



Verizon
Internet
Gateway
for Business

USER GUIDE



CONTENTS

01/

INTRODUCTION

- 1.0 Inside the box 5
- 1.1 Getting to Know Your Verizon Internet Gateway for Business 5
- 1.2 Setting Up Your Verizon Internet Gateway for Business 9

02/

CONFIGURING YOUR VERIZON INTERNET GATEWAY FOR BUSINESS

- 2.0 Configure Your Verizon Internet Gateway for Business 15
- 2.1 Computer Network Configuration 19
- 2.2 Main Screen 26

03/

WI-FI SETTINGS

- 3.0 Overview 34
- 3.1 Basic Settings 35
- 3.2 Advanced Settings 44

04/

CONNECTED DEVICES

- 4.0 Device Settings 52
- 4.1 Setting Content Controls 57
- 4.2 Universal Plug & Play 61

05/

CONFIGURING ADVANCED SETTINGS

- 5.0 Security & Firewall 68
- 5.1 Network Settings 84
- 5.2 Diagnostics & Monitoring 118
- 5.3 System 124

06/

TROUBLESHOOTING

- 6.0 Troubleshooting Tips 142
- 6.1 Frequently Asked Questions 149

07/

SPECIFICATIONS

- 7.0 General Specifications 156
- 7.1 Connections 157

08/

NOTICES

- 8.0 Regulatory Compliance Notices 160

01 /

INTRODUCTION

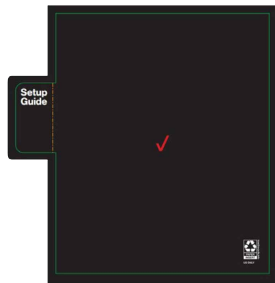
- 1.0** Inside the box
- 1.1** Getting to Know Your Verizon Internet Gateway for Business
- 1.2** Setting Up Your Verizon Internet Gateway for Business

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 Internet Gateway for Business
- Setup guide
- Power adapter
- Ethernet cable



1.1/ GETTING TO KNOW YOUR VERIZON INTERNET GATEWAY FOR BUSINESS

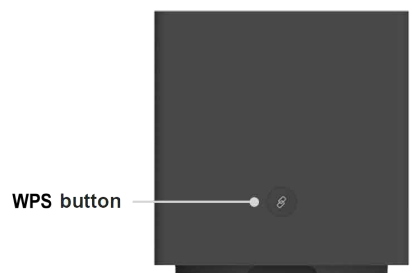
Your Verizon Internet Gateway for Business provides fast dual-band Wi-Fi (with channel steering) for all your devices, and features built-in network security as well as contents controls, guest Wi-Fi and automatic software updates.

Take a moment to familiarize with your product:

Front



Back



Bottom



GETTING TO KNOW YOUR VERIZON INTERNET GATEWAY FOR BUSINESS

1.1a/ RESET BUTTON

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

1.1b/ WPS BUTTON

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 41 for more information.

1.1c/ LED

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

Front LED Mode	Status	LED Pattern
Bootup	System Off	Off
	System Booting	Soft Blink White
	Firmware update (FOTA)	Fast Blink White

Front LED Mode	Status	LED Pattern
Cellular signal (or after single click pair button)	Passing signal	Solid White
	No Signal/Cold SIM	Solid Red
	No SIM Card	Hard Blink Red
Regular usage	Setup complete	50% Bright White
	Wi-Fi disabled by user	Solid Green
Paring	WPS Paring	Hard blink Blue
Other	Factory Reset	Fast blink yellow
	FW Error	Soft blink red

Note: Installation mode lasts for 45 minutes only during first bootup, after which the Verizon Internet Gateway for Business will switch to regular usage mode.

SETTING UP YOUR VERIZON INTERNET GATEWAY

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 YOUR VERIZON INTERNET GATEWAY FOR BUSINESS

Your Verizon Internet Gateway for Business comes with a pre-installed SIM card and can be up and running in just a couple of minutes. The SIM card is only authorized for use in the Verizon Internet Gateway for Business. You may not remove the SIM card and insert it into another device.

1.2a/ POSITIONING YOUR VERIZON INTERNET GATEWAY FOR BUSINESS

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

- Place the Gateway in a central area near a window.
- Avoid keeping the device in the basement to get better signal.
- Avoid having obstacles near the device, clear any objects near the window that could interfere with getting a signal.
- Keep the 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/ SETUP REQUIREMENTS

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

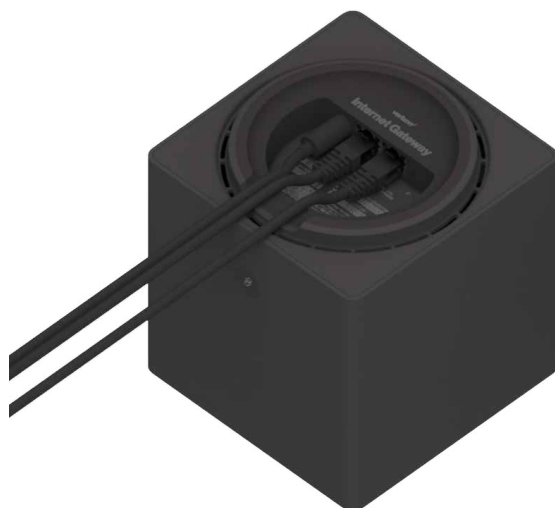
- For Wired Connection: Ethernet RJ-45 (LAN) port (10Base-T/100Base-TX/1000Base-TX)
- For Wi-Fi Connection: IEEE 802.11a/b/g/n/ac/ax wireless capability
- An installed TCP/IP service
- Web browser such as Microsoft Edge, Firefox, Safari, or Google Chrome

SETTING UP YOUR VERIZON INTERNET GATEWAY

1.2c/ SETTING UP

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

1. Plug the Verizon Internet Gateway for Business into a power outlet with the included power adapter.
2. Wait for a couple of minutes for the Gateway to power up and establish an LTE/5G connection. The LED should display on (white) after starting up.
3. That's it! You can connect your wireless devices to the Gateway's Wi-Fi networks named Verizon_<your network> (check your Gateway's product label on the bottom side for your unique Wi-Fi network name and password). You can also connect Internet devices to your Gateway by connecting the device's LAN ports with an Ethernet cable.



- Wi-Fi Network

You can automatically connect your device to the Gateway by scanning the QR code on the product label.

To connect manually:

- i. Scan available Wi-Fi networks with your mobile device.
- ii. Select the Wi-Fi network named Verizon_<your network> from the list of discovered Wi-Fi networks. Check your Gateway's product label on the bottom side for your unique Wi-Fi network name.
- iii. Enter the password that is printed next to the Password on the label on the bottom of your Gateway.

The Verizon Internet Gateway for Business has one Wi-Fi name supporting 2.4 GHz and 5 GHz signals. The Self-Organizing Network (SON) feature lets your devices move between the two signals automatically for an optimized Wi-Fi connection.

4. Go to 2.2/ Main Screen to login to your Gateway and configure settings such as Wi-Fi security.

02 /

CONFIGURING YOUR VERIZON INTERNET GATEWAY FOR BUSINESS

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

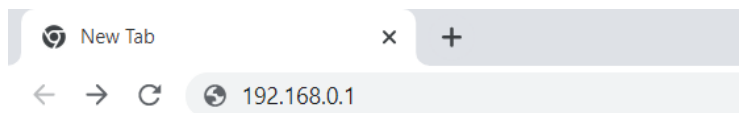
Connecting your Verizon Internet Gateway for Business and accessing its web-based User Interface (UI) are both simple procedures.

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

CONFIGURE YOUR VERIZON INTERNET GATEWAY FOR BUSINESS

2.0/ CONFIGURE YOUR VERIZON INTERNET GATEWAY FOR BUSINESS

1. Open a web browser on the device connected to your Verizon Internet Gateway for Business network.
2. In the browser address field (URL), enter: <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

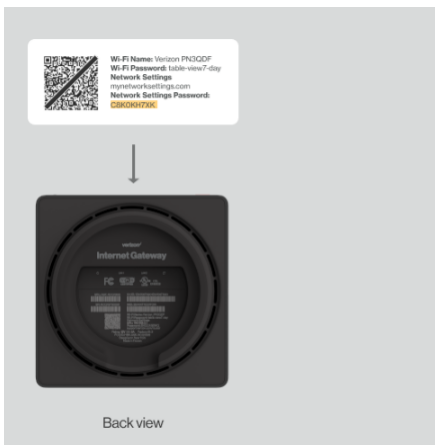
This server could not prove that it is 192.168.0.1; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

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

- 4. The login screen will appear.

The first time you access your Verizon Internet Gateway for Business, 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 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

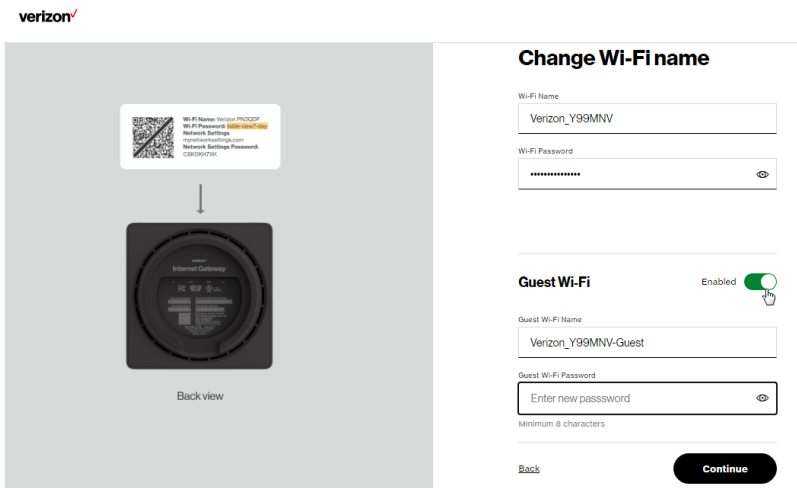
Keep Me Signed In ⓘ

Log In



CONFIGURE YOUR VERIZON INTERNET GATEWAY FOR BUSINESS

6. Click **Continue**. 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.

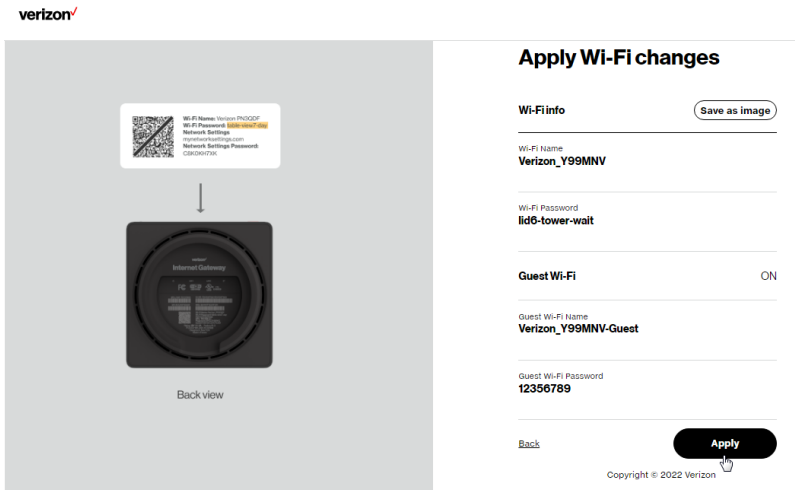


For your protection, your Verizon Internet Gateway for Business is pre-set at the factory to use WPA2 (Wi-Fi Protected Access II) encryption for your Wi-Fi network. This is the best setting for most users and provides security.

7. Click **Continue**. The **Apply Wi-Fi changes** screen appears. You have an option of saving the Wi-Fi settings as an image on your device by clicking the **Save as image** button. After you click **Save as image** to save your Wi-Fi settings as an image, click **Apply** to save the Wi-Fi changes to your Verizon Internet Gateway for Business.

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.



verizon

Wi-Fi Name: Verizon_790000
 Wi-Fi Password: 1234567890
 Network Settings: http://myverizon.com
 Network Settings Password: 00000000

Back view

Apply Wi-Fi changes

Wi-Fi info Save as image

Wi-Fi Name
Verizon_Y99MNV

Wi-Fi Password
ld6-tower-wait

Guest Wi-Fi ON

Guest Wi-Fi Name
Verizon_Y99MNV-Guest

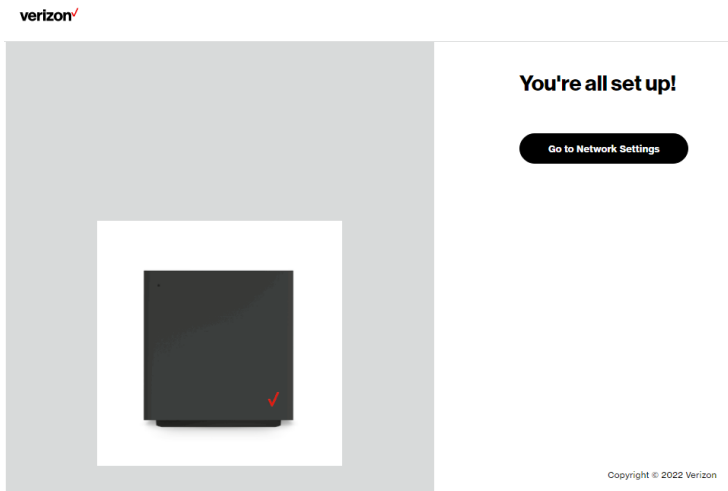
Guest Wi-Fi Password
12356789

[Back](#) Apply

Copyright © 2022 Verizon

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 Verizon Internet Gateway for Business.

CONFIGURE YOUR VERIZON INTERNET GATEWAY FOR BUSINESS



If your Verizon Internet Gateway for Business 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 Verizon Internet Gateway for Business 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 Verizon Internet Gateway for Business configuration).

MACINTOSH OS X

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

2.1b/ CONNECTING OTHER COMPUTERS AND NETWORK DEVICES

You can connect your Verizon Internet Gateway for Business 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 bottom 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.

COMPUTER NETWORK CONFIGURATION

CONNECTING A WI-FI DEVICE USING WPS

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

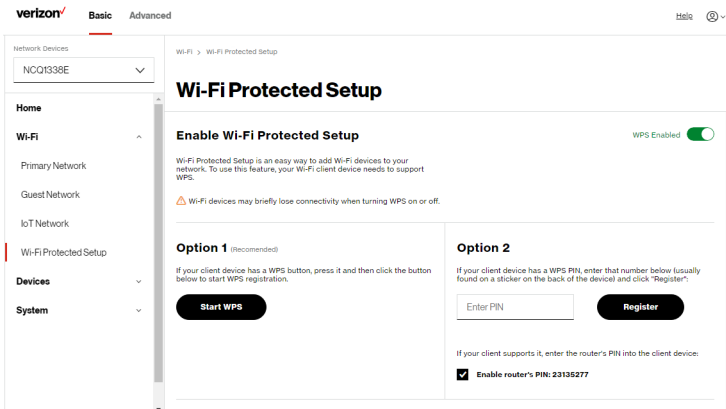
In most cases, this only requires the pressing of two buttons – one on your Gateway and one on the Wi-Fi client. This could be either a built-in button or one on a compatible Wi-Fi adapter/card, or a virtual button in software. Once completed, this allows Wi-Fi clients to join your Wi-Fi network.

To initialize the WPS process, you can either press and hold the WPS button located on the rear 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.

COMPUTER NETWORK CONFIGURATION

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 front of 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 Verizon Internet Gateway for Business 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 Verizon Internet Gateway for Business.

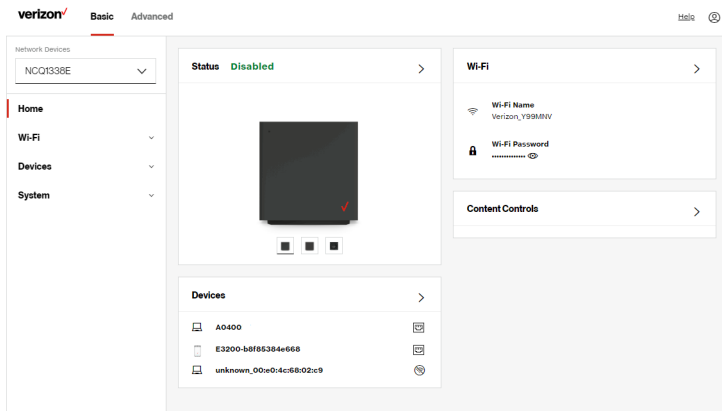


5. Verify the changes were implemented by using the device's web browser to access a site on the internet.
6. Repeat these steps for every device that you are connecting with Wi-Fi to your Gateway.

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, Parental Controls, and connection status, and Basic quick links.

MAIN SCREEN



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 Internet Gateway for Business and Wi-Fi extender(s) (if connected).

The screenshot shows the Verizon System Status page. The top navigation bar includes the Verizon logo, tabs for 'Basic' and 'Advanced', and a 'Help' icon. A dropdown menu for 'Network Devices' is set to 'NCO1338E'. The left sidebar contains navigation links: Home, Wi-Fi, Devices, System, System Status (highlighted), and Open Source Software. The main content area is titled 'System Status' and features an 'Auto-refresh' toggle and a 'Refresh' button. The page is divided into two columns: 'Broadband IPv4' and 'Broadband IPv6'.

Broadband IPv4	Broadband IPv6
Status Disabled	Status Disconnected
IPv4 address is from:	IPv6 address is from: Cellular Modem
IPv4 address	Assigned Prefix /
Subnet Mask	IPv6 Address
IPv4 Default Gateway	Link-Local Address fe80::200:f1fe00:0
IPv4 DNS Address 1	IPv6 Default Gateway
IPv4 DNS Address 2	IPv6 DNS Address 1
NATs Supported (used / max)	IPv6 DNS Address 2

MAIN SCREEN

verizon **Basic** Advanced Help ⓘ

Network Devices
NCO1338E

Home
Wi-Fi
Devices
System
System Status
Open Source Software

System > System Status

System Status

Auto-refresh **Refresh**

Modem

Firmware Version
223111

Mobile Number
-

IMEI
357776720000029

ICCID
-

Sim Status
Absent

Roaming Status
-

4G LTE Signal Strength
-

5G Signal Strength
-

verizon **Basic** Advanced Help ⓘ

Network Devices
NCO1338E

Home
Wi-Fi
Devices
System
System Status
Open Source Software

System > System Status

System Status

Auto-refresh **Refresh**

Router

Firmware Version
3.2.0.11

Hardware Version
1

Model Name
ASK-NCO1338E

Serial Number
AA13600002

LAN IPv4 Address
192.168.0.1

Broadband Physical Connection
Cellular

Router has been active for
0 day(s) 2 hours 31 minutes 39 seconds

LED Status
Self activation

The screenshot shows the Verizon Business System Status page for a device with Network ID NCG1338E. The left sidebar contains navigation options: Home, Wi-Fi, Devices, System, System Status (selected), and Open Source Software. The main content area is titled "System Status" and includes an "Auto-refresh" toggle and a "Refresh" button. The "Extender" section displays the following information:

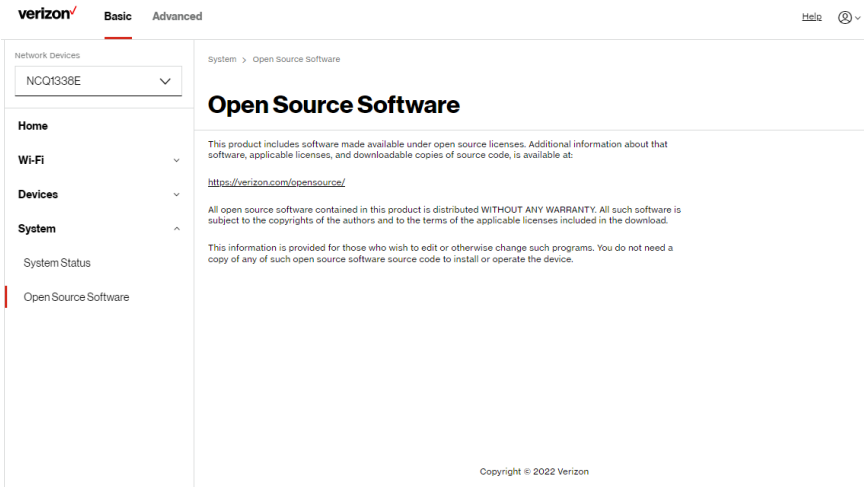
- Device Name: E3200-b8f85384e668
- Model name: E3200
- Firmware Version: 3.1115
- Hardware Version: 1102
- Serial Number: E301120071800005
- MAC Address: B8:F8:53:84:E6:68
- System Up Time: 0 day(s) 2 hours 31 minutes 24 seconds
- LED Status: Normal operation

This screenshot shows the same Verizon Business System Status page, but with the "Ethernet" section expanded. The "System Up Time" is now visible at the top of the main content area. The "Ethernet" section displays the following information:

- LED Status: Normal operation
- Backhaul Type: Ethernet
- Bit Rate: 1.0 Gbps
- IPv4 Address: 192.168.0.100
- IPv6 Address: (empty field)
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.0.1

MAIN SCREEN

OPEN SOURCE SOFTWARE



The screenshot displays the Verizon Open Source Software page. At the top left, the Verizon logo is followed by 'Basic' (underlined) and 'Advanced' tabs. On the top right, there is a 'Help' link and a user profile icon. The left navigation pane includes 'Network Devices' (with a dropdown menu showing 'NCO1338E'), 'Home', 'Wi-Fi', 'Devices', 'System' (highlighted with a red bar), 'System Status', and 'Open Source Software'. The main content area shows the breadcrumb 'system > Open Source Software', the title 'Open Source Software', and a disclaimer: 'This product includes software made available under open source licenses. Additional information about that software, applicable licenses, and downloadable copies of source code, is available at: <https://verizon.com/opensource/>. All open source software contained in this product is distributed WITHOUT ANY WARRANTY. All such software is subject to the copyrights of the authors and to the terms of the applicable licenses included in the download. This information is provided for those who wish to edit or otherwise change such programs. You do not need a copy of any of such open source software source code to install or operate the device.' At the bottom right, it says 'Copyright © 2022 Verizon'.

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

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

OVERVIEW

3.0/ OVERVIEW

Your Verizon Internet Gateway for Business 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.

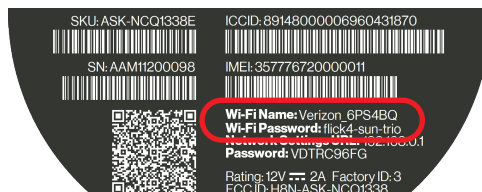
802.11b has a maximum data rate of 11 Mbps, 802.11a and 802.11g have a maximum data rate of 54 Mbps, 802.11n has a maximum data rate of 450 Mbps, 802.11ac has a maximum data rate of 3.12 Gbps, and 802.11ax has a maximum data rate of 4.8 Gbps.

802.11b and g standards operate in the 2.4 GHz range. 802.11ac operates in the 5 GHz range. 802.11n and ax operate in both the 2.4 GHz and 5 GHz ranges.

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

The Wi-Fi service and Wi-Fi security are activated by default. The level of security is preset to WPA2 encryption using a unique default WPA2 key (also referred to as a passphrase or password) pre-configured at the factory. This information is displayed on a sticker located on the bottom of your Verizon Internet Gateway for Business.

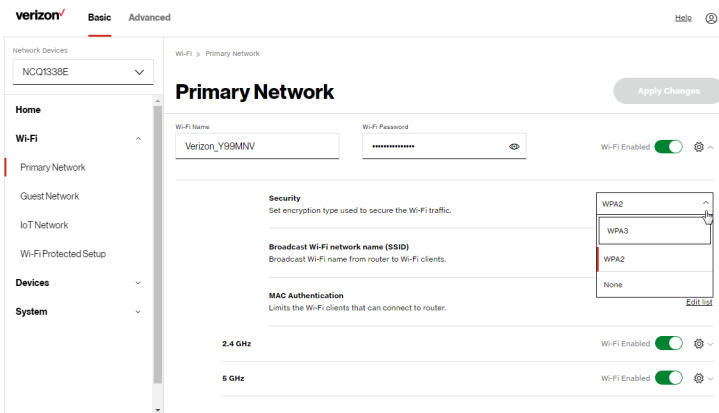
Your Gateway integrates multiple layers of security. These include Wi-Fi Protected Access, and firewall.



3.1/ BASIC SETTINGS

3.1a/ PRIMARY NETWORK

You can configure the basic security settings for either 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**.
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.

BASIC SETTINGS

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.

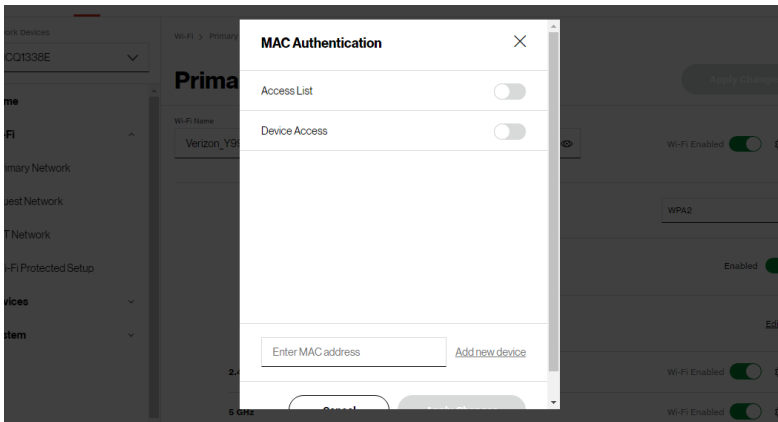
- **Broadcast Wi-Fi network name (SSID)**

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**.

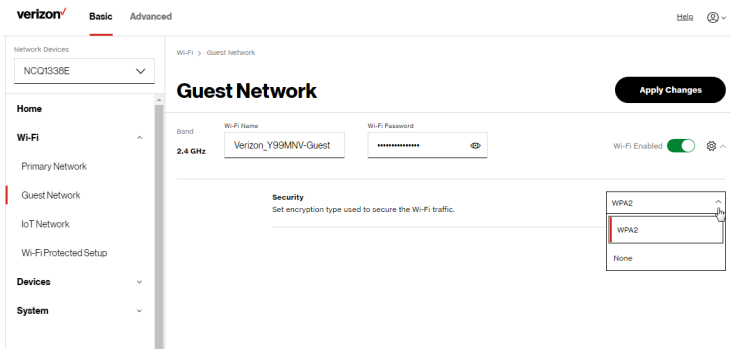
BASIC SETTINGS

4. Repeat step 2 and step 3 to add additional devices, as needed.
5. When all changes are complete, click **Apply Changes** to save the changes.

3.1b/ GUEST NETWORK

The **Guest Network** is designed to provide internet connectivity to your guests 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 Internet Gateway for Business 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.

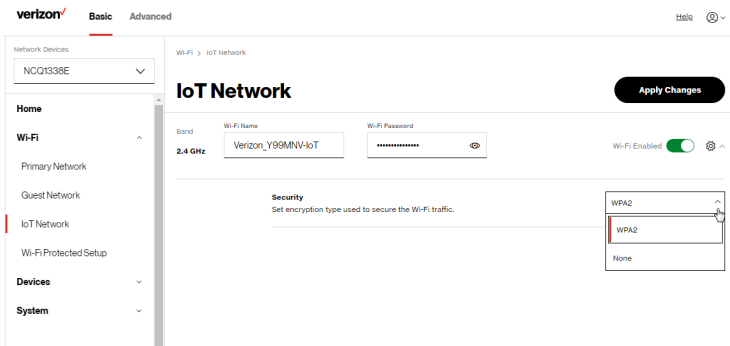
Important: It is not recommended to create a guest network without a password.

BASIC SETTINGS

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 Verizon Internet Gateway for Business 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”.



To enable IoT Wi-Fi link:

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

3.1d/ WI-FI PROTECTED SETUP (WPS)

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

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

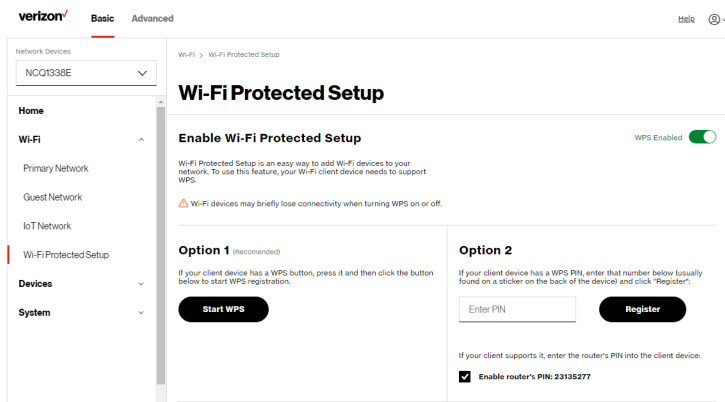
To initialize the WPS process, you can either press and hold the WPS button located on the rear of your Gateway for more than two seconds or use the UI and press the on-screen button.

BASIC SETTINGS

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

To access WPS using the user interface:

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



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 the front of 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 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.*

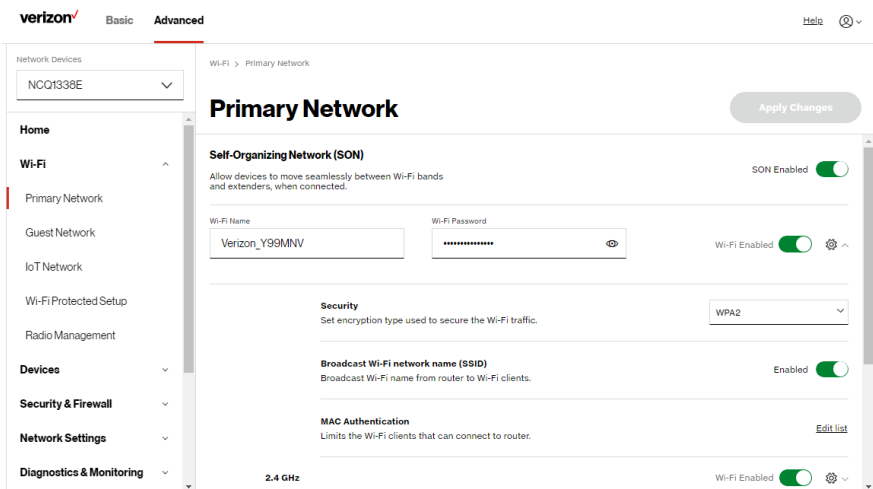
ADVANCED SETTINGS

3.2/ ADVANCED SETTINGS

3.2a/ PRIMARY NETWORK

Self-Organizing Network (SON)

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



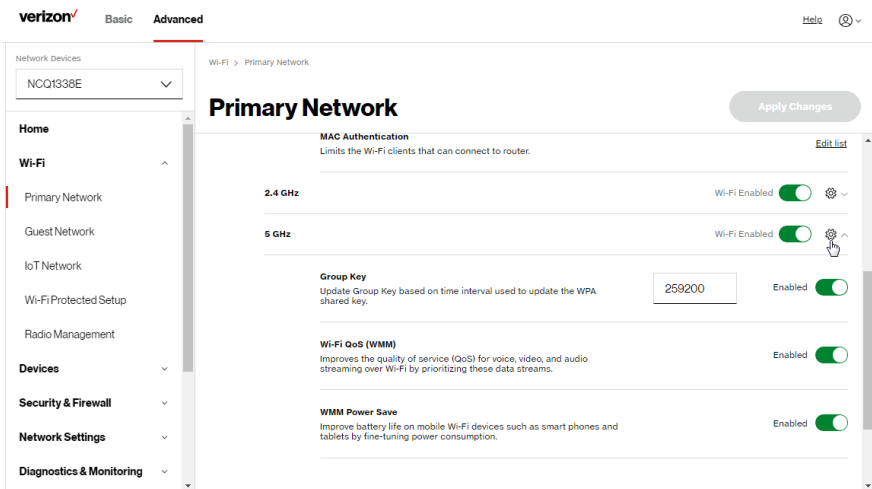
To configure SON, Wi-Fi radio, SSID and security settings:

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.
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.



The screenshot displays the Verizon Business Gateway Advanced settings for the Primary Network. The network name is NCO1338E. The MAC Authentication section is expanded, showing settings for 2.4 GHz and 5 GHz bands, both with 'Wi-Fi Enabled' toggles turned on. The 'Group Key' section shows a '259200' interval and an 'Enabled' toggle. Other sections include 'Wi-Fi QoS (WMM)' and 'WMM Power Save', both also enabled. An 'Apply Changes' button is visible in the top right.

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.

ADVANCED SETTINGS

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

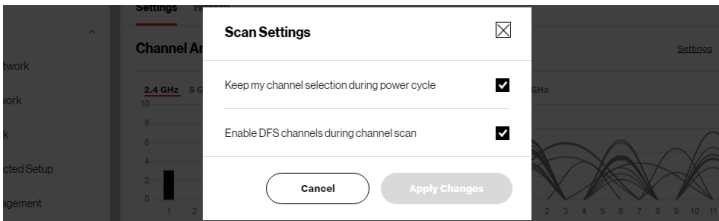
3.2b/ RADIO MANAGEMENT

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

The screenshot shows the Verizon Wi-Fi management interface. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' selected. The page title is 'Radio Management'. On the left, a navigation menu includes 'Home', 'Wi-Fi', 'Primary Network', 'Guest Network', 'IoT Network', 'Wi-Fi Protected Setup', 'Radio Management' (highlighted), 'Devices', 'Security & Firewall', 'Network Settings', and 'Diagnostics & Monitoring'. The main content area is titled 'Radio Management' and has an 'Apply Changes' button. Below this, there are two tabs: 'Settings' (selected) and 'History'. The 'Settings' tab contains a 'Channel Analysis' section with two graphs: a bar chart for '2.4 GHz' and a line graph for '5 GHz'. The 2.4 GHz bar chart shows signal strength across channels 1-11, with channel 11 having the highest signal. The 5 GHz line graph shows signal strength across channels 1-14. Below the graphs, it says 'Recent scan: Wait for NTP server to synchronize'. The 'Channel Settings' section at the bottom shows 'Band' set to '2.4 GHz', 'Channel' set to 'Ch. 1 (Auto)', 'Width' set to '20/40MHz', and 'Health' at '3.07'. A 'Radio Enabled' toggle switch is turned on.

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 Verizon Internet Gateway for Business 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 Verizon Internet Gateway for Business to identify the radio channels providing the best Wi-Fi performance.

ADVANCED SETTINGS

4. On the **Radio Management** page for either 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 router 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.
 - **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 and ax devices can connect.

- Legacy – This is the default mode setting on 2.4 GHz, providing broad connection support for old and new Wi-Fi devices. 802.11a,b,g,n and ac devices can connect.

Notes:

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

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

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.

The screenshot shows the Verizon Business Internet Gateway interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. The left sidebar contains a navigation menu with categories like Home, Wi-Fi, Devices, Security & Firewall, Network Settings, and Diagnostics & Monitoring. The main content area is titled 'Radio Management' and has two tabs: 'Settings' and 'History'. The 'History' tab is active, displaying a table with the following data:

Band	Channel	Time	Date
2.4 GHz	Ch. 11	N/A	N/A
2.4 GHz	Ch. 6	N/A	N/A
5 GHz	Ch. 140	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. 6	N/A	N/A
5 GHz	Ch. 112	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 Internet Gateway for Business.

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

With that question in mind, the Content Controls of your Verizon Internet Gateway for Business 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.

Network Devices

Basic Advanced

Home

Wi-Fi

Devices

Devices 2

Content Controls 0

System

Devices > Devices > All

Devices Add Device

All (2) Primary (2) Guest (0) IoT (0)

Online

Name	Connection	Connected to	MAC address	Content Controls
A0400	Ethernet	NGQ1338E	48-5b-39-4f-56-08	None
E3200-b8f653d4e668	Ethernet	NGQ1338E	b8-f8-53-04-e6-68	None

Offline

unknown_00e0-4c-6802c9	Offline	NGQ1338E	00e0-4c-6802c9	None
------------------------	---------	----------	----------------	------

Network Devices

Basic Advanced

Home

Wi-Fi

Devices

Devices 2

Content Controls 0

System

Devices > Devices > All

Devices Add Device

All (2) Primary (2) Guest (0) IoT (0)

Online

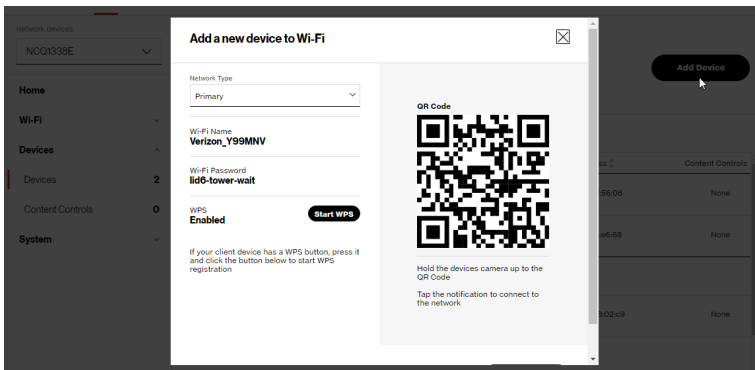
Connection	Connected to	MAC address	Content Controls	Block/Allow
Ethernet	NGQ1338E	48-5b-39-4f-56-08	None	<input checked="" type="checkbox"/>
Ethernet	NGQ1338E	b8-f8-53-04-e6-68	None	<input checked="" type="checkbox"/>

Clear list

Offline

Offline	NGQ1338E	00e0-4c-6802c9	None	<input checked="" type="checkbox"/>
---------	----------	----------------	------	-------------------------------------

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 41 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.

DEVICE SETTINGS

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 57.

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

The screenshot shows the Verizon Device Settings interface. At the top, there are tabs for 'Basic' (selected) and 'Advanced'. The page title is 'Device Settings' with a 'Save' button. On the left, a navigation menu includes 'Home', 'Wi-Fi', 'Devices' (with a sub-menu for 'Devices' showing 2 items), 'Content Controls' (0 items), and 'System'. The main content area is titled 'Device Information' and includes an 'Edit' button and a 'Reset to Default' button. The device is identified as 'Extender' and is 'Online'. Fields include 'Name' (E3200-b8185384e668), 'Host Name' (E3200-b8185384e668), 'Location' (a dropdown menu), and 'Mobility' (Portable). Below this is the 'Device Add-Ons' section, which includes 'Port Forwarding' and 'DMZ host'.

This screenshot shows the 'Device Add-Ons' and 'Device Connection' sections of the Verizon Device Settings page. The 'Device Add-Ons' section includes 'Port Forwarding' (N/A) and 'Access Control' (N/A), both with gear icons. The 'Device Connection' section includes 'Connection Info' and 'Network Info'. 'Connection Info' shows 'Connection' as Ethernet and 'Phy Rate / Modulation Rate' as 1000 Mbps. 'Network Info' shows 'Mac Address' as b8:18:53:84:e6:68, 'Connected to' as NCI01338E, 'IPv4 Address' as 192.168.0.100, and 'Subnet Mask' as 255.255.255.0. The 'DMZ host' and 'DNS Server' are both listed as N/A.

The screenshot shows the Verizon Business Internet Gateway interface. The top navigation bar includes the Verizon logo, 'Basic' (selected), and 'Advanced' tabs. A breadcrumb trail reads 'Devices > Devices > Device Settings'. The left sidebar contains a 'Network Devices' dropdown menu with 'NQ01338E' selected, and a list of categories: Home, Wi-Fi, Devices (with a count of 2), Content Controls (with a count of 0), and System. The main content area is titled 'Device Settings' and features a 'Save' button. The configuration fields are as follows:

- Subnet Mask: 255.255.255.0
- IPv4 DNS: 192.168.0.1
- IPv4 Address Allocation: Dynamic
- Lease Type: DHCP
- DHCP lease time remaining: 1261 minutes 12 seconds
- IPv6 LAN Prefix: 2001:470:f29:c713::/64
- IPv6 Global: [empty]
- IPv6 Type / Address Allocation: Stateless
- IPv6 link-local: [empty]

This screenshot shows the same Verizon Business Internet Gateway interface, but with the IPv6 configuration fields visible. The layout and navigation are identical to the previous screenshot. The configuration fields are:

- IPv6 Type / Address Allocation: Stateless
- IPv6 link-local: [empty]
- IPv6 DNS: 2001:0470:FD29:C713:8ADE:7CFF:FE52:9A00
- Network Connection: Bridge
- Ping Test: Test Connectivity
- Time on the network: 2 hour(s) 58 minutes 48 seconds

– Device Information:

- **Device Type, Name/Host Name, Location, and Mobility** - Displays the current known information of the device. These can be updated or corrected as needed. Click **Edit** and **Save** to apply any changes.

DEVICE SETTINGS

- This section also provides the device MAC Address, Access Point information the device is connected to as well as the IPv4 Address of the device.

– Device Add-Ons

Port Forwarding - Port Forwarding allows your network to be exposed to the internet in specific limited and controlled ways. For example, you could allow specific applications, such as gaming, voice, and chat, to access servers in the local network. To access the Port Forwarding page, click the setup button.

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

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

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

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

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

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

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

– Device Connection

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

4.1/ SETTING 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.

The screenshot shows the Verizon Business Gateway web interface. The top navigation bar includes the Verizon logo, 'Basic' (selected), and 'Advanced' tabs. A breadcrumb trail reads 'Devices > Content Controls > All'. The main content area is titled 'Content Controls' and features a 'New Rule' button. Under the 'Rule Templates' section, three templates are displayed: 'Bedtime' (No Wi-Fi 9pm - 8am), 'School Day' (School Sites Only 8am - 3pm), and 'Off Limits' (Blocked Sites Always on). Below this, the 'Active Rules' section shows a single rule named 'test' with the following details: 'All Internet Off Mon,Tue,Wed,Thu,Fri 12:00 am - 12:00 am', 'unknown_00e04c8b62c9', and 'Enabled' (indicated by a green toggle switch). 'Remove' and 'Edit' buttons are visible for the active rule.

SETTING CONTENT CONTROLS

To limit device access:

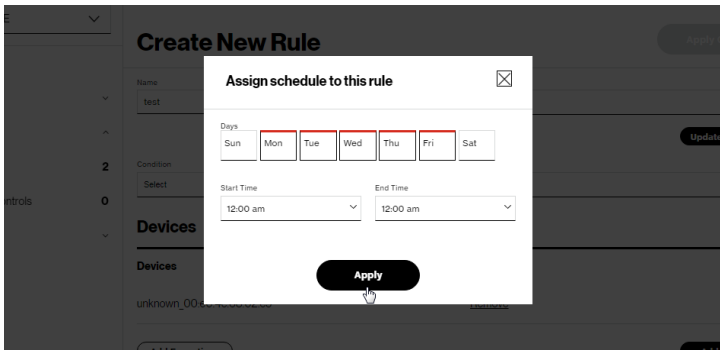
1. From the **Basic** menu, select **Devices** from the left pane and then click **Content Controls**.
2. To use the default **Rule Templates**, select one of the pre-defined rules as shown on screen to quickly setup access policy for devices on your network.
3. To create a new access policy, click on the **New Rule** and the configuration page displays.

The screenshot shows the Verizon network management interface. The top navigation bar includes the Verizon logo, 'Basic' (selected), and 'Advanced'. On the right, there are links for 'Help' and a user profile icon. The left sidebar contains a navigation menu with 'Home', 'Wi-Fi', 'Devices', 'Content Controls', and 'System'. The 'Content Controls' section is active, showing a list of rules: 'Internet is always on' (2 devices), 'Internet is always off' (0 devices), and 'Internet is always on' (1 device). The main content area is titled 'Create New Rule' and contains the following fields and buttons:

- Name:** A text input field containing 'test'.
- Schedule:** A dropdown menu set to 'User defined'.
- Condition:** A dropdown menu set to 'Internet is always on'.
- Devices:** A dropdown menu set to 'User defined'.
- Action:** A text input field containing 'unknown_00:e0:4c:68:02:c9'.

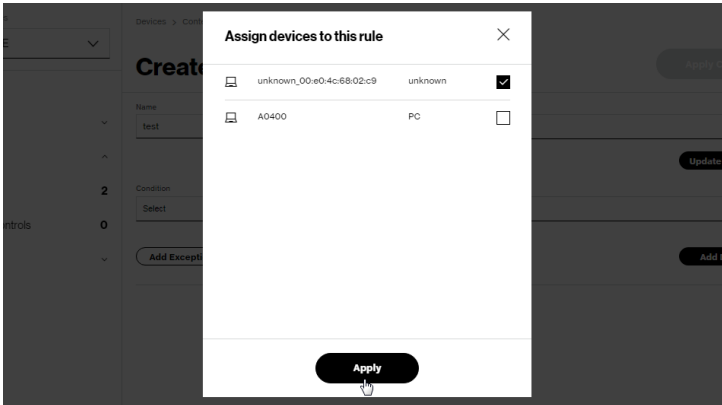
Buttons include 'Apply Changes' (top right), 'Update Schedule' (below Schedule), 'Add Exceptions' (bottom left), and 'Add Devices' (bottom right).

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

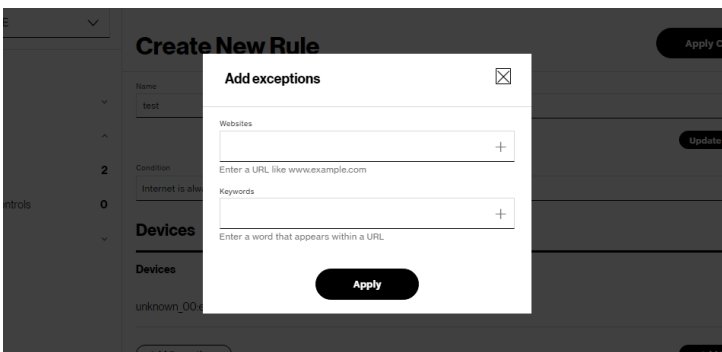


6. Select the days of the week when the rule will be active or inactive.
7. Set the time when the rule will be active or inactive, then specify the start time and end time.
8. Click **Apply** to save changes.
9. Select the **Condition** rule of **Internet is always off/Internet is always on** to block/allow 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.

SETTING CONTENT CONTROLS



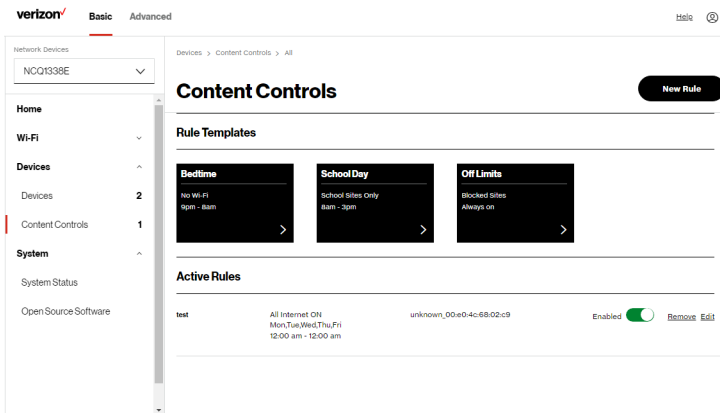
11. Click **Apply** to save changes.
12. To remove a device from the list, click **Remove** for the assigned device.
13. Click **Add Exceptions** for the following exception options:
 - Enter the name of the website or keywords within a URL to block/allow the specified websites and websites with names containing the specified keyword.



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

4.1b/ ACTIVE RULES

You can view the rules created for your Verizon Internet Gateway for Business 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 Verizon Internet Gateway for Business.

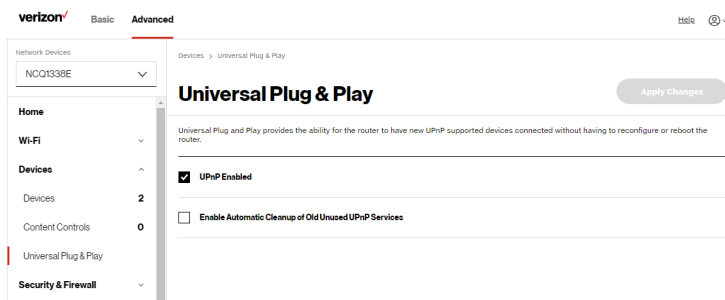
In addition, you can enable the automatic cleanup of invalid rules. When enabled, this functionality verifies the validity of all UPnP services and rules every five minutes. Old and unused UPnP defined services are removed, unless a user-defined rule depends on it.

UNIVERSAL PLUG & PLAY

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

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

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.

SECURITY & FIREWALL

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

For example, when accessing a website on the internet, a request is sent to the internet for this site. When the request reaches your Verizon Internet Gateway for Business, 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:

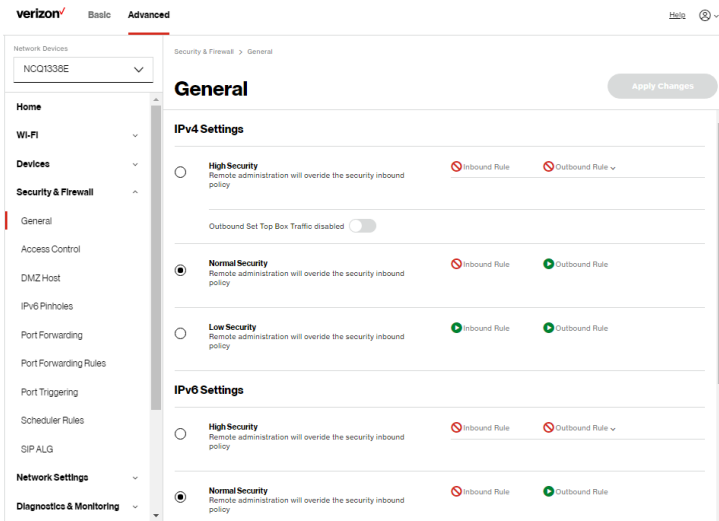
- Blocked traffic – no access allowed, except as configured in Port Forwarding and Remote Access
- Limited – permits only commonly used services, such as email and web browsing
- Unrestricted – permits full access of incoming traffic from the internet and allows all outgoing traffic, except as configured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

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.

SECURITY & FIREWALL



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

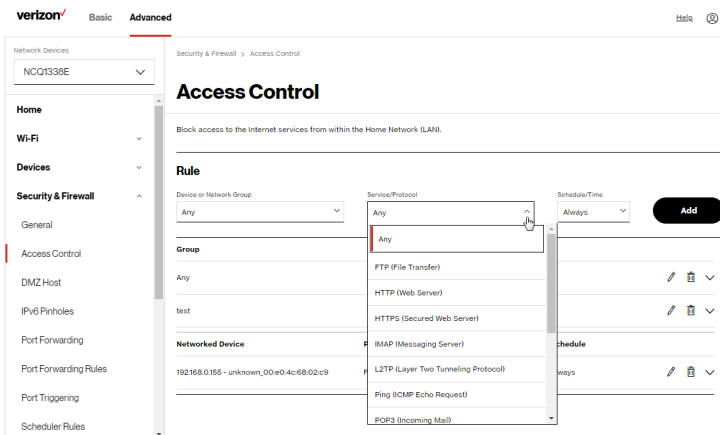
You can block individual computers on your local network from accessing specific services on the internet. For example, you could block one computer from accessing the internet, then block a second computer from transferring files using FTP as well as prohibit the computer from receiving incoming email.

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

ALLOW OR RESTRICT SERVICES

To allow or restrict services:

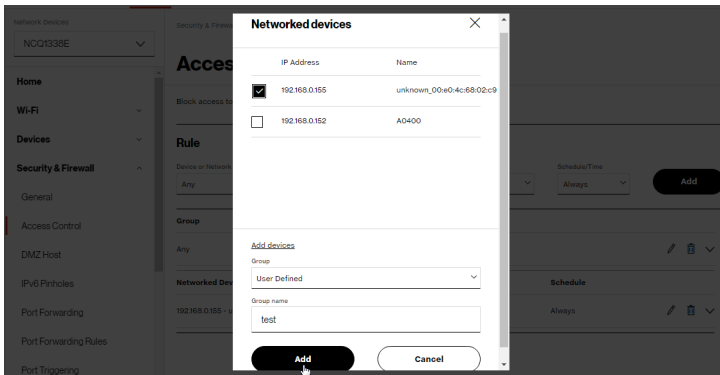
1. From the **Advanced** menu, select **Security & Firewall** from the left pane and then click **Access Control**. The **Access Control** page opens with the allowed and blocked status displayed. The allowed section only displays when the firewall is set to maximum security.



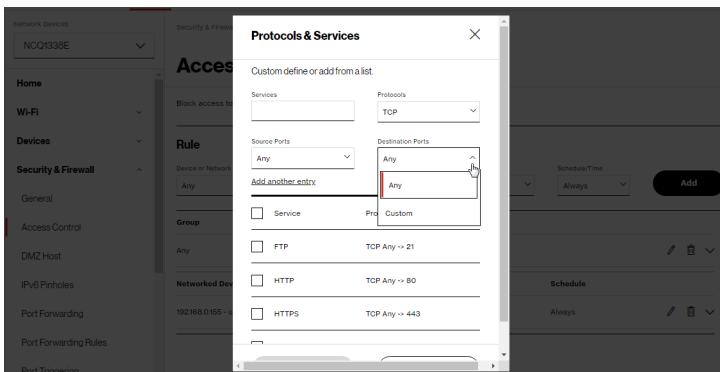
2. To apply the rule to:
 - Networked Device or Network Group - select **Any**.
 - Specific devices only – select networked device or **User Defined**.
3. Select the networked device to be allowed or blocked in the list.

SECURITY & FIREWALL

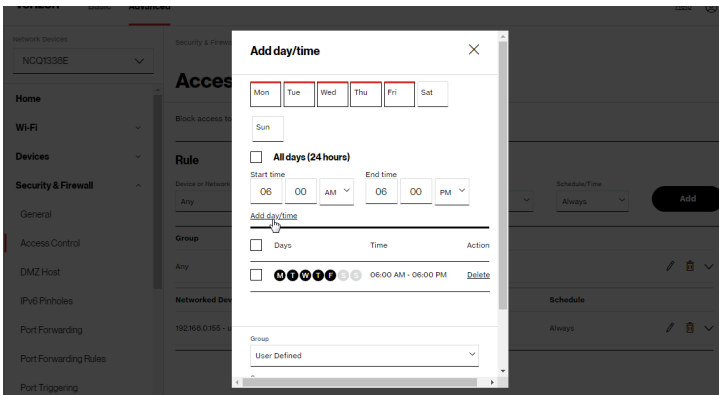
4. In the **Add devices**, enter the group name, then click **Add**. The new network group is automatically added to the **Access Control** section.



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.
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.

SECURITY & FIREWALL

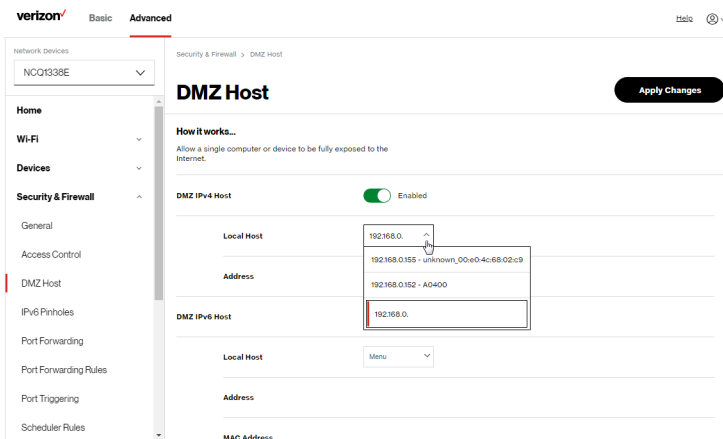
5.0c/ DMZ HOST

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 Verizon Internet Gateway for Business 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**.

The screenshot shows the Verizon Internet Gateway for Business configuration interface. The top navigation bar includes the Verizon logo, 'Basic', 'Advanced', and 'Help' options. The left sidebar lists various settings categories: Network Devices, Home, Wi-Fi, Devices, Security & Firewall (selected), Access Control, DMZ Host, IPv6 Pinholes (highlighted), Port Forwarding, Port Forwarding Rules, Port Triggering, and Scheduler Rules. The main content area is titled 'IPv6 Pinholes' and includes a 'How it works...' section, a 'Create Rule' section with dropdowns for 'External Host', 'Internal Host', 'Protocol', and 'Schedule', and a 'Rules List' section. A right-hand panel shows a list of applications and ports, with 'Select application / ports...' selected. An 'Add to list' button is visible at the bottom right of the application list.

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.

SECURITY & FIREWALL

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 Port 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.

Network Devices: NCO1338E

Security & Firewall > Port Forwarding

Port Forwarding

Apply Changes

Open a tunnel between remote computers and a device port on your Home Network (LAN). Supports gaming, IoT, home security devices and more.

Create Rule

Application	Original Port	Protocol
<input type="text"/>	<input type="text" value="0000"/>	Select
Fwd to Addr	Fwd to Port	Schedule
Select	<input type="text" value="0000"/>	Select

Add to list

Rules List

Application	Original Port	Protocol	Fwd to Addr	Fwd to Port	Schedule
4577	TCP	127.0.0.1	4577	Always	
4567	TCP	127.0.0.1	4567	Always	

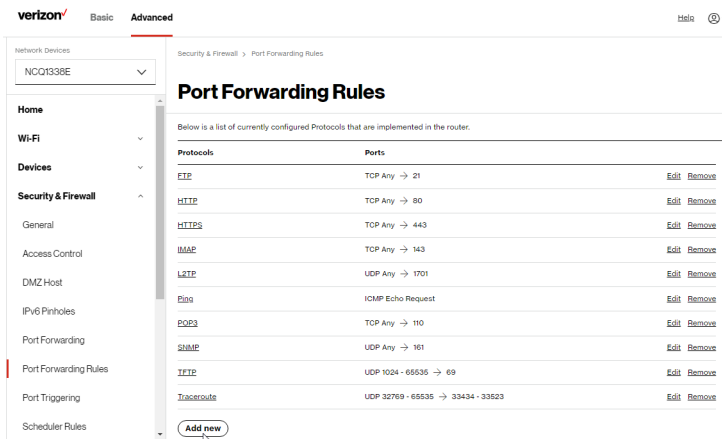
2. To create a new rule, enter the application name, configure its inbound and outbound port numbers, forwarding destination address, then select the protocol.
3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
4. Click **Add to list**. The rule displays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

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.



The screenshot displays the 'Port Forwarding Rules' configuration page in the Verizon Business Internet Gateway interface. The page is titled 'Port Forwarding Rules' and includes a sub-header: 'Below is a list of currently configured Protocols that are implemented in the router.' The main content is a table with two columns: 'Protocols' and 'Ports'. Each row represents a rule with its protocol name, the port range, and 'Edit' and 'Remove' links. An 'Add new' button is located at the bottom of the table.

Protocols	Ports	
FTP	TCP Any → 21	Edit Remove
HTTP	TCP Any → 80	Edit Remove
HTTPS	TCP Any → 443	Edit Remove
IMAP	TCP Any → 143	Edit Remove
L2TP	UDP Any → 1701	Edit Remove
Ping	ICMP Echo Request	Edit Remove
POP3	TCP Any → 110	Edit Remove
SNMP	UDP Any → 161	Edit Remove
TFTP	UDP 1024 - 65535 → 69	Edit Remove
Traceroute	UDP 32769 - 65535 → 33434 - 33523	Edit Remove

SECURITY & FIREWALL

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

The screenshot shows the 'Edit Service' page in the Verizon network management interface. The page is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with categories: Home, Wi-Fi, Devices, Security & Firewall (expanded), Access Control, DMZ Host, IPv6 Pinholes, Port Forwarding, Port Forwarding Rules, and Port Triggering. The main content area is titled 'Edit Service' and contains the following sections:

- Service Name:** A text input field.
- Service Description:** A text input field.
- Service Ports:** A table with two columns: 'Protocols' and 'Ports'. Below the table is an 'Add' button.
- Buttons:** 'Cancel' and 'Apply' buttons at the bottom.

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.

The screenshot shows the 'Edit Service Server Ports' page in the Verizon network management interface. The page is divided into a left sidebar and a main content area. The sidebar is identical to the previous screenshot. The main content area is titled 'Edit Service Server Ports' and contains the following sections:

- Protocol:** A dropdown menu with 'TCP' selected.
- Source Ports:** A dropdown menu with 'Any' selected.
- Destination Ports:** A dropdown menu with 'Any' selected.
- Buttons:** 'Cancel' and 'Apply' buttons at the bottom.

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

5.0g/ PORT TRIGGERING

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

For example, a 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.

SECURITY & FIREWALL

To configure port triggering:

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

The screenshot shows the Verizon Security & Firewall configuration interface. The left sidebar is expanded to 'Security & Firewall' and 'Port Triggering' is selected. The main content area is titled 'Port Triggering' and includes an 'Apply Changes' button. Below the title, there is a 'Create Rule' section with the following fields: Application (PT), Trig Port Range (Start: 12, End: 34), Protocol (TCP), Fwd Port Range (Start: 56, End: 74), and Schedule (Always). An 'Add to list' button is located at the bottom right of the 'Create Rule' section. Below this is a 'Rules List' section with a table containing one rule.

Application	Trig port range	Protocol	Fwd port range	Schedule	
test	11 22	TCP	33 44	Always	<input checked="" type="checkbox"/>

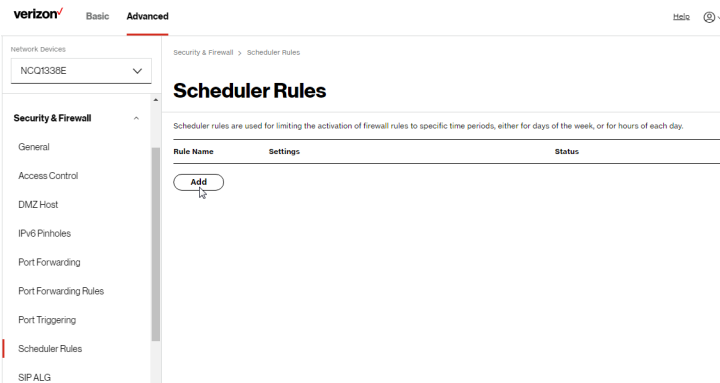
2. To add a service as an active protocol, enter the application name, configure its inbound and outbound (triggered/forwarded) port range, then select the protocol.
3. To schedule the rule, select either **Always** or **User Defined** in the **Schedule** list box.
4. Click **Add to list**. The rule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

5.0h/ SCHEDULER RULES

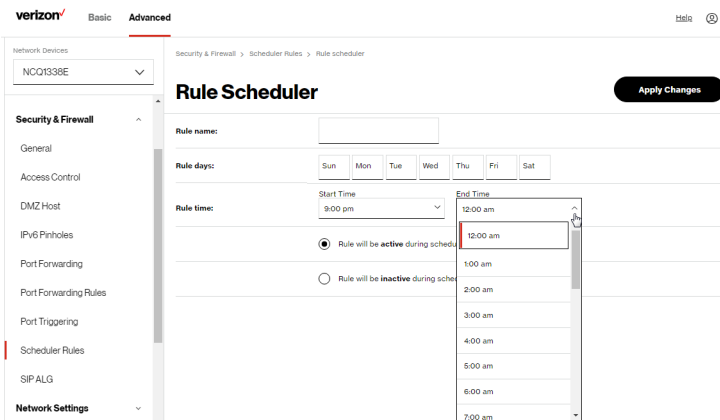
Scheduler Rules are used for limiting the activation of firewall rules to specific time periods. The time periods are either for days of the week or for hours of each day based on activity or inactivity.

To define a rule:

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



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



SECURITY & FIREWALL

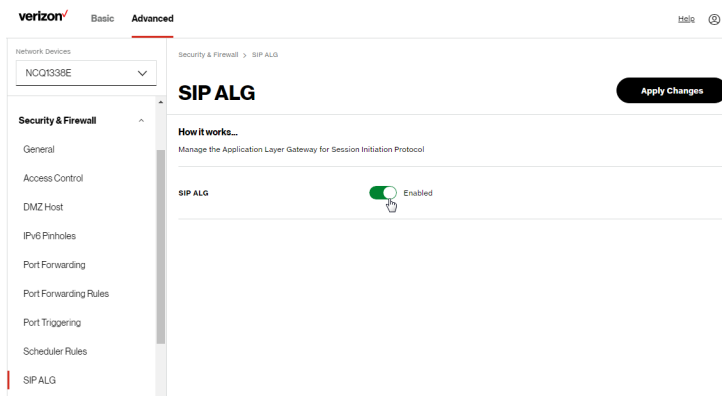
4. Enter the name of the rule, select the active or inactive days of the week and the start and end time range.
5. Specify if the rule is **active** or **inactive** at the scheduled time.
6. Click **Apply Changes** to save changes.

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.



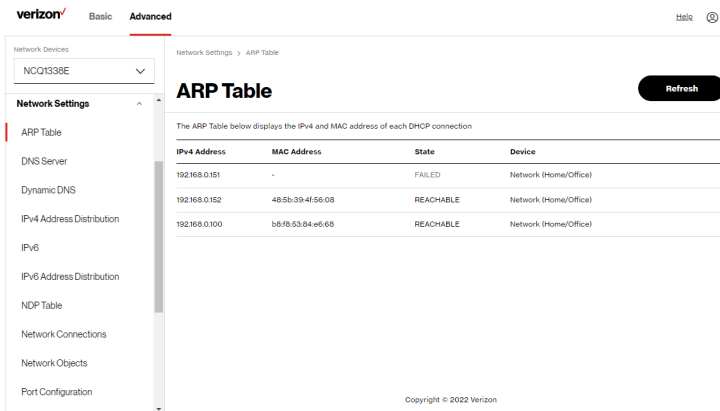
3. Click **Apply Changes** to save changes.

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**.



The screenshot shows the Verizon Business Gateway Advanced Settings page. The left sidebar is expanded to 'Network Settings', and 'ARP Table' is selected. The main content area displays the 'ARP Table' with a 'Refresh' button. Below the title, a note states: 'The ARP Table below displays the IPv4 and MAC address of each DHCP connection'. A table follows with the following data:

IPv4 Address	MAC Address	State	Device
192.168.0.151	-	FAILED	Network (Home/Office)
192.168.0.152	48:5b:39:4f:56:08	REACHABLE	Network (Home/Office)
192.168.0.100	b8:f0:53:04:e6:68	REACHABLE	Network (Home/Office)

Copyright © 2022 Verizon

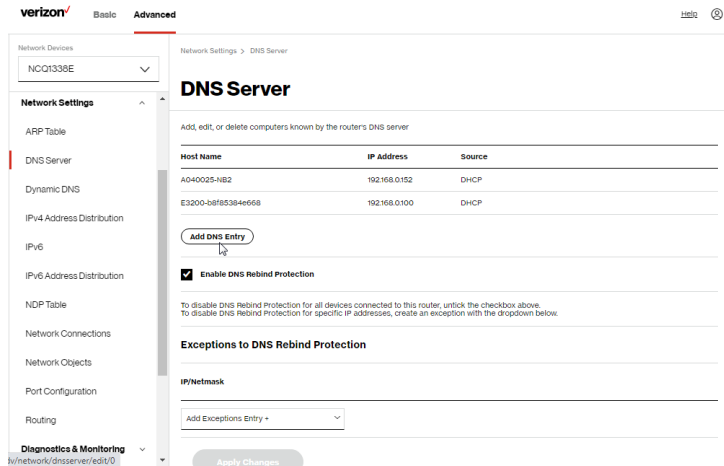
5.1b/ DNS SERVER

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

To access the DNS server:

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

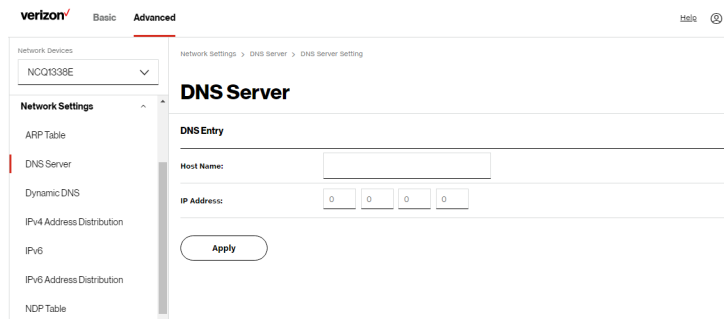
NETWORK SETTINGS



2. 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.

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



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. The **Add Exceptions List** page displays. Edit the IP address.
7. To remove a host from the DNS table, click the **Remove** icon on the screen.
8. Click **Apply Changes** to save changes.

5.1c/ DYNAMIC DNS

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

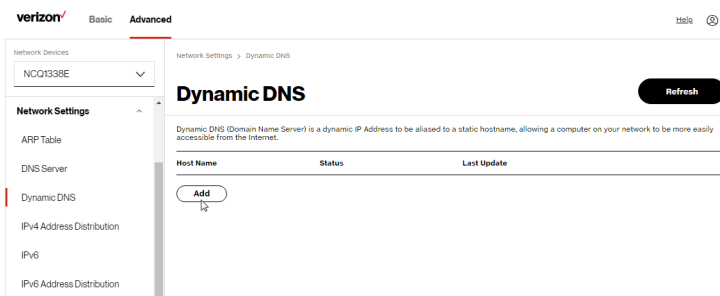
Dynamic DNS allows a static domain name to be mapped to the dynamic IP address, allowing a computer within your network to be more easily accessible from the internet.

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.

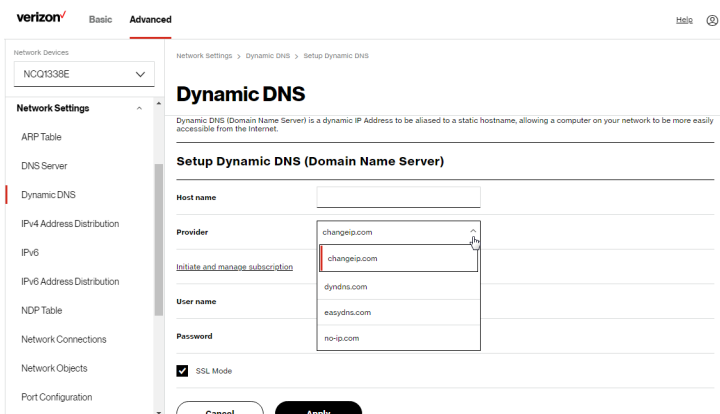
To set up dynamic DNS:

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

NETWORK SETTINGS



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.

- **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.

NETWORK SETTINGS

The DHCP server performs the following functions:

- Displays a list of all DHCP host devices connected to your Verizon Internet Gateway for Business
- 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.

The screenshot shows the Verizon Network Settings interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. A 'Network Devices' dropdown menu is set to 'NCG1338E'. The left sidebar lists 'Network Settings' with sub-items: 'ARP Table', 'DNS Server', 'Dynamic DNS', 'IPv4 Address Distribution' (highlighted), and 'IPv6'. The main content area is titled 'IPv4 Address Distribution' and includes a description: 'IPv4 Address Distribution provides the ability to allocate and configuration parameters to selected hosts.' Below this is a table with columns: 'Name', 'Service', 'Subnet Mask', and 'Dynamic IP Range'. The table contains one entry: 'Network (HomeID...)' with service '192.168.0.1', subnet mask '255.255.255.0', and dynamic IP range '192.168.0.2 - 192.168.0.254'. An 'Edit' icon is visible at the end of the row. A 'Connection List' button is located at the bottom of the table.

Name	Service	Subnet Mask	Dynamic IP Range
Network (HomeID...	192.168.0.1	255.255.255.0	192.168.0.2 - 192.168.0.254

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.

The screenshot shows the Verizon web interface for configuring network settings. The page title is "DHCP Settings for Network (Home/Office)". The "Service" section has "IPv4 Address Distribution" set to "DHCP Server". Below this, the "DHCP Server" section is expanded, showing "Start IP Address" as 192.168.0.2 and "End IP Address" as 192.168.0.254. The "WINS Server" is set to 0.0.0.0, and the "Lease Time in Minutes" is 1440. At the bottom, there is a table for "IPv4 Address Distribution According to DHCP Option 60 (Vendor Class Identifier)" with columns for Vendor Class Id, IP Address, MAC Address, and QoS.

5. To configure the DHCP server, complete the following fields:
 - **Start IP Address** – enter the first IP address that your Verizon Internet Gateway for Business 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.

NETWORK SETTINGS

- **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.

6. Click **Apply** to save changes.

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.

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:

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

The screenshot shows the Verizon Business Gateway interface. The left sidebar is expanded to 'Network Settings' and 'IPv4 Address Distribution'. The main content area is titled 'DHCP Connections' and contains a table of active connections. Below the table is a button labeled 'Add static connection'.

Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expired in	
E3200-b885384e...	192.168.0.100	B8:F8:53:84:E6:68	Dynamic	Network (Home/D...	Active	1042	Search Edit
A0400	192.168.0.152	48:5B:39:4F:56:08	Dynamic	Network (Home/D...	Active	1041	Search Edit

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

The screenshot shows the Verizon Business Gateway interface for configuring a DHCP connection. The left sidebar is expanded to 'Network Settings' and 'IPv4 Address Distribution'. The main content area is titled 'DHCP Connection Settings' and contains form fields for 'Host name', 'IP Address', and 'MAC Address'. Below the form is an 'Apply' button.

Host name:

IP Address:

MAC Address:

3. Enter the host name.
4. Enter the fixed IP address to be assigned.

NETWORK SETTINGS

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:

The screenshot shows the Verizon network settings interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. The 'Advanced' tab is selected. On the right side of the top bar, there are 'Help' and 'Settings' icons. The main content area is titled 'IPv6 Configuration Controls' and features an 'Apply Changes' button. The interface is divided into two main sections: '1. Enable IPv6 Support' and '2. Specify the method to be used to obtain your WAN IPv6 Address'. In the first section, the 'Enable IPv6 Support' toggle is turned on. The second section contains several input fields: 'IPv6 WAN Configuration' (set to 'Static(Auto)'), 'Assigned Prefix' (with a dropdown arrow), 'IPv6 WAN Address' (with a dropdown arrow and a '128' label), 'Default Gateway', 'WAN Link-Local Address' (pre-filled with 'fe80::200:f:fe00:0'), 'IPv6 DNS Address 1', and 'IPv6 DNS Address 2'. On the left side, there is a sidebar menu with 'Network Settings' expanded, showing options like 'ARP Table', 'DNS Server', 'Dynamic DNS', 'IPv4 Address Distribution', 'IPv6', 'IPv6 Address Distribution', 'NDP Table', 'Network Connections', 'Network Objects', and 'Port Configuration'. The 'IPv6' option is highlighted with a red bar.

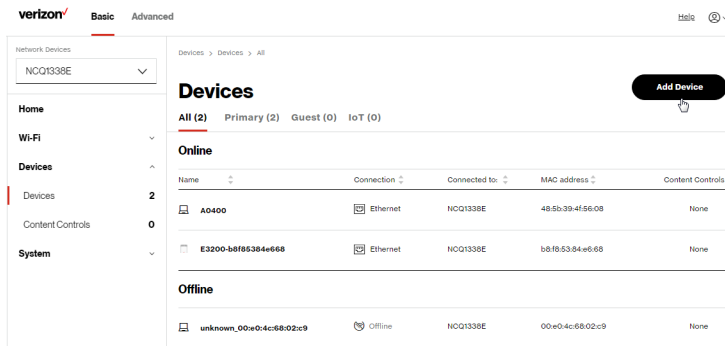
2. Select **Enabled** in the **Enable IPv6 Support** field.
3. Click **Apply Changes** to have changes take effect.

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.



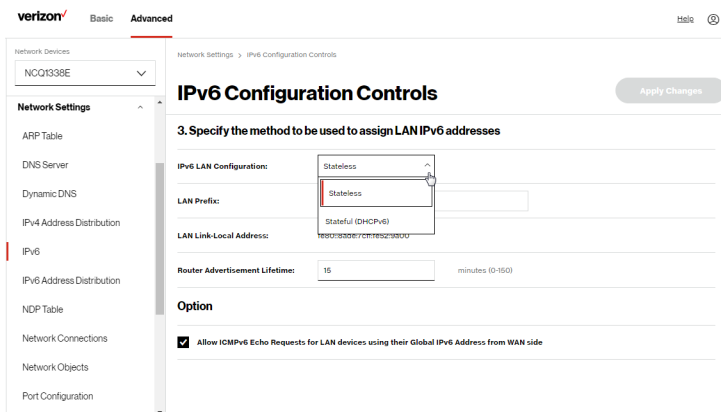
The screenshot shows the Verizon Business Gateway web interface. The left sidebar contains navigation options: Home, Wi-Fi, Devices (selected), Content Controls, and System. The main content area is titled 'Devices' and shows a list of network devices. The list is divided into 'Online' and 'Offline' sections. The 'Online' section contains two devices: 'A0400' and 'E3200-88186384e668'. The 'Offline' section contains one device: 'unknown_00e0:4c:68:02:c9'. Each device entry includes its name, connection type, connected to, MAC address, and content controls.

Name	Connection	Connected to	MAC address	Content Controls
A0400	Ethernet	NG01338E	48:5b:39:4f:56:08	None
E3200-88186384e668	Ethernet	NG01338E	b8:f8:53:84:e6:68	None
unknown_00e0:4c:68:02:c9	Offline	NG01338E	00e0:4c:68:02:c9	None

NETWORK SETTINGS

IPv6 WAN 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 as shown below:



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 Prefix** (automatically populated)
 - **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.

IPv6 WAN with LAN IPv6 Stateful (DHCPv6) Settings

1. Specify the **Stateful (DHCPv6)** settings to be used to assign LAN IPv6 addresses by entering the following details:

The screenshot shows the Verizon Network Settings interface for IPv6 Configuration Controls. The page is titled "IPv6 Configuration Controls" and includes an "Apply Changes" button. The main heading is "3. Specify the method to be used to assign LAN IPv6 addresses". The configuration fields are as follows:

- IPV6 LAN Configuration:** A dropdown menu is open, showing "Stateful (DHCPv6)" selected, with "Stateless" and "Stateful (DHCPv6)" also visible.
- LAN Prefix:** A text input field.
- DHCPv6 Client Address Range:** Two text input fields for start and end addresses.
- LAN Link-Local Address:** A text input field containing "fe80:8ade:7c1f:fe52:9a00".
- Router Advertisement Lifetime:** A text input field containing "15" with a unit of "minutes (0-150)".
- IPv6 Address Lifetime:** A text input field containing "60" with a unit of "minutes (3-150)".
- Option:** A section with a checked checkbox labeled "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)
- **Router Advertisement Lifetime** (minutes between 0-150)
- **IPv6 Address Lifetime** (minutes between 3-150)

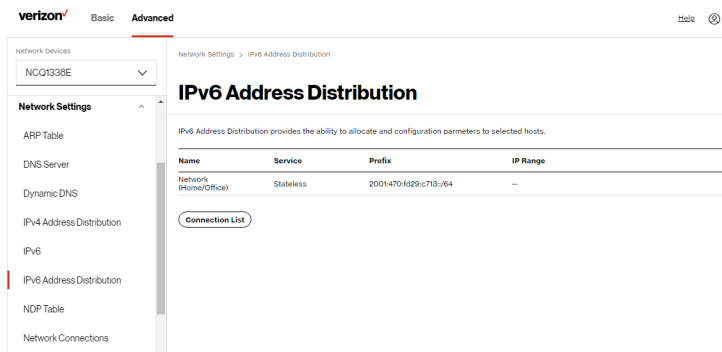
NETWORK SETTINGS

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

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.



The screenshot shows the Verizon Network Settings interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. A breadcrumb trail reads 'Network Settings > IPv6 Address Distribution'. On the left, a sidebar lists 'Network Settings' with sub-items: ARP Table, DNS Server, Dynamic DNS, IPv4 Address Distribution, IPv6, IPv6 Address Distribution (highlighted), NDP Table, and Network Connections. The main content area is titled 'IPv6 Address Distribution' and contains a table with the following data:

Name	Service	Prefix	IP Range
Network (Home/Office)	Stateless	2001:470:8029::7130::/64	--

Below the table is a 'Connection List' button.

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.
 - **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.
4. 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:

1. On the **IPv6 Address Distribution** page, click **Connection List**.
2. To define a new static connection with a fixed IP address, click **Add static connection**.
3. Enter the host name.
4. Enter the fixed IP address to be assigned.

NETWORK SETTINGS

5. Enter the MAC address of the network interface of the computer used with this DHCP static connection.
6. Click **Apply** to save changes.

5.1g/ NDP TABLE

You can view the IPv6 and MAC addresses of each DHCP connection.

To view the IPv6 and MAC addresses for each device: select **NDP** (Neighbor Discovery Protocol) **Table** in the **Network Settings** section.

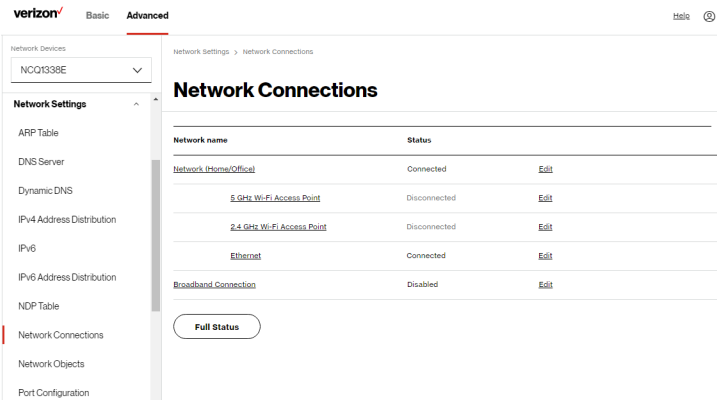
The screenshot shows the Verizon Network Settings interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. A 'Network Devices' dropdown menu is set to 'NCQ1338E'. The left sidebar lists 'Network Settings' with sub-items: ARP Table, DNS Server, Dynamic DNS, IPv4 Address Distribution, IPv6, IPv6 Address Distribution, NDP Table (highlighted), Network Connections, Network Objects, and Port Configuration. The main content area is titled 'NDP Table' and includes a 'Refresh' button. Below the title, a note states: 'The NDP Table below displays the IPv6 and MAC address of each DHCP connection'. A table with the following headers is visible: IPv6 Address, MAC Address, State, Rtr, and Device. The table body is currently empty. A copyright notice 'Copyright © 2022 Verizon' is located at the bottom right of the interface.

5.1h/ NETWORK CONNECTIONS

Caution: The settings described in this chapter should only be configured by experienced network technicians. Changes could adversely affect the operation of your Gateway and your local network.

To view the network connections:

1. From the **Advanced** menu, select **Network Settings** from the left pane and then click **Network Connections**.



2. To view and edit the details of a specific network connection, click the hyperlinked name or the action icon. The following sections detail the types of network connections that you can view.

NETWORK SETTINGS

NETWORK (HOME/OFFICE) CONNECTION

You can view the properties of your local network. This connection is used to combine several network interfaces under one virtual network. For example, you can create a home/office network connection for Ethernet and other network devices.

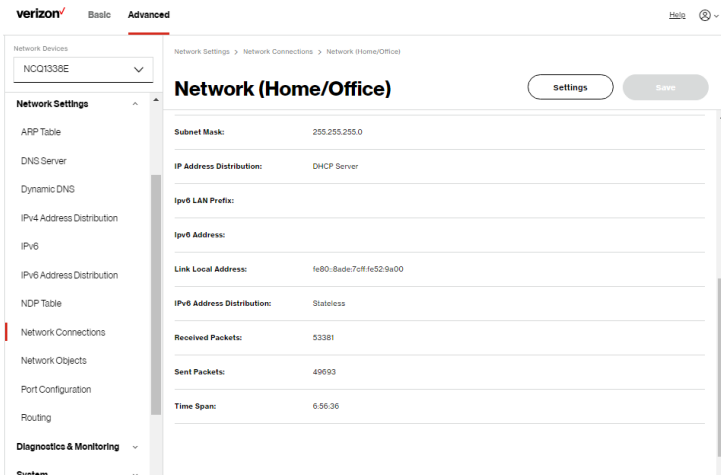
Note: When a network connection is disabled, the underlying devices formerly connected to it will not be able to obtain a new DHCP address from that Verizon Internet Gateway for Business network interface.

To view the connection:

1. On the **Network Connections** page, click the **Network (Home/Office)** connection link. The **Network (Home/ Office) Properties** page displays.

The screenshot displays the Verizon Network (Home/Office) Properties page. The page is divided into a left sidebar and a main content area. The sidebar contains a navigation menu with categories: Network Settings, Network Connections, Network Objects, Port Configuration, Routing, Diagnostics & Monitoring, and System. The main content area is titled 'Network (Home/Office)' and includes a 'Settings' button and a 'Save' button. Below the title, there is a warning message: 'Important: Only advanced technical users should use this feature.' The main content area displays the following information:

Name:	Network (Home/Office)
Status:	Connected
Network:	Network (Home/Office)
Underlying Device:	5 GHz Wi-Fi Access Point 2.4 GHz Wi-Fi Access Point Ethernet
Connection Type:	Bridge
MAC Address:	88:DE:7C:52:9A:00
IPv4 Address:	192.168.0.1
Subnet Mask:	255.255.255.0



2. To rename a network connection, enter the new network name in the **Name** field.
3. Click **Save** to save the changes.

CONFIGURING THE HOME/OFFICE NETWORK

To configure the network connection:

1. In the **Network (Home/Office)** properties page, click **Settings**. The configuration page displays.

NETWORK SETTINGS

verizon Basic **Advanced** Help

Network Devices
NCO1338E

Network Settings

- ARP Table
- DNS Server
- Dynamic DNS
- IPv4 Address Distribution
- IPv6
- IPv6 Address Distribution
- NDP Table
- Network Connections**
- Network Objects
- Port Configuration
- Routing
- Diagnostics & Monitoring
- System

Network Settings > Network Connections > Network (Home/Office)

Network (Home/Office)

Save Changes

Important: Only advanced technical users should use this feature.

General

Status: Connected

Connection Type: Network (Home/Office)

Physical Address: 88.DE.7C.52.9A.00

MTU: Automatic 1500

IP Address: 192 168 0 1

Subnet Mask: 255 255 255 0

Bridge

Name	VLAN	Status	
<input type="checkbox"/> IP Passthrough	Disable	Disabled	Edit
<input checked="" type="checkbox"/> 5 GHz Wi-Fi Access Point	Disable	Disconnected	Edit

verizon Basic **Advanced** Help

Network Devices
NCO1338E

Network Settings

- ARP Table
- DNS Server
- Dynamic DNS
- IPv4 Address Distribution
- IPv6
- IPv6 Address Distribution
- NDP Table
- Network Connections**
- Network Objects
- Port Configuration
- Routing
- Diagnostics & Monitoring
- System

Network Settings > Network Connections > Network (Home/Office)

Network (Home/Office)

Save Changes

Bridge

Name	VLAN	Status	
<input type="checkbox"/> IP Passthrough	Disable	Disabled	Edit
<input checked="" type="checkbox"/> 5 GHz Wi-Fi Access Point	Disable	Disconnected	Edit
<input checked="" type="checkbox"/> 2.4 GHz Wi-Fi Access Point	Disable	Disconnected	Edit
<input checked="" type="checkbox"/> Ethernet	Disable	Connected	Edit

IP Address Distribution: DHCP Server

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

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

Vendor Class ID	IP Address	MAC Address	IPv6
-----------------	------------	-------------	------

The screenshot shows the Verizon Business Internet Gateway configuration interface. The left sidebar contains a menu with options like Network Settings, Network Connections, and System. The main content area is titled 'Network (Home/Office)' and includes fields for End IP Address (192.168.0.254), WINS Server (0.0.0.0), and Lease Time in minutes (1440). Below these fields is a section for IP Address Distribution According to DHCP Option 60 (Vendor Class Identifier), which includes a table with columns for Vendor Class ID, IP Address, MAC Address, and OoS. The Routing Table section is currently empty and has a 'Add new route' button highlighted with a red circle.

2. Configure the following sections, as needed.

General

In the **General** section, verify the following information:

- **Status** – displays the connection status of the network.
- **Connection Type** – displays the type of connection interface.
- **Physical Address** – displays the physical address of the network card used for the network.
- **MTU** – displays the Maximum Transmission Unit (MTU) indicating the largest packet size permitted for internet transmissions:

NETWORK SETTINGS

- **Automatic:** sets the MTU (Maximum Transmission Unit) at 1500.
- **Automatic by DHCP:** sets the MTU according to the DHCP connection.
- **Manual:** allows you to manually set the MTU.
- **IP address and Subnet Mask:** the network connection uses a permanent or static **IP address** and **Subnet Mask** address, provided by Verizon or experienced network technician.

- **Bridge**

In the **Bridge** section of the **Network (Home/Office)** properties, you can configure the various LAN interfaces.

***Caution:** Do not change these settings unless specifically instructed to by Verizon. Changes could adversely affect the operation of your Gateway and your local network.*

Verify the following information:

- **IP Passthrough** – select to disable Wi-Fi and routing capabilities of the Gateway. May be necessary if connecting 3rd party routers to the Gateway using the LAN 2 port of your Gateway for Internet traffic, and LAN 1 will be only used for Web GUI access and disabling the IPPT mode into the device.
- **Status** – displays the connection status of a specific network connection.

- **Action** – contains an **Edit** hyperlink that, when clicked, generates the next level configuration page for the specific network connection or network device.

- **IP Address Distribution**

The **IP Address Distribution** section is used to configure the Dynamic Host Configuration Protocol (DHCP) server parameters of your Verizon Internet Gateway for Business.

Once enabled and configured, the DHCP server automatically assigns IP addresses to any network devices which are set to obtain their IP address dynamically.

If DHCP Server is enabled on your Gateway, configure the network devices as DHCP Clients. There are 2 basic options in this section: **Disabled** and **DHCP Server**.

To set up the Gateway's network bridge to function as a DHCP server:

1. In the **IP Address Distribution** section, select the **DHCP server**. Once enabled, the DHCP server provides automatic IP assignments (also referred to as IP leases) based on the preset IP range defined below.
 - **Start IP Address** – Enter the first IP address in the IP range that the Gateway will automatically begin assigning IP addresses from. Since your Gateway's IP address is 192.168.0.1, the default Start IP Address is 192.168.0.2.

NETWORK SETTINGS

- **End IP Address** – Enter the last IP address in the IP range that the Gateway will automatically stop the IP address allocation at. The maximum end IP address range that can be entered is 192.168.0.254.
- 2. If Windows Internet Naming Service (WINS) is being used, enter the **WINS Server** address.
- 3. In the **Lease time in minutes** field, enter the amount of time a network device is allowed to connect to the Gateway with its currently issued dynamic IP address.
- **IP Address Distribution According to DHCP option 60 (vendor class Identifier)**

DHCP vendor class is related to DHCP option 60 configuration within the Gateway. Adding option 60 configurations allows a particular vendor to get a lease from a specified pool of addresses.

Routing Table

You can configure your Verizon Internet Gateway for Business to use static or dynamic routing.

- **Static routing** – specifies a fixed routing path to neighboring destinations based on predetermined metrics.
- **Dynamic routing** – automatically adjusts how packets travel on the network. The path determination is based on network/device reachability and the status of the network being traveled.

To configure routing:

1. In the **Routing Table** section, click the **Add new route** button to display and modify the new route configuration page.

The screenshot shows the Verizon Network Settings interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. A breadcrumb trail reads: Network Settings > Network Connections > Network (Home/Office) > Route Settings. On the left, a sidebar lists 'Network Settings' with sub-items: ARP Table, DNS Server, Dynamic DNS, IPv4 Address Distribution, IPv6, IPv6 Address Distribution, NDP Table, Network Connections (highlighted), Network Objects, and Port Configuration. The main content area is titled 'Route Settings' and contains the following fields:

- Routing Entry:** A dropdown menu set to 'IPv4'.
- Name:** A text field containing 'Network (Home/Office)'.
- Destination:** Four input boxes, each containing '0'.
- Netmask:** Four input boxes, each containing '0'.
- Gateway:** Four input boxes, each containing '0'.
- Metric:** One input box containing '0'.

An 'Apply' button is located at the bottom of the form.

2. To save your changes click **Apply**.

Wi-Fi ACCESS POINT CONNECTION

A Wi-Fi Access Point network connection allows Wi-Fi devices to connect to the local area network (LAN) using the 2.4 GHz or 5 GHz Wi-Fi network.

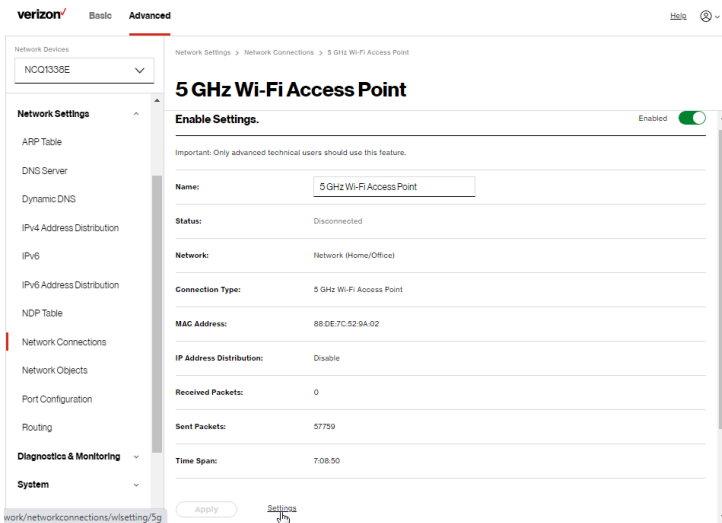
Note: Once disabled, all Wi-Fi devices connected to that Wi-Fi network will be disconnected from the LAN network and internet.

To view the connection settings:

1. From the **Advanced** menu, select **Network Settings** from the left pane and then click **Network Connections**.

NETWORK SETTINGS

2. To access the connection settings pages, click on the link of the Wi-Fi Access Point connections listed under **Network name** on the **Network Connections** page.

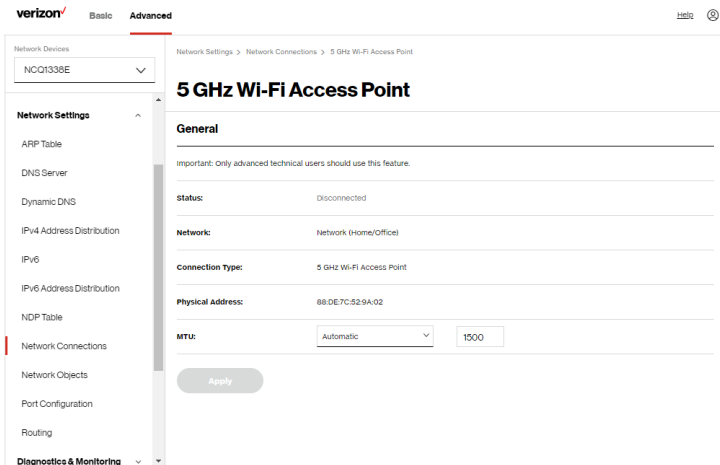


3. From the connection's **Enable Settings** page, to enable or disable the connection, move the selector to **on** or **off**.
4. To rename the connection, enter a name in the **Name** field.
5. Click **Apply** to save the changes.
6. Reboot your Verizon Internet Gateway for Business.

CONFIGURING WI-FI ACCESS POINT PROPERTIES

To configure the connection:

1. On the bottom of the Access Point's specific **Enable Settings** page, click **Settings**. The configuration page displays.



2. Verify the following information:

General

- **Status** - displays the connection status of the network.
- **Network** – displays the type of network connection.
- **Connection Type** – displays the type of connection interface.
- **Physical Address** – displays the physical address of the network card used for the network.
- **MTU** - specifies the largest packet size permitted for internet transmissions:
 - **Automatic:** set the MTU (Maximum Transmission Unit) at 1500.
 - **Automatic by DHCP:** sets the MTU according to the DHCP connection.

NETWORK SETTINGS

- **Manual:** allows you to manually set the MTU.

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

ETHERNET CONNECTION

You can view the properties of your Ethernet LAN connection using an Ethernet cable inserted into one of your Gateway's Ethernet LAN ports.

To view the connection settings:

1. To access the **Ethernet** properties page, click the **Ethernet** link listed under **Network name** on the **Network Connections** page.

The screenshot shows the Verizon Gateway Network Settings interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. The left sidebar lists various network settings categories: Network Devices (with a dropdown showing 'NC01338E'), Network Settings (expanded), ARP Table, DNS Server, Dynamic DNS, IPv4 Address Distribution, IPv6, IPv6 Address Distribution, NDP Table, Network Connections (highlighted), Network Objects, Port Configuration, Routing, and Diagnostics & Monitoring. The main content area is titled 'Ethernet' and contains a table of connection details. A note at the top states: 'Important: Only advanced technical users should use this feature.' The table lists: Name (Ethernet), Status (Connected), Network (Network (Home/Office)), Connection Type (Hardware Ethernet Switch), MAC Address (88:DE:7C:52:99:FF), IP Address Distribution (Disable), Received Packets (50213), Sent Packets (79688), and Time Span (7:11:31). At the bottom of the settings area are 'Apply' and 'Settings' buttons.

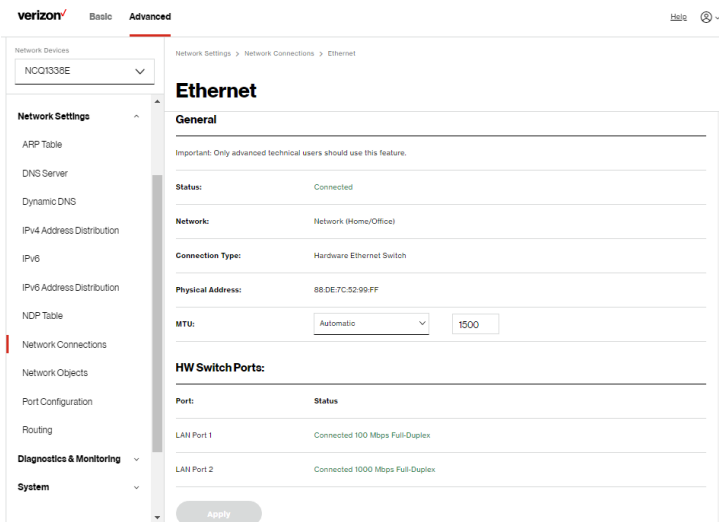
Field	Value
Name	Ethernet
Status	Connected
Network	Network (Home/Office)
Connection Type	Hardware Ethernet Switch
MAC Address	88:DE:7C:52:99:FF
IP Address Distribution	Disable
Received Packets	50213
Sent Packets	79688
Time Span	7:11:31

2. To rename the network connection, enter the new name in the **Name** field.
3. Click **Apply** to save changes.

CONFIGURING ETHERNET PROPERTIES

To configure the connection:

1. In the **Ethernet** page, click **Settings**. The configuration page displays.



2. Verify the following information:

General

- **Status** – displays the connection status of the network.
- **Network** – displays the type name of network connection.
- **Connection Type** – displays as **Hardware Ethernet Switch**.
- **Physical Address** – displays the physical address of the network card used for the network.

NETWORK SETTINGS

- **MTU** - specifies the largest packet size permitted for
 - **Automatic:** sets the MTU (Maximum Transmission Unit at 1500).
 - **Automatic by DHCP:** sets the MTU according to the DHCP connection.
 - **Manual:** allows you to manually set the MTU.
 - **HW Switch Ports** – displays the status of each LAN port.
3. Click **Apply** to save the changes.

5.1i/ NETWORK OBJECTS

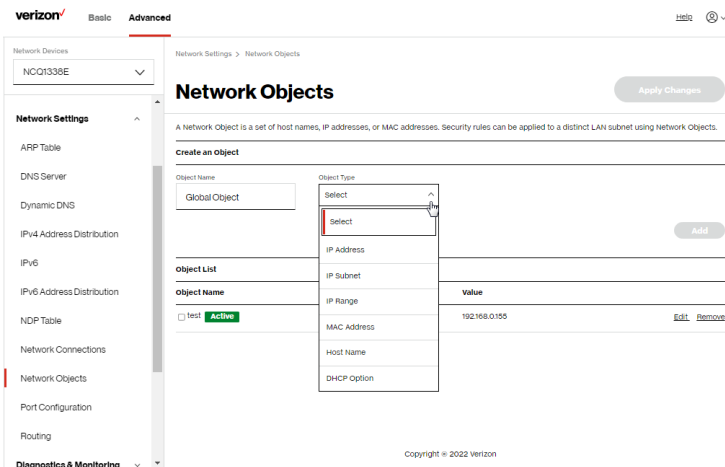
Network objects define a group, such as a group of computers, on your Verizon Internet Gateway for Business network by MAC address, IP address, and/or host name. The defined group becomes a network object. You can apply settings, such as configuring system rules, to all devices defined in the network object.

For example, instead of setting the same website filtering configuration individually to five computers one at a time, you can define the computers as a network object. Website filtering can then be simultaneously applied to all the computers.

You can use network objects to apply security rules based on host names, instead of IP addresses. This is useful since IP addresses change from time to time. In addition, you can define network objects according to MAC address to make the rule application more persistent against network configuration settings.

To define a network object:

1. From the **Advanced** menu, select **Network Settings**.
2. Select **Network Objects** in the **Network Settings** section.



3. To define a network object, enter a name for the network object in the **Objects Name** field.
4. Select and configure the type of network object as IP address, IP subnet, IP range, MAC address, host name, or DHCP option, and click **Add**.
5. The network object displays in the **Objects List** section.
6. Repeat the above steps to create additional network objects.
7. When complete, click **Apply Changes** to save changes.

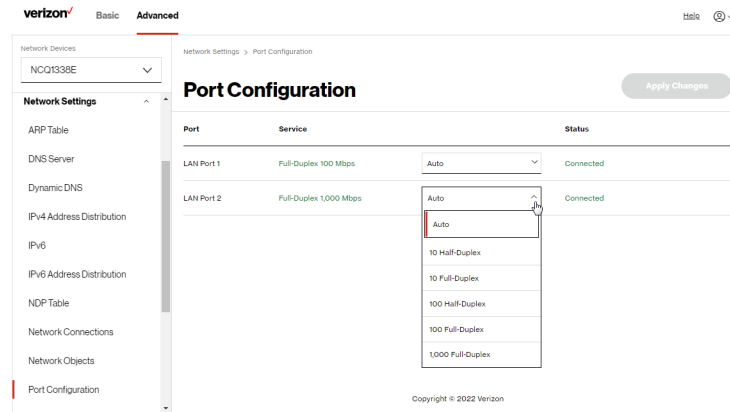
NETWORK SETTINGS

5.1j/ PORT CONFIGURATION

Ethernet port configuration allows you to set up the Ethernet ports as either full- or half-duplex ports, at either 10 Mbps, 100 Mbps, or 1000 Mbps.

To configure the ports:

1. Select **Port Configuration** in the **Network Settings** section.



2. To emulate the speed and duplex configuration of the port with which it's communicating, select **Auto** or select the port speed and duplicity.
3. Click **Apply Changes** to save changes.

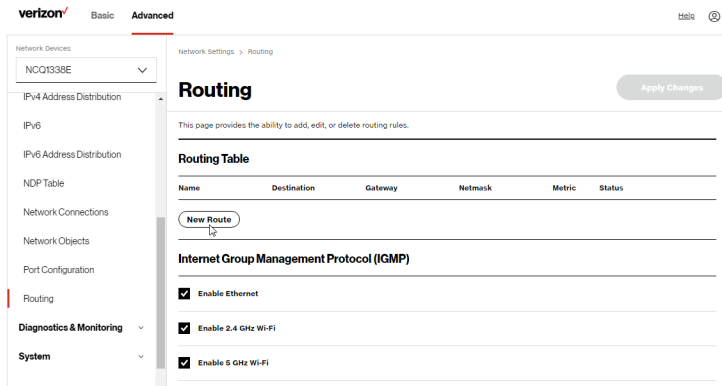
5.1k/ ROUTING

You can view the routing and IP address distribution rules as well as add, edit, or delete the rules.

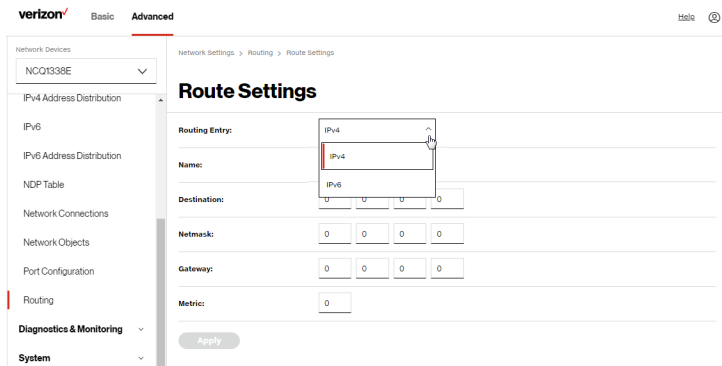
Routing Table

To view the rules:

1. Select **Routing** in the **Network Settings** section.



2. To add a new Route, click **New Route**.



NETWORK SETTINGS

3. Specify the following parameters:
 - **Routing Entry** – select the IP address type.
 - **Name** – the network connection type.
 - **Destination** – enter the destination IP of the destination host, subnet address, network address, or default route. The destination for a default route is 0.0.0.0.
 - **Netmask** – enter the network mask. This is used in conjunction with the destination to determine when a route is used.
 - **Gateway** – enter the IP address of your Verizon Internet Gateway for Business.
 - **Metric** – enter a measurement preference of the route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a specific destination network, the route with the lowest metric is used.
4. Click **Apply** and **Apply Changes** to save changes.

Internet Group Management Protocol (IGMP)

IGMP allows for managing a single upstream interface and multiple downstream interfaces of the IGMP/MLD (Multicast Listener Discovery)-based forwarding. This function enables the system to send IGMP host messages on behalf of hosts that the system discovers through standard IGMP interfaces. Also, IGMP snooping allows an Ethernet switch to “listen in” on the IGMP conversation between hosts and routers, while IGMP querier will send out periodic IGMP queries.

To enable this function:

1. Choose the IGMP interfaces by clicking on the check boxes on the screen.
2. Click **Apply Changes** to save changes.

5.2/ DIAGNOSTICS & MONITORING

5.2a/ BANDWIDTH MONITORING

You can view and monitor the recorded bandwidth usage measured in bytes.

To view the bandwidth:

1. From the **Advanced** menu, select **Diagnostics & Monitoring**.
2. In the **Diagnostics & Monitoring** section, select **Bandwidth Monitoring**.

The screenshot shows the Verizon Business Advanced Settings interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. The left sidebar lists 'Diagnostics & Monitoring' as the active section, with sub-items for 'Bandwidth Monitoring', 'Diagnostics', 'System Logging', 'System-wide Connections', 'Backhaul Logging', and 'System'. The main content area is titled 'Bandwidth Monitoring' and shows a table of usage data. The table has columns for 'Usage', '1hr', '12hr', '24hr', '1Week', and '1Month'. The data shows 0 bytes for all categories. There are also 'Auto-refresh' and 'Refresh' buttons.

Usage	1hr	12hr	24hr	1Week	1Month
Upload	0 bytes	0 bytes	0 bytes	0 bytes	0 bytes
Download	0 bytes	0 bytes	0 bytes	0 bytes	0 bytes

3. To refresh the page, click **Refresh**.
4. To continuously refresh the page, click **Auto-refresh on**.

DIAGNOSTICS & MONITORING

5.2b/ DIAGNOSTICS

You can use diagnostics to test network connectivity.

To diagnose network connectivity:

1. Select **Diagnostics** in the **Diagnostics & Monitoring** section.
2. To ping an IP address, enter the IP address or domain name in the **Destination** field and click **Go**.

The screenshot shows the Verizon network management interface. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' selected. The breadcrumb path is 'Diagnostics & Monitoring > Diagnostics'. On the left, a sidebar menu lists various monitoring options, with 'Diagnostics' highlighted. The main content area is titled 'Diagnostics' and includes a 'How it works...' section explaining that diagnostics ping an IP address to test connectivity. Below this, there are two sections for pinging: 'IPv4 Ping (ICMP Echo)' and 'IPv6 Ping (ICMP Echo)'. The IPv4 section has a 'Destination' input field, a 'Go' button, and a 'Number of pings' field set to '4'. The IPv6 section also has a 'Destination' input field and a 'Go' button.

The diagnostics will display the number of pings, status, packets sent, and round trip time.

If no diagnostic status displays, click refresh in your web browser.

5.2c/ SYSTEM LOGGING

System logging provides a view of the most recent activity of your Verizon Internet Gateway for Business. In addition, you can view additional logs, such as the security, advanced, firewall, WAN link and LAN DHCP.

To view the system log:

1. Select **System Logging** in the **Diagnostics & Monitoring** section.

The screenshot shows the Verizon Internet Gateway for Business interface. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. The left sidebar contains a 'Diagnostics & Monitoring' section with 'System Logging' selected. The main content area is titled 'System Logging' and features a table of log entries. The 'Options' button is highlighted with a mouse cursor.

Time	Event type	Log Level	Details
2022 Sep 19 06:29:04	ASK:NCQ1338E	notice	[SYS] LED dim off
2022 Sep 19 06:29:00	ASK:NCQ1338E	notice	[SYS] LED dim on led pattern: dim
2022 Sep 19 06:27:38	dnsmasq	info	[SYS.6][SYS] using nameserver 8.8.8.8#53
2022 Sep 19 06:27:38	dnsmasq	info	[SYS.6][SYS] using nameserver 20014860-4860-8844#53
2022 Sep 19 06:27:38	dnsmasq	info	[SYS.6][SYS] using nameserver 172.23.100.254#53
2022 Sep 19 06:27:38	dnsmasq	info	[SYS.6][SYS] using nameserver 20014860-4860-8808#53
2022 Sep 19 06:27:38	dnsmasq	info	[SYS.6][SYS] using local addresses only for domain mynetworksettings.com
2022 Sep 19 06:27:38	dnsmasq	info	[SYS.6][SYS] reading /etc/resolv.conf

2. To view a specific time of log event, click on the **Options** button.

DIAGNOSTICS & MONITORING

The screenshot shows the Verizon web interface for System Logging configuration. The top navigation bar includes the Verizon logo, 'Basic', and 'Advanced' tabs. The breadcrumb trail is 'Diagnostics & Monitoring > System Logging > System Log'. The left sidebar shows a navigation menu with 'Diagnostics & Monitoring' expanded, containing 'Bandwidth Monitoring', 'Diagnostics', 'System Logging', 'System-wide Connections', and 'Backhaul Logging'. The main content area is titled 'System Logging' and has a sub-menu with 'System Log', 'Security Log', 'Advanced Log', 'Firewall Log', 'WAN Log', and 'LAN DHCP Log'. Under 'Log viewing options', there are three radio buttons: 'Past day', 'Past week', and 'Custom range'. The 'Custom range' option is selected. Below this, there are four input fields: 'Start Date' (12/31/00), 'Start Time' (12:00 am), 'End Date' (12/31/00), and 'End Time' (12:00 am). At the bottom, there are 'Cancel' and 'Save' buttons.

3. Select your preferred logging time.
4. Click **Save** to save changes.
5. To view a specific type of log event such as Security Log, WAN Log, etc., click the appropriate link in the menu on the top.
6. To update the data, click **Refresh**.

5.2d/ SYSTEM-WIDE CONNECTIONS

You can view a summary of the monitored data collected for your Verizon Internet Gateway for Business.

To view your Gateway's full system status and traffic monitoring data:

1. Select **System-wide Connections** in the **Diagnostics & Monitoring** section.

verizon Basic **Advanced** Help ⓘ

Network Devices
NQ01338E

Devices

Security & Firewall

Network Settings

Diagnostics & Monitoring

Bandwidth Monitoring

Diagnostics

System Logging

System-wide Connections

Backhaul Logging

System

Diagnostics & Monitoring > System-wide Connections

System-wide Connections

Auto-refresh

Name	Network (Home/Office)	Broadband Connection	5 GHz Wi-Fi Access Point	2.4 GHz Wi-Fi Access Point	Ethernet
Status	Connected	Disabled	Disconnected	Disconnected	Connected
Underlying Device	Network (Home/Office)	Broadband Connection	Network (Home/Office)	Network (Home/Office)	Network (Home/Office)
Connection Type	5 GHz Wi-Fi Access Point 2.4 GHz Wi-Fi Access Point Ethernet	Cellular	5 GHz Wi-Fi Access Point	2.4 GHz Wi-Fi Access Point	Ethernet
MAC Address	88:DE:7C:52:9A:00	--	88:DE:7C:52:9A:02	88:DE:7C:52:9A:01	88:DE:7C:52:99:FF
IPv4 Address	192.168.0.1	--	--	--	--
Subnet Mask	255.255.255.0	--	--	--	--

verizon Basic **Advanced** Help ⓘ

Network Devices
NQ01338E

Devices

Security & Firewall

Network Settings

Diagnostics & Monitoring

Bandwidth Monitoring

Diagnostics

System Logging

System-wide Connections

Backhaul Logging

System

Diagnostics & Monitoring > System-wide Connections

System-wide Connections

Auto-refresh

IPv4 Default Gateway	192.168.0.1	--	--	--	--
IPv4 DNS Address 1	--	--	--	--	--
IPv4 DNS Address 2	--	--	--	--	--
IPv4 Address Distrib.	DHCP Server	Disable	Disable	Disable	Disable
IPv6 Prefix	--	--	--	--	--
IPv6 Address	--	--	--	--	--
IPv6 Link-Local Address	fe80::8ade:7cff:fe52:9a00	fe80::200::fe00:0	--	--	--
IPv6 DNS Address 1	--	--	--	--	--
IPv6 DNS Address 2	--	--	--	--	--

DIAGNOSTICS & MONITORING

The screenshot displays the Verizon network management interface. At the top, there are tabs for 'Basic' and 'Advanced', with 'Advanced' selected. The main content area is titled 'System-wide Connections' and includes an 'Auto-refresh' toggle switch. A table lists various connection metrics:

Metric	Stateless	Disable	Disable	Disable	Disable
IPv6 Address Distribution					
Rec'd Packets	9233	0	0	0	8744
Sent Packets	5943	0	4089	1722	13296
Rec'd Bytes	708258	0	0	0	831460
Sent Bytes	10476359	0	444238	197601	10976640
Rec'd Errors	0	0	4095	4095	0
Rec'd Drops	0	0	0	0	0
Time Span	0:26:01	0:00:00	0:26:01	0:26:01	0:26:01

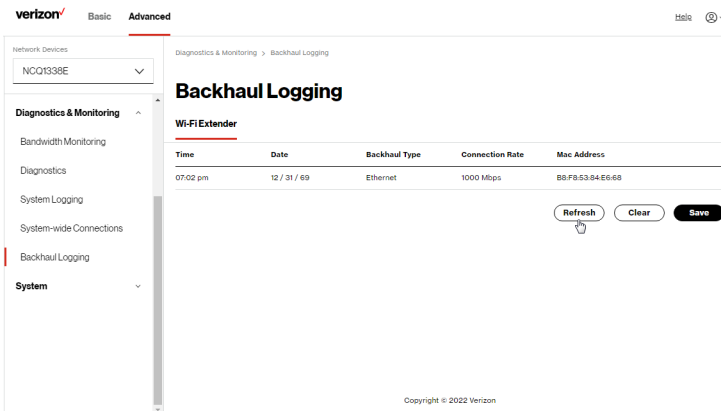
2. To modify the connection properties, click the individual connection links.
3. To continuously refresh the page, click **Auto-refresh on**.

5.2e/ BACKHAUL LOGGING

You can view a summary of the BHM (backhaul modes: Ethernet and Wi-Fi) status of your network.

To view the backhaul modes log:

1. Select **Backhaul Logging** in the **Diagnostics & Monitoring** section.



2. To refresh the page, click **Refresh**.
3. To delete the log information, click **Clear**.
4. To save the log information, click **Save**.

5.3/ SYSTEM

5.3a/ SYSTEM STATUS

To view the status:

1. From the **Advanced** menu, select **System**.
2. You can quickly view your Gateway's status by selecting **System Status** in the **System** section.
3. To refresh the page, click **Refresh**.
4. To continuously refresh the page, click **Auto-refresh on**.

SYSTEM

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 Internet Gateway for Business and extender(s) (if connected).

The screenshot shows the 'System Status' page for a Verizon gateway. The interface includes a Verizon logo, navigation tabs for 'Basic' and 'Advanced', and a user profile icon. A sidebar on the left lists system settings such as System Status, Date & Time, Factory Reset, LED Brightness, Open Source Software, Reboot Router, Remote Administration, and System Settings. The main content area is titled 'System Status' and features an 'Auto-refresh' toggle (which is turned on) and a 'Refresh' button. The page is divided into two columns: 'Broadband IPv4' and 'Broadband IPv6'. The IPv4 section shows 'Status: Disabled' and lists fields for IP address, Subnet mask, IPv4 Default Gateway, and two IPv4 DNS addresses. The IPv6 section shows 'Status: Disconnected' and lists fields for IP address, Assigned Prefix, IPv6 Address, L3/L4 Local Address (fe80:200:f:fc00::0), IPv6 Default Gateway, and two IPv6 DNS addresses. A 'Network Devices' dropdown menu at the top left is set to 'NC01338E'.

This screenshot shows the 'System Status' page with the 'Modem' section selected. The layout is consistent with the previous screenshot, including the Verizon logo, navigation tabs, and sidebar. The main content area displays 'Modem' settings. The 'Firmware Version' is 23311. The 'Mobile Number' is hidden. The 'IMEI' is 357776720000029. The 'iCCID' is hidden. The 'Sim Status' is 'Absent'. The 'Roaming Status' is hidden. The '4G LTE Signal Strength' and '5g Signal Strength' are both shown as hidden. The 'Network Devices' dropdown menu at the top left is set to 'NC01338E'. The 'Auto-refresh' toggle is turned on, and the 'Refresh' button is visible.

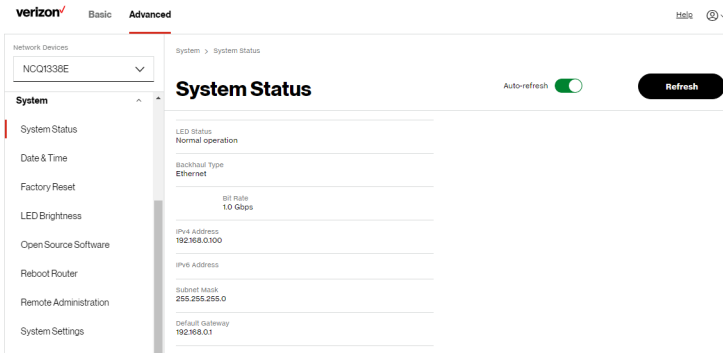
The screenshot shows the Verizon router's System Status page for a Router. The interface includes a navigation menu on the left with options like System Status, Date & Time, Factory Reset, LED Brightness, Open Source Software, Reboot Router, Remote Administration, and System Settings. The main content area displays the following information:

- System Status** (with an Auto-refresh toggle and a Refresh button)
- Router** section containing:
 - Firmware Version: 3.2.0.11
 - Hardware Version: 1
 - Model Name: ASK-NQI1338E
 - Serial Number: AA113600002
 - LAN IPV4 Address: 192.168.0.1
 - Broadband Physical Connection: Cellular
 - Router has been active for: 0 days 10 hours 33 minutes 17 seconds
 - LED Status: Self activation

The screenshot shows the Verizon router's System Status page for an Extender. The interface is similar to the Router page, with a navigation menu on the left. The main content area displays the following information:

- System Status** (with an Auto-refresh toggle and a Refresh button)
- Extender** section containing:
 - Device Name: E3200-b8f65384e668
 - Model Name: E3200
 - Firmware Version: 3.11.15
 - Hardware Version: 1102
 - Serial Number: E301120071800005
 - MAC Address: B8:F6:53:84:E6:68
 - System Up Time: 0 days 10 hours 33 minutes 22 seconds
 - LED Status: Normal operation

SYSTEM

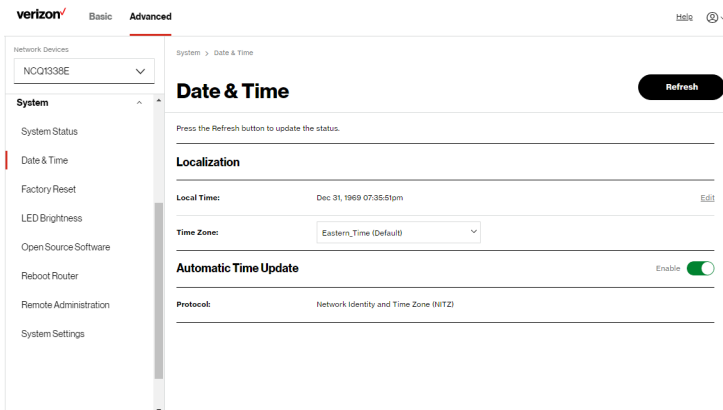


5.3b/ DATE & TIME SETTINGS

You can set the time zone and enable automatic time updates.

To configure the settings:

1. From the **Advanced** menu, select **System**.
2. Select **Date & Time** in the **System** section.



3. Select the local time zone. Your Verizon Internet Gateway for Business automatically detects daylight saving times for selected time zone.
4. In the **Automatic Time Update** section, select the **Enable** check box to perform an automatic time update.
5. To refresh the page, click **Refresh**.

5.3c/ FACTORY RESET

You can use this functionality to save and load configuration files. These files are used to backup and restore the current configuration of your Verizon Internet Gateway for Business.

Only configuration files saved on a specific Verizon Internet Gateway for Business can be applied to that Verizon Internet Gateway for Business. You cannot transfer configuration files between Gateways.

***Warning:** Manually editing a configuration file can cause your Verizon Internet Gateway for Business to malfunction or become completely inoperable.*

Restore Options

You can restore your configuration settings to your Gateway factory default settings. Restoring the default settings erases the current configuration, including user defined settings and network connections. All connected DHCP clients must request new IP addresses. Your Verizon Internet Gateway for Business must restart.

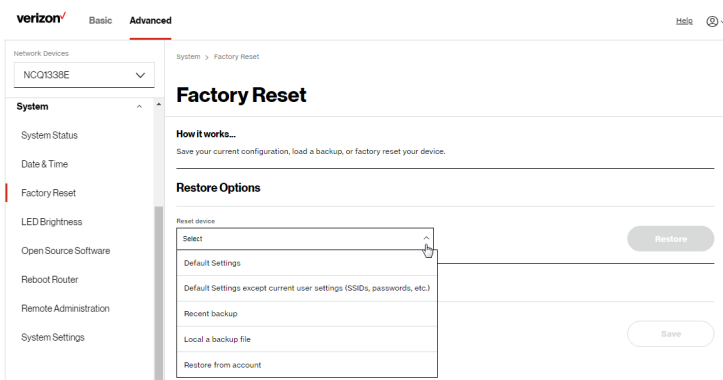
SYSTEM

Prior to restoring the factory defaults, you may want to save your current configuration to a file. This allows you to reapply your current settings and parameters to the default settings, as needed.

Note: When restoring defaults, the setting and parameters of your Verizon Internet Gateway for Business are restored to their default values. This includes the administrator password. A user-specified password will no longer be valid.

To restore your Verizon Internet Gateway for Business' factory default settings:

1. Click **Factory Reset** in the **System** section.
2. Select **Default Settings** or **Default Settings except current user settings**.
 - **Default Settings** – will erase all router settings including user settings for SSID and Passwords.
 - **Default Settings except current user settings** – will erase all router settings but will retain the user settings for SSID and passwords.



3. Click the **Restore** button. The factory default settings are applied and your Verizon Internet Gateway for Business restarts. Once complete, the Login page for the First Time Easy Setup Wizard displays.

To load the configuration file:

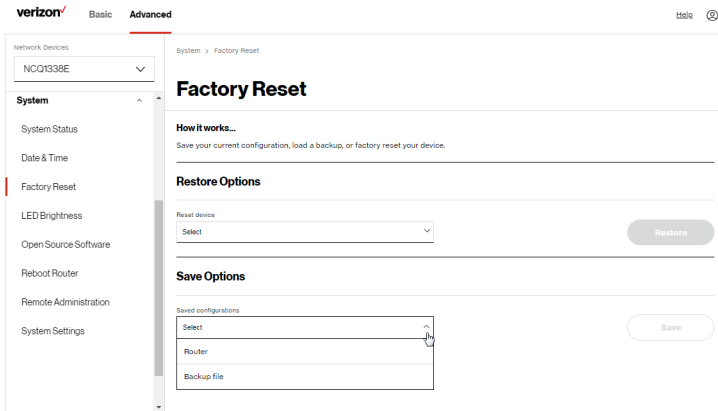
1. Select **Factory Reset** in the **System** section.
2. To load a previously saved configuration file, select **Recent backup** or **Load a backup file** then click **choose file**.
3. Browse to the location of the file, and click the **Restore** button to begin the configuration uploading process.
4. Accessing the **My Fios App** or the **My Verizon** account also allows you to restore the previously saved settings. Select **Restore from account** and use **My Fios App** or **My Verizon** account to restore the saved settings to the Gateway.
5. Click the **Restore** button. Your Verizon Internet Gateway for Business will automatically restart with that configuration.

Save Options

To save the configuration file:

1. From the **Advanced** menu, select **System**.
2. Select **Factory Reset** in the **System** section.

SYSTEM



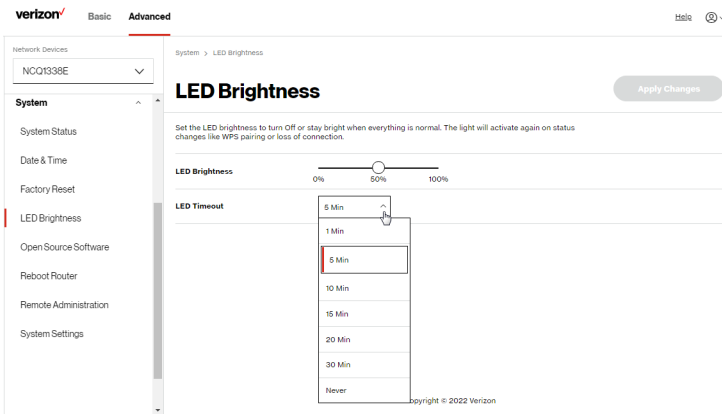
3. Select **Router** or **Backup file** to save the current configuration, then click **Save** button.
4. If you select **Backup file**, the configuration file is saved to you web browser's download folder.
5. Click **Save** button to begin the configuration backup process.

5.3d/ LED BRIGHTNESS

The Verizon Internet Gateway for Business allows you to set the LED brightness to turn Off (0%) or stay bright (50% or 100%) using the user interface.

To control the LED brightness:

1. Select **LED Brightness** in the **System** section.

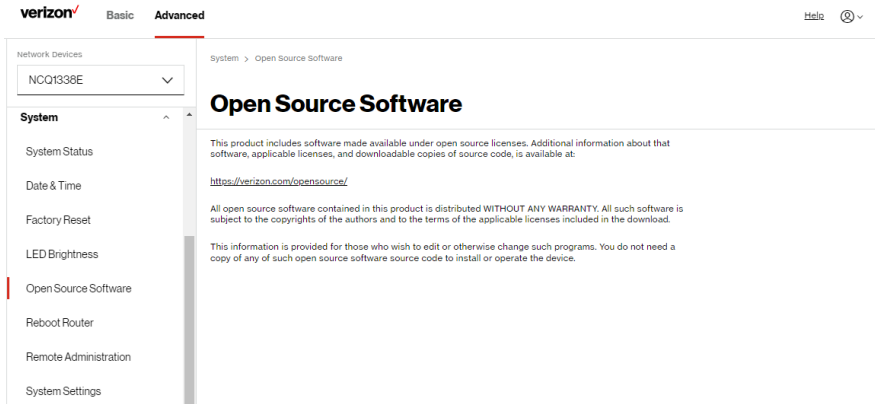


2. Slide the bar to adjust the brightness of the LED.
3. Select your preferred timeout period (in minutes) from the dropdown list for the LED dimming setting. The Status LED will automatically turn off after the timeout period.
4. Click **Apply Changes** to save changes.

Note: *The light will activate again on status changes like WPS pairing or loss of connection.*

SYSTEM

5.3e/ OPEN SOURCE SOFTWARE



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

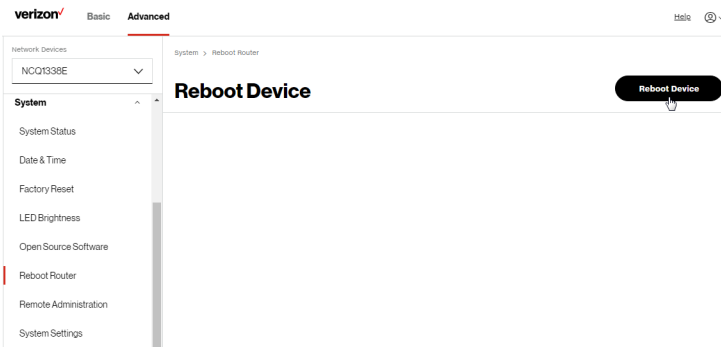
5.3f/ REBOOT VERIZON INTERNET GATEWAY FOR BUSINESS

Warning: Only select *Reboot Router* if instructed to do so by Verizon support.

You can reboot your Verizon Internet Gateway for Business using the Reboot Router feature. Refer to 1.1a/ Reset Button for factory reset function.

To reboot your Gateway using the user interface:

1. Select **Reboot Router** in the **System** section.



2. To reboot, click **Reboot Device**. Your Gateway will reboot. This may take up to a minute.
3. To access your Verizon Internet Gateway for Business user interface, refresh your web browser.
4. After the Status LED on the front panel turns solid white, you will automatically be sent to the web browser login page.

5.3g/ REMOTE ADMINISTRATION

Caution: *Enabling Remote Administration places your Gateway network at risk from outside attacks.*

You can access and control your Verizon Internet Gateway for Business not only from within the local network, but also from the internet using **Remote Administration**.

SYSTEM

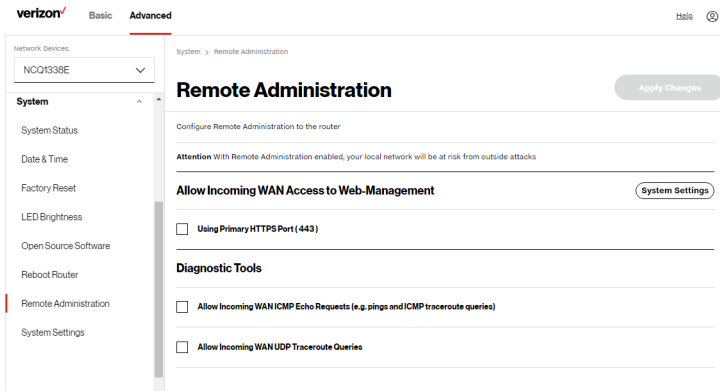
You can allow incoming access to the following:

- **Allow Incoming WAN Access to Web-Management** - used to obtain access to your Gateway's UI and gain access to all settings and parameters through a web browser.
- **Diagnostic Tools** - used for troubleshooting and remote system management by a user or Verizon.

Remote administration access of Web Management may be used to modify or disable firewall settings. Web Management services should be activated only when absolutely necessary.

To enable remote administration:

1. Select **Remote Administration** in the **System** section.



2. To enable access, select the check box.
3. To remove access, clear the check box.
4. Click **Apply Changes** to save changes.

5.3h/ SYSTEM SETTINGS

You can configure various system and management parameters.

To configure system settings:

1. Select **System Settings** in the **System** section.

The screenshot shows the Verizon System Settings page for a router (NCQ1338E). The left sidebar lists various system settings, with "System Settings" selected. The main content area is titled "System Settings" and contains two sections: "Router Status" and "User Settings".

Router Status

- Router's Hostname: NCQ1338E
- Local Domain: mynetworksettings.com
- Location: Other

User Settings

- User name: Admin
- Set new password: [input field] (minimum 8 characters)
- Retype new password: [input field]

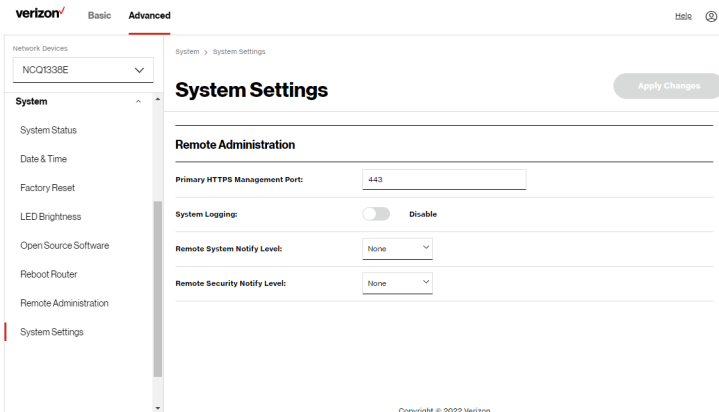
The screenshot shows the Verizon System Settings page for a router (NCQ1338E). The left sidebar lists various system settings, with "System Settings" selected. The main content area is titled "System Settings" and contains two sections: "Router" and "Remote Administration".

Router

- Retype new password: [input field]
- Unsuccessful Login Attempts: 10 (maximum attempts)
- Automatic Refresh of System Monitoring Web Pages
- Prompt for Password When Accessing via LAN
- Warn User Before Configuration Changes
- Session lifetime: 2700 seconds
- Number of concurrent sessions that can be logged into the router: 10

Remote Administration

SYSTEM



2. In the **Router Status** section, configure the following:
 - **Router's Hostname** – enter the host name of your Verizon Internet Gateway for Business.
 - **Local Domain** – view the local domain of the network.
 - **Location** – select your current location of the Gateway from the dropdown list.
3. In the **User Settings** section, you can view the administration user that can currently access your Wi-Fi network. In addition, you can modify the login password and manage the number of unsuccessful login attempts the administration user can enter before your Verizon Internet Gateway for Business temporarily denies all further login attempts by the user.

-
4. In the **Router** section, configure the following by selecting the check box:
 - **Automatic Refresh of System Monitoring Web Pages** – activates the automatic refresh of system monitoring web pages.
 - **Prompt for Password when Accessing via LAN** – causes your Gateway to ask for a password when trying to connect to the network.
 - **Warn User Before Configuration Changes** – activates user warnings before network configuration changes take effect.
 - In the **Session Lifetime** field, specify the length of time required before re-entering the login password after your Verizon Internet Gateway for Business has been inactive.
 - In the **Number of concurrent sessions that can be logged into the router** field, select the number of users that can access your Verizon Internet Gateway for Business at the same time.

 5. In the **Remote Administration** section, configure the following:
 - Enter the **Primary HTTP Management Port**.
Refer to 5.3g Remote Administration for using this feature.
 - In the **System Logging** section move the selector to **on** to activate system logging.

SYSTEM

- **Remote System Notify Level** – specify the type of information, such as none, error, warning, and information, received for remote system logging.
 - **Remote Security Notify Level** – specify the type of information, such as none, error, warning, and information, received for remote network security logging.
6. Click **Apply Changes** to save changes.

06 /

TROUBLE SHOOTING

6.0 Troubleshooting Tips

6.1 Frequently Asked Questions

This chapter lists solutions for issues that may be encountered while using your Verizon Internet Gateway for Business as well as frequently asked questions.

Although the majority of internet connectivity is automatic and transparent, if an issue does occur accessing the internet (e.g. complete loss of connectivity, inability to access services, etc.), you may need to take additional steps to resolve the problem.

TROUBLESHOOTING TIPS

Note: The advanced settings should only be configured by experienced network technicians to avoid adversely affecting the operation of your Verizon Internet Gateway for Business and your local network.

6.0/ TROUBLESHOOTING TIPS

6.0a/ IF YOU ARE UNABLE TO CONNECT TO THE INTERNET:

- The first thing to check is whether your Verizon Internet Gateway for Business is powered on and is connected to the internet. Check the Status LED on the front of the Verizon Internet Gateway for Business. Be sure to refer to the “1.1c/ LED” on page 7 to determine status of the Gateway.
- If the prior tips do not resolve your connection issue, try power cycling the Verizon Internet Gateway for Business by unplugging the power cord from the power supply and wait 2 minutes. During the 2 min. wait period, also power cycle the network device (e.g. the computer, tablet, etc.) and then plug the power cable back into the Gateway. After 3-5 minutes, recheck the Status LED and try again to access the internet.
- If rebooting your Verizon Internet Gateway for Business does not resolve your connection issue, try resetting the Gateway back to its factory default state by manually pressing the reset button on the bottom panel of the Gateway for 3+ seconds (the Status LED should go off) to begin resetting your Gateway. Your Gateway will perform a factory reset and return the Gateway to default settings. The Verizon Internet Gateway for Business

will return to service in 3-5 minutes depending on your network connection. Check Status LED and if it is solid white, try again to access the internet.

6.0b/ IF YOU ARE UNABLE TO CONNECT TO YOUR VERIZON INTERNET GATEWAY FOR BUSINESS USING WI-FI:

- Be sure your Wi-Fi device is within range of your Verizon Internet Gateway for Business; move it closer to see if your connection improves.
- Check your network device's Wi-Fi settings to be sure your device's Wi-Fi is on (enabled) and that you have the correct Wi-Fi network and password (if using a Wi-Fi password) as configured on your Gateway.
- Be sure you are connecting to the correct Wi-Fi network; check to be sure you are using your Gateway's SSID. In some cases, if using a Wi-Fi password, you may need to enter the Wi-Fi password into your network device again to be sure your device accepts the password.
- Check to be sure you are running the latest software for your network device.
- Try turning your network device's Wi-Fi off and on, and try to connect.
- If you have made any changes in your network settings and turning your network device's Wi-Fi off and on does not help, try to restart your network device.

TROUBLESHOOTING TIPS

- You may need to turn the Wi-Fi settings from on to off, and back to on again and apply the changes.
- If you are still unable to access your Verizon Internet Gateway for Business, you may need to try connecting to the Gateway using another network device. If the issue goes away with another network device, the issue is likely with that individual network device's configuration.

6.0c/ ACCESSING YOUR VERIZON INTERNET GATEWAY FOR BUSINESS IF YOU ARE LOCKED OUT

- If your Verizon Internet Gateway for Business connection is lost while making configuration changes, a setting that locks access to Gateway's UI may have inadvertently been activated.

The common ways to lock access to your Verizon Internet Gateway for Business are:

- Scheduler - If a schedule has been created that applies to the computer over the connection being used, your Verizon Internet Gateway for Business will not be accessible during the times set in the schedule.
- Access Control - If the access control setting for the computer is set to block the computer, access to your Verizon Internet Gateway for Business is denied.

To gain access, restore the default settings to your Verizon Internet Gateway for Business.

6.0d/ RESTORING YOUR VERIZON INTERNET GATEWAY FOR BUSINESS' DEFAULT SETTINGS

There are two ways to restore the default settings of your Verizon Internet Gateway for Business. It is important to note that after performing either procedure, all previously save settings on your Gateway will be lost.

For additional information regarding the Restore Defaults feature, refer to section 5.3c/ Factory Reset/Restore Options.

- Using the tip of a paperclip or similar object, press and hold the Reset button on the bottom of your Gateway for over three seconds.
- Access the UI and navigate to the Advanced Settings page. Select the 5.3c/ Factory Reset option. After saving your configuration, if desired, click the Factory Default radio button. For additional details, refer to the 5.3c/ Factory Reset/Restore Options section of this guide.

Note: *If you reset or reboot your Verizon Internet Gateway for Business, you may also need to disconnect your Gateway's power supply for a few minutes (3 or more) and then reconnect the power cable.*

TROUBLESHOOTING TIPS

6.0e/ LAN CONNECTION FAILURE

To troubleshoot a LAN connection failure:

- Verify your Verizon Internet Gateway for Business is properly installed, LAN connections are correct, and that the Verizon Internet Gateway for Business and communicating network devices are all powered on.
- Confirm that the computer and Gateway are both on the same network segment.

If unsure, let the computer get the IP address automatically by initiating the DHCP function, then verify the computer is using an IP address within the default range of 192.168.0.2 through 192.168.0.254. If the computer is not using an IP address within the correct IP range, it will not connect to your Verizon Internet Gateway for Business.

- Verify the subnet mask address is set to 255.255.255.0.

6.0f/ TIMEOUT ERROR OCCURS WHEN ENTERING THE URL OR IP ADDRESS

Verify the following:

- All computers are working properly.
- IP settings are correct.
- Verizon Internet Gateway for Business is on and connected properly.

- Verizon Internet Gateway for Business settings are the same as the computer.

For connections experiencing lag or a slow response:

- Check for other devices on the network utilizing large portions of the bandwidth and if possible temporarily stop their current utilization and recheck the connection.
- If lag still exists, clear the cache on the computer and if still needed, unplug the Ethernet cable or disable the Wi-Fi connection to the computer experiencing the slow connection and then reconnect or enable the Wi-Fi connection and try the connection again.

In rare cases you may also need to:

- Unplug the Ethernet cable to your Verizon Internet Gateway for Business and restart the Gateway, wait 1-2 mins. and insert the Ethernet cable again.
- Under limited circumstances you may use a port forwarding configuration on the Gateway, based on the application you are using (refer to the 5.0e/ Port Forwarding section or Verizon's support online help for more details).

TROUBLESHOOTING TIPS

6.0g/ FRONT LED AND WPS BUTTON

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

The rear panel's WPS Button allows quick access to the Wi-Fi Protected Setup (WPS) feature and handset paging/paring mode.

6.0h/ BOTTOM LIGHTED INDICATORS

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

6.1/ FREQUENTLY ASKED QUESTIONS

6.1a/ I'VE RUN OUT OF ETHERNET PORTS ON MY VERIZON INTERNET GATEWAY FOR BUSINESS. HOW DO I ADD MORE COMPUTERS OR DEVICES?

Plugging in an Ethernet hub or switch expands the number of ports on your Verizon Internet Gateway for Business.

- Run a straight-through Ethernet cable from the Uplink port of the new hub to the Gateway.

FREQUENTLY ASKED QUESTIONS

Use a crossover cable if there is no Uplink port/switch on your hub, to connect to the Gateway.

- Remove an existing device from the Ethernet port on your Gateway and use that port.

6.1b/ HOW DO I CHANGE THE PASSWORD ON MY VERIZON INTERNET GATEWAY FOR BUSINESS UI?

To change the password:

1. On the main screen, select **Advanced**, then select **System Settings** in the **System** section.
2. In the **User Settings** section, set a new password.

6.1c/ IS THE WI-FI OPTION ON BY DEFAULT ON MY VERIZON INTERNET GATEWAY FOR BUSINESS?

Yes, your Gateway's Wi-Fi option is activated out of the box.

6.1d/ IS THE WI-FI SECURITY ON BY DEFAULT WHEN THE WI-FI OPTION IS ACTIVATED?

Yes, with the unique WPA2 (Wi-Fi Protected Access II) key, also called the Wi-Fi Password, that is printed on the sticker on the bottom of your Verizon Internet Gateway for Business.

6.1e/ ARE MY VERIZON INTERNET GATEWAY FOR BUSINESS' ETHERNET PORTS AUTO-SENSING?

Yes. Either a straight-through or crossover Ethernet cable can be used.

6.1f/ CAN I USE AN OLDER WI-FI DEVICE TO CONNECT TO MY VERIZON INTERNET GATEWAY FOR BUSINESS?

Yes, your Verizon Internet Gateway for Business can interface with 802.11b, g, n, ac or ax devices. The Gateway also can be setup to handle only n Wi-Fi cards, g Wi-Fi cards, b Wi-Fi cards, or any combination of the three.

6.1g/ CAN MY WI-FI SIGNAL PASS THROUGH FLOORS, WALLS, AND GLASS?

The physical environment surrounding your Verizon Internet Gateway for Business can have a varying effect on signal strength and quality. The denser the object, such as a concrete wall compared to a plaster wall, the greater the interference. Concrete or metal reinforced structures experience a higher degree of signal loss than those made of wood, plaster, or glass.

FREQUENTLY ASKED QUESTIONS

6.1h/ HOW DO I LOCATE THE IP ADDRESS THAT MY COMPUTER IS USING?

In Windows 8 or Windows 10, click the Windows button and select **Settings**, then click **Network & Internet** and **Status**. Click the **Properties** button for details of IP address.

On Mac OS X, open System Preferences and click the Network icon. The IP address displays near the top of the screen.

To find the IP address from the router GUI:

1. From the **Basic** menu, select **Devices** from the left pane.
2. Click the Settings icon to access the **Device Settings** page for that device to view detailed IP address information for the device.

6.1i/ I USED DHCP TO CONFIGURE MY NETWORK. DO I NEED TO RESTART MY COMPUTER TO REFRESH MY IP ADDRESS?

No. In Windows 8, Windows 10 and Mac OSX, unplug the Ethernet cable or Wi-Fi card, then plug it back in.

6.1j/ I CANNOT ACCESS MY VERIZON INTERNET GATEWAY FOR BUSINESS UI. WHAT SHOULD I DO?

If you cannot access the UI, verify the computer connected to your Verizon Internet Gateway for Business is set up to dynamically receive an IP address.

6.1k/ I HAVE A FTP OR WEB SERVER ON MY NETWORK. HOW CAN I MAKE IT AVAILABLE TO USERS ON THE INTERNET?

For a web server, enable port forwarding for port 80 to the IP address of the server. Also, set up the web server to receive that port. Configuring the server to use a static IP address is recommended.

For a FTP server, enable port forwarding for port 21 to the IP address of the server. Also, set up the web server to receive that port. Configuring the server to use a static IP address is recommended.

6.1l/ HOW MANY COMPUTERS CAN BE CONNECTED THROUGH MY VERIZON INTERNET GATEWAY FOR BUSINESS?

Your Verizon Internet Gateway for Business is capable of 254 connections, but we recommend having no more than 132 connections. As the number of connections increases, the available speed for each computer decreases.

07 /

SPECIFICATIONS

7.0 General Specifications

7.1 Connections

The specifications for your Verizon Internet Gateway for Business are as follows.

This includes standards, cabling types and environmental parameters.

GENERAL SPECIFICATIONS

Note: The specifications listed in this chapter are subject to change without notice.

7.0/ GENERAL SPECIFICATIONS

Model Number:	ASK-NCQ1338E
Technical Standard:	LTE Category 18, 5G NR Sub 6
Frequency band:	LTE Band: B2/B5/B13/B48/B66, DL 4x4 MIMO 5G Band: 256 QAM, DL 4x4 MIMO n2/n5/n48/n66/n77
Wi-Fi Standard:	802.11 a/b/g/n/ac/ax
Dimensions:	130mm x 136mm x 136mm (L x W x H)
Certifications:	FCC, UL
Operating Temperature:	5° C to 40° C (41° F to 104° F)
Storage Temperature:	-45° C to 70° C (-49° F to 158° F)
Operating Humidity:	5% to 90%
Storage Humidity:	5% to 95% (non-condensing)

7.1/ CONNECTIONS

DC Input: source adapter: 12V/2A

Ethernet: RJ-45 LAN * 2

08 /

NOTICES

8.0 Regulatory Compliance Notices

This chapter lists various compliance and modification notices, as well as the NEBS requirements and GPL.

REGULATORY COMPLIANCE NOTICES

8.0/ REGULATORY COMPLIANCE NOTICES

8.0a/ Class B Equipment

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

FCC regulations restrict the operation of this device to indoor use only.

RF Exposure:

To comply with FCC RF exposure compliance requirements, the antenna used for this transmitter must be installed to provide a separation distance of at least 28cm from all persons (indoor), and must not be co-located or operating in conjunction with any other antenna or transmitter.

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

8.0b/ NEBS (Network Equipment Building System) Statement

An external SPD is intended to be used with ASK-NCQ1338E.

WARNING: The intra-building ports of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly **MUST NOT** be metalically connected to interfaces that connect to the OSP or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 4 ports as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metalically to OSP wiring.

REGULATORY COMPLIANCE NOTICES

Caution: The Verizon Internet Gateway for Business must be installed inside the home or office. The Gateway is not designed for exterior installation.

8.0c/ GENERAL PUBLIC LICENSE

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

<https://verizon.com/opensource/>

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

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