verizon

User Guide

Verizon Internet Gateway

Revision History

Date (yyyy/mm/dd)	Ver.	Revised Sections	Descriptions
2022/05/11	0.1	Preliminary draft	Preliminary release
2022/05/16	0.2	Chapter 1 and 2	Enhanced graphics and updated contents
2022/05/20	0.3	Cover page	Modified product name and added model number
2022/06/07	0.4	Chapter 5	Added Chapter 5 to provide Web GUI walkthrough

Table of Contents

1. Inside the box

Thank you for choosing Verizon Internet Gateway (Model Num. FSNO21VA). Once you open the product package, you should find the following items inside:

Verizon Internet Gateway

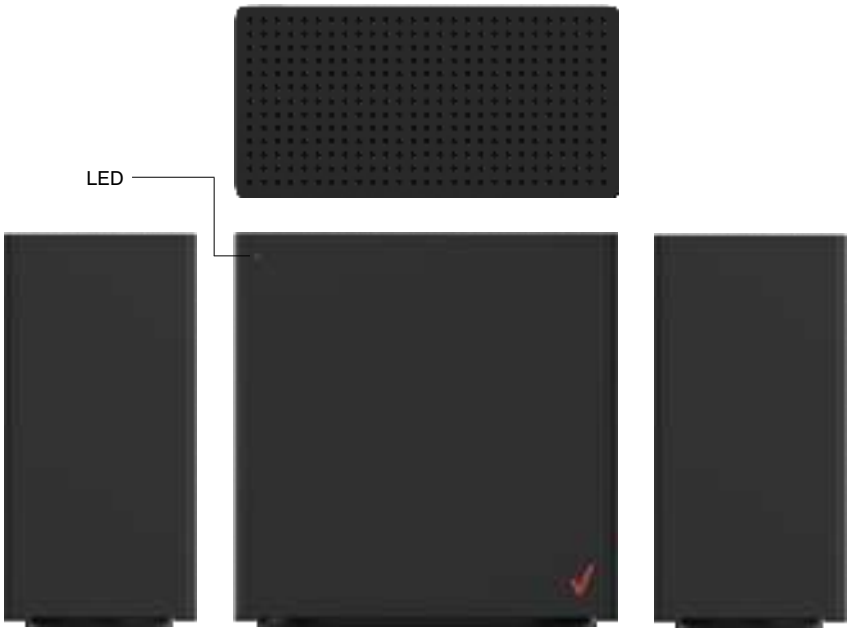
Power Adapter

Ethernet Cable

2. Introducing Your Verizon Internet Gateway

Your Verizon Internet Gateway supports multi-connectivity of 5G, 4G LTE, and Wi-Fi 6 to provide users with fast wireless networks, and offers connectivity up to 128 devices (64 devices for 2.4 GHz and 5.0 GHz each) within the range. This feature-rich router is also designed with various functions including band-steering, security, routing, and service improvements.

Take a quick tour of your device.




WAN
DC IN
WPS Button
LAN 1 - 4 Ports
Product Label
Reset Pin Hole
SIM Card Slot Door
(Flip Type)
Internet Gateway
Barcode Label
Screw for Bracket

2.1 Parts and Functions

Parts	Description
LED	Indicate the status of power and connectivity, as well as WPS connectivity.
LAN 1 - 4 ports	Four RJ-45 GbE LAN ports for connections with external devices through Ethernet cable(s).
WAN	The WAN port supports WAN connectivity using another CPE (customer premise equipment) or external modem.
DC IN	DC Power In - The DC power jack that connects the 5G Internet Router to a power outlet.
WPS button	Push this button to enable WPS (Wi-Fi Protected Setup). Use WPS to add supported Wi-Fi devices to your network. Remember to enable WPS on the Wi-Fi devices you wish to add.
SIM card slot door	Flip the door cover to locate the SIM card slot and insert/remove Nano SIM card.
Reset pin hole	Press the reset pin hole with pin to force a cold reset of your router. Your router will return to factory default setting. Only use the Reset when you experience issues with the router or have to revert all the settings you have configured for the router.
Label	The label provides default URL and password for you to connect to wireless network at the first time you set up this device. The label also provides information about the product's ID and regulatory standards.

2.2 LED Status and Indications

LED Mode	Status	LED Pattern
Bootup	System Off	Off
	System Booting	Soft Blink White
	Firmware Update (FOTA)	Fast Blink White
Cellular signal (or after single-clicking the 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
	Wi-Fi Disabled by User	Solid Green
Paring	WPS Pairing	Hard Blink Blue
Other	Factory Reset	Fast Blink Yellow
	FW Error	Soft Blink Red

2.3 Ethernet Port LED Mode

Ethernet Port LED Mode	Status	Left LED	Right LED
Wired LAN connection	Ethernet > 100M* Link	Off	Solid White
	Ethernet > 100M* Activity	Off	Blinking White
	Ethernet < 100M* Link	Solid Yellow	Off
	Ethernet < 100M* Activity	Blinking Yellow	Off
	No Ethernet Connection	Off	Off

Note about *: Threshold level can be determined based on port capability.

3. Setting Up Your Verizon Internet Gateway

Your Verizon Internet Gateway comes with a pre-installed SIM card and the following sections will help you connect and configure your device to the network.

Note: Before you start setting up your router, remove the protective film on the housing first to prevent overheating.

3.1 Positioning Your Router

Before setting up the router, it is recommened to take the following into considerations for optimal signal strength:

- Near a window where the signal is mostly uninterrupted
- On a flat surface
- In an open space with as few blocking objects or obstructions as possible
- Elevated surface
- Keep the router away from 802.11g or 20MHz only Wi-Fi devices, 2.4GHz computer peripherals, Bluetooth devices, cordless phones, heavy-duty motors, fluorescent lights, and some industrial equipments that may generate signal interferences with your router.
- Avoid positioning it
  - next to a wall that may obstruct the signal
  - near heavy-duty appliances
  - close to metal fixtures, enclosures, cabinets, or thick concrete.
  - in a basement

Note: Try not to reposition the router if the signal is good. If the position of the installation changes, the signal strength may be affected.

3.2 Setup Requirements

To configure wireless network with a PC, your computer shall meet the following 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
- TCP/IP protocol support
- Web browser such as Microsoft Edge , Firefox, Safari, or Google Chrome

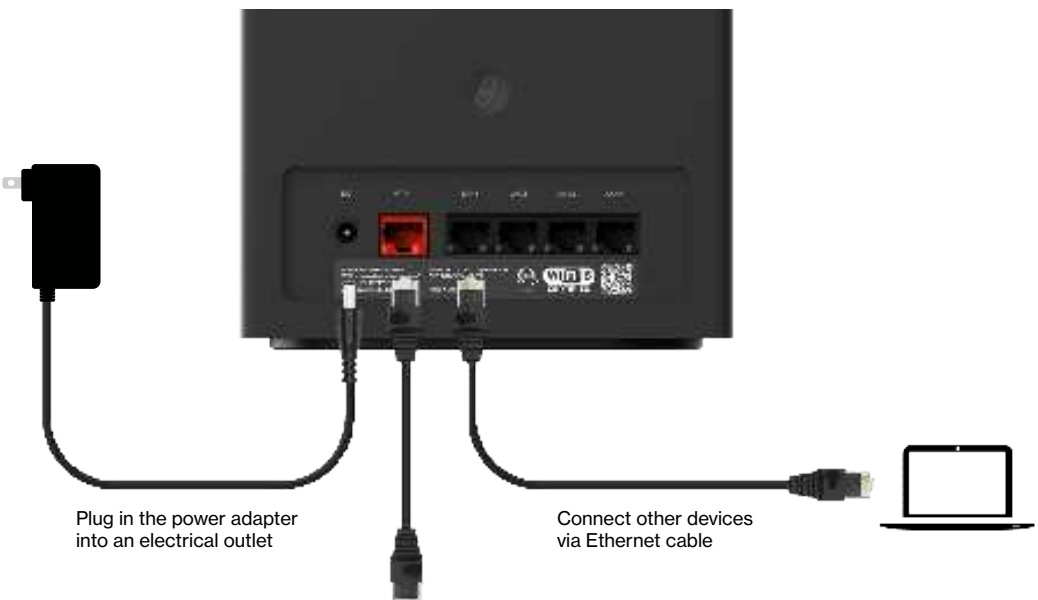
3.3 Setting Up

1. Connect the included Power Adapter to the DC IN power port of the router.
2. Plug the Power Adapter to an electrical outlet.
3. Wait for a short moment for the router to power up and connect to 4G LTE/5G network.
4. The LED shall display ON (White) after powering up.
5. Your Internet device shall be able to connect to the Wi-Fi network of your router named **Verizon_<your network>**.

   For information about the default name and password of the router's Wi-Fi network, check the product label on the back side of your router.

Connecting via Ethernet

- The router can connect to other devices via Ethernet connections. Use the supplied Ethernet cable and plug one end into one of the LAN ports of the router (as shown below), and plug another end of the cable into an available LAN port of the other device.
- The router can also connect to a CPE or an external modem via WAN port by using the supplied Ethernet cable.



4. Log in Your Verizon Internet Gateway

Once you have connected your device to your router, you can log in to your router's Web User Interface (Web UI) to access network information such as connected devices and data usage, and to confgure the setting and functions, such as Wi-Fi security. You may log to the Web UI through a computer or a mobile device.

The following sections will describe how to access the Web UI and perform your configurations.

4.1 Connect and Log in via Wi-Fi

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 (the image below is a sample screenshot from a mobile phone).

3. Select the Wi-Fi network named **Verizon_<your network>** (check your router's product label on the back 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 back side of the unit.
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 back side of the router, labeled **Admin URL and Admin password**).

4.2 Connect and Log in via Ethernet

1. You can use an Ethernet cable to connect your computer to the router 's LAN port for configuration (instead of Wi-Fi). Simply connect to one of the four LAN ports by using the supplied Ethernet cable.
2. Open a web browser and enter the router 's default address **http://192.168.0.1** in the address bar.
3. Log in default password (the default address and password are displayed on the product label on the back side of the router, labeled **Admin URL and Admin password**).

5. Configuring with Your Router with Web GUI

You can configure functions of your router on the Web GUI. To access the Web GUI, open a web browser and enter the gateway's admin address **http://192.168.0.1** in the address bar. Then, enter the default admin password (check the product label of your gateway for your default admin password).

5.1 Home

> **Home**

The **Home** page features the Menu at the left side to navigate the functions, and shows the general system information of your router, including the number of connected devices, network status, and Wi-Fi status.

Menu	Use the Menu at the left side to navigate functions of your router, such as Wi-Fi Settings, Internet Control, Device Settings, Network, Diagnostic, Security, and NAT Forwarding.
Logout	Click it to log out. You will be asked if you want to continue to log out.
No. of connected device	Shows the number of connected devices via Wi-Fi (Primary) and Ethernet.
Network info	Displays general network information, including Cellular Network, Status, IP Address, MAC Address, and Software version
Wi-Fi status	Shows the general status of the Wi-Fi connections of your router.

Note: the images in this chapter serve as reference only and are subject to change due to future updates without prior notices.

5.2 Wi-Fi Settings

> **Wi-Fi settings**

From the Wi-Fi Settings screen, you can set your bandsteering preferences, Wi-Fi name (SSID) and password, security level, and encryption types. Your router supports dual-band Wi-Fi frequencies (2.4GHz and 5GHz) for enhanced wireless network performance.

5.2.1 Basic

> **Wi-Fi settings** > **Basic**

From the Basic page, you can configure your basic Wi-Fi settings.

Band Steering enables your router to dynamically assign wireless devices (smartphones, laptops, or tablets) to their capable frequency (2.4GHz or 5GHz). For example, if your device supports 5GHz band, it will be steered to that frequency while legacy connected devices are assigned to 2.4GHz. When Band Steering is enabled, your dual-band router will have one Wi-Fi name (SSID).

To save changes, click **Save**.

Bandsteering settings

Band steering	Use the toggle switch to enable or disable it. When Band Steering is enabled, your dual-band router will show one Wi-Fi name (SSID), and your wireless devices will be assigned to their capable frequencies (2.4GHz or 5GHz) automatically. When enabled, all the settings in this tab can be configured. **Note:** Information under Basic Tab is automatically filled on 2.4 GHz and 5 GHz Tabs. It should not be updatable in 2.4 GHz and 5 GHz Tab
Wi-Fi Name (SSID)	This is the name of your Wi-Fi network for identification, which is also known as “SSID”.
Wi-Fi Password	Enter the password for your Wi-Fi network. A complex, strong password is highly recommended.
Security	Select a Wi-Fi security type from the drop down menu, which includes None, Mix WPA/WPA2, WPA2, and WPA3.
Version	Shows which version of security type is in use. The version corresponds to the selected Wi-Fi security type.
Encryption	Displays encryption type according to the selected version. AES encryption is the default encryption type for WPA standards.

5.2.2 2.4GHz/5.0GHz

> **Wi-Fi settings** > **2.4GHz / 5GHz**

If you disable Band Steering, you will have to configure 2.4GHz or 5GHz separately in their respective tab(s).

2.4GHz / 5GHz Wi-Fi settings

WI-FI 2.4G/5G	Use the toggle switch to enable or disable this Wi-Fi frequency.
Wi-Fi Name (SSID)	This is the name of this Wi-Fi network for identification
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 more secure.
Wi-Fi Password	Enter the password for this Wi-Fi network. A complex, strong password is highly recommended.
Security	Select a Wi-Fi security type from the drop down menu, which includes None, Mix WPA/WPA2, WPA2, and WPA3.
Version	Shows which version of security type is in use. The version corresponds to the selected Wi-Fi security type.
Encryption	Displays encryption type according to the selected version. AES encryption is the default encryption type for WPA standards.

2.4GHz / 5GHz Channel settings

Mode	Select the wireless standard for the router's Wi-Fi network. The supported standards for 2.4 GHz include 802.11b only, 802.11b/g mixed, 802.11g/n mixed, and 802.11ax. The supported standards for 5 GHz include 802.11a only, 802.11a/n mixed, 802.11ac only, 802.11a/ac/n mixed, and 802.11ax.
Channel	Select a wireless radio channel from the drop-down menu. The default is **Auto**. Changing the radio channel may positively or negatively influence the signal depending on how crowded the channel is with other radio signals and interference.
Channel Bandwidth	Set the channel bandwidth: • 20 MHz (lower performance but less interference) • 20/40 MHz (40 MHz offers higher throughputs and better performance, but higher interferences • 20/40/80 MHz (for 5 GHz) • 20/40/80/160 MHz (for 5 GHz)

To save changes, click **Save**.

5.2.3 Secondary

> **Wi-Fi settings** > **Secondary**

If you enable this setting, you can add a 2.4 GHz / 5 GHz Secondary Network for better channel utilization and preventing guest(s) from accessing your primary Wi-Fi network. Once enabled with the toggle switch, you can set the SSID, password, and security type for the secondary network.

To save changes, click **Save**.

5.2.4 WPS

> **Wi-Fi settings** > **WPS**

Wi-Fi Protected Setup (WPS) is a simple way to add Wi-Fi devices to your network. To use this function, your Wi-Fi client device(s) must be WPS compatible.

If your client device has a WPS button, push it and click the **Pair** button below to start WPS pairing.

Warning: Wi-Fi devices may briefly lose connectivity when turning WPS On/Off.

5.3 Internet Control

> **Internet Control**

The **Internet Control** feature allows you to restrict selected devices to access Internet on your network at specified times.

To start using this feature, click **Add New** to set the connected device with Internet access controls.

Internet Control settings

Enable this entry	Use the toggle switch to enable this entry of the connected device to be restricted or controlled.
Schedule Internet Control	Use the toggle switch to enable Schedule Internet Control.
Client (Device Nickname and Mac Address)	Use the drop-down arrow to select a device from a list of connected devices (via Wi-Fi/Ethernet). Once you select a device, the Device Nickname and Mac Address of the selected device will be auto-filled. You may choose Manually to fill out the Device Nickname and Mac Address manually.
Sun - Sat	Select the day(s) from Sunday to Saturday
Start time	Set the start time for the scheduled Internet Control
End time	Set the end time for the scheduled Internet Control

To save settings, click **Save**.

5.4 Network

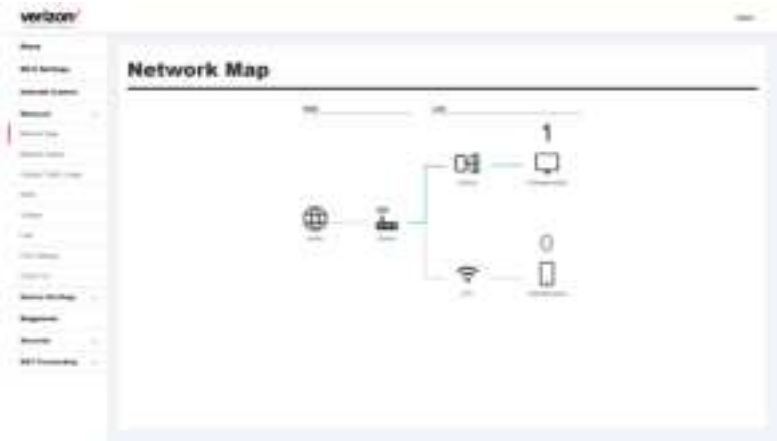
> **Network**

The **Network** menu shows available options to set the networking functions of your router.

5.4.1 Network Map

> **Network** > **Network Map**

When you click **Network Map**, you will see a visual overview and status information of the network and devices on your wireless network. You may click on **Connected devices** to view information of your connected client devices, for example, Mac Address, IP address, and IPv6 address for devices connnected through Ethernet, as well as devices under Primary/ Secondary network of your Wi-Fi. Green lines indicate the connection has been established.



5.4.2 Network Status

> **Network** > **Network Status**

Network Status displays the status of the network in Internet, Cellular, LAN, Wi-Fi, and System Information.

> **Network** > **Network Status** > **Internet**

Internet v4
Displays IPv4 parameter information about your router's Internet connection. IPv4 is the default Internet protocol on the Internet.

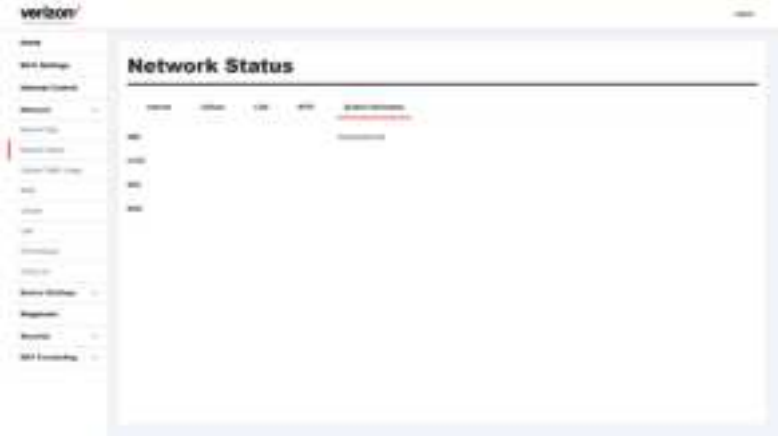
Internet v6
Displays IPv6 parameter information about your router's Internet connection. IPv6 is the next-generation Internet protocol which will replace IPv4 to deal with the anticipated address exhaustion. To set up IPv6, go to **Network > IPv6 Settings**.

> **Network** > **Network Status** > **Cellular**
Displays cellular network information including Operator name, SIM status, Roaming status and TECH status.

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

> **Network** > **Network Status** > **Wi-Fi 2.4GHz & 5GHz**
Displays your router 's Wi-Fi information for both 2.4GHz & 5GHz frequencies, including network name (SSID), radio, mode, channel bandwidth and other parameter information. To edit these Wi-Fi settings, go to **Wi-Fi Settings**.

> **Network** > **Network Status** > **System Information**
Displays system identifiers unique to your hardware.



5.4.3 Cellular Traffic Usage

> **Network** > **Cellular Traffic Usage**

Cellular Traffic Usage displays your network data usage, with upload and download data displayed in MB/KB for monthly and current periods.

Ensure that your router 's date and time settings are correct for accurate Monthly usage information. To check date and time settings, go to **Device Settings** > **Date / Time**.

5.4.4 WAN Settings

> **Network** > **WAN**

WAN Settings allows you to assign Dynamic IP or Static IP for the connected WAN device. You may use the toggle switch to enable or disable IP Passthrough function. If IP Passthrough is enabled, Wi-Fi, IPv6, firewall and ALG will be off (the Wi-Fi, the IPv6, the firewall and the ALG setting pages will show IP Passthrough is on. To enable these functions again, IP Passthrough must be disabled).

Once the Dynamic IP is set, the page will display Dynamic IP information.

In advanced setting, you may choose to get DNS address dynamically from ISP (Internet Service Providers or manually input the Primary/Secondary DNS addresses if you choose Use the following Address.

To save settings, click **Save**.

5.4.5 Cellular Settings

> **Network** > **Cellular**

Cellular Settings displays your cellular status including Internet status, SIM status, cellular type (4G/5G) and other parameters.

You may click Refresh to refresh the displayed status, or click Connect/Disconnect if necessary.

In APN Settings, you may input or set your APN information.

To save settings, click **Save**.

5.4.6 LAN Settings

> **Network** > **LAN**

LAN Settings page allows you to configure your router on your Local Area Network (LAN). You may assign an IP address and corresponding subnet mask for your router, and configure your router as a DHCP server to assign IP addresses and/or DNS to other devices on your LAN.

Basic

- **IP Address**: enter an IP address for your router.
- **Subnet mask**: use the drop-down menu to select an available subnet mask.

Advanced

- **DHCP**: use the toggle switch to enable/disable your router as a DHCP server.
- **IP Address Pool:** provides a sequential range of IP addresses within a certain network for you to assign to devices on your LAN network.
- **Address Lease Time (hours)**: enter the address lease time
- **Primary/Secondary DNS (optional)**: enter the primary/secondary DNS. This is optional.

To save settings, click **Save**.

5.4.7 IPv6 Settings

> **Network** > **IPv6 Settings**

IPv6 Settings allows you to enable/disable IPv6 protocol and set the related features.

- **IPv6**: use the toggle switch to enable/disable IPv6 protocol.
- **WAN**: use the drop-down menu to select your preferred WAN connection (for instance, Ethernet or wireless mobile network)
- **Profile name**: use the drop-down menu to select your profile name.

WAN DHCP Settings
- **DNS Address**: use the drop-down menu to choose Get dynamically from ISP or Use the following Address. If you choose Get dynamically from ISP, the Primary/Secondary DNS will be auto-filled. If you choose Use the following Address, you will have to manually input the addresses.
- **Primary/Secondary DNS**: these items will be auto-filled if you choose Get dynamically from ISP in the last parameter. If you choose Use the following Address, you will have to fill out these two items manually.

LAN Settings:
- **IPv6 Address**: displays IPv6 address.
- **IPv6 Prefix Length**: displays IPv6 prefix length.
- **IPv6 Address type: us**e the drop-down menu to select from SLAAC + RDNSS, SLAAC + DHCPv6, or DHCPv6.
- **Life time (Minutes)**: input the life time.

To save settings, click **Save**.

5.4.8 Client List

> **Network** > **Client List**

Client List displays general device information under your LAN and Wi-Fi networks.

5.5 Device Settings

> **Device Settings**

From **Device Settings** menu, you can configure various administrative functions of your router, including the Web UI login password, router date & time settings, backup, and router firmware updates.

5.5.1 Change Admin Password

> **Device Settings** > **Admin Password**

From **Admin Password** page, you can change the login password for the router's Web UI. It is essential to change the password regularly for the security of your router. Use complex, strong password with a mixed combination of numbers, letters and symbols.

To change admin password for your router,

1. Enter the current password.
2. Enter your new password in the New Password field and again in Confirm New Password to confirm.
3. To save new password, click **Save**.

5.5.2 Date / Time

> **Device Settings** > **Date / Time**

The Date and Time for your router is configured automatically over the cellular network by default and is displayed in Gateway Current Time.

You may select SNTP mode to enter NTP server and time zone manually.

To save settings, click **Save**.

5.5.3 Backup and Restore

> **Device Settings** > **Backup & Restore**

From the **Backup & Restore** page, you can save and backup your router's current settings as a file in your local device storage (e.g. a computer storage). You can then restore your router to the previously saved settings by loading this file. If necessary, you may also reset your router back to factory default settings.

If the router is not responding or experiences some issues, it is recommended that you first reboot the device. If the issue(s) remains, you may reset the device back to factory default settings. To perform a cold reset to factory default settings, use a pin to insert the Reset Hole on the front of the device for few seconds.

Backup	Save a copy of your current settings. To save current settings as a backup file, click or tap **Backup**.
Restore	Restore saved settings from a file. To restore saved settings, click or tap **Select File** to locate a file on your device storage (e.g. a computer storage).
Factory Default Restore	Reset the router to its factory default values. To perform a factory reset, click or tap **Factory Restore**.

5.5.4 Firmware Update

> **Device Settings** > **Firmware Update**

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

5.6 Diagnostic Setting

> **Diagnostic**

From **Diagnostic** menu, you can run **Ping / Tracerroute** diagnostic tests with the router. Enter the IP address to use for the test and click **Start**. The results will be displayed in the **Result** box.

Ping / Traceroute	Use the drop-down menu to select Ping or Traceroute as the diagnostic tool.
Type	Use the drop-down menu to select IPv4 or IPv6 as the protocol type.
IP Address / Domain Name	Enter the IP address or domain name to run the diagnostic.

5.7 Security

> **Security**

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

5.7.1 Firewall Settings

> **Security** > **Firewall**

The router features a built-in firewall with four modules to give your network comprehensive protections from unauthorized intrusions from malicious attacks on the Internet. Use the toggle switches to enable or disable the four firewall modules.

SPI Firewall	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 abnormal 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.

To save settings, click **Save**.

5.7.2 IP/MAC Binding Settings

> **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 used to host 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.

To set IP/ MAC binding,

1. Use the toggle switch to enable IP/MAC Binding.
2. Click or tap **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.

To save settings, click **Save**.

5.7.3 Access Control Settings

> **Security** > **Access Control**

Access Control is a security feature that can help prevent unauthorized users from connecting to your router. You can set the access mode of network devices as permitted (Whitelist) or denied (Blacklist) to connect to the router. Each device is identified by its unique MAC address or IP address.

To set Access Control,

1. Use the toggle switch to enable Access Control
2. Select Blacklist (not permitted) or Whitelist (permitted), and click **Add New**.
3. Use the toggle switch to turn on Enable This Entry
4. Select a device from the Client menu or enter the MAC address manually.
5. Enter the Name of the device for easy reference.

To save settings, click **Save**.

5.8 NAT Forwarding

> **NAT Forwarding**

The **Network Address Translation (NAT) Forwarding** menu provides functional configurations to improve network performance and security of your network.

5.8.1 DMZ Settings

> **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.

To set DMZ,

1. Use the toggle switch to set DMZ to active.
2. Enter the IP Address of the computer to provide the DMZ service. Make sure this computer is using a Static IP Address.
3. To save settings, click **Save**.

5.8.2 UPnP Settings

> **NAT Forwarding** > **UPnP**

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

Some devices may require UPnP to be enabled to function properly. Use the toggle switch to enable or disable UPnP, according to requirements by your device(s).

If there are security concerns, use the toggle switch to disable UPnP.

To save settings, click **Save**.

5.8.3 ALG Settings

> **NAT Forwarding** > **ALG**

Application Level Gateway (ALG) settings are NAT functions to solve issues for services that are disrupted by the firewall. Each ALG module is a security component that reinforces the firewall. Services such as VPNs or Virtual Servers may require certain ALG modules enabled.

By default all ALG modules are active. Use the toggle switches to disable any ALG module if necessary. 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) Passthrough allows PPTP to pass through NAT router, which enables VPN clients connected to the router to make PPTP connections.
L2TP Passthrough	Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol for point-to-point sessions via the Internet on layer 2. It is another passthrough protocol to transmit packets in VPNs.
IPSec Passthrough	Internet Protocol Security (IPsec) is a protocol suite for data packet encryptions and secure network connections. IPSec Passthrough allows IPSec tunnels to pass through the router.
FTP ALG	File Transfer Protocol is a widely and commonly used method of exchanging files over IP networks. The FTP ALG scans PORT and PASV commands, as well as 227 responses. It performs NAT on the IP and port, or both in the data transfer between client and server.
TFTP ALG	Trivial File Transfer Protocol (TFTP) is a simple protocol used for processing TFTP packets and sends requests to UDP destination port 69. Certain firewall and NAT services require TFTP ALG configurations.
RTSP ALG	The Real Time Streaming Protocol (RTSP) is a network control protocol that controls the delivery of real-time media data. This ALG is mostly used in servers that control streaming media.
SIP ALG	The Session Initiation Protocol (SIP) is a communications protocol for managing VoIP. The SIP ALG monitors VoIP traffic and modifies the data packets when needed. However, some interruptions may happen to VoIP due to firewall.

5.8.4 Virtual Servers Settings

> **NAT Forwarding** > **Virtual Servers**

Virtual Servers allows you to set up a server in the local network to host online services, such as FTP, VoIP, printer, HTTP, or web servers. Meanwhile, the virtual server can keep the local network invisible to the public Internet. Internet traffic is directed to a specifically assigned port(s) of a router (or routers) on your local network. Different services can be redirected to certain ports. For instance, Port 80 is set for FTP service. You may establish various sets of port redirections to provide multiple Internet services on different local computers through a single Internet IP address.

To set up virtual servers,
1. Click **Add New** in the Binding List.
2. Use the toggle switch to turn on Enable This Entry.
3. Enter the parameters to set up a virtual server.

Parameters

Service Type	Specify the service type, for example, HTTP, FTP, etc.
External Port	Specify the external/public port to access the computer on your local network.
Client	Select a device from the menu or manually assign Internal (Private) IP & Port.
Internal IP	Enter the IP address of the computer on your local network. If you select a device from the drop-down menu, Internal IP will be auto-filled.
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.


verizon
Virtual Servers Settings


verizon
Virtual Servers Settings

6. Technical Specifications

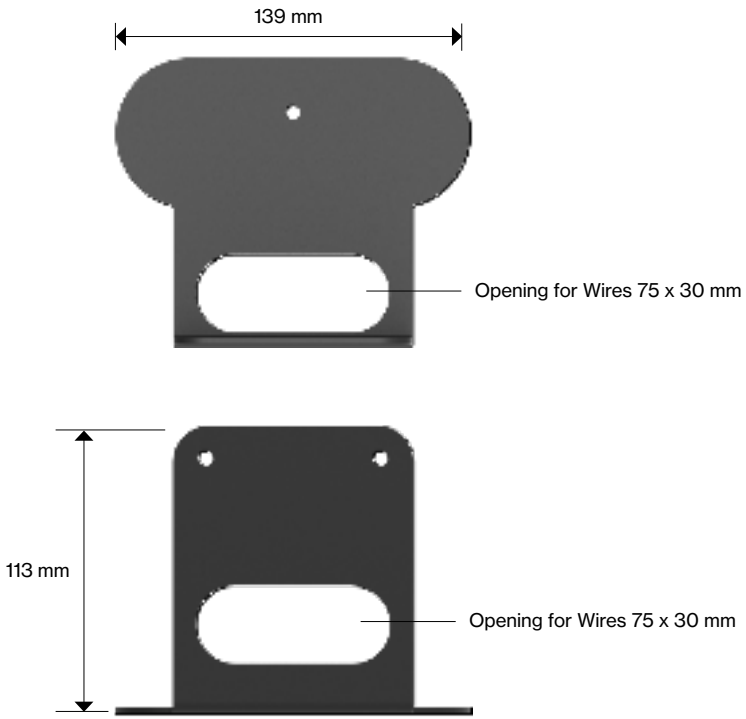
Frequency bands	5G NR: n2, n5, n48, n66, n77 4G LTE: B2, B5, B13, B48, B66
Memory	RAM: 1GB ROM: 8GB
Wi-Fi	Wi-Fi 6 (802.11 a/b/g/n/ac/ax) Support simultaneous 2.4Hz (2x2 MIMO) and 5GHz (4x4 MIMO), 4x SSID w/ band-steering (Single SSID on both 2.4/5GHz) WiFi coverage supports 64 simultaneous clients Downlink CA of LTE B5 with 4X4 MIMO and LTE B13 with 4X4 MIMO
LED	Front-facing dimmable tri-color LED x 1
WPS	WPS button x 1
Max. connected devices	Up to 128 devices (64 devices for 2.4 GHz and 5 GHz each)
LAN	RJ-45 Gigabit LAN ports x 4
WAN	WAN port x 1
Reset	Reset pin hole x 1
Power	DC power jack x 1
SIM	SIM card slot door x 1
Dimensions	164 x 160 x 80 mm
Weight	970g
Accessories	12V/3A AC Adapter Ethernet cable Optional Wall/Ceiling Mounting Brackets
OS	Linux
Built-in features	WebUI, TR-69, REST API, OMA-DM, IP Pass-through

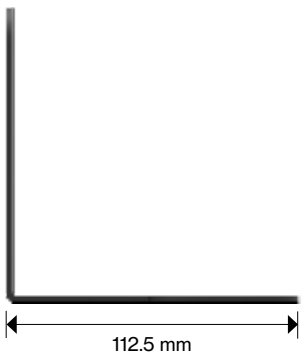
7. Troubleshooting

If you are experiencing some issues in using the router, 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, use a pin to insert the Reset Hole for a few 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 or Mac OS, for detailed instructions how to do this.
Where can I get more help?	If you have any problem setting up your router, please visit setup.verizon.com/businessinternetgateway for help. For further assistance, call the Verizon Technical Support Team at 1.800.922.0204. Please have yoru order confirmation email ready when you make the call.

8. Mounting Your Gateway onto the Wall (Optional)




112.5 mm

FCC Declaration of Conformance

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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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.

Operations in the 5.850-5.895GHz band are restricted to indoor usage only.

FCC RF Radiation Exposure Statement (SAR)

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

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 35 centimeters between the radiator and your body.

Safety Warnings

Adapter

- Do not use any other power adaptor except the one that accompanies this unit or a power adaptor identified in the list below.
- Use of another adapter could result in damage to the unit.
- The following power adaptor is qualified for use with this Verizon 5G Internet Gateway: (specified the adapter specifications, brand, make, type and other restrictions)

Caution

Ensure to connect the power cord of power adapter to a socket-outlet with grounding connection.

Safety and Compliance

Read before Use

We recommend you read the following sections thoroughly before use. Verizon is not liable for malfunctions or damages resulted from misuse of the handset.

Safety Precaution

Pay full attention to the following safety precautions.

- Use the chargers, cables or accessories approved by the device manufacturer.
- Do NOT disassemble or modify the device. Doing so voids the warranty.
- Prevent wetness from penetrating internal parts. Using the device in wet or damp environment may result in malfunctions.
- Do NOT use this device near source of heat or fire, such as oven, microwave, stove, or heater.
- Keep your device away from cooking appliances.
- Do NOT place the device in places with heated atmosphere (dryer, sauna, hot water).
- Do NOT use the device and disconnect all cables at places with fire or explosion risks.
- Avoid strong physical impact (heavy objects or excessive force).
- Keep your device away from liquid or conductive materials.
- Do NOT charge the device when either the device, the adapter, or the cable is wet. It may cause short-circuit.
- Power off the device when near medical equipment or high-precision control systems to avoid potential interference.
- Charge with specified voltage only.
- Do NOT charge device in a wet environment (bathtub, sauna).
- Place the device on a flat, stable surface for optimal use.
- Keep the device and adapter away from children and pets.
- The device must be disposed of in accordance with the locally applicable. environmental regulations.
- Keep the device away from magnetic items such as magnetic strip cards or items that generate strong electronic or magnetic fields, such as a microwave.
- Do NOT store the device in a wet or overheated environment.
- Do NOT use the device when it is overheated.
- Disconnect all the the cable connections when the device is not in use.
- Place the device in places with good signal strength.
- Make sure the adapter you use with the device meets the approved standards and specifications.

Disposal and Recycling

Do not dispose of the phone in a household garbage bin.
Products with this label must be taken to specific collection points at the end of their life.

You can learn more about how to recycle your mobile device by visiting the CTIA website at
www.ctia.org/news/how-to-recycle-your-mobile-device

Maintenance & Care

- Avoid extreme temperature or direct sunlight
- Clean handset with soft, dry cloth. Do NOT use alcohol solvent (color may fade)
- Warranty does not cover malfunctions caused by misuse.
- Stop all the applications and shut down the device before cleaning it.
- Keep the device and its accessories dry at all times.
- If anomaly occurs, contact Verizon service or authorized retail immediately.
- When storing the device, do NOT store it in a container with dampness or under extended heat.
- Avoid dropping the device or strong physical impact at all times.

Warranty

Verizon warrants that this product is free from any defect in workmanship and material, under normal use and condition, for a period of one (1) year from the original date of purchase shown on your original invoice or receipt. If any such defects are found in this product within the applicable warranty period, Verizon shall, at its option during the applicable warranty period, carry out repair or replacement for the defected product or part. Such repair or replacement is subject to verification of the defect or malfunction and proof of purchase shall be confirmed by showing the model number on receipt of invoice with the original date of purchase.

The warranty does not apply if any of the following circumstances occurs:

- The warranty period has expired.
- Proof of purchase is absent.
- Normal wear or tear of the product due to natural ambient conditions or force majeure, such as humidity, oxidization, corrosion, penetration of liquids, and extreme temperatures.
- Damage caused by connection with accessories, equipment, or peripherals that are not specified by the manufacturer or not compatible with this product.
- Damage caused by disassembly, modification or repair performed by unauthorized technician or individual.
- Damage caused by non-compliance with the recommended device use instructed in the User's Manual.
- The IMEI label on this product has been modified, altered or removed.

The purchaser or user will be responsible for any cost regarding replacement of parts, reinstallation, transportation, and any other cost that may be incurred for the repair or replacement if any of the circumstances mentioned above is determined.

This warranty statement constitutes the entirely expressed warranty granted by Verizon. No other party, whether dealer, service center or agent, or employee(s) of such, is authorized to extend or transfer this warranty on behalf of Verizon. By law, Verizon disclaims any and all liability for direct or indirect damages or losses, or for any incidental or consequential damages of any nature whatsoever, including but not limiting to loss of commercial profit or data resulting from a defect in this product.

To the extend the law permits, the repair or replacement of this product does not, under any circumstances, extend the original warranty period. However, the repaired or the replaced parts are warranted in the same manner.

Legal Notices

Copyright Statements

Trademark Statements

Limitations of Libability

To the legal extent, the product and service are provided “as is”, based on the “current condition”. Verizon Wireless and its affiliates do not guarantee that the product does not contain any fault or the service will not be interrupted. Verizon Wireless, along with its affiliates, disclaims (1) any explicit or implicit warranty of the availability, accuracy, reliability, ownership information, intellectual property rights, or suitability in the content or information of the product, software and services, including Third-Party Software; (2) any direct or indirect guarantee and has no direct control of the services, signal integrity, or network coverage of telecom operator; (3) any liability of the direct or indirect damages caused by improper use or misconduct of the product or software; (4) any liability of the direct, indirect, accidental, commercial, or punitive damages or losses arise from using the product or software.

Changes

The functions of the product and associated peripherals or accessories are described in this document are based on the current hardware, software and/or local network conditions at the time of writing, and thus may vary due to conditions set by local network service providers or carriers. Therefore, all information described herein is subject to change without prior notice.