Mobile 4G LTE Router and Wi-Fi Extender

User Manual

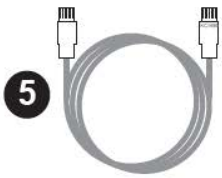
Thank you for purchasing a KING PASSPORT

Powered by travlfi

This Quick Reference Guide provides an overview of the KING Passport, including setup, first-time login information, and basic operating information for use as either a router or Wi-Fi extender.

CONTENTS

1. KING Passport
2. (2) LTE Antennas (unattached in box)
3. (4) Wi-Fi Antennas (unattached in box)
4. Power Adapter
5. Ethernet Cable
6. Quick Reference Guide



SETUP

TIP Determine the best location for the Passport before making connections.

- The Passport can be set up next to a window or windshield.
- Cabinets may be suitable but can degrade cellular reception.
- Do not block side vents or set other devices on top of the Passport.

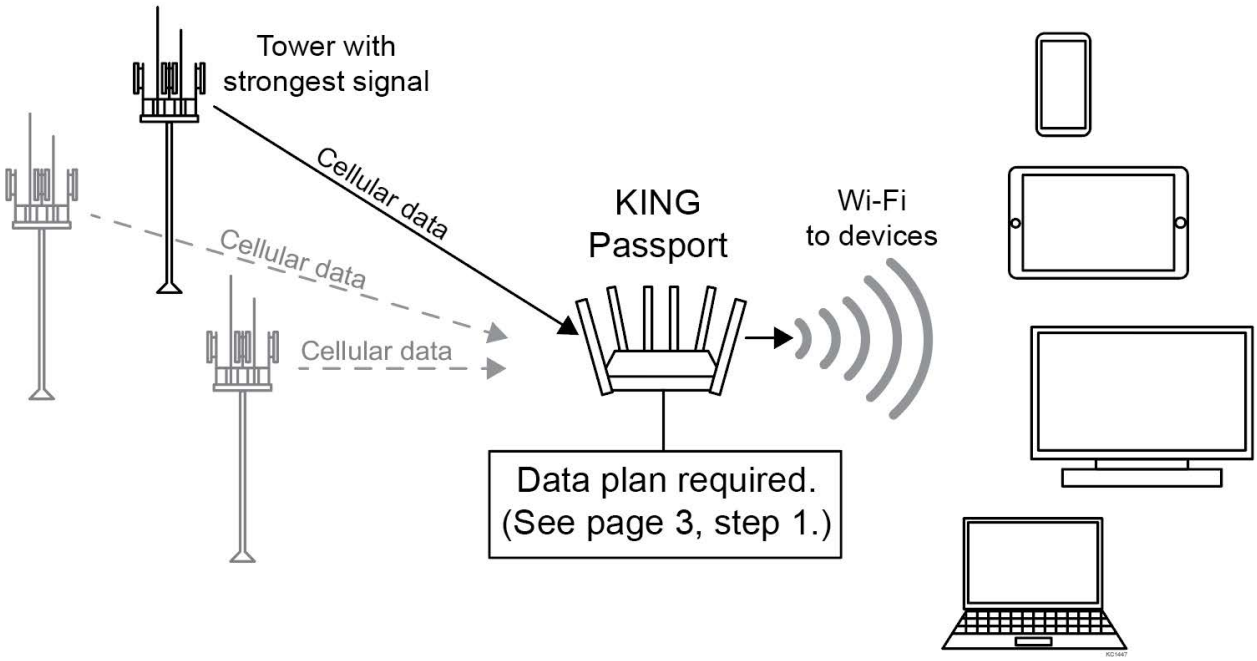
All ports and antennas are labeled for easy setup!

1. Connect the LTE antennas to the LTE ports.

2. Connect the 2.4G antennas to the ports labeled 2.4G, and the 5G antennas to the ports labeled 5G.

⚠ Make sure to connect Wi-Fi antennas to the correct 2.4G and 5G ports.

3. Connect the power adapter. **USE ONLY THE SUPPLIED POWER ADAPTER.**



CELLULAR ACTIVATION AND CHOOSING A DATA PLAN

1. Call **(855) 433-2285** or scan the QR code below to activate your router with a TravlFi Pay As You Go data plan of your choice.

2. After activation, go to your device's Wi-Fi settings page. The 2.4 GHz and 5 GHz Wi-Fi frequencies that match the SSID located on the bottom of the unit should appear. Connect to your desired frequency using the password located on the bottom of the unit.

BOTTOM OF PASSPORT (Graphics may vary)

Model: CPE-0001
Input:12V ⎓ 1.5A

Default Wi-Fi Details
2.4G SSID: #CPE0001_2.4_k79
5G SSID:#CPE0001_5_k79
Wi-Fi Password:xxxxxxxxxx
MAC: 48:C8:62:0C:13:D1
Device ID: xxxxxxxxxx

Default Router Login Details
IP Address: http://192.168.0.1
Username: admin
Password: admin
SN: xxxxxxxxxxxxxx

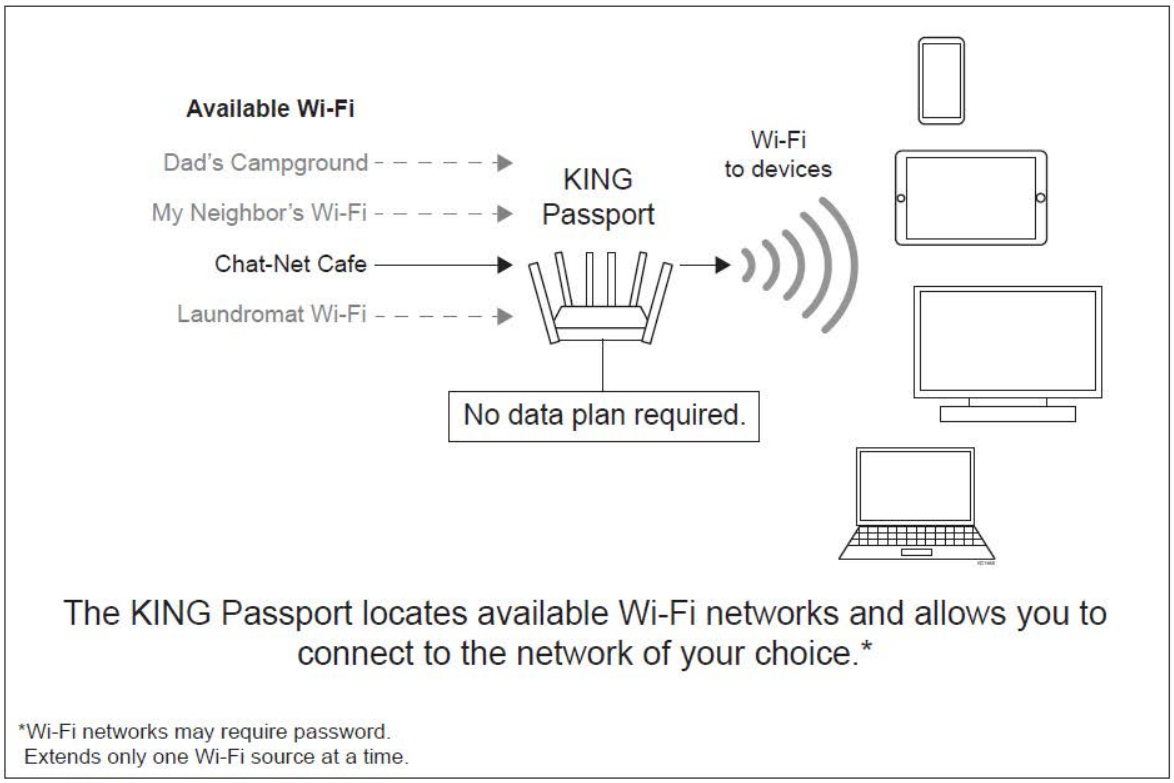
FCC ID:GVQ-CPE-0001
Made in China
Contains FCC ID: 2AJYU-8MH0011

1 Scan to activate.

OPERATING NOTES: After startup, the device may need a few minutes to find the best cellular signal available in your area.

Once this process is complete, internet/data connection will automatically function over Wi-Fi and LAN.

USING THE PASSPORT AS AN EXTENDER / REPEATER



The KING Passport locates available Wi-Fi networks and allows you to connect to the network of your choice.*

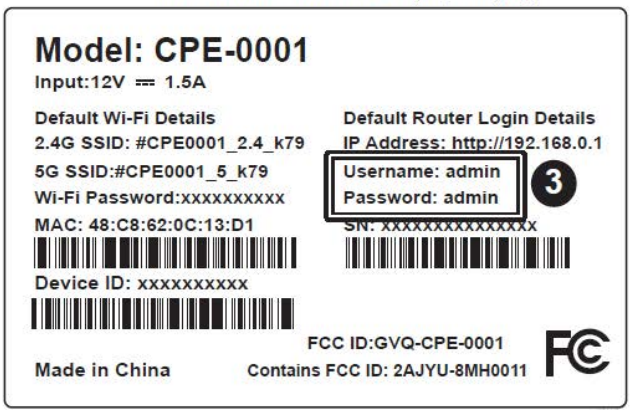
*Wi-Fi networks may require password.
Extends only one Wi-Fi source at a time.

1. Ensure you are connected to the Passport's Wi-Fi. Open a new web browser window.
2. Go to the web address: **http://192.168.0.1**.
3. Type in the administrative username and password, and proceed to login.

TIP The default administrative login details (admin username and password) are found on the bottom of the Passport.

Make sure to use a lower case "a" for both instances of "admin."

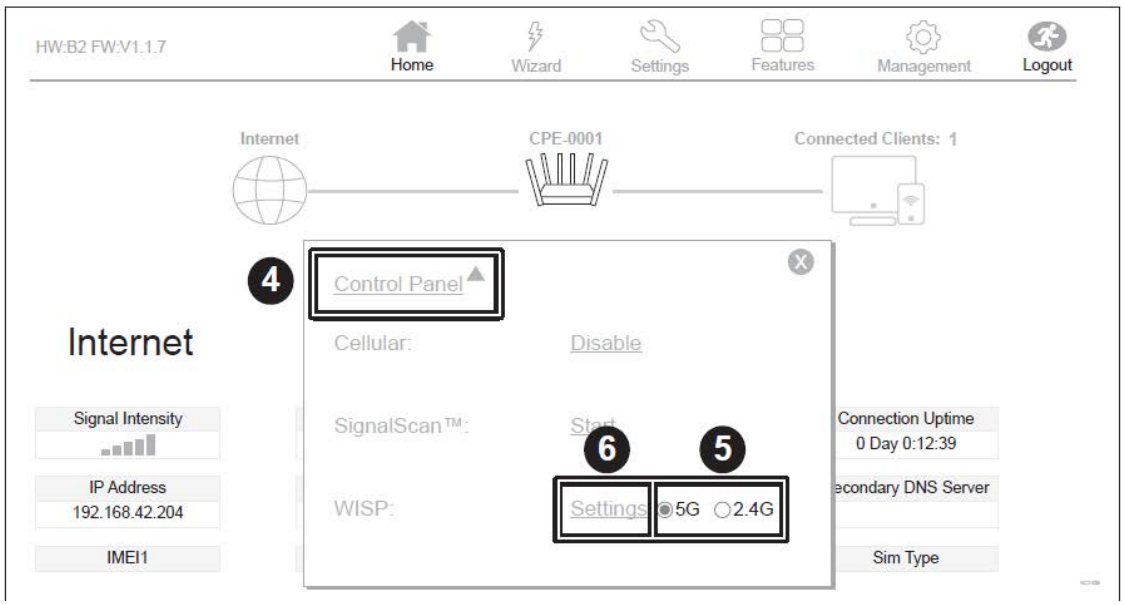
BOTTOM OF PASSPORT (Graphics may vary)



4. After logging in, select “Control Panel” to open the drop-down menu.

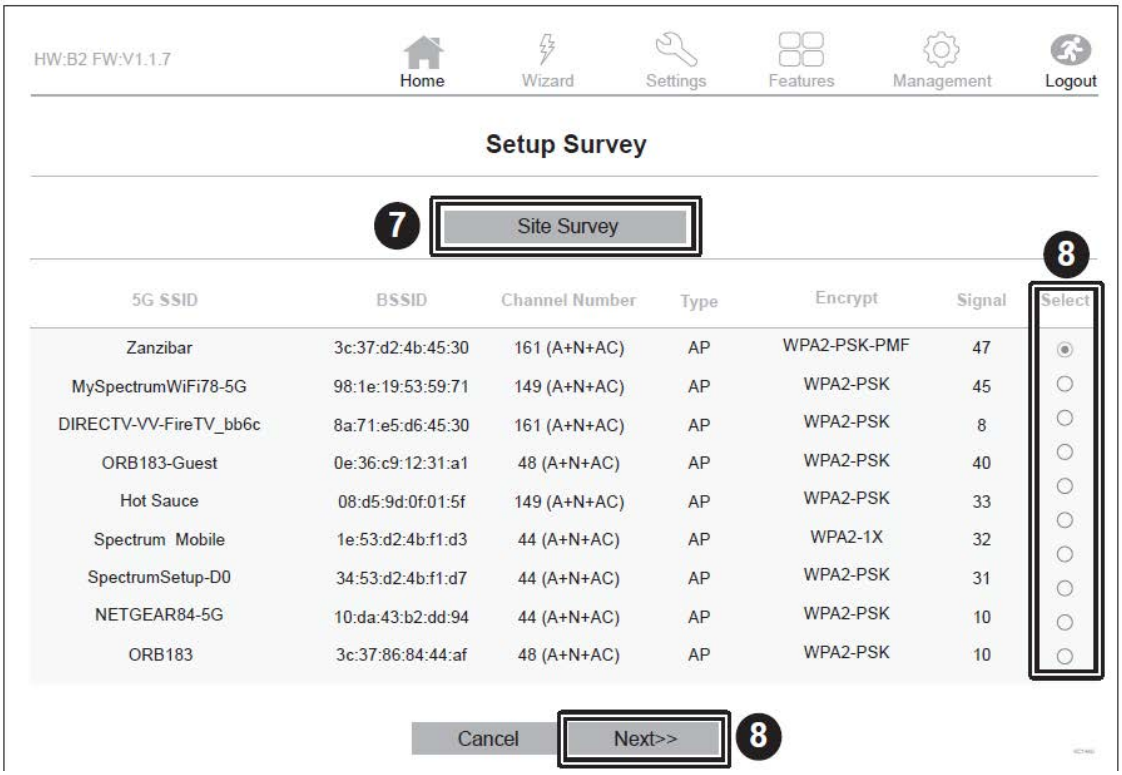
5. Locate “WISP” (Wireless ISP) at the bottom of the drop-down menu and select either “5G” or “2.4G.” This will determine the specific Wi-Fi band that the Passport uses to search for and repeat Wi-Fi.

6. After selecting 5G or 2.4G, select “Settings” to go to the next step to scan for Wi-Fi connections.



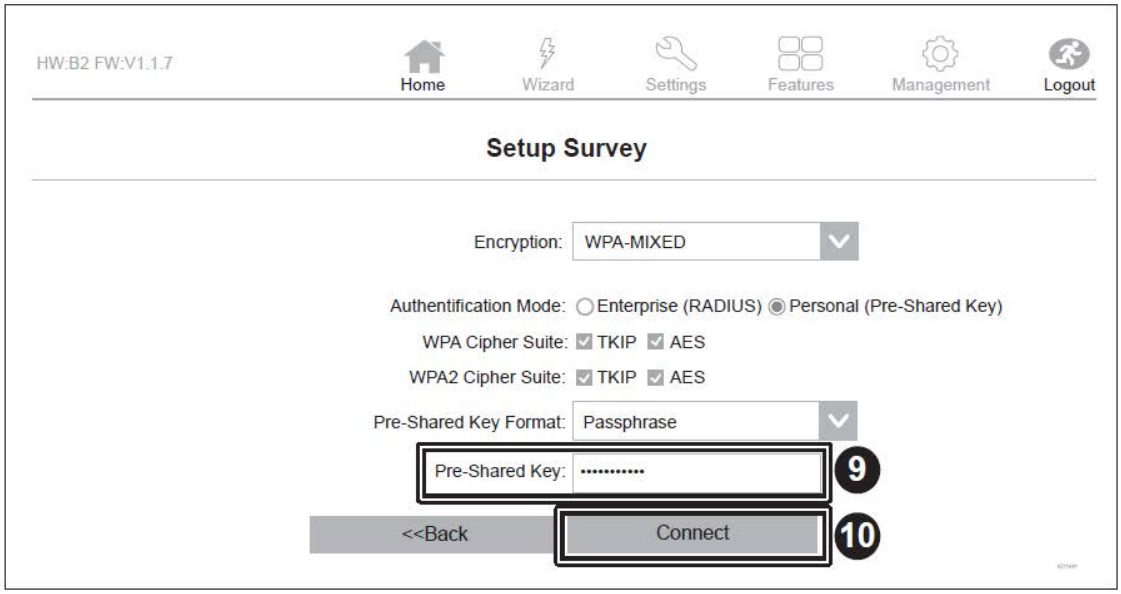
7. Select “Site Survey” and the Passport will scan for Wi-Fi access points in the area. After scanning, check that you are still connected to the Passport’s Wi-Fi.

8. Select the network you want to connect to. Select “Next>>” to continue.

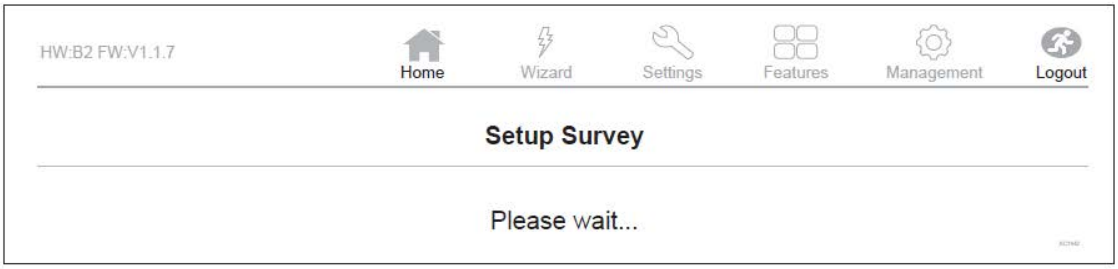


9 Enter the password (Pre-Shared Key) for your selected Wi-Fi network.

10 Select the “Connect” button.

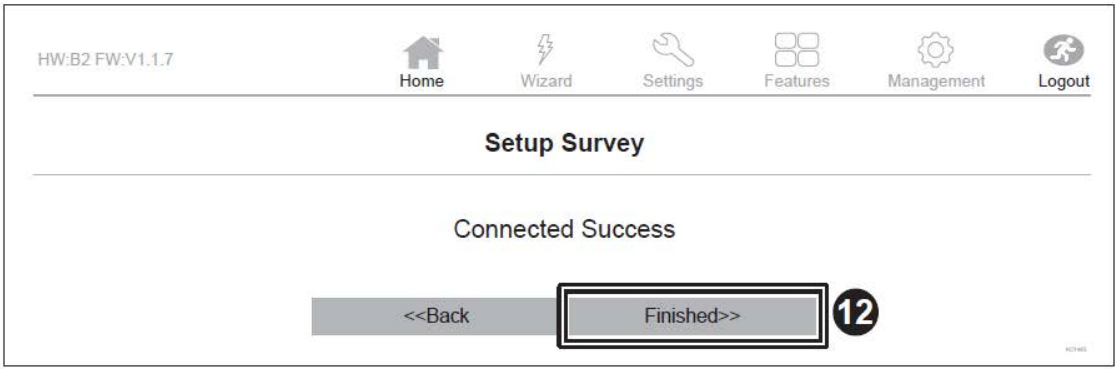


11 The Passport will now attempt to connect to the Wi-Fi network.



12 If the connection is successful, you will see this screen.

Select “Finished>>.”



13 The Passport will now reconfigure for Wi-Fi repeating.

Wait 30 seconds and reconnect to the Passport's Wi-Fi.

TIP! Ensure you re-connect to the Passport using the opposite band Wi-Fi network. Example: If repeating a 2.4 GHz network, select the 5.8 GHz Wi-Fi network from the Passport and vice versa.

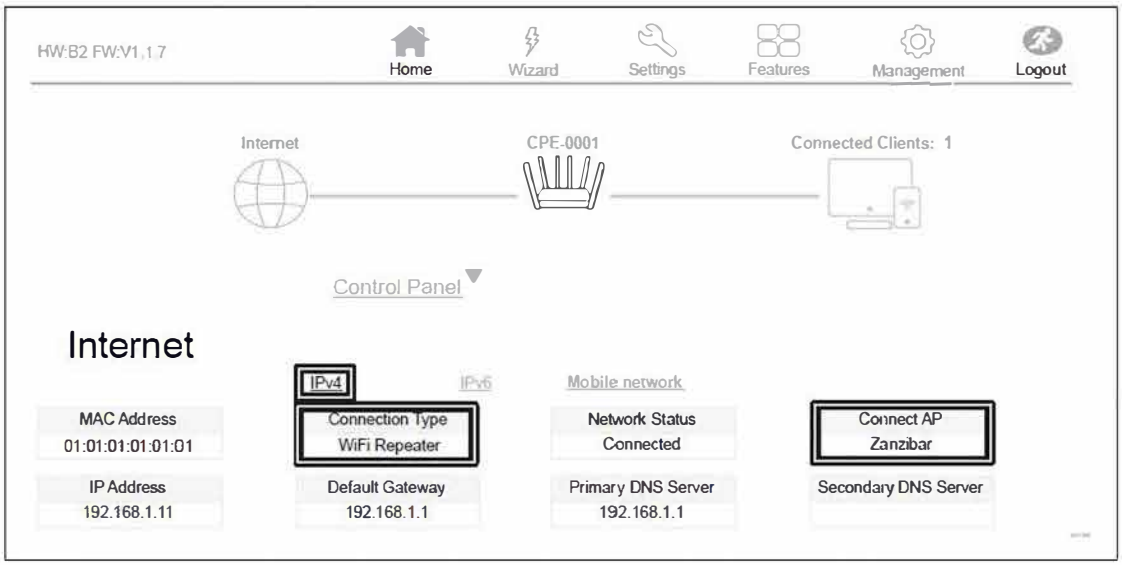
After approximately 30 seconds, the Passport should now be repeating Wi-Fi.

OPERATING NOTES: Wi-Fi and Connection Status

To confirm that the Passport is connected and repeating Wi-Fi, go to your web browser and return to http://192.168.0.1. If required, log back into the Passport.

On the Home page, select IPv4. "Connection Type" should display "WiFi Repeater."

After a few seconds, the section under "Connect AP" should list the name of the current Wi-Fi network being repeated by the Passport (you chose this network on page 5.)



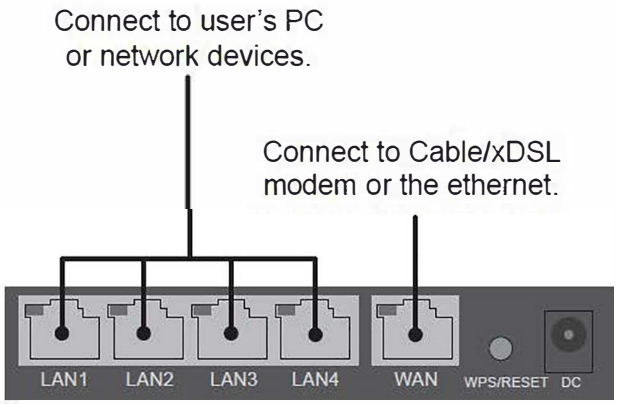
OPERATING NOTES: Switching between Wi-fi Repeating and Cellular Data

If you'd like to switch back to Cellular data at any time, go to the "Settings" page. Under "Default Route" select the drop-down menu next to "Default Mode" and select "Cellular" instead of "WAN 1." Then select "Save and Apply" at the bottom of the page.

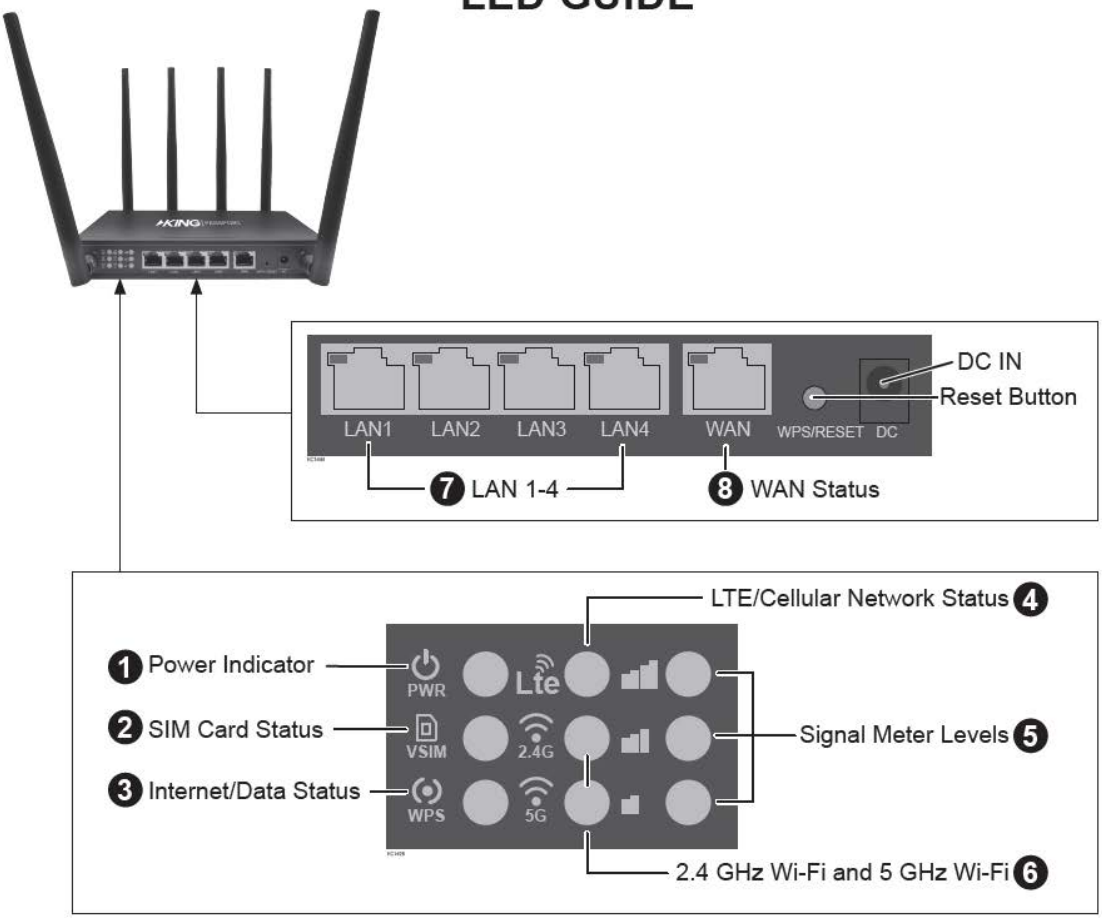
To switch back to active Wi-Fi, open the drop-down and re-select "WAN 1."
Then select "Save and Apply" again.

TIP You must manually switch between Cellular Data mode and Wi-Fi repeating/extending mode. The Passport does not switch automatically.

OPTIONAL HARD-WIRED CONNECTIONS



LED GUIDE



LED		STATE	FUNCTION
1	Power Indicator	ON	Device power on.
		OFF	Device power off.
2	SIM Card Status	ON	Virtual SIM mode is on.
		OFF	Physical SIM mode is on.
3	Internet/Data Status	FLASH	WPS is activated and ready to connect.
		OFF	WPS is not activated.
4	LTE/Cellular Network Status	ON	LTE is connected.
		FLASH	Device is transmitting data over LTE.
		OFF	LTE is not working.
5	Signal Meter Levels	ALL OFF	Device is not connecting over LTE.
		1 LED	LTE signal strength is low.
		2 LED	LTE signal strength is medium.
		3 LED	LTE signal strength is high.
6	2.4GHz/5GHz Wi-Fi	ON	The 2.4GHz/5GHz Wi-Fi is on.
		FLASH	Device is transmitting data over 2.4GHz/5GHz Wi-Fi.
		OFF	The 2.4GHz/5GHz Wi-Fi is off.
7	LAN 1-4	ON	LAN port is connected.
		FLASH	Device is transmitting data via the port.
		OFF	LAN port is not connected.
8	Wan Status	ON	WAN port is connected.
		FLASH	Device is transmitting data via WAN port.
		OFF	WAN port is not connected.

TROUBLESHOOTING

1 How do I restore factory settings?

With the router connected to power, use a pointed object (like the end of a paper clip) to press the reset button for 10 seconds. Release the button. After about 5 seconds the LAN/WAN lights will blink 3 times. The router should now be reset and the power light should turn on.
NOTE: Restoring to factory settings will revert the router to its default settings.

2 What should I do if I forget the Wi-Fi password or the login password for the Router Management Portal?

Restore the router to its factory settings, and then use the default Wi-FI password and username on the bottom of the router to access the portal.

3 What should I do if the internet connection cannot be established?

1. Restore the router to factory settings and try again.
2. Contact your service provider and request assistance.

4 What should I do if the internet speed is slow?

1. Check the LTE signal strength indicator on your router. If it shows a weak signal, adjust the router direction, or move it close to a window to improve signal reception.
2. If your device is connected to the router over Wi-Fi, adjust your device's position or move it closer to the router to receive a better signal.
3. Try restarting the router and your connected device.

5 If you are experiencing any other issues with the router:

1. Restart the router.
2. Restore the router to its factory settings.
3. Contact your service provider.

APPENDIX

FCC 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 into 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

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), and at least 48cm from all persons (outdoor). It must not be co-located or operating in conjunction with any other antenna or transmitter.

SAFETY WARNINGS

Do not use any other power adapter except the one that accompanies this unit as listed below.
The use of another adapter could result in damage to the unit.
The following power adapter is qualified for use with this KING Passport: model DCT18W120150US-A0 AC/DC adapter.

Connect the power cord of the power adapter to a socket outlet with a grounding connection.

Do not use the Passport in a damp or wet location.

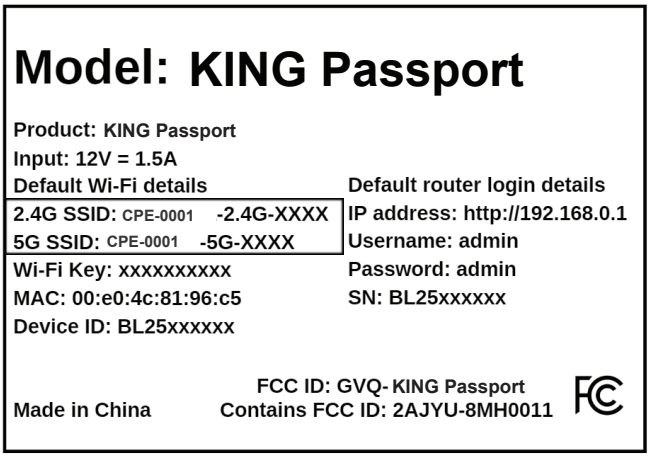
REFERENCE

Accessing the Web User Interface: Log In and Set Up: Setup Wizard

3.1. Login

After turning on the Passport connect to it via Wi-Fi by following these steps:

1. Locate the default SSID (network name) and the default Wi-Fi key (password) on the sticker located on the bottom of the router.
2. On your mobile device, access the Wi-Fi settings menu. Select the SSID (network name) and enter the default Wi-Fi key (password) from Step 1.
    a. Either 2.4G SSID or 5G SSID is fine to connect to.

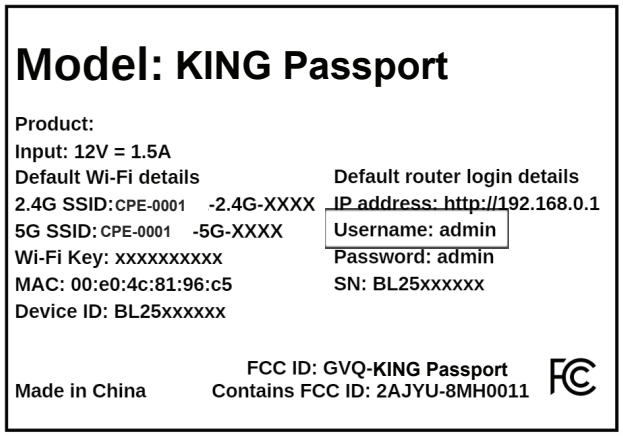


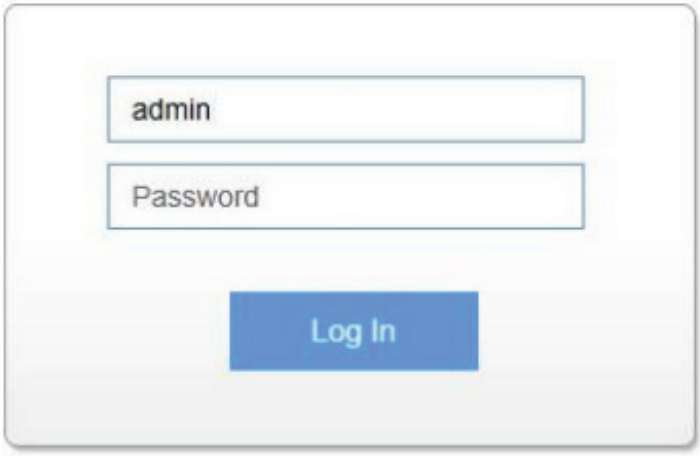
After connecting to Wi-Fi, access the Web User Interface by following this step:

1. On your mobile device, navigate to an internet search browser, and input the IP address of **192.168.0.1**, then click enter.

After navigating to the Web User Interface, log in by following this step:

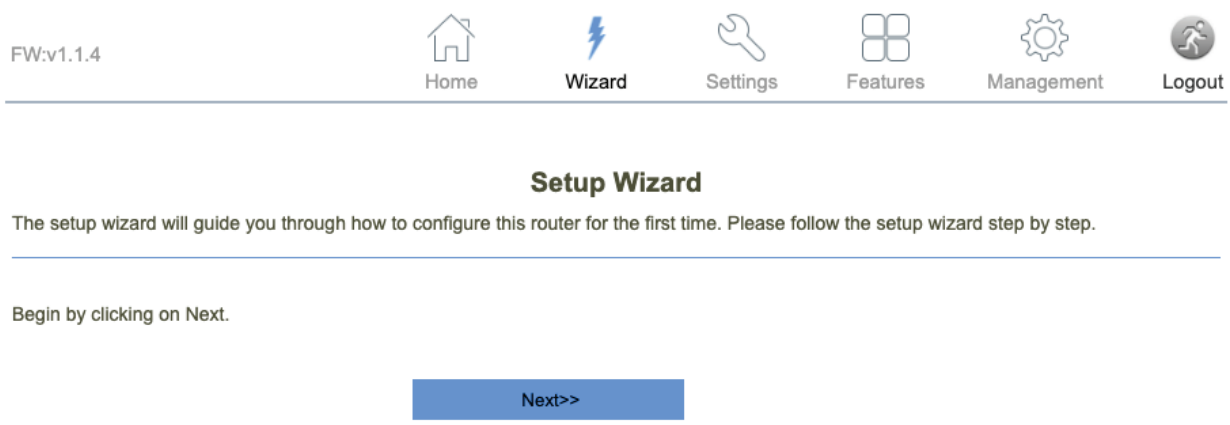
1. On your mobile device, login to the Web User Interface's **Home Page** using the default user name of **admin** and the default password which will be a series of letters and numbers. Both of these can be found on the sticker located on the bottom of the router.



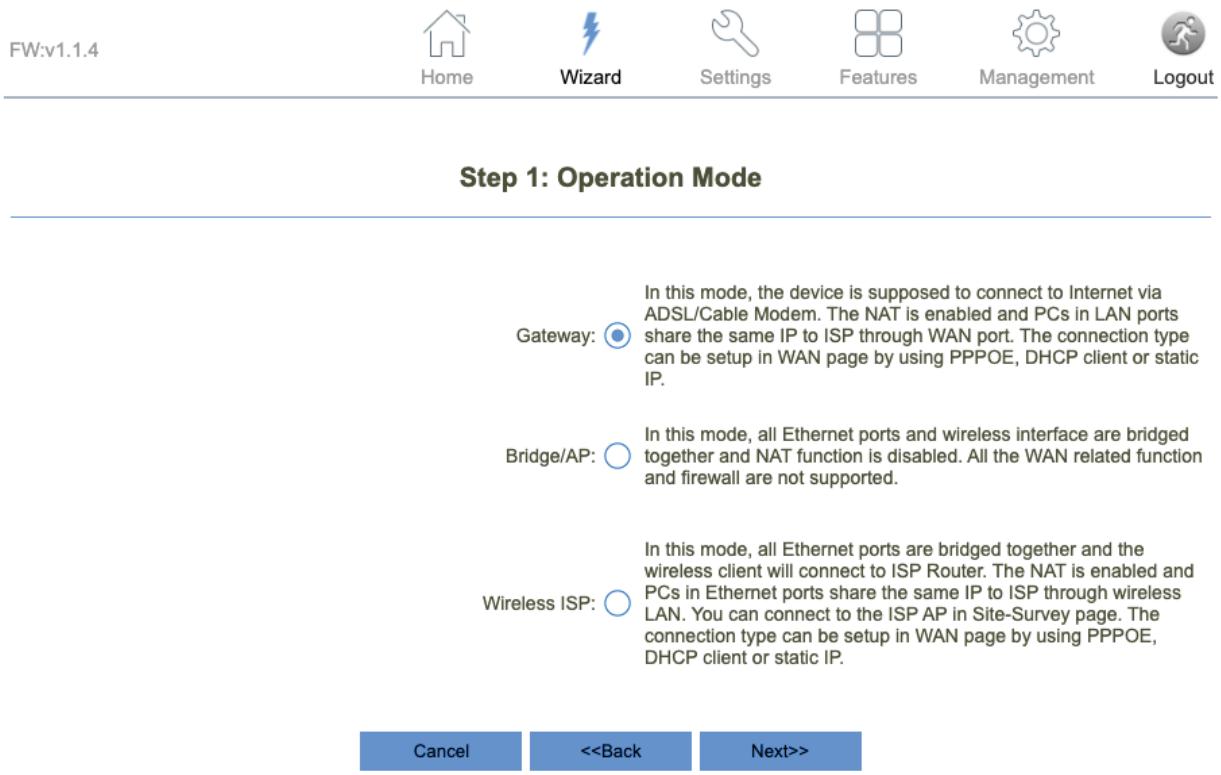


3.2 Setup Wizard

After logging into the Passport , the **Setup Wizard** will appear. The **Setup Wizard** will guide users along the Passport configuration steps, it is imperative they follow the guide step by step.



Step 1: Operation Mode



The **Operation Mode** page is used to toggle the Passport between different operational modes; Gateway, Bridge/AP mode, and Wireless ISP.

To ensure your device works on your pre-selected data plan, you must start by selecting **Gateway**, you can always go back and change this selection at a later time if you wish.

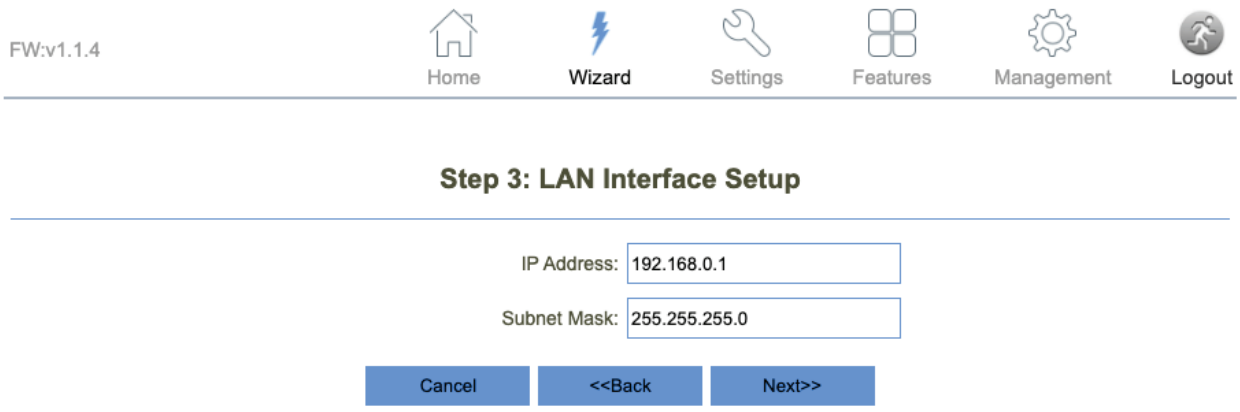
Step 2: WAN Interface Setup

The **WAN Interface Setup** page is used to set the WAN Access Type.

You do not need to set up the WAN Interface at this moment, you can always go back and set it up at a later time.

Skip this step and click Next.

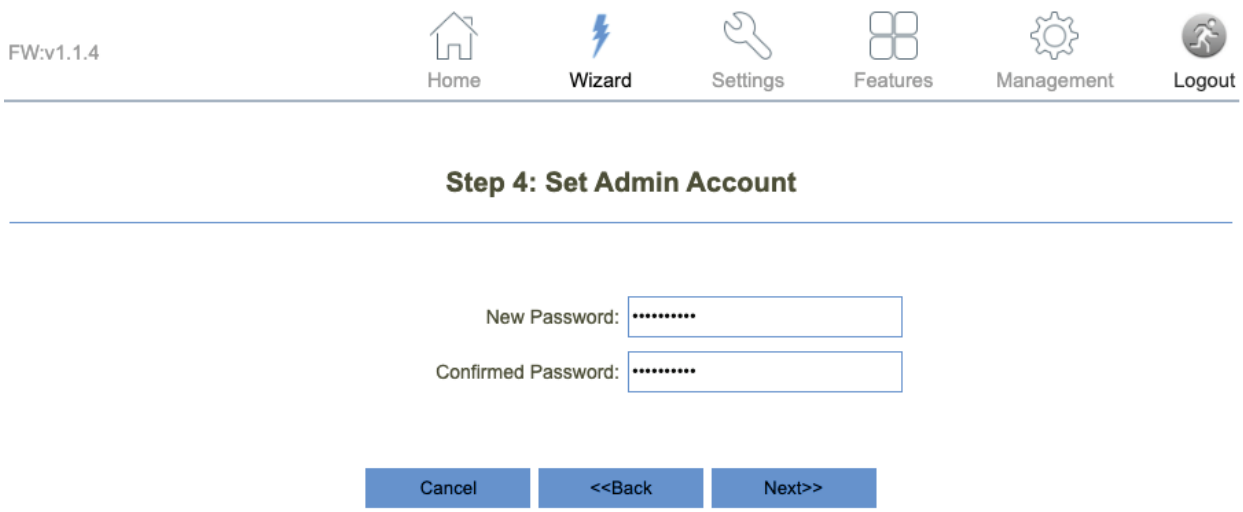
Step 3: LAN Interface Setup



The **LAN Interface Setup** page is used to configure the IP Address and Subnet Mask if you are connecting an external router to the Passport via LAN.

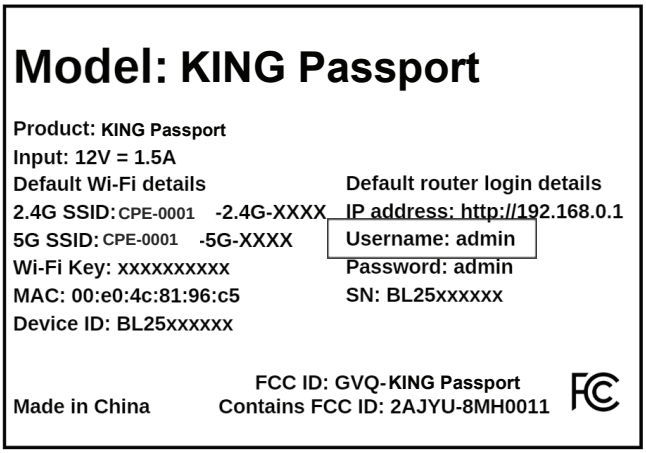
You do not need to set up the LAN Interface at this moment, you can always go back and set it up at a later time.

Step 4: Set Admin Account



The **Set Admin Account** page is used to set the new user interface (router log-in) password.

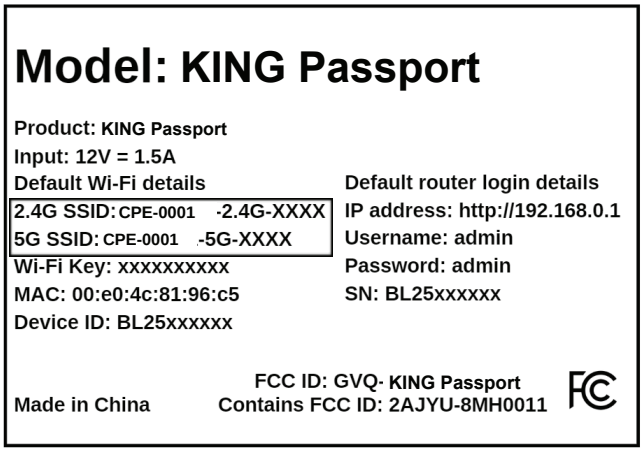
The pre-set user and password can be found on the sticker located on the bottom of the router.



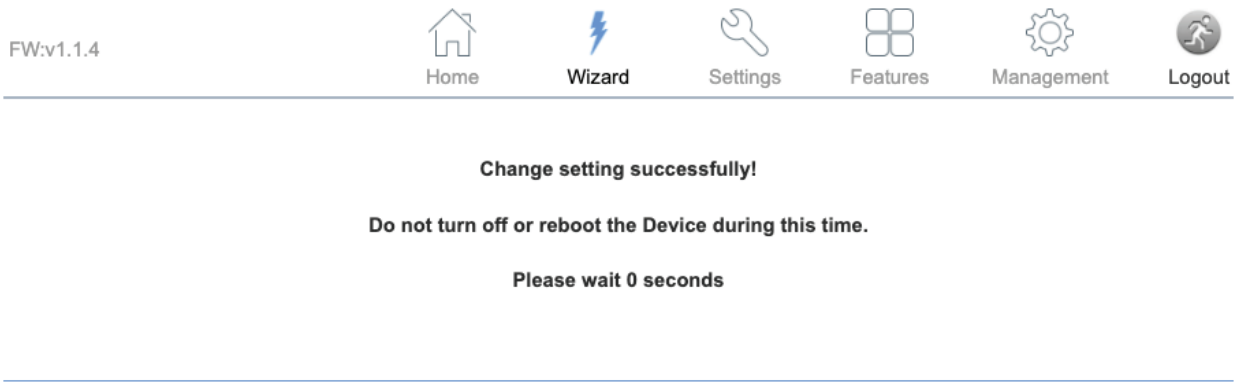
Step 5: Setup Wireless

The **Setup Wireless** page is used to set the SSID and password for both the 2.4GHz and 5GHz Wi-Fi networks.

It is also used to enable or disable either of the Wi-Fi networks.



Step 6: Automatic Reboot



The Passport will reboot once you have clicked the finished button on Step 6 to apply the changes you have made.

Remember to connect back to the router's broadcasted Wi-Fi network to connect to it again.

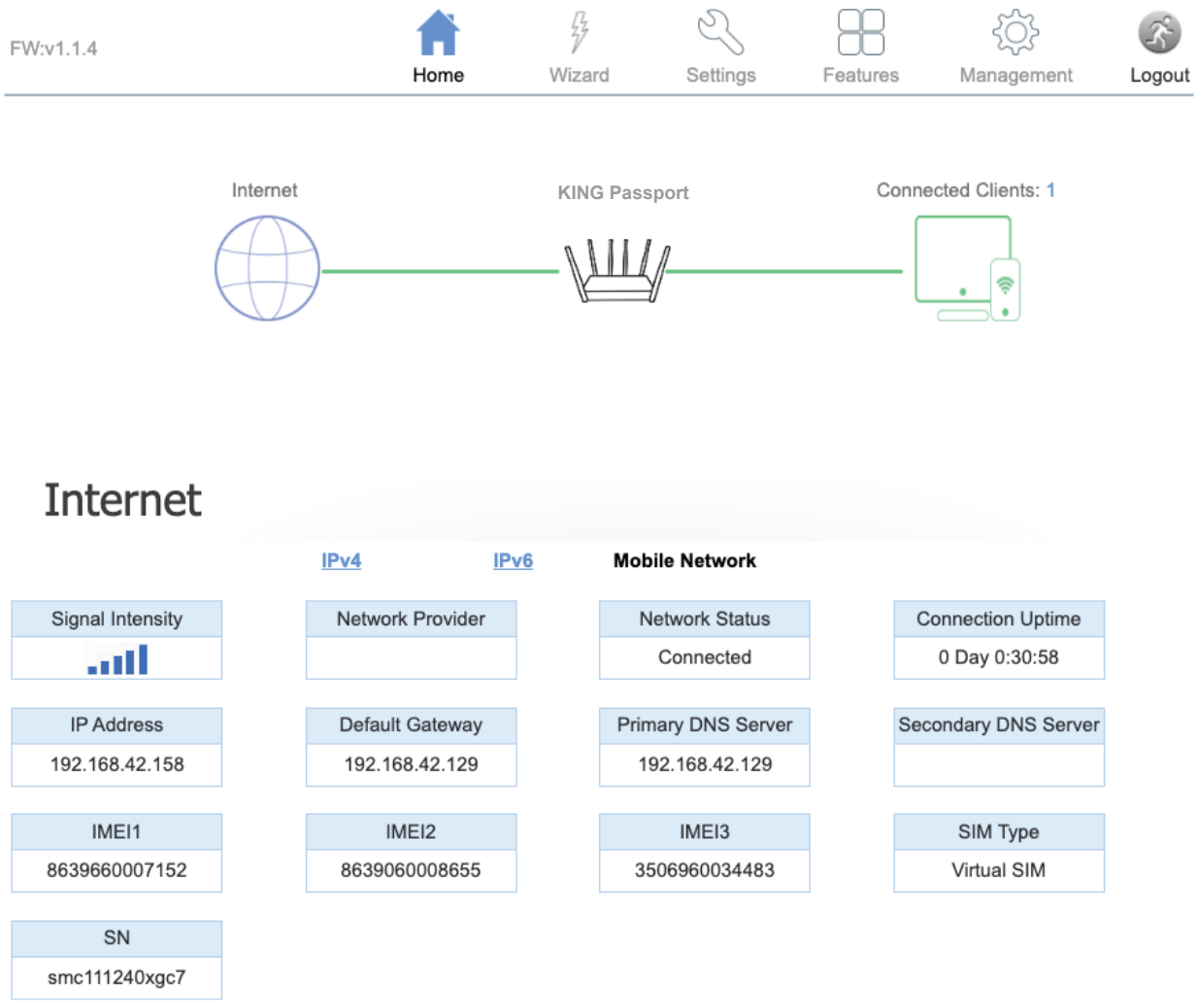
Remember, you may have changed what that looks like in the previous step.

Chapter 3

Accessing the Web User Interface: Understanding the Home Page

3.3. Home Page/Main Section

After completing the Setup Wizard, the **Home Page** of the Passport will appear.

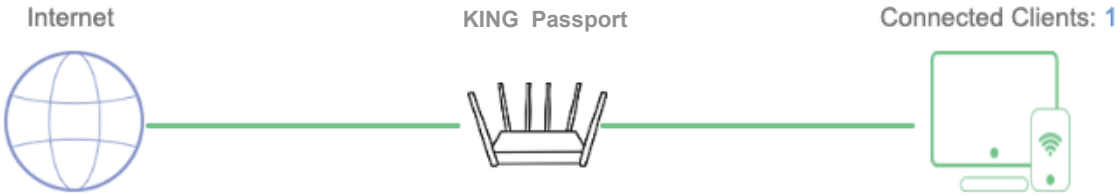


The **Home Page** is where users can check the connection status between the Passport and the Internet, and adjust settings such as Wi-Fi options, parental controls, and more.

3.3.1 Banner

At the top of the **Home Page**, a banner consisting of icons is presented. Each of these icons represents a sub-section, we will explore each sub section in this guide. We have already explored the Wizard sub-section earlier in this chapter. To the left of the icons, the current firmware version (FW) of the Passport is displayed.

3.3.2 Network Map



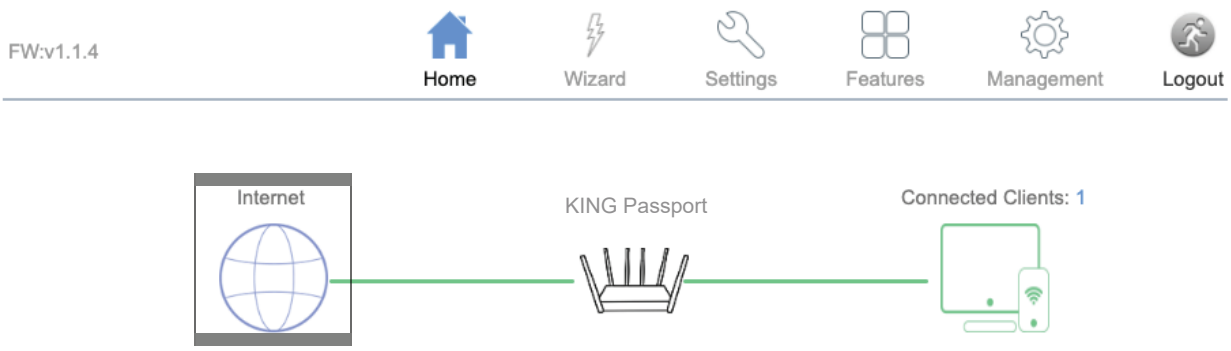
The **Network Map** is located in the middle of the **Home Page.** The line between the Internet Globe, the Passport , and the Internet devices on the map indicate the connection status between them.

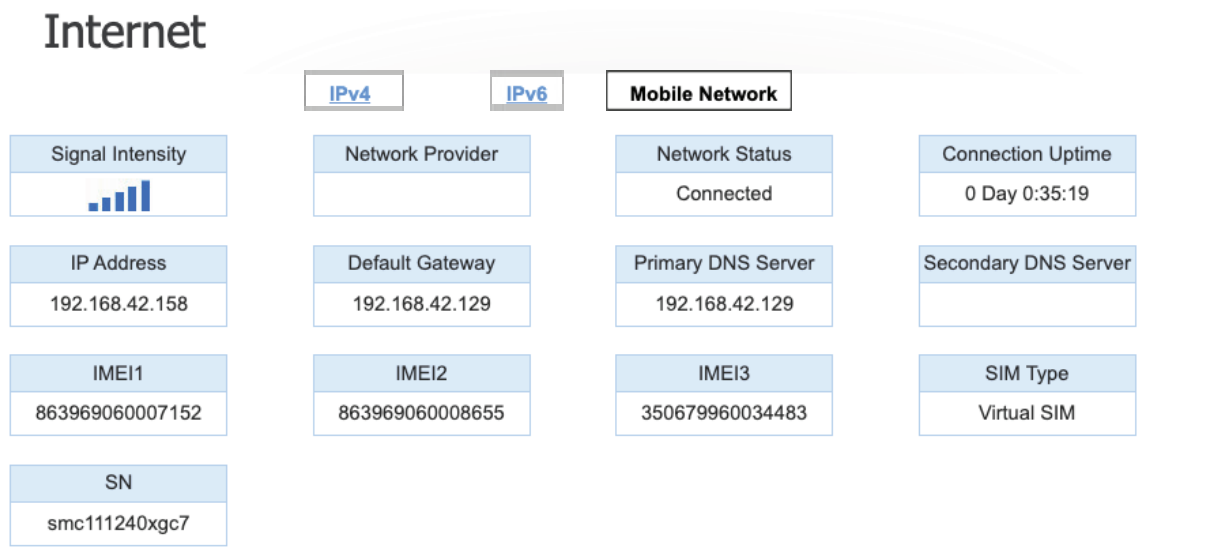
A solid green line indicates a successful connection, whereas a red line with an x in the idle indicates that there is no connection.

If there is a red line with an x in the idle between the Internet Globe and the Passport there is no 4G LTE connection present. If there is a red line with an x in the idle between the Internet Globe and Passport it is an indication that there is no Wi-Fi connection between the Passport and Internet devices either over Wi-Fi or via LAN.

The Internet Globe image, the Passport image, and the Desktop Image are all clickable and reveal menus.

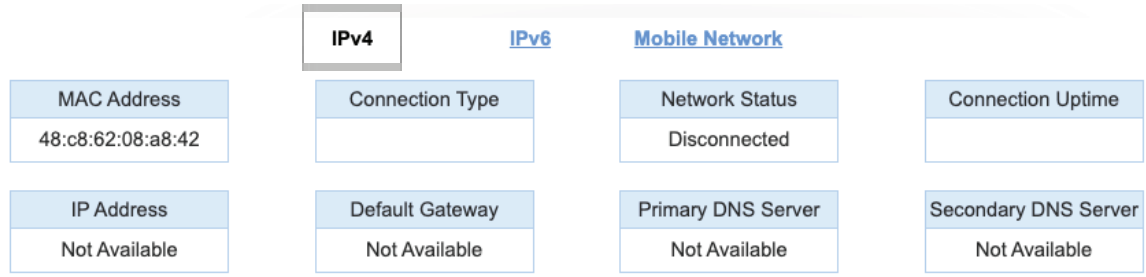
3.3.3 Internet





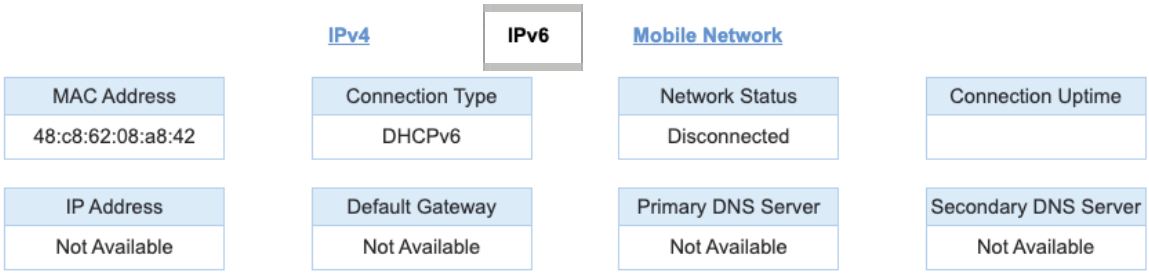
The **Internet** section is divided into three distinct sections: IPv4, IPv6, and Mobile Network.

3.3.3.1 IPv4 or Internet Protocol Version 4



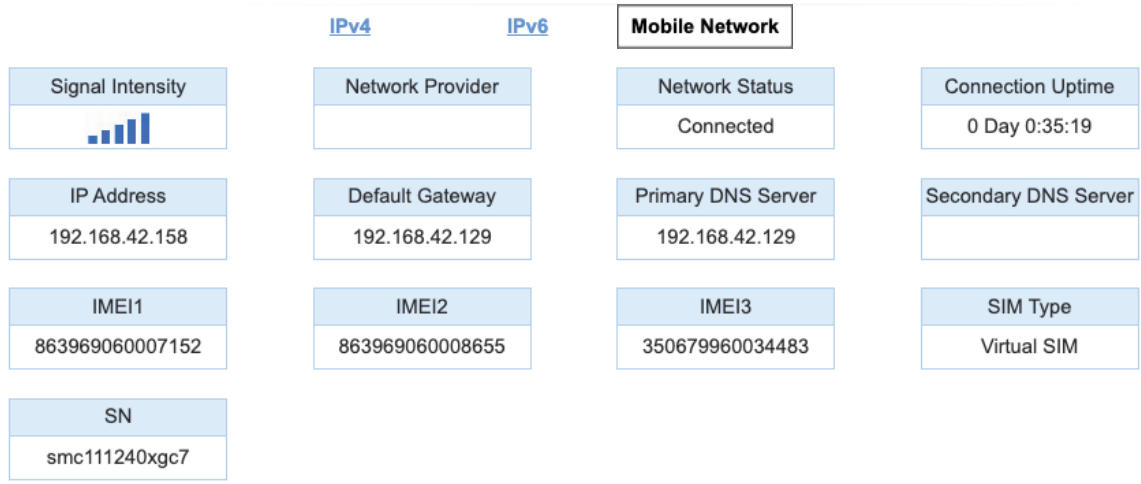
Item	Description
MAC Address	The MAC Address or the Media Access Control address is a unique serial number in the network circuitry of every Ethernet and Wi-Fi device.
Connection Type	Dynamic Host Configuration Protocol Version
Network Status	The connection status between the Passport and the internet when using the WAN port.
Connection Uptime	The period of time the Passport has been connected to the internet.
IP Address	An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network.
Default Gateway	The IP address of another router yourPassport sends traffic too.
Primary DNS Server	The first touchpoint for a browser asking where to find a site.
Secondary DNS Server	The second touchpoint for a browser asking where to find a site in the case that the Primary DNS Server is unavailable.

3.2.2.2 IPv6 or Internet Protocol Version 6



Item	Description
MAC Address	The MAC Address or the Media Access Control address is a unique serial number in the network circuitry of every Ethernet and Wi-Fi device.
Connection Type	Dynamic Host Configuration Protocol Version
Network Status	The connection status between the Passport and the internet when using the WAN port.
Connection Uptime	The period of time the Passport has been consistently connected to the internet.
IP Address	An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network.
Default Gateway	The IP address of another router your Passport sends traffic too.
Primary DNS Server	The first touchpoint for a browser asking where to find a site.
Secondary DNS Server	The second touchpoint for a browser asking where to find a site in the case that the Primary DNS Server is unavailable.

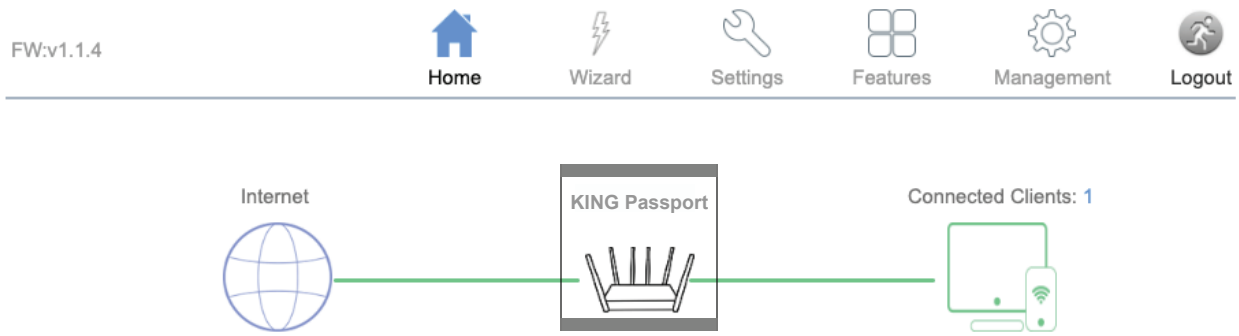
3.2.2.3 Mobile Network



Item	Description
Signal Intensity	The cellular signal strength of the Passport .
Network Provider	The local cellular network your Passport connects to.
Network Status	The connection status between the Passport and the internet when using vSIM.
Connection Uptime	The period of time the Passport has been connected to the internet.
IP Address	An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network.
Default Gateway	The IP address of another router your Passport sends traffic too.
Primary DNS Server	The first touchpoint for a browser asking where to find a site.
Secondary DNS Server	The second touchpoint for a browser asking where to find a site in the case that the Primary DNS Server is unavailable.

IMEI (1,2,3)	IMEI or International Mobile Equipment Identity is a unique number for identifying a device on a mobile network.
SIM Type	Whether the Passport is connecting to the internet via Virtual Sim or Physical Sim.
SN	The Passport 's Serial Number.

3.3.4



IPv4 Network	
MAC Address:	48:c8:62:08:a8:41
Router IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0

IPv6 Network	
Link-Local Address:	fe80::4ac8:62ff:fe08:a841
Router IPv6 Address:	Not Available

System	
Uptime:	3 Days 0:59:51
Build Time:	Mon Sep 26 09:41:47 CST 2022

CPU	
CPU Usage:	18.00%
Memory (Free/Total):	51776/106080

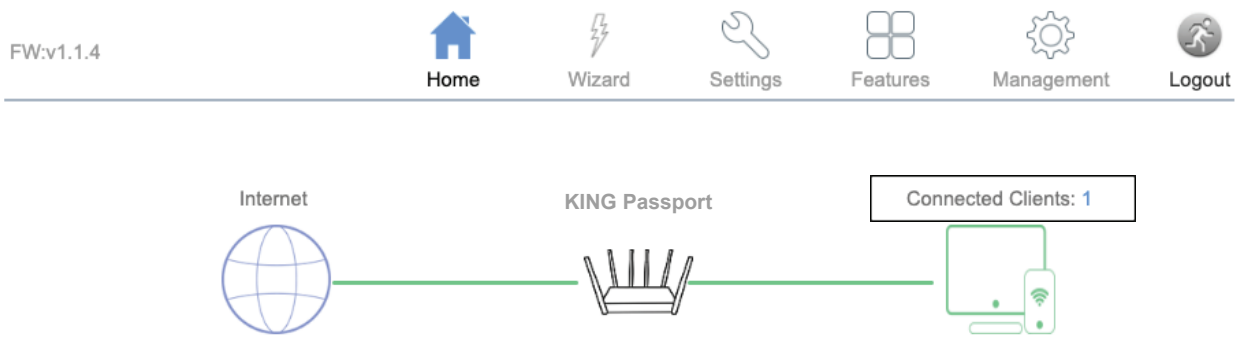
Wi-Fi 2.4GHz	
Status:	Up
Wi-Fi Name (SSID):	Passport -2.4G-a841
Encryption:	WPA2-WPA3-Mixed
BSSID:	48:c8:62:d8:a8:41
Channel Number:	7

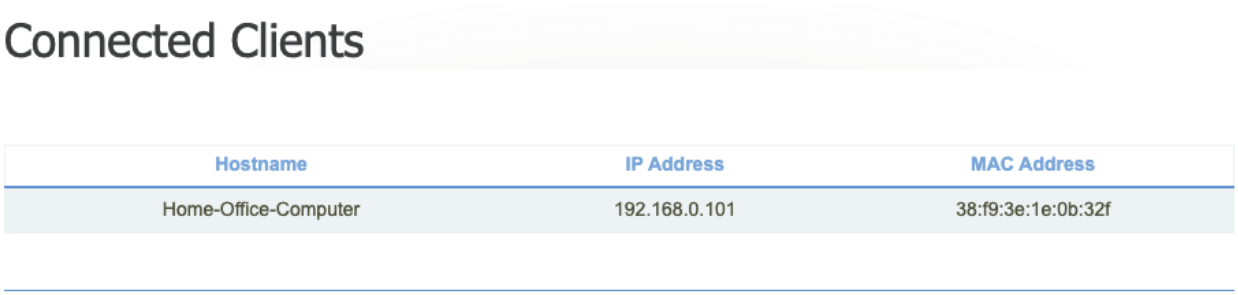
Wi-Fi 5GHz	
Status:	Up
Wi-Fi Name (SSID):	Passport -5G-a841
Encryption:	WPA2-WPA3-Mixed
BSSID:	48:c8:62:58:a8:41
Channel Number:	161

Clicking the Passport image provides a combined overview of the same internet sections that were found under the Global Internet Image.

Item	Description
MAC Address	The cellular signal strength of the Passport .
Router IP Address	The Passport ’s IP address.
Subnet Mask	A number that resembles an IP address. It reveals how many bits in the IP address are used for the network by masking the network portion of the IP address
Link-Local Address	A network address that is valid only for communications within the subnetwork that the host is connected to.
Router IPv6 Address	A numeric label that is used to identify and locate a network interface of a computer or a network node participating in a computer network using IPv6.
CPU Usage	The percentage of total CPU capacity being used at any given time.
Memory (Free/Total)	The amount of memory used.
Status	An indication of whether or not the 2.4GHz and 5GHz Wi-Fi networks are emitting.
WiFi Name (SSID)	The network name.
Encryption	The encryption type currently being used to secure your wireless network with an authentication protocol.
BSSID	Basic Service Set Identifier.
Channel Number	The Wi-Fi channel your Passport is emitting Wi-Fi through.

3.2.1 Connected Clients





There is a clickable number and logo above the Connected Client's image which represents the number of devices connected at any given point in time.

Item	Description
Hostname	Name(s) of the connected personal devices to the Passport 's emitted Wi-Fi network.
IP Address	An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network.

MAC Address	The MAC Address or the Media Access Control address is a unique serial number in the network circuitry of every Ethernet and Wi-Fi device.

Chapter 3
Accessing the Web User Interface: Settings

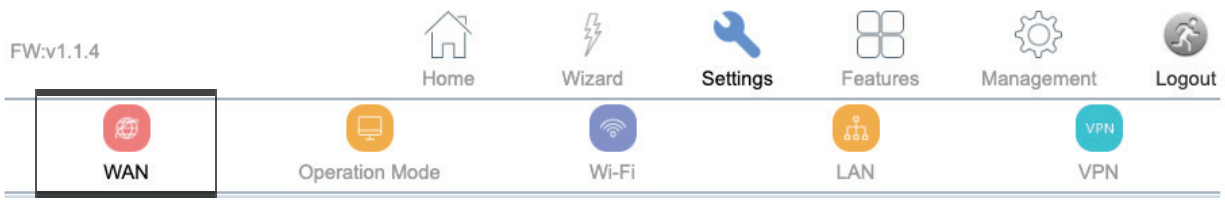
3.4. Settings

After selecting the wrench tool icon on the banner atop the GUI, the **Settings** of the Passport will appear.

The **Settings** is where users can toggle the Passport between Virtual and Physical Sim, rename the default SSID (network name), change the default Wi-Fi password, set the Wi-Fi security mode, scan for access points, enable or disable WPS functions, and set the Wi-Fi band as either 2.4GHz or 5.0GHz, amongst other features. It is divided into five distinct sections which all have their own subsections.

3.4.1 WAN

The **WAN** page is used to configure the parameters for the internet network that connects to the WAN port of the Passport. The page is divided into six distinct sections, those being Default Route, SIM Mode, IPv4, IPv6, Status, and VLAN.



3.4.1.1 Default Route

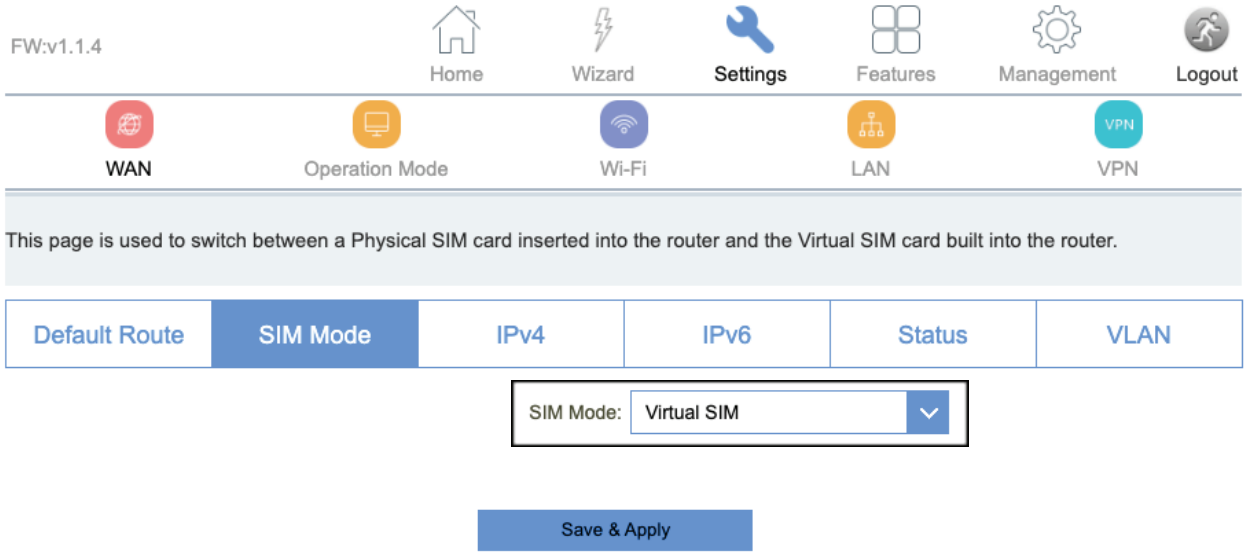
The **Default Route** page enables the user to select which WAN connection (WAN1 or Cellular) provides the source of the internet to the Passport .

Selecting “enable WAN failover to Cellular”, allows the Passport to automatically continue providing internet through Virtual Sim, if the router that you connected to it via the WAN port has failed.

3.4.1 SIM Mode

The **SIM Mode** page is used a toggle between a Physical SIM inserted in the router for internet and a Virtual built into the router for internet.

Virtual SIM

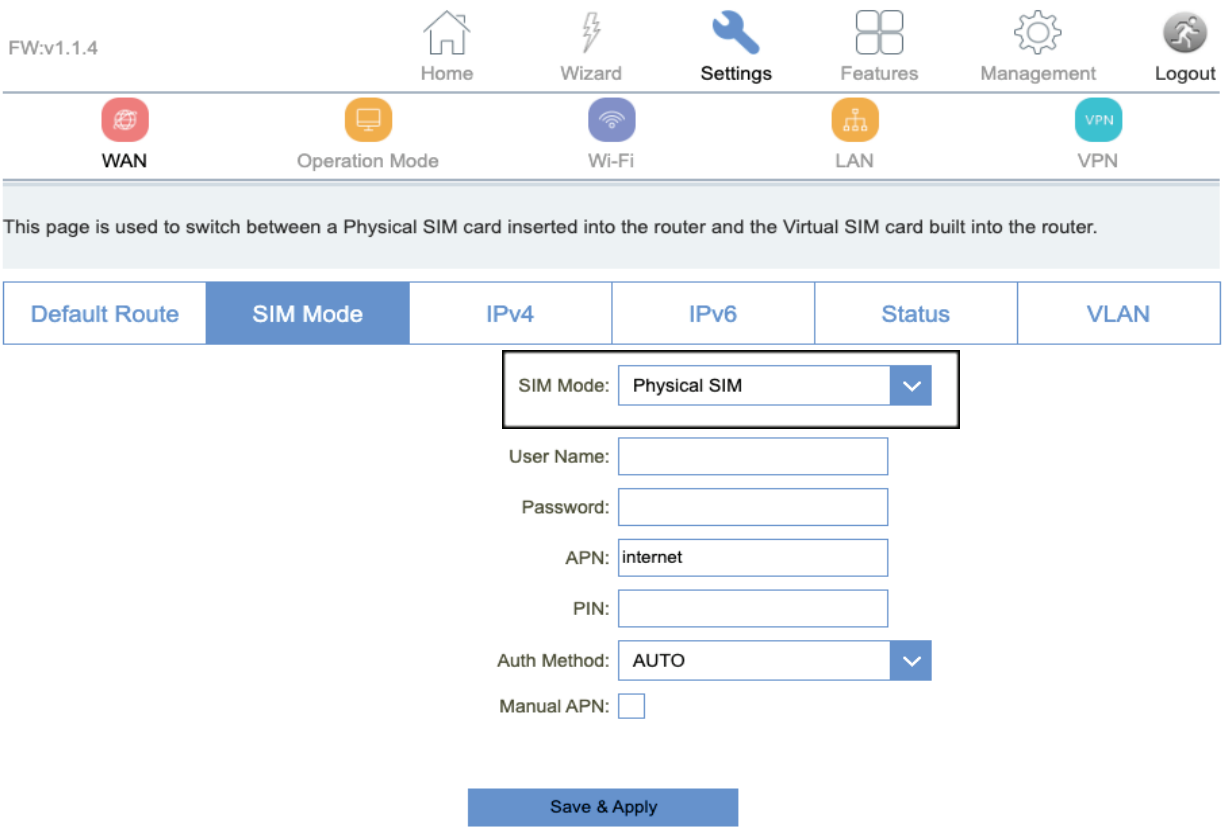


Make sure that Virtual SIM is selected so that your Passport will work on your data plan.

When using a Physical SIM card, toggle to Physical SIM and a menu will appear. Once you have inputted your desired changes click “Save & Apply”.

The Passport will reboot with your saved changes after 30 seconds. Be sure to connect to the Passport’s Wi-Fi network once the reboot is complete.

Physical SIM



Item	Description
SIM Mode	Physical Sim or Virtual SIM
User Name	The username associated with your physical sim data plan.
Password	The password associated with your physical sim data plan.
APN	The APN provided by your internet service provider.
PIN	The PIN provider by your internet service provider.
Auth Method PAP	Password Authentication Protocol
Auth Method CHAP	Challenge-Handshake Authentication Protocol

3.4.1.1 IPv4

The **IPv4** page is used to toggle between three WAN Access Types (modes) that can be used; DHCP, Static IP, and PPPoE. A fourth mode is available and takes the form of a VLAN tag and can be used if necessary.

3.4.1.1.1 DHCP (Dynamic IP)

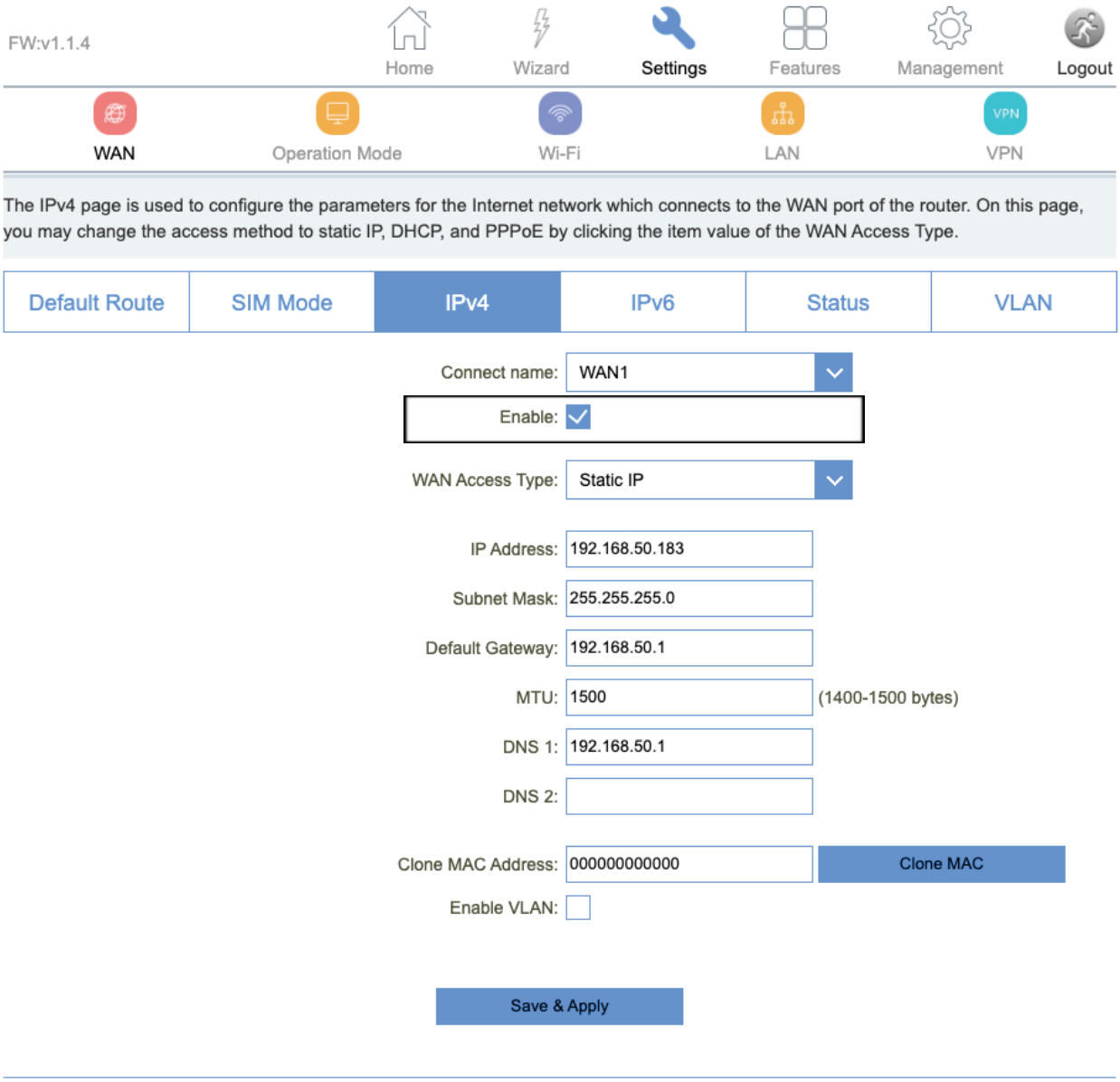
Selecting the Dynamic IP (DHCP) WAN Access Type will enable the router to automatically obtain IP addresses, subnet masks, and gateway addresses.

Selecting Dynamic IP (DHCP) WAN Access Type also enables you to set the MTU to allow smaller or larger data packages to flow into the Passport . You should not have to adjust this metric.

For large locations such as an office building or campus with a large grouping of computers or other devices all located in the same place, VLAN can be enabled.

Item	Description
MTU	Minimum Transmission Unit (to be kept as default).
VLAN ID	Identifies the VLAN to which a data frame belongs.

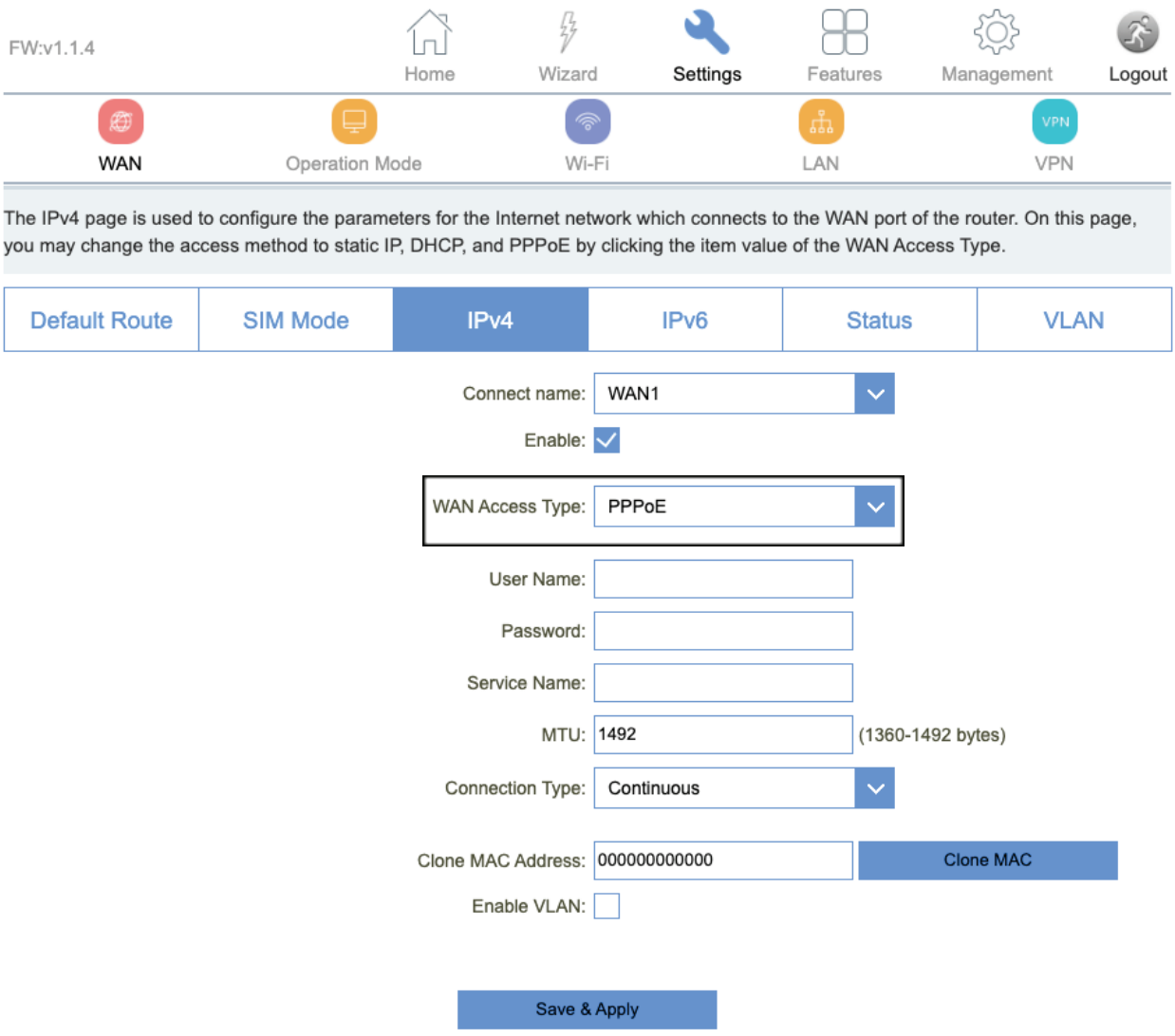
3.4.1.1.2 Static IP



Selecting the Static IP Access Type will enable the router to support Static IP as a WAN connection type.

Item	Description
IP Address	The cellular signal strength of the Passport .
Subnet Mask	A number that resembles an IP address. It reveals how many bits in the IP address are used for the network by masking the network portion of the IP address
Default Gateway	The IP address of another router your Passport sends traffic too.
DNS 1	Domain Name System 1
DNS 2	Domain Name System 2
MTU	Minimum Transmission Unit (to be kept as default).
VLAN ID	Identifies the VLAN to which a data frame belongs.

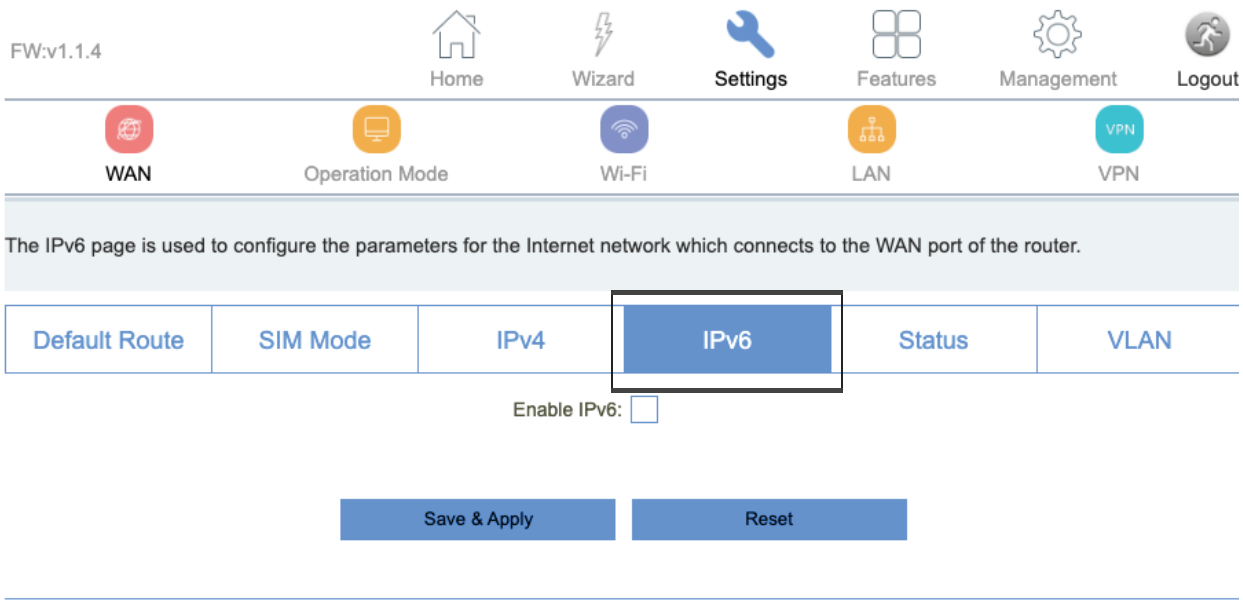
3.4.1.1.2 PPPoE



Selecting the PPPoE Access Type will enable the router to support PPPoE as a WAN connection type.

Item	Description
VLAN ID	Identifies the VLAN to which a data frame belongs.
Service Name	Passport
MTU	Minimum Transmission Unit (to be kept as default).
Connection Type: Continuous	Continuous
Connection Type: Connect on Demand	Connect on Demand
Connection Type: Manual	Manual

3.4.1.2 IPv6



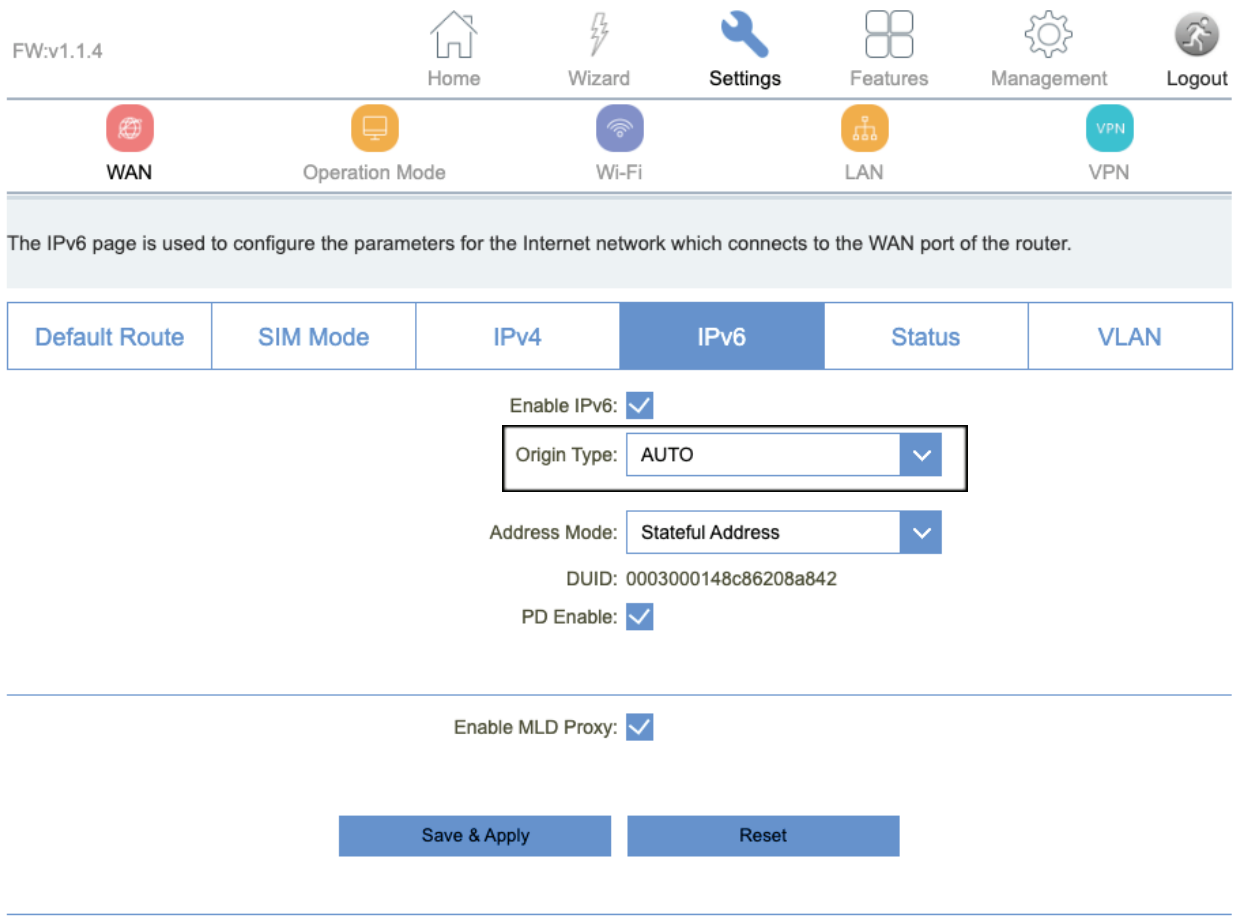
By enabling IPv6, a collapsable menu will appear, enabling the user to toggle between three distinct origin types, STATIC, AUTO, and 6RD.

3.4.1.2.1 STATIC

Item	Description
IP Address	The cellular signal strength of the Passport.

Default Gateway	The IP address of another router your Passport sends traffic too.
DNS 1	Domain Name System
MLD Proxy	Multicast Listener Discovery

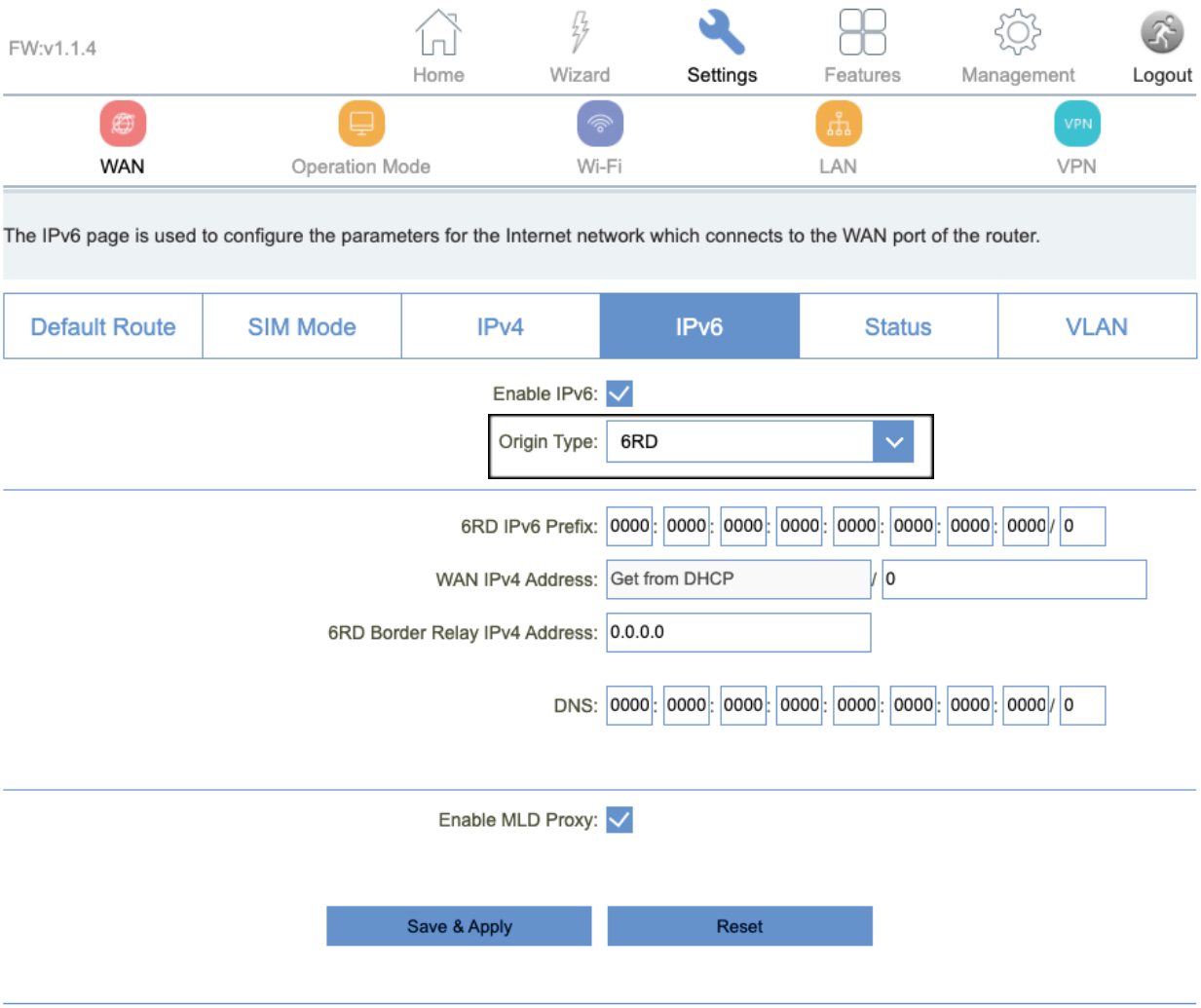
3.4.1.2.2 AUTO



Item	Description
Stateful Address	DHCP will supply an IPv6 address.

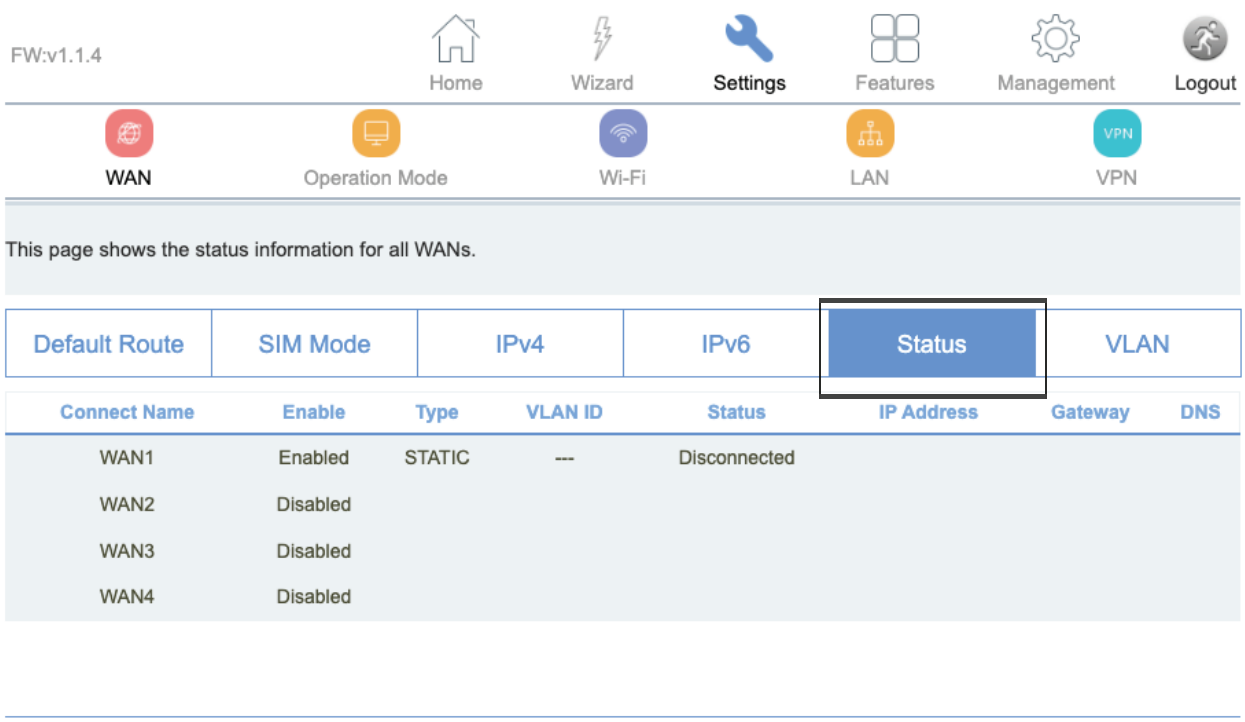
Stateless Address	DHCPv6 server does not provide IP addresses at all.
DUID	The DUID identified a DHCPv6 device.
PD	Prefix Delegation
MLD Proxy	Multicast Listener Discovery

3.4.1.2.1 6RD



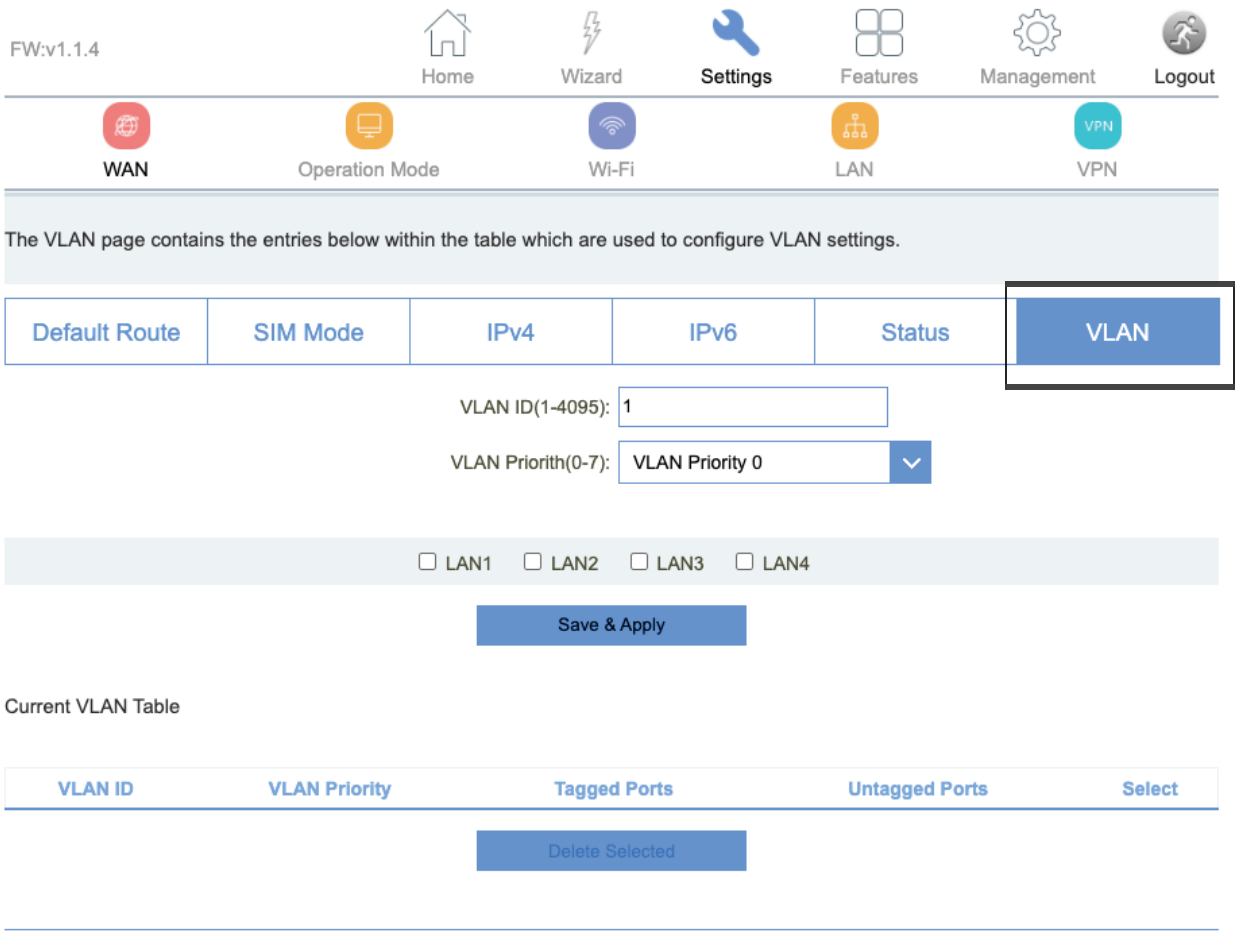
Item	Description
6RD IPv6 Prefix	WAN IPv6 prefix delegation.
WAN IPv4 Address	WAN IPv4 Address.
6RD Border Relay IPv4 Address	Border Relay IPv4 Address
DNS	Domain Name System
MLD Proxy	Multicast Listener Discovery

3.4.1.3 Status



The **Status** page will display the status of each WAN connection; WAN1, WAN2, WAN3, WAN4.

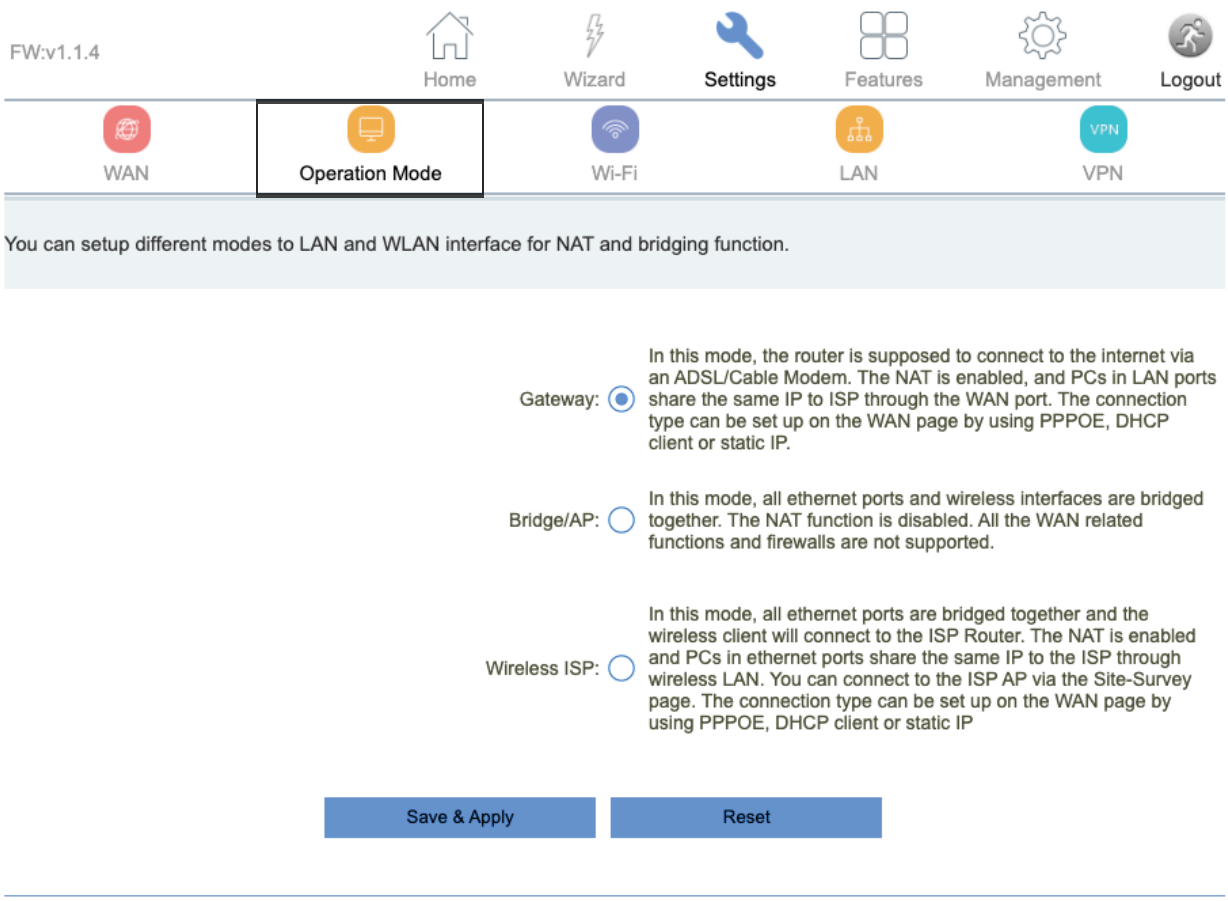
3.4.1.4 VLAN



The **VLAN** page is used to configure the VLAN settings.

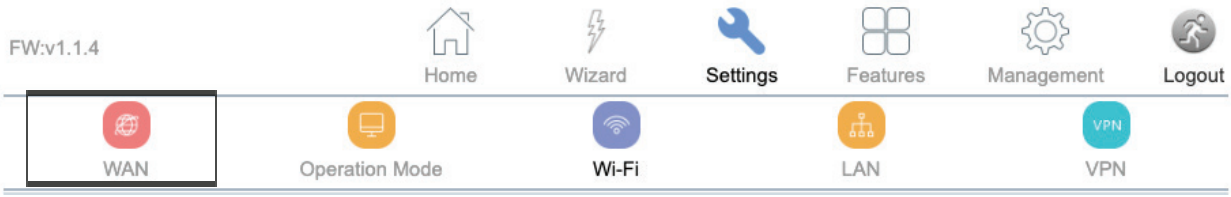
3.4.2.2 Operation Mode

The **Operation Mode** page is used to toggle the Passport between the different operational modes; Gateway, Bridge Mode, and Wireless ISP.



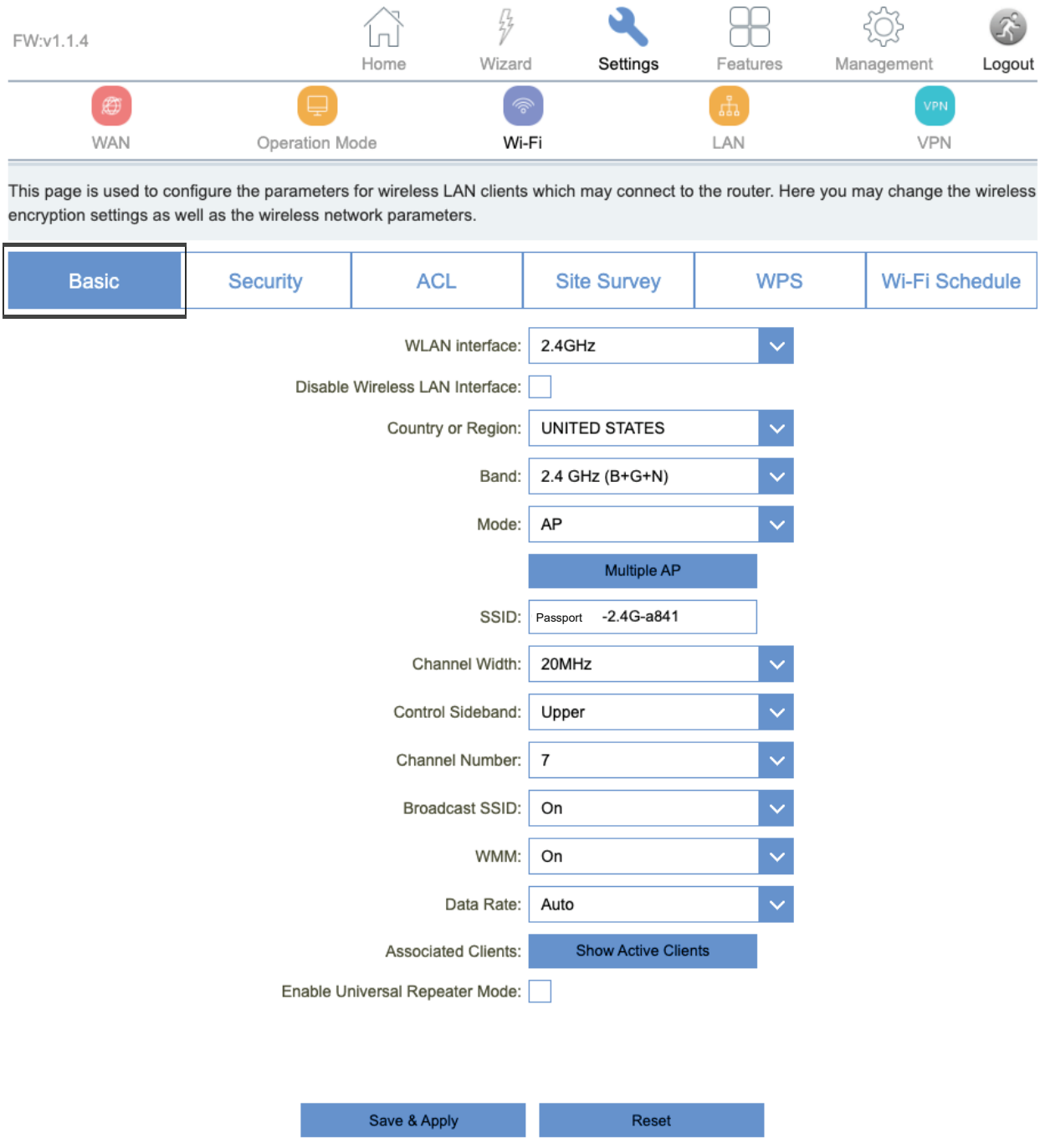
The Passport must remain on Gateway mode to work with your data plan.

3.4.3 Wi-Fi



The **Wi-Fi** section is used to configure the Passport ’s Wi-Fi settings.

3.4.3.1 Basic


FW:v1.1.4
Home
Wizard
Settings
Features
Management
Logout
WAN
Operation Mode
Wi-Fi
LAN
VPN
VPN
This page is used to configure the parameters for wireless LAN clients which may connect to the router. Here you may change the wireless encryption settings as well as the wireless network parameters.
Basic
Security
ACL
Site Survey
WPS
Wi-Fi Schedule
WLAN interface:
2.4GHz
Disable Wireless LAN Interface:
Country or Region:
UNITED STATES
Band:
2.4 GHz (B+G+N)
Mode:
AP
Multiple AP
SSID:
Passport -2.4G-a841
Channel Width:
20MHz
Control Sideband:
Upper
Channel Number:
7
Broadcast SSID:
On
WMM:
On
Data Rate:
Auto
Associated Clients:
Show Active Clients
Enable Universal Repeater Mode:
Save & Apply
Reset

The **Basic** page is used to toggle between and set up both the 2.4GHz and 5.0GHz Wi-Fi interfaces (bands).

Wi-Fi as a feature can also be shut off on this page by selecting the ‘Disable Wireless LAN Interface’ box.

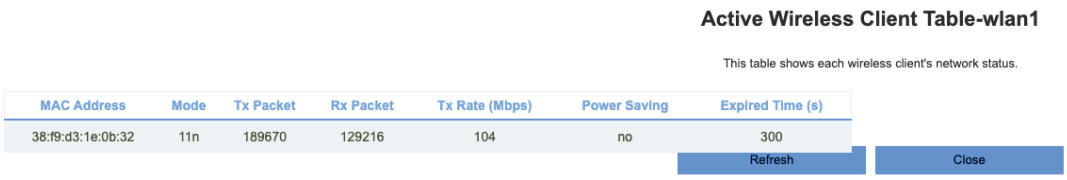
The Passport ’s SSID (network name) and guest SSID can both be edited on this page. Edits include the ability to rename the SSID and toggle its broadcasting status (whether or not it comes up as an option when users are viewing available Wi-Fi networks to connect to on their mobile devices). In addition, users can view Associated Clients which provides a list of all devices connected to the Passport ’s Wi-Fi network at that exact moment.

For more technically savvy users, the Wi-Fi channel width, sideband, and number can all be toggled from within the Wi-Fi page as well.

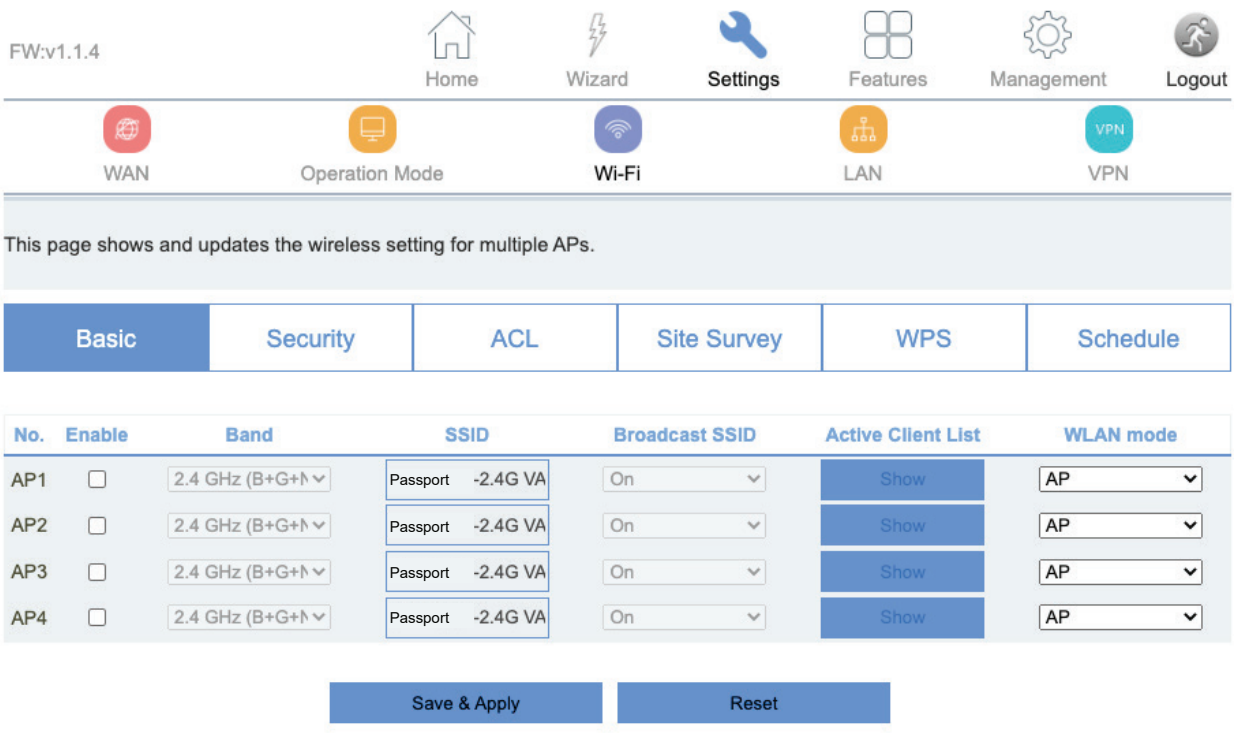
Item	Description
Disable WIreless LAN Interface	You may choose to enable or disable the wireless function.
Wireless Band	Default is “Mixed 802.11b/g/n”. It is strongly recommended that you set the Band to “802.11b/g/n”, that way all 802.11b, 802.11g, and 802.11n wireless stations can connect to the Passport.
Multiple AP	You can set the guest SSID from this button.
Network Type	You can configure the WLAN network type with this parameter.
SSID	Set a Wi-Fi name (SSID) for your wireless network. If you switch to Client Mode, this field becomes the SSID of the AP you want to connect with.
Channel Width	Select a proper channel bandwidth to enhance wireless performance. When there are 11b/g and 11n wireless clients, please select the 802.11n mode of 20/40MHz frequency band.
Control Sideband	Control channels are only applicable if your gateway is operating at 40 MHz bandwidth and the 802.11n mode is configured as Automatic.
Channel Number	For optimal wireless performance, you may select the least interferential channel. It is advisable that you select an unused channel or “Auto” to let the Passport detect and select the best possible channel for your wireless network to operate on from the drop-down list.
Broadcast SSID	You may choose a visible or invisible SSID broadcast. When it is enabled, the Passport ’s SSID will be broadcast in the wireless network so that it can be scanned by wireless clients and they can join the wireless network with this SSID.

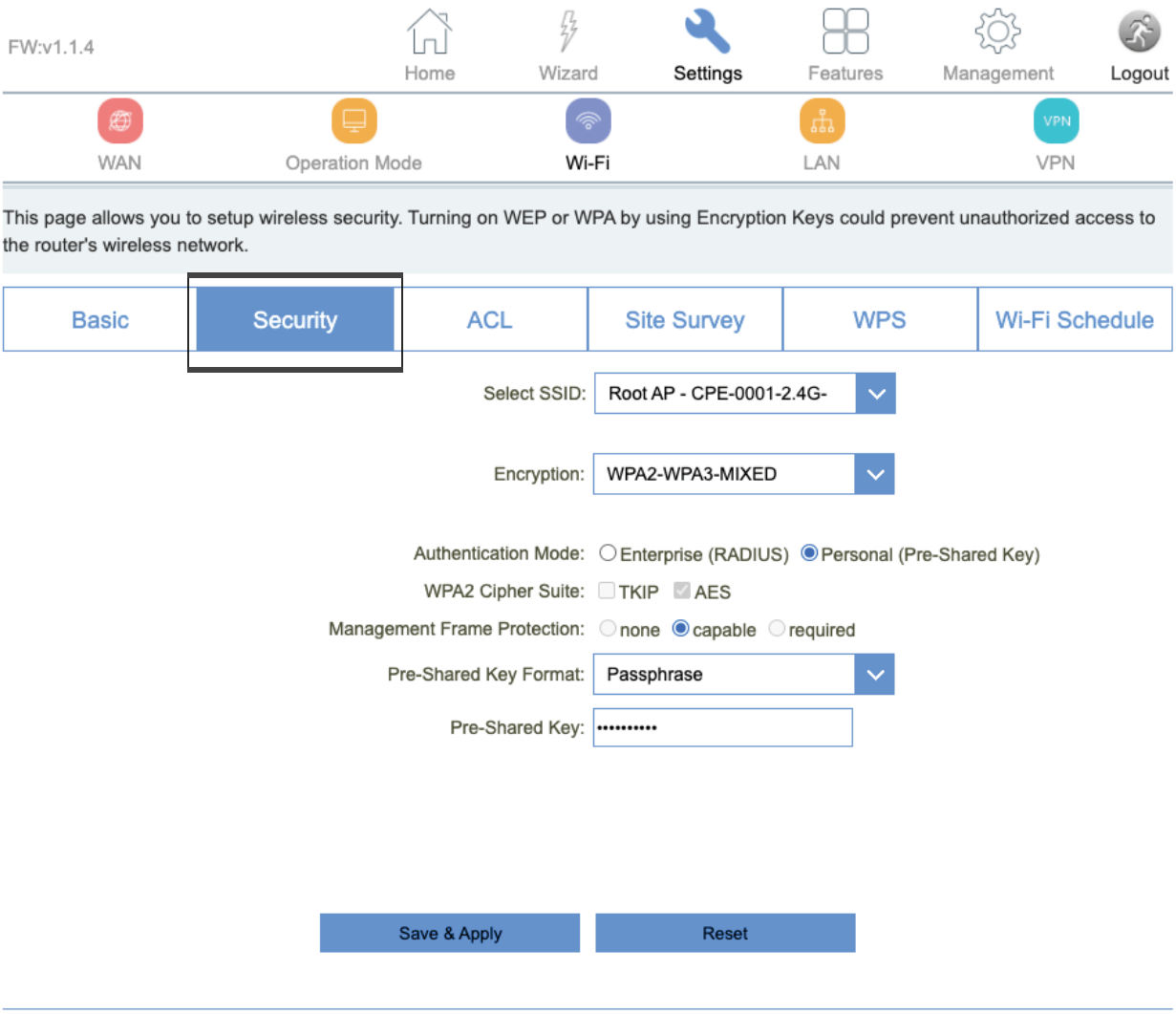
WMM	WMM provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories: voice, video, best effort, and background.
Associated Clients	This option shows you all the clients who are connected to a SSID.
Enable Universal Repeater Mode	Repeater mode.

Selecting **Show Active Clients** leads to the Active Wireless Client Table which displays a list of the current devices that are connected to the Passport at any given point in time.



Selecting **Multiple AP** leads to a view of the wireless settings for multiple APs.





3.4.3.2 Security

The **Security** page is used to set the Wi-Fi encryption type.

Item	Description
Encryption	Select the security mode from the Encryption drop down list. There are 4 options in the Security Mode drop down list: • Disable • WEP • WPA2

	• WPA-Mixed
Enterprise (RADIUS)	Remote Authentication Dial In User Service
TKIP	Temporal Key Integrity Protocol
AES	Advanced Encryption Standard

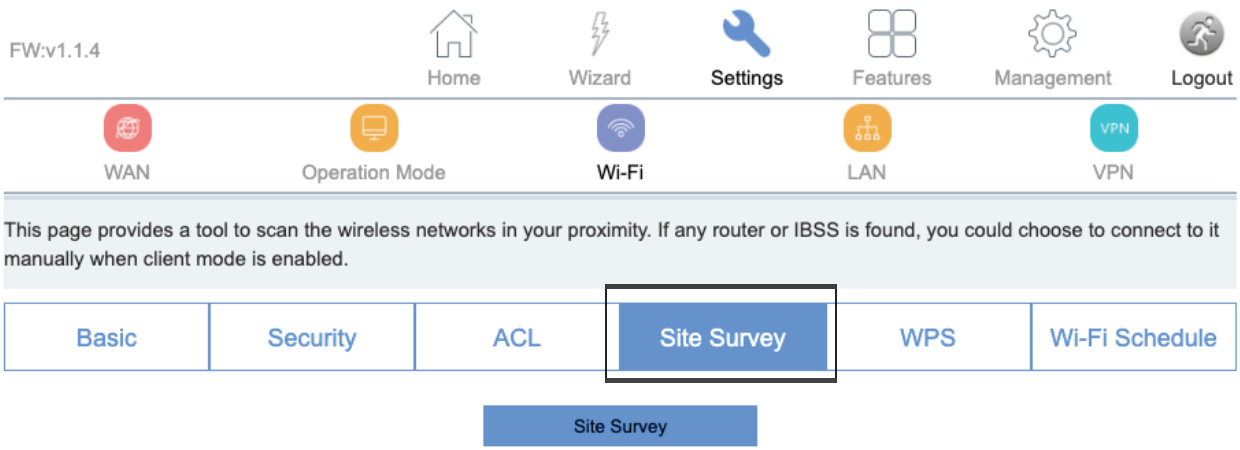
3.4.3.3 ACL

The **ACL** page enables user's to specify which wireless device MAC addresses are permitted to connect to the Passport's Wi-Fi network and which are not permitted.

Keep this mode disabled if you want to keep your Wi-Fi free for any device in your RV or home to connect to without limitation.

Item	Description
Wireless ACL Mode	If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect to the Access Point.
MAC Address	The MAC address of the client.

3.4.3.4 Site Survey

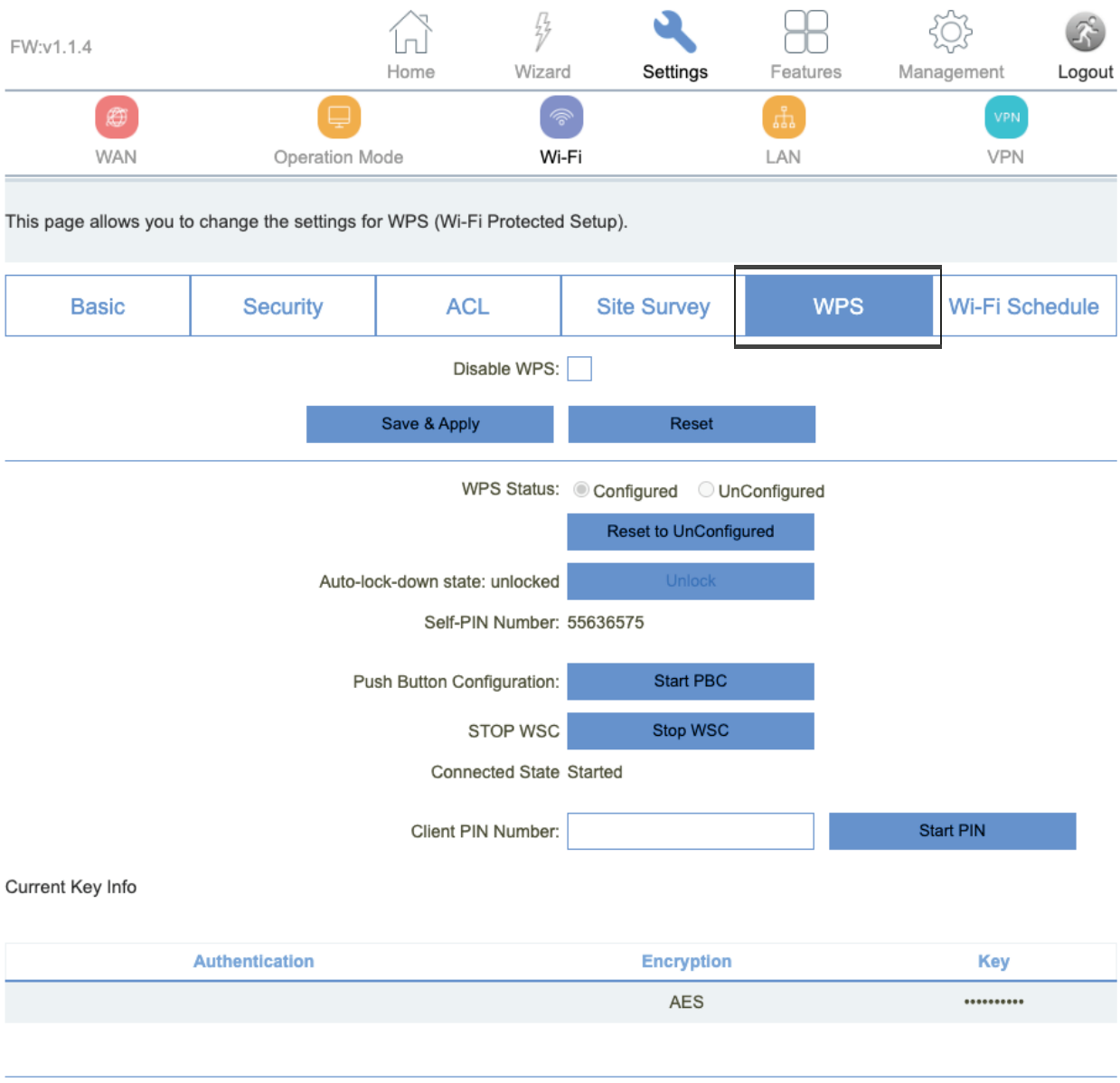


SSID	BSSID	Channel Number	Type	Encrypt	Signal
TDPQ	40:b0:76:c0:bf:f0	7(B+G+N+AC)	AP	WPA2-PSK	55
WTPD	3a:1a:52:28:46:1a	7 (G+N)	AP	WPA2-PSK	42
SRVC	40:e3:d6:5e:13:24	11 (B+G+N)	AP	WPA2-PSK	33
chargingstations	40:e3:d6:5e:13:25	11 (B+G+N)	AP	WPA2-PSK	33
DIRECT-2E-HP ENVY 6000 series	86:2a:fd:95:f4:2e	6 (G+N)	AP	WPA2-PSK	30
WWA	f0:9f:c2:3d:99:24	1 (B+G+N)	AP	WPA2-PSK	29

The **Site Survey** page enables user's to scan all the Wi-Fi networks available to them in the immediate vicinity of the Passport .

When the Passport is set in client mode, it can act as a repeater and connect to those specific Wi-Fi networks, rendering the plan unusable.

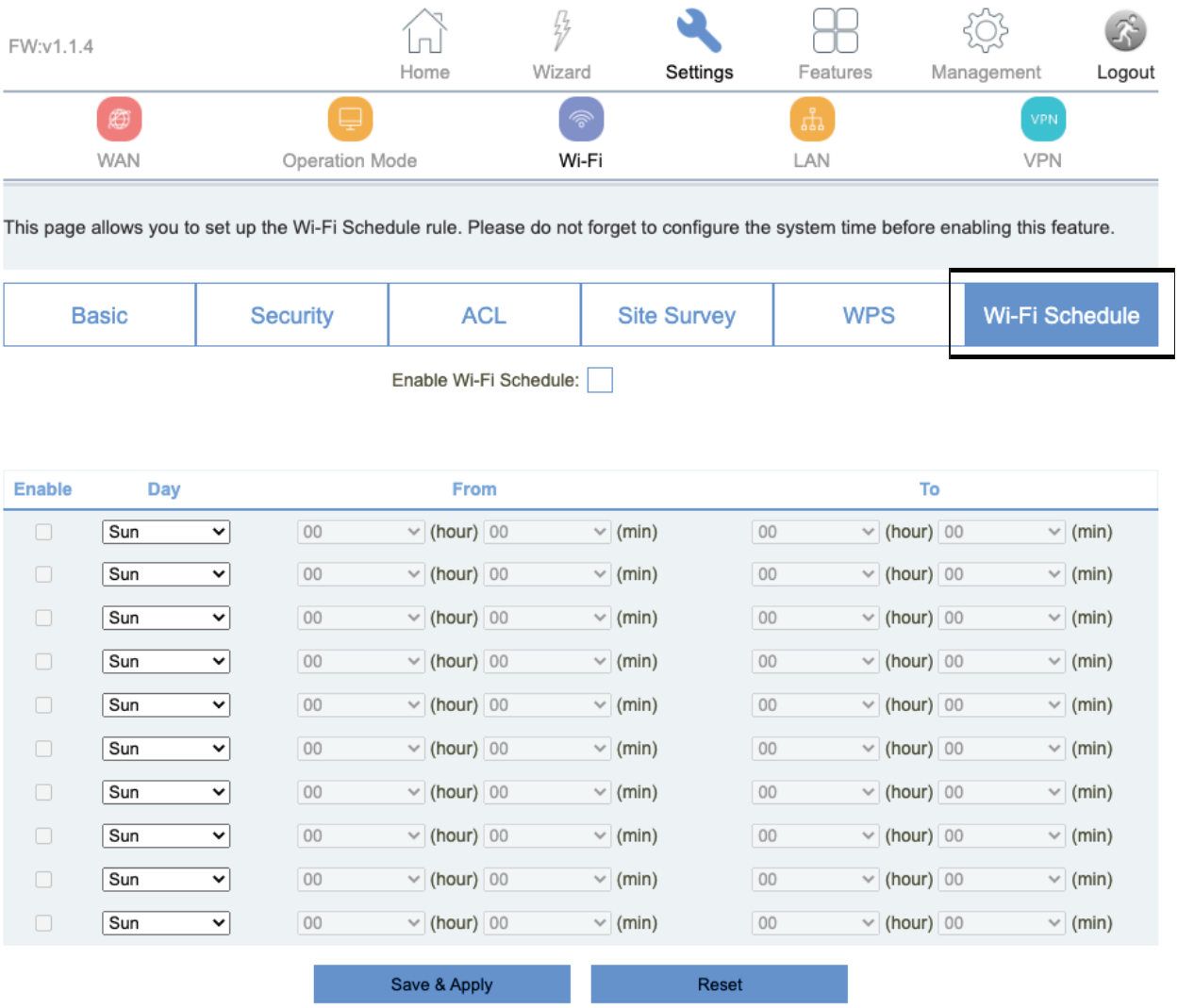
3.4.3.5 WPS



The **WPS** page enables the user to change the settings for Wi-Fi Protected Setup. Specifically enabling the user to enable or disable WPS, and permit certain devices to connect to the Passport via WPS.

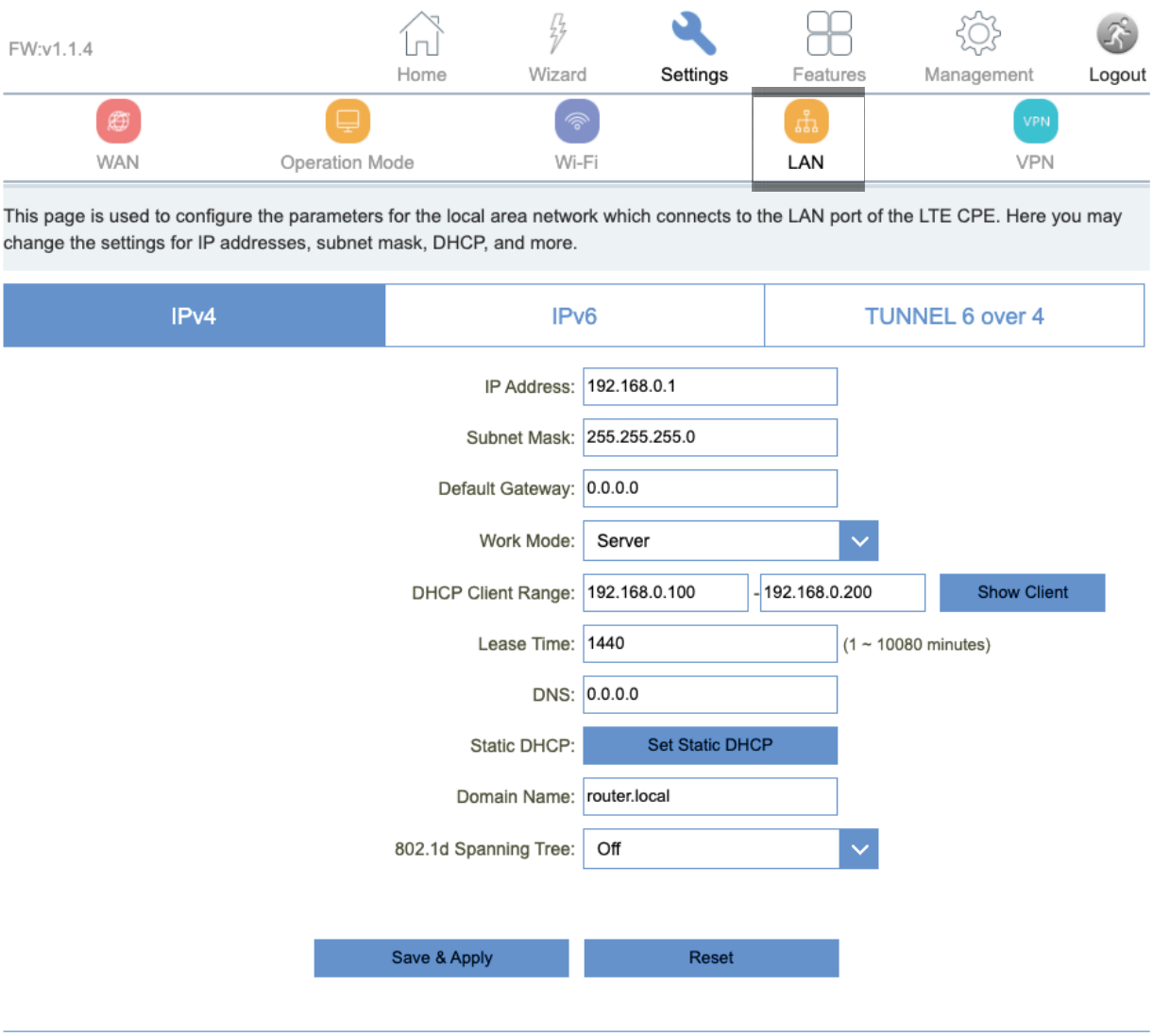
Item	Description
WPS	This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to an Access Point in a minute without any hassle.
Disable WPS	Enable or disable WPS function.

3.4.3.6 Wi-Fi Schedule



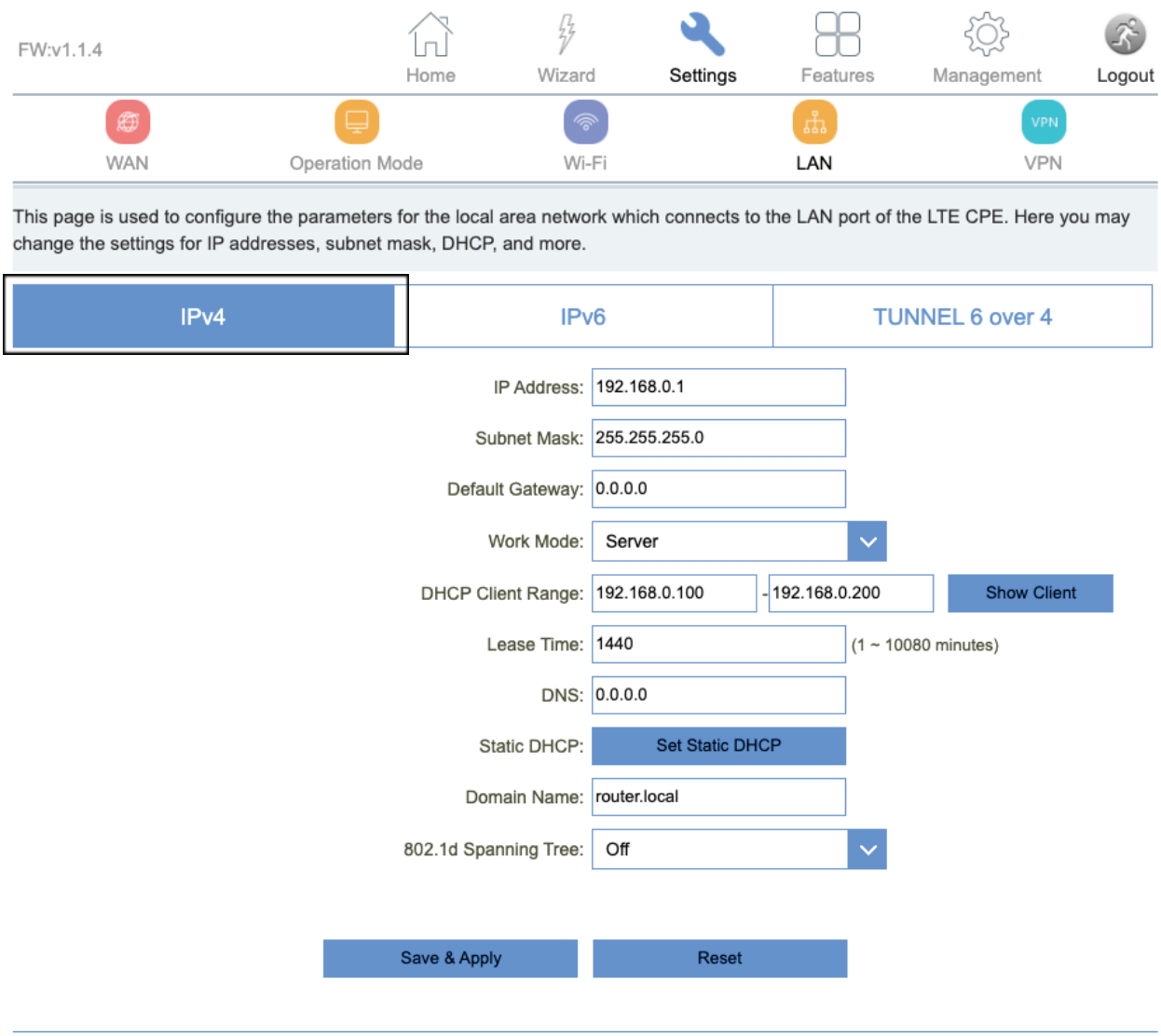
3.4.5 LAN

The **LAN** section enables the user to configure the parameters for the local area network.



3.4.5.1 IPv4

The **IPv4** page enables the user to change the settings for several LAN-related parameters with focus on settings around the DHCP function.



Item	Description
LAN IP Address	The default is 192.168.0.1. You can change it according to your needs.
Subnet Mask	The router's LAN subnet mask.
Work Mode	If this is selected, the router serves as the DHCP server and automatically assigns IP addresses to all computers in the LAN.
DHCP Client Range	Enter the start and end IP address of all the available successive IPs.
Lease Time	Select the time for using one assigned IP from the drop down list. After the lease time, the AP automatically assigns new IP addresses to all connected computers.
Static DHCP	This page allows you to reserve IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the DHCP server.
Domain Name	Set the domain name of the server.
802.1d Spanning Tree	Enable or disable spanning tree function.

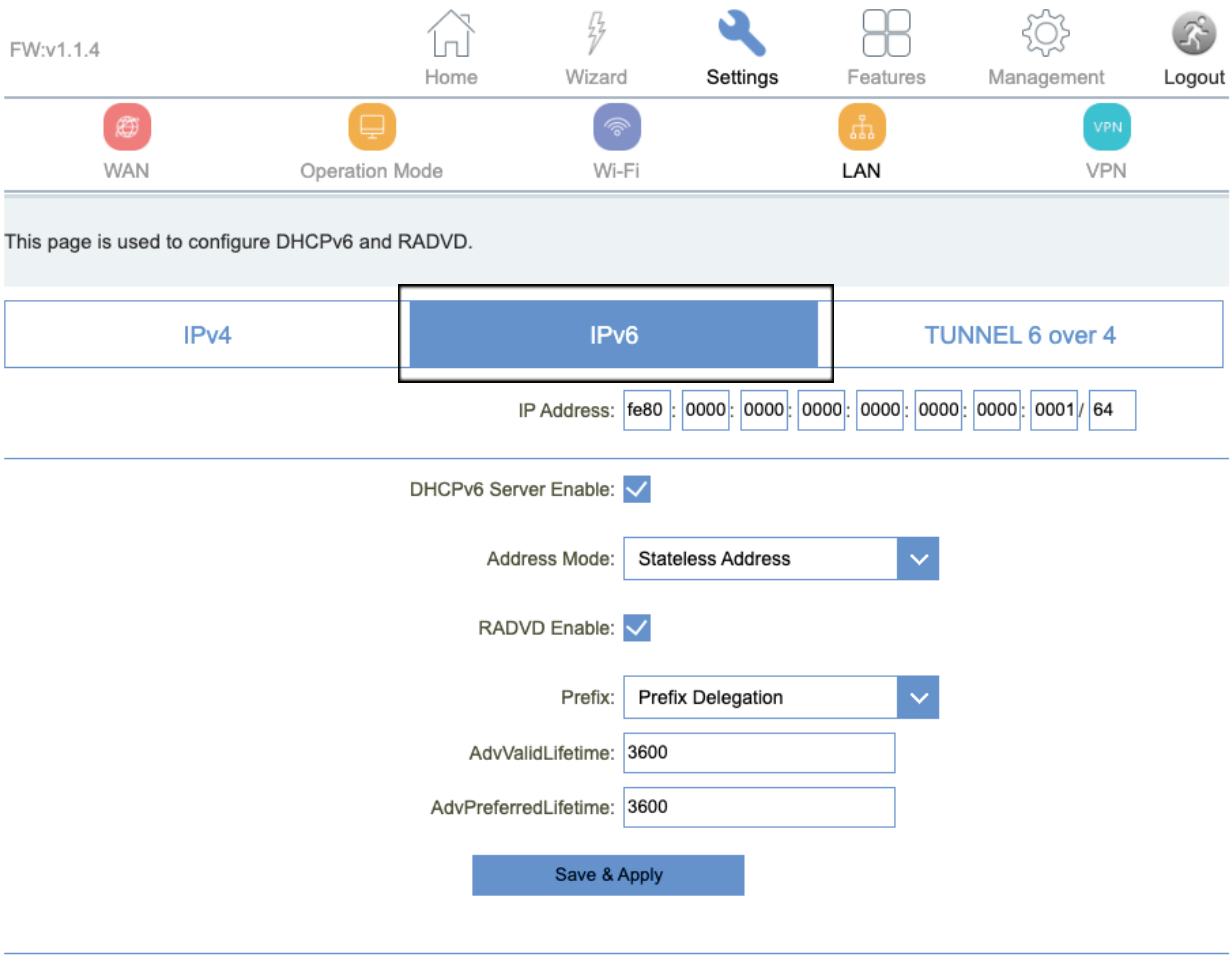
3.4.5.2 Static DHCP

Entering the **Static DHCP** page by clicking the “Set Static DHCP” button enables users to reserve a specific IP address for a device by granting them access to bind the MAC address of the said device to an IP address that is specified by the user on this page.

Click the “Set Static DHCP” button also reveals the RADVD page.

3.4.5.3 IPv6

The **IPv6** page enables the user to permit the Passport to serve as the DHCP server and automatically assigns IPv6 addresses to all connected mobile devices on the LAN.



Item	Description
IP Address	Router's LAN IPv6 address.
RADVD	Router Advertisement Dameon

Stateful Address	DHCP will supply an IPv6 address.
Stateless Address	DHCPv6 server does not provide IP addresses at all.
6RD IPv6 Prefix	WAN IPv6 prefix delegation.

3.4.5.4 RADVD

Configuring Router Advertisement
IPv4
IPv6
RADVD
TUNNEL 6 over 4
Enable:
radvdinterfacename: br0
MaxRtrAdvInterval: 15
MinRtrAdvInterval: 10
MinDelayBetweenRAs: 10
AdvManagedFlag:
AdvOtherConfigFlag:
AdvLinkMTU: 0
AdvReachableTime: 0
AdvRetransTimer: 0
AdvCurHopLimit: 0
AdvDefaultLifetime: 45
AdvDefaultPreference: high
AdvSourceLLAddress:
UnicastOnly:
Prefix1
Enabled:
Prefix2
Enabled:
Save & Apply
default
reset

The **RADVD** page enables the user to set up all the settings around IPv6 RADVD, including the specified time delays between packets, maximum and minimum retry intervals, and advertisement settings.

Item	Description
radvdinterfacename	Interface name.
MaxRtrAdvInterval	Max retry advertisement interval.
MinRtrAdvInterval	Min retry advertisement interval.
MinDelayBetweenRAs	Min delay between router advertisement.
AdvManagedFlag	Advertisement managed flag.
AdvOtherConfigFlag	Advertisement other config flag.
AdvLinkMTU	Advertisement link MTU.
AdvReachableTime	Advertisement reachable time.
AdvRetransTimer	Advertisement retrains timer.
AdvCurHopLimit	Advertisement current hop limit.
AdvDefaultLifetime	Advertisement default lifetime.
AdvDefaultPreference	“High”, “medium” or “low” for the advertisement default preference.
AdvSourceLLAddress	Advertisement source link local address.
UnicastOnly	Unicast only.
Prefix1 Enabled	Enable or disable prefix.
Prefix	Enter the prefix and prefix length.
AdvOnLinkFlag	Advertisement on link flag.
AdvAutonomousFlag	Advertisement autonomous flag.

AdvValidLifetime	Advertisement valid lifetime.
AdvPreferredLifetime	Advertisement preferred life time.
AdvRouterAddr	Advertisement router address.
If6to4	Enter the interface 6to4.

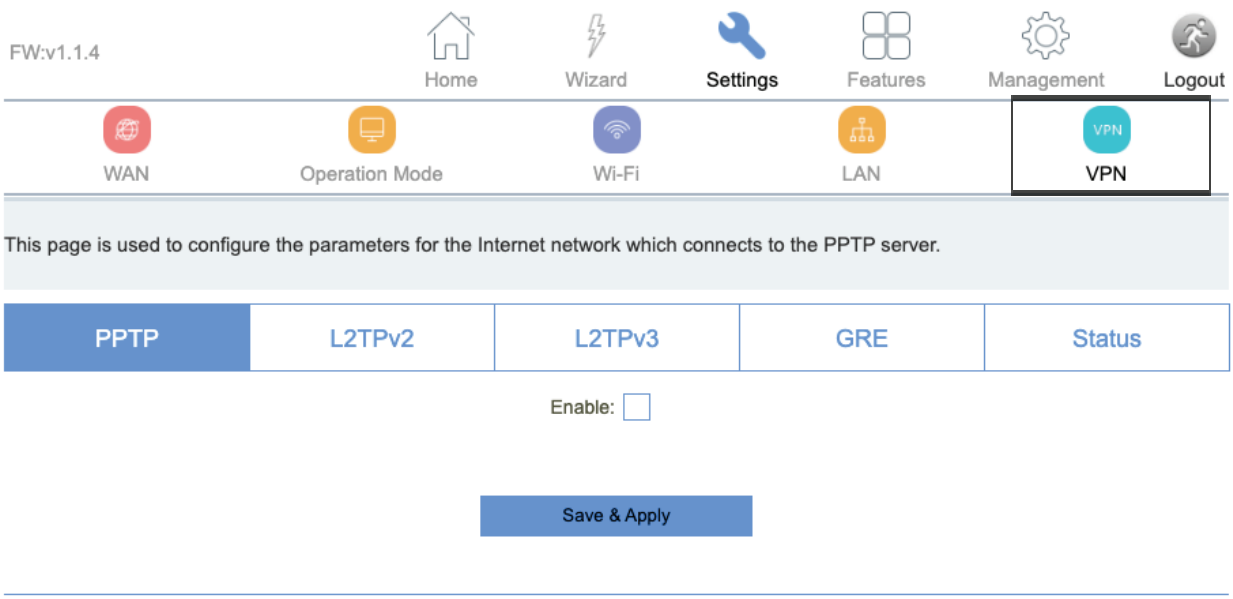
3.4.5.5 TUNNEL 6 over 4

The **TUNNEL 6 over 4** page enables users to either enable or disable tunnel 6 over 4.

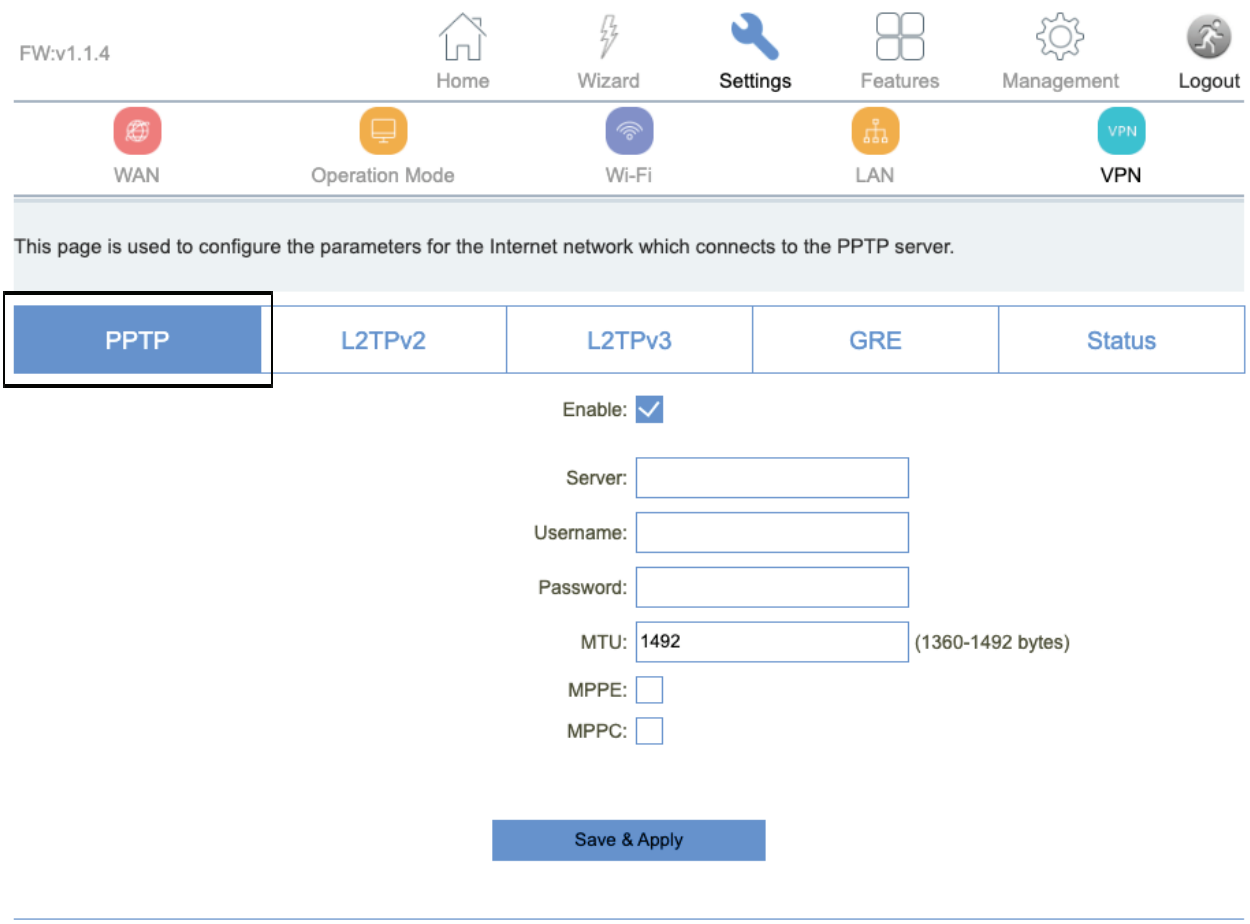
Item	Description
Enable	Enable or disable tunnel 6 over 4.

3.4.6 VPN

The **VPN** section enables the user to configure the settings for PPTP, L2TPv2, and L2TPv3 and view the Status of each.



3.4.6.1 PPTP

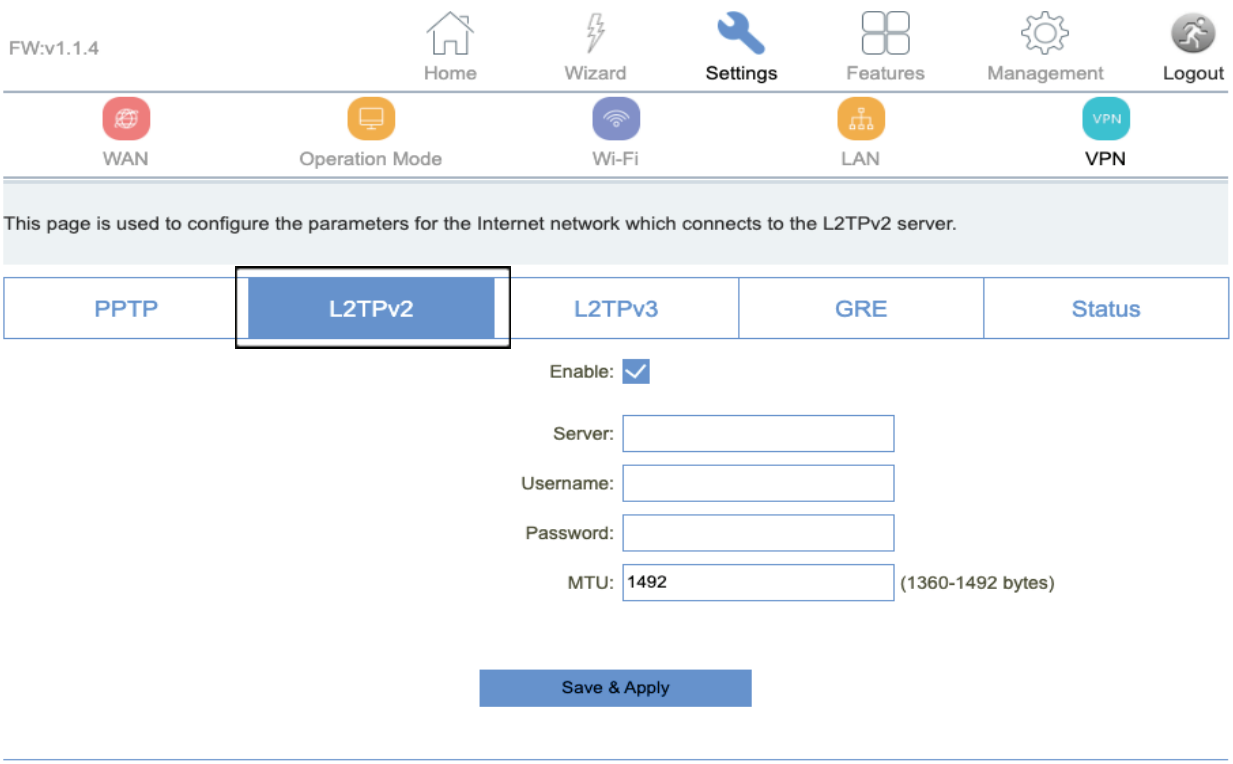


The **PPTP** page enables user's to configure the parameters for the internet network which connects to the PPTP server.

Item	Description
Server	The name of PPTP Server.
Username	The user name provided by the cellular carrier.

Password	The password provided by the cellular carrier.
MTU	You can keep the maximum transmission unit (MTU) as default.

3.4.6.2 L2TPv2

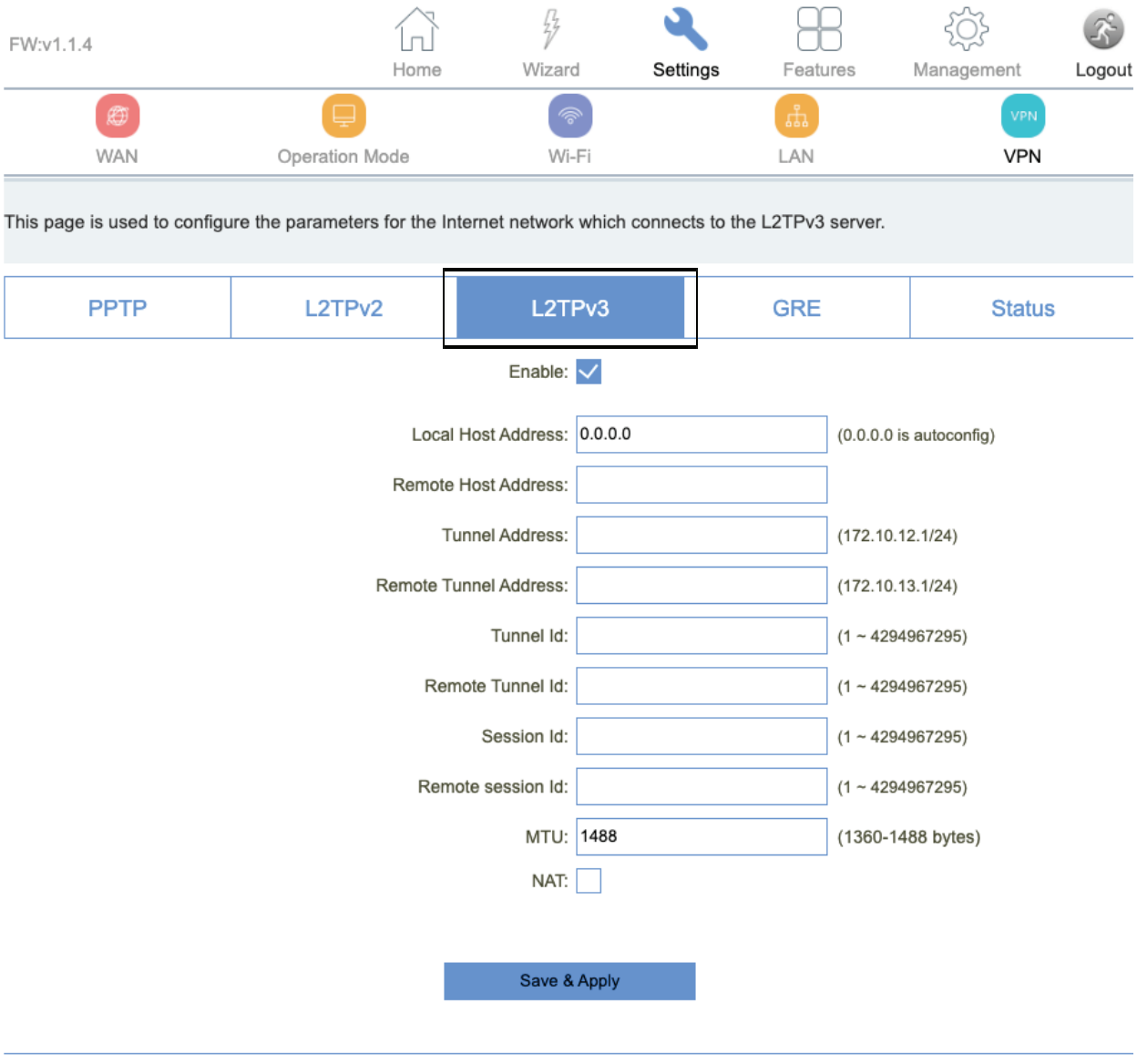


The **L2TPv2** page is used to configure the parameters for the internet network which connects to the L2TPv2 server.

Item	Description
Server	The name of L2TP Server.
Username	The user name provided by the cellular carrier.

Password	The password provided by the cellular carrier.
MTU	You can keep the maximum transmission unit (MTU) as default.

3.4.6.3 L2TPv3

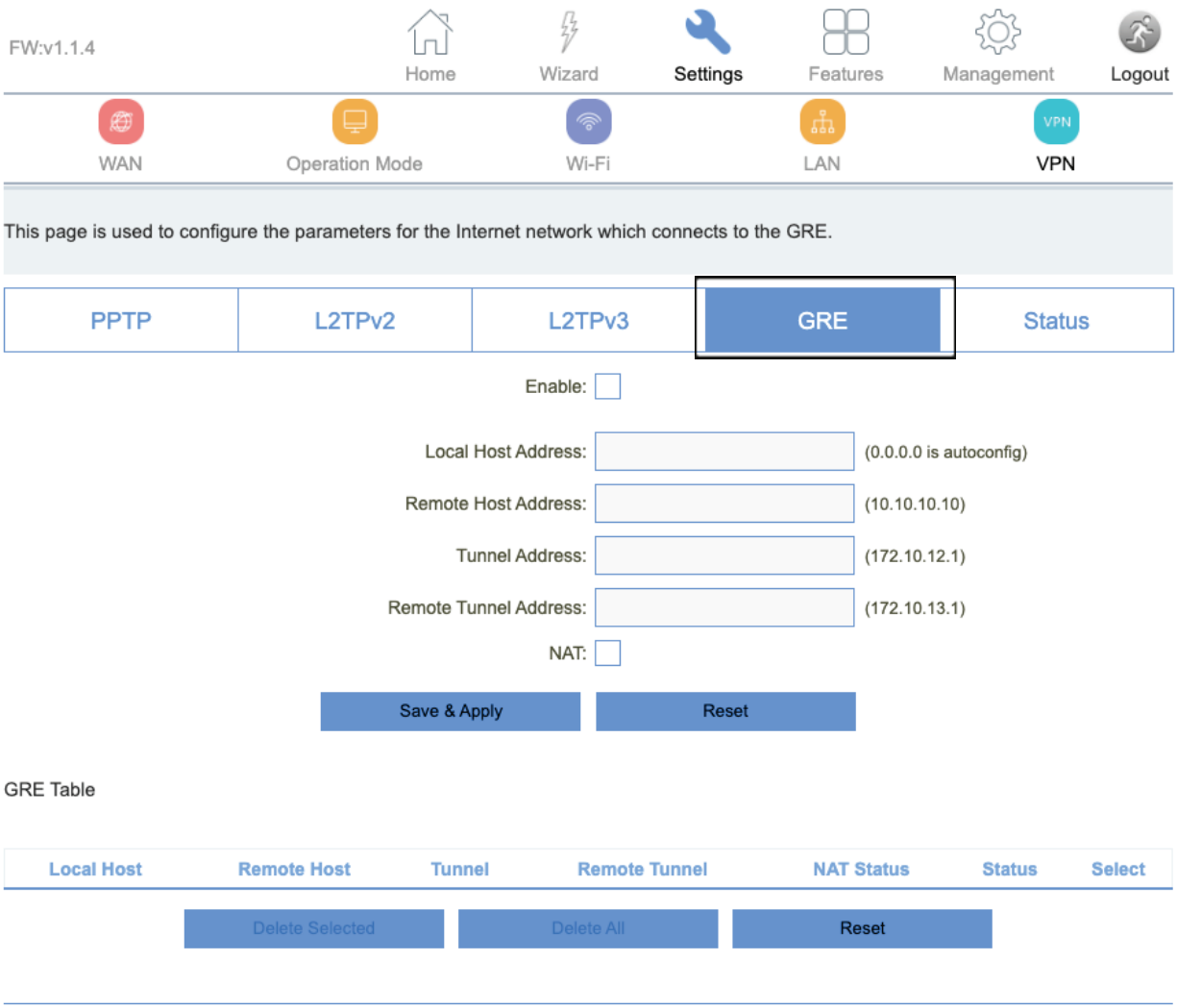


The **L2TPv3** page is used to configure the parameters for the internet network which connects to the L2TPv3 server.

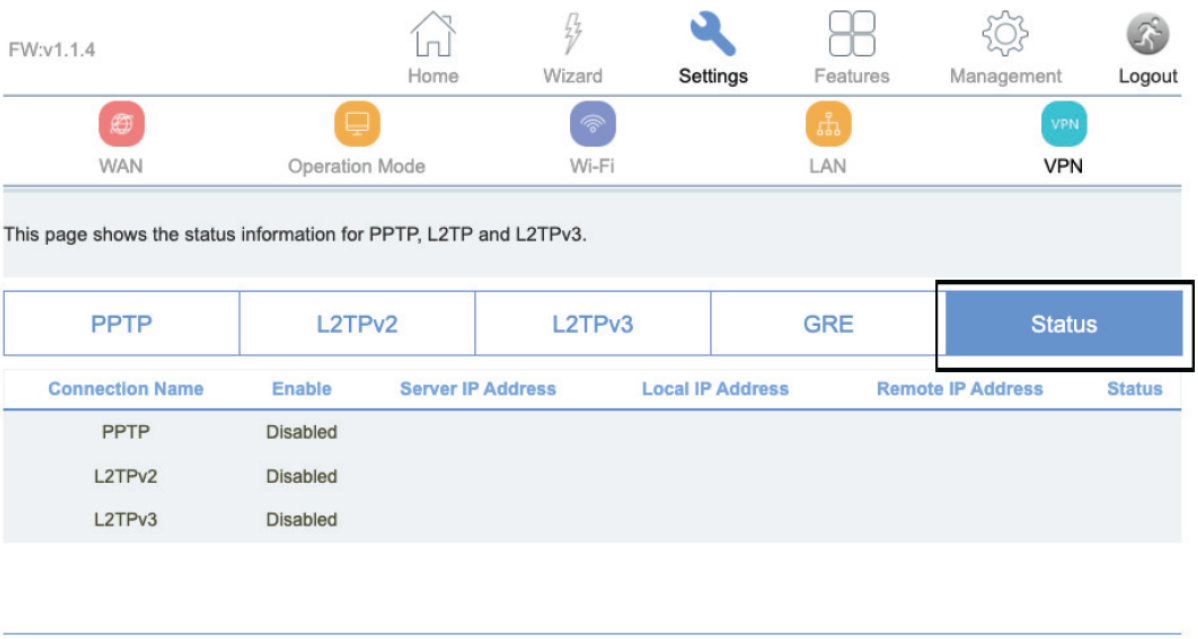
Item	Description
Local Host Address	The address of the LAN side device of the local, eg:192.168.0.2.
Remote Host Address	The address of the LAN side device of the remote host, eg:192.168.8.2.
Local Udp Port	Lan side device udp port.
Remote Udp Port	Remote device udp port.
Tunnel Address	Wan interface ip address.
Remote Tunnel Address	Remote device wan interface ip address.
Tunnel Id	Local device tunnel id.
Remote Tunnel Id	Remote device tunnel id.
Session Id	Local device session id.
Remote session Id	Remote device session id.
MTU	You can keep the maximum transmission unit (MTU) as default.

3.4.6.5 GRE

The **GRE** page is used to configure the parameters for the internet network which connects to the Generic Routing Encapsulation tunneling protocol.



3.4.6.4 Status



The **Status** page presents an overview of the status information for PPTP, L2TPv2, and L2TPv3.

Chapter 3
Accessing the Web User Interface: Features

3.5. Features

The **Features** section enables the user to configure QoS, Firewalls, Port Forwarding, URL filtering, Routes, and Dynamic DNS.

3.5.1 QoS

FW:v1.1.4
Home
Wizard
Settings
Features
Management
Logout
QoS
Firewall
Port Forwarding
URL Filter
Route
Dynamic DNS
Entries in this table improve your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.
Enable QoS:
Automatic Uplink Speed:
Automatic Downlink Speed:
Name:
QoS Type:
IPv4
protocol:
Both
Local IP Address:
Local Port:
Remot IP Address:
Remote Port:
Mode:
Guaranteed minimum
Uplink Bandwidth (Kbps):
Downlink Bandwidth (Kbps):
Priority:
(0-7,7 is highest priority)
Remark DSCP:
(0-63)
Comment:
Save & Apply
Reset
Current QoS Rules Table
Name
IP Version
Protocol
Local IP Address
Local Port
Remote IP Address
Remote Port
Local IPv6 addr
MAC Address
Phyport
DSCP
Mode
Uplink Bandwidth
Downlink Bandwidth
Priority
Weight
Remark DSCP
Select
Delete Selected
Delete All
Reset

The **Quality of Service (QoS** page enables user's to limit the upload and download speeds that a specific mobile device is receiving.

Quality of Service is an excellent and underutilized tool that allows you to train your Passport to divide up your available bandwidth between applications. With good QoS rules, you can ensure that your streaming video doesn't stutter because a big file is downloading at the same time, or that your work laptop isn't sluggish when you're trying to meet that last-minute deadline while your kids are playing games online.

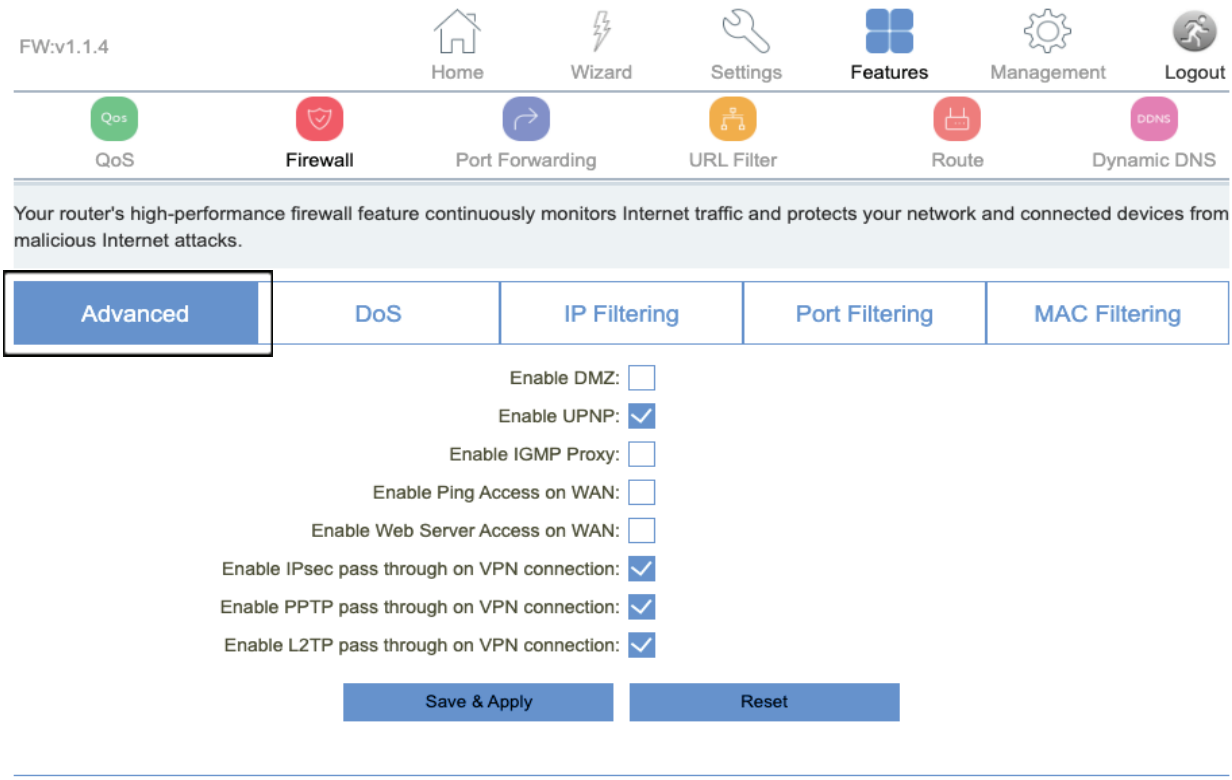
Item	Description
Automatic Uplink Speed	Automatic uplink speed.
Manual Uplink Speed (Kbps)	Set the download speed of your internet access.
Automatic Downlink Speed	Automatic downlink speed.
Manual Downlink Speed (Kbps)	Set the upload speed of your internet access.
Name	QoS rule name.

3.5.2 Firewall

The **Firewall** page enables user's to set up a plethora of firewall-related features and functions.

3.5.2.1 Advanced

The **Advanced** page contains a series of checkboxes allowing user to toggle on or off specific fire-wall related functions, access, and VPN pass throughs.



Item	Description
Enable DMZ	DMZ function.
Enable UPnP	UPnP function.
Enable IGMP Proxy	IGMP Proxy function.
Enable Telnet Access on WAN	Telnet by wan access.
Enable Ping Access on WAN	Ping Access on WAN function.
Enable Web Server Access on WAN	Enable Web Server Access on WAN function.
Enable IPSec pass through on VPN connection	IPSEC to pass through IPSEC communication data.
Enable PPTP pass through on VPN connection	PPTP to pass through PPTP communication data.

Enable L2TP pass through on VPN connection	Enable or disable L2TP to pass through L2TP communication data.

3.5.2.2 Dos

The **Denial-of-Service (DoS)** page enables users to protect their Passport from DoS attack's by setting certain parameters relating to network security.

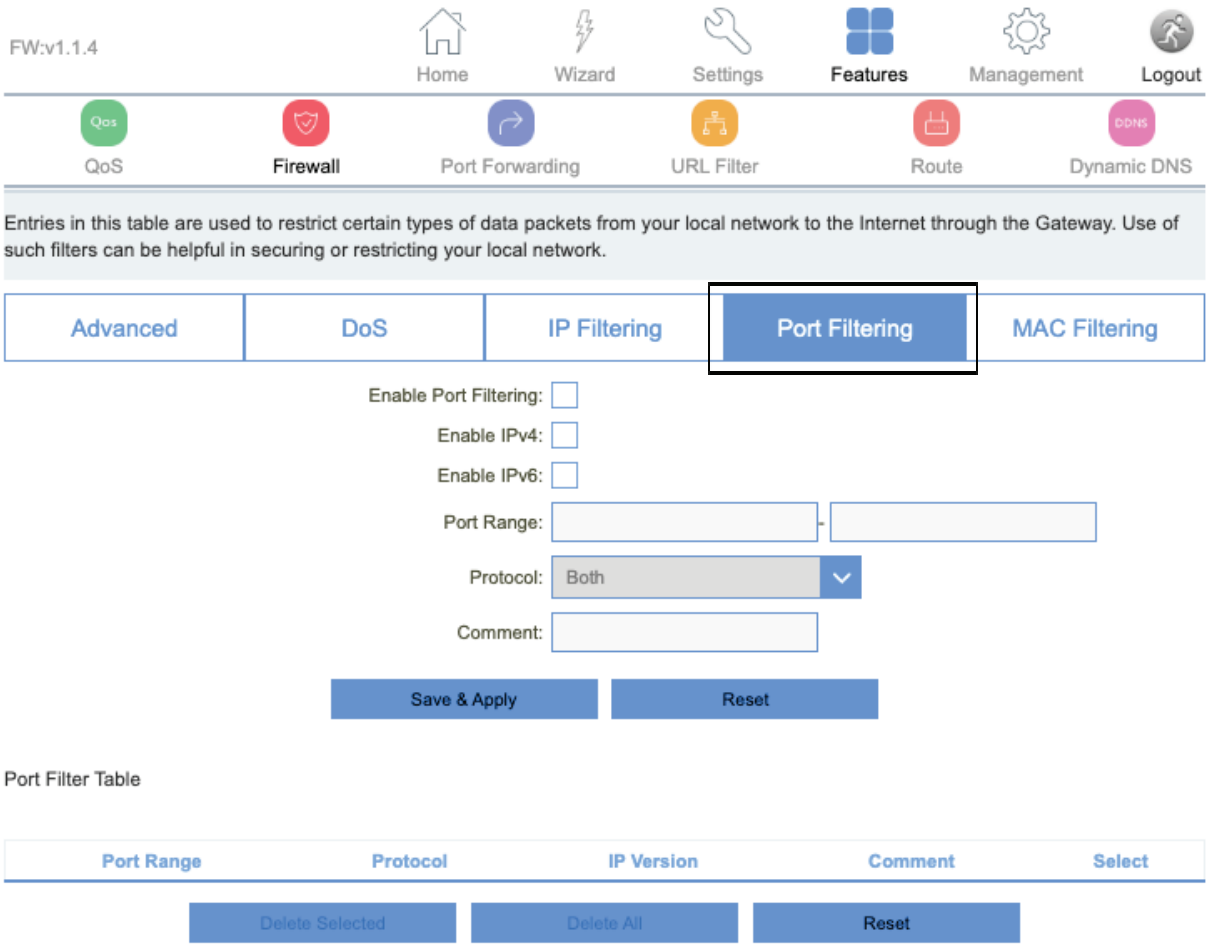
3.5.2.3 IP Filtering

The **IP Filtering** page enables users to control what IP traffic will be allowed into and out of the Passport's network.

Item	Description
Enable IP Filtering	IP Filtering function.
Enable IPv4	IPv4 Filtering feature.
Enable IPv6	IPv6 Filtering feature.
Local IPv4 Address	LAN side source IPv4 address.
Local IPv6 Address	LAN side source IPv6 address.
Protocol	“TCP”, “UDP” or” Both”.

3.5.2.4 Port Filtering

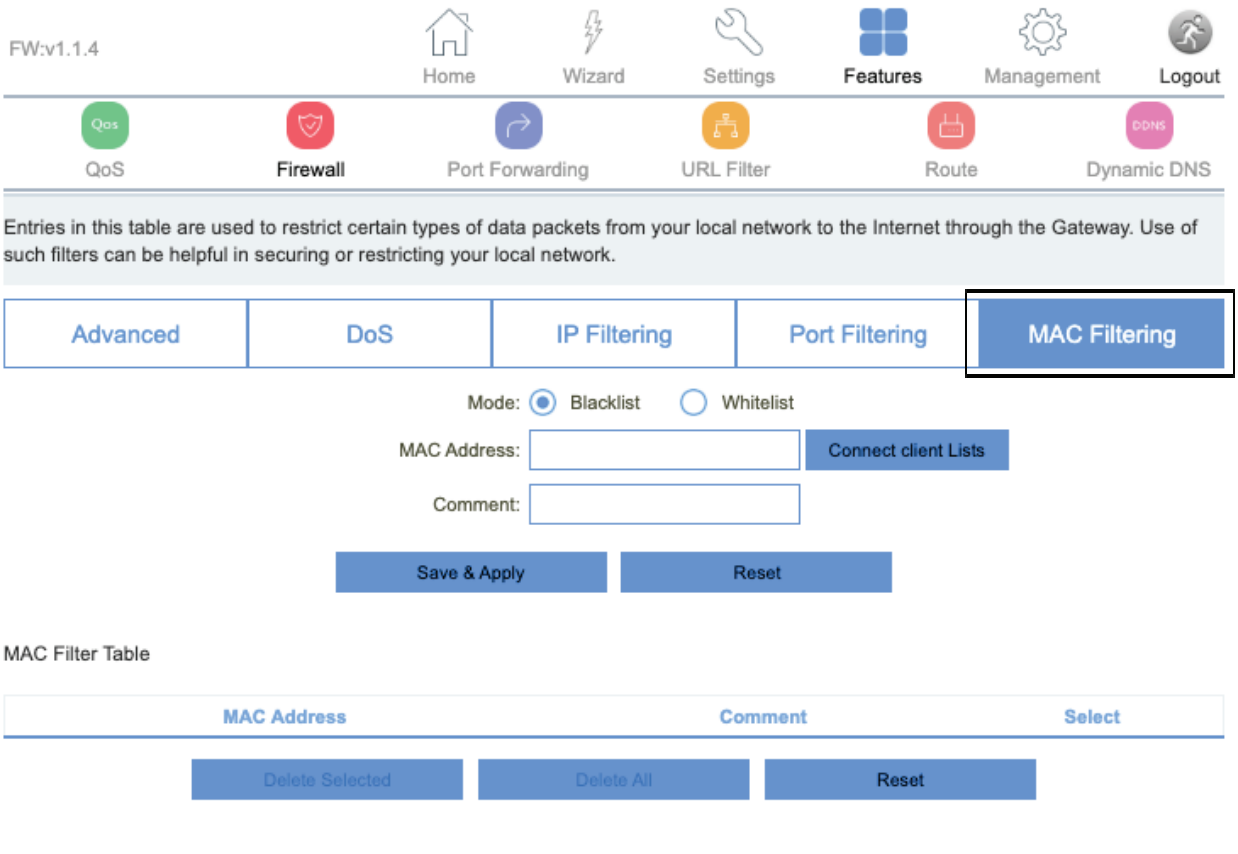
The **Port Filtering** page enables users to allow or block certain network packers from following into and out of the Passport’s network based on their port number.



Item	Description
Enable Port Filtering	Enable or disable IP Filtering function.
Enable IPv4	Enable or disable IPv4 Filtering feature.
Enable IPv6	Enable or disable IPv6 Filtering feature.
Port Range	Set the port range for port filtering.
Protocol	Select “TCP”, “UDP” or” Both”.
Comment	Comment for the rule.

3.45.2.5 MAC Filtering

The **Mac Filtering** page enables users to allow or block certain mobile devices from connecting to the Passport’s Wi-Fi network based on their MAC address.



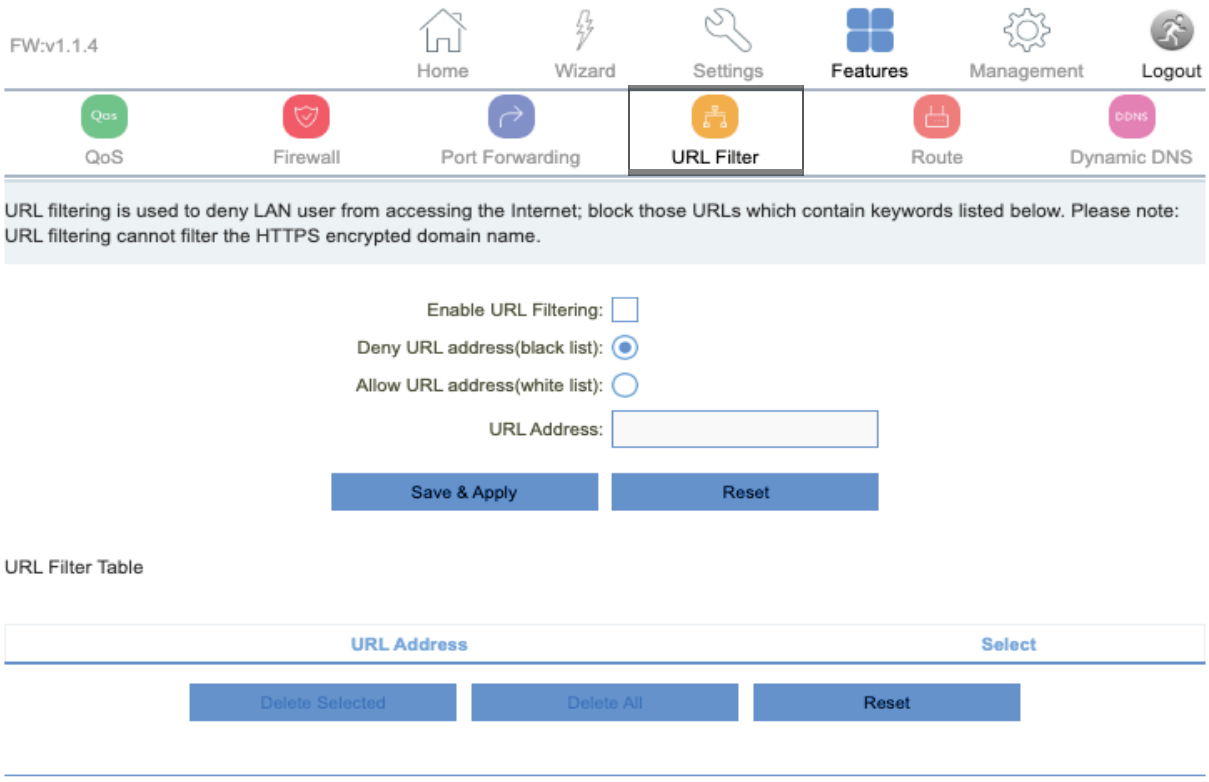
Item	Description
Blacklist	Block certain website URs from being accessed.
Whitelist	Allow certain website URLs from being accessed.
MAC Address	The MAC Address or the Media Access Control address is a unique serial number in the network circuitry of every Ethernet and Wi-Fi device.

3.5.3 Port Forwarding

The **Port Forwarding** page enables users to enable or disable port forwarding and set the port IP addresses that will be used to engage in allowing incoming traffic from outside the network to be sent to a local connected mobile device based on the requested port.

Item	Description
Enable Port Forwarding	Port Forwarding function.
Local IP Address	LAN IP address.
Local Port Start	LAN side start port.
Local Port End	LAN side end port.
Protocol	“TCP”, “UDP” or “Both”.
Remote IP Address	WAN IP address.
Remote Port Start	External start port.
Remote Port End	External end port.
Comment	Port number.

3.5.4 URL Filter



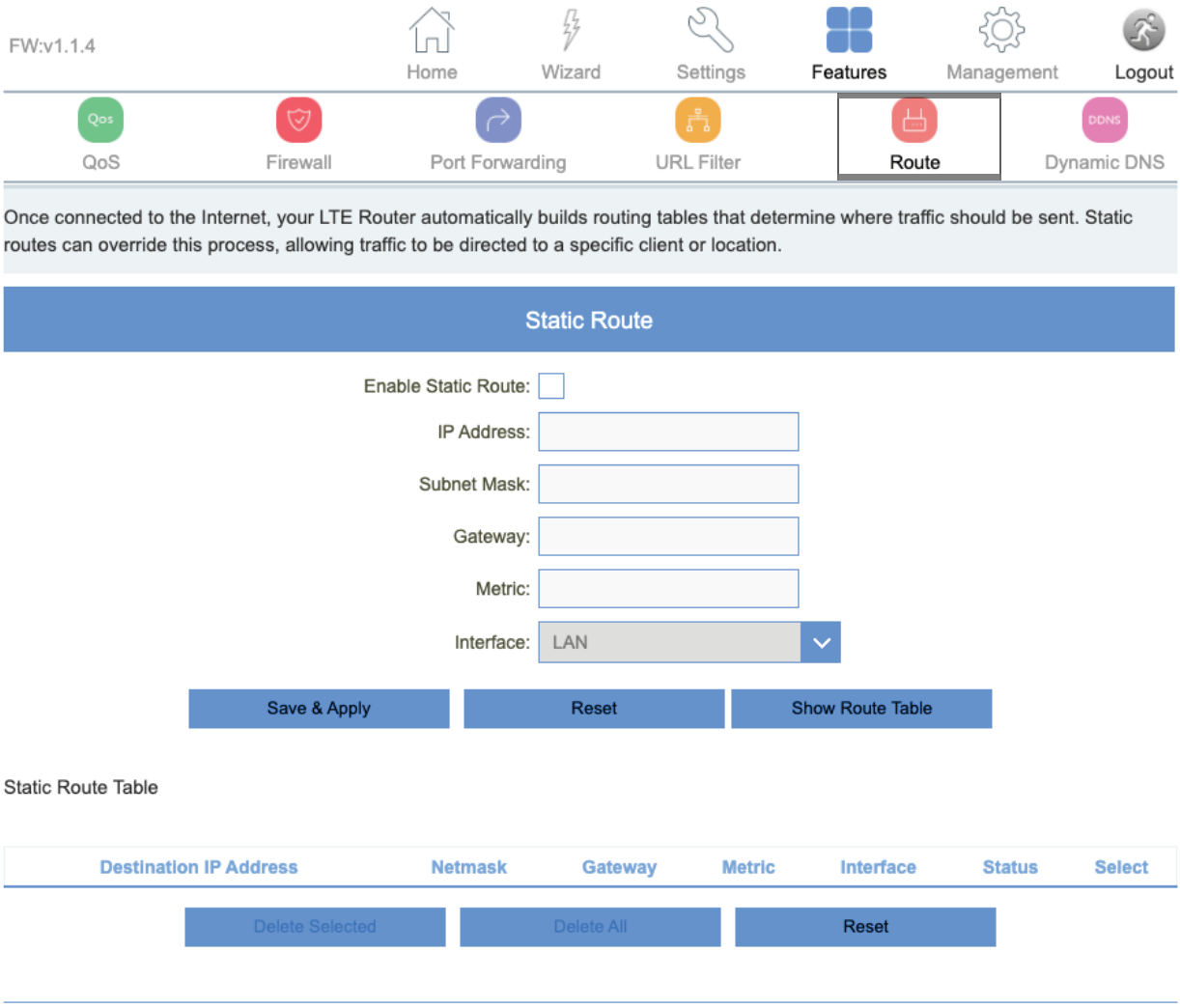
The **URL Filter** page is used to deny LAN users from accessing the internet. Users can block certain URLs that contain specific keywords.

Item	Description
Enable URL Filtering	Enable or disable URL Filtering function.
Deny URL address (black list)	Blocking access to the URL list.
Allow URL address (white list)	Allowing access to the URL list.

URL Address	Block or allow access URL.

3.5.5 Route

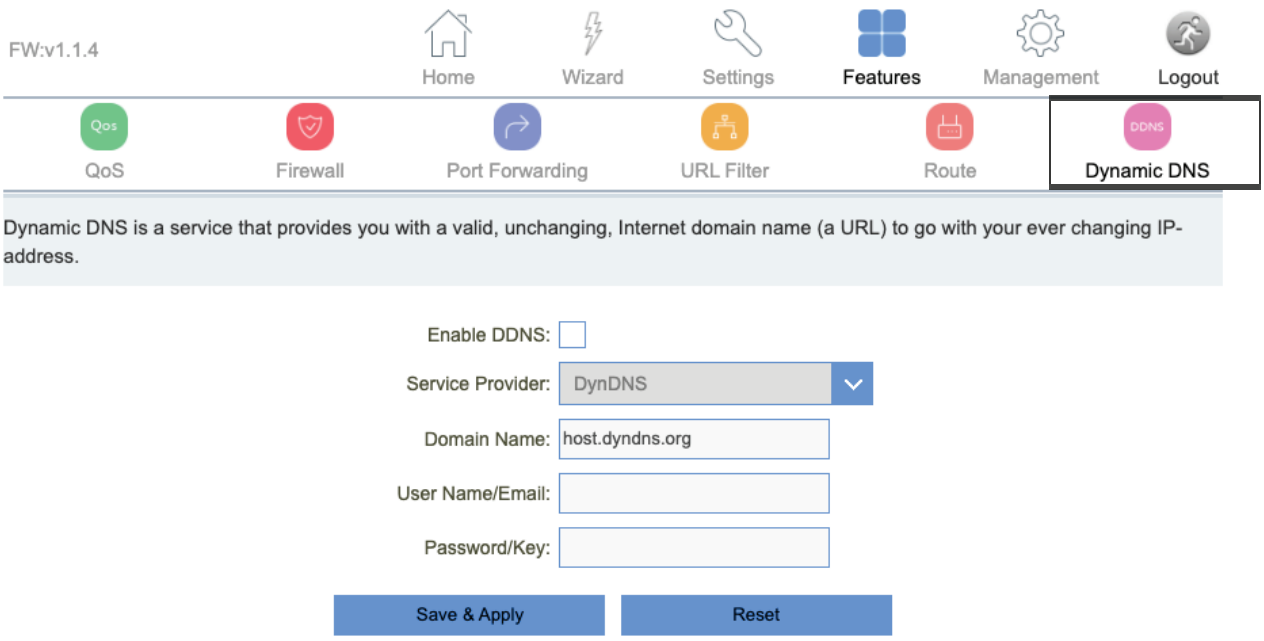
The **Static Route** page enables user's to enable or disable the Static route and input the items around it.



Item	Description
Enable Static Route	Enable or disable Static route.
IP Address	An IP address, or Internet Protocol address, is a series of numbers that identifies any device on a network.
Subnet Mask	A number that resembles an IP address. It reveals how many bits in the IP address are used for the network by masking the network portion of the IP address
Gateway	The IP address of another router your Passport sends traffic too.
Metric	The routing metric.

3.5.6 Dynamic DNS

The **Dynamic Domain Name Services (Dynamic DNS)** page allows a dynamic public IP address to be associated with a static host name in any of the many domains and allows access to a specific host from various locations on the internet. DDNS requires that an account be set up with one of the supported DDNS service providers.



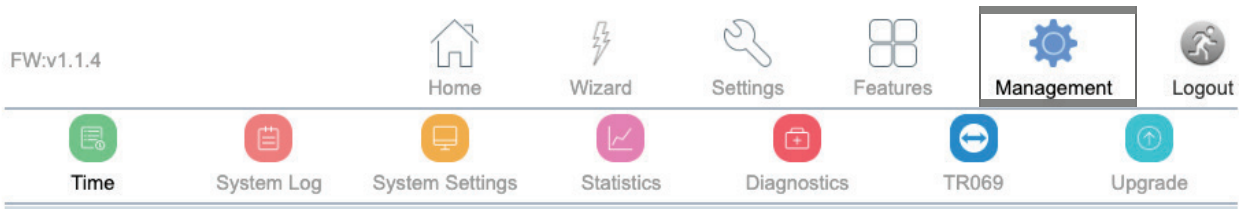
Item	Description
Server Provider	Select server from the drop-down list DynDNS TZO
Domain Name	The host name.
User Name/Email	The user name.
Password/Key	The password.

Chapter 3

Accessing the Web User Interface: Management

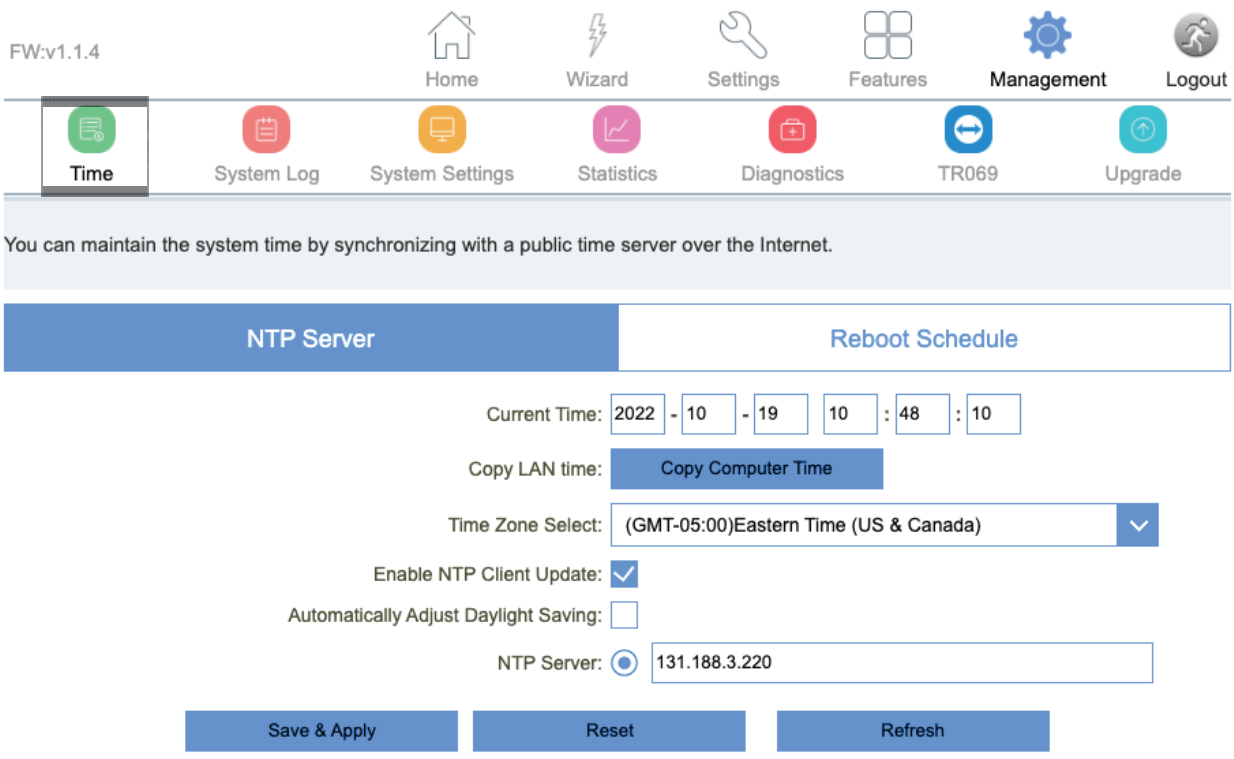
3.6. Management

The **Management** section enables the user to perform key system updates such as setting the CPE-0001's IP address log-in username and password, enabling or disabling TR069, and upgrading the CPE-0001's firmware.



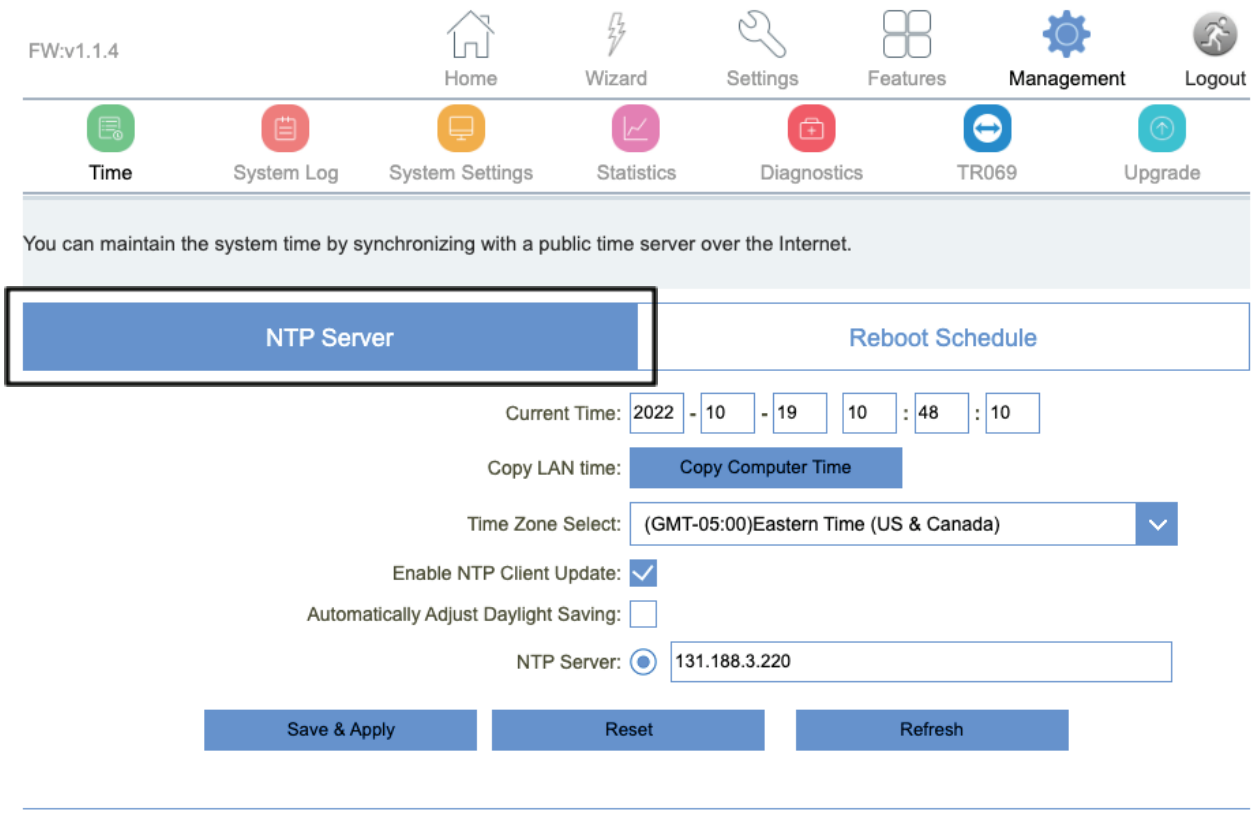
3.6.1 Time

The **Time** sub-section contains several pages related to time-related settings.



3.6.1.1 NTP Server

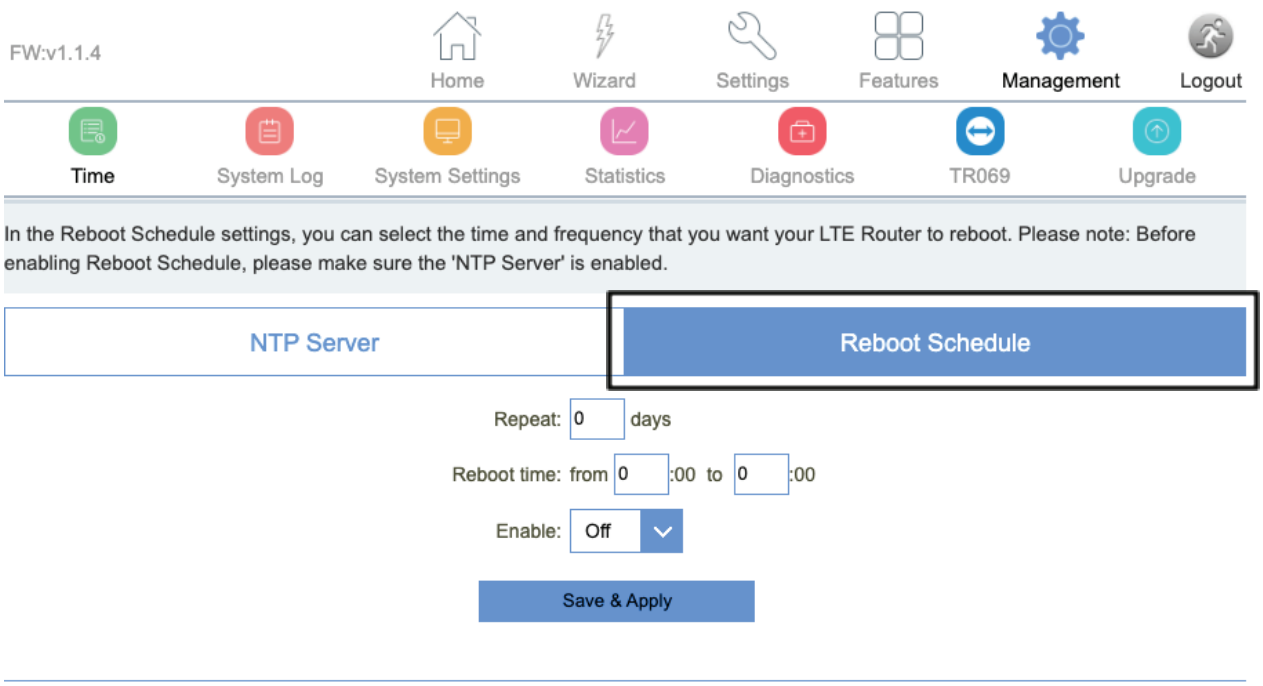
The **NTP Server** page enables user's to set the current time and time zone onto their Passport, in addition to setting NTP server.



Item	Description
Current Time	Select the time zone in your area.
Copy LAN time	Copy time from computer.
Time Zone Select	Select the time zone from the drop box.
Enable NTP client update	NTP client update.

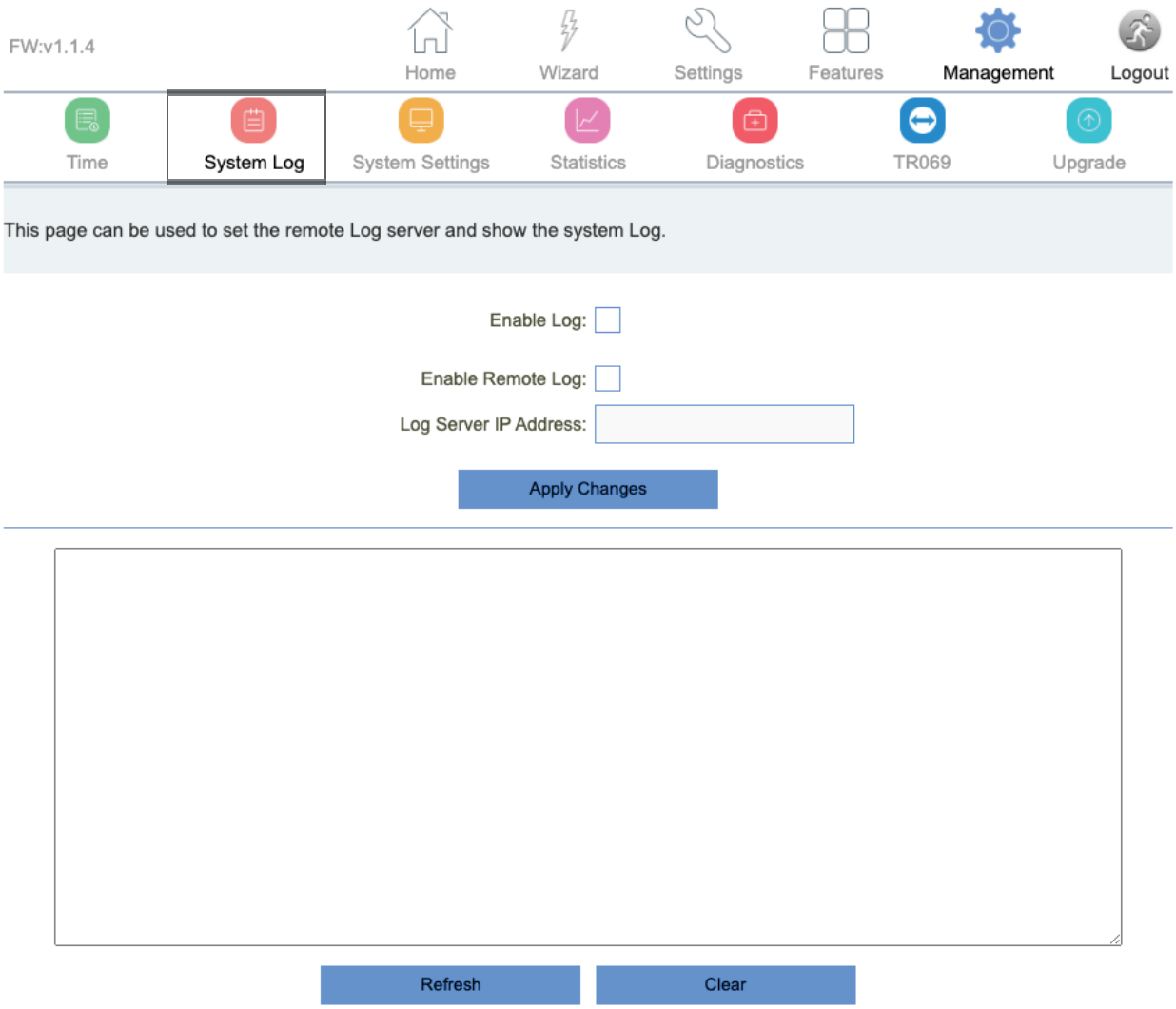
Automatically Adjust Daylight Saving	Daylight savings function.
NTP Server	Select the well known NTP Server.
Manual IP Setting	Enter the server manually.

3.6.1.2 Reboot Schedule



The **Reboot Schedule** page enables user's to allow their Passport to reboot automatically at a specified time.

3.6.1 System Log

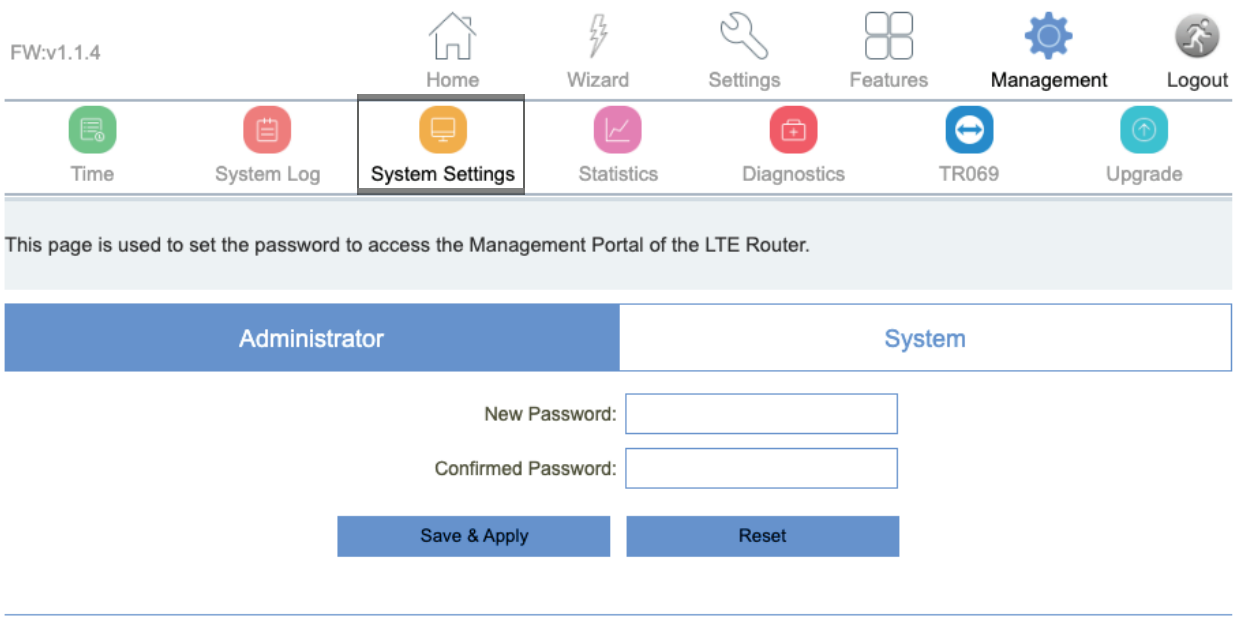


Item	Description
Enable Log	Log function.
System All	Print all log information.

Wireless	Print wireless log information.
DoS	Print DoS log information.
Enable Remote Log	“Logging to Syslog Server”.
Log Server IP Address	Enter the Syslog server IP address.

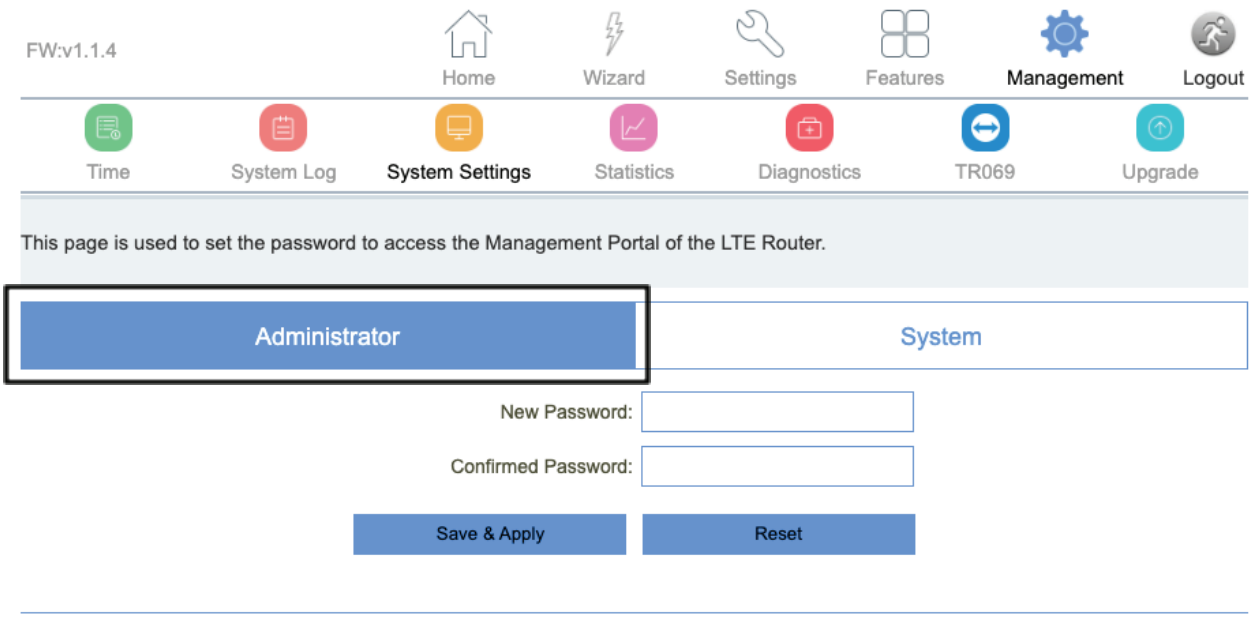
3.6.2 System Settings

The **System Settings** subsection contains several pages related to basic administration settings.

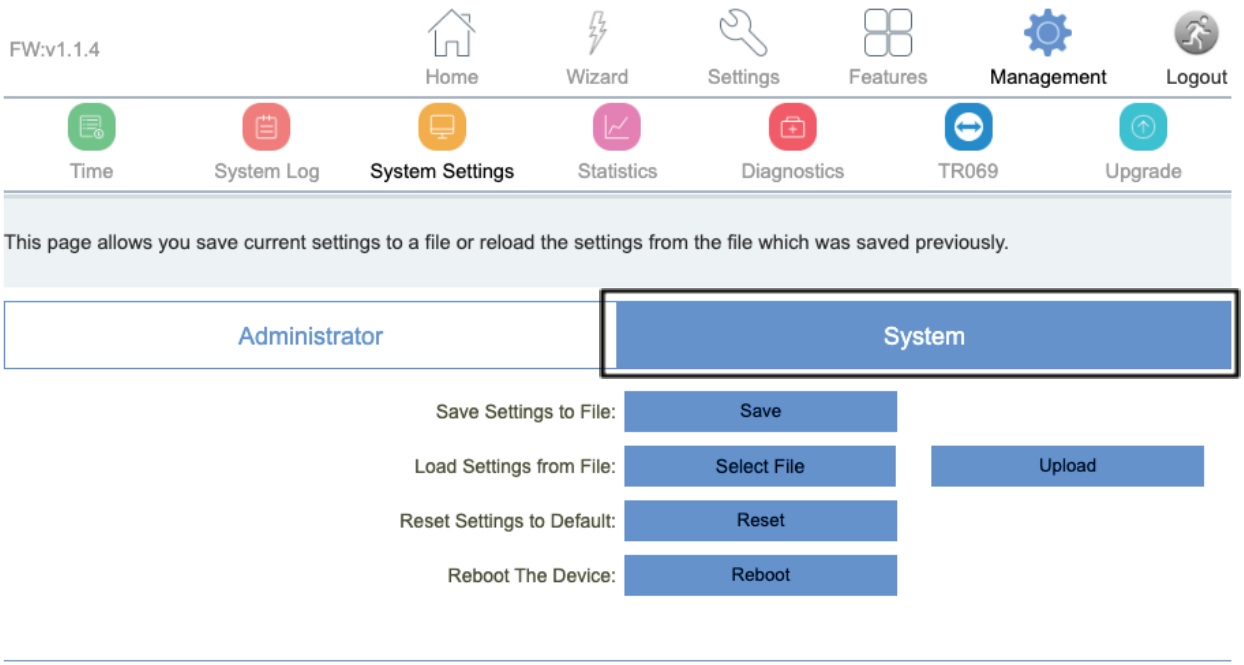


3.6.2.1 Administrator

The **Administrator** page allows users to set the Passport's IP address log-in username and password.



3.6.2.2 System

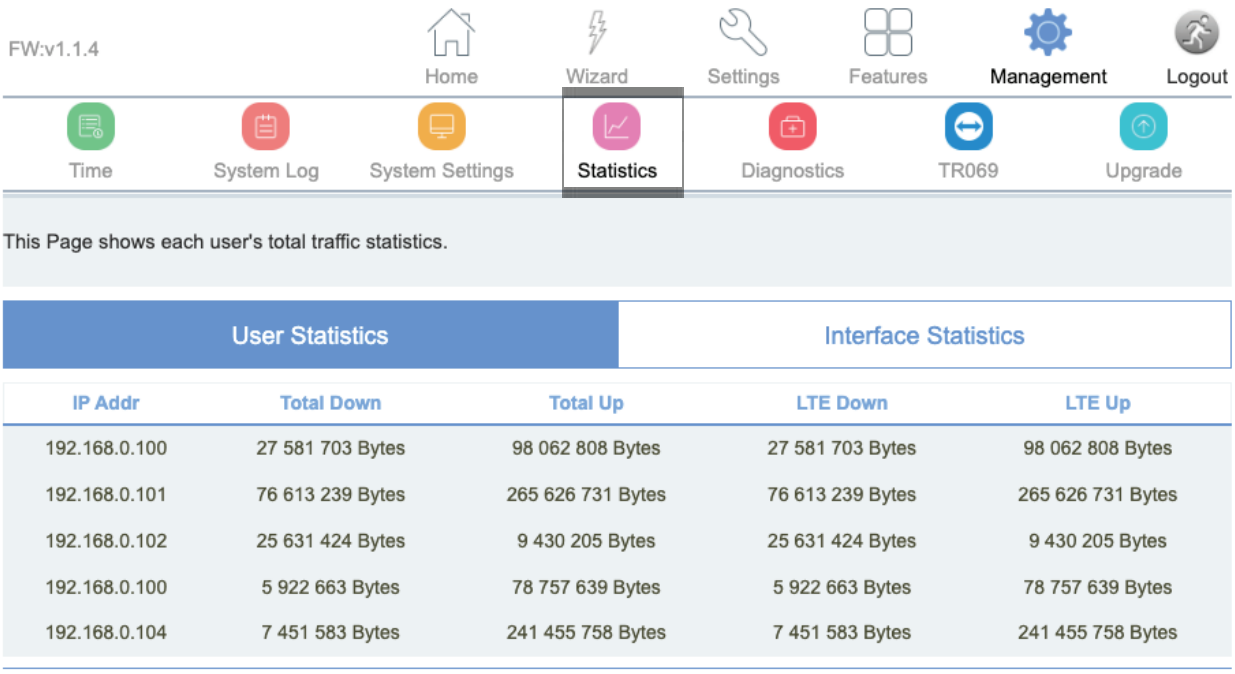


Item	Description
Save settings to file	Save the settings to the local PC.
Load settings from File	Load the settings from the local PC.
Reset Settings to Default	Restore the device to factory default.
Reboot the device	Press the button to reboot the device.

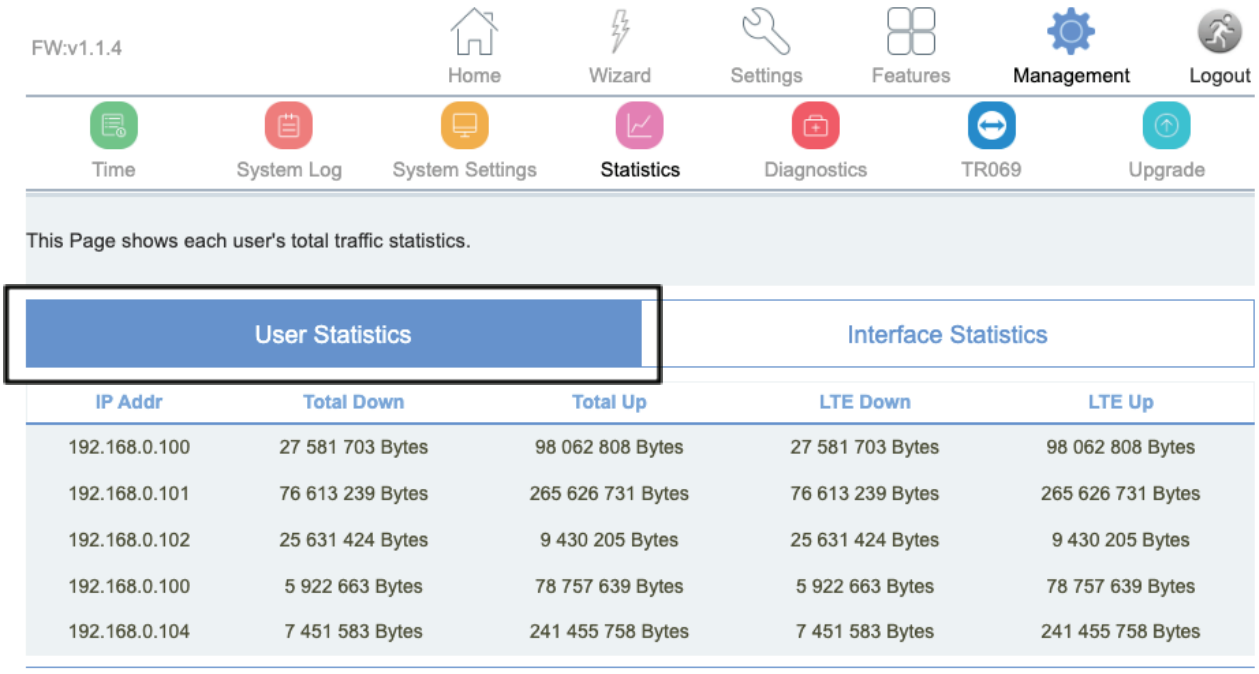
The **System** page allows user's to back up, restore, and erase the Passport's current settings. Once you provision your router to your liking, it is recommended to back up the settings so that they are saved as a file on your computer. In the future, you can then restore the Passport's settings from this file.

3.6.3 Statistics

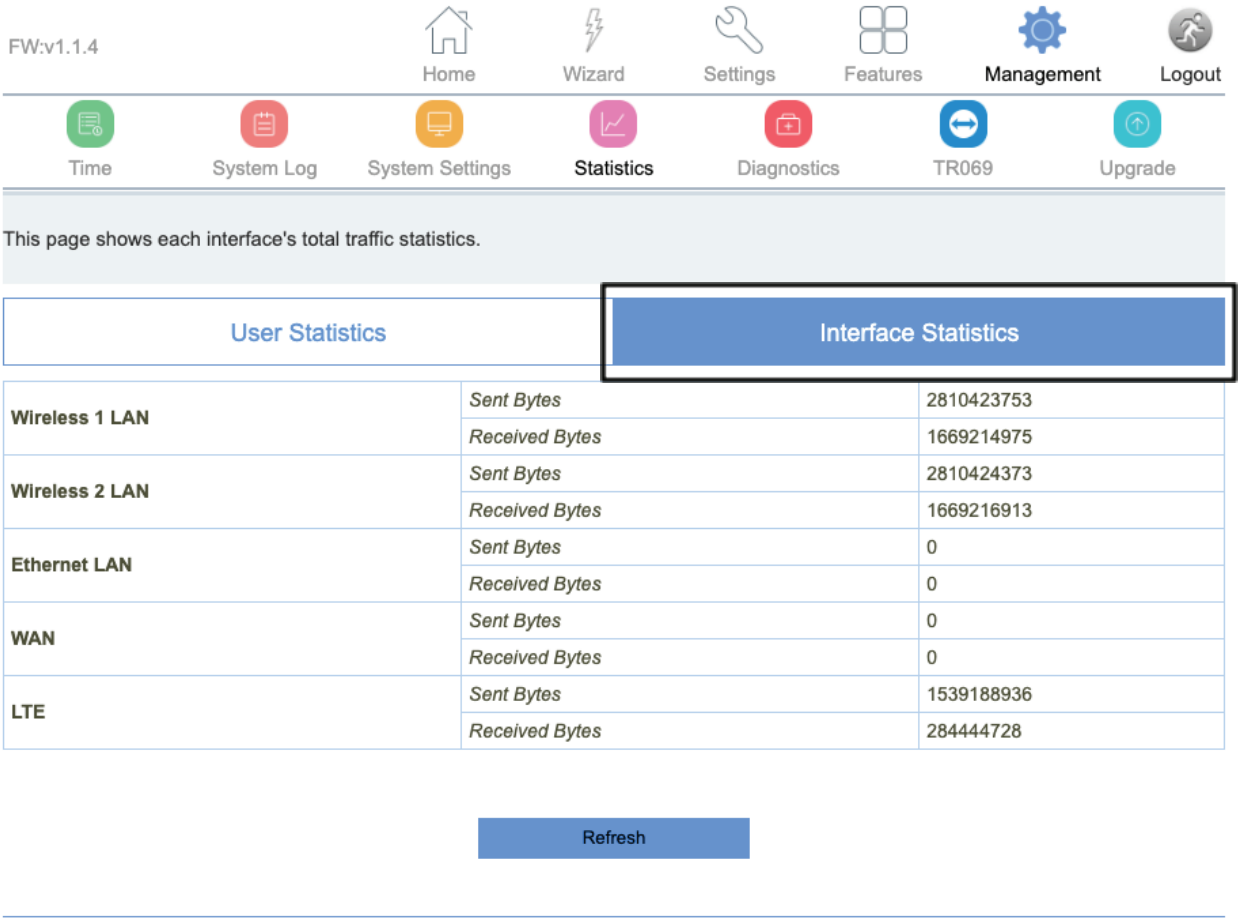
The **Statistics** subsection contains several pages related to basic administration settings.



3.6.3.1 User Statistics

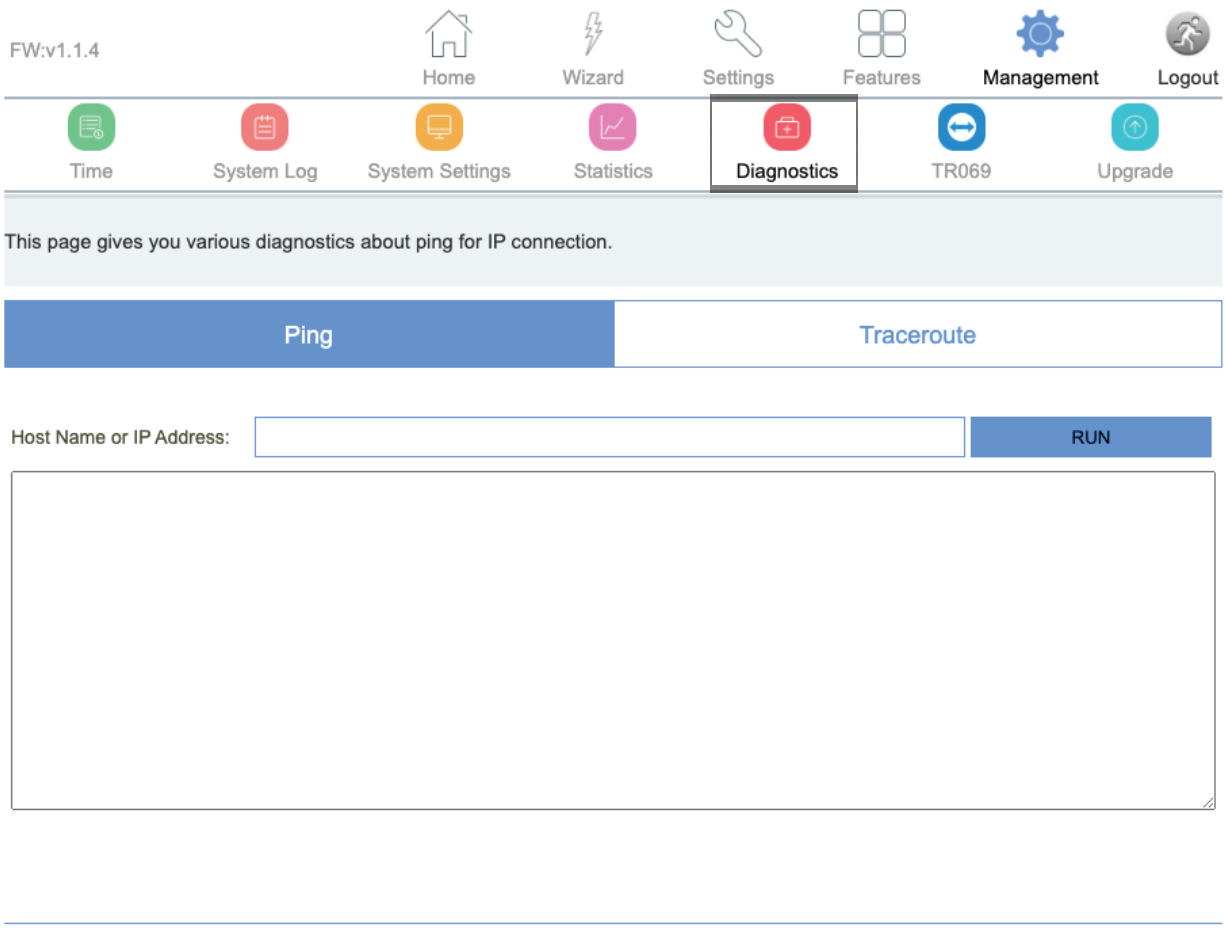


3.6.3.2 Interface Statistics

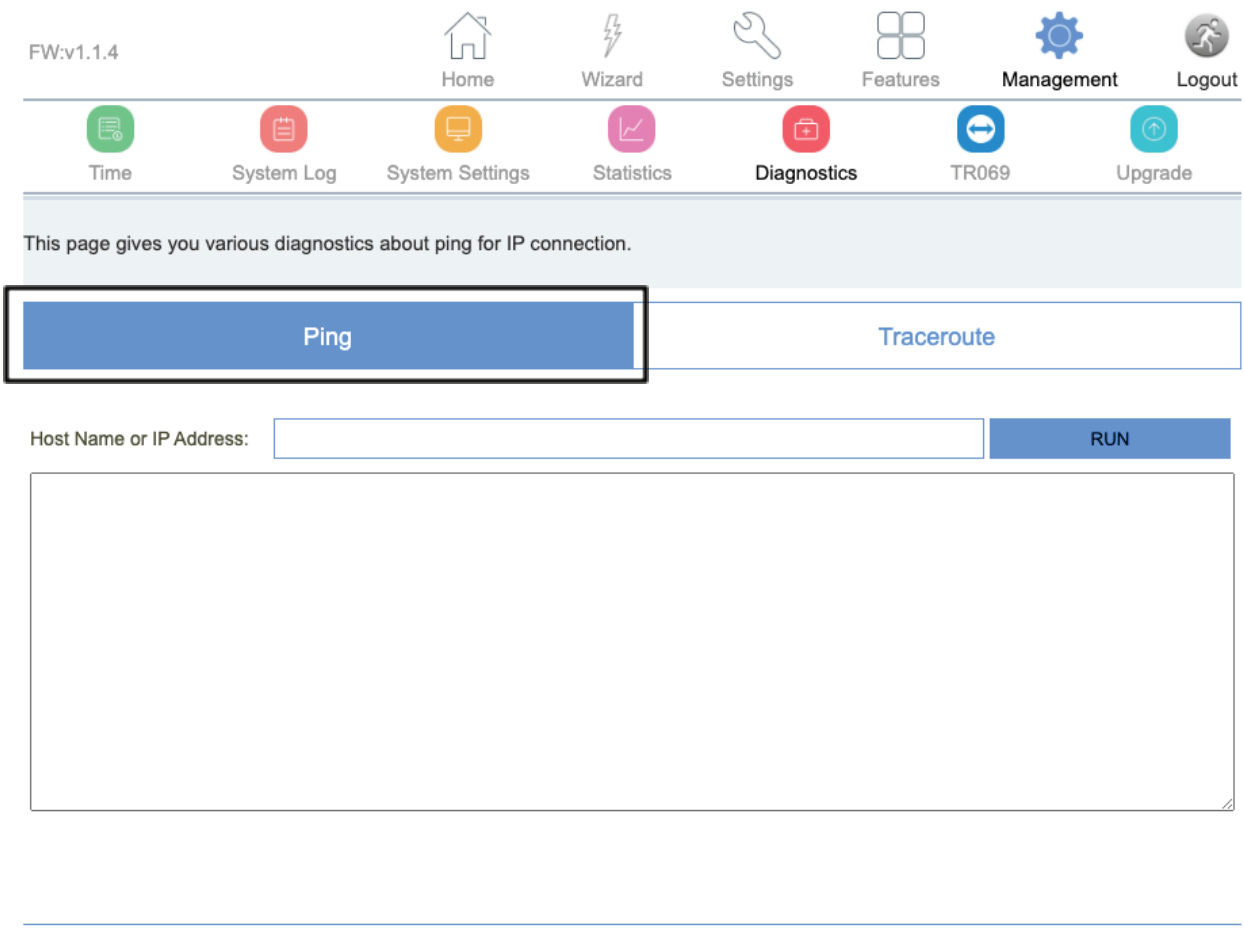


3.6.4 Diagnostics

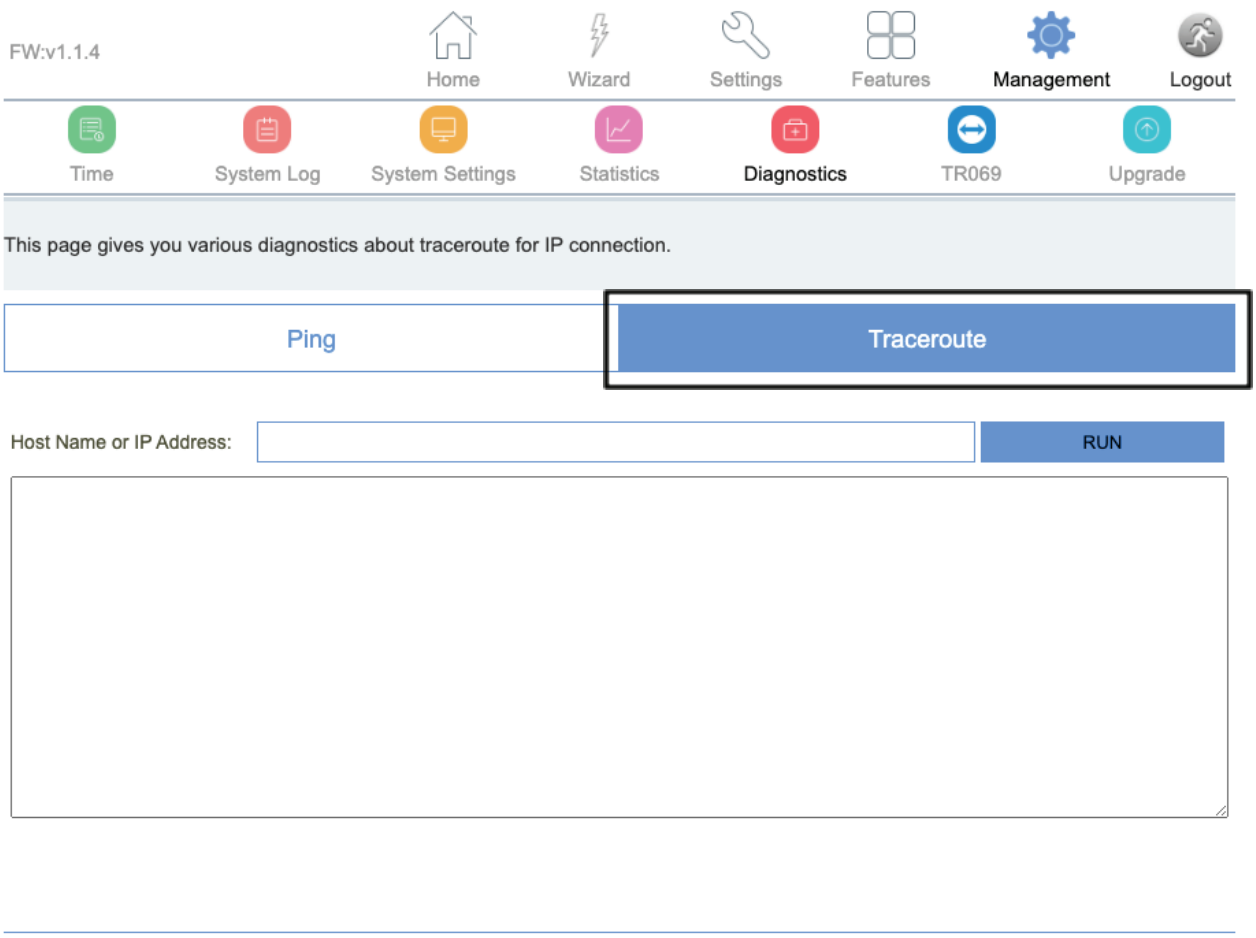
The **Diagnostics** page provides various diagnostics surrounding ping and traceroute for IP connection.



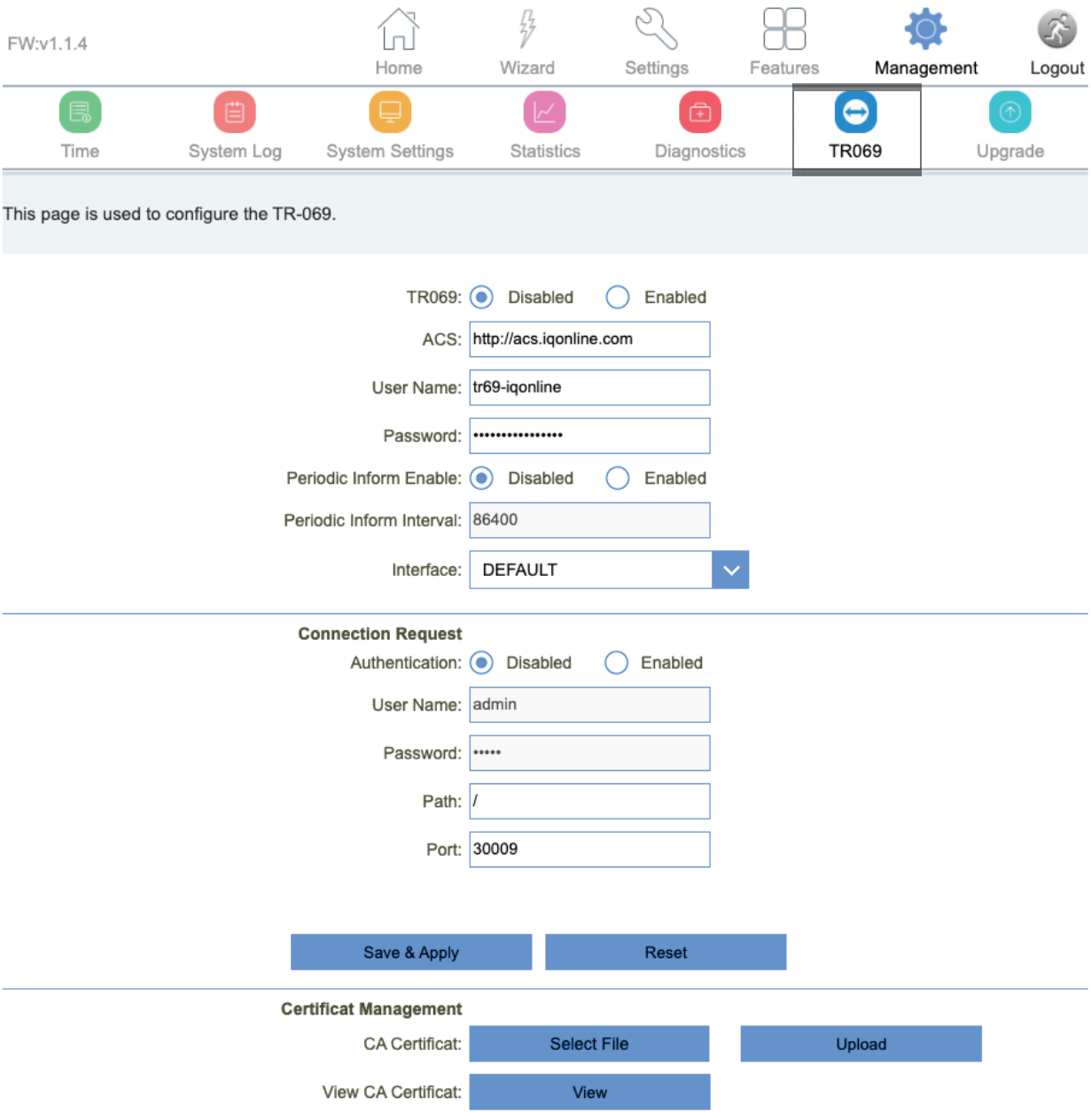
3.6.4.1 Ping


FW:v1.1.4
Home
Wizard
Settings
Features
Management
Logout
Time
System Log
System Settings
Statistics
Diagnostics
TR069
Upgrade
This page gives you various diagnostics about ping for IP connection.
Ping
Traceroute
Host Name or IP Address:
RUN

3.6.4.1 Traceroute



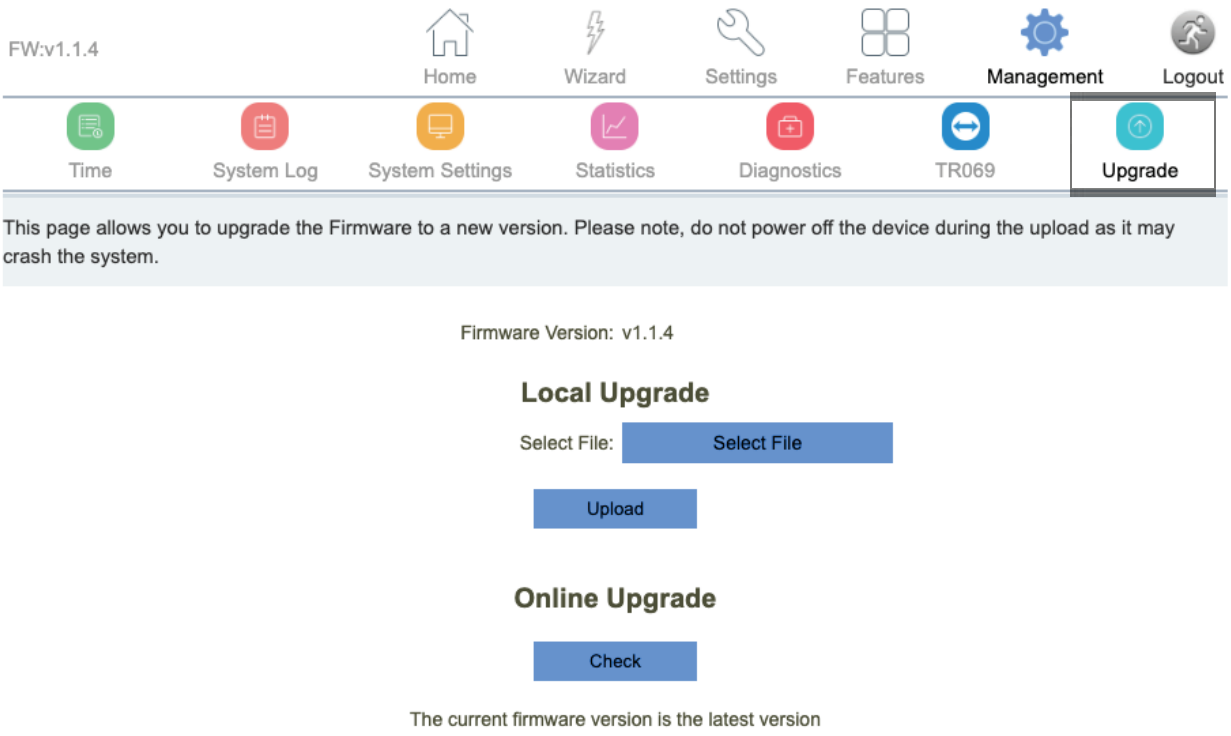
3.6.5 TR069



The **TR069** page is used to configure the TR069 functionalities in addition to setting the ACS's parameters.

Item	Description
TR069	Technical Report 069
ACS	ACS server domain or IP Address.
User Name	Username for connection to ACS.
Password	Password for connection to ACS.
Periodic Inform Enable	Periodic inform.
Periodic Inform Interval	Periodic inform interval.
Connection Request User Name	User Name used form ACS connection to TR069.
Connection Request Password	Password used form ACS connection to TR069.
Path	Connection request path.
Port	Connection port.

3.6.5 Upgrade



From time to time, new versions may be released of the Passport's Firmware. Firmware updates contain improvements and fix existing problems.

The **Local Upgrade** page enables users to upgrade the Passport's software.

The **Online Upgrade** section of the page enables users to upgrade the mobile module firmware to a new version.

Do not power off the device during the upload as it may crash the system.

LIMITED WARRANTY

Each new KING Passport is thoroughly inspected and tested before leaving the factory, and is covered by the following limited warranty from the date of original purchase:

- Two-year parts warranty: The customer is not responsible for the cost of replacement parts if the original part is determined to be defective under the terms of the warranty. The customer is responsible for the cost of replacement parts after two years.

Only KING and certified dealers may perform warranty evaluations and repairs. Depending upon the problem, KING may authorize a dealer to perform the necessary repairs. Any warranty labor outside of that performed at the factory is not covered unless 1) the product has been installed by an authorized dealer/installer or OEM manufacturer and 2) the dealer/installer receives prior authorization to perform the repair.

A certified dealer must not perform any repair without first contacting KING for a Service Order Number. KING will advise the dealer on how to proceed with any repairs.

Should any trouble develop during the warranty period, contact KING at (952) 345-8147. You must contact KING before the warranty period expires. The customer must supply proof of purchase (such as a dated sales receipt) when requesting warranty service. If the customer cannot supply proof of purchase, warranty period shall start 30 days after date of manufacture.

If it is determined that the unit needs to be returned to KING, customer must return COMPLETE product, freight prepaid, to:
KING, 11200 Hampshire Avenue South, Bloomington, MN 55438-2453.
If inspection shows the trouble is caused by defective workmanship or material, KING will repair (or at its option, replace) without charge.

When returning product, KING will supply an RMA number (Return Merchandise Authorization). This number must be clearly written on the box. Failure to clearly write RMA number on box will result in delays in processing claim. Along with product, the customer should include in the box: name, address, phone number, proof of purchase and description of the problem.

This warranty does not cover installation and external wiring, or remanufactured units. This warranty does not cover damage caused by the use of an accessory other than a KING accessory designed for the product. This warranty is not transferable from the original owner.

KING cannot be held responsible for changes in the expanding and changing digital and analog communications market that cause the product to no longer operate correctly.

This warranty also does not apply where:

- The product has been abused, misused, improperly installed or improperly maintained.
- The product has been used with an accessory other than a KING accessory designed for the product.
- Repairs have been made or attempted by others that are not certified by KING to do such repairs.
- Repairs are required because of normal wear and tear.
- Alterations have been made to the product.
- The product or any associated component has been opened without authorization or disassembled to any degree.
- Damage has been caused by power washing.
- Circumstances beyond the control of KING cause the product to no longer operate correctly.
- Customer is not the original owner.

In no event shall KING be liable for any indirect, incidental, or consequential damages from the sale or use of the product. This disclaimer applies both during and after the term of this warranty.

KING disclaims liability for any implied warranties, including implied warranties of "merchantability" and "fitness for a specific purpose," after the term of this warranty.

This warranty gives you specific legal rights, and you may also have other rights, which vary from state to state. Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you. Some states do not allow limitations on how long an implied warranty lasts, so the above limitation may not apply to you.

11200 Hampshire Avenue South, Bloomington, MN 55438

PH 952.922.6889 || FAX 952.922.8424 || kingconnect.com

© KING 2023 24489 Rev A

All trademarks are the sole property of their respective owners.