

# Verizon Router **USER GUIDE**



Model CR1000B

©2022 Verizon

### CONTENTS

#### 01/ INTRODUCTION

1.0/ Package Contents	6
1.1/ System Requirements	6
1.2/ Features	6
1.3/ Getting to Know Your Verizon Router	9
<i>O2 /</i> CONNECTING YOUR VERIZ ROUTER 2.0/ Setting up Your Verizon Router	ZON 21

- 2.1/ Computer Network Configuration 30
- 2.2/ Main Screen 37

# *03 /* WI-FI SETTINGS 3.0/ Overview

3.1/ Basic Settings 44

43

3.2/ Advanced Settings 53

# 04/

CONNECTED DEVICES	
4.0/ Device Settings	62
4.1/ Setting Parental	
Controls	67

4.2/ Universal Plug & Play 71

05/	
CONFIGURING ADVANO SETTINGS	CED
5.0/ Security & Firewall	78
5.1/ Network Settings	94
5.2/ Diagnostics & Monitoring	151
5.3/ System	157

# 06/

TROUBLESHOOTING 6.0/ Troubleshooting Tips 175

6.1/ Frequently Asked Questions 182

189
190
191

#### 08/ NOTICES

8.0/ Regulatory Compliance Notices 195

# O1/ INTRODUCTION

- 1.0 Package Contents
- **1.1** System Requirements
- **1.2** Features
- **1.3** Getting to Know Your Verizon Router

Verizon Router lets you transmit and distribute digital entertainment and information to multiple devices in your home/office.

Your Verizon Router supports networking using coaxial cables, Ethernet, or Wi-Fi, making it one of the most versatile and powerful routers available.

# PACKAGE CONTENTS, SYSTEM REQUIREMENTS AND FEATURES

#### **1.0/ PACKAGE CONTENTS**

Your package contains:

- Verizon Router
- Power adapter
- Ethernet cable, three meters (white)

#### **1.1/ SYSTEM REQUIREMENTS**

System and software requirements are:

- A computer or other network device supporting Wi-Fi or wired Ethernet
- A web browser, such as Chrome<sup>™</sup>, Firefox<sup>®</sup>, Internet Explorer 8<sup>®</sup> or higher, or Safari<sup>®</sup> 5.1 or higher

#### **1.2/ FEATURES**

Your Verizon Router features include:

- Support for multiple networking standards, including
  - WAN 10 Gigabit Ethernet
  - LAN 802.11 a/b/g/n/ac/ax, 10/2.5 Gigabit Ethernet and MoCA 2.5 interfaces
- Integrated wired networking with 3-port Ethernet switch and Coax (MoCA)
  - Ethernet supports speeds up to 10 Gbps

- MoCA 2.5 LAN enabled to support speeds up to 2500 Mbps over coaxial cable
- One Type-C USB 3.0 port
- Integrated Wi-Fi networking with 802.11a/b/g/n/ac/ax access point featuring:
  - backward compatible to 802.11a/b/g/n/ac
  - 2.4 GHz 11ax 4x4
  - 5 GHz 11ax 4x4
  - 6 GHz 11ax 4x4
- Enterprise-level security, including:
  - Fully customizable firewall with Stateful Packet Inspection (SPI)
  - Content filtering with URL-keyword based filtering, parental controls, and customizable filtering policies per computer
  - Intrusion detection with Denial of Service protection against IP spoofing attacks, scanning attacks, IP fragment overlap exploit, ping of death, and fragmentation attacks
  - Virtual server functionality; providing protected access to internet services such as web, FTP, email, and telnet
  - DMZ (demilitarized zone) host support of a network security neutral zone between a private network and the internet
  - Event logging
  - Home Network Protection
  - SIP ALG

# FEATURES

- Static NAT
- Port forwarding
- Port triggering
- Access control
- Advanced Wi-Fi protection featuring WPA2 & WPA3 Modes and MAC address filtering
- Wi-Fi Multimedia (WMM) for Wi-Fi QoS (quality-of-service)
- Dual-stack network configuration of IPv4 and IPv6
- DHCP server
- WAN interface auto-detection
- Dynamic DNS
- DNS server
- LAN IP and WAN IP address selection
- MAC address cloning
- QoS support (end to end layer 2/3) featuring: Differentiated Services (Diffserv), 802.1p/q prioritization, and pass-through of WAN-side DSCPs, Per Hop Behaviors (PHBs), and queuing to LAN-side devices
- Secure remote management using HTTPS or Verizon app
- Static routing
- VPN (VPN pass through only)
- IGMP
- Daylight savings time support

#### **1.3/ GETTING TO KNOW YOUR VERIZON ROUTER 1.3a/ FRONT PANEL**

The Router Status LED will be solid white when your Verizon Router is turned on, connected to the internet, and functioning normally.

Condition Status	LED Color	Verizon Router
Normal	WHITE	Normal operation (50% solid)
		Setup complete (solid)
		Router is booting (soft blink)
		System restart (fast blink)
	BLUE	Pairing mode (hard blink)
		WPS pairing successful (fast blink)
	GREEN	Wi-Fi has been turned off (solid)
Issue(s)	YELLOW	No internet connection (solid)
	RED	Hardware/System failure detected (hard blink)
		Overheating (fast blink)
		WPS pairing failure (fast blink)
Power	OFF	Power off

Router Status LED

# GETTING TO KNOW YOUR VERIZON ROUTER

#### 1.3b/ REAR PANEL

The rear panel of your router has a label that contains important information about your device, including the default settings for the Verizon Router's Wi-Fi name (SSID), Wi-Fi password (WPA2 key), local URL for accessing the router's network settings, and network settings password. The label also contains a QR code that you can scan with your smartphone, tablet, or other camera-equipped Wi-Fi device to allow you to automatically connect your device to your Wi-Fi network without typing in a password (requires a QR code reading app with support for Wi-Fi QR codes).

Wi-Fi Name: Verizon_HHYN49 Wi-Fi Password: uptown-woo7-web Network Settings URL: mynetworksettings.com Network Settings Password: P9K9DSZ7V Support URL: support.verizon.com/router	
---	--

The rear panel has six ports; F-type coax, Ethernet LAN (three), Ethernet WAN, and USB. The rear panel also includes a DC power jack and a reset button.



• WPS Button - allows quick access to the Wi-Fi Protected Setup (WPS) feature and pairing mode.

The WPS button is used to initiate Wi-Fi Protected Setup. This is an easy way to add WPS capable devices to your Wi-Fi network. To activate the WPS function, press and hold the WPS button located on the rear of your Verizon Router for more than two seconds. When WPS is initiated from your router, the Router Status LED slowly flashes blue for up to two minutes, allowing time to complete the WPS pairing process on your Wi-Fi device (also known as a Wi-Fi client). When a device begins connecting to your router using WPS, the Router Status LED rapidly flashes blue for a few seconds, and then solid white as the connection completes.

If there is an error during the WPS pairing process, the Router Status LED rapidly flashes red for two minutes after the error occurs.

Refer to the "Connecting A Wi-Fi Device Using WPS" on page 33 for more details. In addition, the Router Status LED also provides a quick view of the operational state of the Verizon Router using various colors as indicated in the chart above.

- Ethernet LAN connects devices to your Verizon Router using Ethernet cables to join the local area network (LAN). The three Ethernet LAN ports:
  - one 10GE LAN port is 100 Mbps, 1/2.5/5/10 Gbps auto-sensing
  - the other two 2.5GE LAN ports are 10/100 Mbps, 1/2.5 Gbps auto-sensing

# GETTING TO KNOW YOUR VERIZON ROUTER

- **Type-C USB** provides up to 1000 mA at 5 VDC for attached devices. For example, you could charge a cell phone.
- **10Gbps Ethernet WAN** connects your Verizon Router to the internet using an Ethernet cable.
- **Coax LAN** connects your router to other MoCA devices using a coaxial cable.

*Warning:* The coax port is intended for connection to Verizon devices only. It must not be connected to any exterior or interior coaxial wires not designated for Verizon devices.

- **Reset Button** allows you to reset your router to the factory default settings. To perform a soft reboot, press and hold the button for at least three seconds. To reset your router to the factory default settings, press and hold the button for at least ten seconds.
- **Power** connects your Verizon Router to an electrical wall outlet using the supplied power adapter.

*Warning:* The included power adapter is for home use only, supporting voltages from 105-125 voltage in AC. Do not use in environments with greater than 125 voltage in AC.

#### **1.3c/ REAR LIGHTED INDICATORS** LAN/WAN Ethernet

• Unlit – Indicates no Ethernet link or dims after 5 minutes idle

#### Left LED

- Solid yellow Indicates less than 1 Gbps link
- Flash yellow Indicates LAN/WAN activity. The traffic can be in either direction.

#### **Right LED**

- Solid white Indicates 1/2.5/5/10 Gbps link
- Flash white Indicates LAN/WAN activity. The traffic can be in either direction.

#### **1.3d/** MOUNTING THE VERIZON ROUTER TO A WALL

For optimum performance, the Verizon Router is designed to stand in a vertical upright position. Verizon does not recommend wall mounting the Verizon Router. However, if you wish to mount your Verizon Router, you can purchase a wall mount bracket from the Verizon Accessories Store at verizon.com/home/accessories/networking-wifi

To mount your Verizon Router to a wall:

1. Select a mounting spot near a power outlet and the Ethernet port of the device that provides internet on your premises.

# GETTING TO KNOW YOUR VERIZON ROUTER

- 2. Mark screw hole positions on the wall. Drill holes for the wall anchors using a 1/4 inch (6.35 mm) drill bit.
- 3. Insert the anchors in the drilled holes and hammer until they are flush with the wall.



4. Place the screws into the small holes of the bracket and tighten the screws into your wall for securing the wall mount bracket.



# GETTING TO KNOW YOUR VERIZON ROUTER

5. Align the mounting hole located on the bottom of the router to the screw of the wall mount bracket.



6. Rotate and align the router to the preferred position. While using the hole in the mounting bracket, connect the Ethernet cable providing internet to the router's WAN port and other cables as needed. Tighten the bracket screw to lock the device in place.



# GETTING TO KNOW YOUR VERIZON ROUTER

7. To fasten the attached cables of the router, manage the cables, then tighten the Velcro<sup>®</sup> strap with buckle.



# CONNECTING YOUR VERIZON ROUTER

- 2.0 Setting up Your Verizon Router
- 2.1 Expanding Wi-Fi Coverage
- 2.2 Computer Network Configuration
- 2.3 Main Screen

20

Connecting your Verizon Router and accessing its web-based User Interface (UI) are both simple procedures.

Accessing the UI may vary slightly, depending on your device's operating system and web browser.

# **SETTING UP YOUR VERIZON ROUTER**

#### 2.0/ SETTING UP YOUR VERIZON ROUTER

Before you begin, if you are replacing an existing router, disconnect it. Remove all old router components, including the power supply. They will not work with your new Verizon Router.

#### 2.0a/ INSTALLATION INSTRUCTIONS

- 1. CONNECT YOUR CABLES
  - A. Connect the coax cable from the coax port on your router to a coax outlet. (Required for Fios TV; skip for 5G Home installation)
    - Separate subscription required for Fios TV; not available in all areas.
  - B. Connect the Ethernet cable from your router's WAN port to an Ethernet outlet. (Required for internet speeds greater than 100 Mbps)
  - C. Connect the power cord to your router then to an electrical outlet.



D. Router will take up to 10 minutes to update completely. Move on when the front light is solid white.

#### 2. CONNECT YOUR DEVICES

Wired or Wi-Fi? Your choice.

Wired

- A. Connect the Ethernet cable to any LAN port on your router.
- B. Connect the other end to your computer.

#### Wi-Fi

A. Get the Wi-Fi name and password off the label on your router. Wired connection



Router label

- B. On your device, choose your Wi-Fi name when it appears.
- C. Enter the Wi-Fi password exactly as it is on your router label.

# **SETTING UP YOUR VERIZON ROUTER**

#### Wi-Fi Network

The Verizon Router has one Wi-Fi name supporting 2.4 and 5 GHz signals. 6 GHz can be enabled and included as well with heightened security, WPA3. The Self-Organizing Network (SON) feature lets your devices move between these signals automatically for an optimized Wi-Fi connection.

#### 3. COMPLETE ACTIVATION

Activate your service by opening a web browser on your computer and following the prompts.

#### 2.0b/ CONFIGURE YOUR VERIZON ROUTER

- 1. Open a web browser on the device connected to your Verizon Router network.
- In the browser address field (URL), enter: <u>mynetworksettings.com</u>, then press the Enter key on your keyboard.

Alternately, you can enter: https://192.168.1.1



3. You may see a security message warning that Your connection is not private when you visit <u>mynetworksettings.</u> <u>com (https://192.168.1.1)</u> for GUI management. To get to the login screen, click the ADVANCED button, then on Proceed to 192.168.1.1 (unsafe) link.



4. The login screen will appear.

The first time you access your Verizon Router, an Easy Setup Wizard displays to help step you through the setup process.

5. On the Step 1: Please log in to your router screen, enter the password that is printed next to the Network Settings Password on the label on the rear of your router. Click Continue.

# **SETTING UP YOUR VERIZON ROUTER**



- 6. The Change Wi-Fi name screen displays. You can continue with the default settings or customize them as needed. For your protection, your Verizon Router is pre-set at the factory to use WPA2 (Wi-Fi Protected Access II) encryption for your Wi-Fi network. This is the best setting for most users and allows the most devices to securely connect.
- 7. You can optionally set up the **Guest Wi-Fi** network by toggling the selection to **On**. You can continue with the default settings or customize them as needed.

 You can optionally enable the 6 GHz Wi-Fi band by toggling the selection to On. Review the notification that enabling 6 GHz will modify the existing 2.4 & 5 GHz security from WPA2 to WPA2/WPA3 and 6 GHz will be enabled using WPA3. You can continue to use one Wi-Fi Name and Password across all Wi-Fi bands.

The IoT Wi-Fi will also be enabled for any devices that do not support WPA3, and this will use a unique Wi-Fi name and password based on the default SSID & Password. Devices on this Wi-Fi will be able to communicate with other devices on the Primary network with no firewall restrictions separating them.

- 9. Click **Continue** to review your settings.
- The Apply Wi-Fi changes screen is displayed. Review your current settings. You may optionally save your settings as an image on your device by selecting the button, Save as Image. Click Apply to save the Wi-Fi changes to your Verizon Router.

# **SETTING UP YOUR VERIZON ROUTER**

	Change Wi-Fi name
	Wi-Fi Name
Wi-FIName: Verizon GHYGHN Wi-FI Password: mac1-car7-rex5 Network Settings URL: unpretworksettings.com	Verizon_Z7KXTL
Network Settings Password: QOU98NHA7 Support URL: support verizon.com/router	Wi-Fi Password
ļ	••••••
	Guest Wi-Fi Enabled
	4
	Quest Wi-Fi Name Verizon_Z7fXXTL-Guest
	Curest Wi-Fi Hame Verizon_Z7KXTL-Guest Guest Wi-Fi Password
	Guest Wi-Fi Hame Verizon_Z7KXTL-Guest Guest Wi-Fi Password Enter new passsword
Back view	Guest Wi-Fi Hame Verizon_Z7KXTL-Guest Guest Wi-Fi Password Enter new passsword

For your protection, your Verizon Router is pre-set at the factory to use WPA2 (Wi-Fi Protected Access II) encryption for your Wi-Fi network. This is the best setting for most users and provides security.

11. Click Continue. The Apply Wi-Fi changes screen appears. You have an option of saving the Wi-Fi settings as an image on your device by clicking the Save as image button. After you click Save as image to save your Wi-Fi settings as an image, click Apply to save the Wi-Fi changes to your Verizon Router. *Note:* If you select *Save as image*, the image file is saved to your web browser's download folder.

Important: If you are on a Wi-Fi device when setting up your Verizon Router and changes are made to the Wi-Fi name or password, then you will be disconnected from the Wi-Fi network. When this occurs, review the Wi-Fi networks available and choose the network name when it appears. Enter the Wi-Fi password you have applied, and your device will reconnect to the Verizon Router.

.....

	Apply Wi-Fi changes
Wi-Fi Name: <u>Writzon, 9HY9HN</u> Wi-Fi Passaword: mact-car7rex5 Network Settings URL: mynethoologicings.com	WI-FIInfo Save as imag
Network Settings Password: QOU98NHA7 Support URL: support verizon.com/router	Wi-Fi Name Verizon_Z7KXTL
1	W-FI Password
	Security WPA2/WPA3 (2.4 & 5 GHz) WPA3 (6 GHz)
	Gueat WI-FI C
0	Guest Wi-Fi Name Verizon_Z7KXTL-Guest
Back view	Guest Wi-Fi Password 123450789

# **SETTING UP YOUR VERIZON ROUTER**

The **You're all set up!** screen displays once your Verizon Router verifies the final settings and has successfully connected to the internet and is ready for use. You can click on **Go to Network Settings** to access the main screen of the Verizon Router.



If your Verizon Router is subsequently reset to the factory default settings, the settings printed on the label will again be in effect.

If your Verizon Router fails to connect, follow the troubleshooting steps in the Troubleshooting section of this guide.

#### **2.1/ COMPUTER NETWORK CONFIGURATION**

Each network interface on your computer should either automatically obtain an IP address from the upstream Network DHCP server (default configuration) or be manually configured with a statically defined IP address and DNS address. We recommend leaving this setting as it is.

#### 2.1a/ CONFIGURING DYNAMIC IP ADDRESSING

To configure a computer to use dynamic IP addressing:

#### WINDOWS 7/8

- 1. In the Control Panel, locate **Network and Internet**, then select **View Network Status and Tasks**.
- 2. In the View your active networks Connect or disconnect section, click Local Area Connection in the Connections field. The Local Area Connection Status window displays.
- 3. Click **Properties**. The Local Area Connection Properties window displays.
- Select Internet Protocol Version 4 (TCP/IPv4), then click Properties. The Internet Protocol Version 4 (TCP/IPv4) Properties window displays.
- 5. Click the **Obtain an IP address automatically** radio button.
- 6. Click the Obtain DNS server address automatically radio button, then click OK.

# **COMPUTER NETWORK CONFIGURATION**

- 7. In the Local Area Connection Properties window, click **OK** to save the settings.
- To configure Internet Protocol Version 6 (TCP/IPv6) to use dynamic IP addressing, repeat steps 1 to 7. However for step 4, select Internet Protocol Version 6 (TCP/IPv6) in the Properties option (refer to IPv6 section for Verizon Router configuration).

#### WINDOWS 10

- 1. On the Windows desktop, click on the **Start** icon. Select **Settings** and click **Network & Internet**.
- 2. In the Network & Internet, click Ethernet.
- 3. Select Network and Sharing Center. The View your basic network information and set up connections window displays.
- 4. In the View your active networks, click Ethernet in the Connections field. The Ethernet Status window displays.
- 5. Click **Properties**. The **Ethernet Properties** window displays.
- Select Internet Protocol Version 4 (TCP/IPv4), then click Properties. The Internet Protocol Version 4 (TCP/IPv4) Properties window displays.
- 7. Click the Obtain an IP address automatically radio button.
- 8. Click the **Obtain DNS server address automatically** radio button, then click **OK**.

- 9. In the Local Area Connection Properties window, click OK to save the settings.
- To configure Internet Protocol Version 6 (TCP/IPv6) to use dynamic IP addressing, repeat steps 1 to 9. However for step 6, select Internet Protocol Version 6 (TCP/IPv6) in the Properties option (refer to IPv6 section for Verizon Router configuration).

#### MACINTOSH OS X

- 1. Click the **Apple** icon in the top left corner of the desktop. A menu displays.
- 2. Select **System Preferences**. The System Preferences window displays.
- 3. Click Network.
- 4. Verify that **Ethernet**, located in the list on the left, is highlighted and displays **Connected**.
- 5. Click Assist Me.
- 6. Follow the instructions in the **Network Diagnostics Assistant**.

#### 2.1b/ CONNECTING OTHER COMPUTERS AND NETWORK DEVICES

You can connect your Verizon Router to other computers or set top boxes using an Ethernet cable, Wi-Fi connection (Wi-Fi), or coaxial cable.

# **COMPUTER NETWORK CONFIGURATION**

#### ETHERNET

- 1. Plug one end of an Ethernet cable into one of the open Ethernet ports on the back of your Verizon Router.
- 2. Plug the other end of the Ethernet cable into an Ethernet port on the computer.
- 3. Repeat these steps for each computer to be connected to your Verizon Router using Ethernet. You can connect up to three.

#### **CONNECTING A WI-FI DEVICE USING WPS**

Wi-Fi Protected Setup (WPS) is an easier way for many devices to set up a secure Wi-Fi network connection. Instead of manually entering passwords or multiple keys on each Wi-Fi client, such as a laptop, printer, or external hard drive, your Verizon Router creates a secure Wi-Fi network connection.

In most cases, this only requires the pressing of two buttons – one on your Verizon Router and one on the Wi-Fi client. This could be either a built-in button or one on a compatible Wi-Fi adapter/card, or a virtual button in software. Once completed, this allows Wi-Fi clients to join your Wi-Fi network.

To initialize the WPS process, you can either press and hold the WPS button located on the rear of your Verizon Router for more than two seconds or use the UI and press the on-screen button.

You can easily add Wi-Fi devices to your Wi-Fi network using the WPS option if your Wi-Fi device supports the WPS feature.

To access WPS using the user interface:

1. From the **Basic** menu, select **Wi-Fi** settings, then click **Wi-Fi Protected Setup**.

verizon Basic	Advance	d	Hele & ~
Network Devices Verizon Router	~	WHT > WHT Protected Setup	
Home		••••••	
WI-FI	^	Enable Wi-Fi Protected Setup	WPS Enabled
Primary Network		Wi-Fi Protected Setup is an easy way to add Wi-Fi devices to your network. To use this feature, your Wi-Fi client device needs to support WPS.	
Guest Network		⚠ Wi-Fi devices may briefly lose connectivity when turning WPS on or off.	
IoT Network			
Wi-Fi Protected Setup		Option 1 (Recomended)	Option 2
Devices	Ý	If your client device has a WPS button, press it and then click the button below to start WPS registration.	If your client device has a WPS PIN, enter that number below (usually found on a sticker on the back of the device) and click "Register":
System	Ý	Start WPS	Register
			If your client supports it, enter the router's PIN into the client device:  Figure 2 Enable router's PIN: 22422613

- 2. Enable the protected setup by moving the selector to on.
- 3. Use one of the following methods:
  - If your Wi-Fi client device has a WPS button, press the WPS button on your router for more than two seconds, then click the start WPS button in the Option 1 to start the WPS registration process.
  - If your client device has a WPS PIN, locate the PIN printed on the client's label or in the client documentation. Enter the PIN number in the **Enter PIN** field. The **Client WPS PIN** field is located in the **Option 2** on the user interface.
  - Click Register.

# **COMPUTER NETWORK CONFIGURATION**

- Alternatively, you can enter the router's PIN shown on this screen into the WPS user interface of your device, if this PIN mode is supported by your Wi-Fi device.
- 4. After pressing the WPS button on your router, you have two minutes to press the WPS button on the client device before the WPS session times out.

When the WPS button on your router is pressed, the Router Status LED on the front of your router begins flashing blue. The flashing continues until WPS pairing to the client device completes successfully. At this time, the Router Status LED turns solid white.

If WPS fails to establish a connection to a Wi-Fi client device within two minutes, the Router Status LED on your router flashes red for two minutes to indicate the WPS pairing process was unsuccessful. After flashing red, the light returns to solid white to indicate that Wi-Fi is on.

*Note:* Wi-Fi Protected Setup (WPS) cannot be used if WPA3 security is enabled or SSID broadcast is disabled or if MAC address authentication is enabled with an empty white list.

#### **CONNECTING A WI-FI DEVICE USING A PASSWORD**

- 1. Verify each device that you are connecting with Wi-Fi has built-in Wi-Fi or an external Wi-Fi adapter.
- 2. Open the device's Wi-Fi settings application.

- 3. Select your Verizon Router's Wi-Fi network name (SSID) from the device's list of discovered Wi-Fi networks.
- 4. When prompted, enter your Verizon Router's Wi-Fi password (WPA2 or WPA3 key) into the device's Wi-Fi settings. Your router's default Wi-Fi network name and password are located on the sticker on the rear panel of your Verizon Router.



- 5. Verify the changes were implemented by using the device's web browser to access a site on the internet.
- 6. Repeat these steps for every device that you are connecting with Wi-Fi to your router.

#### COAX

- 1. Verify all coax devices are turned off.
- 2. Disconnect any adapter currently connected to the coaxial wall jack in the room where your router is located.
- 3. Connect one end of the coaxial cable to the coaxial wall jack and the other end to the coax port on your network device.
- 4. Power up the network device.
## **MAIN SCREEN**

#### 2.2/ MAIN SCREEN

When you log into your router, the dashboard main page displays the navigation menus of Basic and Advanced settings, Wi-Fi settings, Devices, Parental Controls, and connection status, and Basic quick links.

Network Devices					
Venzon Houter N	, Status Off	ine	>	Wi-Fi	<u>,</u>
Home Wi-Fi Devices System	~			Wi-Fi Name     Wi-Fi Name     Wi-Fi Passnord     Wi-Fi Passnord     Parental Controls	>
	Devices	8f85384e668	>		

The configuration options available via the left-hand main menu are described in the following chapters:

- Basic Settings
  - System this chapter
  - Wi-Fi Chapter 3
  - Devices Chapter 4
- Advanced Settings Chapter 5

#### 38

### 2.2a/ SYSTEM SYSTEM STATUS

To view the status:

- 1. Access the dashboard Home page.
- You can quickly view your router's status by clicking System\System Status on the screen. This section displays the status of your router's local network (LAN) and internet connection (WAN), firmware and hardware version numbers, MAC Address, IP settings of Verizon Router and Extender Mini(s) (if connected).

Vertoon Router  Vertoon Router  System Status  System Status  Auto-refresh  Kana  Becommented  Becommented  Prof address  Prof a	
me     Production       FI     v       statum     v       statum     Production       pen Source Software	tefresh
Image: Product in the state	
Vacce         *         Statut Disconnected Disconneco Disconnected Disconneco Disconnected Disconnected Di	
Item         Notes         Provide address is from         Provide address is from           pen Source Software         Provide address is from         Provide address is from         Provide address is from           pen Source Software         Provide address is from         Provide address is from         Provide address is from           pen Source Software         Provide address is from         Provide address is from         Provide address is from           Provide Provide Address 1         Provide Address 1         Provide Address 1         Provide Address 1           Provide Address 1         Provide Address 1         Provide Address 1         Provide Address 1	
Unit-Pro-         Unit-Pro-           Per Source Software         Pr4 address         Despated Prefix           Subset Mask         Pr4 Address         Pr4 Address           Pr4 Despated Prefix         Pr4 Address         Pr4 Address           Pr4 Despated Prefix         Pr4 Address         Pr4 Address           Pr4 Despated Prefix         Pr4 Despated Prefix         Pr4 Despated Prefix           Pr4 Despate Prefix         Pr4 Despate Prefix         Pr4 Despate Prefix	
Pr4 Dris Adress 1 Pr4 Dris Adress 2 Pr4 Dris Adress 1 Pr4 Dris Adress 1 Pr4 Dris Adress 1 Pr4 Dris Adress 1 Pr4 Dris Adress 1	
Pr4 Detaut Gateway Pr4 Detaut Gateway Pr4 Dets Address 1 Pr4 Dets Address 2 Pr4 Dets Address 2 Pr4 Dets Address 1 Pr4 Dets Addr	
IPv4 DHS Address 1 IPv4 DHS Address 2 IPv4 DHS Address 1	
IPv4 DNS Address 2 IPv6 DNS Address 1	
NATs Supported (used / max) IPv6 DNS Address 2 0 / 30000	
Router	

## **MAIN SCREEN**

verizon Basic Ad	lvanced	Help	8
etwork Devices	System > System Status		
Verizon Router	System Status	Auto-refresh Refresh	
ome	3.11.4b-eng0		
I-FI	Hardware Version     EVT4		
evices	V Model Name		
rstem	CR1000B		
System Status	AAD14800442		
pen Source Software	LAN IPv4 Address 192.168.11		
	Broadband MAC address C0:D7:AA:54:7F:12		
	Broadband Physical Connection Disconnected		
	Router has been active for O day(s) 6 hours 55 minutes 53 seconds		
	LED Status No internet connection		
	Evtandar	—	
	Device Name		
	E3200-b8185384e668		
	Model Name E3200		
erizon Basic Ad	lvanced	Hele	8
work Devices	System > System Status		
	System Status	Auto-refresh Bofresh	
ome	E3200		
I-FI	<ul> <li>Firmware Version 3.1115</li> </ul>		
evices	Hardware Version     102		
stem	Serial Number		
lystem Status	E301120071800005		
Open Source Software	88,F8,53,84,E6:68		
	Bystem Up Time O day(s) 8 hours 16 minutes 30 seconds		
	LED Status Normal operation		
	Backhaul Type Ethernet		
	Bit Rate 1.0 Gbps		
	IPv4 Address 192.158.1.100		
	IPv6 Address		
	Subnet Mask 255.255.255.0		
	Default Gateway		



#### 2.2b/ OPEN SOURCE SOFTWARE

verizon Basic	Advance	sd	<u>Helo</u>	® ~
Network Devices	~	system > Open Source Software		
Home Wi-Fi Devices System System Status Open Source Software	~	This product includes offware mode available under open source licenses. Additional information about that obtainurs, selficiable licenses, and downloadable options of source code, is anniable at: <a href="https://www.example.code.code.code.code.code.code.code.cod</td> <td></td> <td></td>		
		Copyright © 2021 Verizon		

*To view:* From the **Basic** menu, select **System** from the left pane and then click **Open Source Software**.

# 03/ WI-FISETTINGS

- 3.0 Overview
- 3.1 Basic Settings
- 3.2 Advanced Settings

Wi-Fi networking enables you to free yourself from wires, making your devices more accessible and easier to use.

You can create a Wi-Fi network, including accessing and configuring Wi-Fi security options.

## **OVERVIEW**

## 3.0/ OVERVIEW

Your Verizon Router provides you with Wi-Fi connectivity using the 802.11a, b, g, n, ac or ax standards. These are the most common Wi-Fi standards.

The Verizon Router contains 2.4 GHz, 5 GHz and 6 GHz Wi-Fi bands, and the operation modes and speeds are listed as follows:

- 2.4 GHz
  - Legacy operation mode: supports IEEE 802.11b/g/n with maximum theoretical rate at 600 Mbps
  - Compatibility mode: supports IEEE 802.11ax
    - backward compatible with IEEE 802.11b/g/n/ac
    - maximum theoretical rate up to 1.1 Gbps
- 5 GHz
  - Legacy operation mode: supports IEEE 802.11a/n/ac with maximum theoretical rate at 2.2 Gbps
  - Compatibility mode: supports IEEE 802.11ax
    - backward compatible with IEEE 802.11a/n/ac
    - maximum theoretical rate up to 2.4 Gbps
- 6 GHz
  - Operation mode: supports IEEE 802.11ax
  - Maximum rate up to 4.8 Gbps

*Note:* 802.11a, 802.11b, and 802.11g are legacy modes and are not recommended. Even one such device connected to the network will slow your entire Wi-Fi network.

The Wi-Fi service and Wi-Fi security are activated by default. The level of security is preset to WPA2 encryption using a unique default WPA2 key (also referred to as a passphrase or password) preconfigured at the factory. This information is displayed on a sticker located on the rear of your router.

Your router integrates multiple layers of security. These include Wi-Fi Protected Access, and firewall.



#### **3.1/ BASIC SETTINGS 3.1a/ PRIMARY NETWORK**

You can configure the basic security settings for 2.4 GHz, 5 GHz or 6 GHz of your Wi-Fi network.

ced	Help (8)
Wi-Fi > Primary Network	
Primary Network	
Wi-Fi Name Wi-Fi Password Verizon_Z7KXTL	♥ Wi-Fi Enabled ● ♀ ∧
	<u>ل</u>
Security Set encryption type used to secure the WI-FI traffic.	WPA2 ~
Broadcast Wi-Fi network name (\$\$ID) Broadcast Wi-Fi name from router to Wi-Fi clients.	Enabled
MAC Authentication	
Limits the Wi-Fi clients that can connect to router.	<u>Edit list</u>
2.4 0Hz	Wi-Fi Enabled 💽 🔅 🗸
5 GHz	Wi-Fi Enabled 💽 💩 🗸
8 GHz	Wi-Fi Disabled 🖉 🖉 🗸
	ever VICT 3 Primary Network VICT 3 Primary Network VICT 0 Primary Network

## **BASIC SETTINGS**

*To configure the Primary Wi-Fi name & password and security settings:* 

- 1. From the **Basic** menu, select **Wi-Fi** from the left pane and then click **Primary Network**.
- 2. To activate the Wi-Fi radio, move the selector to **on**. If the radio is not enabled, no Wi-Fi devices will be able to connect to the home network.
- 3. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.

*Note:* The SSID is the network name. All devices must use the same SSID.

 To configure the Wi-Fi Security, click the setup <sup>(a)</sup> button and select WPA2 or WPA3.

*Caution:* These settings should only be configured by experienced network technicians. Changing the settings could adversely affect the operation of your router and your local network.

Broadcast Wi-Fi network name (SSID)

You can configure the Verizon Router's SSID broadcast capabilities to allow or disallow Wi-Fi devices from automatically using a broadcast SSID name to detect your router Wi-Fi network.

To enable SSID broadcasting, move the selector to on.
 SSID broadcast is enabled by default. The SSID of the Wi-Fi network will be broadcast to all Wi-Fi devices.

- To disable SSID broadcasting, move the selector to off. The public SSID broadcast will be hidden from all Wi-Fi devices. You will need to manually configure additional Wi-Fi devices to join the Wi-Fi network.
- MAC Authentication

You can configure your router to limit access to your Wi-Fi network to only those devices with specific MAC addresses.

Prima	MAC Authentication	×	
A Verizon 77	Access List		Wi-Fi Enabled
	Device Access		
			Enabled
Ŷ			
2.4	Enter MAC address	Add new device	Wi-Fi Enabled 🌕 🛭 🕸 🗸
5 (			Wi-Fi Enabled 💽 🔅 🗸
6 (	Cancel	Apply Changes	
	Prima     with Name     Werden_277	MAC Authentication     MAC Authentication     Mac Authentication     Access List     Uetron_277     Device Access     Enter MAC address     Cancel	

To set Wi-Fi MAC authentication:

- 1. To setup access control, click on the Edit list.
- 2. Select either:
  - Access List allows the listed devices to access the Wi-Fi network.

## **BASIC SETTINGS**

*Warning:* This will block Wi-Fi network access for all devices not in the list. Only devices in the list will be able to connect to the Wi-Fi network.

- **Device Access** Wi-Fi devices will be able to access the Wi-Fi network if they use the correct Wi-Fi password.
- 3. Enter the MAC address of a device and click **Add new device**.
- 4. Repeat step 2 and step 3 to add additional devices, as needed.
- 5. When all changes are complete, click **Apply Changes** to save the changes.

#### **3.1b/ GUEST NETWORK**

The **Guest Network** is designed to provide internet connectivity to your guests but restricts access to your primary network and shared files. The primary network and the guest network are separated from each other through firewalls. You create one Guest Wi-Fi SSID and one password, and use it for all guests. The guest network SSID does not change when you make a change to your primary network SSID.

The Verizon Router is shipped from the factory with Guest Wi-Fi turned off. The default SSID for Guest Wi-Fi is preconfigured at the factory to the default Wi-Fi network name (SSID) which is displayed on a sticker located at the rear of the router followed by hyphen guest (-Guest). For example – if the router is shipped with a default SSID of "Fios-ABCDE" then the default SSID for Guest Wi-Fi is "Fios-ABCDE-Guest".

verizon Basic	Advance	a	Help 🛞 -
Network Devices Verizon Router	$\sim$	Wi-F1 > Guest Network	
Home		Guest Network	
WI-FI	^	Band WrTI Name WrTI Password 2.4 GHz Verizon_Z7KXTL-Guest	Wi-Fi Enabled 🌒 🏘 ^
Primary Network			<u>(</u> )
Guest Network		Security Set encryption type used to secure the Wi-Fi traffic.	WPA2
IoT Network			WPA2
Devices	÷		
System	~		

To configure the security settings for your guest network:

- 1. From the **Basic** menu, select **Wi-Fi** and then click **Guest Network**.
- 2. Move the selector to on.
- 3. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.
- 4. Press Apply Changes to save the changes.

*Important:* It is not recommended to create a guest network without a password.

## **BASIC SETTINGS**

#### **3.1c/IOT NETWORK**

The router supports connection of multiple IoT devices on a separate Wi-Fi SSID. The IoT Network is designed to provide an easier setup experience for your Internet of Things (IoT) devices which benefit from connecting to the 2.4 GHz band while keeping your Primary Network settings unchanged. IoT devices and Primary devices can communicate with no firewall restrictions separating them.

The Verizon Router is shipped from the factory with IoT Wi-Fi turned off. The default SSID for IoT Wi-Fi is preconfigured at the factory to the default Wi-Fi network name (SSID) which is displayed on a sticker located at the rear of the router followed by hyphen IoT (-IoT). For example – if the router is shipped with a default SSID of "Fios-ABCDE" then the default SSID for IoT Wi-Fi is "Fios-ABCDE-IoT".

verizon Basic Advance	rd	Help 🛞 -
Verizon Router	WFFI > IoT Network	
Home		
WI-FI ^	Dand         W-F1 Name         W-F1 Password           2.4 OHz         Verizon_27/KXTL-IoT	Wi-Fi Enabled 🌑 🦉 ^
Primary Network		0
Guest Network	Security Set encryption type used to secure the Wi-Fi traffic.	WPA2 ^
IoT Network		WPA2
Wi-Fi Protected Setup		None
Devices ~		
System ~		

#### To enable IoT Wi-Fi link:

- 1. From the **Basic** menu, select **Wi-Fi** and then click **IoT Network**.
- 2. Move the selector to on.
- 3. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.
- 4. Press Apply Changes to save the changes.

#### **3.1d/ WI-FI PROTECTED SETUP (WPS)**

Wi-Fi Protected Setup (WPS) is an easier way for many devices to set up a secure Wi-Fi network connection. Instead of manually entering passwords or multiple keys on each Wi-Fi client, such as a laptop, printer, or external hard drive, your Verizon Router creates a secure Wi-Fi network connection.

In most cases, this only requires the pressing of two buttons – one on your Verizon Router and one on the Wi-Fi client. This could be either a built-in button or one on a compatible Wi-Fi adapter/card, or a virtual button in software. Once completed, this allows Wi-Fi clients to join your Wi-Fi network.

To initialize the WPS process, you can either press and hold the unified button located on the front of your Verizon Router for more than two seconds or use the UI and press the on-screen button.

## **BASIC SETTINGS**

You can easily add Wi-Fi devices to your Wi-Fi network using the WPS option if your Wi-Fi device supports the WPS feature.

To access WPS using the user interface:

1. From the **Basic** menu, select **Wi-Fi** and then click **Wi-Fi Protected Setup (WPS)**.

verizon Basic	Advance	d	Hala 🛞 -
Network Devices	~	Wi-Fi > Wi-Fi Protected Setup	
Home		Wi-Fi Protected Setup	*
WI-FI	^	Enable Wi-Fi Protected Setup	WPS Enabled
Primary Network		Wi-Fi Protected Setup is an easy way to add Wi-Fi devices to your network. To use this feature, your Wi-Fi client device needs to support WPS.	
Guest Network		△ Wi-Fi devices may briefly lose connectivity when turning WPS on or off.	
IoT Network			
Wi-Fi Protected Setup		Option 1 (Recomended)	Option 2
Devices	v	If your client device has a WPS button, press it and then click the button below to start WPS registration.	If your client device has a WPS PIN, enter that number below (usually found on a sticker on the back of the device) and click "Register":
System	ř	Start WPS	Register
			If your client supports it, enter the router's PIN into the client device:  Enable router's PIN: 22422013

- 2. Enable the protected setup by moving the selector to on.
- 3. Use one of the following methods:
  - If your Wi-Fi client device has a WPS button, press the unified button on your router for more than two seconds, then click the start WPS button in the Option 1 to start the WPS registration process.
  - If your client device has a WPS PIN, locate the PIN printed on the client's label or in the client documentation.
     Enter the PIN number in **Option 2** on the user interface.

- Click Register.
- Alternatively, you can enter the router's PIN shown on this screen into the WPS user interface of your device, if this PIN mode is supported by your Wi-Fi device.
- 4. After pressing the unified button (WPS) on your router, you have two minutes to press the WPS button on the client device before the WPS session times out.

When the unified button (WPS) on your router is pressed, the Router Status LED on the front of your router begins flashing blue. The flashing continues until WPS pairing to the client device completes successfully. At this time, the Router Status LED turns solid blue.

If WPS fails to establish a connection to a Wi-Fi client device within two minutes, the Router Status LED on your router flashes red for two minutes to indicate the WPS pairing process was unsuccessful. After flashing red, the light returns to solid white to indicate that Wi-Fi is on.

*Note:* Wi-Fi Protected Setup (WPS) cannot be used if WPA3 security is enabled or SSID broadcast is disabled or if MAC address authentication is enabled with an empty white list.

## **ADVANCED SETTINGS**

#### **3.2/ ADVANCED SETTINGS 3.2a/ PRIMARY NETWORK**

#### Self-Organizing Network (SON)

The Verizon Router supports 2.4 GHz, 5 GHz and 6 GHz signals. The Self-Organizing Network (SON) feature lets your devices move between these signals automatically for an optimized Wi-Fi connection.

verizon Basic	Advanced	d				Help Q ~
Network Devices	~	Wi-Fi > Primary Network				
Home	<b>^</b>	Primary N	Network			Apply Changes
Wi-Fi	^	Self-Organizing Netw Allow devices to move se and extenders, when con	<b>vork (SON)</b> eamlessly between Wi-Fi nnected.	bands		SON Enabled
Primary Network Guest Network		Wi-Fi Name Verizon_Z7KXTL		Wi-Fi Password	Ø	Wi-Fi Enabled 🚺 🔯 ^
IoT Network						(b
Wi-Fi Protected Setup			Security Set encryption type us	ed to secure the Wi-Fi traffic.		WPA2 ~
Radio Management						
Devices	ř		Broadcast Wi-Fi netwo Broadcast Wi-Fi name	from router to Wi-Fi clients.		Enabled
Security & Firewall	ř		MAC Authentication			T do too
Network Settings	×		Limits the Wi-Fi clients	that can connect to router.		East list
Diagnostics & Monitoring	~ _	2.4 GHz				Wi-Fi Enabled 💽 🔅 🗸 🖕

To configure SON, Wi-Fi radio, SSID and security settings:

- 1. From the Advanced menu, select Wi-Fi from the left pane and then click Primary Network.
- 2. To enable SON, move the selector to on.

- 3. To activate the Wi-Fi radio, move the selector to **on**. If the radio is not enabled, no Wi-Fi devices will be able to connect to the primary network.
- 4. If desired, enter a new name and password for the Wi-Fi network or leave the default name and password that displays automatically.

*Note:* The SSID is the network name. All devices must use the same SSID.

twork Devices		Wi-Fi > Primary Networ	rk		
Verizon Router	$\sim$				
	-	Primary	Network		
ome	- 1		MAC Authentication Limits the Wi-Fi clients that can connect to router.		Edit list
/i-Fi	^				
Primary Network		2.4 GHz		Wi-Fi Enabled	0
Guest Network		5 GHz		Wi-Fi Enabled	ŝ
loT Network	- 1		Group Key		
Wi-Fi Protected Setup			Update Group Key based on time interval used to update the WPA shared key.	259200 Enabled	
Radio Management			Wi-Fi QoS (WMM)		
evices	~		Improves the quality of service (QoS) for voice, video, and audio streaming over Wi-Fi by prioritizing these data streams.	Enabled	
ecurity & Firewall	~		WMM Power Save		
etwork Settings			Improve battery life on mobile Wi-Fi devices such as smart phones and tablets by fine-tuning power consumption.	Enabled	

5. To configure the Wi-Fi security, click the setup 🍩 button.

*Caution:* These settings should only be configured by experienced network technicians. Changing the settings could adversely affect the operation of your router and your local network.

## **ADVANCED SETTINGS**

- Group key to update the WPA shared key, move the selector to on.
- Wi-Fi QoS (WMM) improves the quality of service (QoS) for voice, video, and audio streaming over Wi-Fi by prioritizing these data streams.
- WMM Power Save improves battery life on mobile Wi-Fi devices such as smart phones and tablets by fine-tuning power consumption.

#### **3.2b/**RADIO MANAGEMENT

You can configure the channel settings for the 2.4 GHz, 5 GHz and 6 GHz band(s) of your Wi-Fi network.

verizon Basic	Advance		Help Q ~
Network Devices Verizon Router	$\sim$	Wi-Fi > Radio Management	
Home	A	Radio Management Setting: History	
Wi-Fi	^	Channel Analysis	Cattinga Cont
Primary Network			b scan
Guest Network		2.4 GHz 5 GHz 6 GHz 10	
IoT Network		8	
Wi-Fi Protected Setup		4 2	
Radio Management		0 1 2 3 4 5 6 7 8 9 10 11 1 2 3 4 5	6 7 8 9 10 11 12 13 14
Devices	~	Score Channel Signal Recent scan: Wait for NTP server to synchronize	Channel
Security & Firewall	×	Channel Settings	
Network Settings	~	Channel Setungs	
Diagnostics & Monitoring	· .	Band         Channel         Width         Health           2.4 GHz         Ch. 6 (Auto)         V         20/40MHz         V	Radio Enabled 💽 🗡 🖕

To view and configure the channel settings:

- 1. From the Advanced menu, select Wi-Fi and then click Radio Management.
- 2. Click on **Settings** on the top right-hand side of the **Radio Management** page to configure the channel scan settings:

^	Channel Ar	Scan Settings	×				[	Setting	5
twork vork	2.4 GHz 5 G	Keep my channel selection during power cycle		GHz (					
k	6	Enable DFS channels during channel scan	~						
cted Setup	4 2	Cancel Apply Changes							
agement	1 2								11

- Select the Keep my channel selection during power cycle check box to save your channel selection when your Verizon Router is rebooted.
- Enable DFS channels during channel scan: DFS channels are enabled by default during channel scans.

*Note:* DFS channels are a subset of the 5 GHz network that is shared with radar systems. Some consumer devices do not support these channels and cannot connect to routers using them. Examples include some media streaming devices. Disabling this feature will allow the router to select the best available channel to broadcast on and allow these devices to connect.

• Press Apply Changes to save the changes.

## **ADVANCED SETTINGS**

- 3. Click **Scan** to perform channel availability scan for the Verizon Router accommodating the best radio channel and providing the best Wi-Fi performance.
- 4. On the **Channel Settings** page for either 2.4 GHz, 5 GHz or 6 GHz, the following information displays and can be configured:
  - Channel Analysis scans and displays channel bandwidth and signal strength of available APs. Channel Score displays a network congestion score of one to ten in each Wi-Fi channel. It can be used to determine which channels to use or to avoid. Higher score indicates less congestion in a channel.
  - Channel Settings this is the radio channel used by the Wi-Fi router and its clients to communicate with each other. The channel must be the same on the router and all of its Wi-Fi clients. Select the channel you want the Wi-Fi radio to use to communicate, or accept the default (Auto) channel selection. Then the router will automatically assign itself a radio channel.
  - Width displays the Wi-Fi channel currently in use on each band. Users can select from available channels.

#### • 802.11 Mode

You can limit the Wi-Fi access to your network by selecting the 2.4 GHz and 5 GHz Wi-Fi communication standard best suited for the devices you allow to access your Wi-Fi network.

Select the Wi-Fi mode as follows:

- Compatibility This is the default mode setting on 5 GHz, providing a good balance of performance and interoperability with existing Wi-Fi devices. 802.11a,n,ac and ax devices can connect.
- Legacy This is the default mode setting on 2.4 GHz, providing broad connection support for old and new Wi-Fi devices. 802.11a,b,g,n and ac devices can connect.

#### Notes:

802.11n is available on both 2.4 GHz and 5 GHz frequencies.

*Connecting 802.11a, b or g devices will cause your Wi-Fi network to slow on that radio and is not recommended.* 

• Transmit Power – adjusts the power of the Wi-Fi signal.

## **ADVANCED SETTINGS**

To view the channel settings history:

- 1. From the Advanced menu, select Wi-Fi and then click Radio Management.
- 2. Click on **History** to display the channel settings history.

verizon Basic	Advance	ed				<u>Help</u>	®~
Network Devices		Wi-Fi > Radio Mana	agement				
Verizon Router	$\sim$		_				
Home	A	Settings Hist	/lanageme <sup>wy</sup>	ent			
Wi-Fi	^	Band	Channel	Time	Date		
Primary Network	- 1						
Guest Network							
IoT Network	- 1						
Wi-Fi Protected Setup							
Radio Management	- 1						
Devices	~						
Security & Firewall	×						
Network Settings	~						
Diagnostics & Monitoring	× .			Copyrig	ht © 2021 Verizon		

## 04/ CONNECTED DEVICES

- **4.0** Device Settings
- 4.1 Setting Parental Controls
- 4.2 Universal Plug & Play

You can view the settings of the network devices connected to your Verizon Router's network.

The abundance of harmful information on the internet poses a serious challenge for employers and parents alike as they ask "How can I regulate what my employee or child does on the internet?"

With that question in mind, your Verizon Router's Parental Controls were designed to allow control of internet access on all locally networked devices.

## **DEVICE SETTINGS**

## 4.0/ DEVICE SETTINGS

To view and manage the connected devices on your network:

- 1. From the **Basic** menu, select **Devices** from the left pane.
- 2. The screen displays information about connected devices including **Device Name** and identifiers, **Parental Controls**, the type of network connection, and settings that you can view and configure.

verizon Basic	Advance	ed			ł	<u>telp</u> ® ~
Network Devices		Devices > Devices > All				
Verizon Router	$\sim$					
		Devices			Add D	evice
Home		All (2) Primary (2) Gue	st (0) IoT (0)			
WI-FI	~	Online				
Devices	~					
Devices	2	Device Name 🤤	Connection 👙	Parental Controls 👙	Block/Allow -	
Parantal Controls	•	A040025-NB2	Ethernet	None		\$
Parental Controls	Ŭ	E2200.b9f95294a669	Intel Ethernot	Nana		~
System	v	Large-201803846008	E chemer	None		105
		Offline			(	Clear list

- 3. To easily add a new device to the network:
  - i. Click Add Device button on the screen.
  - ii. Select the preferred **Network Type** from the dropdown list (**Primary**, **Guest** or **IoT**).
  - iii. Scan the provided QR code with the device's camera.
  - iv. Tap the push notification to connect the device to your network.

#### 04 / CONNECTED DEVICES



	ork Devices	Devices 3 Devices 3 All		
Ver	erizon Router 🗸 🗸	Add a new device to Wi-Fi	$\boxtimes$	Add Device
Hom	ne	Network Type		
WI-F	FI ~	Primary V OR Code		
Devi	ntces ^	Vii-Fi Name Verizon_Z7KXTL		
Dev	nices 2	Wi-Fi Password	5	
Pan	rental Controls 0	mew3-jobs-adopt	2	
Syst	tem ~	Enabled Startwoo	6	
		If your olient device has a WPS button, press it and adak the butter hadren to clast WPS	8.	(Clear list)
		registration Book to state W S Hold the devices camera up to the GR Code	he	
		Tap the notification to connect to network	o the	
			_	
		Don	Ne	

- v. You can add the new device to your Wi-Fi network using the WPS option if your Wi-Fi device supports the WPS feature. Refer to "3.1d/ Wi-Fi Protected Setup (WPS)" on page 50.
- vi. Click Done to save the changes.
- 4. Click the **Block/Allow** option to quickly disable/enable a device from having internet access.

For additional information about blocking websites, refer to "Setting Parental Controls" on page 67.

## **DEVICE SETTINGS**

5. Click the Settings icon to access the **Device Settings** page for that device:

work Devices		Devices > Devices > Device Settings			
Verizon Router	$\sim$	Device Settings			
ome					
I-FI	~	Device Information Edit			
vices	^	Device		Name	
levices	2	Online Extender		E3200-b8f85384e668	
arental Controls	0			Host Name	
	-			E3200-b8f85384e668	
stem	Ŷ			Location	
				Select V	
				Mobility	
				Portable	×
		Device Add-Ons			
		Port Forwarding N/A	8	DMZ host N/A	0
		Access Control	0	DNS Server	8

vork Devices		Devices > Devices > Device Settings		
/erizon Router	$\sim$	Device Settings		
me				
-FI	Ý	Device Add-Ona		
vices	^	N/A State St	N/A	10
evices	2	Access Control	DNS Server N/A	¢.
arental Controls	0	Device Connection		
stem	Ý	Connection Info	Network Info	
		Connection Ethernet	Mao Address b8:f8:53:84:e6:68	
		Phy Rate / Modulation Rate 1000 Mbps	Connected to CR1000B	
			IPv4 Address 192.168.1.100	
			Subnet Mask 255.255.255.0	
			IPv4 DNS 192.168.1.1	
			Ipv4 Address Allocation	



verizon Basic Advanc	ed	Help	® ~
Verizon Router	Devices > Device Softings Device Settings		
Home			_
WI-FI ~	Ipv4 Address Allocation Dynamic		
Devices ^	Lease Type DHCP		
Devices 2	DHCP lease time remaining 1224 minutes 27 seconds		
Parental Controls 0	IPv6 LAN Prefix 0/0		
System ~	IPv6 Global		
	IPv6 Type / Address Allocation Stateless		
	IPv6 link-local ::		
	IPv6 DNS		
	Network Connection Bridge		
	Ping Test Test Connectivity 4 <sup>1</sup> m		
/monitoring/diagnostics	Time on the network 3 hourts) 34 minutes 25 seconds		-

- Device Information:
  - Device Type, Name/Host Name, Location, and Mobility

     Displays the current known information of the device.
     These can be updated or corrected as needed. Click Edit and Save to apply any changes.
  - This section also provides the device MAC Address, Access Point information the device is connected to as well as the IPv4 Address of the device.
- Device Add-Ons

**Port Forwarding** - Port Forwarding allows your network to be exposed to the internet in specific limited and controlled ways. For example, you could allow specific applications, such as gaming, voice, and chat, to access

## **DEVICE SETTINGS**

servers in the local network. To access the Port Forwarding page, click the setup button.

For additional information, refer to the Port Forwarding section in Chapter 5 Configuring Advanced Settings.

Access Control - Access Control restricts access from the local network to the internet. To access the Access Control page, click the setup button.

For additional information, refer to the Access Control section in Chapter 5 Configuring Advanced Settings.

**DMZ host** - DMZ host allows a single device on your primary network to be fully exposed to the internet for special purposes such as internet gaming. To access the DMZ host page, click the setup button.

For additional information, refer to the section in Chapter 5 Configuring Advanced Settings.

**DNS Server** - DNS Server manages the DNS server host name and IP address. To access the DNS Server page, click the setup button.

For additional information, refer to the section in Chapter 5 Configuring Advanced Settings.

#### Device Connection

This section displays Connection information of how and how well the device is connected to the Access Point. It also displays the Network related information, including IPv6 addresses and a **Ping Test** option.

#### **4.1/ SETTING PARENTAL CONTROLS 4.1a/ ACTIVATING PARENTAL CONTROLS**

You can create a basic access policy or using the provided **Rule Templates** for any computer or device on your Verizon Router network. Parental controls limit internet access to specific websites based on a schedule that you create.

Access can be limited on specific websites or keywords embedded in a website. For example, you can block access to the 'www. anysite.com' as well as block any website that has the word 'any' in its site name.

work Devices	Devices > Pi	arental Controls > All				
Verizon Router	~					
ome	Pare	ntal Controls			•	New Rule
I.FI	Home No	twork Protection				Get app no
	Get more rot Start using if	oust security features to protect you today on the My Fios app.	ur devices in your home or b	usiness.		
FVICES	n Darla Tar					
levices		ipiates				
arental Controls	1 Bedtime	Schoo	ol Day	Off Limits		
stem	V No Wi-Fi 9pm - 8am	School : 8am - 3	Sites Only pm	Blocked Sites Always on		
		>	>	>		
	Active R	ules				
	test	All Internet ON	A040		Enabled 🚺	Remove Edit

To limit device access:

1. From the **Basic** menu, select **Devices** from the left pane and then click **Parental Controls**.

## SETTING PARENTAL CONTROLS

- 2. To use the default **Rule Templates**, select one of the predefined rules as shown on screen to quickly setup access policy for devices on your network.
- 3. To create a new access policy, click on the **New Rule** and the configuration page displays.

verizon Basic	Advance	rd	Hele & ~
Network Devices	~	Devices > Parental Controls > All	Apply Changes
Home		Create new Rule	<u></u>
WI-FI	~	Name test	User defined V
Devices	^		Update Schedule
Devices	2	Condition	Devices User defined
Parental Controls	0		
System	~	Devices	
		Devices	Action
		A040	Bemove
		Add Exceptions	Add Devices

- 4. Create a rule name.
- 5. Create a schedule by selecting **User defined** from the dropdown list.

uter	~	Create	New Rule			
		Name	Assign schedule to this rule	2	×	
			Sun Mon Tue Wed Thu	Fri Sat		
introls	2	Select	Start Time End Ti	me		
and of the second se	Ý	Add Excepti	12:00 am V 12:0	0 am	<u> </u>	
			Apply			

- 6. Select the days of the week when the rule will be active or inactive.
- 7. Set the time when the rule will be active or inactive, then specify the start time and end time.
- 8. Click Apply to save changes.
- 9. Select the **Condition** rule of **Internet is always off/Internet is always on** to block/allow the access to all internet websites.
- Create the Devices rule by selecting User defined from the dropdown list and select the computers or clicking Add Devices to add a device where you are limiting access.

s uter N		Devices > Parer	Assign devic	es to this rule		×	
			묘 A040		PC		
		test					Update
introls	2	Condition Select					
		Add Excepti					Add t
				Apply			

- 11. Click Apply to save changes.
- 12. To remove a device from the list, click **Remove** to the assigned device.

## SETTING PARENTAL CONTROLS

- 13. Click Add Exceptions for the following exception options:
  - Enter the name of the website or keywords within a URL to block/allow the specified websites and websites with names containing the specified keyword.

		Create	e New Rule		Apply Cl
			Add exceptions	$\boxtimes$	
			Websites		
				+	Updates
	2	Internet is alw	Enter a URL like www.example.com Keywords		
ntrols	0	Devices		+	
			Enter a word that appears within a URL		
		Devices	Apply		
		A040			

14. Click Apply to save changes.

#### 4.1b/ ACTIVE RULES

You can view the rules created for your Verizon Router shown on the **Parental Controls** page.

	Devices > Par	ental Controls > All			
Verizon Router	~ _			4	
	Parer	ntal Controls			New Rule
Alle					
-FI	Home Net	twork Protection			Get app now
vices	Start using it b	oday on the My Flos app.	tes in your nome or business.		
Nevices	2 Rule Temp	Rule Templates			
arental Controls	1 Bedtime	School Day	Off Limite		
stem	V No.WI-FI	School Sites O	nly Blocked Sites		
	0pm - 8am	8em - 3pm	Always on		
		>	>	>	
	Active Ru	les			

## 4.2/ UNIVERSAL PLUG & PLAY

You can use Universal Plug and Play (UPnP) to support new devices without configuring or rebooting your Verizon Router.

In addition, you can enable the automatic cleanup of invalid rules. When enabled, this functionality verifies the validity of all UPnP services and rules every five minutes. Old and unused UPnP defined services are removed, unless a user-defined rule depends on it.

UPnP services are not deleted when disconnecting a computer without proper shutdown of the UPnP applications, such as messenger. Services may often not be deleted and eventually this leads to the exhaustion of rules and services. No new services can be defined. The cleanup feature locates the invalid services and removes them, preventing services exhaustion.

To access this setting:

1. From the Advanced menu, select Devices from the left pane and then click Universal Plug & Play.

verizon Basic	Advance	t Hale @~
Network Devices		Devices > Universal Plug & Play
Verizon Router	$\sim$	
Home	^	Universal Plug & Play Apply Changes
Wi-Fi	•	Universal Plug and Play provides the ability for the router to have new UPnP supported devices connected without having to reconfigure or reboot the router.
Devices	^	VPnP Enabled
Devices	2	
Parental Controls	o	Enable Automatic Cleanup of Old Unused UPnP Services
Universal Plug & Play		
Security & Firewall	×	

## **UNIVERSAL PLUG & PLAY**

- 2. To enable UPnP and allow UPnP services to be defined on any network hosts, select the **UPnP Enabled** check box.
- To enable automatic cleanup of invalid rules, select Enable Automatic Cleanup of Old Unused UPnP Services check box.
- 4. Click Apply changes to save changes.
# CONFIGURING ADVANCED SETTINGS

- 5.0 Security & Firewall
- 5.1 Network Settings
- **5.2** Diagnostics & Monitoring
- 5.3 System

Advanced settings cover a wide range of sophisticated configurations for your Verizon Router's firmware, security setup and network.

Verizon Router's security suite includes comprehensive and robust security services, such as stateful packet inspection, firewall security, user authentication protocols, and password protection mechanisms.

These and other features help protect your computers from security threats on the internet.

# This chapter covers the following advanced features:

## Security & Firewall

- General Firewall select the security level for the firewall.
- Access Control restrict access from the local network to the internet.
- DMZ Host allows a single device on your primary network to be fully exposed to the internet for special purposes such as internet gaming.
- IPv6 Pinholes provide access tunnel to a service on a host for a particular application.
- Port Forwarding enable access from the internet to specified services provided by computers on the local network.
- Port Forwarding Rules displays port forwarding rules.
- Port Triggering define port triggering entries to dynamically open the firewall for some protocols or ports.
- Scheduler Rules Settings limits the activation of firewall rules to specific time periods.
- SIP ALG supports the Application Layer Gateway for Session Initiation Protocol.

#### 76

### **Network Settings**

- ARP Table displays active devices with their IP and MAC addresses.
- DNS Server manages the DNS server host name and IP address.
- Dynamic DNS allows a static domain name to be mapped to the dynamic IP address.
- IPv4/IPv6 Address Distribution adds computers configured as DHCP clients to the network.
- IPv6 enables IPv6 support.
- MAC Cloning clones the MAC address.
- NDP (Neighbor Discovery Protocol) Table displays active devices with their IPv6 and MAC addresses of DHCP connection.
- Network Connections displays and manages the details of a specific network connection.
- Network Objects defines a group, such as a group of computers.
- Port Configuration sets up the Ethernet ports as either full- or half-duplex ports, at either 10 Mbps, 100 Mbps, or 1000 Mbps.
- Routing manages the routing and IP address distribution rules.
- Static NAT allow multiple static NAT IP addresses to be designated to devices on the network.

**Diagnostics & Monitoring** - performs diagnostic tests and displays the details and status of:

- Bandwidth Monitoring
- System Logging
- Full Status/System wide Monitoring of Connections/Traffic Monitoring
- Backhaul Logging

## **Advanced System Settings**

- Date & Time Settings sets the time zone and enables automatic time updates.
- Factory Reset resets your Verizon Router to its default settings.
- LED Brightness controls the Router Status LED light to either dim or brighten.
- Reboot Router restarts your Verizon Router.
- Remote Administration enable remote configuration of your Verizon Router from any internet-accessible computer.
- System Settings sets up various system and management parameters.

The firewall is the cornerstone of the security suite for your Verizon Router. It has been exclusively tailored to the needs of the residential or office user and is pre-configured to provide optimum security.

The firewall provides both the security and flexibility that home and office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as internet gaming and video conferencing.

Additional features, including surfing restrictions and access control, can also be configured locally through the user interface or remotely by a service provider.

The firewall regulates the flow of data between the local network and the internet. Both incoming and outgoing data are inspected, then either accepted and allowed to pass through your Verizon Router or rejected and barred from passing through your Verizon Router, according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing local network users access to internet services.

The firewall rules specify the type of services on the internet that are accessible from the local network and types of services in the local network that are accessible from the internet.

Each request for a service that the firewall receives is checked against the firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, all subsequent data associated with this request or session is also allowed to pass, regardless of its direction.

For example, when accessing a website on the internet, a request is sent to the internet for this site. When the request reaches your Verizon Router, the firewall identifies the request type and origin, such as HTTP and a specific computer in the local network. Unless your Verizon Router is configured to block requests of this type from this computer, the firewall allows this type of request to pass to the internet.

When the website is returned from the web server, the firewall associates the website with this session and allows it to pass; regardless HTTP access from the internet to the local network is blocked or permitted. It is the origin of the request, not subsequent responses to this request, which determines whether a session can be established.

# **5.0a/ SETTING FIREWALL CONFIGURATION**

You can select a normal, high, or low security level to limit, block, or permit all traffic. The following table shows request access for each security level.

Security Level	Internet Requests Incoming Traffic	Local Network Requests Outgoing Traffic
High	Blocked	Limited
Normal	Blocked	Unrestricted
Low	Unrestricted	Unrestricted

The request access is defined as:

- Blocked traffic no access allowed, except as configured in Port Forwarding and Remote Access
- Limited permits only commonly used services, such as email and web browsing
- Unrestricted permits full access of incoming traffic from the internet and allows all outgoing traffic, except as configured in Access Control

## SPECIFYING GENERAL SETTINGS FOR IPV4 OR IPV6

To set your firewall configuration:

 From the Security & Firewall General settings page, click on desired IPv4 settings/IPv6 settings option to configure IPv4/ IPv6 security.

etwork Devices		Securit	ty & Firewall > General		
Verizon Router	$\sim$	~			
Home	Â	Ge	eneral		
Wi-Fi	v	IPv4	Settings		
Devices	÷	0	High Security Remote administration will overide the security inbound	O Inbound Rule	🚫 Outbound Rule 🗸
Security & Firewall	^		policy		
General	- 1		Outbound Set Top Box Traffic disabled		
Access Control	- 1		Normal Security	<b>O</b>	<b>0</b> • • • • • • •
DMZ Host	- 1	۲	Remote administration will overide the security inbound policy		
IPv6 Pinholes					
Port Forwarding		0	Lew Security Remote administration will overide the security inbound policy	Inbound Rule	Outbound Rule
Port Forwarding Bules					

- 2. Select a security level by clicking one of the radio buttons. Using the **Low Security** setting may expose the local network to significant security risks, and should only be used for short periods of time to allow temporary network access.
- 3. Click Apply Changes to save changes.

# 5.0b/ ACCESS CONTROL

You can block individual computers on your local network from accessing specific services on the internet. For example, you could block one computer from accessing the internet, then block a second computer from transferring files using FTP as well as prohibit the computer from receiving incoming email.

Access control incorporates a list of preset services, such as applications and common port settings.

# **ALLOW OR RESTRICT SERVICES**

To allow or restrict services:

 From the Advanced menu, select Security & Firewall from the left pane and then click Access Control. The Access Control page opens with the Allows and Blocked sections displayed. The Allowed section only displays when the firewall is set to maximum security.

verizon Basic	Advance	d				Hele Q ~
Network Devices		Security & Firewall > Access C	ontrol			
Verizon Router	~	Access Co	ntrol			
Home	Î					
Wi-Fi	×	Block access to the Internet	services from within the Home Network (	LAN).		
Devices	×	Create Rule				
Security & Firewall	^	Networked Device	Network Address	Protocols	Status	Action
General	- 1		Y	ou have no rules.		
Access Control	- 1					
DMZ Host		Add				
IPv6 Pinholes						

2. To block a service, click Add. The Add Access Control page displays.

verizon Basic	Advance	d -	Hele	®~
Network Devices		Security & Firewall > Access Control > Create rule		
Verizon Router	$\sim$	Assess Control		
Home	*	Access Control		
Wi-Fi	÷	Biock access to the Internet services from within the Home Network (LAN).		
Devices	~	Add Access Control		
Security & Firewall	^	Networked Device Any ~		-
General	- 1			
Access Control		Protocol Any ~		
DMZ Host		When should rule occur?		
IPv6 Pinholes		Always		
Port Forwarding		Cancel User Defined		

©2022 Verizon. All Rights Reserved

- **3**. To apply the rule to:
  - Networked Computer/Device select Any.
  - Specific devices only select User Defined.
- 4. In the Protocol field, select the internet protocol to be allowed or blocked. If the service is not included in the list, select User Defined. The Edit Service page displays. Define the service, then click Apply. The service is automatically added to the Add Access Control section.
- 5. Specify when the rule is active as **Always** or **User Defined**.

verizon Basic	Advance	ed										Helo	@ ~
Network Devices	_	Security & Firewall > Access Con	trol > Create ru	le									
Verizon Router	~	Access Con	trol										
Home	^	Accession											
Wi-Fi	~	Block access to the Internet set	vices from with	in the Hon	ne Netwo	rk (LAN).							
Devices	~	Set Rule Schedule											
Security & Firewall	^	Rule name:											
General	- 1	Rule days:	Sun	Mon	Tue	Wed	Thu	Fri	Sat				
Access Control	- 1		Start Ti	me			End Tim	ie .					
DMZ Host		Rule time:	9:00 p	m		~	12:00	am		~			
IPv6 Pinholes			RL     R	ile will be	active du	ring sche	duled tim	e					
Port Forwarding			O Ru	ule will be i	inactive	during sol	neduled ti	me					
Port Forwarding Rules													
Port Triggering		Cancel	Apply										

- 6. Enter the rule name, specify days of the week, and set the start time and end time when the rule will be active or inactive.
- 7. Click **Apply** to save changes.
- 8. The Access Control page displays a summary of the new access control rule.

# DISABLE ACCESS CONTROL

You can disable an access control and enable access to the service without removing the service from the Access Control table. This can make the service available temporarily and allow you to easily reinstate the restriction later.

- To disable an access control, clear the check box next to the service name.
- To reinstate the restriction, select the check box next to the service name.
- To remove an access restriction, select the service and click **Remove**. The service is removed from the Access Control table.

# 5.0c/ DMZ HOST

DMZ Host allows a single device on your primary network to be fully exposed to the internet for special purposes like internet gaming.

*Warning:* Enabling DMZ Host is a security risk. When a device on your network is a DMZ Host, it is directly exposed to the internet and loses much of the protection of the firewall. If it is compromised, it can also be used to attack other devices on your primary network.

Follow these steps to designate a device on your primary network as a DMZ Host:

- 1. From the Advanced menu, select Security & Firewall and then click DMZ Host.
- 2. Select **Enable** for the DMZ Host.

3. Enter the IP address or select the MAC address of the device you want to designate as the DMZ Host.

verizon Basic	Advance	d		Hele Q ~
Network Devices		Security & Firewall > DMZ Host		
Verizon Router	$\sim$	DMT		
Home	^	DIVIZ HOSt		
Wi-Fi	÷	How it works	second to the	
Devices	÷	Internet.		
Security & Firewall	^	DMZ IPv4 Host	Disabled	
General		Local Host	192.168.1. V	
Access Control	- 1			
DMZ Host		Address	192 168 1 0	
IPv6 Pinholes		DMZ IPv6 Host	Disabled	
Port Forwarding				
Port Forwarding Rules		Local Host	NOTETICA *	
Port Triggering	-	Address		

4. Click Apply Changes to save changes.

# 5.0d/ IPV6 PINHOLES

The IPv6 Pinhole feature of the Verizon Router allows an application to send incoming packets for a certain port number to the destination computer by setting up the rule of authorization.

To configure the rules:

1. From the Advanced menu, select Security & Firewall and then click IPv6 Pinhole.

#### 05 / CONFIGURING ADVANCED SETTINGS



	verizon Basic	Advanced		FTP (File Transfer)
	Network Devices Verizon Router	~	Security & Firewall > IPv6 Pinholes	HTTP (Web Server) HTTPS (Secured Web Server)
	Home	ŕ	IPv6 Pinholes	IMAP (Messaging Server) L2TP (Layer Two Tunneling Protocol)
	Wi-Fi	~	How it works	POP3 (Incoming Mail)
	Devices	v	Open a tunnel between remote computers and a device port on your Home Net gaming, IoT, home security devices and more.	SMTP (Outgoing Mail) SNMP (Simple Network Management Protocol)
	Security & Firewall	^	Create Rule	Telnet (Remote Connection)
	General		External Host Internal Host Protocol	TFTP (Trivial File Transfer Protocol)
	Access Control		Select external hos Y Select Internal host Y TCP Y	Select applicative Always Add to list
	DMZ Host		Bulaa List	
I.	IPv6 Pinholes		Rules List	Annliesting (Anat Cakedula
	Port Forwarding		External must Protocol	Application/Port ocleane
	Port Forwarding Rules			
	Port Triggering			

- 2. Select external and internal host, protocol and the application port type.
- 3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
- 4. Click Add to list. The screen displays opened pinhole port and its status. It shows the IP addresses of remote device and connected device on your network.
- 5. Click **Apply Changes** to save changes.

## 5.0e/ PORT FORWARDING

You can activate port forwarding to expose the network to the internet in a limited and controlled manner. For example, enabling applications, such as gaming and voice, to work from the local network as well as allowing internet access to servers within the local network.

To create port forwarding rules:

1. From the Advanced menu, select Security & Firewall from the left pane and then click Port Forwarding. The Port Forwarding page opens with the current rules displayed.

verizon <sup>4</sup> Basic	Advance	d							Hele	®~
Network Devices		Security & Firewall >	Port Forwarding							
Verizon Router	$\sim$	- ·-								
Home	^	PortFo	rwardin	g						
Wi-Fi	v	Open a tunnel betw	reen remote compute	ers and a o	levice port on	your Home Network	(LAN). Supports ga	iming, IoT, home secu	urity devices and more.	_
Devices	v	Create Rule								
Security & Firewall	^	Application			Original Po	rt		Protocol		
General	- 1				0000			Select	×	/
Access Control	- 1	Fwd to Addr			Fwd to Por	ı		Schedule		
DMZ Host	- 1	Select		~	0000			Select	`	_
IPv6 Pinholes									Add to list	
Port Forwarding		Rules List								
Port Forwarding Rules		Application	Original Port	Proto	col	Fwd to Addr	Fwd to Port	Schedule		
Port Triggering			4567	TCP		127.0.0.1	4567	Always		
	-		4677	TCP		127.0.0.1	4577	Always		

- 2. To create a new rule, enter the application name, configure its inbound and outbound port numbers, forwarding destination address, then select the protocol.
- 3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
- 4. Click Add to list. The rule displays in the Rules List section.
- 5. Click Apply Changes to save changes.

# **5.0f/ PORT FORWARDING RULES**

You can view, modify, and delete port forwarding rules.

To access the rules:

1. Select **Port Forwarding Rules** in the **Security & Firewall** section.

verizon Basic	Advance	d		н	11 Q	v
Network Devices		Security & Firewall > Port Forwarding Rules				
Verizon Router	$\sim$					
Home		Port Forwarding Ru	les			
Wilei		Below is a list of currently configured Protocols the	at are implemented in the router.			
		HTTPS	TCP Any $\rightarrow$ 443	Edit	Remove	
Devices	×	IMAP	TCP Any $ ightarrow$ 143	Edit	Bemove	
Security & Firewall	^	L2TP	UDP Any $ ightarrow$ 1701	Edit	Remove	
General	- 1	Ping	ICMP Echo Request	Edit	Remove	
Access Control	- 1	POP3	TCP Any $\rightarrow$ 110	Edit	Bemove	
DMZ Host	- 1	SMTP	TCP Any $ ightarrow$ 25	Edit	Remove	
		SNMP	UDP Any $\rightarrow$ 161	Edit	Remove	
IPV6 PINNoles		Teinet	TCP Any $\rightarrow$ 23	Edit	Remove	
Port Forwarding		IFTP	UDP 1024 - 65535 $\rightarrow$ 69	Edit	Bemove	
Port Forwarding Rules		Traceroute	UDP 32769 - 65535 $\rightarrow$ 33434 - 33523	Edit	Remove	
Port Triggering		Add new				

2. To create or edit a protocol rule, click the **Add new** or **Edit** icon in the action column. The **Edit Service** page displays.

verizon <sup>4</sup> Ba	asic	Advance	rd Hair @ ~
Network Devices			Security & Firewall > Port Forwarding Rules > Edit Service
Verizon Router		~	Edit Service
Home		<u>^</u>	
Wi-Fi		v	Edit Service
Devices		×	Service Name
Security & Firewall		^	Service Description
General			Service Ports
Access Control		. 1	
DMZ Host		- 1	Add
IPv6 Pinholes			
Port Forwarding			Cancel
Port Forwarding Rul	es		

- 3. Modify the Service Name and Service Description, as needed.
- 4. To add server ports, click Add.
- 5. To modify the current protocol, click the **Edit** icon in the action column. The **Edit Service Server Ports** page displays.

verizon Basic	Advance	d			Help	®~
Network Devices		Security & Firewall > Port Forwarding Rul	les > Edit Service			
Verizon Router	~	Edit Service				
Home Wi-Fi	•	Edit Service Server Ports				_
Devices	×	Protocol	тср	~		
Security & Firewall	^	Source Ports	Any	~		
General	- 1	Destination Ports	Any	~		
Access Control	- 1					
DMZ Host		Cancel	pply			
IPv6 Pinholes						
Port Forwarding						
Port Forwarding Rules						

- 6. Enter the **Protocol, Source Ports** and **Destination Ports**, as needed.
- 7. Click Apply to save changes.

# 5.0g/ PORT TRIGGERING

Port triggering can be described as dynamic port forwarding. By setting port triggering rules, inbound traffic arrives at a specific network host using ports that are different than those used for outbound traffic. The outbound traffic triggers the ports where the inbound traffic is directed.

For example, a gaming server is accessed using UDP protocol on port 2222. The gaming server then responds by connecting the user using UDP on port 3333, when a gaming session is initiated.

In this case, port triggering must be used since it conflicts with the following default firewall settings:

- Firewall blocks inbound traffic by default.
- Server replies to your Verizon Router IP, and the connection is not sent back to the host since it is not part of a session.

To resolve the conflict, a port triggering entry must be defined, which allows inbound traffic on UDP port 3333 only after a network host generated traffic to UDP port 2222. This results in your Verizon Router accepting the inbound traffic from the gaming server and sending it back to the network host which originated the outgoing traffic to UDP port 2222.

## To configure port triggering:

1. From the Advanced menu, select Security & Firewall and then click Port Triggering.

letwork Devices		Security & Firewall	> Port Triggering				
Verizon Router	$\sim$						
	*	Port Tr	iggering				
Security & Firewall	^	Open a tunnel bet	ween remote computers and a	device port on your	Home Network (LAN). Support	s gaming, IoT, home se	curity devices and more.
General	- 1	On the Darks					
Access Control	- 1	Create Rule					
DMZ Host	- 1	Application	Triggered Port Range	Protocol	Forwarded Port Range	Schedule	
	- 1		Start End		Start End		
IPv6 Pinholes	- 1			TCP	×	Always	✓ Add to 1
Port Forwarding	- 1	Rules List					
Port Forwarding Rules	- 1				Formated Part		
Port Triggering		Application	Triggered Port Range	Protocol	Range	Schedule	Enable
				You have n	o rules. Add a rule above.		

- 2. To add a service as an active protocol, enter the application name, configure its inbound and outbound (triggered/ forwarded) port range, then select the protocol.
- 3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
- 4. Click Add to list. The rule displays in the Rules List section.
- 5. Click **Apply Changes** to save changes.

# 5.0h/ SCHEDULER RULES

**Scheduler Rules** are used for limiting the activation of firewall rules to specific time periods. The time periods are either for days of the week or for hours of each day based on activity or inactivity.

To define a rule:

1. Verify that the date and time of your Verizon Router is correct.



2. Select Scheduler Rules in the Security & Firewall section.

verizon	Basic	Advan	ced					Helo	®~
Network Devices			Security & Firewall	> Scheduler Rules					
Verizon Rout	er	$\sim$							
			Sched	uler Rules					
Security & Fin	ewall	^	Scheduler rules ar	e used for limiting the acti	vation of firewall ru	es to specific time periods, eithe	r for days of the week, or for hours of each	day.	
General		- 1	Rule Name	Settings			Status		
Access Contr	ol		Add						
DMZ Host			4						
IPv6 Pinholes									
Port Forwardi	ng								
Port Forwardi	ng Rules								
Port Triggerin	0								
Scheduler Ru	les								
SIP ALG									
Network Setti	ngs	ν.	-			Copyright © 2021 Verizon			

3. Click Add. The Rule Schedule page displays.

verizon <sup>4</sup> Basic	Advance	d		Hela Q ~
Network Devices		Security & Firewall > Scheduler Rules >	Pule scheduler	
Verizon Router	~	Bula Cabadula	Appl	v Changes
	^	Rule Schedule		
Security & Firewall	^	Rule name:		
General	- 1			
Access Control	- 1	Rule days:	Sun Mon Tue Wed Thu Pri Sat	
DMZ Host	- 1	Rule time:	Start Time         End Time           7:00 am         7:00 pm         0	
IPv6 Pinholes	- 1		Rule will be active during schedul	
Port Forwarding	- 1		1:00 am	
Port Forwarding Rules	- 1		Rule will be inactive during sched 2:00 am	
Dest Tripperior	- 1		3:00 am	
Fortinggering			4:00 am	
Scheduler Rules			5:00 am	
SIPALG			6:00 am	
Network Settings	v .		Copyright © 202 7:00 am	

4. Enter the name of the rule, select the active or inactive days of the week and the start and end time range.

- 5. Specify if the rule is **active** at the scheduled time or **inactive** at the scheduled time.
- 6. Click Apply changes to save changes.

# 5.0i/ SIP ALG

SIP ALG (Application Level Gateway) - supports various multiple application protocols by allowing dynamic ephemeral TCP/ UDP ports to communicate with the known ports which a particular client application (such as FTP, VoIP service, net meeting or streaming media) requires.

To enable the SIP ALG settings:

- 1. From the Advanced menu, select Security & Firewall and then click SIP ALG.
- 2. Select Enabled for the SIP ALG.

	verizon <sup>4</sup> Basic	Advanced	Hele ® ~
	Network Devices		Security & Firewall > SIP ALG
	Verizon Router	$\sim$	
		*	SIP ALG
	Security & Firewall	^	How it works
	General	- 1	Manage the Application Layer Gateway for Session Initiation Protocol
	Access Control	- 1	
	DMZ Host	- 1	SIP ALG
	IPv6 Pinholes	- 1	
	Port Forwarding	- 1	
	Port Forwarding Rules	- 1	
	Port Triggering		
	Scheduler Rules		
Ì	SIPALG		
	Network Settings		Copyright © 2021 Verizon

3. Click Apply Changes to save changes.

# **5.1/ NETWORK SETTINGS 5.1a/ ARP TABLE**

You can view the IPv4 and MAC addresses of each DHCP connection.

*To view the IPv4 and MAC addresses for each device:* From the **Advanced** menu, select **Network Settings** and then click **ARP Table**.

verizon	Basic	Advanc	ed				Hele Q ~	
Network Devices			Network Settings	ARP Table				
Verizon Rou	Verizon Router 🗸 🗸							
Network Set	tings	^ <b>*</b>	ARP Ta	able			Refresh	
ARP Table			The ARP Table be	The ARP Table below displays the IPv4 and MAC address of each DHCP connection				
DNS Server		- 1	IPv4 Address	MAC Address	State	Device		
0		- 1	192.168.1.151		FAILED	Network (Home/Office)		
Dynamic DN	IS	- 1	192.168.1.152	48:5b:39:4f:56:08	REACHABLE	Network (Home/Office)		
IPv4 Addres	s Distribution	- 1	192.168.1.100	b8:f8:53:84:e6:68	REACHABLE	Network (Home/Office)		
IPv6		- 1						
IPv6 Addres	s Distribution	- 1						
MAC Clonin	a	- 1						
NDP Table								
Network Co	nnections							
Network Ob	jects				Copyright © 2021 Verizo	on		

# 5.1b/ DNS SERVER

You can edit the host name and/or IP address, if the host was manually added to the DNS table. If not, you can only modify the host name.

To access the DNS server:

1. From the Advanced menu, select Network Settings and then click DNS Server.

# **NETWORK SETTINGS**

etwork Devices		Network Settings > DNS Server			
Verizon Router	$\sim$				
Network Settings	^ <b>*</b>	DNS Server			
ARP Table		Add, edit, or delete computers known	n by the router's DNS server		
DNS Server		Host Name	IP Address	Source	
Dynamic DNS	- 1	E3200-b8f85384e668	192.168.1.100	DHCP	
IPv4 Address Distribution		A040025-NB2	192.168.1.152	DHCP	
IPv6		Add DNS Entry			
IPv6 Address Distribution		Enable DNS Rebind Protectio	n		
MAC Cloning		To disable DNS Rebind Protection fo To disable DNS Rebind Protection fo	r all devices connected to this route r specific IP addresses, create an ex	r, untick the checkbox above. ception with the dropdown below.	
NDP Table		Exceptions to DNS Rebind	Protection		
Network Connections					
Network Objects		IP/Netmask			

2. To disable DNS rebind protection for all devices connected to the Verizon Router, untick the check box of **Enable DNS Rebind Protection.** 

*Warning: Disabling this protection may create a risk of cybersecurity attack to devices connected to this router.* 

3. To add a computer stored in the DNS table, click Add DNS Entry. The DNS Entry page displays.

	verizon	Basic	Adva	nced		<u>Helo</u>	®~
Network Devices			Network Settings > DNS Server > DNS Server Setting				
	Verizon Router	r	$\sim$		RNO O		
	Network Settin	gs	^	•	DNS Server		
	ARP Table				DNS Entry		
l	DNS Server			i.	Host Name:		
	Dynamic DNS			L	IP Address: 0 0 0 0		
	IPv4 Address D	Nistribution		L			
	IPv6			L	Apply		
	IPv6 Address D	listribution		L			
	MAC Clonina			_			

- 4. In the **Host Name** field, enter the name of the computer, then enter the **IP address** and click **Apply** to save changes.
- 5. Then the **DNS Server** page displays.
- To add a new IP address entry, select the Add Exceptions Entry in the Exceptions to DNS Rebind Protection section. The Add Exceptions List page displays. Edit the IP address.
- 7. To remove a host from the DNS table, click the **Remove** icon on the screen.
- 8. Click **Apply changes** to save changes.

# **5.1c/ DYNAMIC DNS**

Typically, when connecting to the internet, your router is assigned an unused public IP address from a pool, and this address changes periodically.

Dynamic DNS allows a static domain name to be mapped to the dynamic IP address, allowing a computer within your network to be more easily accessible from the internet.

When using Dynamic DNS, each time the public IP address changes, the DNS database is automatically updated with the new IP address. In this way, even though the IP address changes often, the domain name remains constant and accessible.

To set up dynamic DNS:

1. Select **Dynamic DNS** in the **Network Settings** section.