User Guide

CMAX6000

Wireless AX DOCSIS 3.1 Cable Modem Router

ASUS
IN SEARCH OF INCREDIBLE

CMAX6000

First Edition

March 2020

Copyright © 2020 ASUSTeK Computer Inc. All Rights Reserved.

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 5

1.1 Package contents 5

1.2 Your cable modem router 5

1.3 Positioning your router 5

1.4 Product label 5

1.5 Hardware Setup 5

2 Configuring the General Settings 6

2.1 Internet service 6

2.2 Basic Network Setup 7

3 Setting up Your Gateway 8

3.1 At a Glance 8

3.2 Connection 8

3.2.1 Status 9

3.2.2 Cable Network 9

3.2.3 Local IP Configuration 11

3.2.4 Wi-Fi 12

3.3 Firewall 21

3.3.1 IPv4 Firewall / IPv6 Firewall 21

3.4 Software 22

3.5 Hardware 22

3.5.1 Hardware System 22

3.5.2 LAN 23

3.5.3 Wireless 24

3.6 Wizard 24

4 Managing Network Clients 26

4.1 Connected Devices 26

4.1.1 Reserved IP 27

4.2 Setting up Parental Control....28
4.2.1 Managed Sites....29
4.2.2 Managed Services....30
4.2.3 Managed Devices....32
4.2.4 Reports....33

5 Configuring the Advanced Settings....34
5.1 Port Forwarding....34
5.2 Port Triggering....36
5.3 Remote Management....38
5.4 DMZ....39
5.5 Device Discovery....40

6 Troubleshooting....42
6.1 Logs....42
6.2 Diagnostic Tools....43
6.3 Wi-Fi Spectrum Analyzer....44
6.4 Reset/Restore Gateway....45
6.5 Change Password....46
6.6 Feedback....47

1 Getting to know your cable modem router

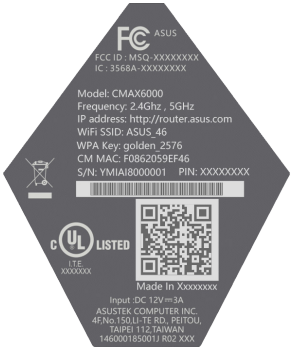
1.1 Package contents

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.



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.

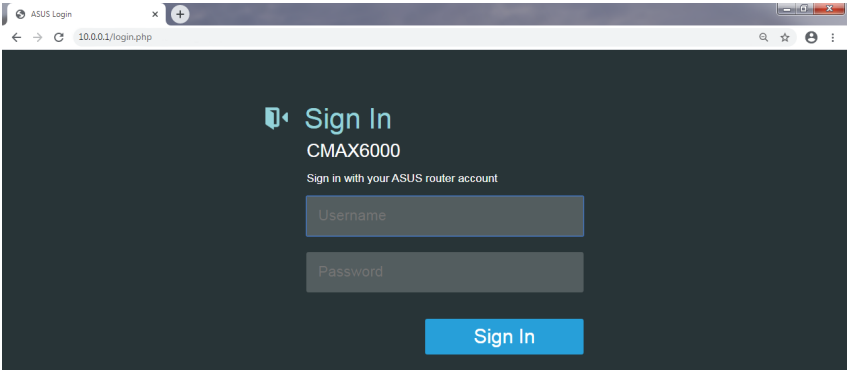
NOTES:

- 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.

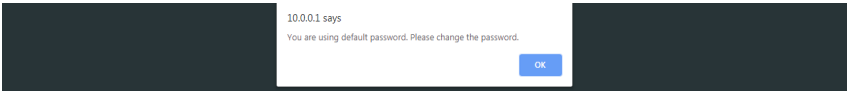
2.2 Basic Network Setup

To set up your CMAX6000 settings:

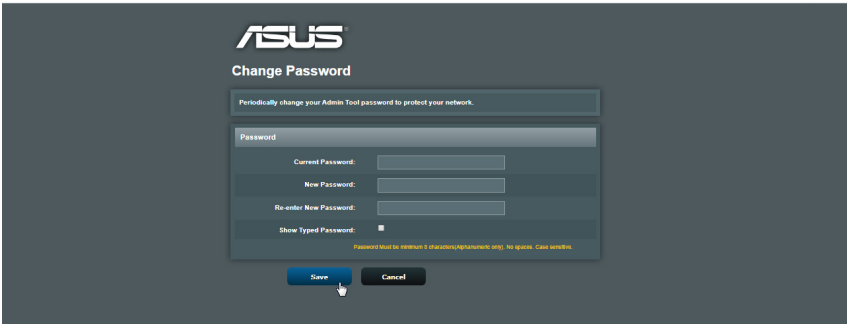
1. Launch your web browser and go to Enter the default IP address, **router.asus.com** or **http://10.0.0.1**.
2. Enter default login name "**admin**" and password "**password**" on the login screen.
3. Click **Sign In** to log into the software configuration interface.



4. Set up a new password when prompted.



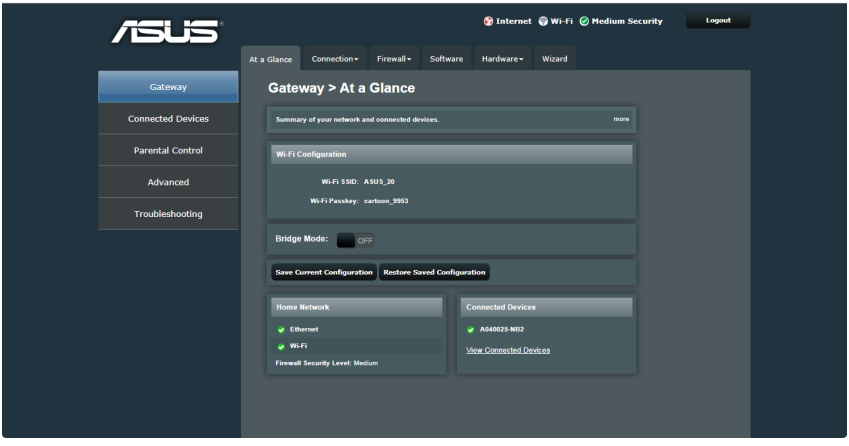
5. Click **Save** and log into the software configuration interface with your new password.



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.

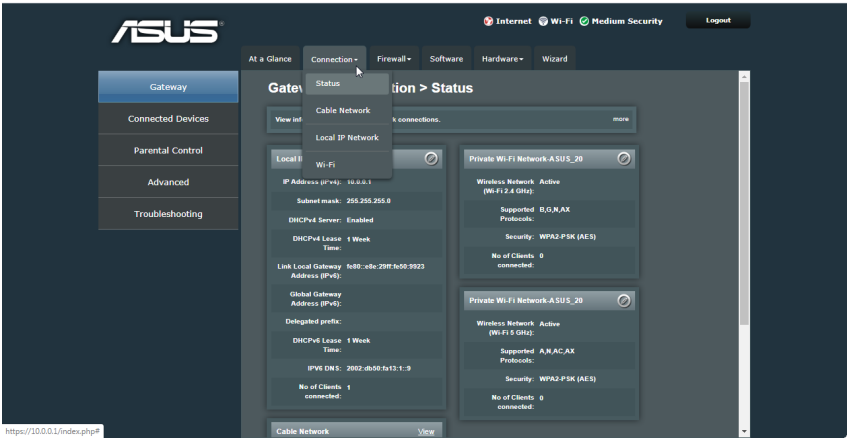


3.2 Connection

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.

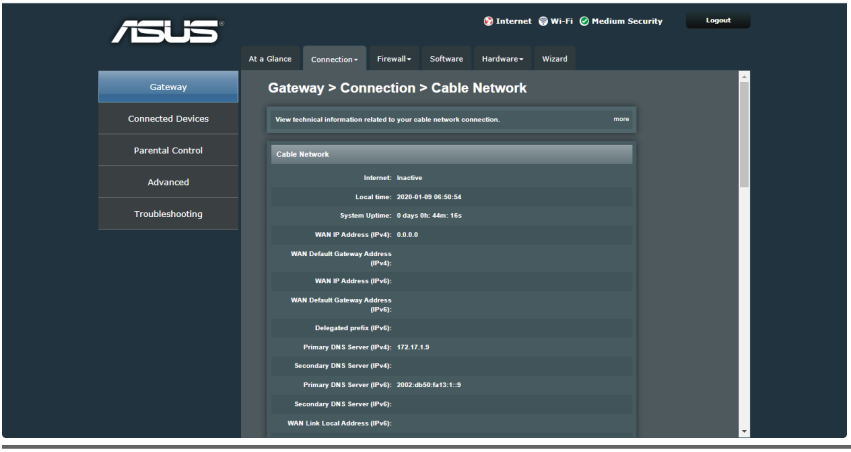


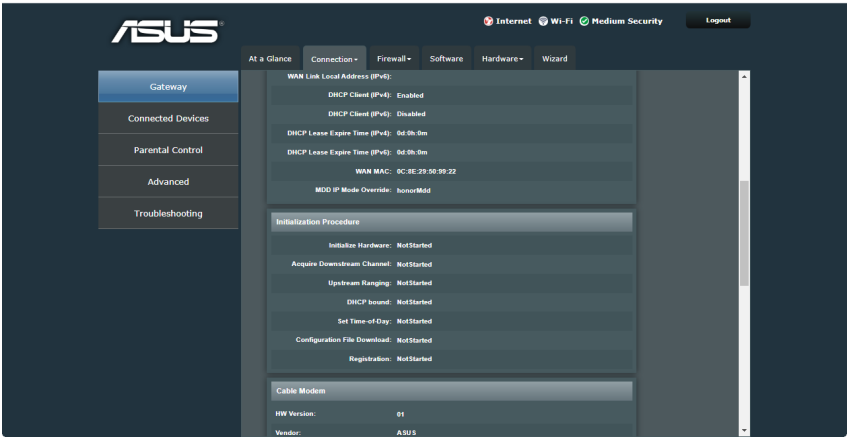
To view your network connection status:

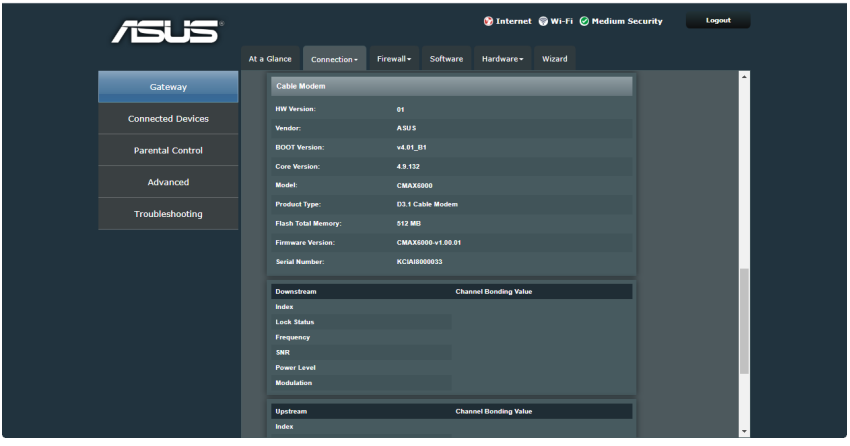
1. From the navigation panel, go to **Gateway** > **Connection** tab.
2. Select **Status** from the dropdown menu of the **Connection** section.

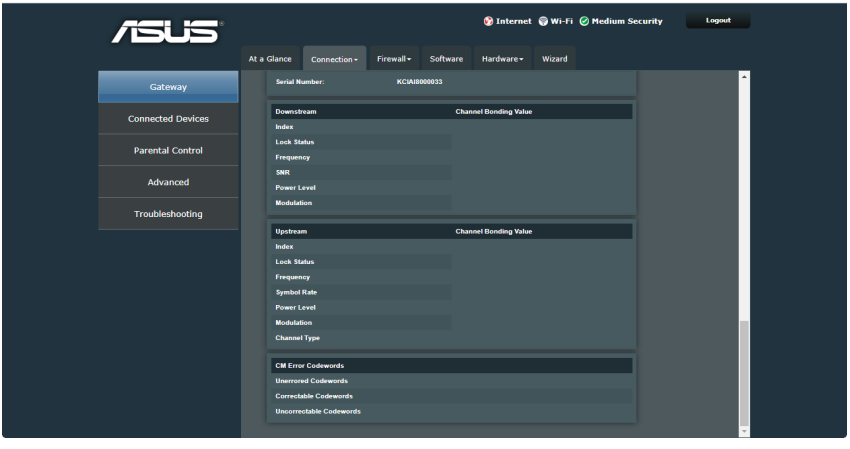
3.2.2 Cable Network

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




Internet
Wi-Fi
Medium Security
Logout
At a Glance
Connection
Firewall
Software
Hardware
Wizard
Gateway
Connected Devices
Parental Control
Advanced
Troubleshooting
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: ASUS


Internet
Wi-Fi
Medium Security
Logout
At a Glance
Connection
Firewall
Software
Hardware
Wizard
Gateway
Connected Devices
Parental Control
Advanced
Troubleshooting
Cable Modem
HW Version: 01
Vendor: ASUS
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

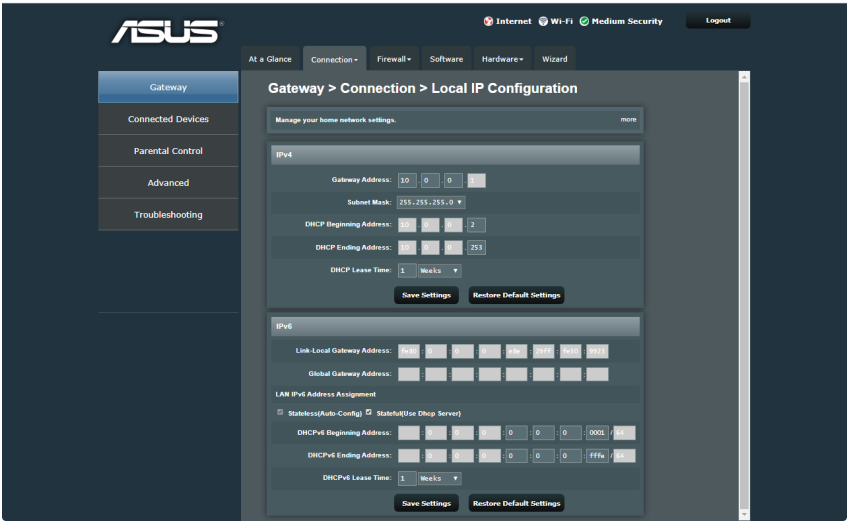

Internet
Wi-Fi
Medium Security
Logout
At a Glance
Connection
Firewall
Software
Hardware
Wizard
Gateway
Connected Devices
Parental Control
Advanced
Troubleshooting
Serial Number: KCIAI8000033
Downstream
Channel Bonding Value
Index
Lock Status
Frequency
SNR
Power Level
Modulation
Upstream
Channel Bonding 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.



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

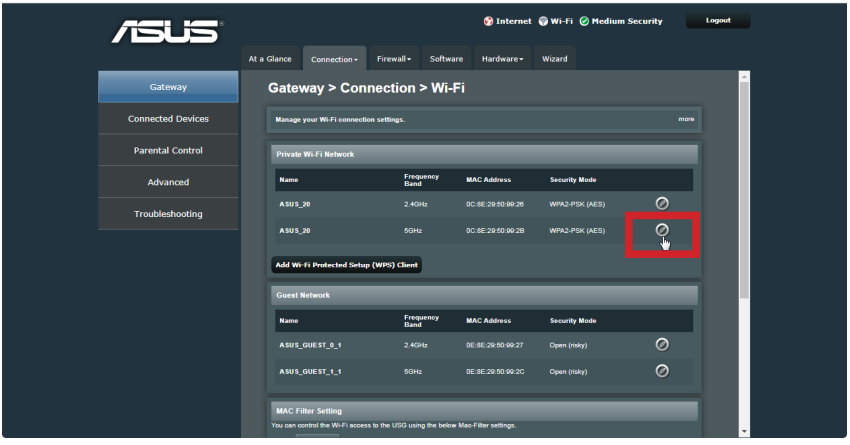
To modify the LAN IP settings:

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.

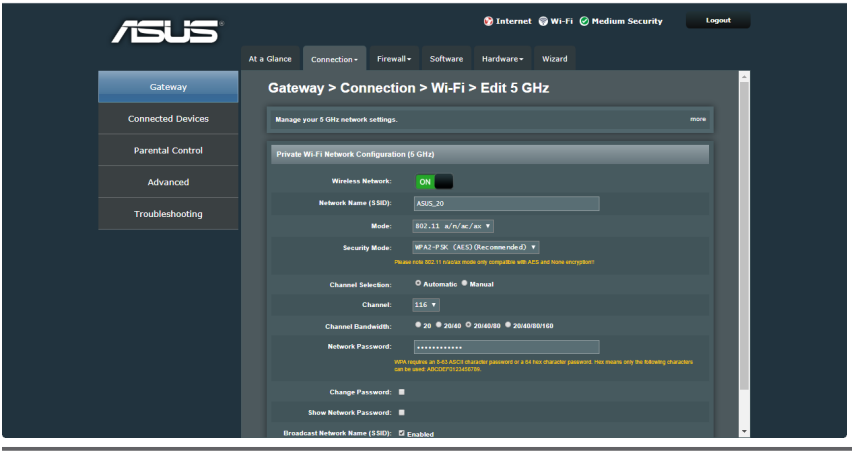
Private Wi-Fi Network



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.



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:

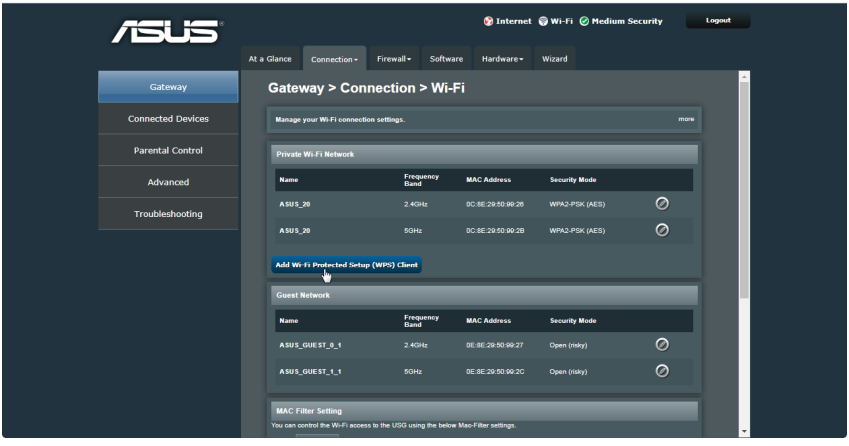
   - **20/40/80 MHz (default)**
   - **20/40/80/160 MHz**

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

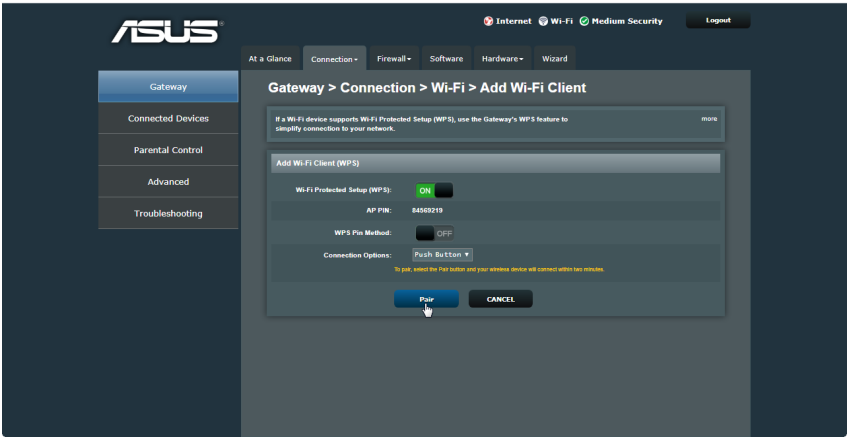
WPS (Wi-Fi Protected Setup) is a wireless security standard that allows you to easily connect devices to a wireless network. You can configure the WPS function via the PIN code or WPS button.

NOTE: Ensure that the devices support WPS.



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:

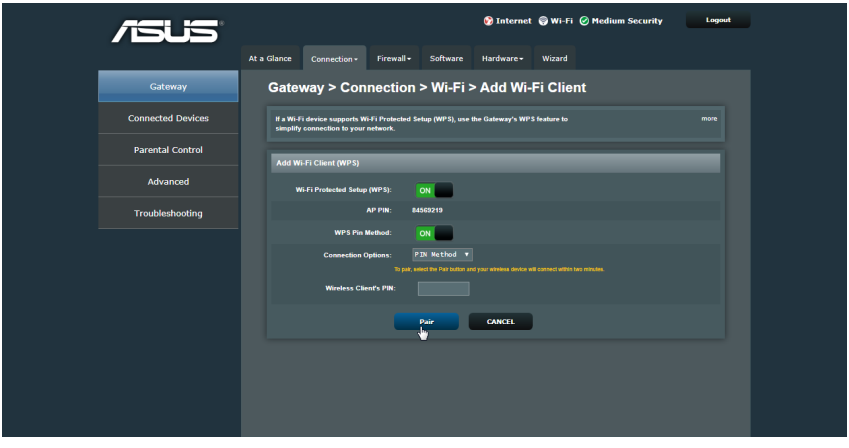


a. Click **Pair** or press the WPS button found at the rear of the wireless router.

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:



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.

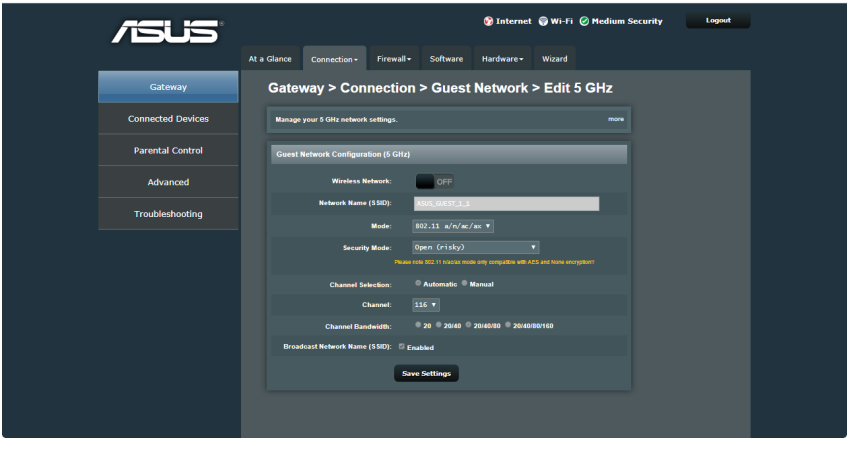
3.2.4.2 Guest Network

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.



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**

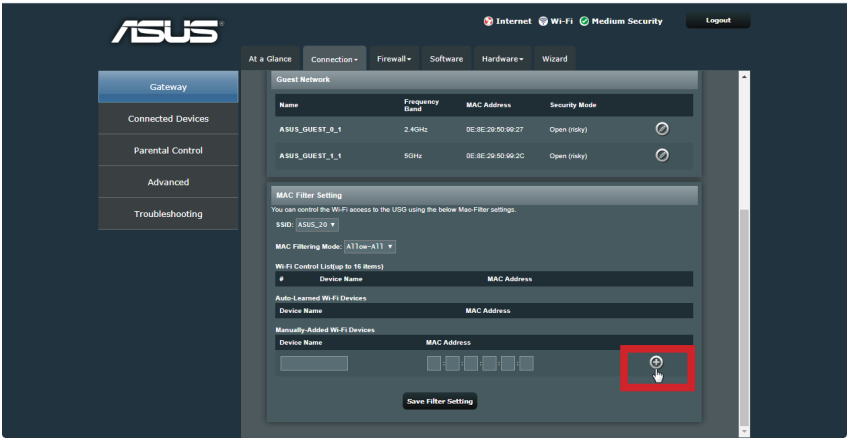
   5 GHz bands:

   - **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.



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**.

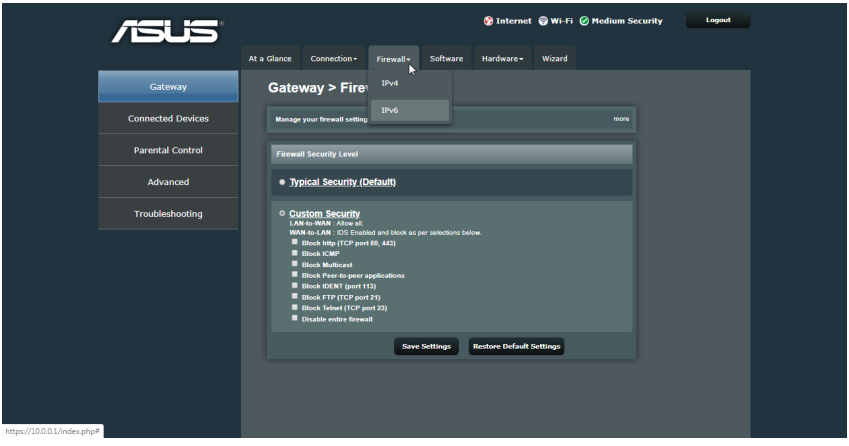
3.3 Firewall

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.

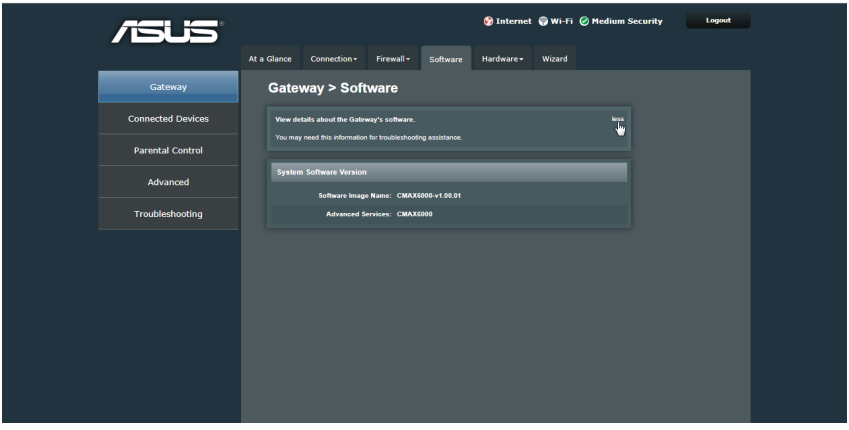


To set up a network service filter by blocking specified services:

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

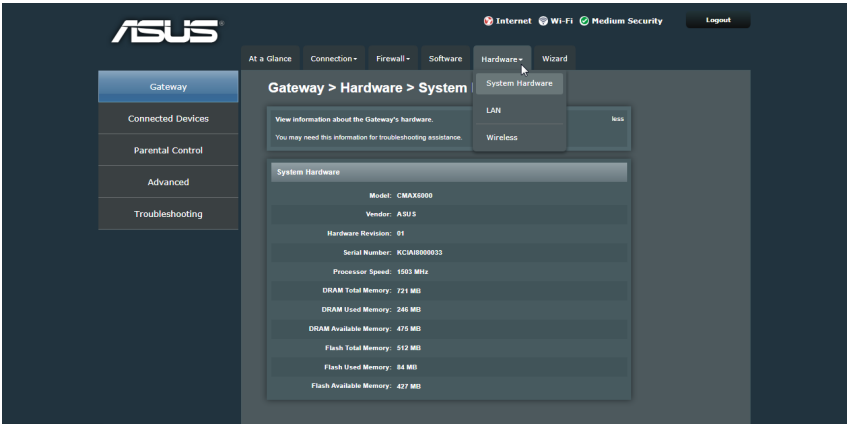
The Software screen displays firmware version number and device model number.



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.

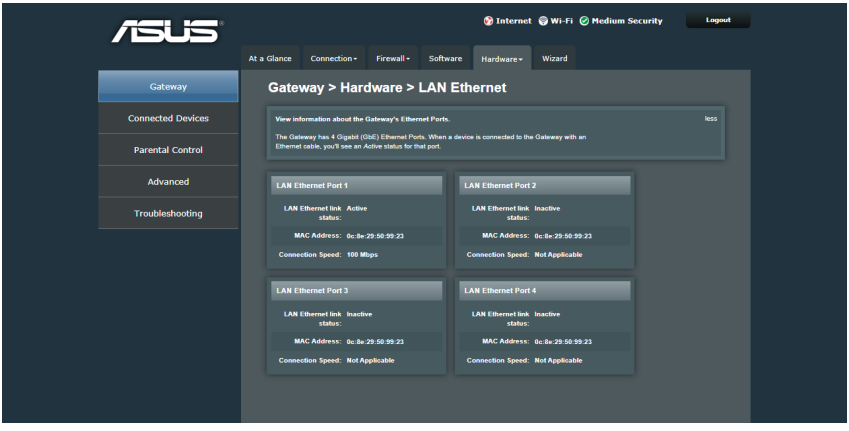


To view your hardware information:

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.

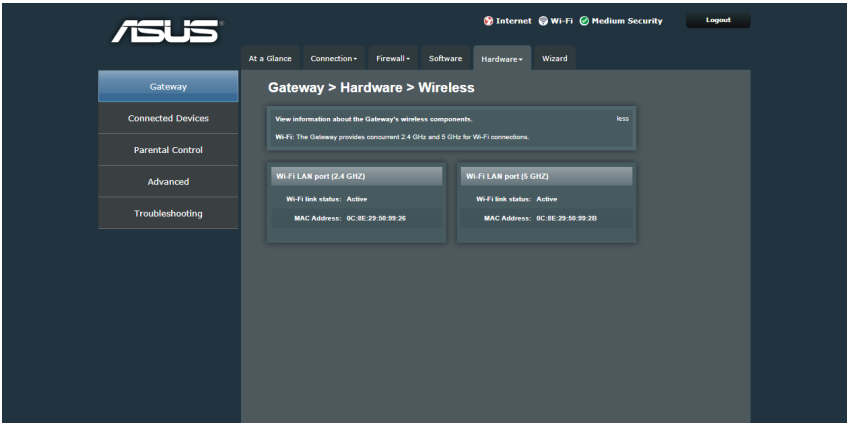


To view your LAN status:

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.

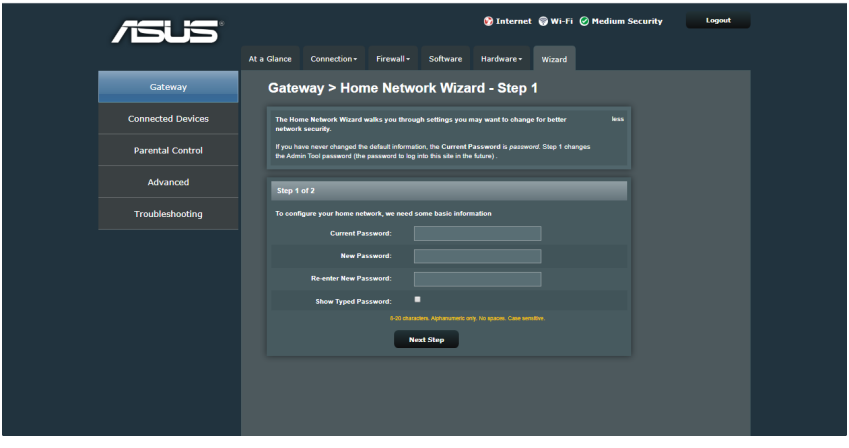


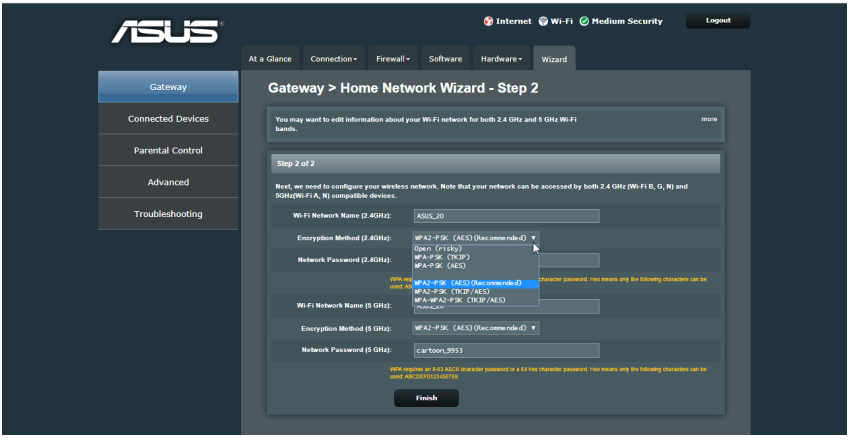
To view your Wireless status:

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.





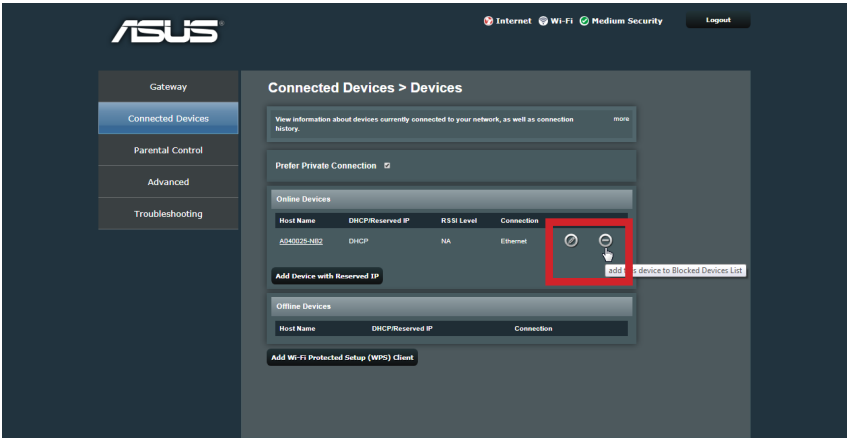
To change your login password and Wi-Fi security:

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

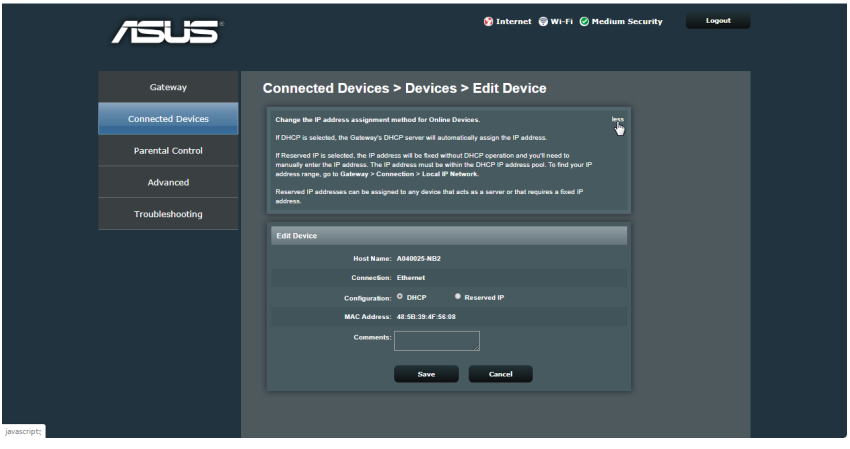
4.1 Connected Devices

The connection status is displayed as the following screen.



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.

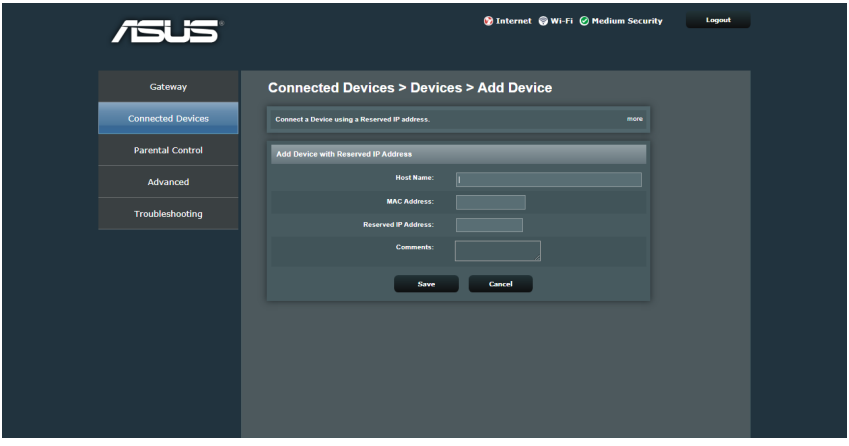


3. When done, click **Save**.

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.



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.

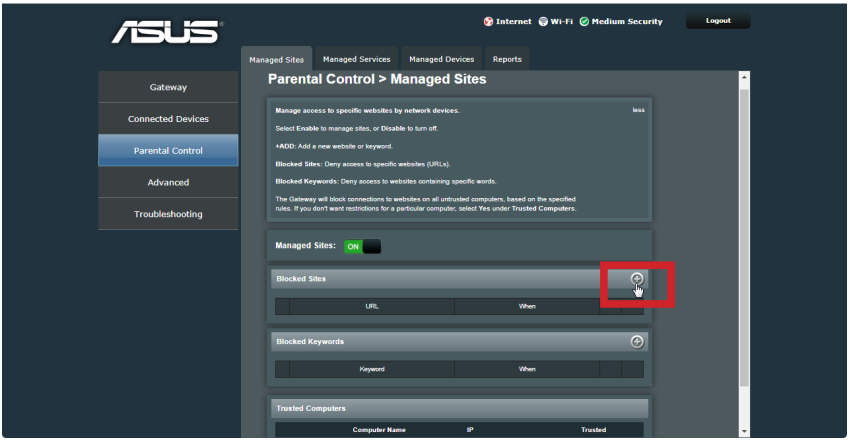
---

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

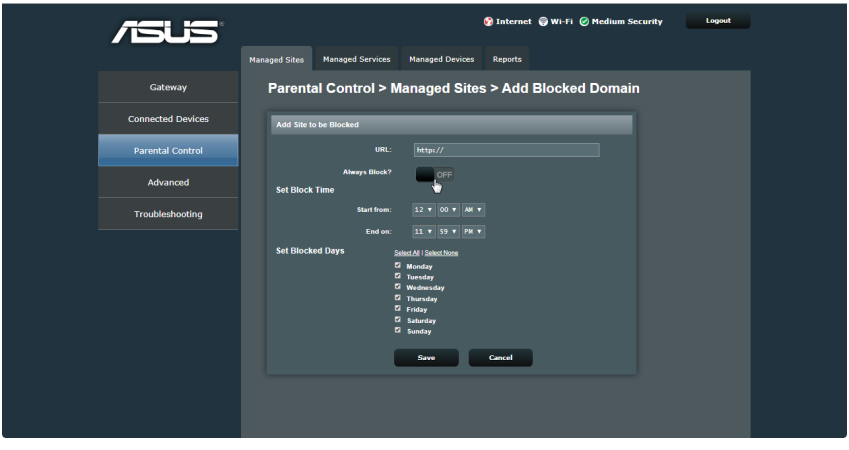
Parental Control allows you to control the Internet access time, web sites and services or applications. Users can set the access limit for a client's network usage and view the control activity.

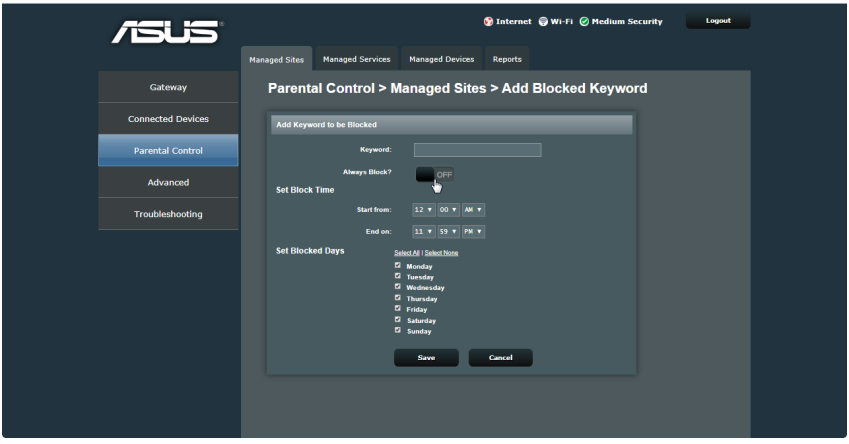
4.2.1 Managed Sites



To set up the Managed Sites:

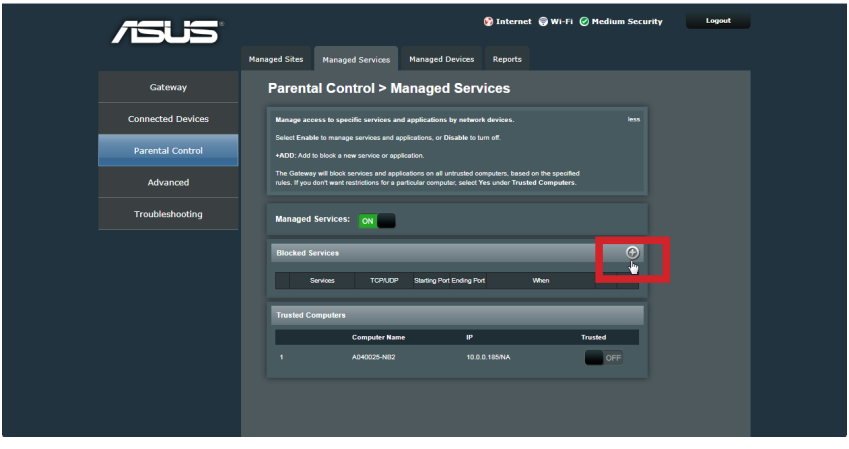
1. From the navigation panel, go to **Parental Control > Managed Sites** tab.
2. Move the slider to **ON** to deny user access to specific web sites.
3. Click on the add icon and enter either a full **URL** address or just a **Keyword**.





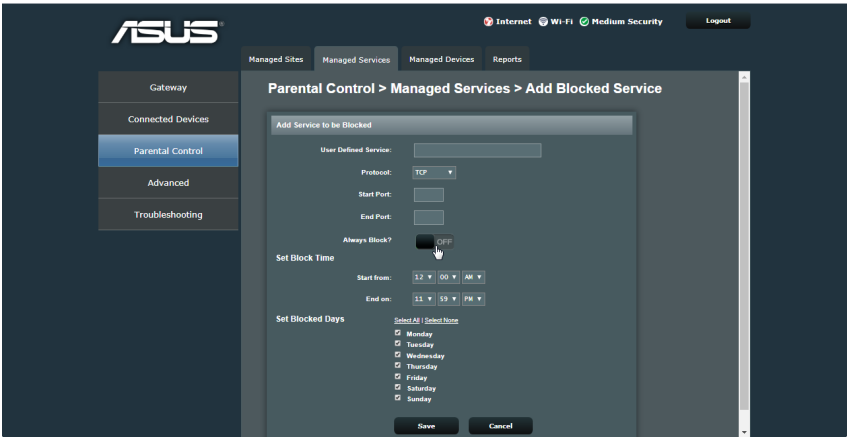
4. Select the time rule on the screen to set the blocking schedule.
5. Move the slider to **ON** to activate the **Always Block** if you like to.
6. When done, click **Save**.
7. To allow a connected client to access Internet web sites, move the slider to **ON** on the **Trusted Computers**.

4.2.2 Managed Services



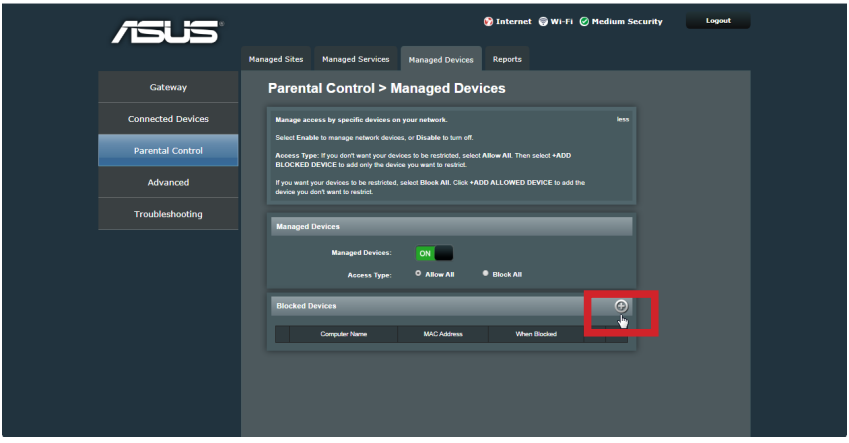
To set up the Managed Services:

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.



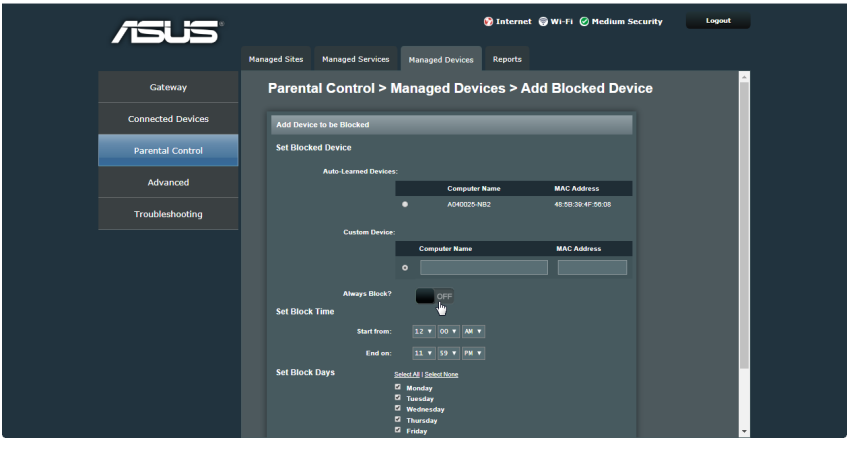
4. Select the time rule on the screen to set the blocking schedule.
5. Move the slider to **ON** to activate the **Always Block** if you like to.
6. When done, click **Save**.
7. To allow a connected client to access Internet web sites, move the slider to **ON** on the **Trusted Computers**.

4.2.3 Managed Devices



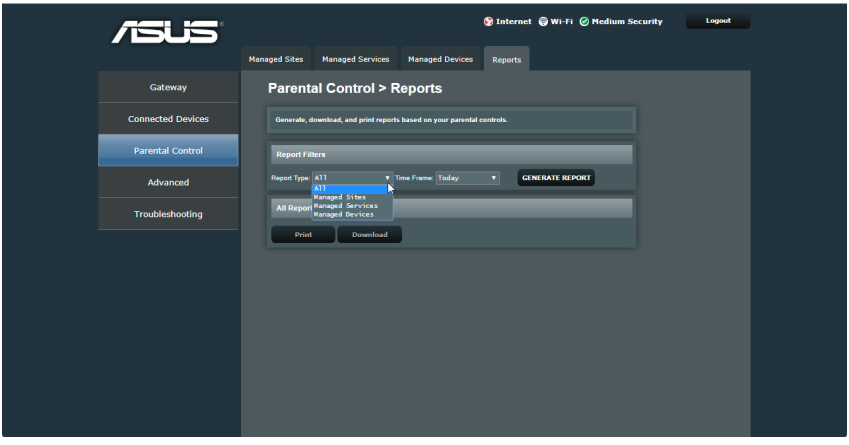
To set up the Managed Devices:

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.



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



To view the firewall filtering status:

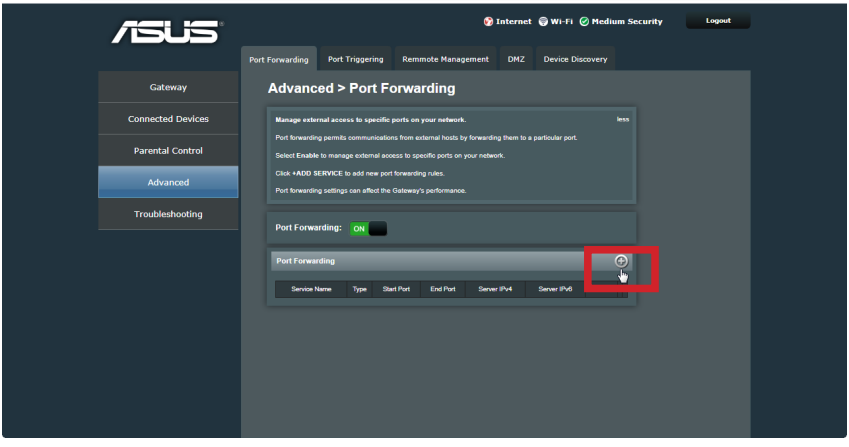
1. From the navigation panel, go to **Parental Control** > **Reports** tab.
2. Select the access control types and time in the **Report Filters** field and click on the **GENERATE REPORT** button to display descriptive list of filtering schedule and rules defined.
3. Click on the **Print**/**Download**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

5 Configuring the Advanced Settings

5.1 Port Forwarding

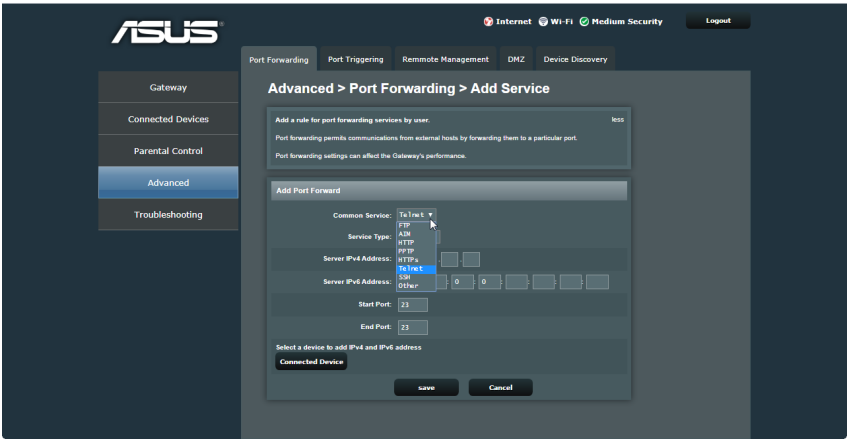
Port forwarding is a method to direct network traffic from the Internet to a specific port or a specific range of ports to a device or number of devices on your local network. Setting up Port Forwarding on your router allows PCs outside the network to access specific services provided by a PC in your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



To set up Port Forwarding:

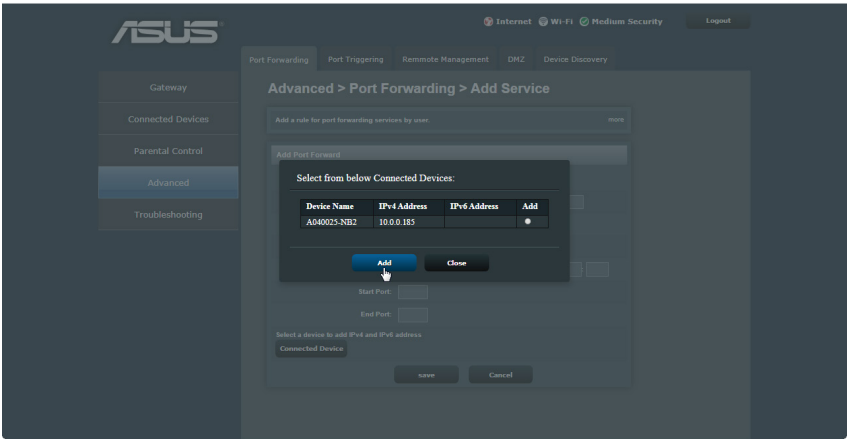
1. From the navigation panel, go to **Advanced** > **Port Forwarding** tab.
2. Move the slider to **ON** to enable **Port Forwarding**.
3. Click on the add icon and configure the following settings below.



- **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.

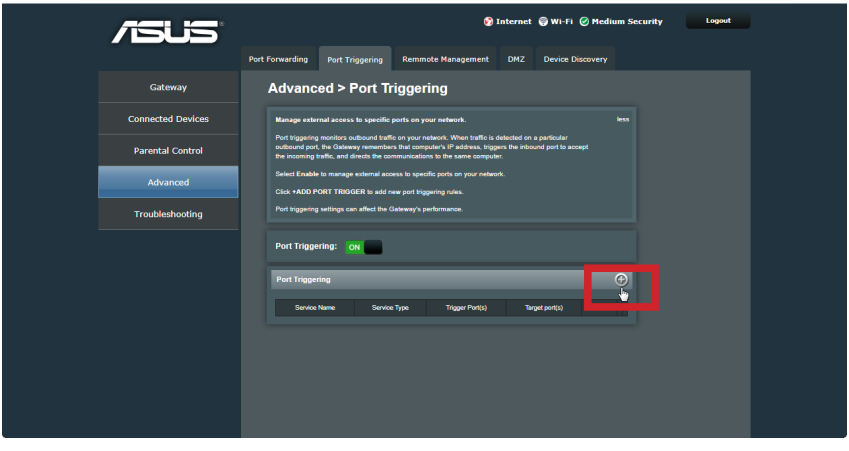


- When done, click **Save**.

5.2 Port Triggering

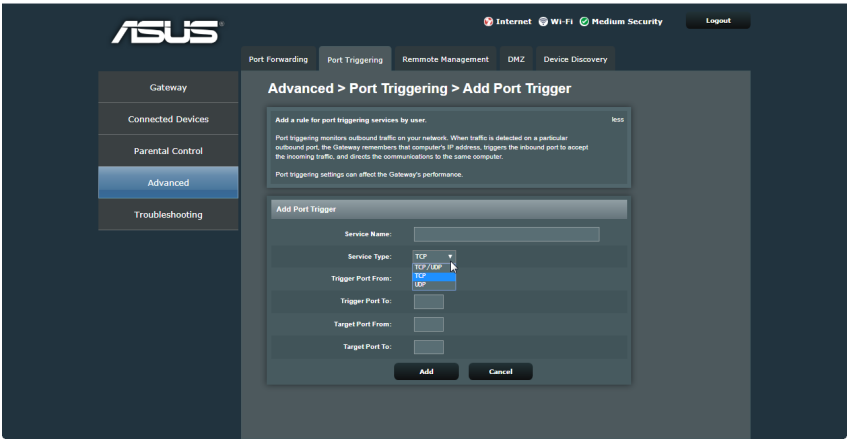
Port range triggering opens a predetermined incoming port for a limited period of time whenever a client on the local area network makes an outgoing connection to a specified port. Port triggering is used in the following scenarios:

- 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.



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.

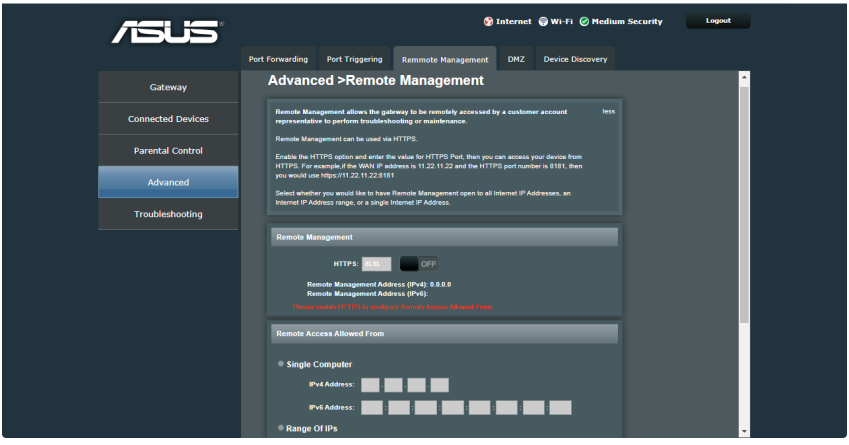


- **Service Name**: Enter a short name or description for the service.
- **Service Type**: Select the protocol, TCP, or UDP.
- **Trigger Port From**: Specify a starting trigger port number to open the incoming port.
- **Trigger Port To**: Specify an end trigger port number to open the incoming port.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



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.

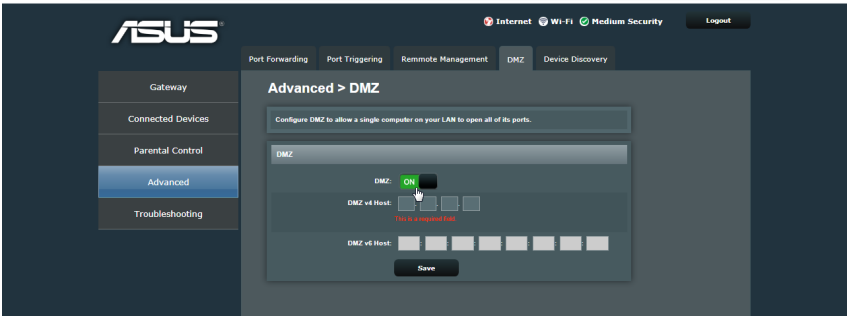
5.4 DMZ

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.

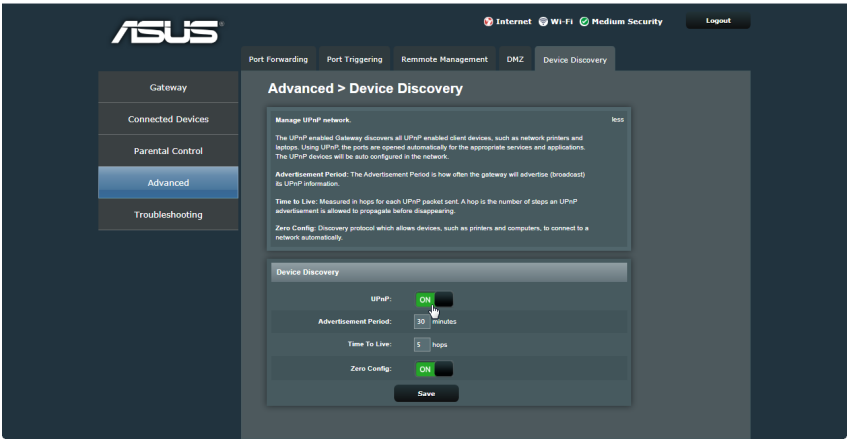


To set up DMZ:

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.



To set up Device Discovery:

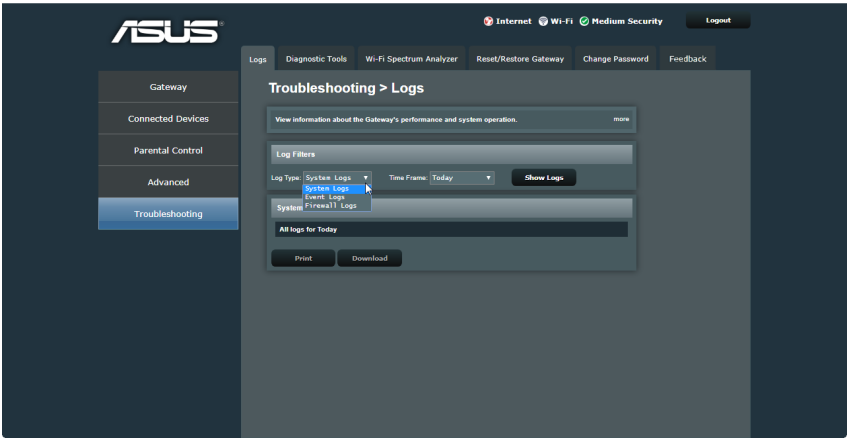
1. From the navigation panel, go to **Advanced** > **Device Discovery** tab.
2. Move the slider to **ON** for using UPnP.

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.

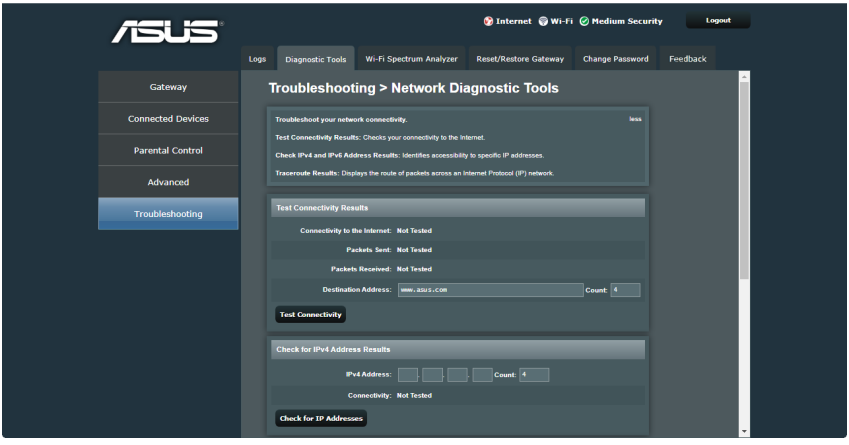


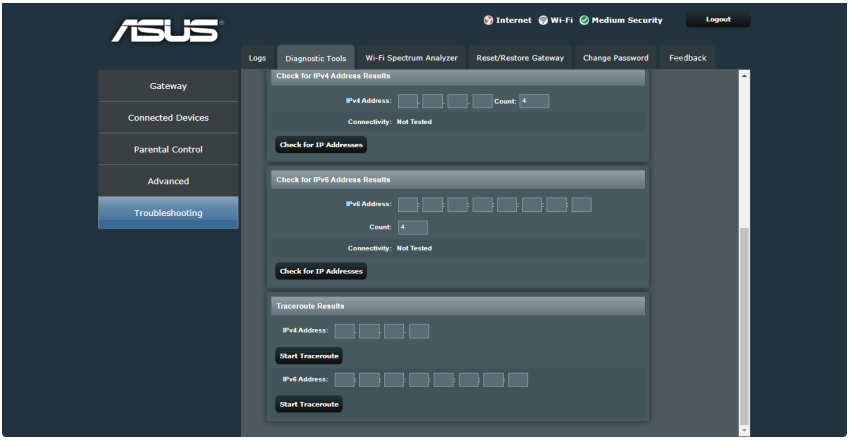
To view the system log information:

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.





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:

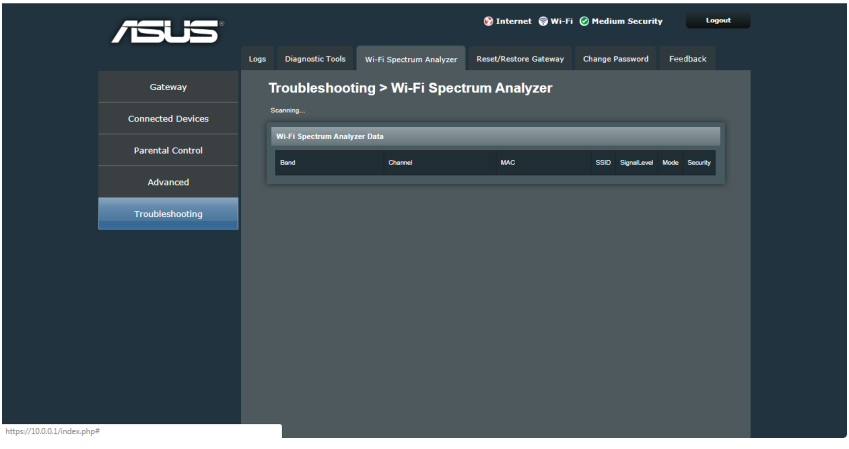
1. From the navigation panel, go to **Troubleshooting > Diagnostic Tools** tab.
2. Enter the IP address in the **Check for IPv4 Address Results/ Check for IPv6 Address Results** fields.
3. Click the **check for IP Address** button to execute the ping test and check the Internet connection.

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

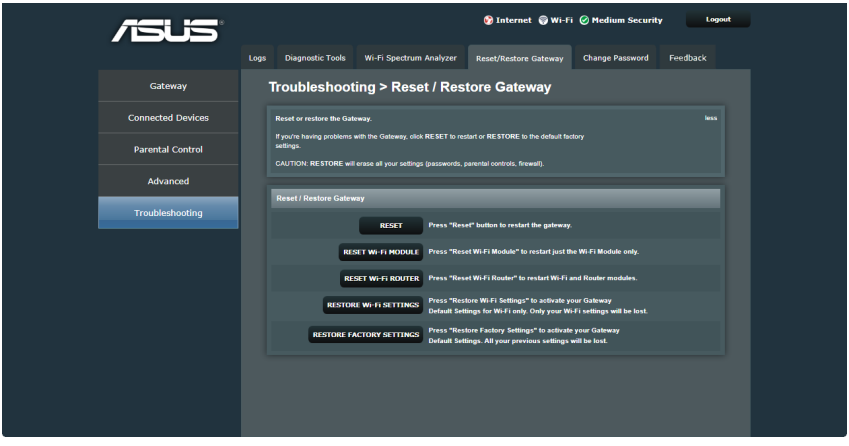
Wi-Fi Spectrum Analyzer is an ASUS WLAN device discovery utility that detects an ASUS router device, and allows you to configure the wireless networking settings.



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



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

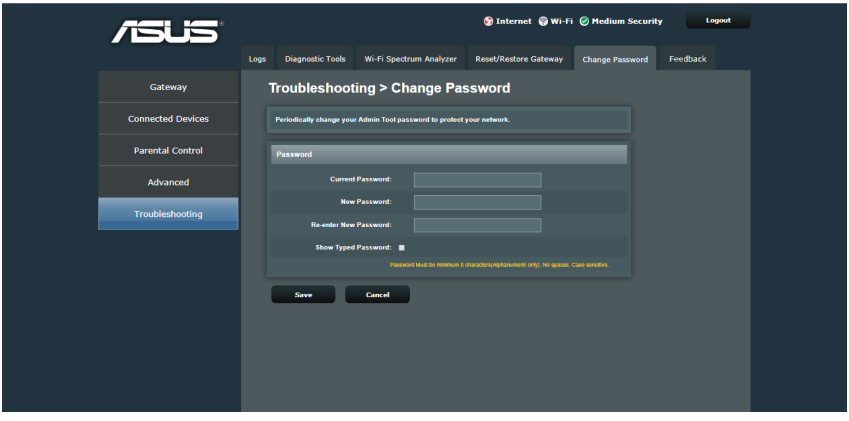
To set up the settings:

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.

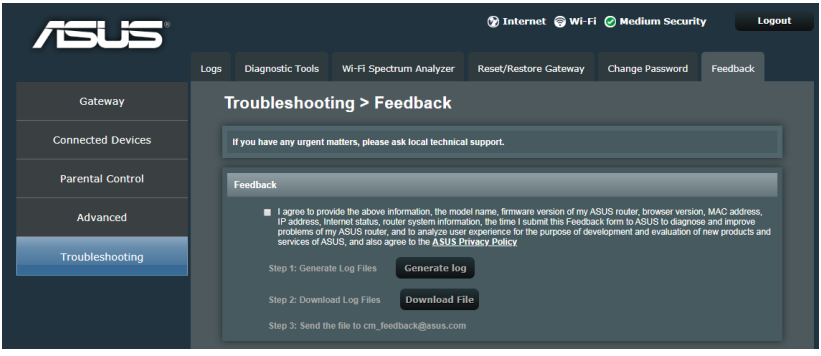


To change the login password:

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



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.