SMC® Networks

Wireless Data Gateway

D3G0804W
User Manual

FastFind Links

SMC Networks
20 Mason
Irvine, CA 92618
U.S.A.

Information furnished by SMC Networks, Inc. (SMC) is believed to be accurate and reliable. However, no responsibility is assumed by SMC for its use, or for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of SMC. SMC reserves the right to change specifications at any time without notice

Microsoft and Windows are registered trademarks of Microsoft Corporation. Apple and Macintosh are registered trademarks of Apple, Inc. All other brands, product names, trademarks, or service marks are property of their respective owners.

This product (Model : D3G0804W) includes software code developed by third parties, including software code subject to the GNU General Public License (“GPL”) or GNU Lesser General Public License (LGPL”). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL used in this product, are available to you at http://gpl.smc.com/. The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL Code and LGPL Code for this product and the terms of the GPL and LGPL.

D3G0804W User Manual

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 and follow these instructions.
- Keep these instructions.
- Heed all warnings.
- Only use attachments/accessories specified by the manufacturer.
- Do not use this product near water.
- Do not install near any heat sources.
- Clean only with a dry cloth.
- Do not block any ventilation openings.
- Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus.
- Unplug this apparatus during lightning storms or when unused for long periods of time.
- Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as a power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.
- Do not defeat the purpose of the polarized or grounding type plug.
- Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.

SMC Wireless Data Gateway complies with applicable requirements for performance, construction, labeling, and information when used as outlined below:

WARNING

Risk of Shock

Mains voltages inside this unit. No user-serviceable parts inside. Refer service to qualified personnel only!

CAUTION

Potential equipment damage

Potential loss of service

Connection of the Wireless Data Gateway to existing telephone wiring should only be performed by a professional installer. Physical connections to the previous telephone provider must be removed and the wiring must be checked; there must not be any voltages. Cancellation of telephone service is not adequate. Failure to do so may result in loss of service and/or permanent damage to the Wireless Data Gateway.

- The Wireless Data Gateway is designed to be connected directly to a telephone.
- Connecting the Wireless Data Gateway to the home’s existing telephone wiring should only be performed by a professional installer.
- Do not use product near water (i.e. wet basement, bathtub, sink or near a swimming pool, etc.), to avoid risk of electrocution.
- Avoid using and/or connecting the equipment during an electrical storm, to avoid risk of electrocution.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- Do not locate the equipment within 6 feet (1.9m) of a flame or ignition source (i.e. heat registers, space heaters, fireplaces, etc.).
- Only use power supply and power cord included with the equipment.
- Equipment should be installed near the power outlet and should be easily accessible.
- The shield of the coaxial cable must be connected to earth (Grounded) at the entrance to the building in accordance with applicable national electrical installation codes. In the U.S., this is

required by NFPA 70 (National Electrical Code) Article 820. In the European Union and in certain other countries, CATV installation equipment bonding requirements are specified in IEC 60728-11, Cable networks for television signals, sound signals and interactive service, Part 11: Safety. This equipment is intended to be installed in accordance with the requirements of IEC 60728-11 for safe operation.

- In areas of high surge events or poor grounding situation and areas prone to lightning strikes, additional surge protection may be required (i.e. PF11VNT3 or 3020J from American Power Conversion) on the AC, RFM Ethernet and Phones lines.

Contents

Preface

Congratulations on your purchase of the D3G0804W Wireless Data Gateway. The D3G0804W is a multimedia Gateway that delivers video, and data for applications such as Home Security and Automation, and IPTV distribution. The Gateway is a versatile and robust all-in-one solutions that make it ideal for homes and businesses to connect their local-area network (LAN) to the Internet.

This user manual contains all the information you need to install and configure your new D3G0804W Wireless Data Gateway.

Key Features

This section summarizes the key features of the D3G0804W Gateways.

- **DOCSIS 3.0 Cable Modem**. The Gateway includes an 8x4 DOCSIS 3.0 cable modem capable of maximum downstream speeds of 320 Mbps and maximum upstream speeds of 120 Mbps.
- **High-Speed Connections**. The Gateway provides four 10/100/1000 Ethernet ports, so users can take full advantage of their high-speed WAN connections by enjoying the broadest spectrum of multimedia, including IP telephony, instant high-speed Web access, file sharing, multimedia conferencing, video streaming and download, high-performance gaming, and MP3 downloading. The Gateway includes leading software features for maximizing user experiences, including SPI firewall, port triggering, port forwarding, and parental control features.
- **WiFi Alliance certified 802.11 a/b/g/n**. The Gateway supports 2.4GHz and 5GHz concurrently. It supports up-to 300Mbps* maximum network bandwidth with its six built-in antennas and allows faster wireless connections over longer distances.

Note: Cable modems can provide maximum downstream speeds of 320 Mbps and upstream speeds of 120 Mbps. However, the actual rate provided by your specific service provider may vary dramatically from these maximum speeds.

Document Organization

This document consists of four chapters and two appendixes.

Chapter 1 - describes the contents in your Gateway package, system requirements, and an overview of the Gateway's front and rear panels.

Chapter 2 - describes how to install your Gateway.

Chapter 3 - describes how to prepare the Gateway for configuration.

Chapter 4 - describes how to configure the Gateway.

Appendix A - describes how to mount your Gateway on a wall.

Appendix B - contains compliance information.

Before using this document, familiarize yourself with the Table of Contents on page vi. All first-time users should read Chapter 1. Installation should not be attempted without reading Chapter 2. Configuration should not be attempted without reading Chapters 3 and 4. Troubleshooting suggestions are on page 88.

Document Conventions

In this document, the term "Gateway" is used to refer collectively to the SMCD3G0804W Wireless EMTA Gateways. If information applies to only one model, that model is identified.

This document uses the following additional conventions to draw your attention to certain information.

Symbol	Meaning	Description
ℹ	Note	Notes emphasize or supplement important points of the main text.
💡	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
⚠	Warning	Warnings indicate that failure to take a specified action could result in damage to the device.
⚡	Electric Shock Hazard	This symbol warns users of electric shock hazard. Failure to take appropriate precautions such as not opening or touching hazardous areas of the equipment could result in injury or death.

1 Getting to Know Your Gateway

Topics:

Before you install your D3G0804W Wireless Data Gateway, check the package contents and become familiar with the Gateway's front and back panels.

This chapter describes the items that come in the Gateway package and the major components of the Gateway hardware.

Unpacking Package Contents

Unpack the items and confirm that no items are missing or damaged. Your package should include:

- One SD3G0804W Wireless Data Gateway
- One power supply and a power cord
- One Category 5E Ethernet cable
- One Installation Instructions

If any items are missing or damaged, please contact your place of purchase. Keep the carton, including the original packing material, in case you need to store the product or return it.

System Requirements

To complete your installation, you will need the following items:

- Provisioned Internet access on a cable network that supports cable modem service
- A computer with a wired network adapter with TCP/IP installed
- A Java-enabled Web browser, such as Microsoft Internet Explorer 5.5 or above
- Microsoft® Windows® 2000 or higher for USB driver support
- A battery that can be installed in your Gateway to support voice service. Please contact your service provider for more information.

Becoming Familiar with the Gateway Hardware

The following sections describe the Gateway hardware.

Front Panel

The front panel of your Gateway contains a set of light-emitting diode (LED) indicators. These LEDs show the status of your Gateway and simplify troubleshooting. At the bottom of the front panel are **WPS** and **ON/OFF** buttons.

Figure 1 shows the front panel of the Gateway.

Table 1 describes the front panel LEDs and Table 2 describes the front panel push-buttons.

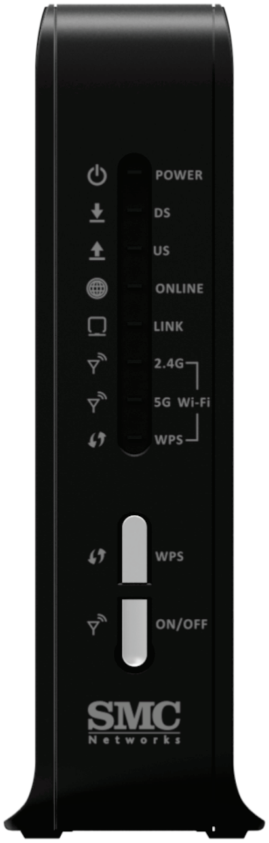


Figure 1. Front Panel of the Gateway

Table 1. Front Panel LEDs

Symbol	LED	Color	Description
⏻	POWER	Red	ON = Off/Standby, AC power switch in Off/Standby position OFF = DC power is not supplied to the Gateway
		Green	ON = DC power is supplied to the Gateway and power switch is in the ON position

⤓	DS	Blue	Blinking = scanning for downstream channel
			ON = locked on DOCSIS 3.0 downstream channel
			OFF = no power

		Green	On = locked on DOCSIS 2.0 downstream channel
⤒	US	Blue	Blinking = ranging is in progress ON = ranging is complete, DOCSIS 3.0 bonded upstream OFF = no power or not locked on upstream channel
		Green	ON = ranging is complete, DOCSIS 2.0 bonded upstream
🌐	ONLINE	Blue	Blinking = DHCP and registration in progress ON = online in DOCSIS 3.0 mode OFF = no power or upstream ranging not complete
		Green	ON = online in DOCSIS 2.0 mode

▢	LINK	Blue	Blinking = data activity
			ON = Gigabit Ethernet LAN device connected
			OFF = no LAN devices connected

		Green	Blinking = data activity
			ON = 10/100 Ethernet LAN device connected

📡	2.5G	Green	Blinking = data activity
			ON = 2.4 GHz Wireless Access Point (WAP) is ON
			OFF = WAP is OFF

📡	5G	Blue	Blinking = data activity
			ON = 5 GHz WAP is ON
			OFF = WAP is OFF

⟲	WPS	Green	Blinking = Wireless Protected Setup (WPS) enabled for device pairing OFF = WPS pairing is OFF

Table 2. Front Panel Push-Buttons

Symbol	Button	Description
	WPS	Press this button to establish a wireless connection between the Gateway and a WPS-enabled client (see “Configuring WPS Settings” on page 39).
	ON/OFF	Press to turn ON the Gateway. Press again to turn OFF the Gateway.

Rear Panel

The rear panel of the Gateway contains a reset button and ports for attaching the supplied power cord and making other connections. Figure 2 shows the rear panel components and Table 3 describes them.

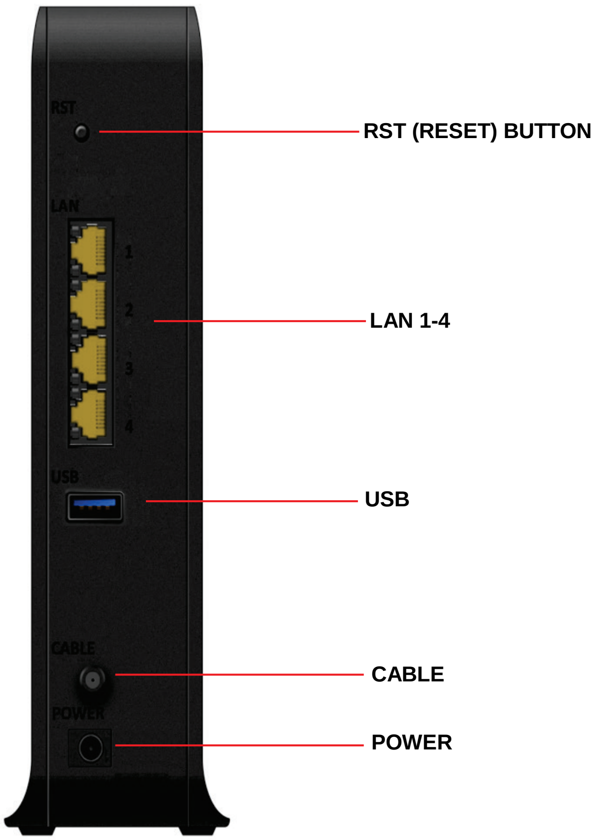


Figure 2. Rear View of the Gateway

Table 3. Gateway Rear Panel Components

Port / Switch	Description
RST	Use this button to reboot the Gateway or restore the default factory settings (see "Resetting or Rebooting the Gateway" below). This button is recessed to prevent accidental resets of your Gateway.
LAN 1-4	Four 10/100/1000 auto-sensing RJ-45 switch ports. Connect devices on your LAN, such as a computer, hub, or switch, to these ports.
USB	This Gateway provides one USB 2.0 host port. Use this port to connect to a USB printer, hard drive, or other peripheral.
CABLE	Connect your coaxial cable line to this port.
POWER	Connect the supplied power cord to this port.

Resetting or Rebooting the Gateway

You can use the **RST** button on the Gateway rear panel to power cycle the Gateway or reset the Gateway to its original factory default settings.

Note: You can also reset or reboot the Gateway using the Restore/Reboot page (see page 91).

Rebooting the Gateway

To reboot the Gateway and keep any customized overrides you made to the default settings:

1. Leave power cord connected to the Gateway.
2. Press and hold the **RST** button on the Gateway back panel for about 10 seconds, then release the **RST** button.
3. Wait for the Gateway to reboot.

Restoring Factory Defaults

To reset the Gateway to its original factory default settings:

1. Leave power plugged into the Gateway.
2. Press and hold the **RST** button on the Gateway back panel for about 15 seconds, then release the **RST** button.
3. Wait for the Gateway to reboot with factory default settings.

2 Installing Your Gateway

Topics:

This chapter describes how to install the Gateway.

Finding a Suitable Location

You can install the Gateway in any location with access to the cable network. All of the cables connect to the rear panel of the Gateway for better organization and utility. The LED indicators on the front panel are easily visible to provide you with information about network activity and status.

For optimum performance, the location you choose should:

- Be close to a working AC power outlet.
- Allow the Gateway to be mounted vertically for optimized wireless performance.
- Allow sufficient air flow around the Gateway to keep the device as cool as possible.
- Not expose the Gateway to a dusty or wet environment.
- Be an elevated location such as a high shelf, keeping the number of walls and ceilings between the Gateway and your other devices to a minimum.
- Be away from electrical devices that are potential sources of interference, such as ceiling fans, home security systems, microwaves, or the base for a cordless phone.
- Be away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

Connecting to the LAN

Using an Ethernet LAN cable, you can connect the Gateway to a desktop computer, notebook, hub, or switch. The Gateway supports auto-MDI/MDIX, so you can use either a standard straight-through or crossover Ethernet cable.

1. Connect either end of an Ethernet cable to one of the four LAN ports on the rear panel of the Gateway (see Figure 3).

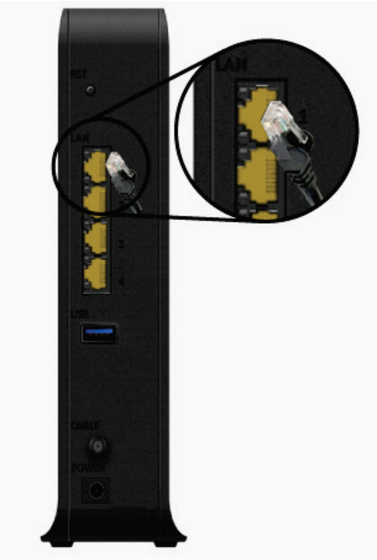


Figure 3. Connecting to a LAN Port on the Gateway Rear Panel<

2. Connect the other end of the cable to your computer’s network-interface card (NIC) or to another network device (see Figure 4).

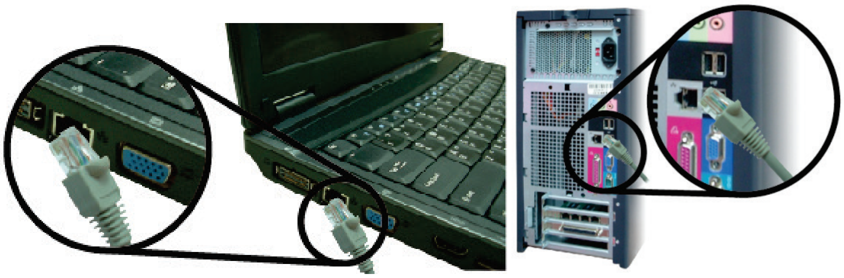


Figure 4. Connecting the Gateway to a Laptop or Desktop Computer

Connecting the WAN

To connect your Gateway to a Wide Area Network (WAN) interface:

1. Connect a coaxial cable from a cable port in your home or office to the port labeled **CABLE** on the rear panel of the Gateway (see Figure 2 on page 5). Use only manufactured coaxial patch cables with F-type connectors at both ends for all connections.
2. Hand-tighten the connectors to secure the connection.
3. If the modem was not installed by your cable provider (ISP) or is replacing another cable modem, contact your cable operator to register the Gateway. If the modem is not registered with your cable operator, it will not be able to connect to the cable network system.

Powering on the Gateway

After making your LAN and WAN connections, use the following procedure to power on the Gateway.

1. Connect the supplied power cord to the port labeled **POWER** on the rear panel of the Gateway (see Figure 2 on page 5).
2. Connect the other end of the power cord to a working DC power outlet. The outlet should not be controlled by a wall switch to avoid someone unknowingly turning off power to the outlet.
3. Press the **ON/OFF** button on the front panel of the Gateway (see Figure 1 on page 3). The Gateway powers on automatically. The **POWER** LED on the front panel goes ON and the other front panel LEDs show the Gateway’s status.

⚠ **WARNING:** Only use the power supply furnished with the Gateway. Using a different power supply can damage your Gateway and void the warranty.

3 Preparing to Configure Your Gateway

Topics:

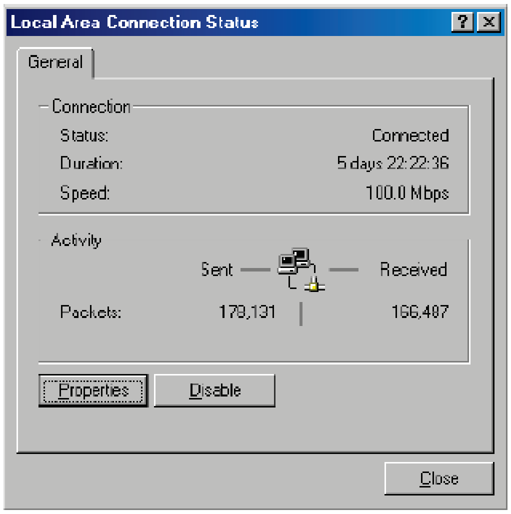
Before you can access the Gateway's GUI, configure the TCP/IP settings in your computer's operating system that will be used to configure the Gateway.

This chapter describes how to configure the TCP/IP settings for various operating systems.

Configuring Microsoft Windows 2000

Use the following procedure to configure your computer if your computer has Microsoft Windows 2000 installed.

1. On the Windows taskbar, click **Start**, point to **Settings**, and then click **Control Panel**.
2. In the Control Panel window, double-click the **Network and Dial-up Connections** icon. If the Ethernet adapter in your computer is installed correctly, the **Local Area Connection** icon appears.
3. Double-click the **Local Area Connection** icon for the Ethernet adapter connected to the Gateway. The Local Area Connection Status dialog box appears (see Figure 5).



Status: Connected

Duration: 5 days 22:22:36

Speed: 100.0 Mbps

Packets: 179,131 | 166,487

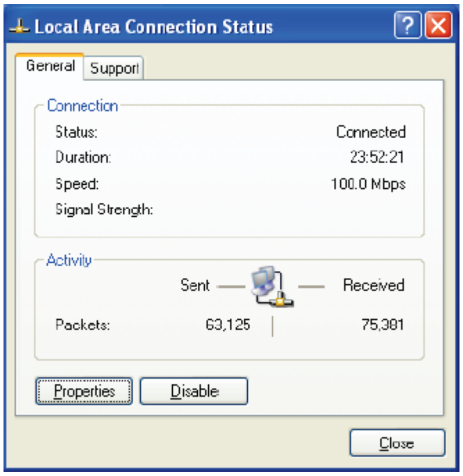
Figure 5. Local Area Connection Status Window

4. In the Local Area Connection Status dialog box, click the **Properties** button. The Local Area Connection Properties dialog box appears.
5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IP)** is checked. Then select **Internet Protocol (TCP/IP)** and click the **Properties** button.
6. Click **Obtain an IP address automatically** to configure your computer for DHCP.
7. Click the **OK** button to save this change and close the Local Area Connection Properties dialog box.
8. Click **OK** button again to save these new changes.
9. Restart your computer.

Configuring Microsoft Windows XP

Use the following procedure to configure a computer running Microsoft Windows XP with the default interface. If you use the Classic interface, where the icons and menus resemble previous Windows versions, perform the procedure under “Configuring Microsoft Windows 2000”.

1. On the Windows taskbar, click **Start**, click **Control Panel**, and then click **Network and Internet Connections**.
2. Click the **Network Connections** icon.
3. Double-click **Local Area Connection** for the Ethernet adapter connected to the Gateway. The Local Area Connection Status dialog box appears.
4. In the Local Area Connection Status dialog box, click the **Properties** button (see Figure 6). The Local Area Connection Properties dialog box appears.



Local Area Connection Status

Connection
Status: Connected
Duration: 23:52:21
Speed: 100.0 Mbps
Signal Strength:

Activity
Sent — Received
Packets: 63,125 | 75,381

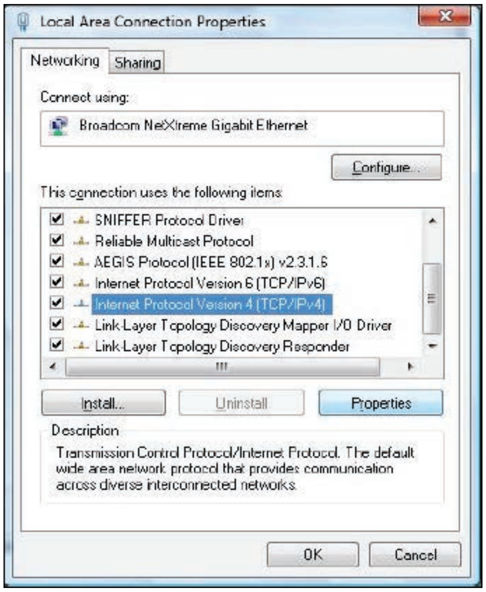
Figure 6. Local Area Connection Status Window

5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IP)** is checked. Then select **Internet Protocol (TCP/IP)** and click the **Properties** button. The Internet Protocol (TCP/IP) Properties dialog box appears.
6. In the Internet Protocol (TCP/IP) Properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP. Click the **OK** button to save this change and close the Internet Protocol (TCP/IP) Properties dialog box.
7. Click the **OK** button again to save your changes and restart your computer.

Configuring Microsoft Windows Vista

Use the following procedure to configure a computer running Microsoft Windows Vista with the default interface. If you use the Classic interface, where the icons and menus resemble previous Windows versions, perform the procedure under “Configuring Microsoft Windows 2000”.

1. On the Windows taskbar, click **Start**, click **Control Panel**, and then select **Network and Internet** Icon.
2. Click **View Networks Status** and tasks and then click **Management Networks Connections**.
3. Right-click the **Local Area Connection** icon and click **Properties**.
4. Click **Continue**. The Local Area Connection Properties dialog box appears.
5. In the Local Area Connection Properties dialog box, verify that **Internet Protocol (TCP/IPv4)** is checked. Then select **Internet Protocol (TCP/IPv4)** and click the **Properties** button (see Figure 7). The Internet Protocol Version 4 Properties dialog box appears.



Connect using:

Broadcom NetXtreme Gigabit Ethernet

This connection uses the following items:

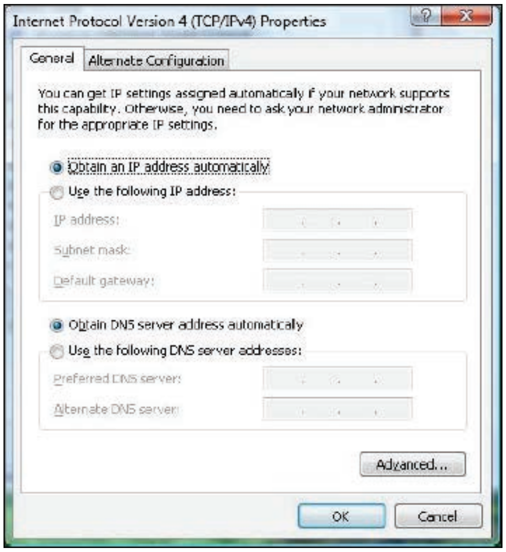
- ☑ SNIFFER Protocol Driver
- ☑ Reliable Multicast Protocol
- ☑ AEGIS Protocol (IEEE 802.1x) v2.3.1.6
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 7. Local Area Connection Properties Window

6. In the Internet Protocol Version 4 Properties dialog box, click **Obtain an IP address automatically** to configure your computer for DHCP (see Figure 8).



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

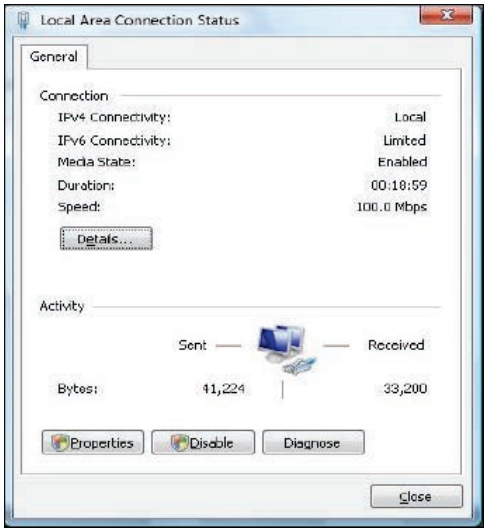
Preferred DNS server: . . .

Alternate DNS server: . . .

Figure 8. Internet Protocol Properties Window

7. Click the **OK** button to save your changes and close the dialog box.

8. Click the **OK** button again to save your changes (see Figure 9).



Connection

IPv4 Connectivity:	Local
IPv6 Connectivity:	Limited
Media State:	Enabled
Duration:	00:18:59
Speed:	100.0 Mbps

Activity

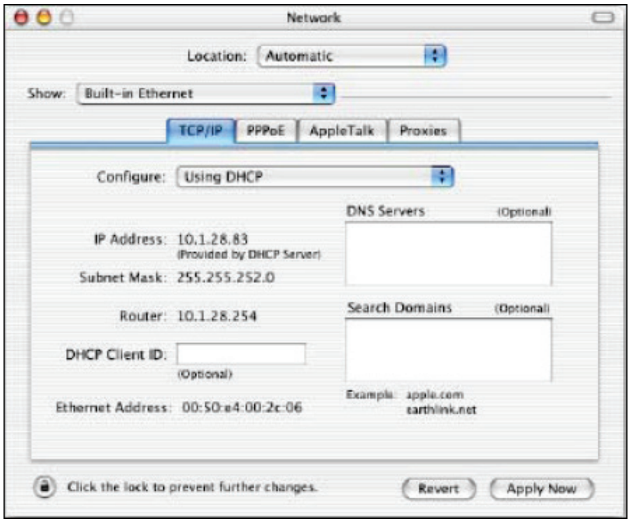
	Sent	Received
Bytes:	41,224	33,200

Figure 9. Local Area Connection Status Window

Configuring an Apple® Macintosh® Computer

The following procedure describes how to configure TCP/IP on an Apple Macintosh running Mac OS 10.2. If your Apple Macintosh is running Mac OS 7.x or later, the steps you perform and the screens you see may differ slightly from the following. However, you should still be able to use this procedure as a guide to configuring your Apple Macintosh for TCP/IP.

1. Pull down the Apple Menu, click **System Preferences**, and select **Network**.
2. Verify that NIC connected to the Gateway is selected in the **Show** field.
3. In the Configure field on the **TCP/IP** tab, select **Using DHCP** (see Figure 10).
4. Click **Apply Now** to apply your settings and close the TCP/IP dialog box.



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 10.1.28.83
(Provided by DHCP Server)

Subnet Mask: 255.255.252.0

Router: 10.1.28.254

DHCP Client ID:
(Optional)

Ethernet Address: 00:50:e4:00:2c:06

DNS Servers (Optional)

Search Domains (Optional)

Example: apple.com
earthlink.net

Figure 10. Selecting Using DHCP in the Configure Field

Disabling Proxy Settings

Before using the Gateway GUI, disable proxy settings in your Web browser. Otherwise, you will not be able to view the Gateway's Web-based configuration pages.

Disabling Proxy Settings in Internet Explorer

The following procedure describes how to disable proxy settings in Internet Explorer 5 and later.

1. Start Internet Explorer.
2. On your browser's **Tool** menu, click **Options**. The Internet Options dialog box appears.
3. In the Internet Options dialog box, click the **Connections** tab.
4. In the **Connections** tab, click the **LAN settings** button. The Local Area Network (LAN) Settings dialog box appears.
5. In the Local Area Network (LAN) Settings dialog box, uncheck all check boxes.
6. Click **OK** until the Internet Options window appears.
7. In the Internet Options window, under Temporary Internet Files, click Settings.
8. For the option Check for newer versions of stored pages, select Every time I visit the webpage.
9. Click **OK** until you close all open browser dialog boxes.

Disabling Proxy Settings in Firefox

The following procedure describes how to disable proxy settings in Firefox.

1. Start Firefox.
2. On your browser's **Tools** menu, click **Options**. The Options dialog box appears.
3. Click the **Advanced** tab.
4. In the Advanced tab, click the **Network** tab.
5. Click the **Settings** button.
6. Click **Direct connection to the Internet**.
7. Click the **OK** button to confirm this change.

Disabling Proxy Settings in Safari

The following procedure describes how to disable proxy settings in Safari.

1. Start Safari.
2. Click the Safari menu and select **Preferences**.
3. Click the **Advanced** tab.
4. In the **Advanced** tab, click the **Change Settings** button.
5. Choose your location from the **Location** list (this is generally **Automatic**).
6. Select your connection method. If using a wired connection, select **Built-in Ethernet**. For wireless, select **Airport**.
7. Click the **Proxies** tab.
8. Be sure each proxy in the list is unchecked.
9. Click **Apply Now** to finish.

Disabling Firewall and Security Software

Before configuring the Gateway using the Gateway GUI, disable any firewall or security software that may be running on your computer. For more information, refer to the documentation for your firewall.

Confirming Your Gateway's Link Status

Before configuring the Gateway using the Gateway GUI, confirm that the Ethernet Port's LED on the rear panel of the Gateway panel is ON. If the LED is OFF, replace the Ethernet cable connecting your computer and Gateway.

4 Configuring the Gateway

Topics:

- *Logging in to the Gateway’s Web Management Interface (page 20)*
- *Understanding the Web Management Interface Screens (page 21)*
- *Web Management Interface Menus (page 24)*

To configure the Gateway’s user settings, prepare your computer as described in Chapter 3. Then use the information in this chapter to configure the Gateway’s user settings.

Logging in to the Gateway's Web Management Interface

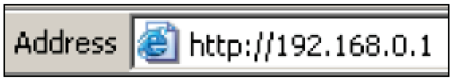
To access the Gateway's configuration settings, launch a Web browser (Microsoft Internet Explorer version 5.0 or later) on the computer you configured in Chapter 3 and log in to the Gateway's admin interface.

To access the Gateway's admin configuration settings, use the following procedure.

1. Launch a Web browser.

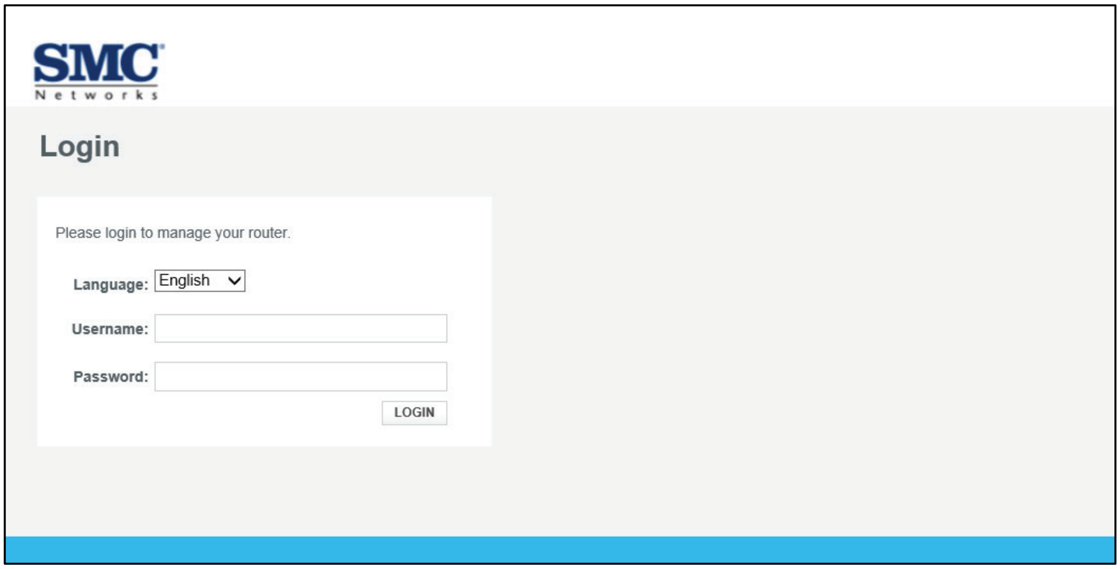
Note: Your computer does not have to be online to configure your Gateway.

2. In the browser address bar, type **http://192.168.0.1** and press the **Enter** key. For example:



Address http://192.168.0.1

The Login screen appears (see Figure 11).



SMC Networks

Login

Please login to manage your router.

Language: English

Username:

Password:

LOGIN

Figure 11. Login Screen

3. In the Login screen, use the **Language** drop-down box to select a language. The Web management interface will appear in the selected language after you log in.

4. In the **Username** and **Password** fields, enter the default user username and the default user password provided by SMC. Both the username and password are case sensitive. For security, each typed password character is masked as a dot (•).

   – Default username: **admin**

   – Default user password: **password**

Note: Your service provider may have customized your login credentials. Please check with your service provider for the appropriate username and password to use when logging in.

5. Click the **LOGIN** button to access the Gateway. The Web management interface starts and Step 1 of the Home Network Wizard appears (see page 51).

Tip: After you log in to the Web management interface, we recommend you change the default username and password on the **Gateway > Home Network Wizard** page (see page 51).

Understanding the Web Management Interface Screens

The left side of the management interface contains a menu bar for you to configure the Gateway. When you click a menu, information and any configuration settings associated with the menu appear in the workspace (see Figure 13). If the displayed information exceeds what can be shown in the workspace, scroll bars appear to the right of the workspace so you can scroll up and down through the information.

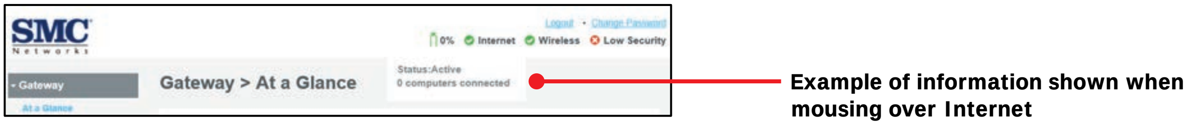
The top of the workspace shows the path (or “breadcrumbs”) associated with the information displayed in the workspace. For example, if you click the **Gateway** menu, **Gateway > At a Glance** appears at the top of the workspace.

The top-right area shows links for changing the login password and logging out of your current session.

Below the links are status icons that show the:

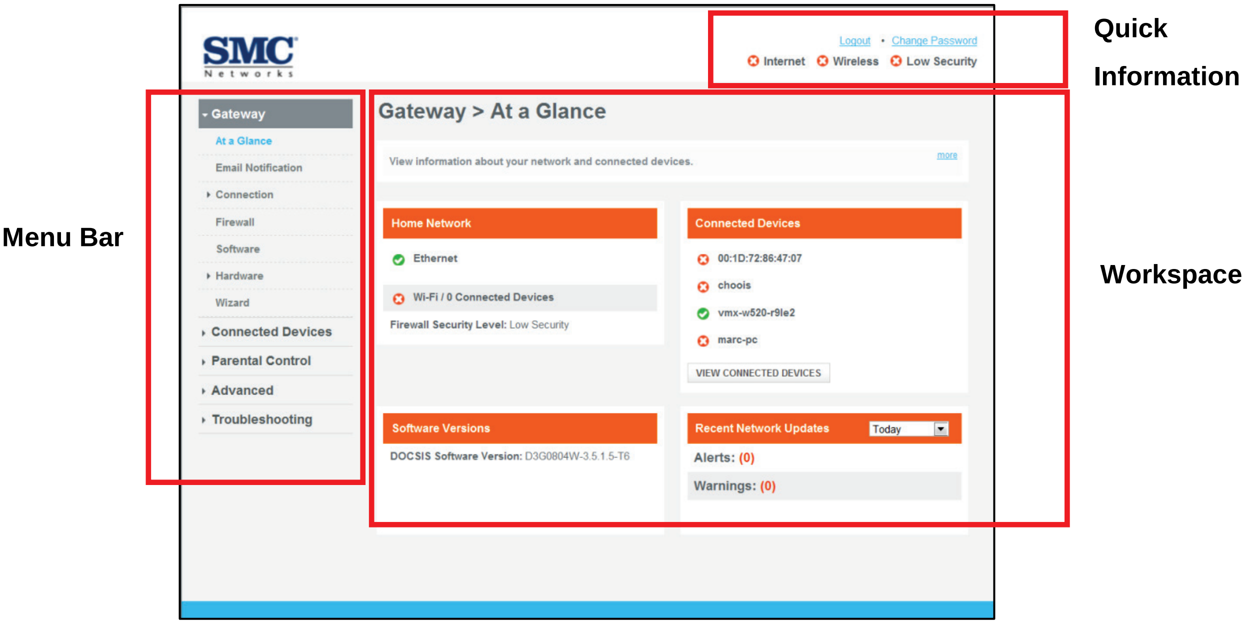
- Gateway’s Internet access
- Status of the Gateway’s wireless connection
- Custom security level

Moving the mouse over the **Internet**, **Wireless**, and **Security** level icons displays additional information. For example, hovering your mouse pointer over **Internet** displays the number of active computers connected to the Gateway (see Figure 12).


SMC Networks
Logout • Change Password
0% Internet Wireless Low Security
Gateway
At a Glance
Gateway > At a Glance
Example of information shown when mousing over Internet

Status:Active
0 computers connected

Figure 12. Example of Hovering Over the Internet Icon



View information about your network and connected devices.

Wi-Fi / 0 Connected Devices

Firewall Security Level: Low Security

DOCSIS Software Version: D3G0804W-3.5.1.5-T6

Alerts: (0)

Warnings: (0)

Figure 13. Main Areas on the Web Management Interface

All menus have submenus associated with them. If you click a menu in the menu bar, the submenus appear below it. For example, if you click the **Gateway** menu, the submenus **At a Glance**, **Email Notification**, **Connection**, **Firewall**, **Software**, **Hardware**, and **Wizard** appear below the **Gateway** menu (see Figure 14).

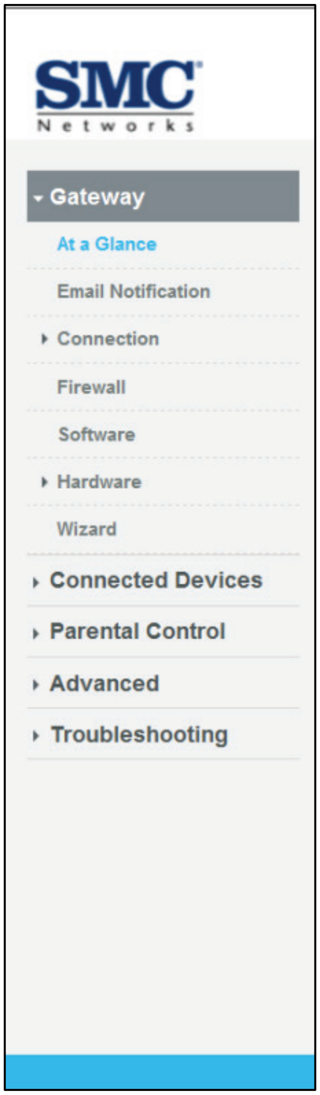


Figure 14. Example of Gateway Submenus

Web Management Interface Menus

Table 4 describes the pages in the Web management interface.

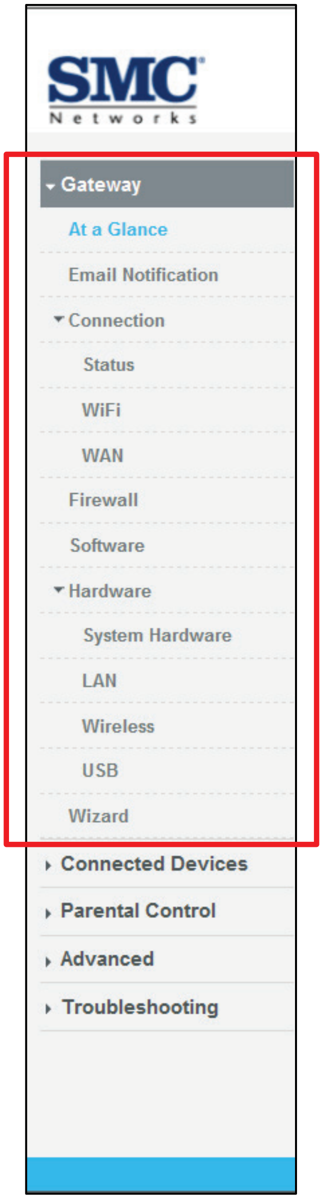
Table 4. Web Management Interface Menus and Submenus

Menus and Submenus	Description	See Page
Gateway > At a Glance	Reports information about your network, connected devices, software versions, and recent network updates.	27
Gateway > Email Notification	Lets you configure the Gateway to send email notifications when there is a firewall breach, parental control breach, alerts or warnings, or a request is made to send logs to a destination.	28
Gateway > Connection > Status	Lets you edit settings for the local IP network, and view the settings of the Wi-Fi network and XFINITY network.	30
Gateway > Connection > WiFi	Reports technical information specific to your Wi-Fi connection.	32
Gateway > Connection > WAN	Reports technical information about the Wide Area Network, cable modem, and downstream and upstream bonding values.	41
Gateway > Firewall	Configures the security level of the Gateway's internal firewall.	43
Gateway > Software	Reports system software and handset software information.	46
Gateway > Hardware > System Hardware	Reports information about the Gateway system hardware.	47
Gateway > Hardware > LAN	Reports link status and MAC address of the Gateway's four Gigabit Ethernet LAN ports.	48
Gateway > Hardware > Wireless	Reports connection status and MAC address of the wireless network.	49
Gateway > Hardware> USB	Reports status information about USB devices connected to the Gateway.	50
Gateway > Wizard	Runs the Home Network wizard to help you set up a home network.	51
Connected Devices > Computers	Reports computers connected to the Gateway's LAN.	55

Table 4. Web Management Interface Menus and Submenus

Menus and Submenus	Description	See Page
Parental Control > Managed Sites	Configures blocked sites, blocked keywords, and trusted computers.	57
Parental Control > Managed Services	Configures blocked services and trusted computers.	64
Parental Control > Managed Devices	Configures managed and blocked devices.	69
Parental Control > Reports	Generates, prints, and downloads reports based on user-defined criteria.	74
Advanced > Port Forwarding	Enables or disables the Gateway's port forwarding feature.	77
Advanced > Port Triggering	Enables or disables the Gateway's port triggering feature.	79
Advanced > DMZ	Configures a computer for unrestricted two-way Internet access.	82
Advanced > QoS	Configures the Gateway to deliver better resource reservation control.	84
Advanced > Device Discovery	Enables or disables the Gateway's Universal Plug and Play (UPnP) feature for dynamic connectivity to devices on the network.	86
Troubleshooting > Diagnostic Tools	Tests connectivity to an IP address.	89
Troubleshooting > Restore/Reboot	Reboots the Gateway, reboots the Wi-Fi router only, restores Wi-Fi settings only, or restores factory settings.	91
Troubleshooting > Change Password	Changes the password used to log in to the Gateway's Web interface.	92

Gateway Menu



The **Gateway** menu contains the following pages for performing basic Gateway configuration procedures:

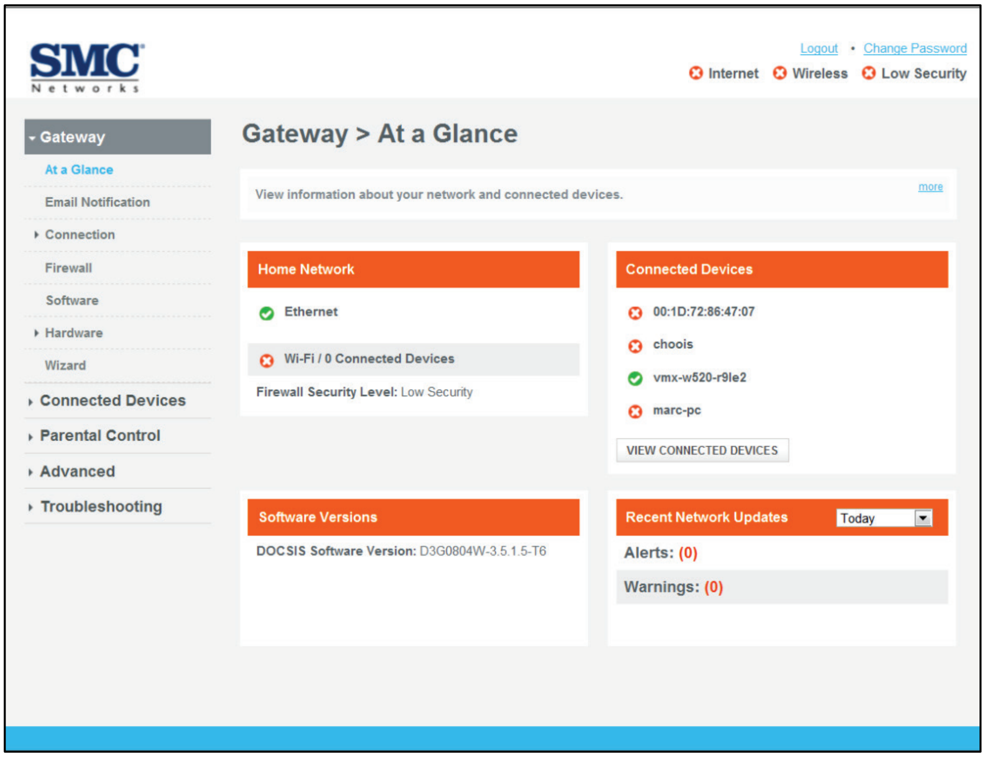
- **At a Glance** - view home network, connected devices, software versions, and recent network updates. See page 27.
- **Email Notification** - configures email notifications. See page 28.
- **Connection** – shows the following submenus:
  - **Status** - shows the Gateway network status. See page 30.
  - **WiFi** – configures the Gateway's Wi-Fi settings. See page 32.
  - **WAN** - shows WAN, cable modem, and downstream and upstream bonding values. See page 41.
- **Firewall** - configures the Gateway's internal firewall. See page 43.
- **Software** – shows eMTA and DOCSIS software version, and the packet cable modem name. See page 46.
- **Hardware** - contains the following submenus:
  - **System Hardware** - shows hardware information. See page 47.
  - **LAN** – shows link, duplex, and MAC address of the four Gigabit Ethernet LAN ports. See page 48.
  - **Wireless -** shows Wi-Fi link status and MAC address of the Gateway's 2.4 GHz and 5 GHz Wi-Fi LAN ports. See page 49.
  - **USB** - shows the device attached to the USB port. See page 50.
- **Wizard** – runs a wizard to configure a home network. See page 51.

At a Glance Page

Path: **Gateway > At a Glance**

The At a Glance page shows information about your network and connected devices. This page is organized into four areas:

- **Home Network** shows the connection status of Ethernet, wireless devices, and firewall security level.
- **Connected Devices** shows the MAC address of the devices connected to the Gateway. A **VIEW CONNECTED DEVICES** button opens the Computers page for viewing devices that the Gateway automatically detects using DHCP (see page 55).
- **Software Versions** shows the eMTA, DOCSIS software, and packet cable versions.
- **Recent Network Updates** shows alerts and warnings issued by the Gateway. A drop-down list lets you filter the information to show updates from today, yesterday, last week, last month, and the last 90 days.



Gateway > At a Glance

View information about your network and connected devices.

Home Network

✓ Ethernet

☒ Wi-Fi / 0 Connected Devices

Firewall Security Level: Low Security

Connected Devices

☒ 00:1D:72:86:47:07

☒ choois

✓ vmx-w520-r9le2

☒ marc-pc

Software Versions

DOCSIS Software Version: D3G0804W-3.5.1.5-T6

Recent Network Updates

Alerts: (0)

Warnings: (0)

Figure 15. At a Glance Page

Email Notifications Page

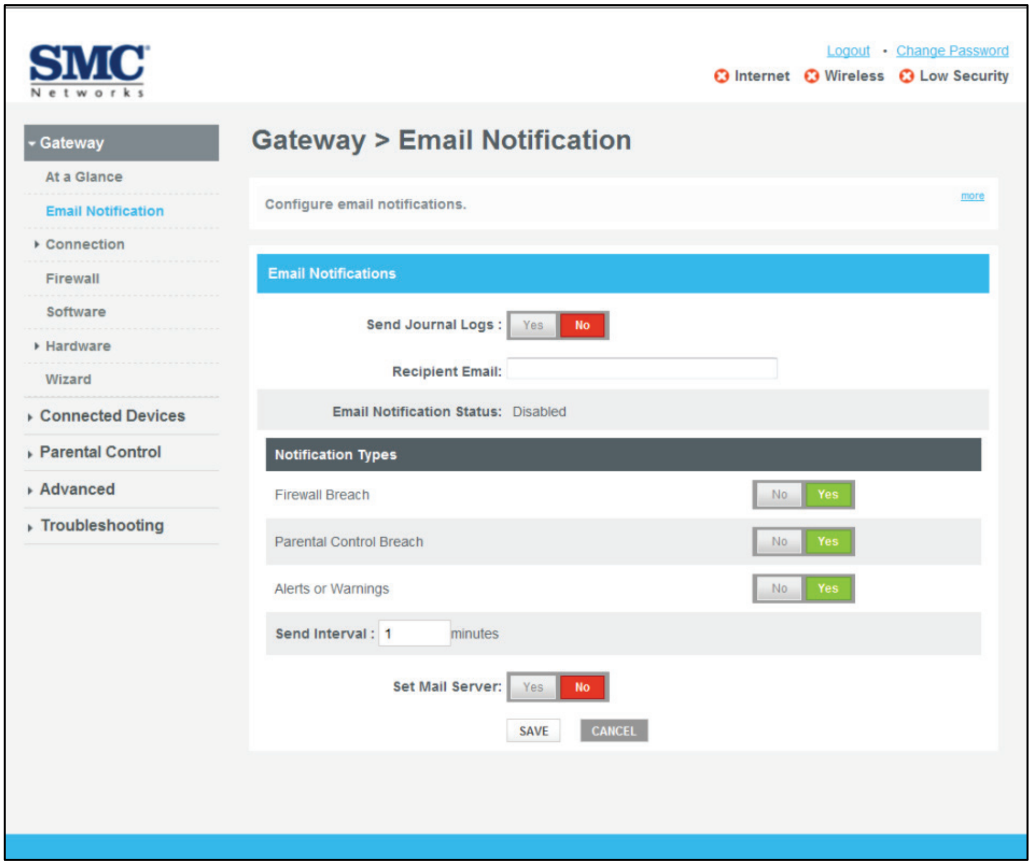
Path: **Gateway > Email Notification**

The Email Notification page lets you configure the Gateway to send email notifications automatically when any of the following events occurs:

- Firewall breach
- Parental control breach
- Alerts or warnings

This page also lets you receive logs along with email notifications.

Note: This configuration assumes that the Simple Mail Transfer Protocol (SMTP) mail server the Gateway will use is configured and operating properly.



Gateway > Email Notification

Configure email notifications.

Email Notifications

Send Journal Logs : Yes [✓ No]

Recipient Email:

Email Notification Status: Disabled

Notification Types

Firewall Breach No [✓ Yes]

Parental Control Breach No [✓ Yes]

Alerts or Warnings No [✓ Yes]

Send Interval : 1 minutes

Set Mail Server: Yes [✓ No]

Figure 16. Email Notification Page

Table 5. Email Notification Page Options

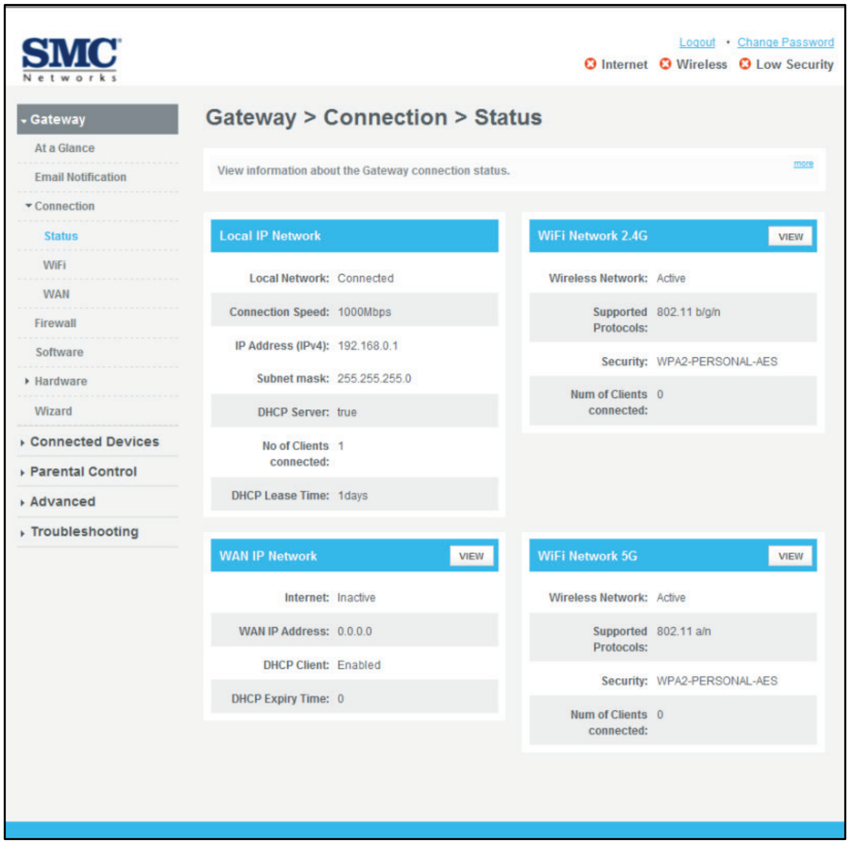
Option	Description
Email Notifications	
Send Journal Logs	Determines whether journal logs are sent along with the email notifications. • Yes = journal logs are sent with email notifications. If you select this option, complete the Recipient Email field and view the Email Notification Status field. • No = journal logs are not sent with email notifications.
Recipient Email	If you set Send Journal Logs to Yes, enter the email address of the person that will receive email notifications. To change email addresses, click the X at the right side of the field to delete the current email address, and then type a new address.
Email Notification Status	A read-only field that shows the status of your email notification configuration.
Notification Types	
Firewall Breach	Determines whether the Gateway sends email notifications if an attempt was made to breach the firewall. • Yes = email notification is sent. If you set Send Journal Logs to Yes, the journal logs accompany the email notification; otherwise, only the email notification is sent. • No = email notification is not sent.
Parental Control Breach	Determines whether the Gateway sends email notifications if an attempt was made to breach a parental control. • Yes = email notification is sent. If you set Send Journal Logs to Yes, the journal logs accompany the email notification; otherwise, only the email notification is sent. • No = email notification is not sent.
Alerts or Warnings	Determines whether the Gateway sends email notifications if an alert or warning occurred that requires attention. • Yes = email notification is sent. If you set Send Journal Logs to Yes, the journal logs accompany the email notification; otherwise, only the email notification is sent. • No = email notification is not sent.
Send Interval	Specifies the minimum time, in minutes, between different notifications. This option prevents more than one notification in a short time for the same event.
Set Mail Server	Enables or disables the Gateway's internal mail server. To receive email notifications and journal logs, the mail server must be enabled. • Yes = Gateway mail server is enabled. Complete the SMTP Server Address, Server Username, and SMTP Password fields. • No = Gateway mail server is disabled.
SMTP Server Address	If you set Enable Set Mail Server to Yes, enter the SMTP server address of your email server.
SMTP Username	If you set Enable Set Mail Server to Yes, enter the SMTP username used to log into the server.
SMTP Password	If you set Enable Set Mail Server to Yes, enter the SMTP password used to log into the server. For security, each typed password character is masked as a dot (•).
SAVE Button	After configuring the settings on this page, click this button to save your settings.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.

Status Page

Path: **Gateway > Connection > Status**

The Status page displays information about the Gateway’s connection status. This page is organized into four areas:

- **Local IP Network** shows the local network status, connection speed, IPv4 address, subnet mask, DHCP server status, number of clients connected, and DHCP lease time.
- **WiFi Network 2.4G** shows the status, protocols, security type, and number of connected wireless clients on the wireless 2.4G network. A **VIEW** button lets you view Wi-Fi LAN port information (see “Wireless Hardware Info Page” on page 49).
- **WAN IP Network** shows the Internet connection status, WAN IP address, DHCP client status, and DHCP expiration time. A **VIEW** button lets you view information about the Wide Area Network connection (see “WAN Page” on page 41).
- **WiFi Network 5G** shows the status, protocols, security type, and number of connected wireless clients on the wireless 5G network. A **VIEW** button lets you view Wi-Fi LAN port information (see “Wireless Hardware Info Page” on page 49).



Gateway > Connection > Status

View information about the Gateway connection status.

Local IP Network

Local Network:	Connected
Connection Speed:	1000Mbps
IP Address (IPv4):	192.168.0.1
Subnet mask:	255.255.255.0
DHCP Server:	true
No of Clients connected:	1
DHCP Lease Time:	1days

WiFi Network 2.4G

Wireless Network:	Active
Supported Protocols:	802.11 b/g/n
Security:	WPA2-PERSONAL-AES
Num of Clients connected:	0

WAN IP Network

Internet:	Inactive
WAN IP Address:	0.0.0.0
DHCP Client:	Enabled
DHCP Expiry Time:	0

WiFi Network 5G

Wireless Network:	Active
Supported Protocols:	802.11 a/n
Security:	WPA2-PERSONAL-AES
Num of Clients connected:	0

Figure 17. Status Page

WiFi Page

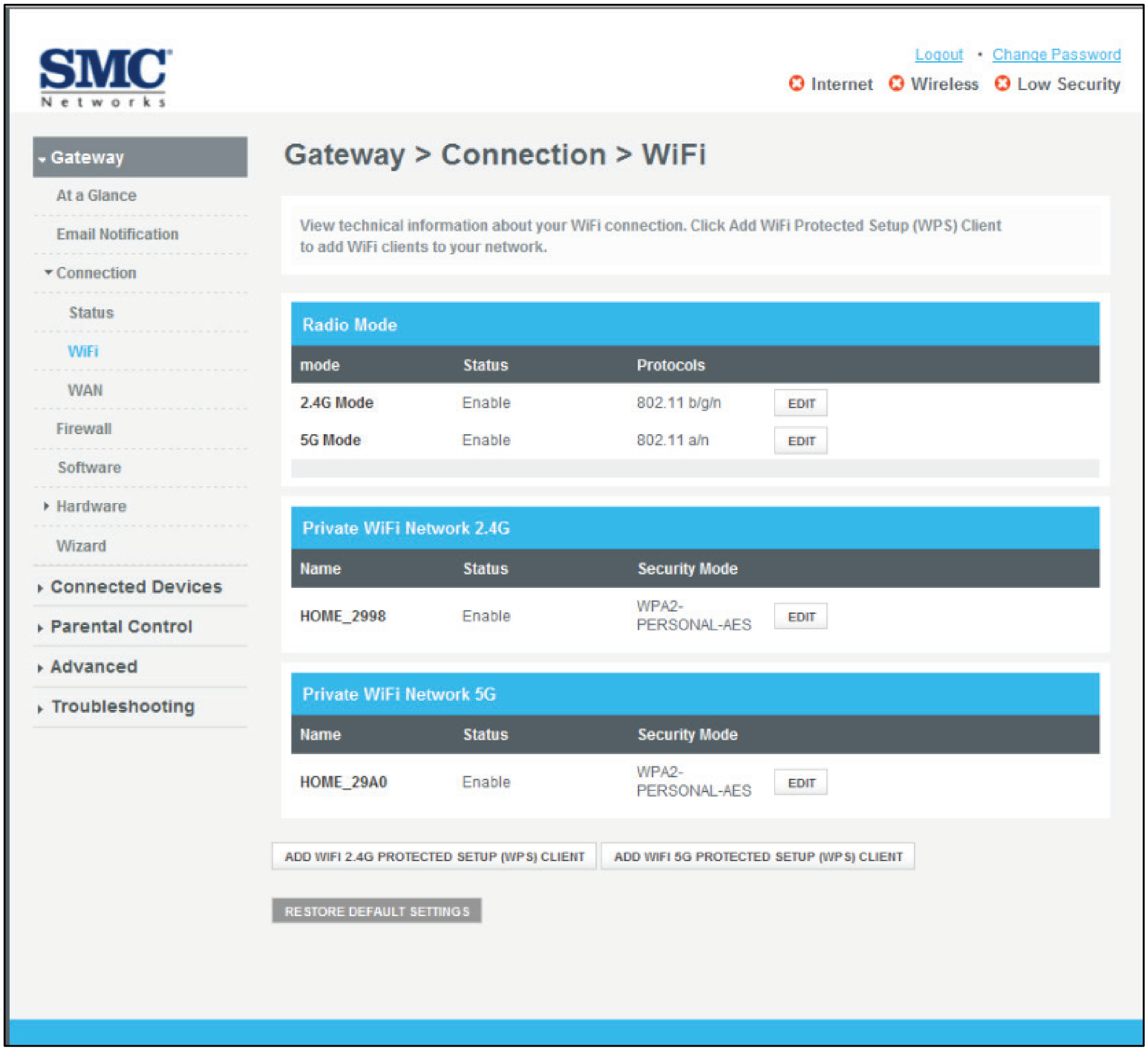
Path: **Gateway > Connection > WiFi**

The WiFi page shows advanced information about the Gateway’s Wi-Fi connections. This page is organized into the following areas:

- **Radio Mode** shows the mode, status, and protocols configured for the Gateway’s 2.4 GHz and 5 GHz wireless radios.
  - An **EDIT** button lets you configure the Gateway’s basic Wi-Fi network settings. See “Editing Basic Radio Mode Setting” on page 34.
- **Private WiFi Network 2.4G** shows the name of the 2.4G Wi-Fi network to which the Gateway is connected, along with the status and security mode of the Gateway’s Wi-Fi network connection.
  - An **EDIT** button lets you configure the private 2.4G Wi-Fi network configuration settings and MAC filter settings. See “Editing Private Wi-Fi Network Settings” on page 36.
- **Private WiFi Network 5G** shows the name of the 5G Wi-Fi network to which the Gateway is connected, along with the status and security mode of the Gateway’s Wi-Fi network connection.
  - An **EDIT** button lets you configure the private 5G Wi-Fi network configuration settings and MAC filter settings. See “Editing Private Wi-Fi Network Settings” on page 36.

ADD WIFI 2.4G PROTECTED SETUP (WPS) CLIENT and **ADD WIFI 5G PROTECTED SETUP (WPS) CLIENT** buttons at the bottom of the page lets you enable or disable WPS for these networks, add wireless clients, and unlock a WPS 2 lock condition (see “Configuring WPS Settings” on page 39).

A **RESTORE DEFAULT SETTINGS** at the bottom of the page returns the Gateway to its default factory settings.



Gateway > Connection > WiFi

View technical information about your WiFi connection. Click Add WiFi Protected Setup (WPS) Client to add WiFi clients to your network.

Radio Mode

mode	Status	Protocols	
2.4G Mode	Enable	802.11 b/g/n	EDIT
5G Mode	Enable	802.11 a/n	EDIT

Private WiFi Network 2.4G

Name	Status	Security Mode	
HOME_2998	Enable	WPA2-PERSONAL-AES	EDIT

Private WiFi Network 5G

Name	Status	Security Mode	
HOME_29A0	Enable	WPA2-PERSONAL-AES	EDIT

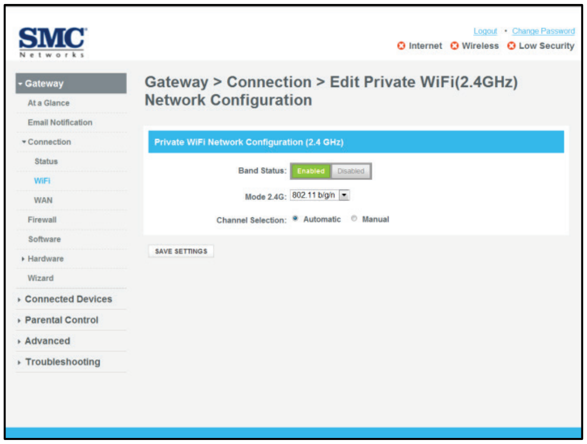
Figure 18. WiFi Page

Editing Basic Radio Mode Settings

The **Radio Mode** area of the WiFi page provides an **EDIT** button for editing basic settings for the Gateway's 2.4 GHz and 5 GHz wireless radios.

The following procedure describes how to change the basic radio mode settings for the Gateway's wireless radios. Separate **EDIT** buttons are provided for the Gateway's 2.4 GHz and 5 GHz radios.

1. Under **Radio Mode**, click the **EDIT** button next to the appropriate radio:
   - For 2.4 GHz Wi-Fi radio settings, a page similar to the left page in Figure 19 appears.
   - For 5 GHz Wi-Fi radio settings, a page similar to the right page in Figure 19 appears.
2. Complete the options in the page (see Table 6 on page 35).
3. Click **SAVE SETTINGS**.



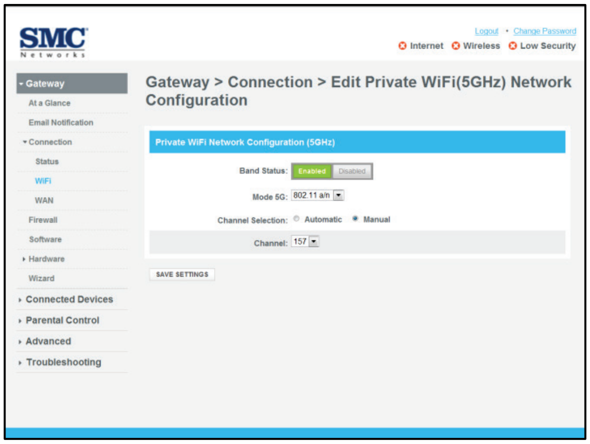
Gateway > Connection > Edit Private WiFi(2.4GHz) Network Configuration

Private WiFi Network Configuration (2.4 GHz)

Band Status: Enabled Disabled

Mode 2.4G: 802.11 b/g/n

Channel Selection: ● Automatic ○ Manual



Gateway > Connection > Edit Private WiFi(5GHz) Network Configuration

Private WiFi Network Configuration (5GHz)

Band Status: Enabled Disabled

Mode 5G: 802.11 a/n

Channel Selection: ○ Automatic ● Manual

Channel: 157

2.4 GHz Page

5 GHz Page

Figure 19. Edit Private WiFi Network Configuration Pages

Table 6. Edit Private WiFi Network Configuration Options

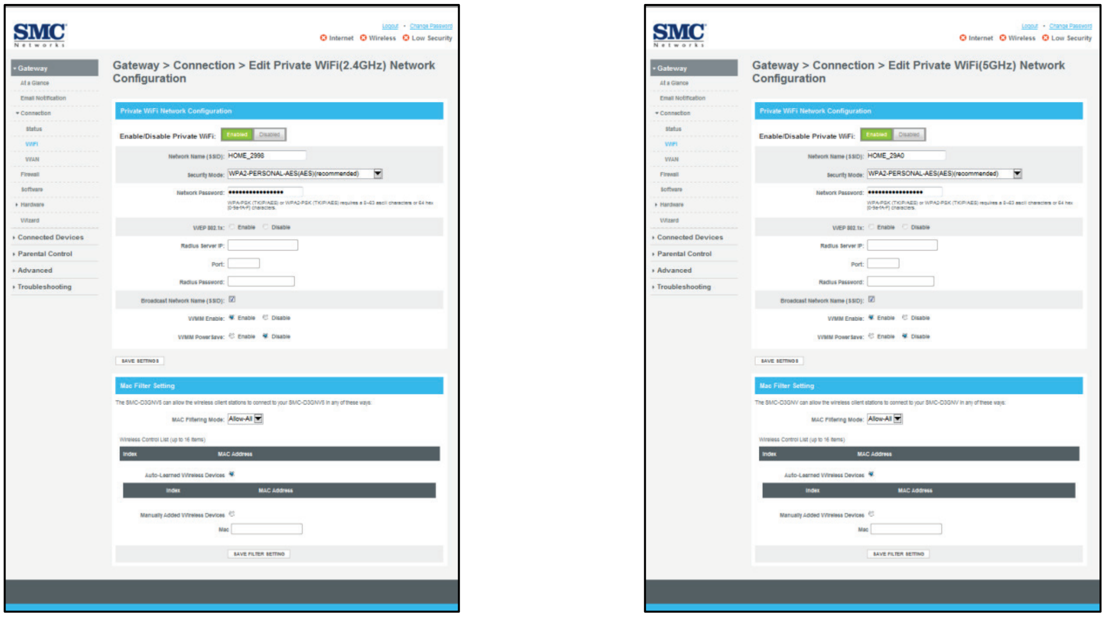
Option	Description
Band Status	Enables or disables the Gateway's 2.4 GHz or 5 GHz radio. • If you clicked the EDIT button for 2.4G, enable or disable the Gateway's 2.4 GHz radio. • If you clicked the EDIT button for 5G, enable or disable the Gateway's 5 GHz radio.
Mode Mode 2.4G Mode 5G	Use this field to select the Gateway wireless mode: If you clicked the EDIT button for 2.4G, choices are: • 802.11 b = select this setting if your wireless network consists of IEEE 802.11b devices only. • 802.11 g = select this setting if your wireless network consists of IEEE 802.11g devices only. • 802.11 n = select this setting if your wireless network consists of IEEE 802.11n devices only. • 802.11 b/g = select this setting if your wireless network consists of IEEE 802.11b and 802.11g devices. • 802.11 g/n = select this setting if your wireless network consists of IEEE 802.11g and 802.11n devices. • 802.11 b/g/n = select this setting if your wireless network consists of IEEE 802.11b, 802.11g, and 802.11n devices. If you clicked the EDIT button for 5G, choices are: • 802.11 a = select this setting if your wireless network consists of IEEE 802.11a devices only. • 802.11 a/n = select this setting if your wireless network consists of IEEE 802.11a and 802.11n devices.
Channel Selection	Select how the Gateway will select a channel for communicating over the wireless network. Choices are: • Automatic = the Gateway selects the channel automatically. • Manual = the Gateway uses the channel specified in the Channel option.
Channel	If Channel Selection is set to Manual, select a channel on which the radio is to operate. This option does not appear when Channel Selection is set to Automatic.
SAVE SETTINGS Button	After configuring the settings on this page, click this button to save your settings.

Editing Private Wi-Fi Network Settings

The **Private WiFi Network 2.4G** and **Private WiFi Network 5G** areas of the WiFi page provide an **EDIT** button for editing private Wi-Fi network settings.

- The **EDIT** button under **Private WiFi Network 2.4G** displays the same page for configuring the Gateway’s 2.4 GHz Wi-Fi network settings.
- The **EDIT** button under **Private WiFi Network 5G** displays the same page for configuring the Gateway’s 5 GHz Wi-Fi network settings.

1. Under **Private WiFi Network 2.4G or Private WiFi Network 5G** on the WiFI page, click the **EDIT** button next to the appropriate radio:
   – For 2.4 GHz Wi-Fi network settings, a page similar to the left page in Figure 20 appears.
   – For 5 GHz Wi-Fi network settings, a page similar to the right page in Figure 20 appears.
2. Complete the options in the page (see Table 7).
3. Click **SAVE SETTINGS**.



Gateway > Connection > Edit Private WiFi(2.4GHz) Network Configuration

Private WiFi Network Configuration

Enable/Disable Private WiFi: [✓ Enabled] Disabled

Network Name (SSID): HOME_2998

Security Mode: WPA2-PERSONAL-AES(AES)(recommended)

Network Password: ●●●●●●●●●●●●●●●●

WPA-PSK (TKIP/AES) or WPA2-PSK (TKIP/AES) requires a 8-63 ascii characters or 64 hex (0-9a-fA-F) characters.

WEP 802.1x: ○ Enable ○ Disable

Radius Server IP:

Port:

Radius Password:

Broadcast Network Name (SSID): ☑

WMM Enable: ● Enable ○ Disable

WMM Power Save: ○ Enable ● Disable

SAVE SETTINGS

Mac Filter Setting

The SMC-D3GNV5 can allow the wireless client stations to connect to your SMC-D3GNV5 in any of these ways:

MAC Filtering Mode: Allow-All

Wireless Control List (up to 16 items)

Index	MAC Address

Auto-Learned Wireless Devices ●

Index	MAC Address

Manually Added Wireless Devices ○

Mac

SAVE FILTER SETTING

2.4 GHz Page

Gateway > Connection > Edit Private WiFi(5GHz) Network Configuration

Private WiFi Network Configuration

Enable/Disable Private WiFi: [✓ Enabled] Disabled

Network Name (SSID): HOME_29A0

Security Mode: WPA2-PERSONAL-AES(AES)(recommended)

Network Password: ●●●●●●●●●●●●●●●●

WPA-PSK (TKIP/AES) or WPA2-PSK (TKIP/AES) requires a 8-63 ascii characters or 64 hex (0-9a-fA-F) characters.

WEP 802.1x: ○ Enable ○ Disable

Radius Server IP:

Port:

Radius Password:

Broadcast Network Name (SSID): ☑

WMM Enable: ● Enable ○ Disable

WMM Power Save: ○ Enable ● Disable

SAVE SETTINGS

Mac Filter Setting

The SMC-D3GNV can allow the wireless client stations to connect to your SMC-D3GNV in any of these ways:

MAC Filtering Mode: Allow-All

Wireless Control List (up to 16 items)

Index	MAC Address

Auto-Learned Wireless Devices ●

Index	MAC Address

Manually Added Wireless Devices ○

Mac

SAVE FILTER SETTING

5 GHz Page

Figure 20. Edit Private WiFi Network Configuration Pages

Table 7. Edit Private WiFi Network Configuration Page Options

Option	Description
Private WiFi Network Configuration	
Enable/Disable Private WiFi	Enables or disables the Gateway's private Wi-Fi 2.4/5 GHz band operation.
Network Name (SSID)	Enter a name for the wireless network. The Wi-Fi name will make it more obvious for other devices to know which network they are connecting to.
Security Mode	To prevent other computers in the area from using your Internet connection, secure your wireless network by selecting an encryption method from this drop-down list. There are several selections available, including the following. (Risky appears next to selections that provide little or no protection.) • OPEN = wireless transmissions are not protected. • WEP = basic encryption and therefore least secure (i.e., it can be easily cracked, but is compatible with a wide range of devices including older hardware). WEP 64- and 128-bit selections are provided. • WPA–PERSONAL–TKIP (TKIP) = a Wi-Fi standard that is stronger than WEP encryption. This selection uses Temporal Key Integrity Protocol (TKIP) encryption to provide protection against hackers. If you use WPA, each device in your wireless network must use the same WPA method and network password, or the network will not work properly. • WPA2-PERSONAL = several versions are provided. Some use TKIP encryption, while others use Advanced Encryption System (AES), which utilizes a symmetric 128-bit block data encryption. WPA2 Personal is stronger than WPA encryption. Each device in your wireless network must use the same WPA method and network password, or the network will not work properly. • WPA-ENTERPRISE = this option uses WPA and should be used with a RADIUS server connected to the Gateway. Each device in your wireless network must use the same WPA method and network password, or the network will not work properly. This setting requires a RADIUS server to be connected to the Gateway. • WPA2-ENTERPRISE = this option uses WPA2 and should be used with a RADIUS server connected to the Gateway. WPA2-ENTERPRISE supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP. Each device in your wireless network must use the same WPA method and network password, or the network will not work properly. This setting requires a RADIUS server to be connected to the Gateway. • WPA-WPA2-ENTERPRISE = allows your devices to connect using the strongest security option they support, WPA or WPA2. Each device in your wireless network must use the same WPA method and network password, or the network will not work properly. This setting requires a RADIUS server to be connected to the Gateway.
Network Password	If you select one of the WEP, WPA, or WPA2 encryption settings, enter the case-sensitive password used for encryption and decryption. For security, each typed password character is masked as a dot (•). If you specify a hexadecimal password, use the letters A to F and numbers 0 to 9. • WEP 64 requires a 5 ASCII character or 10 hexadecimal character password. • WEP 128: requires a 13 ASCII character or 16 hexadecimal character password. • Remaining encryption methods require at least an 8 ASCI- character or a 64 hexadecimal character password.
WEP 802.1x	If Security Mode is set to one of the WEP options, use this option to enable or disable WEP 802.1x. WEP 802.1x is a robust security protocol that uses port control with dynamically changing encryption keys automatically updated over the network. WEP 802.11x uses a Remote Authentication Dial-in Service (RADIUS) server for authentication purposes. This server must be physically connected to the Gateway. If you enable this option, set the next three RADIUS options.
Radius Server IP	If WEP 802.1x is enabled, enter the IP address of the RADIUS server.
Port	If WEP 802.1x is enabled, enter the port number of the RADIUS server.
Radius Password	If WEP 802.1x is enabled, enter the password of the RADIUS server.
Broadcast Network Name (SSID)	Check to enable broadcasting of the SSID. When wireless devices survey wireless networks with which to associate, they will detect the SSID broadcast by the Gateway. If enabled, the SSID of the Gateway's wireless network will be broadcast wirelessly.

Option	Description
WMM Enable	Wi-Fi Multimedia (WMM) WMM uses a protocol called Enhanced Distributed Channel Access (EDCA) to prioritize traffic on the wireless network. Enabling this setting helps with streaming applications such as audio, video, and voice over wireless connections if the destination wireless device also supports WMM. For example: • In a Voice Over IP (VoIP) phone conversation, you are less likely to hear delays. • Watching video, you are more likely to see smooth action. This delays other network traffic of a less critical nature, such as downloading large files, where a small delay is acceptable.
WMM Power Save	Enables or disables WMM power save. WMM Power Save provides advanced power savings and is optimized for latency-sensitive applications, such as VOIP Internet telephony applications and applications that pass audio and video traffic. WMM Power Save uses fewer frames to transmit the same amount of data in a shorter time, and extends the time devices can remain in a low-power state.
SAVE SETTINGS Button	After configuring the Private WiFi Network Configuration settings on this page, click this button to save your settings.
Mac Filter Setting	
Mac Filtering Mode	The Media Access Control (MAC) address filtering mode controls network access based on the MAC address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to allow all, allow, or deny network/Internet access to devices based on their MAC address. The MAC address can be automatically learned by the Gateway or manually specified using the options under Index MAC Address. Use this drop-down list to select the method used by the client stations to connect to the Gateway. Choices are: • Allow-All = allow all wireless stations to join (authenticate with) the Wi-Fi network. • Allow = allow only the auto-learned or manually added MAC address specified under Index MAC Address to join the Wi-Fi network. • Deny = prevent the auto-learned or manually added MAC address specified under Index MAC Address from joining the Wi-Fi network.
Index MAC Address	Specify how the MAC filter list is filled. Choices are: • Auto-Learned Wireless Devices = the Gateway learns the MAC addresses of the devices whose presence it has automatically learned. • Manually Added Wireless Devices = enter the MAC address of the device.
SAVE FILTER SETTING Button	After configuring the Mac Filter Settings on this page, click this button to save your settings.

Configuring WPS Settings

The WIFI page provides two buttons for configuring WPS settings:

- **ADD WIFI 2.4G PROTECTED SETUP (WPS) CLIENT** lets you configure WPS settings for the Gateways 2.4 GHz wireless radio.
- **ADD WIFI 5G PROTECTED SETUP (WPS) CLIENT** lets you configure WPS settings for the Gateways 5 GHz wireless radio.

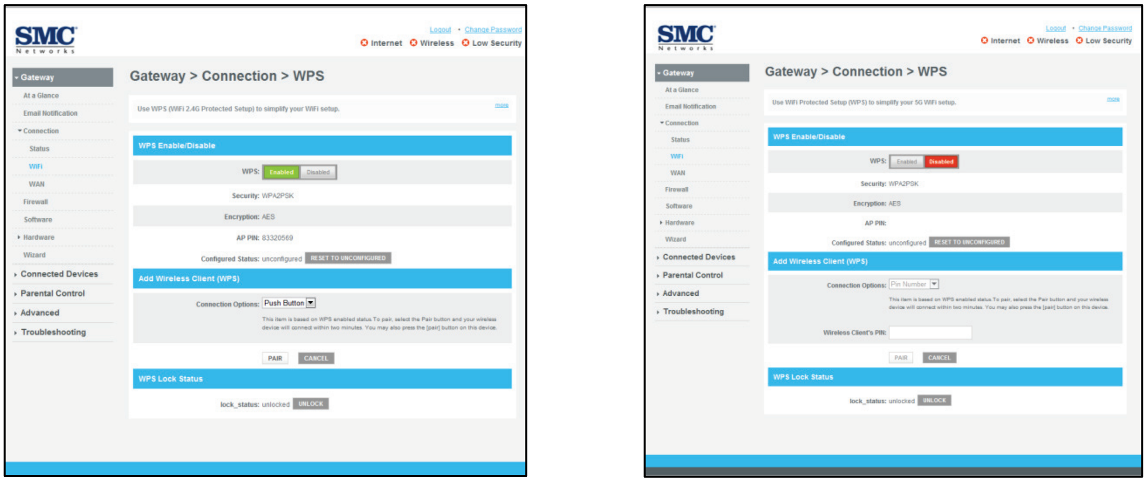
The WPS settings for the 2.4 GHz and 5 GHz wireless radios are the same.

You can also display these pages by clicking **ADD WIFI PROTECTED SETUP (WPS 2.4G) CLIENT** or **ADD WIFI PROTECTED SETUP (WPS 5G) CLIENT** from the Connected Devices > Computers page.

Note: You must enable WPS before a wireless device can connect to the Gateway using WPS.

To configure WPS settings:

1. Click the appropriate **ADD WIFI PROTECTED SETUP (WPS) CLIENT** button for the wireless radio you want to configure:
   - – For 2.4 GHz Wi-Fi radio settings, a page similar to the left page in Figure 21 appears.
   - – For 5 GHz Wi-Fi radio settings, a page similar to the right page in Figure 21 appears.
2. Complete the options in the WPS page (see Table 8).



Gateway > Connection > WPS

Use WPS (WiFi 2.4G Protected Setup) to simplify your WiFi setup.

WPS: Enabled

Security: WPA2PSK

Encryption: AES

AP PIN: 83320569

Configured Status: unconfigured

Connection Options: Push Button

This item is based on WPS enabled status. To pair, select the Pair button and your wireless device will connect within two minutes. You may also press the [pair] button on this device.

lock_status: unlocked

2.4 GHz Page

Gateway > Connection > WPS

Use WiFi Protected Setup (WPS) to simplify your 5G WiFi setup.

WPS: Disabled

Security: WPA2PSK

Encryption: AES

AP PIN:

Configured Status: unconfigured

Connection Options: Pin Number

This item is based on WPS enabled status. To pair, select the Pair button and your wireless device will connect within two minutes. You may also press the [pair] button on this device.

Wireless Client's PIN:

lock_status: unlocked

5 GHz Page

Figure 21. WPS Pages

Table 8. WPS Page Options

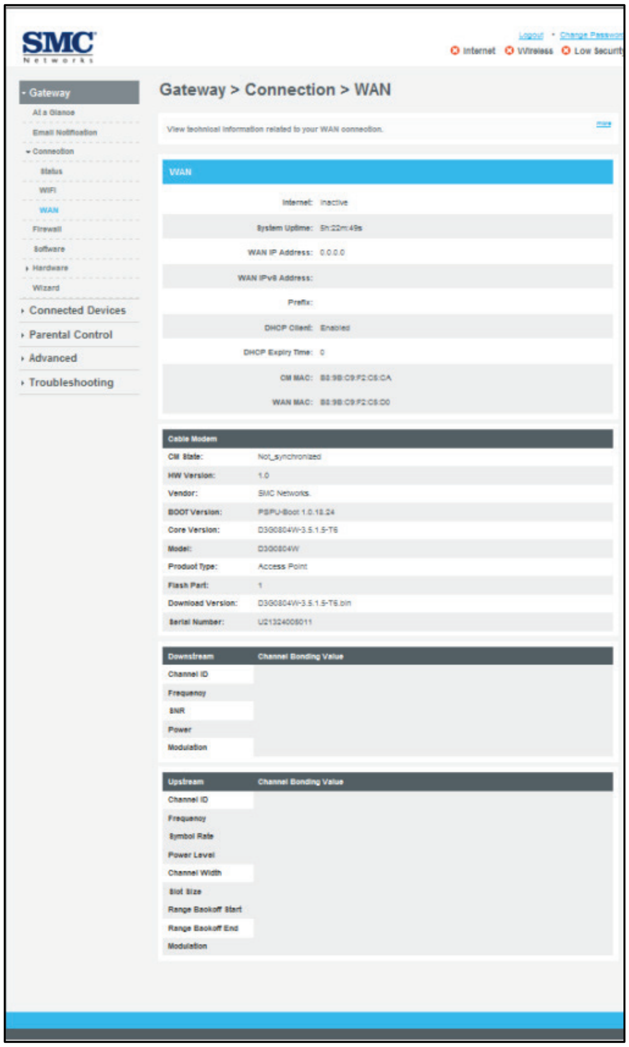
Option	Description
WPS Enable/Disable	
WPS	Enables or disables WPS. If you click Enabled, complete the remaining fields on the page.
Security	A read-only field that shows the Gateway's security settings.
Encryption	A read-only field that shows the Gateway's encryption settings.
AP PIN	A read-only field that shows the Access Point's personal identification number.
Configured Status	A read-only field that shows the configuration status of the Gateway. Clicking RESET TO UNCONFIGURED resets the WPS settings.
Add Wireless Client (WPS)	
Connection Options	Select the method used to make the Wi-Fi Protected Setup (WPS) connection between wireless devices and the Gateway. Choices are: • Push Button = select this option to use the WPS button on the front panel of the Gateway and the wireless device to make the connection. • Pin Number = a PIN is a unique number that can be used to add a client to an existing network or to create a new network. Select this option to enter an 8-digit PIN to configure WPS. Then, enter the same 8-digit PIN in both the Wireless Client's PIN field and at the wireless client to make the wireless connection.
Wireless Client's PIN	If Connection Options is set to Pin Number, enter the PIN used with the wireless client to make the wireless connection. This option does not appear if Connection Options is set to Push Button.
PAIR Button	If Connection Options is set to Push Button, click this button and push the WPS button on the wireless client to create the wireless connection. The wireless connection is made within two minutes. You can also press the WPS button on the front panel of this Gateway to initiate WPS instead of clicking the PAIR button.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.
WPS Lock Status	
lock_status	A read-only field that shows the Gateway's lock status. WPS is a method for setting up a new wireless Gateway using a push button or PIN.WPS has a vulnerability that makes a PIN susceptible to brute force attempts. The Gateway protects itself after several failed attempts to authenticate via a PIN by entering a lock state. During the lock state, all WPS attempts using the Gateway PIN will not work. While the Gateway is in a lock state, users can still use the WPS button method to connect to the wireless network. Clicking UNLOCK returns the Gateway from the lock state.

WAN Page

Path: **Connection > WAN**

The WAN page shows information about the Wide Area Network, cable modem, and downstream and upstream bonding values. This information is useful when contacting Customer Center or troubleshooting technical problems.

Note: This page is also available from the Status page by clicking the **VIEW** button in the **WAN IP Network** area.



Gateway > Connection > WAN

View technical information related to your WAN connection.

WAN

Internet: Inactive

System Uptime: 5h:22m:49s

WAN IP Address: 0.0.0.0

WAN IPv6 Address:

Prefix:

DHCP Client: Enabled

DHCP Expiry Time: 0

CM MAC: B8:9B:C9:F2:C5:CA

WAN MAC: B8:9B:C9:F2:C5:D0

Cable Modem	
CM State:	Not_synchronized
HW Version:	1.0
Vendor:	SMC Networks.
BOOT Version:	PSPU-Boot 1.0.18.24
Core Version:	D3G0804W-3.5.1.5-T6
Model:	D3G0804W
Product Type:	Access Point
Flash Part:	1
Download Version:	D3G0804W-3.5.1.5-T6.bin
Serial Number:	U21324008011

Downstream	Channel Bonding Value
Channel ID	
Frequency	
SNR	
Power	
Modulation	

Upstream	Channel Bonding Value
Channel ID	
Frequency	
Symbol Rate	
Power Level	
Channel Width	
Slot Size	
Range Backoff Start	
Range Backoff End	
Modulation	

Figure 22. WAN Page

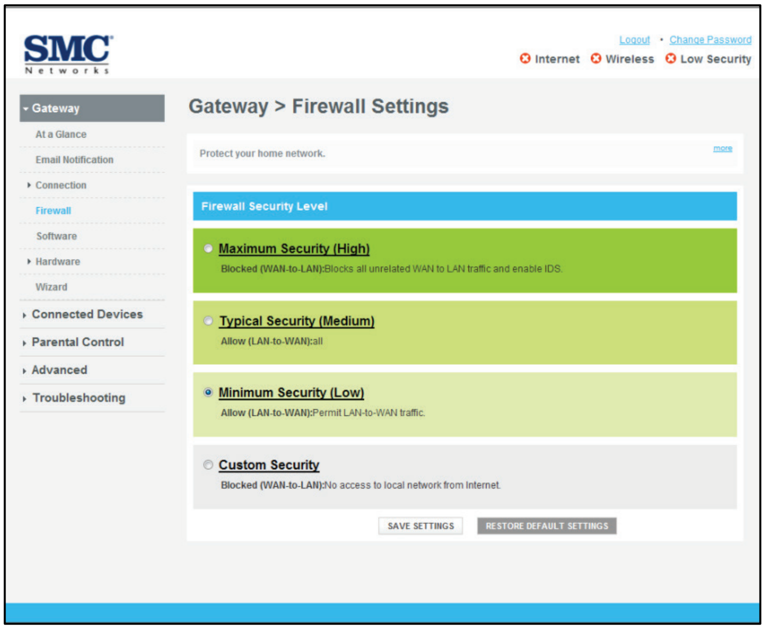
Table 9. WAN Page Options

Option	Description
WAN	
Internet	A read-only field that shows the Internet connection status.
System Uptime	A read-only field that shows the system uptime counting from its bootup.
WAN IP Address	A read-only field that shows the WAN IP v4 address obtained from the service provider.
WAN IPv6 Address	A read-only field that shows the WAN IP v6 address obtained from the service provider.
Prefix	A read-only field that shows the IPv6 prefix length.
DHCP Client	A read-only field that shows the DHCP Client function is enable or disable.
DHCP Expiry Time	A read-only field that shows the expired time currently left of DHCP client. Once the time expires, the configuration might stop working.
CM MAC	A read-only field that shows the MAC address of the CM.
WAN MAC	A read-only field that shows the MAC address of the Gateway's WAN interface.
Cable Modem	
Read-only fields that show technical information related to your cable modem, such as the hardware version, vendor, and boot and core versions.	
Downstream Channel Bonding Value	
Downstream channel bonding lets the Gateway receive downstream traffic on multiple downstream channels. These read-only fields show the downstream channel bonding values, such as channel ID, frequency, signal-to-noise ratio, power, and modulation.	
Upstream Channel Bonding Value	
Upstream channel bonding is a way to increase upstream bandwidth by transmitting data on multiple upstream channels simultaneously. These read-only fields show the upstream channel bonding values, such as channel ID, frequency, power level, range backoff start and end, and modulation.	

Firewall Settings Page

Path: **Gateway > Firewall**

The Gateway includes a built-in firewall whose security level can be selected using the Firewall Settings page. Security levels range from minimum (low security) to maximum (high security).



Gateway > Firewall Settings

Protect your home network.

Firewall Security Level

○ Maximum Security (High)
Blocked (WAN-to-LAN):Blocks all unrelated WAN to LAN traffic and enable IDS.

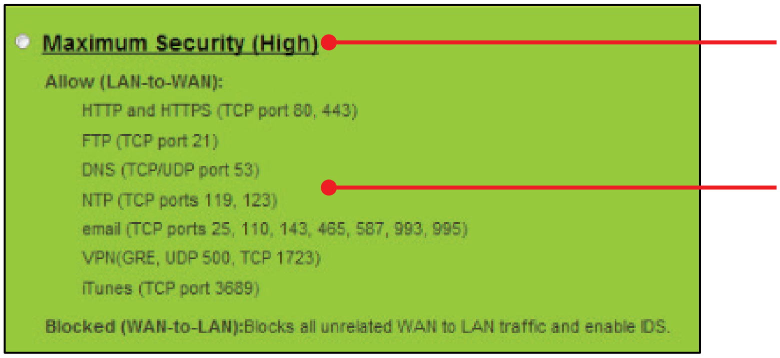
○ Typical Security (Medium)
Allow (LAN-to-WAN):all

● Minimum Security (Low)
Allow (LAN-to-WAN):Permit LAN-to-WAN traffic.

○ Custom Security
Blocked (WAN-to-LAN):No access to local network from Internet.

Figure 23. Firewall Settings Page

To select a security level, click the radio button next to the level and then click the **SAVE SETTINGS** button. To see the protection associated with a security level, click the name of the security level to expand the security level. If you click the words **Maximum Security Level** (not the radio button next to the words), for example, the maximum security area on the page expands as shown in Figure 24.



○ Maximum Security (High)

Allow (LAN-to-WAN):

HTTP and HTTPS (TCP port 80, 443)
FTP (TCP port 21)
DNS (TCP/UDP port 53)
NTP (TCP ports 119, 123)
email (TCP ports 25, 110, 143, 465, 587, 993, 995)
VPN(GRE, UDP 500, TCP 1723)
iTunes (TCP port 3689)

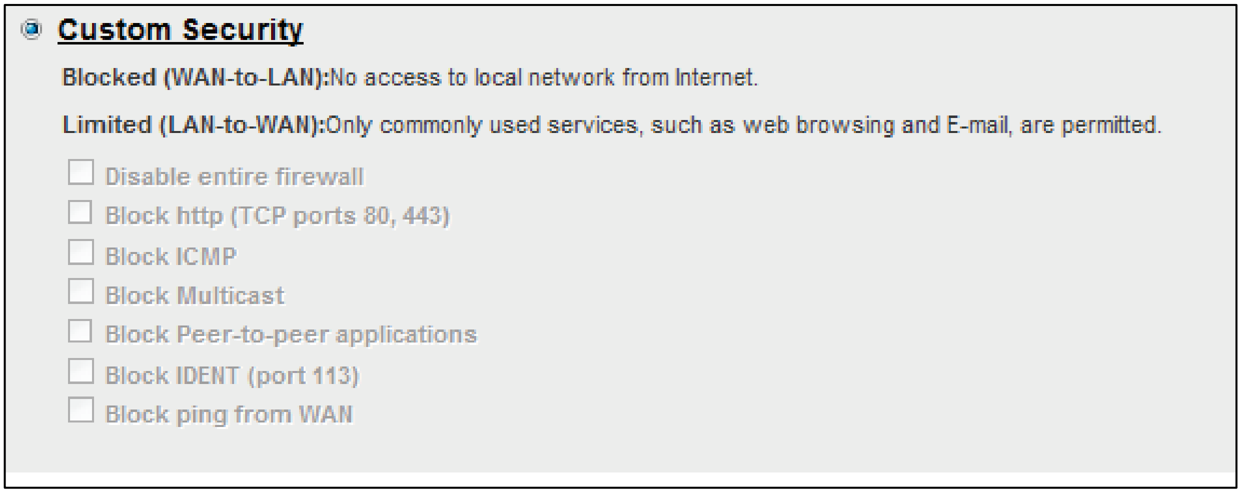
Blocked (WAN-to-LAN):Blocks all unrelated WAN to LAN traffic and enable IDS.

Clicking the underlined security level…

…displays this expanded list of items that are allowed or blocked.

Figure 24. Example of Expanding Maximum Security

If you click the words **Custom Security** option (not the radio button next to the words), the options in Figure 25 appear. You can then choose the desired options to customize security settings to suit your requirements. After checking the desired options, click the radio button to select custom security.



● Custom Security

Blocked (WAN-to-LAN):No access to local network from Internet.

Limited (LAN-to-WAN):Only commonly used services, such as web browsing and E-mail, are permitted.

□ Disable entire firewall
□ Block http (TCP ports 80, 443)
□ Block ICMP
□ Block Multicast
□ Block Peer-to-peer applications
□ Block IDENT (port 113)
□ Block ping from WAN

Figure 25. Example of Expanding Custom Security

Table 10. Firewall Settings Page Options

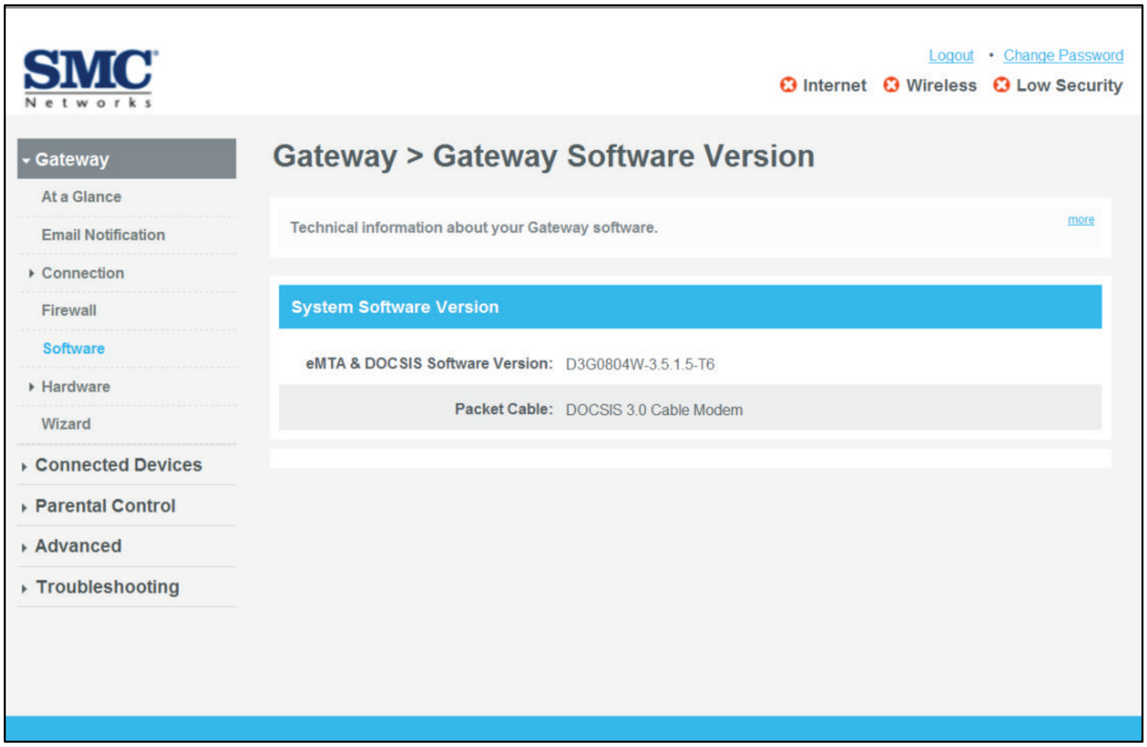
Option	Description
Maximum Security (High)	Maximum security is the highest level of firewall security. This level blocks all applications including voice applications (such as Gtalk and Skype) and P2P applications, but permits Internet browsing, email, VPN, DNS, and iTunes services.
Typical Security (Medium)	Typical security is the medium level of firewall security. This level blocks P2P applications and pings to the Gateway, while permitting all other traffic.
Minimum Security (Low)	Minimum security is the lowest level of firewall security. It does not block applications and traffic. Select this level if you are not familiar with firewall settings.
Custom Security	This security level is pre-configured to block all local network access from the Internet, except “trusted computers" defined on the Managed Sites page (see page 57) and Managed Services page (see page 64). Only commonly used services, such as Web browsing and E-mail, are permitted. If you select this option, a list of check boxes let you disable the entire firewall or block certain traffic (see Figure 25).
SAVE SETTINGS Button	After configuring the settings on this page, click this button to save your settings.
RESTORE DEFAULT SETTINGS Button	Click this button to return the Gateway to its default settings. A precautionary message does not appear before the Gateway reverts to its default settings. If you click this button, the Gateway logs you out of the Web management interface and you must log in to the interface again.

Gateway Software Version Page

Path: **Gateway > Software**

The Gateway Software Version page shows the:

- eMTA and DOCSIS software version
- Name of the packet cable modem



Gateway > Gateway Software Version

Technical information about your Gateway software.

System Software Version

eMTA & DOCSIS Software Version: D3G0804W-3.5.1.5-T6

Packet Cable: DOCSIS 3.0 Cable Modem

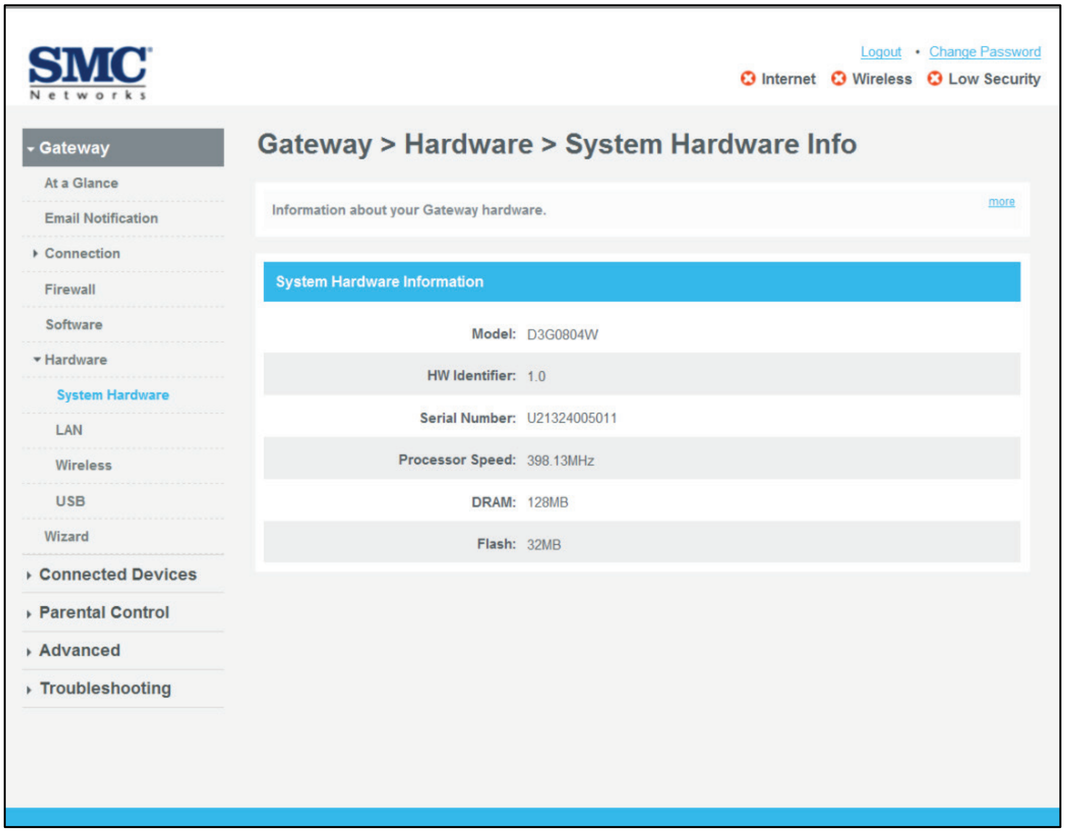
Figure 26. Gateway Software Version Page

System Hardware Info Page

Path: **Gateway > Hardware > System Hardware**

The System Hardware Info page shows the following information about the Gateway hardware:

- Model, hardware identifier, and serial number
- Processor speed
- Dynamic Random Access Memory (DRAM) and flash



Gateway > Hardware > System Hardware Info

Information about your Gateway hardware.

System Hardware Information

Model: D3G0804W

HW Identifier: 1.0

Serial Number: U21324005011

Processor Speed: 398.13MHz

DRAM: 128MB

Flash: 32MB

Figure 27. System Hardware Info Page

LAN Ethernet Hardware Info Page

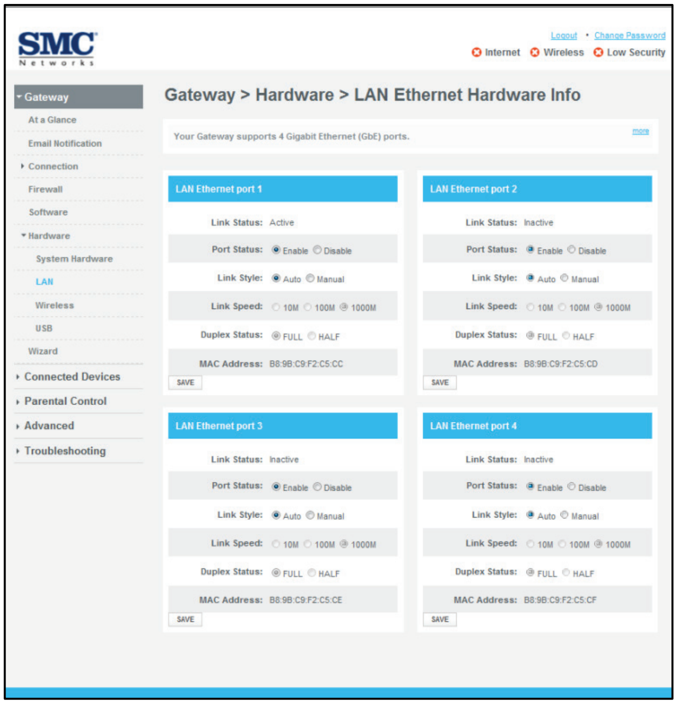
Path: **Gateway > Hardware > LAN**

The LAN Ethernet Hardware Info page lets you configure the following settings for the Gateway's four Ethernet ports:

- Link status – if a device is connected to a Gigabit Ethernet port, the **Link Status** is **Active**; otherwise, the **Link Status** is **Inactive**.
- Port status
- Link style and link speed
- Duplex status

This page also shows the MAC address for each Ethernet port.

If you change the settings for an Ethernet port, the new settings do not take effect until you click the **SAVE** button for that port.



Gateway > Hardware > LAN Ethernet Hardware Info

Your Gateway supports 4 Gigabit Ethernet (GbE) ports.

LAN Ethernet port 1

Link Status: Active
Port Status: ● Enable ○ Disable
Link Style: ● Auto ○ Manual
Link Speed: ○ 10M ○ 100M ● 1000M
Duplex Status: ● FULL ○ HALF
MAC Address: B8:9B:C9:F2:C5:CC

LAN Ethernet port 2

Link Status: Inactive
Port Status: ● Enable ○ Disable
Link Style: ● Auto ○ Manual
Link Speed: ○ 10M ○ 100M ● 1000M
Duplex Status: ● FULL ○ HALF
MAC Address: B8:9B:C9:F2:C5:CD

LAN Ethernet port 3

Link Status: Inactive
Port Status: ● Enable ○ Disable
Link Style: ● Auto ○ Manual
Link Speed: ○ 10M ○ 100M ● 1000M
Duplex Status: ● FULL ○ HALF
MAC Address: B8:9B:C9:F2:C5:CE

LAN Ethernet port 4

Link Status: Inactive
Port Status: ● Enable ○ Disable
Link Style: ● Auto ○ Manual
Link Speed: ○ 10M ○ 100M ● 1000M
Duplex Status: ● FULL ○ HALF
MAC Address: B8:9B:C9:F2:C5:CF

Figure 28. LAN Ethernet Hardware Info Page

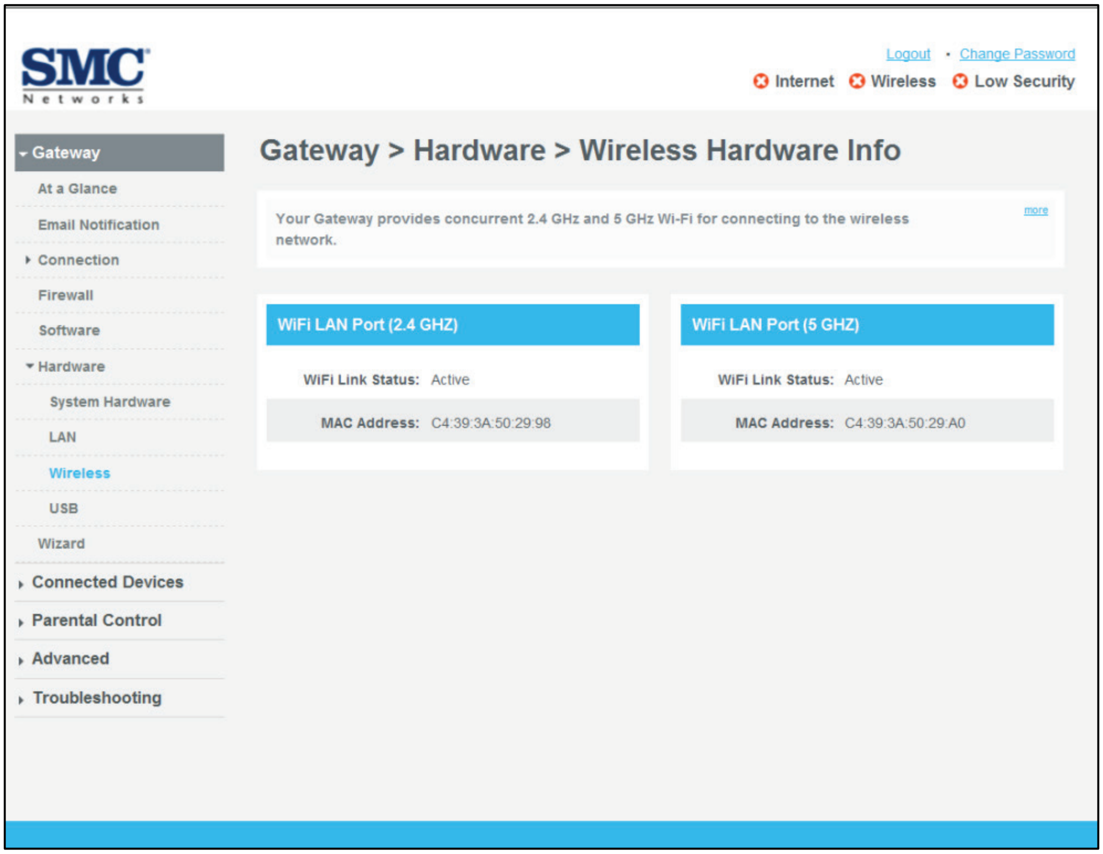
Wireless Hardware Info Page

Path: **Gateway > Hardware > Wireless**

The Gateway supports concurrent 2.4 GHz and 5 GHz Wi-Fi wireless connections. The Wireless Hardware Info page shows the Wi-Fi link status and MAC address of the Gateway’s 2.4 GHz and 5 GHz Wi-Fi LAN ports.

If a wireless client is connected to the Gateway Wi-Fi LAN ports, the **WiFi Link Status** is **Active** for that port; otherwise, the **WiFi Link Status** is **Inactive**.

Note: This page is also available from the Status page by clicking the **VIEW** button in the **WiFi Network 2.4G** or **WiFi Network 5G** area.



Gateway > Hardware > Wireless Hardware Info

Your Gateway provides concurrent 2.4 GHz and 5 GHz Wi-Fi for connecting to the wireless network.

WiFi LAN Port (2.4 GHZ)

WiFi Link Status: Active

MAC Address: C4:39:3A:50:29:98

WiFi LAN Port (5 GHZ)

WiFi Link Status: Active

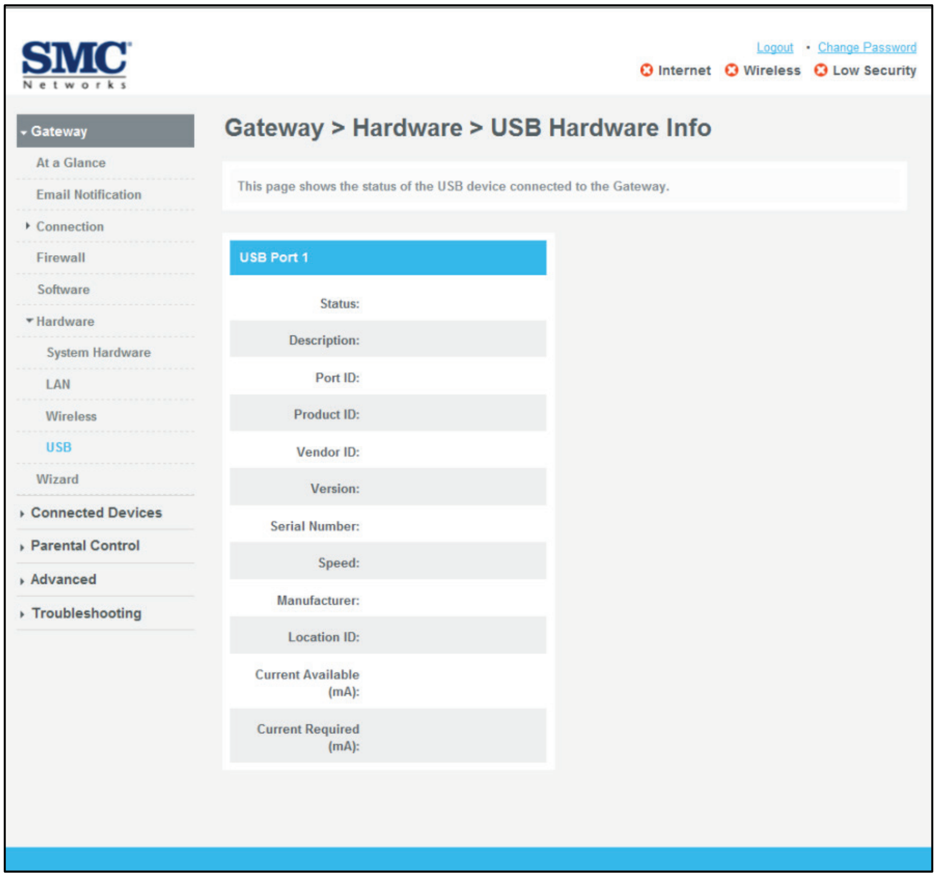
MAC Address: C4:39:3A:50:29:A0

Figure 29. Wireless Hardware Info Page

USB Hardware Info Page

Path: **Gateway > Hardware > USB**

The Gateway has one USB port for accommodating a device with a USB interface. The USB Hardware Info page shows information about the USB device connected to the Gateway's USB port.



Gateway > Hardware > USB Hardware Info

This page shows the status of the USB device connected to the Gateway.

USB Port 1

Status:	
Description:	
Port ID:	
Product ID:	
Vendor ID:	
Version:	
Serial Number:	
Speed:	
Manufacturer:	
Location ID:	
Current Available (mA):	
Current Required (mA):	

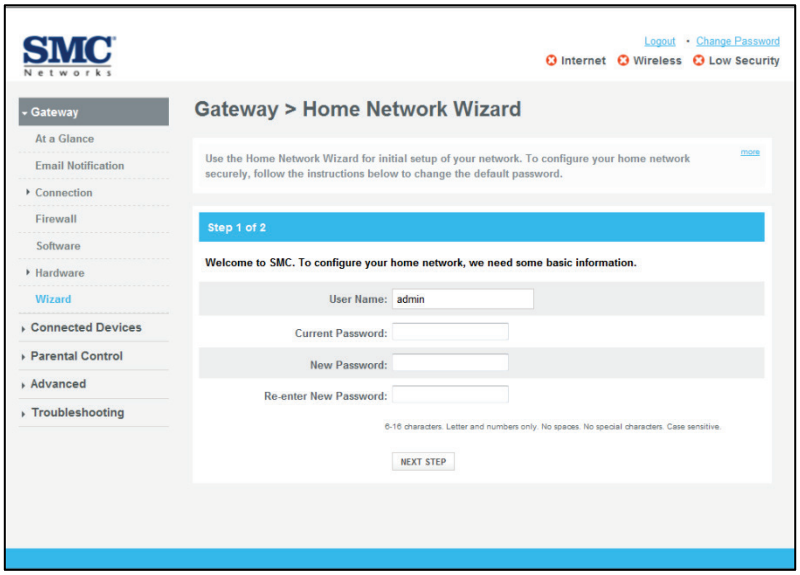
Figure 30. USB Hardware Info Page

Home Network Wizard Page

Path: **Gateway > Wizard**

The Home Network Wizard is a 2-page wizard for configuring your home network. If you are a new or novice user, we recommend you use the wizard to configure the Gateway's basic settings. The wizard is the first page that appears when you log in to the Web management interface.

Figure 31 shows the first page of the wizard and Table 11 describes the options. When you complete the first page, click **NEXT STEP** to display the second page (see Figure 32 and Table 12).



Gateway > Home Network Wizard

Use the Home Network Wizard for initial setup of your network. To configure your home network securely, follow the instructions below to change the default password.

Step 1 of 2

Welcome to SMC. To configure your home network, we need some basic information.

User Name: admin

Current Password:

New Password:

Re-enter New Password:

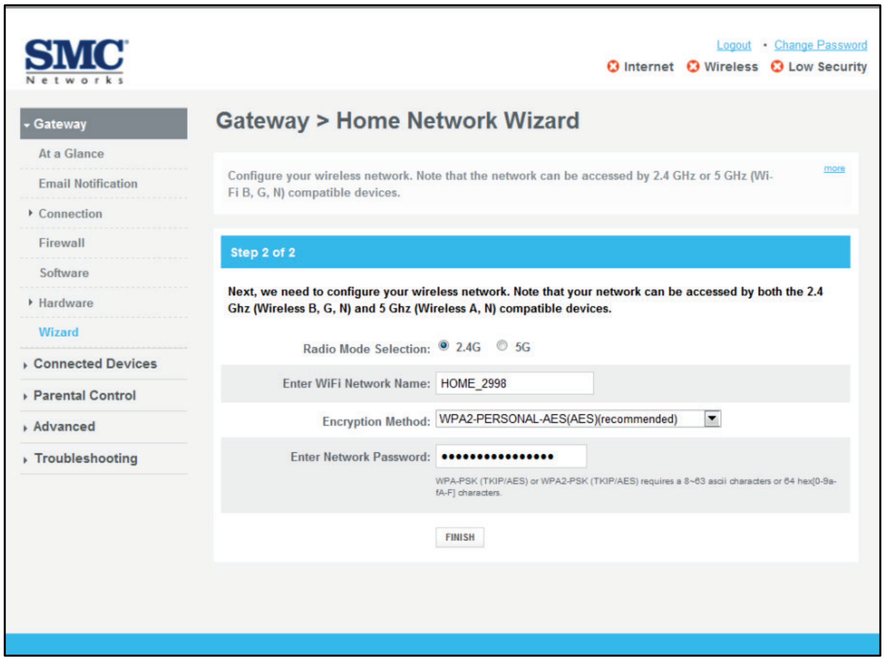
6-16 characters. Letter and numbers only. No spaces. No special characters. Case sensitive.

Figure 31. Example of Home Network Wizard – Page 1

Table 11. Home Network Wizard – Page 1 Options

Option	Description
User Name	Enter the user name used to log in to the Web management interface. The user name is case sensitive and can contain from 8 to 20 alphanumeric characters, but no spaces or special characters.
Current Password	Enter the current case-sensitive password used to log in to the Web management interface. For security purposes, every typed character is masked with a dot (•). The default password is not shown for security purposes. The password is case sensitive and can contain from 8 to 32 characters, but no spaces or special characters.
New Password	Enter the new case-sensitive password you want to use. The password can contain from 8 to 32 alphanumeric characters, but no spaces or special characters. Spaces count as password characters. For security purposes, every typed character is masked with a dot (•).
Re-enter New Password	Enter the same case-sensitive password you typed in the New Password field. For security purposes, every typed character is masked as a dot (•).

NEXT STEP Button	Displays the second page of the wizard.



Gateway > Home Network Wizard

Configure your wireless network. Note that the network can be accessed by 2.4 GHz or 5 GHz (Wi-Fi B, G, N) compatible devices.

Next, we need to configure your wireless network. Note that your network can be accessed by both the 2.4 Ghz (Wireless B, G, N) and 5 Ghz (Wireless A, N) compatible devices.

Radio Mode Selection: ● 2.4G ○ 5G

Enter WiFi Network Name: HOME_2998

Encryption Method: WPA2-PERSONAL-AES(AES)(recommended)

Enter Network Password: ••••••••••••••••

WPA-PSK (TKIP/AES) or WPA2-PSK (TKIP/AES) requires a 8~63 ascii characters or 64 hex[0-9a-fA-F] characters.

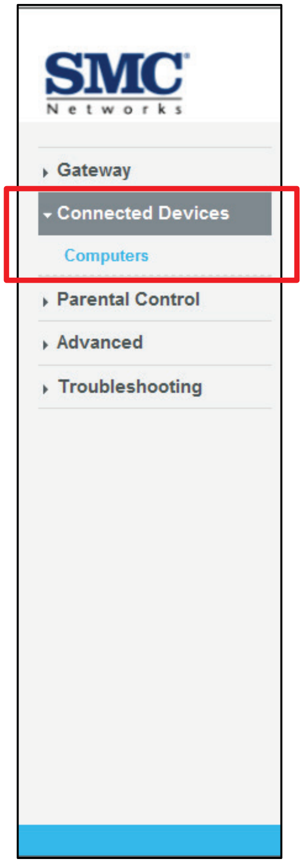
Figure 32. Example of Home Network Wizard - Page 2

Table 12. Home Network Wizard – Page 2 Options

Option	Description
Radio Mode Selection	Select whether the home network will use the Gateway's 2.4 GHz or 5 GHz wireless network. The default WiFi network name changes based on your selection.
Enter WiFi Network Name	Accept or change the name for your wireless network (typically, this is the network's SSID). The WiFi network name will make it more obvious for other devices to know the network to which they are connecting.

Option	Description
Encryption Method	To prevent other computers in the area from using your Internet connection, secure your wireless network by selecting an encryption method from this drop-down list. There are several selections available, including the following. (Risky appears next to selections that provide little or no protection.) • OPEN = wireless transmissions are not protected. • WEP = basic encryption and therefore least secure (i.e., it can be easily cracked, but is compatible with a wide range of devices including older hardware). WEP 64- and 128-bit selections are provided. • WPA–PERSONAL–TKIP (TKIP) = a Wi-Fi standard that is stronger than WEP encryption. This selection uses Temporal Key Integrity Protocol (TKIP) encryption to provide protection against hackers. If you use WPA, each device in your wireless network must use the same WPA method and network password, or the network will not work properly. • WPA2-PERSONAL = several versions are provided. Some use TKIP encryption, while others use Advanced Encryption System (AES), which utilizes a symmetric 128-bit block data encryption. WPA2 Personal is stronger than WPA encryption. Each device in your wireless network must use the same WPA method and network password, or the network will not work properly. • WPA-ENTERPRISE = this option uses WPA and should be used with a RADIUS server connected to the Gateway. Each device in your wireless network must use the same WPA method and network password, or the network will not work properly. This setting requires a RADIUS server to be connected to the Gateway. • WPA2-ENTERPRISE = this option uses WPA2 and should be used with a RADIUS server connected to the Gateway. WPA2-ENTERPRISE supports two encryption methods, TKIP and AES, with dynamic encryption keys. Select the type of algorithm, AES or TKIP. Each device in your wireless network must use the same WPA method and network password, or the network will not work properly. This setting requires a RADIUS server to be connected to the Gateway. • WPA-WPA2-ENTERPRISE = allows your devices to connect using the strongest security option they support, WPA or WPA2. Each device in your wireless network must use the same WPA method and network password, or the network will not work properly. This setting requires a RADIUS server to be connected to the Gateway.
Enter Network Password	If you select one of the WEP, WPA, or WPA2 encryption settings, enter the case-sensitive password used for encryption and decryption. For security, each typed password character is masked as a dot (●). If you specify a hexadecimal password, use the letters A to F and numbers 0 to 9. • WEP 64 requires a 5 ASCII character or 10 hexadecimal character password. • WEP 128: requires a 13 ASCII character or 16 hexadecimal character password. • The remaining encryption methods require at least an 8 ASCI character or a 64 hexadecimal character password.
FINISH Button	Click this button to save your settings and exit the wizard.

Connected Devices Menu



The **Connected Devices** menu contains the single option **Computers**, which lets you view and edit computers connected to the Gateway's LAN. See "Computers Page" on the next page.

Computers Page

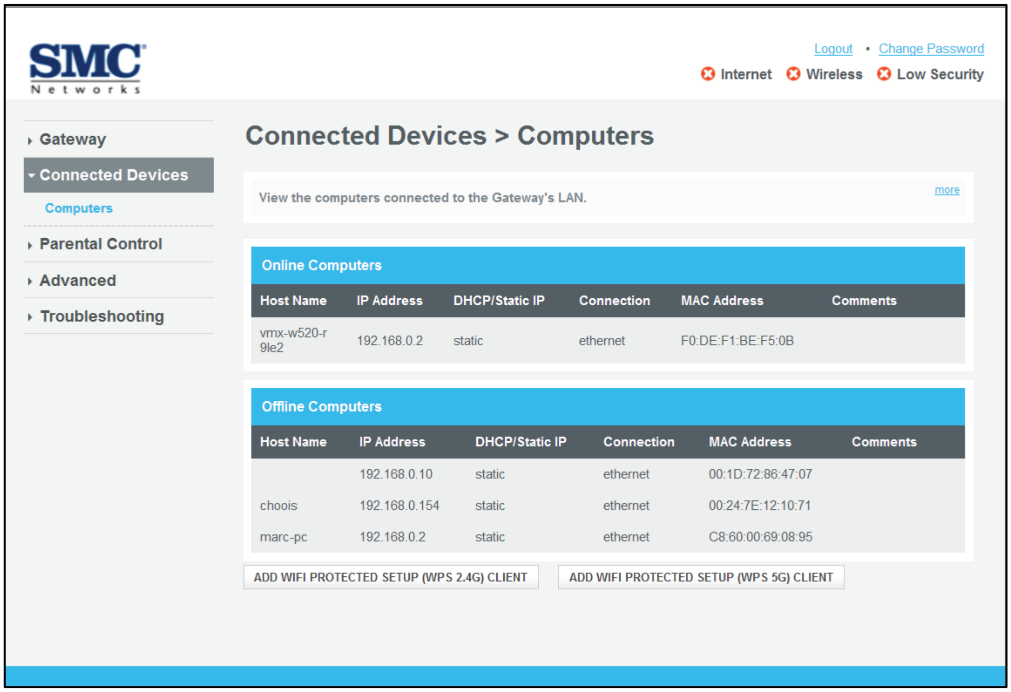
Path: **Connected Devices > Computers**

The Gateway uses DHCP to automatically discover computers attached to it and displays this information on the Computers page. This page contains two areas:

- **Online Computers** shows attached computers that are currently online.
- **Offline Computers** shows devices that had been connected to your network, but are not currently connected.

At the bottom of the page, the **ADD WIFI PROTECTED SETUP (WPS 2.4G) CLIENT** and **ADD WIFI PROTECTED SETUP (WPS 5G) CLIENT** buttons let you enable or disable WPS, add wireless clients, and unlock a WPS lock condition. For more information, see “Configuring WPS Settings” on page 39.

Note: You must enable WPS before a wireless device can connect to the Gateway using WPS.



Connected Devices > Computers

View the computers connected to the Gateway's LAN.

Online Computers

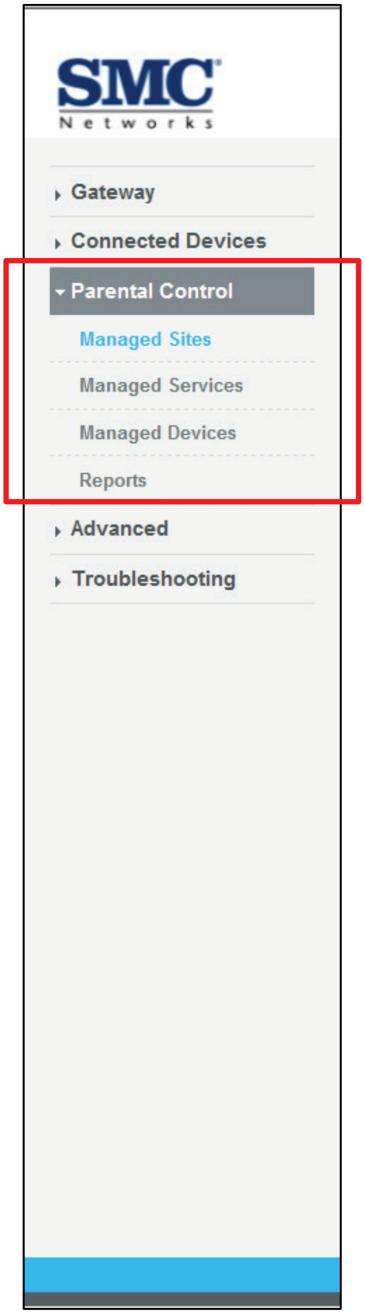
Host Name	IP Address	DHCP/Static IP	Connection	MAC Address	Comments
vmx-w520-r 9le2	192.168.0.2	static	ethernet	F0:DE:F1:BE:F5:0B	

Offline Computers

Host Name	IP Address	DHCP/Static IP	Connection	MAC Address	Comments
	192.168.0.10	static	ethernet	00:1D:72:86:47:07	
choois	192.168.0.154	static	ethernet	00:24:7E:12:10:71	
marc-pc	192.168.0.2	static	ethernet	C8:60:00:69:08:95	

Figure 33. Computers Page

Parental Control Menu



Regulating Web browsing can prevent children and workers from accessing dangerous content on the Internet, or having to make judgment calls over suitable relationships in chat-rooms. The fact is, Web sites, chat-room users, and downloaded programs may not have the best interests of you, your family, or your workers at heart. The unscrupulous may try to manipulate the people you care about or try to gain trust, which may result in unacceptable access to your family, your coworkers, your computer, or personal information.

The **Parental Control** menu contains the following pages for regulating Internet access:

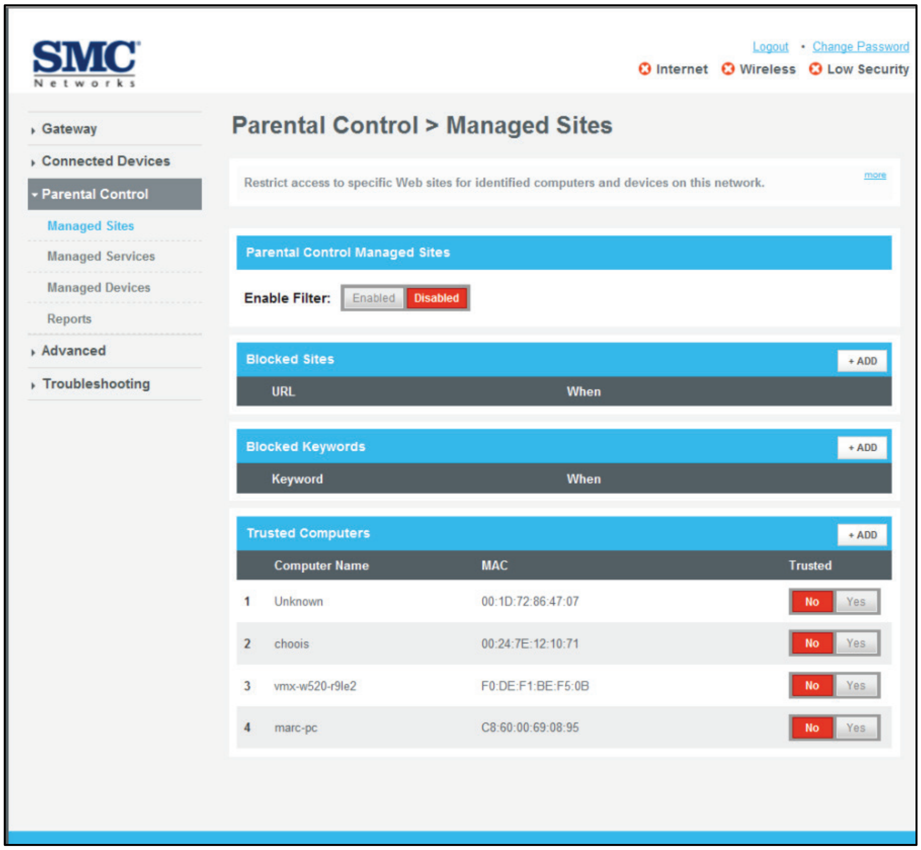
- **Managed Sites** - restricts access to certain Web sites and keywords, and define trusted computers that can access these Web sites and keywords. See page 57.
- **Managed Services** - restricts access to services and define trusted computers that can access these services. See page 64.
- **Managed Devices** - configures the device list to allow or block connection to the network. See page 69.
- **Reports** – generates, prints, and downloads reports. See page 74.

Managed Sites Page

Path: **Parental Control > Managed Sites**

The Managed Sites page lets you configure:

- Blocked sites – see page 58.
- Blocked keywords – see page 60.
- Trusted computers that can access the blocked sites and keywords – see page 62.



Parental Control > Managed Sites

Restrict access to specific Web sites for identified computers and devices on this network.

Parental Control Managed Sites

Enable Filter: Enabled [✓ Disabled]

Blocked Sites

URL	When

Blocked Keywords

Keyword	When

Trusted Computers

	Computer Name	MAC	Trusted
1	Unknown	00:1D:72:86:47:07	[✓ No] Yes
2	chooís	00:24:7E:12:10:71	[✓ No] Yes
3	vmx-w520-r9le2	F0:DE:F1:BE:F5:0B	[✓ No] Yes
4	marc-pc	C8:60:00:69:08:95	[✓ No] Yes

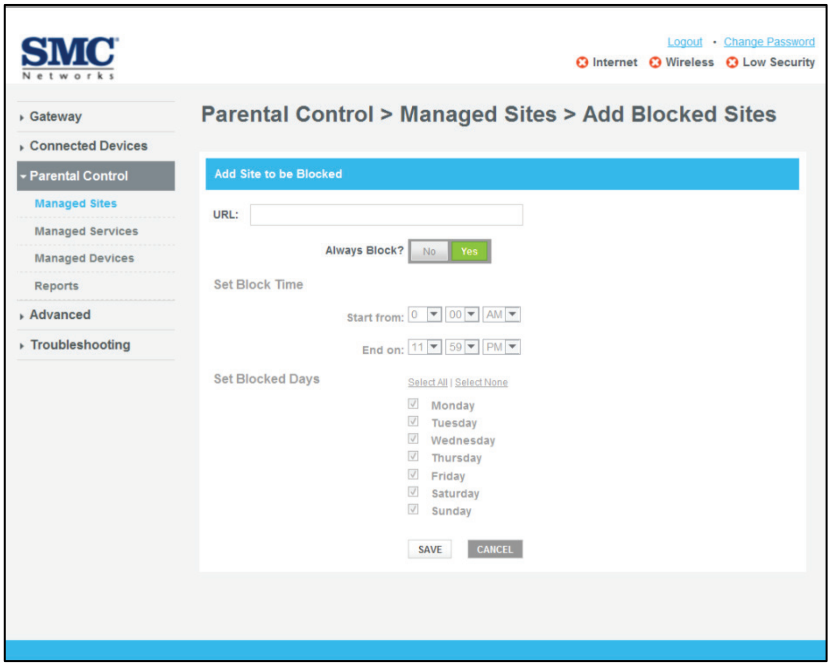
Figure 34. Managed Sites Page

Configuring Blocked Sites

Using the Managed Sites page, you can block access to certain Web sites from local computers.

To define blocked sites on the Managed Sites page:

1. In the **Blocked Sites** table, click the **+ADD** button. The Add Blocked Sites page appears (see Figure 35).
2. Complete the fields in the Add Blocked Sites page (see Table 13).
3. Click **SAVE**. The blocked URL and the start and end time when the URL will be blocked appear in the Blocked Sites table of the Managed Sites page.
4. Next to **Enable Filter** on the Managed Sites page, click **Enabled** to enable the parental control filters configured on this page. (To disable the parental control filters configured on this page, click **Disabled**.)
5. To edit a blocked site, click the **EDIT** button next to the blocked site you want to modify, edit the settings (see Table 13), and click **SAVE**.
6. To delete a blocked site, click the **X** next to the site. When a precautionary message appears, click **OK** to delete the blocked site or **CANCEL** to retain it.



Parental Control > Managed Sites > Add Blocked Sites

Add Site to be Blocked

URL:

Always Block? No [✓ Yes]

Set Block Time

Start from: 0 00 AM

End on: 11 59 PM

Set Blocked Days

Select All | Select None

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

SAVE CANCEL

Figure 35. Add Blocked Sites Page

Table 13. Add Blocked Sites Page Options

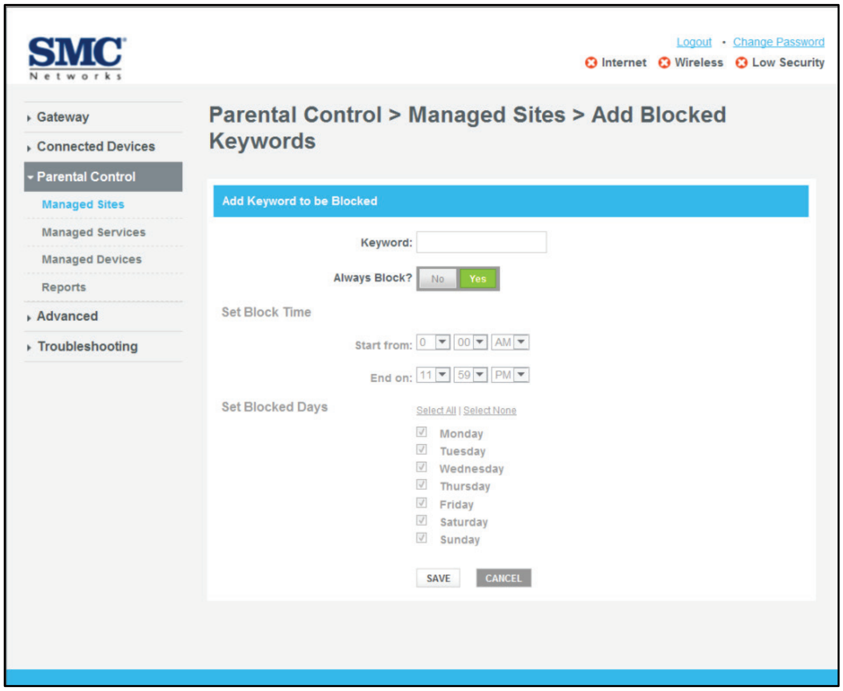
Option	Description
URL	Enter the URL of the site you want to block.
Always Block?	Select whether you want the Gateway to always block this URL. Choices are: • No = the Gateway does not always block this URL. Use Set Block Time and Set Blocked Days to instruct the Gateway when to start and stop blocking this URL. • Yes = the Gateway always blocks this URL until you remove the block.
Set Block Time	If you set Always Block to No, select the time when the Gateway is to block this URL. • Start from = select the start time when the Gateway starts blocking the URL. • End on = select the end time when the Gateway stops blocking the URL.
Set Blocked Days	If you set Always Block to No, select the days when the Gateway will block this URL. Links and check boxes are provided for selecting all days, no days, or individual days of the week. • Select All = click this link to select all seven days. • Select None = click this link to deselect all seven days. • Monday – Sunday = check the check boxes that correspond to the days when you want the Gateway to block this URL.
SAVE Button	After configuring the settings on this page, click this button to save your settings.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.

Configuring Blocked Keywords

Using the Managed Sites page, you can block access to certain key words from local computers.

To define blocked keywords on the Managed Sites page:

1. In the **Blocked Keywords** table, click the **+ADD** button. The Add Blocked Keywords page appears (see Figure 36).
2. Complete the fields in the Add Blocked Keywords page (see Table 14).
3. Click **SAVE**. The blocked keyword and the start and end time when the keyword will be blocked appear in the Blocked Sites table of the Managed Sites page.
4. Next to **Enable Filter** on the Managed Sites page, click **Enabled** to enable the parental control filters configured on this page. (To disable the parental control filters configured on this page, click **Disabled**.)
5. To edit a blocked keyword, click the **EDIT** button next to the blocked keyword you want to modify, edit the settings (see Table 14), and click **SAVE**.
6. To delete a blocked keyword, click the **X** next to the keyword. When a precautionary message appears, click **OK** to delete the blocked keyword or **CANCEL** to retain it.



Parental Control > Managed Sites > Add Blocked Keywords

Add Keyword to be Blocked

Keyword:

Always Block? No [✓ Yes]

Set Block Time

Start from: 0 : 00 AM

End on: 11 : 59 PM

Set Blocked Days

Select All | Select None

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Figure 36. Add Blocked Keywords Page

Table 14. Add Blocked Keywords Page Options

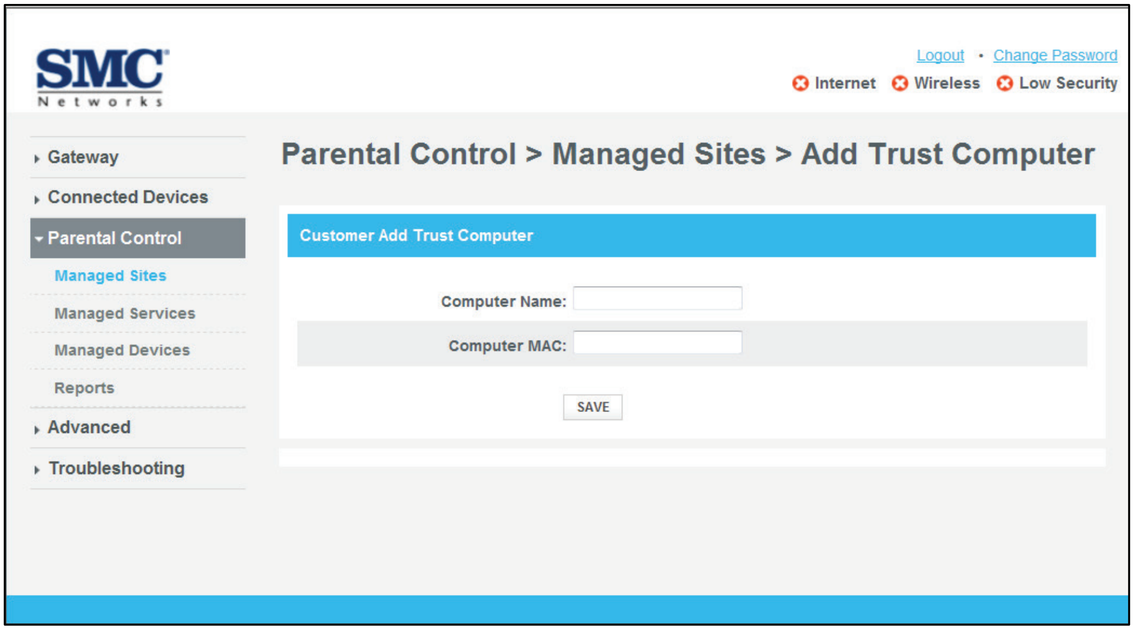
Option	Description
Keyword	Enter the keyword you want to block.
Always Block?	Select whether you want the Gateway to always block this keyword. Choices are: • No = the Gateway does not always block this keyword. Use Set Block Time and Set Blocked Days to instruct the Gateway when to start and stop blocking this keyword. • Yes = the Gateway always blocks this keyword until you remove the block.
Set Block Time	If you set Always Block to No, select the time when the Gateway is to block this keyword. • Start from = select the start time when the Gateway starts blocking the keyword. • End on = select the end time when the Gateway stops blocking the keyword.
Set Blocked Days	If you set Always Block to No, select the days when the Gateway will block this keyword. Links and check boxes are provided for selecting all days, no days, or individual days of the week. • Select All = click this link to select all seven days. • Select None = click this link to deselect all seven days. • Monday – Sunday = check the check boxes that correspond to the days when you want the Gateway to block this keyword.
SAVE Button	After configuring the settings on this page, click this button to save your settings.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.

Configuring Trusted Computers

Using the Managed Sites page, you can define trusted computers that are allowed to access the blocked Web sites and keywords.

To configure trusted computers on the Managed Sites page:

1. In the **Trusted Computers** area, click the **+ADD** button. The Add Trust Computer page appears (see Figure 37).
2. Complete the fields in the Add Trust Computer page (see Table 15).
3. Click **SAVE**. The name of the trusted computer and its MAC address appear in the Trusted Computers table in the Managed Sites page.
4. Next to **Enable Filter** on the Managed Sites page, click **Enabled** to enable the parental control filters configured on this page. (To disable the parental control filters configured on this page, click **Disabled**.)
5. After a trusted computer has been defined, use the **No** or **Yes** buttons next to the trusted computer on the Managed Sites page to toggle between trusted and untrusted.



Parental Control > Managed Sites > Add Trust Computer

Customer Add Trust Computer

Computer Name:

Computer MAC:

Figure 37. Add Trust Computer Page

Table 15. Add Trust Computer Options

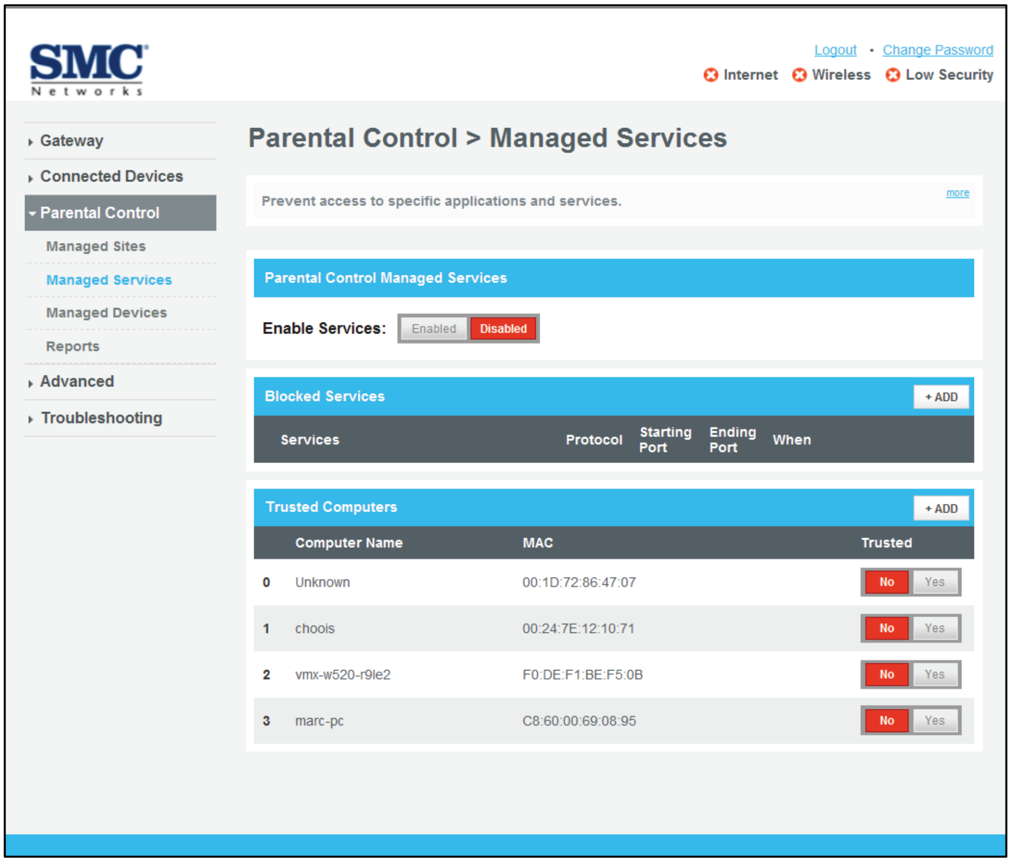
Option	Description
Computer Name	Enter a name for the computer you want to designate as the trusted computer. The name should be unique and allow you to differentiate this trusted computer from others you may define.
Computer MAC	Enter the MAC address of the computer you want to designate as the trusted computer.
SAVE Button	After configuring the settings on this page, click this button to save your settings.

Managed Services Page

Path: **Parental Control > Managed Services**

The Managed Services page lets you configure:

- Blocked services – see page 65.
- Trusted computers that can access the blocked services – see page 66.



Parental Control > Managed Services

Prevent access to specific applications and services.

Parental Control Managed Services

Enable Services: Enabled [✓ Disabled]

Blocked Services

Services	Protocol	Starting Port	Ending Port	When

Trusted Computers

	Computer Name	MAC	Trusted
0	Unknown	00:1D:72:86:47:07	[✓ No] Yes
1	choois	00:24:7E:12:10:71	[✓ No] Yes
2	vmx-w520-r9le2	F0:DE:F1:BE:F5:0B	[✓ No] Yes
3	marc-pc	C8:60:00:69:08:95	[✓ No] Yes

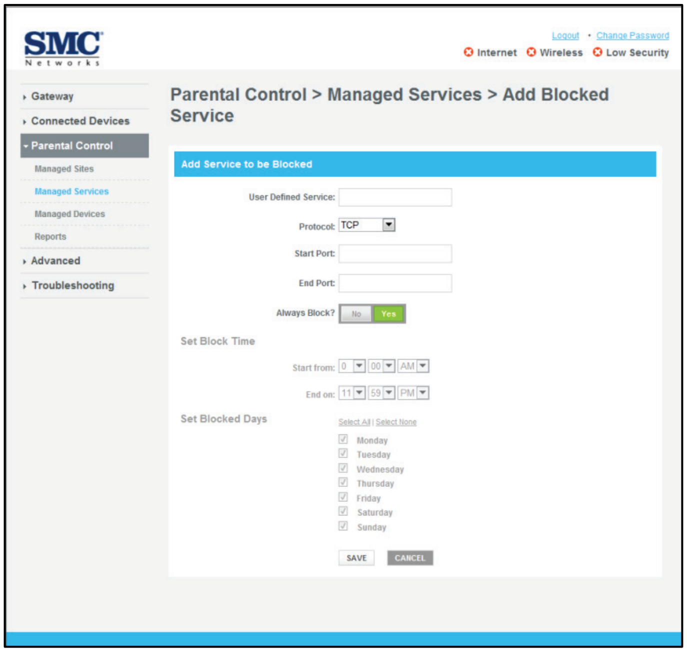
Figure 38. Managed Services Page

Configuring Blocked Services

Using the Managed Services page, you can block access to certain services from local computers.

To define blocked services on the Managed Services page:

1. In the **Blocked Services** area, click the **+ADD** button. The Add Blocked Service page in Figure 39 appears.
2. Complete the fields in the Add Blocked Service page (see Table 16).
3. Click **SAVE**. The blocked service appears in the Blocked Services table in the Managed Services page, along with the associated protocol, starting and stopping ports, and blocked day and time.
4. Next to **Enable Services** on the Managed Services page, click **Enabled** to enable the parental control filters configured on this page. (To disable the parental control filters configured on this page, click **Disabled**.)
5. To edit a blocked service, click the **EDIT** button next to the blocked service you want to modify, edit the settings (see Table 16), and click **SAVE**.
6. To delete a blocked service, click the **X** next to the service. When a precautionary message appears, click **OK** to delete the blocked service or **CANCEL** to retain it.



Parental Control > Managed Services > Add Blocked Service

Add Service to be Blocked

User Defined Service:

Protocol: TCP

Start Port:

End Port:

Always Block? No [✓ Yes]

Set Block Time

Start from: 0 : 00 AM

End on: 11 : 59 PM

Set Blocked Days

Select All | Select None

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

SAVE CANCEL

Figure 39. Add Blocked Service Page

Table 16. Adding Blocked Service Page

Option	Description
User Defined Service	Enter the service you want blocked.
Protocol	The type of protocol associated with the service to be blocked. Choices are: • TCP • UDP • TCP/UDP
Start Port	Starting port number on which the block will be applied. If necessary, contact the application vendor for this information.
End Port	Ending port number on which the block will be applied. If necessary, contact the application vendor for this information.
Always Block?	Select whether you want the Gateway to always block this service. Choices are: • No = the Gateway does not always block this service. Use Set Block Time and Set Blocked Days to instruct the Gateway when to start and stop blocking this service. • Yes = the Gateway always blocks this service until you remove the block.
Set Block Time	If you selected No for Always Block?, select the time when the Gateway is to block this service. • Start from = select the start time when the Gateway starts blocking the service. • End on = select the end time when the Gateway stops blocking the service.
Set Blocked Days	If you selected No for Always Block?, select the days when the Gateway will block this service. Links and check boxes are provided for selecting all days, no days, or individual days of the week. • Select All = click this link to select all seven days. • Select None = click this link to deselect all seven days. • Monday – Sunday = check the check boxes that correspond to the days when you want the Gateway to block this service.
SAVE Button	After configuring the settings on this page, click this button to save your settings.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.

Configuring Trusted Computers

Using the Managed Services page, you can define trusted computers that are allowed to access the blocked services and applications.

To define trusted computers on the Managed Services page:

1. In the **Trusted Computers** area, click the **+ADD** button. The Add Trust Computer page appears (see Figure 40).
2. Complete the fields in the Add Trust Computer page (see Table 17).
3. Click **SAVE**. The name of the trusted computer and its MAC address appear in the Trusted Computers table in the Managed Services page.
4. Next to **Enable Services** on the Managed Services page, click **Enabled** to enable the parental control filters configured on this page. (To disable the parental control filters configured on this page, click **Disabled**.)
5. After a trusted computer has been defined, use the **No** or **Yes** buttons next to the trusted computer on the Managed Services page to toggle between trusted and untrusted.

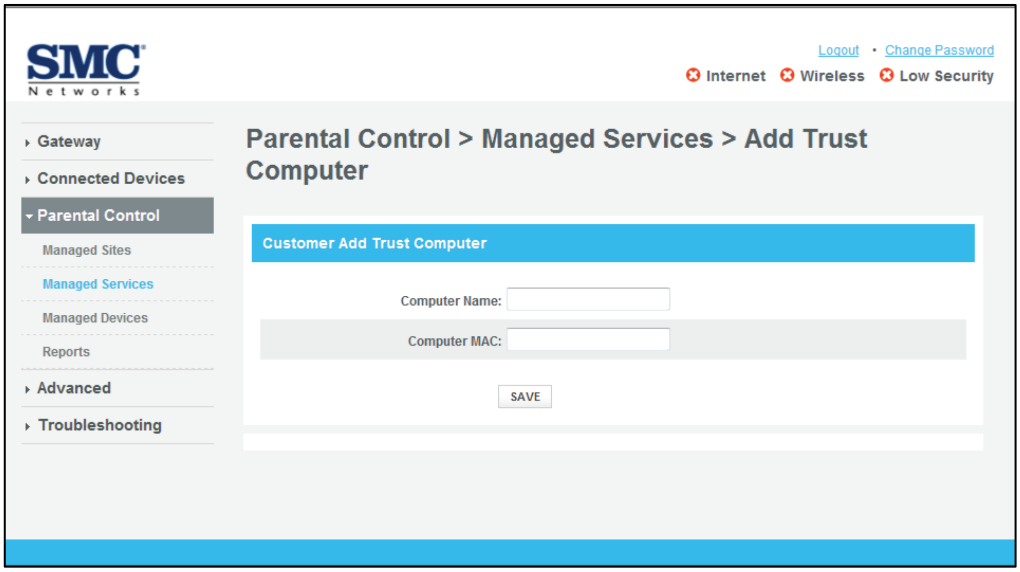


Figure 40. Add Trust Computer Page

Table 17. Add Trust Computer Page Options

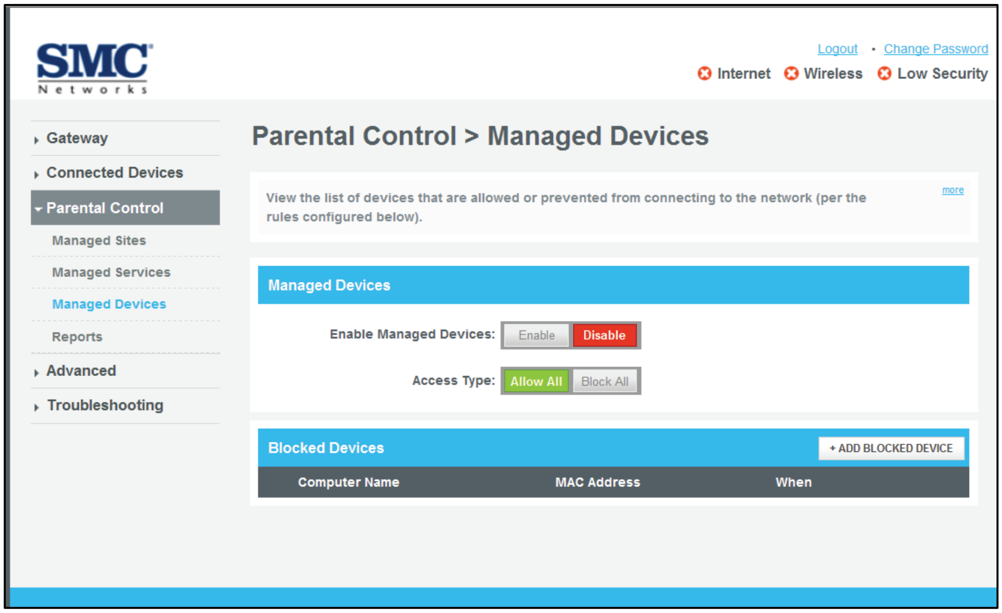
Option	Description
Computer Name	Enter a name for the computer you want to designate as the trusted computer. The name should be unique and allow you to differentiate this trusted computer from others you may define.
Computer MAC	Enter the MAC address of the computer you want to designate as the trusted computer.
SAVE Button	After configuring the settings on this page, click this button to save your settings.

Managed Devices Page

Path: **Parental Control > Managed Devices**

The Managed Devices page lets you create a list of devices that are:

- Allowed to connect to the Internet – see page 70.
- Blocked from connecting to the Internet – see page 72.



Parental Control > Managed Devices

View the list of devices that are allowed or prevented from connecting to the network (per the rules configured below).

Managed Devices

Enable Managed Devices: Disable

Access Type: Allow All

Blocked Devices

Computer Name	MAC Address	When

Figure 41. Managed Devices Page

Allowing Devices

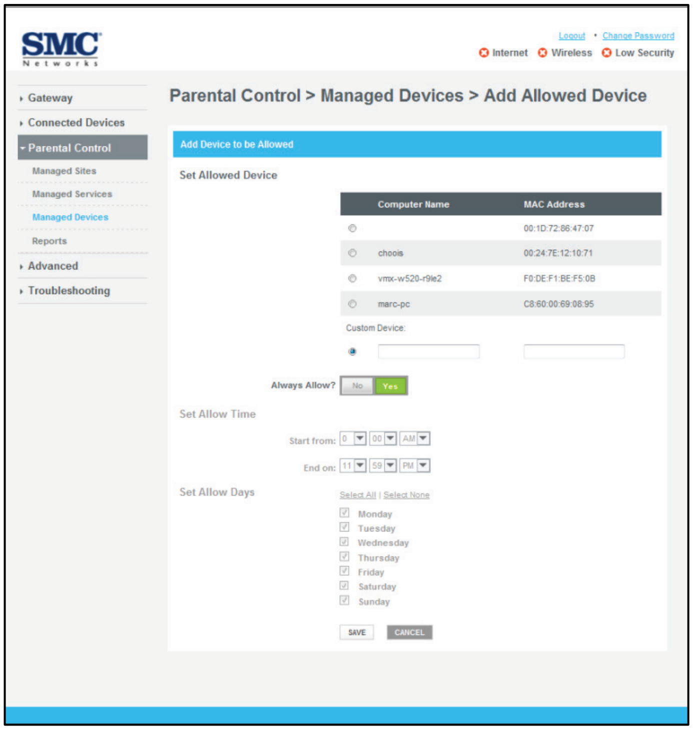
Using the Managed Devices page, you can create a list of devices that are allowed to connect to the Internet according to the administrator-defined rules you specify.

To add allowed devices on the Managed Devices page:

1. Under **Managed Devices**, check whether **Access Type** is configured to **Block All**. If it is set to **Allow All**, click **Block All**.

   Note: If you configured blocked devices, changing access types by clicking **Block All** displays a message that changing access types will remove the original device list. Click **OK** to continue and delete the original device list or click **Cancel** to cancel the operation and keep the original device list.

2. Under **Allowed Devices**, click the **+ADD ALLOWED DEVICE** button. The Add Allowed Device page appears (see Figure 42).
3. Complete the fields in the Add Allowed Device page (see Table 18).
4. Click **SAVE**. The name of the allowed device computer, its MAC address, and the allow date and time appear in the Allowed Devices table in the Managed Devices page.
5. Under **Managed Devices**, next to **Enable Managed Devices** on the Managed Sites page, click **Enable** to enable the managed devices configured on this page. (To disable the managed devices configured on this page, click **Disable**.)
6. After an allowed device has been added, you can edit it by clicking the **EDIT** button next to the device, changing the settings, and clicking **SAVE**.
7. To delete an allowed device, click the **X** next to it. When a precautionary message asks whether you want to delete the device, click **OK** to delete the device or **CANCEL** to retain it.



Parental Control > Managed Devices > Add Allowed Device

Add Device to be Allowed

Set Allowed Device

	Computer Name	MAC Address
○		00:1D:72:86:47:07
○	choois	00:24:7E:12:10:71
○	vmx-w520-r9le2	F0:DE:F1:BE:F5:0B
○	marc-pc	C8:60:00:69:08:95

Custom Device:

●

Always Allow? No [✓ Yes]

Set Allow Time

Start from: 0 ▾ 00 ▾ AM ▾

End on: 11 ▾ 59 ▾ PM ▾

Set Allow Days

Select All | Select None

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Figure 42. Add Allowed Device Page

Table 18. Add Allowed Device Page Options

Option	Description
Set Allowed Device	Select a device you want to allow. This can be a device whose computer name and MAC address are already displayed on this page or a custom device whose computer name and MAC address you enter under Custom Device.
Always Allow?	Select whether you want the Gateway to always allow this device. Choices are: • No = the Gateway does not always allow this device. Use Set Allow Time and Set Allowed Days to instruct the Gateway when to allow this device. • Yes = the Gateway always allows this device until you remove the allow.
Set Allow Time	If Always Allow? Is set to No, select the time when the Gateway is to allow this device. • Start from = select the start time when the Gateway starts allowing the device. • End on = select the end time when the Gateway stops allowing the device.
Set Allow Days	If Always Allow? Is set to No, select the days when the Gateway will allow this device. Links and check boxes are provided for selecting all days, no days, or individual days of the week. • Select All = click this link to select all seven days. • Select None = click this link to deselect all seven days. • Monday – Sunday = check the check boxes that correspond to the days when you want the Gateway to allow this device.
SAVE Button	After configuring the settings on this page, click this button to save your settings.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.

Blocking Devices

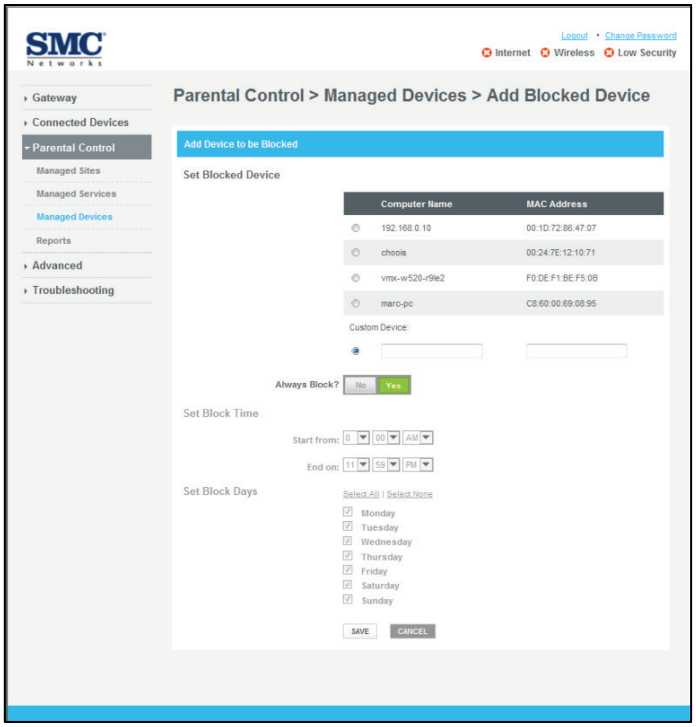
Using the Managed Devices page, you can create a list of devices that are blocked from connecting to the Internet according to the administrator-defined rules you specify.

To add blocked devices on the Managed Devices page:

1. Under **Managed Devices**, check whether **Access Type** is configured to **Allow All**. If it is set to **Block All**, click **Allow All**.

   Note: If you configured allowed devices, changing access types by clicking **Allow All** displays a message that changing access types will remove the original device list. Click **OK** to continue and delete the original device list or click **Cancel** to cancel the operation and keep the original device list.

2. Under **Blocked Devices**, click the **+ADD BLOCKED DEVICE** button. The Add Blocked Device page appears (see Figure 43).
3. Complete the fields in the Add Blocked Device page (see Table 19).
4. Click **SAVE**. The name of the blocked device computer, its MAC address, and the block date and time appear in the Blocked Devices table in the Managed Devices page.
5. Under **Managed Devices**, next to **Enable Managed Devices** on the Managed Sites page, click **Enable** to enable the managed devices configured on this page. (To disable the managed devices configured on this page, click **Disable**.)
6. After a blocked device has been added, you can edit it by clicking the **EDIT** button next to the device, changing the settings, and clicking **SAVE**.
7. To delete a blocked device, click the **X** next to it. When a precautionary message asks whether you want to delete the device, click **OK** to delete the device or **CANCEL** to retain it.



Parental Control > Managed Devices > Add Blocked Device

Add Device to be Blocked

Set Blocked Device

	Computer Name	MAC Address
○	192.168.0.10	00:1D:72:86:47:07
○	choois	00:24:7E:12:10:71
○	vmx-w520-r9le2	F0:DE:F1:BE:F5:0B
○	marc-pc	C8:60:00:69:08:95

Custom Device:

●

Always Block? No [✓ Yes]

Set Block Time

Start from: 0 00 AM

End on: 11 59 PM

Set Block Days

Select All | Select None

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
☑ Saturday
☑ Sunday

Figure 43. Add Blocked Device Page

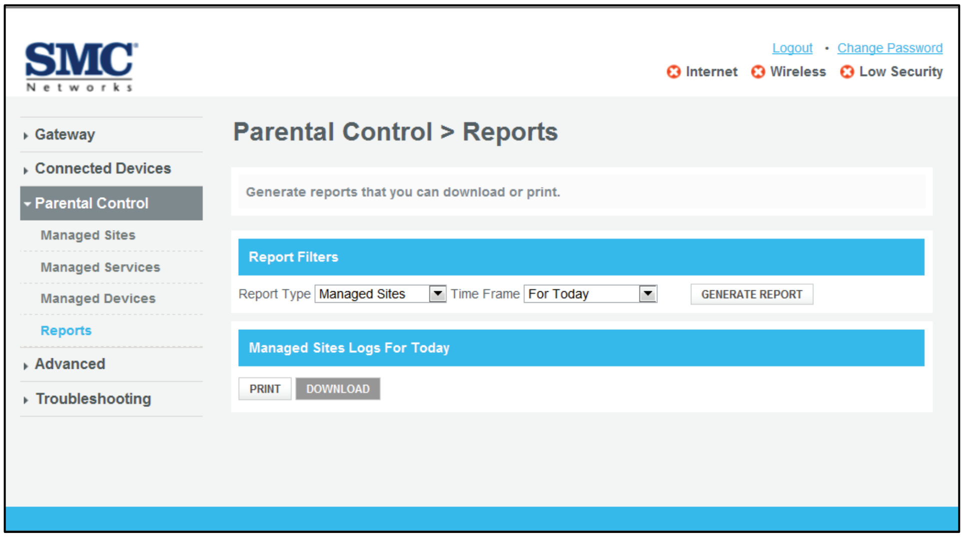
Table 19. Options for Add Blocked Device

Option	Description
Set Blocked Device	Select a device you want to block. This can be a device whose computer name and MAC address are already displayed in this dialog box or a custom device whose computer name and MAC address you enter under Custom Device.
Always Block?	Select whether you want the Gateway to always block this device. Choices are: • No = the Gateway does not always block this device. Use Set Block Time and Set Block Days to instruct the Gateway when to block this device. • Yes = the Gateway always blocks this device until you remove the block.
Set Block Time	If you set Always Block to No, select the time when the Gateway is to block this device. • Start from = select the start time when the Gateway starts blocking the device. • End on = select the end time when the Gateway stops blocking the device.
Set Block Days	If you set Always Block to No, select the days when the Gateway will block this device. Links and check boxes are provided for selecting all days, no days, or individual days of the week. • Select All = click this link to select all seven days. • Select None = click this link to deselect all seven days. • Monday – Sunday = check the check boxes that correspond to the days when you want the Gateway to block this device.
SAVE Button	After configuring the settings on this page, click this button to save your settings.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.

Reports Page

Path: **Parental Control > Reports**

The Reports page lets you generate, print, and download parental control reports. Reports are downloaded as text files.



Parental Control > Reports

Generate reports that you can download or print.

Report Filters

Report Type: Managed Sites   Time Frame: For Today

Managed Sites Logs For Today

Figure 44. Reports Page

Generating Reports

The **Report Filters** area on the Reports page lets you generate reports based on the type of report you want to generate and the timeframe that the report is to cover.

To generate a report:

1. In the **Report Filters** area on the Reports page, use the **Report Type** drop-down list to select the report you want to generate. Choices are:
   - Managed Sites
   - Managed Services
   - Managed Devices

2. Use the **Time Frame** drop-down list to select the timeframe that the report is to cover. Choices are:
   - For Today
   - From Yesterday
   - From Last week
   - From Last month
   - From Last 90 days
3. Click **GENERATE REPORT** to generate the report. The report appears on the Reports page. If the report has more than one page, use the **PREV** or **NEXT** button to move to the previous or next page.

Printing Reports

After you generate a report, you can print it.

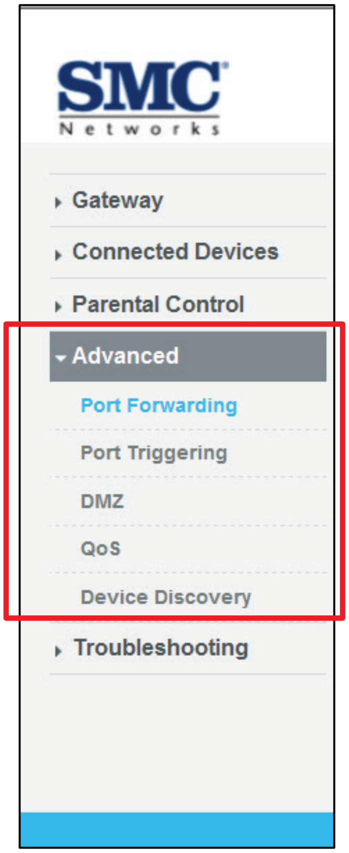
1. Click **PRINT**.
2. When the Print dialog box appears, select your printer and print options, and then click **Print**.

Downloading Reports

After you generate a report, you can download it as a text file.

1. Click **DOWNLOAD**.
2. When prompted, click **Open** to open the file or **Save** to save the file.

Advanced Menu



The **Advanced** menu contains pages for performing the following advanced configuration procedures:

- **Port Forwarding** - enables or disables port forwarding. See page 77.
- **Port Triggering** - enables or disables port triggering. See page 79.
- **DMZ** - configures a computer for unrestricted two-way Internet access by defining it as a virtual DMZ host. See page 82.
- **QoS** - configures the Gateway's QoS settings. See page 84.
- **Device Discovery** - configures the Gateway to automatically discover Universal Plug and Play (UPnP)-enabled devices on the network. See page 86.

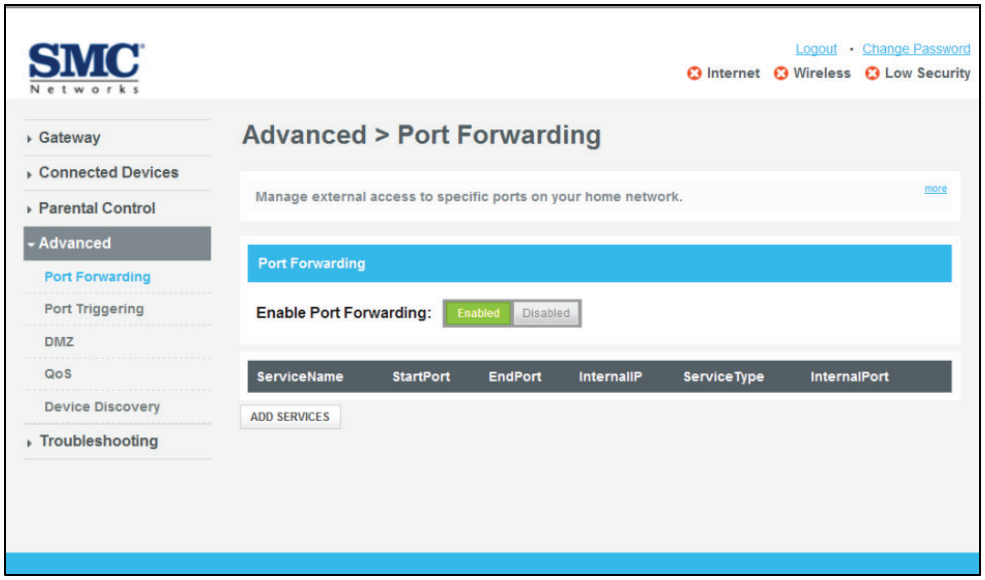
Port Forwarding Page

Path: **Advanced > Port Forwarding**

Port forwarding is a method of making a computer on your network accessible to computers on the Internet, even though you are behind the Gateway. The Port Forwarding page lets you configure port-forwarding services that allow Internet users access to predefined services such as HTTP (80), FTP (20/21), and AIM/ICQ (5190) as well as custom-defined (other) services. You perform port forwarding by redirecting the WAN IP address and the service port to a local IP address and service port.

Every program on your computer that uses the internet is programmed to send its packets through specific ports. Ports are virtual pathways over which information on the Internet travels. A good analogy is to think of ports like extensions on a phone system. Sometimes the ports are selected arbitrarily by the programmers of the software, but other times programmers use a standard port, depending on the functionality of the software. Examples of industry-standard uses for common ports are:

- HTML pages: port 80
- FTP file transferring: port 21
- POP3 email: port 110
- MSN Messenger: port 6901 and ports 6891-6900



Advanced > Port Forwarding

Manage external access to specific ports on your home network.

Port Forwarding

Enable Port Forwarding: [✓ Enabled] Disabled

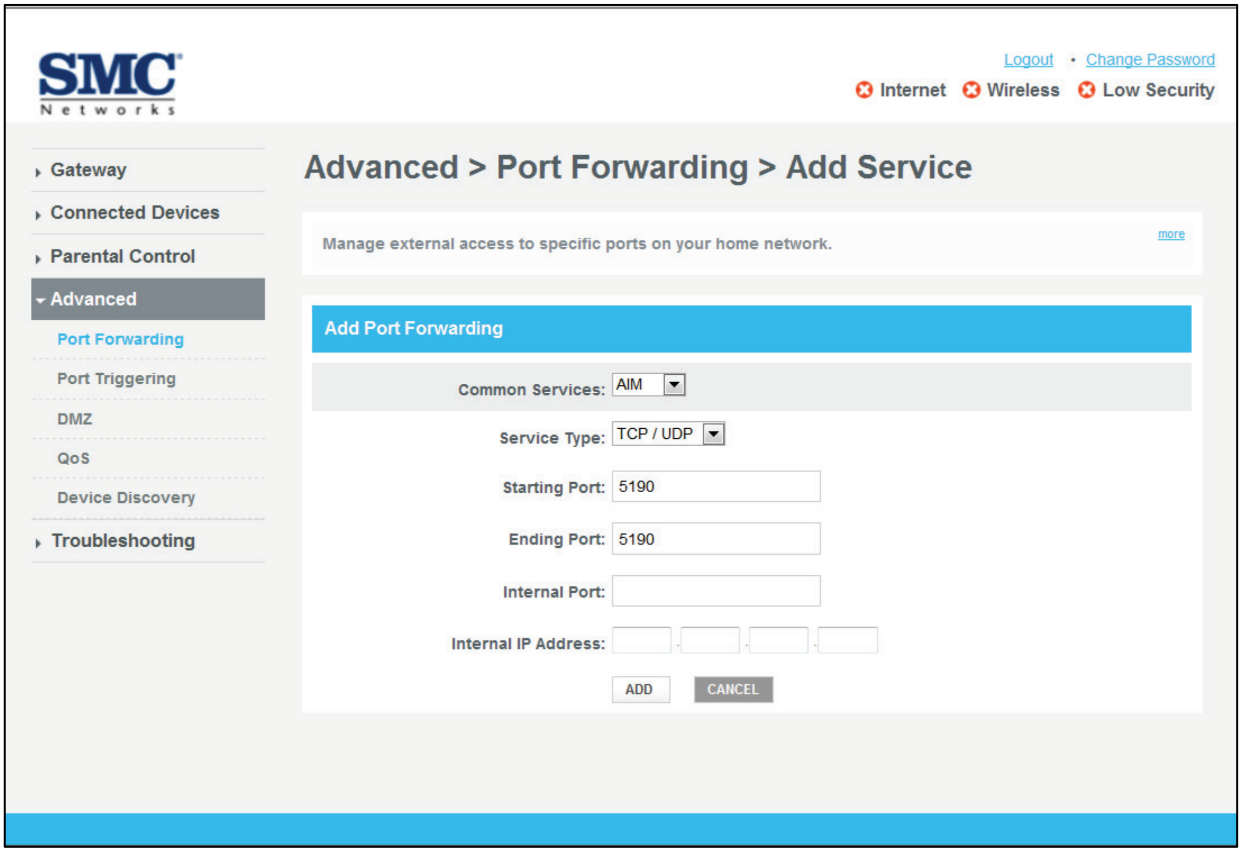
ServiceName	StartPort	EndPort	InternalIP	ServiceType	InternalPort

Figure 45. Port Forwarding Page

Adding a Port Forwarding Service

To add a port forwarding service on the Port Forwarding page:

1. Next to **Enable Port Forwarding**, click **Enabled**.
2. Click the **ADD SERVICES** button. The Add Service page appears (see Figure 46).
3. Complete the fields in Add Service page (see Table 20).
4. Click **ADD**. The port forwarding service appears in the Port Forwarding table on the Port Forwarding page.
5. To edit a blocked service, click the **EDIT** button next to the service you want to modify, edit the settings (see Table 20), and click **ADD**.
6. To delete a port forwarding rule, click the **X** next to the rule. When a precautionary message appears, click **OK** to delete the port forwarding rule or **CANCEL** to retain it.



Advanced > Port Forwarding > Add Service

Manage external access to specific ports on your home network.

Add Port Forwarding

Common Services:	AIM
Service Type:	TCP / UDP
Starting Port:	5190
Ending Port:	5190
Internal Port:	
Internal IP Address:	. . .

Figure 46. Add Service Page

Table 20. Add Service Page Options

Option	Description
Common Services	Select the service for which the port forwarding rule is being defined. Choices are: • AIM • FTP • IRC • HTTP • Other = enter the name of the service in the Other Service field.
Other Service	If you set Common Services to Other, enter the name of the service you want to add.
Service Type	Select the protocol associated with the service. Choices are: • TCP/UDP • TCP • UDP
Starting Port	Enter a starting port on which the service is provided.
Ending Port	Enter an ending port on which the service is provided.
Internal Port	Enter the port number of the LAN PC or server where requests are forwarded.
Internal IP Address	Enter the IP address of the LAN PC or server where requests are forwarded.
SAVE Button	After configuring the settings on this page, click this button to save your settings.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.

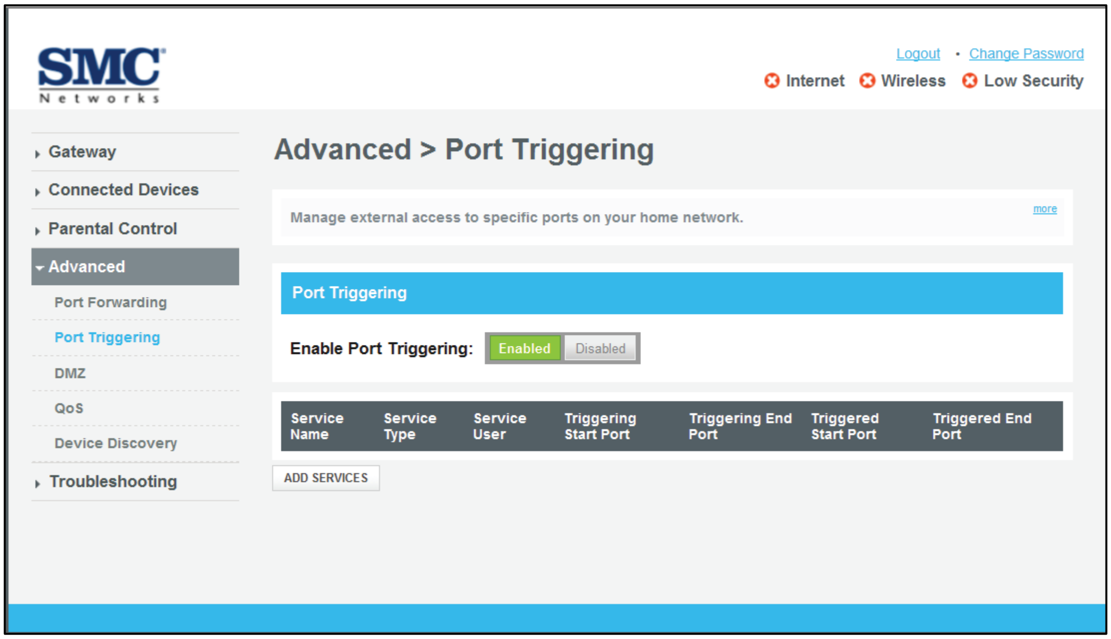
Port Triggering Page

Path: **Advanced > Port Triggering**

The Port Triggering page lets you manage external access to specific ports on your home network using automatic triggering.

When port triggering is enabled, the Gateway monitors outbound traffic. If the Gateway detects traffic on the specified outbound port, it remembers the IP address of the computer that sent the data, triggers the incoming port, and then forwards the incoming traffic to the triggering computer.

To use port triggering, you specify which service type and port number you want to track, along with other related parameters. This allows the Gateway to pass the special applications to the appropriate ports you specified.



Advanced > Port Triggering

Manage external access to specific ports on your home network.

Port Triggering

Enable Port Triggering: [✓ Enabled] Disabled

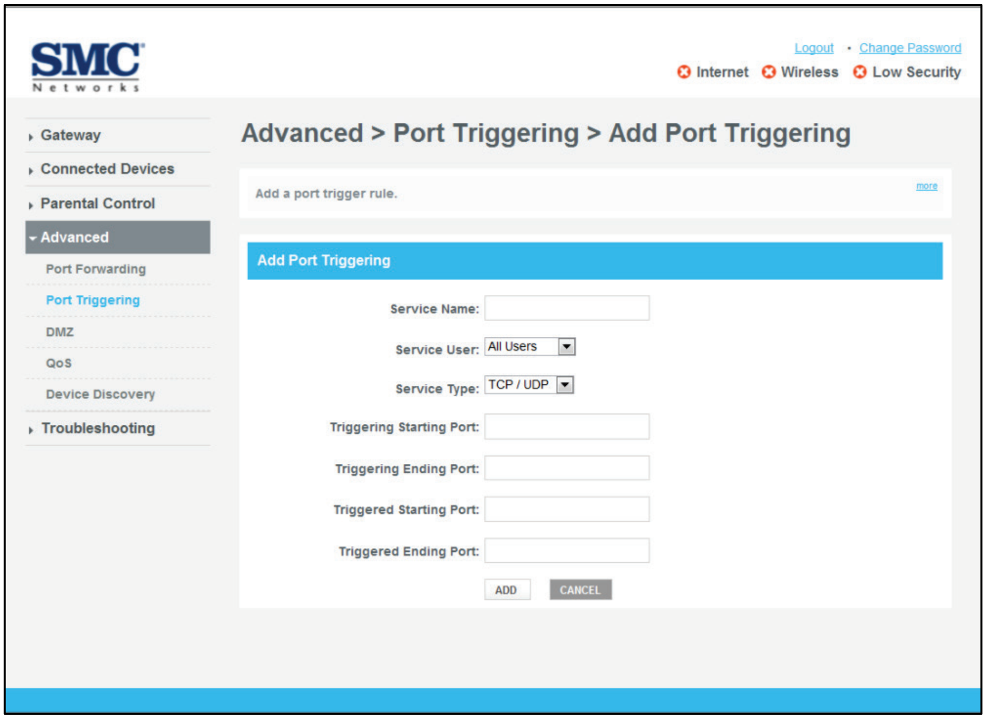
Service Name	Service Type	Service User	Triggering Start Port	Triggering End Port	Triggered Start Port	Triggered End Port

Figure 47. Port Triggering Page

Adding a Port Triggering

To define a port trigger on the Port Triggering page:

1. Next to **Enable Port Triggering**, click **Enabled**.
2. Click the **ADD SERVICES** button. The Add Port Triggering page appears (see Figure 48).
3. Complete the fields in Add Port Triggering page (see Table 21).
4. Click **ADD**. The port trigger appears in the Port Triggering table on the Port Triggering page.
5. To edit a port trigger, click the **EDIT** button next to the port trigger you want to modify, edit the settings (see Table 21), and click **ADD**.
6. To delete a port trigger, click the **X** next to the trigger. When a precautionary message appears, click **OK** to delete the port triggering rule or **CANCEL** to retain it.



Advanced > Port Triggering > Add Port Triggering

Add a port trigger rule.

Add Port Triggering

Service Name:

Service User: All Users

Service Type: TCP / UDP

Triggering Starting Port:

Triggering Ending Port:

Triggered Starting Port:

Triggered Ending Port:

Figure 48. Add Port Triggering Page

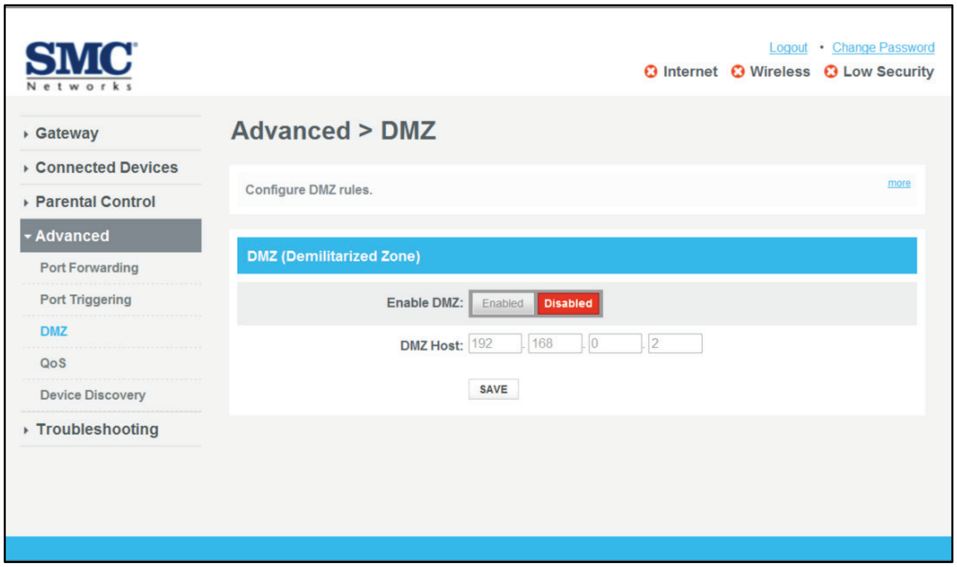
Table 21. Add Port Triggering Page Options

Option	Description
Service Name	Enter a name to identify the trigger. The name should be unique and allow you to differentiate this service from others you may define.
Service User	Select a service user from the user list. Choices are: • All Users • Single User = enter the IP address of the user in the IP Address field.
IP Address	If you set Service User to Single User, enter the IP address of the user.
Service Type	Select the type of protocol you want to use with the trigger. Choices are: • TCP/UDP • TCP • UDP For example, to track the H.323 protocol, the protocol type should be TCP.
Triggering Starting Point	Enter a starting port to be used as the trigger for the special application. For example, to track the H.323 protocol, the starting port should be 1720.
Triggering Ending Point	Enter an ending port to be used as the trigger for the special application. For example, to track the H.323 protocol, the ending port should be 1720.
Triggered Starting Port	Enter the starting port to be forwarded.
Triggered Ending Port	Enter the ending port to be forwarded.
ADD Button	After configuring the settings on this page, click this button to save your settings.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.

DMZ Page

Path: **Advanced > DMZ**

If you have a local client computer that cannot run an Internet application properly behind the firewall, you can configure the computer for unrestricted two-way Internet access by defining it as a Virtual DMZ host. A DMZ allows a single computer on your LAN to expose its ports to the Internet. When doing this, the exposed computer is no longer “behind” the firewall. Therefore, placing a computer in the DMZ should be considered temporary because the firewall is no longer able to provide any security to it.



Advanced > DMZ

Configure DMZ rules.

DMZ (Demilitarized Zone)

Enable DMZ: Enabled [✓ Disabled]

DMZ Host: 192 . 168 . 0 . 2

Figure 49. DMZ Page

Table 22. DMZ Page Options

Option	Description
Enable DMZ	Enables or disables the Gateway’s DMZ setting. Choices are: • Enabled = enable Gateway’s DMZ feature. • Disabled = disable Gateway’s DMZ feature. This selection makes the DMZ Host field unavailable.
DMZ Host	Enter the IP address of the computer to be used as the DMZ server.
SAVE Button	After configuring the settings on this page, click this button to save your settings.

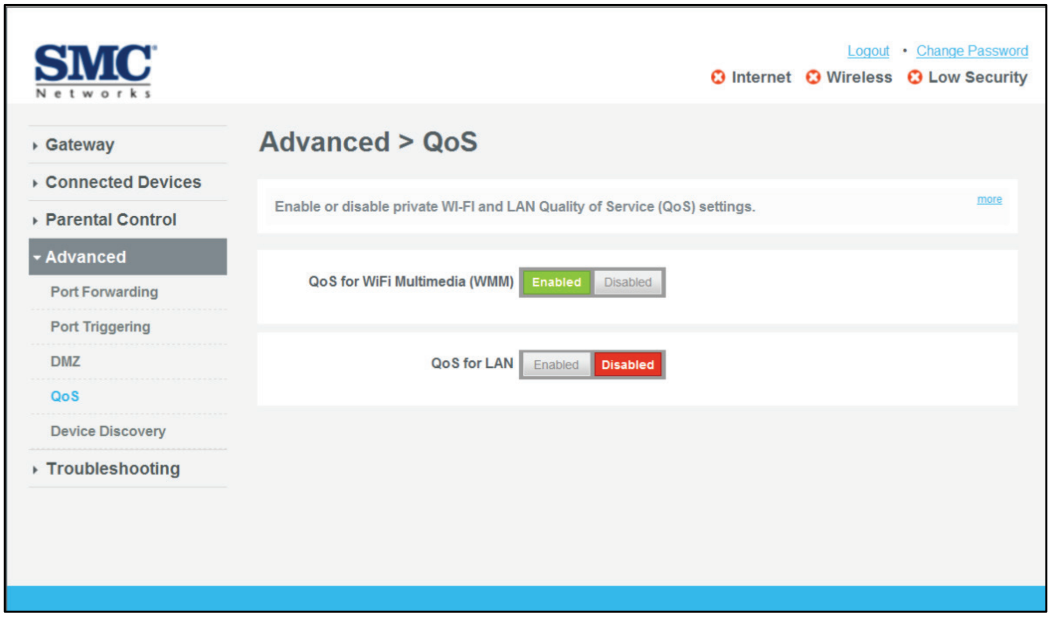
QoS Page

Path: **Advanced > QoS**

The QoS page lets you configure the Gateway to deliver better resource reservation control. Wireless networks offer an equal opportunity for all devices to transmit data from any type of application. Although this is acceptable for most applications, multimedia audio and video applications are particularly sensitive to the delay and throughput variations that result from this “equal opportunity” wireless access method. For multimedia applications to run well over a wireless network, a Quality of Service (QoS) mechanism is required to prioritize traffic types and provide an “enhanced opportunity” wireless access method.

The QoS page lets you enable or disable QoS settings.

Note: You can change QoS settings without having to reboot the Gateway.



Advanced > QoS

Enable or disable private WI-FI and LAN Quality of Service (QoS) settings.

QoS for WiFi Multimedia (WMM) [✓ Enabled] Disabled

QoS for LAN Enabled [✓ Disabled]

Figure 50. QoS Page

Table 23. QoS Page Options

Option	Description
QoS for WiFi Multimedia (WMM)	Determines whether the Gateway enables or disables Quality of Service for Wi-Fi Multimedia. Choices are: • Enabled = enable QoS for WMM. • Disabled = disable QoS for WMM.
QoS for LAN	Determines whether the Gateway enables or disables Quality of Service for the local-area network (LAN). Choices are: • Enabled = enable QoS for LAN. • Disabled = disable QoS for LAN.

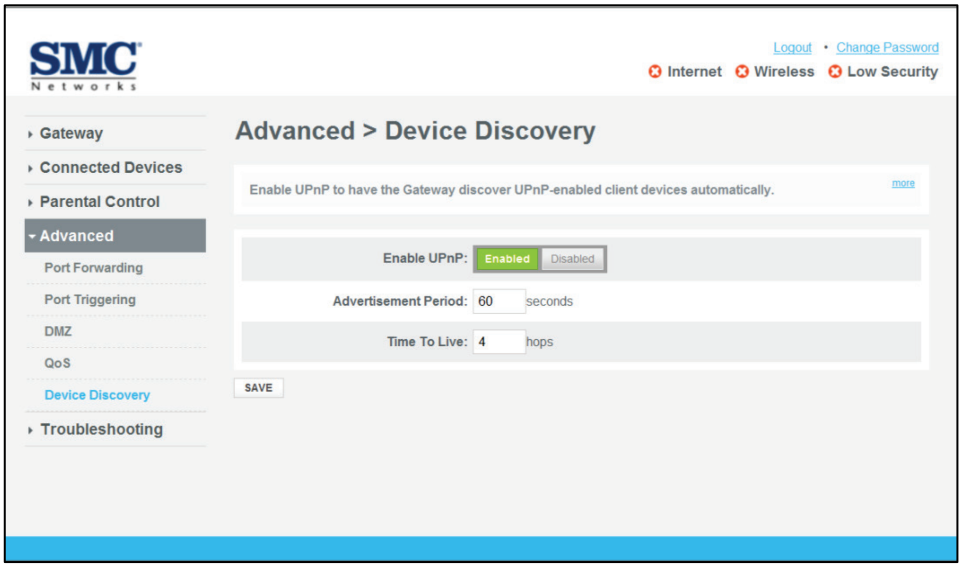
Device Discovery Page

Path: **Advanced > Device Discovery**

Universal Plug and Play (UPnP) is an architecture that allows for dynamic connectivity between devices on a network. The goal of UPnP is to support zero-configuration, "invisible" networking of devices including intelligent appliances, PCs, printers and other smart devices using standard protocols.

Using UPnP, devices can add themselves to a network dynamically, without requiring user intervention or configuration. An UPnP-enabled device can obtain an IP address, advertise its capabilities, learn about other connected UPnP devices, and then communicate directly with those devices. The same device can end its connection cleanly when it wishes to leave the UPnP community.

Using the Device Discovery page, you can configure the Gateway to discover UPnP-enabled devices on the network.



Advanced > Device Discovery

Enable UPnP to have the Gateway discover UPnP-enabled client devices automatically.

Enable UPnP: [✓ Enabled] Disabled

Advertisement Period: 60 seconds

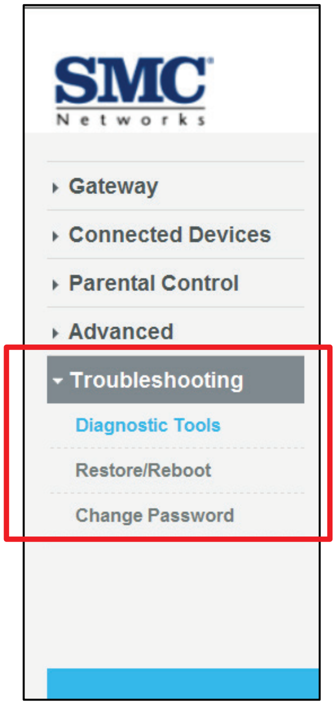
Time To Live: 4 hops

Figure 51. Device Discovery Page

Table 24. Device Discovery Page Options

Option	Description
Enable UPnP	Determines whether the Gateway's UPnP capabilities are enabled or disabled. Choices are: • Enabled = enable the Gateway's UPnP capabilities. • Disabled = disable the Gateway's UPnP capabilities.
Advertisement Period	Specify how often, in seconds, the Gateway broadcasts its UPnP information. This value can range from 1 to 2147483648 seconds. Short durations ensure that control points have current device status at the expense of additional network traffic. Long durations can compromise the freshness of the device status, but can significantly reduce network traffic.
Time To Live	Time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value of 4 hops should be fine for most home networks. If some devices are not being updated or reached correctly, increase this value slightly.
SAVE Button	After configuring the settings on this page, click this button to save your settings.

Troubleshooting Menu



The Troubleshooting menu provides the following pages to help you identify and resolve problems:

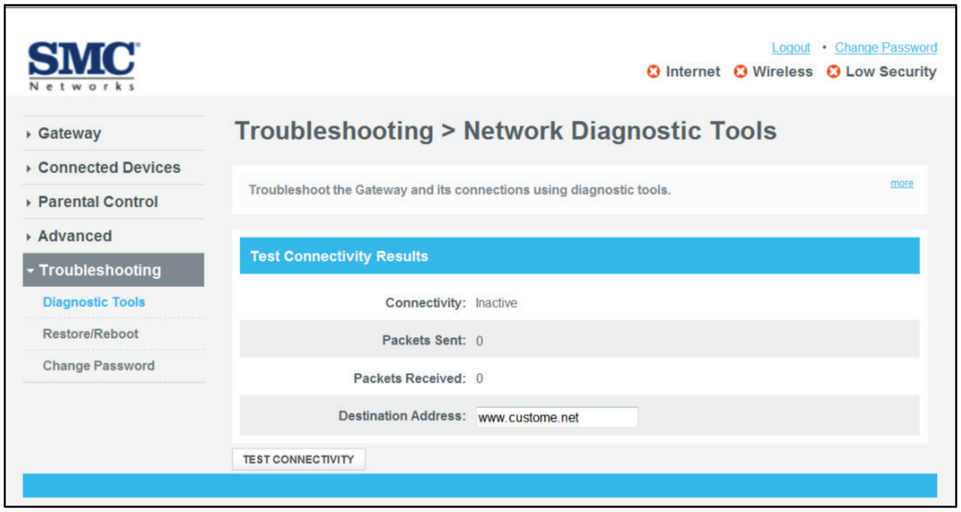
- **Diagnostic Tools** – lets you troubleshoot problems. See page 89.
- **Restore/Reboot** – restores Gateway settings or reboots the Gateway. See page 91.
- **Change Password** – changes the password used to log in to the Web management interface. See page 92.

Network Diagnostic Tools Page

Path: **Troubleshooting > Diagnostic Tools**

There may be times when you encounter a problem trying to reach a certain destination. If you examine the Gateway's configuration and operation and everything looks fine, the problem might be with a router up the line from the Gateway or with the line itself.

To help you identify such issues, use the Network Diagnostic Tools page to test connectivity to a destination or IP address.



Troubleshooting > Network Diagnostic Tools

Troubleshoot the Gateway and its connections using diagnostic tools.

Test Connectivity Results

Connectivity: Inactive

Packets Sent: 0

Packets Received: 0

Destination Address: www.custome.net

Figure 52. Network Diagnostic Tools Page

Testing Connectivity to a Destination Address

To test the Gateway’s connectivity to a destination address:

1. In the Network Diagnostic Tools page, under **Test Connectivity Results**, enter the IP address of a known working site in the **Destination Address** field.

Note: This procedure assumes that the destination address you enter is valid and operational.

2. Click the **TEST CONNECTIVITY** button. A message appears with the results. Click **OK** to remove the message. The **Packets Sent** and **Packets Received** counters show the number of packets sent and received during the test.

If the test succeeds, the destination you are having difficulty reaching is alive and physically reachable. If there are routers between the Gateway and the destination and you are having difficulty reaching, the problem might be at one of the routers.

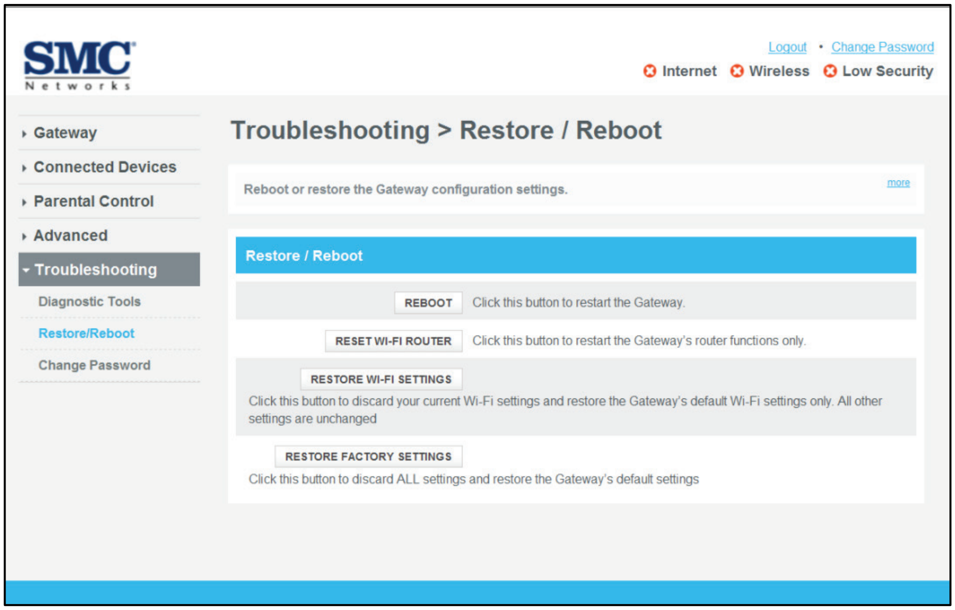
If the Gateway sent packets to a destination address, but did not receive any back, an error message appears; click **OK** to clear the message and confirm that you typed a valid destination address.

Restore/Reboot Page

Path: **Troubleshooting > Restore/Reboot**

The Restore / Reboot page provides buttons for performing the following activities:

- **REBOOT** = restarts the Gateway, but keeps overrides made to the factory default settings.
- **RESET WI-FI Router** = removes overrides made to the Gateway's Wi-Fi router settings only and returns those settings to their default values. All other Gateway settings remain unchanged.
- **RESTORE WIFI SETTINGS** = removes overrides made to the Gateway's wireless settings and returns the wireless settings to their default values. All other Gateway settings remain unchanged.
- **RESTORE FACTORY SETTINGS** = removes overrides made to all Gateway settings, including passwords, parental controls, and firewall, and returns the Gateway to its factory default values.



Reboot or restore the Gateway configuration settings.

REBOOT Click this button to restart the Gateway.

RESET WI-FI ROUTER Click this button to restart the Gateway's router functions only.

RESTORE WI-FI SETTINGS Click this button to discard your current Wi-Fi settings and restore the Gateway's default Wi-Fi settings only. All other settings are unchanged

RESTORE FACTORY SETTINGS Click this button to discard ALL settings and restore the Gateway's default settings

Figure 53. Restore / Reboot Page

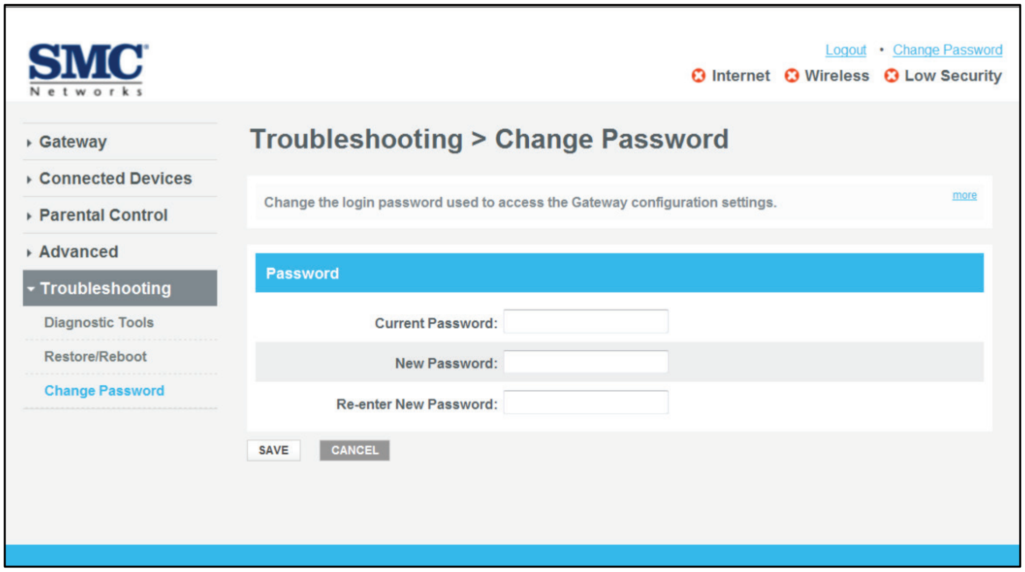
Change Password Page

Path : **Troubleshooting > Change Password**

The Change Password page lets you change the password used to log in to the Gateway's Web interface. For security, we recommend you change the default log in password the first time you log in to the Web management interface to protect the Gateway against unauthorized users.

This page is also available by clicking the **Change Password** link at the top-right area of the Web management interface.

Note: To change the Wi-Fi password, use the Gateway > Connection > WiFi page (see "Editing Private Wi-Fi Network Settings" on page 36).



Troubleshooting > Change Password

Change the login password used to access the Gateway configuration settings.

Password

Current Password:

New Password:

Re-enter New Password:

Figure 54. Change Password Page

Table 25. Change Password Options

Option	Description
Current Password	Enter the current case-sensitive password. For security purposes, every typed character is masked as a dot (•).
New Password	Enter the new case-sensitive password you want to use. The new password is case sensitive and can contain from 8 to 20 alphanumeric characters, but no spaces or special characters. For security purposes, every typed character is masked as a dot (•).
Re-enter New Password	Enter the same case-sensitive password you typed in the New Password field. For security purposes, every typed character is masked as a dot (•).
SAVE Button	After configuring the settings on this page, click this button to save your settings.
CANCEL Button	Click this button to discard your changes on this page and return to the previous page settings.

Appendix A - Wall-Mounting the Gateway

You can mounted the Gateway a wall by hanging the unit along its width using the two wall mount keyholes on the side of the unit.

⚠ **WARNING:** The Gateway should be wall mounted to concrete or plaster-wall-board. Before drilling holes, check the structure for potential damage to water, gas, or electric lines.

1. Use 3.5 mm x 40-50 mm (#6 x 1.5 to2 inches) pan head screws with a maximum screw head diameter of 6.5 mm (0.25 inches) to mount the Gateway.
2. Use a center punch to mark the location on the wall for each mounting screw. The screws must be oriented horizontal to each other and spaced at 101.6 mm (4 inches) on center.
3. Drill holes to a depth and diameter appropriate for the size and type of hardware you have selected.
4. Using a screwdriver, turn each screw until the head protrudes from the wall so that there is a distance of 12.5 mm (0.5 inches) between the wall and the underside of the screw head.
5. Orient the Gateway with the mounting keyholes above the mounting screws, and then slide the Gateway down so it stops against the top of the keyhole opening.
6. Reconnect the coaxial cable and Ethernet cables. Reconnect the power cord to the Gateway and the electrical outlet.

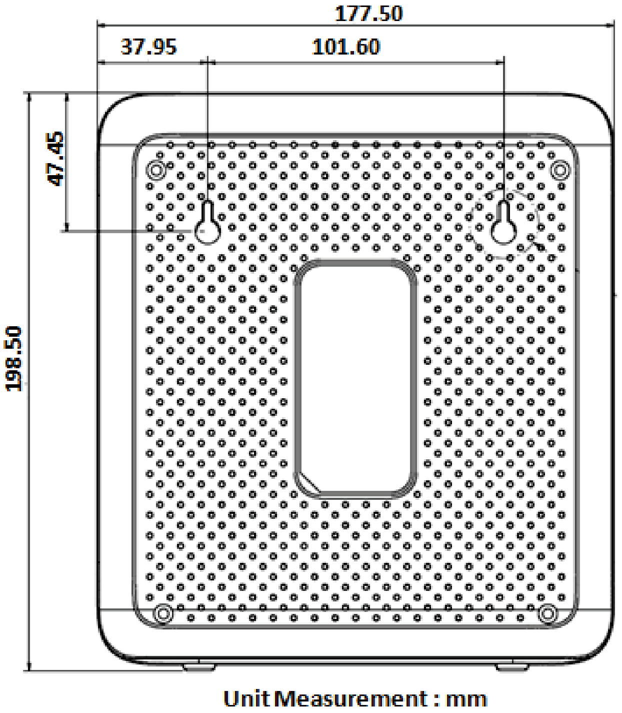


Figure 55. Wall-Mounting the Gateway (drawing not to scale)

Appendix B - Compliances

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 radio interference in a commercial environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures are necessary to correct the interference. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

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

The 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 the party responsible for compliance could void the user's authority to operate this equipment.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device is can be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

IMPORTANT NOTE:

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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 destination. The firmware setting is not accessible by the end user.

Note to CATV System Installer - This reminder is provided to call the CATV systems installer's attention to Section 820-40 of the National Electric Code (Section 54 of the Canadian Electrical Code, Part 1) which provide guideline for proper grounding and, in particular, specify 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.

Index

20 Mason
Irvine, CA. 92618
U.S.A.
http://na.smc.com

Document number: 3515GWT60080513