verizon

User Guide

Verizon Internet Gateway

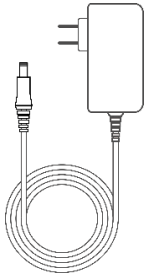
verizon

1. Inside the box

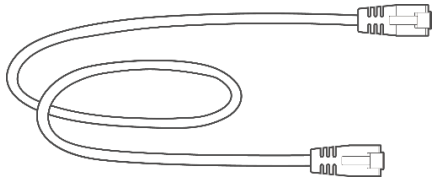
Inside the product package you should find the following items. Contact Verizon if any item is missing or damaged.

Verizon Internet Gateway

Power Adapter



Ethernet Cable

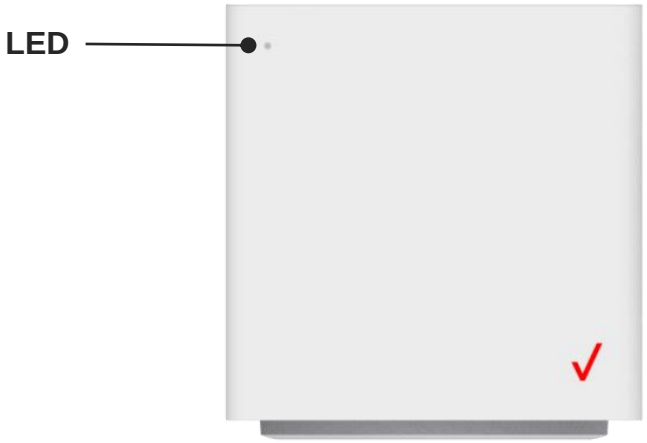


2. Your Verizon Internet Gateway

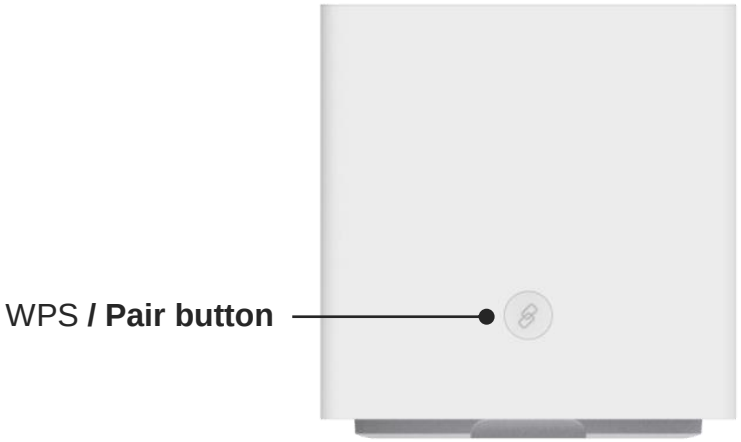
Your Verizon Internet Gateway provides fast dual-band Wi-Fi (with channel steering) for all your devices, and features built-in network security as well as parental controls, guest Wi-Fi and automatic software updates.

Take a moment to familiarize with your product:

Front



Back



Bottom

Reset Button

If you experience difficulties with your router or you want to revert all settings that you have changed, the reset function allows you to reset the router back to its factory default state. To perform a factory reset and return the Verizon Internet Gateway to default settings, press and hold the reset button for 3+ seconds. The LED will flash yellow to indicate a reset has been triggered, followed by fading in/out (white) while the router restarts.

WPS

WPS is an easy way to add supported Wi-Fi devices to your network. Press the WPS button on the back of the router to activate WPS. You will need to activate WPS on your Wi-Fi device too. Refer to **5.2.5 Wi-Fi Settings > WPS** for more information.

LED

The LED indicates the system and connection status, and WPS activity.

Front LED Mode	Status	LED1 Pattern
Bootup	System Off	Off
	System Booting	Soft blink White
	Firmware update (FOTA)	Fast blink white
Cellular signal (or after single click pair button)	Passing signal	Solid White
	No Signal, Cold SIM	Solid Red
	No SIM Card	Hard blink red
Regular usage	Setup complete	50% bright White
	WiFi disabled by user	Solid Green
Paring	WPS Paring	Hard blink Blue
Other	Factory Reset	Fast blink yellow
	FW Error	Soft blink red

Ethernet Port LED Mode	Status	Left LED	Right LED
Wired LAN connection	Ethernet > 100M* Link	Off	Solid White
	Ethernet > 100M* Activity	Off	Blinking White

* Threshold level can be decided based on port capability	Ethernet < 100M* Link	Solid Yellow	Off
	Ethernet < 100M* Activity	Blinking Yellow	Off
	No Ethernet connection	Off	Off

3. Setting Up Your Verizon Internet Gateway

Your Verizon Internet Gateway comes with a pre-installed SIM card and can be up and running in just a couple of minutes.

3.1 Positioning Your Router

For the best wireless signal transmission from the router to your network devices:

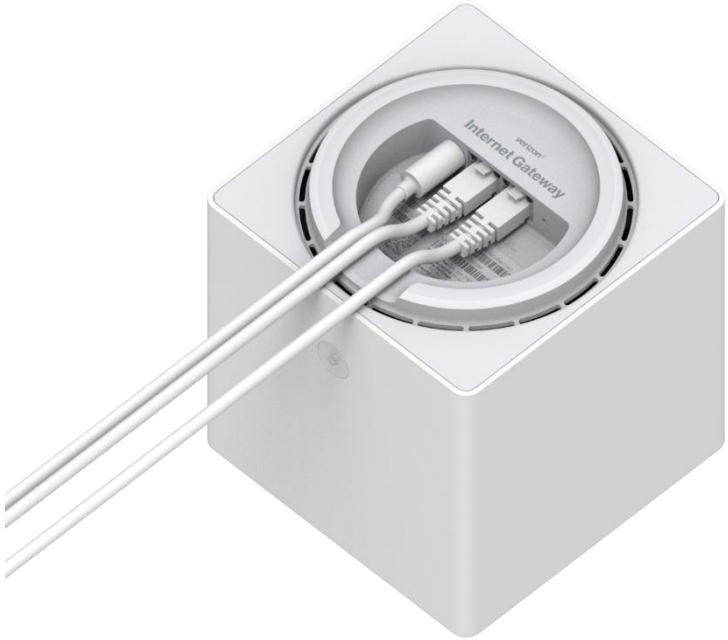
- Place the router in a central area near a window.
- Avoid keeping the device in the basement to get better signal.
- Avoid having obstacles near the device, clear any objects near the window that could interfere with getting a signal.
- Keep the router away from metal obstructions and away from direct sunlight.
- Keep the router away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, transformers, heavy-duty motors, fluorescent lights, microwave ovens, refrigerators, and other industrial equipment to prevent signal interference or loss.

3.2 Setup Requirements

To configure your wireless network via computer, you need a computer that meets the following system requirements:

- For Wired Connection -> Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/1000BaseTX)
- For Wi-Fi Connection -> IEEE 802.11a/b/g/n/ac/ax wireless capability
- An installed TCP/IP service
- Web browser such as Microsoft Edge, Firefox, Safari, or Google Chrome

3.3 Setting Up



1. Plug the router into a power outlet with the included power adapter.

2. Wait for a couple of minutes for the router to power up and establish a LTE/5G connection. The LED should display on (white) after starting up.

3. That’s it! You can connect your Internet devices to the router’s Wi-Fi networks named **Verizon_<your network>** (check your router’s product label on the bottom side for your unique Wi-Fi network name and password). You can also connect Internet devices to your router by Ethernet cable, by connecting your device’s LAN ports.

4. Go to **3. Login to your Verizon Internet Gateway** to login to your router and configure settings such as Wi-Fi security.

4. Login to Your Verizon Internet Gateway

You can login to your router's Web User Interface (Web UI) to access and change any of your router's settings and functions, such as Parental Controls and Wi-Fi security. You can also access network information such as connected devices and data usage.

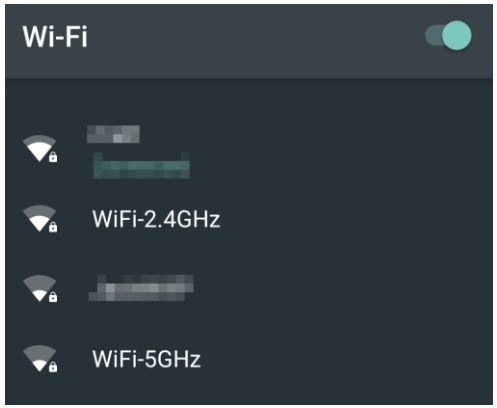
You can login to the Web UI using a computer or mobile device.

First connect your device to your router, then access the Web UI, as shown below.

4.1 Connect & Login by Mobile Device

1. You can automatically connect your device by scanning the QR code on the product label. To connect manually, move to step 2.

2. Scan available Wi-Fi networks with your mobile device:

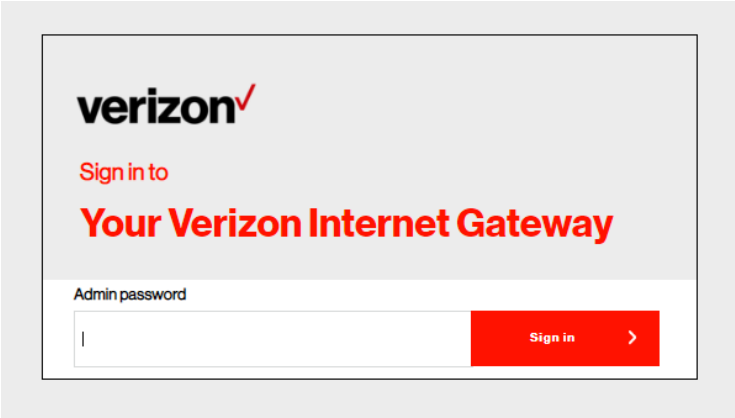


3. Select the WiFi network named **Verizon_<your network>** (check your router's product label on the bottom side for your unique Wi-Fi network name).

4. Enter your Wi-Fi password, which can also be found on your router's product label on the bottom side.

5. Open a web browser and enter the router's default address **http://192.168.0.1** in the address bar.

6. Log in using the default password (the default address and password are displayed on the product label on the bottom side of the router, labeled **Network Settings: URL and Password.**)



7. Check **5. Web User Interface** in this guide for more information about your router's settings.

4.2 Connect & Login by Computer

1. Scan available Wi-Fi networks with your computer.

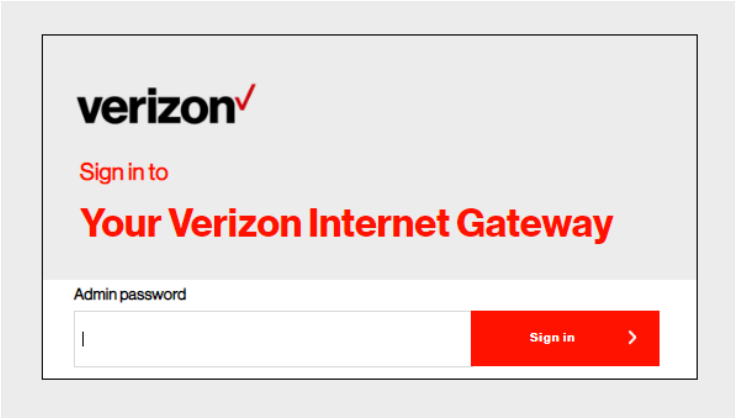
2. Select WiFi network named **Verizon_<your network>** (check your router's product label on the bottom side for your unique Wi-Fi network name).

3. Enter your Wi-Fi password, which can also be found on your router's product label on the bottom side.

4. If preferred, you can use an Ethernet cable to connect your computer to the router's LAN port for configuration (instead of Wi-Fi). Simply connect the two devices' LAN ports by Ethernet cable.

5. Open a web browser and enter the router's default address **http://192.168.0.1** in the address bar.

6. Log in default password (the default address and password are displayed on the product label on the bottom side of the router, labeled **Network Settings: URL and Password.**)



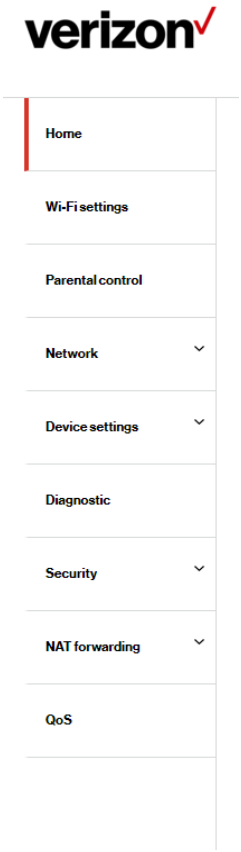
7. Check **5. Web User Interface** in this guide for more information about your router's settings.

5. Web User Interface

Your router's Web User Interface (Web UI) allows you to set up and configure its various functions. You can access the Web UI anytime by entering the router's default address **http://192.168.0.1** in the address bar of web browser on a device connected to the router. Check your router's product label for your unique GUI Password.

Menu

Use the left side menu to navigate:



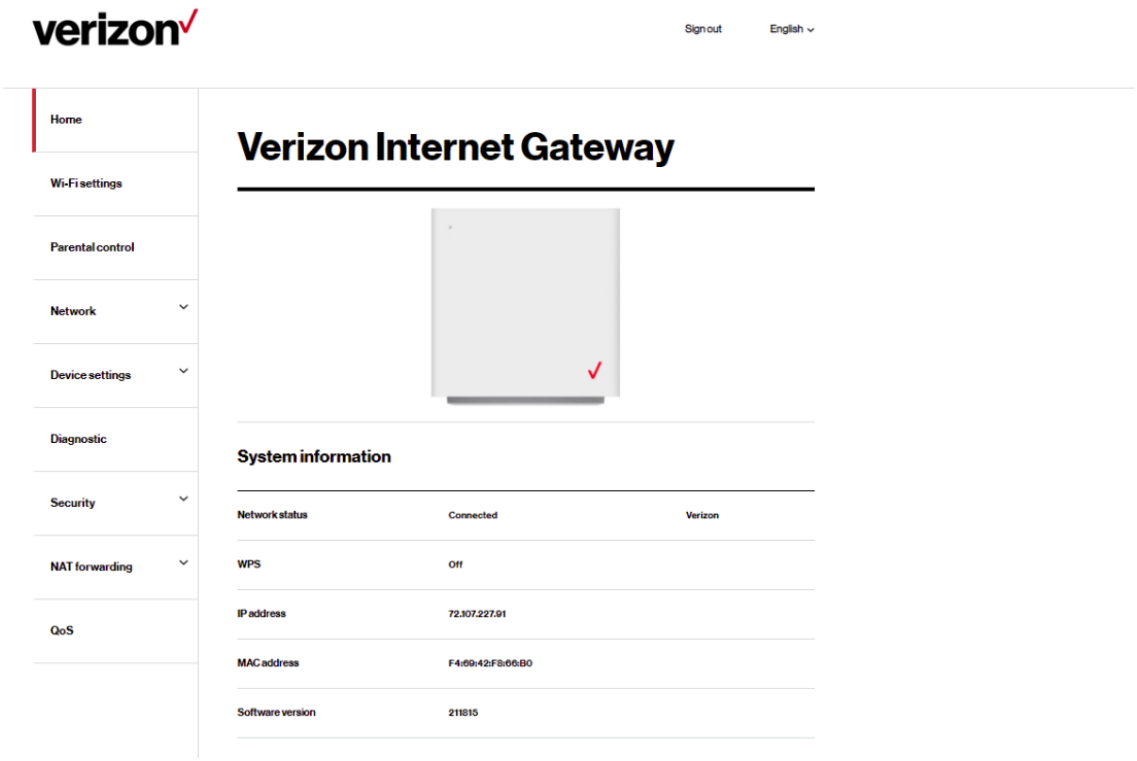
Save

Remember to save your settings with the save button after making changes.

5.1 Home

> Home

The **Home** page shows your network status and key system information. Network Status should display **Connected** to indicate a cellular network connection. If you don't see this, check the router's LEDs and refer to **Troubleshooting** for more help.



System Information

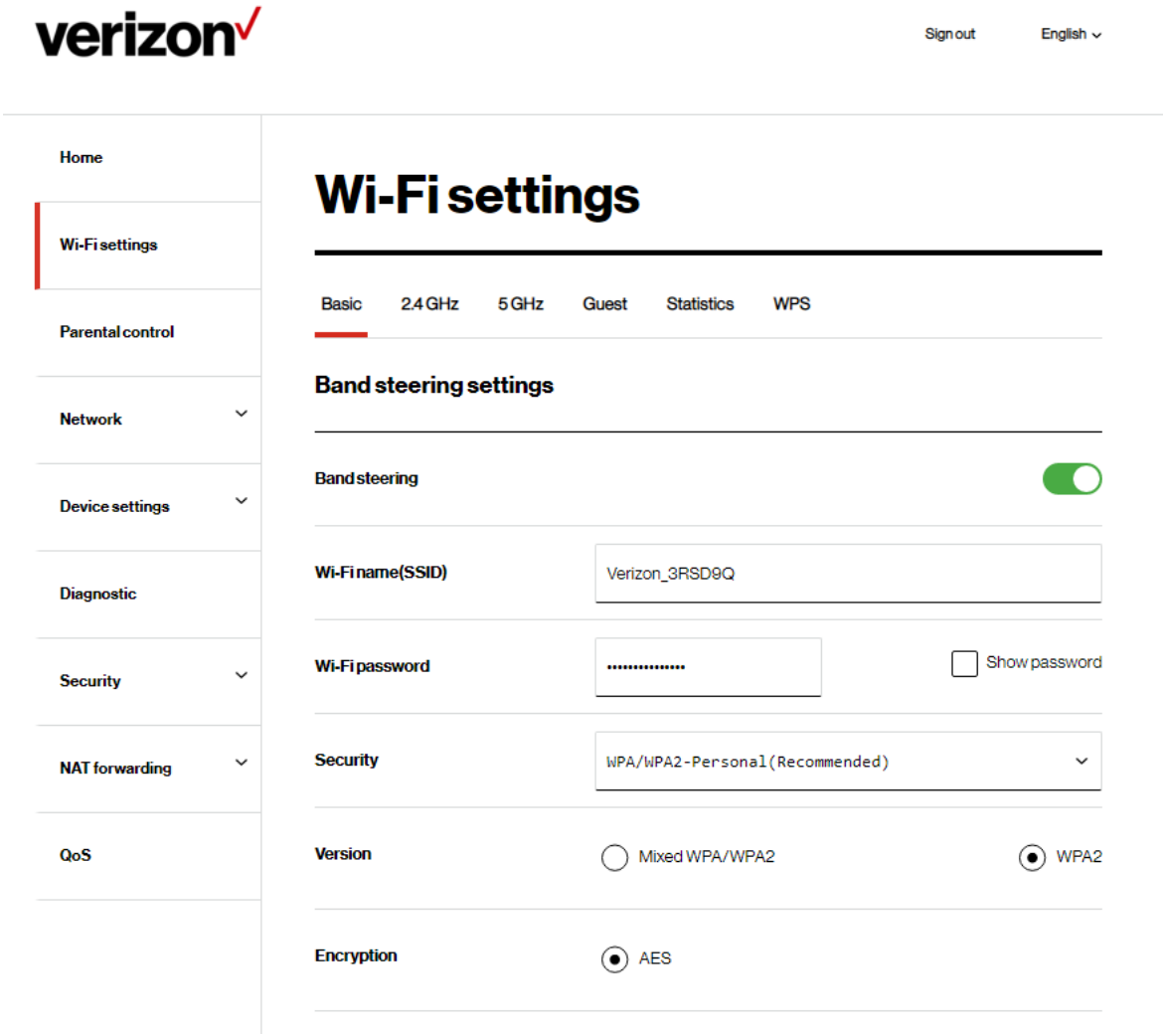
Network Status	Displays the status of your router's Information and connection status.
WPS	The WPS status of your router is shown here, indicating whether WPS is active or off.
IP Address	Your router's public IP Address is displayed here.
MAC Address	Displays the MAC address of your router. A MAC Address is a unique fixed identifier for any device on a network.

Software Version	Displays the current software version your router is running.

5.2 Wi-Fi Settings

> Wi-Fi Settings

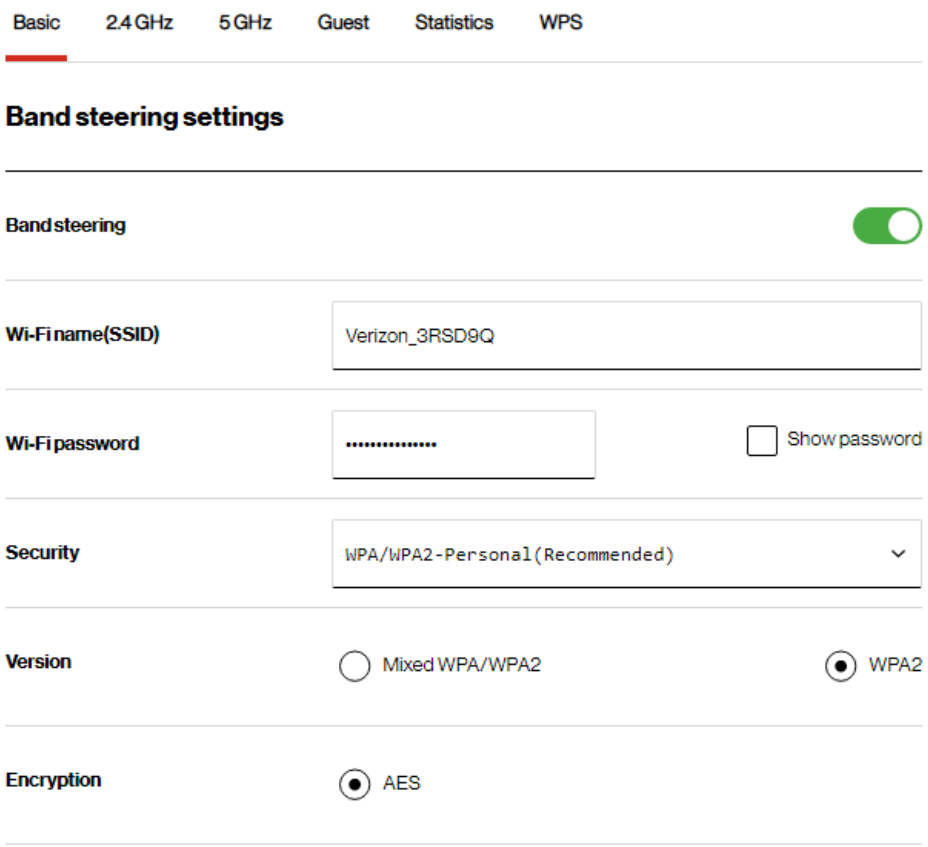
The **Wi-Fi Settings** screen displays advanced settings for your router's Wi-Fi, as well as WPS settings. Your router is dual-band and uses two Wi-Fi frequencies (2.4GHz & 5GHz) for better wireless performance on your devices.



5.2.1 Basic

> Wi-Fi Settings > Basic

All of your basic WiFi settings can be configured here. Band Steering is a feature which enables your router to dynamically assign wireless devices (smartphones, laptops etc.) to the best wireless frequency (2.4GHz or 5GHz). When Band Steering is enabled your dual-band router's network will have one Wi-Fi name.



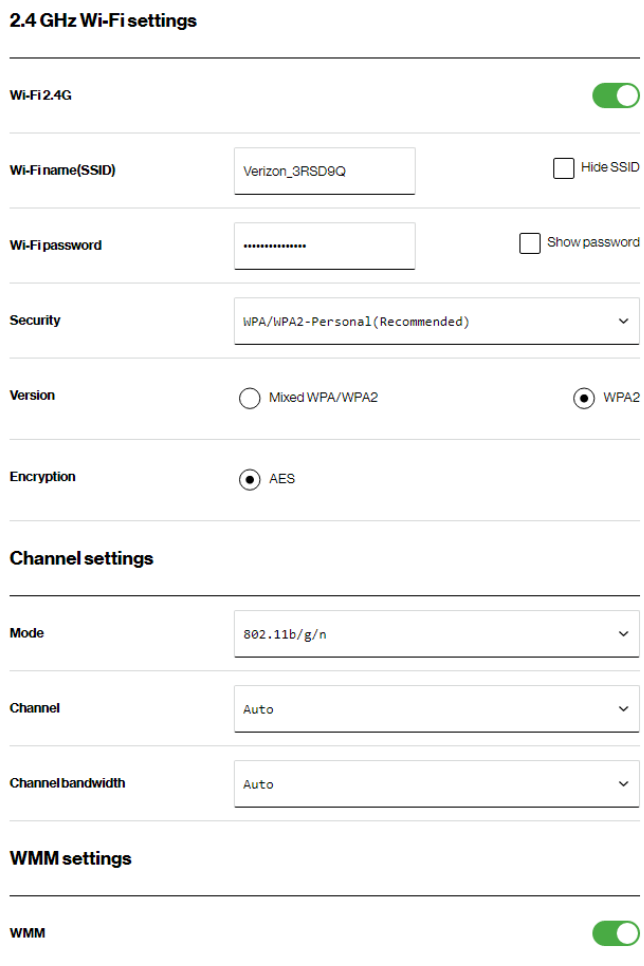
Band steering settings

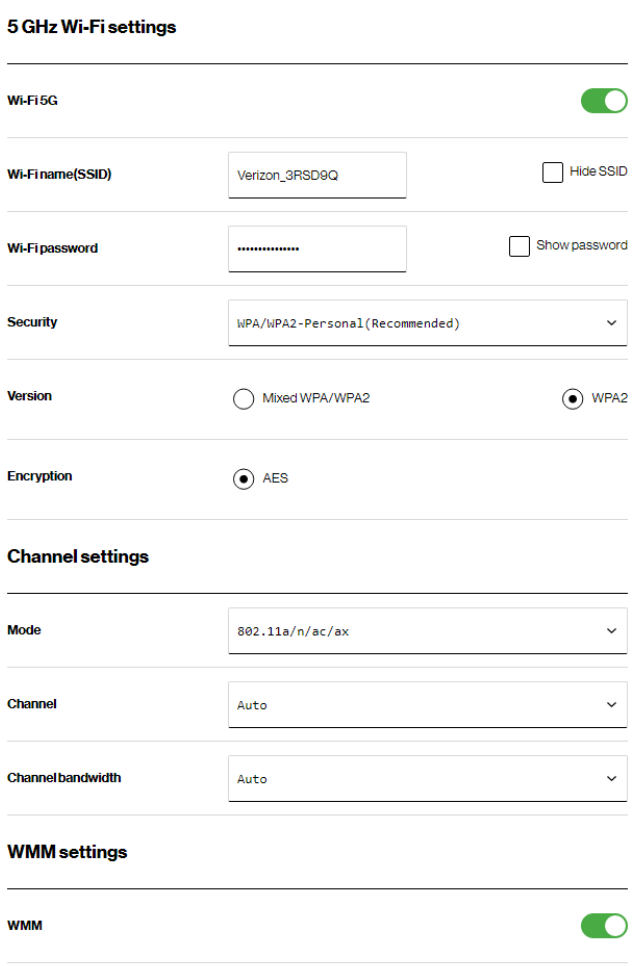
Band steering	Toggle to enable or disable Band Steering. When Band Steering is enabled your dual-band router's network will have one WiFi name, and your wireless devices will be assigned to the best frequency (2.4GHz or 5GHz) automatically. While enabled, all of the settings for your WiFi network can be configured in this tab. When disabled, your router will display two separate WiFi networks (2.4GHz & 5GHz) and the settings for each frequency can be configured from their respective tabs in the top menu.
Wi-Fi Name (SSID)	This is the name of your Wi-Fi network for identification, also sometimes referred to as "SSID". The SSID can consist of any combination of up to 32 alphanumerical characters.
Wi-Fi Password	Enter your Wi-Fi password. A complex, hard-to-guess password is recommended.
Security	Select a Wi-Fi security type from the drop-down menu. WPA/WPA2 is the default setting and the most secure. Security can be disabled by selecting None, but this is not recommended.
Version	Select which version of security type to use. WPA2 is the most secure, but is not supported by all wireless clients. Selecting Mixed WPA/WPA2 ensures wireless client compatibility.
Encryption	Displays encryption type according to version. AES encryption is the default setting for WPA2, while Mixed TKIP+AES is the default for Mixed WPA/WPA2.

5.2.2 2.4GHz / 5GHz

> Wi-Fi Settings > 2.4GHz / 5GHz

You can edit advanced settings for 2.4GHz or 5GHz by disabling Band Steering and updating the settings on the respective tab(s).





2.4 / 5 GHz Wi-Fi Settings

WI-FI 2.4GHz/5GHz	Toggle to enable or disable this Wi-Fi frequency.
Wi-Fi Name (SSID)	This is the name of your Wi-Fi network for identification, also sometimes referred to as “SSID”. The SSID can consist of any combination of up to 32 alphanumerical characters.
Hide SSID	Check the box to hide your SSID. When hidden, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden SSID is typically more secure than a visible SSID.
Wi-Fi Password	Enter your Wi-Fi password. A complex, hard-to-guess password is recommended.
Security	Select a Wi-Fi security type from the drop-down menu. WPA/WPA2 is the default setting and the most secure. Security can be disabled by selecting None, but this is not recommended.
Version	Select which version of security type to use. WPA2 is the most secure, but is not supported by all wireless clients. Selecting Mixed WPA/WPA2 ensures wireless client compatibility.
Encryption	Displays encryption type according to version. AES encryption is the default setting for WPA2, while Mixed TKIP+AES is the default for Mixed WPA/WPA2.

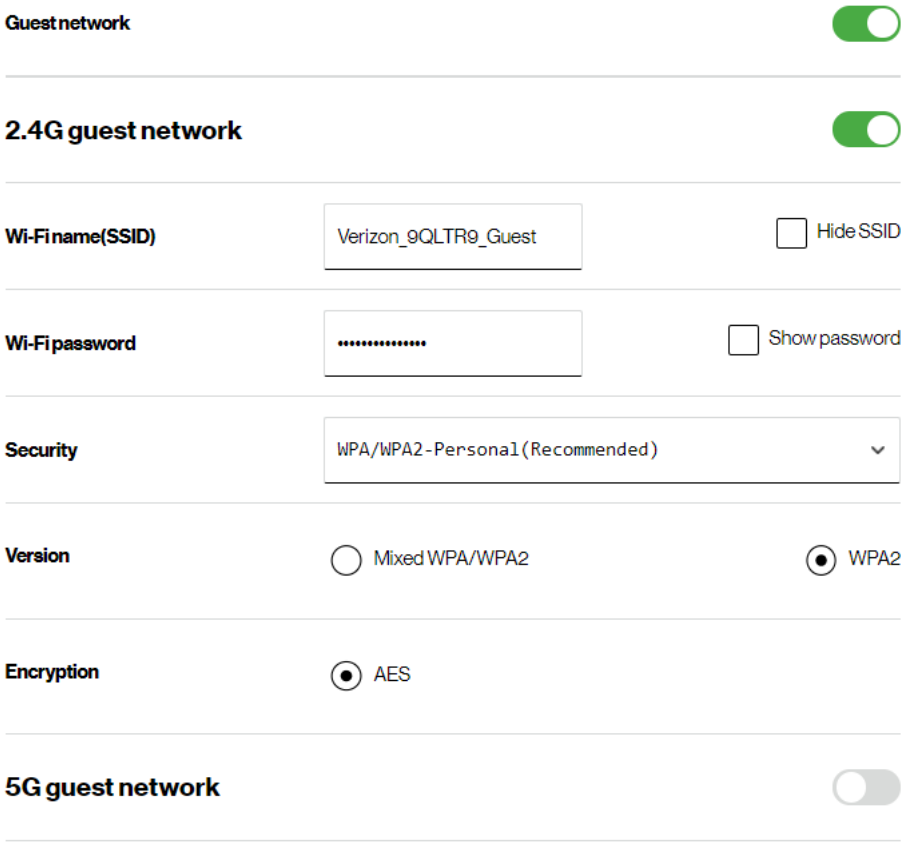
2.4 / 5 GHz Channel Settings

Mode	Select the wireless standard used for the router’s Wi-Fi. 802.11b/g mixed means 802.11b and 802.11g wireless clients can connect to the router, 802.11g/n mixed means 802.11g and 802.11n wireless clients can connect to the router, etc.
Channel	Select a wireless radio channel or use the default “Auto” setting from the drop-down menu. Changing the radio channel can improve Wi-Fi signal depending on how crowded the channel is with other radio signals and interference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (better performance but likely more interference), or Auto (automatically select based on interference level).
WMM	Toggle to enable or disable WiFi Multimedia (WMM). WMM is a feature which prioritizes bandwidth for audio and video applications in order to maintain best network performance.

5.2.3 Guest

> Wi-Fi Settings > Guest

You can set up additional “Guest” Wi-Fi networks (2.4GHz and/or 5GHz), so guest users can enjoy Wi-Fi connectivity without accessing your primary networks. The “Guest” tab displays settings for your guest Wi-Fi networks.



Guest

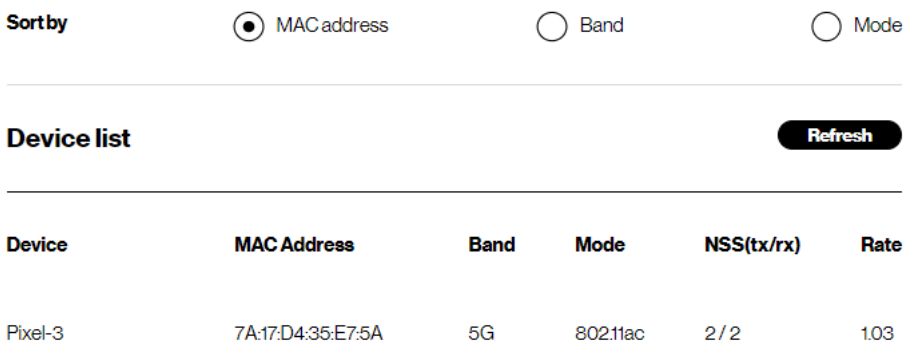
Guest Network	Toggle to enable or disable all guest networks.

2.4GHz / 5GHz Guest Network	Toggle to enable or disable guest network for displayed frequency, either 2.4GHz or 5GHz.
Wi-Fi Name (SSID)	This is the name of your Wi-Fi network for identification, also sometimes referred to as “SSID”. The SSID can consist of any combination of up to 32 alphanumerical characters.
Hide SSID	Check the box to hide your SSID. When hidden, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden SSID is typically more secure than a visible SSID.
Wi-Fi Password	Enter your Wi-Fi password. A complex, hard-to-guess password is recommended.
Security	Select a Wi-Fi security type from the drop-down menu. WPA/WPA2 is the default setting and the most secure. Security can be disabled by selecting None, but this is not recommended.
Version	Select which version of security type to use. WPA2 is the most secure, but is not supported by all wireless clients. Selecting Mixed WPA/WPA2 ensures wireless client compatibility.
Encryption	Displays encryption type according to version. AES encryption is the default setting for WPA2, while Mixed TKIP+AES is default for Mixed WPA/WPA2.

5.2.4 Statistics

> Wi-Fi Settings > Statistics

Displays statistics and information about each connected network device, sortable by MAC address, frequency band or mode.



Statistics

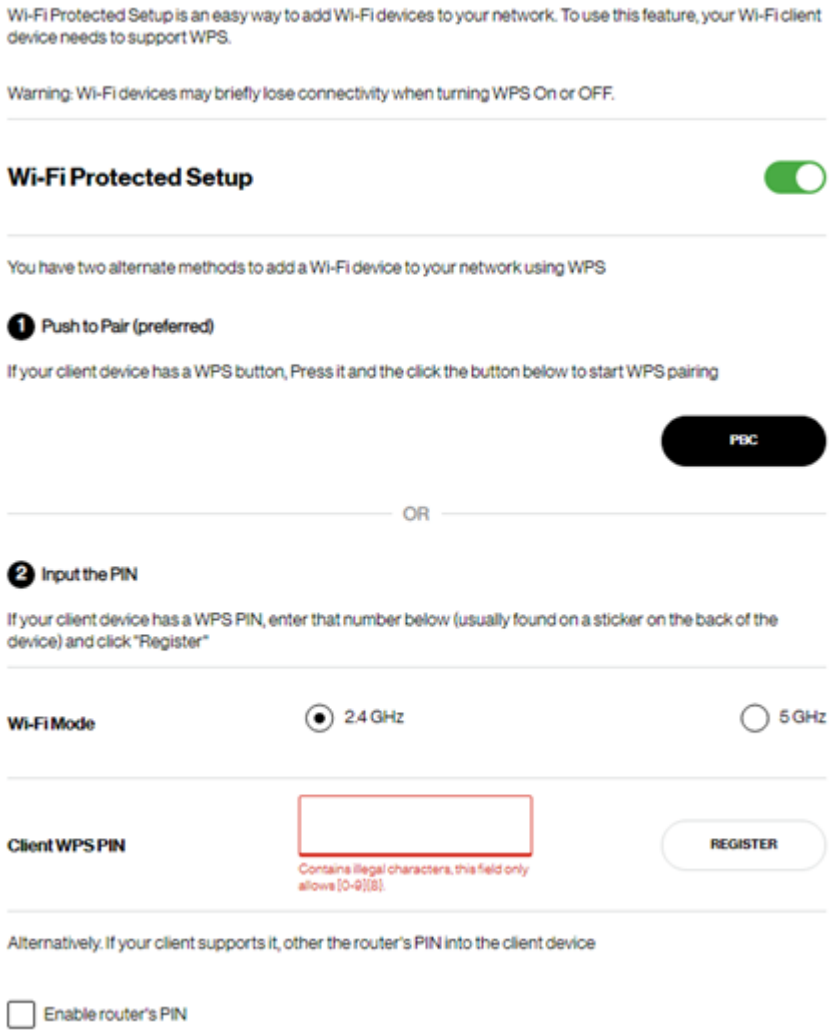
Sort by	Sort entries in the devices list by MAC address, frequency band or mode.
Device	Name of the device (smartphone, laptop etc.) connected to the router.
MAC Address	MAC address of the network device. A MAC Address is a unique fixed identifier for any device on a network.
Band	The wireless frequency band (2.4GHz or 5GHz) to which the network device is connected.
Mode	The wireless mode (standard) which is used by the device for the network connection.
NSS (Tx/Rx)	No. of spatial streams for data transmitted (Tx) and received (Rx). WiFi Spatial Streaming is a transmission technique used in MIMO wireless communication for better performance.
Rate	Represents the maximum transmission rate between router and client.

5.2.5 WPS

> Wi-Fi Settings > WPS

Wi-Fi Protected Setup (WPS) is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the device or from within the device's firmware/configuration interface (known as PBC or "Push Button Configuration"). When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. "PIN code WPS" is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.

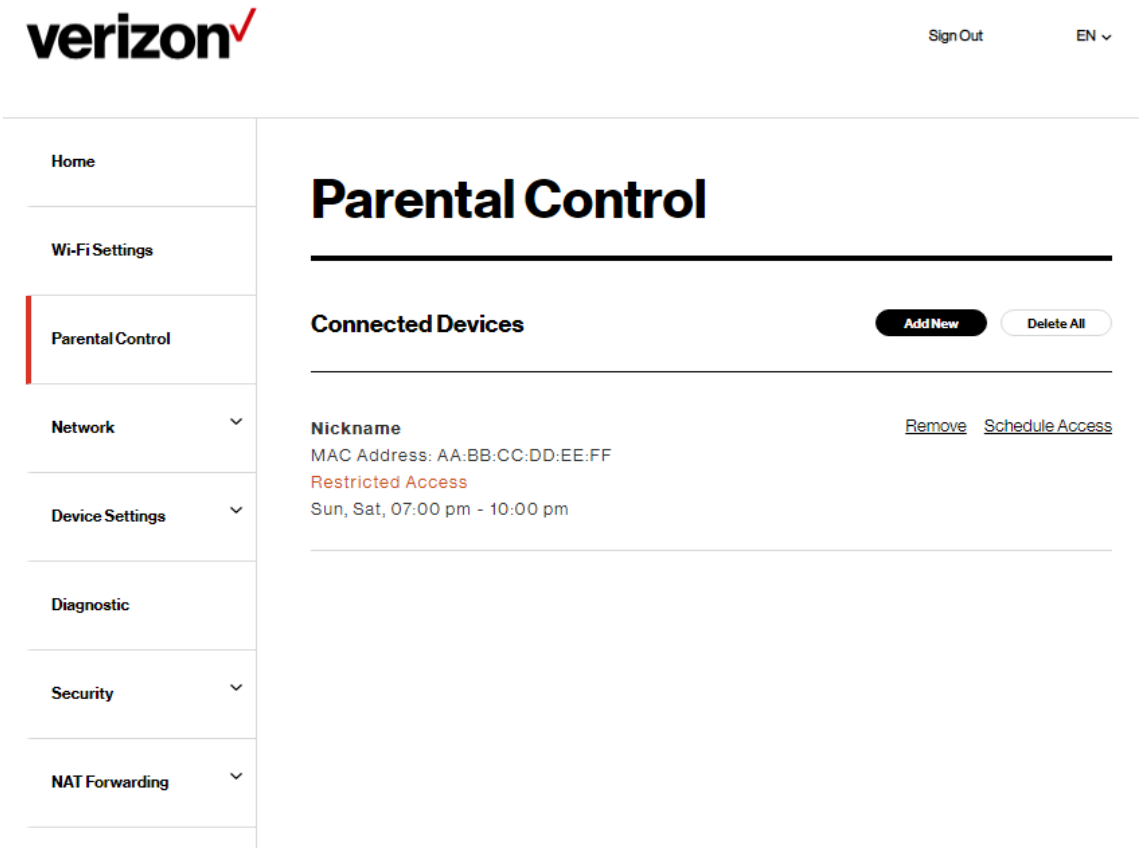
Follow the instructions on screen.



5.3 Parental Control

> Parental Control

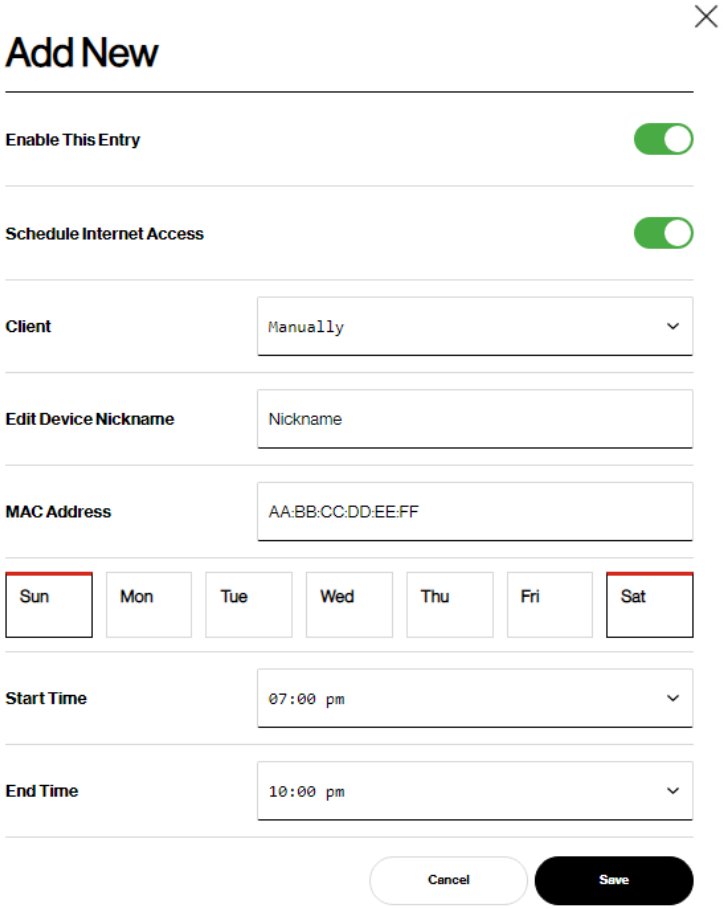
The **Parental Control** feature allows you to restrict Internet access to selected devices on your network at specified times e.g. disabling Internet access for a child's smartphone.



1. Click **Add New** to add and setup a new device for parental controls.
2. Toggle **Enable This Entry** to enable/disable this parental control setup.
3. Toggle **Schedule Internet Access** to enable/disable the schedule for Internet access:

4. Select a device from the Client menu or enter the MAC address manually below.

5. Specify a Device Name and enter a Description of the device for easy reference.



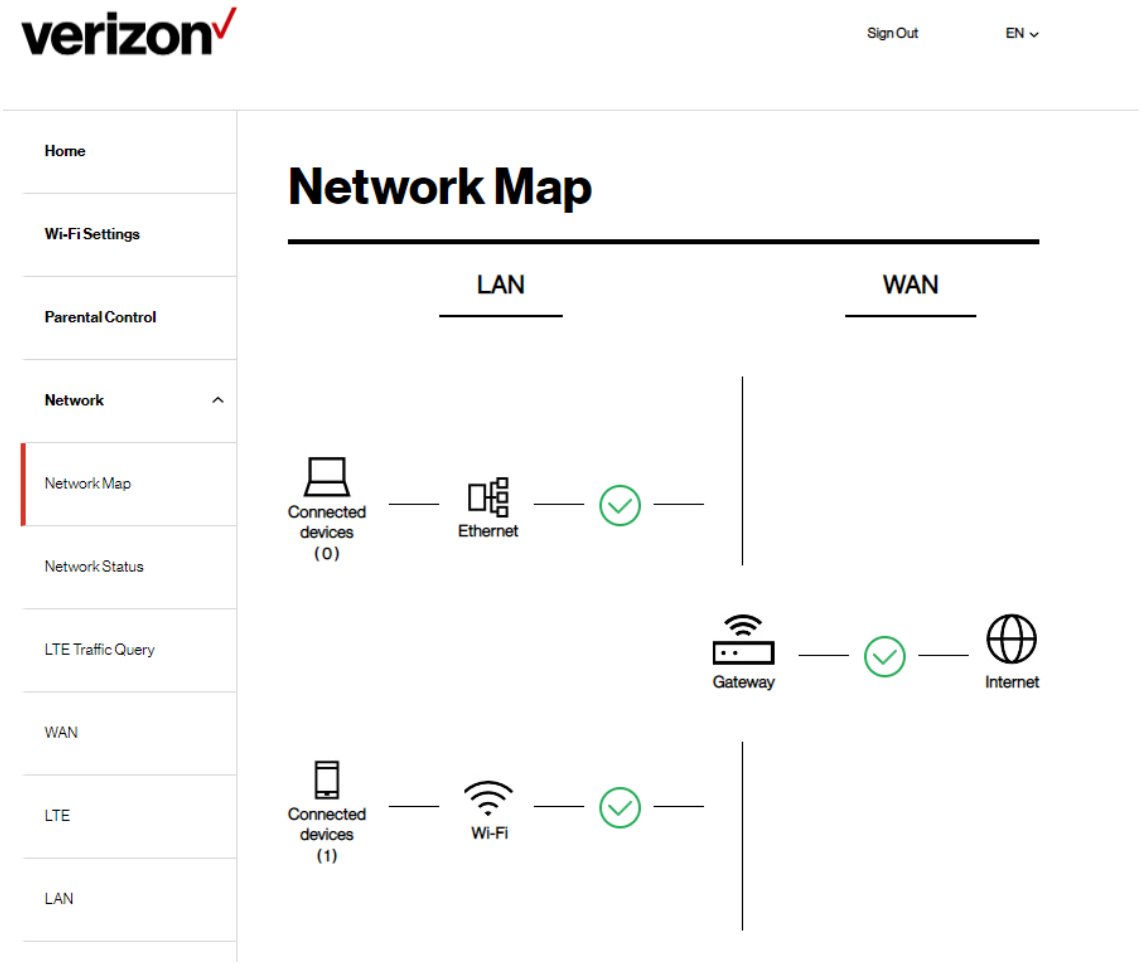
6. Click to select and specify which days to apply the parental control restrictions, and set the start and end times.

7. Click **Save** to save the schedule and the device's Internet access will now be restricted according to the schedule.

5.4 Network

> Network

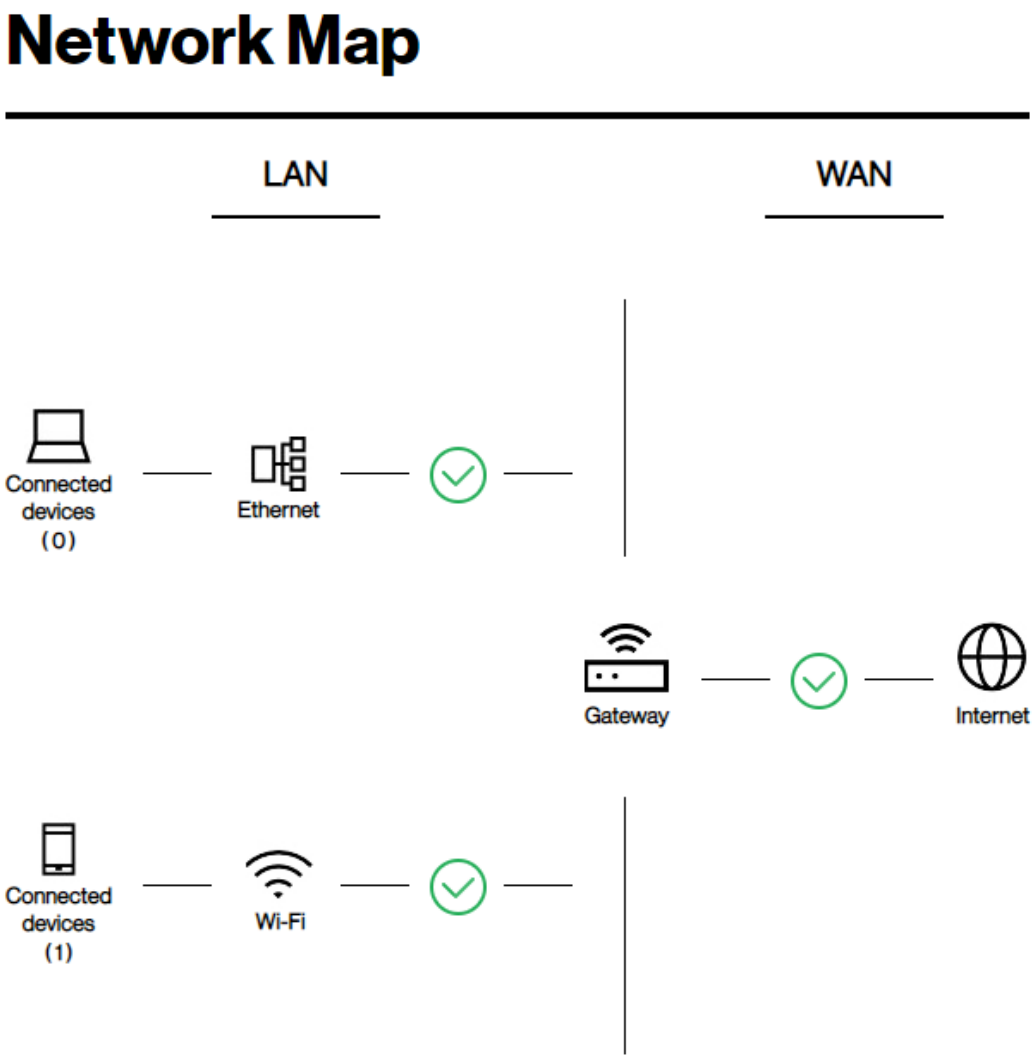
The **Network** menu provides quick links to the networking functions of your router. When you select the Network menu, the Network Map page is displayed as below.



5.4.1 Network Map

> Network > Network Map

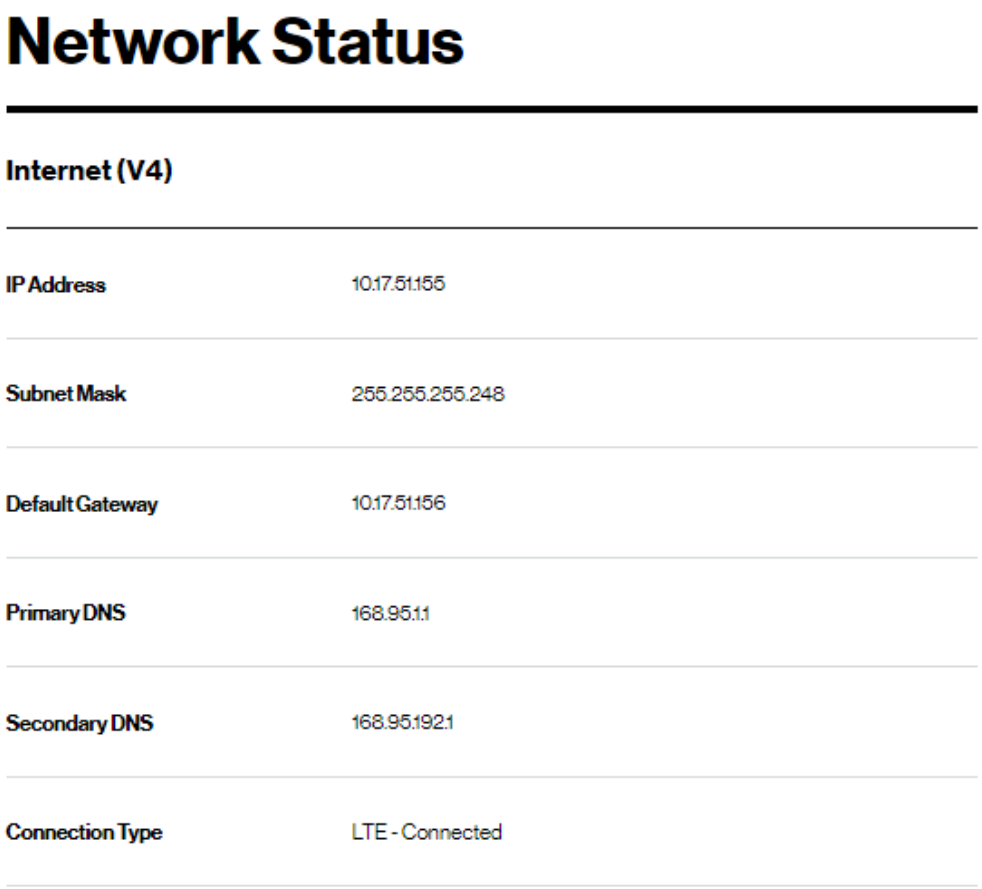
The **Network Map** provides a visual overview and status information of the network and devices on the network, with quick links to LAN & WAN settings and connected device / client lists. Green check marks indicate everything is working correctly.



5.4.2 Status

> Network > **Network** Status

Network Status displays the status of the network across six categories: Internet v4, Internet v6, LTE, LAN, Wireless & System Information.



Internet v4

Displays IPv4 Wide Area Network (WAN) information about your router's LTE connection. IPv4 is the default Internet protocol widely used across the Internet.

Internet v6

Displays IPv6 Wide Area Network (WAN) information about your router's LTE connection. IPv6 is an alternative Internet protocol which is not yet widely supported. To set up IPv6 go to **Network > IPv6.**

Network > Cellular

Displays cellular data information including signal strength.

LAN

Displays the router's Local Area Network (LAN) information including MAC Address, IP Address and Subnet Mask, and DHCP Server status. To edit LAN settings go to **Network > LAN.**

Wireless 2.4GHz & 5GHz

Displays your router's Wi-Fi information for both 2.4GHz & 5GHz frequencies. Includes network name (SSID) and radio & channel information. To edit these Wi-Fi settings, go to **Wi-Fi Settings.**

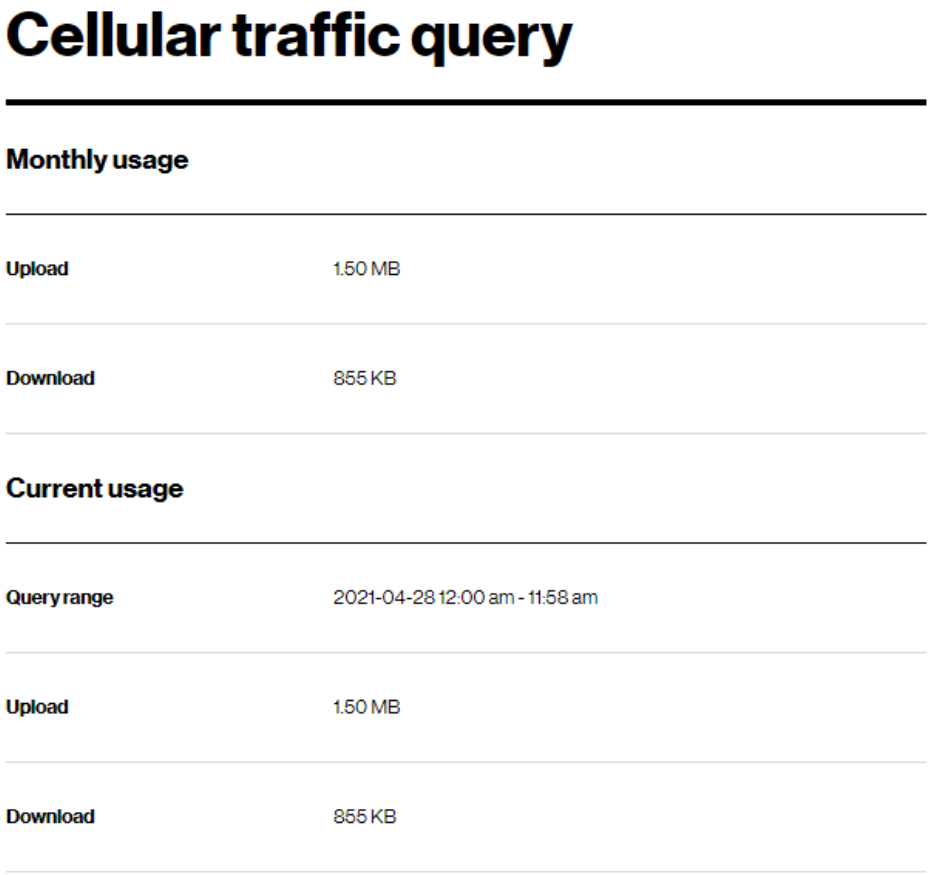
System Information

Displays system identifiers unique to your hardware.

5.4.3 Cellular Traffic Query

> Network > Cellular Traffic Query

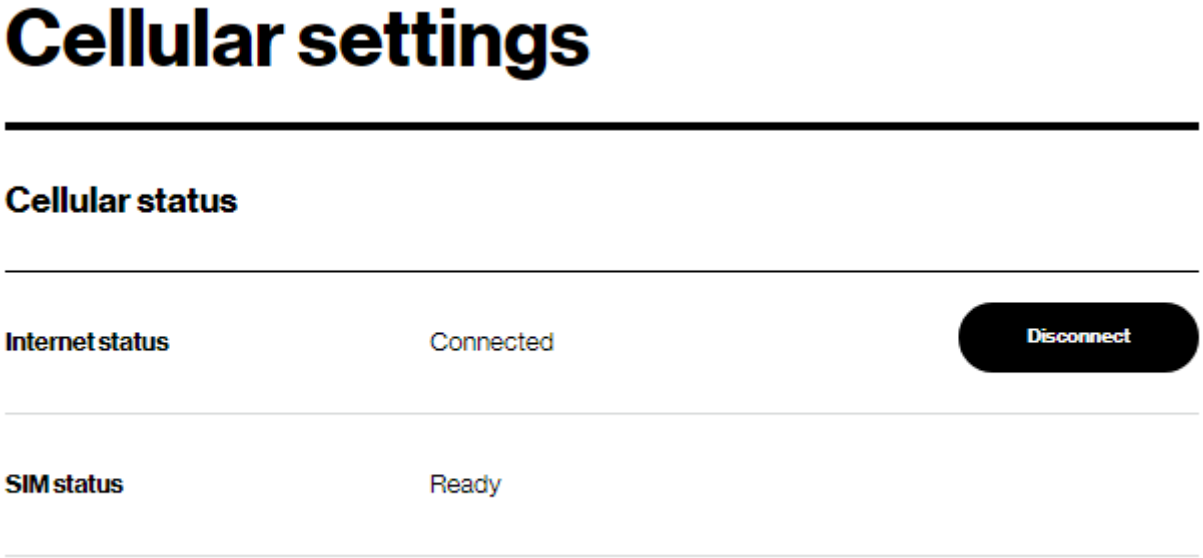
Traffic Query displays your network data usage, with upload and download data displayed in MB and KB for monthly and current periods. Ensure that your router's date and time settings are correct in **Device Settings > Date / Time** for accurate Monthly usage information.



5.4.4 Cellular

> Network > Cellular

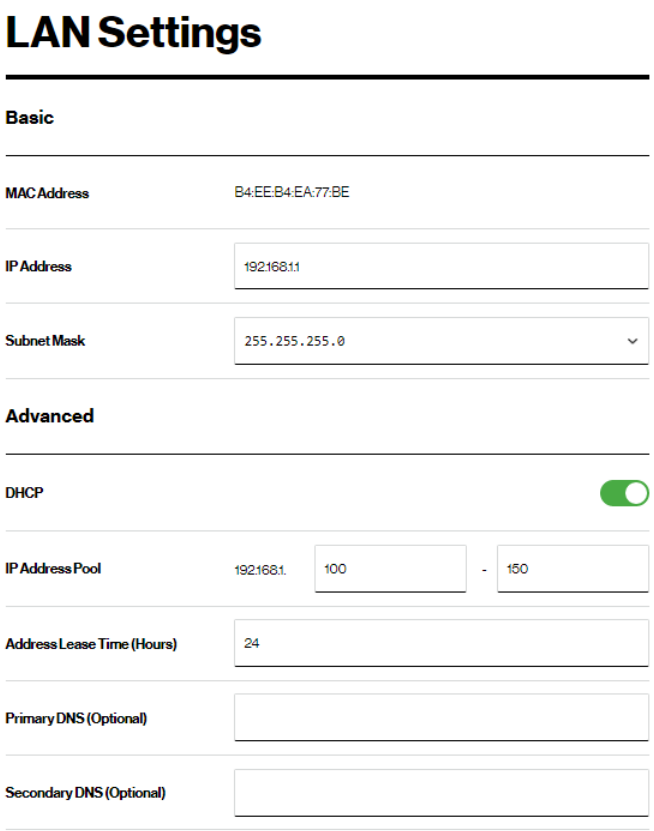
Cellular settings are pre-configured by default. You can disconnect the cellular connection using the Disconnect button if needed, and the connection and SIM status are displayed accordingly.



5.4.5 LAN

> Network > LAN

The **LAN Settings** page allows you to configure your router on your Local Area Network (LAN). You can specify a static IP address for your router, and configure your router as a DHCP server to assign IP addresses to other devices on your LAN.



Basic

MAC Address	Displays the MAC address of your router. A MAC address is a unique fixed identifier for every device on a network.
IP Address	Specify the IP address here. This IP address will be assigned to your router and will replace the default IP address.

Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0

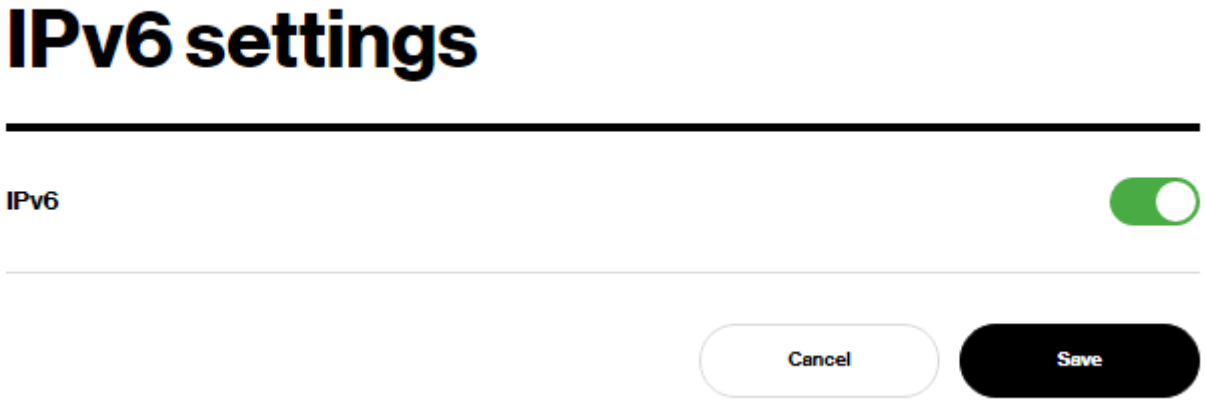
Advanced

DHCP	Toggle the switch to enable or disable DHCP server.
IP Address Pool	Enter the start and end IP address of the IP address range which your router’s DHCP server will assign to devices on the network.
Address Lease Time	Enter an address lease time in hours. IP addresses will be assigned for this period of time before being reassigned.
Primary DNS Address	Enter a primary DNS address.
Secondary DNS Address	Enter a secondary DNS address.

5.4.6 IPv6

> Network > IPv6

To enable/disable IPv6 settings.

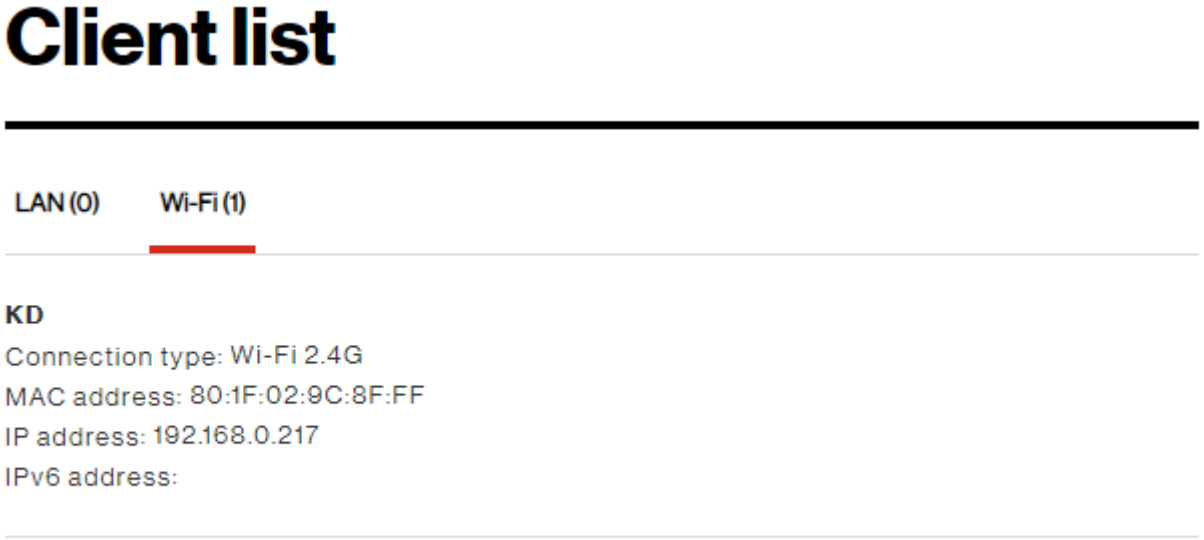


j

5.4.7 Client List

> Network > Client List

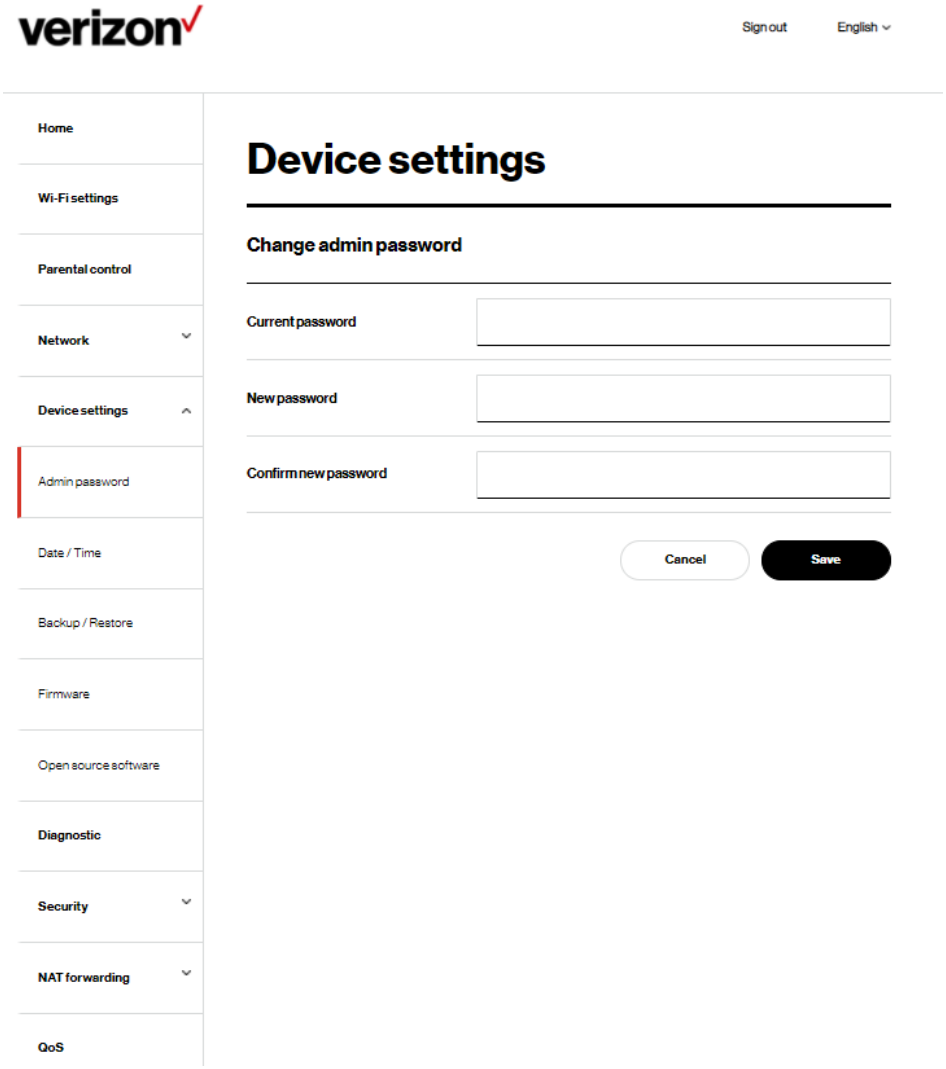
Displays all devices (clients) connected to your router, by Ethernet (LAN) or Wi-Fi (wireless) e.g. laptops, smartphones. The device name, connection type, MAC address, IP address and (where applicable) IPv6 address is listed for each device.



5.5 Device Settings

> Device Settings

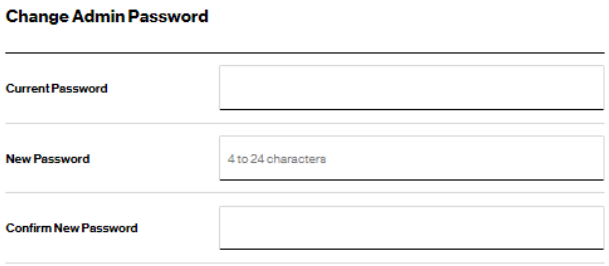
Various administrative functions of your router can be configured from the **Device Settings** menu, including the Web UI login password, router date & time settings, backup, router firmware and system logs.



5.5.1 Admin Settings

> Device Settings > Admin Settings

The **administration** function allows you to change the login password for the router's Web UI. It's essential to change this password for the security of your router. Use hard-to-guess password, which should include combinations of numbers, letters and symbols, and change your password regularly.



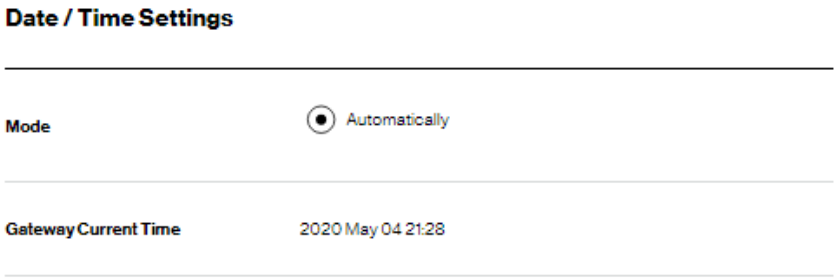
1. Enter the current password for authentication.

2. Enter your name password in the New Password field and again to confirm, and choose **Save** to save the new settings.

5.5.2 Date & Time

> Device Settings > Date & Time

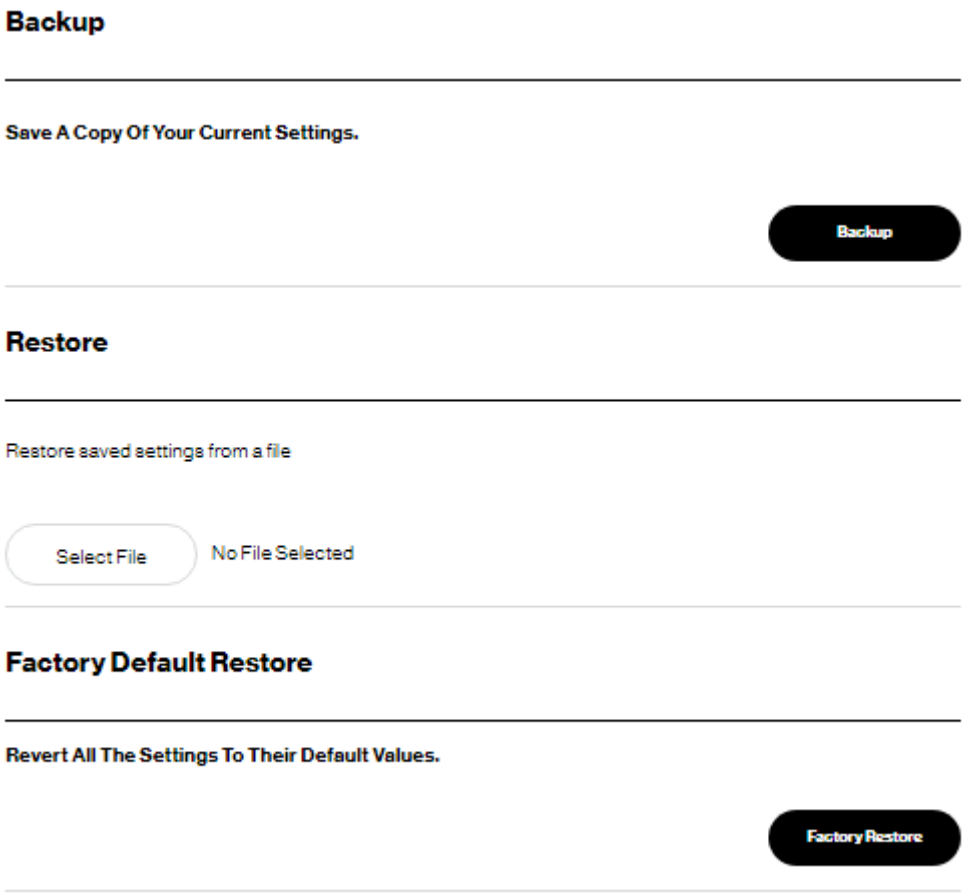
The **date and time** for your router is configured automatically over the cellular network and is displayed here.



5.5.3 Backup / Restore

> Device Settings > Backup / Restore

The Backup / Restore page enables you to save/backup the router's current settings as a file to your local computer, or restore your router to previously saved settings by loading a backed up file. You can also reset the router back to factory default settings. If the router malfunctions or is not responding, then it is recommended that you first reboot the device, and if still experiencing problems, reset the device back to its factory default settings. To perform a factory reset and return the Verizon Internet Gateway to default settings, press and hold the reset button for 1-2 seconds.



Backup

Save a copy of your current settings	Save a copy of your current settings.

Restore

Restore saved settings from a file	Choose Select File to locate a previously saved settings file on your computer and select it to load the file to your router.

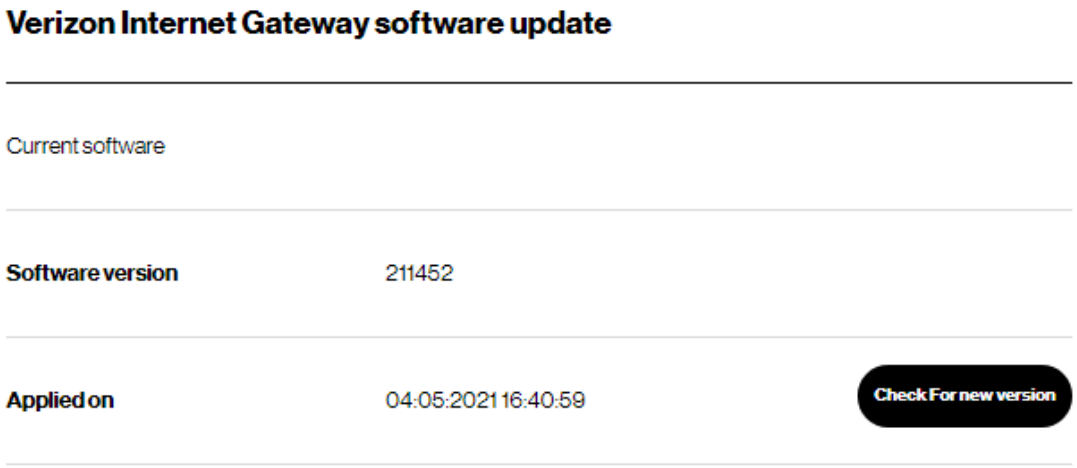
Factory Default Restore

Revert all the settings to their default values.	Select Factory Restore to revert your router to its original factory default state. This resets all settings.

5.5.4 Firmware

> Device Settings > Firmware

The **Firmware** page displays your router's firmware version information. Firmware is the software that your router runs on. You can click **Check for New Version** to manually initiate a check to see if new firmware is available.



5.5.5 Open source software

> Device Settings > Open source software

Open source software

This product includes software made available under open source licenses. Additional information about that software, applicable licenses, and downloadable copies of source code, is available at:

https://verizon.com/opensource/

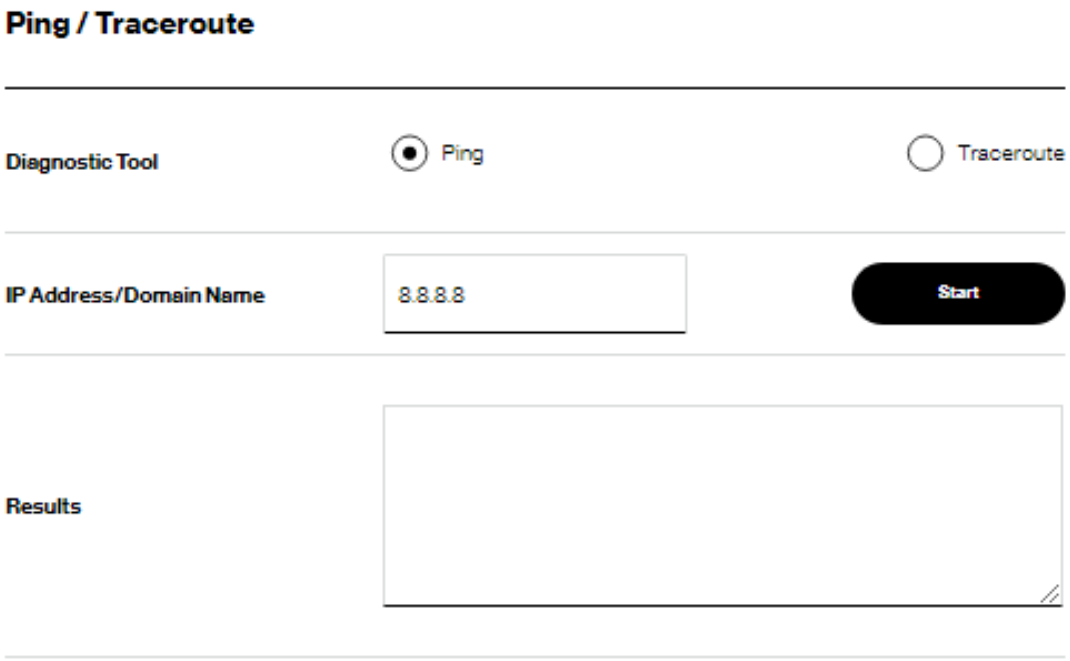
All open source software contained in this product is distributed WITHOUT ANY WARRANTY. All such software is subject to the copyrights of the authors and to the terms of the applicable licenses included in the download.

This information is provided for those who wish to edit or otherwise change such programs. You do not need a copy of any of such open source software source code to install or operate the device.

5.6 Diagnostic

> Diagnostic

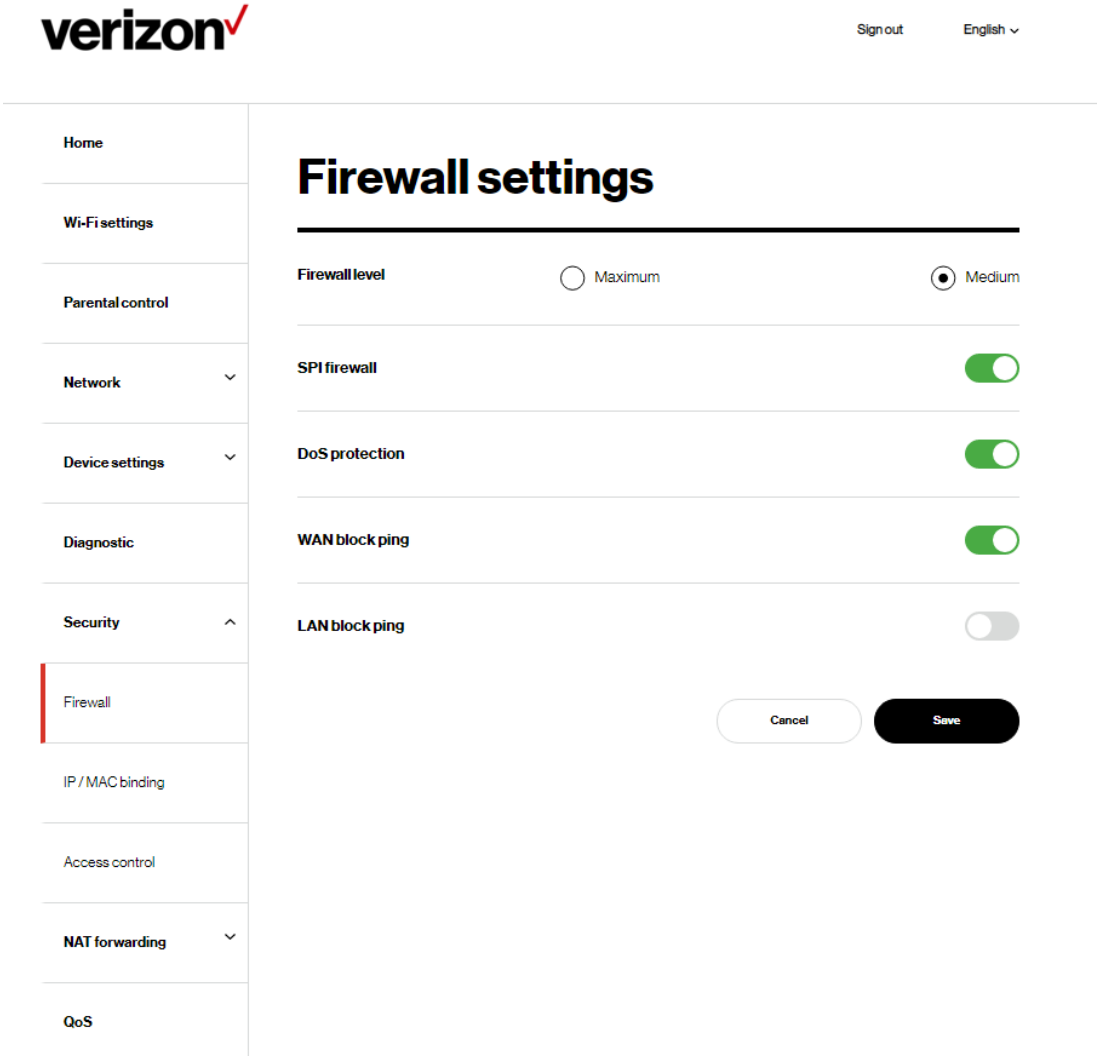
You can run **Ping & Traceroute diagnostic** tests with the router. Enter the IP address to use for the test and click Start; results are displayed in the box.



5.7 Security

> Security

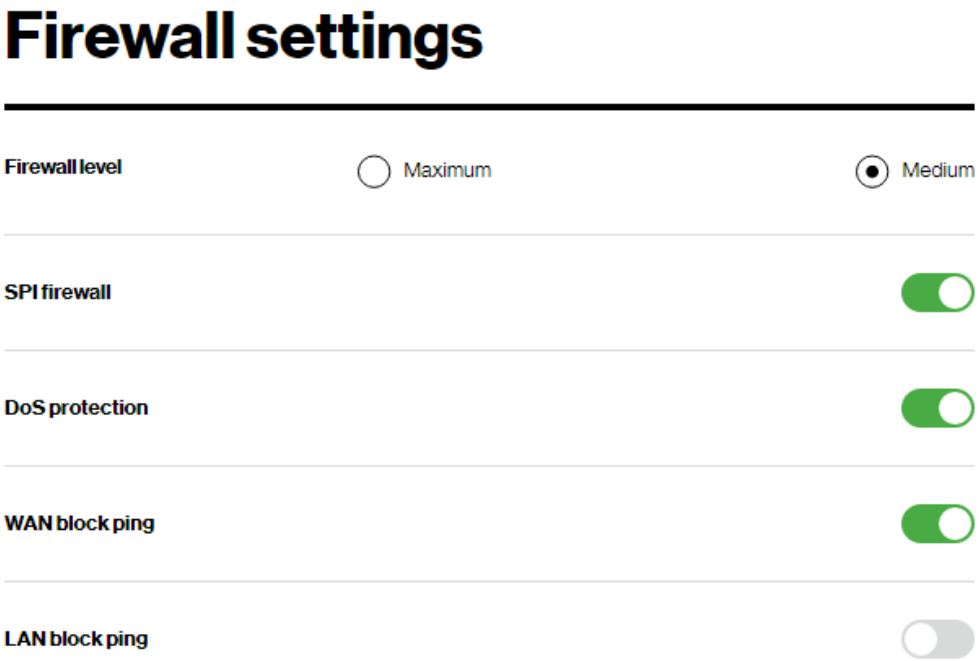
Use the **Security** menu to configure various security functions if needed, including Firewall, IP/MAC Binding and Access Control.



5.7.1 Firewall

> Security > Firewall

The router features a built-in firewall that provides protection to your network from unauthorized intrusions from the Internet. The firewall features four modules which can be enabled or disabled using the switches.



Firewall level

Firewall can be increased to Maximum level for even greater protection but can be used safely at medium level with less potential interference with normal network activities.

SPI Firewall

Stateful Packet Inspection (SPI) firewall protection means only packets matching a known active connection will be allowed by the firewall, and others will be rejected. An SPI firewall goes beyond stateless filtering and checks an entire packet's content, rather than only packet headers. This is a security feature to help distinguish between legitimate packets of information and potentially harmful packets, and provides greater

security for your network.

DoS Protection

Denial-of-Service (DoS) is a common form of malicious attack against a network. The router's firewall can protect against such attacks by filtering unreasonable packets that could flood and disable a network with large amounts of traffic.

WAN Block Ping

When active the router will not answer ping requests from the Internet. This can increase security, as pinging is a common method used by hackers to test networks.

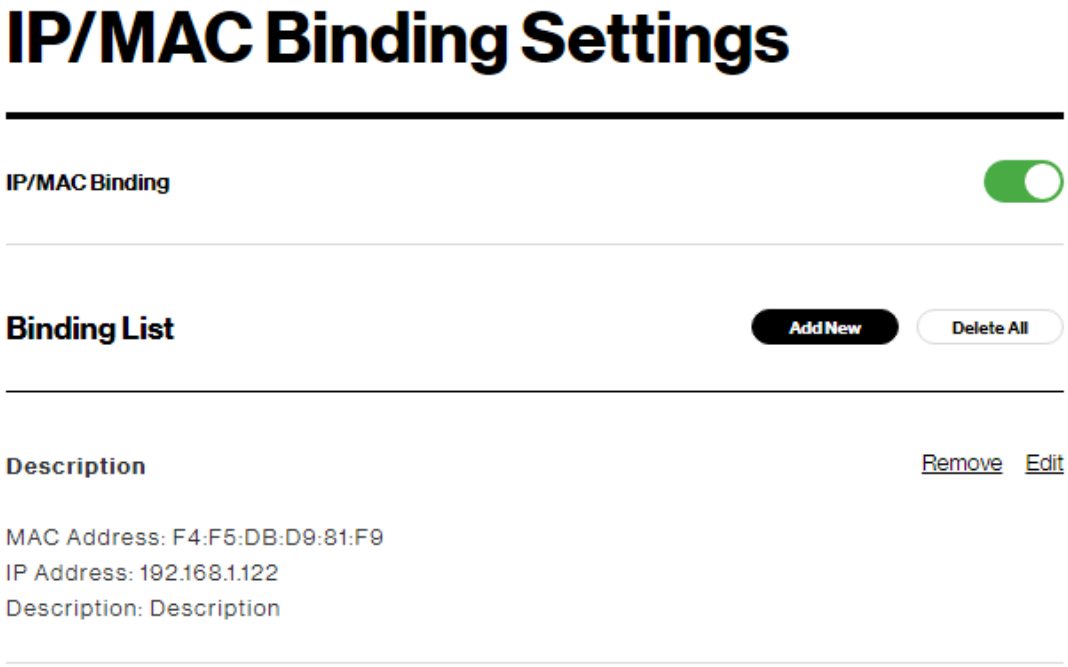
LAN Block Ping

When active, the router will not answer ping requests from the local network. This can increase security, as pinging is a common method used by hackers to test networks.

5.7.2 IP / MAC Binding

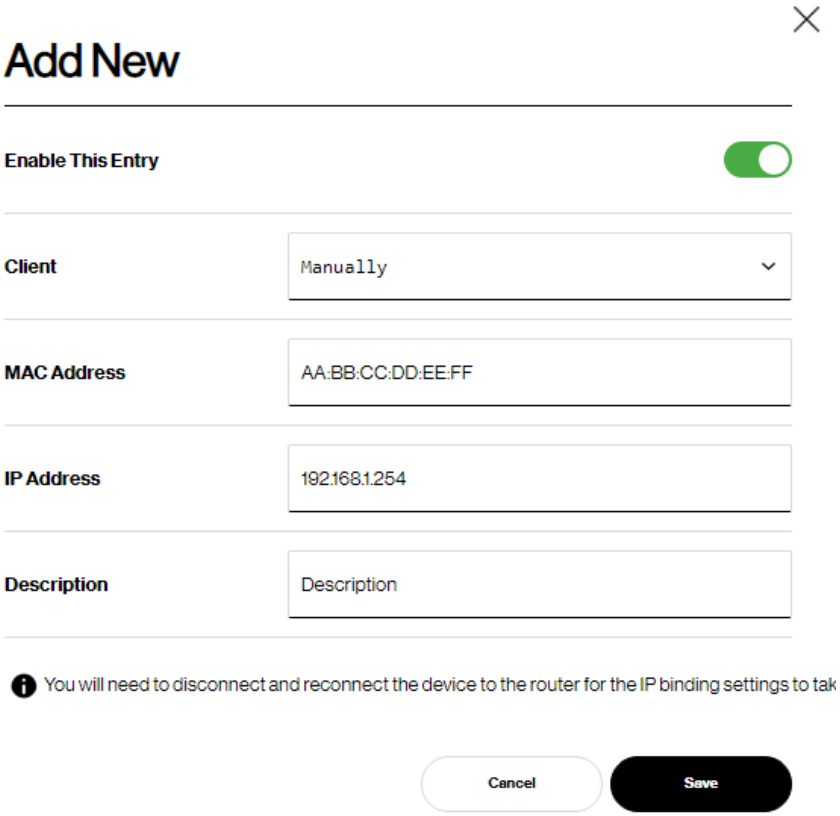
> Security > IP / MAC Binding

IP/MAC Binding allows you to reserve a static IP address for a device on the network, rather than being assigned a new (dynamic) IP address by the router's DHCP Server every time the device connects to the router. Static IP addresses can be useful for using various services on the local network. Every device is identified by a unique MAC address, and the IP address can be bound to the MAC address.



1. Switch **IP/MAC** Binding on using the toggle switch.
2. Click **Add New** to setup a new client for IP/MAC Binding.
3. Select a device from the Client menu or enter the MAC address manually.

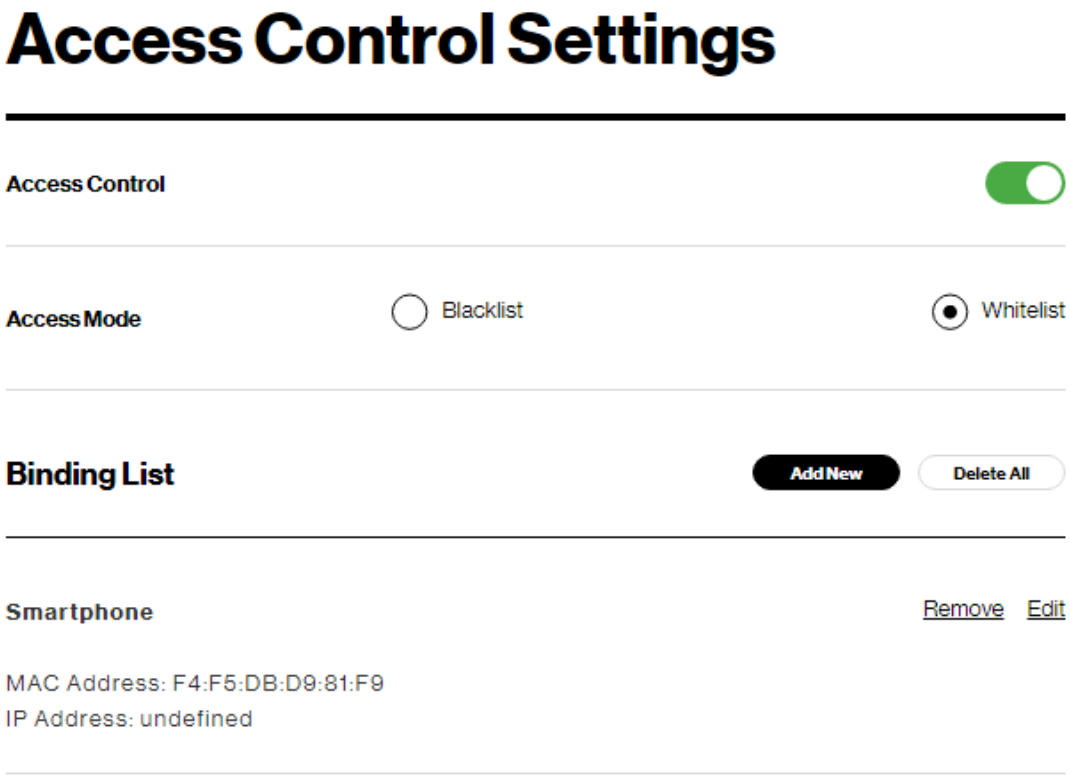
4. Specify the IP Address the client will use, and enter a Description of the device for easy reference.



5.7.3 Access Control

> Security > Access Control

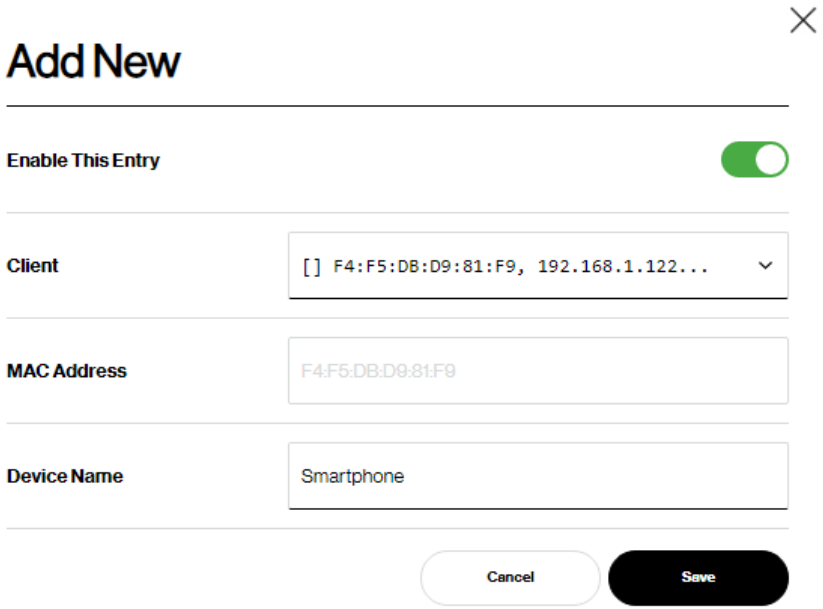
Access Control is a security feature that can help to prevent unauthorized users from connecting to your router. You can define a list of network devices permitted (whitelist) or denied (blacklist) to connect to the router. Devices are each identified by their unique MAC address or IP address.



1. Switch Access Control on using the switch.
2. Select Blacklist (not permitted) or Whitelist (permitted), and click **Add New**.

3. Select a device from the Client menu or enter the MAC address manually.

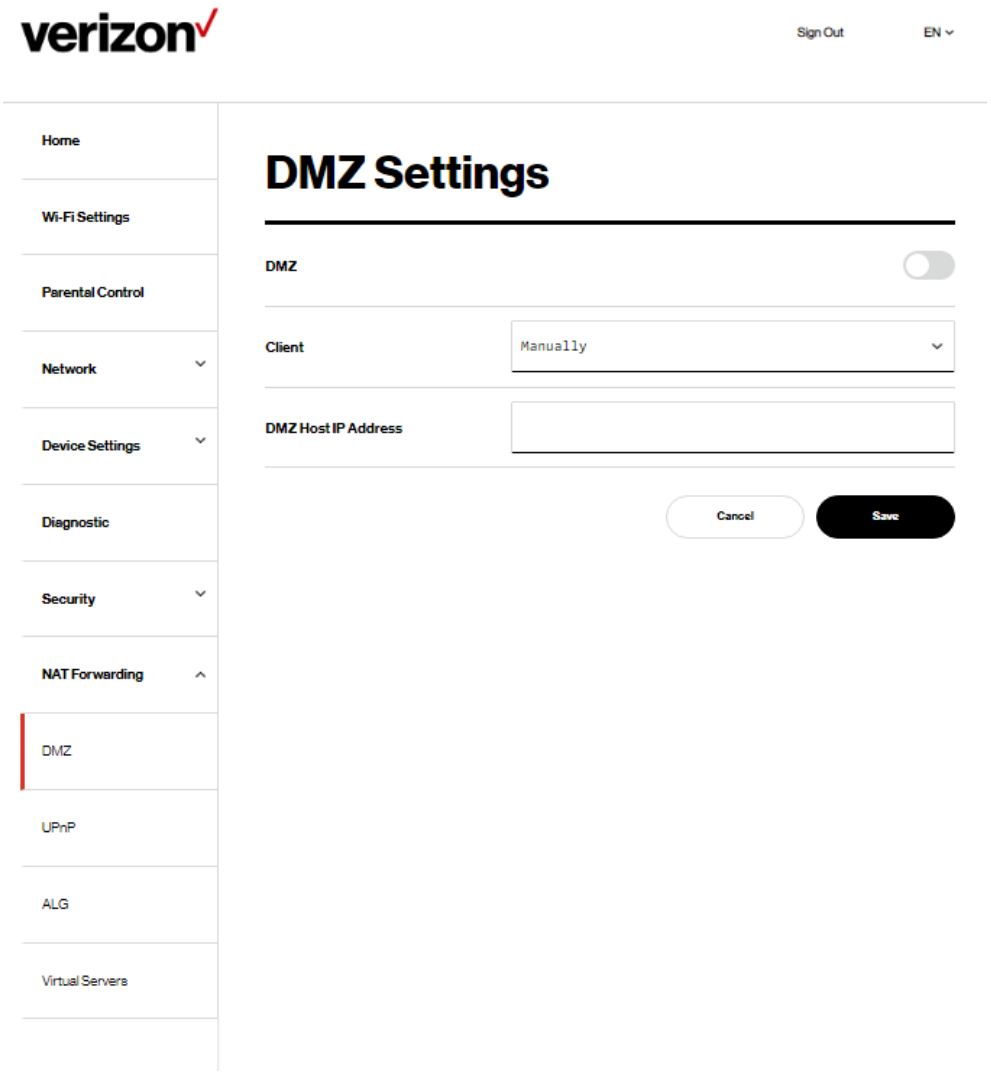
4. Enter the Name of the device for easy reference.



5.8 NAT Forwarding

> NAT Forwarding

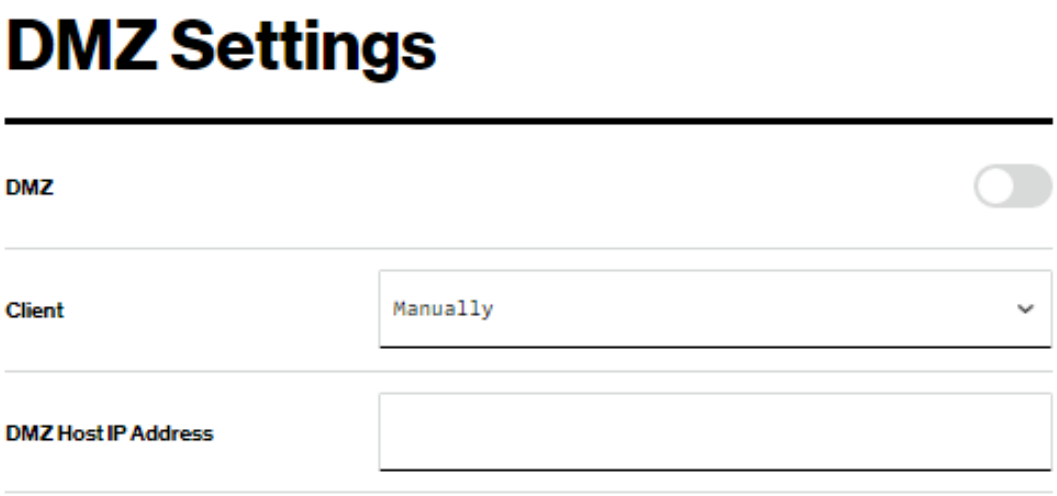
Functions in the **Network Address Translation** (**NAT**) **Forwarding** menu can improve network performance and security.



5.8.1 DMZ

> NAT Forwarding > DMZ

A **Demilitarized Zone (DMZ)** is an isolated area in your local network where a computer runs outside the firewall and receives/intercepts all incoming Internet traffic. This can provide an extra layer of security to the rest of the network, or can be useful if a network client PC cannot run an application properly from behind an NAT firewall. However, since it opens the client up to unrestricted two-way access this computer is vulnerable. DMZ should be configured only by expert network users aware of the security risks.



1. Use the switch to set DMZ to **active**.
2. Enter the IP Address of the computer to provide the DMZ service (ensure this computer is using a Static IP Address)

5.8.2 UPnP

> NAT Forwarding > UPnP

Universal plug-and-play (**UPnP**) is a set of networking protocols which enables network devices to communicate and automatically establish working configurations with each other, such as computers, printers, mobile devices etc.

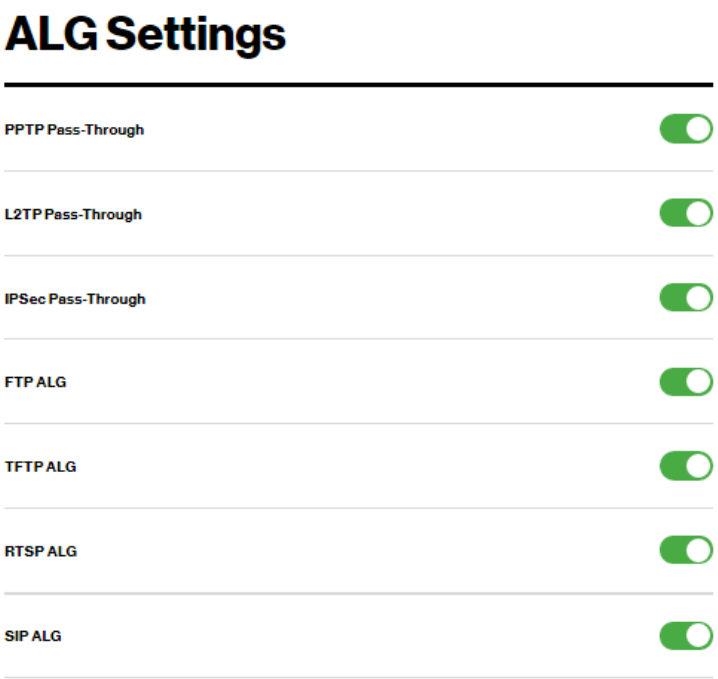
It’s typically used for data sharing, communications and entertainment purposes, although sometimes not preferred, due to security concerns. Some devices may require UPnP to be enabled to function properly. Use the switch to set UPnP to active or inactive, according to your requirements.

5.8.3 ALG

> NAT Forwarding > ALG

Application Level Gateway (ALG) settings are advanced functions that can resolve issues where services are disrupted by the firewall. Each ALG module is a security component that augments the firewall. Services such as VPNs or Virtual Servers may require ALG modules enabled. By default, all ALG modules are active. Use the switches to disable any ALG module required. ALG Settings are recommended for expert users only.

SIP ALG may disrupt Wi-Fi calling for cellphones connected to the network.



Manage ALG Settings

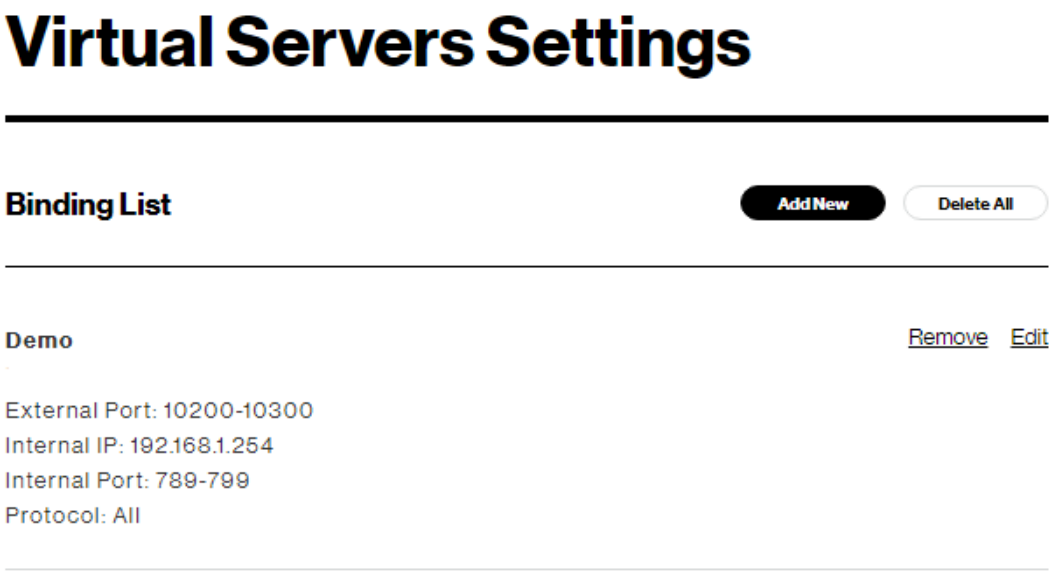
PPTP Passthrough	Point-to-Point Tunneling Protocol (PPTP) is a module for implementing virtual private networks.
L2TP Passthrough	Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs.

IPSec Passthrough	Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
FTP ALG	File Transfer Protocol is a widely and commonly used method of exchanging files over IP networks. The FTP ALG monitors PORT, PASV, and 227 commands. It performs NAT on the IP, port, or both in the message and gate opening on the device as necessary
TFTP ALG	Trivial File Transfer Protocol (TFTP) is a simple protocol used for files transfer (RFC 1350). TFTP is implemented on top of UDP, with destination port 69 as the well-known port. The TFTP Application Layer Gateway (ALG) processes TFTP packets that initiate the request.
RTSP ALG	The Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to control streaming media servers.
SIP ALG	The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging all over Internet Protocol (IP) networks.

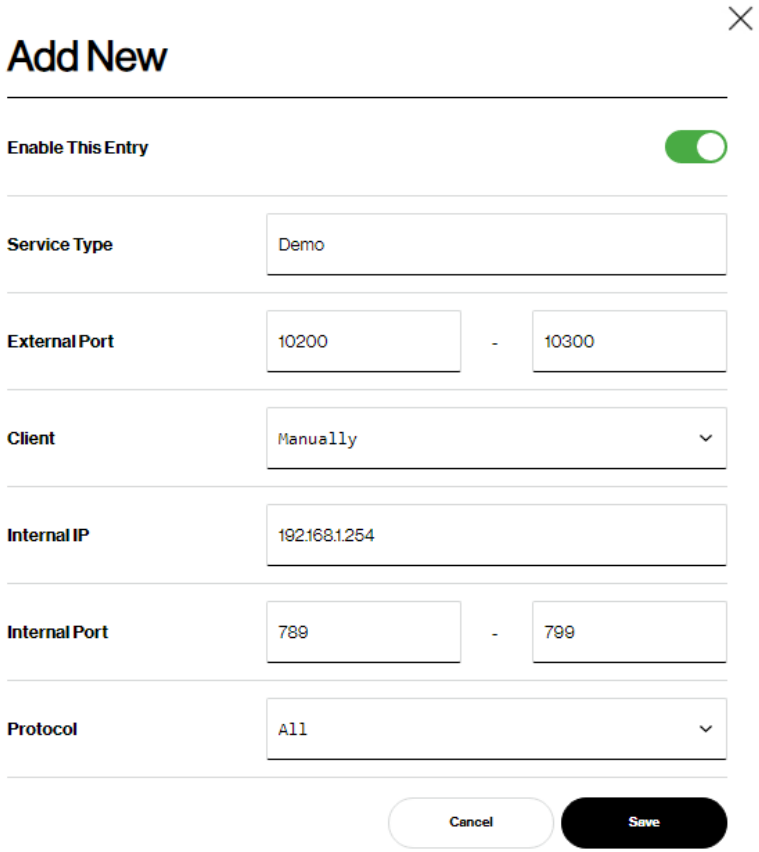
5.8.4 Virtual Servers

> NAT Forwarding > Virtual Servers

This function allows you to set up an internet service on a local computer, without exposing the local computer to the internet. Internet traffic is directed to a specific port or range of ports on a device or devices on your local network. You can also build various sets of port redirection, to provide various internet services on different local computers via a single Internet IP address. It also allows PCs outside the network to access services provided by a computer in the local network.



1. Click **Add New** and enter the parameters to setup a virtual server:

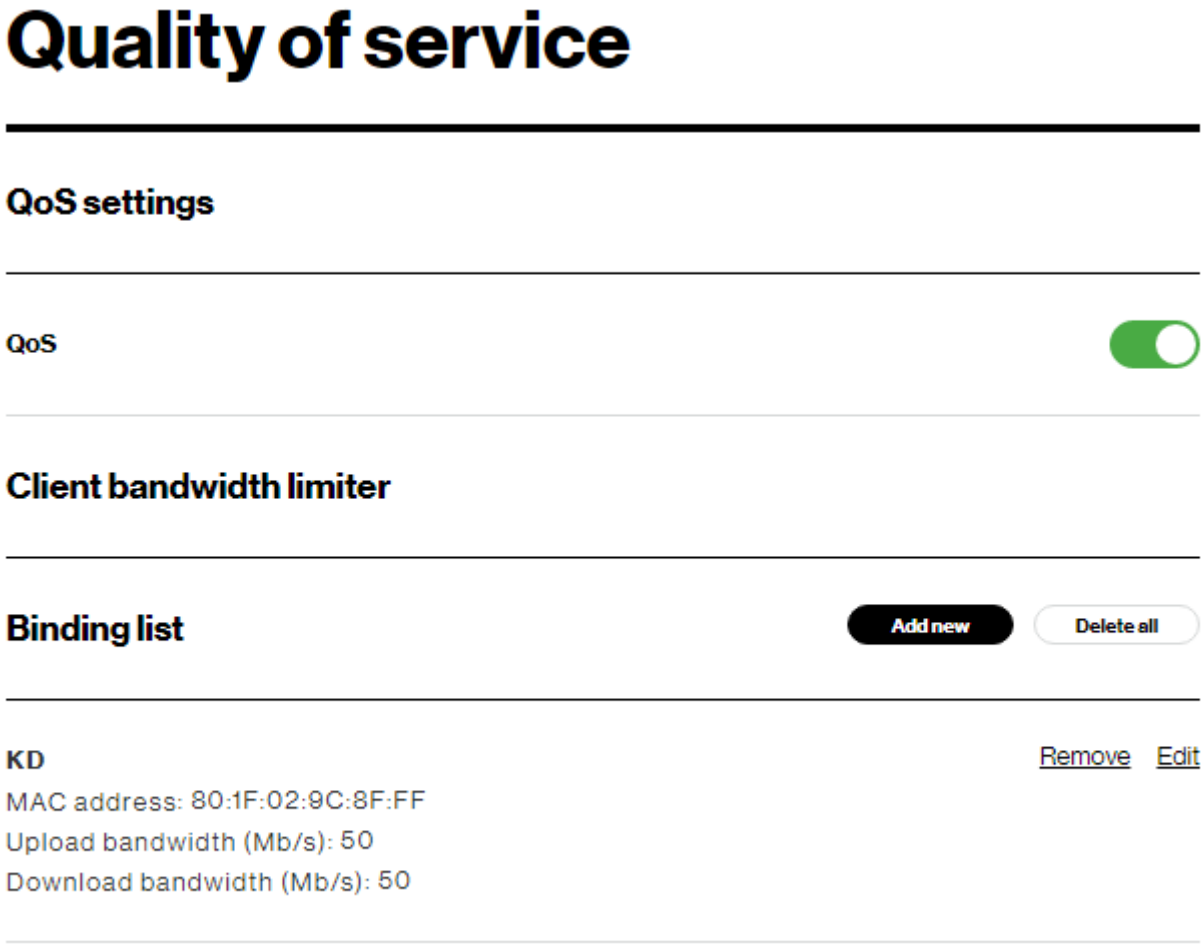


Service Type	Specify the service type e.g. HTTP, FTP etc.
External Port	Specify the external/public port to access the computer on your local network.
Client	Select whether to manually assign Internal (Private) IP & Port.
Internal IP	Enter the IP address of the computer on your local network.
Internal Port	Specify the internal/private port you wish to use on the computer in your local network.
Protocol	Select the connection protocol: TCP, UDP or All.

5.8.5 QoS

> NAT Forwarding > QoS

Quality of Service (QoS) is a feature to manage and prioritize bandwidth efficiently. Some applications require more bandwidth than others to function properly, and QoS allows you to ensure that sufficient bandwidth is available by limiting bandwidth available for specific network devices.



1. Toggle QoS on using the switch.

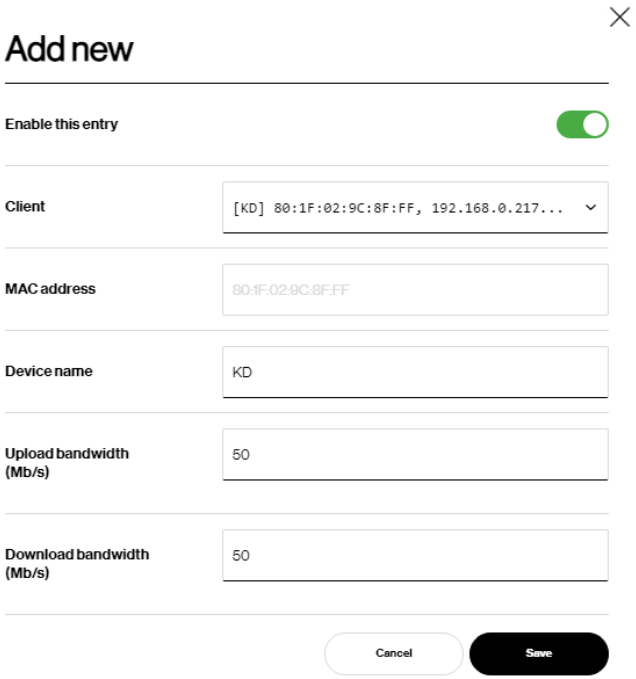
2. Click **Add new** under Client bandwidth limiter, and select a device from the Client menu or enter the MAC address manually.

3. Enter or edit the Name of the device for easy reference.

4. Enter an amount in M/bs to limit upload and download bandwidth for the specified device.

5. You can use the toggle in the top right (Enable this entry) to enable or disable the entry anytime.

6. Click Save to save the entry. Once saved, you can remove or edit any entry in the list.



6. Troubleshooting

If you are experiencing any trouble, try here first for some quick fixes to common problems.

Dropped Wi-Fi connection

Wi-Fi connections can occasionally drop for any number of reasons, such as interference or system updates. Try to ensure the space between your router and Wi-Fi devices is as clear as possible and make sure you're not moving too far away from your router. Check that your router has a good cellular connection and that your Wi-Fi device isn't trying to connect to any other saved Wi-Fi networks.

Can't connect to Wi-Fi

If your router's Wi-Fi doesn't appear when scanning available networks on your device, or if you can't make a connection, try switching both your router and Wi-Fi device off and back on again, and move closer to your router. If your router has a good cellular connection and you still can't establish a Wi-Fi connection, try a factory reset. To perform a factory reset and return the Verizon Internet Gateway to default settings, press and hold the reset button for 3+ seconds.

Can't login to the Web UI

If you can't access the Web UI, it might be an issue with your device or computer's proxy or IP address settings. Make sure that proxy settings are disabled and that your device or computer can be allocated an IP address on the network by the router's DHCP server. You'll need to check the support for your device or computer's operating system, e.g. Windows, Mac OS, for detailed instructions how to do this.

Where can I get more help?

Visit http://support.verizon.com/router find your nearest Verizon store or for 24/7 help with live chat and device-specific support.

7. Technical Specification

General

Technical Standard	LTE Category 18, 5G NR Sub 6
Frequency band	LTE Band: B2/B4/B5/B13/B48/B66, DL 4x4 MIMO 5G Band: 256 QAM, DL 4x4 MIMO n2/n5/n48/n66/n77
Wi-Fi Standard	802.11 a/b/g/n/ac/ax
Dimensions (L x W x H)	130mm x 130mm x 136mm
Operating temperature range	+5°C to +40°C
Storage temperature range	-45 – 70 °C

Connections

DC Input	1st source adapter: 12V/ 3A 2nd source adapter: 12V/2A
Ethernet	RJ-45 LAN * 2

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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 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 party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

RF Exposure Information (MPE)

This device has been tested and meets applicable limits for Radio Frequency (RF) exposure.
This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.