



SURFboard™ SBG6782-AC Wireless Gateway with MoCA®

User Guide

© 2015 ARRIS Enterprises, Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from ARRIS Enterprises, Inc. ("ARRIS"). ARRIS reserves the right to revise this publication and to make changes in content from time to time without obligation on the part of ARRIS to provide notification of such revision or change.

ARRIS and the ARRIS logo are all trademarks or registered trademarks of ARRIS Enterprises, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and the names of their products. ARRIS disclaims proprietary interest in the marks and names of others.

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.

ARRIS 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.

Table of Contents

1. Safety and Regulatory Information.....	5
2. Getting Started	10
Introduction.....	10
In The Box.....	10
Additional Items Needed (Not Included).....	11
System Requirements.....	11
Contact Information	12
3. Product Overview	13
Front Panel	13
Wi-Fi Protected Setup™ (WPS)	14
Rear Panel.....	15
Gateway Label	16
4. Installing the Gateway	17
Connect the SBG6782-AC to Your Computer	17
Establish an Internet Connection	18
Connect Your MoCA Devices.....	19
5. Setting Up a Wireless Network Connection	20
Launch the SBG6782-AC Quick Start Wizard.....	20
Set Up a Wireless Network Using Your Computer	27
Quick Connect Using the Windows Taskbar	27
Connect Using the Windows Control Panel.....	30
Test Your Wireless Network Connection.....	32
Connect Your WPS-Enabled Wireless Devices	33
6. Using the Gateway Web Manager	34
Start the Gateway Web Manager.....	34
Gateway Web Manager Menu Options.....	35
Get Help.....	37
Overview Help	37
Help Links.....	38
Field Level Help.....	38
Exit the SBG6782-AC Web Manager.....	39

7. Configuring Your Wireless Network	40
Set Up Your Wireless Primary Network.....	40
Set Up WPS on Your Wireless Network.....	42
Set Up a Wireless Guest Network	43
Change Your Wireless Network Name (SSID).....	46
Change the Wireless Channel.....	47
8. Configuring Your MoCA Network	49
Set Up Your MoCA Network	49
9. Protecting & Monitoring Your Wireless Network	51
Prevent Unauthorized Access.....	51
Change the Default Username and Password.....	51
Set Up Firewall Protection.....	54
Set Up Parental Controls	56
Set Up IP Filtering	58
Set Up MAC Filtering	59
Set Up Port Filtering	60
Set Up Port Triggers.....	61
Set Up Port Forwarding	62
Set Up the DMZ Host.....	65
Set Up Firewall Event Log Notifications	65
Store Remote Firewall Logs.....	66
10. Managing Your Gateway and Connected Networks	68
View the Gateway Status Using the Device Status Button	68
View the Gateway Product Information	69
View the Gateway Network Connection Status.....	70
Back Up Your Gateway Configuration	71
Restore Your Gateway Configuration Settings.....	71
Reset Your Gateway Settings	72
11. Troubleshooting Tips	73
Solutions	73
Front Panel LED Icons and Error Conditions.....	74
12. Warranty Information	76

Safety and Regulatory Information

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 of the instructions listed here and/or in the user manual before you operate this device. Give particular 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 electrical 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 particular 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 electrical 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.
- It is recommended that the customer install an electrical surge protector in the electrical outlet to which this device is connected. 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.
- Do not use this product near water: for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement, or near a swimming pool.
- 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.
- 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 THE ABOVE INSTRUCTIONS

Note to CATV System Installer — This reminder is provided to call the CATV system installer's attention to Article 820.93 and 820.100 of the National Electric Code, which provides guidelines for proper grounding and, in particular, specifies that the Coaxial cable shield shall 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:

- Reorient or relocate the receiving antenna.
- 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.

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

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.

INDUSTRY CANADA (IC) STATEMENT

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- This device may not cause interference, and
- This device must accept any interference, including interference that may cause undesired operation of the device.

CAN ICES-3 (B)/NMB-3 (B)

In Canada, RLAN devices are restricted from using the 5600-5650 MHz frequency band.

CAUTION: To reduce the potential for harmful interference to co-channel mobile satellite systems, use of the 5150-5250 MHz frequency band is restricted to indoor use only.

High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz frequency bands. These radars could cause interference and/or damage to License Exempt–Local Area Network (LE-LAN) devices.

IC Radiation Exposure Statement

IMPORTANT NOTE: *This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator and your body.*

AVIS D'INDUSTRIE CANADA (IC)

Cet appareil est conforme à la réglementation RSS-210 d'Industrie Canada. Son utilisation est assujettie aux deux conditions suivantes :

- Cet appareil ne doit pas causer d'interférences et
- Cet appareil doit accepter toute interférence reçue, y compris les interférences causant un fonctionnement non désiré.

CAN ICES-3 (B)/NMB-3 (B)

Au Canada, les appareils de réseau local sans fil ne sont pas autorisés à utiliser les bandes de fréquence 5600-5650 MHz.

AVERTISSEMENT: afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux, les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur

Les radars à haute puissance sont définis en tant qu'utilisateurs principaux (c.-à-d. prioritaires) des bandes de fréquences 5250-5350 MHz et 5650-5850 MHz. Ces radars peuvent causer de l'interférence ou des dommages susceptibles de nuire aux appareils exempts de licence–réseau local (LAN-EL).

Déclaration de IC sur L'Exposition aux Rayonnements

NOTE IMPORTANTE: *cet équipement est conforme aux limites d'exposition aux rayonnements établies par IC pour un environnement non contrôlé. Cet équipement doit être installé et utilisé de manière à maintenir une distance d'au moins 20 cm entre la source de rayonnement et votre corps.*

Wireless LAN Information

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.*

SECURITY 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, see [Change the Default Username and Password](#) in this guide for instructions or visit the ARRIS Support website at www.arris.com/consumers.

CARING FOR THE ENVIRONMENT BY RECYCLING



When you see this symbol on an ARRIS product, do not dispose of the product with residential or commercial waste.

Recycling your ARRIS Equipment

Please do not dispose of this product with your residential or commercial waste. Some countries or regions, such as the European Union, have set up systems to collect and recycle electrical and electronic waste items. Contact your local authorities for information about practices established for your region. If collection systems are not available, call ARRIS Customer Service at **1-877-466-8646** for assistance.

Getting Started

Introduction

Welcome to the next generation of ultra high-speed Wi-Fi gateways. The ARRIS SURFboard® SBG6782-AC Wireless Cable Modem Gateway with MoCA® (Multimedia over Coax) provides wireless high-speed data and multimedia service access on your home or small business network. With built-in MoCA technology, the SBG6782-AC also provides high-speed Internet access to multiple MoCA devices using the existing coaxial cable connection in your home. The SBG6782-AC includes a Wi-Fi Pairing option for quick and easy connections for your WPS-enabled wireless devices.

This guide provides instructions for installing and configuring your SBG6782-AC, setting up a secure wireless network connection, and managing your gateway and network configurations.

In The Box

Before installing the SBG6782-AC, check that the following items are also included in the box. If any items are missing, please call ARRIS Technical Support at **1-877-466-8646** for assistance.

Table 1. SBG6782-AC Package Contents

Item		Description
SBG6782-AC Wireless Gateway		DOCSIS 3.0 high-speed cable wireless modem and router with MoCA
Power Cord		Power cord for an electrical wall outlet connection
Ethernet Cable		Standard Category 5 (CAT5) or higher network cable

Item		Description
Software License & Regulatory Card		Safety and regulatory information, software license, and warranty for the gateway
Support Information Card		Provides contact information for obtaining technical support assistance with any issues you may have with your SURFboard device.
SBG6782-AC Quick Start Guide		Provides basic information for installing the gateway and setting up a secure wireless connection on your home network.

Additional Items Needed (Not Included)

The following items are not included in the 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 7 Service Pack 1 (SP1)
 - Windows Vista™ SP2 or later
 - Windows XP SP3



Note: Microsoft no longer supports Windows XP. The SBG6782-AC should still function without any problems.

- 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/consumer
- Call ARRIS Technical Support: **1-877-466-8646**

Product Overview

Front Panel

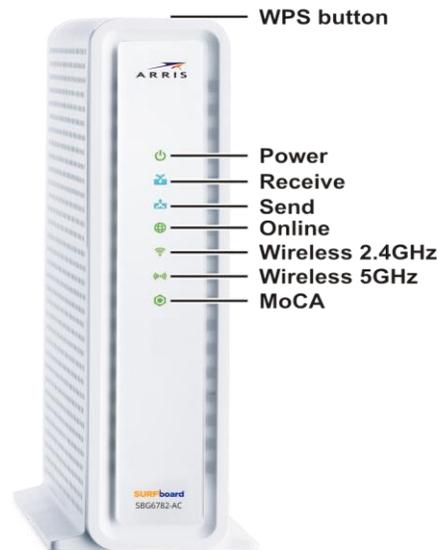


Figure 1: SBG6782-AC Front View

Table 2. SBG6782-AC Front Panel LED Icons

LED Icon	Blinking	On (Solid)
 WPS Button	Not applicable – no LED on button. Note: The Wireless LEDs will blink Amber to indicate the WPS Pairing process is in progress.	Not applicable – no LED on button.
 POWER	Not applicable – icon does not blink.	Green: Power is properly connected.
 RECEIVE	Scanning for a downstream (receive) channel connection.	Green: Non-bonded downstream channel is connected. Blue*: High-speed Internet connection with bonded downstream channels.

LED Icon	Blinking	On (Solid)
	Scanning for an upstream (send) channel connection.	Green: Non-bonded upstream channel is connected. Blue*: High-speed Internet connection with bonded upstream channels.
	Scanning for an Internet connection.	Green: Start-up process completed.
	Green: Wi-Fi enabled with encrypted/unencrypted wireless data activity. Amber: Flashes during the wireless pairing process and lights up SOLID green after five seconds or less.	Green: 2.4 GHz wireless connection is made between the SBG6782-AC and another Wi-Fi enabled device on your home network; for example, Wi-Fi telephone, tablet, or laptop.
	Green: Wi-Fi enabled with encrypted wireless data activity. Amber: Flashes during the wireless pairing process and lights up SOLID green after five seconds or less.	Green: 5 GHz wireless connection is made between the SBG6782-AC and another Wi-Fi enabled device on your home network; such as a printer, tablet, or laptop.
	Green: Indicates MoCA activity in progress	Green: A MoCA device is connected and running.

***Blue** - Indicates DOCSIS 3.0 operation (high-speed Internet access) which may not be available in all locations. Check with your service provider for availability in your area.

Wi-Fi Protected Setup™ (WPS)

Wi-Fi Protected Setup (WPS) is a wireless network setup option that provides a quick and easy solution for setting up a secure wireless network connection for any WPS-enabled wireless device; such as a computer, tablet, gaming device, or printer. WPS automatically configures your wireless network connections and sets up wireless security. See [Connect Your WPS-Enabled Wireless Devices](#) for more information.

Rear Panel

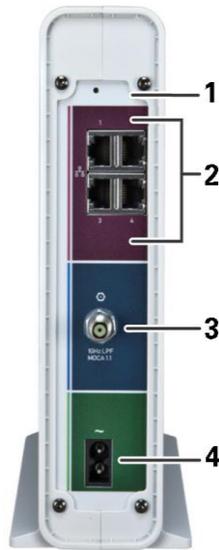
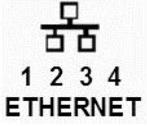


Figure 2: SBG6782-AC Rear View

Table 3. SBG6782-AC Rear Panel Ports & Connectors

Port Name	Description
1 Reset Button	<p>Recessed button used to either reboot the wireless gateway or reset the gateway configuration settings.</p> <p>To reboot (or restart) the gateway, use the end of a paper clip or other small object with a narrow tip to press and hold the indented Reset button for three to four seconds only, and then release. Do not press the Reset button for more than seven seconds. If you do, the gateway configuration settings will automatically reset to the factory default settings and your custom gateway settings will be deleted (see warning below).</p> <p>To reset your gateway configuration back to the factory default settings, use the end of a paper clip or other small object with a narrow tip to press and hold the indented Reset button for 10 seconds or until the front panel LEDs flash, and then release. See Restore Your Configuration Settings for more information on an alternative method to reset the gateway settings using the Web Manager.</p> <p> WARNING! Resetting the gateway configuration settings to the factory defaults will also delete your custom gateway configuration, including your user password, wireless network name (SSID), and other configuration settings. You should first back up your gateway configuration files before resetting your gateway. See Back Up Your Gateway Configuration for more information.</p>

Port Name	Description
2  1 2 3 4 ETHERNET	Four one-gigabit Ethernet ports for RJ-45 cable connections Green LED is ON - Indicates a data transfer rate of one gigabit per second Amber LED is ON - Indicates a data transfer rate of less than one gigabit per second
3  CABLE	Coaxial Cable connector
4  POWER	100 – 240 VAC Power connector

Gateway Label

The gateway label is located on the bottom of the SBG6782-AC. It contains specific gateway ID information that you may need when contacting your service provider or ARRIS Technical Support.

To receive Internet service, you will have to contact your service provider for assistance. You may need to provide the following information listed on the gateway label:

- Gateway model name (**SBG6782-AC**)
- Gateway MAC address (**HFC MAC ID**)
- Gateway serial number (**S/N**)

Installing the Gateway



Caution: 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.

Connect the SBG6782-AC to Your Computer

Before installing the SBG6782-AC:

- Check with your service provider to ensure broadband cable service is available in your area.

To set up a wireless network, you will need a high-speed Internet connection provided by an Internet service provider.



Note: When contacting your service provider, you may need your gateway information listed on the gateway label located on the bottom of your SBG6782-AC (see [Gateway Label](#) ("Gateway Label" page 16)).

- Choose a location in your home where your computer and gateway are preferably near existing cable and electrical wall outlets.

For the best Wi-Fi coverage, a central location in your home or building is recommended.



Note: The following installation procedure covers the wired Ethernet connection process so that you can confirm that the SBG6782-AC was properly installed and can connect to the Internet.

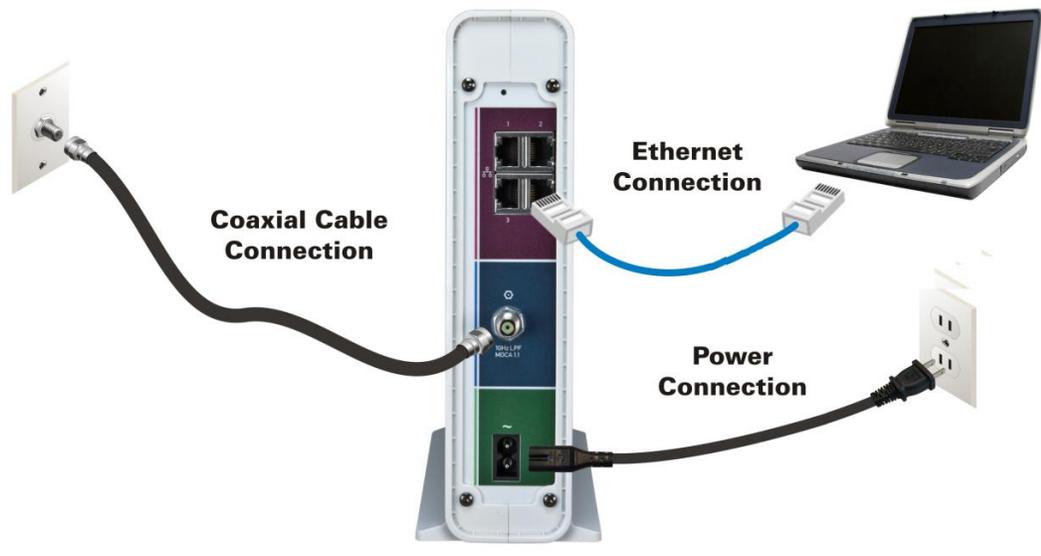


Figure 3: SBG6782-AC Connection Diagram

1. Check that a coaxial cable is already connected to a cable wall outlet or RF splitter (optional).
2. Connect the other end of the coaxial cable to the **Cable** connector on the rear of the SBG6782-AC.
Use your hand to tighten the connectors to avoid damaging them.
3. Connect the Ethernet cable to an available **Ethernet** port on the rear of the SBG6782-AC.
4. Connect the other end of the Ethernet cable to the **Ethernet** port on your computer.
Optional: Repeat steps 3 and 4 for an additional computer or other network device that you want to install as a wired connection on your home network.
5. Connect the power cord to the **Power** port on the rear of the SBG6782-AC.
6. 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 the SBG6782-AC.

Establish an Internet Connection

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

1. Power ON the computer connected to the SBG6782-AC, if it is turned off, and then log in.
2. Contact your service provider to activate (provision) the SBG6782-AC. You may have to provide the HFC MAC ID listed on the gateway label.



Note: Your service provider may allow for automatic activation which will automatically launch its own special website when you open a web browser.

3. After the SBG6782-AC is activated, open a web browser (such as Internet Explorer, Google Chrome, Firefox, or Safari) on your computer.
4. Type a valid URL (such as www.surfboard.com) in the address bar and then press **Enter**. The ARRIS website should open. If it fails to open, please contact your service provider for assistance.
5. Check that the **Power, Receive, Send, and Online** front panel LEDs on the SBG6782-AC light up in sequential order. See [Product Overview](#) for additional LED status information.
 - If all four LEDs did not light up solid and you also do not have an Internet connection, you may have to contact your service provider to reactivate the SBG6782-AC or check for signal issues.
 - If you still cannot connect to the Internet, the SBG6782-AC may be defective. Please call ARRIS Technical Support at **1-877-466-8646** for assistance.

Connect Your MoCA Devices

You can also connect any MoCA devices, such as a Smart TV, to the SBG6782-AC. You will need an RF cable splitter (not included) and an additional coaxial cable (not included) to connect the MoCA device and SBG6782-AC. Follow the instructions included with the MoCA device to complete the applicable connections.



Note: The MoCA LED on the SBG6782-AC front panel will light up **SOLID green** when the gateway detects other MoCA devices on your home network.

Setting Up a Wireless Network Connection

It is highly recommended that you first verify that your computer can connect to the Internet using an Ethernet connection before configuring your wireless home network.

You must already have access to an Internet service in your home before setting up a wireless network connection. Also, make sure your computer and the SBG6782-AC are connected through an Ethernet connection.

Choose **one** of the following options to set up your wireless network connection:

- [Launch the SBG6782-AC Quick Start Wizard](#) (page 20)
- [Set Up a Wireless Network Using Your Computer](#) (page 27)

After setting up a wireless connection on your home network, check that your wireless network connection was set up properly. See [Test Your Wireless Network Connection](#) for more information.

Launch the SBG6782-AC Quick Start Wizard

The SBG6782-AC Quick Start Wizard is a seven-step application to help you quickly customize the default wireless network settings on your SBG6782-AC. The wizard configures your SBG6782-AC wireless network name (SSID), Wi-Fi Security Key (network password), and Wi-Fi Security mode.

IMPORTANT NOTE: *The quick start wizard uses the default settings already configured for your SBG6782-AC to help you quickly set up your wireless home network. However, the wizard will only let you change the wireless network name (SSID) and Wi-Fi Security Key (network password). After completing the wizard and getting your SBG6782-AC connected to the Internet, you will be able to make additional network configuration changes to further customize your wireless home network and connect your wireless devices. See [Configuring Your Wireless Network](#) for more information.*

1. Open a web browser (such as Internet Explorer, Google Chrome, Firefox, or Safari) on the computer connected to the SBG6782-AC.
2. Type the default LAN IP address, **192.168.0.1**, in the Address bar and then press **Enter**.
The SBG6782-AC Login screen displays.

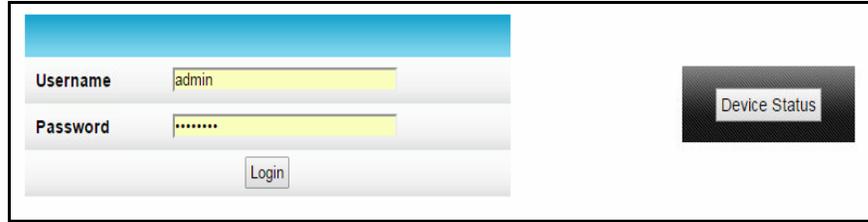


Figure 4: Gateway Login Screen with Device Status Button



Note: The Device Status button provides a quick method for you to view the current configuration settings and connection status of your SBG6782-AC without having to log in to the SBG6782-AC Web Manager (see [View the Gateway Status Using the Device Status Button](#) for more information).

3. Type the default username and password. Both entries are case-sensitive.
 - Username: **admin**
 - Password: **motorola**
4. Click **Login** to open the SBG6782-AC Web Manager. The Launch Quick Start Wizard screen displays.



Note: If the default username and password are not working, your service provider may have to set up alternate login credentials. Please contact your service provider or ARRIS Technical Support for assistance.

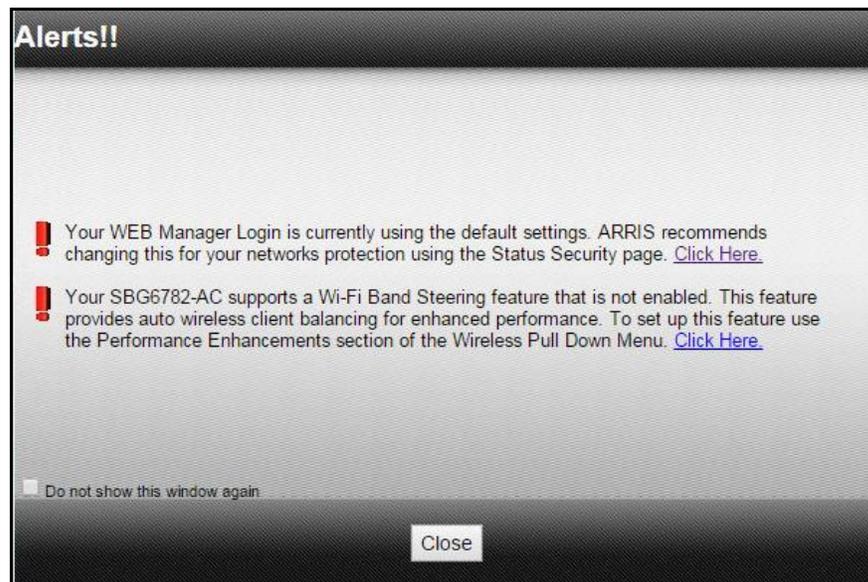


Figure 5: Login Alerts Screen

The Login Alerts screen displays when you log in using the default username and password. It is highly recommended that you change the username and password for network security purposes. There are two options available:

- Quick Start Wizard (continue with step 5 below)
- SBG6782-AC Web Manager (see [Change the Default Username and Password](#) for more information)

For now, continue with the following steps to set up your wireless network connection.

5. Click **Close** to close the Login Alerts screen. The Launch Quick Start Wizard screen displays.

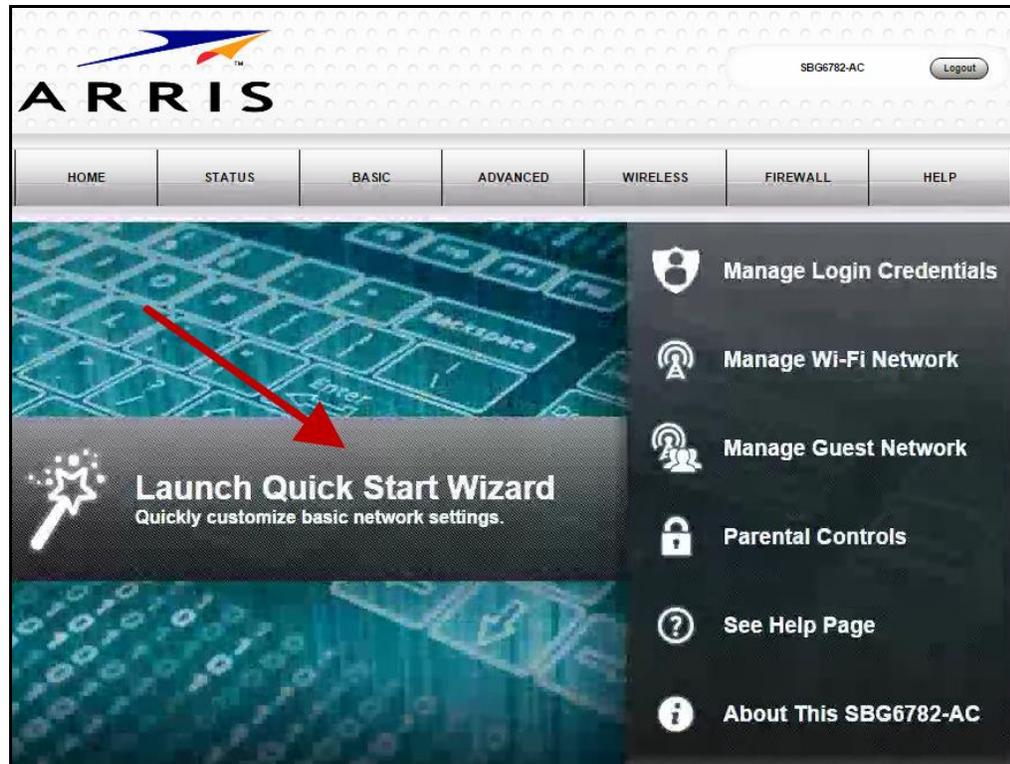


Figure 6: SBG6782-AC Quick Start Wizard Opening Screen

6. Click **Launch Quick Start Wizard** to start the wizard. The Welcome screen displays (see Figure 7).

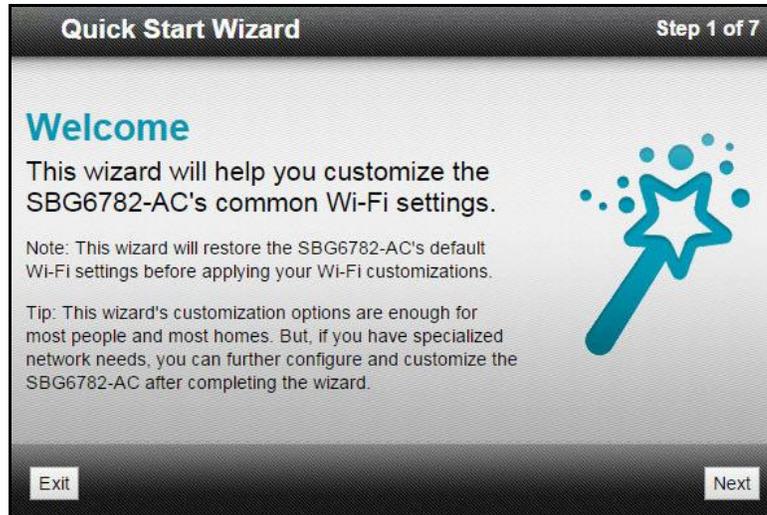


Figure 7: SBG6782-AC Quick Start Wizard Welcome Screen

7. Click **Next** to open the Wi-Fi Network Name & Passphrase screen.

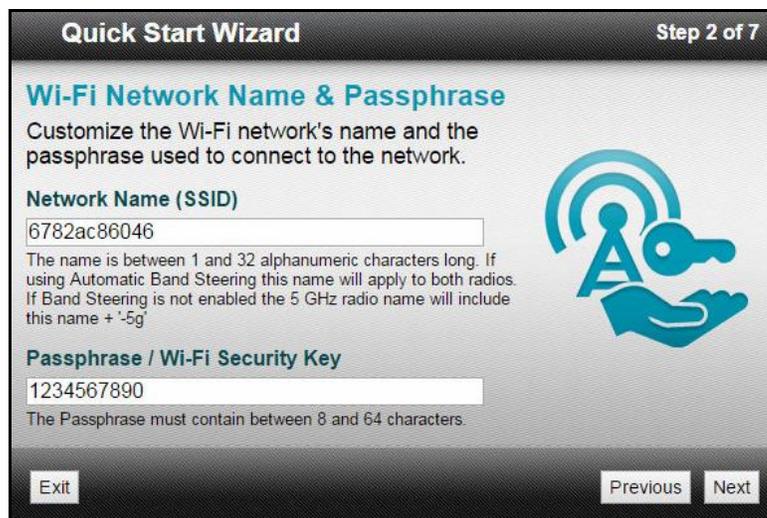


Figure 8: SBG6782-AC Quick Start Wizard-Step 2 of 7 Screen

8. Do **one** of the following to set up your wireless network name in the **Network Name (SSID)** field for connecting to your wireless home network:
 - Keep the default network name or SSID (also listed on the SBG6782-AC gateway label).
 -  **Note:** You must keep the default network name as listed if this is your first time setting up your wireless network. You cannot change the network name until after you have completed the installation wizard.
 - Enter a different name for your wireless network. Your new network name must contain from one to 32 alphanumeric characters.



Note: You have the option to change your wireless network name (SSID) only after you have finished setting up your wireless home network for the first time. The SBG6782-AC Web Manager is also available to change your SSID (see [Change Your Wireless Network Name \(SSID\)](#) for more information).

9. Do **one** of the following to change your wireless network password in the **Passphrase / Wi-Fi Security Key** field:
 - Keep the default passphrase or Wi-Fi Security key (also listed on the SBG6782-AC gateway label).
 - Enter a different password for your wireless network.

The passphrase or Wi-Fi Security key is the sign-on access code for your wireless network. The access code must contain from eight to 64 characters consisting of any combination of letters, numbers, and symbols. Your network password should be as unique as possible to protect your wireless network and also deter hackers or unauthorized access to your wireless home network.



Note: It is highly recommended that you change the default Wi-Fi Security Key to a more secure wireless password to protect your wireless home network from unauthorized access. See [Prevent Unauthorized Access](#) for more information.

10. Click **Next** to open the 2.4 GHz & 5 GHz Networks screen.



Figure 9: SBG6782-AC Quick Start Wizard-Step 3 of 7 Screen

This screen shows the two Wi-Fi frequency bands available on the SBG6782-AC, 2.4 GHz and 5 GHz. The wizard configures the default 2.4 GHz default frequency band. See [Change the Wireless Channel](#) to change the Wi-Fi frequency.



Note: The 2.4 GHz frequency range is recommended for backward compatibility purposes because older wireless devices cannot connect to 5 GHz frequencies.

11. Click **Next** to open the Wi-Fi Security Configuration screen.



Figure 10: SBG6782-AC Quick Start Wizard-Step 4 of 7 Screen

The wizard configures **WPA2-PSK** as the default wireless network security code. It is the highest wireless network security level. See [Set Up Your Wireless Primary Network](#) to change the wireless network security code for your wireless home network.

12. Click **Next** to open the User Security Configuration screen.



Figure 11: SBG6782-AC Quick Start Wizard-Step 5 of 7 Screen

This screen allows you to change the current (or default) login username and user password to log on to the SBG6782-AC Web Manager.



Note: To change your username and password, you must first select the **Change Username** and **Change Password** checkboxes to activate the fields. If a checkbox is not selected, the field is disabled. The **Next** button is also disabled, if the username or password was not entered correctly. Make sure to repeat the same username and password in their respective fields.

To change your username and password:

- Select Change Username checkbox and then enter your new username in both Username fields.
- Select Change Password checkbox and then enter your new user password in both Password fields.

13. Click **Next** to open the Review Settings screen and confirm your wireless network settings.



Figure 12: SBG6782-AC Quick Start Wizard-Step 6 of 7 Screen

14. Click **Apply** to accept your wireless network settings and open the Settings Applied screen or click **Previous** to go back and change your wireless network name and/or user password.

If you clicked **Apply**, wait for your wireless network settings to be saved. When it is complete, the Settings Applied screen will open.



Figure 13: SBG6782-AC Quick Start Wizard-Step 6 of 7 Screen

15. Click **Exit** to close the SBG6782-AC Quick Start Wizard.



Note: You can click **Print** to print a copy of your wireless network settings from a connected (wired or wireless) printer. This can be helpful for keeping a record of your new wireless network settings.

Set Up a Wireless Network Using Your Computer

Use one of the following options to create your wireless network:

- [Quick Connect Using the Windows Taskbar](#)
- [Connect Using the Windows Control Panel](#)



Note: The steps for setting up a wireless network may differ slightly depending on the Windows operating system running on your computer. The steps used in this section apply to Windows 7.

Quick Connect Using the Windows Taskbar

1. From the Windows taskbar on your computer (see Figure 14), click the **Wireless Link** icon to open the list of available wireless networks (see Figure 15).



Figure 14: Windows Taskbar



Note: If the **Wireless Link** icon is not visible, left-click on the **Show hidden icons** button (see Figure 14) on the Windows taskbar to open and select from the list of additional icons.

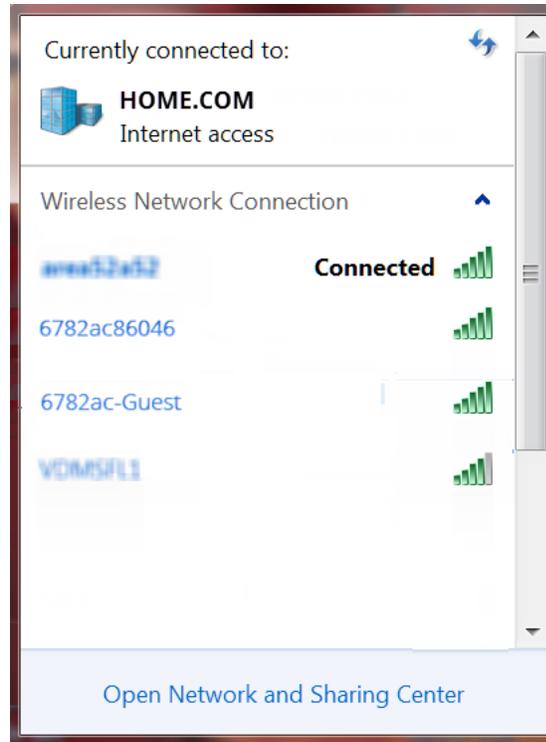


Figure 15: Sample Available Wireless Networks Window

2. Click on the SBG6782-AC wireless network name or SSID (for example, **6782ac#####**) for your SBG6782-AC from the list of available wireless networks.



Note: Check the gateway label on the bottom of your SBG6782-AC to locate the default SSID. You must use the default SSID listed on the gateway label when installing the gateway and setting up your first wireless network connection. You can change the SSID after your network connections are up and running. See [Change Your Wireless Network Name \(SSID\)](#) for more information.

3. Select **Connect automatically** to set up your wireless devices to automatically log on to your home network without having to enter the password.



Figure 16: Sample Wireless Network Connect Window

4. Click **Connect** to open the Connect to a Network window and set up your new network password.



Figure 17: Network Connection Window

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



Note: You can use the **Wi-Fi Security Key** code listed on the gateway label or enter your own personal wireless network password. See [Prevent Unauthorized Access](#) for more information on creating user passwords.

6. Select **Hide characters** and then click **OK** to encrypt (or hide) your network password.



Figure 18: Network Connection-Create Network Password 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.

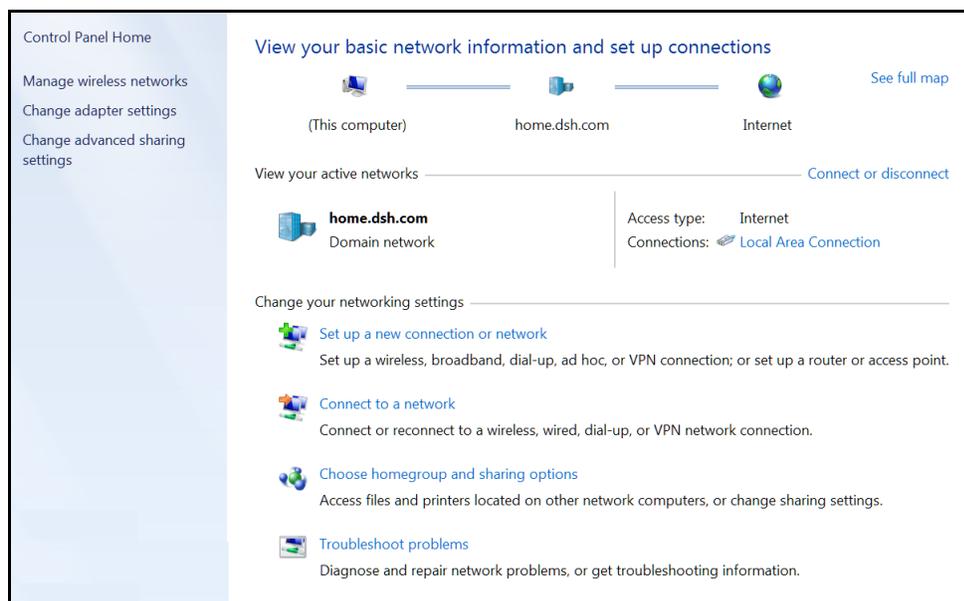


Figure 19: Control Panel-Network and Sharing Center Window

3. Click **Manage wireless networks** in the Control Panel Home side panel to open the **Manage Wireless Networks** window.

- Click Add to open the Manually Connect to a Wireless Network window.

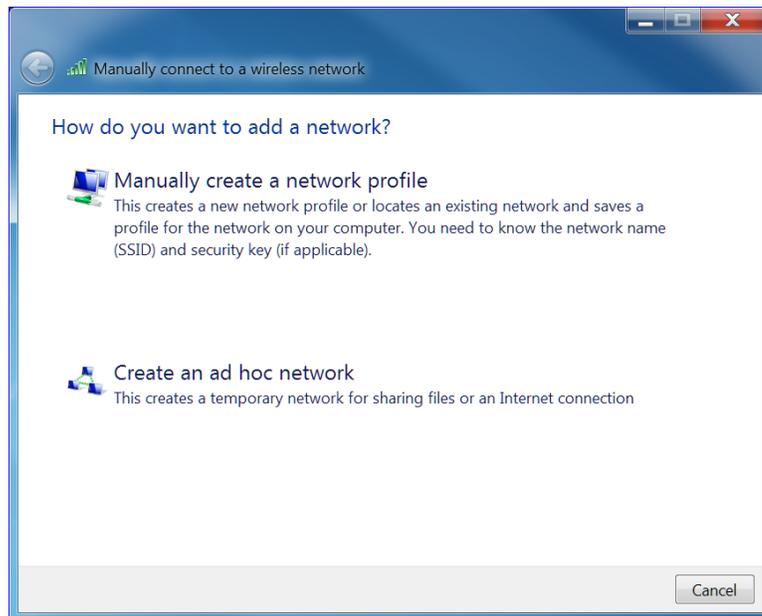


Figure 20: Manually Connect to a Wireless Network Window

- Click **Manually create a network profile** to open another **Manually Connect to a Wireless Network**.



Figure 21: Manually Connect to a Wireless Network Window

- Enter the wireless network name or SSID (**6782ac#####**) for your SBG6782-AC in the **Network name** field.

The SSID is listed on the gateway label on the bottom of your SBG6782-AC.



Note: You have the option to customize your wireless network name or SSID after completing your initial wireless network connection. However, you must use the default SSID listed on the gateway label for the initial gateway installation. See [Change Your Wireless Network Name \(SSID\)](#) for more information.

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



Note: WPA2-Personal is the recommended wireless security level for your wireless home network. It is the default security level for the SBG6782-AC and also the highest security level available.

8. Select the password encryption type from the **Encryption type** drop-down list. This is used for securing your wireless network.
 - TKIP – Temporal Key Integrity Protocol
 - AES – Advanced Encryption Standard (recommended). AES is the default encryption type for the SBG6782-AC.

9. Enter a **Security code** or passphrase for your wireless network password in the **Security Key** field.

You can use the **WI-FI SECURITY KEY** listed on the SBG6782-AC gateway label or create your own personal password.



Note: Remember to use a unique combination of letters, numbers, and characters to create a more secure password. See [Prevent Unauthorized Access](#) for more information.

10. Select **Hide characters** to prevent your Security Key or password from displaying in the field.
11. Select **Start this connection automatically** so that your wireless devices will automatically connect to your wireless network upon login.
12. Click **Next** to complete the wireless network setup.

The **Successfully added <Network name>** message for your new wireless network should appear.

13. Click **Close** to exit.

Test Your Wireless Network Connection

Perform the following connectivity test to check that wireless connections were established for the SBG6782-AC and other wireless devices on your home network:

1. Check if your wireless devices successfully connected to your wireless network, then disconnect the Ethernet cable on your computer and SBG6782-AC.
2. Open a web browser on your computer.
3. Type a valid URL (such as www.surfboard.com) in the address bar, and press **Enter**.

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

Connect Your WPS-Enabled Wireless Devices

You can use the Wi-Fi Protected Setup (WPS) Pairing button on the SBG6782-AC to connect your WPS-enabled wireless devices. WPS automatically assigns a random wireless network name (SSID) and Wi-Fi Security Key (password) to the SBG6782-AC and your other WPS-enabled wireless devices to connect to your wireless network.



Note: To use the WPS Pairing button option, your computer hardware must support WPS and also have WPA security compatibility.

1. Power ON your SBG6782-AC and other WPS-enabled wireless devices that you want to connect to your wireless network.
2. Press and hold the WPS button located on the top of the SBG6782-AC for five to 10 seconds and then release (see [Product Overview](#)) for the Wireless Cable Modem Gateway front view).
3. If applicable, press the WPS button on your WPS-enabled computer or other WPS-enabled wireless device.
4. Repeat step 3 for each additional WPS-enabled wireless device that you want to connect onto your home network.

Using the Gateway Web Manager

Use the SBG6782-AC Web Manager to view and monitor the configuration settings and operational status of your Wireless Cable Modem Gateway. You can also configure your network connections and wireless security settings. See [Protecting & Monitoring Your Wireless Network](#) for more information.



Note: *If you did not purchase your gateway from a retail store, you may notice a few blocked configuration settings in the SBG6782-AC Web Manager that cannot be modified. This may be due to some restrictions set up by your service provider to prevent unauthorized changes to certain configuration parameters.*

Start the Gateway Web Manager



Note: *You must use the default user name and password (listed below) to log in to the SBG6782-AC Web Manager for the first time. For network security purposes, we highly recommend that you change the default user name and password after logging onto the SBG6782-AC for the first time. See [Change the Default Username and Password](#) for more information.*

1. Open any web browser on the computer connected to the SBG6782-AC.
2. Type the default LAN IP address, **192.168.0.1**, in the Address bar and then press **Enter**. The SBG6782-AC Login screen displays.
3. Type the default user name and password. Both entries are case-sensitive.
Username: **admin**
Password: **motorola**
4. Click **Login** to open the SBG6782-AC Web Manager. The SBG6782-AC Web Manager Main Screen displays.



Note: *If the default user name and password are not working, your service provider may have to set up alternate login credentials. Please contact your service provider or ARRIS Technical Support for assistance.*

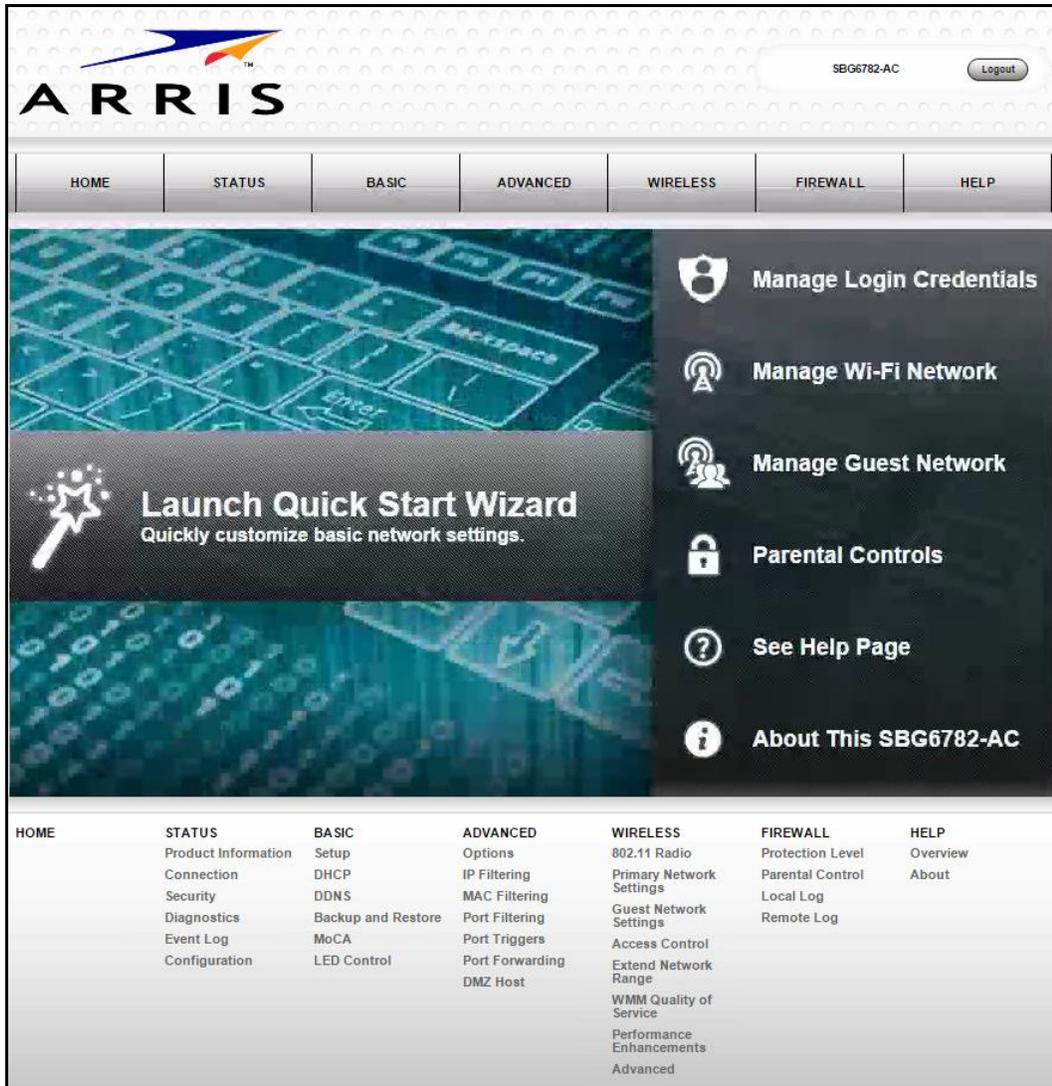


Figure 22: SBG6782-AC Web Manager Main Screen

Gateway Web Manager Menu Options

Main Menu Buttons

The SBG6782-AC main menu buttons are displayed along the top of the SBG6782-AC Web Manager screen. To display the drop-down submenu options, click the menu button.

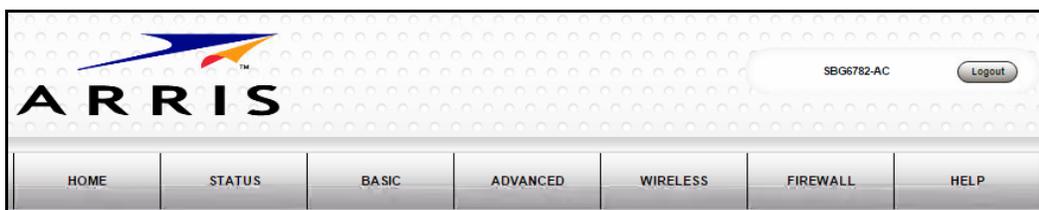


Figure 23: SBG6782-AC Web Manager Main Menu Buttons

Main Menu Links

The SBG6782-AC main menu and related submenu option links are also displayed along the bottom of the SBG6782-AC Web Manager screen. To open a submenu option, click the link.

HOME	STATUS Product Information Connection Security Diagnostics Event Log Configuration	BASIC Setup DHCP DDNS Backup and Restore MoCA LED Control	ADVANCED Options IP Filtering MAC Filtering Port Filtering Port Triggers Port Forwarding DMZ Host	WIRELESS 802.11 Radio Primary Network Settings Guest Network Settings Access Control Extend Network Range WMM Quality of Service Performance Enhancements Advanced	FIREWALL Protection Level Parental Control Local Log Remote Log	HELP Overview About
------	--	---	--	--	---	---------------------------

Figure 24: SBG6782-AC Web Manager Main Menu Links

Table 4. SBG6782-AC Web Manager Main Menu Options

Menu Option	Function
Home	Displays the Quick Start Wizard main screen.
Status	Provides information about the gateway hardware and software, MAC address, gateway IP address, serial number, and related information. Additional screens provide diagnostic tools and also allow you to change your gateway user name and password.
Basic	Configures the gateway IP-related configuration data, including Network Configuration, WAN Connection Type, DHCP, and DDNS.
Advanced	Controls Internet protocols which configure and monitor how the gateway routes IP traffic on the SBG6782-AC.
Wireless	Configures and monitors the gateway wireless networking features.
Firewall	Configures and monitors the gateway firewall.
Help	Provides general information to help you set up your home network.
Logout	Closes the SBG6782-AC Web Manager.

Get Help

You can choose any of the following three options to obtain help information for any SBG6782-AC Web Manager function. General help information is available for any SBG6782-AC menu option when you click the **Help** button on that page.

- [Overview Help](#)
- [Help Links](#)
- [Field Level Help](#)

Overview Help

General help information is available when you click **Help, Overview** on the SBG6782-AC Main Menu.

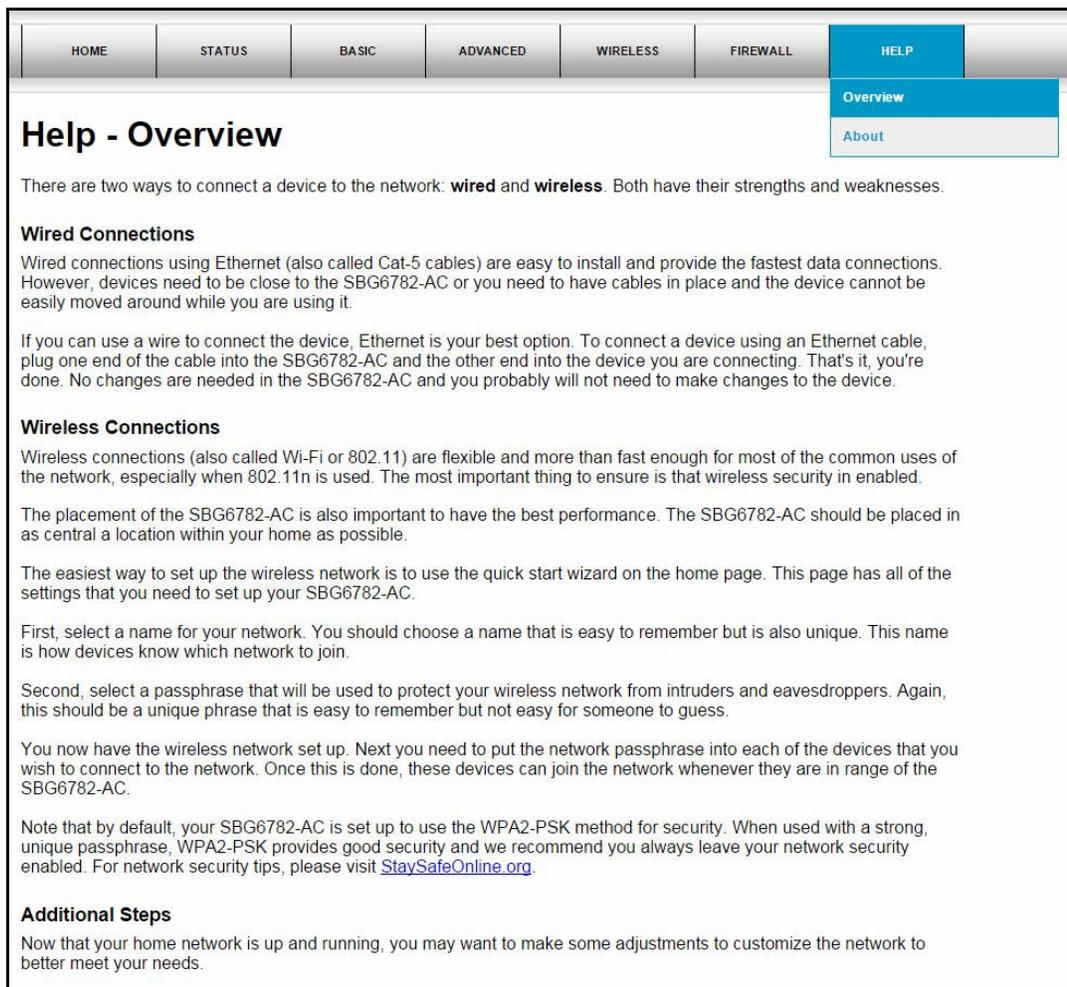


Figure 25: SBG6782-AC Help Overview Screen

Help Links

Provides a concise list of your gateway configuration settings with applicable links for easy access when you click **Help**, **About** on the SBG6782-AC Main Menu. The link opens the related configuration screen.

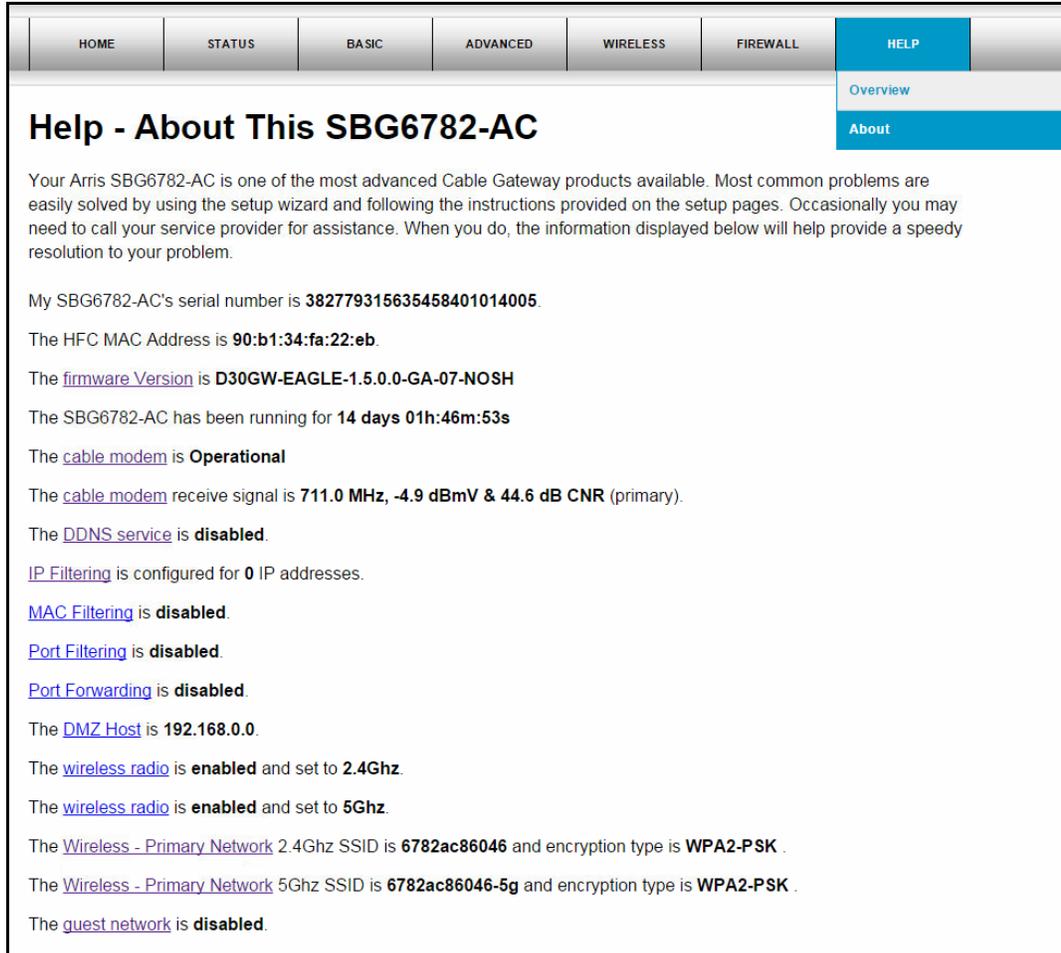


Figure 26: SBG6782-AC Help About Screen

Field Level Help

More specific help information is available throughout the web manager for field level help when you click Help located to the right of the applicable field (see sample screenshot below).



Figure 27: SBG6782-AC Field Level Help

Exit the SBG6782-AC Web Manager

To log out and close the SBG6782-AC Web Manager:

- Click **Logout** located in the upper right corner of the screen above the SBG6782-AC Main Menu buttons.

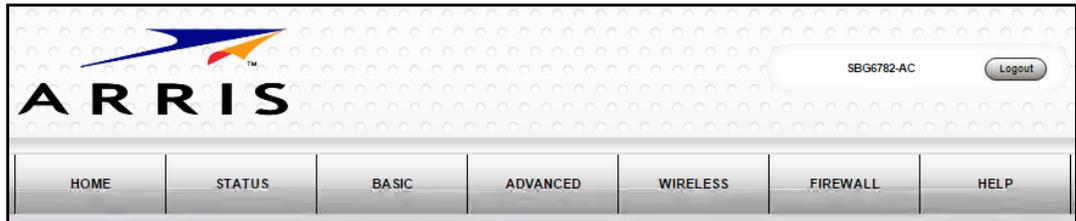


Figure 28: SBG6782-AC Web Manager Logout Button

Configuring Your Wireless Network

The SBG6782-AC supports a secure method for setting up multiple wireless access points on your home network. This enables you to designate a separate guest access point on your wireless network for visitors, friends, or other family members without giving them access to your content or other network devices on your primary network.

Set Up Your Wireless Primary Network

1. From the SBG6782-AC Web Manager, click **Wireless** on the SBG6782-AC Main Menu bar.
2. Click **Primary Network Settings** from the Wireless submenu options.

2.4 GHz		5 GHz
2.4 GHz Wi-Fi Network F8:0B:BE:9A:8F:02		
Wireless Network	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	▶ Help
Network Name (SSID)	<input type="text" value="6782ac86046"/>	▶ Help
Network Name (SSID) Broadcast	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	▶ Help
Wireless Security	<input type="text" value="WPA2-PSK"/>	▶ Help
WPA2-PSK Security Settings		
Encryption	<input checked="" type="radio"/> AES <input type="radio"/> AES+TKIP	▶ Help
Passphrase	<input type="text" value="0ddft64bx"/>	▶ Help
Wi-Fi Protected Setup (WPS) Automatic Security Configuration		
WPS	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	▶ Help
WPS Add Client (Push Button Method)	Press the button on the SBG6782-AC to start WPS pairing.	▶ Help
WPS Add Client (Gateway PIN Method)	<input type="text" value="37206819"/> <input type="button" value="Generate PIN"/>	▶ Help
Configure by External Registrar	<input type="text" value="Allow"/>	▶ Help
WPS Add Client (Client PIN Method)	<input type="text"/> <input type="button" value="Add"/>	▶ Help
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

Figure 29: 2.4 GHz Wireless Primary Network Screen

The screenshot displays the configuration interface for a 5 GHz Wi-Fi network. At the top, there are tabs for '2.4 GHz' and '5 GHz', with '5 GHz' selected. Below the tabs, the title '5 GHz Wi-Fi Network' is shown along with the MAC address 'F8:0B:BE:9A:8F:03'. The main configuration area consists of several sections:

- Wireless Network:** A radio button is selected for 'Enabled', with 'Disabled' as an alternative. A 'Help' link is present.
- Network Name (SSID):** A text input field contains '6782ac86046-5g'. A 'Help' link is present.
- Network Name (SSID) Broadcast:** A radio button is selected for 'Enabled', with 'Disabled' as an alternative. A 'Help' link is present.
- Wireless Security:** A dropdown menu is set to 'WPA2-PSK'. A 'Help' link is present.
- WPA2-PSK Security Settings:**
 - Encryption:** A radio button is selected for 'AES', with 'AES+TKIP' as an alternative. A 'Help' link is present.
 - Passphrase:** A text input field contains '1234567890'. A 'Help' link is present.
- Wi-Fi Protected Setup (WPS) Automatic Security Configuration:**
 - WPS:** A radio button is selected for 'Enabled', with 'Disabled' as an alternative. A 'Help' link is present.
 - WPS Add Client (Push Button Method):** A text area contains the instruction 'Press the button on the SBG6782-AC to start WPS pairing.' A 'Help' link is present.
 - WPS Add Client (Gateway PIN Method):** A text input field contains '37206819', followed by a 'Generate PIN' button. A 'Help' link is present.
 - Configure by External Registrar:** A dropdown menu is set to 'Allow'. A 'Help' link is present.
 - WPS Add Client (Client PIN Method):** A text input field is empty, followed by an 'Add' button. A 'Help' link is present.

At the bottom of the screen, there are 'Apply' and 'Cancel' buttons.

Figure 30: 5 GHz Wireless Primary Network Screen

- Click the **2.4 GHz** or **5 GHz** tab at the top of the screen to select the wireless frequency range for your wireless network.
- Select **Enabled** or **Disabled** in the Wireless Network field to turn ON or OFF wireless networking on your wireless network.
- Do one of the following to set the network name for your wireless network in the Network Name (SSID) field:
 - Keep the default network name listed in the field (also listed on your gateway label).
 - Enter a new network name for your wireless primary network.
 - The wireless network name cannot be the same name as any other SSID on your home network. You can use any combination of letters (lowercase and uppercase), numbers, and/or special characters (symbols) up to a maximum of 32 characters.
- Select **Enabled** or **Disabled** in the Network Name (SSID) Broadcast field to turn ON or OFF displaying your SSID as an available wireless network to outside users.

When **SSID Broadcast** is enabled, your SSID is visible and also available to unauthorized wireless users that are within range of your home network to connect to it.
- Select one of the following wireless network security options for your wireless gateway from the Wireless Security drop-down list:
 - WPA2-PSK:** Wi-Fi Protected Access version 2 with Pre-Shared Key (recommended)
 - WPA2-PSK + WPA-PSK:** combination Wi-Fi Protected Access version 2 with Pre-Shared Key and Wi-Fi Protected Access with Pre-Shared Key
 - Unencrypted:** Network security is not set for your wireless network. This network security option allows access to your wireless network without a Wi-Fi Security Key (network password)

- WPA-PSK: Wi-Fi Protected Access with Pre-Shared Key; standard encryption
 - WPA2 (Enterprise): Wi-Fi Protected Access version 2 provides additional network security and requires a user name and password for network logon
 - WPA2 + WPA (Enterprise): combination Wi-Fi Protected Access version 2 and Wi-Fi Protected Access provides additional network security and requires a user name and password for logging onto your wireless network
8. Choose the wireless network encryption type for your wireless network in the Encryption field:
 - AES – Advanced Encryption Standard: Provides the strongest encryption (recommended)
 - AES+TKIP – Advanced Encryption Standard and Temporal Key Integrity Protocol
Allows both AES and TKIP-capable clients to connect to your wireless network
 9. Enter your wireless network password in the Passphrase field.
You can use any combination of letters, numbers, and/or special characters for your network password.
 10. Click **Apply** if you are done or continue with the WPS Automatic Security Configuration section (see below) to set up WPS on your home network so that you can connect your WPS-enabled wireless devices.

Set Up WPS on Your Wireless Network

1. From the Wireless Primary Network Settings screen, click the **2.4 GHz** or **5 GHz** tab at the top of the screen to select the wireless frequency range for your wireless network.
2. Scroll down to the **Wi-Fi Protected Setup (WPS) Automatic Security Configuration** section.

The screenshot shows the 'Wi-Fi Protected Setup (WPS) Automatic Security Configuration' screen. It includes the following elements:

- WPS:** A toggle switch set to 'Enabled' (radio button selected) with a 'Help' link.
- WPS Add Client (Push Button Method):** A text field containing '37206819' and a 'Generate PIN' button, with a 'Help' link.
- WPS Add Client (Gateway PIN Method):** A text field with an 'Add' button, with a 'Help' link.
- Configure by External Registrar:** A dropdown menu set to 'Allow', with a 'Help' link.
- WPS Add Client (Client PIN Method):** A text field with an 'Add' button, with a 'Help' link.
- At the bottom, there are 'Apply' and 'Cancel' buttons.

Figure 31: WPS Setup Screen

3. Select **Enabled** in the WPS field to turn ON the Wi-Fi Protected Setup (WPS) network security on your home network and then continue with step 4.
- or -
- Select **Disabled** in the WPS field to turn OFF the Wi-Fi Protected Setup (WPS) network security on your home network and then proceed to step 5 to finish.

4. Select one of the following WPS Pairing methods to connect or pair your WPS-enabled wireless devices to your wireless network:

- **Push Button** – Press the WPS button on the SBG6782-AC to start the WPS pairing process with the WPS-enabled wireless device you want to connect to your home network.

Repeat for each additional WPS-enabled wireless device.

- **Gateway PIN**
 - 1) Either enter the PIN number listed in the WPS Add Client field or click **Generate PIN** to create a new numeric PIN (password) for logging onto your home network.
 - 2) Select **Allow** or **Deny** (recommended) from the **Configure by External Registrar** drop-down list to set the Gateway PIN method for pairing your WPS-enabled wireless devices.

***Note:** The Gateway PIN method is not recommended. It should be disabled to protect your wireless network from possible outside attacks, e.g., viruses and hackers.*

- **Client PIN** – Enter your PIN number (numeric password) for your WPS-enabled wireless device in the WPS Add Client field and then click Add.
5. Click **Apply**, when done.

Set Up a Wireless Guest Network



***Note:** This feature may be disabled on your SBG6782-AC. Some service providers or cable operators do not allow for secondary (or guest) wireless networks on their gateway devices.*

1. From the SBG6782-AC Web Manager, click **Wireless** on the SBG6782-AC Main Menu bar.
2. Click **Guest Network Settings** from the Wireless submenu options (see Figure 32 or Figure 33).
3. Click the **2.4 GHz** or **5 GHz** tab at the top of the screen to select the wireless frequency range for your guest network.
4. Select the guest network from the Selected Guest Network drop-down list.
5. Select **Enabled** or **Disabled** in the Guest Network field to turn ON or OFF the selected wireless guest network.
6. Do one of the following to set the network name for your wireless guest network in the Guest Network Name (SSID) field:
 - Keep the default guest network name listed in the field (also listed on your gateway label).
 - Enter a new name for your guest network.

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

2.4 GHz		5 GHz	
2.4 GHz Wi-Fi Network Settings & Security			
Selected Guest Network	SBG6782AC_GUEST (FA:0B:BE:9A:8F:03)		▶ Help
Guest Network	Enabled		▶ Help
Guest Network Name (SSID)	SBG6782AC_GUEST		▶ Help
IP Network	Guest		▶ Help
IP Address	192.168.1.1		▶ Help
Lease Pool Starting IP Address	192.168.1.10		▶ Help
Lease Pool Ending IP Address	192.168.1.99		
Lease Time	86400		▶ Help
UPnP Enable	Enabled		
Firewall Enable	Enabled		
DHCPv6 Server	Enabled		
Wireless Security	WPA2-PSK		▶ Help
WPA2-PSK Security Settings			
Encryption	TKIP+AES		▶ Help
Passphrase	<input type="text"/>	Show Passphrase <input type="checkbox"/>	▶ Help
		Apply	Restore Guest Network Defaults

Figure 32: 2.4 GHz Wireless Guest Network Screen

2.4 GHz		5 GHz	
5 GHz Wi-Fi Network Settings & Security			
Selected Guest Network	SBG6782AC_GUEST (FA:0B:BE:9A:8E:04)		▶ Help
Guest Network	Enabled		▶ Help
Guest Network Name (SSID)	SBG6782AC_GUEST		▶ Help
IP Network	Guest		▶ Help
IP Address	192.168.21.1		▶ Help
Lease Pool Starting IP Address	192.168.21.10		▶ Help
Lease Pool Ending IP Address	192.168.21.99		
Lease Time	86400		▶ Help
UPnP Enable	Enabled		
Firewall Enable	Enabled		
DHCPv6 Server	Enabled		
Wireless Security	WPA2-PSK		▶ Help
WPA2-PSK Security Settings			
Encryption	TKIP+AES		▶ Help
Passphrase	<input type="text"/>	Show Passphrase <input type="checkbox"/>	▶ Help
		Apply	Restore Guest Network Defaults

Figure 33: 5 GHz Wireless Guest Network Screen

7. Select **LAN** or **Guest** from the IP Network drop-down list.
 - LAN – Configures the guest network to be part of your primary network and allow guest users to connect to your primary network
 - Guest – Configures the guest network to only allow access to a specific network and not your primary network
8. Enter the IP address for the SBG6782-AC on the Guest network in the IP Address field.
9. Enter the first IP address of the range of IP addresses for the guest network lease pool in the Lease Pool Starting IP Address field.

The SBG6782-AC assigns these IP addresses to the wireless devices on your guest network.
10. Enter the last IP address of the range of IP addresses for the guest network lease pool in the Lease Pool Ending IP Address field.
11. Enter the amount of time (in seconds) that an IP address will be available to a device on your guest network in the Lease Time field.
12. Select **Enabled** or **Disabled** in the UPnP (Universal Plug and Play) Enable field to allow or block any network devices, such as computers, smart phones, tablets, gaming devices, or printers to automatically connect to your wireless home network.
13. Select **Enabled** or **Disabled** in the Firewall Enable field to turn ON or OFF the gateway firewall.
14. Select **Enabled** or **Disabled** in the DHCPv6 Server field to allow the DHCPv6 server to send leases to the guest network clients from the guest network lease pool you specified earlier.

Note: If the DHCP server is disabled, you must assign static IP addresses to the guest network STAs.
15. Select one of the following wireless network security options for your guest network from the Wireless Security drop-down list:
 - **WPA2-PSK**: Wi-Fi Protected Access version 2 with Pre-Shared Key (recommended)
 - **WPA2-PSK + WPA-PSK**: combination Wi-Fi Protected Access version 2 with Pre-Shared Key and Wi-Fi Protected Access with Pre-Shared Key
 - **WPA-PSK**: Wi-Fi Protected Access with Pre-Shared Key, standard encryption
 - **Unencrypted**: Turns off network security
 - **WPA2 + WPA (Enterprise)**: combination Wi-Fi Protected Access version 2 and Wi-Fi Protected Access provides additional network security and requires a user name and password for network logon
 - **WPA2 (Enterprise)**: Wi-Fi Protected Access version 2 provides additional network security and requires a user name and password for network logon
16. Choose the wireless network encryption type in the Encryption field:
 - **AES** – Advanced Encryption Standard: Provides the strongest encryption (recommended)
 - **TKIP+AES** –Temporal Key Integrity Protocol and Advanced Encryption Standard: Allows both AES and TKIP-capable clients to connect to your wireless network
17. Enter any combination of characters and letters for the wireless guest network password in the Passphrase field.
18. Select **Show Passphrase** to display your password.

19. When done, deselect **Show Passphrase** so that your password will not be visible.
20. Click **Apply**, when done.

Change Your Wireless Network Name (SSID)

The SSID (Service Set Identification) is the wireless network name assigned to your SBG6782-AC wireless primary and guest networks. The default SSID which is listed on the gateway label is automatically populated in the network configuration screens. A list of SSIDs of available wireless networks in close proximity of your home (for example, neighbors or local businesses) will display when you or someone else in your home attempt to establish a wireless network connection. For security purposes and quick recognition of your wireless network, it is highly recommended that you change the default SSID. You should also consider changing the default wireless password or passphrase (see [Prevent Unauthorized Access](#) for more information).

Note: When you change the SSID, any wireless devices that are already connected to your wireless network will be disconnected from the network. The wireless devices will have to be reconnected to the wireless network using the new SSID.

Do the following to change your wireless network name or SSID:

1. From the SBG6782-AC Web Manager, click **Wireless** on the SBG6782-AC Main Menu bar.
2. Click **Primary Network Settings** from the Wireless submenu options to open the Wi-Fi Network screen.

2.4 GHz		5 GHz
2.4 GHz Wi-Fi Network B0:77:AC:87:15:E2		
Wireless Network	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	▶ Help
Network Name (SSID)	<input type="text"/>	▶ Help
Network Name (SSID) Broadcast	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	▶ Help
Wireless Security	WPA2-PSK	▶ Help
WPA-PSK+WPA2-PSK Security Settings		
Encryption	<input type="radio"/> AES <input checked="" type="radio"/> AES+TKIP	▶ Help
Passphrase	<input type="text"/>	▶ Help



Figure 34: Change Your Network Name (SSID) and Password Screens

3. Click the **2.4 GHz** or **5 GHz** tab at the top of the screen to select the wireless frequency range for your guest network.
4. Make sure **Enabled** is selected in the Wireless Network field. This turns ON wireless networking on your home network.
5. Delete the current network name in the Network Name (SSID) field and then enter a new name for your wireless network.
You can use any combination of up to 32 alphanumeric characters for the network name.
6. Select **Enabled** or **Disabled** in the Network Name (SSID) Broadcast field to turn ON or OFF displaying your SSID as an available wireless network to outside users.
7. Delete the current wireless network password (passphrase) in the Passphrase field and then enter a new network password. See [Prevent Unauthorized Access](#) for more information.
8. Click **Apply** at the bottom of the screen.

The new wireless network name should appear in the list of available wireless networks when you reconnect your wireless devices.

Change the Wireless Channel

Network interference may occur at any time when using a wireless network connection. This may be caused by other wireless access points that are using the same wireless channel as your SBG6782-AC and are also operating within close proximity in your home. When experiencing wireless network interference, changing the wireless channel on the SBG6782-AC can improve network connectivity (or signal strength) and avoid network interference. By default, the Wi-Fi Channel on your SBG6782-AC is set on **Auto** for 2.4 GHz and **149** for 5 GHz.

Do the following to change the wireless channel on the SBG6782-AC:

1. From the SBG6782-AC Web Manager, click **Wireless** on the SBG6782-AC Main Menu bar.
2. Click **802.11 Radio** from the Wireless submenu options to open the Wireless 802.11 Radio screen.

- Click the **2.4 GHz** or **5 GHz** tab at the top of the screen to select the wireless frequency range for your wireless home network.

2.4 GHz 5 GHz

2.4 GHz Wi-Fi Network

Wireless Radio Enable ▾

Output Power ▾ ▶ Help

802.11 Mode ▾ ▶ Help

Bandwidth ▾ Current Bandwidth: 20MHz ▶ Help

Channel ▾ Current Channel: 1 ***Interference Level: Acceptable

2.4 GHz **5 GHz**

5 GHz Wi-Fi Network

Wireless Radio Enable ▾

Output Power ▾ ▶ Help

802.11 Mode ▾ ▶ Help

Bandwidth ▾ Current Bandwidth: 20MHz ▶ Help

Channel ▾ Current Channel: 149 ***Interference Level: Acceptable

Figure 35: 2.4 GHz & 5 GHz Wireless 802.11 Radio Screens

- Select **Enabled** from the Wireless Radio Enable drop-down list to turn ON the Wi-Fi Radio on the SBG6782-AC.
- Select a channel number from the **Channel** drop-down list that is different from the channel number listed as the Current Channel.

Note: It is recommended that you 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 wireless network performance. Channels 1, 6, and 11 are used for better network performance and stability because they do not overlap.

- Click **Apply**, when done.

Configuring Your MoCA Network

With the SBG6782-AC MoCA interface, you can create a reliable home network using your existing coaxial wiring. MoCA provides Internet Protocol (IP) connectivity with your set-top boxes, Smart TVs, and any other Ethernet-enabled electronic devices in your home. You can also use MoCA adapters to further extend your MoCA home network to connect additional Smart TVs, computers, gaming consoles, and other network devices.

You can enable or disable the SBG6782-AC MoCA interface. If the SBG6782-AC is not set up as the MoCA Network Controller, it will not have any control over the other devices on the MoCA network. If you disable the SBG6782-AC as the MoCA Network Controller, then you are allowing another device to become the MoCA Network Controller.

Set Up Your MoCA Network

1. From the SBG6782-AC Web Manager, click **Basic** on the SBG6782-AC Main Menu bar.
2. Click **MoCA** from the Basic submenu options to open the MoCA Configuration and Status screen.

Configuration								
MoCA	<input type="checkbox"/> Enabled							▶ Help
Operational Frequency	SCAN							▶ Help
Available D-Band Channels - (D-Band: 1150-1500 MHz)								
1150MHz (D1)	1200MHz (D2)	1250 MHz (D3)	1300MHz (D4)	1350MHz (D5)	1400MHz (D6)	1450MHz (D7)	1500MHz (D8)	Select All
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Max Beacon Power Level	10 (Max)							▶ Help
Transmit Power Level	10 (Max)							▶ Help
Privacy	<input checked="" type="checkbox"/> Enabled 458401014005							▶ Help
Apply								
Status								
Link State	Down							▶ Help

Figure 36: MoCA Configuration and Status Screen

3. Select **Enabled** in the MoCA field to set the SBG6782-AC as the MoCA Network Controller.

4. Select the operational frequency range for the MoCA data transmission rate from the Operational Frequency drop-down list.
 - Normal range is between 1150 MHz to 1500 MHz
 - Most cable TV systems use 1150 MHz
5. Select the maximum number of beacon signals for data transmission from the Max Beacon Power Level drop-down list.
Default level is **10**.
6. Select the transmit Power level from the Transmit Power Level drop-down list.
Default level is **10**.
7. Select **Enabled** to require a 12 to 17 numeric digit password for the MoCA controller to encrypt data.



Note: *The password must be the same on all MoCA devices on your home network.*

8. Click **Apply**.

Protecting & Monitoring Your Wireless Network

After you have successfully connected the SBG6782-AC Wireless Gateway and your wireless devices, you should configure the SBG6782-AC to protect your wireless network from unwanted and unauthorized access by any wireless devices within range of your wireless network. Although security for the SBG6782-AC is already configured, you can use the SBG6782-AC Configuration Manager to set the level of security and access that you want to allow on your home network.

Prevent Unauthorized Access



Caution: To prevent unauthorized access and configuration to your wireless network, we highly recommend that you immediately change the default user name and password after connecting to the Internet and logging on to the SBG6782-AC for the first time.

One of the most important recommendations for securing your wireless home network is to change the default administrator password on your SBG6782-AC and other wireless devices as well. Default passwords are commonly used and shared on the Internet.

To ensure that your wireless home network is secure, it is recommended that you follow these best practices for user passwords:

- 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.
- Continue to change your administrator password on a regular basis.



Note: *If your service provider supplied the SBG6782-AC Wireless Gateway, you may not have the necessary user privileges to change the login user name.*

Change the Default Username and Password

To change the default user name:

1. Log in to the SBG6782-AC Web Manager from any web browser on the computer connected to the SBG6782-AC.
2. Type the default LAN IP address, **192.168.0.1**, in the Address bar and then press **Enter**.

The SBG6782-AC Login screen displays.

3. Type the default username and password as they appear below:
 - Username: **admin**
 - Password: **motorola**
4. Click **Login** to open the SBG6782-AC Web Manager.

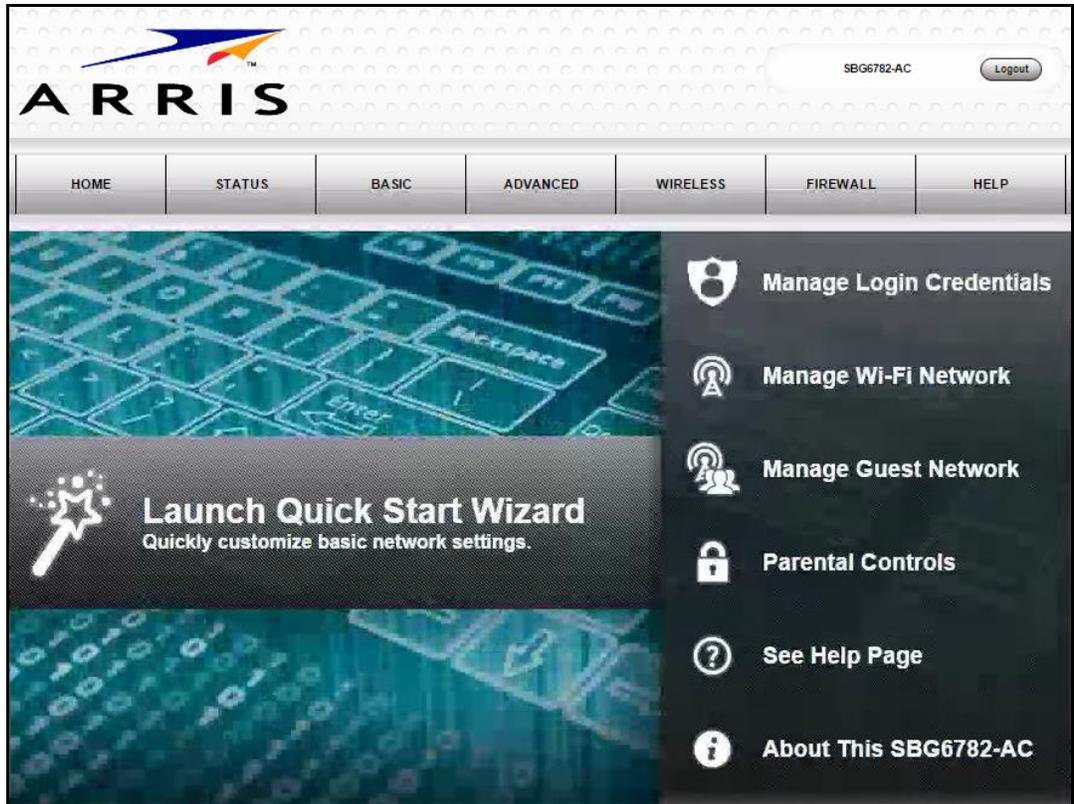


Figure 37: SBG6782-AC Web Manager Main Screen

5. Click **Status** on the menu bar and then click **Security** to display the Status Security screen (see Figure 38).
6. Confirm that **Change Username** is displayed in the drop-down selection box at the top of the screen.

Change Username

Change Username

Enter Current Username

Enter Current Password

Enter New Username

Re-Enter New Username

Apply

Restore Factory Defaults

Yes No

Apply

Figure 38: Change Username Screen

7. Complete each field entry, but note the following:
 - All fields are case-sensitive.
 - Current username is either your default username or your last username change.
 - Make sure **No** is selected for Restore Factory Defaults before clicking Apply.
 - Find a secure place to write down and keep your new user name.
8. Click **Apply** to update your username.
9. Click **Change Username** drop-down arrow at the top of the screen to display **Change Password**.

Change Password

Change User Password

Enter Username

Enter Current Password

Enter New Password

Re-Enter New Password

Apply

Restore Factory Defaults

Yes No

Apply

Figure 39: Change User Password Screen

10. Complete each field entry, but note the following:
 - All fields are case-sensitive.
 - Username is your new user name, if you changed it.

- Current password is either your default password or your last password change.
- Find a secure place to write down and keep your new user name and password.
- Make sure **No** is selected for Restore Factory Defaults.

11. Click **Apply** to update your password.



Note: If your service provider supplied the SBG6782-AC Wireless Gateway, you may not have the necessary user privileges to change the login user name.

If, at any time, you lose your new user name and/or password, you will have to perform a factory reset using the **Reset** button on the rear of the SBG6782-AC (see [Reset Button](#) for more information). This will restore the factory defaults on your SBG6782-AC and allow you to log on to the SBG6782-AC Web Manager using the default user name and password.

Set Up Firewall Protection

You can set up firewall filters and firewall alert notifications on your home network. You can also block Java Applets, Cookies, ActiveX controls, popup windows, Proxies, and website access.

To set the Firewall Protection level:

1. From the SBG6782-AC Web Manager, click **Firewall** on the SBG6782-AC Main Menu bar.
2. Click **Protection Level** from the Firewall submenu options to open the Firewall Protection Level screen.

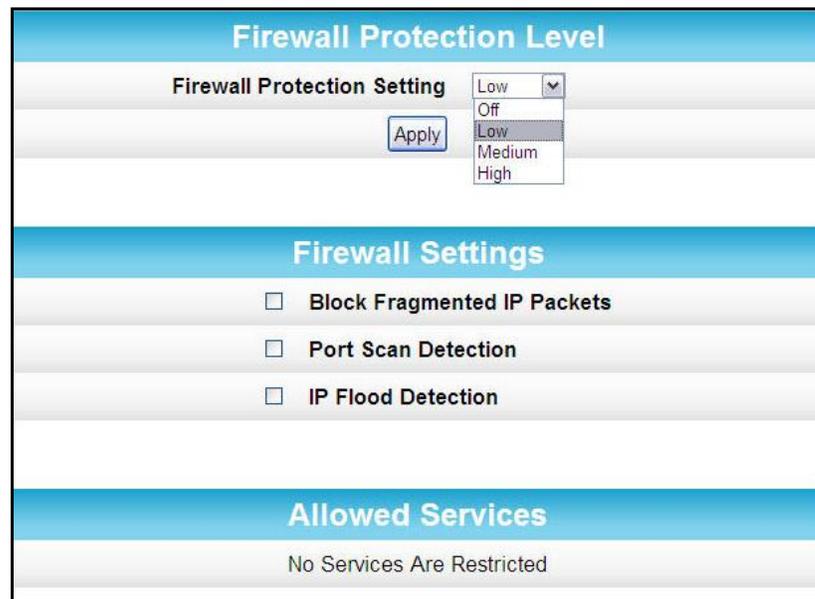


Figure 40: Firewall Protection Level Screen

- Click the Firewall Protection Setting drop-down button to select the firewall protection level.

Available Firewall protection levels:

- Off** – No security, highest risk



Note: Selecting **Off** will disable firewall protection on your home network. Your computer(s) and other Ethernet-enabled devices on your network will be at risk for possible attacks from viruses and hackers.

- Low** – Common security, higher risk
- Medium** – Safer configuration, modest risk

Allowed Services		
Service	Port	Protocol
AIM / ICQ	5190	TCP
DHCPv6	546	UDP
DNS	53	Both
FTP-S	989-990	UDP
HTTP	80	TCP
HTTP Alternate	8080	TCP
HTTP-S	443	TCP
IMAP	143	TCP
IMAP-S	993	TCP
IPSec NAT-T	4500	TCP
NTP	123	UDP
POP3	110	TCP
POP3-S	995	TCP
Radius	1812	Both
SMTP	25	TCP
SMTP-S	435	TCP
SSH	22	TCP
Steam	1725	UDP
Steam Friends	1200	UDP
Telnet-S	992	TCP
XBOX Live	3074	Both
World of Warcraft	3724	Both
Yahoo Messenger	5050	TCP

Figure 41: Firewall Protection Level – Medium Screen

- **High** – Safest configuration, highest security

Allowed Services		
Service	Port	Protocol
DNS	53	Both
HTTP	80	TCP
HTTP-S	443	TCP
IMAP-S	993	TCP
IPSec NAT-T	4500	TCP
NTP	123	UDP
POP3-S	995	TCP
SMTP	25	TCP
SMTP-S	435	TCP
SSH	22	TCP

Figure 42: Firewall Protection Level – High Screen

4. Select the firewall settings for your gateway firewall.
5. Click **Apply**, when done.

Set Up Parental Controls

You can set up the following Parental Controls on your home network:

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



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

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

To set Parental Controls:

1. From the SBG6782-AC Web Manager, click **Firewall** on the SBG6782-AC Main Menu bar.
2. Click **Parental Control** from the Firewall submenu options to open the Firewall Parental Control screen.



Note: Before setting up any Parental Control filters, you must first set the time zone on your SBG6782-AC for your current location.

Figure 43: Parental Control-Change Time Zone Screen

3. Click **Current Time Zone** drop-down button to select your time zone.
4. Select **Yes** or **No** to automatically adjust the time for Daylight Saving Time.
5. Click **Apply** to set the time zone.
6. Click **Create** to continue setting up Parental Controls.

Figure 44: Create Parental Controls Screen

7. Enter a name for the user profile that you want to create in the Description field.
8. Enter the 12-digit (hexadecimal) MAC address of the device for which you are creating Parental Controls in the MAC Address field.
9. Enter the web address of the Internet site that you want to block or access.
10. Enter the Starting port number of the in the Start Port field.
11. Enter the Ending port number of the in the End Port field.
12. Select the days of the week that you want to allow the selected user to access the Internet.
13. Select the time range that you want to allow the selected user to access the Internet.
14. Select to **Allow** or **Block** Internet access for the time and days you set previously.
15. Select **On** or **Off** in the Enabled field to enable or disable this Parental Control restriction.
16. Click **Apply**, when done.

Set Up IP Filtering

You can use IP Filtering to configure Internet access restrictions on specific network devices on your home network using their IP addresses. You will have to create IP address filters that contain the starting and ending IP address range of each device for which you want to block Internet access.

To configure IP filters:

1. From the SBG6782-AC Web Manager, click **Advanced** on the SBG6782-AC Main Menu bar.
2. Click **IP Filtering** from the Advanced submenu options to open the Advanced IP Filtering screen.

IP Filtering		
Start Address	End Address	Enabled
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
192.168.0. <input type="text" value="0"/>	192.168.0. <input type="text" value="0"/>	<input type="checkbox"/>
<input type="button" value="Apply"/>		

Figure 45: Set Up IP Filters Screen

3. Enter the least significant byte of the starting IP address for the range you are setting up in the Start Address field.
4. Enter the least significant byte of the ending IP address for the range you are setting up in the End Address field.
5. Select **Enabled** to activate the IP address filter.
6. Repeat steps 3 thru 5 for each additional range of IP addresses that you want to block Internet access.
7. Click **Apply** to create your IP filters.

Set Up MAC Filtering

MAC filtering allows you to define up to twenty Media Access Control (MAC) address filters to prevent computers from sending outgoing TCP/UDP traffic to the WAN via their MAC addresses. This is useful because the MAC address of a specific NIC card never changes, unlike its IP address, which can be assigned via the DHCP server or hard-coded to various addresses over time.

To configure MAC filters:

1. From the SBG6782-AC Web Manager, click **Advanced** on the SBG6782-AC Main Menu bar.
2. Click **MAC Filtering** from the Advanced submenu options to open the Advanced MAC Filters screen.

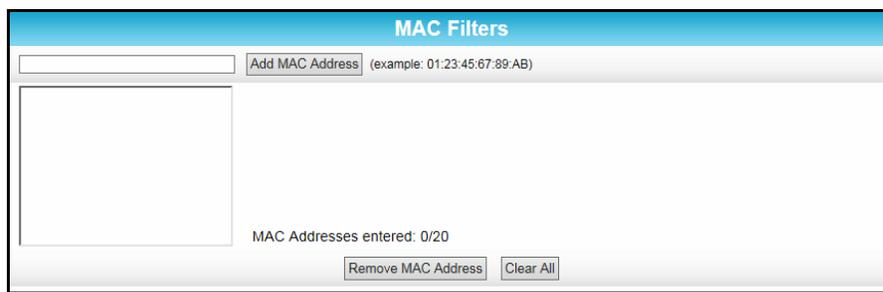


Figure 46: Set Up MAC Filters Screen

3. Enter the MAC address for the computer you want to block in the MAC Address field.
4. Click **Add MAC Address**.
Repeat steps 3 and 4 to add up to 20 MAC addresses.
5. Click on the MAC address in the MAC Address list that you want to delete from the list.
6. Click **Remove MAC Address**.
Repeat steps 5 and 6 for each additional MAC Address that you want to delete.
7. Click **Clear All** button to delete all MAC addresses from the MAC Address list.

Set Up Port Filtering

You can use Port filtering to define port filters to prevent all network devices from sending outgoing TCP/UDP traffic to the WAN on specific IP ports. By specifying a starting and ending port range, you can determine what TCP/UDP traffic is allowed out to the WAN on a per-port basis.

Note: The specified port ranges are blocked for ALL computers, and this setting is not IP address or MAC address specific. For example, if you wanted to block all computers on your home network from accessing HTTP sites (or web surfing), you would create the following port filter.

- Set **Start Port** to **80**
- Set **End Port** to **80**
- Set **Protocol** to **TCP**
- Select **Enabled**

To configure Port filters:

1. From the SBG6782-AC Web Manager, click **Advanced** on the SBG6782-AC Main Menu bar.
2. Click **Port Filtering** from the Advanced submenu options to open the Advanced Port Filtering screen.
3. Enter the starting port number of the Port Filtering range in the Start Port field.
4. Enter the ending port number of the Port Filtering range in the End Port field.
5. Select **TCP**, **UDP**, or **BOTH** from the drop-down Protocol list.
6. Select **Enabled** to activate the selected IP port filters. Otherwise, leave unchecked.
7. Click **Apply** to create your port filters.

Start Port	End Port	Protocol	Enabled
1	8080	Both	<input type="checkbox"/>
1	8080	Both	<input type="checkbox"/>
1	8080	Both	<input type="checkbox"/>
1	8080	Both	<input type="checkbox"/>
1	8080	Both	<input type="checkbox"/>
1	8080	Both	<input type="checkbox"/>
1	8080	Both	<input type="checkbox"/>
1	8080	Both	<input type="checkbox"/>
1	8080	Both	<input type="checkbox"/>
1	8080	Both	<input type="checkbox"/>

Apply

Figure 47: Advanced Port Filtering Screen

Set Up Port Triggers

You can use Port Triggers to configure dynamic triggers to specific devices on your home network (LAN). This allows special applications that require specific port numbers with bi-directional traffic to function properly. Applications such as video conferencing, voice, gaming, and some messaging program features may require these special settings.



Note: If you enable the firewall and set up custom port triggers, then you must set the firewall protection level to **Low** or **Off** to allow traffic through those custom ports. See [Set Up Firewall Protection](#) for more information.

To configure Port Triggers:

1. From the SBG6782-AC Web Manager, click **Advanced** on the SBG6782-AC Main Menu bar.
2. Click **Port Triggers** from the Advanced submenu options to open the Advanced Port Triggers screen.

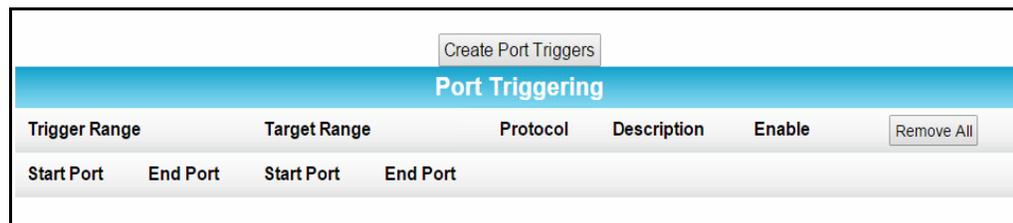


Figure 48: Advanced Port Triggers Screen

3. Click **Create Port Triggers** button to open the Add Port Triggering Entry screen.



Figure 49: Advanced Add Port Triggers Screen

4. Enter the starting port number for the port to be triggered in the Trigger Start Port field.
5. Enter the ending port number for the port to be triggered in the Trigger End Port field.
6. Enter the starting port number of the Port Trigger range in the Target Start Port field.
7. Enter the ending port number of the Port Trigger range in the Target End Port field.
8. Select **TCP**, **UDP**, or **BOTH** from the Internet Protocol drop-down list.
9. Enter a unique name for the port in the Description field.
10. Select **On** to enable IP port triggers or **Off** to disable them.

11. Click **Apply** to create your port triggers.
12. Repeat steps 3 thru 11 for each additional port trigger that you want to create.

Set Up Port Forwarding

You can use Port Forwarding to set up a computer or other network device on your home network (LAN) to be accessible to computers or other remote network devices on the Internet. This allows you to open specific ports behind the firewall on your LAN to set up dedicated connections between your computer and other remote computers for online gaming or other online services. Some allowable services are predefined under the Commonly Forwarded Ports. See Figure 51 for the Commonly Used Ports drop-down list or Figure 52 for a sample list of commonly used port numbers.



Note: It is recommended that you manually configure the TCP/IP settings listed below on the computer you are setting up for remote access. Otherwise, remote access to your computer 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 the SBG6782-AC Web Manager, click **Advanced** on the SBG6782-AC Main Menu bar.
2. Click **Port Forwarding** from the Advanced submenu options to open the Port Forwarding screen.

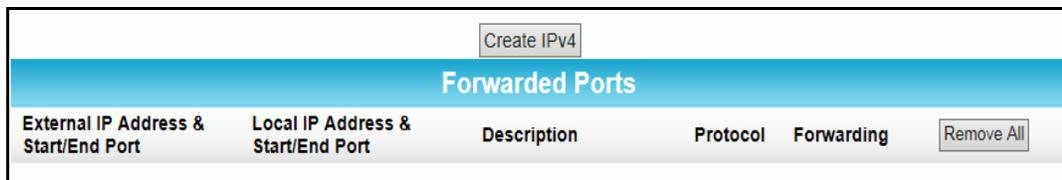


Figure 50: Port Forwarding Screen

3. Click **Create IPv4** button to open the Port Forwarding IPv4 Entry screen.



Note: To map a port, you would enter the range of port numbers that you want forwarded locally and the IP address for sending traffic to those ports. If you only want a single port specification, enter the same port number in the start and end locations for that IP address.

The screenshot shows the 'IPv4 Entry' configuration screen. It has a table with the following columns: 'External IP Address & Start/End Port', 'Local IP Address & Start/End Port', 'Description', 'Protocol', and 'Enabled'. The 'External IP Address' field contains '0.0.0.0'. The 'Local IP Address' field contains '0.0.0.0'. The 'Protocol' dropdown is set to 'TCP'. The 'Enabled' dropdown is set to 'Off'. Below the table, there is a 'Commonly Forwarded Ports' dropdown menu and 'Apply' and 'Cancel' buttons. Below the main form is a 'Forwarded Ports' section with a table that has columns for 'External IP Address & Start/End Port', 'Local IP Address & Start/End Port', 'Description', 'Protocol', 'Forwarding', and a 'Remove All' button.

Figure 51: Add Forwarded Ports Screen

4. Do one of the following to set up the External IP Address:
 - Keep the IP Address set at 0.0.0.0 in the External IP Address field and then enter the port number in the Start Port field. Repeat the same port number in the End Port field. This allows incoming data traffic on the specified ports from any remote IP address.
 - Enter a specific remote IP address of your choice in the External IP Address field and then enter the specific port numbers in the Start and End Port fields. This allows incoming data traffic on the specified ports from only one remote IP address.



Note: To forward a range of ports, enter the first number of the port range in the Start Port field and the last number of the port range in the End Port field.

5. Do the following to set up your Local IP Address:
 - a. Enter the IP address of your local computer that you are setting up for port forwarding.
 - b. Enter the port number of your choice in the Start Port field (see the Commonly Forwarded Ports drop-down list).
 - c. Repeat the same port number in the End Port field (see the Commonly Forwarded Ports drop-down list).



Note: To forward a range of ports, enter the first number of the port range in the Local Start Port field and the last number of the port range in the local End Port field.

6. Enter a description to name the forwarded port you are creating.
7. Select **TCP**, **UDP**, or **BOTH** from the Internet Protocol drop-down list.
8. Select **On** to enable port forwarding or **Off** to disable it.
9. Click **Apply**.
10. Repeat steps 3 thru 9 for each additional forwarded port that you want to create.

Commonly Forwarded Ports	
Battle.net.....	6112 / TCP
BitTorrent.....	6881-6999 / Both
Call of Duty.....	28960 / UDP
eMule.....	4662 / TCP
eMule.....	4672 / UDP
GameSpy Arcade.....	6500 / TCP
Gnutella.....	6346-6347 / Both
Half-Life.....	27015 / Both
Halo.....	2302 / UDP
Internet Radio.....	8000 / Both
IRC.....	6665-6669 / TCP
MS Media Server....	1755 / Both
Playstation 3.....	80 / TCP
Playstation 3.....	3478 / UDP
Playstation 3.....	443 / TCP
Playstation 3.....	3479 / UDP
Playstation 3.....	5223 / TCP
Playstation 3.....	3658 / UDP
Quicktime.....	6970 / UDP
Second Life.....	12035-12036 / UDP
Slingbox.....	5001 / UDP
Steam.....	1725 / UDP
Steam Friends.....	1200 / UDP
Synergy.....	24800 / TCP
TeamSpeak.....	8767 / UDP
Ventrillo.....	3784-3785 / Both
War of Warcraft....	3724 / Both
XBOX 360.....	80 / TCP
XBOX 360.....	88 / UDP

Figure 52: Commonly Used Forwarded Ports List



Note: To map a port, you would enter the range of port numbers that you want forwarded locally and the IP address for sending traffic to those ports. If you only want a single port specification, enter the same port number in the start and end locations for that IP address.

Port Forwarding						
Service List		Web Server (HTTP) <input type="button" value="Add"/>			<input type="button" value="Help"/>	
Clear entry		1 <input type="button" value="Clear"/>			<input type="button" value="Help"/>	
Port Forwarding Table						
Enable	Description	Inbound port	Type	Private IP address	Private port	
1. <input checked="" type="checkbox"/>	Internet Radio	8000 - 8000	BOTH	192.168.0.	8000 - 8000	
2. <input checked="" type="checkbox"/>	Web Server (H)	80 - 80	TCP	192.168.0.	80 - 80	
<input type="button" value="Apply"/>						

Figure 53: Forwarded Ports Screen

11. Click **Apply**, when done.

Set Up the DMZ Host



WARNING! The gaming DMZ host is not protected by the SBG6782-AC firewall. It is exposed to the Internet and thus vulnerable to attacks or hacking from any computer on the Internet. Consider carefully before configuring a device to be in the DMZ.

You can configure one computer on your home network to be the DMZ Host. That computer will operate outside of the SBG6782-AC firewall and allow remote access from the Internet to your computer, 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 the SBG6782-AC Web Manager, click **Advanced** on the SBG6782-AC Main Menu bar.
2. Click **DMZ Host** from the Advanced submenu options to open the DMZ Host screen.



Figure 54: Advanced DMZ Host Screen

3. 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.
4. Click **Apply**.



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 Firewall Event Log Notifications

When a firewall attack is detected on your home network, a separate email alert notification is generated and a local log or report of the event is created. You can set up automatic email alert notifications for whenever a firewall attack is detected on the SBG6782-AC.

To set up Firewall Event Log notifications:

1. From the SBG6782-AC Web Manager, click **Firewall** on the SBG6782-AC Main Menu bar.
2. Click **Local Log** from the Firewall submenu options to open the Firewall Local Log screen.

The screenshot shows the 'Alert System' configuration page. It includes several input fields: 'Contact Email Address', 'SMTP Server Name', 'SMTP Username' (with 'admin' entered), and 'SMTP Password' (with masked characters). There is an 'Email Alerts' checkbox labeled 'Enable' which is currently unchecked. An 'Apply' button is located below the form. Below the form is a table with the following columns: 'Description', 'Count', 'Last Occurrence', 'Target', and 'Source'. At the bottom of the table are two buttons: 'E-mail Log' and 'Clear Log'.

Figure 55: Firewall Local Log Screen

3. Enter your email address in the Contact Email Address field.
4. Enter the name of the email server in the SMTP Server Name field. Check with your service or email provider.
5. Enter the user name for your email account.
6. Enter the password for your email account.
7. Select **Enable** checkbox in the E-mail Alerts field to allow for automatic Email alerts.
8. Click **Apply**, when done.

Store Remote Firewall Logs

You can store firewall attack reports or logs on a computer in your home, so that multiple instances can be logged over a period of time. You can select individual attack or configuration items to send to the SysLog server, so that only the items of interest will be monitored.



Note: The SysLog server must be on the same network as the Private LAN behind the Configuration Manager (typically **192.168.0.x**).

To store remote Firewall logs:

1. From the SBG6782-AC Web Manager, click **Firewall** on the SBG6782-AC Main Menu bar.
2. Click **Remote Log** from the Firewall submenu options to open the Firewall Remote Log screen.



Figure 56: Firewall Remote Log Screen

3. Select all desired event types that you want to monitor.
This will activate the SysLog monitoring feature.
4. Enter the last digits from **2** to **254** of the SysLog server's IP address.



Note: Normally, the IP address of this SysLog server is hard-coded so that the address always matches the entry on this page.

5. Click **Apply**.

Managing Your Gateway and Connected Networks

You can use the SBG6782-AC Web Manager to view and monitor the network configuration settings and operational status of your wireless gateway. You can also configure your network connections and wireless security settings. See [Protecting & Monitoring Your Wireless Network](#) for more information.

View the Gateway Status Using the Device Status Button

You can use the Device Status button on the SBG6782-AC Login screen to obtain a quick view of the current configuration and network connection status of your SBG6782-AC without having to login to the SBG6782-AC Web Manager.

1. Open any web browser on the computer connected to the SBG6782-AC.
2. Type the default LAN IP address, **192.168.0.1**, in the Address bar and then press **Enter**.
The SBG6782-AC Login screen displays.



Figure 57: Device Status Button

3. Click **Device Status** button to open the SBG6782-AC Device Status screen (see Figure 57).
4. Click **Close** to exit.



Figure 58: Device Status Screen

View the Gateway Product Information

The Status Product Information screen displays general product information, including the software (or firmware) version and the current network connection status of the gateway.

To open the Status Product Information page:

1. Click **Status** on the SBG6782-AC Main Menu bar.
2. Click **Product Information** from the Status submenu options.
3. Click the **Refresh** button (F5) in your web browser to reload the information on the screen.

Information	
Standard Specification Compliant	DOCSIS 3.0
Hardware Version	1
Software Version	D30GW-EAGLE-1.5.0.0-GA-07-NOSH
Cable Modem MAC Address	90:b1:34:fa:22:eb
Serial Number	382779315635458401014005
Status	
Up Time	14 days 04h:08m:56s
Cable Modem IP Address	-----

Figure 59: SBG6782-AC Status – Product Information Screen

View the Gateway Network Connection Status

The Status Connection screen displays information about the RF upstream and downstream channels, including downstream channel frequency, upstream channel ID, and upstream and downstream signal power and modulation.

This screen also displays IP lease information including the current IP address of the cable modem, the duration of both leases, the expiration time of both leases, and the current system time from the DOCSIS time server.

To open the Status Connection screen:

1. Click **Status** on the SBG6782-AC Main Menu.
2. Click **Connection** from the Status submenu options.

Startup Procedure								
Procedure			Status	Comment				
Acquire Downstream Channel				Locked				
Connectivity State			OK	Operational				
Boot State			OK	Operational				
Configuration File			OK					
Security			Enabled	BPI+				
DOCSIS Network Access Enabled			Allowed					

Downstream Bonded Channels								
Channel	Lock Status	Modulation	Channel ID	Frequency	Power	SNR	Corrected	Uncorrectables
1	Locked	QAM256	2	711000000 Hz	-4.9 dBmV	44.7 dB	17	0
2	Locked	QAM256	1	705000000 Hz	-4.8 dBmV	44.6 dB	10	0
3	Locked	QAM256	3	717000000 Hz	-4.8 dBmV	44.6 dB	8	0
4	Locked	QAM256	4	723000000 Hz	-4.8 dBmV	44.5 dB	16	0
5	Locked	QAM256	5	729000000 Hz	-5.0 dBmV	43.9 dB	5	0
6	Locked	QAM256	6	735000000 Hz	-4.9 dBmV	44.7 dB	10	7
7	Locked	QAM256	7	741000000 Hz	-5.1 dBmV	44.6 dB	5	0
8	Locked	QAM256	8	747000000 Hz	-4.9 dBmV	44.6 dB	10	0

Upstream Bonded Channels						
Channel	Lock Status	US Channel Type	Channel ID	Symbol Rate	Frequency	Power
1	Locked	ATDMA	1	5120 Ksym/sec	30700000 Hz	47.5 dBmV
2	Locked	TDMA and ATDMA	2	2560 Ksym/sec	18500000 Hz	47.0 dBmV
3	Locked	ATDMA	3	5120 Ksym/sec	23300000 Hz	47.5 dBmV
4	Locked	TDMA and ATDMA	4	2560 Ksym/sec	35500000 Hz	47.2 dBmV

Figure 60: SBG6782-AC Status Connection Screen

Back Up Your Gateway Configuration

You can save a backup copy of the current configuration settings to your local computer. You can use the backup file to restore your custom settings in the event that you made changes that you no longer want.



Caution: We highly recommend that you perform the configuration backup using the SBG6782-AC default login username and password.

To create a backup copy of your configuration settings:

1. Click **Basic** on the SBG6782-AC Main Menu.
2. Click **Backup and Restore** from the Basic submenu options.



Figure 61: SBG6782-AC Backup and Restore Screen

3. Click **Choose File** and type the path and file name where you want to store the backup file on your computer, or search for an existing configuration file that you want to update.
4. Click **Backup** to create a backup file of your SBG6782-AC configuration settings.

Restore Your Gateway Configuration Settings



WARNING! This action will delete your current gateway configuration settings and allow you to restore a previously saved configuration.



Note: After the gateway configuration settings are restored, the SBG6782-AC will automatically reboot and you will have to log on using the default username (**admin**) and password (**motorola**).

1. Click **Basic** on the SBG6782-AC Main Menu.
2. Click **Backup and Restore** from the Basic submenu options.
3. Click **Browse** to search for a previously saved configuration file from the Downloads folder on your computer.
4. Click **Restore**. The SBG6782-AC will automatically reboot.

Reset Your Gateway Settings



WARNING! This process also deletes any custom Wireless Cable Modem Gateway configurations you may have already created. We recommend that you create a backup copy of your configuration before resetting the Wireless Cable Modem Gateway. See [Back Up Your Wireless Cable Modem Gateway Configuration](#) for more information.

From the SBG6782-AC Web Manager, do the following to open the Status Security screen:

1. Click **Status** on the SBG6782-AC Main Menu.
2. Click **Security** from the Status submenu options.

Figure 62: SBG6782-AC Restore Factory Defaults Screen

3. Select **Yes** under Restore Factory Defaults.
4. Click **Apply** to reset the default username and password and restore the original configuration.
The message, This action will restore factory default settings. Please reboot the modem for new settings to take effect, displays.
5. Click **OK**.
6. Click **Status** on the SBG6782-AC Main Menu.
7. Click **Configuration** from the Status submenu options to display the Status Configuration screen.
8. Click **Reboot**.
9. Log back in using the default username and password.

Username: **admin**

Password: **motorola**

Troubleshooting Tips

If the solutions listed in this section do not solve your problem, contact your service provider for assistance.

Your service provider may ask for the status of the LEDs as described in [Front Panel LED Icons and Error Conditions](#) (page 74).

You may have to reset the SBG6782-AC gateway configuration to its original factory settings if the gateway is not functioning properly.

Solutions

Table 5. Troubleshooting Solutions

Gateway Problem	Possible Solution
POWER LED Icon is OFF	<ul style="list-style-type: none"> ■ Check the power connection on the gateway and to the electrical outlet. ■ Check that the electrical outlet is working. Is the outlet controlled by a light switch? If so, disconnect the gateway power cord and connect it to another electrical outlet that is not controlled by a wall light switch.
Cannot Send or Receive Data	<ul style="list-style-type: none"> ■ Check each end of the coaxial cable connection on the gateway and cable outlet. Hand tighten each connector, if necessary. ■ Check the Ethernet cable to make sure it is properly connected to the gateway and computer. ■ Check the status of the LED icons on the front panel and then refer to Front Panel LED Icons and Error Conditions to identify the problem. ■ If you have cable television service, check your television to ensure your cable service is operating properly. ■ 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.

Gateway Problem	Possible Solution
Cannot Access the Internet	<ul style="list-style-type: none"> Check that all cable and power connections on your gateway and computer are properly connected. Check that the Power, Online, and Wireless LED icons on the front panel are lit up solid. Contact your service provider for assistance.
Wireless devices cannot send or receive data	<ul style="list-style-type: none"> If the problem still persists after checking the coaxial cable and Ethernet connections and your IP address, check the Wireless Security Mode setting on the Wireless Primary Network screen. If you enabled WPA and configured a passphrase on the gateway, be sure each affected wireless client has the identical passphrase. If this does not solve the problem, check if the wireless client supports WPA. If you enabled WEP and configured a key on the gateway, be sure each affected wireless client has the identical WEP key. If this does not solve the problem, check whether the client's wireless adapter supports the type of WEP key configured on the gateway.

Front Panel LED Icons and Error Conditions

The SBG6782-AC front panel LED icons provide status information for the following error conditions:

Table 6. Front Panel LED Icons and Error Conditions

LED Icon	Status	If, During Start up:	If, During Normal Operation
 POWER	OFF	Gateway is not properly plugged into the electrical outlet	wireless cable modem gateway is unplugged
 RECEIVE	BLINKING	Downstream receive channel cannot be acquired	Downstream channel is lost
 SEND	BLINKING	Upstream send channel cannot be acquired	Upstream channel is lost
 ONLINE	BLINKING	IP registration is unsuccessful	IP registration is lost

LED Icon	Status	If, During Start up:	If, During Normal Operation
 WIRELESS	OFF	LED is disabled	LED is disabled
 WIRELESS	OFF	LED is disabled	LED is disabled
 MoCA	OFF	No connected device is detected	Device is disconnected

Warranty Information

SURFboard SBG6782-AC Wireless Gateway
ARRIS Enterprises, 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 telephone number **1-877-466-8646**. Technical support charges may apply. 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 insure 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 number, **1-877-466-8646** for warranty service or technical support. Technical support charges may apply.

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

ARRIS · Suwanee · Georgia · 30024 · USA

Telephone: 1-678-473-2000

Fax: 1-678-473-8470

www.arris.com

365-095-23865 x.3 11/2015