WG103 ProSafe 802.11g Wireless Access Point Reference Manual

NETGEAR

NETGEAR, Inc.
350 East Plumeria Drive
San Jose, CA 95134 USA

202-10466-01
February 2009
v.1.0

Manual abstract:

@@@@Information is subject to change without notice. all rights reserved. Statement of Conditions NOTE: 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. NOTE: Modifications made to the product, unless expressly approved by Netgear, could void the userâ□□s authority to operate the equipment. NETGEAR does not assume any liability that may occur due to such condition. NOTE: The availability of some specific channels and/or operational frequency bands are country-dependent and have been programmed in the firmware at the factory to match the intended destination. The firmware setting is not accessible by the end user. FCC Statement Declaration of Conformity We, Netgear, 350 East Plumeria Drive San Jose, CA 95134 USA Tel: +1 408 907 8000 declare under our sole responsibility that the product(s) WG103 (Model Designation) 802. 11g ProSafe Wireless Access Point (Product Name) complies with Part 15 of FCC Rules.

NOTE: 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 ii v1. 0 , February 2009 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: â□¢ â□¢ â□¢ â□¢ 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. FCC CAUTION: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the userâ□□s authority to operate this equipment.

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. placement and Range Guidelines Indoors , computers can connect over 802. 11 wireless networks at a maximum range of several hundred feet for 802. 11b/g 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: â□¢ â□¢ 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. 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.

Further, the antennas shall not be colocated with other antennas or radio transmitters. Com for an updated list of wireless accessories approved to be used with the WG103 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 numerique de classe B respecte les exigences du reglement du Canada sur le materiel brouilleur NMB-003. 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 device has been designed to operate with an antenna having a maximum gain of 5 dB. An antenna that has a higher gain is strictly prohibited per regulations of Industry Canada. 0, February 2009 Radiation Exposure Statement: This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20cm (7. 11g Wireless Access Point is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

0, February 2009 Certificate of the Manufacturer/Importer It is hereby certified that the WG103 ProSafe 802. 11g Wireless Access Point has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions. Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

Com and use the search feature to find an updated list of wireless accessories approved to be used with the WG103 in the European Community. 6-1 No LEDs are Lit on the Wireless Access Point . 6-3 You Cannot Access the Internet or the LAN from a Wireless-Capable Computer . 6-3 You Cannot Configure the Wireless Access Point from a Browser . 11g Wireless Access Point Reference Manual describes how to install, configure and troubleshoot the WG103 ProSafe 802.

11g Wireless Access Point. The information in this manual is intended for readers with intermediate computer and Internet skills. How to Use This Book This document describes configuration menu commands for the WG103 Access Point software. The commands can all be accessed from the Web interface. Â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ Chapter 1, â□□Introduction,â□□ describes the features and hardware of your WG103 Access Point. Chapter 2, â□□Basic Installation and Configuration,â□□ describes how to install and configure your WG103 Access Point for wireless connectivity. Chapter 3, â□□Wireless Security,â□□ describes how to wireless security for your WG103 Access Point and wireless network.

Chapter 6, â□□Troubleshooting,â□□ describes how to troubleshoot your WG103 Access Point. Appendix C, â□□Command Line Reference,â□□ provides the command line interface (CLI) of your WG103 Access Point. 11g Wireless Access Point Reference Manual Conventions, Formats, and Scope The conventions, formats, and scope of this manual are described in the following paragraphs: â□¢ Typographical Conventions.

This manual uses the following typographical conventions: Italic Bold Fixed italic Emphasis, books, CDs, file and server names, extensions User input, IP addresses, GUI screen text Command prompt, CLI text, code URL links â□¢ Formats. This manual 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. â□¢ Scope. This manual is written for the WG103 Access Point according to these specifications: Product Version Manual Publication Date WG103 ProSafe 802. 11g Wireless Access Point Reference Manual Note: Product updates are available on the NETGEAR, Inc. How to Use This Manual The HTML version of this manual includes the following: â□¢ â□¢ Buttons, at a time.

And , for browsing forward or backward through the manual one page A button that displays the table of contents and a button that displays an index. Double-click a link in the table of contents or index to navigate directly to where the topic is described in the manual. Online knowledge base for the product â□¢ â□¢ 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 options, according to your needs. â□¢ â□¢ Printing a page from HTML.

Each page in the HTML version of the manual is dedicated to a major topic. Select File > Print from the browser menu to print the page contents. printing from PDF. 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.

Use the PDF of This Chapter link at the top left corner of any page. Â□¢ Click the PDF of This Chapter link at the top left corner of any page in the chapter you want to print. The PDF version of the chapter you were viewing opens in a browser window. Click the print icon in the upper left of your browser window. Use the Complete PDF Manual link at the top left corner of any page. Â□¢ â□¢ Click the Complete PDF Manual link at the top left corner 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 corner of your browser 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. revision History Part Number 202-10468-01 Version Date Number 1.

0 February 2009 Description Initial release of this Reference Manual xiv v1. Minimal requirements for installation are in â□□System Requirementsâ□□ on page 1-4. About the Wireless Access Point The WG103 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 WG103 antenna interacts with wireless network interface cards (NIC) in wireless devices within a fixed range or area of coverage. Typically, a wireless access point inside a building works best with devices within a 100 foot radius. The WG103 can support a small group of users in a range of several hundred feet. Most wireless access points are rated between 30-50 users simultaneously. The WG103 acts as a bridge between the wired LAN and wireless clients. Connecting multiple WG103 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 wireless access point, it moves into the range of another. As a result, wireless clients can freely roam from one wireless access point to another and still maintain seamless connection to the network. Supported Features, Standards, and Conventions The WG103 is easy to use and provides complete wireless and networking support. Supported Standards and Conventions The following standards and conventions are supported: â□¢ â□¢ Standards Compliant. The wireless access point complies with the IEEE 802.

WPA and WPA2 enterprise class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. WPA-PSK and WPA2-PSK pre-shared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA. dHCP Client Support. DHCP provides a dynamic IP address to PCs and other devices upon request. The WG103 can act as a client andt; â□¢ â□¢ â□¢ â□¢ â□¢ WG103 ProSafe 802. Contact your reseller or customer support in your area if there are any missing or damaged parts. See 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 1-4 v1. 0 , February 2009 Introduction WG103 ProSafe 802. 11g Wireless Access Point Reference Manual packing materials to repack the WG103 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. Hardware Description The hardware functions of the WG103 front and rear panels are described below. Front Panel Power LAN WLAN Test Figure 1-1 Viewed from left to right, the WG103 has these four status LEDs: PWR, TEST, LAN, and WLAN. If this LED does not come on with the power adapter and cord correctly installed, see Chapter 6, â□□Troubleshooting. Front Panel LEDs (continued) LED LAN Description Ethernet link indicator Off Amber On Amber Flashing Green On Green Flashing WLAN Off Green Blink No connection detected on the Ethernet link 10 Mbps Ethernet link detected Data is being transmitted or received on the 10 Mbps Ethernet link 100 Mbps Fast Ethernet link detected.

Data is being transmitted or received on the 100 Mbps Ethernet link No wireless link activity. wireless link activity. Wireless LAN Link Activity Indicator Rear Panel 2 1 3 4 5 6 Figure 1-2 Viewed from left to right, the rear panel of the WG103 provides the following: 1. Security slot to allow you to lock the WG103 (you must provide the lock).

This restores the default factory settings. Use the WG103 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or Power Over Ethernet (POE) switch. This connects to the WG103 power adapter. Bottom Panel The bottom panel of the WG103 contains a label that shows compliance information, factory default login information, and the MAC and serial numbers. 0, February 2009 Introduction Chapter 2 Basic Installation and Configuration This chapter describes how to install and configure your WG103 ProSafe 802. 11g Wireless Access Point for wireless connectivity to your LAN.

This basic configuration will enable computers with 802. 11b or 802. 11g wireless adapters to connect to the Internet, or access printers and files on your LAN. In planning your wireless network, consider the level of security required. Chapter 3, â□□Wireless Securityâ□□ describes how to set up wireless security for your network.

This chapter includes: â□¢ â□¢ â□¢ â□¢ â□□What You Need before You Beginâ□□ on this page â□□Installing and Configuring the Wireless Access Pointâ□□ on page 2-2 â□□Testing Basic Wireless Connectivityâ□□ on page 2-12 â□□Deploying the Wireless Access Pointâ□□ on page 2-12 What You Need before You Begin You need to consider the following guidelines and requirements before you can set up your wireless access point. see also â□□System Requirementsâ□□ on page 1-4. Wireless Equipment Placement and Range Guidelines The range of your wireless connection can vary significantly based on the location of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices. Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless access point.

For complete performance specifications, see Appendix A, â□□Technical Specifications. Â□□ For best results, place your wireless access point according to the following guidelines: â□¢ Near the center of the area in which your PCs will operate. Â□¢ In an elevated location such as a high shelf where the wirelessly connected PCs have line-ofsight access (even if through walls). If using multiple wireless access points, it is better if adjacent wireless access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent wireless access points is five channels (for example, use channels 1 and 6, or 6 and 11, or 1 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. Ethernet Cabling Requirements The wireless access point connects to your LAN via twisted-pair category 5 Ethernet cable with RJ-45 connectors. LAN Configuration Requirements For the initial configuration of your wireless access point, you need to connect a computer to the wireless access point.

Note: For assistance with DHCP configuration, see the online document that you can access from â□□Preparing Your Networkâ□□ in Appendix B. Computer Hardware Requirements To connect to the wireless access point on your network, each computer must have a 802. Installing and Configuring the Wireless Access Point Before installing the wireless access point, make sure that your Ethernet network is up and working. You will be connecting the wireless access point to the Ethernet network. Then computers with 802. 11b or 802. 11g wireless adapters will be able to communicate with the Ethernet network. 11g Wireless Access Point Reference Manual In order for this to work correctly, verify that you have met all of the system requirements, shown in â□□System Requirementsâ□□ on page 1-4. Install and configure your wireless access point in this order: 1. Connect the Wireless Access Point to a Computer Set up the wireless access point: Tip: Before mounting the wireless access point in a high location, first set up and test the wireless access point to verify wireless network connectivity.

1. Unpack the box and verify the contents. 2. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.

3. Configure the computer with a static IP address of 192. Connect an Ethernet cable from the wireless access point to the computer. 5. Turn on your computer, connect the power adapter to the wireless access point, and verify the following: â□¢ Power LED.

The power LED (PWR) should be lit. If the power LED is not lit, check the connections and check to see if the power outlet is controlled by a wall switch that is turned off. test LED. The test LED (TEST) blinks when the wireless access point is first turned on. lAN LED. The LAN LED (LAN) on the wireless access point should be lit (amber for a 10 Mbps connection and green for a 100 Mbps connection). If not, make sure the Ethernet cable is securely attached at both ends. 11g Wireless Access Point Reference Manual Log in to the Wireless Access Point The default IP address of your wireless access point is 192. The wireless access point is set, by default, for the DHCP client to be disabled. Connect to the wireless access point by entering its default address of http://192.

Enter the default user name of admin and the default password of password. The Web browser displays the Basic General Settings screen under the Configuration tab of the main menu as shown in Figure 2-3 on page 2-5. 11g Wireless Access Point Reference Manual Configure LAN Access and Set the Time First, configure LAN access, and then set the time: 1. Log in to the wireless access point as described in â□□Log in to the Wireless Access Pointâ□□ on page 2-4. The Web browser displays the General screen. (The full path to his screen is Configuration > System > Basic > General.) Figure 2-3 2. Specify the following fields, or use the default values, which work for most users and situations: â□¢ Access Point name. This unique name is the wireless access point NetBIOS name. The device can be accessed by entering either its name or IP address in the location bar of your browser.

The default wireless access point name is on the bottom label of the wireless access point. You can modify the default name with a unique name up to 15 characters long. The default is netgearxxxxxx8, where xxxxx represents the first five digits of the last six digits of the wireless access pointâ□□s MAC address. These five digits are followed by an eight (8). Note: The MAC address for the wireless access point always ends with a zero (0) but the NetBIOS name always ends with an eight (8).

For example, if the MAC address 1234567890A0, then the NetBIOS name is netgear7890A8. â□¢ Country/Region. This is the region where the wireless access point 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. For products sold in the United States, the Country/Region field is preset according to regulatory requirements.

For products sold outside the United States, a country domain must be selected. (The full path to his screen is Configuration > System > Basic > Time.) Figure 2-4 Specify the following fields: â□¢ â□¢ â□¢ Time Zone. Select the time zone to match your location. current Time. The current time, as used on the wireless access point, is displayed. Your wireless access point synchronizes with a Network Time Protocol (NTP) server. disable. Your wireless access point does not synchronize with an NTP server. use Custom NTP Server.

Enable this check box if you want to use a custom NTP server. hostname / IP Address. Provide the hostname or IP address of the time server that the wireless access point must use to keep its time correct. Note: You must have an Internet connection to use an NTP server that is not on your local network. Log in to the wireless access point as described in â□□Log in to the Wireless Access Pointâ□□ on page 2-4. The IP Settings screen displays: Figure 2-5 Specify the following fields: â□¢ DHCP Client. by default , the Dynamic Host Configuration Protocol (DHCP) client is disabled. After installation, you can enable DHCP to let the wireless access point get its TCP/IP configuration from the DHCP server on your network. The wireless access point gets the IP address, subnet mask and the default gateway settings automatically from the DHCP server if DHCP is enabled. iP Address.

The default IP address is 192. If you want to change the address, enter an unused IP address from the address range that is used on your LAN, or enable DHCP. iP Subnet Mask. Enter the subnet mask value used on your LAN. Enter the IP address of the gateway for your LAN.

For more complex networks, enter the address of the router for the network segment to which the wireless access point is connected. Enter the IP address of the domain name system (DNS) server you wish to use. secondary DNS Server. Enter the IP address of a secondary DNS server, which will be used when the primary DNS server is not available Network Integrity Check. Select this check box to enable the wireless access point to validate that the upstream link is active before allowing wireless associations.

If you select this check box, you must ensure that your default gateway is configured. Configure Basic Wireless Settings Warning: If you configure the wireless access point from a wireless computer and you change the wireless access pointâ□□s SSID, channel or wireless 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 wireless access pointâ□□s new settings. to configure the basic wireless settings: 1. Log in to the wireless access point as described in â□□Log in to the Wireless Access Pointâ□□ on page 2-4. 11g wireless stations can still be used if they can operate in 802. This is the default mode. turn Radio On. On by default, you can also turn off the radio to disable access through the wireless access point. Doing so can be helpful for configuration, network tuning, or troubleshooting activities.

wireless Network Name (SSID). The SSID is also known as the wireless network name. The SSID separates network traffic from different wireless networks. To connect any wireless device to a wireless network, you need to use the SSID. The wireless access point default SSID is: NETGEAR_11g for the first profile, NETGEAR_11g-1 for the second profile, NETGEAR_11g-2 for the third profile, NETGEAR_11g-3 for the fourth profile, and so on. You can enter a value of up to 32 alphanumeric characters. For more information about SSIDs, see â□□Security Profilesâ□□ on page 3-3. 11g Wireless Access Point Reference Manual Note: The SSID of any wireless adapters must match the SSID of the wireless access point. If they do not match, a wireless connection to the wireless access point cannot be established. If you disable broadcast of the SSID, only stations that know the SSID can connect to the wireless access point.

Disabling the SSID broadcast somewhat hampers the wireless network discovery feature of some products. This drop-down menu lets you specify which operating frequency is used. the default setting is Auto. You should not need to change the channel unless you notice interference problems, or are setting up the wireless access point near another wireless access point. Observe the following guidelines: â□□ Wireless access points use a fixed channel.

You can select the channel used. This lets you choose a channel that provides the least interference and best performance. In the USA and Canada, 11 channels are available. If using multiple wireless access points, it is better if adjacent wireless access points use different channels to reduce interference. The recommended channel spacing between adjacent wireless access points is five channels (for example, use channels 1 and 6, or 6 and 11).

in â□□infrastructureâ□□ mode , wireless stations normally scan all channels , looking for a wireless access point. If more than one wireless access point can be used, the one with the strongest signal is used. This can happen only when the wireless access points use the same SSID. Â□¢ â□□ â□□ See the online document that you can access from â□□Wireless Networking Basicsâ□□ in Appendix B for more information about wireless channels. â□¢ Data Rate. This drop-down menu lets you specify the transmit data rate of the wireless network. the default settings is Best. The smallest data rate that you can select is 1 Mbps; the largest is 54 Mbps. output Power. This drop-down menu lets you specify the transmit signal strength of the wireless access point.

The options are Full, Half, Quarter, Eighth, and Minimum. Decrease the transmit power if two or more wireless access points are close together and using the same channel frequency. 11g Wireless Access Point Reference Manual Configure Basic QoS Settings The QoS screen lets you modify the quality of service (QoS) settings for upstream traffic flowing from a client station to the wireless access point and the downstream traffic flowing from the wireless access point to a client station. to configure the basic QoS settings: 1. Log in to the wireless access point as described in â□□Log in to the Wireless Access Pointâ□□ on page 2-4. Select the Enable radio button to ensure that applications that require better throughput and performance are provided special queues with higher priority.

For example, video and audio applications are given higher priority over applications, such as FTP. Select the Enable radio button to let power-saving devices that connect to the wireless access point conserve power. 11g Wireless Access Point Reference Manual Testing Basic Wireless Connectivity After you have installed and configured the wireless access point as explained in the previous section, test your computers for wireless connectivity: 1. Configure the wireless adapters of your computers so that they all have the same SSID and channel that you have configured on the wireless access point.

2. Verify that your computers have a wireless link to the wireless access point and are able to obtain an IP address through DHCP from the wireless access point. If you have trouble connecting to the wireless access point, see Chapter 6, â□□Troubleshooting. Â□□ Now that your computers can connect to the wireless access point, you can configure the wireless security as described in Chapter 3, â□□Wireless Security. Â□□ Deploying the Wireless Access Point After you have tested basic wireless connectivity (see the previous section) and have set up wireless security as described in Chapter 3, â□□Wireless Security,â□□ you are ready to deploy the wireless access point in your network.

If needed, you can now reconfigure the computer that you used for this process back to its original TCP/IP settings. to deploy the wireless access point 1. Disconnect the wireless access point 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. Connect an Ethernet cable from your wireless access point to a LAN port on your router, switch, or hub.

11g Wireless Access Point Reference Manual Note: By default, the wireless access point is set with the DHCP client disabled. If your network uses dynamic IP addresses, you must change this setting. 4. Connect the power adapter to the wireless access point, and plug the power adapter in to a power outlet. The PWR and LAN LEDs should light up. tip: The wireless access point supports Power Over Ethernet (PoE). If you have a switch that provides PoE, you will not need to use the power adapter to power the wireless access point. This can be especially convenient when the wireless access point is installed in a high location far away from a power outlet. Using a computer with an 802. 11b or 802.

11g wireless adapter with the correct wireless settings (see â□□Testing Basic Wireless Connectivityâ□□ on page 2-12), verify connectivity by using a browser such as Internet Explorer or Mozilla Firefox to browse the Internet, or check for file and printer access on your network. Note: If you are unable to connect, see Chapter 6, â□□Troubleshooting. 11g Wireless Access Point Reference Manual Chapter 3 Wireless Security This chapter describes how to use your WG103 ProSafe 802. 11g Wireless Access Point to set up wireless security for your wireless network. This chapter includes: â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ â□□Wireless Data Security Optionsâ□□ on this page â□□Security Profilesâ□□ on page 3-3 â□□Configuring the RADIUS Server Settingsâ□□ on page 3-9 â□□Configuring WEPâ□□ on page 3-10 â□□Configuring WPAâ□□ on page 3-12 â□□Restricting Wireless Access by MAC Addressâ□□ on page 3-14 Wireless Data Security Options Indoors, computers can connect over 802. 11g wireless networks at a maximum range of 300 feet. Typically, a wireless access point inside a building works best with devices within a 100 foot radius. Such distances can allow for others outside your immediate area to access your network. Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment.

The wireless access point provides highly effective security features that are covered in detail in this chapter. Deploy the security features appropriate to your needs. 11g Wireless Access Point Reference Manual Figure 3-1 There are several ways you can enhance the security of your wireless network: â□¢ Use Multiple BSSIDs combined with VLANs. You can configure combinations of VLANS and BSSIDs with stronger or less restrictive access security according to your requirements. For example, visitors could be given wireless Internet access but be excluded from any access to your internal network.

For information about how to configure BSSIDs, see â□□Creating and Editing Security Profilesâ□□ on page 3-5. restrict Access based by MAC address. You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the wireless access point. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. For information about how to restrict access by MAC address, see â□□Restricting Wireless Access by MAC Addressâ□□ on page 3-14.

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 exposed. For information about how to turn of broadcast of the SSID, see â□□Creating and Editing Security Profilesâ□□ on page 3-5. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper. this data encryption mode has been superseded by WPA-PSK and WPA2-PSK. For information about how to configure WEP, see â□□Configuring WEPâ□□ on page 3-10. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. For information about how to configure WEP, see â□□Configuring WPAâ□□ on page 3-12. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise.

For information about how to configure WEP, see â□□Configuring WPAâ□□ on page 3-12. Â□¢ Security Profiles Security profiles let you configure unique security settings for each SSID. The wireless access point supports up to eight BSSIDs that you can configure in the Profile Settings screen (see â□□Creating and Editing Security Profilesâ□□ on page 3-5). To set up a security profile you select its network authentication type, data encryption, wireless client security separation, and VLAN ID: â□¢ Network Authentication The wireless access point is set by default as an open system with no authentication.

When you configure network authentication, bear in mind the following: â â If you are using Access Point mode, then all options are available. In other modes such as Repeater or Bridge, some options may be unavailable. Not all wireless adapters support WPA or WPA2. Windows XP, Windows 2000 with Service Pack 3, and Windows Vista do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings.

You can configure the wireless access point to use the types of network authentication that are shown in Table 3-1 on page 3-7. Â¢ Data Encryption Select the data encryption that you want to use. The available options depend on the network authentication setting above (otherwise, the default is None). The Data Encryption settings are explained in Table 3-2 on page 3-8. 11g Wireless Access Point Reference Manual â¢ Wireless Client Security Separation If enabled, the associated wireless clients (using the same SSID) will not be able to communicate with each other.

This feature is used for hotspots and other public access situations. the default settings is disabled. VLAN ID If enabled and if the network devices (hubs and switches) on your LAN support the VLAN (802. 1Q) standard, the default VLAN ID for the wireless access point will be associated with each profile. The default profile VLAN ID must match the IDs that are used by the other network devices.

Â¢ Before You Change the SSID and WEP Settings For a new wireless network, print or copy this form and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the Country/Region correctly as the first step. Store this information in a safe place. Â¢ SSID: The Service Set Identification (SSID) identifies the wireless local area network. You may customize it by using up to 32 alphanumeric characters. Write your SSID on the line. SSID: ___________________________________ 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 âShared Keyâ 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 and have the same keys in the same positions as those in the WG103. wEP Encryption Keys For all four 802. 11b keys, choose the Key Size. Circle one: 64, 128, or 152 bits Key 1: ___________________________________ Key 2: ___________________________________ Key 3: ___________________________________ â¢ Key 4: ___________________________________ WPA-PSK (Pre-Shared Key) WPA2-PSK (Pre-Shared Key) Record the WPA-PSK key: Record the WPA2-PSK key: Key: ________________________________ Key: ________________________________ â¢ â¢ 3-4 v1. 0 , February 2009 Wireless Security WG103 ProSafe 802. 11g Wireless Access Point Reference Manual â¢ WPA RADIUS Settings For WPA, record the following settings for the primary and secondary RADIUS servers: Server Name/IP Address: Primary __________________ Secondary __________________ Port: ___________________________________ â¢ Shared Secret: ___________________________________ WPA2 RADIUS Settings For WPA2, record the following settings for the primary and secondary RADIUS servers: Server Name/IP Address: Primary __________________ Secondary __________________ Port: ___________________________________ Shared Secret: ___________________________________ Creating and Editing Security Profiles To create or edit a security profile with its own unique BSSID: 1. @@@@The Profile Settings screen displays information about the eight profiles: Figure 3-2 Wireless Security v1. To select a security profile without editing it, select the corresponding check box in the Enable column and proceed to step 6. To edit a security profile, select the corresponding radio button from the list, and click Edit. The Edit Security Profile screen opens for the selected security profile.

Figure 3-3 shows an example with a Open System network authentication. figure 3-3 4. Enter the profile definitions in the Edit Security Profile screen: â¢ â¢ Security Profile Name. Use a name that makes it easy to recognize the profile, and to tell profiles apart. wireless Network Name (SSID).

The SSID is also known as the wireless network name. The SSID separates network traffic from different wireless networks. To connect any wireless device to a wireless network, you need to use the SSID. The wireless access point default SSID is: NETGEAR_11g for the first profile, NETGEAR_11g-1 for the second profile, NETGEAR_11g-2 for the third profile, NETGEAR_11g-3 for the fourth profile, and so on. You can enter a value of up to 32 alphanumeric characters. Some concepts and guidelines regarding the SSID are explained below: â A Basic Service Set (BSS) is a group of wireless stations and a single wireless access point, all using the same SSID. Â An Extended Service Set (ESS) is a group of wireless stations and multiple wireless access points, all using the same ID (ESSID). 11g Wireless Access Point Reference Manual â â Different wireless access points within an ESS can use different channels. To reduce interference, adjacent wireless access points should use different channels. Roaming is the ability of wireless stations to connect wirelessly when they physically move from one BSS to another within the same ESS. The wireless station automatically changes to the wireless access point with the least interference or best performance. â¢ Broadcast Wireless Network Name (SSID). These radio buttons let you enable and disable the SSID broadcast. If disable the SSID broadcast, then only stations that know the SSID can connect. Disabling the SSID broadcast somewhat hampers the wireless network discovery feature of some products.

Enter the authentication settings in the Edit Security Profile screen: â¢ Network Authentication. Use the information in the following table to set the network authentication. 1x WPA with Radius WPA2 with Radius Description Can be used with WEP encryption, or no encryption. At least one shared key must be entered. see âConfiguring WEPâ on page 3-10. You must configure the RADIUS Server Settings to use this option. see âConfiguring WPAâ on page 3-12. You must configure the RADIUS Server Settings to use this option. Select this option only if all clients support WPA2. If selected, you must use AES encryption, and configure the RADIUS Server Settings Screen.

see âConfiguring WPAâ on page 3-12. This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES).

If selected, encryption must be TKIP + AES, and you must also configure the RADIUS Server Settings Screen. see â□□Configuring WPAâ□□ on page 3-12. You must use TKIP encryption, and enter the WPA passphrase (Network key).

Select this option only if all clients support WPA2. If selected, you must use AES encryption, and enter the WPA passphrase (Network key). see â□□Configuring WPAâ□□ on page 3-12. This option allows clients to use either WPA (with TKIP) or WPA2 (with AES). if selected , encryption must be TKIP + AES.

The WPA passphrase (Network key) must also be entered. Use the information in the following table to configure the data encryption. Note that the types of data encryption that are available depend on the selection of the network authentication type. Proprietary mode that will work only with other wireless devices that support this mode. see â□□Configuring WEPâ□□ on page 3-10. This is the standard encryption method used with WPA. see â□□Configuring WPAâ□□ on page 3-12. This is the standard encryption method for WPA2. Some clients may support AES with WPA, but this is not supported by this wireless access point. see â□□Configuring WPAâ□□ on page 3-12.

This setting supports both WPA and WPA2. broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. Wireless client security separation must be enabled to block unicast, multicast, and broadcast traffic between the clients of the same virtual access point (VAP). From the pull-down menu, select one of the following options: â□□ â□□ Disable. Enter the VLAN ID that is associated with this profile. Configuring the RADIUS Server Settings To view or change the RADIUS server settings: 1. @@@@View or change the RADIUS server and authentication settings: â□¢ Primary Authentication Server Secondary Authentication Server Primary Accounting Server Secondary Accounting Server Wireless Security v1. 0 , February 2009 3-9 WG103 ProSafe 802. 11g Wireless Access Point Reference Manual For authentication, accounting, or both authentication and accounting using RADIUS, you must configure primary servers.

You can configure a secondary RADIUS server that is used in case the primary RADIUS server fails. â□□ IP Address. The IP address of the RADIUS server. â□□ Port Number. The port number of the RADIUS server.

The default port for an authentication server is 1812; the default port for a accounting server is 1813. â□□ Shared Secret. This value is shared between the wireless access point and the RADIUS server while authenticating the supplicant. â□¢ Reauthentication Time (Seconds). The time interval in seconds after which the supplicant will be authenticated again with the RADIUS server.

Select this check box to enable re-keying of the global key, and enter a value in seconds. The global key re-key can be done based on time interval in seconds. Configuring WEP Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the wireless access point from a wired computer to make further changes. to configure WEP data encryption: 1. @@@@Select a profile by selecting the corresponding radio button from the list, and click Edit. the Edit Security Profile screen displays. Figure 3-5 on page 3-11 shows an example with a Shared Key network authentication. You can select an authentication scheme that requires a shared key but still leaves the data transmissions unencrypted. If you require strong security, use both the Shared Key and WEP encryption settings.

To use a passphrase to generate the WEP keys, enter a word or group of characters, and click Generate Keys. The four key fields will be automatically populated with key values. You can also enter the keys manually. If you choose to enter the keys manually, enter hexadecimal digits (any combination of 0â□□9, aâ□□f, or Aâ□□F). Select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can be used only to decrypt received data. These key values must be identical on all computers and access points in your network. (For more information, see â□□Security Profilesâ□□ on page 3-3. Enter the VLAN ID that is associated with this profile.

For more information about WEP, see the online document that you can access from â□□Wireless Networking Basicsâ□□ in Appendix B. configuring WPA WPA-PSK data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA makes it virtually impossible to compromise. Not all wireless adapters support Wi-Fi Protected Access (WPA). Consult the product documentation for your wireless adapter for instructions for configuring WPA settings.

Note: If you use a wireless computer to configure wireless security settings, you will be disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the wireless access point from a wired computer to make further changes. to configure WPA data encryption: 1. @@@@Select a profile by selecting the corresponding radio button from the list, and click Edit. the Edit Security Profile screen displays.

Figure 3-5 shows an example with a WPA2-PSK network authentication. figure 3-6 4. From the Network Authentication pull-down menu, select the WPA or WPA2 option of your choice: â□¢ Legacy 802. Some options require that you configure one ore more RADIUS servers (see â□□Configuring the RADIUS Server Settingsâ□□ on page 3-9). 5. If you have selected WPA-PSK, WPA2-PSK, or WPA-PSK & WPA2-PSK, enter the passphrase in the WPA Passphrase (Network Key) field. All wireless stations must use the same passphrase (network key). The passphrase must be from 8 to 63 characters in length. (For more information, see â□□Security Profilesâ□□ on page 3-3. Enter the VLAN ID associated with this profile.

@@@@@@@@@@ to restrict access based on MAC addresses: 1. @@@@@@@@@@@@ â□¢ Local MAC Address Database. @@@@@@@@@@@@ 11g Wireless Access Point. @@@@The following procedures explain how to do these tasks. Backing up the Configuration To back up the configuration: 1. @@@@@@You can give the file a meaningful name at this time, such as WG103. cfg. Restoring the Configuration To restore your settings from a saved configuration file: 1. @@@@Enter the full path to the file on your computer or click Browse to locate the file. After completing the upload, the wireless access point reboots automatically.

11g Wireless Access Point Reference Manual Rebooting and Restoring the Default Configuration You can erase the wireless access point configurations, and return to the factory default settings. After erasing, the wireless access pointâ□□s password will be password, the SSID will be NETGEAR, the DHCP client will be disabled, the default LAN IP address will be 192.

229, and the access wireless access point name is reset to the name printed on the label on the bottom of the unit. Using the Reset Button to Reboot or Restore Factory Default Settings If you do not know the login password or IP address, you can still restore the factory default configuration settings with the Reset button. This button is on the rear panel of the wireless access point (see â□□Rear Panelâ□□ on page 1-6).

The Reset button has two functions: â□¢ â□¢ Reboot. When pressed and released, the wireless access point reboots (restarts). reset to Factory Defaults. When pressed and held down, it clears all data and restores all settings to the factory default values. To clear all data and restore the factory default values: 1.

Hold the Reset button until the LEDs blink twice, usually more than five seconds. The factory default configuration has now been restored, and the wireless access point is ready for use. Using the Software to Reboot the Wireless Access Point To use the software to reboot the wireless access point: 1. @@@@Using the Software to Restore Factory Default Settings To use the software to restore all settings to the factory default values: 1. @@@@11g Wireless Access Point Reference Manual Upgrading the Wireless Access Point Firmware Warning: When uploading firmware to the wireless access point, do not 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 firmware, and render the wireless access point completely inoperable. You cannot upgrade the firmware from a computer that is connected to the wireless access point with a wireless link. You must use a computer that is connected to the wireless access point with an Ethernet cable. The wireless access point firmware is stored in flash memory, and can be upgraded as NETGRA releases new firmware. You can download the upgrade file (in tar format) from the NETGEAR Web site.

Note: The Web browser used to upload new firmware into the wireless access point must support HTTP uploads, such as Microsoft Internet Explorer 6. To upgrade the firmware on the wireless access point: 1. Download the upgrade file from NETGEAR and save it to your hard disk. 1. @@@@ 2. Back up the current configuration as described in â□□Backing up the Configurationâ□□ on page 4-1. Click Browse to navigate to the location where the upgrade file is stored. When the upload completes, your wireless access point automatically restarts. In some cases, you might need to reconfigure the wireless access point after upgrading. Network Management Information The wireless access point provides a variety of status and usage information, which are discussed in the following sections.

Viewing the Activity Log You can view the activity log on screen or send it to a syslog server. Viewing the Activity Log on Screen To view the activity log on screen: 1. @@@@Figure 4-6 The Activity Log Window displays the wireless access pointâ□□s system activity. Sending the Activity Log to a Syslog Server To send the activity log to a syslog server: 1. @@@@Enter the syslog information in the following fields: â□¢ â□¢ â□¢ Enable Syslog.

Select this check box to enable the syslog server. syslog Server IP address. The IP address of the syslog server. port Number. The port number that is configured on the syslog server on your LAN.

The wireless access point sends all the system activity information to the specified IP address. @@@@You can configure these settings in â□□Configure LAN Access and Set the Timeâ□□ on page 2-5. Access Point Name (NetBIOS name) MAC Address Country/Region The default name may be changed if desired. The MAC Address of the wireless access pointâ□□s Ethernet port. 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. The version of the firmware currently installed. System time as available on the wireless access point. System Information Fields (continued) Field Description Current IP Settings You can configure these settings in â□□Configure Basic IP Settingsâ□□ on page 2-7. IP Address Subnet Mask Default Gateway DHCP Client Current Wireless Settings Access Point Mode The operating mode of the wireless access point: access point, pointto-point bridge, multi-point bridge, or repeater.

To change these settings, see â□□Wireless Bridging and Repeatingâ□□ on page 5-9. The channel the wireless port uses. the default channel setting is automatic channel selection. To change these settings, see â□□Configure Basic Wireless Settingsâ□□ on page 2-8. For the frequencies used on each channel, see the online document that you can access from â□□Wireless Networking Basicsâ□□ in Appendix B. indicates whether rogue AP detection is enabled or not. To change these settings, see â□□Enabling Rogue AP Detectionâ□□ on page 4-19. The IP address of the wireless access point. The subnet mask for the wireless access point. The default gateway for the wireless access point communication.

If this is enabled, the current IP address was obtained from a DHCP server on your network. disabled indicates a static IP configuration. Channel/Frequency Rogue AP Detection Viewing Statistics To view the network traffic statistics for the wired (Ethernet LAN) and wireless (WLAN) interfaces of the wireless access point: 1. @@@@Network Statistics Field Wired Ethernet Packets Bytes Wireless LAN Unicast Packets Broadcast Packets Multicast Packets Total Packets Total Bytes Description Received/Transmitted The number of packets sent since the wireless access point was restarted. The number of bytes sent since the wireless access point was restarted.

received/Transmitted The Unicast packets sent since the wireless access point was restarted. The Broadcast packets sent since the wireless access point was restarted. The Multicast packets sent since the wireless access point was restarted. The Wireless packets sent since the wireless access point was restarted. The Wireless bytes sent since the wireless access point was restarted.

11g Wireless Access Point Reference Manual Viewing the Available Wireless Stations Table The Available Wireless Stations table contains a table of all wireless devices associated with the wireless access point for the wireless network name (SSID). to display the Available Wireless Stations table: 1. @@@@Figure 4-10 For each device, the table shows details such as the MAC address, BSSID, SSID, channel, rate, and status (whether or not the device is allowed to communicate with the wireless access point). For full details about a wireless station, select the corresponding radio button, and click Details. Note that if the wireless access point is rebooted, the table data is lost until the wireless access point rediscovers the devices.

To force the wireless access point to look for associated devices, click Refresh. 11g Wireless Access Point Reference Manual Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This extends the reach of the wireless network. Users can roam from one wireless access point to another, providing seamless network connectivity. If this is the case, only the stations associated with this wireless access point are shown in the Available Wireless Stations table.

Viewing AP Statistics The wireless access point can detect both unknown (rogue) and known APs and wireless stations. For information about excluding rogue APs and wireless stations, see âEnabling Rogue AP Detectionâ on page 4-19. Viewing the Unknown AP List To display the Unknown AP List: 1. @@@@Viewing the Known AP List To display the Known AP List: 1. @@@@The Known AP List displays: Figure 4-12 To save the screen to a file, click Save. 11g Wireless Access Point Reference Manual Changing the Administrator Password The default password for the is password. Change this password to a more secure password. You cannot change the user name. Tip: Be sure to change the wireless access point default password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper case and lower case), numbers, and symbols.

Your password can be up to 30 characters. to change the password: 1. @@@@The Change Password screen displays: Figure 4-13 To change the password: 1. Next to Restore Default Password, select the No check box. Next to Restore Default Password, select the Yes check box.

Remote Management You can remotely configure, upgrade, and check the status of your wireless access point by using Simple Network Management Protocol (SNMP) or by using the command-line interface (CLI) via a secure shell (SSH) or (secure) Telnet connection. SNMP Remote Management Simple Network Management Protocol (SNMP) forms part of the internet protocol suite as defined by the Internet Engineering Task Force (IETF). SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications Enable SNMP to allow SNMP network management software such as HP OpenView to manage the wireless access point via the SNMPv1/v2 protocol.

to enable remote management: 1. @@@@Enter the following information according to the requirements of your location: â¢ Read-Only Community Name. The community string to allow the SNMP manager to read the MIB objects of the wireless access point. The community string to allow the SNMP manager to read and write the MIB objects of the wireless access point. The community name that is associated with the IP address to receive traps. â¢ IP Address to Receive Traps. Enter the IP address of the device that should receive the traps that are sent from the wireless access point. If you do not want traps to be sent, leave this field blank. â¢ Trap Port. The port number where traps will be sent.

Enter the IP address of the SNMP manager. You can access the CLI from a Telnet client over the Ethernet port of the wireless access point. The CLI commands are listed in Appendix C, âCommand Line Reference. â Note: You must use a secure Telnet client such as Absolute Telnet. Also, when you configure the client, use the SSH1, 3DES option. When you use the Telnet client to connect over the Ethernet port, use the IP address of the wireless access point as the host name. The remote console lets you enable secure shell (SSH) and (secure) Telnet. to use the remote console: 1. @@@@Select the Enable radio button to allow remote access to the wireless access point through secure shell and secure Telnet. Select the Enable radio button to restrict access to the wireless access point through regular Telnet.

11g Wireless Access Point Reference Manual Enabling Rogue AP Detection The wireless access point can detect unknown (rogue) APs and wireless stations and can prevent them from connecting to the wireless access point. to enable rogue AP detection: 1. @@@@Select the Turn Rogue AP Detection On check box to enable rogue AP detection. The wireless access point continuously scans the wireless network and collects information about all APs detected on its channel. There are several other actions you can initiate from the Rogue AP screen.

These actions are described in Table 4-3 on page 4-20. Rogue AP Screen Actions Action Import AP List from a file Refresh Move Delete Description See âImporting Rogue APs List from a Fileâ on this page. Under the Unknown AP List, click Refresh to discover the APs Select an AP from the Unknown AP List by selecting the corresponding check box, and then click Move to add the AP to the Known AP List. Select an AP from the Known AP List by selecting the corresponding check box, and then click Delete to remove an AP from the Known AP List. click Apply to save your changes.

Apply Importing Rogue APs List from a File To replace the existing Known AP list: 1. Create a text file that contains the MAC address of each known AP, separated by a space. The following example shows a list of six known APs that an administrator might upload to the wireless access point: 00:0c:41:d7:ee:a5 00:0f:b5:92:cd:49 00:12:17:70:85:3d 00:14:bf:ae:b1:e4 00:40:f4:f8:47:03 00:0c:41:d7:ee:b4 2. Select one of the following options: â¢ Select the Replace radio button to replace the existing list of known APs. Â¢ Select the Merge radio button to add the new MAC addresses to the existing list. 3. Click Browse and navigate to the location where you saved the text file. Click Apply to upload the list to the wireless access point. 4-20 v1. 0, February 2009 Managing Your Network Chapter 5 Advanced Configuration This chapter describes how to configure the advanced features of your WG103 ProSafe 802.

11g Wireless Access Point. These features can generally be found under Advanced under the main options of the Configuration tab such as System, Wireless, and Security (as an example, see Figure 5-1 on page 5-2). This chapter includes: â¢ â¢ â¢ â¢ â¢ â¢ âEthernet Link Configurationâ on this page. âHotspot Settingsâ on page 5-2. This section describes how to redirect HTTP requests. This section describes how to configure station and access point Enhanced Distributed Channel Access (EDCA) settings. ÂWireless Bridging and Repeatingâ on page 5-9 Ethernet Link Configuration The Ethernet link configuration settings allow you to select or set the type of Ethernet link for the wireless access point.