



Verizon Business Internet Gateway **USER GUIDE**



CONTENTS

01/

INTRODUCTION

1.0	Inside the box	5
1.1	Getting to Know Your Verizon Business Internet Gateway	5
1.2	Setting Up Verizon Business Internet Gateway	10

02/

CONFIGURING YOUR VERIZON BUSINESS INTERNET GATEWAY

2.0	Configure Your Verizon Business Internet Gateway	17
2.1	Computer Network Configuration	21
2.2	Main Screen	27

03/

WI-FI SETTINGS

3.0	Overview	34
3.1	Basic Settings	35
3.2	Advanced Settings	43

04/

CONNECTED DEVICES

4.0	Device Settings	52
4.1	Setting Content Controls	56
4.2	Universal Plug & Play	60

05 /
**CONFIGURING ADVANCED
SETTINGS**

5.0	Security & Firewall	66
5.1	Network Settings	82
5.2	Diagnostics & Monitoring	126
5.3	System	132

06 /
TROUBLESHOOTING

6.0	Troubleshooting Tips	146
6.1	Frequently Asked Questions	153

07 /
SPECIFICATIONS

7.0	General Specifications	158
7.1	Connections	158

08 /
NOTICES

8.0	Regulatory Compliance Notices	161
8.1	Battery Safety Instructions	163

01/

INTRODUCTION

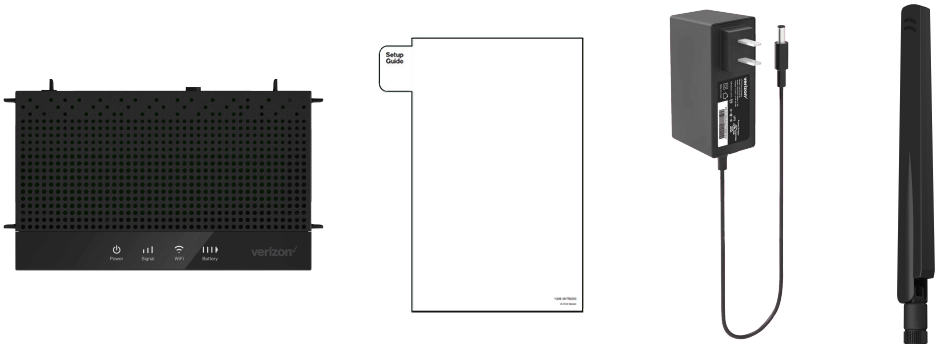
- 1.0** Inside the box
- 1.1** Getting to Know Your Verizon Business Internet Gateway
- 1.2** Setting Up Verizon Business Internet Gateway

INSIDE THE BOX

1.0/ INSIDE THE BOX

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

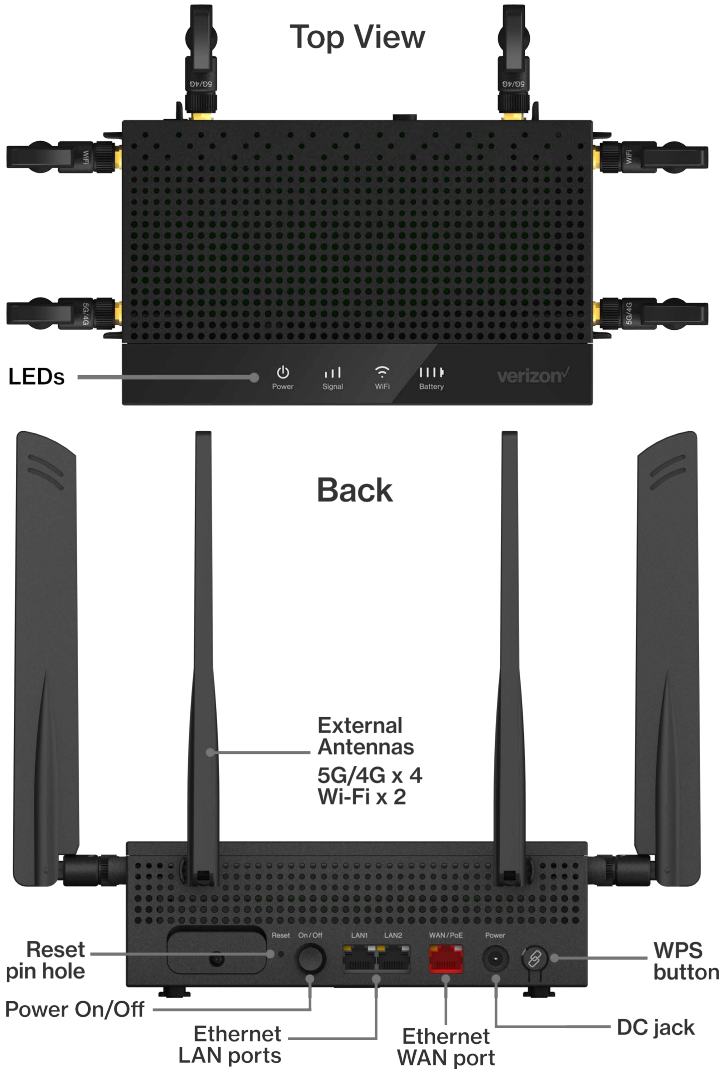
- Verizon Business Internet Gateway
- Setup guide
- Power adapter
- Paddle antenna - 5G/4G x 4, Wi-Fi x 2



1.1/ GETTING TO KNOW YOUR VERIZON BUSINESS INTERNET GATEWAY

Your Verizon Business Internet Gateway (Gateway) can be used as a wireless mobile hotspot and allows you to access Verizon's 5G/4G LTE network for fast apps, uploads and downloads. The Gateway also provides fast dual-band Wi-Fi (with channel steering) for all your devices, and features built-in network security as well as content controls, guest Wi-Fi and automatic software updates.

Take a moment to familiarize with your product:



GETTING TO KNOW YOUR VERIZON BUSINESS INTERNET GATEWAY

1.1a/ RESET PIN HOLE

The reset PIN hole allows you to reset the gateway back to its factory default state. Using the reset function will revert all settings and changes made during the setup process. To perform a factory reset and return the Verizon Business Internet Gateway to default settings, press and hold the reset PIN hole for 3+ seconds. The System LED will flash yellow to indicate a reset has been triggered, followed by fading in/out (white) while the gateway restarts.

1.1b/ WPS

WPS is an easy way to add supported Wi-Fi devices to your network. Press the WPS button on the back of the Gateway to activate WPS. You will need to activate WPS on your Wi-Fi device too. Refer to “3.1d/ Wi-Fi Protected Setup (WPS)” on page 40.

1.1c/ LEDS

The LEDs indicate the system and connection status, and WPS activity.

System LED

LED Mode	Status	LED Pattern
System Status (Power)		
Bootup	System booting	Soft blink white
	Firmware update	Fast blink white
Regular usage mode	Rest mode	Solid white
Wired WAN connectivity	In service	Solid blue
IP Passthrough mode	IPPT (IP Passthrough) enabled	Solid green

LED Mode	Status	LED Pattern
Other	Factory reset	Fast blink yellow
	Hardware error	Soft blink red
	No SIM card	Hard blink red
	No signal; not connected to Internet	Solid red

Signal Strength LEDs

LED Mode	Status	LED Pattern
Regular usage mode	Rest mode	50% dim white
3 bars ()	Excellent 5G or 4G coverage	Solid white
2 bars ()	Good 5G or 4G coverage	Solid white
1 bar ()	Weak 5G or 4G coverage	Solid white

Wi-Fi LED

LED Mode	Status	LED Pattern
		
Regular usage mode	Passing signal	Solid white
	Setup complete	Solid white
	Not connected to Internet	Solid red
	Rest mode	Solid dim white

GETTING TO KNOW YOUR VERIZON BUSINESS INTERNET GATEWAY

LED Mode	Status	LED Pattern
Pairing	Pairing WPS (in progress)	Hard blink blue
	WPS connection success	Fast blink blue
	WPS connection unsuccessful (time out)	Fast blink red
	WPS connection failure (interrupted)	Hard blink red
Other	Hardware error	Soft blink red

Battery LEDs

LED Mode	Status	LED Pattern
	More bars indicates more battery life	Solid white

Ethernet Port LEDs

Ethernet Port LED Mode	Status	Left LED	Right LED
Wired LAN connection * Threshold level can be decided based on port capability.	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

1.2/ SETTING UP VERIZON BUSINESS INTERNET GATEWAY

1.2a/ POSITIONING YOUR GATEWAY

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

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

1.2b/ CONNECTING EXTERNAL ANTENNAS

The Verizon Business Internet Gateway comes with six detachable antennas. To connect the external antennas:

1. Ensure the Gateway is powered off and unplugged from the power outlet.

SETTING UP VERIZON BUSINESS INTERNET GATEWAY

2. Connect the six antennas to their appropriate ports on the Gateway. Ensure the labels on the ports match those on the antenna labeled either Wi-Fi or 4G/5G. Please ensure the antennas are securely hand tightened for optimal performance.



3. For the best reception, position the antennas so that they are in an upright position as illustrated.



SETTING UP VERIZON BUSINESS INTERNET GATEWAY

1.2c/ SETTING UP

Before you begin, if you are replacing an existing gateway, disconnect it. Remove all old gateway components, including the power supply. They will not work with the new Verizon Business Internet Gateway.

1. Before you use your Verizon Business Internet Gateway, be sure to charge the battery for at least three hours to ensure a full initial charge.
 - i. It normally takes at least 3-5 hours with the wall charger to fully charge the battery.
 - ii. The battery discharges faster as additional devices connect with your Gateway.
 - iii. Battery life depends on the network, signal strength, temperature, features, and active connection time.
 - iv. When charging, keep your Gateway near room temperature.
 - v. Never leave the Gateway in an unattended vehicle due to uncontrolled temperatures that may be outside the desired temperatures for your Gateway.
 - vi. It is normal for batteries to gradually wear down and require longer charging time.
2. Place it on an elevated surface near a window.
3. Wait up to 15 minutes for the system light to turn off.

The light will blink white while the Gateway is powering on and updating software. Don't turn off the power to the Gateway.

If it turns solid red: No signal in this location. Move the Gateway to another location.

If it blinks red: Activation error. Power off the Gateway and turn it back on.

4. Check the signal strength. One signal bar is all you need, but you can try to find an even stronger signal by checking different areas.

5. Wait up to 15 minutes for the Wi-Fi light to turn on.

Once it lights up solid white, you're ready to connect your devices. If it blinks red: Activation error. Power off the Gateway and turn it back on.

6. Connect your network devices.

Connect to your new network using the Wi-Fi name and password printed on the bottom panel of the Gateway, or scan the QR code there to connect automatically.

02 /

CONFIGURING YOUR VERIZON BUSINESS INTERNET GATEWAY

- 2.0** Configure Your Verizon Business Internet Gateway
- 2.1** Computer Network Configuration
- 2.2** Main Screen

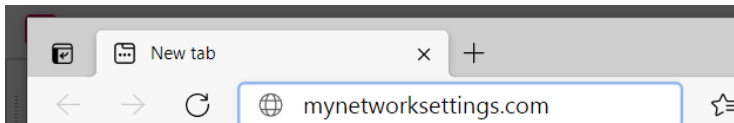
Connecting your Verizon Business Internet Gateway and accessing its web-based User Interface (UI) are both simple procedures.

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

CONFIGURE YOUR VERIZON BUSINESS INTERNET GATEWAY

2.0/ CONFIGURE YOUR VERIZON BUSINESS INTERNET GATEWAY

1. Open a web browser on the device connected to your Verizon Business Internet Gateway network.
2. In the browser address field (URL), enter: mynetworksettings.com (<https://192.168.0.1>), then press the **Enter** key on your keyboard.



3. You may see a security message warning that **Your connection is not private** when you visit <https://192.168.0.1> for GUI management. To get to the login screen, click the **ADVANCED** button, then on [Proceed to 192.168.0.1 \(unsafe\)](#) link.



Your connection is not private

Attackers might be trying to steal your information from **192.168.0.1** (for example, passwords, messages, or credit cards). [Learn more](#)

NET:ERR_CERT_AUTHORITY_INVALID

💡 To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced

Back to safety

This server could not prove that it is **192.168.0.1**: its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

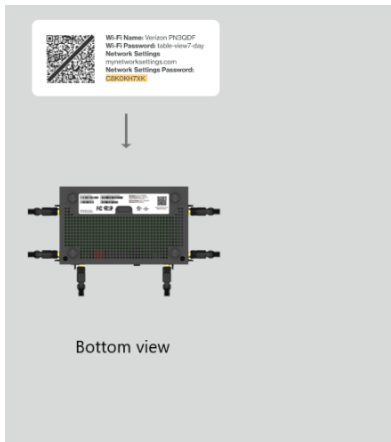
[Proceed to 192.168.0.1 \(unsafe\)](#)



4. The login screen will appear.

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

5. On the **Log in to Verizon Internet Gateway** screen, enter the password that is printed next to the **Network Settings Password** on the label on the bottom of your Gateway.



Log in to Verizon Internet Gateway

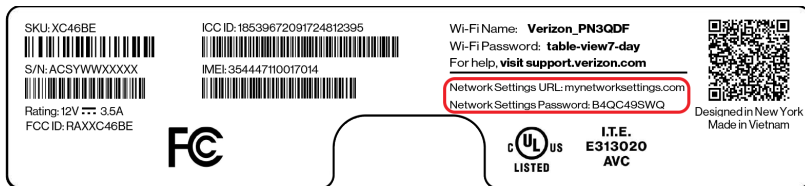
Enter the Network Settings Password located on the information sticker on your router.

Network Settings Password

☐ Keep Me Signed In ⓘ

Log in

Copyright © 2024 Verizon



CONFIGURE YOUR VERIZON BUSINESS INTERNET GATEWAY

- Click **Log In**. The **Change Wi-Fi name** screen displays. Move the selector to **on** for setting up your **Guest Wi-Fi** to personalize your Guest Wi-Fi Name and Password.

verizon

Help

Change Wi-Fi name

Wi-Fi Name
WLAN-123456

Wi-Fi Password

Guest Wi-Fi Enabled ☒

Guest Wi-Fi Name
WLAN-123456-Guest

Guest Wi-Fi Password

Minimum 8 characters

[Back](#) [Continue](#)

Copyright © 2024 Verizon

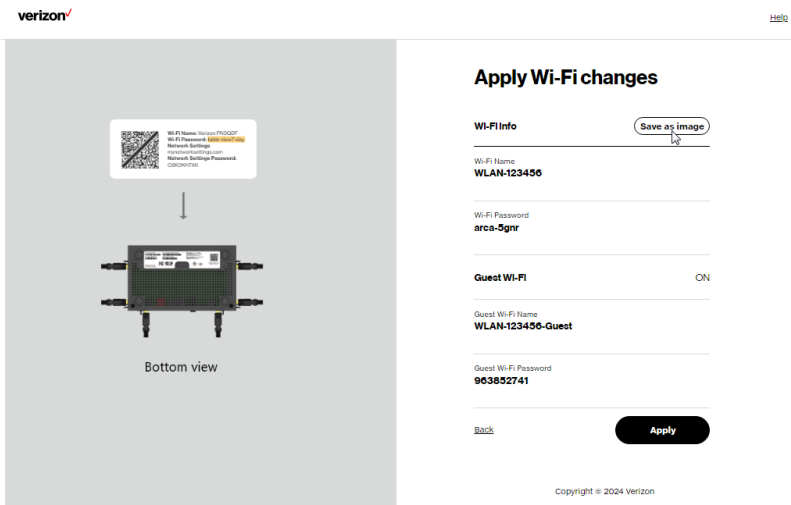
Bottom view

For your protection, your Gateway 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.

- 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 Gateway.

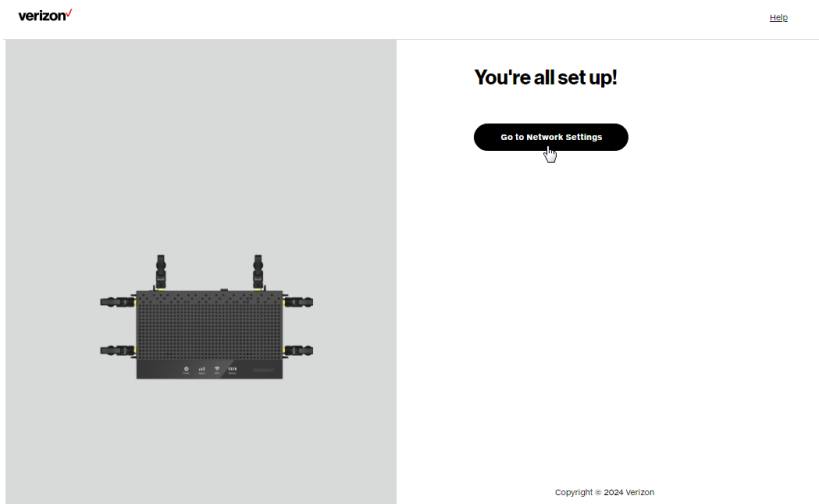
Note: If you select **Save as image**, the image file is saved to your web browser's download folder.

Important: If you are on a Wi-Fi device when setting up your Gateway, you will be disconnected from the Wi-Fi network when you change the Wi-Fi name or Wi-Fi password. When this occurs, your Gateway will detect this situation and prompt you to reconnect using the new settings.



The **You're all set up!** screen displays once your Gateway 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 Gateway.

CONFIGURE YOUR VERIZON BUSINESS INTERNET GATEWAY



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

If your Gateway 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.
4. 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**.
7. In the Local Area Connection Properties window, click **OK** to save the settings.
8. 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 Gateway configuration).

COMPUTER NETWORK 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.
6. 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.
10. 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 Gateway 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 Gateway to other computers or set top boxes using an Ethernet cable or Wi-Fi connection.

ETHERNET

1. Plug one end of an Ethernet cable into one of the Ethernet ports on the back of your Gateway.
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 Gateway using Ethernet.

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 Gateway creates a secure Wi-Fi network connection.

In most cases, this only requires the pressing of two buttons – one on your Gateway 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.

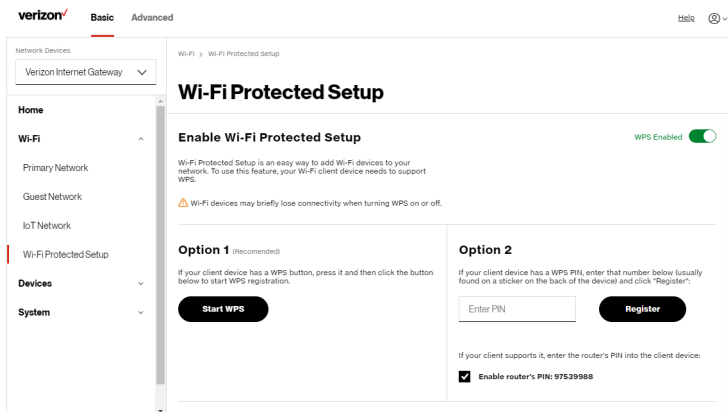
COMPUTER NETWORK CONFIGURATION

To initialize the WPS process, you can either press and hold the WPS button located on the bottom of your Gateway 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**.



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 Gateway for more than two seconds, then click the **Start WPS** button in **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 Gateway'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 Gateway, 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 Gateway is pressed, the Status LED on your Gateway begins flashing blue. The flashing continues until WPS pairing to the client device completes successfully. At this time, the Status LED turns solid blue.

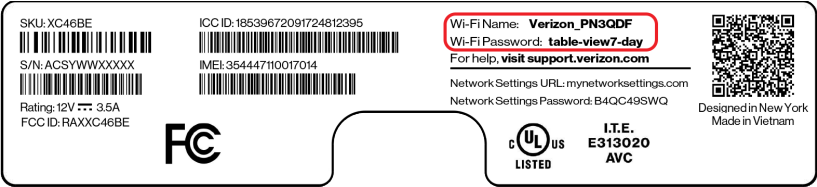
If WPS fails to establish a connection to a Wi-Fi client device within two minutes, the Status LED on your Gateway flashes red for two minutes to indicate the WPS pairing process was unsuccessful. After flashing red, the light returns to solid white to indicate that Wi-Fi is on.

***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 the Wi-Fi network name (SSID) of your Gateway from the device's list of discovered Wi-Fi networks.
4. When prompted, enter your Gateway's Wi-Fi password (WPA2 or WPA3 key) into the device's Wi-Fi settings. Your Gateway's default Wi-Fi network name and password are located on the sticker on the bottom of your Gateway.

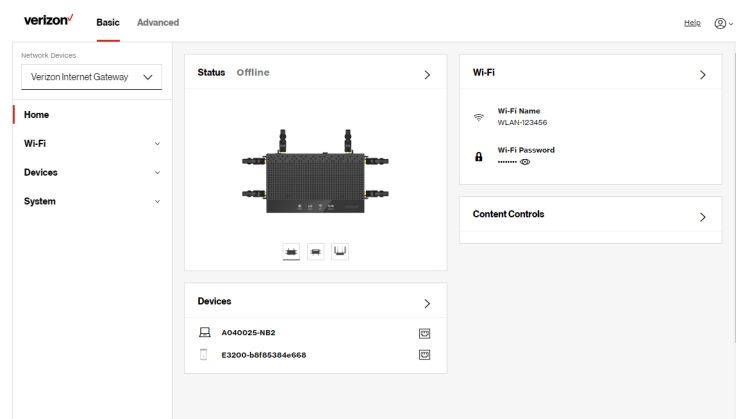
MAIN SCREEN



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 Gateway.

2.2/ MAIN SCREEN

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



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

2.2a/ SYSTEM

SYSTEM STATUS

To view the status:

1. Access the dashboard **Home** page.
2. You can quickly view your Gateway's status by clicking **System**
System Status on the screen. This section displays the status of your Gateway's local network (LAN) and internet connection (WAN), firmware and hardware version numbers, MAC Address, IP settings of Verizon Business Internet Gateway and Wi-Fi extender(s) (if connected).

MAIN SCREEN

verizon

Basic

Advanced

Basic

Help

Settings

Network Devices

Verizon Internet Gateway

Home

Wi-Fi

Devices

System

System Status

Open Source Software

System > System Status

System Status

Auto-refresh

Refresh

WAN1 (Ethernet)

Broadband IPv4

Status
Disconnected

IPv4 address is from:
DHCP

IPv4 address

Subnet Mask

IPv4 Default Gateway

IPv4 DNS Address 1

IPv4 DNS Address 2

NATs Supported (used / max)
0 / 30000

Broadband IPv6

Status
Disconnected

IPv6 address is from:
DHCPv6-FO

Delegated Prefix

IPv6 Address

Link-Local Address

IPv6 Default Gateway

IPv6 DNS Address 1

IPv6 DNS Address 2

verizon

Basic

Advanced

Basic

Help

Settings

Network Devices

Verizon Internet Gateway

Home

Wi-Fi

Devices

System

System Status

Open Source Software

System > System Status

System Status

Auto-refresh

Refresh

WAN2 (Cellular)

Broadband IPv4

Status
Disconnected

IPv4 address is from:
Cellular Modem

IPv4 address

Subnet Mask

IPv4 Default Gateway

IPv4 DNS Address 1

IPv4 DNS Address 2

NATs Supported (used / max)
0 / 30000

Broadband IPv6

Status
Disconnected

IPv6 address is from:
Cellular Modem

Assigned Prefix

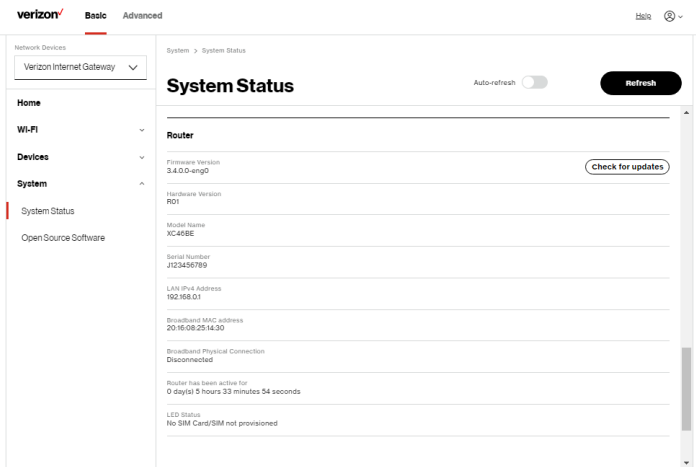
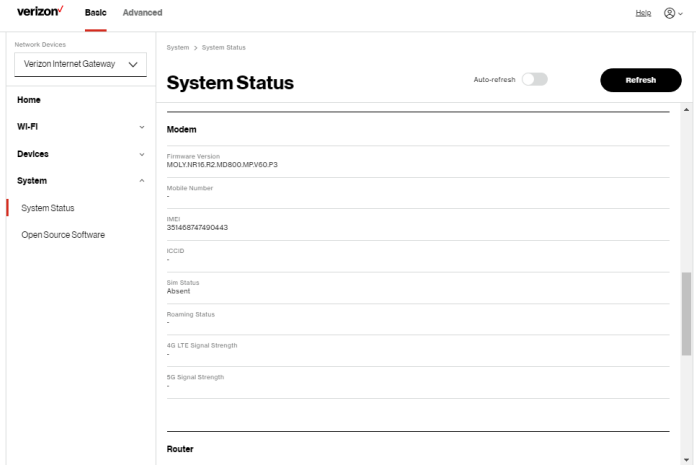
IPv6 Address

Link-Local Address

IPv6 Default Gateway

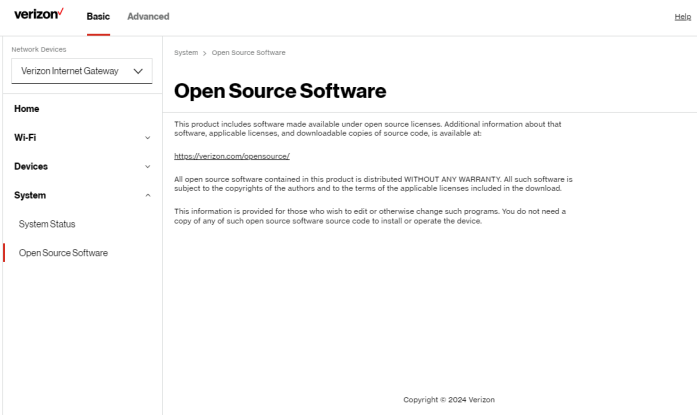
IPv6 DNS Address 1

IPv6 DNS Address 2



MAIN SCREEN

OPEN SOURCE SOFTWARE



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

03 /

WI-FI SETTINGS

3.0 Overview

3.1 Basic Settings

3.2 Advanced Settings

Wi-Fi networking can enable you to free yourself from wires, which can make 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

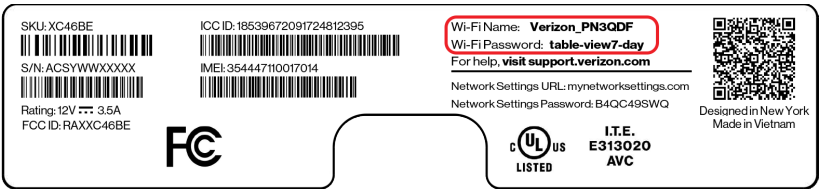
The Verizon Business Internet Gateway provides you with Wi-Fi connectivity using the 802.11a, b, g, n, ac or ax standards. These are the most common Wi-Fi standards.

The Gateway supports 2.4 GHz and 5 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 of 300 Mbps
 - Compatibility mode: supports IEEE 802.11be
 - backward compatible with IEEE 802.11b/g/n/ax
 - maximum theoretical rate up to 688 Mbps
- 5 GHz
 - Legacy operation mode: supports IEEE 802.11a/n/ac with maximum theoretical rate of 960 Mbps
 - Compatibility mode: supports IEEE 802.11be
 - backward compatible with IEEE 802.11a/n/ac/ax
 - maximum theoretical rate up to 2.8 Gbps

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) pre-configured at the factory. This information is displayed on a sticker located on the bottom of your Gateway.

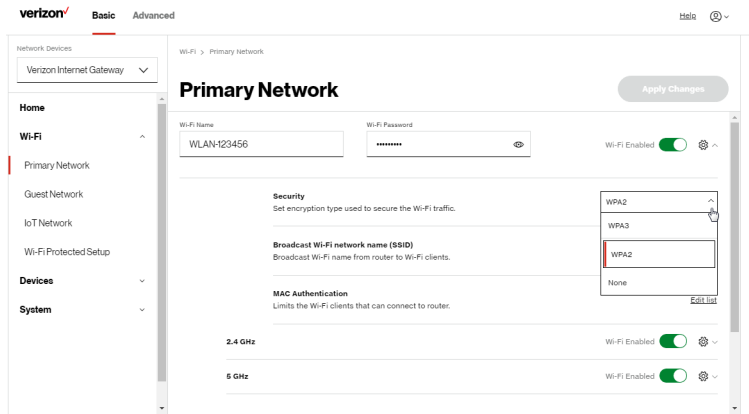
Your Gateway integrates multiple layers of security. These include Wi-Fi Protected Access, and firewall.



3.1/ BASIC SETTINGS

3.1a/ PRIMARY NETWORK

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



To configure the basic security radio, SSID and security settings:

1. From the **Basic** menu, select **Wi-Fi** from the left pane and then click **Primary Network**.

BASIC SETTINGS

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 office 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.

4. To configure the Wi-Fi **Security**, click the setup  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 Gateway and your local network.

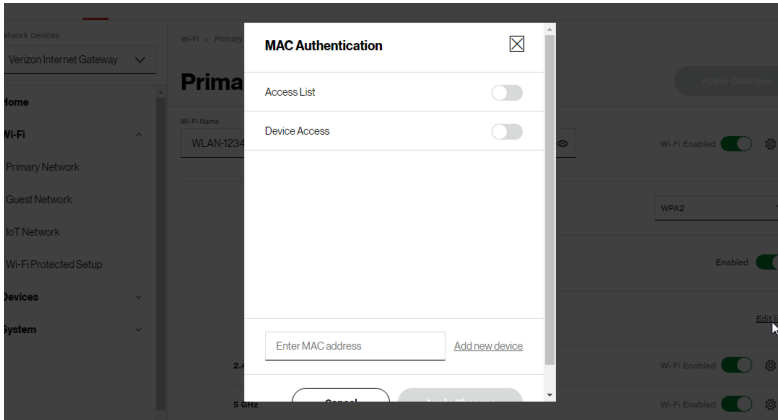
- **Broadcast Wi-Fi network name (SSID)**

You can configure the Gateway's SSID broadcast capabilities to allow or disallow Wi-Fi devices from automatically using a broadcast SSID name to detect your gateway 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 Gateway to limit access to your Wi-Fi network to only those devices with specific MAC addresses.



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.

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.

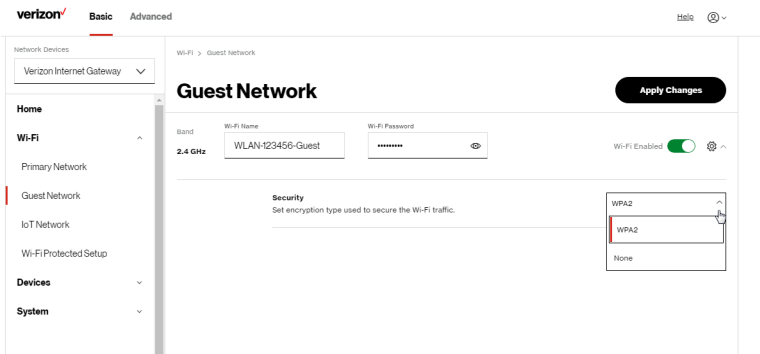
- **Device Access** – Wi-Fi devices will be able to access the Wi-Fi network if they use the correct Wi-Fi password.
3. Enter the MAC address of a device and click **Add new device**.
4. Repeat step 2 and step 3 to add additional devices, as needed.
5. When all changes are complete, click **Apply Changes**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

BASIC SETTINGS

3.1b/ GUEST NETWORK

The **Guest Network** is designed to provide internet connectivity to your guests while restricting 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 Business Internet Gateway 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 on the bottom of the Gateway followed by hyphen guest (-Guest). For example, if the Gateway is shipped with a default SSID of “Verizon-ABCDE” then the default SSID for Guest Wi-Fi is “Verizon-ABCDE-Guest”.



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.

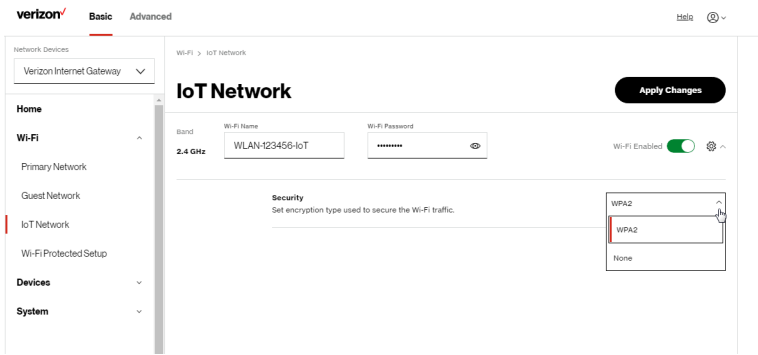
4. Press **Apply Changes** to save the changes.

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

3.1c/ IOT NETWORK

The Gateway 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 Gateway 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 on the bottom of the Gateway followed by hyphen IoT (-IoT). For example, if the Gateway is shipped with a default SSID of “Verizon-ABCDE” then the default SSID for IoT Wi-Fi is “Verizon-ABCDE-IoT”.



BASIC SETTINGS

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 Gateway creates a secure Wi-Fi network connection.

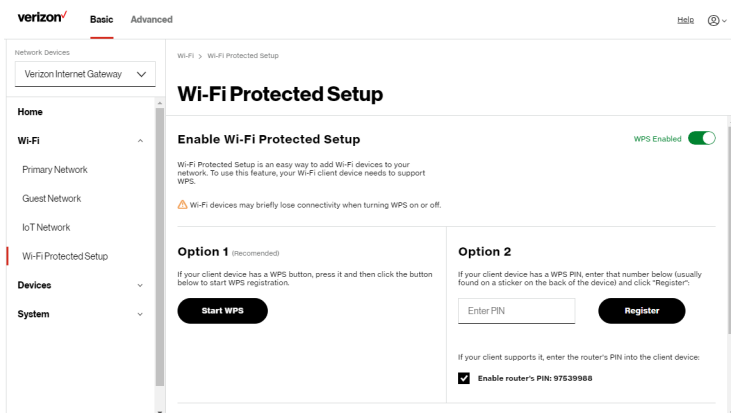
In most cases, this only requires the pressing of two buttons – one on your Gateway and one on the Wi-Fi client. This could be either a built-in button or one on a compatible Wi-Fi adapter/card, or a virtual button in software. Once completed, this allows Wi-Fi clients to join your Wi-Fi network.

To initialize the WPS process, you can either press and hold the WPS button located on the bottom of your Gateway 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** and then click **Wi-Fi Protected Setup (WPS)**.



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 Gateway for more than two seconds, then click the **Start WPS** button in **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 Gateway'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.

BASIC SETTINGS

4. After pressing the WPS button on your Gateway, 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 Gateway is pressed, the Status LED on the Gateway begins flashing blue. The flashing continues until WPS pairing to the client device completes successfully. At this time, the Status LED turns solid white.

If WPS fails to establish a connection to a Wi-Fi client device within two minutes, the Status LED on your Gateway 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.

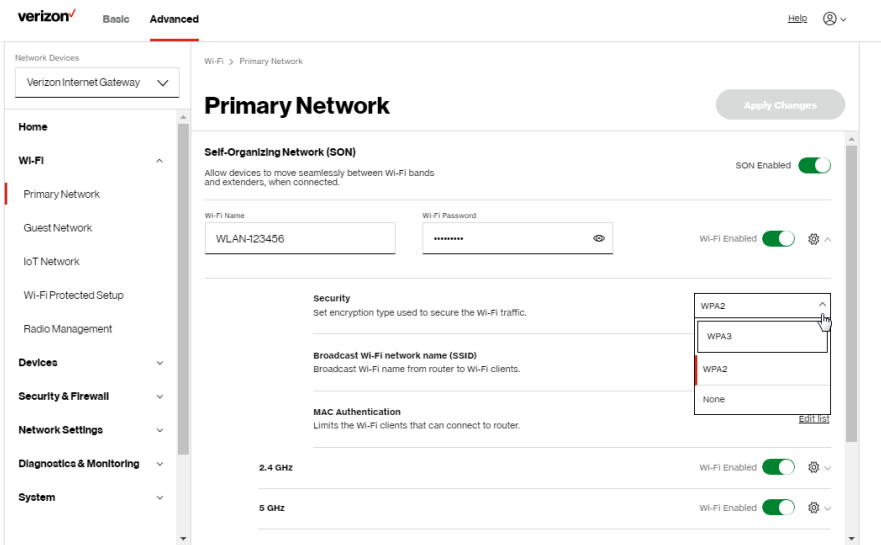
***Note:** Wi-Fi Protected Setup (WPS) cannot be used if WPA3 security is enabled or SSID broadcast is disabled or if MAC address authentication is enabled with an empty white list.*

3.2/ ADVANCED SETTINGS

3.2a/ PRIMARY NETWORK

Self-Organizing Network (SON)

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



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

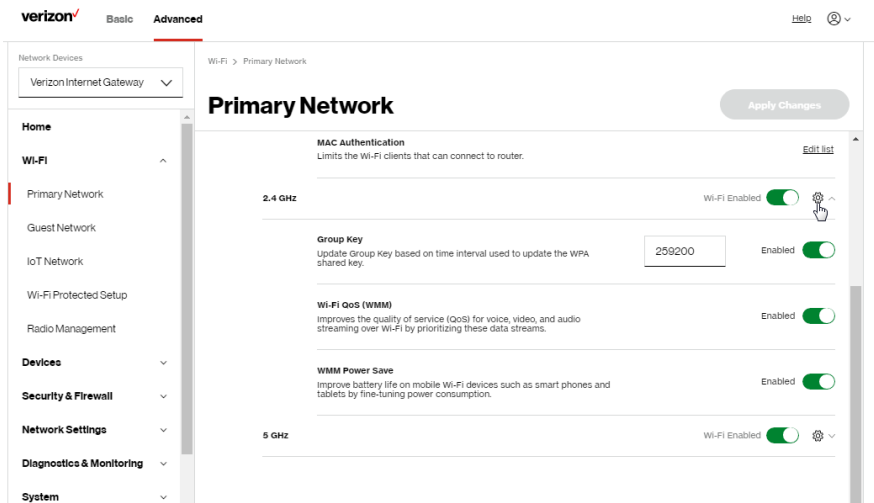
1. From the **Advanced** menu, select **Wi-Fi** from the left pane and then click **Primary Network**.
2. To enable SON, move the selector to **on**.
3. To activate the Wi-Fi radio, move the selector to **on**. If the radio is not enabled, no Wi-Fi devices will be able to connect to the primary network.

ADVANCED SETTINGS

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.

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

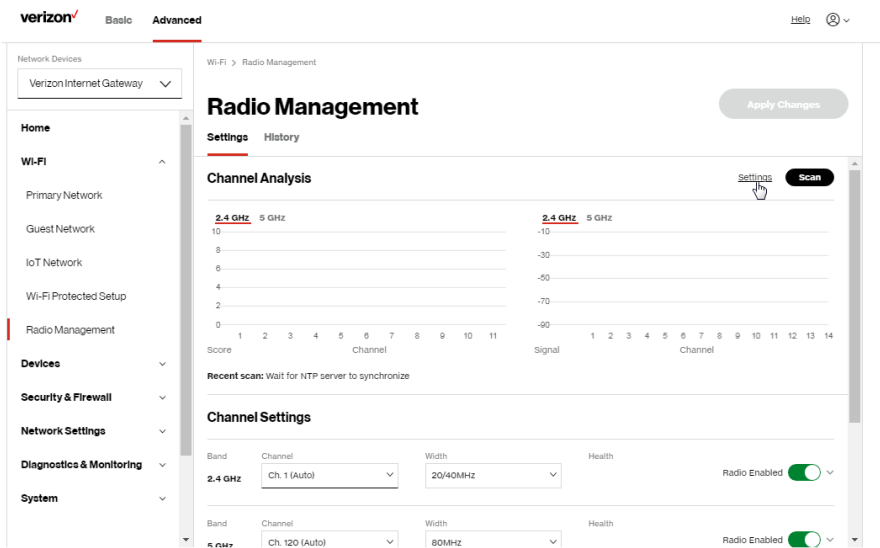


Caution: These settings should only be configured by experienced network technicians. Changing the settings could adversely affect the operation of your Gateway and your local network.

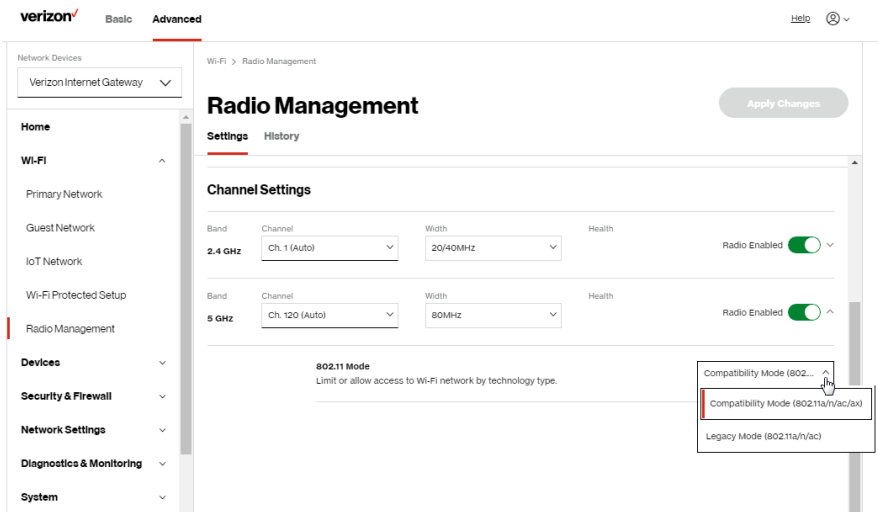
- **Group key** - to update the WPA shared key, move the selector to on.
- **Wi-Fi QoS (WMM)** - improves the quality of service (QoS) for voice, video, and audio streaming over Wi-Fi by prioritizing these data streams.
- **WMM Power Save** - improves battery life on mobile Wi-Fi devices such as smart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

3.2b/ RADIO MANAGEMENT

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

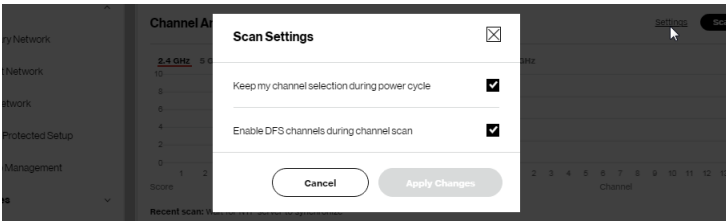


ADVANCED SETTINGS



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:



- Select the **Keep my channel selection during power cycle** check box to save your channel selection when your Gateway 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 gateways using them. Examples include some media streaming devices. Disabling this feature will allow the Gateway to select the best available channel to broadcast on and allow these devices to connect.

- Press **Apply Changes** to save the changes.
3. Click **Scan** to perform a channel availability scan for the Gateway to identify the radio channels providing the best Wi-Fi performance.
 4. On the **Radio Management** page for 2.4 GHz or 5 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 zero 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 Gateway and its clients to communicate with each other. The channel must be the same on the Gateway 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 Gateway will automatically assign itself a radio channel.

ADVANCED SETTINGS

- **Width** - displays the bandwidth available to 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,ax and b 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. 802.11b,g,n,ax and b 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.

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

BasicAdvanced

Help

Network Devices

Verizon Internet Gateway

Home

Wi-Fi

Primary Network

Guest Network

IoT Network

Wi-Fi Protected Setup

Radio Management

Devices

Security & Firewall

Network Settings

Diagnostics & Monitoring

System

Wi-Fi > Radio Management

Radio Management

SettingsHistory

Band	Channel	Time	Date
2.4 GHz	Ch. 11	N/A	N/A
2.4 GHz	Ch. 6	N/A	N/A
2.4 GHz	Ch. 11	N/A	N/A
2.4 GHz	Ch. 1	N/A	N/A
2.4 GHz	Ch. 11	N/A	N/A
5 GHz	Ch. 157	N/A	N/A
5 GHz	Ch. 112	N/A	N/A
5 GHz	Ch. 157	N/A	N/A

04 /

CONNECTED DEVICES

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

You can view the settings of the network devices connected to the network of your Verizon Business Internet Gateway.

The abundance of harmful information on the internet poses a serious challenge for employers as they ask “How can I regulate what my employee does on the internet?”

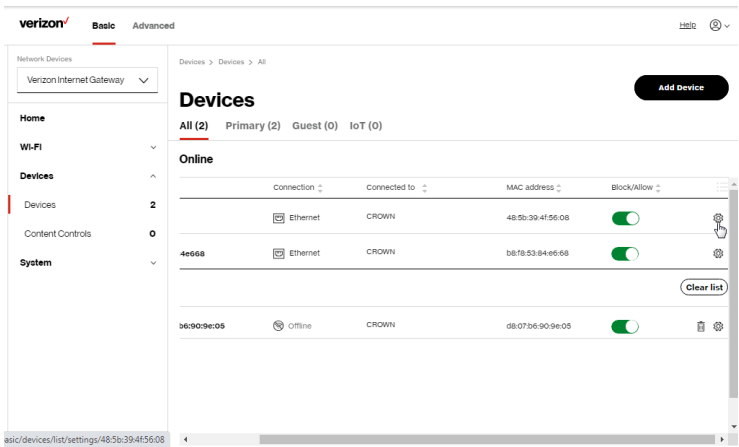
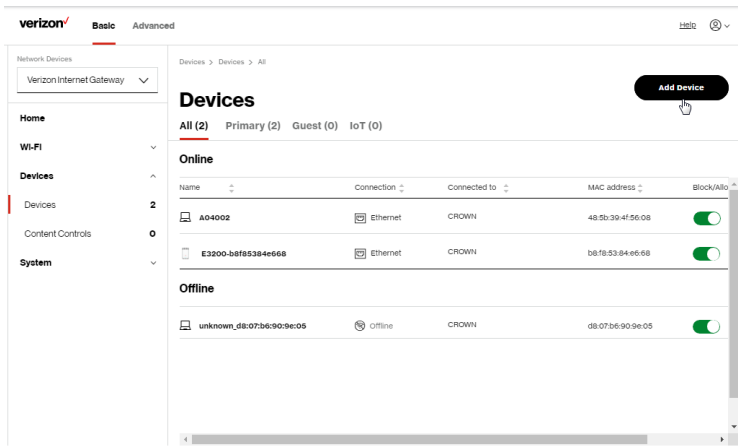
With that question in mind, the Content Controls of your Gateway were designed to allow control of internet access on all locally networked devices.

DEVICE SETTINGS

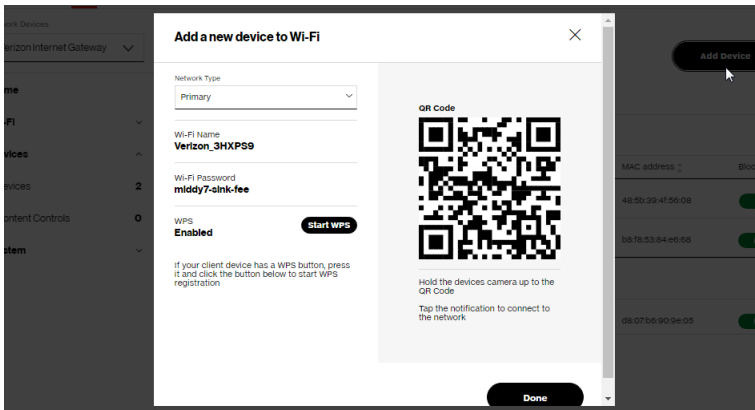
4.0/ DEVICE SETTINGS

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, **Content Controls**, the type of network connection, and settings that you can view and configure.



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 new device's camera.
 - iv. Tap the push notification to connect the device to your network.



- v. You can add the new device to your Wi-Fi network by clicking the **Start WPS** button if your Wi-Fi device supports the WPS feature. Refer to “3.1d/ Wi-Fi Protected Setup (WPS)” on page 40 for detailed information.
 - vi. Click **Done** to save the changes.
4. Click and drag the horizontal scrolling bar to the right on the screen for device configuration.
5. Click the **Block/Allow** option to quickly disable/enable a device from having internet access.

For additional information about blocking websites, refer to “Setting Content Controls” on page 56.

DEVICE SETTINGS

6.
- Click the Settings icon to access the **Device Settings** page for that device:

verizon

Basic

Advanced

Network Devices

Verizon Internet Gateway

Home

Wi-Fi

Devices

Devices

Content Controls

System

Devices > Devices > Device Settings

Device Settings

Save

Device Information

Edit

Reset to Default

Device

Online

Extender

Name

2F4

Host Name

E3200-0d8f5364e668

Location

Bedroom1

Mobility

Portable

Device Add-Ons

Port Forwarding

N/A

DMZ host

N/A

Access Control

N/A

DNS Server

N/A

Device Connection

Connection Info

Network Info

Connection

Ethernet

Phy Rate / Modulation Rate

1000 Mbps

Misc Address

18-18-53-B4-e6-08

Connected to

CROWN

IPv4 Address

192.168.1.100

Subnet Mask

255.255.255.0

IPv4 DNS

192.168.1.1

IPv4 Address Allocation

Dynamic

Lease Type

DHCP

DHCP lease time remaining

1127 minutes 56 seconds

IPv6 LAN Prefix

0/0

verizon

Basic

Advanced

Network Devices

Verizon Internet Gateway

Home

Wi-Fi

Devices

Devices

Content Controls

System

Devices > Devices > Device Settings

Device Settings

Save

Device Connection

Connection Info

Network Info

Connection

Ethernet

Phy Rate / Modulation Rate

1000 Mbps

Misc Address

18-18-53-B4-e6-08

Connected to

CROWN

IPv4 Address

192.168.1.100

Subnet Mask

255.255.255.0

IPv4 DNS

192.168.1.1

IPv4 Address Allocation

Dynamic

Lease Type

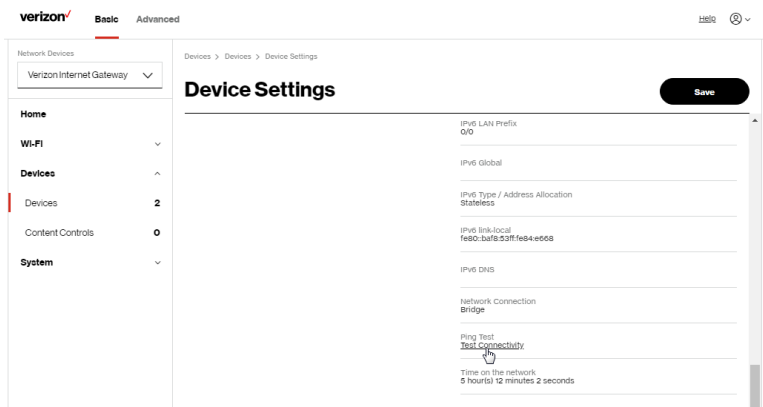
DHCP

DHCP lease time remaining

1127 minutes 56 seconds

IPv6 LAN Prefix

0/0



- **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.
- **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 video conferencing, voice, and chat, to access 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.

SETTING CONTENT CONTROLS

DMZ host - DMZ host allows a single device on your primary network to be fully exposed to the internet for special purposes such as an email server. 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**

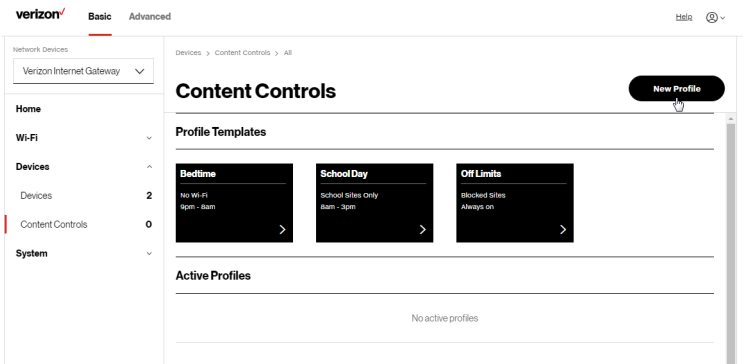
- This section provides the device MAC Address, Access Point information the device is connected to as well as the IPv4 Address of the device.
- This section displays Connection information of how and how well the device is connected to the Access Point. It also displays the Network related information, including IPv6 addresses and a **Ping Test** option.

4.1/ SETTING CONTENT CONTROLS

4.1a/ ACTIVATING CONTENT CONTROLS

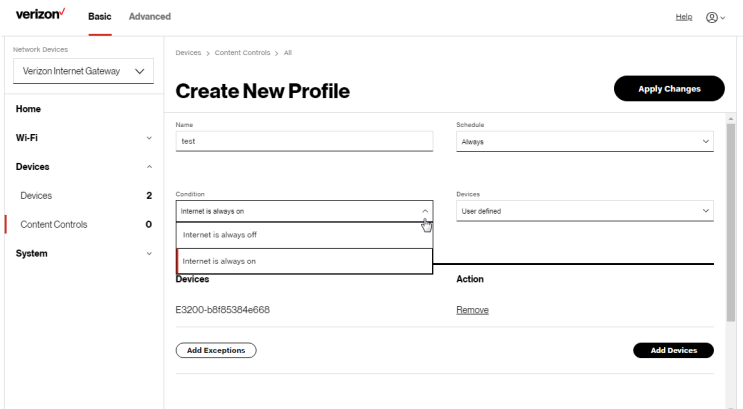
You can create a basic access policy by using the provided **Rule Templates** for any computer or device on your Gateway network. Content Controls limit internet access to specific websites based on a schedule that you create.

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.



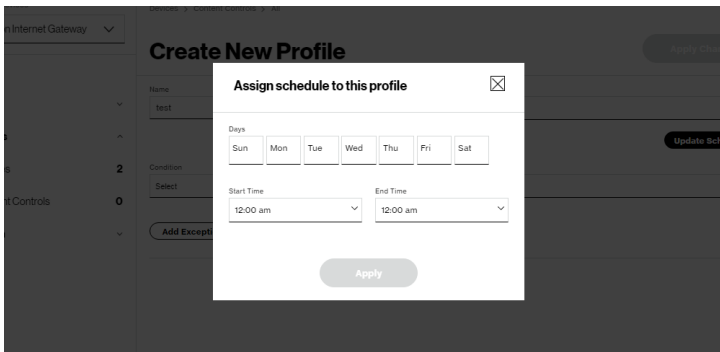
To limit device access:

1. From the **Basic** menu, select **Devices** from the left pane and then click **Content Controls**.
2. To use the default **Rule Templates**, select one of the pre-defined 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.

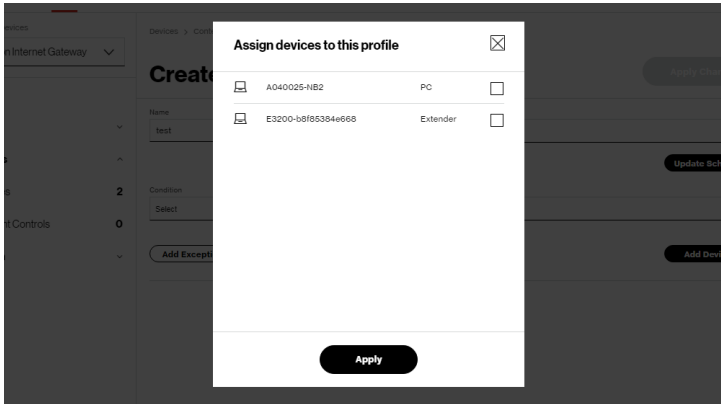


SETTING CONTENT CONTROLS

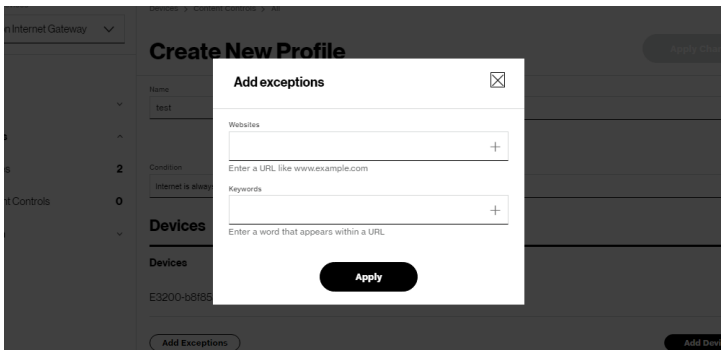
4. Create a rule name.
5. Create a **Schedule** by selecting **User defined** from the dropdown list.



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.
10. 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.



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

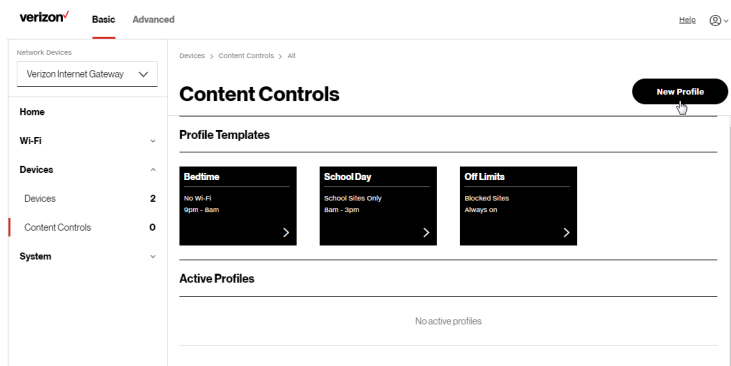


14. Click **Apply** to save changes.

UNIVERSAL PLUG & PLAY

4.1b/ ACTIVE RULES

You can view the rules created for your Gateway shown on the **Content Controls** page.



4.2/ UNIVERSAL PLUG & PLAY

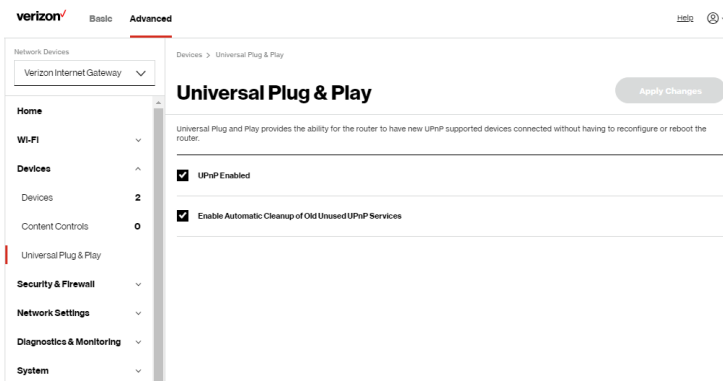
You can use Universal Plug and Play (UPnP) to support new devices without configuring or rebooting your Gateway.

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**.



2. To enable UPnP and allow UPnP services to be defined on any network hosts, select the **UPnP Enabled** check box.
3. 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.

05 /

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 Business Internet Gateway's firmware, security setup and network.

The security suite of your Gateway 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 – manages the security level for the firewall.
- Access Control – restricts 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 video conferencing.
- IPv6 Pinholes – provides access tunnel to a service on a host for a particular application.
- Port Forwarding – enables access from the internet to specified services provided by computers on the local network.
- Port Forwarding Rules – displays port forwarding rules.
- Port Triggering – defines 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.

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.

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 Gateway to its default settings.
- **LED Brightness** – controls the Status LED light to either dim or brighten.
- **Reboot Router** – restarts your Gateway.
- **Remote Administration** - enables remote configuration of your Gateway from any internet-accessible computer.
- **System Settings** – sets up various system and management parameters.

SECURITY & FIREWALL

5.0/ SECURITY & FIREWALL

The firewall is the cornerstone of the security suite for your Gateway. 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 office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as 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 Gateway or rejected and barred from passing through your Gateway, 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 Gateway, the firewall identifies the request type and origin, such as HTTP and a specific computer in

the local network. Unless your Gateway 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:

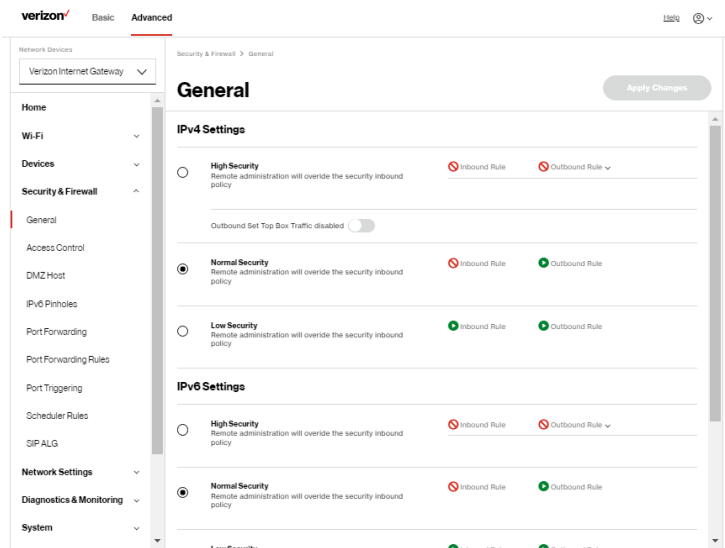
- Blocked traffic – no access allowed, except as configured in Port Forwarding and Remote Access
- Limited – permits only commonly used services, such as email and web browsing
- Unrestricted – permits full access of incoming traffic from the internet and allows all outgoing traffic, except as configured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

SECURITY & FIREWALL

SPECIFYING GENERAL SETTINGS FOR IPV4 OR IPV6

To set your firewall configuration:

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



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

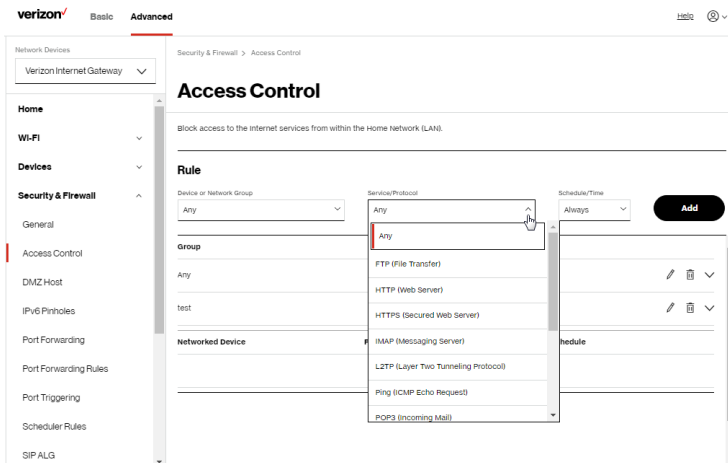
You can block individual computers on your local network from accessing specific services on the internet. For example, you could block one computer from accessing the internet, then block a second computer from transferring files using FTP as well as prohibit the computer from receiving incoming email.

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

ALLOW OR RESTRICT SERVICES

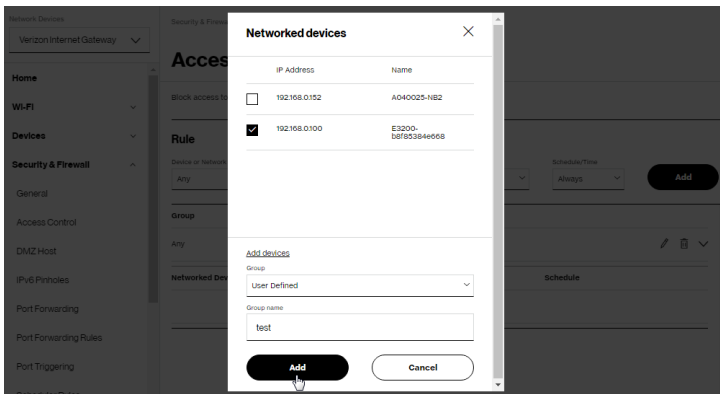
To allow or restrict services:

1. From the **Advanced** menu, select **Security & Firewall** from the left pane and then click **Access Control**. The **Access Control** page opens with the allowed and blocked status displayed. The allowed section only displays when the firewall is set to maximum security.

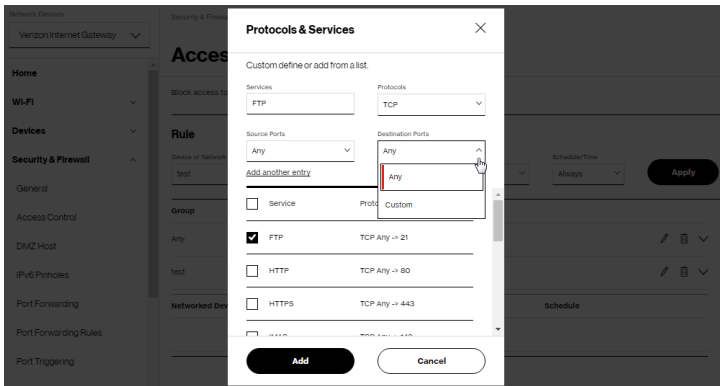


SECURITY & FIREWALL

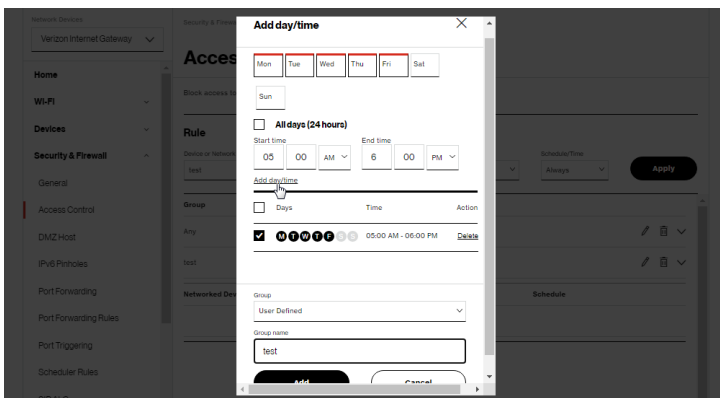
2. To apply the rule to:
 - Networked Device or Network Group - select **Any**.
 - Specific devices only – select networked device or **User Defined**.
3. Select the networked device to be allowed or blocked in the list.
4. In the **Add devices**, enter the group name, then click **Add**. The new network group is automatically added to the **Access Control** section.



5. To block a service, select the internet protocol to be blocked in the **Protocol** field.
6. If the service is not included in the list, select **User Defined**, define the service, then click **Add another entry**.
7. Click **Add**. The service is automatically added to the **Access Control** section.



8. Specify when the rule is active as **Always** or **User Defined**.
9. Specify days of the week, and set the start time and end time when the rule will be active or inactive.



10. Click **Add day/time** to create the schedule time and choose the schedule rule by clicking on the check box on the screen.
11. Click **Add** to apply the changes.

SECURITY & FIREWALL

12. The **Access Control** page displays a summary of the new access control rule.
13. To modify the current settings, click the edit icon in the action column and then the **Apply** button.
14. To remove an access restriction, click the trash icon. The rule is removed from the Access Control table.

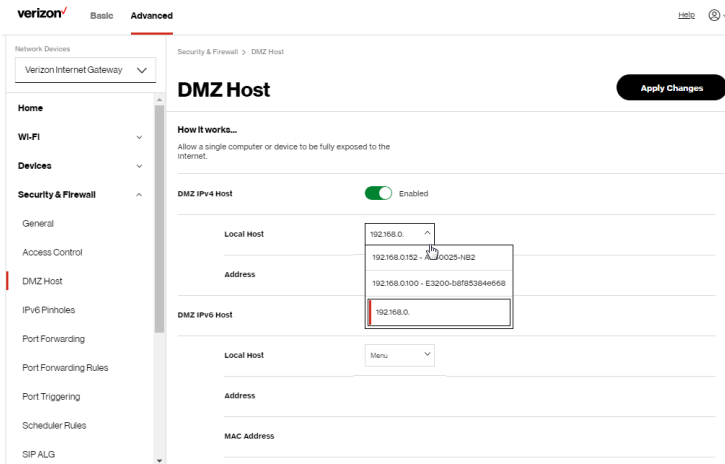
5.0c/ DMZ HOST

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

***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.



4. Click **Apply Changes** to save changes.

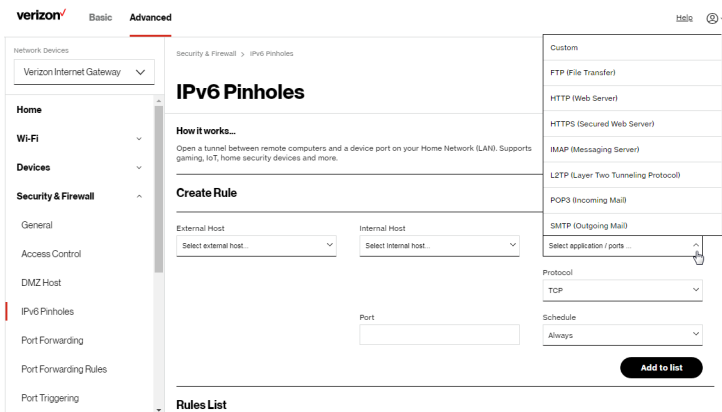
5.0d/ IPV6 PINHOLES

The IPv6 Pinhole feature of the Gateway 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**.

SECURITY & FIREWALL



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 video conferencing 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.

The screenshot shows the Verizon Business Internet Gateway interface. The left sidebar has a menu with 'Security & Firewall' expanded, showing 'Port Forwarding' as the selected option. The main content area is titled 'Port Forwarding' and includes a description: 'Open a tunnel between remote computers and a device port on your Home Network (LAN). Supports gaming, IoT, home security devices and more.' Below this is a 'Create Rule' section with input fields for 'Application', 'Original Port' (0000), 'Protocol' (Select), 'Fwd to Addr' (Select), 'Fwd to Port' (0000), and 'Schedule' (Select). An 'Add to list' button is at the bottom right of the 'Create Rule' section. Below the 'Create Rule' section is a 'Rules List' table with one rule displayed.

Application	Original Port	Protocol	Fwd to Addr	Fwd to Port	Schedule
	4567	TCP	127.0.0.1	4567	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.

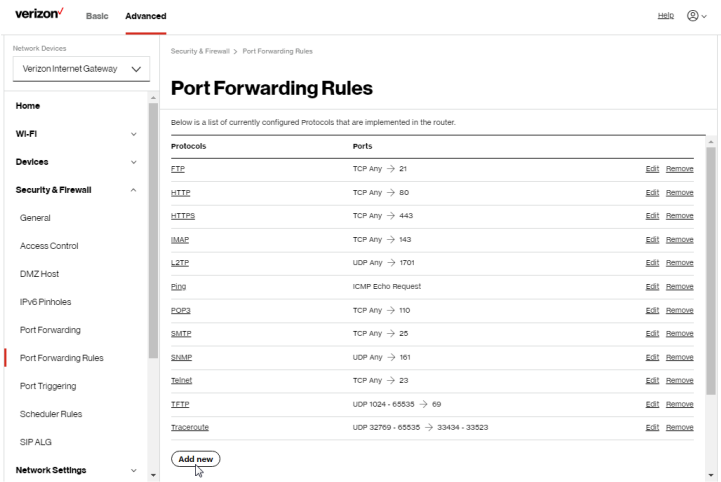
SECURITY & FIREWALL

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.



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 Basic Advanced

Network Devices
Verizon Internet Gateway

Security & Firewall

- General
- Access Control
- DMZ Host
- IPv6 Pinholes
- Port Forwarding
- Port Forwarding Rules
- Port Triggering
- Scheduler Rules
- SIP ALG

Network Settings

Security & Firewall > Port Forwarding Rules > Edit Service

Edit Service

Edit Service

Service Name

Service Description

Service Ports

Protocols	Ports
Add	

Cancel Apply

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 Advanced

Network Devices
Verizon Internet Gateway

Security & Firewall

- General
- Access Control
- DMZ Host
- IPv6 Pinholes
- Port Forwarding
- Port Forwarding Rules
- Port Triggering

Network Settings

Security & Firewall > Port Forwarding Rules > Edit Service

Edit Service

Edit Service Server Ports

Protocol

Source Ports

Destination Ports

Cancel Apply

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

SECURITY & FIREWALL

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 web server is accessed using UDP protocol on port 2222. The web server then responds by connecting the user using UDP on port 3333, when a web 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 Gateway 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 Gateway accepting the inbound traffic from the web 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**.

verizon Basic Advanced

Network Devices
Verizon Internet Gateway

Security & Firewall
General
Access Control
DMZ Host
IPv6 Pinholes
Port Forwarding
Port Forwarding Rules
Port Triggering
Scheduler Rules
SIP ALG

Network Settings
Diagnostics & Monitoring
System

Port Triggering

Trigger opening of ports incoming data.

Create Rule

Application: PT-test2

Trig Port Range: Start 55, End 66

Protocol: TCP

Fwd Port Range: Start 77, End 88

Schedule: PT-test2

Add to list

Rules List

Application	Trig port range	Protocol	Fwd port range	Schedule	
PT-test	11 22	TCP	33 44	test	☒

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.

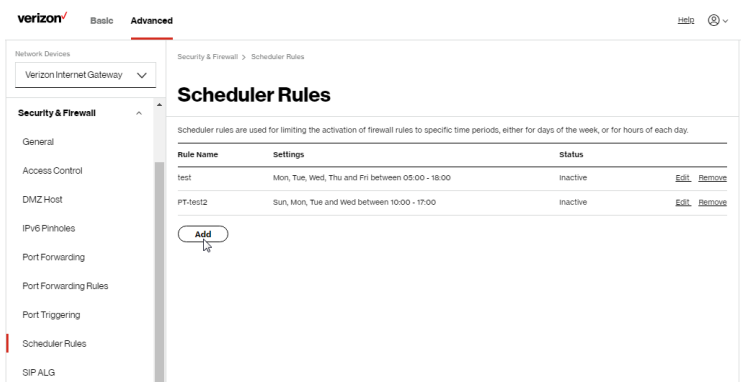
5.0h/ SCHEDULER RULES

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.

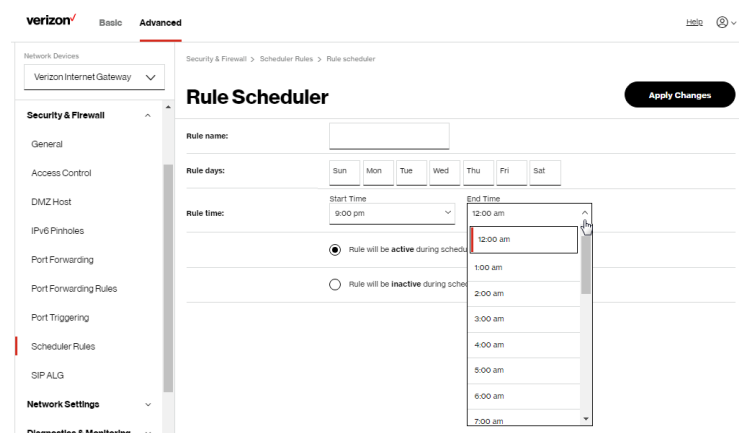
SECURITY & FIREWALL

To define a rule:

- 1. Verify that the date and time of your Gateway is correct.
- 2. Select **Scheduler Rules** in the **Security & Firewall** section.



- 3. Click **Add**. The **Rule Scheduler** page displays.



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

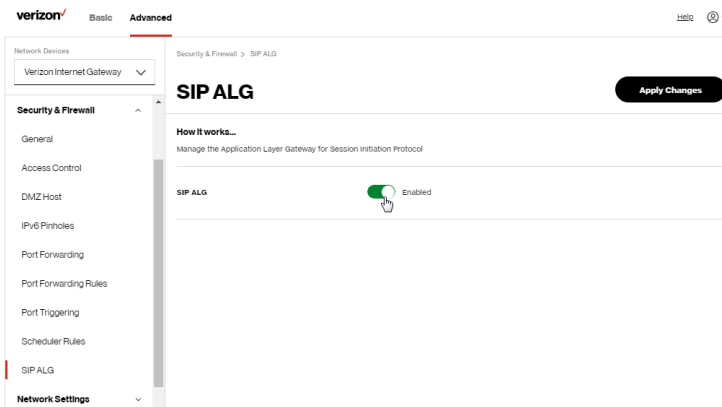
5. Specify if the rule is **active** or **inactive** at the scheduled time.
6. Click **Apply Changes** to save changes.

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.



3. Click **Apply Changes** to save changes.

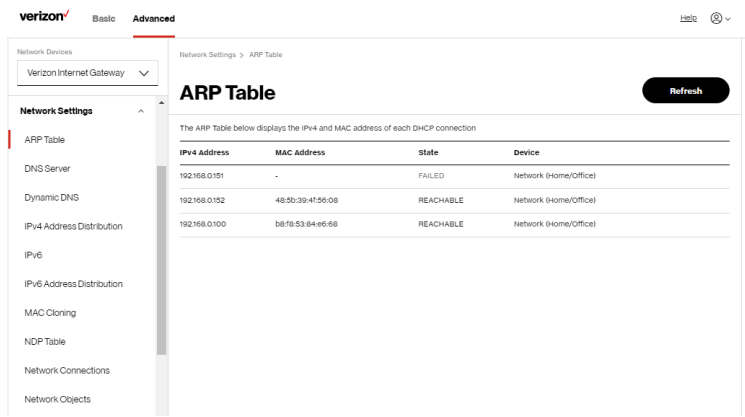
NETWORK SETTINGS

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**.

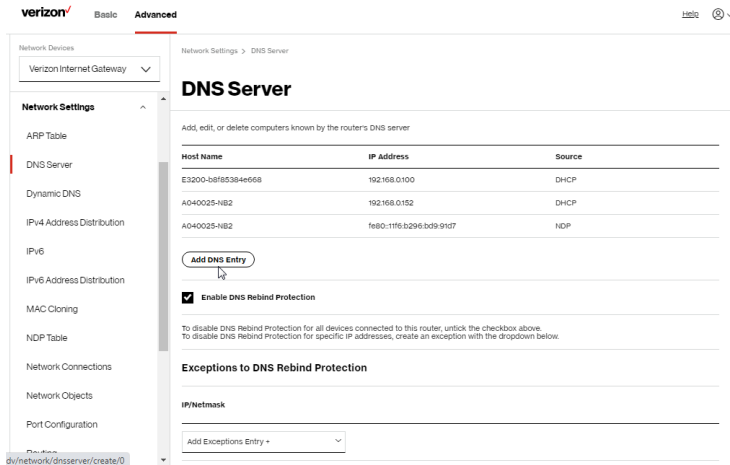


5.1b/ DNS SERVER

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:

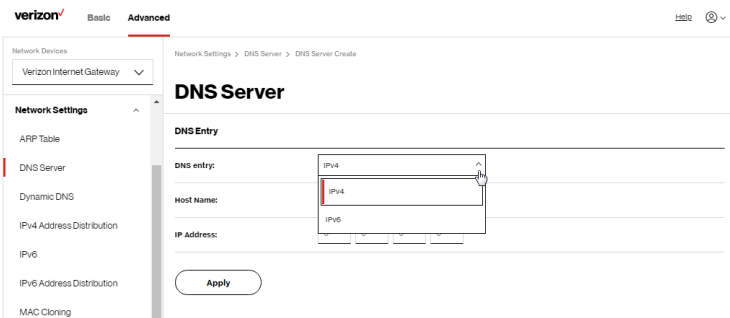
1. From the **Advanced** menu, select **Network Settings** and then click **DNS Server**.



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

Warning: Disabling this protection may create a risk of cyber security attack to devices connected to this Gateway.

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



NETWORK SETTINGS

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.
6. To add a new IP address entry, select the **Add Exceptions Entry** in the **Exceptions to DNS Rebind Protection** section. 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

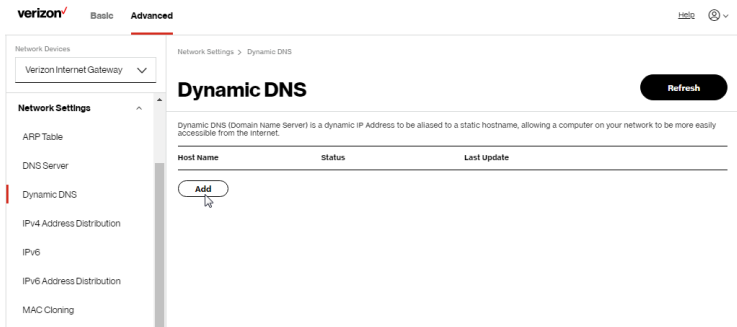
Typically, when connecting to the internet, your Gateway is assigned an unused public IP address from a pool, and this address changes periodically.

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.

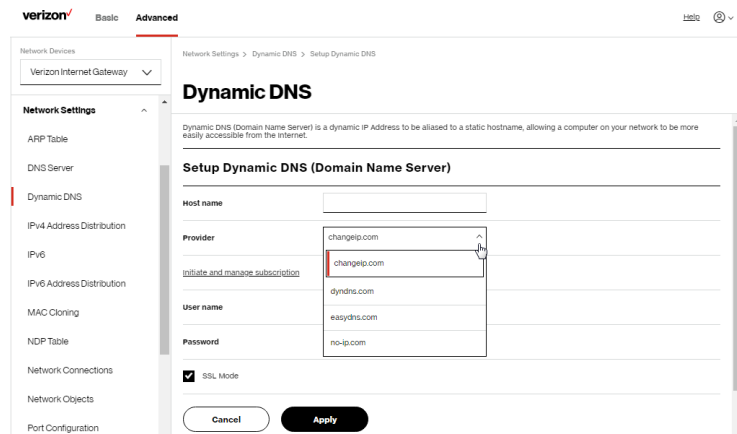
When using Dynamic DNS, each time the public IP address changes, the DNS database is automatically updated with the new IP address. In this way, even though the IP address changes often, the domain name remains constant and accessible.

To set up dynamic DNS:

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



2. To set up a new entry, click the **Add** button.



3. Configure the following parameters:
- **Host Name** – enter the full domain name for your Dynamic DNS domain.
 - **Provider** – select the Dynamic DNS account provider from the menu.
 - **User Name** – enter your user name for your Dynamic DNS account.

NETWORK SETTINGS

- **Password** – enter the password for your Dynamic DNS account.
 - **SSL Mode** – select if your Dynamic DNS service supports SSL.
4. Click **Apply** to save your changes.

5.1d/ IPV4 ADDRESS DISTRIBUTION

You can easily add computers configured as DHCP clients to the network. The DHCP server provides a mechanism for allocating IP addresses to these hosts and for delivering network configuration parameters to the hosts.

For example, a client (host) sends a broadcast message on the network requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as taken. At this point, the host is configured with an IP address for the duration of the lease.

The host can renew an expiring lease or let it expire. If it renews a lease, the host receives current information about network services, as it did during the original lease, allowing it to update its network configurations to reflect any changes that occurred since the first connection to the network.

If the host wishes to terminate a lease before its expiration, it sends a release message to the DHCP server. This makes the IP address available for use by other hosts.

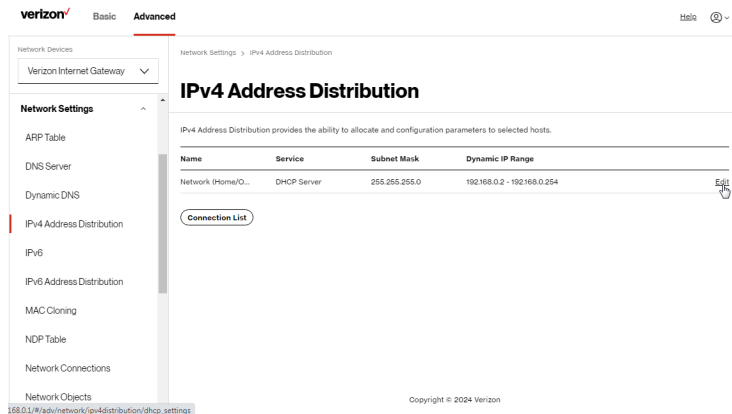
The DHCP server performs the following functions:

- Displays a list of all DHCP host devices connected to your Gateway
- Defines the range of IP addresses that can be allocated in the network
- Defines the length of time the dynamic IP addresses are allocated

- Provides the above configurations for each network device and can be configured and enabled or disabled separately for each network device
- Assigns a static lease to a network computer to receive the same IP address each time it connects to the network, even if this IP address is within the range of addresses that the DHCP server may assign to other computer
- Provides the DNS server with the host name and IP address of each computer connected to the network

To view a summary of the services provided by the DHCP server:

1. Select **IPv4 Address Distribution** in the **Network Settings** section.



2. You can edit the DHCP server settings for a device. On the **IPv4 Address Distribution** page, click the **Edit** icon on the screen. The DHCP Settings page opens with the device information displayed.
3. To enable the DHCP server, select **DHCP Server** in the **IPv4 Address Distribution** field.
4. Once enabled, the DHCP server provides automatic IP assignments (IP leases) based on the preset IP range defined below.

NETWORK SETTINGS

verizon

Basic

Advanced

hello

Network Devices

Verizon Internet Gateway

Network Settings

ARP Table

DNS Server

Dynamic DNS

IPv4 Address Distribution

IPv6

IPv6 Address Distribution

MAC Cloning

NDP Table

Network Connections

Network Objects

Port Configuration

Routing

Network Settings > IPv4 Address Distribution > DHCP Settings

DHCP Settings for Network (Home/Office)

Service

IPv4 Address Distribution: DHCP Server

DHCP Server Disabled

Start IP Address: 192.168.0.2

End IP Address: 192.168.0.254

WINS Server: 0.0.0.0

Lease Time in Minutes: 1440

IPv4 Address Distribution According to DHCP Option 60 (Vendor Class Identifier)

Vendor Class Id	IP Address	MAC Address	QoS
MSFT 5.0	192.168.0.152	48:5B:39:4F:56:08	
Verizon BBRv1 DHCP Detect	192.168.0.100	B8:F8:53:84:E6:68	

5. To configure the DHCP server, complete the following fields:
- Start IP Address** – enter the first IP address that your Gateway will automatically begin assigning IP addresses from. Since your Gateway’s default IP address is 192.168.0.1, the default start IP address should be 192.168.0.2.
 - End IP Address** – enter the last IP address that your Gateway will stop at for the IP address allocation. The maximum end IP address range that can be entered is 192.168.0.254.
 - WINS Server** – determines the IP address associated with a network device.
 - Lease Time in Minutes** – assigns the amount of time in minutes that each device is assigned an IP address by the DHCP server when it connects to the network.

When the lease expires, the server determines if the computer has disconnected from the network. If it has, the server may reassign this IP address to a newly connected computer.

IPv4 Address Distribution According to DHCP option 60 (Vendor Class Identifier)

DHCP vendor class is related to DHCP option 60 configuration within the Gateway. User can add option 60 configurations such that particular vendor can get lease from a specified pool of address. The existing vendor class ID, IP address, MAC address and QoS are shown on the screen above.

- Click **Apply** to save changes.

DHCP Connection List

You can view a list of the connections currently assigned and recognized by the DHCP server.

To view a list of computers:

- On the **IPv4 Address Distribution** page, click **Connection List**.

verizon

BasicAdvanced

Help

Network Devices

Verizon Internet Gateway

Network Settings

ARP Table

DNS Server

Dynamic DNS

IPv4 Address Distribution

IPv6

IPv6 Address Distribution

MAC Cloning

NDP Table

Network Connections

Network Objects

Network Settings > IPv4 Address Distribution > DHCP Connections

DHCP Connections

IPv4 Address Distribution provides the ability to allocate and configuration parameters to selected hosts.

Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expired in	
E3200-5d95384e...	192.168.0.100	88:F8:53:84:E6:68	Dynamic	Network (Home/O...	Active	1119	Search Edit
A040025-NB2	192.168.0.152	48:5B:39:4F:56:08	Dynamic	Network (Home/O...	Active	1110	Search Edit

Add static connection

NETWORK SETTINGS

5.1e/ DHCP Static Connection Settings

2. To define a new static connection with a fixed IP address, click **Add static connection**.

The screenshot shows the Verizon Network Settings interface. At the top, there's a navigation bar with 'verizon' logo, 'Basic', and 'Advanced' tabs. Below this, a breadcrumb trail reads 'Network Settings > IPv4 Address Distribution > DHCP Connection Settings'. The main heading is 'DHCP Connection Settings'. On the left, a sidebar lists various network settings: Network Devices (with a dropdown for 'Verizon Internet Gateway'), Network Settings (expanded), ARP Table, DNS Server, Dynamic DNS, IPv4 Address Distribution (highlighted with a red bar), IPv6, IPv6 Address Distribution, MAC Cloning, NDP Table, Network Connections, and Network Objects. The main content area contains three input fields: 'Host name:' with a text box, 'IP Address:' with four numeric boxes (0, 0, 0, 0), and 'MAC Address:' with six numeric boxes (00, 00, 00, 00, 00, 00). An 'Apply' button is located at the bottom of the form.

3. Enter the host name.
4. Enter the fixed IP address to be assigned.
5. Enter the MAC address of the network interface of the computer used with this DHCP static connection.
6. Click **Apply** to save changes.

5.1e/ IPV6

Use the IPv6 feature settings to enable, disable, or configure an IPv6 Internet connection and IPv6 LAN settings.

1. To configure your network to use the IPv6 Internet connection type, select **IPv6** in the **Network Settings** section to display the IPv6 service options:

verizon Basic Advanced

Network Devices
Verizon Internet Gateway

Network Settings

ARP Table

DNS Server

Dynamic DNS

IPv4 Address Distribution

IPv6

IPv6 Address Distribution

MAC Cloning

NDP Table

Network Connections

Network Objects

Port Configuration

Routing

Static NAT

IPv6 Configuration Controls

Apply Changes

1. Enable IPv6 Support Enabled

2. Specify the method to be used to obtain your WAN IPv6 Address

IPv6 WAN Configuration: DHCPv6-PD

Delegated Prefix: None

Expires In: DHCPv6-PD

Prefix Lifetime: Static (Auto-Configure)

Static (Manually Configure)

WAN Link-Local Address:

☒ Obtain IPv6 DNS Server address automatically

☐ Use the following IPv6 DNS Server addresses

3. Specify the method to be used to assign LAN IPv6 addresses

IPv6 LAN Configuration: Stateless

2. Select **Enabled** in the **Enable IPv6 Support** field.
3. Click **Apply Changes** to have changes take effect.

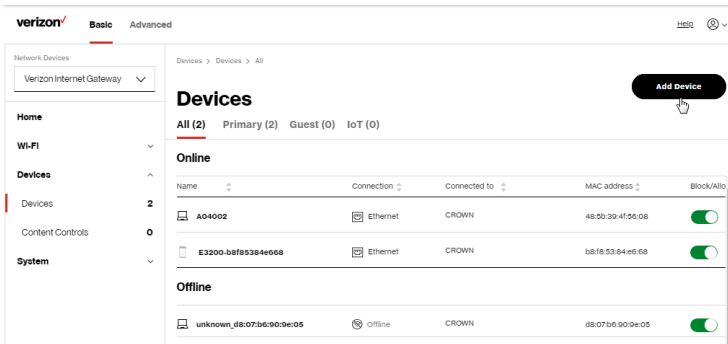
***Note:** The Internet IPv6 service is required for this feature to work over the internet.*

4. To disable the IPv6 service, move the selector to **off** in the **Enable IPv6 Support** field.
5. Click **Apply Changes** to have changes take effect.

Once configured using valid IPv6 WAN and LAN configurations, you should not see any errors when you click on the **Apply Changes** button and the **Basic/System/System Status** page will reflect the Gateway's new IPv6 address.

You should also see the IPv6 address for all IPv6 supported devices on your local network displayed on the **Basic/Devices/Devices** page by selecting the Settings icon to access the **Device Settings** page for that device.

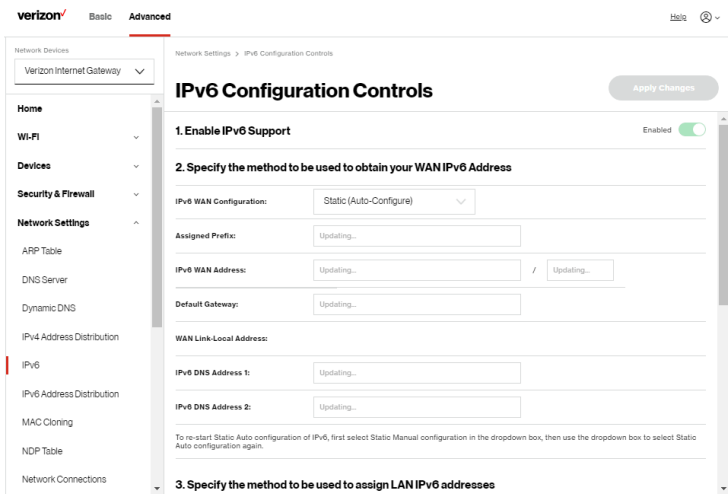
NETWORK SETTINGS



Static - WAN IPv6 Address Connection

The IPv6 WAN Static configurations are IPv6 settings that you enter manually. These specific IPv6 addresses and settings are not expected to change frequently.

1. To configure IPv6 WAN Static mode, select the **Static** option on the **IPv6 Configuration Controls** page as shown below:



2. Specify the settings to be used to assign LAN IPv6 addresses by entering the following details:
 - **IPv6 WAN Configuration** (select Static)
 - **Assigned Prefix** (A numeric value between 16 and 128)
 - **IPv6 WAN Address**
 - **Default Gateway:** Verizon Business Internet Gateway
 - **IPv6 (Primary) DNS Address 1**
 - **IPv6 (Secondary) DNS Address 2**
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

DHCPv6 PD - WAN IPv6 Address Connection

The IPv6 WAN DHCPv6 configurations are IPv6 settings that you enter that will allow your IPv6 connection to be updated by the ISP as needed.

1. To configure IPv6 WAN Stateful (DHCPv6) mode, select the **DHCPv6-PD** option on the **IPv6 Configuration Controls** page as shown below:

NETWORK SETTINGS

The screenshot shows the Verizon Network Settings interface. On the left is a sidebar with 'Network Settings' expanded, listing options like ARP Table, DNS Server, Dynamic DNS, IPv4 Address Distribution, IPv6 (highlighted), IPv6 Address Distribution, MAC Cloning, NDP Table, Network Connections, Network Objects, Port Configuration, Routing, and Static NAT. The main content area is titled 'IPv6 Configuration Controls' and includes an 'Apply Changes' button. It contains three sections: 1. 'Enable IPv6 Support' with a toggle switch set to 'Enabled'. 2. 'Specify the method to be used to obtain your WAN IPv6 Address' with a dropdown menu for 'IPv6 WAN Configuration' showing 'DHCPv6-PD' selected, and other options like 'None', 'DHCPv6-PD', 'Static (Auto-Configure)', and 'Static (Manually Configure)'. 3. 'Specify the method to be used to assign LAN IPv6 addresses' with a dropdown menu for 'IPv6 LAN Configuration' showing 'Stateless' selected. There are also radio buttons for 'Obtain IPv6 DNS Server address automatically' (selected) and 'Use the following IPv6 DNS Server addresses'.

2. Check to either **Obtain IPv6 DNS Server address automatically**, or **Use the following IPv6 DNS Server addresses**
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

WAN IPv6 with LAN IPv6 Stateful (DHCPv6) Settings

1. To configure IPv6 WAN Stateful (DHCPv6) mode, select the **Stateful (DHCPv6)** option on the **IPv6 Configuration Controls** page.
2. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:

verizon Basic Advanced

Network Devices
Verizon Internet Gateway

Network Settings
ARP Table
DNS Server
Dynamic DNS
IPv4 Address Distribution
IPv6
IPv6 Address Distribution
MAC Cloning
NDP Table
Network Connections
Network Objects
Port Configuration
Routing

Network Settings > IPv6 Configuration Controls

IPv6 Configuration Controls

Apply Changes

3. Specify the method to be used to assign LAN IPv6 addresses

IPv6 LAN Configuration: Stateful (DHCPv6)
Stateless
Stateful (DHCPv6)

LAN Prefix:

DHCPv6 Client Address Range:

LAN Link-Local Address:

Subnet ID: 00

Router Advertisement Lifetime: 15 minutes (0-150)

IPv6 Address Lifetime: 60 minutes (3-150)

Option

☒ Allow ICMPv6 Echo Requests for LAN devices using their Global IPv6 Address from WAN side

- **IPv6 LAN Configuration** (select **Stateful** from the dropdown list)
- **LAN Prefix** (automatically populated)
- **DHCPv6 Client Address Range** (start and end)
- **LAN Link Local Address** (automatically populated)
- **Subnet ID** - set the site topology for your internal site
- **Router Advertisement Lifetime** (minutes between 0-150)
- **IPv6 Address Lifetime** (minutes between 3-150)
- **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP

3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

NETWORK SETTINGS

WAN IPv6 with LAN IPv6 Stateless Settings

1. To configure IPv6 LAN Stateless mode with DHCPv6 WAN, select the **Stateless** option on the **IPv6 Configuration Controls** page.
2. Specify the settings to be used to assign LAN IPv6 addresses by entering the following details:

The screenshot shows the Verizon Network Settings interface. The 'Advanced' tab is selected. The left sidebar lists various network settings, with 'IPv6' highlighted. The main content area is titled 'IPv6 Configuration Controls'. Under the heading '3. Specify the method to be used to assign LAN IPv6 addresses', there is a dropdown menu for 'IPv6 LAN Configuration' with 'Stateless' selected. Below this are fields for 'LAN Prefix', 'LAN Link-Local Address', 'Subnet ID' (set to 00), and 'Router Advertisement Lifetime' (set to 15 minutes). An 'Option' section at the bottom has a checked checkbox for 'Allow ICMPv6 Echo Requests for LAN devices using their Global IPv6 Address from WAN side'. An 'Apply Changes' button is in the top right corner.

- **IPv6 LAN Configuration** (select **Stateless** from the dropdown list)
 - **LAN Prefix** (automatically populated)
 - **LAN Link Local Address** (automatically populated)
 - **Subnet ID** - set the site topology for your internal site
 - **Router Advertisement Lifetime** (minutes between 0-150)
 - **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

LAN IPv6 Configuration without An IPv6 WAN Connection

1. To configure IPv6 to use either the IPv6 LAN Stateful or Stateless mode without using an IPv6 Internet WAN connection, select the **None** option on the **IPv6 Configuration Controls** page.

The screenshot displays the 'IPv6 Configuration Controls' page in the Verizon Business Internet Gateway setup interface. The page is divided into three main sections:

- 1. Enable IPv6 Support:** A toggle switch labeled 'Enabled' is turned on.
- 2. Specify the method to be used to obtain your WAN IPv6 Address:**
 - IPv6 WAN Configuration:** A dropdown menu is open, showing options: 'DHCPv6-PD', 'None' (highlighted), 'DHCPv6-PD', 'Static (Auto-Configure)', and 'Static (Manually Configure)'.
 - Delegated Prefix:** A text input field.
 - Expires In:** A dropdown menu with 'DHCPv6-PD' selected.
 - Prefix Lifetime:** A dropdown menu with 'Static (Auto-Configure)' and 'Static (Manually Configure)' options.
 - WAN Link-Local Address:** A text input field.
 - Obtain IPv6 DNS Server address automatically:** A radio button that is selected.
 - Use the following IPv6 DNS Server addresses:** A radio button that is unselected.
- 3. Specify the method to be used to assign LAN IPv6 addresses:**
 - IPv6 LAN Configuration:** A dropdown menu with 'Stateless' selected.

2. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

LAN IPv6 Stateful (DHCPv6) with No WAN Settings

1. To configure IPv6 LAN Stateful mode with no WAN connection, select the Stateful option on the **IPv6 Configuration Controls** page as shown below:

NETWORK SETTINGS

The screenshot shows the Verizon Network Settings interface. On the left is a sidebar with a 'Network Settings' section containing links for ARP Table, DNS Server, Dynamic DNS, IPv4 Address Distribution, IPv6 (highlighted), IPv6 Address Distribution, MAC Cloning, NDP Table, Network Connections, Network Objects, Port Configuration, Routing, and Static NAT. The main content area is titled 'IPv6 Configuration Controls' and includes an 'Apply Changes' button. It is divided into two sections: '2. Specify the method to be used to obtain your WAN IPv6 Address' and '3. Specify the method to be used to assign LAN IPv6 addresses'. In section 2, 'IPv6 WAN Configuration' is set to 'None'. In section 3, 'IPv6 LAN Configuration' is set to 'Stateful (DHCPv6)', 'DHCPv6 Client Address Range' is set to '100::1-100::100', and 'LAN Link-Local Address' is set to 'fe80::'. 'Router Advertisement Lifetime' is 15 minutes and 'IPv6 Address Lifetime' is 60 minutes. An 'Option' section at the bottom has a checked checkbox for 'Allow ICMPv6 Echo Requests for LAN devices using their Global IPv6 Address from WAN side'.

verizon Basic Advanced

Network Settings > IPv6 Configuration Controls

IPv6 Configuration Controls

Apply Changes

2. Specify the method to be used to obtain your WAN IPv6 Address

IPv6 WAN Configuration: None

WAN Link-Local Address:

3. Specify the method to be used to assign LAN IPv6 addresses

IPv6 LAN Configuration: Stateful (DHCPv6)

DHCPv6 Client Address Range: 100::1-100::100

LAN Link-Local Address: fe80::

Router Advertisement Lifetime: 15 minutes (0-150)

IPv6 Address Lifetime: 60 minutes (3-100)

Option

☒ Allow ICMPv6 Echo Requests for LAN devices using their Global IPv6 Address from WAN side

2. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:
 - **IPv6 LAN Configuration** (select **Stateful** from the dropdown list)
 - **DHCPv6 Client Address Range** (start and end)
 - **LAN Link Local Address** (automatically populated)
 - **Router Advertisement Lifetime** (minutes between 0-150)
 - **IPv6 Address Lifetime** (minutes between 3-150)
 - **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

LAN IPv6 Stateless with No WAN Settings

1. To configure IPv6 LAN Stateless mode with no WAN connection, select the **Stateless** option on the **IPv6 Configuration Controls** page as shown below:

The screenshot displays the 'IPv6 Configuration Controls' page in the Verizon Business Internet Gateway interface. The page is divided into three main sections:

- 1. Enable IPv6 Support:** A toggle switch labeled 'Enabled' is turned on.
- 2. Specify the method to be used to obtain your WAN IPv6 Address:** The 'IPv6 WAN Configuration' dropdown is set to 'None'. The 'WAN Link-Local Address' field is empty.
- 3. Specify the method to be used to assign LAN IPv6 addresses:** The 'IPv6 LAN Configuration' dropdown is open, showing three options: 'stateless' (selected), 'Stateless', and 'Stateful (DHCPv6)'. The 'LAN Link-Local Address' field is empty. The 'Router Advertisement Lifetime' is set to 'no' minutes (0-150).

At the bottom, there is an 'Option' section with a checkbox labeled 'Allow ICMPv6 Echo Requests for LAN devices using their global IPv6 Address from WAN side', which is checked. An 'Apply Changes' button is located in the top right corner.

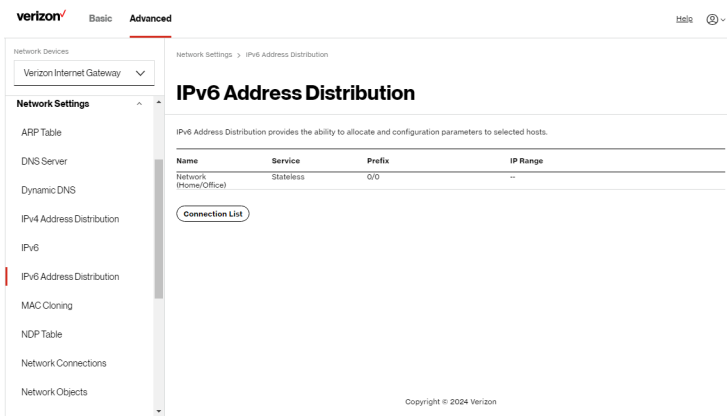
2. Specify the settings to be used to assign LAN IPv6 addresses by entering the following details:
 - **IPv6 LAN Configuration** (select **Stateless** from the dropdown list)
 - **LAN Link Local Address** (automatically populated)
 - **Router Advertisement Lifetime** (minutes between 0-150)
 - **Option: Allow ICMPv6 Echo Request for LAN devices using their Global IPv6 Address from WAN side** - requesting an IPv6 address from any available DHCPv6 servers available on the ISP
3. After entering all appropriate IPv6 settings, click **Apply changes** to have changes take effect.

NETWORK SETTINGS

5.1f/ IPV6 ADDRESS DISTRIBUTION

To view a summary of the services provided by the DHCP server:

1. Select **IPv6 Address Distribution** in the **Network Settings** section.



2. You can edit the DHCP server settings for a device. On the **IPv6 Address Distribution** page, click the **Edit** icon on the screen column. The DHCP Settings page opens with the device information displayed.
3. To configure the DHCP server complete the following fields:
 - **Start IPv6 Address** – the starting IPv6 address in the consecutive list of addresses that makes up this LAN pool for the DHCPv6 server.
 - **End IPv6 Address** – the ending IPv6 address in the consecutive list of addresses that makes up this LAN pool for the DHCPv6 server.