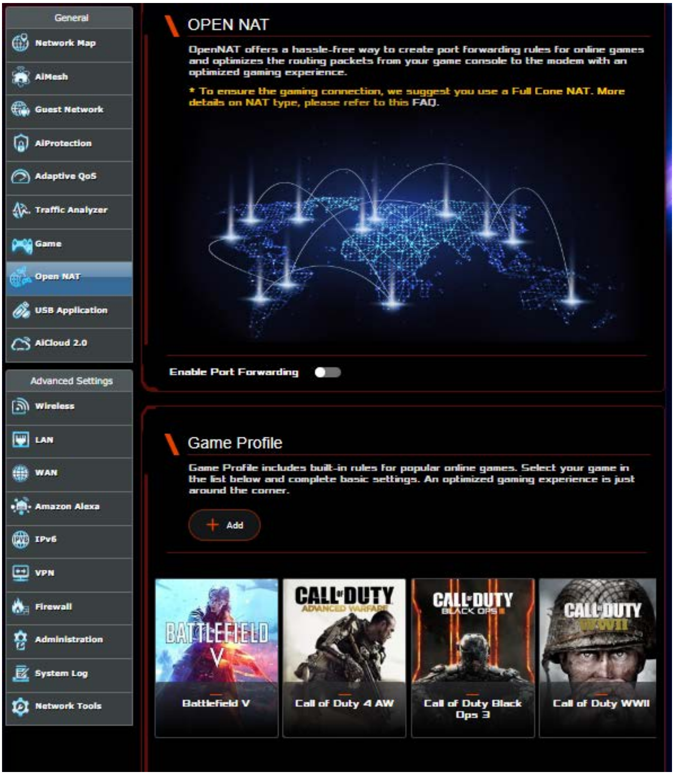
Open NAT

From navigation panel, go to **General** > **Game** > **Open NAT**, click **GO** to set up port forwarding in 3 steps. Refer to the section **Open NAT** for more information.

3.9 Open NAT

Open NAT offers a hassle-free way to create port forwarding rules for online games and optimizes the routing packets from your game console to the modem with an optimized gaming experience.

When playing PC or console games, there may be some connection issues due to the ISP or router settings in your environment such as NAT and port blocks. Game Profile helps ensure that ROG STRIX gaming router is not blocking the game connection.



OPEN NAT

OpenNAT offers a hassle-free way to create port forwarding rules for online games and optimizes the routing packets from your game console to the modem with an optimized gaming experience.

* To ensure the gaming connection, we suggest you use a Full Cone NAT. More details on NAT type, please refer to this FAQ.

Enable Port Forwarding

Game Profile

Game Profile includes built-in rules for popular online games. Select your game in the list below and complete basic settings. An optimized gaming experience is just around the corner.

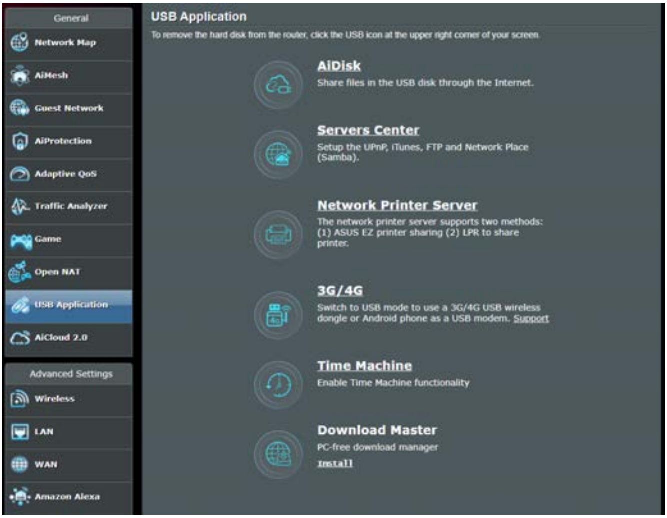
To configure Open NAT:

1. From the navigation panel, go to **General > Open NAT**.
2. Slide on **Enable Port Forwarding**.
3. From the **Game List**, select a game and complete basic settings.
4. Click **OK**.

3.10 Using the USB Application

The USB Applications function provides AiDisk, Servers Center, Network Printer Server and Download Master submenus.

IMPORTANT! To use the server functions, you need to insert a USB storage device, such as a USB hard disk or USB flash drive, in the USB 3.0 port on the rear panel of your wireless router. Ensure that the USB storage device is formatted and partitioned properly. Refer to the ASUS website at http://event.asus.com/2009/networks/disksupport/ for the file system support table.



USB Application

To remove the hard disk from the router, click the USB icon at the upper right corner of your screen.

AiDisk
Share files in the USB disk through the Internet.

Servers Center
Setup the UPnP, iTunes, FTP and Network Place (Samba).

Network Printer Server
The network printer server supports two methods: (1) ASUS EZ printer sharing (2) LPR to share printer.

3G/4G
Switch to USB mode to use a 3G/4G USB wireless dongle or Android phone as a USB modem. Support

Time Machine
Enable Time Machine functionality

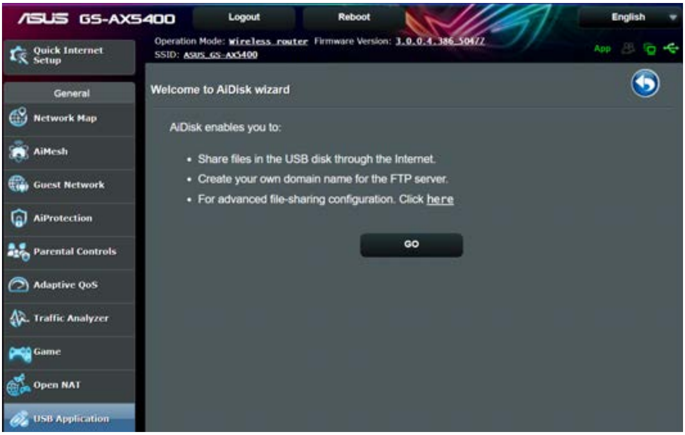
Download Master
PC-free download manager
Install

3.10.1 Using AiDisk

AiDisk allows you to share files stored on a connected USB device through the Internet. AiDisk also assists you with setting up ASUS DDNS and an FTP server.

To use AiDisk:

1. From the navigation panel, go to **General** > **USB Application**, then click the **AiDisk** icon.
2. From the Welcome to AiDisk wizard screen, click **Go**.



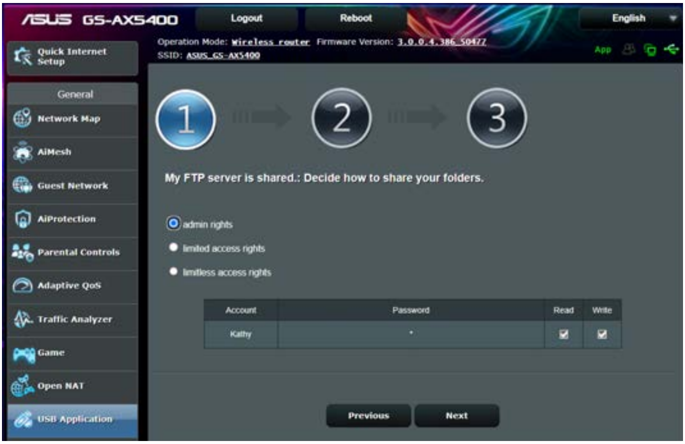
Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_50477
SSID: ASUS_GS-AX5400

Welcome to AiDisk wizard

AiDisk enables you to:

- Share files in the USB disk through the Internet.
- Create your own domain name for the FTP server.
- For advanced file-sharing configuration. Click here

3. Select the access rights that you want to assign to the clients accessing your shared data.



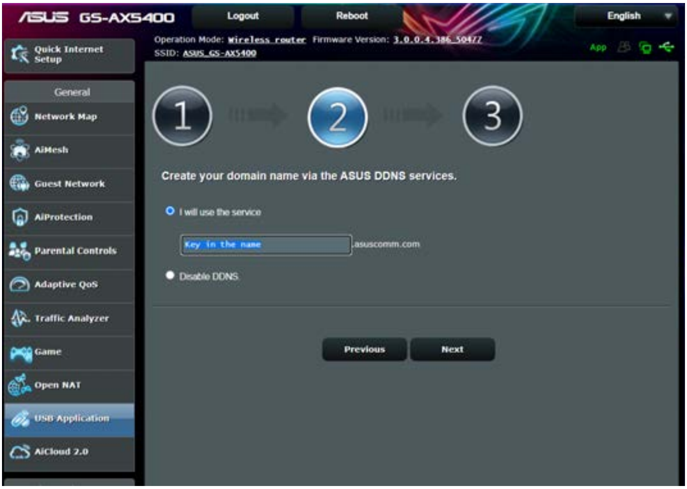
Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_50477
SSID: ASUS_GS-AX5400

My FTP server is shared.: Decide how to share your folders.

◉ admin rights
● limited access rights
● limitless access rights

Account	Password	Read	Write
Kathy	*	☑	☑

4. Create your domain name via the ASUS DDNS services, read the Terms of Service and then select **I will use the service and accept the Terms of service** and key in your domain name. When done, click **Next**.



Operation Mode: Wireless router Firmware Version: 3.0.0.4.386_50477
SSID: ASUS_GS-AX5400

Create your domain name via the ASUS DDNS services.

○ I will use the service

Key in the name .asuscomm.com

● Disable DDNS

You can also select **Skip ASUS DDNS settings** then click **Next** to skip the DDNS setting.

5. Click **Finish** to complete the setting.

6. To access the FTP site that you created, launch a web browser or a third-party FTP client utility and key in the ftp link (**ftp://<domain name>.asuscomm.com**) you have previously created.

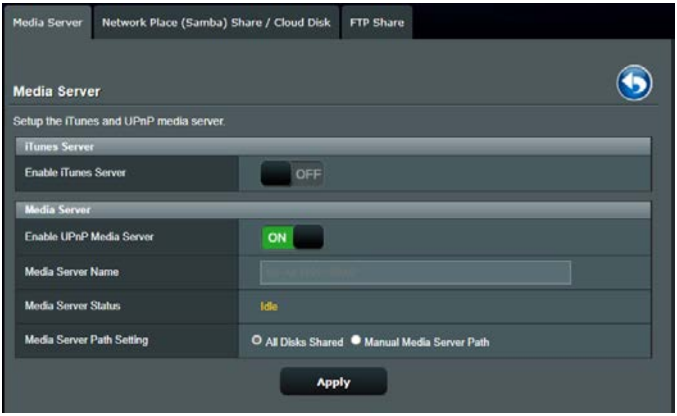
3.10.2 Using Servers Center

Servers Center allows you to share the media files from the USB disk via a Media Server directory, Samba share service, or FTP share service. You can also configure other settings for the USB disk in the Servers Center.

Using Media Server

Your wireless router allows DLNA-supported devices to access multimedia files from the USB disk connected to your wireless router.

> **NOTE:** Before using the DLNA Media Server function, connect your device to the router's network.



Media Server

Setup the iTunes and UPnP media server.

iTunes Server	
Enable iTunes Server	OFF

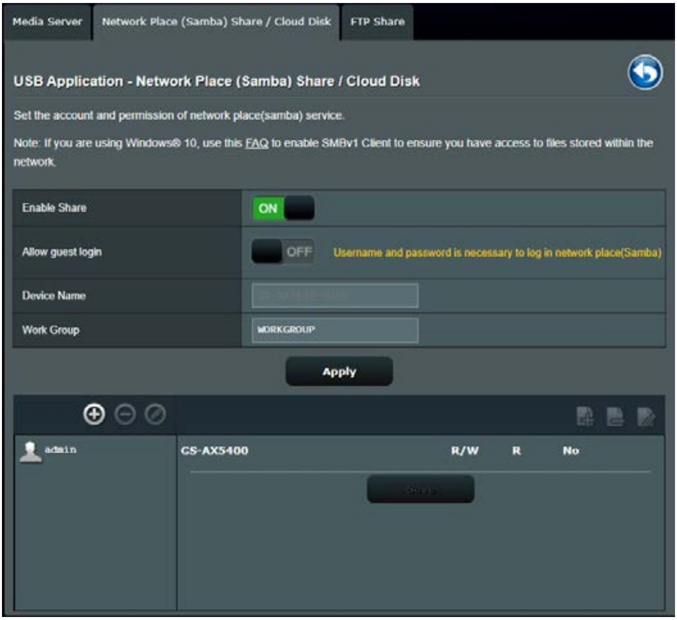
Media Server	
Enable UPnP Media Server	ON
Media Server Name	
Media Server Status	Idle
Media Server Path Setting	○ All Disks Shared ● Manual Media Server Path

To launch the Media Server setting page, go to **General** > **USB Application** > **Media Server** tab. Refer to the following for the descriptions of the fields:

- **Enable iTunes Server**: Select ON/OFF to enable/disable the iTunes Server.
- **Enable UPnP Media Server**: Select ON/OFF to enable/disable the DLNA Media Server.
- **Media Server Status**: Displays the status of the media server.
- **Media Server Path Setting**: Select **All Disks Shared** or **Manual Media Server Path**.

Using Network Place (Samba) Share service

Network Place (Samba) Share allows you to set up the accounts and permissions for the Samba service.



USB Application - Network Place (Samba) Share / Cloud Disk

Set the account and permission of network place(samba) service.

Note: If you are using Windows® 10, use this FAQ to enable SMBv1 Client to ensure you have access to files stored within the network.

Enable Share	ON
Allow guest login	OFF Username and password is necessary to log in network place(Samba)
Device Name	
Work Group	WORKGROUP

admin	GS-AX5400	R/W	R	No

To use Samba share:

1. From the navigation panel, go to **General** > **USB Application** > **Network Place (Samba) Share / Cloud Disk** tab.

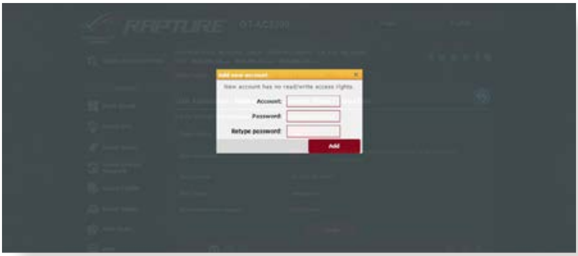
NOTE: Network Place (Samba) Share is enabled by default.

2. Follow the steps below to add, delete, or modify an account.

To create a new account:

a) Click ⊕ to add new account.

b) In the **Account** and **Password** fields, key in the name and password of your network client. Retype the password to confirm. Click **Add** to add the account to the list.



New account has no read/write access rights.

Account:
Password:
Retype password:

To delete an existing account:

a) Select the account that you want to delete.

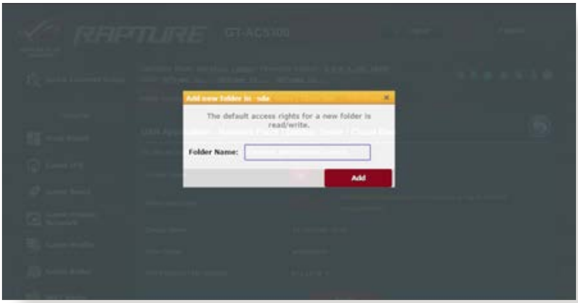
b) Click ⊖.

c) When prompted, click **Delete** to confirm the account deletion.

To add a folder:

a) Click .

b) Enter the folder name, and click **Add**. The folder that you created will be added to the folder list.



The default access rights for a new folder is read/write.

Folder Name:

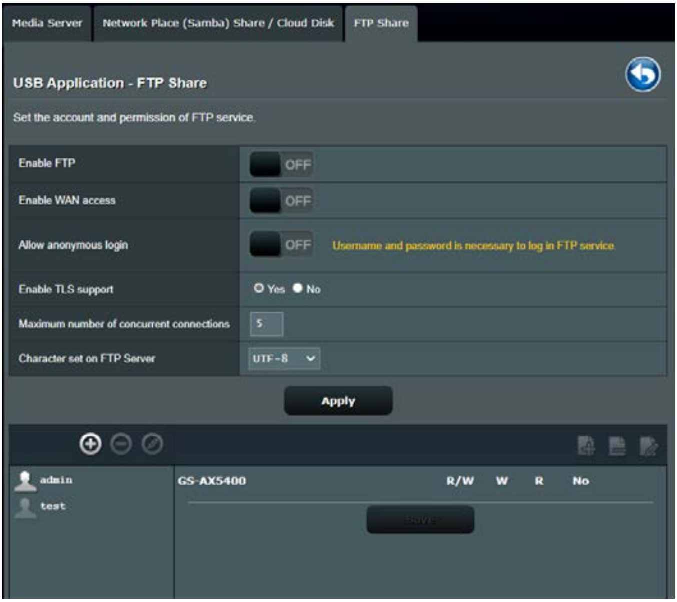
3. From the list of folders, select the type of access permission that you want to assign for specific folders:
   - **R/W**: Select this option to assign read/write access.
   - **R**: Select this option to assign read-only access.
   - **No**: Select this option if you do not want to share a specific file folder.
4. Click **Apply** to apply the changes.

Using the FTP Share service

FTP share enables an FTP server to share files from USB disk to other devices via your local area network or via the Internet.

IMPORTANT!

- Ensure that you safely remove the USB disk. Incorrect removal of the USB disk may cause data corruption.
- To safely remove the USB disk, refer to the section **Safely removing the USB disk** under **3.2.3 Monitoring your USB device**.



USB Application - FTP Share

Set the account and permission of FTP service.

Enable FTP	OFF
Enable WAN access	OFF
Allow anonymous login	OFF Username and password is necessary to log in FTP service.
Enable TLS support	○ Yes ● No
Maximum number of concurrent connections	5
Character set on FTP Server	UTF-8

To use FTP Share service:

NOTE: Ensure that you have set up your FTP server through AiDisk. For more details, refer to the section **3.10.1 Using AiDisk**.

1. From the navigation panel, click **General** > **USB Application** > **FTP Share** tab.

2. From the list of folders, select the type of access rights that you want to assign for specific folders:
    - **R/W**: Select to assign read/write access for a specific folder.
    - **W**: Select to assign write only access for a specific folder.
    - **R**: Select to assign read only access for a specific folder.
    - **No**: Select this option if you do not want to share a specific folder.
3. If you prefer, you can set the **Allow anonymous login** field to **ON**.
4. In the **Maximum number of concurrent connections** field, key in the number of devices that can simultaneously connect to the FTP share server.
5. Click **Apply** to confirm the changes.
6. To access the FTP server, key in the ftp link **ftp://<hostname>.asuscomm.com** and your user name and password on a web browser or a third-party FTP utility.

3.10.3 3G/4G

3G/4G USB modems can be connected to the router to allow Internet access.

NOTE: For a list of verified USB modems, please visit: http://event.asus.com/2009/networks/3gsupport/

To set up 3G/4G internet access:

1. From the navigation panel, click **General** > **USB Application** > **3G/4G**.
2. In the **Enable USB Modem** field, select **Yes**.
3. Set up the following:
    - **Location**: Select your 3G/4G service provider's location from the dropdown list.
    - **ISP**: Select your Internet Service Provider (ISP) from the dropdown list.
    - **APN (Access Point Name) service (optional)**: Contact your 3G/4G service provider for detailed information.
    - **Dial Number and PIN code**: The 3G/4G provider's access number and PIN code for connection.

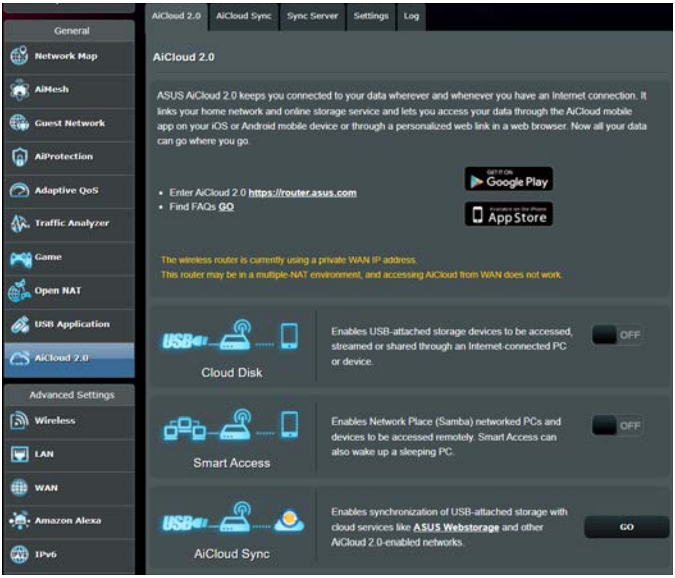
    NOTE: PIN code may vary from different providers.

    - **Username / Password:** The username and password will be provided by the 3G/4G network carrier.
    - **USB Adapter**: Choose your USB 3G / 4G adapter from the dropdown list. If you are not sure of your USB adapter's model or the model is not listed in the options, select **Auto**.
4. Click **Apply**.

NOTE: The router will reboot for the settings to take effect.

3.11 Using AiCloud 2.0

AiCloud 2.0 is a cloud service application that allows you to save, sync, share, and access your files.



AiCloud 2.0

ASUS AiCloud 2.0 keeps you connected to your data wherever and whenever you have an Internet connection. It links your home network and online storage service and lets you access your data through the AiCloud mobile app on your iOS or Android mobile device or through a personalized web link in a web browser. Now all your data can go where you go.

- Enter AiCloud 2.0 https://router.asus.com
- Find FAQs GO

The wireless router is currently using a private WAN IP address.
This router may be in a multiple-NAT environment, and accessing AiCloud from WAN does not work.

Enables USB-attached storage devices to be accessed, streamed or shared through an Internet-connected PC or device.

Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC.

Enables synchronization of USB-attached storage with cloud services like ASUS Webstorage and other AiCloud 2.0-enabled networks.

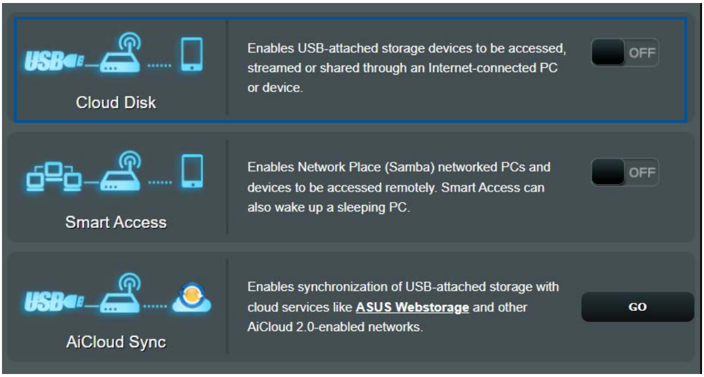
To use AiCloud:

1. From Google Play Store or Apple Store, download and install the ASUS AiCloud app to your smart device.
2. Connect your smart device to your network. Follow the instructions to complete the AiCloud setup process.

3.11.1 Cloud Disk

To create a cloud disk:

1. Insert a USB storage device into the wireless router.
2. Turn on **Cloud Disk**.

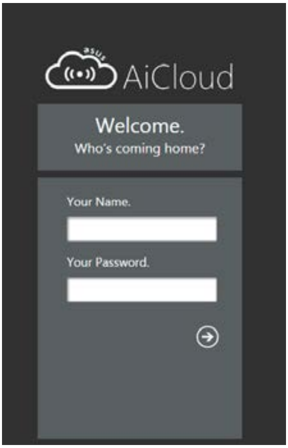


Cloud Disk — Enables USB-attached storage devices to be accessed, streamed or shared through an Internet-connected PC or device. OFF

Smart Access — Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC. OFF

AiCloud Sync — Enables synchronization of USB-attached storage with cloud services like **ASUS Webstorage** and other AiCloud 2.0-enabled networks. GO

3. Go to **https://router.asus.com** and enter the router login account and password. For better user experience, we recommend that you use **Google Chrome** or **Firefox**.



AiCloud

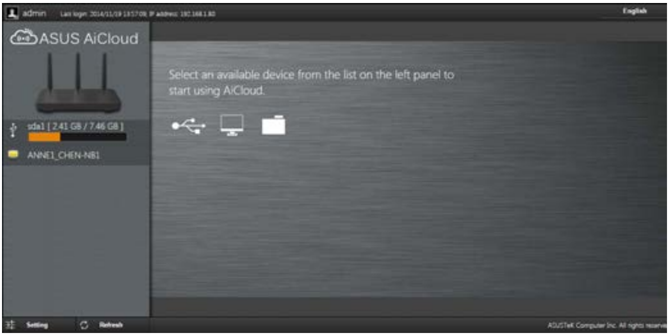
Welcome.
Who's coming home?

Your Name.

Your Password.

4. You can now start accessing Cloud Disk files on devices connected to the network.

NOTE: When accessing the devices that are connected to the network, you need to enter the device's user name and password manually, which will not be saved by AiCloud for security reason.

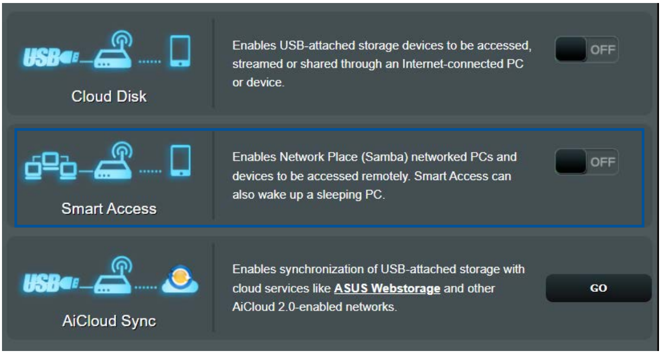


Select an available device from the list on the left panel to start using AiCloud.

admin
Last login: 2014/11/19 13:57:09, IP address: 192.168.1.80
English
ASUS AiCloud
sda1 [2.41 GB / 7.46 GB]
ANNE1_CHEN-NB1
Setting
Refresh
ASUSTeK Computer Inc. All rights reserve

3.11.2 Smart Access

The Smart Access function allows you to easily access your home network via your router's domain name.



Cloud Disk

Enables USB-attached storage devices to be accessed, streamed or shared through an Internet-connected PC or device.

Smart Access

Enables Network Place (Samba) networked PCs and devices to be accessed remotely. Smart Access can also wake up a sleeping PC.

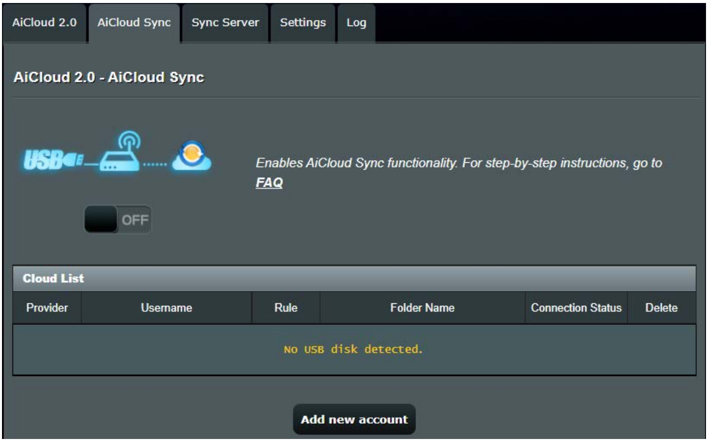
AiCloud Sync

Enables synchronization of USB-attached storage with cloud services like ASUS Webstorage and other AiCloud 2.0-enabled networks.

NOTES:

- You can create a domain name for your router with ASUS DDNS. For more details, refer to section **4.3.6 DDNS**.
- By default, AiCloud provides a secure HTTPS connection. Key in https://[yourASUSDDNSname].asuscomm.com for a very secure Cloud Disk and Smart Access usage.

3.11.3 AiCloud Sync



AiCloud 2.0 - AiCloud Sync

Enables AiCloud Sync functionality. For step-by-step instructions, go to ***FAQ***

Cloud List

Provider	Username	Rule	Folder Name	Connection Status	Delete
No USB disk detected.					

To use AiCloud Sync:

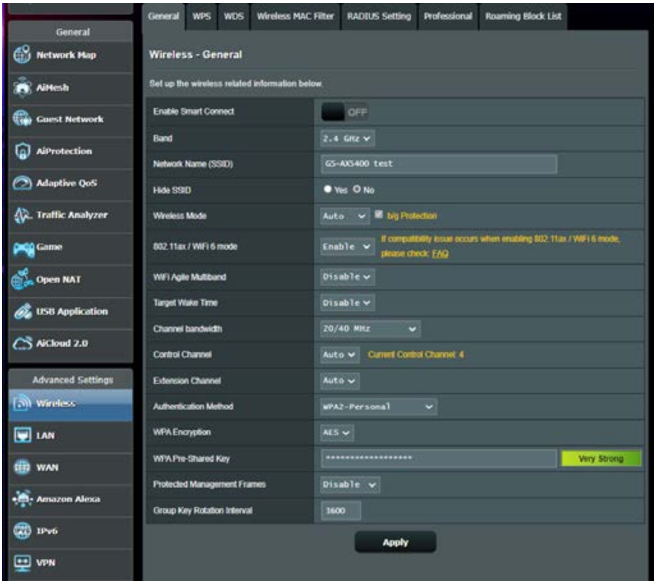
1. Launch AiCloud, click **AiCloud Sync** > **Go**.
2. Select **ON** to enable AiCloud Sync.
3. Click **Add new account**.
4. Enter your ASUS WebStorage account password and select the directory that you want to sync with WebStorage.
5. Click **Apply**.

4 Configuring the Advanced Settings

4.1 Wireless

4.1.1 General

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



Wireless - General

Set up the wireless related information below.

Enable Smart Connect	OFF
Band	2.4 GHz
Network Name (SSID)	GS-AX5400 test
Hide SSID	● Yes ○ No
Wireless Mode	Auto ☑ b/g Protection
802.11ax / WiFi 6 mode	Enable If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check: FAQ
WiFi Agile Multiband	Disable
Target Wake Time	Disable
Channel bandwidth	20/40 MHz
Control Channel	Auto Current Control Channel: 4
Extension Channel	Auto
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	****************** Very Strong
Protected Management Frames	Disable
Group Key Rotation Interval	3600

To configure the basic wireless settings:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **General** tab.
2. Select 2.4GHz or 5GHz as the frequency band for your wireless network.
3. If you want to use the Smart Connect function, move the slider to **ON** in the **Enable Smart Connect** field. This function automatically connect the clients in your network to the appropriate band 2.4GHz or 5GHz for optimal speed.

4. Assign a unique name containing up to 32 characters 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.

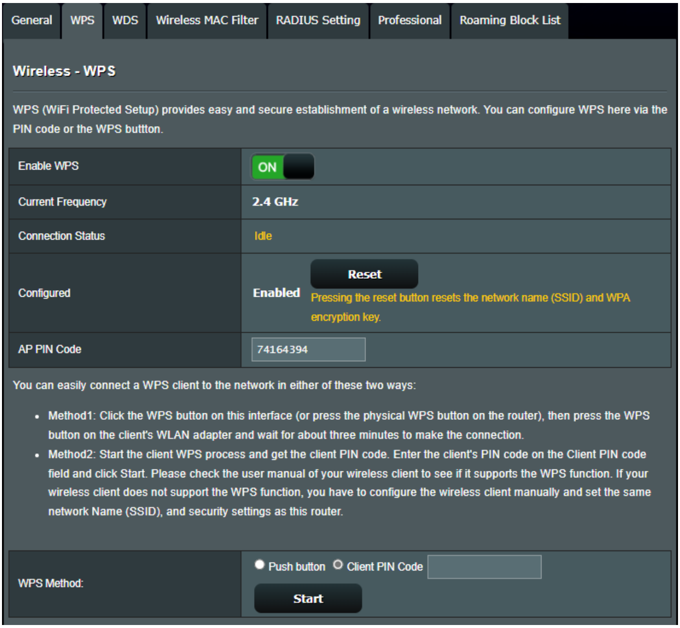
NOTE: You can assign unique SSIDs for the 2.4 GHz and 5GHz frequency bands.

5. 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.
6. Select any of these wireless mode options to determine the types of wireless devices that can connect to your wireless router:
   - **Auto**: Select Auto to allow 802.11ac, 802.11n, 802.11g, and 802.11b devices to connect to the wireless router.
   - **N only**: Select **N only** to maximize wireless N performance. This setting prevents 802.11g and 802.11b devices from connecting to the wireless router.
   - **Legacy**: Select **Legacy** to allow 802.11b/g/n devices to connect to the wireless router. Hardware that supports 802.11n natively, however, will only run at a maximum speed of 54Mbps.
7. Select the operating/control channel for your wireless router. Select **Auto** to allow the wireless router to automatically select the channel that has the least amount of interference.
8. Select the channel bandwidth to accommodate higher transmission speeds.
9. Select the authentication method.
10. When done, click **Apply**.

4.1.2 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.



Wireless - WPS

WPS (WiFi Protected Setup) provides easy and secure establishment of a wireless network. You can configure WPS here via the PIN code or the WPS buttton.

Enable WPS	ON
Current Frequency	2.4 GHz
Connection Status	Idle
Configured	Enabled Reset Pressing the reset button resets the network name (SSID) and WPA encryption key.
AP PIN Code	74164394

You can easily connect a WPS client to the network in either of these two ways:

- Method1: Click the WPS button on this interface (or press the physical WPS button on the router), then press the WPS button on the client's WLAN adapter and wait for about three minutes to make the connection.
- Method2: Start the client WPS process and get the client PIN code. Enter the client's PIN code on the Client PIN code field and click Start. Please check the user manual of your wireless client to see if it supports the WPS function. If your wireless client does not support the WPS function, you have to configure the wireless client manually and set the same network Name (SSID), and security settings as this router.

WPS Method:	● Push button ○ Client PIN Code Start

To enable WPS on your wireless network:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **WPS** tab.
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/WPA2/WPA3-Personal. WPS does not support a wireless network that uses a Shared Key, WPA-Enterprise, WPA2-Enterprise, and RADIUS encryption method.

4. In the WPS Method field, select **Push button** or **Client PIN Code**. If you select **Push Button**, go to step 5. If you select **Client PIN Code**, go to step 6.

5. To set up WPS using the router's WPS button, follow these steps:

   a. Click **Start** or press the WPS button found at the rear of the wireless router.

   b. Press the WPS button on your wireless device. This is normally identified by the WPS logo.

   NOTE: Check your wireless device or its user manual for the location of the WPS button.

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

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

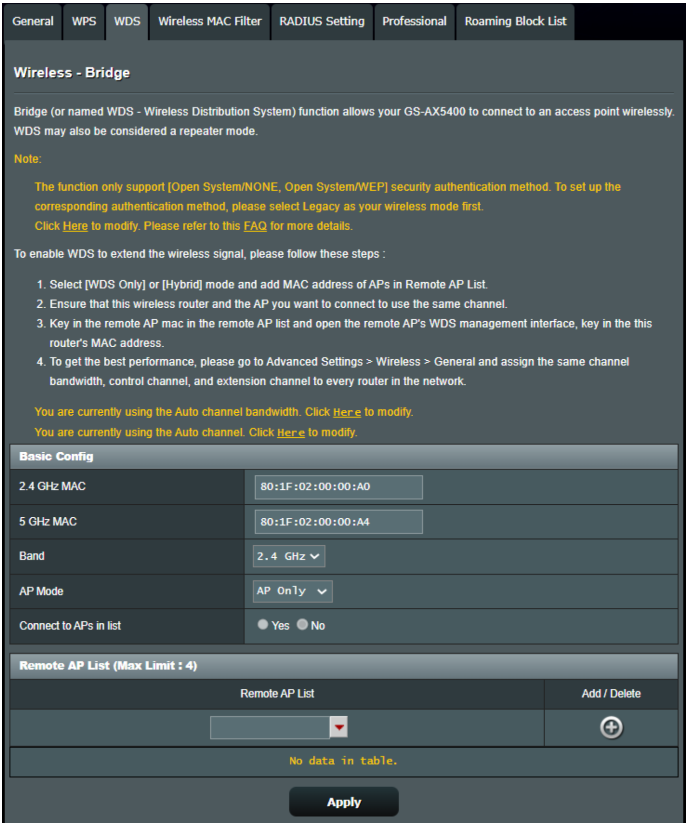
   a. Locate the WPS PIN code on your wireless device's user manual or on the device itself.

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

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

4.1.3 Bridge

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



Wireless - Bridge

Bridge (or named WDS - Wireless Distribution System) function allows your GS-AX5400 to connect to an access point wirelessly. WDS may also be considered a repeater mode.

Note:

The function only support [Open System/NONE, Open System/WEP] security authentication method. To set up the corresponding authentication method, please select Legacy as your wireless mode first.
Click Here to modify. Please refer to this FAQ for more details.

To enable WDS to extend the wireless signal, please follow these steps :

1. Select [WDS Only] or [Hybrid] mode and add MAC address of APs in Remote AP List.
2. Ensure that this wireless router and the AP you want to connect to use the same channel.
3. Key in the remote AP mac in the remote AP list and open the remote AP's WDS management interface, key in the this router's MAC address.
4. To get the best performance, please go to Advanced Settings > Wireless > General and assign the same channel bandwidth, control channel, and extension channel to every router in the network.

You are currently using the Auto channel bandwidth. Click Here to modify.
You are currently using the Auto channel. Click Here to modify.

Basic Config	
2.4 GHz MAC	80:1F:02:00:00:A0
5 GHz MAC	80:1F:02:00:00:A4
Band	2.4 GHz
AP Mode	AP Only
Connect to APs in list	○ Yes ○ No

Remote AP List (Max Limit : 4)

Remote AP List	Add / Delete
	⊕

No data in table.

To set up the wireless bridge:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **WDS** tab.

2. Select the frequency band for the wireless bridge.

3. In the **AP Mode** field, select any of these options:
   - **AP Only**: Disables the Wireless Bridge function.
   - **WDS Only**: Enables the Wireless Bridge feature but prevents other wireless devices/stations from connecting to the router.
   - **Hybrid**: Enables the Wireless Bridge feature and allows other wireless devices/stations to connect to the router.

   NOTE: In Hybrid mode, wireless devices connected to the ASUS wireless router will only receive half the connection speed of the Access Point.

4. In the **Connect to APs in list** field, click **Yes** if you want to connect to an Access Point listed in the Remote AP List.
5. By default, the operating/control channel for the wireless bridge is set to **Auto** to allow the router to automatically select the channel with the least amount of interference.

   You can modify the **Control Channel** from **Advanced Settings** > **Wireless** > **General** tab.

   NOTE: Channel availability varies per country or region.

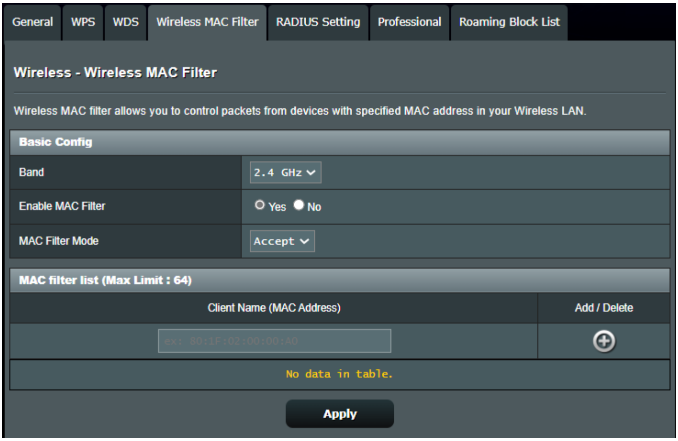
6. On the Remote AP List, key in a MAC address and click the **Add** button ⊕ to enter the MAC address of other available Access Points.

   NOTE: Any Access Point added to the list should be on the same Control Channel as the ASUS wireless router.

7. Click **Apply**.

4.1.4 Wireless MAC Filter

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



Wireless - Wireless MAC Filter

Wireless MAC filter allows you to control packets from devices with specified MAC address in your Wireless LAN.

Basic Config	
Band	2.4 GHz
Enable MAC Filter	○ Yes ● No
MAC Filter Mode	Accept

MAC filter list (Max Limit : 64)

Client Name (MAC Address)	Add / Delete
ex: 80:1F:02:00:00:A0	⊕

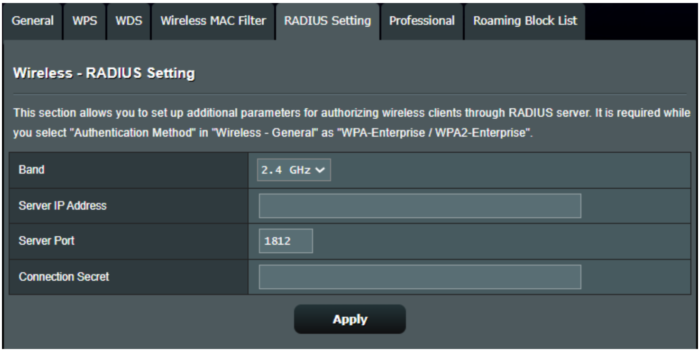
No data in table.

To set up the Wireless MAC filter:

1. From the navigation panel, go to **Advanced Settings** > **Wireless** > **Wireless MAC Filter** tab.
2. Select the frequency band.
3. Tick **Yes** in the **Enable Mac Filter** field.
4. 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.
5. On the MAC filter list, click the **Add** ⊕ button and key in the MAC address of the wireless device.
6. Click **Apply**.

4.1.5 RADIUS Setting

RADIUS (Remote Authentication Dial In User Service) Setting provides an extra layer of security when you choose WPA-Enterprise, WPA2-Enterprise, or Radius with 802.1x as your Authentication Mode.



Wireless - RADIUS Setting

This section allows you to set up additional parameters for authorizing wireless clients through RADIUS server. It is required while you select "Authentication Method" in "Wireless - General" as "WPA-Enterprise / WPA2-Enterprise".

Band	2.4 GHz
Server IP Address	
Server Port	1812
Connection Secret	

To set up wireless RADIUS settings:

1. Ensure that the wireless router's authentication mode is set to WPA-Enterprise or WPA2-Enterprise.

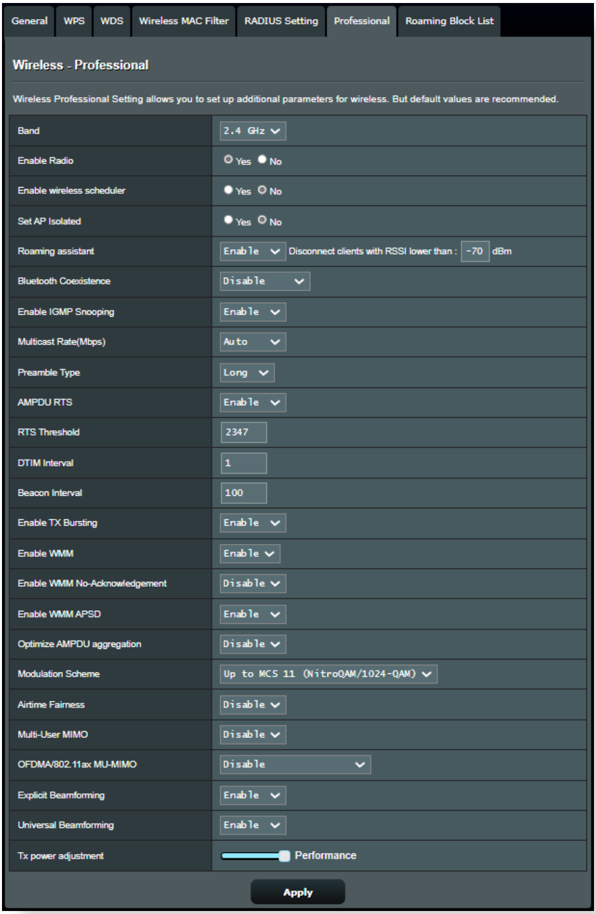
   NOTE: Please refer to section **4.1.1 General** for configuring your wireless router's Authentication Mode.

2. From the navigation panel, go to **Advanced 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 **Server Port** field, key in the server port.
6. In the **Connection Secret** field, assign the password to access your RADIUS server.
7. Click **Apply**.

4.1.6 Professional

The Professional screen provides advanced configuration options.

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



Wireless - Professional

Wireless Professional Setting allows you to set up additional parameters for wireless. But default values are recommended.

Band	2.4 GHz
Enable Radio	○ Yes ● No
Enable wireless scheduler	● Yes ○ No
Set AP Isolated	● Yes ○ No
Roaming assistant	Enable Disconnect clients with RSSI lower than : -70 dBm
Bluetooth Coexistence	Disable
Enable IGMP Snooping	Enable
Multicast Rate(Mbps)	Auto
Preamble Type	Long
AMPDU RTS	Enable
RTS Threshold	2347
DTIM Interval	1
Beacon Interval	100
Enable TX Bursting	Enable
Enable WMM	Enable
Enable WMM No-Acknowledgement	Disable
Enable WMM APSD	Enable
Optimize AMPDU aggregation	Disable
Modulation Scheme	Up to MCS 11 (NitroQAM/1024-QAM)
Airtime Fairness	Disable
Multi-User MIMO	Disable
OFDMA/802.11ax MU-MIMO	Disable
Explicit Beamforming	Enable
Universal Beamforming	Enable
Tx power adjustment	Performance

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**: Select **Yes** to enable and configure wireless scheduler. Select **No** to disable wireless scheduler.
  - **Date to Enable Radio (weekdays)**: You can specify which days of the week wireless networking is enabled.
  - **Time of Day to Enable Radio**: You can specify a time range when wireless networking is enabled during the week.
  - **Date to Enable Radio (weekend)**: You can specify which days of the weekend wireless networking is enabled.
  - **Time of Day to Enable Radio**: You can specify a time range when wireless networking is enabled during the weekend.
- **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 router 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 router 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.
- **Optimize AMPDU aggregation**: Optimize the max number of MPDUs in an AMPDU and avoid packets get lost or corrupted during transmission in error-prone wireless channels
- **Airtime Fairness**: With airtime fairness, the speed of the network is not determined by the slowest traffic. By allocating time equally among clients, Airtime Fairness allows every transmission to move at its highest potential speed.
- **Explicit Beamforming**: The client's WLAN adapter and router both support beam forming technology. This technology allows these device to communicate the channel estimation and steering direction to each other to improve download and uplink speed.

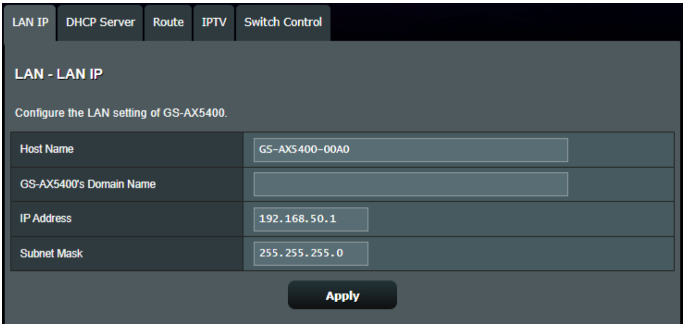
- **Universal Beamforming**: For legacy wireless network adapter that do not support beam forming, the router estimates the channel and determines the steering direction to improve the downlink speed.

4.2 LAN

4.2.1 LAN IP

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

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



LAN - LAN IP

Configure the LAN setting of GS-AX5400.

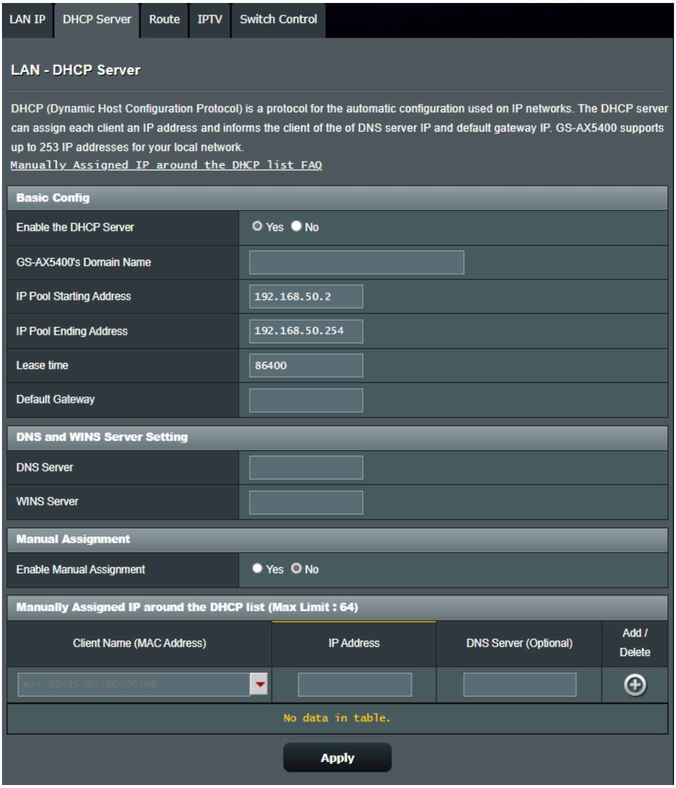
Host Name	GS-AX5400-00A0
GS-AX5400's Domain Name	
IP Address	192.168.50.1
Subnet Mask	255.255.255.0

To modify the LAN IP settings:

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

4.2.2 DHCP Server

Your wireless router uses DHCP to assign IP addresses automatically on your network. You can specify the IP address range and lease time for the clients on your network.



LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the of DNS server IP and default gateway IP. GS-AX5400 supports up to 253 IP addresses for your local network.

Manually Assigned IP around the DHCP list FAQ

Basic Config	
Enable the DHCP Server	○ Yes ● No
GS-AX5400's Domain Name	
IP Pool Starting Address	192.168.50.2
IP Pool Ending Address	192.168.50.254
Lease time	86400
Default Gateway	

DNS and WINS Server Setting	
DNS Server	
WINS Server	

Manual Assignment	
Enable Manual Assignment	● Yes ○ No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Add / Delete
ex: 80:1F:02:00:00:A0			⊕

No data in table.

To configure the DHCP server:

1. From the navigation panel, go to **Advanced Settings** > **LAN** > **DHCP Server** tab.

2. In the **Enable the DHCP Server** field, tick **Yes**.

3. In the **GS-AX5400's Domain Name** text box, enter a domain name for the wireless router.

4. In the **IP Pool Starting Address** field, key in the starting IP address.

5. In the **IP Pool Ending Address** field, key in the ending IP address.
6. In the **Lease time** field, specify in seconds when an assigned IP address will expire. Once it reaches this time limit, the DHCP server will then assign a new IP address.

NOTES:

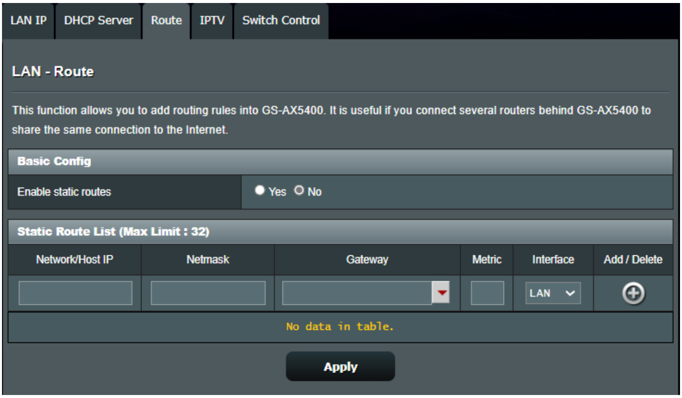
- We recommend that you use an IP address format of 192.168.1.xxx (where xxx can be any number between 2 and 254) when specifying an IP address range.
- An IP Pool Starting Address should not be greater than the IP Pool Ending Address.

7. In the **DNS and WINS Server Setting** section, key in your DNS Server and WINS Server IP address if needed.
8. Your wireless router can also manually assign IP addresses to devices on the network. On the **Enable Manual Assignment** field, choose **Yes** to assign an IP address to specific MAC addresses on the network. Up to 32 MAC Addresses can be added to the DHCP list for manual assignment.

4.2.3 Route

If your network makes use of more than one wireless router, you can configure a routing table to share the same Internet service.

NOTE: We recommend that you do not change the default route settings unless you have advanced knowledge of routing tables.



LAN - Route

This function allows you to add routing rules into GS-AX5400. It is useful if you connect several routers behind GS-AX5400 to share the same connection to the Internet.

Basic Config

Enable static routes ● Yes ○ No

Static Route List (Max Limit : 32)

Network/Host IP	Netmask	Gateway	Metric	Interface	Add / Delete
				LAN	⊕

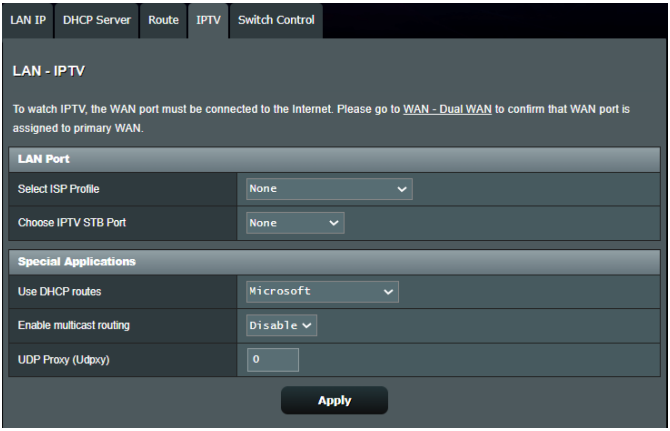
No data in table.

To configure the LAN Routing table:

1. From the navigation panel, go to **Advanced Settings** > **LAN** > **Route** tab.
2. On the **Enable static routes** field, choose **Yes**.
3. On the **Static Route List**, enter the network information of other access points or nodes. Click the **Add** ⊕ or **Delete** ⊖ button to add or remove a device on the list.
4. Click **Apply**.

4.2.4 IPTV

The wireless router supports connection to IPTV services through an ISP or a LAN. The IPTV tab provides the configuration settings needed to set up IPTV, VoIP, multicasting, and UDP for your service. Contact your ISP for specific information regarding your service.



LAN - IPTV

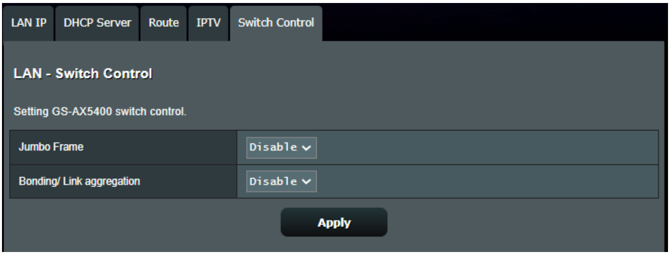
To watch IPTV, the WAN port must be connected to the Internet. Please go to WAN - Dual WAN to confirm that WAN port is assigned to primary WAN.

LAN Port	
Select ISP Profile	None
Choose IPTV STB Port	None

Special Applications	
Use DHCP routes	Microsoft
Enable multicast routing	Disable
UDP Proxy (Udpxy)	0

4.2.5 Switch Control

The Switch Control screen allows you to enable to disable Jumbo Frame or Bonding/Link aggregation.



LAN - Switch Control

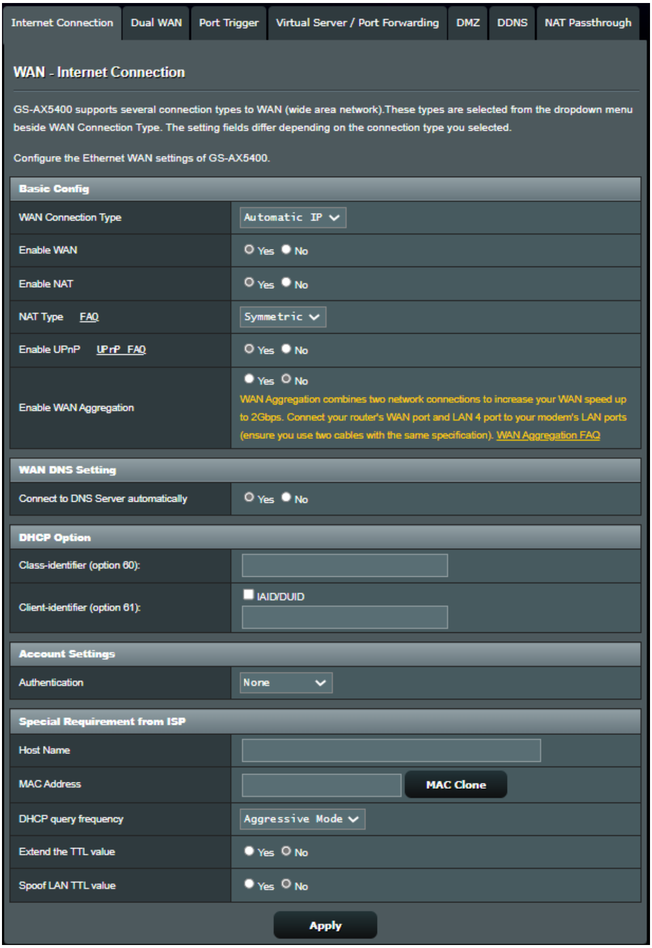
Setting GS-AX5400 switch control.

Jumbo Frame	Disable
Bonding/ Link aggregation	Disable

4.3 WAN

4.3.1 Internet Connection

The Internet Connection screen allows you to configure the settings of various WAN connection types.



WAN - Internet Connection

GS-AX5400 supports several connection types to WAN (wide area network).These types are selected from the dropdown menu beside WAN Connection Type. The setting fields differ depending on the connection type you selected.

Configure the Ethernet WAN settings of GS-AX5400.

Basic Config	
WAN Connection Type	Automatic IP
Enable WAN	○ Yes ● No
Enable NAT	○ Yes ● No
NAT Type FAQ	Symmetric
Enable UPnP UPnP FAQ	○ Yes ● No
Enable WAN Aggregation	● Yes ○ No WAN Aggregation combines two network connections to increase your WAN speed up to 2Gbps. Connect your router's WAN port and LAN 4 port to your modem's LAN ports (ensure you use two cables with the same specification). WAN Aggregation FAQ
WAN DNS Setting	
Connect to DNS Server automatically	○ Yes ● No
DHCP Option	
Class-identifier (option 60):	
Client-identifier (option 61):	□ IAID/DUID
Account Settings	
Authentication	None
Special Requirement from ISP	
Host Name	
MAC Address	MAC Clone
DHCP query frequency	Aggressive Mode
Extend the TTL value	● Yes ○ No
Spoof LAN TTL value	● Yes ○ No

To configure the WAN connection settings:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Internet Connection** tab.

2. Configure the following settings below. When done, click **Apply**.

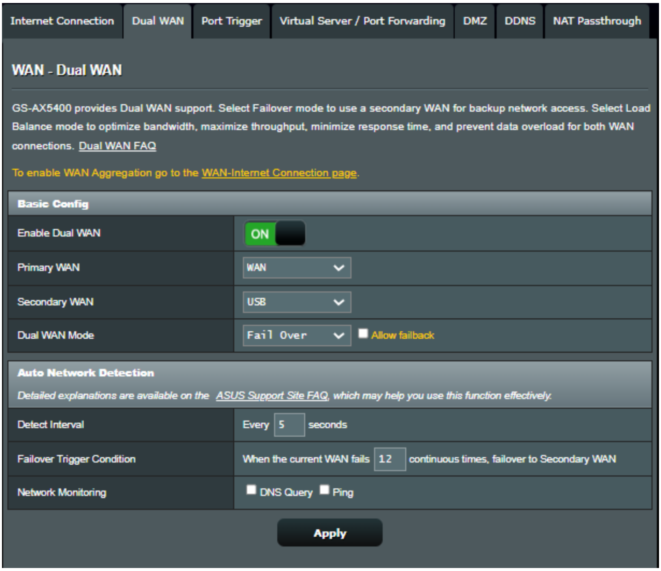
- **WAN Connection Type**: Choose your Internet Service Provider type. The choices are **Automatic IP**, **PPPoE**, **PPTP**, **L2TP** or **static IP**. Consult your ISP if the router is unable to obtain a valid IP address or if you are unsure the WAN connection type.
- **Enable WAN**: Select **Yes** to allow the router Internet access. Select **No** to disable Internet access.
- **Enable NAT**: NAT (Network Address Translation) is a system where one public IP (WAN IP) is used to provide Internet access to network clients with a private IP address in a LAN. The private IP address of each network client is saved in a NAT table and is used to route incoming data packets.
- **Enable UPnP**: UPnP (Universal Plug and Play) allows several devices (such as routers, televisions, stereo systems, game consoles, and cellular phone), to be controlled via an IP-based network with or without a central control through a gateway. UPnP connects PCs of all form factors, providing a seamless network for remote configuration and data transfer. Using UPnP, a new network device is discovered automatically. Once connected to the network, devices can be remotely configured to support P2P applications, interactive gaming, video conferencing, and web or proxy servers. Unlike Port forwarding, which involves manually configuring port settings, UPnP automatically configures the router to accept incoming connections and direct requests to a specific PC on the local network.
- **Connect to DNS Server automatically**: Allows this router to get the DNS IP address from the ISP automatically. A DNS is a host on the Internet that translates Internet names to numeric IP addresses.
- **Authentication**: This item may be specified by some ISPs. Check with your ISP and fill them in if required.

- **Host Name**: This field allows you to provide a host name for your router. It is usually a special requirement from your ISP. If your ISP assigned a host name to your computer, enter the host name here.
- **MAC Address**: MAC (Media Access Control) address is a unique identifier for your networking device. Some ISPs monitor the MAC address of networking devices that connect to their service and reject any unrecognized device that attempt to connect. To avoid connection issues due to an unregistered MAC address, you can:
  - Contact your ISP and update the MAC address associated with your ISP service.
  - Clone or change the MAC address of the ASUS wireless router to match the MAC address of the previous networking device recognized by the ISP.
- **DHCP query frequency**: Changes the DHCP Discovery interval settings to avoid overloading the DHCP server.

4.3.2 Dual WAN

Your ASUS wireless router provides dual WAN support. You can set the dual WAN feature to any of these two modes:

- **Fail Over Mode**: Select this mode to use the secondary WAN as the backup network access.
- **Load Balance Mode**: Select this mode to optimize bandwidth, minimize response time and prevent data overload for both primary and secondary WAN connections.



WAN - Dual WAN

GS-AX5400 provides Dual WAN support. Select Failover mode to use a secondary WAN for backup network access. Select Load Balance mode to optimize bandwidth, maximize throughput, minimize response time, and prevent data overload for both WAN connections. Dual WAN FAQ

To enable WAN Aggregation go to the WAN-Internet Connection page.

Basic Config	
Enable Dual WAN	ON
Primary WAN	WAN
Secondary WAN	USB
Dual WAN Mode	Fail Over □ Allow failback

Auto Network Detection

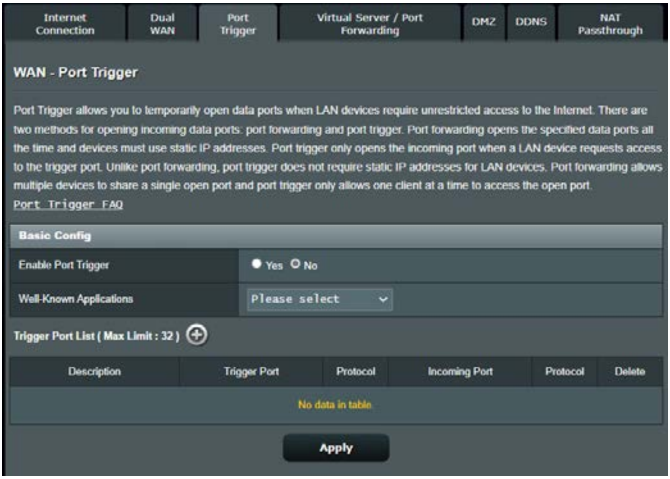
Detailed explanations are available on the ASUS Support Site FAQ, which may help you use this function effectively.

Detect Interval	Every 5 seconds
Failover Trigger Condition	When the current WAN fails 12 continuous times, failover to Secondary WAN
Network Monitoring	□ DNS Query □ Ping

4.3.3 Port Trigger

Port range triggering opens a predetermined incoming port for a limited period of time whenever a client on the local area network makes an outgoing connection to a specified port. Port triggering is used in the following scenarios:

- More than one local client needs port forwarding for the same application at a different time.
- An application requires specific incoming ports that are different from the outgoing ports.



WAN - Port Trigger

Port Trigger allows you to temporarily open data ports when LAN devices require unrestricted access to the Internet. There are two methods for opening incoming data ports: port forwarding and port trigger. Port forwarding opens the specified data ports all the time and devices must use static IP addresses. Port trigger only opens the incoming port when a LAN device requests access to the trigger port. Unlike port forwarding, port trigger does not require static IP addresses for LAN devices. Port forwarding allows multiple devices to share a single open port and port trigger only allows one client at a time to access the open port.

Port Trigger FAQ

Basic Config

Enable Port Trigger: ● Yes ○ No

Well-Known Applications: Please select

Trigger Port List (Max Limit : 32)

Description	Trigger Port	Protocol	Incoming Port	Protocol	Delete
No data in table					

To set up Port Trigger:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Port Trigger** tab.
2. On the **Enable Port Trigger** field, tick **Yes**.
3. On the **Well-Known Applications** field, select the popular games and web services to add to the Port Trigger List.
4. On the **Trigger Port List** table, key in the following information:
   - **Description**: Enter a short name or description for the service.

- **Trigger Port**: Specify a trigger port to open the incoming port.
- **Protocol**: Select the protocol, TCP, or UDP.
- **Incoming Port**: Specify an incoming port to receive inbound data from the Internet.
- **Protocol**: Select the protocol, TCP, or UDP.

5. Click the **Add** ⊕ to enter the port trigger information to the list. Click the **Delete** ⊖ button to remove a port trigger entry from the list.

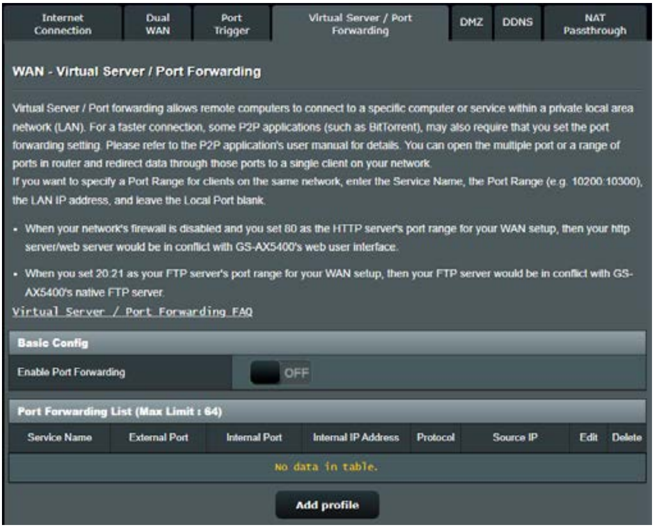
6. When done, click **Apply**.

NOTES:

- When connecting to an IRC server, a client PC makes an outgoing connection using the trigger port range 66660-7000. The IRC server responds by verifying the username and creating a new connection to the client PC using an incoming port.
- If Port Trigger is disabled, the router drops the connection because it is unable to determine which PC is requesting for IRC access. When Port Trigger is enabled, the router assigns an incoming port to receive the inbound data. This incoming port closes once a specific time period has elapsed because the router is unsure when the application has been terminated.
- Port triggering only allows one client in the network to use a particular service and a specific incoming port at the same time.
- You cannot use the same application to trigger a port in more than one PC at the same time. The router will only forward the port back to the last computer to send the router a request/ trigger.

4.3.4 Virtual Server/Port Forwarding

Port forwarding is a method to direct network traffic from the Internet to a specific port or a specific range of ports to a device or number of devices on your local network. Setting up Port Forwarding on your router allows PCs outside the network to access specific services provided by a PC in your network.



WAN - Virtual Server / Port Forwarding

Virtual Server / Port forwarding allows remote computers to connect to a specific computer or service within a private local area network (LAN). For a faster connection, some P2P applications (such as BitTorrent), may also require that you set the port forwarding setting. Please refer to the P2P application's user manual for details. You can open the multiple port or a range of ports in router and redirect data through those ports to a single client on your network.
If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port blank.

- When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with GS-AX5400's web user interface.
- When you set 20:21 as your FTP server's port range for your WAN setup, then your FTP server would be in conflict with GS-AX5400's native FTP server.

Virtual Server / Port Forwarding FAQ

Basic Config

Enable Port Forwarding: OFF

Port Forwarding List (Max Limit : 64)

Service Name	External Port	Internal Port	Internal IP Address	Protocol	Source IP	Edit	Delete
No data in table.							

To set up Port Forwarding:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **Virtual Server / Port Forwarding** tab.
2. On the **Enable Port Forwarding** field, move the slider to **ON**.
3. On the **Famous Server List** field, select the type of service you want to access.
4. On the **Famous Game List** field, select the popular game that you want to access. This item lists the port required for your selected popular online game to work properly.

5. On the **Port Forwarding List** table, key in the following information:
    - **Service Name**: Enter a service name.
    - **Port Range**: If you want to specify a Port Range for clients on the same network, enter the Service Name, the Port Range (e.g. 10200:10300), the LAN IP address, and leave the Local Port empty. Port range accepts various formats such as Port Range (300:350), individual ports (566,789) or Mix (1015:1024,3021).

    NOTES:

    - When your network's firewall is disabled and you set 80 as the HTTP server's port range for your WAN setup, then your http server/web server would be in conflict with the router's web user interface.
    - A network makes use of ports in order to exchange data, with each port assigned a port number and a specific task. For example, port 80 is used for HTTP. A specific port can only be used by one application or service at a time. Hence, two PCs attempting to access data through the same port at the same time would fail. For example, you cannot set up Port Forwarding for port 100 for two PCs at the same time.

    - **Local IP**: Key in the client's LAN IP address.

    NOTE: Use a static IP address for the local client to make port forwarding work properly. Refer to section **4.2 LAN** for information.

    - **Local Port**: Enter a specific port to receive forwarded packets. Leave this field blank if you want the incoming packets to be redirected to the specified port range.
    - **Protocol**: Select the protocol. If you are unsure, select **BOTH**.
6. Click the **Add** ⊕ to enter the port trigger information to the list. Click the **Delete** ⊖ button to remove a port trigger entry from the list.
7. When done, click Apply.

To check if Port Forwarding has been configured successfully:

- Ensure that your server or application is set up and running.
- You will need a client outside your LAN but has Internet access (referred to as "Internet client"). This client should not be connected to the ASUS router.
- On the Internet client, use the router's WAN IP to access the server. If port forwarding has been successful, you should be able to access the files or applications.

Differences between port trigger and port forwarding:

- Port triggering will work even without setting up a specific LAN IP address. Unlike port forwarding, which requires a static LAN IP address, port triggering allows dynamic port forwarding using the router. Predetermined port ranges are configured to accept incoming connections for a limited period of time. Port triggering allows multiple computers to run applications that would normally require manually forwarding the same ports to each PC on the network.
- Port triggering is more secure than port forwarding since the incoming ports are not open all the time. They are opened only when an application is making an outgoing connection through the trigger port.

4.3.5 DMZ

Virtual DMZ exposes one client to the Internet, allowing this client to receive all inbound packets directed to your Local Area Network.

Inbound traffic from the Internet is usually discarded and routed to a specific client only if port forwarding or a port trigger has been configured on the network. In a DMZ configuration, one network client receives all inbound packets.

Setting up DMZ on a network is useful when you need incoming ports open or you want to host a domain, web, or e-mail server.

> **CAUTION:** Opening all the ports on a client to the Internet makes the network vulnerable to outside attacks. Please be aware of the security risks involved in using DMZ.

To set up DMZ:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **DMZ** tab.
2. Configure the setting below. When done, click **Apply**.

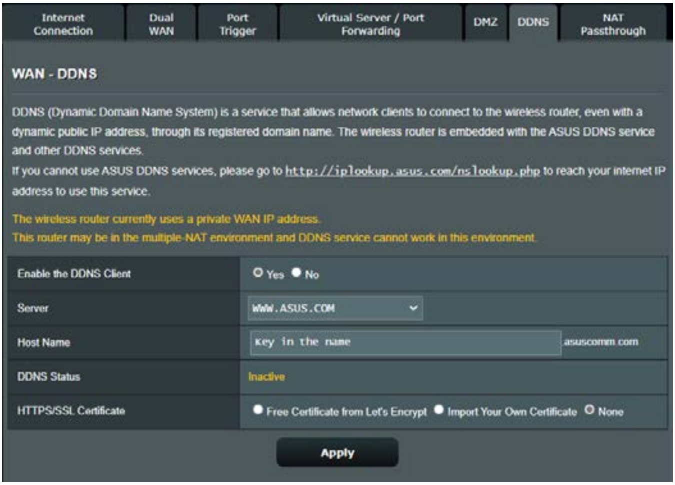
- **IP address of Exposed Station:** Key in the client's LAN IP address that will provide the DMZ service and be exposed on the Internet. Ensure that the server client has a static IP address.

To remove DMZ:

1. Delete the client's LAN IP address from the **IP Address of Exposed Station** text box.
2. When done, click **Apply**.

4.3.6 DDNS

Setting up DDNS (Dynamic DNS) allows you to access the router from outside your network through the provided ASUS DDNS Service or another DDNS service.



WAN - DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name. The wireless router is embedded with the ASUS DDNS service and other DDNS services.
If you cannot use ASUS DDNS services, please go to http://iplookup.asus.com/nslookup.php to reach your internet IP address to use this service.

The wireless router currently uses a private WAN IP address.
This router may be in the multiple-NAT environment and DDNS service cannot work in this environment.

Enable the DDNS Client	○ Yes ● No
Server	WWW.ASUS.COM
Host Name	Key in the name .asuscomm.com
DDNS Status	Inactive
HTTPS/SSL Certificate	● Free Certificate from Let's Encrypt ● Import Your Own Certificate ○ None

To set up DDNS:

1. From the navigation panel, go to **Advanced Settings** > **WAN** > **DDNS** tab.
2. Configure the following settings below. When done, click **Apply**.

- **Enable the DDNS Client**: Enable DDNS to access the ASUS router via the DNS name rather than WAN IP address.
- **Server** and **Host Name**: Choose ASUS DDNS or other DDNS. If you want to use ASUS DDNS, fill in the Host Name in the format of xxx.asuscomm.com (xxx is your host name).
- If you want to use a different DDNS service, click FREE TRIAL and register online first. Fill in the User Name or E-mail Address and Password or DDNS Key fields.
- **Enable wildcard**: Enable wildcard if your DDNS service requires one.

NOTES:

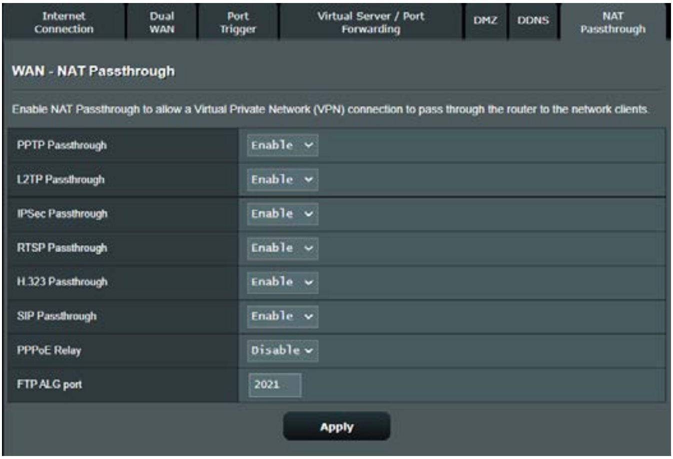
DDNS service will not work under these conditions:

- When the wireless router is using a private WAN IP address (192.168.x.x, 10.x.x.x, or 172.16.x.x), as indicated by a yellow text.
- The router may be on a network that uses multiple NAT tables.

4.3.7 NAT Passthrough

NAT Passthrough allows a Virtual Private Network (VPN) connection to pass through the router to the network clients. PPTP Passthrough, L2TP Passthrough, IPsec Passthrough and RTSP Passthrough are enabled by default.

To enable / disable the NAT Passthrough settings, go to the **Advanced Settings** > **WAN** > **NAT Passthrough** tab. When done, click **Apply**.



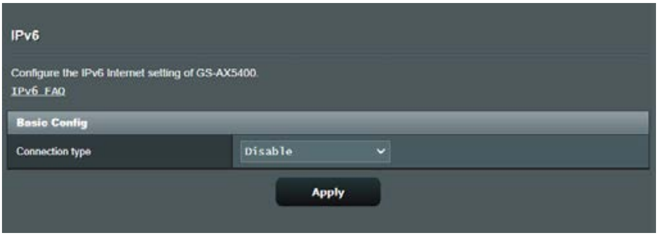
WAN - NAT Passthrough

Enable NAT Passthrough to allow a Virtual Private Network (VPN) connection to pass through the router to the network clients.

PPTP Passthrough	Enable
L2TP Passthrough	Enable
IPSec Passthrough	Enable
RTSP Passthrough	Enable
H.323 Passthrough	Enable
SIP Passthrough	Enable
PPPoE Relay	Disable
FTP ALG port	2021

4.4 IPv6

This wireless router supports IPv6 addressing, a system that supports more IP addresses. This standard is not yet widely available. Contact your ISP if your Internet service supports IPv6.



IPv6

Configure the IPv6 Internet setting of GS-AX5400.

IPv6 FAQ

Basic Config

Connection type: Disable

To set up IPv6:

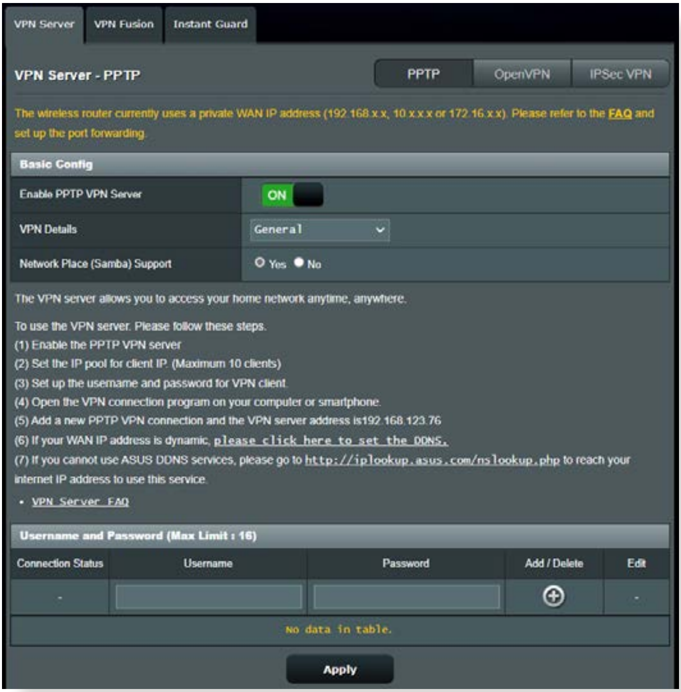
1. From the navigation panel, go to **Advanced Settings** > **IPv6**.
2. Select your **Connection type**. The configuration options vary depending on your selected connection type.
3. Enter your IPv6 LAN and DNS settings.
4. Click **Apply**.

NOTE: Please refer to your ISP regarding specific IPv6 information for your Internet service.

4.5 VPN

A virtual private network (VPN) provides a secure communication with a remote computer or network over a public network such as the Internet.

> **NOTE:** Before setting up a VPN connection, you would need the IP address or domain name of the VPN server.



VPN Server - PPTP

The wireless router currently uses a private WAN IP address (192.168.x.x, 10.x.x.x or 172.16.x.x). Please refer to the FAQ and set up the port forwarding.

Basic Config

Enable PPTP VPN Server	ON
VPN Details	General
Network Place (Samba) Support	○ Yes ● No

The VPN server allows you to access your home network anytime, anywhere.

To use the VPN server. Please follow these steps.
(1) Enable the PPTP VPN server
(2) Set the IP pool for client IP. (Maximum 10 clients)
(3) Set up the username and password for VPN client.
(4) Open the VPN connection program on your computer or smartphone.
(5) Add a new PPTP VPN connection and the VPN server address is192.168.123.76
(6) If your WAN IP address is dynamic, please click here to set the DDNS.
(7) If you cannot use ASUS DDNS services, please go to http://iplookup.asus.com/nslookup.php to reach your internet IP address to use this service.

- VPN Server FAQ

Username and Password (Max Limit : 16)

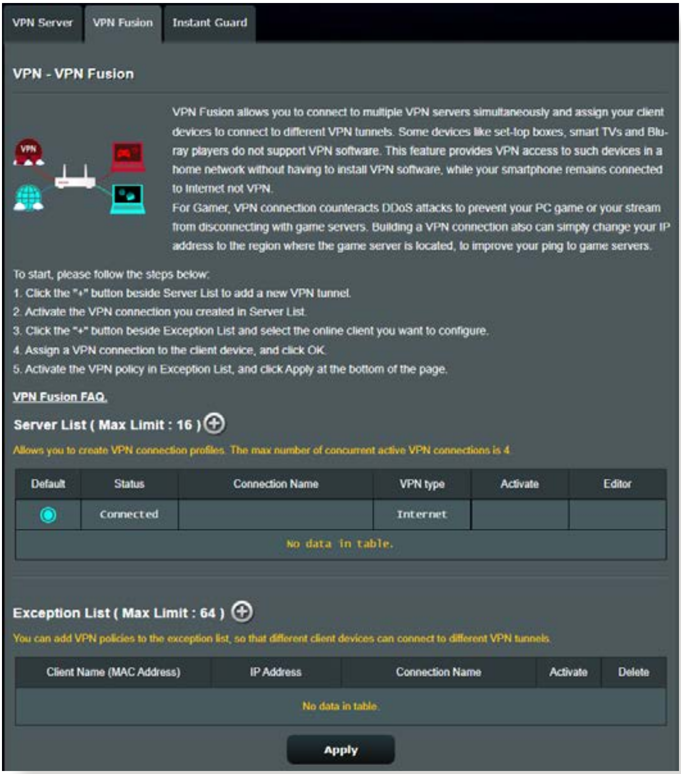
Connection Status	Username	Password	Add / Delete	Edit
-			⊕	-
No data in table.				

To set up access to a VPN server:

1. From the navigation panel, go to **Advanced Settings** > **VPN**.
2. On the **Enable PPTP VPN Server** field, select **ON**.
3. On the **VPN Details** dropdown list, select **Advanced Settings** to configure the advanced VPN settings such as broadcast support, authentication, MPPE Encryption, and Client IP address range.
4. On the **Network Place (Samba) Support** field, select **Yes**.
5. Enter the user name and password for accessing the VPN server. Click ⊕.
6. Click **Apply**.

4.5.1 VPN Fusion

VPN Fusion allows you to connect to multiple VPN servers simultaneously and assign your client devices to connect to different VPN tunnels. Some devices like set-top boxes, smart TVs and Blu-ray players do not support VPN software. This feature provides VPN access to such devices in a home network without having to install VPN software, while your smartphone remains connected to Internet not VPN. For Gamer, VPN connection counteracts DDoS attacks to prevent your PC game or your stream from disconnecting with game servers. Building a VPN connection also can simply change your IP address to the region where the game server is located, to improve your ping time to game servers.



VPN - VPN Fusion

VPN Fusion allows you to connect to multiple VPN servers simultaneously and assign your client devices to connect to different VPN tunnels. Some devices like set-top boxes, smart TVs and Blu-ray players do not support VPN software. This feature provides VPN access to such devices in a home network without having to install VPN software, while your smartphone remains connected to Internet not VPN.

For Gamer, VPN connection counteracts DDoS attacks to prevent your PC game or your stream from disconnecting with game servers. Building a VPN connection also can simply change your IP address to the region where the game server is located, to improve your ping to game servers.

To start, please follow the steps below:

1. Click the "+" button beside Server List to add a new VPN tunnel.
2. Activate the VPN connection you created in Server List.
3. Click the "+" button beside Exception List and select the online client you want to configure.
4. Assign a VPN connection to the client device, and click OK.
5. Activate the VPN policy in Exception List, and click Apply at the bottom of the page.

VPN Fusion FAQ

Server List (Max Limit : 16) ⊕

Allows you to create VPN connection profiles. The max number of concurrent active VPN connections is 4.

Default	Status	Connection Name	VPN type	Activate	Editor
●	Connected		Internet		
No data in table.					

Exception List (Max Limit : 64) ⊕

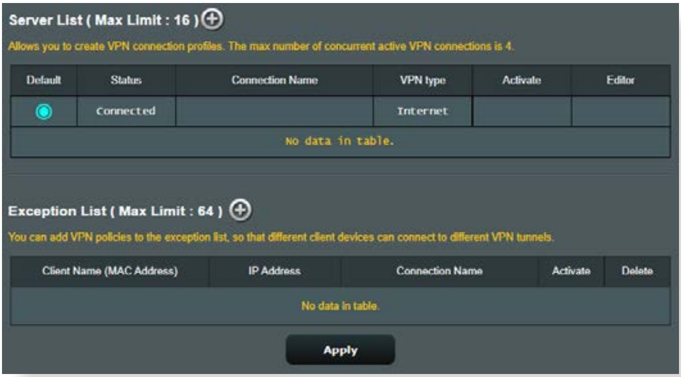
You can add VPN policies to the exception list, so that different client devices can connect to different VPN tunnels.

Client Name (MAC Address)	IP Address	Connection Name	Activate	Delete
No data in table.				

Apply

To start, please follow the steps below:

1. Click ⊕ beside **Server List** to add a new VPN tunnel.
2. Activate the VPN connection you created in Server List.
3. Click ⊕ beside **Exception List** and select the online client you want to configure.
4. Assign a VPN connection to the client device, and click **OK**.
5. Activate the VPN policy in **Exception List**, and click **Apply** at the bottom of the page.



Server List (Max Limit : 16) ⊕

Allows you to create VPN connection profiles. The max number of concurrent active VPN connections is 4.

Default	Status	Connection Name	VPN type	Activate	Editor
●	Connected		Internet		

No data in table.

Exception List (Max Limit : 64) ⊕

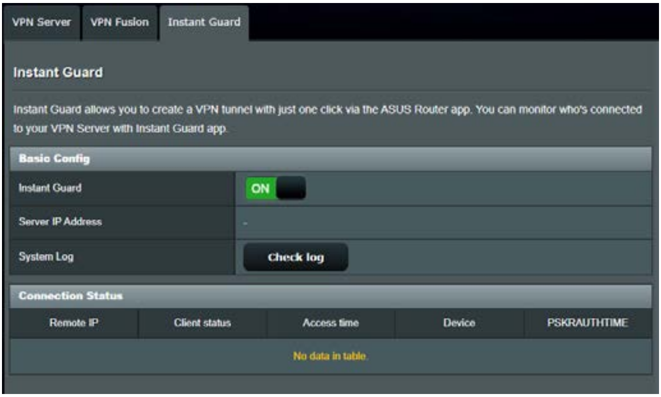
You can add VPN policies to the exception list, so that different client devices can connect to different VPN tunnels.

Client Name (MAC Address)	IP Address	Connection Name	Activate	Delete

No data in table.

4.5.2 Instant Guard

Instant Guard runs your own private VPN server on your own router. When you use a VPN tunnel, all your data passes through the server. With Instant Guard, you're in total control of your own server, making it the safest possible solution.



Instant Guard

Instant Guard allows you to create a VPN tunnel with just one click via the ASUS Router app. You can monitor who's connected to your VPN Server with Instant Guard app.

Basic Config

Instant Guard	ON
Server IP Address	-
System Log	Check log

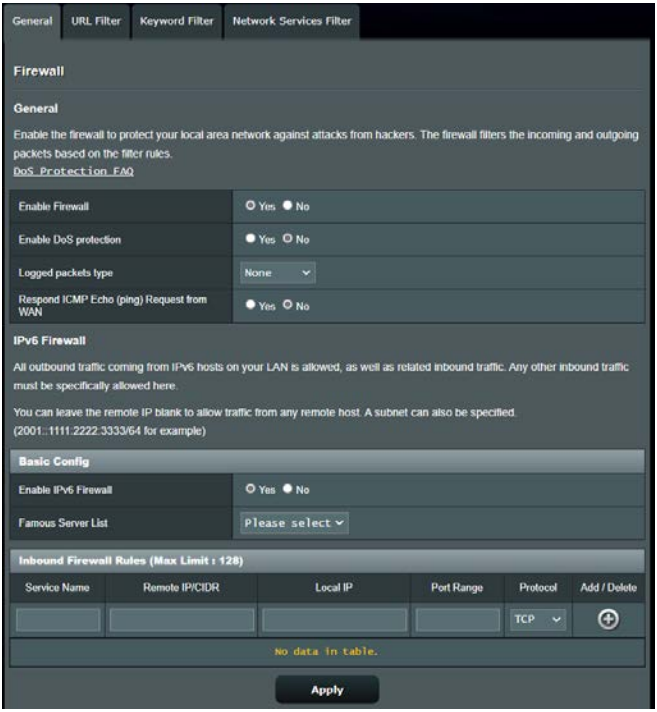
Connection Status

Remote IP	Client status	Access time	Device	PSKRAUTHTIME
No data in table.				

4.6 Firewall

The wireless router can serve as a hardware firewall for your network.

NOTE: The Firewall feature is enabled by default.



Firewall

General

Enable the firewall to protect your local area network against attacks from hackers. The firewall filters the incoming and outgoing packets based on the filter rules.

DoS Protection FAQ

Enable Firewall	○ Yes ● No
Enable DoS protection	● Yes ○ No
Logged packets type	None
Respond ICMP Echo (ping) Request from WAN	● Yes ○ No

IPv6 Firewall

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified. (2001::1111:2222:3333/64 for example)

Basic Config

Enable IPv6 Firewall	○ Yes ● No
Famous Server List	Please select

Inbound Firewall Rules (Max Limit : 128)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
				TCP	⊕

No data in table.

4.6.1 General

To set up basic Firewall settings:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **General** tab.
2. On the **Enable Firewall** field, select **Yes.**
3. On the **Enable DoS protection**, select **Yes** to protect your network from DoS (Denial of Service) attacks though this may affect your router's performance.

4. You can also monitor packets exchanged between the LAN and WAN connection. On the Logged packets type, select **Dropped**, **Accepted**, or **Both**.

5. Click **Apply**.

4.6.2 URL Filter

You can specify keywords or web addresses to prevent access to specific URLs.

> **NOTE:** The URL Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the URL Filter.

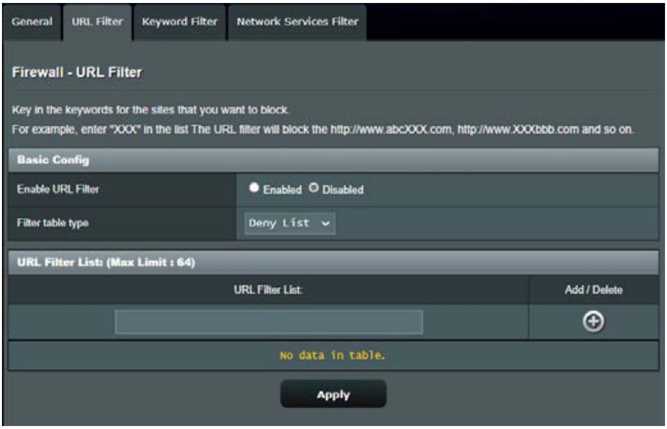
To set up a URL filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **URL Filter** tab.

2. On the **Enable URL Filter** field, select **Enabled**.

3. Enter a URL and click the ⊕ button.

4. Click **Apply**.



Firewall - URL Filter

Key in the keywords for the sites that you want to block.
For example, enter "XXX" in the list The URL filter will block the http://www.abcXXX.com, http://www.XXXbbb.com and so on.

Basic Config

Enable URL Filter	● Enabled ○ Disabled
Filter table type	Deny List

URL Filter List: (Max Limit : 64)

URL Filter List	Add / Delete
	⊕

No data in table.

4.6.3 Keyword filter

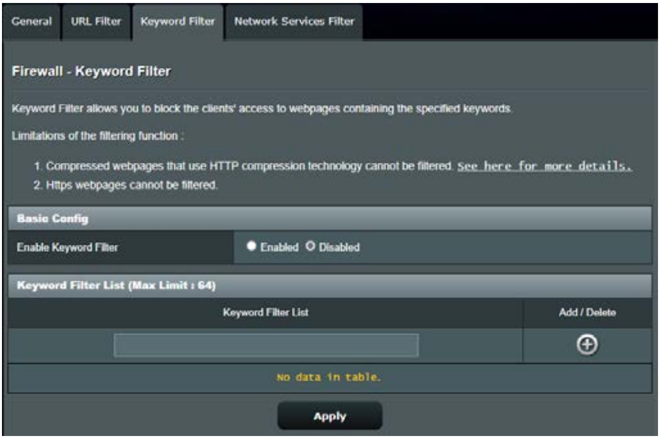
Keyword filter blocks access to webpages containing specified keywords.

To set up a keyword filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **Keyword Filter** tab.
2. On the **Enable Keyword Filter** field, select **Enabled**.
3. Enter a word or phrase and click the ⊕ button.
4. Click **Apply**.

NOTES:

- The Keyword Filter is based on a DNS query. If a network client has already accessed a website such as http://www.abcxxx.com, then the website will not be blocked (a DNS cache in the system stores previously visited websites). To resolve this issue, clear the DNS cache before setting up the Keyword Filter.
- Web pages compressed using HTTP compression cannot be filtered. HTTPS pages also cannot be blocked using a keyword filter.



Firewall - Keyword Filter

Keyword Filter allows you to block the clients' access to webpages containing the specified keywords.

Limitations of the filtering function :

1. Compressed webpages that use HTTP compression technology cannot be filtered. See here for more details.
2. Https webpages cannot be filtered.

Basic Config

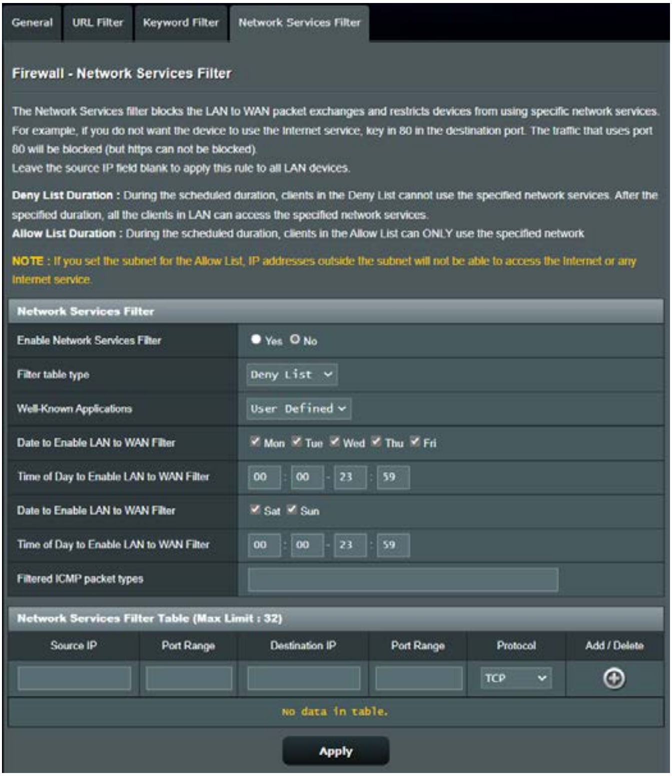
Enable Keyword Filter ● Enabled ○ Disabled

Keyword Filter List (Max Limit : 64)

Keyword Filter List	Add / Delete
	⊕
No data in table.	

4.6.4 Network Services Filter

The Network Services Filter blocks LAN to WAN packet exchanges and restricts network clients from accessing specific web services such as Telnet or FTP.



Firewall - Network Services Filter

The Network Services filter blocks the LAN to WAN packet exchanges and restricts devices from using specific network services. For example, if you do not want the device to use the Internet service, key in 80 in the destination port. The traffic that uses port 80 will be blocked (but https can not be blocked).
Leave the source IP field blank to apply this rule to all LAN devices.

Deny List Duration : During the scheduled duration, clients in the Deny List cannot use the specified network services. After the specified duration, all the clients in LAN can access the specified network services.
Allow List Duration : During the scheduled duration, clients in the Allow List can ONLY use the specified network

NOTE : If you set the subnet for the Allow List, IP addresses outside the subnet will not be able to access the Internet or any Internet service.

Network Services Filter

Enable Network Services Filter	● Yes ○ No
Filter table type	Deny List
Well-Known Applications	User Defined
Date to Enable LAN to WAN Filter	☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59
Date to Enable LAN to WAN Filter	☑ Sat ☑ Sun
Time of Day to Enable LAN to WAN Filter	00 : 00 - 23 : 59
Filtered ICMP packet types	

Network Services Filter Table (Max Limit : 32)

Source IP	Port Range	Destination IP	Port Range	Protocol	Add / Delete
				TCP	⊕

No data in table.

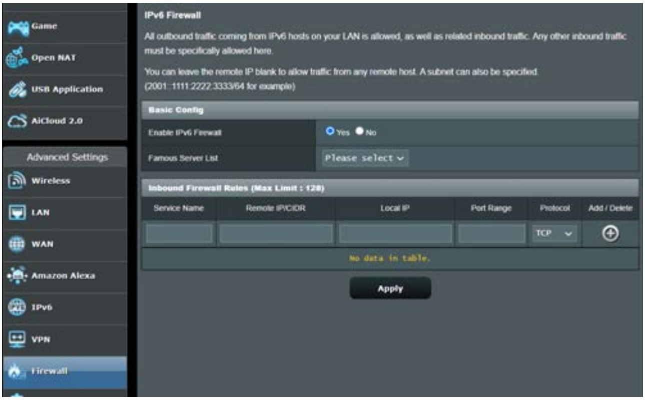
To set up a Network Service filter:

1. From the navigation panel, go to **Advanced Settings** > **Firewall** > **Network Service Filter** tab.
2. On the **Enable Network Services Filter** field, select **Yes**.
3. Select the Filter table type. **Black List** blocks the specified network services. **White List** limits access to only the specified network services.

4. Specify the day and time when the filters will be active.
5. To specify a Network Service to filter, enter the Source IP, Destination IP, Port Range, and Protocol. Click the ⊕ button.
6. Click **Apply**.

4.6.5 IPv6 Firewall

By default, your ASUS wireless router blocks all unsolicited incoming traffic. The IPv6 Firewall function allows incoming traffic coming from specified services to go through your network.



IPv6 Firewall

All outbound traffic coming from IPv6 hosts on your LAN is allowed, as well as related inbound traffic. Any other inbound traffic must be specifically allowed here.

You can leave the remote IP blank to allow traffic from any remote host. A subnet can also be specified (2001::1111:2222:3333/64 for example)

Basic Config

Enable IPv6 Firewall	● Yes ○ No
Famous Server List	Please select

Inbound Firewall Rules (Max Limit : 128)

Service Name	Remote IP/CIDR	Local IP	Port Range	Protocol	Add / Delete
				TCP	⊕

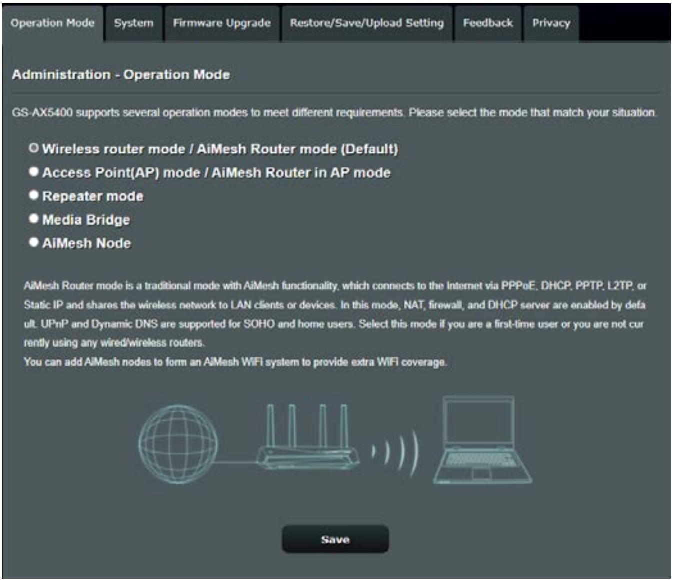
No data in table.

Apply

4.7 Administration

4.7.1 Operation Mode

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



Administration - Operation Mode

GS-AX5400 supports several operation modes to meet different requirements. Please select the mode that match your situation.

○ Wireless router mode / AiMesh Router mode (Default)
● Access Point(AP) mode / AiMesh Router in AP mode
● Repeater mode
● Media Bridge
● AiMesh Node

AiMesh Router mode is a traditional mode with AiMesh functionality, which connects to the Internet via PPPoE, DHCP, PPTP, L2TP, or Static IP and shares the wireless network to LAN clients or devices. In this mode, NAT, firewall, and DHCP server are enabled by default. UPnP and Dynamic DNS are supported for SOHO and home users. Select this mode if you are a first-time user or you are not currently using any wired/wireless routers.
You can add AiMesh nodes to form an AiMesh WiFi system to provide extra WiFi coverage.

To set up the operating mode:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Operation Mode** tab.

2. Select any of these operation modes:

   - **Wireless router mode / AiMesh Router mode (Default)**: In wireless router mode, the wireless router connects to the Internet and provides Internet access to available devices on its own local network.

   - **Access Point(AP) / AiMesh Router in AP mode**: In this mode, the router creates a new wireless network on an exising network.

- **Repeater mode**: In Repeater mode, GS-AX5400 wirelessly connects to an existing wireless network to extend the wireless coverage. In this mode, the firewall, IP sharing, and NAT functions are disabled.
- **Media Bridge**: This setup requires two wireless routers. The second router serves as a media bridge where multiple devices such as Smart TVs and gaming consoles can be connected via ethernet.
- **AiMesh node**: This setup requires at least two ASUS routers which support AiMesh. Enable AiMesh node, and log in AiMesh router web UI to search for available AiMesh nodes nearby to join your AiMesh system. AiMesh system provides whole-home coverage and centralized management.

3. Click **Apply**.

NOTE: The router will reboot when you change the modes.

4.7.2 System

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

To set up the System settings:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **System** tab.
2. You can configure the following settings:
   - **Change router login password**: You can change the password and login name for the wireless router by entering a new name and password.
   - **Time Zone**: Select the time zone for your network.
   - **NTP Server**: The wireless router can access a NTP (Network time Protocol) server in order to synchronize the time.
   - **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 router access.
- **Enable Web Access from WAN**: Select **Yes** to allow devices outside the network to access the wireless router GUI settings. Select **No** to prevent access.
- **Allow only specified IP address**: Click **Yes** if you want to specify the IP addresses of devices that are allowed access to the wireless router GUI settings from WAN.
- **Client List**: Enter the WAN IP addresses of networking devices allowed to access the wireless router settings. This list will be used if you clicked **Yes** in the **Only allow specific IP** item.

3. Click **Apply**.

4.7.3 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 **Advanced Settings** > **Administration** > **Firmware Upgrade** tab.
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 router 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 **5.2 Firmware Restoration**.

4.7.4 Restore/Save/Upload Setting

To restore/save/upload wireless router settings:

1. From the navigation panel, go to **Advanced Settings** > **Administration** > **Restore/Save/Upload Setting** tab.
2. Select the tasks that you want to do:
    - To restore to the default factory settings, click **Restore**, and click **OK** in the confirmation message.
    - To save the current system settings, click **Save**, navigate to the folder where you intend to save the file and click **Save**.
    - To restore from a saved system settings file, click **Browse** to locate your file, then click **Upload**.

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

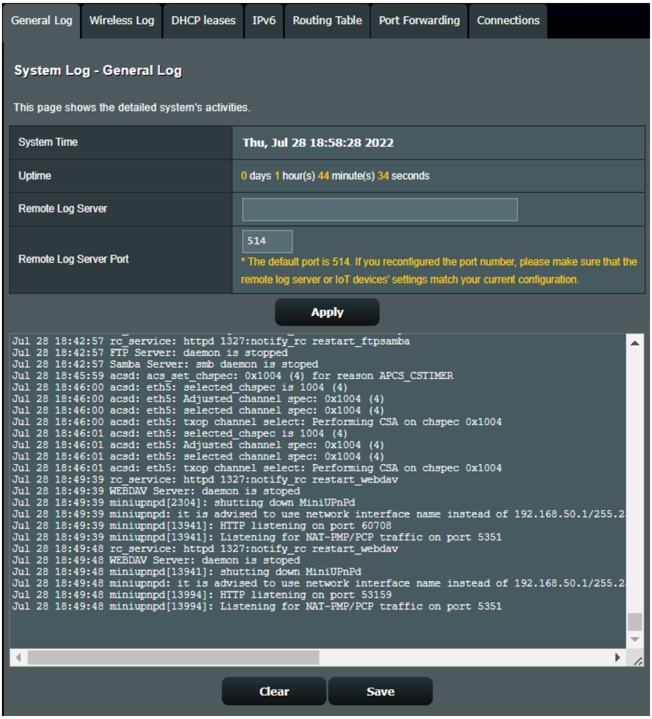
4.8 System Log

System Log contains your recorded network activities.

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

To view your system log:

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



System Log - General Log

This page shows the detailed system's activities.

System Time	Thu, Jul 28 18:58:28 2022
Uptime	0 days 1 hour(s) 44 minute(s) 34 seconds
Remote Log Server	
Remote Log Server Port	514 * The default port is 514. If you reconfigured the port number, please make sure that the remote log server or IoT devices' settings match your current configuration.

```
Jul 28 18:42:57 rc_service: httpd 1327:notify_rc restart_ftpsamba
Jul 28 18:42:57 FTP Server: daemon is stopped
Jul 28 18:42:57 Samba Server: smb daemon is stoped
Jul 28 18:45:59 acsd: acs_set_chspec: 0x1004 (4) for reason APCS_CSTIMER
Jul 28 18:46:00 acsd: eth5: selected_chspec is 1004 (4)
Jul 28 18:46:00 acsd: eth5: Adjusted channel spec: 0x1004 (4)
Jul 28 18:46:00 acsd: eth5: selected channel spec: 0x1004 (4)
Jul 28 18:46:00 acsd: eth5: txop channel select: Performing CSA on chspec 0x1004
Jul 28 18:46:01 acsd: eth5: selected_chspec is 1004 (4)
Jul 28 18:46:01 acsd: eth5: Adjusted channel spec: 0x1004 (4)
Jul 28 18:46:01 acsd: eth5: selected channel spec: 0x1004 (4)
Jul 28 18:46:01 acsd: eth5: txop channel select: Performing CSA on chspec 0x1004
Jul 28 18:49:39 rc_service: httpd 1327:notify_rc restart_webdav
Jul 28 18:49:39 WEBDAV Server: daemon is stoped
Jul 28 18:49:39 miniupnpd[2304]: shutting down MiniUPnPd
Jul 28 18:49:39 miniupnpd: it is advised to use network interface name instead of 192.168.50.1/255.2
Jul 28 18:49:39 miniupnpd[13941]: HTTP listening on port 60708
Jul 28 18:49:39 miniupnpd[13941]: Listening for NAT-PMP/PCP traffic on port 5351
Jul 28 18:49:48 rc_service: httpd 1327:notify_rc restart_webdav
Jul 28 18:49:48 WEBDAV Server: daemon is stoped
Jul 28 18:49:48 miniupnpd[13941]: shutting down MiniUPnPd
Jul 28 18:49:48 miniupnpd: it is advised to use network interface name instead of 192.168.50.1/255.2
Jul 28 18:49:48 miniupnpd[13994]: HTTP listening on port 53159
Jul 28 18:49:48 miniupnpd[13994]: Listening for NAT-PMP/PCP traffic on port 5351
```

4.9 Smart Connect

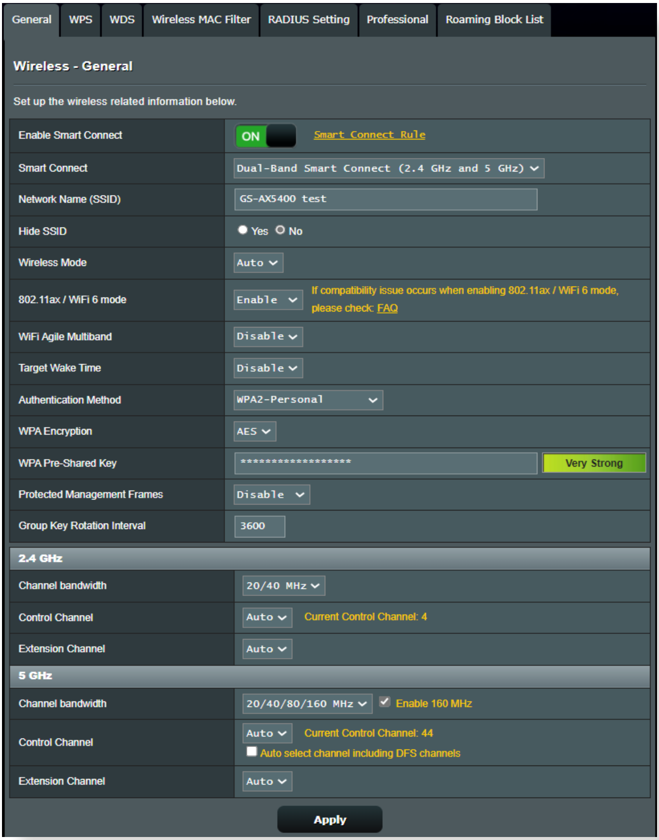
Smart Connect is designed to automatically steer clients to one of three radios (2.4 GHz and 5 GHz) to maximize total wireless throughput use.

4.9.1 Setting up Smart Connect

You can enable Smart Connect from the Web GUI through the following two ways:

- ***Via the Wireless screen***

1. On your web browser, manually key in the wireless router's default IP address: http://www.asusrouter.com.
2. On the login page, key in the default user name (**admin**) and password (**admin**) and click **OK**. The QIS page launches automatically.
3. From the navigation panel, go to **Advanced Settings** > **Wireless** > **General** tab.
4. Move the slider to **ON** in the **Enable Smart Connect** field. This function automatically connect the clients in your network to the appropriate band for optimal speed.



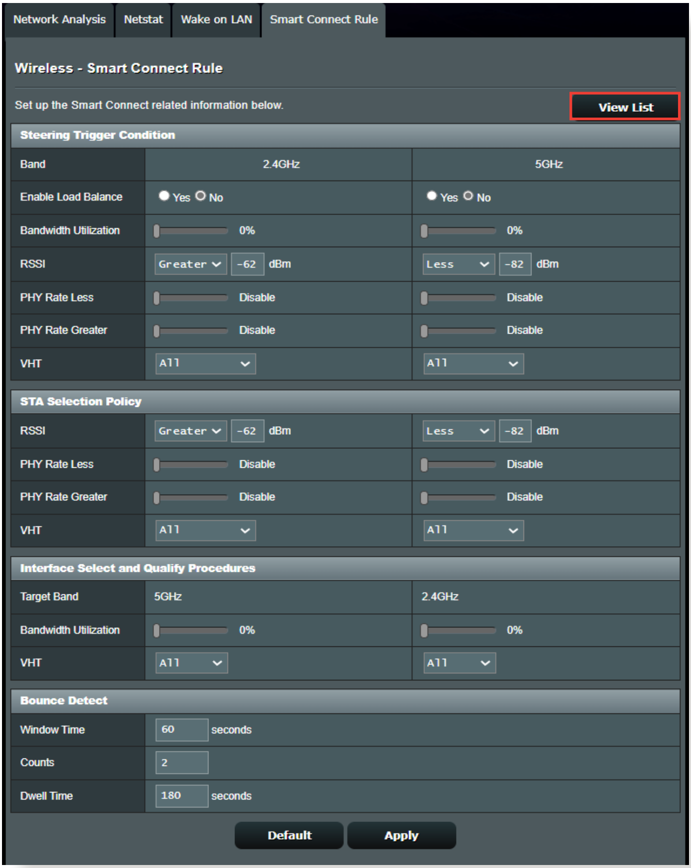
Wireless - General

Set up the wireless related information below.

Enable Smart Connect	ON Smart Connect Rule
Smart Connect	Dual-Band Smart Connect (2.4 GHz and 5 GHz)
Network Name (SSID)	GS-AX5400 test
Hide SSID	● Yes ○ No
Wireless Mode	Auto
802.11ax / WiFi 6 mode	Enable If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check: FAQ
WiFi Agile Multiband	Disable
Target Wake Time	Disable
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	****************** Very Strong
Protected Management Frames	Disable
Group Key Rotation Interval	3600
2.4 GHz	
Channel bandwidth	20/40 MHz
Control Channel	Auto Current Control Channel: 4
Extension Channel	Auto
5 GHz	
Channel bandwidth	20/40/80/160 MHz ☑ Enable 160 MHz
Control Channel	Auto Current Control Channel: 44 □ Auto select channel including DFS channels
Extension Channel	Auto

4.9.2 Smart Connect Rule

ASUSWRT provides default condition settings to trigger switching mechanism. You can also change the trigger conditions according to your networking surroundings. To change the settings, go to the **Smart Connect Rule** tab on the Network Tools screen.



Wireless - Smart Connect Rule

Set up the Smart Connect related information below.

Steering Trigger Condition		
Band	2.4GHz	5GHz
Enable Load Balance	● Yes ○ No	● Yes ○ No
Bandwidth Utilization	0%	0%
RSSI	Greater -62 dBm	Less -82 dBm
PHY Rate Less	Disable	Disable
PHY Rate Greater	Disable	Disable
VHT	All	All

STA Selection Policy		
RSSI	Greater -62 dBm	Less -82 dBm
PHY Rate Less	Disable	Disable
PHY Rate Greater	Disable	Disable
VHT	All	All

Interface Select and Qualify Procedures		
Target Band	5GHz	2.4GHz
Bandwidth Utilization	0%	0%
VHT	All	All

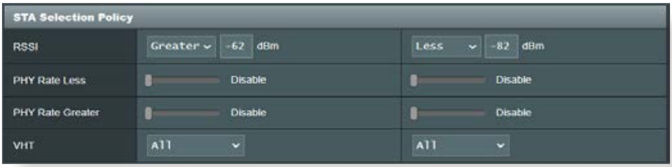
Bounce Detect	
Window Time	60 seconds
Counts	2
Dwell Time	180 seconds

Smart Connect Rule controls are divided into four sections:

- Steering Trigger Condition
- STA Selection Policy
- Interface Select and Qualify Procedures
- Bounce Detect

Steering Trigger Condition

This set of controls sets the criteria to initiate band steering.



STA Selection Policy

RSSI	Greater -62 dBm	Less -82 dBm
PHY Rate Less	Disable	Disable
PHY Rate Greater	Disable	Disable
VHT	All	All

- **Bandwidth Utilization**

  When bandwidth use exceeds this percentage, steering will be initiated.

- **Enable Load Balance**

  This controls load balancing.

- **RSSI**

  If the received signal level of any associated client meets this criteria, steering will be triggered.

- **PHY Rate Less / PHY Rate Greater**

  These controls determine STA link rates that trigger band steering.

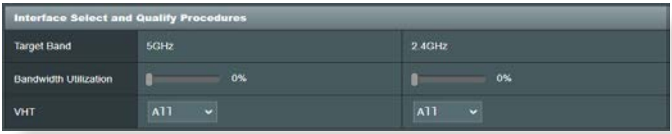
- **VHT**

  This controls determines how 802.11ac and non-ac clients are handled.

  - **ALL** (default) means any type of client can trigger steering.
  - **AC only** means a client must support 802.11ac to trigger steering.
  - **Not-allowed** means only non-802.11ac clients will trigger steering, i.e. 802.11a/b/g/n.

STA Selection Policy

Once steering has been triggered, ASUSWRT will follow the STA Selection Policy to select a client(STA) that is going to be steered to the most appropriate band.



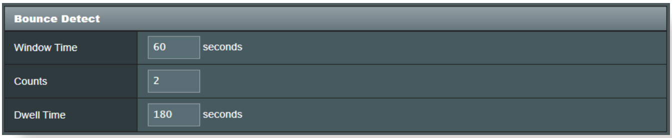
Interface Select and Qualify Procedures		
Target Band	5GHz	2.4GHz
Bandwidth Utilization	0%	0%
VHT	All	All

Interface Select and Qualify Procedures

These controls determine where the steered client will end up. The **Target Band** controls specify first and second choice of steering targets. Clients meeting the STA selection policy criteria for the radio will be steered to the first target if that radio's **Bandwidth Utilization** is less than the set value. Otherwise, the client will be sent to the second **Target Band** radio.

Bounce Detect

This set of controls determines how often a client can be steered. This is intended to prevent clients from constantly moving around. It does not, however, prevent clients from disconnecting on their own, or counting them as bounces if they do. Each client can be steered N **Counts** within the **Window Time**. When the Count limit is hit, the client will not be steered again for **Dwell Time**.



Bounce Detect	
Window Time	60 seconds
Counts	2
Dwell Time	180 seconds

5 Utilities

NOTES:

- Download and install the wireless router'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.

5.1 Device Discovery

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

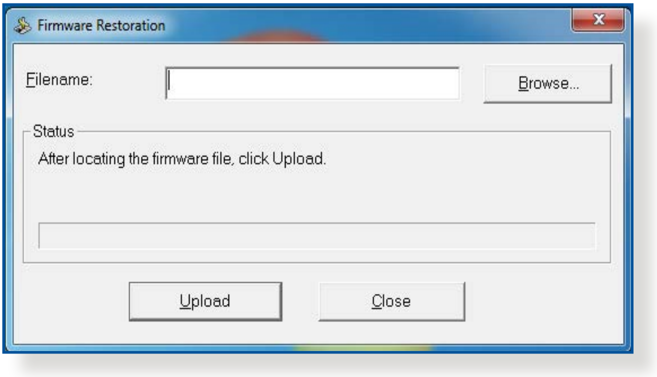
To launch the Device Discovery utility:

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

5.2 Firmware Restoration

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



After locating the firmware file, click Upload.

IMPORTANT! Launch the rescue mode on the router 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 router from the power source.
2. Hold the Reset button at the rear panel and simultaneously replug the wireless router into the power source. Release the Reset button when the Power LED at the front panel flashes slowly, which indicates that the wireless router 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 GS-AX5400 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 Router. Normal firmware upgrades must be done through the web interface. Refer to **Chapter 4: Configuring the Advanced Settings** for more details.

5.3 Setting up your printer server

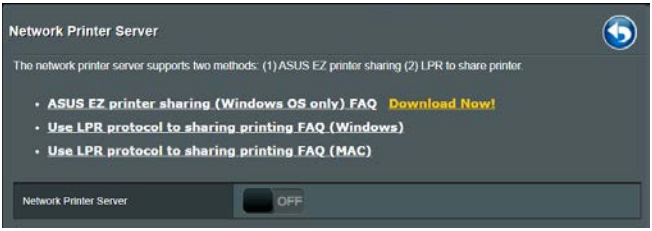
5.3.1 ASUS EZ Printer Sharing

ASUS EZ Printing Sharing utility allows you to connect a USB printer to your wireless router's USB port and set up the print server. This allows your network clients to print and scan files wirelessly.

NOTE: The print server function is supported on Windows® 7/8/8.1/10.

To set up the EZ Printer sharing mode:

1. From the navigation panel, go to **Advanced Settings** > **USB Application** > **Network Printer Server**.
2. Click **Download Now!** to download the network printer utility.



Network Printer Server

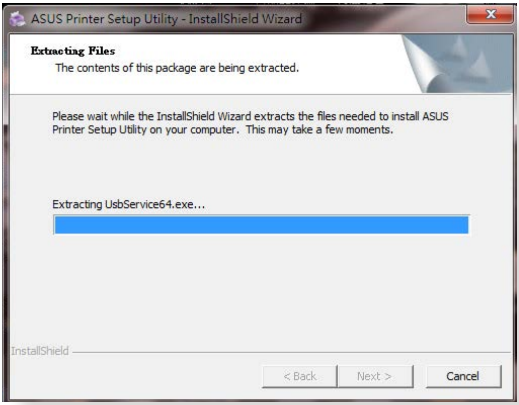
The network printer server supports two methods: (1) ASUS EZ printer sharing (2) LPR to share printer.

- ASUS EZ printer sharing (Windows OS only) FAQ Download Now!
- Use LPR protocol to sharing printing FAQ (Windows)
- Use LPR protocol to sharing printing FAQ (MAC)

Network Printer Server OFF

NOTE: Network printer utility is supported on Windows® 7/8/8.1/10. To install the utility on Mac OS, select **Use LPR protocol for sharing printer**.

3. Unzip the downloaded file and click the Printer icon to run the network printer setup program.



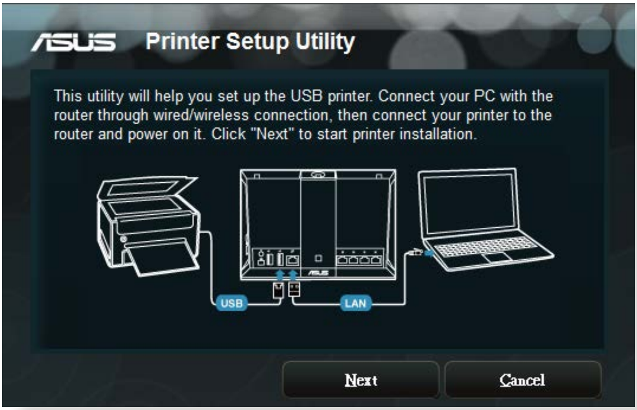
Extracting Files

The contents of this package are being extracted.

Please wait while the InstallShield Wizard extracts the files needed to install ASUS Printer Setup Utility on your computer. This may take a few moments.

Extracting UsbService64.exe...

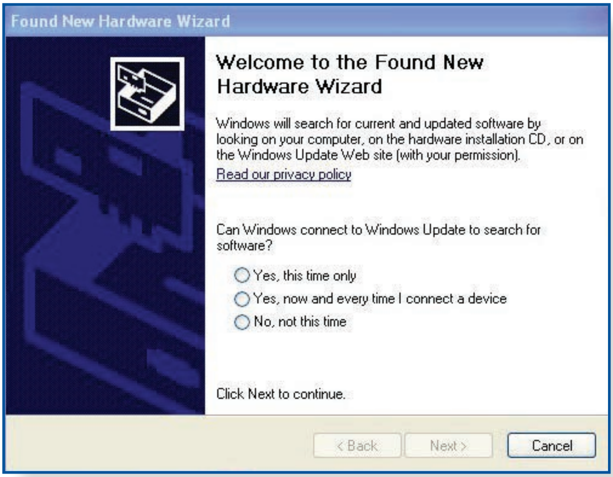
4. Follow the onscreen instructions to set up your hardware, then click **Next**.



This utility will help you set up the USB printer. Connect your PC with the router through wired/wireless connection, then connect your printer to the router and power on it. Click "Next" to start printer installation.

5. Wait a few minutes for the initial setup to finish. Click **Next**.
6. Click **Finish** to complete the installation.

7. Follow the Windows® OS instructions to install the printer driver.


Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

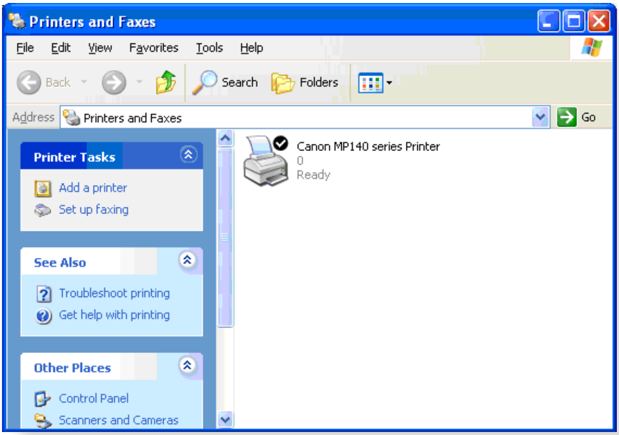
Read our privacy policy

Can Windows connect to Windows Update to search for software?

○ Yes, this time only
○ Yes, now and every time I connect a device
○ No, not this time

Click Next to continue.

8. After the printer's driver installation is complete, network clients can now use the printer.


Printers and Faxes

Address: Printers and Faxes

Canon MP140 series Printer
0
Ready

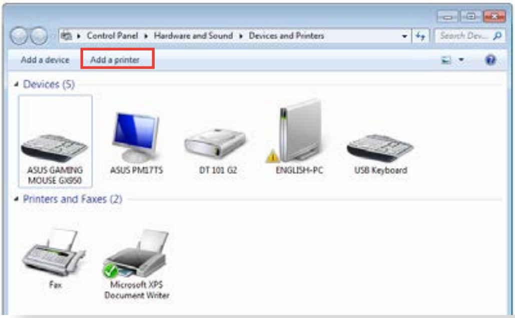
5.3.2 Using LPR to Share Printer

You can share your printer with computers running on Windows® and MAC operating system using LPR/LPD (Line Printer Remote/ Line Printer Daemon).

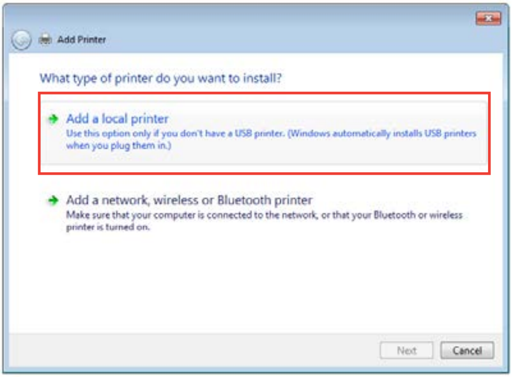
Sharing your LPR printer

To share your LPR printer:

1. From the Windows® desktop, click **Start** > **Devices and Printers** > **Add a printer** to run the **Add Printer Wizard**.



2. Select **Add a local printer** and then click **Next**.

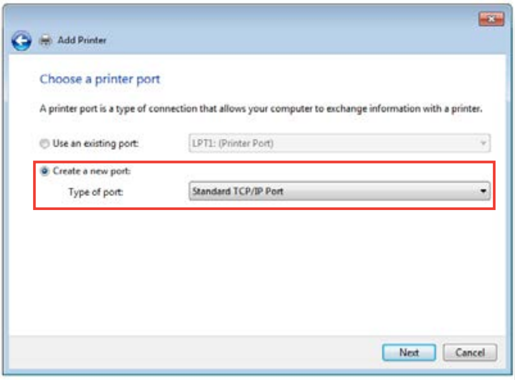


What type of printer do you want to install?

→ Add a local printer
Use this option only if you don't have a USB printer. (Windows automatically installs USB printers when you plug them in.)

→ Add a network, wireless or Bluetooth printer
Make sure that your computer is connected to the network, or that your Bluetooth or wireless printer is turned on.

3. Select **Create a new port** then set **Type of Port** to **Standard TCP/IP Port**. Click **Next**.



Choose a printer port

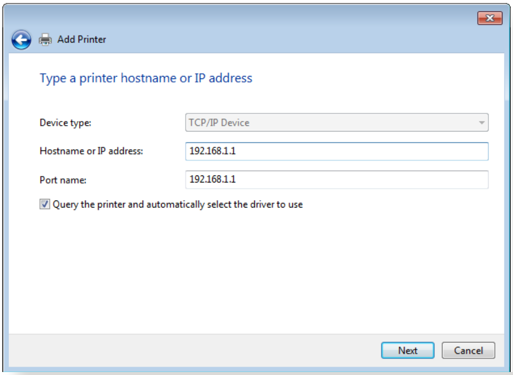
A printer port is a type of connection that allows your computer to exchange information with a printer.

○ Use an existing port: LPT1: (Printer Port)

● Create a new port:

Type of port: Standard TCP/IP Port

4. In the **Hostname or IP address** field, key in the IP address of the wireless router then click **Next**.



Type a printer hostname or IP address

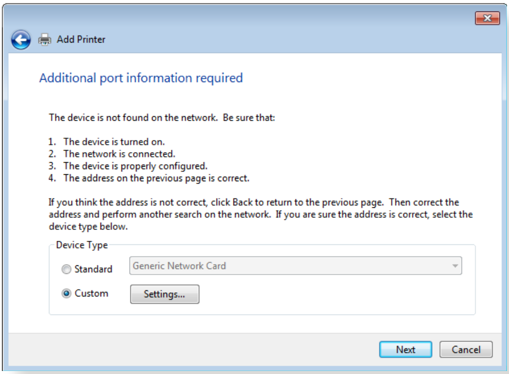
Device type: TCP/IP Device

Hostname or IP address: 192.168.1.1

Port name: 192.168.1.1

☑ Query the printer and automatically select the driver to use

5. Select **Custom** then click **Settings**.



Add Printer

Additional port information required

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

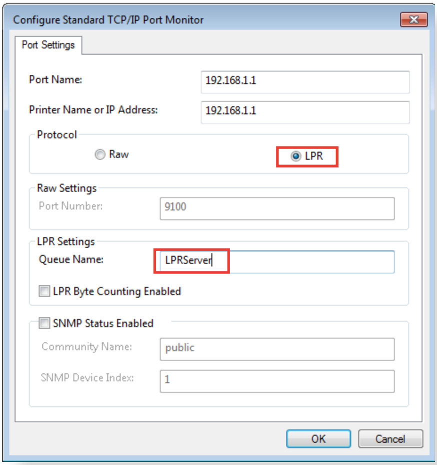
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

○ Standard Generic Network Card

● Custom Settings...

6. Set **Protocol** to **LPR**. In the **Queue Name** field, key in **LPRServer** then click **OK** to continue.



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: 192.168.1.1

Printer Name or IP Address: 192.168.1.1

Protocol

○ Raw ● LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: LPRServer

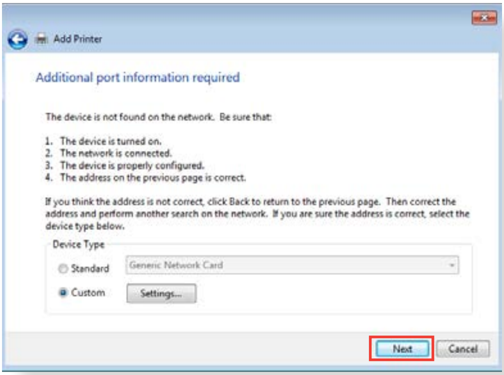
□ LPR Byte Counting Enabled

□ SNMP Status Enabled

Community Name: public

SNMP Device Index: 1

7. Click **Next** to finish setting up the standard TCP/IP port.



Additional port information required

The device is not found on the network. Be sure that:

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is correct.

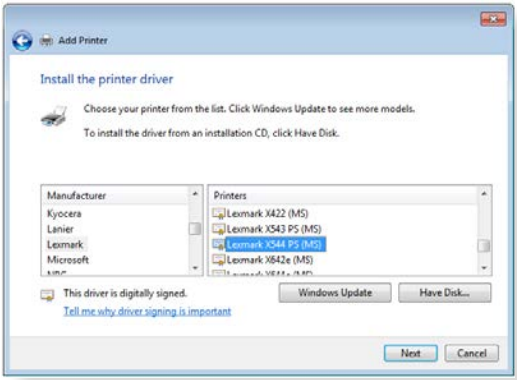
If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.

Device Type

○ Standard Generic Network Card

● Custom

8. Install the printer driver from the vendor-model list. If your printer is not in the list, click **Have Disk** to manually install the printer drivers from a CD-ROM or file.



Install the printer driver

Choose your printer from the list. Click Windows Update to see more models.

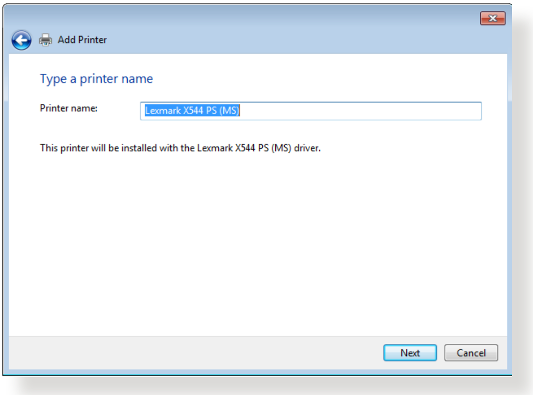
To install the driver from an installation CD, click Have Disk.

Manufacturer	Printers
Kyocera	Lexmark X422 (MS)
Lanier	Lexmark X543 PS (MS)
Lexmark	Lexmark X544 PS (MS)
Microsoft	Lexmark X642e (MS)

This driver is digitally signed.

Tell me why driver signing is important

9. Click **Next** to accept the default name for the printer.



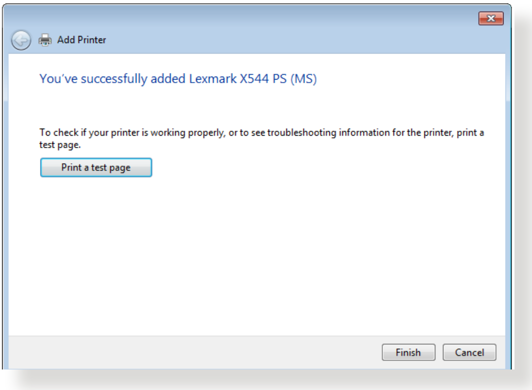
Add Printer

Type a printer name

Printer name: Lexmark X544 PS (MS)

This printer will be installed with the Lexmark X544 PS (MS) driver.

10. Click **Finish** to complete the installation.



Add Printer

You've successfully added Lexmark X544 PS (MS)

To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page.

5.4 Download Master

Download Master is a utility that helps you download files even while your laptops or other devices are switched off.

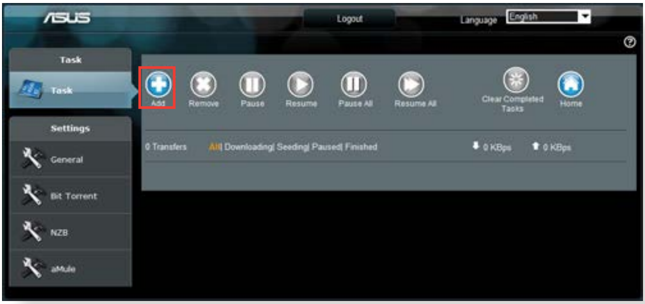
> **NOTE:** You need a USB device connected to the wireless router to use Download Master.

To use Download Master:

1. Click **General** > **USB Application** > **Download Master** to download and install the utility automatically.

> **NOTE:** If you have more than one USB drive, select the USB device you want to download the files to.

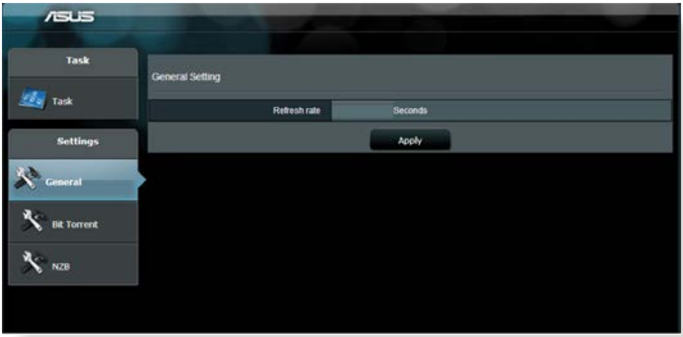
2. After the download process is finished, click the Download Master icon to start using the utility.
3. Click **Add** to add a download task.



4. Select a download type such as BitTorrent, HTTP, or FTP. Provide a torrent file or a URL to begin downloading.

> **NOTE:** For details on Bit Torrent, refer to section **5.4.1 Configuring the Bit Torrent download settings**.

5. Use the navigation panel to configure the advanced settings.

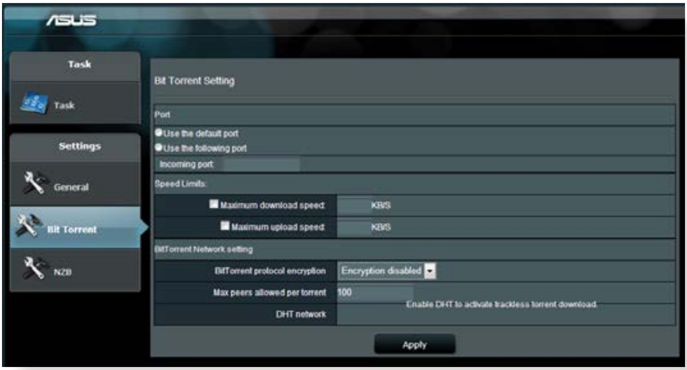


General Setting

Refresh rate Seconds

Apply

5.4.1 Configuring Bit Torrent download settings



Bit Torrent Setting

Port

● Use the default port

● Use the following port

Incoming port

Speed Limits:

□ Maximum download speed KB/S

□ Maximum upload speed KB/S

BitTorrent Network setting

BitTorrent protocol encryption: Encryption disabled

Max peers allowed per torrent: 100

DHT network: Enable DHT to activate trackless torrent download.

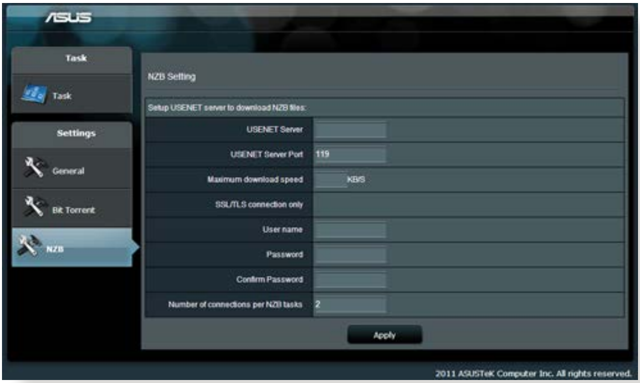
Apply

To configure BitTorrent download settings:

1. From Download Master's navigation panel, click **Bit Torrent** to launch the **Bit Torrent Setting** page.
2. Select a specific port for your download task.
3. To prevent network congestion, you can limit the maximum upload and download speeds under **Speed Limits**.
4. You can limit the maximum number of allowed peers and enable or disable file encryption during downloads.

5.4.2 NZB settings

You can set up a USENET server to download NZB files. After entering USENET settings, **Apply**.



NZB Setting

Setup USENET server to download NZB files:

USENET Server	
USENET Server Port	119
Maximum download speed	KB/S
SSL/TLS connection only	
User name	
Password	
Confirm Password	
Number of connections per NZB tasks	2

2011 ASUSTeK Computer Inc. All rights reserved.

6 Troubleshooting

This chapter provides solutions for issues you may encounter with your router. 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.

6.1 Basic Troubleshooting

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

Upgrade Firmware to the latest version.

1. Launch the Web GUI. Go to **Advanced Settings** > **Administration** > **Firmware Upgrade** tab. Click **Check** to verify if the latest firmware is available.
2. If the latest firmware is available, visit the ASUS global website at https://rog.asus.com/networking/rog-strix-gs-ax5400-model/helpdesk_download to download the latest firmware.
3. From the **Firmware Upgrade** page, click **Browse** to locate 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 router and computers.
4. Plug in the modem.
5. Turn on the modem and then wait for 2 minutes.
6. Turn on the router and then wait for 2 minutes.
7. Turn on computers.

Check if your Ethernet cables are plugged properly.

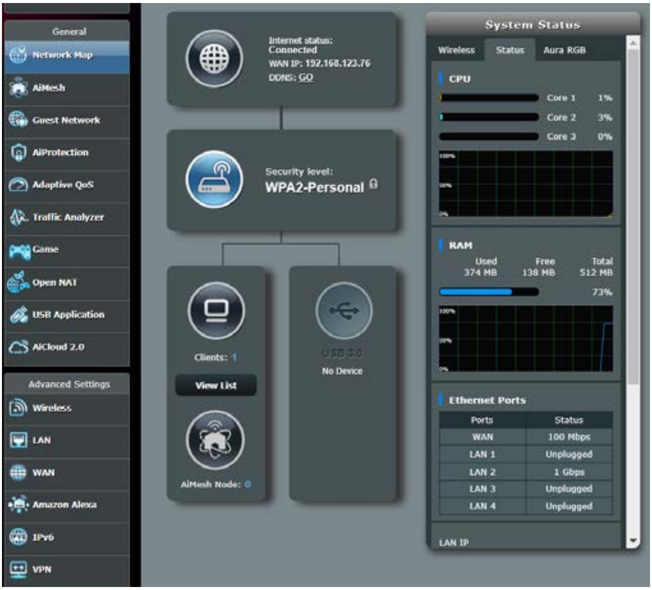
- When the Ethernet cable connecting the router with the modem is plugged in properly, the WAN LED will be on.
- When the Ethernet cable connecting your powered-on computer with the router is plugged in properly, the corresponding LAN LED will be on.

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

- When you connect your computer to the router wirelessly, ensure that the SSID (wireless network name), encryption mehtod, 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 router'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, **Network Map** > **Clients** page, and hover the mouse pointer over your device in **Client Status**.



Internet status: Connected
WAN IP: 192.168.123.76
DDNS: GO

Security level: WPA2-Personal

Clients: 1

AiMesh Node: 0

No Device

CPU

Core 1 1%
Core 2 3%
Core 3 0%

RAM

Used	Free	Total
374 MB	138 MB	512 MB

73%

Ethernet Ports

Ports	Status
WAN	100 Mbps
LAN 1	Unplugged
LAN 2	1 Gbps
LAN 3	Unplugged
LAN 4	Unplugged

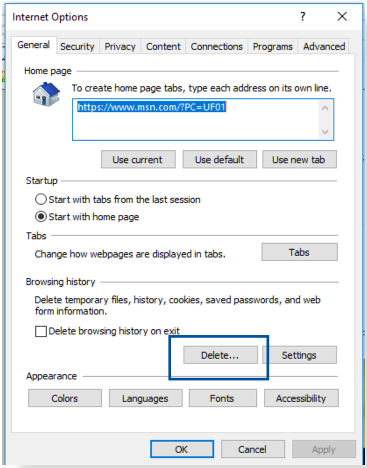
LAN IP

6.2 Frequently Asked Questions (FAQs)

I cannot access the router 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 is "admin/admin". 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**.



To create home page tabs, type each address on its own line.

https://www.msn.com/?PC=UF01

○ Start with tabs from the last session

● Start with home page

Change how webpages are displayed in tabs.

Delete temporary files, history, cookies, saved passwords, and web form information.

□ Delete browsing history on exit

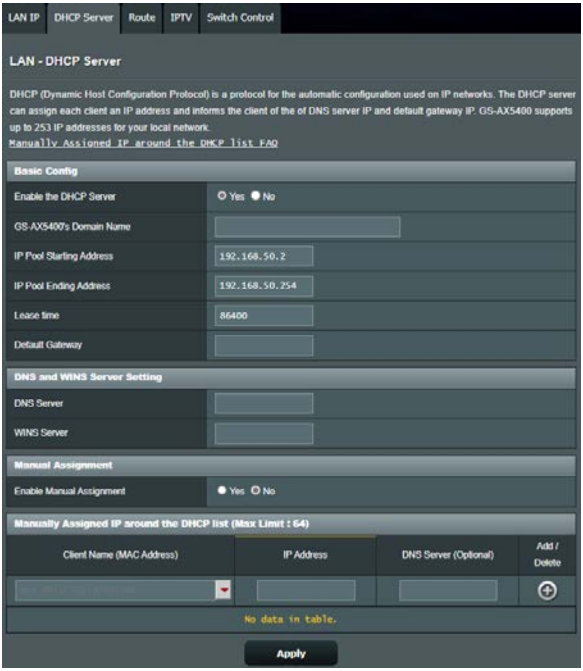
NOTES:

- 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 router.

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 router closer to the wireless client.
  - Try to adjust antennas of the router to the best direction as described in section **1.4 Positioning your router**.
- **DHCP server has been disabled:**
  1. Launch the web GUI. Go to **General** > **Network Map**> **Clients** and search for the device that you want to connect to the router.
  2. If you cannot find the device in the **Network Map**, go to **Advanced Settings** > **LAN** > **DHCP Server**, **Basic Config** list, select **Yes** on the **Enable the DHCP Server**.



LAN - DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a protocol for the automatic configuration used on IP networks. The DHCP server can assign each client an IP address and informs the client of the of DNS server IP and default gateway IP. GS-AX5400 supports up to 253 IP addresses for your local network.

Manually Assigned IP around the DHCP list FAQ

Basic Config

Enable the DHCP Server	○ Yes ● No
GS-AX5400's Domain Name	
IP Pool Starting Address	192.168.50.2
IP Pool Ending Address	192.168.50.254
Lease time	86400
Default Gateway	

DNS and WINS Server Setting

DNS Server	
WINS Server	

Manual Assignment

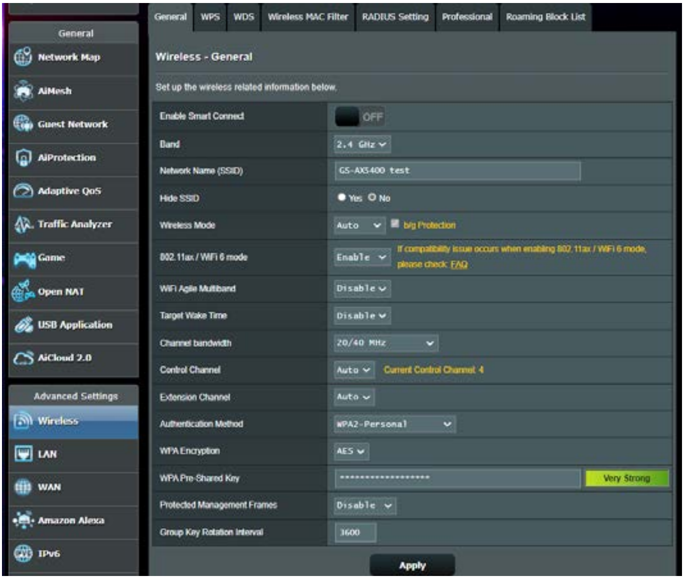
Enable Manual Assignment	● Yes ○ No

Manually Assigned IP around the DHCP list (Max Limit : 64)

Client Name (MAC Address)	IP Address	DNS Server (Optional)	Add / Delete
			⊕

No data in table.

- SSID has been hidden. If your device can find SSIDs from other routers but cannot find your router's SSID, go to **Advanced Settings** > **Wireless** > **General**, select **No** on **Hide SSID**, and select **Auto** on **Control Channel**.



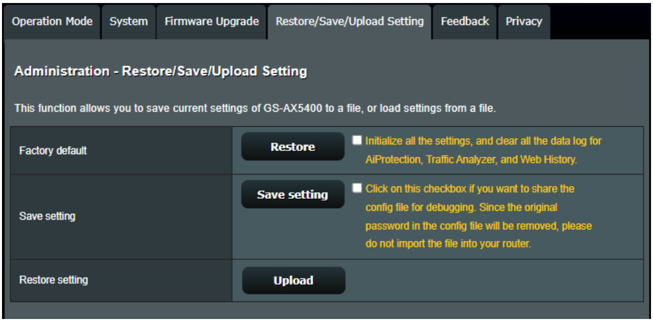
Wireless - General

Set up the wireless related information below.

Enable Smart Connect	OFF
Band	2.4 GHz
Network Name (SSID)	GS-AX5400 test
Hide SSID	● Yes ○ No
Wireless Mode	Auto ■ b/g Protection
802.11ax / WiFi 6 mode	Enable If compatibility issue occurs when enabling 802.11ax / WiFi 6 mode, please check: FAQ
WiFi Agile Multiband	Disable
Target Wake Time	Disable
Channel bandwidth	20/40 MHz
Control Channel	Auto Current Control Channel: 4
Extension Channel	Auto
Authentication Method	WPA2-Personal
WPA Encryption	AES
WPA Pre-Shared Key	****************** Very Strong
Protected Management Frames	Disable
Group Key Rotation Interval	3600

- 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 router wirelessly, you can reset your router to factory default settings. In the router GUI,click **Administration** > **Restore/Save/Upload Setting** and click **Restore**.



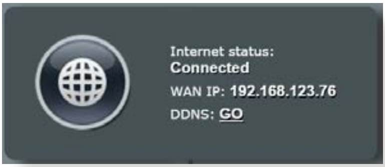
Administration - Restore/Save/Upload Setting

This function allows you to save current settings of GS-AX5400 to a file, or load settings from a file.

Factory default	Restore □ Initialize all the settings, and clear all the data log for AiProtection, Traffic Analyzer, and Web History.
Save setting	Save setting □ Click on this checkbox if you want to share the config file for debugging. Since the original password in the config file will be removed, please do not import the file into your router.
Restore setting	Upload

Internet is not accessible.

- Check if your router can connect to your ISP's WAN IP address. To do this, launch the web GUI and go to **General** > **Network Map**, and check the **Internet status**.
- If your router 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**.



Internet status:
Connected

WAN IP: 192.168.123.76

DDNS: GO

- The device has been blocked via the Parental Control function. Go to **General** > **AiProtection > Parental Controls** tab and see if the device is in the list. If the device is listed under **Client Name**, remove the device using the **Delete** button or adjust the Time Management Settings.
- 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 router. If the WAN LED on the wireless router 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 **Network Map**, click the router icon, enter a new SSID and encryption key, and then click **Apply**.
- Reset your router to the default settings. Launch the web GUI, go to **Administration** > **Restore/Save/Upload Setting**, and click **Restore**. The default login account and password are both "admin".

How to restore the system to its default settings?

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

  The following are the factory default settings:

User Name:	admin
Password:	admin
Enable DHCP:	Yes (if WAN cable is plugged in)
IP address:	http://www.asusrouter.com (or 192.168.1.1)
Domain Name:	(Blank)
Subnet Mask:	255.255.255.0
DNS Server 1:	192.168.1.1
DNS Server 2:	(Blank)
SSID (2.4GHz):	ASUS_XX_2G
SSID (5GHz):	ASUS_XX_5G

Firmware upgrade failed.

Launch the rescue mode and run the Firmware Restoration utility. Refer to section **5.2 Firmware Restoration** on how to use the Firmware Restoration utility.

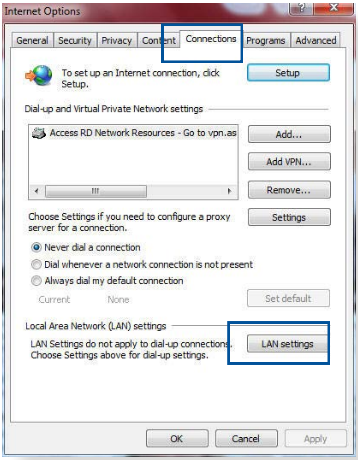
Cannot access Web GUI

Before configuring your wireless router, 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** tab > **LAN settings**.



To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Access RD Network Resources - Go to vpn.as

Choose Settings if you need to configure a proxy server for a connection.

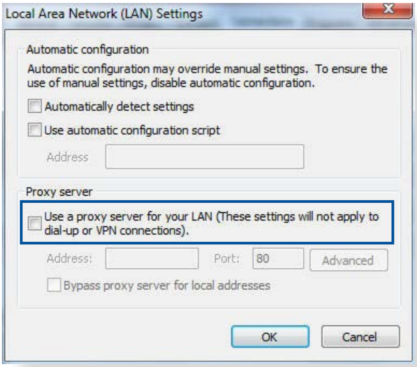
● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

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



Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

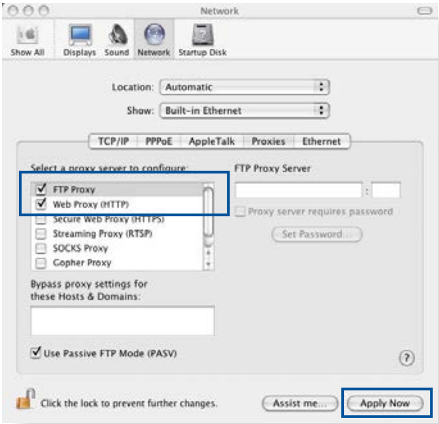
Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

MAC OS



Location: Automatic

Show: Built-in Ethernet

Select a proxy server to configure:

☑ FTP Proxy
☑ Web Proxy (HTTP)
□ Secure Web Proxy (HTTPS)
□ Streaming Proxy (RTSP)
□ SOCKS Proxy
□ Gopher Proxy

FTP Proxy Server

□ Proxy server requires password

Bypass proxy settings for these Hosts & Domains:

☑ Use Passive FTP Mode (PASV)

Click the lock to prevent further changes.

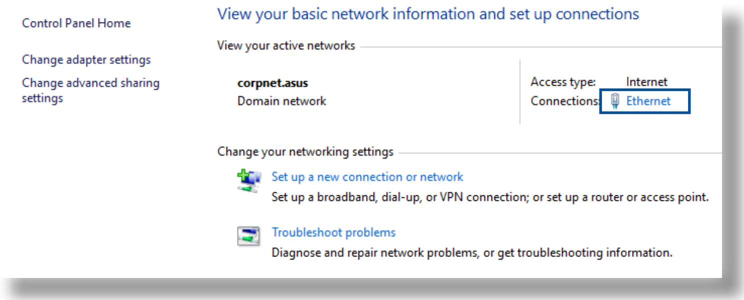
1. From your Safari browser, click **Safari** > **Preferences** > **Advanced** > **Change Settings...**
2. From the Network screen, deselect **FTP Proxy** and **Web Proxy (HTTP)**.
3. Click **Apply Now** when done.

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.



View your basic network information and set up connections

View your active networks

corpnet.asus
Domain network

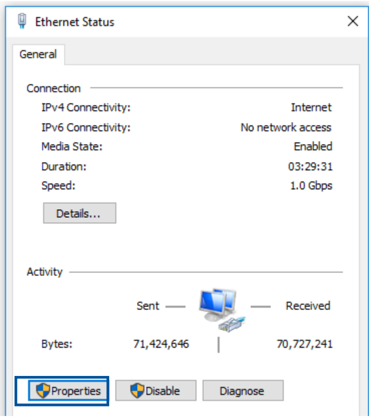
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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



Ethernet Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

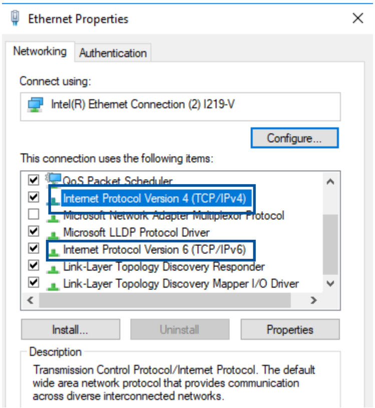
Duration: 03:29:31

Speed: 1.0 Gbps

Activity

Bytes: Sent 71,424,646 Received 70,727,241

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



Ethernet Properties

Networking Authentication

Connect using:

Intel(R) Ethernet Connection (2) I219-V

This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Link-Layer Topology Discovery Responder
- ☑ Link-Layer Topology Discovery Mapper I/O Driver

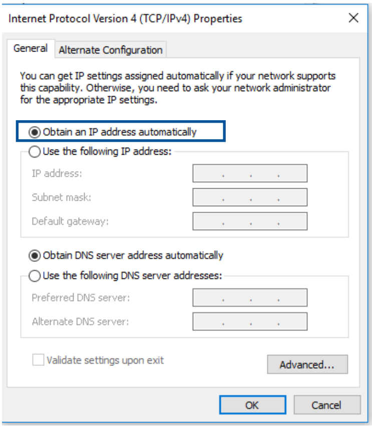
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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.



Internet Protocol Version 4 (TCP/IPv4) Properties

General Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

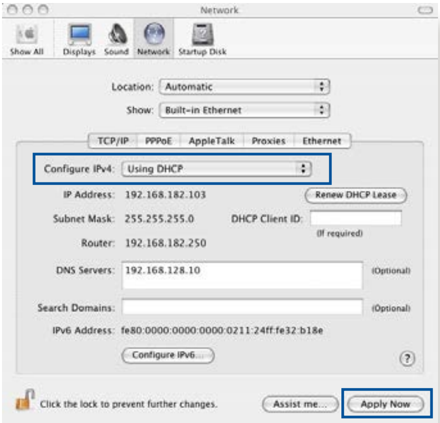
Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

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.



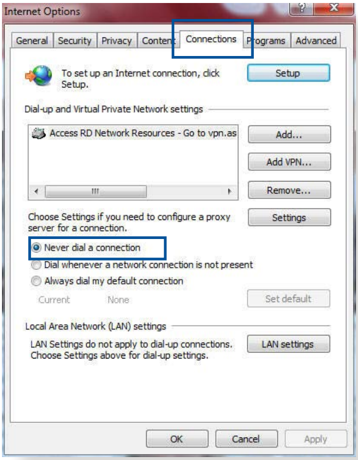
Location: Automatic
Show: Built-in Ethernet
Configure IPv4: Using DHCP
IP Address: 192.168.182.103
Subnet Mask: 255.255.255.0
DHCP Client ID:
Router: 192.168.182.250
DNS Servers: 192.168.128.10
Search Domains:
IPv6 Address: fe80:0000:0000:0000:0211:24ff:fe32:b18e

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** tab.
3. Tick **Never dial a connection**.
4. Click **OK** when done.



To set up an Internet connection, click Setup.

Access RD Network Resources - Go to vpn.as

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

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

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

Service and Support

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