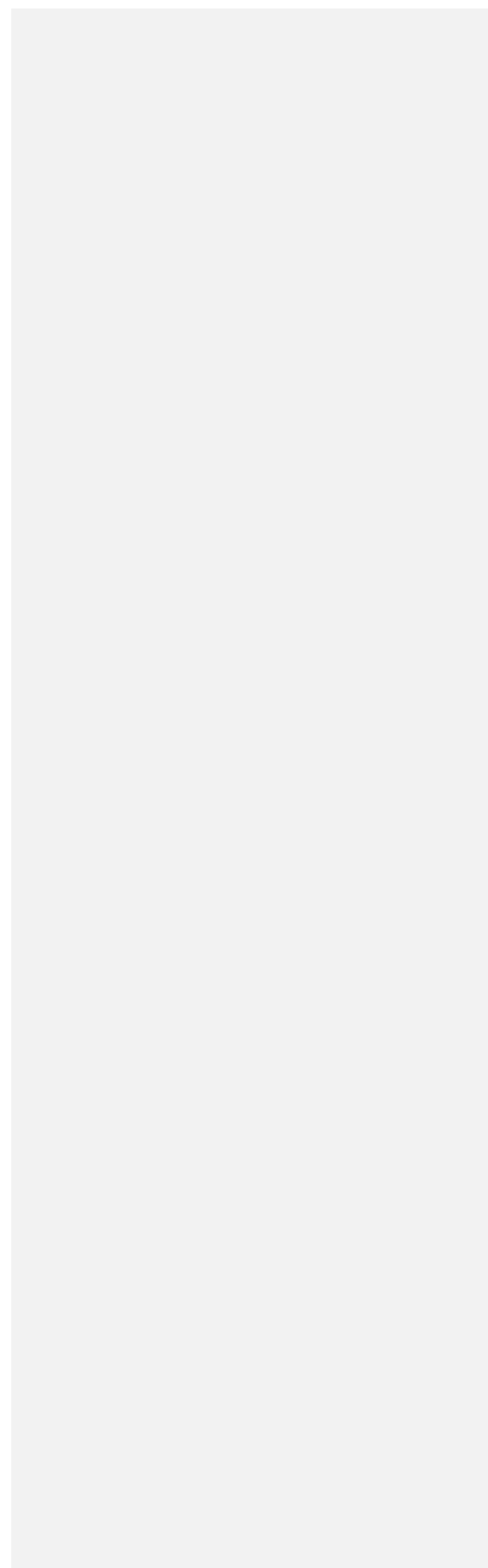


5G FWAR

Quick Start Guide

Version 2



RF Exposure Statement

To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons (indoor), at least 49cm from all persons (outdoor), and must not be co-located or operating in conjunction with any other antenna or transmitter.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

RF EXPOSURE STATEMENT.....	1
CHAPTER 1 INTRODUCTION	1
1.1 IN THE BOX.....	1
1.2 SIDE AND BOTTOM PANEL	2
1.3 LED BEHAVIOR.....	3
1.4 SIM CARD INSTALLATION	4
CHAPTER 2 INSTALLATION AND MOUNTING.....	5
2.1 INSTALLING THE 5G FWAR	5
2.2 RE-INSTALLING YOUR 5G FWAR	7
CHAPTER 3 ACCESSING THE WEB USER INTERFACE	8
3.1 LOGIN	8
3.2 HOME PAGE/MAIN SECTION.....	8
3.3 WI-FI SETTINGS.....	12
3.4 CONNECTED DEVICES	18
3.5 FIREWALL.....	20
3.6 PARENTAL CONTROLS.....	24
3.7 SYSTEM SETTINGS.....	25
CHAPTER 4 PRODUCT SPECIFICATIONS	29
APPENDIX I INSTALLATION GUIDE	30

Chapter 1

Introduction

The 5G FWAR provides users with an improved solution for 5G home service. The innovative design of the 5G FWAR makes it easy for all the family to connect their favorite devices to the 5G Network.

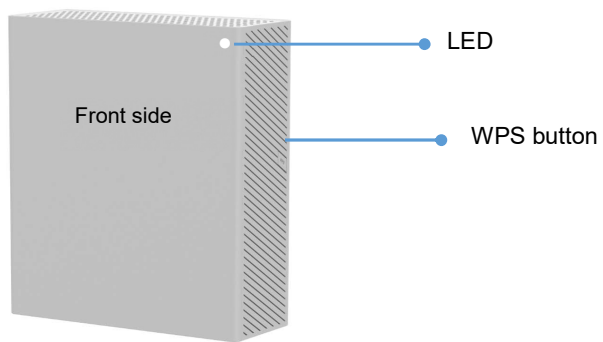
1.1 In the Box

The package contains the following items:

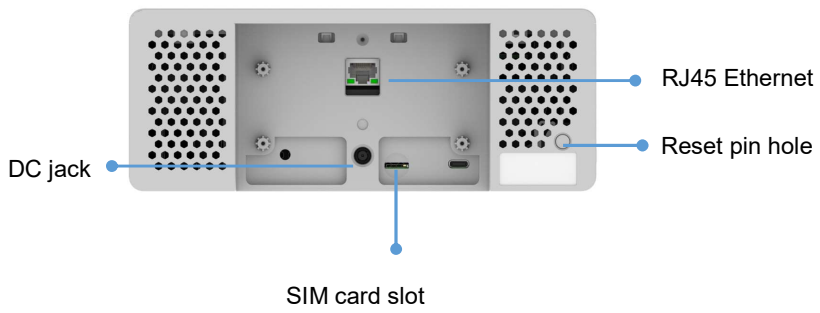
- 5G FWAR × 1
- Power adaptor × 1
- AC power cable × 1

1.2 Side and Bottom Panel

Side panel



Bottom panel



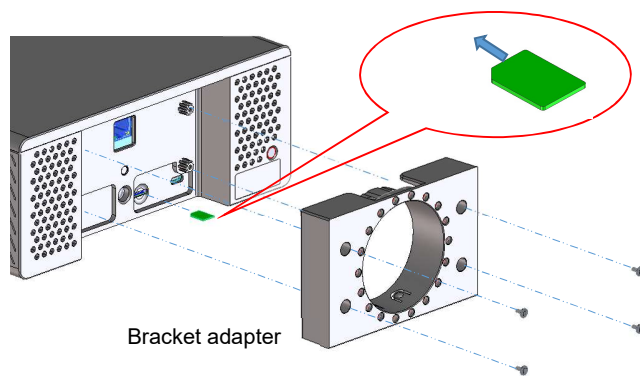
1.3 LED Behavior

Status	Meaning
White Breathing Light	Device is powering up
Solid Red	No 5G signal (when in installation mode)
Solid Amber	Poor 5G signal, but not at threshold (when in installation mode)
Solid Green	Acceptable 5G signal (when in installation mode)
Blink Blue	Firmware update/Factory reset
Blink Red	Error (Fault)
Blink Green	Internet access is ready
Blink Amber	Wi-Fi is disabled
Blink Purple	WPS

1.4 SIM Card Installation

Step 1 Insert the Nano (4FF) SIM card into the SIM card slot.

Step 2 Assemble the device with the bracket adapter using four tapping screws.



Chapter 2

Installation and Mounting

2.1 Installing the 5G FWAR

Step 1 5G FWAR front side should face indoor. 5G FWAR rear side should face the 5G signal (outdoor). Power on the 5G FWAR. The device will enter installation mode.

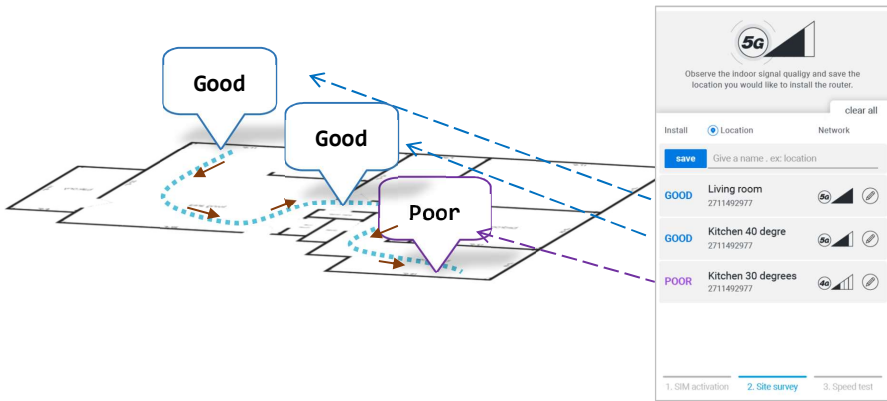
Step 2 Connect the 5G FWAR to your smart phone. First turn off the Wi-Fi function on your phone, then turn on the camera and scan the QR code printed on the product label.

Step 3 A pop-up window will appear asking if you wish to join the Wi-Fi network as indicated in the popup window.

Note: In order to enable Wi-Fi automatic connection via QR code scanning, the operating system on your phone must be Android 10/ iOS 11 or above. If not, you will need to input information manually.

Step 4 After you join the Wi-Fi network, a browser page will pop up automatically to direct you to the installation page.

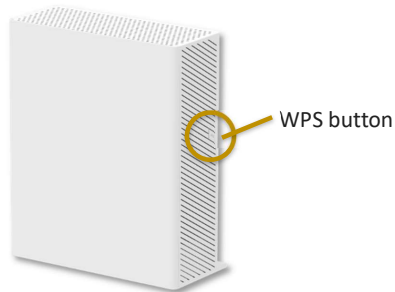
Step 5 Site Survey: Place the 5G FWAR near different walls/windows and observe signal quality. Click on the Save button to save the signal quality of the room. The webpage will indicate whether a saved room is recommended for installing the 5G FWAR. Make sure you install your device in a room with good signal quality.



已註解 [SC1]: Someone has to fix the English in the app below

2.2 Re-installing your 5G FWAR

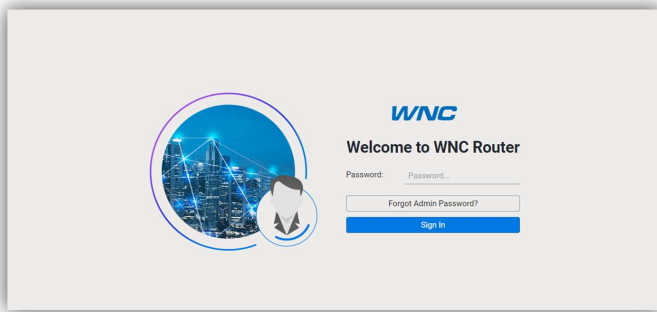
- Step 1** Press and hold the WPS button for 10 seconds. The device will switch to installation mode, and all user settings will be retained.
- Step 2** Remove the device from the mounting kit.
- Step 3** Follow the instructions in the webpage to install the device.



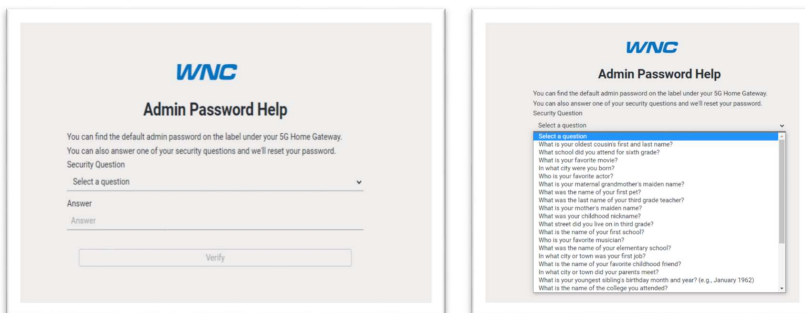
Chapter 3 Accessing the Web User Interface

3.1 Login

After you connect and turn on the 5G FWAR, a **Sign In** screen will appear.



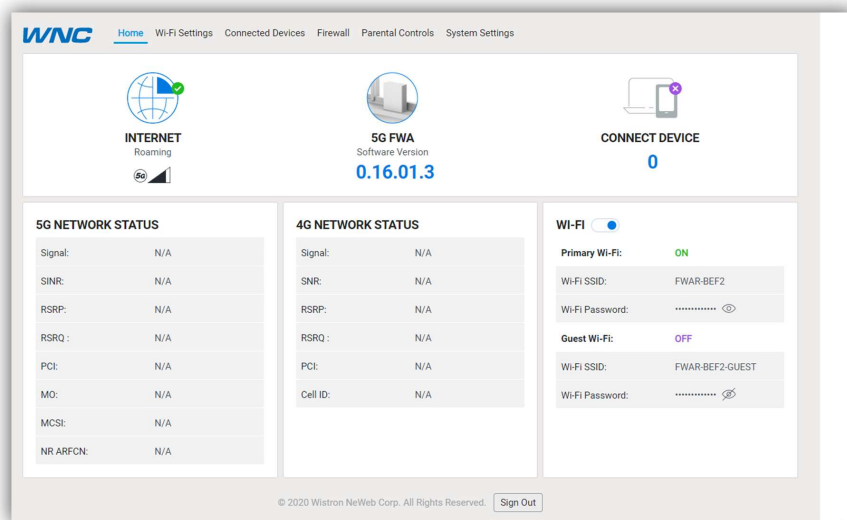
Enter your admin password to log into the **Home Page** of the 5G FWAR's Web GUI. If you forget your password, answer one of the security questions to reset the password to factory default settings.



You can find the default password on the label under the 5G FWAR.

3.2 Home Page/Main Section

The **Home Page** of the 5G FWAR will appear after you log in.



The **Home Page** is where users can check the connection status between the 5G FWAR and the Internet/mesh network, conduct network speed tests, and adjust settings such as Wi-Fi options. In the upper right panel of the screen, the **Network Map** presents a list of devices that are currently connected to the 5G FWAR. Below that, the screen is divided into three columns: **5G Network Status** on the left, **4G Network Status** in the middle, and **Wi-Fi** on the right.

The drop-down menu on the upper right of the **Home Page** includes selections such as **Admin Settings**, **Restart 5G FWAR**, and **Sign Out**.

3.2.1 Network Map (Speed test, Mesh network)

The **Network Map** is located in the upper-right section of the **Home Page**. The lines between the 5G FWAR and the Internet/mesh network/devices on the map indicate the connection status between them. A solid green line indicates an accessible network, and a gray line with a red x in the middle indicates that there is no connection.

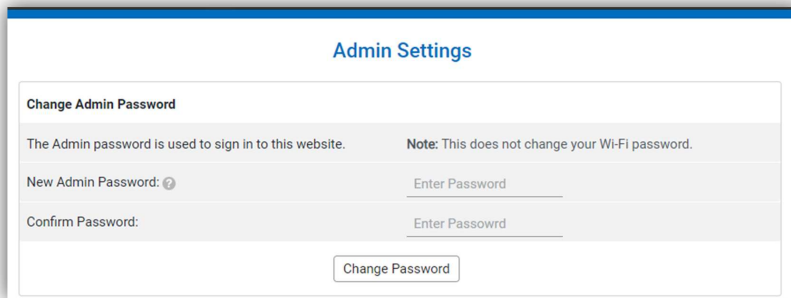
To test the connection speed between the 5G FWAR and the Internet/other networks, click the Test Speed button on the lower left of the **Network Map**.

The number of APs and clients currently connected to the network are indicated in the lower right section of the **Network Map**.

3.2.2 Admin Settings

The Change Admin Password section enables you to change the Admin password that is used to sign in to the 5G FWAR's **Home Page**. Type the desired admin password in the New Admin Password field, then type the admin password again in the Confirm Password field. Click **Change Password** to apply the new password.

If the password you enter contains three consecutive or repeating alphanumeric characters, a window will pop up as a warning of insufficient password strength.



The screenshot shows a web interface titled "Admin Settings". Under the heading "Change Admin Password", there is a note: "The Admin password is used to sign in to this website. Note: This does not change your Wi-Fi password." Below this, there are two input fields: "New Admin Password: ?" with a placeholder "Enter Password" and "Confirm Password:" with a placeholder "Enter Password". At the bottom of the form is a button labeled "Change Password".

In the **Security Questions** section, you can choose three security questions, then enter the answer for each question. If a user forgets their admin password, one of the questions will be used to restore the admin password to factory default settings. Click **Save** to save your changes. Click **Close** to close the Admin Settings window.

Security Questions		
If you forget your admin password, one of these questions will be used to change the password.		
Security Question 1	Select a question	Answer 1
Security Question 2	Select a question	Answer 2
Security Question 3	Select a question	Answer 3
<input type="button" value="Save"/>		
<input type="button" value="Close"/>		

3.2.3 Restarting the 5G FWAR

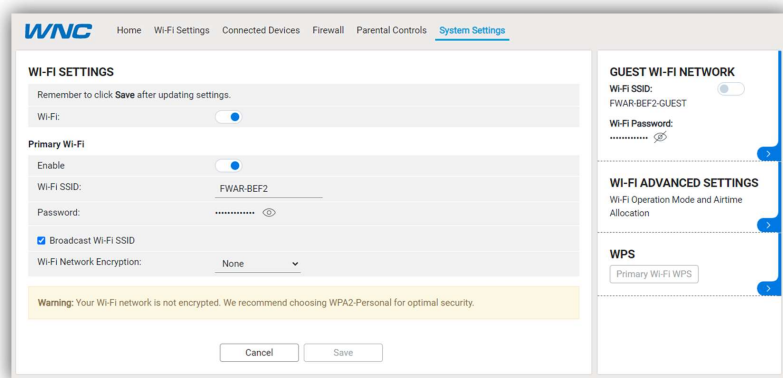
To restart the 5G FWAR, click the drop-down arrow and select **Restart 5G FWAR**. A window will appear on the screen. Click **Restart** to restart the 5G FWAR.

3.2.4 Sign Out

Click **Sign Out** to log off the 5G FWAR.

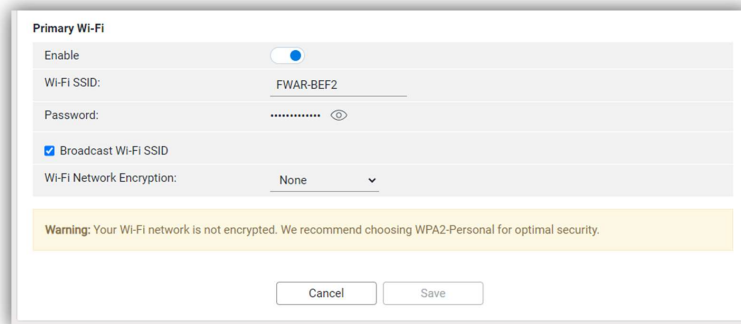
3.3 Wi-Fi Settings

Click the > arrow on the bottom-right side of the **Wi-Fi** column in the **Home Page** to bring up the Wi-Fi page. On this page, you can adjust settings for the Primary Wi-Fi Network, Guest Wi-Fi Network, Wi-Fi Advanced Settings, and WPS.



3.3.1 Primary Wi-Fi Network


Slide the **Enable** switch to the right to activate the Primary Wi-Fi network. The switch will turn blue to indicate that the selected Wi-Fi network is turned on. To turn off the Primary Wi-Fi network, slide the switch to the left.



1. Wi-Fi name (SSID)

The Wi-Fi name (SSID) is the name of the wireless network broadcasting from the 5G FWAR. In order for devices to connect to the local network over a wireless link, they must select this network name from the list of detected wireless networks in the area.

2. Password

Specify a password for your wireless network. Click the  icon to display the selected password for the SSID.

3. New Password

Enter a new password here for the SSID.

4. Confirm Password

Type your new password here.

Note: Passwords must be 8–63 characters long and are case sensitive. Changing your Wi-Fi name or password may cause devices to lose their connection to the primary network.

5. Broadcast Wi-Fi Name (SSID)

Check this box if you want to broadcast your SSID. The SSID will be displayed when you search for available networks.

6. Wi-Fi network encryption

Select one security method from the drop-down menu. The encryption types include None, WEP-64, WPA2-Personal, and WPA-WPA2-Personal.

3.3.2 Guest Wi-Fi Network

Slide the **Enable** switch to the right to activate the Guest Wi-Fi network. The switch will turn blue when the guest network is enabled. To turn off the Guest Wi-Fi network, slide the switch to the left.

Guest Wi-Fi Network

Enable:

Wi-Fi SSID: FWAR-BEP2-GUEST

Password:

New Password: Password

Confirm Password: Password

Note: Password must be 8-63 characters, non-consecutive or repeating alphanumeric characters and is case sensitive. Changing your Wi-Fi name or Wi-Fi password may cause your devices to lose their connection to your primary network.

Broadcast Wi-Fi Name (SSID)


Wi-Fi Network Encryption: WPA2-Personal

Close Save

7. Wi-Fi name (SSID)

The Wi-Fi name (SSID) is the name of the wireless network broadcasting from the 5G FWAR. In order for devices to connect to the local network over a wireless link, they must select this network name from the list of detected wireless networks in the area.

8. Password

Specify a password for your wireless network. Click the  icon to display the selected password for the SSID.

9. New Password

Enter a new password here for the SSID.

10. Confirm Password

Retype the new password here.

Note: Passwords must be 8–63 characters long and are case sensitive. Changing your Wi-Fi name or password may cause devices to lose their connection to the primary network.

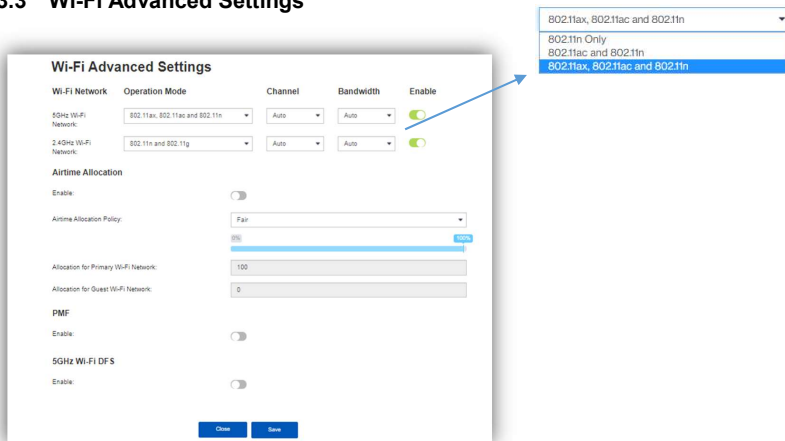
11. Broadcast Wi-Fi Name (SSID)

Check the box if you want to broadcast the SSID. The SSID will be displayed when you search for available networks.

12. Wi-Fi network encryption

Select one security method from the drop-down menu. The encryption types include None, WEP-64, WPA2-Personal, and WPA-WPA2-Personal.

3.3.3 Wi-Fi Advanced Settings



13. Wi-Fi Network Operation Mode

On this page, you can adjust the operation mode, channel, and bandwidth for the 5 GHz and 2.4 GHz primary Wi-Fi networks as well as adjust airtime allocation.

The options provided for the 5 GHz primary Wi-Fi network include:

802.11n only

802.11ac and 802.11n

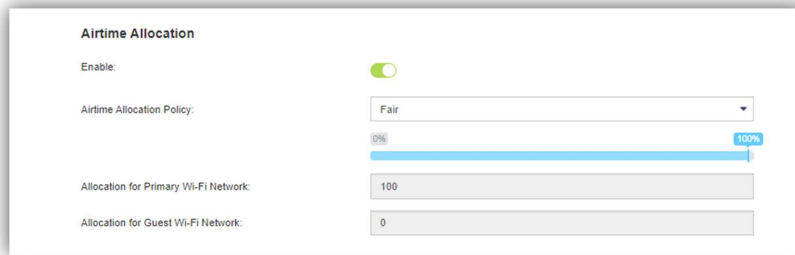
802.11ax, 802.11ac and 802.11n

The options for the 2.4 GHz primary Wi-Fi network include:

802.11n and 802.11g

802.11ax, 802.11n and 802.11g

14. Airtime Allocation



The screenshot shows the 'Airtime Allocation' configuration page. It includes an 'Enable' toggle switch that is currently turned on (blue). Below it is a dropdown menu for 'Airtime Allocation Policy' set to 'Fair'. A slider below the dropdown shows a blue bar extending from 0% to approximately 80%, with '0%' and '100%' labels at the ends. At the bottom, there are two input fields: 'Allocation for Primary Wi-Fi Network' with the value '100' and 'Allocation for Guest Wi-Fi Network' with the value '0'.

Slide the **Enable** switch to the right to activate this function. The switch will turn blue when airtime allocation is enabled. To disable airtime allocation, slide the switch to the left.

When ATF is enabled, the system needs to be restarted for it to take effect.

In the Airtime Allocation Policy pull-down menu, two policy options are available: Fair and Strict.

Use the slider below the Airtime Allocation Policy pull-down menu to adjust the percentage of resources allocated to the primary and guest Wi-Fi networks. Sliding the bar to the right increases the allocation percentage for the primary Wi-Fi network, while sliding the bar to the left increases the allocation percentage for the guest Wi-Fi network. The allocation percentages for the primary and guest Wi-Fi networks are shown in the two fields on the bottom of the page, and change in real-time when the slider is adjusted.

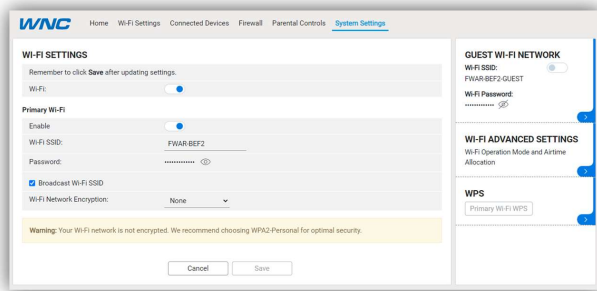
15. PMF



The screenshot shows the 'PMF' configuration page. It includes an 'Enable' toggle switch for 'PMF' that is currently turned on (blue). Below it is an 'Enable' toggle switch for '5GHz Wi-Fi DFS' that is also turned on (blue). At the bottom, there are two buttons: 'Close' and 'Save'.

Slide the switch to the right to enable PMF (protected management frames) on your 5G FWAR.

3.3.4 WPS

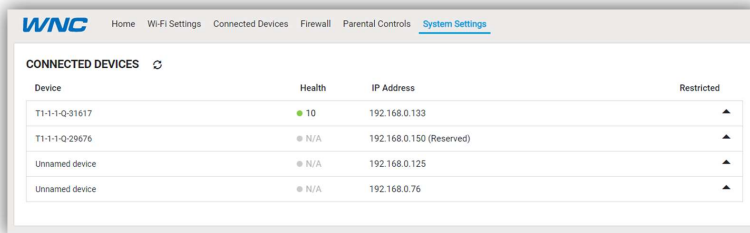


16. Primary Wi-Fi WPS

- WPS allows rapid wireless connection between the 5G FWAR and other WPS-compatible devices. You can trigger the WPS function on Primary Wi-Fi by clicking on the **Primary Wi-Fi WPS** button.

3.4 Connected Devices

This section displays information about the devices connected to the APs, illustrated through a Network Map, as well as the AP list and Connected Devices table.



The screenshot shows the WNC web interface with the 'CONNECTED DEVICES' section. The table lists the following data:

Device	Health	IP Address	Restricted
T1-1-1-Q-31617	● 10	192.168.0.133	▲
T1-1-1-Q-29676	● N/A	192.168.0.150 (Reserved)	▲
Unnamed device	● N/A	192.168.0.125	▲
Unnamed device	● N/A	192.168.0.76	▲

3.4.1 Network Map

- The Network Map illustrates the mesh network comprising the connected APs, their names, as well as their respective connection status.
- The number in the circle indicates the number of clients currently connected to the AP.

3.4.2 AP List

- The section presents detailed information of each AP, including the name of the AP, wireless radio channel information, health of the connection, usage of the 2.4 GHz and 5 GHz Wi-Fi, backhaul usage, and the number of connected clients.

3.4.3 Connected Devices

- The name of each device that has been connected/is currently connected to the 5G FWAR is displayed here. Also displayed are the health of their connection, their IP addresses, which AP a device is connected to, and the restriction policies related to each device (if any).

Device	Health	IP Address	Connected AP	Restricted
T1-1-1-Q-31201	● 10	192.168.0.215	5G Internet Gateway	▼
ASUS_Phone	● N/A	192.168.0.117	[5GHz] 5G Internet Gateway	▼
T1-1-1-Q-29791	● N/A	192.168.0.28	5G Internet Gateway	▼
T1-1-1-Q-29676	● N/A	192.168.0.150	5G Internet Gateway	▼

Select the arrow icon “▼” on the right that corresponds to a connected device, and related information and settings for the device will be displayed, including its IPv6 address, whether to delete the device, block the device, or reserve DHCP IP.

CONNECTED DEVICES ↻

Device	Health	IP Address	Restricted
T1-1-1-Q-31617	● 10	192.168.0.133	▲
<div style="display: flex; justify-content: space-between; align-items: center;"> Delete Device Restrictions Add Schedule Save </div> <p>IPv6 address fe80::e147:7b59:d40f:4e14</p> <p>Block Device <input type="checkbox"/></p> <p>Reserve DHCP IP <input type="checkbox"/></p>			
T1-1-1-Q-29676	● N/A	192.168.0.150 (Reserved)	▲
Unnamed device	● N/A	192.168.0.125	▲
Unnamed device	● N/A	192.168.0.76	▲

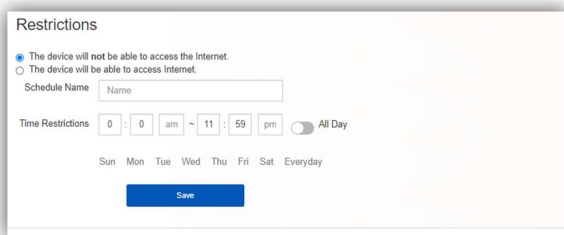
The **Delete Device** button enables you to remove the selected device which has connected to the 5G FWAR. Once removed, the computer/device will not be displayed on this page.



The **Block Device** switch allows you to block or allow computers or devices from establishing a connection to the 5G FWAR. To block a device, slide the **Block Device** switch to the right. The switch will be blue when the feature is enabled.

The **Reserve DHCP IP** switch enables the 5G FWAR to assign the same IP address to a specific device whenever that device connects to your network. To reserve DHCP IP, slide the **Reserve DHCP IP** switch to the right.

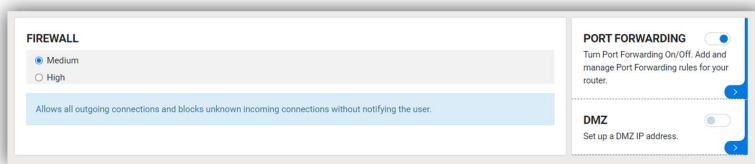
When a Wi-Fi client is connected and the **Airtime Allocation** feature is enabled, you will be able to adjust the airtime percentage for each client. It is recommended that you use 90% to leave a margin for other clients that are not set with a non-zero ATF percentage.

Restrictions



This section enables you to set restriction policies for the selected device. You can specify a time during which the selected device will not be able to access Internet. Alternatively, you may also specify a time during which the selected device will be able to access the Internet. The settings you can perform in this section include the name of the schedule and the time period for the restriction policy. Click **Save** to save your settings. The  icon indicates that the selected device is blocked permanently. The  icon indicates that the device is only restricted during the specified periods of time.

3.5 Firewall



A firewall is used to prevent traffic from entering and/or leaving the areas of your network. In this section you can select **Medium** for a typical level of security, and **High** for a maximum level of security.

3.5.1 Port Forwarding

Port Forwarding

Add Rules

Rule Name:

From Port:

Protocol:

IP Address:

To Port:

Configured Ports

Application	Port From	Protocol	IP Address	Port To	Enabled	Remove
-------------	-----------	----------	------------	---------	---------	--------

Port Forwarding can be used to open certain ports of a device to communicate with an Internet service. To turn on Port Forwarding, slide the Port Forwarding switch on the bottom right of the General Information page to the right. The switch turns blue to indicate that the function is turned on. To turn off this function, slide the switch to the left. To access this page, click Port Forwarding on the General Information page.

From the Port Forwarding page, enter the appropriate forwarding options listed on the page, then click Add to save your changes, or click Cancel to discard any changes you made. Click Close to close this page. The options include:

Add Rules

17. Rule Name

Type the name of the service for which the port forwarding rule has been created in the Rule Name text field.

18. From Port

Type the value of the WAN port from which you want to forward packets. Please note that only a single port (for instance, 3000) or range (for instance, 3000–3005) can be specified. 0 would mean any port.

19. Protocol

Choose the protocol to be used for port forwarding.

The screenshot shows the 'Port Forwarding' configuration window. The 'Add Rules' section is active, showing a dropdown menu for 'Protocol' with options: TCP, UDP, DNS, HTTP, NNTP, POP3, SMTP, SNMP, Telnet, and TFTP. The 'Add' button is visible.

20. IP Address

The local server's IP address.

21. Port To

Type the value of the LAN port to which you want to receive the forwarded packets.

Configured Ports

Application	Port From	Protocol	IP Address	Port To	Enabled	Remove
-------------	-----------	----------	------------	---------	---------	--------

This table displays the ports that have been configured.

22. Application

The created rule name will be displayed here.

23. Port From

This shows the value of the start port.

24. Protocol

This shows the protocol selected for the corresponding port forwarding rule.

25. IP Address

This shows the local server's IP address.

26. Port To

This shows the value of the end port.

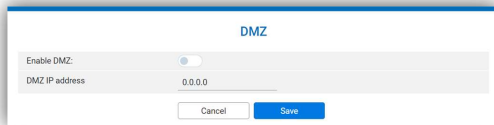
27. Enabled

The icon indicates that the corresponding port forwarding rule has been enabled.

28. Remove

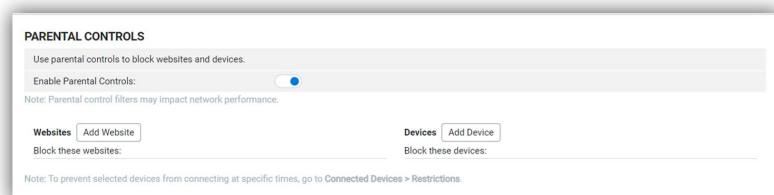
Click on the x icon to delete a port forwarding rule.

3.5.2 DMZ



DMZ (De-Militarized Zone) allows you to specify a DMZ host IP to redirect requests to a virtual DMZ host in order to enhance the security of the local area network. To enable DMZ, slide the **DMZ enable** switch to the right. If this function is enabled, threats from external networks will be directed to the DMZ instead of the network. The **DMZ IP address** field indicates the IP address of the host DMZ. To designate a device as a DMZ host, enter its IP address in the **DMZ IP Address** field. Click **Save** to apply the changes, or click **Cancel** to undo your configuration.


3.6 Parental Controls



By creating Internet access policies, Parental Controls allow you to control and monitor Internet access. Parental Controls can be activated on the Home page by sliding the Filters switch in the Parental Controls column.

You can also enable or disable the function after you enter the Parental Controls page. Slide the Parental controls switch to the right. When the switch is blue, parental control of websites and devices is enabled. To turn off this function, slide the switch to the left.

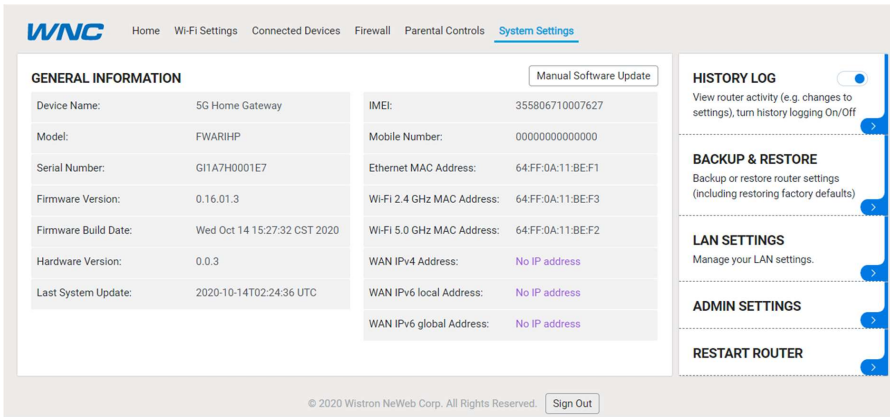
3.6.1 Websites

This function can be used to block computers or devices from accessing certain websites through the 5G FWAR. The websites that have been blocked are displayed on the screen. To add a website to the block list, click **Add Website** and enter the website in the input field. Click **Add** to save your changes, or click on the  icon to remove the selected website from the block list.

3.6.2 Devices

To add a device to the block list, click **Add Device**. A drop-down list will display the devices that are currently connected to the 5G FWAR and their MAC address. Select the device that you want to block, then click **Include**. The devices that appear on this list will be not be able to access any of the websites listed in the [Websites](#) section.

3.7 System Settings

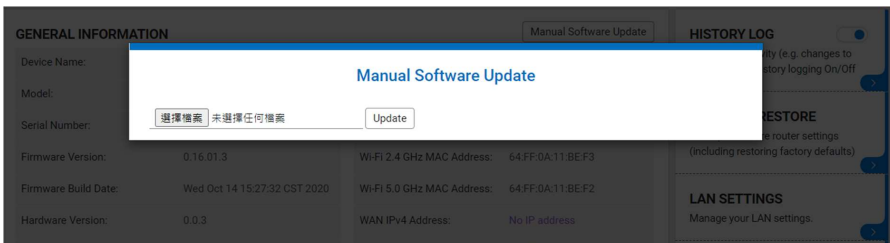


3.7.1 General Information

The **General Information** page provides device information on the 5G FWAR, including the device name, IMEI, model, and more.

3.7.2 Firmware Upgrade

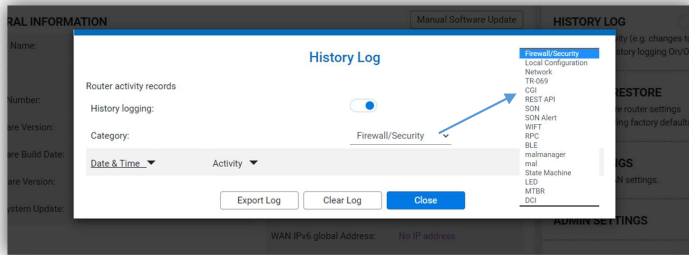
Click the **Manual Software Update** button, and the following window will appear.



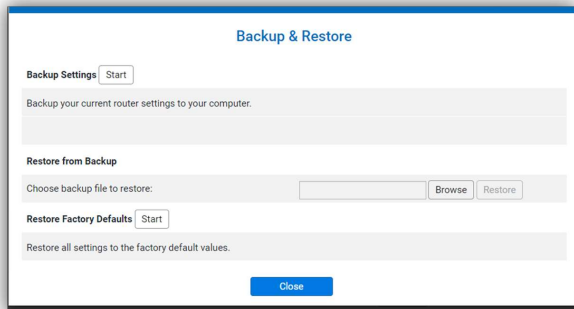
Click the **選擇檔案** button and select the firmware for the update. Then click the **Update** button. After the update is complete, the Web GUI page will refresh automatically.

3.7.3 History Log

The **History Log** page provides various activity records of your 5G FWAR. To access this page, click **History Log** on the General Information page.

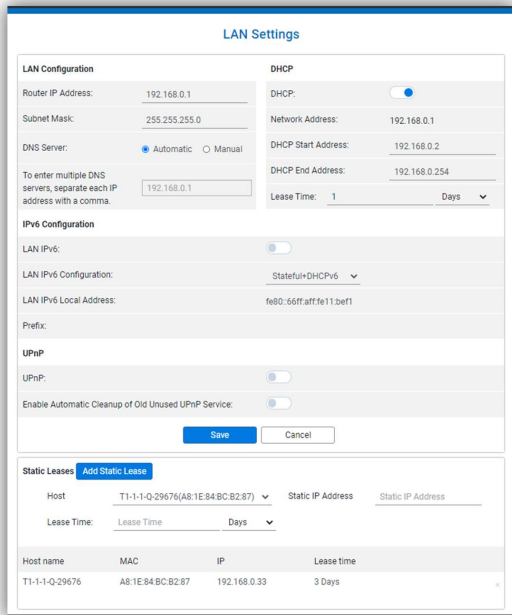


3.7.4 Backup & Restore



The **Backup & Restore** page covers functions for backing up/restoring the settings on your 5G FWAR and resetting it to factory settings. To access this page, click **Backup & Restore** on the **General Information** page.

3.7.5 LAN Settings



The LAN Settings page includes settings to configure advanced LAN settings (e.g., IP address, Subnet mask, DHCP) for your 5G FWAR. To access this page, click LAN Settings on the General Information page.

LAN Configuration

In this section, enter the desired info in the following fields:

29. Router IP address

Specify a range of IP addresses the 5G FWAR may assign to devices. The default LAN IP configuration is 192.168.0.1.

30. Subnet Mask

The subnet mask along with the previously configured IP address defines the network. The default value for subnet mask is 255.255.255.0.

31. DNS Server

Use this function to toggle whether the DNS server is set automatically or manually.

DHCP

DHCP assigns LAN IP addresses for connected devices. You can specify the range of IP addresses the 5G FWAR may assign to devices. Click the DHCP switch to turn the DHCP function on or off. You can also enter the desired information in the following fields:

32. DHCP Start Address

Specify the address that starts the range for the pool of IP addresses in the same subnet as the 5G FWAR.

33. DHCP End Address

Specify the address that ends the range for the pool of IP addresses in the same subnet as the 5G FWAR.

34. Lease Time

You can specify a period of time after which an assigned IP address will be retrieved from devices.

35. UPnP

For devices that support Universal Plug and Play (UPnP), enabling the UPnP function will allow automatic port forwarding. This helps your UPnP devices communicate with the Internet.

Slide the **UPnP** switch to the right to enable the feature. Slide the **Enable Automatic Cleanup of Old Unused UPnP Service** switch to enable the automatic cleanup of invalid rules. When enabled, old and unused UPnP defined services will be removed.

Chapter 4

Product Specifications

5G	<ul style="list-style-type: none">· 5G n260· 5G n2/n5/n66
4G	<ul style="list-style-type: none">· LTE CAT22, Band 2/4/5/12/14/29/48/66
Wi-Fi	<ul style="list-style-type: none">· 2.4GHz 802.11ax 2×2 MIMO· 5GHz 802.11ax 4×4 MIMO· Backwards compatible with 11ac/11n/11b
Memory	<ul style="list-style-type: none">· 5G FWAR: DDR4 RAM 1GB· Router: DDR4 RAM 1GB
Storage	<ul style="list-style-type: none">· 5G FWAR: NAND 1GB· Router: NAND 1GB
Dimensions	<ul style="list-style-type: none">· 246 x 220 × 86 mm
Weight	<ul style="list-style-type: none">· 2.2 kg
Connector	<ul style="list-style-type: none">· 2.5GbE LAN port × 1· DC Jack × 1
Button	<ul style="list-style-type: none">· WPS button × 1· Reset pinhole × 1
Operating Temperature	<ul style="list-style-type: none">· 0 °C–40 °C

Appendix I Installation Guide

Operational Communication Signal

