



SURFboard® G34/G36 DOCSIS® 3.1 Wi-Fi® Cable Modem

User Guide, STANDARD Revision x.5

P/N 365-095-36134

CommScope copyrights and trademarks

© 2021 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change. ARRIS and the ARRIS Logo are trademarks of CommScope, Inc. and/or its affiliates. All other trademarks are the property of their respective owners.

Wi-Fi Alliance®, Wi-Fi®, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi protected access® (WPA), the Wi-Fi Protected Setup logo, and WMM® are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance.

CommScope provides this guide without warranty of any kind, implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. ARRIS may make improvements or changes in the product(s) described in this manual at any time.

The capabilities, system requirements and/or compatibility with third-party products described herein are subject to change without notice.


Safety and regulatory information

Read all safety and regulatory information before installing your device and setting up your home network connection.

Important safety instructions

Read this before you begin — When using your equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock, and injury to persons, including the following:

- Read all the instructions listed here and/or in the user manual before you operate this device. Give attention to all safety precautions. Retain the instructions for future reference.
- This device must be installed and used in strict accordance with manufacturer's instructions, as described in the user documentation that is included with the device.
- Comply with all warning and caution statements in the instructions. Observe all warning and caution symbols that are affixed to this device.
- To prevent fire or shock hazard, do not expose this device to rain or moisture. The device must not be exposed to dripping or splashing. Do not place objects filled with liquids, such as vases, on the device.
- This device was qualified under test conditions that included the use of the supplied cables between system components. To ensure regulatory and safety compliance, use only the provided power and interface cables and install them properly.
- Different types of cord sets may be used for connections to the main POWER supply circuit. Use only a main line cord that complies with all applicable device safety requirements of the country of use.
- Installation of this device must be in accordance with national wiring codes and conform to local regulations.
- Operate this device only from the type of power source indicated on the device's marking label. If you are not sure of the type of power supplied to your home, consult your dealer or local power company.
- Do not overload outlets or extension cords, as this can result in a risk of fire or electric shock. Overloaded AC outlets, extension cords, frayed power cords, damaged or cracked wire insulation, and broken plugs are dangerous. They may result in a shock or fire hazard.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay attention to cords where they are attached to plugs and convenience receptacles; and examine the point where they exit from the device.
- Place this device in a location that is close enough to an electrical outlet to accommodate the length of the power cord.
- Place the device to allow for easy access when disconnecting the power cord of the device from the AC wall outlet.

- Do not connect the plug into an extension cord, receptacle, or other outlet unless the plug can be fully inserted with no part of the blades exposed.
 - Place this device on a stable surface.
 - Avoid damaging the device with static by touching the coaxial cable when it is attached to the earth-grounded coaxial cable-TV wall outlet.
 - Always first touch the coaxial cable connector on the device when disconnecting or reconnecting the Ethernet cable from the device or user's PC.
 - Installation of an AC surge protector in the AC outlet to which this device is connected is recommended. This is to avoid damaging the device by local lightning strikes and other electrical surges.
 - Postpone installation until there is no risk of thunderstorm or lightning activity in the area.
 - Avoid using a telephone (other than a cordless type) during an electrical storm. There is a remote risk of electric shock from lightning. For added protection, unplug the device from the wall outlet and disconnect the cables to avoid damage to this device from lightning and power surges.
 - Do not use this product near water. For example, near a bathtub, washbowl, kitchen sink, laundry tub, swimming pool, or in a wet basement.
 - Do not use the telephone to report a gas leak located near the leak.
 - Do not cover the device or block the airflow to the device with any other objects. Keep the device away from excessive heat and humidity and keep the device free from vibration and dust.
 - Wipe the device with a clean, dry cloth. Never use cleaning fluid or similar chemicals. Do not spray cleaners directly on the device or use forced air to remove dust.
 - For added protection, unplug the device from the wall outlet and disconnect the cables to avoid damage to this device during lightning activity or power surges.
-  **CAUTION:** To reduce the risk of fire, use only No. 26 AWG or larger (e.g., 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord, or national equivalent.
- Upon completion of any service or repairs to this device, ask the service technician to perform safety checks to determine that the device is in safe operating condition.
 - Do not open the device. Do not perform any servicing other than that contained in the installation and troubleshooting instructions. Refer all servicing to qualified service personnel.
 - This device should not be used in an environment that exceeds 104° F (40° C).

SAVE THESE INSTRUCTIONS



Note: To CATV system installer — This reminder is provided to call the CATV system installer's attention to Section 820.93 of the National electric code, which provides guidelines for proper grounding and, in particular, specifies that the coaxial cable shield must be connected to the grounding system of the building, as close to the point of cable entry as practical.

FCC statements

FCC Interference statement

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 environment. 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 device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Increase the separation between the device 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.

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.



CAUTION: Any changes or modifications not expressly approved by CommScope for compliance could void the user's authority to operate the equipment.

FCC Declaration of Conformity

CommScope, Inc, 3871 Lakefield Drive, Suwanee, GA 30024, declares that the SURFboard device complies with 47 CFR Parts 2 and 15 of the FCC rules as a Class B digital device.

FCC Radiation Exposure statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with the FCC RF exposure compliance requirements, the separation distance between the antenna and any person's body (including hands, wrists, feet and ankles) must be at least 8 inches (20.3 centimeters).

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter except those already approved in this filing.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destinations. The firmware setting is not accessible by the end user.

Wireless LAN information



Note: This applies to devices that provide Wi-Fi capability.

This device is a wireless network product that uses Direct Sequence Spread Spectrum (DSSS) and Orthogonal Frequency-Division Multiple Access (OFDMA) radio technologies. The device is designed to be interoperable with any other wireless DSSS and OFDMA products that comply with:

- The IEEE 802.11 Standard on Wireless LANs (Revision AC, Revision B, Revision G, and Revision N), as defined and approved by the Institute of electrical electronics engineers.
- The wireless fidelity (Wi-Fi) certification as defined by the Wireless Ethernet Compatibility Alliance (WECA).



Restrictions on the use of wireless devices

In some situations, or environments, the use of wireless devices may be restricted by the proprietor of the building or responsible representatives of the organization. For example, using wireless equipment in any environment where the risk of interference to other devices or services is perceived or identified as harmful.

If you are uncertain of the applicable policy for the use of wireless equipment in a specific organization or environment, you are encouraged to ask for authorization to use the device prior to turning on the equipment.

The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of the devices included with this product, or the substitution or attachment of connecting cables and equipment other than specified by the manufacturer. Correction of the interference caused by such unauthorized modification, substitution, or attachment is the responsibility of the user.

The manufacturer and its authorized resellers or distributors are not liable for any damage or violation of government regulations that may arise from failing to comply with these guidelines.



Note: The use of the 5150-5250 MHz frequency band is restricted to indoor use only.



Warning: This device allows you to create a wireless network. Wireless network connections may be accessible by unauthorized users. For more information on how to protect your network, refer to the relevant chapters in this document or visit our Consumer Support website at <http://www.arris.com/selfhelp>.

Caring for the environment by recycling your ARRIS equipment



Please do not dispose of this product with your residential or commercial waste. Contact your local authorities for information about practices established for your region. If collection systems are not available, call ARRIS Technical Support at **1-877-466-8646** for assistance.

Table of contents

Chapter 1: Introduction.....	10
In the box.....	10
Additional items needed (not included).....	11
System requirements.....	11
Contact information.....	11
Chapter 2: Product overview.....	12
Front panel and LED behavior.....	12
Rear panel and connectors.....	13
Wi-Fi cable modem label.....	15
Chapter 3: Getting started.....	16
Set up your G34/G36 home Wi-Fi network using your client device.....	16
Chapter 4: Add devices to your home Wi-Fi network	19
Quick connect using the Windows task bar.....	20
Connect using the Windows control panel.....	22
Chapter 5: Test your Wi-Fi network connection.....	25
Chapter 6: Using the Wi-Fi Cable Modem Web Manager.....	26
Start the G34/G36 Web Manager (first-time login).....	26
Start the G34/G36 Web Manager.....	29
G34/G36 Web Manager menu links.....	31
Exit the G34/G36 Web Manager.....	33
Chapter 7: Configuring your Wi-Fi network.....	34
Set up your Wi-Fi network.....	34
Change your Wi-Fi network name (SSID).....	38
Set up WPS on your Wi-Fi network.....	40
Chapter 8: Protecting & monitoring your Wi-Fi network.....	42
Change the login password.....	42
Set up firewall protection.....	44
IPv4 security.....	44
IPv6 security.....	46
Set up Parental Control.....	46

Set up Port Forwarding.....	50
Set up Port Triggers.....	52
Set up the DMZ host.....	54
Set up the ALG.....	55
Restore the G34/G36 default configuration settings.....	56
Exchange the routing information.....	57
Set up Dynamic DNS client.....	57
Manage UPnP network.....	58
Set up MAC bridging.....	59

Chapter 9: Managing your Wi-Fi cable modem and connected

networks.....	61
View the G34/G36 system hardware information.....	61
View the G34/G36 software version.....	62
Set up an Ethernet port connection for your data input.....	62
Reboot the G34/G36.....	64
Reboot the G34/G36 using the Reset button.....	64
Reboot the G34/G36 using the Web Manager.....	65
Restore the G34/G36 default configuration settings.....	66
Exit the G34/G36 Web Manager.....	67

Chapter 10: Troubleshooting tips.....68

Solutions.....	68
----------------	----

Introduction

Welcome to the next generation of ultra, high-speed ARRIS® DOCSIS 3.1® Wi-Fi cable modems. The SURFboard G34/G36 is a combination of DOCSIS 3.1 cable modem and multi-port Ethernet router with Wi-Fi. It uses DOCSIS 3.1 technology to provide ultra, high-speed Internet access in your home or small business network. Using the connection capabilities of the Wi-Fi cable modem, you can connect your computer and other network-enabled devices using the four Ethernet ports or the 2.4 GHz and 5 GHz wireless connections. The G34/G36 connects to the existing coaxial cable connection in your home.




The ARRIS SURFboard Central mobile app assists you with your modem setup and functions. It steps you through installing your home Wi-Fi network using your iOS or Android mobile device and lets you manage your home network access, Parental Control, Guest Access, and more on all your connected devices (e.g., smartphones, cameras, tablets, computers, smart TVs, gaming consoles, and more) across your home Wi-Fi network.


This user guide provides instructions for installing and configuring your G34/G36, setting up secure Wi-Fi network connections for your network devices, and managing your Wi-Fi home network configuration.

In the box

Before installing your G34/G36, check that the items listed in the table below are included in the G34/G36 product box. If any items are missing, please call ARRIS technical support at **1-877-466-8646** for assistance.

Table 1: G34/G36 package contents

Item		Description
G34/G36 Wi-Fi cable modem		High-speed DOCSIS 3.1 cable modem, wireless access point, and four-port Ethernet router
Wall power supply		Power supply for an electrical wall outlet connection
Software License & Warranty card		Contains safety and regulatory information, software license, and warranty for the G34/G36.

Item		Description
SURFboard Quick Start Guide		Provides information for installing your Wi-Fi cable modem and setting up a secure Wi-Fi network connection in your home or small business network.

Additional items needed (not included)

The following items are not included in the product box and must be purchased separately, if required:

- Coaxial (coax) cable - if one is not already connected to a cable wall outlet
- RF splitter - for additional coaxial cable connections, such as a set-top box or smart TV
- Ethernet cable - for each additional Ethernet-enabled device

System requirements

- High-speed Internet access account
- Web browser access – Internet Explorer, Google Chrome, Firefox, or Safari
- Compatible operating systems:
 - Windows® 10
 - Windows 8
 - Windows 8.1
 - Windows 7 service pack 1 (SP1)



Note: Although older versions of Microsoft Windows operating systems are no longer specifically supported, they should still function with your G34/G36.

- Mac® 10.4 or higher
- UNIX®
- Linux®

Contact information

For technical support and additional ARRIS product information:

- Visit the ARRIS Support website: www.arris.com/selfhelp
- Call ARRIS Technical Support: **1-877-466-8646**

Product overview

Front panel and LED behavior

Figure 1: G34/G36 front view



LED behavior

LED behavior	LED action
Amber (Solid)	Power is connected
Green (Blinking)	Acquiring downstream/ upstream connection
Green (Solid)	Online status in DOCSIS 3.0 mode
Blue (Solid)	Online status in DOCSIS 3.1

LED behavior	LED action
	mode
Light Blue (Solid)	WAN over Ethernet mode
Amber (Blinking)	Firmware download

Rear panel and connectors

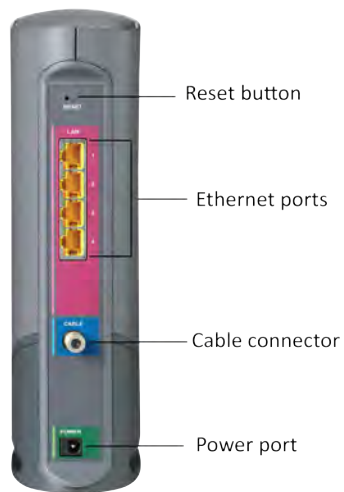


Figure 2a: G34 rear view

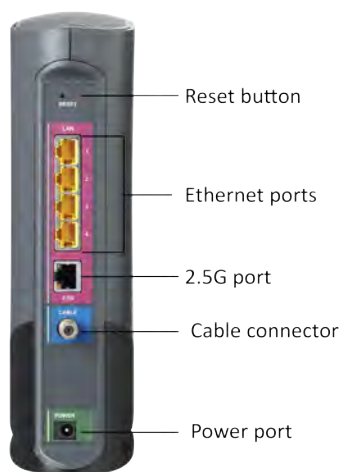





Figure 2b: G36 rear view

Rear panel and connectors

Port name	Description
Reset button	Reset button located on the rear panel of your G34/G36 can be used to either reboot your G34/G36 or reset the G34/G36 configuration settings. See Reboot the G34/G36 using the Reset button (page 64) and Restore the G34/G36 default configuration settings (page 56) for more information.
 ETHERNET 10/100/1000	Four one-gigabit Ethernet ports for RJ-45 network cable connections: <ul style="list-style-type: none"> ■ Green: LED is ON - Indicates a data transfer rate of one gigabit per second ■ Green: LED is Blinking - Indicates data traffic is in progress ■ Amber: LED is ON - Indicates a data transfer rate of less than one gigabit per second ■ Amber: LED is Blinking - Indicates data traffic is in progress
 ETHERNET 2.5 GE (available in G36 unit)	One 2.5 Gigabit Ethernet port for RJ-45 network cable connection: Note: CAT6 Ethernet cable and 2.5-Gigabit Ethernet capable device is required to achieve Ethernet connection throughout up to 2.5 Gbps. <ul style="list-style-type: none"> ■ Green: LED is ON: Indicates a data transfer rate of 2.5 gigabit per second ■ Green: LED is Blinking: Indicates data traffic is in progress ■ Amber: LED is ON: Indicates a data transfer rate of less than 2.5 gigabit per second ■ Amber: LED is Blinking: Indicates data traffic is in progress
 CABLE	Coaxial cable connector
Power port	100 - 240 VAC Power connector must reflect a 12 VDC @2.5A power adapter. Warning: To avoid any damage to your G34/G36, only use the power supply included in the G34/G36 box.
2.5G	This is available in only G36 Wi-Fi cable modem to connect to the 2.5G Ethernet port.

Wi-Fi cable modem label



Figure 3: Sample G34/G36 Wi-Fi cable modem label

The Wi-Fi cable modem labels are located on the bottom of your G34/G36. The labels contain the information you will need to activate the G34/G36 for your home Internet service or technical support issues.

To activate your Internet service, contact your service provider for assistance. When contacting your service provider or [ARRIS Technical Support](#) (page 11), you may have to provide the following information listed on the G34/G36 labels:

- Wi-Fi cable modem Model name (G34/G36)
- Wi-Fi cable modem Serial number (SN)
- Wi-Fi cable modem MAC address (HFC MAC)

Getting started

This product is for indoor use only. Do not route the Ethernet cable(s) outside of the building. Exposure of the cables to lightning could create a safety hazard and damage the product.

Before installing your G34/G36 Check with your service provider (or local cable company) to ensure broadband cable service is available in your area.

Some screenshots throughout this chapter may contain images of a model different than your own, these are simply examples and the app on your mobile device should represent the model you are configuring.

You can set up your G34/G36 home Wi-Fi network in one of the following ways.

- **Using the Surfboard Central app (SBC app):** It is recommended that you set up your home Wi-Fi network using the SBC app. For details on how to set up, refer to the **SURFboard Central User Guide for Wi-Fi Cable Modems** available on the <http://www.arris.com/selfhelp>.
- **Using client device (laptop/desktop):** If you are using your client device (laptop/Desktop) with a wired Ethernet connection to set up your home Wi-Fi network then perform the following task.
 - [Set up your G34/G36 home Wi-Fi network using your client device](#) (page 16)

Set up your G34/G36 home Wi-Fi network using your client device

To set up your Internet connection on your home network using your client device (laptop/desktop):

- Ensure to choose a location in your home where your computer and Wi-Fi cable modem are preferably near existing cable and electrical wall outlets.
- Ensure to keep the information such as Wi-Fi cable modem model name (G34/G36), HFC MAD ID, and the serial number (SN) listed on your cable modem label (available on the bottom of your modem and last page of the Quick Start Card) ready as you may need them while contacting your service provider. See [Wi-Fi cable modem label](#) (page 15)) for more information.



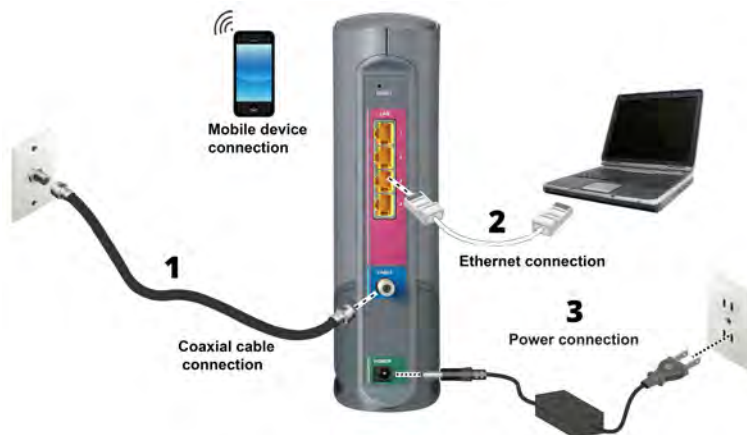
Note: Your G34/G36 supports using an Ethernet port connection for your data input in place of an RF cable connection. You will be able to connect to an alternate Internet connection and use your G34/G36 as your router and Wi-Fi source. This is a

useful feature if you choose to change your Internet service to a provider that is not a cable operator. You can still use the G34/G36 as your Wi-Fi router.

You can enable or disable this feature which is available for the LAN Ethernet port 4 as WAN over Ethernet. See [Set up an Ethernet port connection for your data input](#) (page 62) for more information.



G36 connection diagram



G34 connection diagram

1. Check that a coaxial cable is already connected to a cable wall outlet or RF splitter (not included) and then connect the other end of the coaxial cable to the **Cable** connector on the rear of your G34/G36.
 - Use your hand to tighten the connectors to avoid damaging them. Proceed with step 2.
 - Connect an Ethernet cable to the fourth **Ethernet** port on the rear of your G34/G36. Proceed with step 3.
 2. Connect an Ethernet cable to any available **Ethernet** port on the rear of your G34/G36.
 3. Connect the other end of the Ethernet cable to the **Ethernet** port on your computer.
- Repeat steps 2 and 3 for an additional computer or other network device that you want to install as a wired connection on your home network.

4. Connect the power cord to the **Power** port on the rear of your G34/G36.
5. Plug the other end of the power cord into an electrical wall outlet that is not controlled by a wall switch.



Note: This automatically powers ON your G34/G36. There may be up to a 15 second delay for the LED on the G34/G36 front panel to light up after the power is connected.

Although your computer may already be configured to automatically access the Internet, you should still perform the following connectivity test to verify that the devices were connected properly.

6. Power ON the computer connected to your G34/G36 if it is turned off, and then log in.
7. Contact your service provider to activate (provision) the G34/G36. You may have to provide the **HFC MAC ID** listed on the Wi-Fi cable modem label.
8. Enter your service provider's web browser URL:

- Comcast/Xfinity: <http://www.xfinity.com/activate>
- Cox: <http://www.cox.com/activate>
- Spectrum: <http://spectrum.net/selfinstall>

9. After the G34/G36 is provisioned (or activated), open a web browser (such as Internet Explorer, Google Chrome, Firefox, or Safari) on your computer.

10. Click www.surfboard.com or type a valid URL in the address bar and then press **Enter**.

The ARRIS SURFboard website or your URL of choice should open. If the website fails to open, please contact your service provider for assistance.

11. Check that the front panel LED on the G34/G36 lights up in sequential order. See [Front panel](#) (page 12) for additional LED status information.

- If the LED did not light up and you do not have an Internet connection, you may have to contact your service provider to reactivate the G34/G36 or check for signal issues.
- If you still cannot connect to the Internet, please call ARRIS Technical Support at **1-877-466-8646** for assistance.

Add devices to your home Wi-Fi network



Note: You will need the **Wi-Fi Network Name (SSID)** and **Wi-Fi Security Key (Network Password)** to connect your client devices to your home network. The default network name and network password are listed on the G34/G36 [Wi-Fi cable modem label](#) (page 15).



Choose one of the options listed below for the client device you are using to set up a Wi-Fi network connection on your home network. Repeat for each additional device:

- **Personal Computer (PC)** – Select one of the following:
 - [Quick connect using the Windows task bar](#) (page 20)
 - [Connect using the Windows control panel](#) (page 22)

The steps for setting up your Wi-Fi network connection may differ slightly depending on the version of Microsoft Windows running on your client device. The steps used in this section apply to Windows 7.

Android device

From any screen on your client device:


1. Select  to open the  Settings screen.
2. Select **Wi-Fi** to turn it ON.

Your device will automatically start searching and then display a list of available Wi-Fi networks.

3. Select your Wi-Fi network name (SSID) from the list.
4. If prompted, type your Wi-Fi Security Key (network password). Please note that your network password may be case-sensitive.
5. Select **Connect**. If your Wi-Fi network connection is successful, "Connected" will display under your network name.

Apple computer

From any screen on your client device:

1. Click  (Wi-Fi icon) to display a list of available Wi-Fi networks.
2. Select the Wi-Fi network name (SSID) for your home network from the list.
3. If prompted, enter your network password in the Password field.



Note: Checkmark **Remember this network** if you want your Mac computer/ client device to automatically connect to your home network when you log on. Your computer must be within range of your Wi-Fi network to connect to it.

4. Click **OK**.

Apple mobile device

From the Home screen on your client device:

1. Select **Settings** to open the Wi-Fi screen.
2. Select **Wi-Fi** to turn it ON.

Your device will automatically start searching and then list the available Wi-Fi networks.

3. Select the Wi-Fi network name (SSID) for your home network from the list to connect.

If your Wi-Fi connection is successful, ✓ will display next to the Wi-Fi network name.



Note: For more information on setting up your Wi-Fi network connections, refer to the user documentation for your specific client device.

Quick connect using the Windows task bar

1. From the Windows taskbar on your computer, click the **Wi-Fi Link** icon to open the list of available Wi-Fi networks.



Figure 9: Sample Microsoft Windows taskbar icons



Note: If the **Wi-Fi Link** icon is not visible, left click on the **Show hidden icons** button on the Windows taskbar to open the list of additional icons.

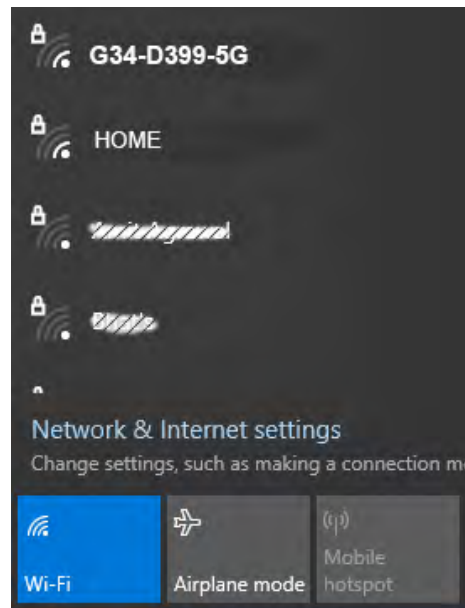


Figure 10: Sample available Wi-Fi networks Microsoft Window

2. Locate and left-click on the G34/G36 Wi-Fi network name or SSID (for example, G34/G36-####) for your G34/G36 from the list of available Wi-Fi networks.

The default SSID is located on the Wi-Fi cable modem on the bottom of your G34/G36.



Note: You must use the default SSID listed on the Wi-Fi cable modem label when installing the Wi-Fi cable modem and setting up your first Wi-Fi network connection. You can change the SSID after your network connections are up and running. See [Change your Wi-Fi network name \(SSID\)](#) (page 38) for more information.

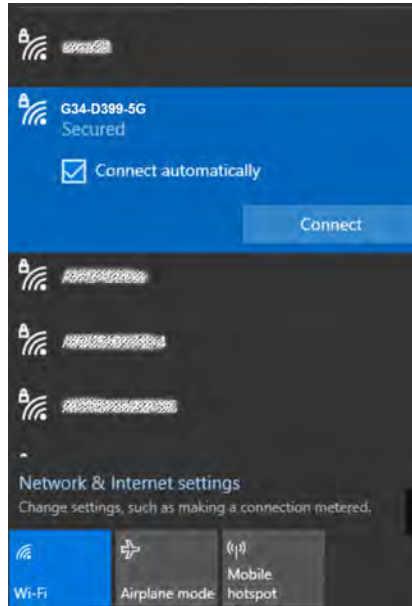


Figure 11: Sample Wi-Fi network connection screen

3. Select **Connect automatically** to set up your Wi-Fi devices to automatically connect to your Wi-Fi network without having to log on using a user password.
4. Click **Connect** to open the Connect to a Network window and set up your new network password.

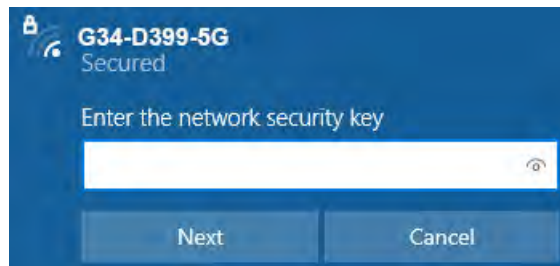


Figure 12: Network security key window

5. Enter the **Network Security Key** (your Wi-Fi network password) in the **Security key** field.



Note: You can use the default Wi-Fi Security Key code listed on the G34/G36 Wi-Fi cable modem label or enter your own personal Wi-Fi network password. See [Change the login password](#) (page 42) for more information on creating login passwords.

If you have already changed your Wi-Fi network password using the G34/G36 Web Manager, enter that password in the **Enter the network security key** field and then click **Next**.

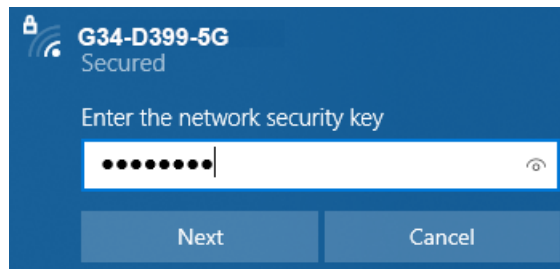
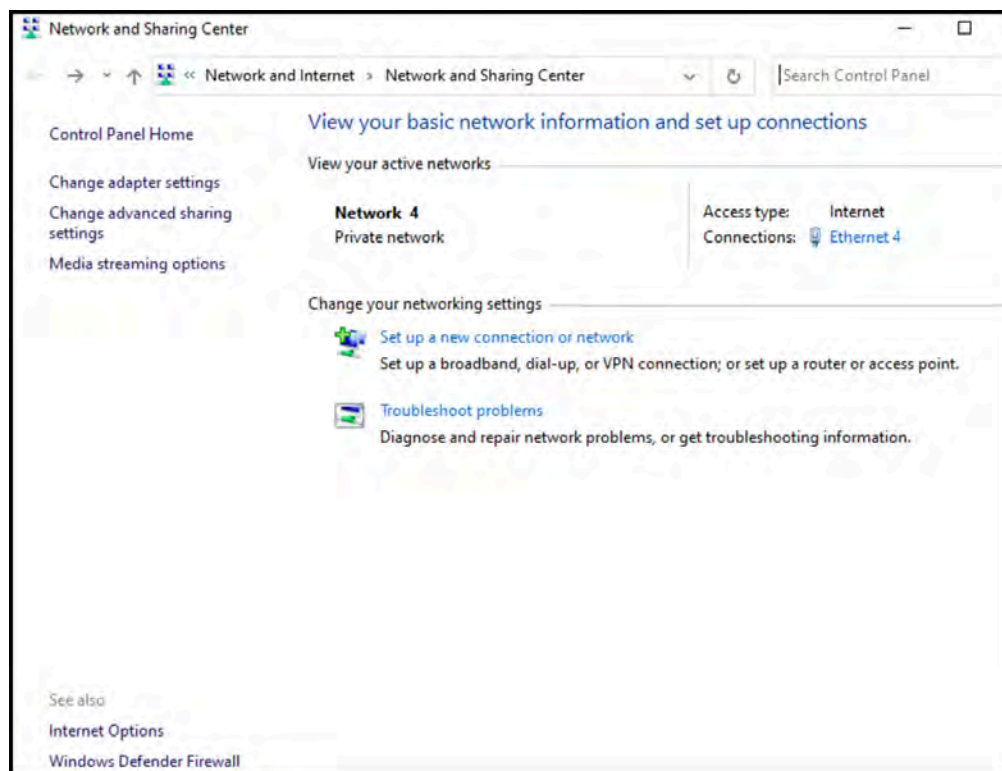


Figure 13: Network security key window

Connect using the Windows control panel

1. From the Windows taskbar on your computer, click **Start** button and then click **Control Panel**.
2. Click **Network and Sharing Center** to open the Network and Sharing Center window.

Figure 14: Control panel-network and sharing center window



3. Click **Set up a new connection or network** under Change your networking settings panel.

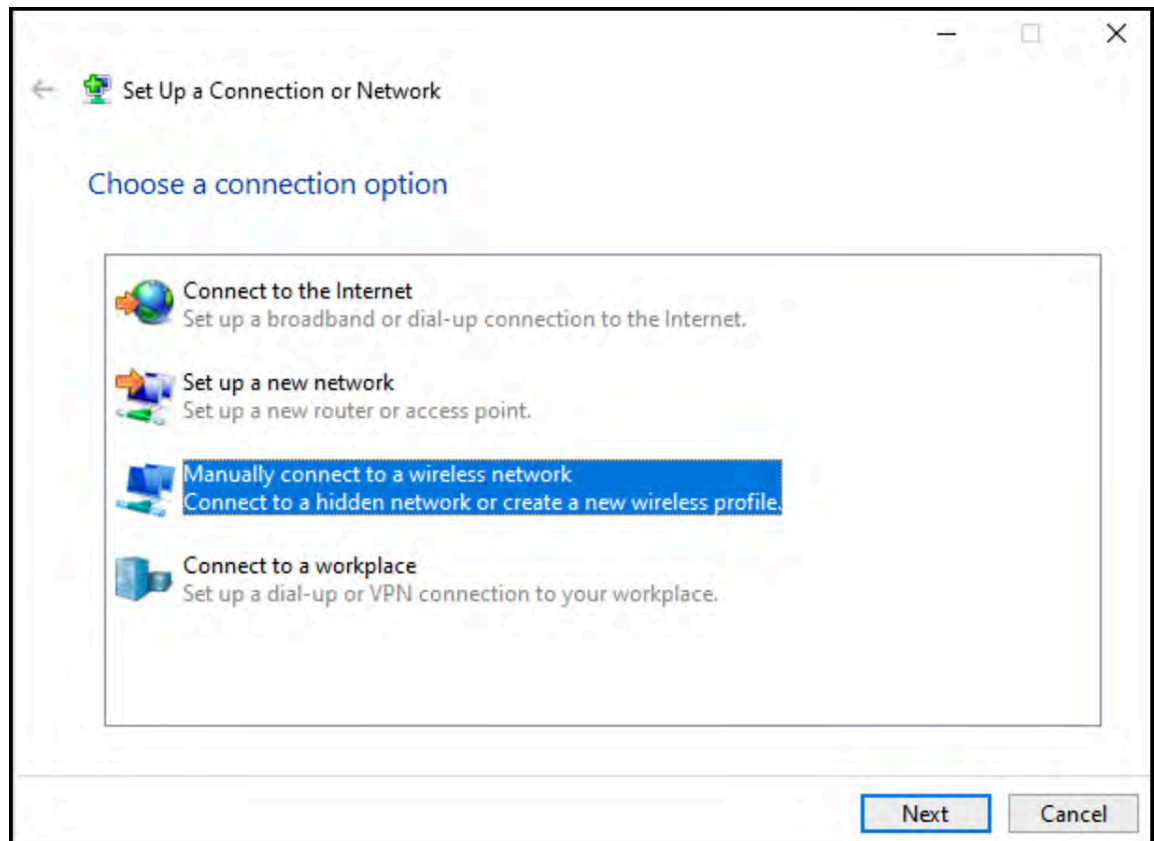


Figure 15: Set up a connection or network window

4. Click **Manually connect to a wireless network** and then click **Next**.

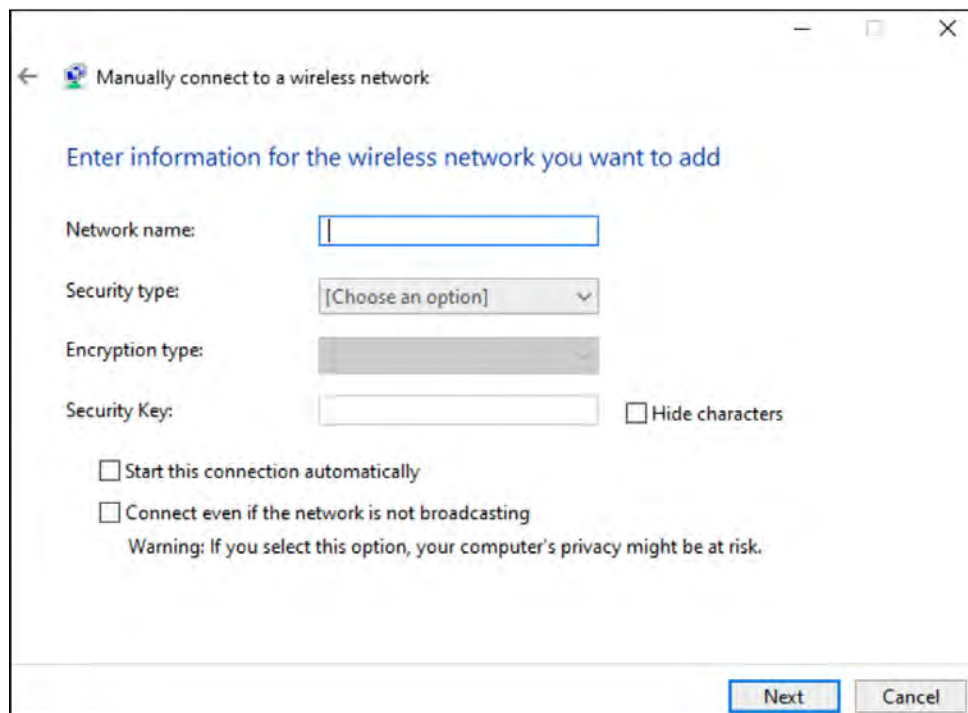


Figure 16: Manually connect to a wireless window

5. Enter the G34/G36 Wi-Fi network name or SSID (G34/G36-####) for your G34/G36 in the **Network name** field.

The default SSID is listed on the Wi-Fi cable modem label on the bottom of your G34/G36.



Note: You have the option to change your Wi-Fi network name or SSID after setting up your Wi-Fi network connection. However, you must use the default SSID listed on the Wi-Fi cable modem label after installing your Wi-Fi cable modem. See [Change your Wi-Fi network name \(SSID\)](#) (page 38) for more information.

6. Select the wireless Security level for your Wi-Fi network from the **Security type** drop-down list.



Note: WPA2-Personal is the recommended wireless security level for your Wi-Fi home network. It is the default security level for the G34/G36 and the highest security level available.

7. Select the password encryption type from the **Encryption type** drop-down list.

This is used for securing your Wi-Fi network.

- TKIP – Temporal Key Integrity Protocol
- AES – Advanced Encryption Standard (recommended). AES is the default encryption type for the G34/G36.

8. Enter a security code (passphrase) for your Wi-Fi network password in the **Security Key** field.

You can use the default **WI-FI SECURITY KEY** listed on the G34/G36 Wi-Fi cable modem label or create your own personal network password.



Note: Remember to use a unique combination of letters, numbers, and special characters to create a more secure password. See [Change the login password](#) (page 42) for more information.

9. Select **Hide characters** checkbox to prevent your Security Key (network password) from displaying in the field.
10. Select **Start this connection automatically** so that your Wi-Fi devices will automatically connect to your Wi-Fi network when they are powered on.
11. Click **Next** to complete the Wi-Fi network setup.

The Successfully added <Network name> message for your new Wi-Fi network should appear.

12. Click **Close** to exit.

Test your Wi-Fi network connection

Perform the following connectivity test to check that Wi-Fi connections were established for the G34/G36 and the other Wi-Fi devices on your home network:

1. Check if your Wi-Fi devices successfully connected to your Wi-Fi network, then disconnect the Ethernet cable, if connected, from your computer and the G34/G36.
2. Check that the LED on the G34/G36 front panel is lit SOLID Green in DOCSIS 3.0 mode and SOLID Blue in DOCSIS 3.1 mode.
3. Open a web browser on your computer, such as Internet Explorer, Google Chrome, Firefox, or Safari.
4. Type a valid URL (such as www.surfboard.com) in the address bar and then press **Enter**.

If the website failed to open, please contact your service provider or call ARRIS Technical Support at **1-877-466-8646** for assistance.

Using the Wi-Fi Cable Modem Web Manager

Use the G34/G36 Web Manager to view and monitor the network configuration settings and operational status of your G34/G36. You can also configure your network connections and Wi-Fi security settings, see [Protecting & monitoring your Wi-Fi network](#) (page 42) for more information.

To ensure that your Wi-Fi home network is secure, ARRIS recommends that you follow these best practices for creating your login password:

- Always create a secure password or pass phrase that is not easily guessed.
- Use phrases instead of names so that it may be easier for you to remember.
- Use a combination of upper and lowercase letters, numbers, and symbols.

Start the G34/G36 Web Manager (first-time login)



Note: Your network security is very important to ARRIS. The first time you log on to the G34/G36, the Gateway Home Network Wizard opens for you to set up your login password. The wizard walks you through setting up your G34/G36 Web Manager login password, Wi-Fi home network security information, and time zone.

1. Open a web browser (such as Internet Explorer, Google Chrome, Firefox, or Safari) on your client device (for example, a computer or a laptop) that is connected to your G34/G36.
2. Type the default LAN IP address, **192.168.0.1**, in the Address bar and then press Enter to log onto the G34/G36.

The G34/G36 Home Network Wizard screen displays (see figure 17).

3. Enter your password in the **New Password** field.



Note:

The password is case-sensitive and must include each of the following:

- Minimum of eight characters
- At least one uppercase alphabetic character: A through Z
- At least one number: 0 to 9
- One of the following special characters:
~ ! @ # \$ % ^ * () - _ = + [] { } | ; , . / ?

- Please note that this password is required to log in to the G34/G36 Web Manager. Write it down and place it in a secure place for future reference and availability, if needed.

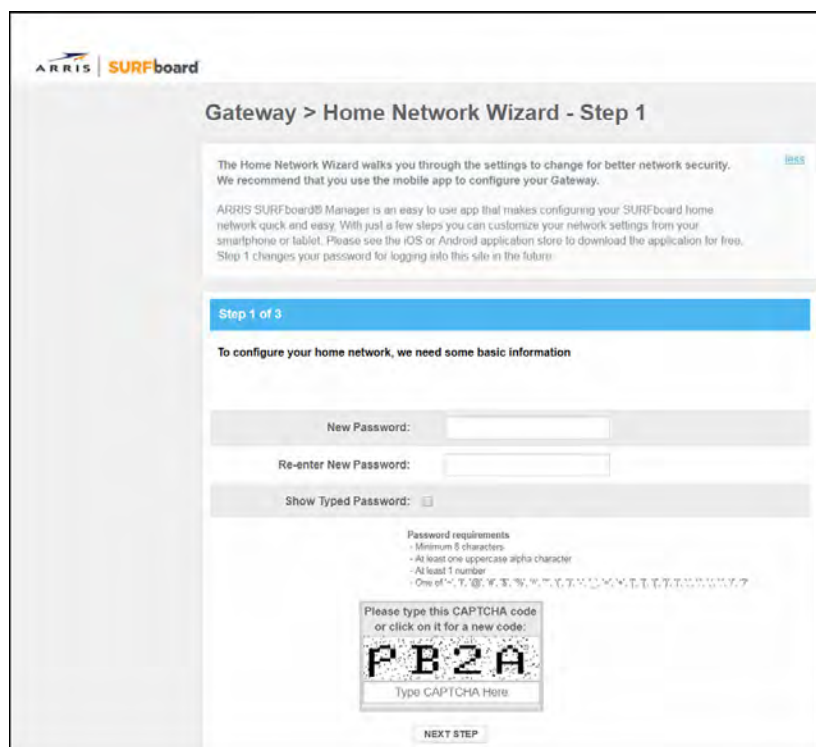


Figure 17: G34/G36 Home Network Wizard-Step 1 screen

- The G34/G36 Home Network Wizard – Step 2 screen displays.

Gateway > Home Network Wizard - Step 2

You may want to edit information about your Wi-Fi network for both 2.4 GHz and 5 GHz Wi-Fi bands. [more](#)

Step 2 of 3

We need to configure your wireless network. Note that your network can be accessed by both 2.4 GHz and 5 GHz compatible devices.

Wi-Fi Network Name (2.4GHz):

Encryption Method (2.4GHz):

Network Password (2.4GHz):

WPA2/3 requires a 8-63 ASCII character password.

Wi-Fi Network Name (5 GHz):

Encryption Method (5 GHz):

Network Password (5 GHz):

WPA2/3 requires a 8-63 ASCII character password.

NEXT STEP

Figure 18: G34/G36 Home Network Wizard-Step 2 screen

8. Keep or change the current default Wi-Fi network name in the **Wi-Fi Network Name (2.4 GHz)** field.

To change the Wi-Fi network name, enter a new name of your choice. The network name can consist of any combination of up to 32 alphanumeric characters.

9. Select one of the following Wi-Fi network security options for your G34/G36 Wi-Fi home network from the **Encryption Method (2.4 GHz)** drop-down list:
 - **Open (risky):** Network security is not set, and your Wi-Fi network is not secure. This network security option allows unauthorized access to your Wi-Fi network without a Wi-Fi Security Key (network password).
 - **WPA2-PSK (AES):** Wi-Fi Protected Access version 2 with Pre-Shared Key.
 - **WPA2/WPA3-PSK (TKIP/AES) (Recommended):** Wi-Fi Protected Access version 2 with Pre-Shared Key (most compatible).
 - **WPA3 Personal (AES):** Wi-Fi Protected Access version 3 with Pre-Shared Key.
 - **WPA 2/WPA3 Mixed Personal (AES) (Recommended):** Combination Wi-Fi Protected Access version 2 and Wi-Fi Protected Access version 3 and provides additional network security.
10. Keep or change the current default Wi-Fi network password in the **Network Password (2.4 GHz)** field.
11. Repeat steps 8 through 10 for your 5 GHz Wi-Fi network settings.
12. Click **NEXT STEP** to continue.

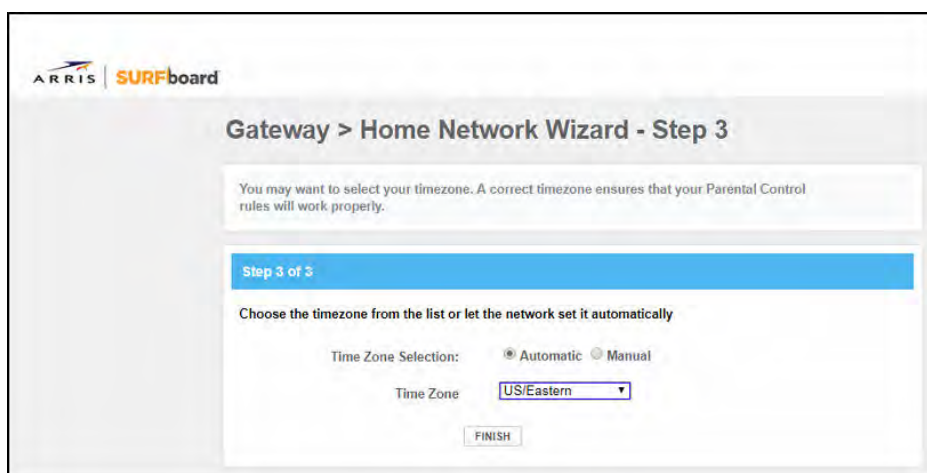


Figure 19: G34/G36 Home Network Wizard-Step 3 screen

13. Select **Automatic** or **Manual** to set up your time zone.
 - Select **Automatic** to allow the network to automatically set your time zone.
 - Select **Manual** to choose your time zone from the **Time Zone** drop-down list.
14. Click **FINISH**.

Start the G34/G36 Web Manager

To open the G34/G36 Web Manager:

1. Open a web browser (such as Internet Explorer, Google Chrome, Firefox, or Safari) on the computer or laptop connected to your G34/G36.
2. Type the default LAN IP address, **192.168.0.1**, in the Address bar and then press **Enter** to log onto the G34/G36 and open the G34/G36 Web Manager Login screen.

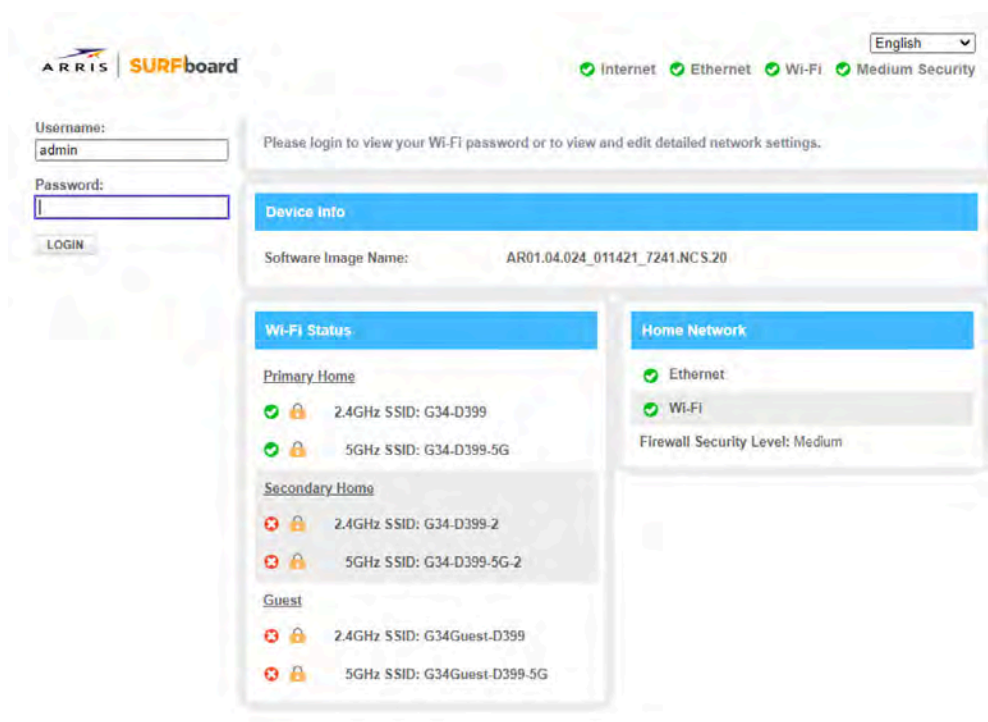


Figure 20: G34/G36 Web Manager Login screen

3. Type **admin** for the default login username (case-sensitive) in the **Username** field.
4. Type your new password in the **Password** field.

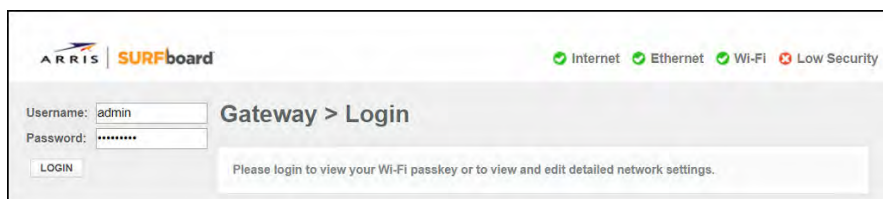


Figure 21: G34/G36 Web Manager Login screen

5. Click **LOGIN** to open the G34/G36 Web Manager.

The Product Registration window opens.

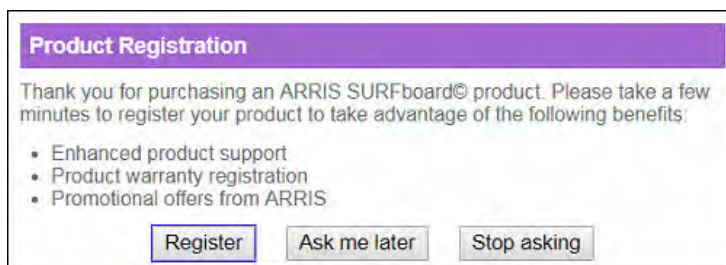


Figure 22: G34/G36 Product Registration screen

6. Click **Register**, **Ask me later**, or **Stop asking** to proceed.

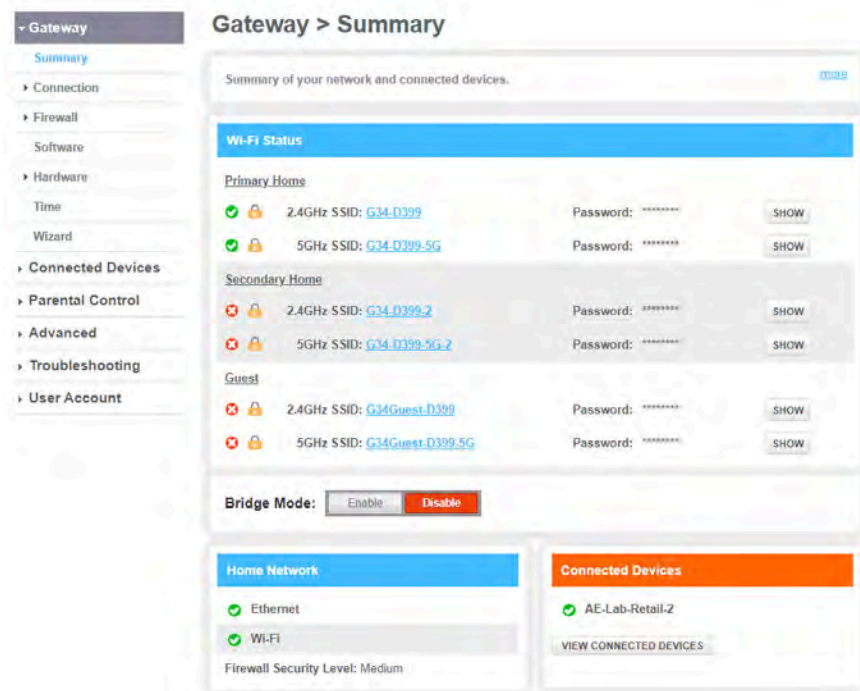


Figure 23: G34/G36 Summary screen



Note: See [Set up your Wi-Fi network](#) (page 34) to configure your home network for Wi-Fi.

G34/G36 Web Manager menu links

The G34/G36 main menu links and related submenu option links are displayed along the left side of the G34/G36 Web Manager screen. Click on the main menu link to expand the list of submenu options.

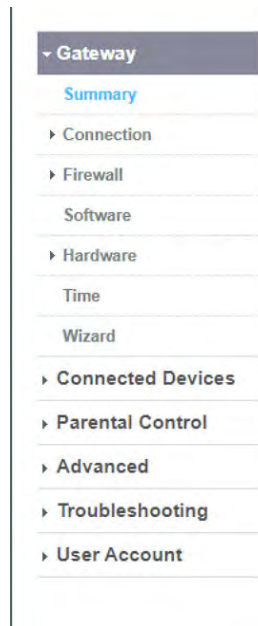


Figure 24: G34/G36 Web Manager menu links

Table 4: G34/G36 Web Manager menu links

Menu link	Function
Gateway	Displays a summary of your network connections and a list of the connected devices on your home network.
Summary	Displays the Wi-Fi status for your home network and network-connected devices.
Connection	Displays the network connection and status information for the G34/G36 network, Local IP network, and your private Wi-Fi network.
Firewall	Configures the G34/G36 firewall settings to protect your home network from possible attacks from hackers or viruses.
Software	Displays information related to the G34/G36 software version.
Hardware	Displays status information for the G34/G36 hardware, such as the battery status, Ethernet connection(s), and Wi-Fi connections.
Time	Allows you to set the time on your G34/G36 based on your selected time zone.
Wizard	Allows you to configure the default network settings on your G34/G36 to set up a secure home network.
Connected Devices	Provides general information for the connected devices on your home network.
Advanced	Allows you to set up Port Forwarding, Port Triggering, Remote Management for troubleshooting or maintenance purposes, the DMZ Host, and manage the UPnP network on your home network.

Menu link	Function
Troubleshooting	Provides several options to help you resolve certain problems that may occur with your G34/G36.

Exit the G34/G36 Web Manager

To log out and close the G34/G36 Web Manager:

- Click **Logout** link located in the upper right corner of the G34/G36 Web Manager screen.



Figure 25: G34/G36 Web Manager logout link

Configuring your Wi-Fi network

You have the option to either use the default network settings which are unique to your G34/G36 for security purposes or you can configure different network settings. The G34/G36 supports a secure method for setting up multiple Wi-Fi networks on your G34/G36.

Set up your Wi-Fi network

1. Open a web browser and log on to the G34/G36 to open the G34/G36 Web Manager.
See [Start the G34/G36 Web Manager \(first-time login\)](#) (page 26) for more information, if necessary.
2. Click the menu links **Gateway > Connection > Wi-Fi > Networks**.
The Gateway Connection Wi-Fi screen appears.



Figure 26: G34/G36 Wi-Fi connection screen

- To set up the Network Security mode for your Wi-Fi home network, click the Home Wi-Fi Network **2.4 GHz EDIT** button.

Figure 27: Wi-Fi network setup screen

The screenshot shows the 'Edit Home 2.4 GHz' configuration page. On the left is a navigation menu with options like Gateway, Connection, Status, WAN, Local IP Network, Wi-Fi, Networks, 2.4 GHz Radio, 5 GHz Radio, MAC Filtering, WPS, Firewall, Software, Hardware, Time, Wizard, Connected Devices, Parental Control, Advanced, Troubleshooting, and User Account. The main content area is titled 'Gateway > Connection > Wi-Fi > Edit Home 2.4 GHz' and includes a 'Manage your Home 2.4 GHz network settings.' link. The 'Home 2.4 GHz' section contains:

- 'Wireless Network:' with 'Enable' and 'Disable' buttons.
- 'Network Name (SSID):' with a text field containing 'G34-D399'.
- 'Security Mode:' with a dropdown menu set to 'WPA2WPA3-PSK (AES) (Recommended)'. A note below states: 'Please note 802.11 n/a mode is only compatible with AES and Open encryption!'.
- 'Network Password:' with a masked text field and a 'SHOW' button. A note below states: 'WPA2/3 requires a 8-63 ASCII character password'.
- 'Broadcast Network Name (SSID):' with a checked 'Enabled' checkbox.
- 'Enable WMM:' with a checked 'Enabled' checkbox.

 At the bottom, there is a 'Save Settings' button and a CAPTCHA challenge box that says 'Please type this CAPTCHA code or click on it for a new code:' with the code 'W6Y3' and a 'Type CAPTCHA Here' input field. 'SAVE' and 'CANCEL' buttons are at the very bottom.

- Choose to either keep the default network name SSID (Service Set Identifier) for your Wi-Fi home network in the **Network Name (SSID)** field or enter a new network name of your choice.



Note: The Wi-Fi network name cannot be the same name as any other SSID on your home network. You can use any combination of lowercase and uppercase letters, numbers, and/or special characters (symbols) up to a maximum of 32 characters.

- Select one of the following Wi-Fi network security options for your G34/G36 from the **Security Mode** drop-down list:
 - **WPA2-PSK (TKIP/AES) (Recommended):** Wi-Fi Protected Access version 2 with Pre-Shared Key (most compatible).
This is the default network security option for your G34/G36. It provides the highest security and performance for your Wi-Fi network.
 - **WPA2-PSK (AES):** Wi-Fi Protected Access version 2 with Pre-Shared Key.
 - **Open (risky)** (not secure and not recommended): This network security option does not provide any level of network security for your Wi-Fi network. It allows outside users to connect to your Wi-Fi network without having to use a Wi-Fi Security Key (network password).
 - **WPA3 Personal (AES):** Wi-Fi Protected Access version 3 with Pre-Shared Key.
 - **WPA 2/WPA3 Mixed Personal (AES) (Recommended):** Combination Wi-Fi Protected Access version 2 and Wi-Fi Protected Access version 3 and provides additional network security.

6. Enter your Wi-Fi network password in the **Network Password** field.



Note: Keep in mind that network passwords are case-sensitive. You can use any combination of uppercase and lowercase letters, special characters, and numbers. Spaces are not acceptable.

7. Select the **Show Network Password** checkbox to view and confirm your network password.

8. Perform one of the following:

- Select the **Broadcast Network Name (SSID) Enabled** checkbox to display your SSID as an available Wi-Fi network to outside users.
- Deselect the **Broadcast Network Name (SSID) Enabled** checkbox to disable displaying your SSID as an available Wi-Fi network to outside users.



Note: When **Broadcast Network Name (SSID)** is enabled, your SSID is visible to unauthorized Wi-Fi clients that are within range of your Wi-Fi network to connect to your home network.

9. Select the **Enable WMM** checkbox to turn ON Wi-Fi Multi-media functionality.

Enabling WMM can help control latency and jitter when transmitting multi-media content over a Wi-Fi connection. This quality of service mechanism uses four access categories:

- Voice
- Video
- Best effort
- Background

WMM ensures that applications with low tolerance for latency and jitter are treated with higher priority than less sensitive data applications. WMM sets different wait times for the above four categories to provide priority network access for applications that are less tolerant of packet delays.

10. Enter the CAPTCHA code located in the Type CAPTCHA Here entry box.

11. Click **SAVE** to save the settings.

12. To set up the Network Security mode for your Wi-Fi home network, click the Home Wi-Fi Network **5 GHz EDIT** button.

13. Perform steps 4 through 11.

14. To enable separate virtual networks for your Wi-Fi clients, in the G34/G36 Wi-Fi connection screen, select the **AP Isolation** checkbox.



Figure 28: G34/G36 Wi-Fi connection screen (1 of 2)



Note: When AP Isolation is enabled, each of your Wi-Fi clients will be in its own virtual network and will not be able to communicate with the other Wi-Fi clients. This may be useful if several guests are using your Wi-Fi network.

15. To turn ON the 2.4 GHz Wi-Fi frequency range for your Wi-Fi home network, click the **2.4 GHz Radio** submenu and then click **Enable** button .
16. Select the wireless networking standard mode for your Wi-Fi home network from the **Mode** drop-down list.
17. Select the Tx (Transmit) Power level of the Wi-Fi radio from the **Tx Power** drop-down list.
18. Select a channel number (Auto, 1 through 11) from the **Channel** drop-down list to set the communications channel for your Wi-Fi cable modem.



Note: For 2.4 GHz Wi-Fi networks, it is recommended to use Channel 1, 6, or 11, if it is not listed as the Current Channel. In the Wi-Fi spectrum, there are multiple channels that overlap and thus degrade Wi-Fi network performance. Channels 1, 6, and 11 are used for better network performance and stability because they do not overlap.

19. Set the channel bandwidth for your Wi-Fi cable modem from the **Channel Bandwidth** box.
20. To enable the dynamic channel selection option, click **Enable** .
21. To set the DCS scan interval, you can choose from the **DCS Scan Interval** drop-down list.
22. Click **SAVE SETTINGS** to save the changes.

23. To turn ON the 5 GHz Wi-Fi frequency range for your Wi-Fi home network, click the **5 GHz Radio** submenu and then click **Enable** button .

Figure 29: Wi-Fi connection 5GHz Radio screen

Gateway > Connection > Wi-Fi > 5 GHz Radio

Manage your Wi-Fi connection settings. [more](#)

5 GHz Wi-Fi Radio Configuration

Wireless Radio: ☒ Enable ☐ Disable

Mode: 802.11 a/n/ac/ax ▼

Tx Power: 100% ▼

DFS: ☒ Disable ☐ Enable

Channel Selection: ☐ Manual ☒ Automatic

Channel: 157 ▼

Channel Bandwidth: ☐ 20 ☐ 20/40 ☒ 20/40/80 ☐ 20/40/80/160 ☐ Auto

Dynamic Channel Selection: ☐ Disable ☒ Enable

DCS Scan Interval: 8 Hours ▼

MU-MIMO: ☐ Disable ☒ Enable

[SAVE SETTINGS](#)

24. Perform steps 16 through 22.

Change your Wi-Fi network name (SSID)

The SSID (Service Set Identification) is the Wi-Fi network name assigned to your G34/G36 Wi-Fi network. The default SSID (listed on the Wi-Fi cable modem label) is automatically populated in the network configuration screens. A list of available Wi-Fi networks (SSIDs) near your home (for example, neighbors or local businesses) will display when you or someone else in your home attempts to establish a Wi-Fi network connection. For security purposes and quick recognition of your Wi-Fi network, ARRIS recommends that you change the default SSID.



Note: When you change the SSID, any Wi-Fi devices that are connected to your Wi-Fi network will be disconnected. The Wi-Fi devices must be reconnected to your Wi-Fi network using the new SSID.

To change your Wi-Fi network name (SSID):

1. Open a web browser and log on to the G34/G36 to open the G34/G36 Web Manager.
See [Start the G34/G36 Web Manager](#) (page 29) for more information, if necessary.
2. From any G34/G36 Web Manager screen, click the **Gateway** menu link and then click the **Connection** submenu options link.

- Click **Wi-Fi** under the **Connection** submenu options to open the Gateway Connection Wi-Fi screen.



Figure 30: G34/G36 change Wi-Fi network name (SSID) screen

- Click the **2.4 GHz EDIT** or **5 GHz EDIT** button in the Home Wi-Fi Network section to select the current Wi-Fi frequency range for your Wi-Fi home network.

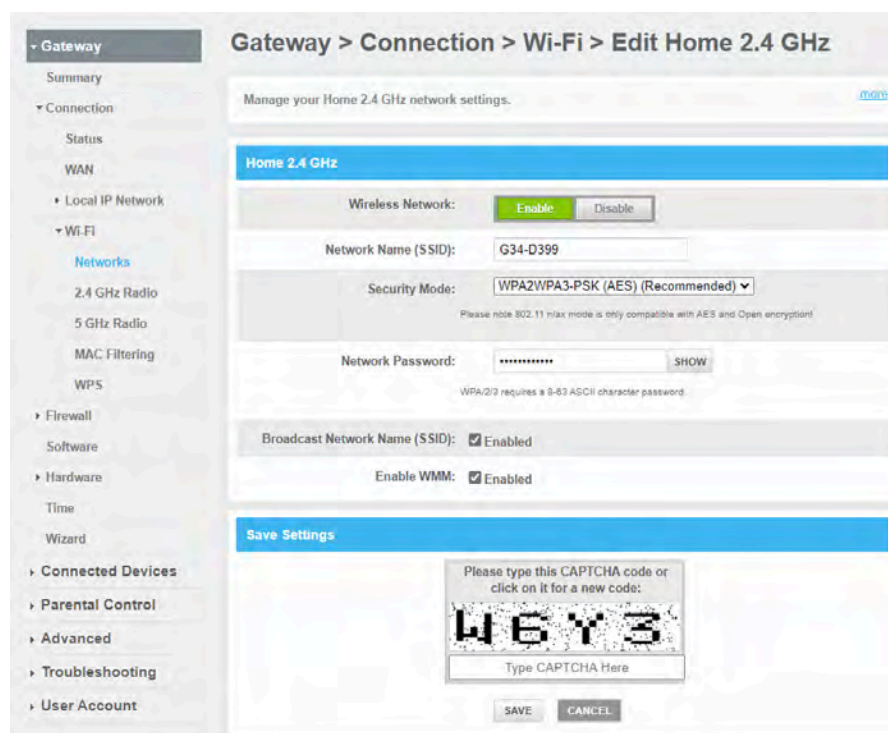



Figure 31: Sample G34/G36 Wi-Fi network setup screen

5. Ensure to select **Enable** in the **Wireless Network** field.
 6. Enter a new network name in the **Network Name (SSID)** field.
The Wi-Fi network name cannot be the same name as any other SSID on your home network. You can use any combination of lowercase and uppercase letters, numbers, and/or special characters (symbols) up to a maximum of 32 characters.
 7. Enter a new network password in the **Network Password** field if you want to change it.
-  **Note:** Remember that network passwords are case-sensitive and that you can use any combination of uppercase and lowercase letters, special characters, and numbers. Spaces are not acceptable.
8. Select the **Show Network Password** checkbox to view your network password.
 9. Enter the CAPTCHA code located in the **Type CAPTCHA Here** entry box.
 10. Click **SAVE SETTINGS** to update your new SSID.

Set up WPS on your Wi-Fi network

You can set up the Wi-Fi Protected Setup (WPS) PIN option on your G34/G36 to connect WPS-enabled devices on your Wi-Fi home network.

1. Open a web browser and log on to the G34/G36 to open the G34/G36 Web Manager.
See [Start the G34/G36 Web Manager](#) (page 29) for more information, if necessary.
2. Click the **Gateway** menu link and then click the **Connection** submenu options link.
3. Click **Wi-Fi > WPS** to open the Gateway Connection Wi-Fi screen.

Add Wi-Fi Client (WPS)

Wi-Fi Protected Setup (WPS): **Enable** **Disable**

AP PIN: 16618442

WPS PIN Method: **Enable** **Disable**

☒ **Push Button (recommended)**
Click PAIR button below to connect your Wireless client to your network.

☐ **PIN Method**
If your Wireless client supports WPS (PIN Type), enter the PIN number here

Enter Wireless Client's PIN:

Press PAIR button to begin pairing

PAIR

Figure 32: G34/G36 WPS device connection screen

4. Do one of the following:
 - Click the Wi-Fi Protected Setup (WPS) **Enable** button to turn ON WPS Wi-Fi networking on your home network using the provided AP PIN number.
 - Click the Wi-Fi Protected Setup (WPS) **Disable** button to turn OFF WPS Wi-Fi networking on your home network.
5. Do one of the following:
 - Click the WPS Pin Method **Enable** button to turn ON WPS Wi-Fi networking.
 - Click the WPS Pin Method **Disable** button to turn OFF WPS Pin connections.
6. To proceed with the PIN method, click the **PIN Method** option and then Enter the WPS Pin number listed in the **AP PIN** field when you are prompted on your WPS device screen.
7. Click **PAIR** to connect your WPS-enabled device.
8. Repeat steps 6 through 8 for each additional WPS-enabled device that you want to connect to your Wi-Fi home network.
9. To proceed with the Push button option, click the **Push Button (recommended)** option to connect your wireless client to your network.
10. Click **PAIR** to connect your WPS-enabled device.

Protecting & monitoring your Wi-Fi network

After you have successfully connected the G34/G36 and your Wi-Fi devices, you should configure the G34/G36 to protect your Wi-Fi network from unwanted and unauthorized access by any Wi-Fi devices that are within range of your Wi-Fi network. Although network security for the G34/G36 is already configured, you can use the G34/G36 Web Manager to set the level of security and network access that you want to allow on your Wi-Fi network.

Change the login password

When logging in to the G34/G36 Web Manager, you will be prompted to change the default login password. You will have the option to either keep the default password or change it (recommended). Please note that if you do not change the default login password, the same message will display every time you log in to the G34/G36 Web Manager.



Note: If you are already logged in to the Web manager, start with step 6 to change your login password.

1. Open a web browser on the computer or laptop connected to your G34/G36.
2. Type the default LAN IP address, **192.168.0.1**, in the Address bar and then press Enter to log on to your G34/G36.

The G34/G36 Login screen displays.

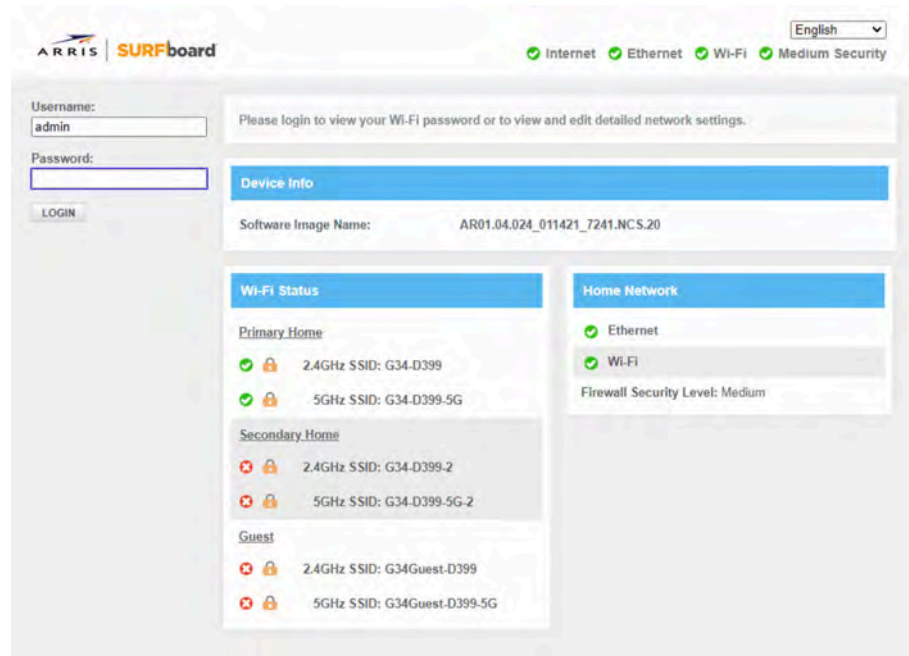


Figure 33: G34/G36 Login screen

3. Type **admin** for the default username (case-sensitive) in the **Username** field.
4. Type your password (case-sensitive) in the **Password** field.
5. Click **LOGIN** to open the G34/G36 Web Manager.
6. Click the **User Account** main menu link to change the password.

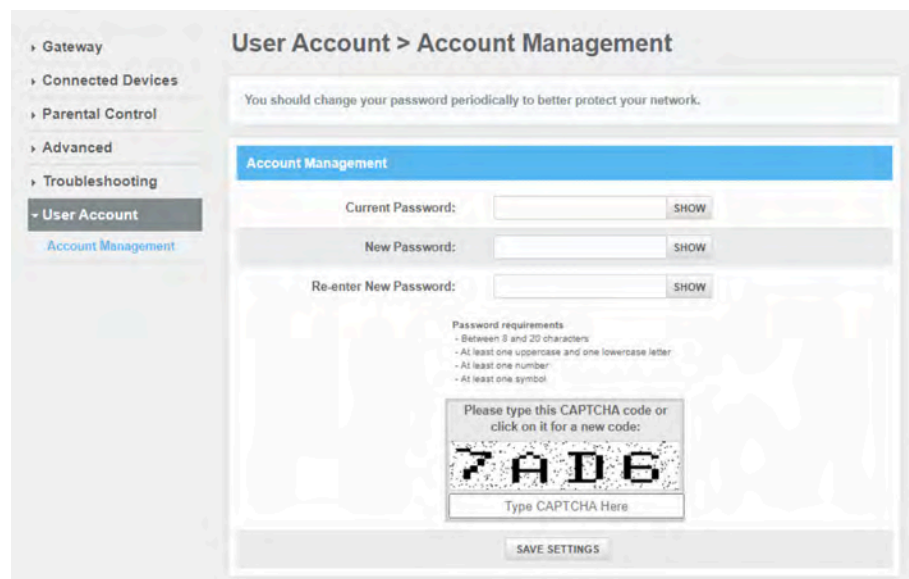


Figure 34: G34/G36 Change Password screen

7. Enter the current admin password in the **Current Password** field.
8. Enter your new admin password in the **New Password** field.



Note: Remember passwords are case-sensitive and that you can use any combination of the following letters, numbers, and special characters:

- Letters: **A** through **Z** (uppercase and lowercase)
 - Numbers: **0** to **9**
 - Special characters: **! @ # \$ % & ***
9. Enter your new admin password in the **Re-enter New Password** field.
 10. Select the **Show Typed Password** checkbox to view the new passwords and confirm that both passwords match.
 11. Enter the CAPTCHA code located in the **Type CAPTCHA Here** entry box.
 12. Click **SAVE** to update your admin password.
 13. Find a secure place to write down and keep your new password for future reference.

Set up firewall protection

You can set up firewall filters and firewall alert notifications to protect your computer(s) and other connected network devices on your Wi-Fi home network. You can also block Java Applets, Cookies, ActiveX controls, popup windows, Proxies, and website access to protect the network devices on your home network from hackers, viruses, and other attacks from the Internet.

To set the firewall protection level on your G34/G36:

1. From any G34/G36 Web Manager screen, click the **Gateway** menu link on the G34/G36 Web Manager screen.
2. Click the **Firewall** submenu link and then click [IPv4 security](#) (page 44) or [IPv6 security](#) (page 46) to display the Gateway Firewall Security Level screens.
3. Select the security level that you want to set for your G34/G36 firewall.
4. When done, click **SAVE SETTINGS**.

IPv4 security

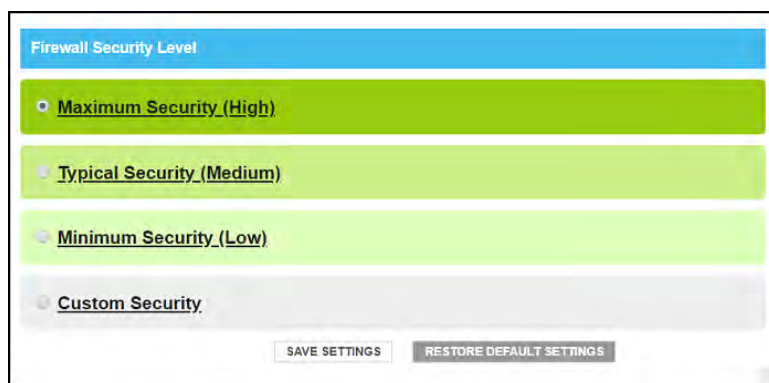


Figure 35: Firewall IPv4 available security levels screen

- **High:** Safest configuration, maximum security level

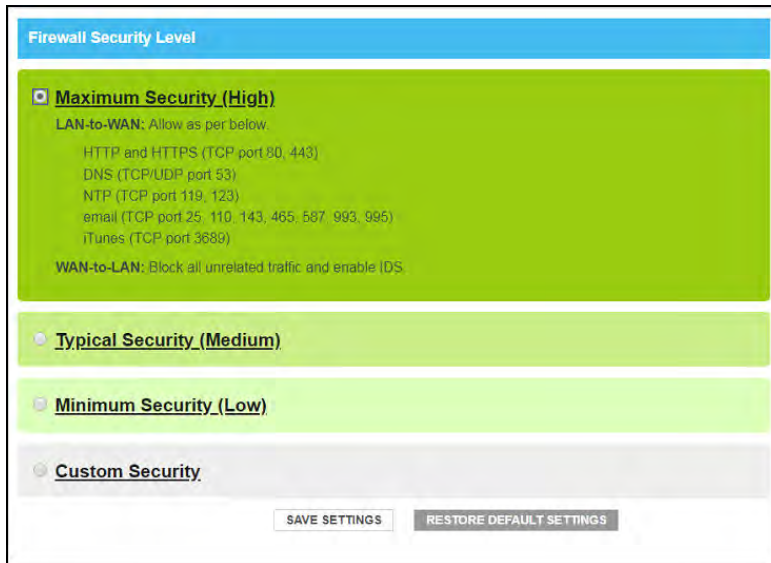


Figure 36: Firewall IPv4 high security level screen

- **Medium:** Safer configuration, medium security level



Figure 37: Firewall IPv4 medium security level screen

- **Low:** Common security, low security level, higher risk

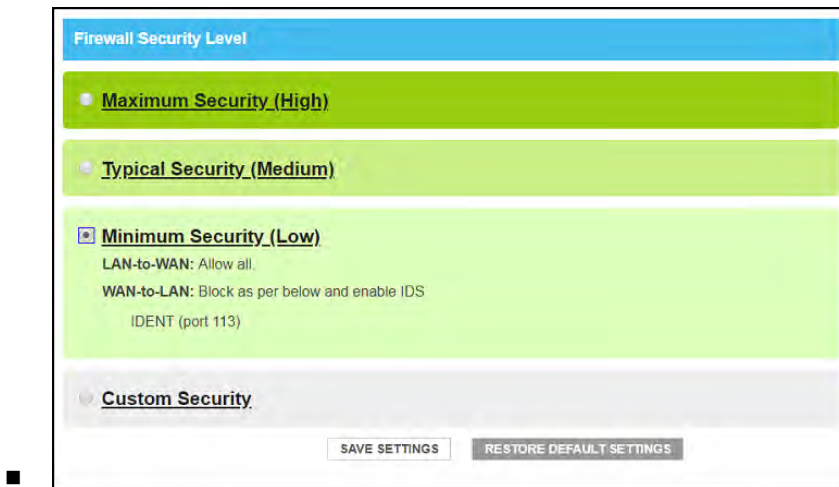


Figure 38: Firewall IPv4 low security level screen

IPv6 security

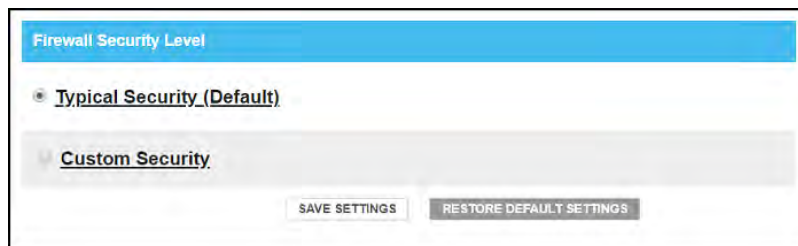


Figure 39: Firewall IPv6 available security levels screen

Set up Parental Control

You can set up the following parental controls to manage and limit the usage and activity for specific users and client devices on your home network:

- Allow or block access to specific Internet sites.
- Allow or block access to specific MAC addresses.
- Allow or block access based on specific keywords.
- Set time limitations for computer usage or Internet access.



Note: Any Parental Control filters that do not include assigned ports, will apply to all ports. This also applies to MAC addresses.

You can also link each user or client device on your home network to specific rules for login, time-access, and content filtering.

► To set up Parental Control on your home network:

1. From any G34/G36 Web Manager screen, click the **Parental Control** menu link on the G34/G36 Web Manager screen.
2. Click **Managed Sites** from the Parental Control submenu options list to display the Parental Control Managed Sites screen.

- Click the Managed Sites **Enable** button to turn ON website and keyword blocking.

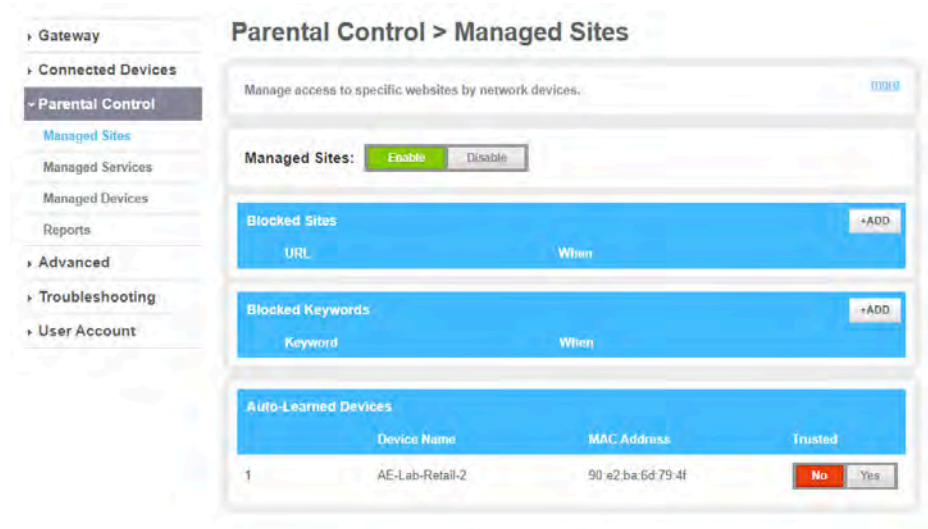


Figure 40: Parental Control Managed Sites screen

- Click **+ADD** button in the Blocked Sites section to open the Add Site to be Blocked screen.

Figure 41: Add Site to be Blocked screen

- To fully block a website, enter the website address in the URL field and then click the **Yes Always Block?** button.
- Click **SAVE**.
- Repeat steps 5 and 6 for each website that you want to block.
- To block a website for specific days and times, enter the website address in the URL field and then click the **No Always Block?** button.
- Select the **Start from** and **End on** times of the day in the Set Block Time section.

10. Select the days of the week in the Set Blocked Days section.
11. Click **SAVE**.
12. To manage network devices' access to specific services and applications, click **Manage Services** from the submenu and then click **Enable**.
13. Click **+ADD** button in the Blocked Services section to add a service to be blocked.

Figure 42: Managed Services screen - Add Blocked Service screen

14. Type the service that you want to block in the **User Defined Service** field.
15. Select **UDP**, **TCP**, or **TCP/UDP** for the port filter type from the **Protocol** drop-down list.
16. Enter the range of port numbers for the port filter range in the **Start Port** and **End Port** fields.
17. To fully block a service, click **Yes**, in the **Always Block?** field.
18. To block a service for specific days and times, click **No**, in the **Always Block?** field and then specify the time and days in the **Set Block Time** and **Set Block Days** fields.
19. Click **SAVE** to save the changes.
20. To manage access to specific devices on your network, click **Manage Devices** from the submenu.

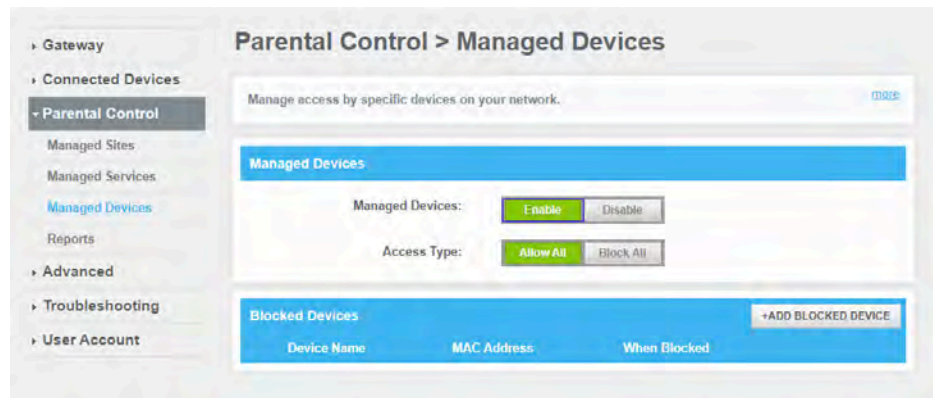


Figure 43: Manage Devices screen

21. To manage devices, click **Enable**.
22. If you do not want to restrict your devices, click **Allow All** and then click **+ADD BLOCKED DEVICE** to add only the device you want to restrict.
23. If you want to restrict your devices, click **Block All** and then click **+ADD ALLOWED DEVICE** to add only the device you do not want to restrict.

Figure 44: Add Blocked device screen

24. To manually block a device, type the **Device name** and the **MAC address** fields.
25. To fully block a device, click **Yes**, in the **Always Block?** field.

26. To block a device for specific days and times, click **No**, in the **Always Block?** field and then specify the time and days in the **Set Block Time** and **Set Block Days** fields.
27. Click **SAVE** to save the changes.
28. To generate, download and print reports based on your parental controls, click **Reports** from the sub menu.

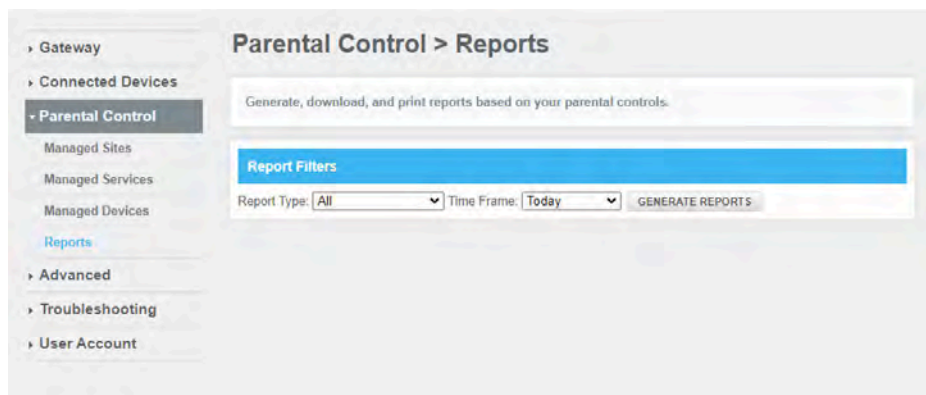


Figure 45: Generate report screen

29. Select the report type from the **Report Types** drop-down list and the time frame from the **Time Frame** drop-down list.
30. Click **GENERATE REPORTS**.

Set up Port Forwarding

Your G34/G36 firewall may be set up to block all device or application connections from the Internet to the devices on your Wi-Fi home network. Port Forwarding allows you to open specific ports or IP addresses on the Internet behind the firewall on your home or small business network. It also allows for remote access to your wireless computer or other client devices. The inbound traffic from the Internet, such as specific websites or online gaming applications, is forwarded to the designated open ports that you set up.



Note:

ARRIS recommends that you manually configure the TCP/IP settings listed below on the client device you are setting up for remote access. Otherwise, remote access to your client device will not be available on the Internet.

- IP address
- Subnet mask
- Default gateway
- DNS address (at least one)

To set up Port Forwarding:

1. From any G34/G36 Web Manager screen, click the **Advanced** menu link on the G34/G36 Web Manager screen.
2. Click **Port Forwarding** from the Advanced submenu options list to display the Port Forwarding Configuration screen.

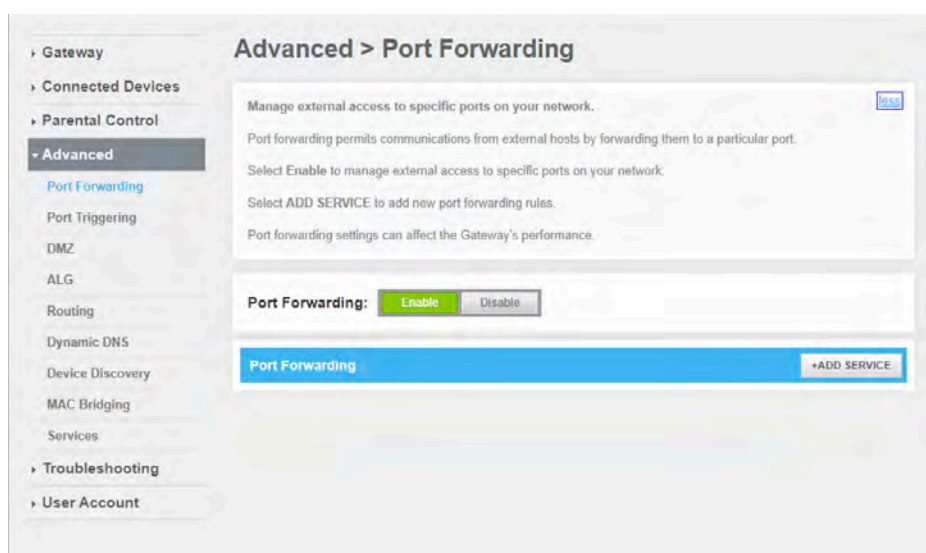


Figure 46: G34/G36 Advanced Port Forwarding screen

3. Click the Port Forwarding **Enable** button.
4. Click the **+ADD SERVICE** button to open the Add Port Forward screen.

Figure 47: Add Port Forward screen

5. Select **FTP**, **AIM**, **HTTP**, **PPTP**, **HTTPs**, **Telnet**, **SSH**, or **Other** for the Internet data transfer protocol from the **Common Service** drop-down list.



Note: When **Other** is selected, the **Service Name** field will display. Enter a name for the service type you will be using.

6. Select **TCP/UDP**, **TCP**, or **UDP** for the Internet data transmission protocol from the **Service Type** drop-down list.
7. Do one of the following:
 - Enter the IP address of your local computer that you are setting up for port forwarding in the **Server IPv4 Address** field.
 - Enter the IP address for your local computer that you are setting up for port forwarding in the **Server IPv6 Address** field.

8. Enter the starting port number of the website or online application in the **Start Port** field.
9. Enter the ending port number of the website or online application in the **End Port** field.
10. Click **CONNECTED DEVICE** button to display the list of connected devices on your Wi-Fi home network.

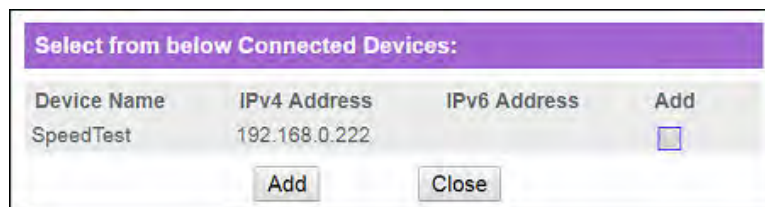


Figure 48: G34/G36 Connected Devices screen

11. Select the **Add** selection box for the device or website you want to connect to.
12. Click **Add** to exit.
13. Click **SAVE**.

Set up Port Triggers

You can use Port Triggers to set up your G34/G36 to monitor outgoing traffic on specific ports on your home network. Port Triggering can be useful for some applications such as video conferencing, online chatting, and online gaming that may require specific port numbers with bi-directional traffic to function properly.



Note: If the G34/G36 firewall is enabled and custom port triggers are set up, then you must configure the firewall to allow traffic through those custom ports. See [Set up firewall protection](#) (page 44) for more information.

To configure Port Triggers:

1. From any G34/G36 Web Manager screen, click the **Advanced** menu link on the G34/G36 Web Manager screen.
2. Click **Port Triggering** from the Advanced submenu options list to display the Port Triggering Configuration screen.

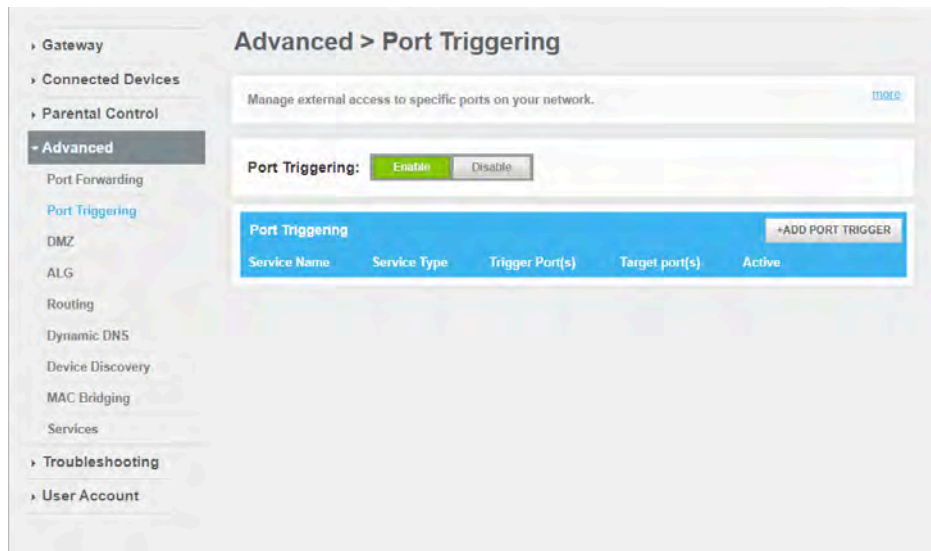


Figure 49: Advanced Port Triggering screen

3. Click the Port Triggering **Enable** button.

Figure 50: Advanced Add Port Trigger screen

4. Click the **+ADD PORT TRIGGER** button to open the Add Port Trigger screen.
5. Enter a name or description for the Port Trigger in the **Service Name** field.
6. Select **TCP/UDP**, **TCP**, or **UDP** from the **Service Type** drop-down list.
7. Enter the starting port number in the **Trigger Port From** field.
8. Enter the ending port number in the **Trigger Port To** field.
9. Enter the starting port number in the **Target Port From** field.
10. Enter the ending port number in the **Target Port To** field.
11. Click **ADD** to create the port trigger.
12. Repeat steps 4 through 11 to create additional port triggers.

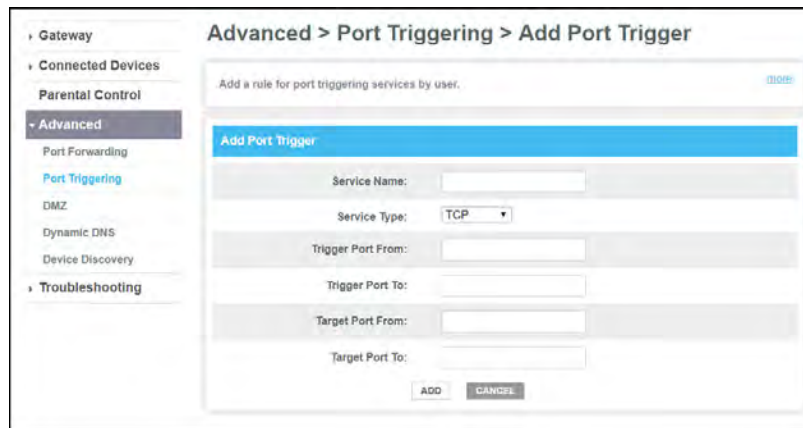


Figure 51: Advanced Add Port Trigger screen

Set up the DMZ host



Warning: The gaming DMZ host is not protected by the G34/G36 firewall. It is exposed to the Internet which makes it vulnerable to attacks or hacking from any client device (e.g., computer or laptop) on the Internet. Consider carefully before configuring a device to be in the DMZ.

You can configure one client device on your home network to be the DMZ Host. That client device will operate outside of the G34/G36 firewall and allow remote access from the Internet to your client device, gaming device, or other IP-enabled device. The DMZ Host feature will only allow outside users to have direct access to the designated DMZ Host device and not your home network.

To create the DMZ host:

1. From any G34/G36 Web Manager screen, click the **Advanced** menu link.
2. Click **DMZ** to display the Advanced DMZ screen.

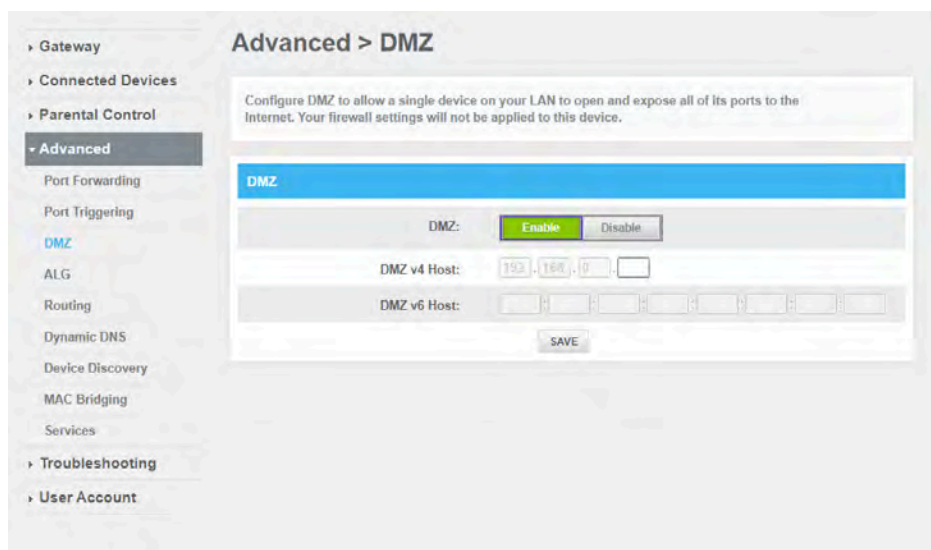


Figure 51: Advanced DMZ host screen

3. Click the **DMZ Enable** button to set up the DMZ Host on your home network.
4. Enter the last one to three digits (from 2 to 254) of the IP address of the computer or gaming device that you are setting up as the DMZ host
5. Click **SAVE** when you are finished.



Note: To disable the DMZ Host, click the **DMZ Disable** button and then click **SAVE**.



Note: Remember to reset the IP address back to 0 (zero) to close all the ports when you are finished with the needed application. If you do not reset the IP address, that computer will be exposed to the public Internet.

Set up the ALG

Application Layer Gateway (ALG) allows your router to recognize and treats certain network protocols.



Note: Please change these settings if recommended by your service provider.

To set up the ALG:

1. From any G34/G36 Web Manager screen, click the **Advanced** menu link.
2. Click **ALG** to display the ALG screen.

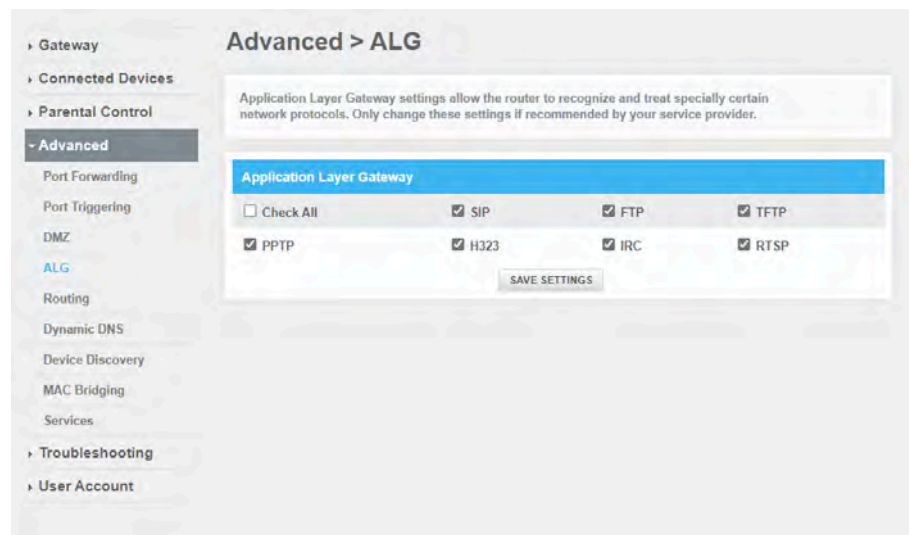


Figure 53: Advanced ALG screen

3. Click the required check boxes and then click **SAVE SETTINGS**.

Restore the G34/G36 default configuration settings



Warning: This action will delete your current G34/G36 configuration settings and allow you to restore the default (original) G34/G36 configuration.



Note: After the configuration settings are restored, the G34/G36 will automatically reboot, and you will have to log in using the default username (**admin**) and your current admin password.

To open the Restart/Restore Gateway screen:

1. From any G34/G36 Web Manager screen, click the **Troubleshooting** menu link.
2. Click **Restart/Restore** from the Troubleshooting submenu links to display the Troubleshooting **Restart/Restore Gateway** screen.

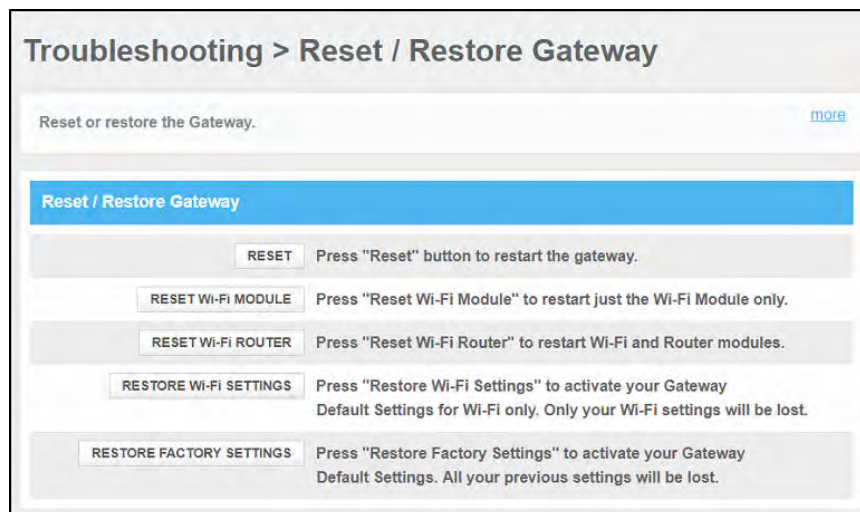


Figure 54: G34/G36 restore settings screen

3. Click **RESTORE WI-FI SETTINGS** to reset your G34/G36 Wi-Fi settings.

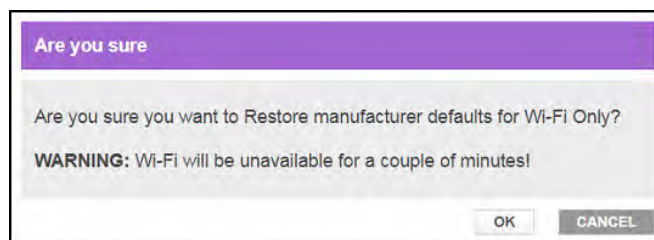


Figure 55: G34/G36 restore settings screen

4. Click **OK** to restore the Wi-Fi factory defaults.

The Operation in Progress for restarting the Wi-Fi radios message displays.

Exchange the routing information

The RIP protocol is used to exchange the routing information between the gateway and the headend.

To enable routing information:

1. From any G34/G36 Web Manager screen, click the **Advanced** menu link.
2. Click **Routing** to display the Routing screen.

Advanced > Routing

The RIP protocol is used to exchange the routing information between the gateway and headend. [Display](#)

If Routed Subnet is enabled, the Routed Subnet Address will be advertised with the next hop as the CM IP address.

RIP (Routing Information Protocol)

RIP:

Interface Name:

RIP Send Version:

RIP Receive Version:

Update Interval: sec

Default Metric:

Authentication Type:

Authentication Key & ID: ID:

Neighbor:

Routed Subnet Configuration

Routed Subnet:

Routed Subnet Address:

Routed Subnet Netmask:

Figure 56: Routing Information screen

3. Click **Enable** button to set up the routing information.
4. Specify the details for the RIP (Routing Information Protocol) and Routed Subnet Configuration.
5. Click **SAVE** to save the changes.

Set up Dynamic DNS client

You can configure your Gateway's router functionality as a Dynamic DNS client.

To create as DNS client:

1. From any G34/G36 Web Manager screen, click the **Advanced** menu link.
2. Click **Dynamic DNS** to display the Dynamic DNS client screen.

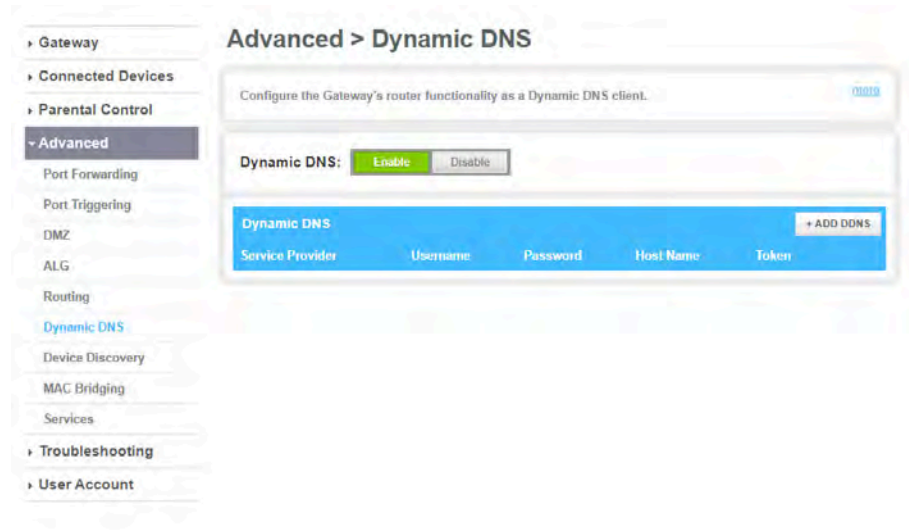


Figure 57: Dynamic DNS client screen

3. Click the **Enable** button to configure your Gateway's router functionality as DNS client.
4. Click **+ADD DDNS** to configure new DDNS.
5. Click **SAVE** to save the changes.



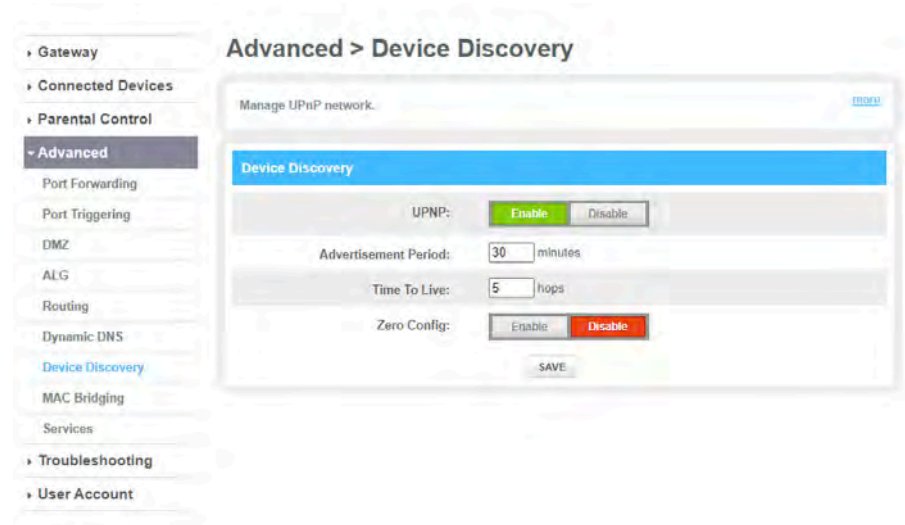
Note: To disable configuring the DNS client, click the **Disable** button and then click **SAVE**.

Manage UPnP network

The UPnP enabled gateway discovers all UPnP devices such as printers and computers. Using UPnP, the ports are automatically open for appropriate services and applications.

1. From any G34/G36 Web Manager screen, click the **Advanced** menu link.
2. Click **Device Discovery** to manage UPnP screen.

Figure 58: Advanced Device Discovery screen



3. Click the **Enable** button for the managing UPnP.
4. Enter the time in the **Advertisement Period** field to allow your gateway to advertise the UPnP information.
5. Enter the number of steps each UPnP advertisement is allowed to propagate before disappearing in the **Time To Live** field.
6. Click the **Enable** button to allow devices such as printers and computers to connect to a network automatically.
7. Click **SAVE**.

Set up MAC bridging

Using MAC bridging mechanism, you can allow devices on your LAN network to directly connect to the WAN network. The bridged device will get the IP address from your Internet provider and does not have access to your local network.

To set up the MAC bridging:

1. From any G34/G36 Web Manager screen, click the **Advanced** menu link.
2. Click **MAC Bridging** to display the MAC Bridging screen.

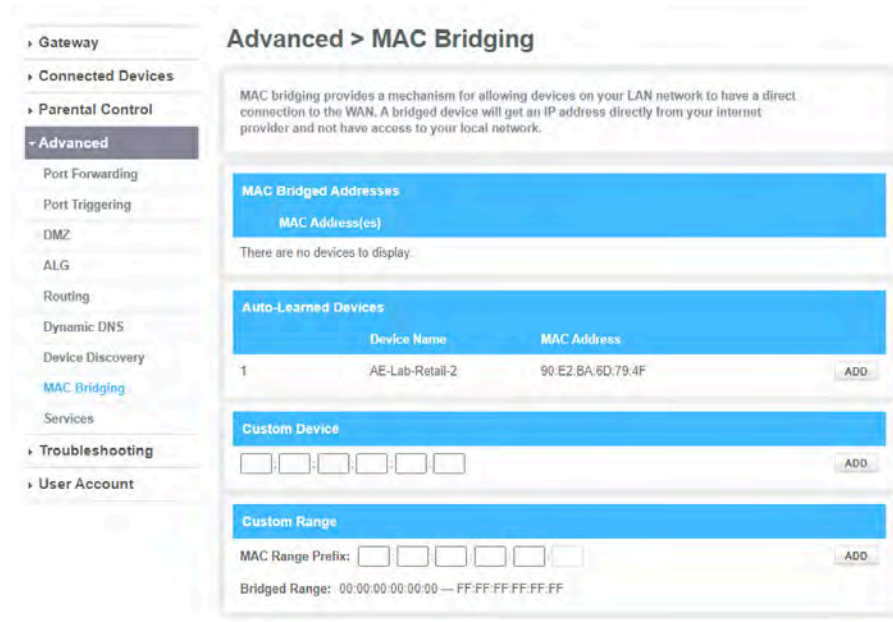


Figure 59: MAC Bridging screen

3. Enter the MAC addresses of the device or the MAC range that you want to allow to connect to the WAN.

Managing your Wi-Fi cable modem and connected networks

You can also use the G34/G36 Web Manager to view and monitor the network configuration settings and operational status of your G34/G36.

View the G34/G36 system hardware information

The Gateway Hardware screen displays system hardware information for your G34/G36. This information may be helpful if you contact ARRIS, Comcast, or Cox for technical assistance.

To open the G34/G36 Hardware screen:

1. From any G34/G36 Web Manager screen, click the **Gateway** menu link.
2. Click **Hardware** from the Gateway submenu links and then click **System Hardware** from the Hardware submenu options to display the Gateway System Hardware screen.

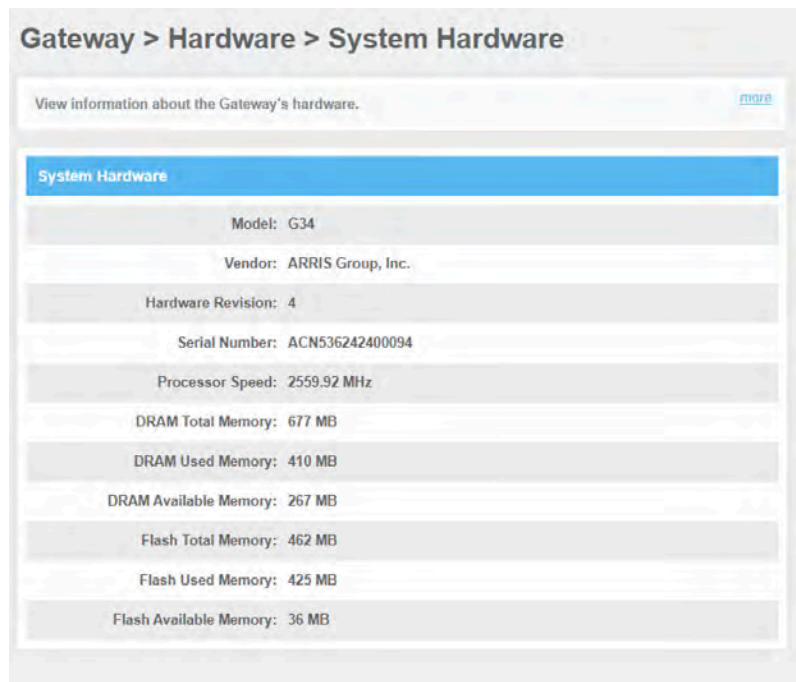


Figure 60: G34/G36 System Hardware screen

View the G34/G36 software version

The Gateway Software Version screen displays device software related information for your G34/G36. This information may be helpful if you have to contact ARRIS or Comcast for technical support.

To open the G34/G36 Software screen:

1. From any G34/G36 Web Manager screen, click the **Gateway** menu link.
2. Click **Software** from the Gateway submenu links to display the Gateway Software screen.

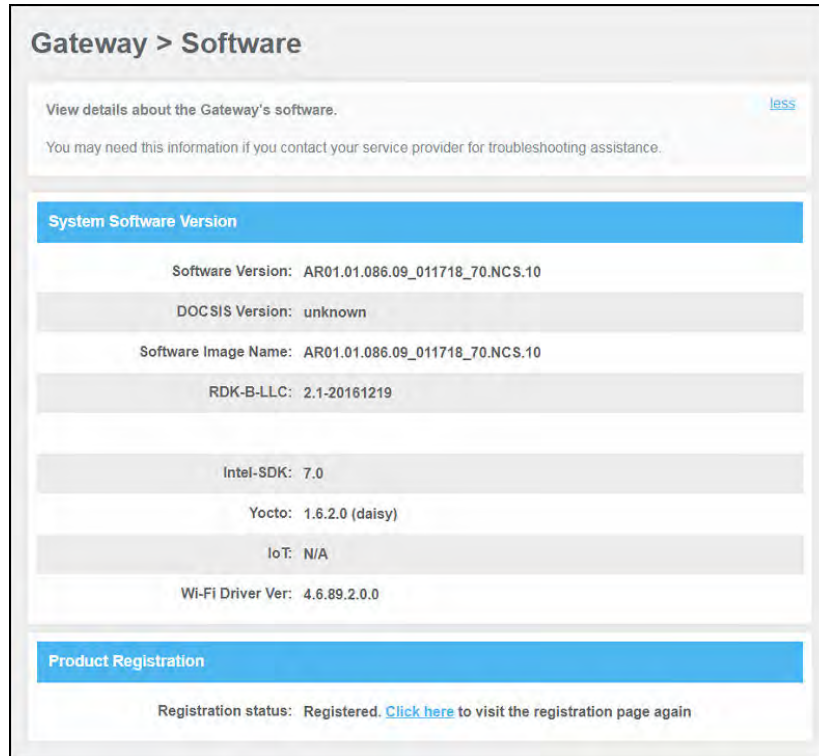


Figure 61: G34/G36 hardware information screen

Set up an Ethernet port connection for your data input

If you have installed your G34/G36 using an Ethernet port for your data input, perform the following to activate the Ethernet port.

To open the Gateway hardware Ethernet screen:

1. From any G34/G36 Web manager screen, click the **Connection** menu link to display the **Status** and **WAN** submenu links.
2. Click the **WAN** submenu link to open the Gateway Connection WAN screen.

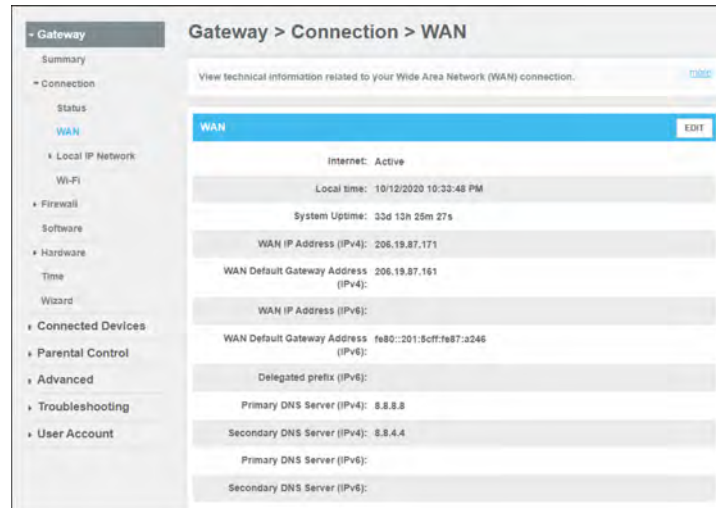


Figure 62: G34/G36 Connection WAN screen

3. Click **EDIT** on the WAN screen.
4. Click **Interface CHANGE** to select either **DOCSIS** (for a regular cable connection) or **Ethernet** (for an input signal from a different modem device) with an Ethernet connection from the modem device to the G34/G36 Ethernet port 4.

From any G34/G36 Web manager screen, click the **Gateway** menu link.

1. Click **Software** from the Gateway submenu links to display the Gateway Software screen.
2. Click **Ethernet** from the Hardware submenu links.

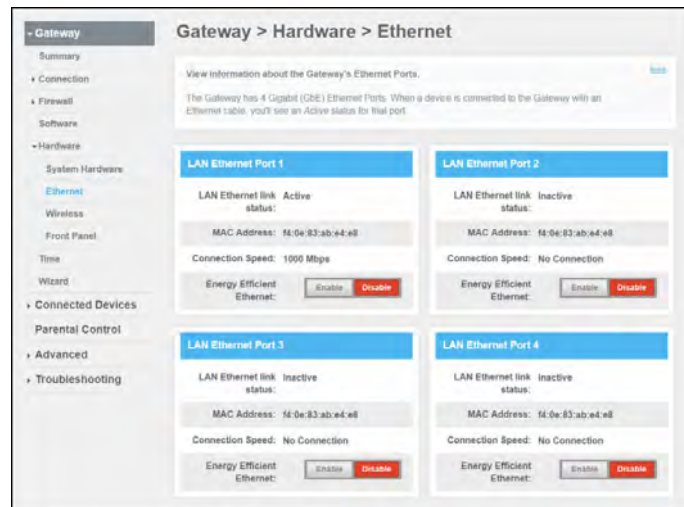


Figure 63: G34/G36 Gateway Hardware Ethernet screen

3. Click the **Enable** button in the **LAN Ethernet Port 4** box.

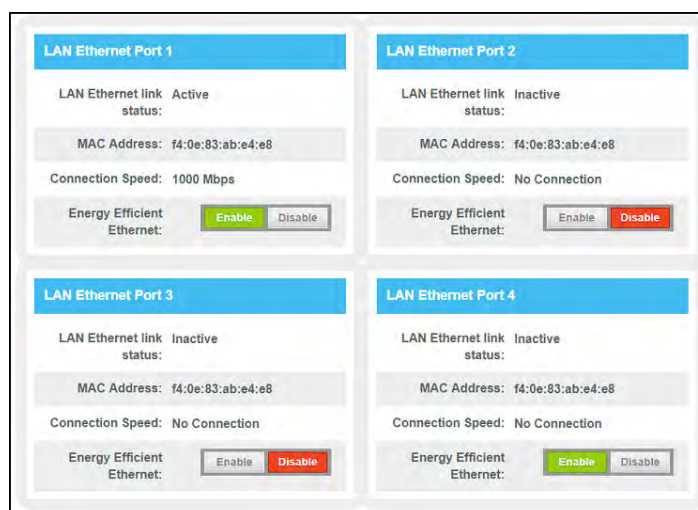


Figure 64: G34/G36 LAN Ethernet Port screen

Reboot the G34/G36

Choose one of the following options to reboot (or restart) your G34/G36:

- [Reboot the G34/G36 using the Reset button](#) (page 64)

OR

- [Reboot the G34/G36 using the Web Manager](#) (page 65)

Reboot the G34/G36 using the Reset button

To reboot (or restart) your G34/G36 using the **Reset** button:

1. Insert the end of a paper clip (or other small object with a narrow tip) into the indented **Reset** button opening on the rear of your G34/G36.



Figure 65: G34/G36 Reset button

2. Press and hold the small object in place for three to four seconds.



Warning: Do not press the **Reset** button for more than five seconds. If you do, your G34/G36 will automatically reset and your custom gateway configuration settings (e.g., admin password, network name (SSID) and password) will be deleted and replaced with the factory default configuration.

3. Remove the paper clip or small object from the **Reset** opening.

Reboot the G34/G36 using the Web Manager

To reboot (or restart) your G34/G36 using the G34/G36 Web Manager:

1. From any G34/G36 Web Manager screen, click the **Troubleshooting** menu link.
2. Click **Restart/Restore Gateway** from the Troubleshooting submenu links.

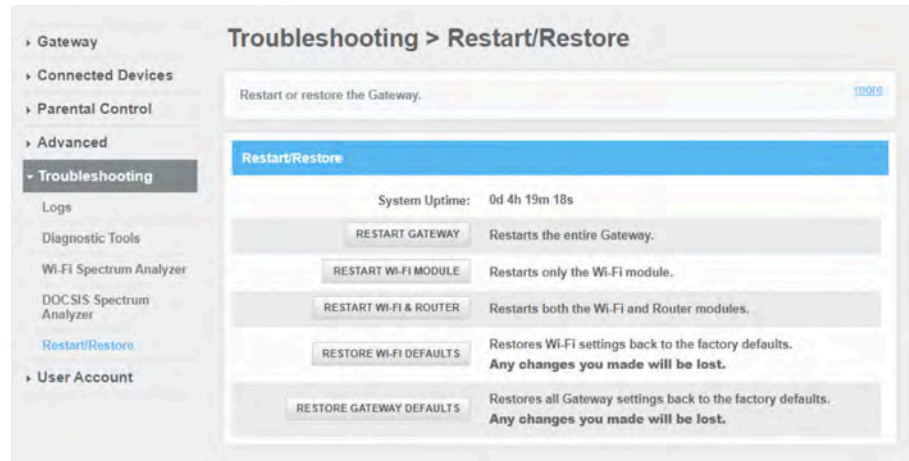


Figure 65: G34/G36 Restart/Restore settings screen

3. Click **RESTART GATEWAY** located in the Reset / Restore Gateway table.

The following message will display:

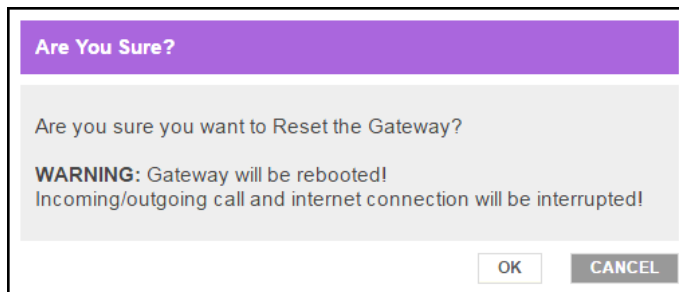


Figure 66: Restart the Gateway message box

4. Click **OK** to reboot the G34/G36 and then log back in.

Restore the G34/G36 default configuration settings



Warning: This action will delete your current G34/G36 configuration settings and allow you to restore the default (original) G34/G36 configuration.



Note: After the configuration settings are restored, the G34/G36 will automatically reboot, and you will have to log in using the default username (**admin**) and your current admin password.

To open the Reset/Restore Gateway screen:

1. From any G34/G36 Web Manager screen, click the **Troubleshooting** menu link.
2. Click **Reset / Restore Gateway** from the Troubleshooting submenu links to display the Troubleshooting **Reset / Restore Gateway** screen.

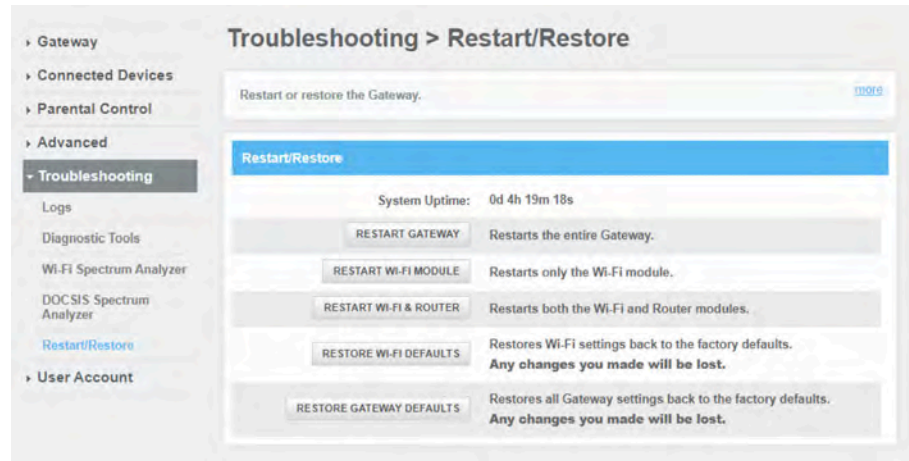


Figure 67: G34/G36 restore settings screen

3. Click **RESTORE WI-FI DEFAULTS** to reset your G34/G36 Wi-Fi settings.

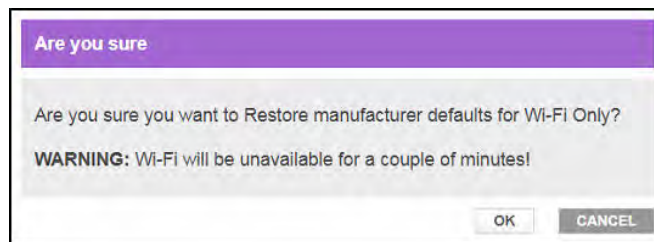


Figure 68: G34/G36 restore settings screen

4. Click **OK** to restore the Wi-Fi factory defaults.

The Operation in Progress for restarting the Wi-Fi radios message displays.

Exit the G34/G36 Web Manager

To log out and close the G34/G36 Web Manager:

- Click the **Logout** link located in the upper right corner of the G34/G36 Web Manager screen.



Figure 69: G34/G36 Web Manager logout link

Troubleshooting tips

If the solutions listed in the Troubleshooting Solutions table below do not solve your problem, please contact your service provider for assistance.

You may have to reset the G34/G36 Wi-Fi cable modem configuration to its original factory settings if the G34/G36 is not functioning properly. See [Restore the G34/G36 default configuration settings](#) (page 56) for more information.

Solutions

problem	Possible solution
Cannot Send or Receive Data	<p>Check each end of the coaxial cable connection on the and cable wall outlet.</p> <p>Use your hand to tighten each connector, if necessary.</p> <p>Check the Ethernet cable (if connected) to make sure it is properly connected to your and computer.</p> <p>If you have cable television service, check your television to ensure your cable service is operating properly.</p> <p>If none of the above solutions resolves the problem, contact your service provider or call ARRIS Technical Support at 1-877-466-8646 for assistance.</p>
Cannot Access the Internet	<p>Check that all cable and power connections on your and computer are properly connected.</p> <p>Check that the front panel LED is lit up solid.</p> <p>Contact your service provider for assistance.</p>
Wi-Fi Devices Cannot Send or Receive Data	<p>If the problem continues after checking the coaxial cable and Ethernet connections and your IP address, check the Wi-Fi Security Mode setting on the Gateway Wi-Fi Connection screen.</p> <p>If you enabled Wi-Fi security and configured a passphrase on your G34/G36, be sure each affected Wi-Fi client has the identical passphrase. If this does not solve the problem, check if the Wi-Fi client supports the selected Wi-Fi security method.</p>

Warranty Information

CommScope, Inc. ("ARRIS")

Retail Purchasers

If you purchased this Product directly from ARRIS or from an authorized ARRIS retail reseller, ARRIS warrants to you, the original end user customer, that (A) the Product, excluding Software, will be free from defects in materials and workmanship under normal use, and (B) with respect to Software, (i) the media on which the Software is provided will be free from defects in material and workmanship under normal use, and (ii) the Software will perform substantially as described in its documentation. This Limited Warranty to you, the original end user customer, continues (A) for Software and the media upon which it is provided, for a period of ninety (90) days from the date of purchase from ARRIS or an authorized ARRIS reseller, and (B) for the Product (excluding Software), for a period of two (2) years from the date of purchase from ARRIS or from an authorized ARRIS reseller. To take advantage of this Limited Warranty or to obtain technical support, you must call the ARRIS toll-free phone number: **1-877-466-8646**. ARRIS' sole and exclusive obligation under this Limited Warranty for retail sales shall be to repair or replace any Product or Software that does not meet this Limited Warranty. All warranty claims must be made within the applicable Warranty Period.

Cable Operator or Service Provider Arrangements

If you did not purchase this Product directly from ARRIS or from a ARRIS authorized retail reseller, ARRIS does not warrant this Product to you, the end-user. A limited warranty for this Product (including Software) may have been provided to your cable operator or Internet Service Provider ("Service Provider") from whom you obtained the Product. Please contact your Service Provider if you experience problems with this Product.

General Information

The warranties described in this Section shall not apply: (i) to any Product subjected to accident, misuse, neglect, alteration, Acts of God, improper handling, improper transport, improper storage, improper use or application, improper installation, improper testing, or unauthorized repair; or (ii) to cosmetic problems or defects which result from normal wear and tear under ordinary use, and do not affect the performance or use of the Product. ARRIS' warranties apply only to a Product that is manufactured by ARRIS and identified by ARRIS owned trademark, trade name or product identification logos affixed to the Product. ARRIS does not warrant to you, the end user, or to anyone else that the Software will perform error free or without bugs.

ARRIS IS NOT RESPONSIBLE FOR, AND PROVIDES "AS IS" ANY SOFTWARE SUPPLIED BY 3RD PARTIES. EXCEPT AS EXPRESSLY STATED IN THIS SECTION ("WARRANTY INFORMATION"), THERE ARE NO WARRANTIES OF ANY KIND RELATING TO THE PRODUCT, EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR THE WARRANTY AGAINST

INFRINGEMENT PROVIDED IN THE UNIFORM COMMERCIAL CODE. Some states do not allow for the exclusion of implied warranties, so the above exclusion may not apply to you.

What additional provisions should I be aware of? Because it is impossible for ARRIS to know the purposes for which you acquired this Product or the uses to which you will put this Product, you assume full responsibility for the selection of the Product for its installation and use. While every reasonable effort has been made to ensure that you will receive a Product that you can use and enjoy, ARRIS does not warrant that the functions of the Product will meet your requirements or that the operation of the Product will be uninterrupted or error-free.

ARRIS IS NOT RESPONSIBLE FOR PROBLEMS OR DAMAGE CAUSED BY THE INTERACTION OF THE PRODUCT WITH ANY OTHER SOFTWARE OR HARDWARE. ALL WARRANTIES ARE VOID IF THE PRODUCT IS OPENED, ALTERED, AND/OR DAMAGED.

THESE ARE YOUR SOLE AND EXCLUSIVE REMEDIES for any and all claims that you may have arising out of or in connection with this Product, whether made or suffered by you or another person and whether based in contract or tort.

IN NO EVENT SHALL ARRIS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION OR ANY OTHER PECUNIARY LOSS), OR FROM ANY BREACH OF WARRANTY, EVEN IF ARRIS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL ARRIS' LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

These matters are governed by the laws of the Commonwealth of Pennsylvania, without regard to conflict of laws principles and excluding the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

Retail Purchasers Only

If you purchased this Product directly from ARRIS or from an ARRIS authorized retail reseller, please call the ARRIS toll-free phone number, **1-877-466-8646**, for warranty service or technical support.

Cable Operator or Service Provider Arrangements

If you did not purchase this Product directly from ARRIS or from an ARRIS authorized retail reseller, please contact your Service Provider for technical support.

Corporate Headquarters
CommScope • Hickory • North Carolina • 28602 • USA
T: 1-828-324-2200
www.commscope.com