User Guide

CMAX6000

Wireless AX DOCSIS 3.1 Cable Modem Router

IN SEARCH OF INCREDIBLE

CMAX6000

First Edition

March 2020

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval

system, or translated into any language in any form or by any means, except documentation kept by the purchaser for backup purposes, without the express written permission of ASUSTeK Computer Inc. ("ASUS").

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.

Contents

1 Getting to know your cable modem router

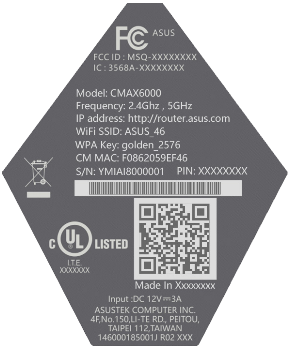
1.1 Package contents

1.2 Your cable modem router

1.3 Positioning your router

1.4 Product label

The product label at the bottom of your cable modem router contains the default Wi-Fi network name (SSID), Wi-Fi password, login information for the web graphical user interface (web GUI), serial number, MAC address, and other information.



ASUS
FCC ID : MSQ-XXXXXXXX
IC : 3568A-XXXXXXXX

Model: CMAX6000
Frequency: 2.4Ghz , 5GHz
IP address: http://router.asus.com
WiFi SSID: ASUS_46
WPA Key: golden_2576
CM MAC: F0862059EF46
S/N: YMIAI8000001 PIN: XXXXXXXX

Made In Xxxxxxxx
Input :DC 12V⎓3A
ASUSTEK COMPUTER INC.
4F,No.150,LI-TE RD., PEITOU,
TAIPEI 112,TAIWAN
146000185001J R02 XXX

1.5 Hardware Setup

2 Configuring the General Settings

2.1 Internet service

Visit your ISP's website and follow the on-screen instructions to activate your Internet service. If you subscribed to automatic IP (DHCP) service, the Internet is accessible now.

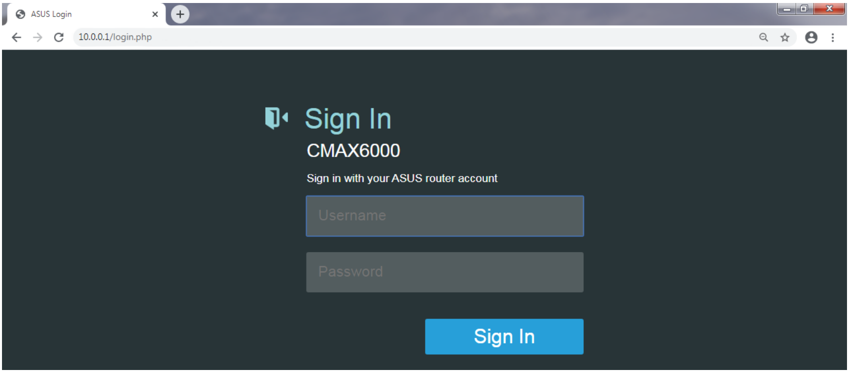
NOTES:

- Your ISP's contact information may change. Visit your ISP's website or check your Internet service billing statement for the latest contact information.
- If your router still does not connect to the Internet, contact your ISP and do the following:
  1. Provide your router's serial number and MAC address located on the product label, and confirm with your ISP if it is already active.
  2. If your router is visible to your ISP but there is still no Internet connection, reboot your router and check the online status again.
  3. If your router is still not visible to your ISP or your ISP can not provide technical support, do the following:
     1) Go to router.asus.com or http://10.0.0.1.
     2) Enter login username and password on the screen and you will be directed to the At a Glance page.
     3) On the left-side menu, click **Troubleshooting** and select **Feedback** tab.
     4) Click the **Generate log** and **Download File** buttons to save the log files and send the log files to cm_feedback@asus.com. We will reply to you as soon as possible.

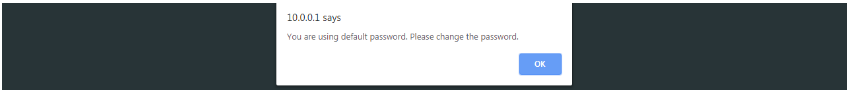
2.2 Basic Network Setup

To set up your CMAX6000 settings:

1. Launch your web browser and go to Enter the default IP address, **router.asus.com** or **http://10.0.0.1**.
2. Enter default login name "**admin**" and password "**password**" on the login screen.
3. Click **Sign In** to log into the software configuration interface.



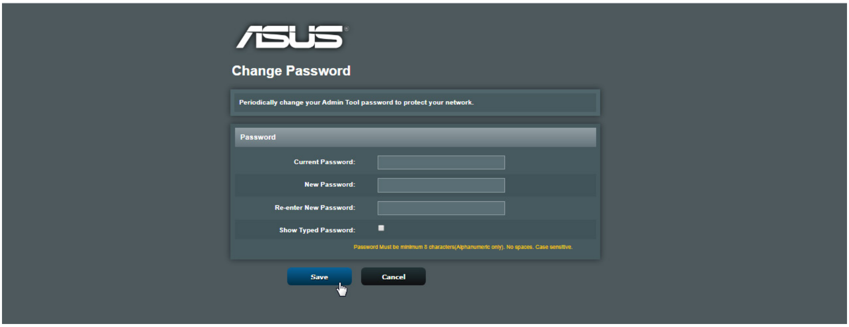
4. Set up a new password when prompted.



10.0.0.1 says

You are using default password. Please change the password.

5. Click **Save** and log into the software configuration interface with your new password.



Change Password

Periodically change your Admin Tool password to protect your network.

Password

Current Password:

New Password:

Re-enter New Password:

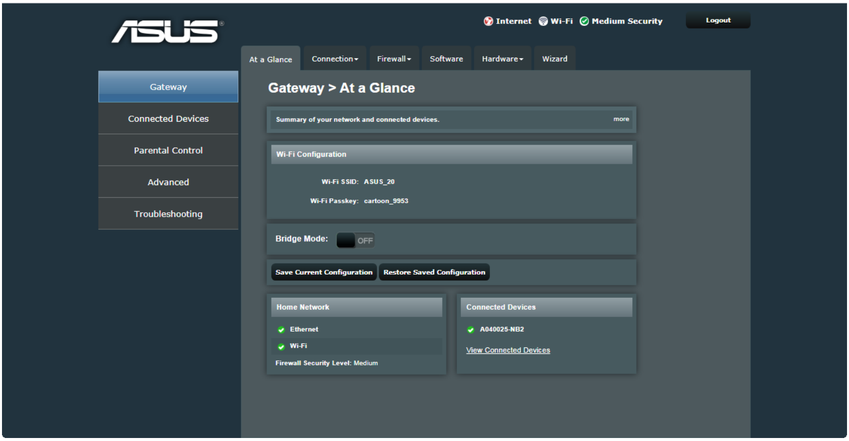
Show Typed Password: □

Password Must be minimum 8 characters(Alphanumeric only). No spaces. Case sensitive.

3 Setting up Your Gateway

3.1 At a Glance

This is the first screen displayed when you successfully log into the web management interface. The **At a Glance** of the **Gateway** section allows you to view the network connectivity and Wi-Fi connection status, to configure your device operation mode as router or bridge, and to save/upload cable modem router settings.



Gateway > At a Glance

Summary of your network and connected devices.

Wi-Fi Configuration

Wi-Fi SSID: ASUS_20

Wi-Fi Passkey: cartoon_9953

Bridge Mode: OFF

Firewall Security Level: Medium

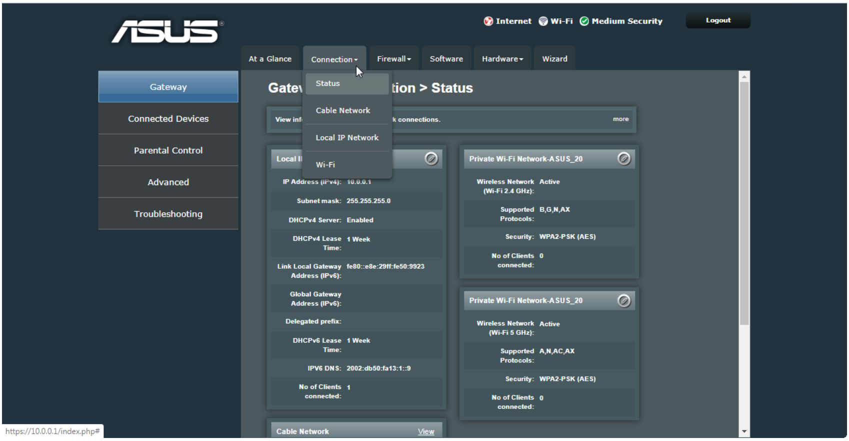
A040025-NB2

3.2 Connection

The **Connection** section allows you to view network connection status, manage your network clients and configure your network's security settings.

3.2.1 Status

The **Status** page displays device information and Cable Network Internet/Wireless/LAN connection status connected to your network.



Gatev tion > Status

View inf k connections.

Local I

IP Address (IPv4): 10.0.0.1
Subnet mask: 255.255.255.0
DHCPv4 Server: Enabled
DHCPv4 Lease Time: 1 Week
Link Local Gateway Address (IPv6): fe80::e8e:29ff:fe50:9923
Global Gateway Address (IPv6):
Delegated prefix:
DHCPv6 Lease Time: 1 Week
IPV6 DNS: 2002:db50:fa13:1::9
No of Clients connected: 1

Private Wi-Fi Network-ASUS_20

Wireless Network (Wi-Fi 2.4 GHz): Active
Supported Protocols: B,G,N,AX
Security: WPA2-PSK (AES)
No of Clients connected: 0

Private Wi-Fi Network-ASUS_20

Wireless Network (Wi-Fi 5 GHz): Active
Supported Protocols: A,N,AC,AX
Security: WPA2-PSK (AES)
No of Clients connected: 0

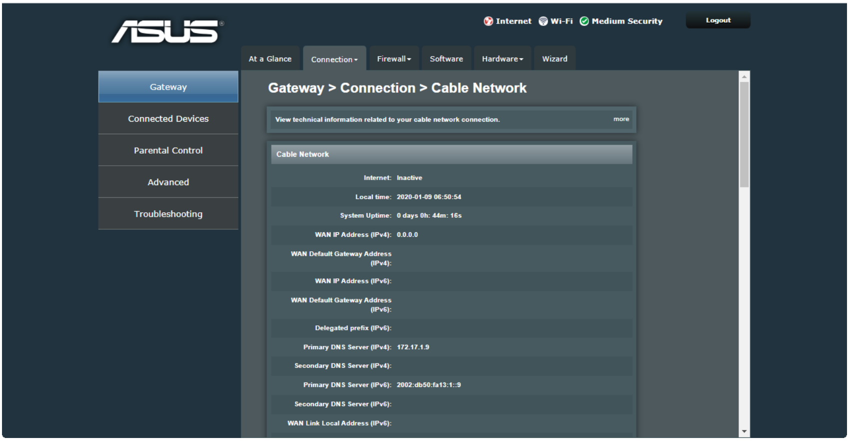
Cable Network

To view your network connection status:

1. From the navigation panel, go to **Gateway > Connection** tab.
2. Select **Status** from the dropdown menu of the **Connection** section.

3.2.2 Cable Network

The **Cable Network** screen displays the settings of WAN connection status.

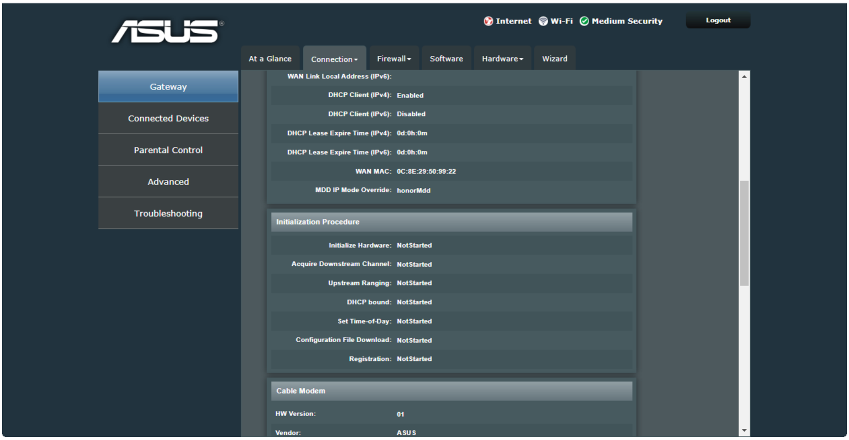


Gateway > Connection > Cable Network

View technical information related to your cable network connection.

Cable Network

Internet: Inactive
Local time: 2020-01-09 06:50:54
System Uptime: 0 days 0h: 44m: 16s
WAN IP Address (IPv4): 0.0.0.0
WAN Default Gateway Address (IPv4):
WAN IP Address (IPv6):
WAN Default Gateway Address (IPv6):
Delegated prefix (IPv6):
Primary DNS Server (IPv4): 172.17.1.9
Secondary DNS Server (IPv4):
Primary DNS Server (IPv6): 2002:db50:fa13:1::9
Secondary DNS Server (IPv6):
WAN Link Local Address (IPv6):



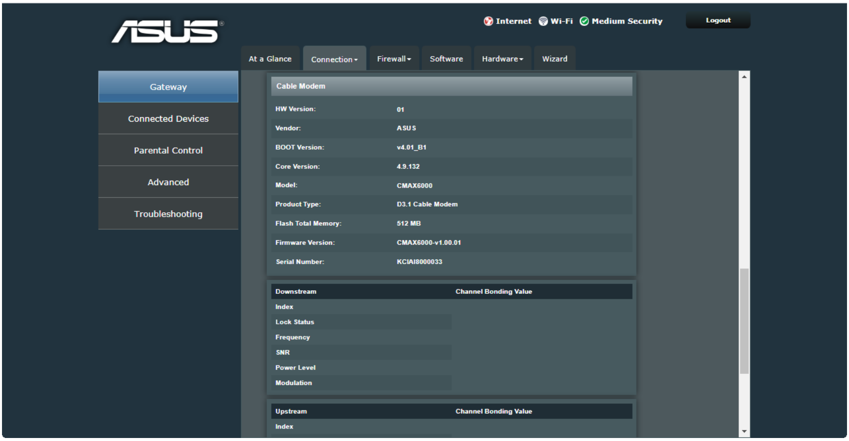
```
       WAN Link Local Address (IPv6):
                  DHCP Client (IPv4):  Enabled
                  DHCP Client (IPv6):  Disabled
     DHCP Lease Expire Time (IPv4):  0d:0h:0m
     DHCP Lease Expire Time (IPv6):  0d:0h:0m
                            WAN MAC:  0C:8E:29:50:99:22
              MDD IP Mode Override:  honorMdd
```

Initialization Procedure

```
               Initialize Hardware:  NotStarted
        Acquire Downstream Channel:  NotStarted
                  Upstream Ranging:  NotStarted
                       DHCP bound:  NotStarted
                  Set Time-of-Day:  NotStarted
       Configuration File Download:  NotStarted
                     Registration:  NotStarted
```

Cable Modem

```
HW Version:                01
Vendor:                    ASU S
```

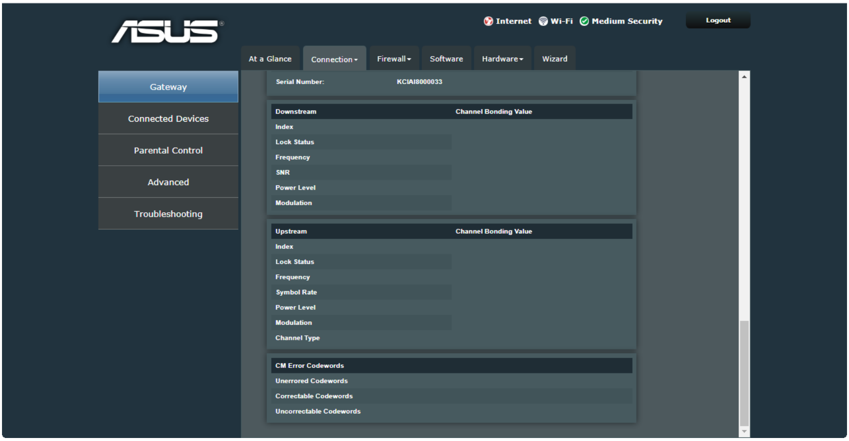


Cable Modem

```
HW Version:                01
Vendor:                    ASU S
BOOT Version:              v4.01_B1
Core Version:              4.9.132
Model:                     CMAX6000
Product Type:              D3.1 Cable Modem
Flash Total Memory:        512 MB
Firmware Version:          CMAX6000-v1.00.01
Serial Number:             KCIAI8000033
```

Downstream	Channel Bonding Value
Index	
Lock Status	
Frequency	
SNR	
Power Level	
Modulation	

Upstream	Channel Bonding Value
Index	



```
Serial Number:             KCIAI8000033
```

Downstream	Channel Bonding Value
Index	
Lock Status	
Frequency	
SNR	
Power Level	
Modulation	

Upstream	Channel Bonding Value
Index	
Lock Status	
Frequency	
Symbol Rate	
Power Level	
Modulation	
Channel Type	

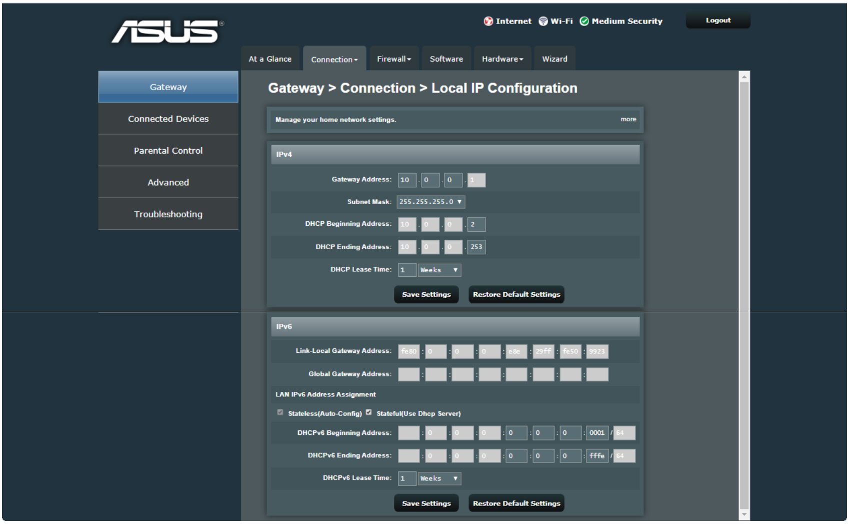
CM Error Codewords
Unerrored Codewords
Correctable Codewords
Uncorrectable Codewords

To view your WAN connection status:

1. From the navigation panel, go to **Gateway > Connection** tab.
2. Select **Cable Network** from the dropdown menu of the **Connection** section.

3.2.3 Local IP Configuration

Your router uses DHCP to assign IP addresses automatically on your network. The **Local IP Configuration** screen allows you to modify the LAN IP settings and specify the DHCP IP address range and lease time for the clients on your network.



Gateway > Connection > Local IP Configuration

Manage your home network settings.

IPv4

Gateway Address: 10 . 0 . 0 . 1
Subnet Mask: 255.255.255.0
DHCP Beginning Address: 10 . 0 . 0 . 2
DHCP Ending Address: 10 . 0 . 0 . 253
DHCP Lease Time: 1 Weeks

IPv6

Link-Local Gateway Address: fe80 : 0 : 0 : 0 : e8e : 29ff : fe50 : 9923
Global Gateway Address: : : : : : : :

LAN IPv6 Address Assignment

☑ Stateless(Auto-Config) ☑ Stateful(Use Dhcp Server)

DHCPv6 Beginning Address: : 0 : 0 : 0 : 0 : 0 : 0 : 0001 / 64
DHCPv6 Ending Address: : 0 : 0 : 0 : 0 : 0 : 0 : fffe / 64
DHCPv6 Lease Time: 1 Weeks

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

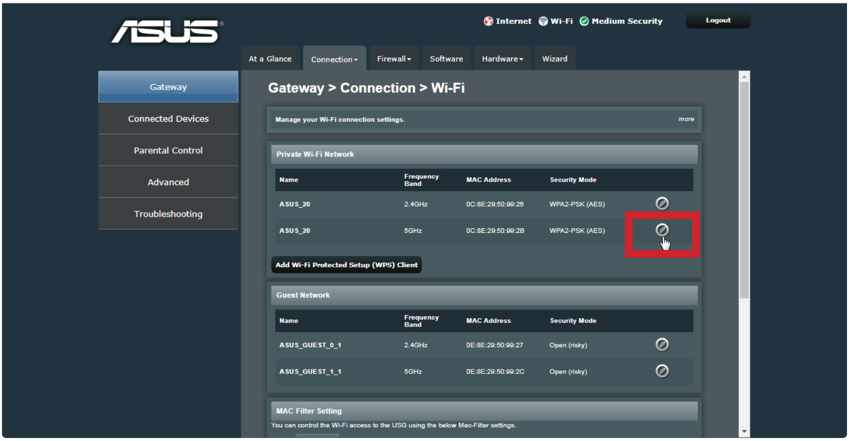
To modify the LAN IP settings:

1. From the navigation panel, go to **Gateway > Connection** tab.
2. Select **Local IP Network** from the dropdown menu.
3. Modify the IP address and subnet mask.
4. Specify the IP address range and lease time for the clients on your network.
5. When done, click **Save Settings**.

3.2.4 Wi-Fi

The CMAX6000 also operates as a wireless access point, allowing wireless computers to communicate with each other.

Private Wi-Fi Network



Gateway > Connection > Wi-Fi

Manage your Wi-Fi connection settings.

Private Wi-Fi Network

Name	Frequency Band	MAC Address	Security Mode
ASUS_20	2.4GHz	DC:8E:29:50:99:26	WPA2-PSK (AES)
ASUS_20	5GHz	DC:8E:29:50:99:2B	WPA2-PSK (AES)

Add Wi-Fi Protected Setup (WPS) Client

Guest Network

Name	Frequency Band	MAC Address	Security Mode
ASUS_GUEST_0_1	2.4GHz	DE:8E:29:50:99:27	Open (risky)
ASUS_GUEST_1_1	5GHz	DE:8E:29:50:99:2C	Open (risky)

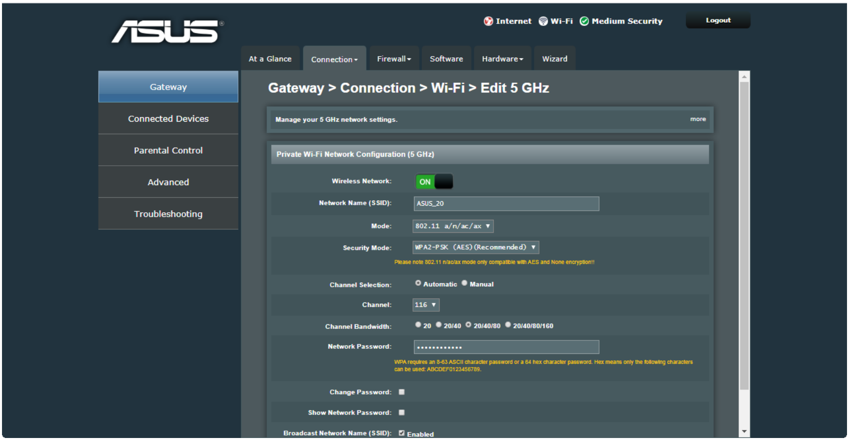
MAC Filter Setting

You can control the Wi-Fi access to the USG using the below Mac-Filter settings.

To configure the private wireless settings:

1. From the navigation panel, go to **Gateway** > **Connection** tab.
2. Select **Wi-Fi** from the dropdown menu.
3. Click the edit icon to configure the wireless settings.

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



Gateway > Connection > Wi-Fi > Edit 5 GHz

Manage your 5 GHz network settings.

Private Wi-Fi Network Configuration (5 GHz)

Wireless Network: ON

Network Name (SSID): ASUS_20

Mode: 802.11 a/n/ac/ax

Security Mode: WPA2-PSK (AES)(Recommended)

Please note 802.11 n/ac/ax mode only compatible with AES and None encryption!!

Channel Selection: ● Automatic ○ Manual

Channel: 116

Channel Bandwidth: ○ 20 ○ 20/40 ● 20/40/80 ○ 20/40/80/160

Network Password: ••••••••••••

WPA requires an 8-63 ASCII character password or a 64 hex character password. Hex means only the following characters can be used: ABCDEF0123456789.

Change Password: □

Show Network Password: □

Broadcast Network Name (SSID): ☑ Enabled

4. Select **On** for the **Wireless Network** to enable the wireless function.
5. Assign a unique name containing up to 32 characters for your **SSID** (Service Set Identifier) network name to identify your wireless network. Wi-Fi devices can identify and connect to the wireless network via your assigned SSID. The SSID information banner are updated on the **Status** page once new SSIDs are saved to the settings.
6. Select any of these wireless **Mode** options to determine the types of wireless devices that can connect to your wireless router:
   - 2.4 GHz: **802.11 b/g, 802.11 b/g/n, 802.11 b/g/n/ax**
   - 5 GHz: **802.11a, 802.11a/n/ac, 802.11a/n/ac/ax**
7. From the **Security Mode** dropdown list, select the authentication method for your wireless security. If you select WPA-PSK (Pre-shared Key)/WPA2-PSK (with TKIP or AES) as the authentication method, key in security passkey in the **Network Password** field.
   - **Open (risky)**: This option provides no security.

   Choose WPA-PSK/WPA2-PSK (with TKIP or AES) or mixed mode as the authentication method to provides strong security.

   - **WPA-PSK (TKIP)**
   - **WPA-PSK (AES)**
   - **WPA2-PSK (AES)(Recommended)**
   - **WPA2-PSK (TKIP/AES)**
   - **WPA-WPA2-PSK (TKIP/AES)**

IMPORTANT! The IEEE 802.11n/ac/ax standard prohibits using High Throughput with WPA/WPA2-PSK with TKIP as the unicast cipher. If you use these encryption methods, your data rate will drop to IEEE 802.11a/IEEE 802.11g connection. Only WPA/WPA2-PSK with AES authentication supports 802.11 n/ac/ax operation mode.

8. Select the operating channel for your wireless router.

   Select **Auto** to allow the wireless router to automatically select the channel that has the least amount of interference.

9. Select any of these **Channel Bandwidth** to accommodate higher transmission speeds:

   2.4 GHz/5 GHz bands:

   - **20 MHz**
   - **20/40 MHz**

   5 GHz bands:

   - **20/40/80 MHz (default)**
   - **20/40/80/160 MHz**

10. Enter the **Network Password**. Passwords can contain from 8~20 alphanumeric characters (A-Z, 0-9) and are case sensitive.

11. You can change the Wi-Fi network password by clicking on the **Change Password** checkbox and entering a new password.

12. Click the checkbox in the **Show Network Password** to conceal the security password if you like to.

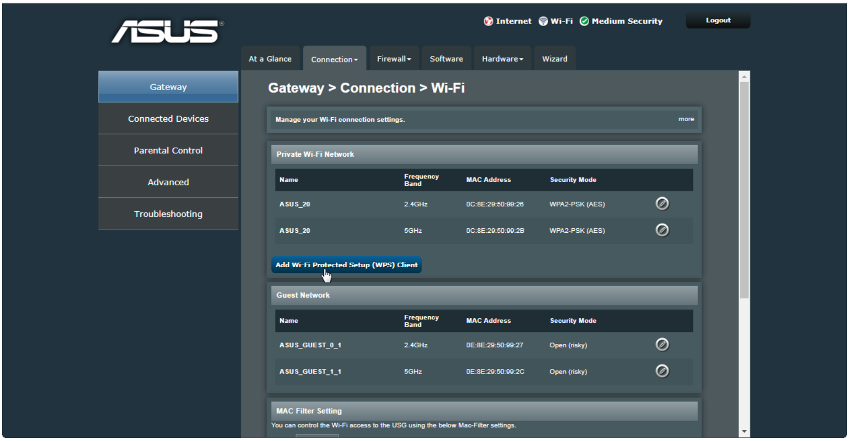
13. **Broadcast Network Name** (SSID): Click on the checkbox to enable the broadcast function of easy connection for the clients. Disable this function to increase security.

14. .When done, click **Save Settings**.

3.2.4.1 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.



Gateway > Connection > Wi-Fi

Manage your Wi-Fi connection settings.

Private Wi-Fi Network

Name	Frequency Band	MAC Address	Security Mode
ASUS_20	2.4GHz	0C:8E:29:50:99:26	WPA2-PSK (AES)
ASUS_20	5GHz	0C:8E:29:50:99:2B	WPA2-PSK (AES)

Guest Network

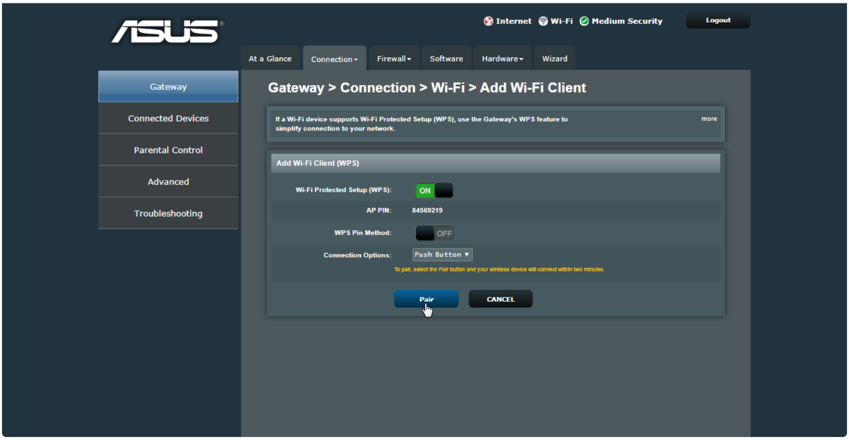
Name	Frequency Band	MAC Address	Security Mode
ASUS_GUEST_0_1	2.4GHz	0E:8E:29:50:99:27	Open (risky)
ASUS_GUEST_1_1	5GHz	0E:8E:29:50:99:2C	Open (risky)

MAC Filter Setting

You can control the Wi-Fi access to the USG using the below Mac-Filter settings.

To enable WPS on your wireless network:

1. From the navigation panel, go to **Gateway > Connection** tab.
2. Select **Wi-Fi** from the dropdown menu.
3. Click on the **Add Wi-Fi Protected Setup (WPS) Client** button.
4. In the **Wi-Fi Protected Setup (WPS)** field, move the slider to **ON**.
5. In the **WPS PIN Method** field, move the slider to **ON**.
6. In the **Connection Options**, select **Push Button** or **PIN Method**. If you select **Push Button**, go to step 7. If you select **PIN Method**, go to step 8.
7. To set up WPS using the router's WPS button, follow these steps:



Gateway > Connection > Wi-Fi > Add Wi-Fi Client

If a Wi-Fi device supports Wi-Fi Protected Setup (WPS), use the Gateway's WPS feature to simplify connection to your network.

Add Wi-Fi Client (WPS)

Wi-Fi Protected Setup (WPS): ON

AP PIN: 84569219

WPS Pin Method: OFF

Connection Options: Push Button

To pair, select the Pair button and your wireless device will connect within two minutes.

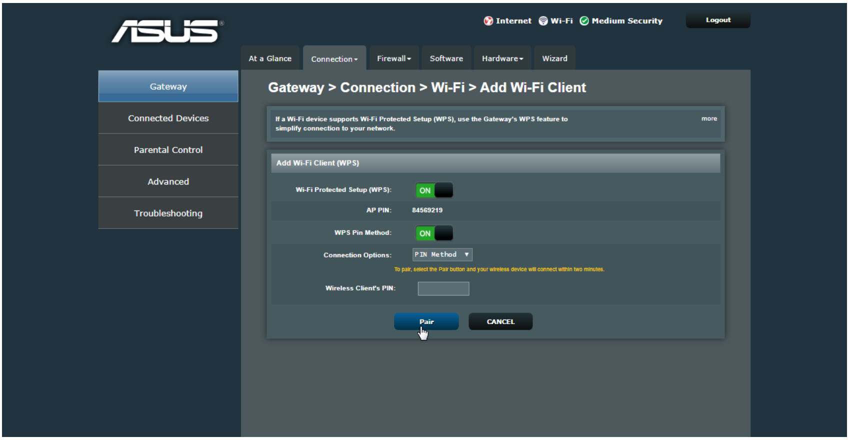
a. Click **Pair** or press the WPS button found at the rear of the wireless router.

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.

---

8. To set up WPS using the **PIN Method**, follow these steps:



Gateway > Connection > Wi-Fi > Add Wi-Fi Client

If a Wi-Fi device supports Wi-Fi Protected Setup (WPS), use the Gateway's WPS feature to simplify connection to your network.

Add Wi-Fi Client (WPS)

Wi-Fi Protected Setup (WPS): ON

AP PIN: 84569219

WPS Pin Method: ON

Connection Options: PIN Method

To pair, select the Pair button and your wireless device will connect within two minutes.

Wireless Client's PIN:

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

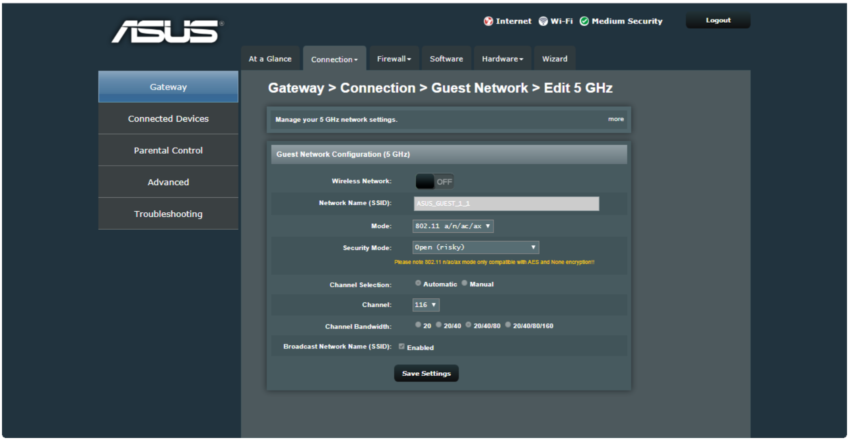
3.2.4.2 Guest Network

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

To configure the guest network settings:

1. From the navigation panel, go to **Gateway > Connection** tab.
2. Select **Wi-Fi** from the dropdown menu.
3. To change a guest's settings, click the edit icon of the guest settings you want to modify.

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



Gateway > Connection > Guest Network > Edit 5 GHz

Manage your 5 GHz network settings.

Guest Network Configuration (5 GHz)

Wireless Network: OFF

Network Name (SSID): ASUS_GUEST_1_1

Mode: 802.11 a/n/ac/ax

Security Mode: Open (risky)

Please note 802.11 n/ac/ax mode only compatible with AES and None encryption!!

Channel Selection: ○ Automatic ○ Manual

Channel: 116

Channel Bandwidth: ○ 20 ○ 20/40 ○ 20/40/80 ○ 20/40/80/160

Broadcast Network Name (SSID): ☑ Enabled

4. Select **On** for the **Wireless Network** to enable the wireless function.
5. Assign a unique name containing up to 32 characters for your **SSID** (Service Set Identifier) network name to identify your wireless network. Wi-Fi devices can identify and connect

to the wireless network via your assigned SSID. The SSID information banner are updated on the **Status** page once new SSIDs are saved to the settings.

6. Select any of these wireless **Mode** options to determine the types of wireless devices that can connect to your wireless router:
    - 2.4 GHz: **802.11 b/g, 802.11 b/g/n, 802.11 b/g/n/ax**
    - 5 GHz: **802.11a, 802.11a/n/ac, 802.11a/n/ac/ax**
7. From the **Security Mode** dropdown list, select the authentication method for your wireless security. If you select WPA-PSK (Pre-shared Key)/WPA2-PSK (with TKIP or AES) as the authentication method, key in security passkey in the **Network Password** field.
    - **Open (risky)**: This option provides no security.

    Choose WPA-PSK/WPA2-PSK (with TKIP or AES) or mixed mode as the authentication method to provides strong security.

    - **WPA-PSK (TKIP)**
    - **WPA-PSK (AES)**
    - **WPA2-PSK (AES)(Recommended)**
    - **WPA2-PSK (TKIP/AES)**
    - **WPA-WPA2-PSK (TKIP/AES)**

IMPORTANT! The IEEE 802.11n/ac/ax standard prohibits using High Throughput with WPA/WPA2-PSK with TKIP as the unicast cipher. If you use these encryption methods, your data rate will drop to IEEE 802.11a/IEEE 802.11g connection. Only WPA/WPA2-PSK with AES authentication supports 802.11 n/ac/ax operation mode.

8. Select the operating channel for your wireless router.

   Select **Auto** to allow the wireless router to automatically select the channel that has the least amount of interference.

9. Select any of these **Channel Bandwidth** to accommodate higher transmission speeds:

   2.4 GHz/5 GHz bands:

   - **20 MHz**
   - **20/40 MHz**

   5 GHz bands:

   - **20/40/80 MHz (default)**
   - **20/40/80/160 MHz**

10. Enter the **Network Password**. Passwords can contain from 8~20 alphanumeric characters (A-Z, 0-9) and are case sensitive.

11. You can change the Wi-Fi network password by clicking on the **Change Password** checkbox and entering a new password.

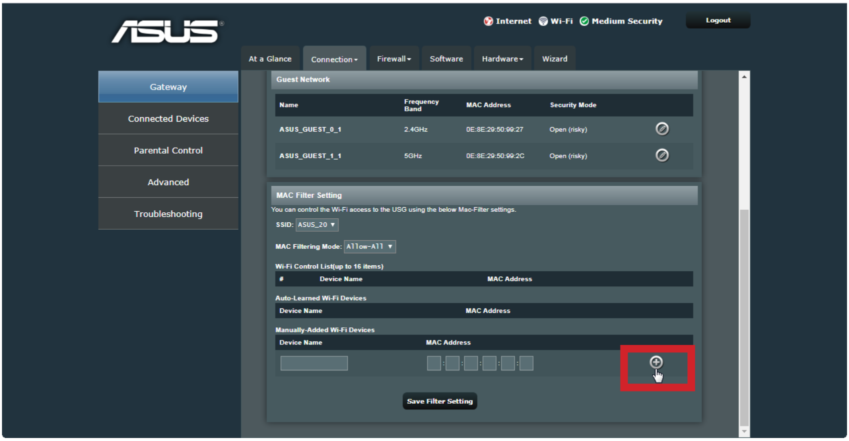
12. Click the checkbox in the **Show Network Password** to conceal the security password if you like to.

13. **Broadcast Network Name** (SSID): Click on the checkbox to enable the broadcast function of easy connection for the clients. Disable this function to increase security.

14. .When done, click **Save Settings**.

3.2.4.3 MAC Filter Setting

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



Guest Network

Name	Frequency Band	MAC Address	Security Mode
ASUS_GUEST_0_1	2.4GHz	0E:8E:29:50:99:27	Open (risky)
ASUS_GUEST_1_1	5GHz	0E:8E:29:50:99:2C	Open (risky)

MAC Filter Setting

You can control the Wi-Fi access to the USG using the below Mac-Filter settings.

SSID: ASUS_20

MAC Filtering Mode: Allow-All

Wi-Fi Control List(up to 16 items)

#	Device Name	MAC Address

Auto-Learned Wi-Fi Devices

Device Name	MAC Address

Manually-Added Wi-Fi Devices

Device Name	MAC Address
	: : : : :

To set up the Wireless MAC filter:

1. From the navigation panel, go to **Gateway > Connection** tab.
2. Select **Wi-Fi** from the dropdown menu.
3. In the **SSID** field, select the network name that you want to use for the Wireless MAC filter.
4. In the **MAC Filtering Mode** dropdown list, select either **Allow** or **Deny**.
   - Select **Allow** to allow devices in the MAC filter list to access to the wireless network.
   - •Select **Deny** to prevent devices in the MAC filter list to access to the wireless network.
5. Click the add icon to on the Wi-Fi device list, or key in the Device Name and its MAC address of the wireless device and click the add icon.
6. When done, click **Save Filter Setting**.

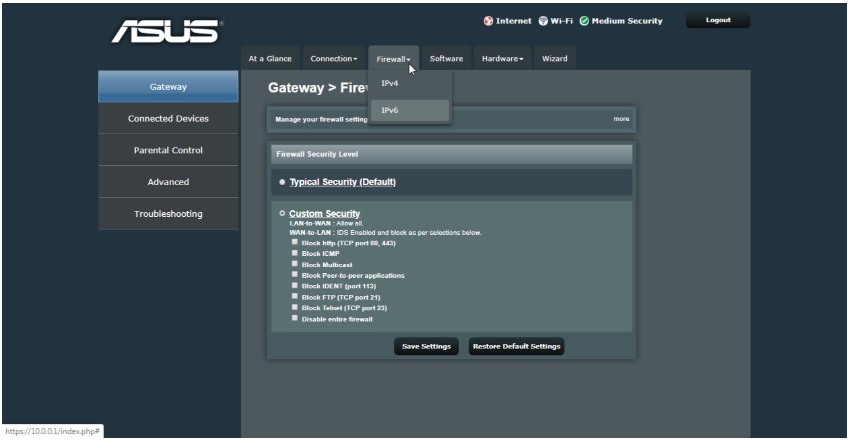
3.3 Firewall

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

NOTE: The Firewall feature is enabled **Typical Security (Medium)** by default.

3.3.1 IPv4 Firewall / IPv6 Firewall

By default, the IPv4 firewall blocks all P2P (peer-to-peer) applications and pings to the router . The IPv6 firewall function blocks all unsolicited incoming traffic.



Gateway > Fire

Manage your firewall setting

Firewall Security Level

● Typical Security (Default)

○ Custom Security

LAN-to-WAN : Allow all.

WAN-to-LAN : IDS Enabled and block as per selections below.

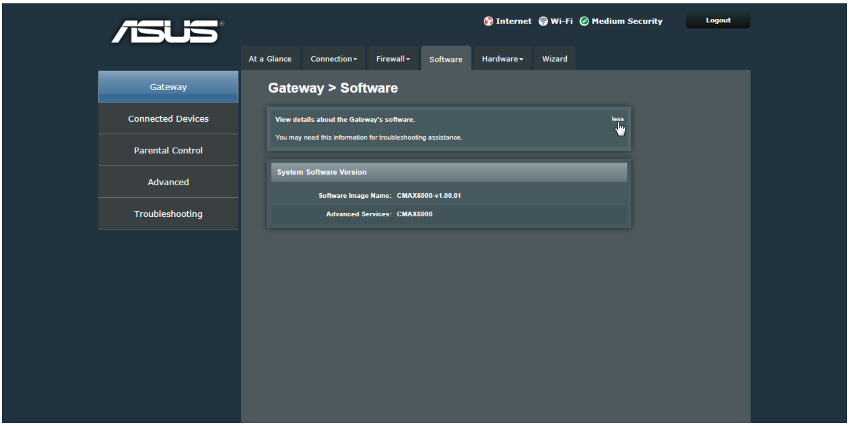
- □ Block http (TCP port 80, 443)
- □ Block ICMP
- □ Block Multicast
- □ Block Peer-to-peer applications
- □ Block IDENT (port 113)
- □ Block FTP (TCP port 21)
- □ Block Telnet (TCP port 23)
- □ Disable entire firewall

To set up a network service filter by blocking specified services:

1. From the navigation panel, go to **Gateway > Firewall** tab.
2. Select **IPv4/IPv6** from the dropdown menu.
3. Click **Custom Security**.
4. Specify the network services as shown on the screen to filter.
5. When done, click **Save Settings**.

3.4 Software

The Software screen displays firmware version number and device model number.



Gateway > Software

View details about the Gateway's software.

You may need this information for troubleshooting assistance.

System Software Version

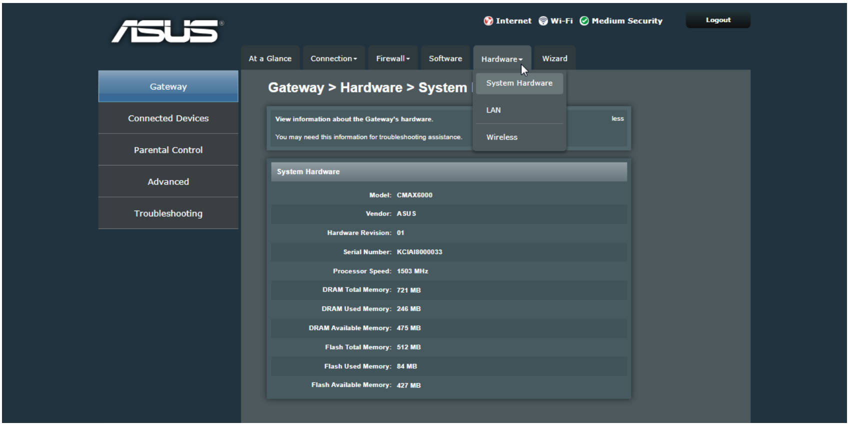
Software Image Name: CMAX6000-v1.00.01

Advanced Services: CMAX6000

3.5 Hardware

3.5.1 System Hardware

The System Hardware screen displays device model number and hardware version number, and serial number, as well as information on the DRAM and Flash memory status.



Gateway > Hardware > System

View information about the Gateway's hardware.

You may need this information for troubleshooting assistance.

System Hardware

Model: CMAX6000

Vendor: ASUS

Hardware Revision: 01

Serial Number: KCIAI8000033

Processor Speed: 1503 MHz

DRAM Total Memory: 721 MB

DRAM Used Memory: 246 MB

DRAM Available Memory: 475 MB

Flash Total Memory: 512 MB

Flash Used Memory: 84 MB

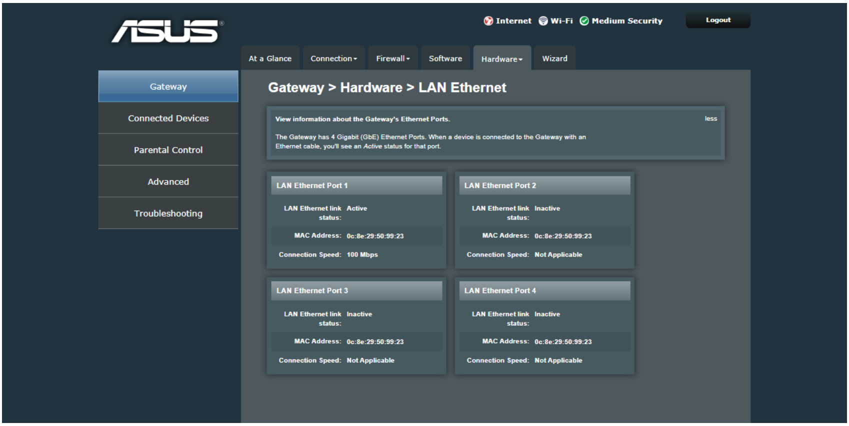
Flash Available Memory: 427 MB

To view your hardware information:

1. From the navigation panel, go to **Gateway** > **Hardware** tab.
2. Select **System Hardware** from the dropdown menu of the **Hardware** section.

3.5.2 LAN

The LAN screen displays LAN connection status and operation speed information on DHCP clients connected to your network.



Gateway > Hardware > LAN Ethernet

View information about the Gateway's Ethernet Ports.

The Gateway has 4 Gigabit (GbE) Ethernet Ports. When a device is connected to the Gateway with an Ethernet cable, you'll see an *Active* status for that port.

LAN Ethernet Port 1

LAN Ethernet link status: Active
MAC Address: 0c:8e:29:50:99:23
Connection Speed: 100 Mbps

LAN Ethernet Port 2

LAN Ethernet link status: Inactive
MAC Address: 0c:8e:29:50:99:23
Connection Speed: Not Applicable

LAN Ethernet Port 3

LAN Ethernet link status: Inactive
MAC Address: 0c:8e:29:50:99:23
Connection Speed: Not Applicable

LAN Ethernet Port 4

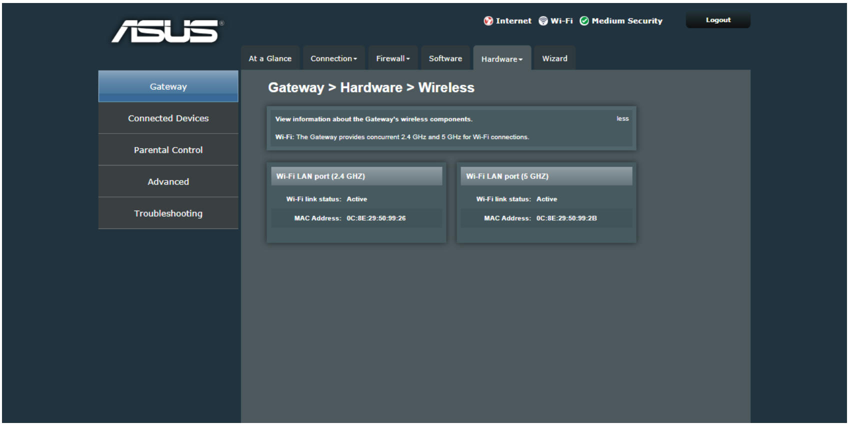
LAN Ethernet link status: Inactive
MAC Address: 0c:8e:29:50:99:23
Connection Speed: Not Applicable

To view your LAN status:

1. From the navigation panel, go to **Gateway** > **Hardware** tab.
2. Select **LAN** from the dropdown menu of the **Hardware** section.

3.5.3 Wireless

The Wireless screen shows wireless status on your network.



Gateway > Hardware > Wireless

View information about the Gateway's wireless components.

Wi-Fi: The Gateway provides concurrent 2.4 GHz and 5 GHz for Wi-Fi connections.

Wi-Fi LAN port (2.4 GHZ)

Wi-Fi link status: Active

MAC Address: 0C:8E:29:50:99:26

Wi-Fi LAN port (5 GHZ)

Wi-Fi link status: Active

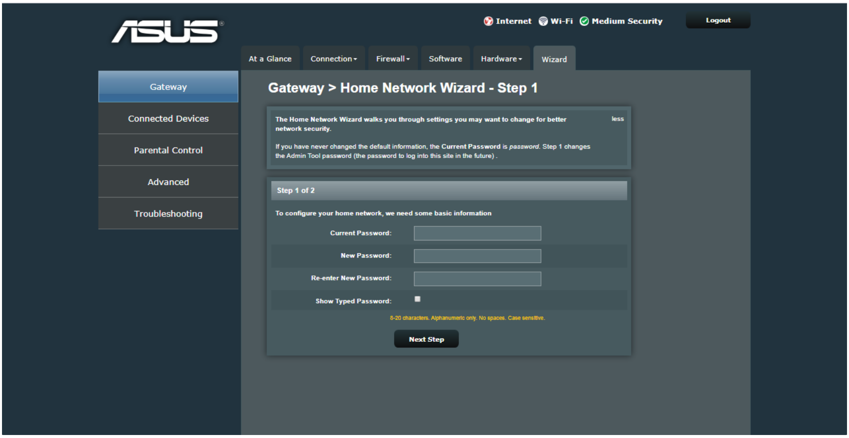
MAC Address: 0C:8E:29:50:99:2B

To view your Wireless status:

1. From the navigation panel, go to **Gateway > Hardware** tab.
2. Select **Wireless** from the dropdown menu of the **Hardware** section.

3.6 Wizard

The setup **Wizard** allows you to quickly set up your security settings.



Gateway > Home Network Wizard - Step 1

The Home Network Wizard walks you through settings you may want to change for better network security.

If you have never changed the default information, the **Current Password** is *password*. Step 1 changes the Admin Tool password (the password to log into this site in the future) .

Step 1 of 2

To configure your home network, we need some basic information

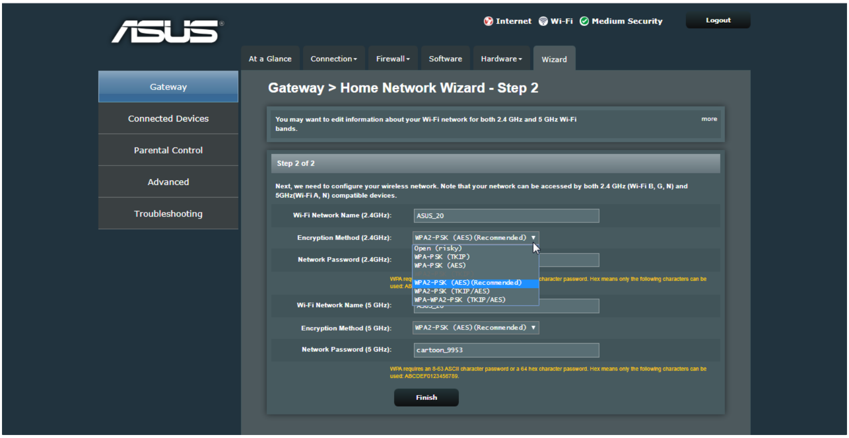
Current Password:

New Password:

Re-enter New Password:

Show Typed Password: □

8-20 characters. Alphanumeric only. No spaces. Case sensitive.



Gateway > Home Network Wizard - Step 2

You may want to edit information about your Wi-Fi network for both 2.4 GHz and 5 GHz Wi-Fi bands.

Step 2 of 2

Next, we need to configure your wireless network. Note that your network can be accessed by both 2.4 GHz (Wi-Fi B, G, N) and 5GHz(Wi-Fi A, N) compatible devices.

Wi-Fi Network Name (2.4GHz): ASUS_20

Encryption Method (2.4GHz): WPA2-PSK (AES)(Recommended)

Network Password (2.4GHz):

WPA req character password. Hex means only the following characters can be used: AB

Wi-Fi Network Name (5 GHz):

Encryption Method (5 GHz): WPA2-PSK (AES)(Recommended)

Network Password (5 GHz): cartoon_9953

WPA requires an 8-63 ASCII character password or a 64 hex character password. Hex means only the following characters can be used: ABCDEF0123456789.

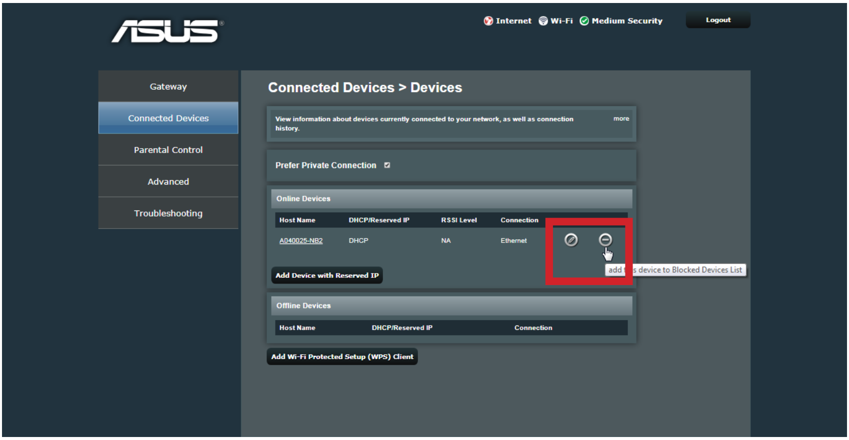
To change your login password and Wi-Fi security:

1. From the navigation panel, go to **Gateway** > **Wizard** tab.
2. Type your current login password.
3. Set a new password and type the new password again. Passwords can contain from 8~20 alphanumeric characters (A-Z, 0-9) and are case sensitive.
4. Click the checkbox in the **Show Typed Password** to conceal the password if you like to.
5. When done, click **Next Step**.
6. On the Wi-Fi setup screen, assign a new SSID (Service Set Identifier) name containing up to 32 characters for your **Wi-Fi Network Name** to identify your wireless network. Wi-Fi devices can identify and connect to the wireless network via your assigned SSID. The SSID information banner are updated on the **Status** page once new SSIDs are saved to the settings.
7. From the **Encryption Method** dropdown list, select the authentication method for your wireless security. If you select WPA-PSK (Pre-shared Key)/WPA2-PSK (with TKIP or AES) as the authentication method, key in security passkey in the **Network Password** field.
8. When done, click **Finish**.

4 Managing Network Clients

4.1 Connected Devices

The connection status is displayed as the following screen.


Internet
Wi-Fi
Medium Security
Logout
Gateway
Connected Devices
Parental Control
Advanced
Troubleshooting
more
add this device to Blocked Devices List
Add Device with Reserved IP
Add Wi-Fi Protected Setup (WPS) Client

Connected Devices > Devices

View information about devices currently connected to your network, as well as connection history.

Prefer Private Connection ☑

Online Devices

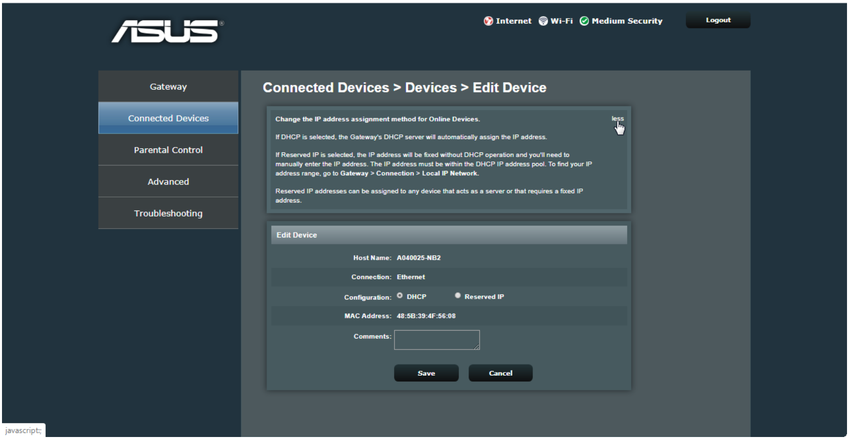
Host Name	DHCP/Reserved IP	RSSI Level	Connection
A040025-NB2	DHCP	NA	Ethernet

Offline Devices

Host Name	DHCP/Reserved IP	Connection

To manage your network clients:

1. From the navigation panel, click on **Connected Devices**.
2. On the **Prefer Private Connection**, select the edit icon to display your network client's information.



Connected Devices > Devices > Edit Device

Change the IP address assignment method for Online Devices.

If DHCP is selected, the Gateway's DHCP server will automatically assign the IP address.

If Reserved IP is selected, the IP address will be fixed without DHCP operation and you'll need to manually enter the IP address. The IP address must be within the DHCP IP address pool. To find your IP address range, go to **Gateway > Connection > Local IP Network.**

Reserved IP addresses can be assigned to any device that acts as a server or that requires a fixed IP address.

Edit Device

Host Name: A040025-NB2

Connection: Ethernet

Configuration: ◉ DHCP ○ Reserved IP

MAC Address: 48:5B:39:4F:56:08

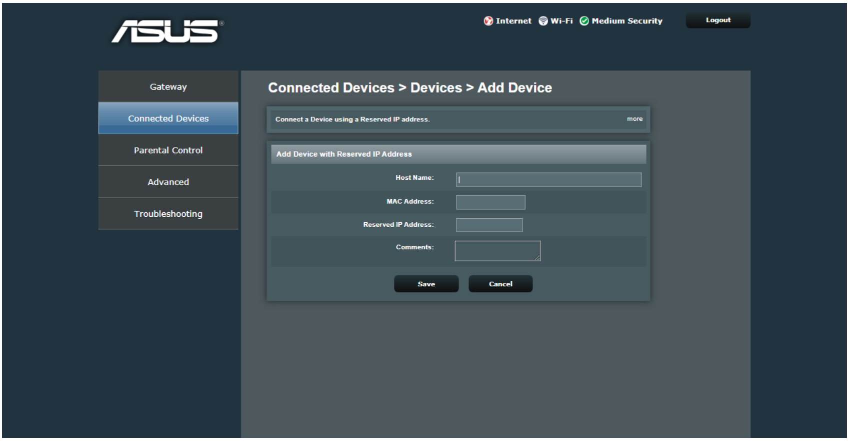
Comments:

3. When done, click **Save**.

4. To block a client's access to your network, click on the block icon on the screen, then click **Yes** to block the client's network access.

4.1.1 Reserved IP

Some specific DHCP clients providing network server services require fixed IP addresses to be assigned to them. You can assign a static IP to a certain MAC address within your network.



Connected Devices > Devices > Add Device

Connect a Device using a Reserved IP address.

Add Device with Reserved IP Address

Host Name:

MAC Address:

Reserved IP Address:

Comments:

To assign a static IP to a certain network client:

1. From the navigation panel, click on **Connected Devices**.
2. On the **Prefer Private Connection**, click on the **Add Device with Reserved IP** button.
3. Enter the enter the network information and IP address to be reserved for the client.
4. When done, click **Save**.

To enable WPS on your wireless network:

1. From the navigation panel, click on **Connected Devices**.
2. Click on the **Add Wi-Fi Protected Setup (WPS) Client** button.

3. In the **Wi-Fi Protected Setup (WPS)** field, move the slider to **ON**.
4. In the **WPS PIN Method** field, move the slider to **ON**.
5. In the **Connection Options**, select **Push Button** or **PIN Method**. If you select **Push Button**, go to step 6. If you select **PIN Method**, go to step 7.
6. To set up WPS using the router's WPS button, follow these steps:
    a. Click **Pair** 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.

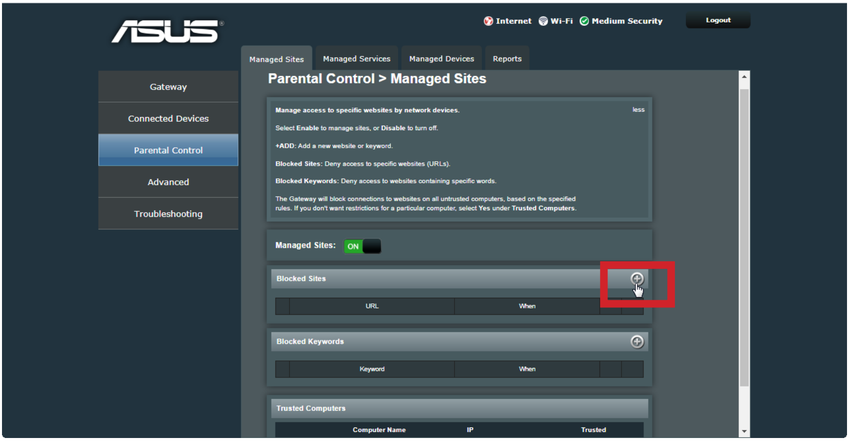
Note: Check your wireless device or its user manual for the location of the WPS button.

7. To set up WPS using the **PIN Method**, 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 **Pair** to put your wireless router into WPS survey mode. The router's LED indicators quickly flash three times until the WPS setup is completed.

4.2 Setting up Parental Control

Parental Control allows you to control the Internet access time, web sites and services or applications. Users can set the access limit for a client's network usage and view the control activity.

4.2.1 Managed Sites



Parental Control > Managed Sites

Manage access to specific websites by network devices. less

Select **Enable** to manage sites, or **Disable** to turn off.

+ADD: Add a new website or keyword.

Blocked Sites: Deny access to specific websites (URLs).

Blocked Keywords: Deny access to websites containing specific words.

The Gateway will block connections to websites on all untrusted computers, based on the specified rules. If you don't want restrictions for a particular computer, select **Yes** under **Trusted Computers**.

Managed Sites: ON

Blocked Sites

	URL	When		

Blocked Keywords

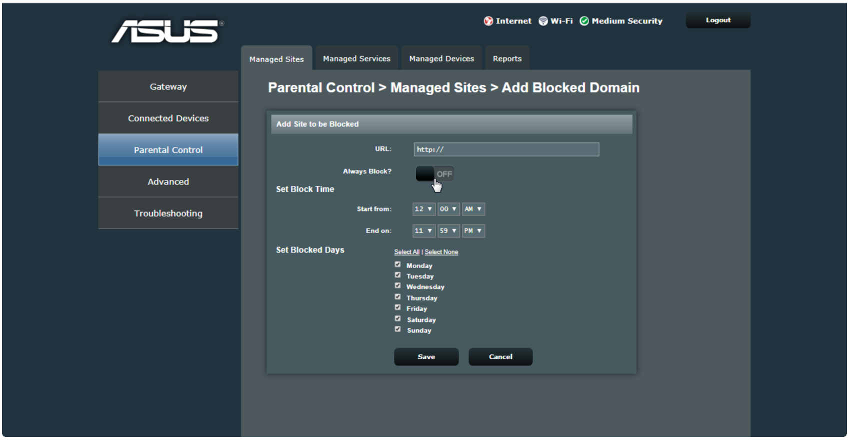
	Keyword	When		

Trusted Computers

Computer Name	IP	Trusted

To set up the Managed Sites:

1. From the navigation panel, go to **Parental Control > Managed Sites** tab.
2. Move the slider to **ON** to deny user access to specific web sites.
3. Click on the add icon and enter either a full **URL** address or just a **Keyword**.



Parental Control > Managed Sites > Add Blocked Domain

Add Site to be Blocked

URL: http://

Always Block? OFF

Set Block Time

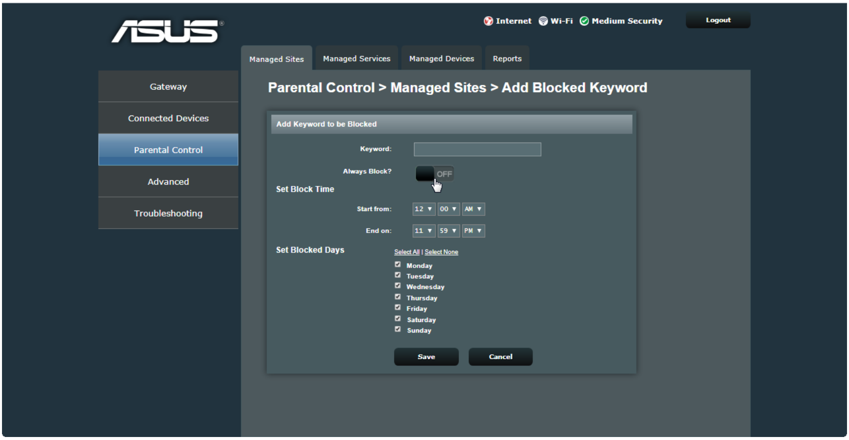
Start from: 12 ▼ 00 ▼ AM ▼

End on: 11 ▼ 59 ▼ PM ▼

Set Blocked Days

Select All | Select None

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday



Parental Control > Managed Sites > Add Blocked Keyword

Add Keyword to be Blocked

Keyword:

Always Block? OFF

Set Block Time

Start from: 12 00 AM

End on: 11 59 PM

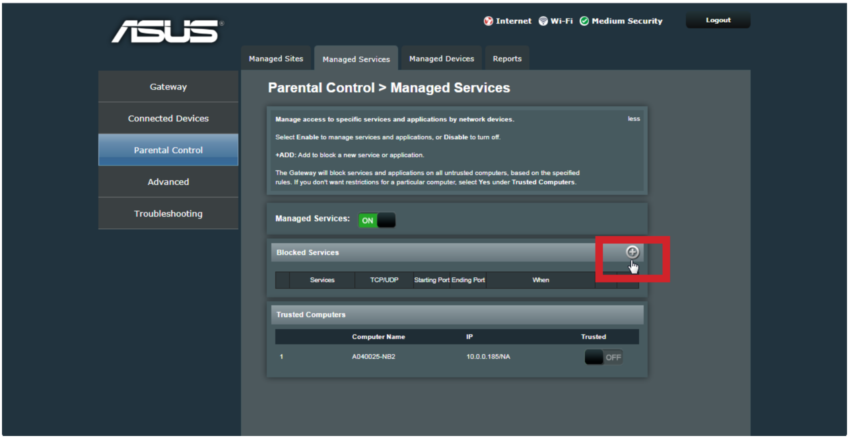
Set Blocked Days

Select All | Select None

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

4. Select the time rule on the screen to set the blocking schedule.
5. Move the slider to **ON** to activate the **Always Block** if you like to.
6. When done, click **Save**.
7. To allow a connected client to access Internet web sites, move the slider to **ON** on the **Trusted Computers**.

4.2.2 Managed Services



Parental Control > Managed Services

Manage access to specific services and applications by network devices.

Select Enable to manage services and applications, or Disable to turn off.

+ADD: Add to block a new service or application.

The Gateway will block services and applications on all untrusted computers, based on the specified rules. If you don't want restrictions for a particular computer, select Yes under Trusted Computers.

Managed Services: ON

Blocked Services

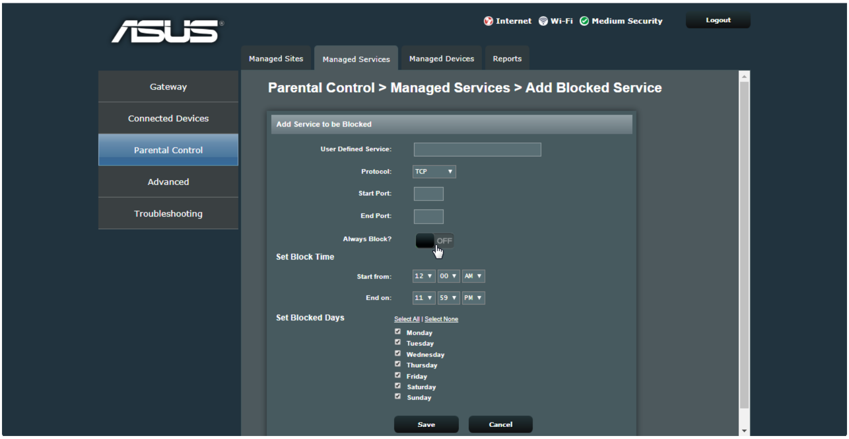
	Services	TCP/UDP	Starting Port	Ending Port	When		

Trusted Computers

	Computer Name	IP	Trusted
1	A040025-NB2	10.0.0.185/NA	OFF

To set up the Managed Services:

1. From the navigation panel, go to **Parental Control > Managed Services** tab.
2. Move the slider to **ON** to block application services.
3. Click on the add icon, define the appropriate rule settings of service name, protocols and port numbers for client PC services.



Parental Control > Managed Services > Add Blocked Service

Add Service to be Blocked

User Defined Service:

Protocol: TCP

Start Port:

End Port:

Always Block? OFF

Set Block Time

Start from: 12 00 AM

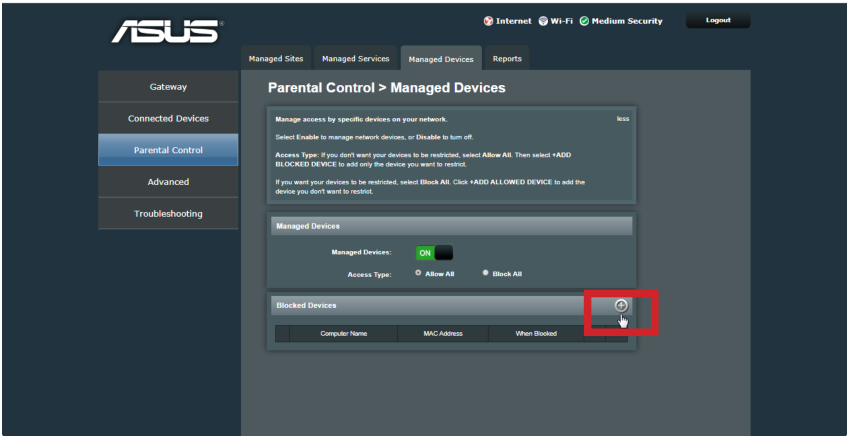
End on: 11 59 PM

Set Blocked Days

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

4. Select the time rule on the screen to set the blocking schedule.
5. Move the slider to **ON** to activate the **Always Block** if you like to.
6. When done, click **Save**.
7. To allow a connected client to access Internet web sites, move the slider to **ON** on the **Trusted Computers**.

4.2.3 Managed Devices



Parental Control > Managed Devices

Manage access by specific devices on your network. less

Select Enable to manage network devices, or Disable to turn off.

Access Type: If you don't want your devices to be restricted, select Allow All. Then select +ADD BLOCKED DEVICE to add only the device you want to restrict.

If you want your devices to be restricted, select Block All. Click +ADD ALLOWED DEVICE to add the device you don't want to restrict.

Managed Devices

Managed Devices: ON

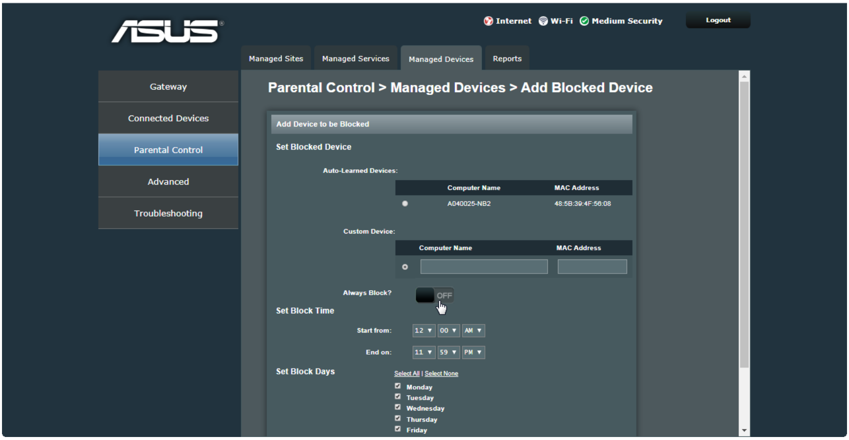
Access Type: ○ Allow All ● Block All

Blocked Devices

	Computer Name	MAC Address	When Blocked		

To set up the Managed Devices:

1. From the navigation panel, go to **Parental Control > Managed Devices** tab.
2. Move the slider to **ON** to enable the access control of your network clients.
3. Select the **Access Type** to **Allow All** or **Block All** for allowing or denying your client devices to access your network.
4. Click on the add icon to add a client device who will be denied access to your network. You may also key in the client's MAC address in the Client MAC Address column.



Parental Control > Managed Devices > Add Blocked Device

Add Device to be Blocked

Set Blocked Device

Auto-Learned Devices:

	Computer Name	MAC Address
●	A040025-NB2	48:5B:39:4F:56:08

Custom Device:

	Computer Name	MAC Address
○		

Always Block? OFF

Set Block Time

Start from: 12 ▾ 00 ▾ AM ▾

End on: 11 ▾ 59 ▾ PM ▾

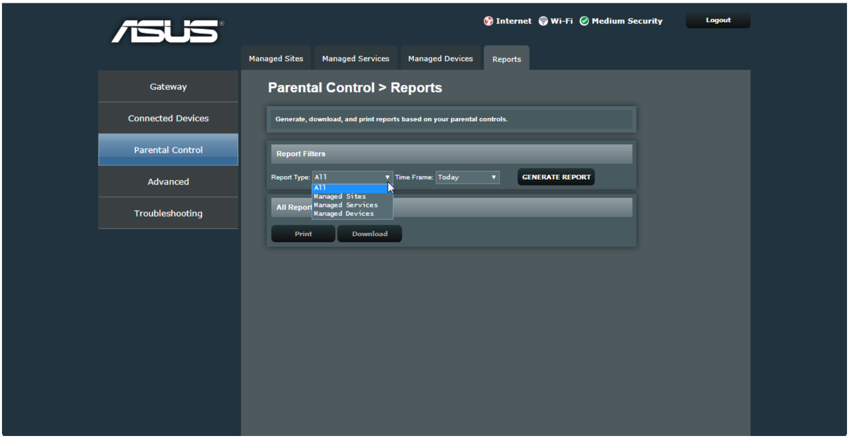
Set Block Days

Select All | Select None

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday

5. Select the time rule on the screen to set the blocking schedule.
6. Move the slider to **ON** to activate the **Always Block** if you like to.
7. When done, click **Save**.

4.2.4 Reports



Parental Control > Reports

Generate, download, and print reports based on your parental controls.

Report Filters

Report Type: All

Time Frame: Today

To view the firewall filtering status:

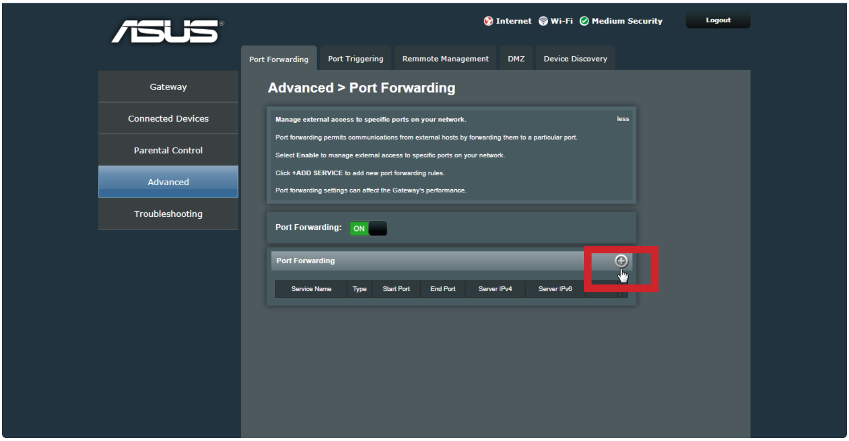
1. From the navigation panel, go to **Parental Control** > **Reports** tab.
2. Select the access control types and time in the **Report Filters** field and click on the **GENERATE REPORT** button to display descriptive list of filtering schedule and rules defined.
3. Click on the **Print**/**Download** button to print/download the reports.

5 Configuring the Advanced Settings

5.1 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.

NOTE: When port forwarding is enabled, the ASUS router blocks unsolicited inbound traffic from the Internet and only allows replies from outbound requests from the LAN. The network client does not have access to the Internet directly, and vice versa.



Advanced > Port Forwarding

Manage external access to specific ports on your network.

Port forwarding permits communications from external hosts by forwarding them to a particular port.

Select **Enable** to manage external access to specific ports on your network.

Click **+ADD SERVICE** to add new port forwarding rules.

Port forwarding settings can affect the Gateway's performance.

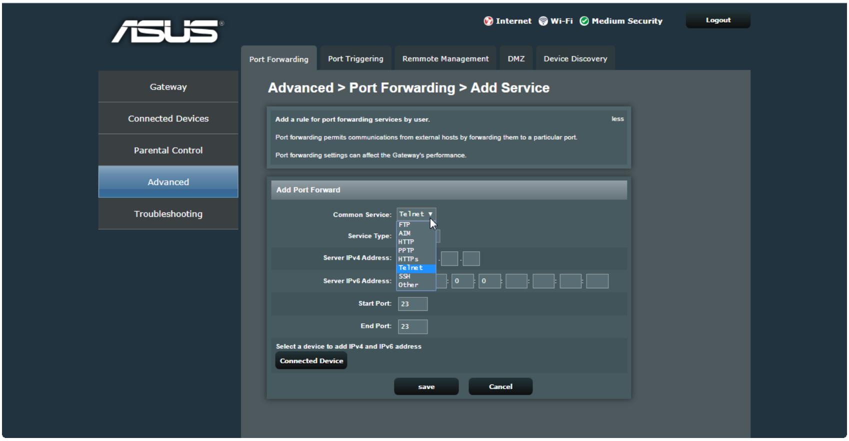
Port Forwarding: ON

Port Forwarding

Service Name	Type	Start Port	End Port	Server IPv4	Server IPv6

To set up Port Forwarding:

1. From the navigation panel, go to **Advanced > Port Forwarding** tab.
2. Move the slider to **ON** to enable **Port Forwarding**.
3. Click on the add icon and configure the following settings below.



Advanced > Port Forwarding > Add Service

Add a rule for port forwarding services by user.

Port forwarding permits communications from external hosts by forwarding them to a particular port.

Port forwarding settings can affect the Gateway's performance.

Add Port Forward

Common Service: Telnet

Service Type:

Server IPv4 Address:

Server IPv6 Address: 0 : 0

Start Port: 23

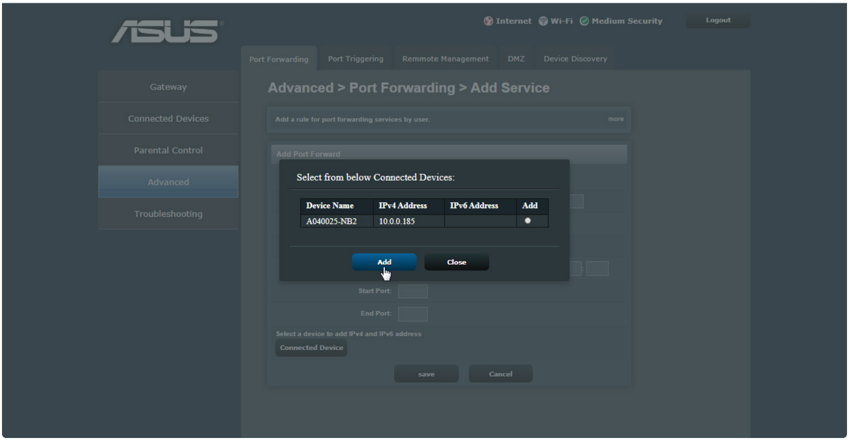
End Port: 23

Select a device to add IPv4 and IPv6 address

- **Common Service**: Select an external virtual server service. The router redirects the external service request to the appropriate server.
- **Service Type**: Determine which type of service you want to access.
- **Server IPv4 Address**: Key in the client's LAN IPv4 address.
- **Server IPv6 Address**: Key in the client's LAN IPv6 address.

NOTE: Internet users can access the service they need at the local address to which you redirect them.

- **Start Port**: Enter the starting port number depending on the requested service.
- **End Port**: Enter the end port number depending on the requested service.
- **Select a device to add IPv4 and IPv6 address**: Click on the **Connected Device** button and click **Add** to easily set up the local LAN IP address.



Advanced > Port Forwarding > Add Service

Add a rule for port forwarding services by user.

Add Port Forward

Select from below Connected Devices:

Device Name	IPv4 Address	IPv6 Address	Add
A040025-NB2	10.0.0.185		●

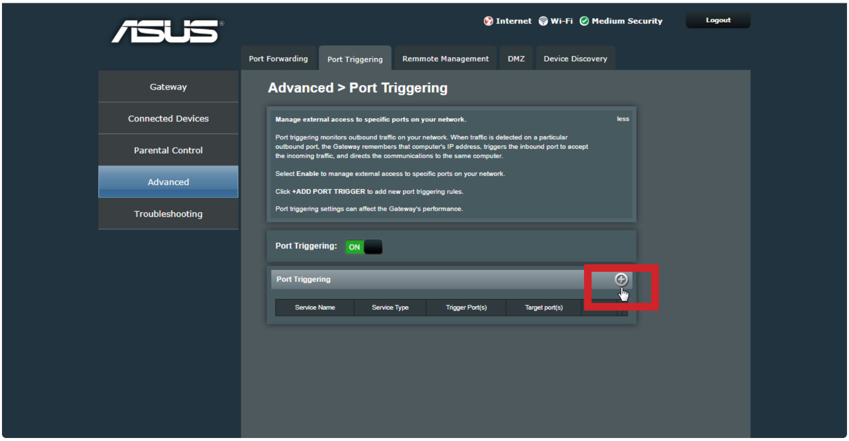
Select a device to add IPv4 and IPv6 address

- When done, click **Save**.

5.2 Port Triggering

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.



Advanced > Port Triggering

Manage external access to specific ports on your network.

Port triggering monitors outbound traffic on your network. When traffic is detected on a particular outbound port, the Gateway remembers that computer's IP address, triggers the inbound port to accept the incoming traffic, and directs the communications to the same computer.

Select **Enable** to manage external access to specific ports on your network.

Click **+ADD PORT TRIGGER** to add new port triggering rules.

Port triggering settings can affect the Gateway's performance.

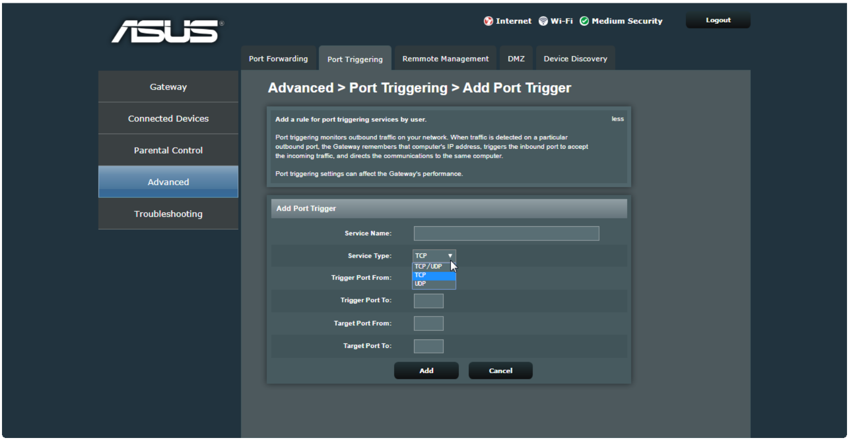
Port Triggering: ON

Port Triggering

Service Name	Service Type	Trigger Port(s)	Target port(s)

To set up Port Triggering:

1. From the navigation panel, go to **Advanced > Port Triggering** tab.
2. Move the slider to **ON** to enable **Port Trigger**.
3. Configure the following settings below.



Advanced > Port Triggering > Add Port Trigger

Add a rule for port triggering services by user.

Port triggering monitors outbound traffic on your network. When traffic is detected on a particular outbound port, the Gateway remembers that computer's IP address, triggers the inbound port to accept the incoming traffic, and directs the communications to the same computer.

Port triggering settings can affect the Gateway's performance.

Add Port Trigger

Service Name:

Service Type: TCP

Trigger Port From:

Trigger Port To:

Target Port From:

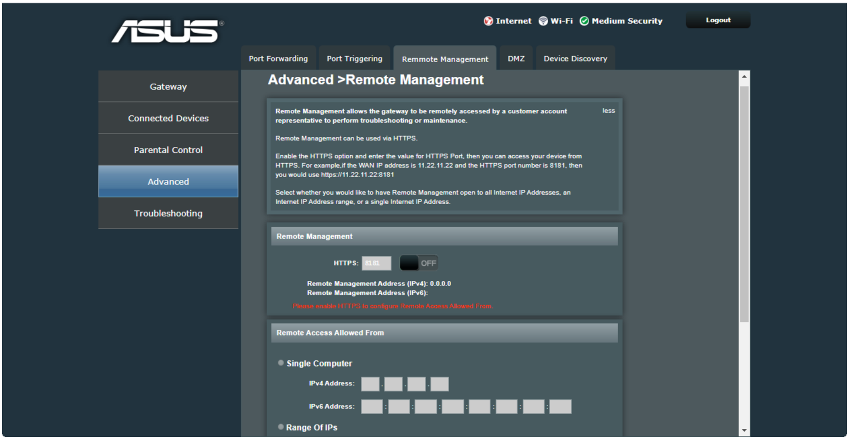
Target Port To:

- **Service Name**: Enter a short name or description for the service.
- **Service Type**: Select the protocol, TCP, or UDP.
- **Trigger Port From**: Specify a starting trigger port number to open the incoming port.
- **Trigger Port To**: Specify an end trigger port number to open the incoming port.
- **Target Port From**: Specify a starting incoming port number to receive inbound data from the Internet.
- **Target Port To**: Specify an end incoming port number to receive inbound data from the Internet.

4. When done, click **Add**.

5.3 Remote Management

HTTPS can be restricted to a subset of IP addresses. The router administrator can define a known PC, single IP address or range of IP addresses that are allowed to access the GUI with HTTPS. The opened port for SSL traffic can be changed from the default of 8181 at the same time as defining the allowed remote management IP address range.



Advanced >Remote Management

Remote Management allows the gateway to be remotely accessed by a customer account representative to perform troubleshooting or maintenance.

Remote Management can be used via HTTPS.

Enable the HTTPS option and enter the value for HTTPS Port, then you can access your device from HTTPS. For example,if the WAN IP address is 11.22.11.22 and the HTTPS port number is 8181, then you would use https://11.22.11.22:8181

Select whether you would like to have Remote Management open to all Internet IP Addresses, an Internet IP Address range, or a single Internet IP Address.

Remote Management

HTTPS: 8181 OFF

Remote Management Address (IPv4): 0.0.0.0
Remote Management Address (IPv6):

Please enable HTTPS to configure Remote Access Allowed From.

Remote Access Allowed From

○ Single Computer

IPv4 Address: ___ . ___ . ___ . ___

IPv6 Address: ___ : ___ : ___ : ___ : ___ : ___ : ___ : ___

○ Range Of IPs

To set up remote access to your router:

1. From the navigation panel, go to **Advanced > Remote Management** tab.
2. Move the slider to **ON** to allow authorized users to access this GUI over the Internet. By default, remote management over the Internet is disabled.
3. Set the port number for remote management over **HTTPS**.
4. Key in the **IPv4 Address/IPv6 Address** of the PC which is given remote management permission if you select Single Computer.
5. Enter a range of IP addresses if you select **Range of IPs** for the access type.

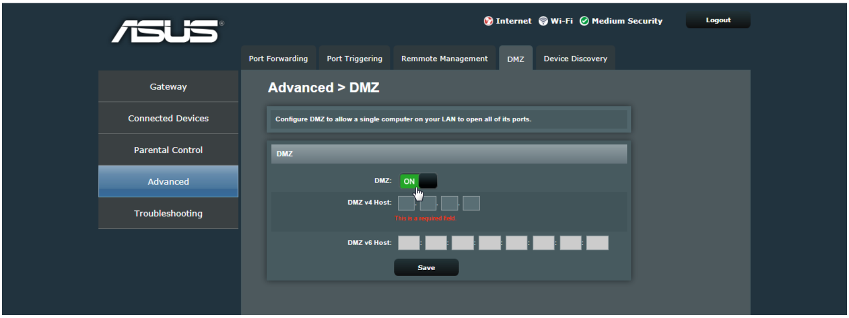
5.4 DMZ

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 email 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.



Advanced > DMZ

Configure DMZ to allow a single computer on your LAN to open all of its ports.

DMZ

DMZ: ON

DMZ v4 Host: . . .

This is a required field.

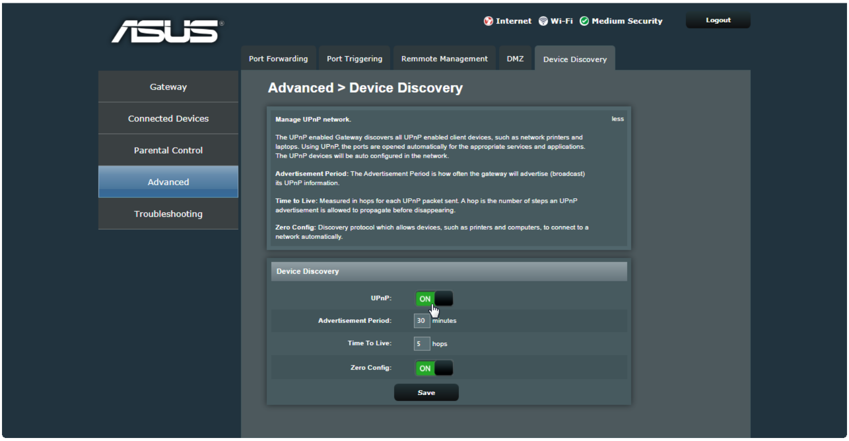
DMZ v6 Host: : : : : : : :

To set up DMZ:

1. From the navigation panel, go to **Advanced** > **DMZ** tab.
2. Move the slider to **ON** for using DMZ.
3. Key in the IPv4 Host Address/IPv6 Host Address that will provide the DMZ service and be exposed on the Internet. Ensure that the server client has a static IP address.
4. When done, click **Save**.

5.5 Device Discovery

Device Discovery provides UPnP (Universal Plug and Play) function. It 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.



Advanced > Device Discovery

Manage UPnP network.

The UPnP enabled Gateway discovers all UPnP enabled client devices, such as network printers and laptops. Using UPnP, the ports are opened automatically for the appropriate services and applications. The UPnP devices will be auto configured in the network.

Advertisement Period: The Advertisement Period is how often the gateway will advertise (broadcast) its UPnP information.

Time to Live: Measured in hops for each UPnP packet sent. A hop is the number of steps an UPnP advertisement is allowed to propagate before disappearing.

Zero Config: Discovery protocol which allows devices, such as printers and computers, to connect to a network automatically.

Device Discovery

UPnP: ON

Advertisement Period: 30 minutes

Time To Live: 5 hops

Zero Config: ON

To set up Device Discovery:

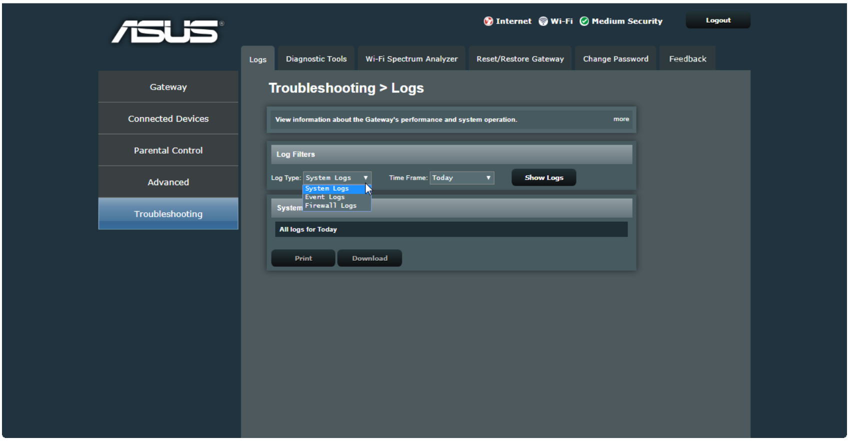
1. From the navigation panel, go to **Advanced > Device Discovery** tab.
2. Move the slider to **ON** for using UPnP.

3. Configure the following settings below.
    - **Advertisement Period**: This is the period (in minutes) of how often this wireless router will broadcast its UPnP information to all devices within its range.
    - **Time to Live**: This is the number (in hops) of steps a packet is allowed to propagate before being discarded.
    - **Zero Config**: Move the slider to **ON** to allow for automatic discovery and configuration of a new network device.
4. When done, click **Save**.

6 Troubleshooting

6.1 Logs

The **Logs** configuration allows you to set the display category and time for monitoring the system activity.



Troubleshooting > Logs

View information about the Gateway's performance and system operation.

Log Type: System Logs

Time Frame: Today

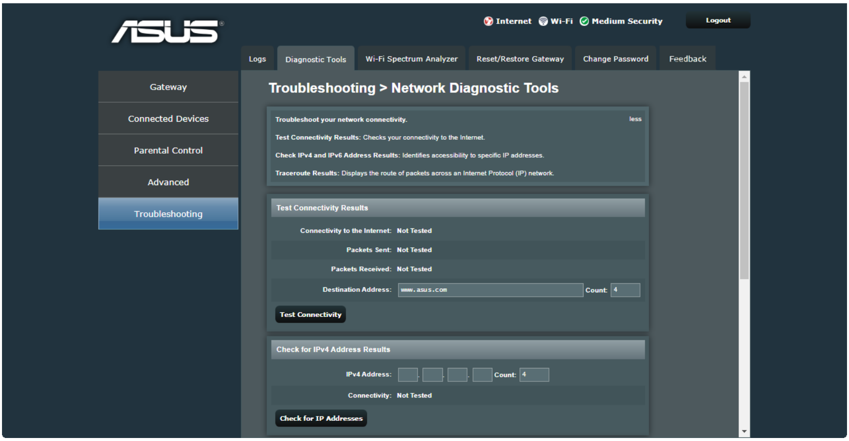
All logs for Today

To view the system log information:

1. From the navigation panel, go to **Troubleshooting** > **Logs** tab.
2. Select the log types and time in the **Log Filters** field, and click on the **Show Logs** button to display a list of filtering type and activity time defined.
3. Click on the **Print**/**Download** button to print/download the log reports.

6.2 Diagnostic Tools

This tool allows you to test Internet connection status, ping test of network clients, and analyze network traffic.



Troubleshooting > Network Diagnostic Tools

Troubleshoot your network connectivity.

Test Connectivity Results: Checks your connectivity to the Internet.

Check IPv4 and IPv6 Address Results: Identifies accessibility to specific IP addresses.

Traceroute Results: Displays the route of packets across an Internet Protocol (IP) network.

Test Connectivity Results

Connectivity to the Internet: Not Tested

Packets Sent: Not Tested

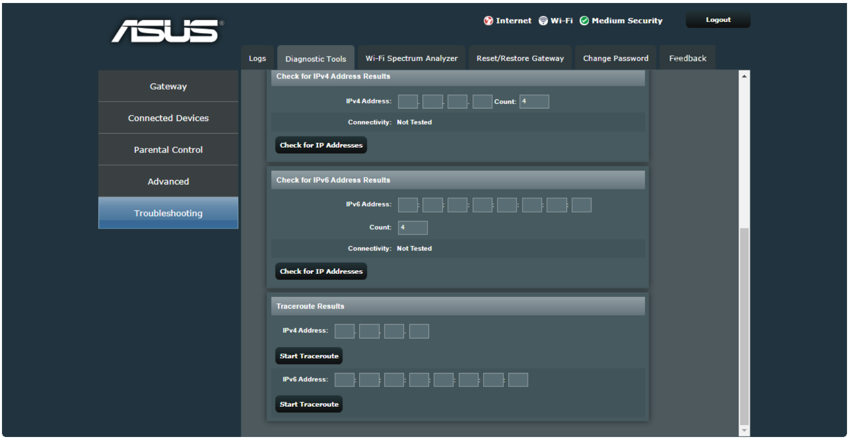
Packets Received: Not Tested

Destination Address: www.asus.com Count: 4

Check for IPv4 Address Results

IPv4 Address: . . . Count: 4

Connectivity: Not Tested



Check for IPv4 Address Results

IPv4 Address: . . . Count: 4

Connectivity: Not Tested

Check for IPv6 Address Results

IPv6 Address: : : : : : : :

Count: 4

Connectivity: Not Tested

Traceroute Results

IPv4 Address: . . .

IPv6 Address: : : : : : : :

To test and display your Internet connection status:

1. From the navigation panel, go to **Troubleshooting > Diagnostic Tools** tab.
2. Click on the **Test Connectivity** button to retrieve information and display the packet contents of the Internet connection.

To check the IP Address of your network clients:

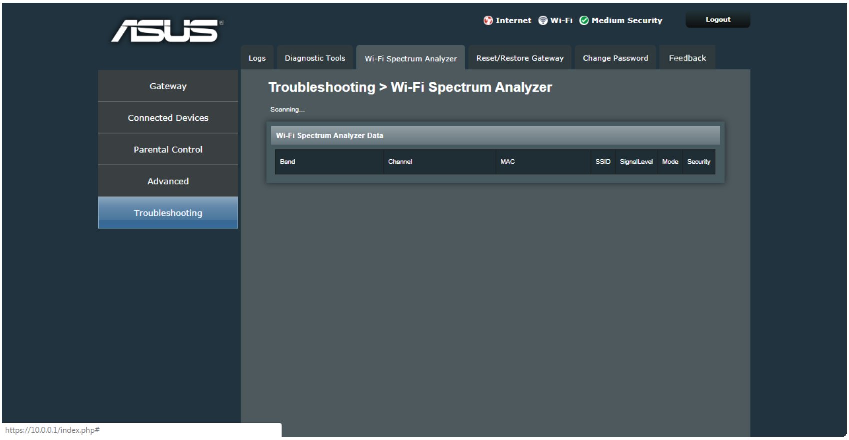
1. From the navigation panel, go to **Troubleshooting > Diagnostic Tools** tab.
2. Enter the IP address in the **Check for IPv4 Address Results/ Check for IPv6 Address Results** fields.
3. Click the **check for IP Address** button to execute the ping test and check the Internet connection.

To trace the route of captured packets pass through your network:

1. Enter the destination **IPv4 Address/ IPv6 Address** in the **Traceroute Results** field.
2. Click the **Start Traceroute** button to display all the gateways/ routers present between the destination IP address and the router.

6.3 Wi-Fi Spectrum Analyzer

Wi-Fi Spectrum Analyzer is an ASUS WLAN device discovery utility that detects an ASUS router device, and allows you to configure the wireless networking settings.



Troubleshooting > Wi-Fi Spectrum Analyzer

Scanning...

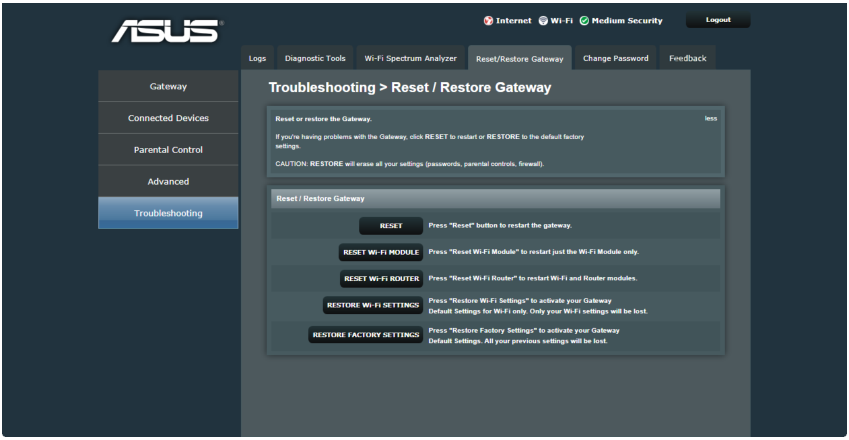
Wi-Fi Spectrum Analyzer Data

Band	Channel	MAC	SSID	SignalLevel	Mode	Security

To use the Device Discovery for displaying available wireless access points (AP) within your network range:

1. From the navigation panel, go to **Troubleshooting > Wi-Fi Spectrum Analyzer** tab.
2. Choose one of scanned AP's to connect to by clicking on the button on the screen for Wi-Fi connectivity.

6.4 Reset/Restore Gateway



Troubleshooting > Reset / Restore Gateway

Reset or restore the Gateway.

If you're having problems with the Gateway, click RESET to restart or RESTORE to the default factory settings.

CAUTION: RESTORE will erase all your settings (passwords, parental controls, firewall).

Reset / Restore Gateway

Press "Reset" button to restart the gateway.

Press "Reset Wi-Fi Module" to restart just the Wi-Fi Module only.

Press "Reset Wi-Fi Router" to restart Wi-Fi and Router modules.

Press "Restore Wi-Fi Settings" to activate your Gateway Default Settings for Wi-Fi only. Only your Wi-Fi settings will be lost.

Press "Restore Factory Settings" to activate your Gateway Default Settings. All your previous settings will be lost.

The **Reset/Restore Gateway** page allows you to configure your wireless router settings.

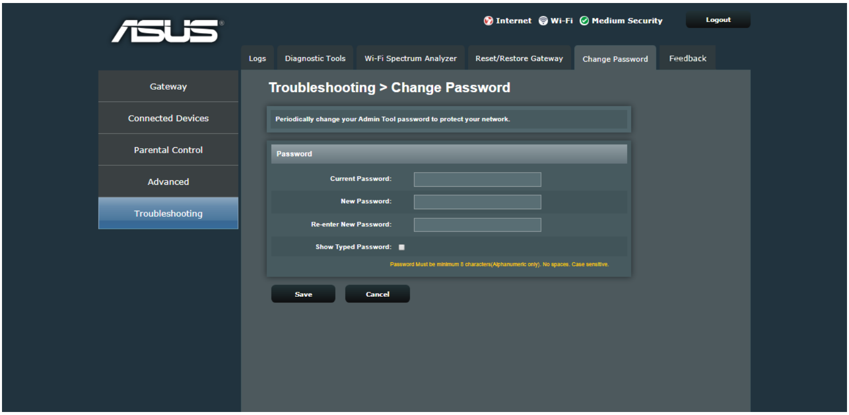
To set up the settings:

1. From the navigation panel, go to **Troubleshooting > Reset/ Restore Gateway** tab.
2. Select the tasks that you want to do:
    - **RESET**: To reboot the router if your router becomes unresponsive.
    - **RESET Wi-Fi MODULE**: To reset the Wi-Fi function of the router. Performing Wi-Fi reset by clicking this button will not change the Wi-Fi settings back to the factory default settings.

- **RESET Wi-Fi ROUTER**: To reset the Wi-Fi and Router functions of the router. Performing a reset by clicking this button will not change the configuration settings back to the factory default settings.
- **RESTORE Wi-Fi SETTINGS**: To reset the Wi-Fi settings of your router back to the default settings. All of the user-defined Wi-Fi settings will be lost.
- **RESTORE FACTORY SETTINGS**: To reset the router back to the original default settings. All of the user configurations and settings will be lost.

6.5 Change Password

You can change the password to log into the router's management interface by entering a new password.



Troubleshooting > Change Password

Periodically change your Admin Tool password to protect your network.

Password

Current Password:

New Password:

Re-enter New Password:

Show Typed Password: □

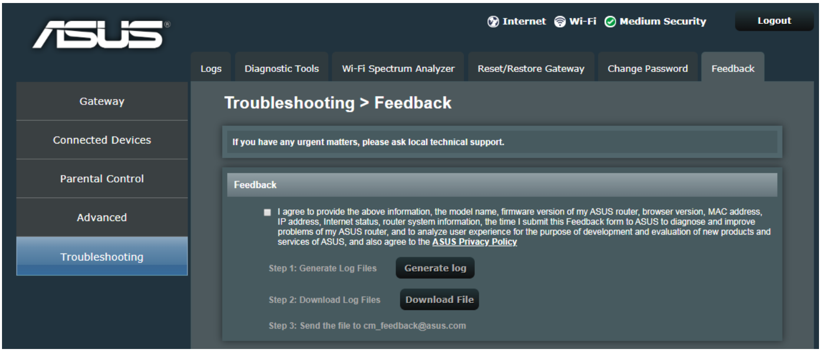
Password Must be minimum 8 characters(Alphanumeric only). No spaces. Case sensitive.

To change the login password:

1. From the navigation panel, go to **Troubleshooting > Change Password** tab.
2. Type your current login password.

3. Set a new password and type the new password again. Passwords can contain from 8~20 alphanumeric characters (A-Z, 0-9) and are case sensitive.
4. Click the checkbox in the **Show Typed Password** to conceal the password if you like to.
5. When done, click **Save**.

6.6 Feedback



Troubleshooting > Feedback

If you have any urgent matters, please ask local technical support.

Feedback

□ I agree to provide the above information, the model name, firmware version of my ASUS router, browser version, MAC address, IP address, Internet status, router system information, the time I submit this Feedback form to ASUS to diagnose and improve problems of my ASUS router, and to analyze user experience for the purpose of development and evaluation of new products and services of ASUS, and also agree to the **ASUS Privacy Policy**

Step 1: Generate Log Files

Step 2: Download Log Files

Step 3: Send the file to cm_feedback@asus.com

If your router does not connect to the Internet, do the following:

1. From the navigation panel, go to **Troubleshooting > Feedback** tab.
2. Click the **Generate log** and **Download File** buttons to save the log files.
3. Send the log files to cm_feedback@asus.com. We will reply to you as soon as possible.