

Reference Manual for the **NETGEAR ProSafe Dual Band Wireless Access Point WAG102**

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

202-10062-03
September 2005



Technical Support

Please register to obtain technical support. Please retain your proof of purchase and warranty information.

To register your product, get product support or obtain product information and product documentation, go to <http://www.NETGEAR.com>. If you do not have access to the World Wide Web, you may register your product by filling out the registration card and mailing it to NETGEAR customer service.

You will find technical support information at:

<http://www.NETGEAR.com/> through the customer service area. If you want to contact technical support by telephone, see the support information card for the correct telephone number for your country.

© 2005 by NETGEAR, Inc. All rights reserved.

Trademarks

NETGEAR is a registered trademark of NETGEAR, INC. Windows is a registered trademark of Microsoft Corporation. Other brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice. All rights reserved.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Modifications made to the product, unless expressly approved by Netgear, could void the user's authority to operate the equipment. NETGEAR does not assume any liability that may occur due to such condition.

Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice

WAG102 ProSafe Dual Band Wireless Access Point



Tested to Comply
with FCC Standards
FOR HOME OR OFFICE USE

FCC ID: PY305200015

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

Placement and Range Guidelines

Indoors, computers can connect over 802.11 wireless networks at a maximum range of 500 feet (152.4 m) for 802.11b devices. However, the operating distance or range of your wireless connection can vary significantly, based on the physical placement of the wireless access point.

For best results, identify a location for your wireless access point according to these guidelines:

- Away from potential sources of interference, such as PCs, large metal surfaces, microwaves, and 2.4 GHz cordless phones.
- In an elevated location such as a high shelf that is near the center of the wireless coverage area for all mobile devices.

Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless access point.

To meet FCC and other national safety guidelines for RF exposure, the antennas for this device must be installed to ensure a minimum separation distance of 20cm (7.9 in.) from persons. Further, the antennas shall not be colocated with other transmitting structures.

FCC Statement

DECLARATION OF CONFORMITY

We Netgear,

4500 Great America Parkway

Santa Clara, CA 95054, USA

Tel: +1 408 907 8000

declare under our sole responsibility that the product(s)

WAG102 (*Model Designation*)

ProSafe Dual Band Wireless Access Point (Product Name)

complies with Part 15 of 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.

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

- Reorient or locate 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.

RF Exposure Warning for North America, and Australia

Warning! To meet FCC and other national safety guidelines for RF exposure, the antennas for this device (see below) must be installed to ensure a minimum separation distance of 20cm (7.9 in.) from persons. Further, the antennas shall not be colocated with other antenna or radio transmitter.

Antenna Statement for North America and Australia

In addition to its own 2 antennas, the WAG102 device has been approved for use with the following detachable antennas and antenna cables:

Approved Antennas	Antenna Gain and type	Approved Antenna Cable	Antenna Cable Length	Maximum Transmitted Power
NETGEAR ANT24D18	18 dBi, directional outdoor/indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	19 dBm + 18 dBi ant.
NETGEAR ANT2409	9 dBi, omnidirectional outdoor/indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	19 dBm + 9 dBi ant.
NETGEAR ANT2405	5 dBi, ceiling/wall indoor	NETGEAR ACC-10314-01 thru 05	1.5 m to 30 m	19 dBm + 5 dBi ant.

* WAG102 maximum radiated power in North America and Australia: 20 dBm – cable loss + antenna gain

Please go to www.netgear.com/go/wag102_fcc for an updated list of wireless accessories approved to be used with the WAG102 in North America and Australia.

Industry Canada Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference Causing Equipment Regulations ICES 003.

Cet appareil numérique de classe B respecte les exigences du règlement du Canada sur le matériel brouilleur NMB-003.

The device is certified to the requirements of RSS-210 for 2.4 GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

Product and Publication Details

Model Number:	WAG102
Publication Date:	September 2005
Product Family:	wireless access point
Product Name:	WAG102 ProSafe Dual Band Wireless Access Point
Home or Business Product:	Business
Language:	English
Publication Part Number:	202-10062-03

Contents

Reference Manual for the NETGEAR ProSafe Dual Band Wireless Access Point WAG102

Chapter 1

About This Manual

Audience, Scope, Conventions, and Formats	1-1
How to Use This Manual	1-2
How to Print this Manual	1-2

Chapter 2

Introduction

About the WAG102 ProSafe Dual Band Wireless Access Point	2-1
Key Features	2-2
802.11a/g Standards-based Wireless Networking	2-3
Autosensing Ethernet Connections with Auto Uplink	2-4
Compatible and Related NETGEAR Products	2-4
System Requirements	2-4
What's In the Box?	2-5
Hardware Description	2-6
Front Panel	2-6
Rear Panel	2-7

Chapter 3

Basic Installation and Configuration

Observing Placement and Range Guidelines	3-2
Cabling Requirements	3-2
Default Factory Settings	3-3
Understanding WAG102 Wireless Security Options	3-4
Installing the WAG102 Access Point	3-5
How to Log In to the WAG102 Using Its Default IP Address	3-11
Understanding Basic Wireless Settings	3-12

Wireless Settings 11a	3-12
Wireless Settings 11b/g	3-15
Understanding WEP/WPA Security Options	3-18
Before You Change the SSID and WEP Settings	3-20
How to Set Up and Test Basic Wireless Connectivity	3-23
How to Restrict Wireless Access by MAC Address	3-24
How to Configure WEP	3-25
How to Configure WPA and/or WPA2 with Radius	3-27
How to Configure WPA-PSK and/or WPA2-PSK	3-30
Changing the Basic IP Settings Options	3-31

Chapter 4
Management

Remote Management	4-1
Using Syslog and Activity Log Information	4-2
Viewing General and Statistical Information	4-3
General Information	4-3
Statistics	4-6
Viewing a List of Attached Devices	4-7
Upgrading the Wireless Access Point Software	4-8
Configuration File Management	4-9
Saving and Retrieving the Configuration	4-9
Restoring the WAG102 to the Factory Default Settings	4-10
Using the Reset Button to Restore Factory Default Settings	4-10
Rebooting the Access Point	4-10
Changing the Administrator Password	4-10

Chapter 5
Advanced Configuration

Redirecting Web Page Requests	5-1
Understanding Advanced Wireless Settings	5-2
Enabling Wireless Bridging and Repeating	5-4
How to Configure a WAG102 as a Point-to-Point Bridge	5-5
How to Configure Multi-Point Wireless Bridging	5-6
How to Configure Wireless Repeating	5-7

Chapter 6
Troubleshooting

No lights are lit on the access point.6-1
The Wireless LAN activity light does not light up.6-2
The LAN light is not lit.6-2
I cannot access the Internet or the LAN with a wireless capable computer.6-2
I cannot connect to the WAG102 to configure it.6-3
When I enter a URL or IP address I get a timeout error.6-3
Using the Reset Button to Restore Factory Default Settings6-4

Appendix A
Specifications

Specifications for the WAG102 A-1

Appendix B
Related Documents

Chapter 1

About This Manual

This chapter describes the intended audience, scope, conventions, and formats of this manual.

Audience, Scope, Conventions, and Formats


This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the Netgear website.


This guide uses the following typographical conventions:


Table 1-1. Typographical Conventions

<i>italics</i>	Emphasis, books, CDs, URL names
bold	User input
<code>fixed</code>	Screen text, file and server names, extensions, commands, IP addresses

This guide uses the following formats to highlight special messages:

	Note: This format is used to highlight information of importance or special interest.
---	--

	Tip: This format is used to highlight a procedure that will save time or resources.
---	--

	Warning: Ignoring this type of note may result in a malfunction or damage to the equipment.
---	--



Danger: This is a safety warning. Failure to take heed of this notice may result in personal injury or death.

This manual is written for the WAG102 Access Point according to these specifications:

Table 1-2. Manual Scope






Product Version	WAG102 ProSafe Dual Band Wireless Access Point
Manual Publication Date	September 2005



Note: Product updates are available on the NETGEAR, Inc. Web site at <http://kbserver.netgear.com/products/WAG102.asp>.

How to Use This Manual

The HTML version of this manual includes the following:

- Buttons,  and , for browsing forwards or backwards through the manual one page at a time
- A  button that displays the table of contents and an  button. Double-click on a link in the table of contents or index to navigate directly to where the topic is described in the manual.
- A  button to access the full NETGEAR, Inc. online knowledge base for the product model.
- Links to PDF versions of the full manual and individual chapters.

How to Print this Manual

To print this manual you can choose one of the following several options, according to your needs.

- **Printing a Page in the HTML View.**

Each page in the HTML version of the manual is dedicated to a major topic. Use the *Print* button on the browser toolbar to print the page contents.

- **Printing a Chapter.**

Use the *PDF of This Chapter* link at the top left of any page.

- Click the *PDF of This Chapter* link at the top right of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window.
- Your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at <http://www.adobe.com>.
- Click the print icon in the upper left of the window.



Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

- **Printing the Full Manual.**

Use the *Complete PDF Manual* link at the top left of any page.

- Click the Complete PDF Manual link at the top left of any page in the manual. The PDF version of the complete manual opens in a browser window.
- Click the print icon in the upper left of the window.



Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature.

Chapter 2

Introduction

This chapter introduces the NETGEAR WAG102 ProSafe Dual Band Wireless Access Point. Minimal prerequisites for installation are presented in [“System Requirements” on page 2-4](#).

About the WAG102 ProSafe Dual Band Wireless Access Point

The WAG102 ProSafe Dual Band Wireless Access Point is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

The WAG102 provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with a wireless network interface card (NIC) via an antenna. Typically, an individual in-building access point provides a maximum connectivity area with about a 300 foot radius. The WAG102 ProSafe Dual Band Wireless Access Point can support a small group of users in a range of several hundred feet. Most access points are rated between 10-30 users simultaneously.

The WAG102 ProSafe Dual Band Wireless Access Point acts as a bridge between the wired LAN and wireless clients. Connecting multiple WAG102 Access Points via a wired Ethernet backbone can further lengthen the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point to another and still maintain seamless connection to the network.

The auto-sensing capability of the WAG102 ProSafe Dual Band Wireless Access Point allows packet transmission at up to 108 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.

Key Features

The WAG102 Access Point is easy-to-use and provides solid wireless and networking support.

The following standards and conventions are supported:

- **Standards Compliant.** The Wireless Access Point complies with the IEEE 802.11a/g for Wireless LANs.
- **WEP support.** Support for WEP is included. 64-bit, 128-bit, and 152-bit keys are supported.
- **DHCP Client Support.** DHCP provides a dynamic IP address to PCs and other devices upon request. The WAG102 can act as a client and obtain information from your DHCP server.
- **SNMP Support.** Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.

The NETGEAR WAG102 provides solid functionality, including these features:

- **Multiple Operating Modes**
 - **Wireless Access Point.** Operates as a standard 802.11a/g.
 - **Point-to-Point Bridge.** In this mode, the WAG102 only communicates with another bridge-mode wireless station. You must enter the MAC address (physical address) of the other bridge-mode wireless station in the field provided. WEP should be used to protect this communication.
 - **Point-to-Multi-Point Bridge.** Select this only if this WAG102 is the “Master” for a group of bridge-mode wireless stations. The other bridge-mode wireless stations must be set to Point-to-Point Bridge mode, using this WAG102’s MAC address. They then send all traffic to this “Master”, rather than communicate directly with each other. WEP should be used to protect this traffic.
 - **Wireless Repeater.** In this half-duplex mode, the WAG102 only communicates with another repeater-mode wireless station. You must enter the MAC address of the root access point. WEP should be used to protect this communication.
- **Upgradeable Firmware.** Firmware is stored in a flash memory and can be upgraded easily, using only your Web browser, and can be upgraded remotely.
- **Access Control.** The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the WAG102 to gain access to your LAN.
- **Simple Configuration.** If the default settings are unsuitable, they are easy to change.

- **Hidden Mode.** The SSID is not broadcast, assuring only clients configured with the correct SSID can connect.
- **Secure Telnet Command Line Interface.** The Telnet command line interface enables direct access over the serial port and easy scripting of configuration of multiple WAG102s across an extensive network via the Ethernet interface. An SSH client is required.
- **Configuration Backup.** Configuration settings can be backed up to a file and restored.
- **Secure and Economical Operation.** Adjustable power output allows more secure or economical operation.
- **Power over Ethernet.** Power can be supplied to the WAG102 over the Ethernet port from any 802.3af compliant mid-span or end-span source such as the NETGEAR FSM7326P Managed Power over Ethernet Layer 3 managed switch.
- **Autosensing Ethernet Connection with Auto Uplink Interface.** Connects to 10/100 Mbps IEEE 802.3 Ethernet networks.
- **LED Indicators.** Power, test, LAN speed, LAN activity, and wireless activity are easily identified.

802.11a/g Standards-based Wireless Networking

The WAG102 ProSafe Dual Band Wireless Access Point provides a bridge between Ethernet wired LANs and 802.11a/g compatible wireless LAN networks. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Additionally, the WAG102 supports the following wireless features:

- Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Beacon generation
- Packet fragmentation and reassembly
- Short or long preamble
- Roaming among access points on the same subnet

Autosensing Ethernet Connections with Auto Uplink

The WAG102 can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation.

The wireless access point incorporates Auto Uplink™ technology. The Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a computer or an ‘uplink’ connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates any concerns about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Compatible and Related NETGEAR Products

For a list of compatible products from other manufacturers, see the Wireless Ethernet Compatibility Alliance Web site (WECA, see <http://www.wi-fi.net>).

The following NETGEAR products work with the WAG102 Access Point:

- WAG511 ProSafe 108 Mbps Dual Band PC Card
- WAG311 ProSafe 108 Mbps Dual Band PCI Card
- WG311T 802.11g 108 Mbps Wireless PCI Card
- WG511T 802.11g 108 Mbps Wireless CardBus Adapter
- WG511 802.11g 54 Mbps Wireless CardBus Adapter
- WG111 801.11g 54 Mbps Wireless Bridge

System Requirements

Before installing the WAG102, make sure your system meets these requirements:

- A 10/100 Mbps Local Area Network device such as a hub or switch
- The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it
- A 100-240 V, 50-60 HZ AC power source
- A Web browser for configuration such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above
- At least one computer with the TCP/IP protocol installed
- 802.11b or 802.11b-compliant devices, such as the NETGEAR WG511 Wireless Adapter

What's In the Box?

The product package should contain the following items:

- WAG102 ProSafe Dual Band Wireless Access Point
- Power adapter and cord (12 V dc, 1 A)
- Straight through Category 5 Ethernet cable
- WAG102 ProSafe Dual Band Wireless Access Point Installation Guide
- *Resource CD for the NETGEAR WAG102 ProSafe Dual Band Wireless Access Point* which includes this manual.
- Support Registration card

Contact your reseller or customer support in your area if there are any missing or damaged parts. You can refer to the Support Information Card for the telephone number of customer support in your area. You should keep the Support Information card, along with the original packing materials, and use the packing materials to repack the WAG102 if you need to return it for repair. To qualify for product updates and product warranty registrations, we encourage you to register on the NETGEAR Web site at: <http://www.NETGEAR.com>.

Hardware Description

The WAG102 front and rear hardware functions are described below.

Front Panel



Figure 2-1

The following table explains the LED indicators:

LED	DESCRIPTION
PWR	Power Indicator
Off	No power.
On	Power is on.
TEST	Self Test Indicator
Blink	Indicates self test, loading software, or system fault (if continues). Note: This LED may blink for a minute before going off.
100 LINK/ACT	Ethernet LAN Speed Indicator
Off	Indicates no 100 Mbps Ethernet link detected
Green Solid On	100 Mbps Fast Ethernet link detected, no activity
Green Blink	Indicates data traffic on the 100 Mbps Ethernet LAN.
10 LINK/ACT	Ethernet LAN Link Activity Indicator
Off	Indicates no 10 Mbps Ethernet link detected.
Green Solid On	10 Mbps Fast Ethernet link detected, no activity.
Green Blink	Indicates data traffic on the 10 Mbps Ethernet LAN.

LED	DESCRIPTION
802.11a WLAN	Wireless LAN Link Activity Indicator (5 GHz)
Off	Indicates no wireless link activity.
Green Blink	Wireless link activity.
802.11g WLAN	Wireless LAN Link Activity Indicator (2.4 GHz)
Off	Indicates no wireless link activity.
Green Blink	Wireless link activity.

Rear Panel



Figure 2-2

- **Left and Right Detachable Antenna**
The WAG102 provides two detachable antennas (2.4 GHz and 5 GHz).
- **Restore to Factory Defaults Button**
The restore to default button located between the Ethernet RJ-45 connector and the power socket restores the WAG102 to the factory default settings.
- **RJ-45 Ethernet Port**
Use the WAG102 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or POE switch.
- **Power Socket**
This socket connects to the WAG102 12V 1 A power adapter.

Chapter 3

Basic Installation and Configuration

This chapter describes how to set up your WAG102 ProSafe Dual Band Wireless Access Point for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b or 802.11a/g wireless adapters to do such things as connect to the Internet, or access printers and files on your LAN.



Note: Indoors, computers can connect over 802.11b or 802.11a/g wireless networks at ranges of several hundred feet or more. This distance can allow for others outside your area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The WAG102 Access Point provides highly effective security features which are covered in detail in [“Understanding WEP/WPA Security Options”](#) on page 3-18. Deploy the security features appropriate to your needs.

You need to prepare these three things before you can establish a connection through your wireless access point:

- A location for the WAG102 that conforms to the [“Observing Placement and Range Guidelines”](#) below.
- The wireless access point connected to your LAN through a device such as a hub, switch, router, or Cable/DSL gateway.
- One or more computers with properly configured 802.11b or 802.11a/g wireless adapters.

Observing Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.



Warning: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the WAG102. For complete performance specifications, see [Appendix A, “Specifications”](#).

For best results, place your wireless access point:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- Putting the antenna in a vertical position provides best side-to-side coverage. Putting the antenna in a horizontal position provides best up-and-down coverage.
- If using multiple access points, it is better if adjacent access points use different radio frequency Channels to reduce interference. The recommended Channel spacing between adjacent access points is 5 Channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Cabling Requirements

The WAG102 Access Point connects to your LAN via twisted-pair Category 5 Ethernet cable with RJ-45 connectors.

Default Factory Settings

When you first receive your WAG102, the default factory settings will be set as shown below. You can restore these defaults with the Factory Default Restore switch on the rear panel — see “[Rear Panel](#)” on page 2-7.

FEATURE	FACTORY DEFAULT SETTINGS
User Name (case sensitive)	admin
Password (case sensitive)	password
Operating Mode	Access Point
Access Point Name	netgearxxxxxx where xxxxxx are the last six digits of the wireless access point's MAC address
Built-in DHCP client	DHCP client disabled
IP Configuration	IP Address: 192.168.0.232 Subnet Mask: 255.255.255.0 Gateway: 0.0.0.0
11a Network Name (SSID)	NETGEAR_11a
11g Network Name (SSID)	NETGEAR_11g
Broadcast Network Name (SSID)	Enabled
802.11a Radio Frequency Channel	52
802.11g Radio Frequency Channel	11
AutoCell RF Management	Enabled
AutoCell Enhanced RF Security 'stealth' mode	Disabled
WEP/WPA	Disabled
Restricting connectivity based on MAC Access Control List	Disabled
Spanning Tree Protocol	Enabled
Time Zone	GMT
Time Zone Adjust for Daylight Saving Time	Disabled
SNMP	Enabled but Trap forwarding is disabled
Secure Telnet	Enabled

Understanding WAG102 Wireless Security Options

Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WAG102 Access Point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

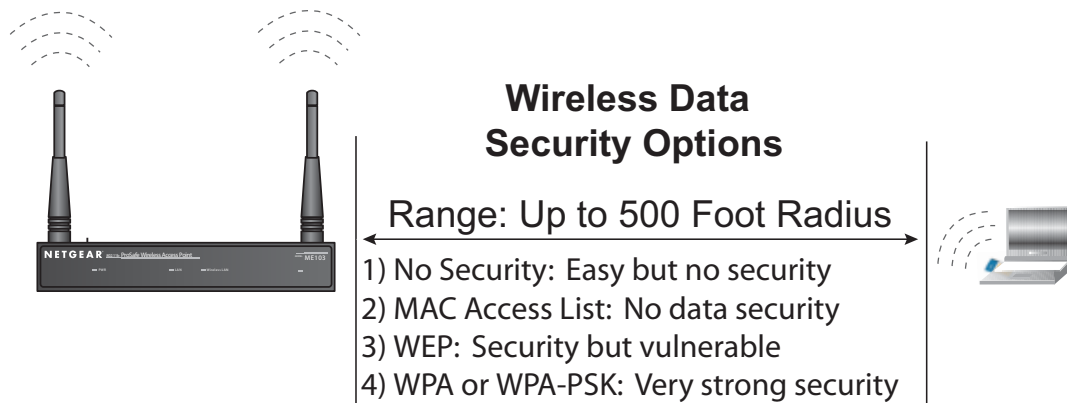


Figure 3-1

There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WAG102. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network ‘discovery’ feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.
- **Use WPA or WPA-PSK.** Wi-Fi Protected Access (WPA) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.

Installing the WAG102 Access Point

Before installing the WAG102 ProSafe Dual Band Wireless Access Point, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11b or 802.11a/g wireless adapters will be able to communicate with computers on the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown on [page 2-4](#).

1. Set up the WAG102 Access Point



Tip: Before mounting the WAG102 in a high location, first set up and test the WAG102 to verify wireless network connectivity.

- a. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.
 - b. Configure the computer with a static IP address of 192.168.0.36 and 255.255.255.0 for the Subnet Mask.
 - c. Connect an Ethernet cable from the WAG102 to the computer.
 - d. Turn on your computer, connect the power adapter to the WAG102 and verify the following:
 - The PWR power light goes on.
 - The LAN light of the wireless access point is lit when connected to a powered on computer.
 - The WLAN LEDs should be blinking.
2. Configure the WAG102 Ethernet port for LAN access.

- a. Connect to the WAG102 by opening your browser and entering <http://192.168.0.232> in the address field. A login window appears.



Figure 3-2

- b. Enter **admin** for the user name and **password** for the password, both in lower case letters. Click **OK**.
- c. The Web browser will then display the WAG102 General information page.

NETGEAR ProSafe Dual Band Wireless Access Point WAG102
settings

General

Setup

- Basic Settings
- Wireless Settings 11a
- Wireless Settings 11b/g

Security

- WEP/WPA Settings 11a
- WEP/WPA Settings 11b/g
- Radius Server Settings
- Access Control 11a
- Access Control 11b/g

Management

- Change Password
- Remote Management
- Upgrade Firmware
- Backup/Restore Settings
- Reboot AP

Information

- Activity Log
- Available Wireless Station List
- Statistics

Advanced

- Hotspot Settings
- Wireless Settings 11a
- Wireless Settings 11b/g
- Access Point Settings 11a
- Access Point Settings 11b/g

General

Access Point Information

Access Point Name	netgear001058
MAC Address	00:C0:02:00:10:50
Country / Region	United States
Firmware Version	V1.0.0

Current IP Settings

IP Address	192.168.0.232
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings 11a

Access Point Mode	Access Point
Operating Mode	802.11a Only
Wireless Network Name (SSID)	NETGEAR_11a
Channel / Frequency	84 / 5.320GHz (Automatic)
WEP / WPA	None

Current Wireless Settings 11b/g

Access Point Mode	Access Point
Operating Mode	Auto(802.11g/802.11b)
Wireless Network Name (SSID)	NETGEAR_11g
Channel / Frequency	11 / 2.462GHz (Automatic)
WEP / WPA	None

General Information Help

The Access Point General Information page displays current settings and statistics for your Access Point. As this information is read-only, any changes must be made on other pages.

Access Point Information: General information.

Current IP Settings: These are the current settings for IP address, Subnet Mask, Default Gateway and DHCP settings.

Current Wireless Settings: These are the current settings for the Access Point.

Figure 3-3

- d. When the wireless access point is connected to the Internet, click the Knowledge Base or the Documentation link under the Web Support menu to view support information or the documentation for the wireless access point.

If you do not click Logout, the wireless access point will wait 5 minutes after there is no activity before it automatically logs you out.

- e. Click the Basic Settings link to view the Basic Settings menu.

Basic Settings

Access Point Name: netgear001058

Country / Region: United States

IP Address

DHCP Client: Enable Disable

IP Address: 192 . 168 . 0 . 232

IP Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

DNS Server: 0 . 0 . 0 . 0

Time Zone

(GMT-08:00) Pacific Time ..US and Canada

Adjust for Daylight Saving Time

Current Time: 2004 Jan 1 00:19:24 GMT

Apply Cancel

Figure 3-4

- f. Configure the settings appropriate for your network. The default values are suitable for most users and situations.
- **Access Point Name:** This unique name is the access point NetBIOS name. The default Access Point Name is located on the bottom label of WAG102. You may modify the default name with a unique name up to 15 characters long. The default is netgearxxxxxx, where xxxxxxxx represents the last 6 digits of the WAG102 MAC address.
 - **Country/Region:** This field identifies the region where the WAG102 can be used. It may not be legal to operate the wireless features of the wireless access point in a region other than one of those identified in this field. Select your country or region from the drop-down list. This field displays the region of operation for which the wireless interface is intended.

If your country or region is not listed, please check with your local government agency or check our website for more information on which channels to use. The 802.11g wireless channel in use will be between 1 to 11 for US and Canada, 1 to 13 for Europe and Australia.

- **IP Address:** By default, the DHCP (Dynamic Host Configuration Protocol) client service is disabled. The default IP address is 192.168.0.232.

- You may enable the DHCP client to let the Access Point getting its TCP/IP configuration from the DHCP server on your network.
 - **DHCP Client:** The access point will get the IP address, subnet mask and the default gateway settings automatically from the DHCP server if DHCP is enabled.
 - **IP Address:** Type the IP address of your Access Point (factory default: 192.168.0.232).
 - **IP Subnet Mask:** The Access Point will automatically calculate the subnet mask based on the IP address that you assign. Otherwise, you can use 255.255.255.0 as the subnet mask.
 - **Default Gateway Address:** The Access Point will use this IP address default gateway for any traffic beyond the local network.
 - **DNS Server:** The Access Point will use this IP address as the Domain Name Server used by stations on your LAN.
 - **Time Zone:** You may select the appropriate local time zone for your Access Point from a list of all available time zones. The default is GMT.
3. Click the Wireless Settings 11a link in the Setup section of the main menu to view the Wireless Settings 11a menu.

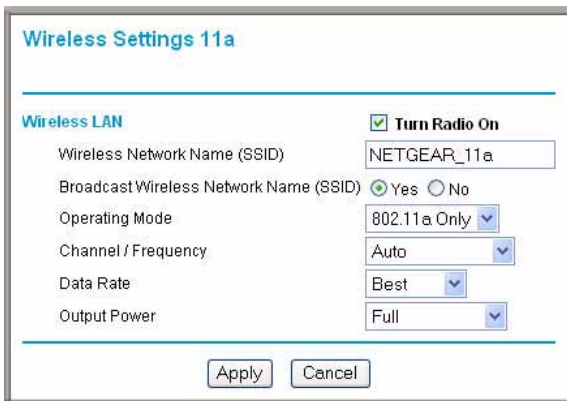


Figure 3-5

4. Click the Wireless Settings 11b/g link in the Setup section of the main menu to view the Wireless Settings 11b/g menu.

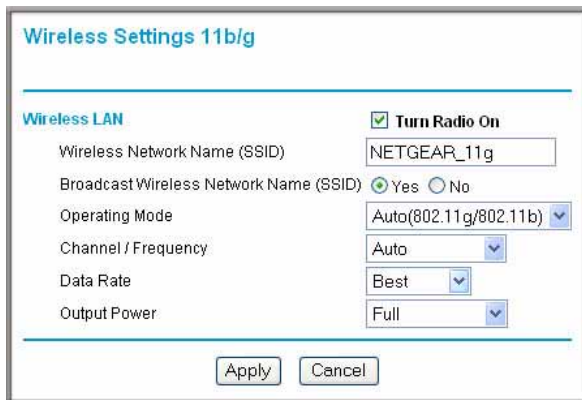



Figure 3-6

5. Configure the wireless interface for wireless access. See the online help or the [Understanding Basic Wireless Settings](#) topic of this Reference Manual for full instructions.

	Note: You must set the Regulatory Domain. It may not be legal to operate the wireless access point in a region other than one of those identified in this field.
---	---

Now that you have finished the setup steps, you are ready to deploy the WAG102 in your network. If needed, you can now reconfigure the computer you used in step 1 back to its original TCP/IP settings.

6. Deploy the WAG102 Access Point
 - a. Disconnect the WAG102 and position it where you will deploy it. The best location is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.
 - b. Lift the antenna on either side so that they are vertical.

Note: Consult the antenna positioning and wireless mode configuration information in the [Chapter 5, “Advanced Configuration”](#) chapter of the Reference Manual.

- c. Connect an Ethernet cable from your WAG102 Access Point to a LAN port on your router, switch, or hub.



Note: By default, WAG102 is set to with the DHCP client disabled. If your network uses dynamic IP addresses, you will need to change this setting.

- d. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet. The PWR, LAN, and Wireless LAN lights and should light up.

7. Verify Wireless Connectivity

Using a computer with an 802.11b or 802.11a/g wireless adapter with the correct wireless settings needed to connect to the WAG102 (SSID, WEP/WPA, MAC ACL, etc.), verify connectivity by using a browser such as Netscape or Internet Explorer to browse the Internet, or check for file and printer access on your network.



Note: If you are unable to connect, see [Chapter 6, “Troubleshooting”](#).”

How to Log In to the WAG102 Using Its Default IP Address

192.168.0.232 is the default IP address of your access point. The WAG102 is set by default with the DHCP client disabled.



Note: The computer you are using to connect to the WAG102 should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.

1. Open a Web browser such as Internet Explorer or Netscape Navigator.
2. Connect to the WAG102 by entering its default address of 192.168.0.232 into your browser. A login window appears.
3. Enter **admin** for the user name and **password** for the password, both in lower case letters. Click **OK**.



Figure 3-7

Once you have entered your access point name, your Web browser should automatically find the WAG102 Access Point and display the home page, as shown in [Figure 3-3 on page 3-7](#).

Understanding Basic Wireless Settings

Wireless Settings 11a

To configure the wireless settings of your wireless access point, click the Wireless Settings 11a link in the Basic section of the main menu of the browser interface. The Wireless Settings 11a menu will appear, as shown below.

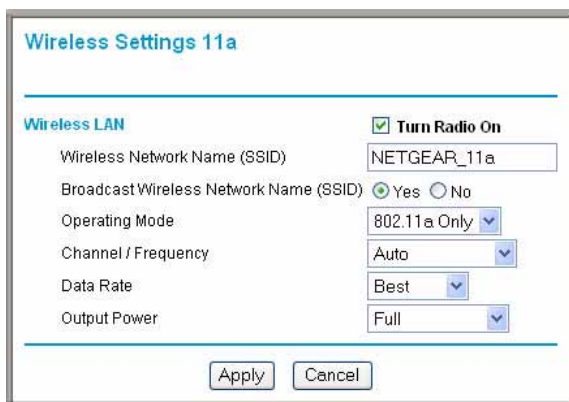


Figure 3-8

The Wireless Settings 11a menu options are discussed below:

- **Turn Radio On.** On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
- **Wireless Network Name (SSID):** The SSID is also known as the wireless network name. Enter a 32-character (maximum) service set ID in this field; the characters are case sensitive. The default is 802.11a only.

In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network will need to use the SSID.

When in infrastructure mode, this field defines the service set ID (SSID). The SSID assigned to the wireless node is required to match the access point SSID in order for the wireless node to communicate with the access point.

- A group of Wireless Stations and a single access point, all using the same ID (SSID), form a Basic Service Set (BSS).
 - Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other. However, some access points allow connections from wireless stations which have their SSID set to “any” or whose SSID is blank (null).
 - A group of wireless stations and multiple access points, all using the same ID (ESSID), form an Extended Service Set (ESS).
 - Different access points within an ESS can use different channels. To reduce interference, it is recommended that adjacent access points *should* use different channels.
 - As wireless stations physically move through the area covered by an ESS, they will automatically change to the access point which has the least interference or best performance. This capability is called roaming.
- **Broadcast Wireless Network Name (SSID):** If set to Yes, the Wireless Access Point will broadcast its SSID, allowing Wireless Stations that have a "null" (blank) SSID to adopt the correct SSID. If set to No, the SSID is not broadcast. The default is NETGEAR_11a.
 - **Operating Mode:** Select the desired wireless operating mode. The options are:
 - 11a Only – Only 802.11a wireless stations can be used. This selection cannot be changed.
 - **Channel/Frequency:** Select the channel you wish to use on your wireless LAN. The default is Auto.

It should not be necessary to change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers). Should this happen, you may need to experiment with different channels to see which is the best. See [“Wireless Communications:” in Appendix B](#) for more information on wireless channels.

- Besides the default Auto selection, you can select a fixed channel. This allows you to choose a channel that provides the least interference and best performance. In the USA and Canada, 13 channels are available.
- If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 8 (for example, use channels 36 and 44, or 44 and 52).
- In “Infrastructure” mode, wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the various access points are using the same SSID.
- **Data Rate:** Shows the available transmit data rate of the wireless network. The possible data rates supported are: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps. The default is Best.
- **Output Power:** Shows the available transmit power of the access point. The possible Tx power options are: Full, Half, Quarter, Eighth, and Minimum. The transmit power may varies depends on the local regulatory regulations. The default is Full.

Wireless Settings 11b/g

To configure the wireless settings of your wireless access point, click the Wireless Settings 11b/g link in the Basic section of the main menu of the browser interface. The Wireless Settings 11b/g menu will appear, as shown below.

Figure 3-9

The Wireless Settings 11b/g menu options are discussed below:

- **Turn Radio On.** On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
- **Wireless Network Name (SSID):** The SSID is also known as the wireless network name. Enter a 32-character (maximum) service set ID in this field; the characters are case sensitive. The default is NETGEAR_11g.

In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network will need to use the SSID.

When in infrastructure mode, this field defines the service set ID (SSID). The SSID assigned to the wireless node is required to match the access point SSID in order for the wireless node to communicate with the access point.

- A group of Wireless Stations and a single access point, all using the same ID (SSID), form a Basic Service Set (BSS).
- Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other. However, some access points allow connections from wireless stations which have their SSID set to “any” or whose SSID is blank (null).

- A group of wireless stations and multiple access points, all using the same ID (ESSID), form an Extended Service Set (ESS).
- Different access points within an ESS can use different channels. To reduce interference, it is recommended that adjacent access points *should* use different channels.
- As wireless stations physically move through the area covered by an ESS, they will automatically change to the access point which has the least interference or best performance. This capability is called roaming.
- **Broadcast Wireless Network Name (SSID):** If set to Yes, the Wireless Access Point will broadcast its SSID, allowing Wireless Stations that have a "null" (blank) SSID to adopt the correct SSID. If set to No, the SSID is not broadcast. The default is Yes.
- **Operating Mode:** Select the desired wireless operating mode. The options are:
 - Auto (11g/11b) – Both 802.11g and 802.11b wireless stations can be supported. This is the default.
 - 11g Only – Only 802.11g wireless stations can be used.
 - 11b Only – All 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode.
- **Channel/Frequency:** Select the channel you wish to use on your wireless LAN. The wireless channel in use will be between 1 to 11 for US and Canada, 1 to 13 for Europe and Australia. The default is Auto.

It should not be necessary to change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers). Should this happen, you may need to experiment with different channels to see which is the best. See [“Wireless Communications:” in Appendix B](#) for more information on wireless channels.

- Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available.



Note: Channel 6 is required for 108 Mbps data rate.

- If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).

- In “Infrastructure” mode, wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the various access points are using the same SSID.
- **Data Rate:** Shows the available transmit data rate of the wireless network. The possible data rates supported are: 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps, 12 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps and 108 Mbps. The default is Best



Note: The 108 Mbps option is available when the Channel/Frequency is set to channel 6 and the operating mode is set to 11g Only.

- **Output Power:** Shows the available transmit power of the access point. The possible Tx power options are: Full, Half, Quarter, Eighth, and Minimum. The transmit power may varies depends on the local regulatory regulations. The default is Full.

Understanding WEP/WPA Security Options

The figure below identifies the various WEP/WPA security options. A full explanation of these standards is available in “Wireless Communications:” in Appendix B.

WEP/WPA Settings 11a menu

WEP/WPA Settings 11b/g menu

Figure 3-10

The WEP/WPA Settings for 11a and 11b/g are explained as follows:

- **Network Authentication:** Specifies the Authentication type used: **Open System**, **Shared Key**, **Legacy 802.1x**, **WPA-PSK**, **WPA with Radius**, **WPA2-PSK**, **WPA-PSK and WPA2-PSK**, **WPA2 with Radius**, or **WPA and WPA2 with Radius**. The default is **Open System**.
 - **Open System.** If selected, you have the option of using WEP encryption or no encryption
 - **Shared Key.** If selected, you must use WEP encryption and enter at least one shared key.
 - **Legacy 802.1x.** If selected, you must configure the Radius Server Settings (see [Figure 3-13 on page 3-27](#)).
 - **WPA-PSK.** If selected, you must use TKIP encryption and enter the WPA passphrase (network key).

- **WPA with Radius.** If selected, you must configure the Radius Server Settings (see [Figure 3-13 on page 3-27](#)).
- **WPA2-PSK.** WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption and enter the WPA passphrase (network key).
- **WPA2 with Radius.** WPA2 is a later version of WPA. Only select this option if all clients support WPA2. If selected, you must use AES encryption and configure the Radius Server Settings (see [Figure 3-13 on page 3-27](#)).
- **WPA and WPA2 with Radius.** This selection allows clients to use either WPA (with TKIP encryption) or WPA2 (with AES encryption). If selected, you must use TKIP + AES encryption and configure the Radius Server Settings (see [Figure 3-13 on page 3-27](#)).
- **Data Encryption:** Select the desired option. If enabled (64 bit, 128 bit or 152 bits) the keys must be entered, and other wireless stations must use the same keys. The default is None.
 - The 64- and 128-bit WEP (Wired Equivalent Privacy) options are the standard encryption strength options.
 - The 152-bit key length is a proprietary WEP mode that will only work with other wireless devices that support this mode.
 - The TKIP option is automatically enabled when either **WPA with Radius** or **WPA-PSK** authentication type is selected.
 - The AES option is automatically enabled when **WPA2-PSK** or **WPA2 with Radius** authentication type is selected. Some clients may support AES encryption with WPA, but such an option is not supported by the WAG102 Access Point.
 - TKIP + AES. This option is automatically selected when **WPA and WPA2 with Radius** authentication type is selected. Broadcast packets always use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP and WPA2 clients use AES.
- **Passphrase:** To use the **passphrase** to generate the keys, enter a passphrase and click the **Generate Keys** button. You can also enter the keys directly. These keys must match the other wireless stations. The key length must be 8 to 63 characters.
- **Key 1, Key 2, Key 3, Key 4:** Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data. The four entries will be disabled if **Legacy 802.1x** or a **WPA/WPA2** authentication option is selected.
- **Re-authentication Time:** The time interval in seconds after which the supplicant will be authenticated again with the Radius Server. The default is 3600 seconds.

- **Global-key Update:** Check on this option to enable Re-keying of Global Key. The Global Key Re-Key can be done based on time interval in seconds or number of packets exchanged using the global key. The default is 3600 seconds.
- **Update if any station disassociates:** Check on this option to refresh global key when any stations disassociate with the wireless Access Point.
- **Wireless Client Security Separator:** The associated wireless clients will not be able to communicate with each other if this feature is enabled. The feature is intended for hotspots and other public-access situations to protect the privacy of each user. The default setting is Disable.

Before You Change the SSID and WEP Settings

802.11a Configuration

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID:** The Service Set Identification (SSID) identifies the wireless local area network. **NETGEAR_11a** is the default WAG102 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID:

- Authentication

Circle one: Open System or Shared Key. Choose Shared Key for more security.

Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the WAG102.

- WEP Encryption Keys

For all four 802.11a keys, choose the Key Size. Circle one: 64, 128, or 152 bits.

Key 1: _____

Key 2: _____

Key 3: _____

Key 4: _____

- WPA-PSK (Pre-Shared Key)

Record the WPA-PSK key:

Key: _____

- WPA RADIUS Settings

For WPA, record the following settings for the primary and secondary RADIUS servers:

Server Name/IP Address: Primary _____ Secondary _____

Port: _____

Shared Secret: _____

Use the procedures described in the following sections to configure the WAG102. Store this information in a safe place.

802.11b/g Configuration

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID:** The Service Set Identification (SSID) identifies the wireless local area network. **NETGEAR_11g** is the default WAG102 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID:

- Authentication

Circle one: Open System or Shared Key. Choose Shared Key for more security.

Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the WAG102.

- WEP Encryption Keys

For all four 802.11b/g keys, choose the Key Size. Circle one: 64, 128, or 152 bits.

Key 1: _____

Key 2: _____

Key 3: _____

Key 4: _____

- WPA-PSK (Pre-Shared Key)

Record the WPA-PSK key:

Key: _____

- WPA RADIUS Settings

For WPA, record the following settings for the primary and secondary RADIUS servers:

Server Name/IP Address: Primary _____ Secondary _____

Port: _____

Shared Secret: _____

Use the procedures described in the following sections to configure the WAG102. Store this information in a safe place.

How to Set Up and Test Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Log in to the WAG102 using its default address of <http://192.168.0.232> or at whatever IP address the unit is currently configured. Use the default user name of **admin** and default password of **password**, or whatever password you set up.
2. Select the Country/Region in which the wireless interface will operate.
3. Click the Wireless Settings link in the main menu of the WAG102.
4. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR_11a or NETGEAR-11g.



Note: The SSID of any wireless access adapters must match the SSID you configure in the WAG102 ProSafe Dual Band Wireless Access Point. If they do not match, you will not get a wireless connection to the WAG102.

5. Set the Channel. It should not be necessary to change the wireless channel unless you notice interference problems or are near another wireless access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless access point. For more information on the wireless channel frequencies see “[Wireless Communications:](#)” in [Appendix B](#).
6. For initial configuration and testing, leave the Data Encryption set to “None” and do not turn on the Access Control List.
7. Click Apply to save your changes.



Note: If you are configuring the WAG102 from a wireless computer and you change the SSID, channel, or security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the new settings.

8. Configure and test your PCs for wireless connectivity.


Program the wireless adapter of your PCs to have the same SSID and channel that you configured in the WAG102. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WAG102.

Once your PCs have basic wireless connectivity to the WAG102, you can configure the advanced wireless security functions.

How to Restrict Wireless Access by MAC Address

To restrict access based on MAC addresses, follow these steps:

1. Log in to the WAG102 using its default address of <http://192.168.0.232> or at whatever IP address the unit is currently configured. Use the default user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.

	<p>Note: When configuring the WAG102 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the wireless access point from a wired computer or from a wireless computer which is on the access control list to make any further changes.</p>
---	--

2. From the Security menu, click the Access Control 11a and 11bg links to display the Access Control menus shown below.

Access Control 11a menu



Access Control 11b/g menu



Figure 3-11

3. The optional Access Control window lets you block the network access privilege of the specified stations through the WAG102 Access Point. When you enable access control, the access point only accepts connections from clients on the selected access control list. This provides an additional layer of security.
 - a. Choose the Turn Access Control On to enable Access Control feature.
 - b. Select the desired Access Control Database options. The options are:
 - Local MAC Address Database – The Access Point will use the local MAC address table for Access Control. This is the default.
 - RADIUS MAC Address Database – The Access Point will use the MAC address table located on the external Radius server on the LAN for Access Control.
 - c. **Trusted Wireless Stations:** This lists any wireless stations you have entered. If you have not entered any wireless stations this list will be empty. To delete an existing entry, select it and then click the "Delete" button.
 - d. **Available Wireless Stations:** Select the stations from the wireless station list and click Add button to add to the Trusted Wireless Stations list.
 - e. **Add new Station Manually:** Use this to add the MAC address of the wireless stations to the Trusted Wireless Stations list.

Now, only devices on this list will be allowed to wirelessly connect to the WAG102.

How to Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the WAG102 using its default address of <http://192.168.0.232> or at whatever IP address the unit is currently configured Use the default user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.
2. Click the WEP/WPA Settings link in the main menu of the WAG102.

WEP/WPA Settings 11a menu

WEP/WPA Settings 11b/g menu

Figure 3-12

3. Choose Open System or Shared Key authentication.
 4. Select Data Encryption.
 5. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.
 - Automatic - enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
 - Manual - enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F) Select which of the four keys will be the default.
- See “[Wireless Communications:](#)” in [Appendix B](#) for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.
6. Click **Apply** to save your settings.



Note: If you use a wireless computer to configure WEP settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless access point from a wired computer to make any further changes.

How to Configure WPA and/or WPA2 with Radius



Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA, follow these steps:

1. Log in at the default LAN address of <http://192.168.0.232> with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. From the Security menu, click Radius Server Settings link to display the Radius Server Settings menu shown below.

Radius Server Settings

Primary Authentication Server

IP Address: 0 . 0 . 0 . 0

Port Number: 1812

Shared Secret:

Secondary Authentication Server

IP Address: 0 . 0 . 0 . 0

Port Number: 1812

Shared Secret:

Primary Accounting Server

IP Address: 0 . 0 . 0 . 0

Port Number: 1813

Shared Secret:

Secondary Accounting Server

IP Address: 0 . 0 . 0 . 0

Port Number: 1813

Shared Secret:

Figure 3-13

3. **Authentication/Access Control Radius Server Configuration:** This configuration is required for authentication using Radius. IP Address, Port No. and Shared Secret is required for communication with a Radius Server. A Secondary Radius Server for use if the Primary Radius Server fails.
 - **IP Address:** The IP address of the Radius Server. The default is 0.0.0.0
 - **Port Number:** Port number of the Radius Server. The default is 1812.
 - **Shared Secret:** This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
4. **Accounting Radius Server Configuration:** This configuration is required for accounting using a Radius Server. IP Address, Port No. and Shared Secret is required for communication with the Radius Server. A Secondary Radius Server can be configured for use if the Primary Radius Server fails.
 - **IP Address:** The IP address of the Radius Server. The default is 0.0.0.0
 - **Port Number:** Port number of the Radius Server. The default is 1813.
 - **Shared Secret:** This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
5. Click **Apply** to save your settings.

- Click **WEP/WPA Settings** in the Security menu.

WEP/WPA Settings 11a menu

WEP/WPA Settings 11a

WEP/WPA

Network Authentication: Open System

Data Encryption: Open System
Shared Key
Legacy 802.1X
WPA-PSK
WPA with Radius
WPA2-PSK
WPA-PSK and WPA2-PSK
WPA2 with Radius
WPA and WPA2 with Radius

Passphrase: _____

Key 1: ○ _____

Key 2: ○ _____

Key 3: ○ _____

Key 4: ○ _____

Advanced WPA 802.1x Parameters

Re-authentication Time: 3600 Seconds

Update Global Key every 3600 Seconds

Update if any station disassociates

Wireless Client Security Separation: No Yes

Apply Cancel

WEP/WPA Settings 11b/g menu

WEP/WPA Settings 11b/g

WEP/WPA

Network Authentication: Open System

Data Encryption: Open System
Shared Key
Legacy 802.1X
WPA-PSK
WPA with Radius
WPA2-PSK
WPA-PSK and WPA2-PSK
WPA2 with Radius
WPA and WPA2 with Radius

Passphrase: _____

Key 1: ○ _____

Key 2: ○ _____

Key 3: ○ _____

Key 4: ○ _____

Advanced WPA 802.1x Parameters

Re-authentication Time: 3600 Seconds

Update Global Key every 3600 Seconds

Update if any station disassociates

Wireless Client Security Separation: No Yes

Apply Cancel

Figure 3-14

- Choose **WPA with Radius**, **WPA2 with Radius**, or **WPA and WPA2 with Radius** from the list.
- Click **Apply** to save your settings.

How to Configure WPA-PSK and/or WPA2-PSK



Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 or above do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK, follow these steps:

1. Log in at the default LAN address of <http://192.168.0.232> with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the WEP/WPA Settings link in the main menu of the WAG102.
3. Choose **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK and WPA2-PSK** from the list.

WEP/WPA Settings 11a menu

WEP/WPA Settings 11b/g menu

Figure 3-15

4. Enter the pre-shared key passphrase.

- Click **Apply** to save your settings.

Changing the Basic IP Settings Options

The Basic IP Settings menu is under the Basic heading of the main menu. Use this menu to configure DHCP, static IP, and access point name settings.

Basic Settings

Access Point Name: netgear001888

Country / Region: United States

IP Address

DHCP Client: Enable Disable

IP Address: 192 . 168 . 0 . 232

IP Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 0 . 0 . 0 . 0

DNS Server: 0 . 0 . 0 . 0

Time Zone

(GMT) UK,GreenWich,Casablanca,Monrovia

Adjust for Daylight Saving Time

Current Time: 2004 Jan 4 23:56:10 GMT

Apply Cancel

Figure 3-16

- Access Point Name (NetBIOS)
Enter a new name for the wireless access point and click Apply to save your changes.
- The IP Address
The wireless access point is shipped preconfigured with its DHCP client disabled and with the following private static IP addresses:
 - IP Address — 192.168.0.232
 - IP Subnet Mask — 255.255.255.0
 - Gateway — 0.0.0.0

– Primary and Secondary DNS Servers — 0.0.0.0

If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu. These settings are only required if the “Use this IP address” radio button is chosen. Remember to click Apply to save your changes.

- Time Zone

Select the time zone location for your setting.



Note: You must have an Internet connection to get the current time.

Chapter 4 Management

This chapter describes how to use the management features of your WAG102 ProSafe Dual Band Wireless Access Point. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

Remote Management

The Remote Management screen lets you specify the simple network management protocol (SNMP) parameters.

Remote Management

SNMP Enable Disable

Public Community Name: public

Private Community Name: private

Manager IP address: 255 . 255 . 255 . 255

IP address to Receive Traps: 0 . 0 . 0 . 0

Apply Cancel

Figure 4-1

Fill out the remote management information:

- **SNMP**
 - Enable **SNMP** to allow the SNMP network management software, such as HP OpenView, to manage the wireless access point via SNMPv1/v2 protocol.
 - **Public Community Name:** The community string to allow the SNMP manager to read the wireless access point's MIB objects. The default is public.
 - **Private Community Name:** The community string to allow the SNMP manager to read and write the wireless access point's MIB objects. The default is private.

- **Manager IP Address:** Enter the IP address of the SNMP manager. If this is set to 255.255.255.255,
- **IP address to Receive Traps:** The IP address of the SNMP manager to receive traps sent from the wireless access point. The default is 0.0.0.0.

Using Syslog and Activity Log Information

The Information contains the Activity Log link you can use for setting up a syslog server and viewing activity log information.

1. From the main menu of the browser interface, under the Information heading, click the Activity Log link to view the list, shown below.

Activity Log

Activity Log Window

```
[2004 Jan 1 00:00:01] AP activated
[2004 Jan 1 00:00:56][2.4GHz] 00:0F:B5:0D:AB:19
authenticated
[2004 Jan 1 00:00:56][2.4GHz] 00:0F:B5:0D:AB:19 associated
[2004 Jan 1 00:02:02][2.4GHz] 00:0F:B5:0D:AB:19
disassociated
[2004 Jan 1 00:02:02][2.4GHz] 00:0F:B5:0D:AB:19
authenticated
[2004 Jan 1 00:02:02][2.4GHz] 00:0F:B5:0D:AB:19 associated
[2004 Jan 1 00:04:35][2.4GHz] 00:0F:B5:0D:AB:19
disassociated
[2004 Jan 1 00:04:57][2.4GHz] 00:0F:B5:0D:AB:19
```

Refresh Save As...

Enable SysLog

Syslog Server IP Address

Port

Apply Cancel

Figure 4-2

The Activity Log Window displays the Access Point system activity.

2. To update the Activity Log display, click Refresh. To save the log contents into a file on your PC, click Save As and save the file to a disk drive.

3. Enable the SysLog option if you have a SysLog server on your LAN. If enabled, you must enter the IP address of your SysLog server and the port number your SysLog server is configured to use.
 - SysLog Server IP address: The access point will send all the SysLog to the specified IP address if SysLog option is enabled. Default: 0.0.0.0
 - Port: The port number configured in the SysLog server on your LAN. Default: 514

Viewing General and Statistical Information

General Information

The General information screen provides a summary of the current WAG102 configuration settings. From the main Menu of the browser interface, click General to view the System Status screen, shown below.

General	
Access Point Information	
Access Point Name	netgear001888
MAC Address	00:C0:02:00:10:58
Country / Region	United States
Firmware Version	V1.0.0
Current IP Settings	
IP Address	192.168.0.232
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled
Current Wireless Settings 11a	
Access Point Mode	Access Point
Operating Mode	802.11a Only
Wireless Network Name (SSID)	NETGEAR_aaaaa
Channel / Frequency	56 / 5.280GHz (Automatic)
WEP / WPA	None
Current Wireless Settings 11b/g	
Access Point Mode	Access Point
Operating Mode	Auto(802.11g/802.11b)
Wireless Network Name (SSID)	NETGEAR_ggggg
Channel / Frequency	11 / 2.462GHz (Automatic)
WEP / WPA	None

Figure 4-3

This screen shows the following parameters:

Table 4-1. General Information Fields

Field	Description
Access Point Information	
Access Point Name (NetBIOS name)	The default name may be changed if desired.
MAC Address	Displays the Media Access Control address (MAC address) of the wireless access point's Ethernet port.
Country/Region	Displays the domain or region for which the wireless access point is licensed for use. It may not be legal to operate this wireless access point in a region other than one of those identified in this field.
Firmware Version	The version of the firmware currently installed.
Current IP Settings	
IP Address	The IP address of the wireless access point.
Subnet Mask	The subnet mask for the wireless access point.
Default Gateway	The default gateway for the wireless access point communication.
DHCP Client	Enabled indicates that the current IP address was obtained from a DHCP server on your network. Disabled indicated a static IP configuration.
Current Wireless Settings 11a	
Access Point Mode	Identifies the operating mode of the WAG102: Access Point, Point-to-point bridge, Point to Multi-point bridge or Repeater.
Operating Mode	Identifies the 802.11 operating mode of the WAG102.
Wireless Network Name (SSID)	Displays the wireless network name (SSID) being used by the wireless port of the wireless access point. The default is NETGEAR_11a.
Channel/Frequency	Identifies the channel the wireless port is using. By default, the channel is set automatically. To manually set the channel, see “Wireless Communications:” in Appendix B.
WEP/WPA	WEP/WPA setting.

Table 4-1. General Information Fields

Field	Description
Current Wireless Settings 11b/g	
Access Point Mode	Identifies the operating mode of the WAG102: Access Point, Point-to-point bridge, Point to Multi-point bridge, or Repeater.
Operating Mode	Identifies the 802.11 operating mode of the WAG102.
Wireless Network Name (SSID)	Displays the wireless network name (SSID) being used by the wireless port of the wireless access point. The default is NETGEAR_11g.
Channel/Frequency	Identifies the channel the wireless port is using. 11 is the default channel setting. By default, the channel is set automatically. To manually set the channel, see “Wireless Communications:” in Appendix B.
WEP/WPA	WEP/WPA setting.

Statistics

The Information - Statistics screen provides various LAN and WLAN statistics.

The screenshot shows a web interface titled "Statistics". It contains three tables of network statistics. The first table is for "Wired Ethernet", showing 0 packets and 0 bytes received, and 13780 packets and 1277629 bytes transmitted. The second table is for "Wireless 11a", showing 0 unicast, 54 broadcast, and 6 multicast packets, with a total of 60 packets and 13718 bytes transmitted. The third table is for "Wireless 11b/g", showing 7459 unicast, 10627 broadcast, and 404 multicast packets, with a total of 18490 packets and 575050 bytes transmitted. A "Refresh" button is located at the bottom of the screen.

Statistics		
Wired Ethernet		
	Received	Transmitted
Packets	0	13780
Bytes	0	1277629
Wireless 11a		
	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	54	13314
Multicast Packets	6	404
Total Packets	60	13718
Total Bytes	7724	1269821
Wireless 11b/g		
	Received	Transmitted
Unicast Packets	7459	8360
Broadcast Packets	10627	2742
Multicast Packets	404	6
Total Packets	18490	11108
Total Bytes	2117184	575050
Refresh		

Figure 4-4

Table 4-1. Statistics Fields

Field	Description
Wired Ethernet	Received/Transmitted
Packets	The number of packets sent since the WAG102 was restarted.
Bytes	The number of bytes sent since the WAG102 was restarted.
Wireless 11a	Received/Transmitted
Unicast Packets	The Unicast packets sent since the WAG102 was restarted.
Broadcast Packets	The Broadcast packets sent since the WAG102 was restarted.
Multicast Packets	The Multicast packets sent since the WAG102 was restarted.
Total Packets	The Wireless packets sent since the WAG102 was restarted.
Total Bytes	The Wireless bytes sent since the WAG102 was restarted.

Table 4-1. Statistics Fields (continued)

Field	Description
Wireless 11b/g	Received/Transmitted
Unicast Packets	The Unicast packets sent since the WAG102 was restarted.
Broadcast Packets	The Broadcast packets sent since the WAG102 was restarted.
Multicast Packets	The Multicast packets sent since the WAG102 was restarted.
Total Packets	The Wireless packets sent since the WAG102 was restarted.
Total Bytes	The Wireless bytes sent since the WAG102 was restarted.
Refresh button	Click the Refresh button to update the statistics on this screen.

Viewing a List of Attached Devices

The Available Wireless Station List contains a table of all IP devices associated with the wireless access point in the wireless network defined by the Wireless Network Name (SSID).

- From the main menu of the browser interface, under the Information heading, click the Available Wireless Station List link to view the list, shown below.

For each device, the table shows the Station ID, MAC address, IP Address, and Status (whether the device is allowed to communicate with the wireless access point or not).

If the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices.



Station ID	MAC Address	Type	IP Address	Status
1	00:0F:B5:0D:AB:19	802.11b/g	192.168.0.65	Associated

Refresh

Figure 4-5

- To force the wireless access point to look for associated devices, click the Refresh button.



Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This enables extending the reach of the wireless network and allows users to roam from one access point to another, providing seamless network connectivity. Under these circumstances, be aware that only the stations associated with this access point will be presented in the Available Station List.

Upgrading the Wireless Access Point Software



Note: When uploading software to the WAG102 Access Point, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload may fail, corrupt the software, and render the WAG102 completely inoperable.

You cannot perform the firmware upgrade from a workstation connected to the WAG102 via a wireless link. The firmware upgrade must be performed via a workstation connected to the WAG102 via the Ethernet LAN interface.

The software of the WAG102 Access Point is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR. Upgrade files can be downloaded from Netgear's Web site. If the upgrade file is compressed (.ZIP file), you must first extract the image (.RMT) file before sending it to the wireless access point. The upgrade file can be sent using your browser.



Note: The Web browser used to upload new firmware into the WAG102 must support HTTP uploads, such as Microsoft Internet Explorer 6.0 or above, or Netscape Navigator 4.78 or above.

1. Download the new software file from NETGEAR, save it to your hard disk, and unzip it.
2. From the main menu Management section, click the Upgrade Firmware link to display the screen below.

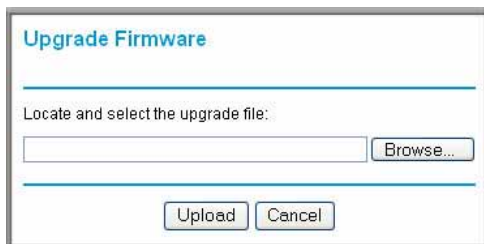


Figure 4-6

3. In the Upgrade Firmware menu, click the Browse button and browse to the location of the image (.RMG) upgrade file.
4. Click Upload.

When the upload completes, your wireless access point will automatically restart. The upgrade process typically takes about one minute.

In some cases, you may need to reconfigure the wireless access point after upgrading.

Configuration File Management

The WAG102 Access Point settings are stored in the wireless access point in a configuration file. This file can be saved (backed up) to a user's computer, retrieved (restored) from the user's computer, or cleared to factory default settings.

From the main menu Management heading, click the Backup/Restore Settings link to bring up the menu shown below.

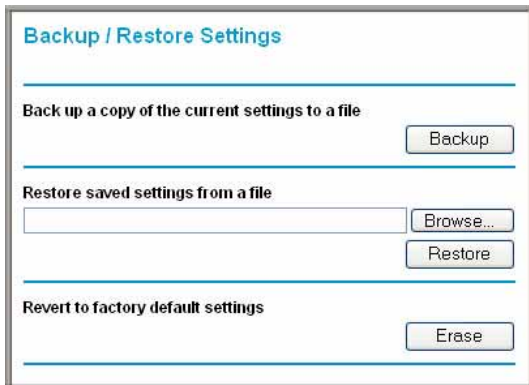


Figure 4-7

The three options displayed are described in the following sections:

Saving and Retrieving the Configuration

The Backup/Restore Settings menu allows you to save or retrieve a file containing your wireless access point's configuration settings.

To save your settings, click the Backup button. Your browser will extract the configuration file from the wireless access point and prompts you for a location on your computer to store the file. You can give the file a meaningful name at this time, such as **WAG102.cfg**.

To restore your settings from a saved configuration file, enter the full path to the file on your computer or click the Browse button to locate the file. When you have located it, click the Restore button to upload the file. After completing the upload, the WAG102 will reboot automatically.

Restoring the WAG102 to the Factory Default Settings

It is sometimes desirable to restore the wireless access point to the factory default settings. This can be done by using the Erase button, which restores all factory settings. After a restore, the wireless access point's password will be **password**, the WAG102's DHCP client is disabled, the default LAN IP address is 192.168.0.232, and the access point name is reset to the name printed on the label on the bottom of the unit.

Using the Reset Button to Restore Factory Default Settings

To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the wireless access point (see [Figure 2-2 on page 2-7](#)). The reset button has two functions:

- **Reboot.** When pressed and released, the Wireless Access Point will reboot (restart).
- **Reset to Factory Defaults.** This button can also be used to clear all data and restore all settings to the factory default values.

To clear all data and restore the factory default values:

1. Power off the WAG102 and power it back on.
2. Use something with a small point, such as a pen, to press the Reset button in and hold it in for at least 5 seconds.
3. Continue holding the Reset Button until the LEDs blink twice.
4. Release the Reset Button.

The factory default configuration has now been restored and the WAG102 is ready for use.

Rebooting the Access Point

1. Click **Reboot AP** under Management on the main menu.
2. Click **Apply**.

Changing the Administrator Password

The default password is **password**. Change this password to a more secure password. You cannot change the administrator login name.

1. From the main menu of the browser interface, under the Management heading, click Change Password to bring up the menu shown below.



The image shows a 'Change Password' dialog box with a light blue border. At the top left, the title 'Change Password' is displayed in blue text. Below the title, there are three text input fields: 'Current Password', 'New Password', and 'Repeat New Password'. Each field is followed by a small rectangular input box. Below these fields, there is a radio button group for 'Restore Default Password', with 'Yes' and 'No' options. The 'No' option is selected, indicated by a filled circle. At the bottom of the dialog box, there are two buttons: 'Apply' and 'Cancel'.

Figure 4-8

2. To change the password, first enter the old password and then enter the new password twice. Click Apply to save your change.

Chapter 5

Advanced Configuration

This chapter describes how to configure the advanced features of your WAG102 ProSafe Dual Band Wireless Access Point:

- **Hotspot Settings:** Redirect HTTP web page requests to the server you specify.
- **Wireless Settings:** Configure advanced wireless LAN parameters.
- **Access Point Settings:** Enable wireless bridging and repeating.

These features can be found under the Advanced heading in the main menu.

Redirecting Web Page Requests

To redirect HTTP (TCP port 80) requests to a web server:

1. In the Advanced section of the main menu, select the Hotspot Settings link.

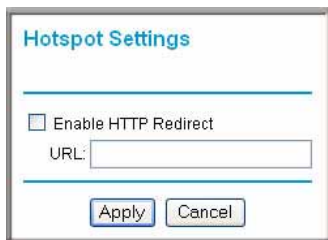


Figure 5-1

2. Click the Enable HTTP Redirect checkbox so that a checkmark is displayed
3. Enter the URL of the web server where you want HTTP requests to be redirected.
4. Click on the Apply button.

Understanding Advanced Wireless Settings

The default advanced wireless LAN parameter settings usually work well and are best for general-purpose use. The settings in these menus can be used to fine-tune performance to the capabilities of your wireless clients.

Advanced Wireless Settings 11a menu

Advanced Wireless Settings 11b/g menu

Figure 5-2

- **Enable Super-A/G Mode:** Enable Super-A/G mode may increase the overall wireless performance if you have compatible wireless clients. The default is Disable.
- **WMM Support:** Wireless Multimedia, a subset of the 802.11e standard. WMM allows wireless traffic to be assigned a priority depending on the kind of data in the packet. Time-dependent information like video or audio will be given a higher priority than normal traffic. For WMM to function correctly, your wireless clients must also support WMM. The default is Disable.



Note: WMM is automatically disabled if you configure your device as a wireless bridge or repeater.

- **RTS Threshold:** Request to Send Threshold. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet as soon as it has waited for the RTS threshold silence period. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. The default is 2346.
- **Fragmentation Length:** This is the maximum packet size used for fragmentation. Packets larger than the size programmed in this field will be fragmented. The Fragment Threshold value must be as large or larger than the RTS Threshold value. The default is 2346.
- **Beacon Interval:** The Beacon Interval. Specifies the interval time between 20ms and 1000ms for each beacon transmission. The default is 100.
- **DTIM Interval:** The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 255. The default is 1.
- **Preamble Type (11b/g only):** A long transmit preamble may provide a more reliable connection or slightly longer range. A short transmit preamble gives better performance. Auto will automatically handle both long and short preamble. the default is Auto.

Enabling Wireless Bridging and Repeating

The WAG102 ProSafe Dual Band Wireless Access Point lets you build large bridged wireless networks.

Advanced Access Point Settings 11a menu Advanced Access Point Settings 11b/g menu

The figure shows two side-by-side screenshots of the configuration interface for the WAG102. The left screenshot is titled 'Advanced Access Point Settings 11a' and the right is 'Advanced Access Point Settings 11b/g'. Both screens have a section for 'Access Point Mode'. In both, the 'Enable Wireless Bridging and Repeating' checkbox is unchecked. Under this, there are three radio button options: 'Wireless Point-to-Point Bridge', 'Wireless Point to Multi-Point Bridge', and 'Repeater with Wireless Client Association'. Each radio button option has an associated 'Enable Wireless Client Association' checkbox and one or more MAC address input fields. The 11a menu has one Remote MAC Address field, while the 11b/g menu has four. Both menus have 'Apply' and 'Cancel' buttons at the bottom.

Figure 5-3

Select the desired Access Point mode for your environment:

- **Wireless Point-to-Point Bridge:** In this mode, the WAG102 will communicate ONLY with another Bridge-mode Wireless Station. You must enter the MAC address (physical address) of the other Bridge-mode Wireless Station in the field provided. WEP can (and should) be used to protect this communication.

- **Wireless Point-to-Multi-Point Bridge:** Select this only if this WAG102 is the "Master" for a group of Bridge-mode Wireless Stations. The other Bridge-mode Wireless Stations must be set to Point-to-Point Bridge mode, using this WAG102's MAC address. They then send all traffic to this "Master", rather than communicate directly with each other. WEP can (and should) be used to protect this traffic.
- **Repeater:** If selected, this AP will operate as a Repeater only, and send all traffic to the remote AP. If selected, you must enter the MAC address (physical address) of the remote AP.

How to Configure a WAG102 as a Point-to-Point Bridge

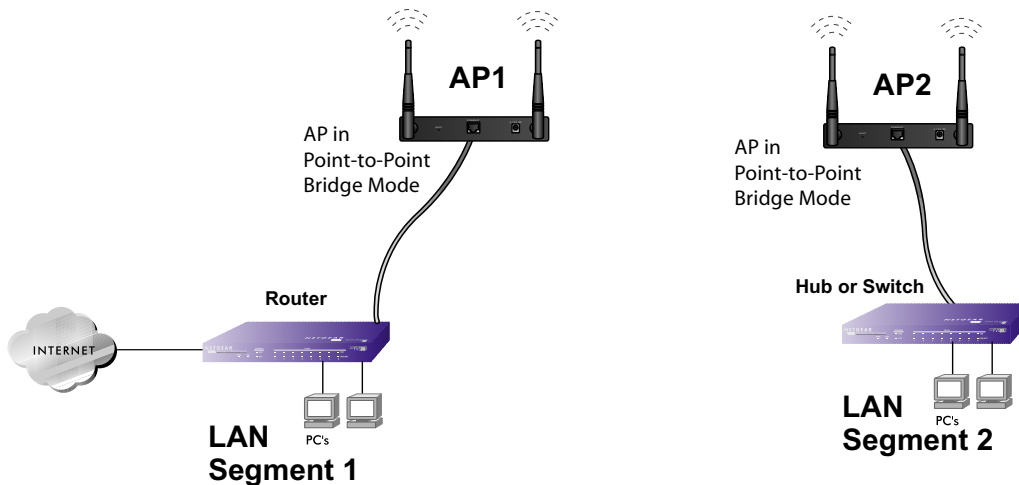


Figure 5-4: Point-to-Point Bridge

1. Configure the WAG102 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode.
2. Configure the WAG102 (AP2) on LAN Segment 2 in Point-to-Point Bridge mode.
AP1 must have AP2's MAC address in its Remote MAC Address field and AP2 must have AP1's MAC address in its Remote MAC Address field.
3. Configure and verify the following parameters for both access points:
 - Verify that the LAN network configuration of the WAG102 Access Points both are configured to operate in the same LAN network address range as the LAN devices
 - Both use the same SSID, Channel, authentication mode, if any, and security settings if security is in use.
4. Verify connectivity across the LAN 1 and LAN 2.

A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other PCs or servers connected to LAN Segment 1 or LAN Segment 2.

How to Configure Multi-Point Wireless Bridging

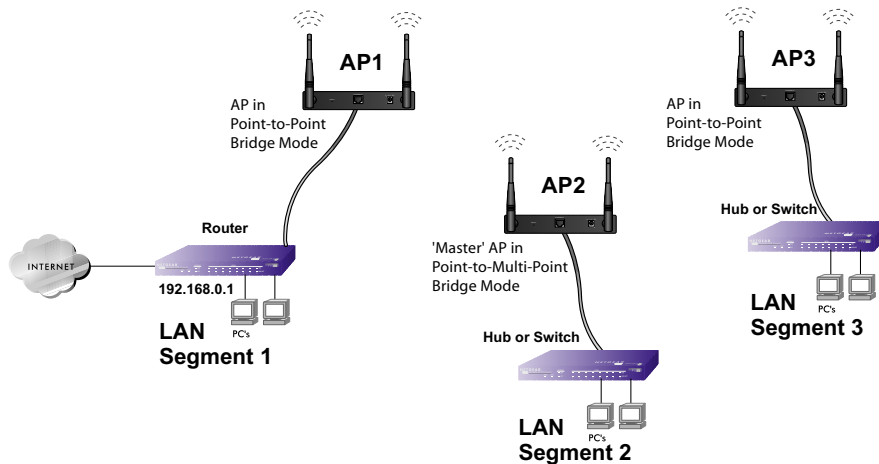


Figure 5-5: Multi-Point bridging

1. Configure the Operating Mode of the WAG102 Access Points.
 - WAG102 (AP1) on LAN Segment 1 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
 - Because it is in the central location, configure WAG102 (AP2) on LAN Segment 2 in Point-to-Multi-Point Bridge mode. The MAC addresses of the adjacent APs are required in AP2.
 - Configure the WAG102 (AP3) on LAN 3 in Point-to-Point Bridge mode with the Remote MAC Address of AP2.
2. Verify the following parameters for all access points:
 - Verify that the LAN network configuration the WAG102 Access Points are configured to operate in the same LAN network address range as the LAN devices
 - Only one AP is configured in Point-to-Multi-Point Bridge mode, and all the others are in Point-to-Point Bridge mode.
 - All APs must be on the same LAN. That is, all the APs LAN IP address must be in the same network.

- If using DHCP, all WAG102 Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
 - All WAG102 Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.
 - All Point-to-Point APs must have AP2’s MAC address in its Remote AP MAC address field.
3. Verify connectivity across the LANs.
- A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.
 - Wireless stations will not be able to connect to the WAG102 Access Points in the illustration above. If you require wireless stations to access any lan segment, you can additional WAG102 Access Points configured in Wireless Access Point mode to any LAN segment.



Note: You can extend this multi-point bridging by adding additional WAG102s configured in Point-to-Point mode for each additional LAN segment. Furthermore, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

How to Configure Wireless Repeating

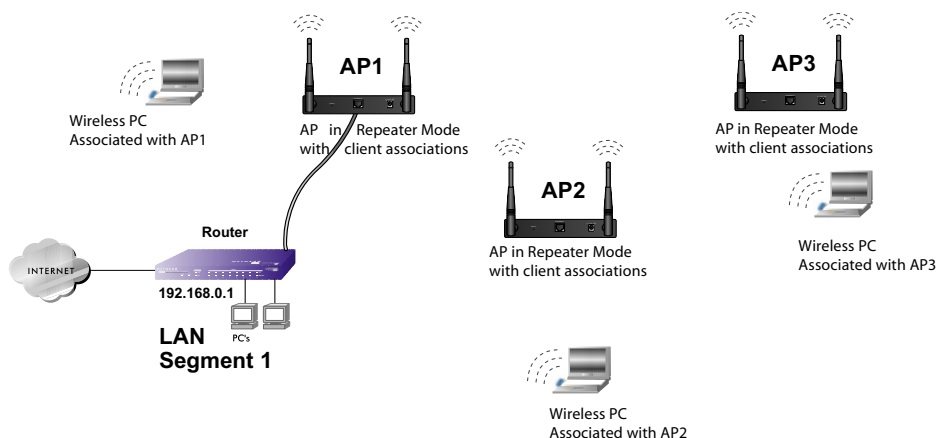


Figure 5-6: Multi-Point bridging

1. Configure the Operating Mode of the WAG102 Access Points.
 - WAG102 (AP1) on LAN Segment 1 in Repeater mode with the Remote MAC Address of AP2.
 - Configure WAG102 (AP2) in Repeater mode with MAC addresses of AP1 and AP3.
 - Configure the WAG102 (AP3) in Repeater mode with the Remote MAC Address of AP2.
2. Verify the following parameters for all access points:
 - Verify that the LAN network configuration the WAG102 Access Points are configured to operate in the same LAN network address range as the LAN devices
 - All APs must be on the same LAN. That is, all the APs LAN IP address must be in the same network.
 - If using DHCP, all WAG102 Access Points should be set to “Obtain an IP address automatically (DHCP Client)” in the IP Address Source portion of the Basic IP Settings menu.
 - All WAG102 Access Points use the same SSID, Channel, authentication mode, if any, and encryption in use.
3. Verify connectivity across the LANs.

A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three WLAN segments.



Note: You can extend this repeating by adding up to 2 additional WAG102s configured in repeater mode. However, since Repeater configurations communicate in half-duplex mode, the bandwidth decreases as you add Repeaters to the network. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Chapter 6

Troubleshooting

This chapter provides information about troubleshooting your WAG102 ProSafe Dual Band Wireless Access Point. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the WAG102 on?
- Have I connected the wireless access point correctly?
Go to “[Installing the WAG102 Access Point](#)” on page 3-5.
- I cannot remember the wireless access point’s configuration password.
Go to “[Changing the Administrator Password](#)” on page 4-10.



Note: For up-to-date WAG102 installation details and troubleshooting guidance visit <http://kbserver.netgear.com/products/WAG102.asp>.

If you have trouble setting up your WAG102, check the tips below.

No lights are lit on the access point.

It takes a few seconds for the power indicator to light up. Wait a minute and check the power light status on the access point.

If the access point has no power.

- Make sure the power cord is connected to the access point.
- Make sure the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet.
- Make sure you are using the correct NETGEAR power adapter supplied with your access point.

The Wireless LAN activity light does not light up.

The access point's antennae are not working.

- If the Wireless LAN activity light stays off, disconnect the adapter from its power source and then plug it in again.
- Make sure the antennas are tightly connected to the WAG102.
- Contact NETGEAR technical support if the Wireless LAN activity light remains off.

The LAN light is not lit.

There is a hardware connection problem. Check these items:

- Make sure the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router). A switch, hub, or router must be installed between the access point and the Ethernet LAN or broadband modem.
- Make sure the connected device is turned on.
- Be sure the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink™ (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

I cannot access the Internet or the LAN with a wireless capable computer.

There is a configuration problem. Check these items:

- You may not have restarted the computer with the wireless adapter to have TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up properly for that network. The usual setting for Windows Network Properties is set to "Obtain an IP address automatically."
- The access point's default values may not work with your network. Check the access point default configuration against the configuration of other devices in your network.

I cannot connect to the WAG102 to configure it.

Check these items:

- The WAG102 is properly installed, LAN connections are OK, and it is powered on. Check that the LAN port LED is green to verify that the Ethernet connection is OK.
- The default configuration of the WAG102 is for a static IP address of 192.168.0.232 and a Mask of 255.255.255.0 with DHCP disabled. Make sure your network configuration settings are correct.
- If you are using the NetBIOS name of the WAG102 to connect, ensure that your computer and the WAG102 are on the same network segment or that there is a WINS server on your network.
- If your computer is set to “Obtain an IP Address automatically” (DHCP client), restart it.
- If your computer uses a Fixed (Static) IP address, ensure that it is using an IP Address in the range of the WAG102. The WAG102 default IP Address is 192.168.0.232 and the default Subnet Mask is 255.255.255.0. If you are not sure about these settings, follow the instructions for [“Installing the WAG102 Access Point”](#) on page 3-5.

When I enter a URL or IP address I get a timeout error.

A number of things could be causing this. Try the following troubleshooting steps.

- Check whether other PCs work. If they do, ensure that your PCs TCP/IP settings are correct. If using a Fixed (Static) IP Address, check the Subnet Mask, Default Gateway, DNS, and IP Addresses.
- If the PCs are configured correctly, but still not working, ensure that the WAG102 is connected and turned on. Connect to it and check its settings. If you cannot connect to it, check the LAN and power connections.
- If the WAG102 is configured correctly, check your Internet connection (DSL/Cable modem etc.) to make sure that it is working correctly.
- Try again.

Using the Reset Button to Restore Factory Default Settings

The Reset button (see [Figure 2-2 on page 2-7](#)) has two functions:

- **Reboot.** When pressed and released quickly, the WAG102 will reboot (restart).
- **Reset to Factory Defaults.** This button can also be used to clear ALL data and restore ALL settings to the factory default values.

To clear all data and restore the factory default values:

1. Power off the WAG102 and power it back on.
2. Use something with a small point, such as a pen, to press the Reset button in and hold it in for at least 5 seconds.
3. Release the Reset button.

The factory default configuration has now been restored, and the WAG102 is ready for use.

Appendix A

Specifications

This appendix provides technical specifications for the WAG102 ProSafe Dual Band Wireless Access Point.

Specifications for the WAG102

Parameter	WAG102 ProSafe Dual Band Wireless Access Point
802.11a Data Rates	6, 9, 12, 18, 24, 36, 48, 54, and 108 Mbps (Auto-rate capable)
802.11a Operating Frequencies	5.15 ~ 5.25 5.25 ~ 5.35 5.57 ~ 5.825
802.11a Encryption	40-bit (also called 64-bit), 128- and 152-bit WEP data encryption
802.11g Data Rates	1, 2, 5.5, 11, 12, 18, 24, 36, 38, 54, & 108 Mbps (Auto-rate capable)
802.11g Operating Frequencies	2.412 ~ 2.462 GHz (US) 2.457 ~ 2.462 GHz (Spain) 2.412 ~ 2.484 GHz (Japan)2.457 ~ 2.472 GHz (France) 2.412 ~ 2.472 GHz (Europe ETSI)
802.11g Encryption	40-bit (also called 64-bit), 128- and 152-bits WEP data encryption
Network Management	Web-based configuration and status monitoring
Maximum Clients	Limited by the amount of wireless network traffic generated by each node; typically 15 to 20 nodes.
Status LEDs	Power/Ethernet LAN/Wireless LAN/Test
Power Adapter	12V DC, 1 A
Electromagnetic Compliance	FCC Part 15 Class B and Class E, CE, and C-TICK
Environmental Specifications	Operating temperature: 0 to 50° C Operating humidity: 5-95%, non-condensing

Appendix B

Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Document	Link
Internet Networking and TCP/IP Addressing:	http://documentation.netgear.com/reference/enu/tcpip/index.htm
Wireless Communications:	http://documentation.netgear.com/reference/enu/wireless/index.htm
Preparing a Computer for Network Access:	http://documentation.netgear.com/reference/enu/wsdhcp/index.htm
Virtual Private Networking (VPN):	http://documentation.netgear.com/reference/enu/vpn/index.htm
Glossary:	http://documentation.netgear.com/reference/enu/glossary/index.htm

