



Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for NETGEAR WN203. You'll find the answers to all your questions on the NETGEAR WN203 in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual NETGEAR WN203
User guide NETGEAR WN203
Operating instructions NETGEAR WN203
Instructions for use NETGEAR WN203
Instruction manual NETGEAR WN203

NETGEAR®

ProSAFE Single Band 802.11n
Wireless Access Point WN203
Reference Manual



June 2013
202-11223-01

350 East Plumeria Drive
San Jose, CA 95134
USA



[You're reading an excerpt. Click here to read official NETGEAR WN203 user guide](http://yourpdfguides.com/dref/5435532)
<http://yourpdfguides.com/dref/5435532>

Manual abstract:

netgear.com. Phone (US & Canada only): 1-888-NETGEAR. Phone (Other Countries): Check the list of phone numbers at <http://support.netgear.com/general/contact/default.aspx>. Trademarks NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. © NETGEAR, Inc. All rights reserved. Revision History Publication Part Number 202-11230-01 Publish Date June 2013 Comments First publication 2 Contents Chapter 1 Introduction About the ProSAFE Single Band 802.11n Wireless Access Point WN203 . 7 What Is in the Box? .

.....
.....

.....
.....
.....
.....
..... 7 System Requirements ...

.....
.....
.....
.....
..... 8 Key Features and Standards ..

.....
.....
.....
.....
..... 8 Supported Standards and Conventions .

.....
.....
.....
.....
..... 8 Key Features

.....
.....
.....
.....
..... 9 802.11b/g/n Standards–Based Wireless Networking ...

.....
.....
.....
.....
..... 10 Autosensing Ethernet Connections with Auto Uplink ...

.....
.....
.....
.....
..... 11 Hardware Description ...

.....
.....
.....
.....
..... 11 Front Panel ...

.....
.....
.....
.....
..... 11 Back Panel

.....
.....
.....
.....
..... 12 Bottom Panel with Product Label and Reset to Factory Defaults Button 13 Chapter 2 Installation and Basic Configuration What You Need Before You

	Begin . . .

...	15 Wireless Equipment Placement and Range Guidelines . .

 15 Ethernet Cabling Requirements

 16 LAN Configuration Requirements. . .

.....	16 Hardware Requirements for Computers on Your LAN . . .

	. 16 Requirements for Entering IP Addresses

.....	16 Install and Configure the Wireless Access Point

 16 Connect the Wireless Access Point to a Computer

	. 17 Log In to the Wireless Access Point

.....	18 Configure Basic General System Settings and Time Settings .

	.. 20 Configure the IP Settings . . .

...	22 Configure the Optional DHCP Server.

	23 Configure the Basic Wireless Settings

	. 25 Test Basic Wireless Connectivity

...	28 Chapter 3 Wireless Configuration and Security Before You Configure Wireless Security . .

 31 Wireless Data Security Options .

	.. 31 Security Profiles . . .

..	33 Security Profile Concepts

.....	34 Write Down Your Wireless Network Settings ..

.....	35 Configure and Enable Security Profiles .

....	36 Configure RADIUS Server Settings

....	45 Restrict Wireless Access by MAC Address

... 46 3	ProSAFE Single Band 802.11n Wireless Access Point WN203 Schedule the Wireless Radios to Be Turned Off .

.....	49 Configure Basic Wireless Quality of Service .

.. 49	Chapter 4 Management Enable Remote Management.

.....	52 SNMP Management ...

.. 52	Secure Shell and Telnet Management ...

... 53	Upgrade the Wireless Access Point Software ..

.....	54 Web Browser Upgrade Procedure

.....	55 TFTP Server Upgrade Procedure.

75	Configure a Point-to-Point Wireless Network	
	
	
. 76	Configure a Point-to-Multipoint Wireless Network	
	
... 81	Configure the Wireless Access Point to Repeat the Wireless Signal Using Point-to-Multipoint Bridge Mode	
	
..... 85	Chapter 6 Monitoring View System Information	
	
	
	
	
	
. 92	Monitor Wireless Clients.	
	
	
	
..... 94	View the Activity Log	
	
	
	
..... 96	Traffic Statistics	
	
	
	
	
	
. 97	Chapter 7 Troubleshooting Basic Functioning	
	
	
	
... 100	Verify the Correct Sequence of Events at Startup	
	
	
100	No LEDs Are Lit on the Wireless Access Point	
	
..... 100	LAN LED Is Not Lit	
	
	
	
	
... 101	WLAN LED Is Not Lit	
	
	
	
..... 101	You Cannot Access the Internet or the LAN from a 4 ProSAFE Single Band 802.11n Wireless Access Point WN203 Wireless-Capable Computer	
	
	
	

.....
.....

.101 You Cannot Configure the Wireless Access Point from a Browser102 When You Enter a URL or IP Address a Time-Out Error Occurs

.103 Troubleshoot a TCP/IP Network Using the Ping Utility. .

.....

.103 Test the LAN Path to Your Wireless Access Point . .

.....

.103 Test the Path from Your Computer to a Remote Device .

.....

.104 Problems with Date and Time

.....

.105 Appendix A Supplemental Information Technical Specifications . .

.....

.107 Factory Default Settings

.....

.108 Appendix B Appendix C Index Command-Line Reference Notification of Compliance 5 1.

Introduction 1 This chapter introduces the NETGEAR® ProSAFE® Single Band 802.11n Wireless Access Point WN203, and describes some of the key features. The chapter includes the following sections: •••••About the ProSAFE Single Band 802.11n Wireless Access Point WN203 What Is in the Box? System Requirements Key Features and Standards Hardware Description Note: For more information about the topics covered in this manual, visit the support website at support.netgear.com. Note: Firmware updates with new features and bug fixes are made available from time to time at downloadcenter.netgear.com.



[You're reading an excerpt. Click here to read official NETGEAR WN203 user guide](http://yourpdfguides.com/dref/5435532)
<http://yourpdfguides.com/dref/5435532>

Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product do not match what is described in this guide, you might need to update your firmware. 6 ProSAFE Single Band 802.11n Wireless Access Point WN203 About the ProSAFE Single Band 802.11n Wireless Access Point WN203 The ProSAFE Single Band 802.11n Wireless Access Point WN203, going forward in this manual referred to as the wireless access point, is a solid building block of a wireless LAN infrastructure.

It provides 2.4 GHz 802.11b/g/n connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Support for two transmit radio chains and two receive radio chains, also referred to as 2x2 multiple input, multiple output (MIMO), can increase wireless throughput considerably. The wireless access point provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage. Typically, an individual in-building wireless access point provides a maximum connectivity area with about a 500-foot radius. The wireless access point can support a maximum of 64 clients in a range of several hundred feet. The throughput is shared between all clients. To meet the required coverage, throughput, and quality of your wireless network, install a sufficient number of wireless access points. The wireless access point acts as a bridge between the wired LAN and wireless clients.

Connecting multiple wireless access points through a wired Ethernet backbone can further increase 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 a seamless connection to the network. The autosensing capability of the wireless access point allows packet transmission at up to 300 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference. What Is in the Box? The product package contains the following items: •••••ProSAFE Single Band 802.

1 In Wireless Access Point WN203 Straight through Category 5 Ethernet cable Power adapter and cord (12V, 1A) Stand Two wall mount screws and anchors Resource CD Installation guide If any parts are missing or damaged, contact your reseller or customer support in your area. Visit the NETGEAR website at <http://support.netgear.com/general/contact/default.aspx> for the telephone number of customer support in your area.

Keep the installation guide, along with the original packing materials. If you need to return the wireless access point for repair, use the packing materials to repack the wireless access point. Introduction 7 ProSAFE Single Band 802.11n Wireless Access Point WN203 External antennas do not come standard with the wireless access point but can be purchased as an option. If you have purchased external antennas, see Configure Advanced Wireless Settings on page 70 for information about how to enable the external antennas. System Requirepoint does not function as an access point for clients but functions only in point-to-multipoint bridge mode to repeat the wireless signal and send all traffic to a remote access point. - - • WMM. Wi-Fi Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data.

Time-dependent information, like video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients also need to support WMM. QoS. Quality of Service (QoS) support lets you configure parameters that affect traffic flowing from the wireless access point to the client station and traffic flowing from the client station to the wireless access point. Hotspot support. You can allow all HTTP (TCP, port 80) requests to be captured and redirected to the URL you specify. Rogue AP detection. Rogue AP filtering ensures that unknown APs are not given access to any part of the secured wireless and wired LAN. •••Introduction 9 ProSAFE Single Band 802.11n Wireless Access Point WN203 •••••Access control.

MAC address filtering can ensure that only trusted wireless clients can use the wireless access point to gain access to the wireless and wired LAN. Security profiles. When using multiple BSSIDs, you can configure unique security settings (encryption, SSID, and so on) for each BSSID. Hidden mode. The SSID is not broadcast, assuring that only clients configured with the correct SSID can connect.

Telnet and SSH command-line interface. Using an application such as PuTTY, you can access the wireless access point over a Telnet or Secure Shell (SSH) connection and use the command-line interface (CLI) to configure the wireless access point. Upgradeable firmware. Firmware is stored in flash memory. You can upgrade it easily, using only your web browser, and you can upgrade it remotely.

You can also use the command-line interface. 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. PoE support. Using Power over Ethernet (PoE), any 802.3af-compliant midspan or end-span sources can supply power to the wireless access point over the Ethernet port. The wireless access point can receive all required power on one Ethernet port from a single PoE source. Autosensing Ethernet connection with Auto Uplink™ interface.

Connects to 10/100/1000 Mbps IEEE 802.3 Ethernet networks. LED indicators. Power, Test, LAN, and WLAN LEDs are easily identified. VLAN security profiles. Each security profile is automatically allocated a VLAN ID when the security profile is modified. •••••802.11b/g/n Standards-Based Wireless Networking The wireless access point provides a bridge between wired Ethernet LANs and 802.11b/g/n-compatible wireless LAN networks. It provides connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, RFID tags, and other devices. In addition, the wireless access point supports the following wireless features: •••••••Aggregation support Reduced InterFrame spacing support 2x2 multiple input, multiple output (MIMO) support Distributed coordinated function (CSMA/CA, back-off procedure, ACK procedure, retransmission of unacknowledged frames) RTS/CTS handshake Beacon generation Packet fragmentation and reassembly Auto or long preamble Introduction 10 ProSAFE Single Band 802.11n Wireless Access Point WN203 • Roaming among wireless access points on the same subnet Autosensing Ethernet Connections with Auto Uplink The wireless access point can connect to a standard Ethernet network.



[You're reading an excerpt. Click here to read official NETGEAR WN203 user guide](http://yourpdfguides.com/dref/5435532)
<http://yourpdfguides.com/dref/5435532>

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 automatically senses 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 then configures itself correctly. This feature also eliminates any concerns about crossover cables, because Auto Uplink accommodates either type of cable to make the right connection. Hardware Description This section describes the front and back hardware functions of the wireless access point. •••

Front Panel Back Panel Bottom Panel with Product Label and Reset to Factory Defaults Button Front Panel The LEDs of the wireless access point are described in the following figure and table: 1 Figure 1. Front panel with LEDs 2 3 4 Introduction 11 ProSAFE Single Band 802.

1 In Wireless Access Point WN203 Table 1. Front panel LEDs Item 1 LED Description Power Off Green 2 Test Off Amber Power is off. Power is on. The wireless access point functions normally. The wireless access point is starting. After about one minute, the LED turns off. New firmware is being loaded. No link is detected on the LAN port. A 100 Mbps or 10 Mbps link is detected on the LAN port. A 1000 Mbps link is detected on the LAN port.

The wireless LAN is not ready, or no wireless activity is detected. The wireless LAN is ready. Wireless activity is detected. Blinking amber 3 LAN Off Amber Green 4 WLAN Off Blue Blinking Blue Back Panel 1 Figure 2. Back panel 2 3 4 5 The back panel components of the wireless access point, from left to right, are described in the following list: 1. Reverse SMA connector for an optional 2.4 GHz antenna. 2. Console port for connecting to an optional console terminal. The port has an RJ-45 connector and supports the following settings: 115200 K default baud rate, (8) data bits, no (N) parity bit, and one (1) stop bit.

3. 10/100/1000BASE-T Gigabit Ethernet RJ-45 LAN port with Auto Uplink (Auto MDI-X) and IEEE 802.3af Power over Ethernet (PoE) support for connection to a switch or router. Introduction 12 ProSAFE Single Band 802.11n Wireless Access Point WN203 4.

Power socket for a 12 VDC, 1A power adapter. 5. Reverse SMA connector for an optional 2.4 GHz antenna. If you have purchased external antennas, see Configure Advanced Wireless Settings on page 70 for information about how to enable the external antennas.

Bottom Panel with Product Label and Reset to Factory Defaults Button The product label on the bottom of the wireless access point's enclosure displays factory default settings, regulatory compliance, and other information. The bottom panel also contains the recessed Reset to Factory Defaults button, which is indicated on the product label. 2.4 Ghz Console LAN http://192.168.0.100 user name: admin password: password Power 12V 1.0A 2.4 Ghz MAC Single Band 802.11n Wireless Access Point ProSAFE WN203 FCC ID: PY312400222 IC: 4054A-12400221 SERIAL This device complies with part 15 of the FCC Rules and Canada ICES-003.

Operation is subject to the following two conditions: (1) this device may not Reset to cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. Factory Defaults Designed by NETGEAR in California Made in China 272-11850-02 Reset to Factory Defaults button Figure 3. Product label on the bottom □ To reset the wireless access point to factory default settings: Use a sharp object to press and hold the Reset to Factory Defaults button for about 10 seconds. All custom configuration settings are lost, and the default password is restored. For more information, see Restore the Wireless Access Point to the Factory Default Settings on page 58. Introduction 13 2. Installation and Basic Configuration 2 This chapter describes how to install and configure the wireless access point for wireless connectivity to your LAN. This basic configuration enables computers with 2.4 GHz 802.11b/g/n 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, Wireless Configuration and Security, describes how to set up wireless security for your network. This chapter includes the following sections: ••• What You Need Before You Begin Install and Configure the Wireless Access Point Test Basic Wireless Connectivity 14 ProSAFE Single Band 802.11n Wireless Access Point WN203 What You Need Before You Begin You need to consider the guidelines and requirements in the following sections before you can set up your wireless access point. See also System Requirements on page 8.

•••• Wireless Equipment Placement and Range Guidelines Ethernet Cabling Requirements LAN Configuration Requirements Hardware Requirements for Computers on Your LAN Requirements for Entering IP Addresses 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 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 connect wirelessly to the wireless access point. For complete performance specifications, see Appendix A, Supplemental Information. For best results, place your wireless access point according to the following general guidelines: •••• Near the center of the area in which the wireless devices will operate.

In an elevated location such as a high shelf where the wirelessly connected devices have line-of-sight access (even if through walls). Away from sources of interference, such as computers, microwaves ovens, and 2.4 GHz cordless phones. Away from large metal surfaces or water. 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. Installation and Basic Configuration 15 ProSAFE Single Band 802.11n Wireless Access Point WN203 Ethernet Cabling Requirements The wireless access point connects to your LAN using 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.

Hardware Requirements for Computers on Your LAN To connect to the wireless access point on your network, each computer needs to have an 802.11b/g/n wireless adapter installed. Requirements for Entering IP Addresses The fourth octet of an IP address needs to be between 0 and 255 (both inclusive).



[You're reading an excerpt. Click here to read official NETGEAR](http://yourpdfguides.com/dref/5435532)

[WN203 user guide](http://yourpdfguides.com/dref/5435532)

<http://yourpdfguides.com/dref/5435532>

This requirement applies to any IP address that you enter on a screen of the web management interface. Install and Configure the Wireless Access Point
Install and configure your wireless access point in the order of the following sections: 1. Connect the Wireless Access Point to a Computer 2. Log In to the Wireless Access Point 3. Configure Basic General System Settings and Time Settings 4. Configure the IP Settings 5. Configure the Optional DHCP Server 6. Configure the Basic Wireless Settings Before installing the wireless access point, make sure that your Ethernet network functions. After you have connected the wireless access point to the Ethernet network, computers with 802.11b/g/n wireless adapters are able to communicate with the Ethernet network. Before you start the installation and configuration process, verify that you have met all the system requirements. See System Requirements on page 8.

Installation and Basic Configuration 16 ProSAFE Single Band 802.11n Wireless Access Point WN203 Connect the Wireless Access Point to a Computer Tip: Before you place the wireless access point in an elevated position that is difficult to reach, first set up and test the wireless access point to verify wireless network connectivity. □ To set up the wireless access point: 1. Unpack the box and verify the contents. 2.

Prepare a computer with an Ethernet adapter: a. 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 192.168.0.210 and 255.255.255.0 as the subnet mask.

3. Connect an Ethernet cable to the Ethernet port (A) of the computer. 4. Securely insert the other end of the Ethernet cable into the wireless access point's LAN port (B). A B 5. Turn on your computer. 6. Connect the power adapter to the wireless access point. Tip: The wireless access point supports Power over Ethernet (PoE). If you have a switch that provides PoE, you do not need to use the power adapter to power the wireless access point.

Using PoE can be especially convenient when the wireless access point is installed in a high location far away from a power outlet. 7. Verify the following: Power LED. The Power LED is green. If the Power LED is off, check the connections, and check if the power outlet is controlled by a wall switch that is turned off.

Installation and Basic Configuration 17 ProSAFE Single Band 802.11n Wireless Access Point WN203 Test LED. The Test LED is amber. After about one minute, the Test LED turns off. LAN LED.

The LAN LED indicates the LAN speed for the LAN port: green for 1000 Mbps or amber for 100 Mbps or 10 Mbps. WLAN LED. The WLAN LED is blue when the wireless LAN (WLAN) is ready. Log In to the Wireless Access Point The default IP address of your wireless access point is 192.168.0.100. By default, the DHCP client on the wireless access point is disabled so you can log in using the default IP address. □ To log in to the wireless access point: 1. Open a web browser such as Microsoft Internet Explorer 8.

0 or later, or Mozilla Firefox 18.0 or later. 2. Connect to the wireless access point by entering its default address of 192.168.0.100 into your browser (use http and not https). The Login screen displays: 3. Enter the default user name of admin and the default password of password. 4.

Click the Login button. The web browser displays the basic General system settings screen under the Configuration tab of the main menu: Installation and Basic Configuration 18 ProSAFE Single Band 802.11n Wireless Access Point WN203 The navigation tabs across the top of the web management interface provide access to all the configuration functions of the wireless access point and remain constant. The menu items in the blue bar change according to the navigation tab that is selected. Figure 4.

Navigation tabs and menu items The bottom right corner on all screens that allow you to make configuration changes show the Apply and Cancel buttons.

Figure 5. Buttons These buttons have the following functions: • • Cancel. Cancels all configuration changes that you made on the screen. Apply. Saves and applies all configuration changes that you made on the screen. The following buttons can be displayed: • • • • • Edit. Lets you edit the existing configuration. Save or Save As. Lets you save the information that is displayed onscreen to a file. Details. Provides more details for the information that is displayed in a table onscreen. Refresh. Refreshes the information that is displayed onscreen. Clear.

Clears the information that is displayed onscreen. Back. Returns to the previous screen. Send. Sends a test command. Installation and Basic Configuration 19 ProSAFE Single Band 802.11n Wireless Access Point WN203 Configure Basic General System Settings and Time Settings After you have successfully logged in to the wireless access point, the basic General system settings screen displays. □ To configure basic system settings: 1. Select Configuration > System > Basic > General. The basic General system settings screen displays: 2.

Configure the settings as described in the following table: Setting AP Name Description This unique name is the wireless access point NetBIOS name. The name is printed on the label of the wireless access point. The default is netgearxxxxx, in which xxxxxx represents the last six digits of the wireless access point MAC address. You can replace the default name with a unique name up to 15 characters long. The access point name can be retrieved through SNMP. From the Country / Region drop-down menu, select the country where the wireless access point is installed. Note: It might not be legal to operate this wireless access point in a region other than one of the regions that you can select from the drop-down menu. Country / Region 3. Click the Apply button. Installation and Basic Configuration 20 ProSAFE Single Band 802.

11n Wireless Access Point WN203 □ To configure time settings: 1. Select Configuration > System > Basic > Time. The Time screen displays: 2. Configure the settings as described in the following table: Setting Time Zone Current Time NTP Client Description Select the time zone to match your location. This is a nonconfigurable field that displays the current date and time. Enable the Network Time Protocol (NTP) client to synchronize the time of the wireless access point with an NTP server. By default the Enable radio button is selected. Select this check box if you want to use a custom NTP server. Note: You need to have an Internet connection to use an NTP server that is not on your local network. Hostname / IP Address Enter the host name or IP address of the custom NTP server.

The default NTP server depends on the selected time zone. For example, for China the default is time-e.netgear.com. Note: If you use a host name, make sure that you have configured a DNS server. For more information, see the next section. Use Custom NTP Server 3. Click the Apply button. Installation and Basic Configuration 21 ProSAFE Single Band 802.



[You're reading an excerpt. Click here to read official NETGEAR](http://yourpdfguides.com/dref/5435532)

[WN203 user guide](http://yourpdfguides.com/dref/5435532)

<http://yourpdfguides.com/dref/5435532>

1 In Wireless Access Point WN203 Configure the IP Settings WARNING: If you enable the DHCP client, the IP address of the wireless access point changes when you click the Apply button, causing you to lose your connection to the wireless access point.

You then need to use the new IP address to reconnect to the wireless access point. Tip: If you enable the DHCP client on the wireless access point, you can discover the new IP address of the wireless access point by accessing the DHCP server on your LAN, or by using a network IP address scanner application. □ To configure the IP settings: 1. Select Configuration > IP > IP Settings. The IP Settings screen displays: Installation and Basic Configuration 22 ProSAFE Single Band 802.

1 In Wireless Access Point WN203 2. Configure the IP settings as described in the following table: Setting DHCP Client Description By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN and you select the Enable radio button, the wireless access point receives its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the wireless access point to your LAN. If you do not enable the DHCP client, enter the IP address of your wireless access point. The default IP address is 192.168.0.100. To change the address, enter an unused IP address from the address range that is used on your LAN. If you do not enable the DHCP client, enter the network number portion of an IP address. Unless you are implementing subnetting, enter 255.255.0.0 as the subnet mask. If you do not enable the DHCP client, enter the IP address of the ISP gateway to which the wireless access point connects.

If you do not enable the DHCP client, enter the IP addresses of the primary and secondary DNS servers. A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your wireless access point during login. If the ISP does not transfer addresses, you need to obtain them from the ISP and enter them manually in these fields. Select this check box to validate that the upstream link is active before allowing wireless associations. Ensure that the default gateway is configured. IP Address IP Subnet Mask Default Gateway Primary DNS Server Secondary DNS Server Network Integrity Check 3. Click the Apply button.

Configure the Optional DHCP Server The wireless access point provides a built-in DHCP server for wireless clients only, which can be especially useful in small networks. By default, the DHCP server is disabled. When the DHCP server is enabled, the wireless access point provides preconfigured TCP/IP configurations to all connected wireless clients. □ To configure DHCP server settings: 1. Select Configuration > IP > DHCP Server Settings.

The DHCP Server Settings screen displays: Installation and Basic Configuration 23 ProSAFE Single Band 802.1 In Wireless Access Point WN203 2. Configure the settings as described in the following table: Setting Description Select the Enable radio button to enable the DHCP server. Use the default settings or specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the wireless access point's LAN IP address.

DHCP Server VLAN ID Enter the VLAN ID for the DHCP server. The VLAN ID range is from 1 to 4094. The default VLAN is 1. Enter the first address in the range of IP addresses to be assigned to DHCP clients. The default address is 192.168.1.02. Enter the last address in the range of IP addresses to be assigned to DHCP clients. The default address is 192.

168.1.50. Enter the subnet mask to be used by DHCP clients. The default mask is 255.255.255.0. Enter the IP address of the default routing gateway to be used by DHCP clients. The default address is 192.

168.0.1. Enter the IP address of the primary Domain Name System (DNS) server available to DHCP clients. Enter the IP address of the secondary DNS server available to DHCP clients.

Enter the IP address of the primary WINS server for the network, if there is any. Starting IP Address Stopping IP Address Subnet Mask Gateway IP Address Primary DNS Server Secondary DNS Server Primary WINS Server Installation and Basic Configuration 24 ProSAFE Single Band 802.1 In Wireless Access Point WN203 Setting Description Secondary WINS Server Enter the IP address of the secondary WINS server for the network, if there is any. Lease Enter the period that the DHCP server grants to DHCP clients to use the assigned IP addresses. The default time is 1 (one day).

3. Click the Apply button. Configure the Basic Wireless Settings For proper compliance and compatibility between similar products in your coverage area, you need to configure the 802.11b/g/n wireless adapter settings correctly, including the operating channel and country. You also need to configure the basic wireless network settings for wireless devices to connect to your network. For other wireless features, including wireless security, see Chapter 3, Wireless Configuration and Security. Operating Frequency (Channel) Guidelines You do not need to change the operating frequency (channel) unless you notice interference problems or you place the wireless access point near another wireless access point. If you do change the operating frequency, observe the following guidelines: • Wireless access points use a fixed channel. You can select a channel that provides the least interference and best performance. In the United States and Canada, 11 channels are available.

If you are 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). In infrastructure mode (which is the default mode for the wireless access point), wireless clients normally scan all channels, looking for a wireless access point. If more than one wireless access point is available, and the wireless access points use the same SSID, a wireless client uses the wireless access point with the strongest signal. • • Configure 802.11b/g/n Wireless Settings The basic Wireless Settings screen lets you configure the wireless mode, SSID, and other wireless settings. WARNING: If you configure the wireless access point from a wireless computer and you change the wireless access point's SSID, channel, or wireless security settings, you lose your wireless connection when you click the Apply button. You then need to change the wireless settings of your computer to match the wireless access point's new settings. Installation and Basic Configuration 25 ProSAFE Single Band 802.1 In Wireless Access Point WN203 □ To configure the 802.11b/g/n wireless settings: 1.



[You're reading an excerpt. Click here to read official NETGEAR WN203 user guide](http://yourpdfguides.com/dref/5435532)
<http://yourpdfguides.com/dref/5435532>

Select Configuration > Wireless > Basic > Wireless Settings. The basic Wireless Settings screen displays. The following figure shows the 11ng settings. Note: The radio wave icon (mode (b, bg, or ng).

) displays next to the enabled wireless 2. Select one of the following 2.4 GHz band radio buttons: • 11b. Both 802.11n- and 802.

11g-compliant devices can connect to the access point because they are backward compatible. • 11bg. 802.11n-compliant devices cannot connect to the access point because they are backward compatible. 11ng. This is the default setting. 802.11b-compliant devices cannot connect to the access point. If you keep the default setting, go to Step 5. When you change the wireless mode, the Turn Radio On check box is automatically cleared, and all fields, buttons, and drop-down menus onscreen are masked out.

3. Turn on the radio by selecting the Turn Radio On check box. A pop-up screen displays. Installation and Basic Configuration 26 ProSAFE Single Band 802.11n Wireless Access Point WN203 Note: Under normal conditions, you want the radio to be turned on. Turning off the radio disables access through the wireless access point, which can be helpful for configuration, network tuning, or troubleshooting activities. 4. Click the OK button to confirm the change of wireless mode. The change does not take effect until after you have completed the wireless configuration and have clicked the Apply button. 5.

Specify the remaining wireless settings as described the following table: Setting Descriptions Wireless Network Name Enter a 32-character (maximum) service set identifier (SSID); the characters are (SSID) case-sensitive. The default is NETGEAR_11ng. The SSID assigned to a wireless device needs to match the wireless access point's SSID for the wireless device to communicate with the wireless access point. If the SSIDs do not match, you do not get a wireless connection to the wireless access point. Wireless On-Off Status This field is not configurable.

It shows the status of the wireless scheduler. For more information, see Schedule the Wireless Radios to Be Turned Off on page 49. Select the Yes radio button to enable the wireless access point to broadcast its SSID, allowing wireless clients that have a null (blank) SSID to adopt the wireless access point's SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button.

From the drop-down menu, select the channel you wish to use for your wireless LAN. The wireless channels and frequencies depend on the country and wireless mode. The default setting is Auto. Note: You should not have to change the wireless channel unless you experience interference (indicated by lost connections or slow data transfers). If this situation occurs, you might want to experiment with different channels to see which is the best. For more information, see Operating Frequency (Channel) Guidelines on page 25. Note: For more information about available channels and frequencies, see Technical Specifications on page 107. Broadcast Wireless Network Name (SSID) Channel / Frequency Installation and Basic Configuration 27 ProSAFE Single Band 802.11n Wireless Access Point WN203 Setting MCS Index / Data Rate 11ng mode only Note: For most networks, the default settings work fine. Descriptions From the drop-down menu, select a Modulation and Coding Scheme (MCS) index and transmit data rate for the wireless network.

The default setting is Best. For a list of all options that you can select, see Technical Specifications on page 107. Channel Width From the drop-down menu, select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, and 40 MHz. The default is 20 MHz. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz. From the drop-down menu, select the guard interval to protect transmissions from interference. The default is Auto, or you can select Long - 800 ns. Some legacy devices can operate only with a long guard interval. Guard Interval Output Power From the drop-down menu, select the transmission power of the wireless access point: Full, Half, Quarter, Eighth, Minimum.

The default is Full. Note: Increasing the power improves performance, but if two or more wireless access points are operating in the same area and on the same channel, interference can occur. Note: Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country. 6. Click the Apply button.

The selected wireless mode is now enabled. Note: For information about how to configure advanced wireless settings, see Configure Advanced Wireless Settings on page 70. Test Basic Wireless Connectivity After you have configured the wireless access point as described in the previous sections, test the computers on your LAN for wireless connectivity before you position the wireless access point at its permanent position. □ To test for wireless connectivity: 1. Configure the 802.

11b/g/n 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. If you have enabled the DHCP server on the wireless access point, verify that your computers are able to obtain an IP address through DHCP from the wireless access point. Installation and Basic Configuration 28 ProSAFE Single Band 802.11n Wireless Access Point WN203 3. Verify network connectivity by using a browser such as Microsoft Internet Explorer 8.0 or later, or Mozilla Firefox 18.0 or later to browse the Internet, or check for file and printer access on your network. Note: If you have trouble connecting to the wireless access point, see Chapter 7, Troubleshooting.

NETGEAR recommends that you complete the following tasks before you deploy the wireless access point in your network: • • Configure wireless security and other wireless features. See Chapter 3, Wireless Configuration and Security. Configure any additional features that you might need. See Chapter 4, Management, and Chapter 5, Advanced Configuration. After you have completed the configuration of the wireless access point, you can reconfigure the computer that you used for this process back to its original TCP/IP settings. Installation and Basic Configuration 29 3. Wireless Configuration and Security 3 This chapter describes how to configure the wireless features of the wireless access point. The chapter includes the following sections: • • • • • Before You Configure Wireless Security Wireless Data Security Options Security Profiles Configure RADIUS Server Settings Restrict Wireless Access by MAC Address Schedule the Wireless Radios to Be Turned Off Configure Basic Wireless Quality of Service 30 ProSAFE Single Band 802.11n Wireless Access Point WN203 Before You Configure Wireless Security Before you set up wireless security and additional wireless features that are described in this chapter, connect the wireless access point, get the Internet connection working, set the country or region correctly, and configure the 802.



[You're reading an excerpt. Click here to read official NETGEAR](http://yourpdfguides.com/dref/5435532)

[WN203 user guide](http://yourpdfguides.com/dref/5435532)

<http://yourpdfguides.com/dref/5435532>

11b, 11bg, or 11ng wireless settings.

See Chapter 2, *Installation and Basic Configuration*. The wireless access point functions with an Ethernet LAN connection. Make sure that you have verified wireless connectivity before you set up wireless security and additional wireless features. **WARNING:** If you are configuring the wireless access point from a wireless computer and you change the wireless access point's SSID, channel, or wireless security settings, you lose your wireless connection when you click the Apply button. You then need to change the wireless settings of your computer to match the wireless access point's new settings.

Wireless Data Security Options Indoors, computers can connect over 802.11n 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. Wireless data security options Range: Up to 300 feet radius 1. No security: Easy but no security at all 2. MAC access list: No data security 3. WEP: Secure but vulnerable 4. WPA or WPA-PSK: Strong security 5. WPA2 or WPA2-PSK: Very strong Figure 6. Wireless data security options Wireless Configuration and Security 31 ProSAFE Single Band 802.

11n Wireless Access Point WN203 There are many ways in which you can enhance the security of your wireless network:

- Use multiple BSSIDs combined with VLANs. You can configure combinations of VLANs and BSSIDs (security profiles) 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 *Configure and Enable Security Profiles* on page 36.
- Restrict access based by MAC address. You can allow only trusted devices to connect so that unknown devices 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 *Restrict Wireless Access by MAC Address* on page 46.
- 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 off broadcast of the SSID, see *Configure and Enable Security Profiles* on page 36.

- WEP. Wired Equivalent Privacy (WEP) data encryption provides data security. 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 the following sections:

- *Configure and Enable Security Profiles* on page 36
- Configure an Open System with WEP or Shared Key with WEP* on page 40
- Legacy 802.1X. Legacy 802.1X uses RADIUS-based 802.*

1x authentication but no data encryption. For information about how to configure Legacy 802.1X, see the following sections: *Configure and Enable Security Profiles* on page 36 *Configure Legacy 802.1X* on page 42

- WPA and WPA-PSK (TKIP). Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) encryption. The very strong authentication along with dynamic per-frame rekeying of WPA makes it virtually impossible to compromise. WPA uses RADIUS-based 802.1x authentication; for more information, see the following sections: *Configure and Enable Security Profiles* on page 36 *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 42

Wireless Configuration and Security 32 ProSAFE Single Band 802.11n Wireless Access Point WN203 WPA-PSK uses a pre-shared key (PSK) for authentication; for more information, see the following sections:

- *Configure and Enable Security Profiles* on page 36
- Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 43

WPA2 and WPA2-PSK (AES). Wi-Fi Protected Access version 2 (WPA2) data encryption provides strong data security with Advanced Encryption Standard (AES) encryption.

The very strong authentication along with dynamic per-frame rekeying of WPA2 makes it virtually impossible to compromise. WPA2 uses RADIUS-based 802.1x authentication; for more information, see the following sections: *Configure and Enable Security Profiles* on page 36 *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 42

WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see the following sections:

- *Configure and Enable Security Profiles* on page 36
- Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 43

WPA & WPA2 and WPA-PSK & WPA2-PSK mixed modes. These modes support data encryption either with both WPA and WPA2 clients or with both WPA-PSK and WPA2-PSK clients and provide the most reliable security. WPA & WPA2 uses RADIUS-based 802.1x authentication; for more information, see the following sections: *Configure and Enable Security Profiles* on page 36 *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 42

WPA-PSK & WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see the following sections: *Configure and Enable Security Profiles* on page 36 *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 43

Security Profiles This section describes the main components of security profiles and explains how to configure and enable security profiles.

- Security Profile Concepts Write Down Your Wireless Network Settings

Configure and Enable Security Profiles Wireless Configuration and Security 33 ProSAFE Single Band 802.11n Wireless Access Point WN203 Security profiles let you configure unique security settings for each SSID on each radio of the wireless access point. For each radio, the wireless access point supports up to eight security profiles (BSSIDs) that you can configure on the individual Edit Wireless Network screens that are accessible from the Edit Security Profile screen (see *Configure and Enable Security Profiles* on page 36).

Security Profile Concepts Security profiles include the following main components:

- 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 that not all wireless adapters support WPA or WPA2.



[You're reading an excerpt. Click here to read official NETGEAR](http://yourpdfguides.com/dref/5435532)

[WN203 user guide](http://yourpdfguides.com/dref/5435532)

<http://yourpdfguides.com/dref/5435532>

Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions about how to configure WPA or WPA2 settings. For information about the types of network authentication that the wireless access point supports, see *Configure and Enable Security Profiles* on page 36. • Data encryption The available data encryption options depend on the network authentication setting that you select (the default is no encryption).

The data encryption settings are explained in *Configure and Enable Security Profiles* on page 36.

Wireless client security separation If this feature is enabled, the associated wireless clients (using the same SSID) are not able to communicate with each other. This feature is useful for hotspots and other public access situations. By default, wireless client separation is disabled. For more information, see *Configure and Enable Security Profiles* on page 36. **VLAN ID** If this feature is enabled and if the network devices (hubs and switches) on your LAN support the VLAN (802.

IQ) standard, the default VLAN ID for the wireless access point is associated with each profile. The default VLAN ID needs to match the IDs that are used by the other network devices. For more information, see *Configure and Enable Security Profiles* on page 36. •• Some concepts and guidelines regarding the SSID are explained in the following list: • A basic service set (BSS) consists of a group of wireless clients and a single wireless access point that use the same security profile or service set identifier (BSSID). The actual identifier in the BSSID is the MAC address of the wireless radio. (A wireless radio can have multiple MAC addresses, one for each security profile.) An extended service set (ESS) consists of a group of wireless clients and multiple wireless access points that use the same identifier (ESSID). 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 clients to connect wirelessly when they physically move from one BSS to another one within the same ESS.

The wireless client automatically changes to the wireless access point with the least interference or best performance. ••• *Wireless Configuration and Security 34 ProSAFE Single Band 802.11n Wireless Access Point WN203 Write Down Your Wireless Network Settings* For a new wireless network, print or copy the following form and fill in the settings. For an existing wireless network, the network administrator can provide this information. Print the form and store the security information in a safe place: • SSID. The service set identifier (SSID) identifies the wireless local area network. You can customize it by using up to 32 alphanumeric characters. Write your SSID on the line. SSID: _____ The SSID in the wireless access point is the SSID you configure on the wireless adapter card. All wireless nodes in the same network need to be configured with the same SSID.

• WEP key size and authentication Choose the key size by circling one: 64, 128, or 152 bits. Choose the authentication type by circling one: open system or shared key. Passphrase: _____ Note: If you select shared key, the other devices in the network cannot connect unless they are set to shared key and have the same keys in the same positions as those in the wireless access point. • WPA-PSK (pre-shared key) and WPA2-PSK Record the WPA-PSK passphrase: WPA-PSK passphrase: _____ Record the WPA2-PSK passphrase: WPA2-PSK passphrase: _____ • WPA RADIUS settings For WPA, record the following settings for the primary and secondary RADIUS servers: Server name or IP address: Primary _____ Secondary _____ Port: _____ 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: _____

Wireless Configuration and Security 35 ProSAFE Single Band 802.11n Wireless Access Point WN203 Configure and Enable Security Profiles 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: • If you are using access point mode (which is the default mode if you did not enable wireless bridging), all options are available. In other modes such as bridge mode, some options might be unavailable. Not all wireless adapters support WPA or WPA2. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions about how to configure WPA or WPA2 settings. WARNING: If you use a wireless computer to configure wireless security settings, you are disconnected when you click the Apply button.

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 and enable a security profile: 1. Select Configuration > Security > Profile Settings. The Profile Settings screen displays eight wireless security profiles. (If the radio is disabled, the Enable column is masked out.) *Wireless Configuration and Security 36 ProSAFE Single Band 802.11n Wireless Access Point WN203* The following table explains the fields of the Profile Settings screen: Setting Profile Name Description The unique name of the wireless security profile that makes it easy to recognize the profile. The wireless network name (SSID) for the wireless security profile. The configured wireless authentication method for the wireless security profile. The default VLAN ID that is associated with the wireless security profile.

The check box that lets you select the wireless security profile so you can enable it by clicking the Apply button. SSID Security VLAN Enable 2. Select the radio button to the left of the wireless security profile that you want to configure, and click the Edit button. The Edit Security Profile screen displays for the selected wireless security profile (see the following figure). The screen has two sections: •• Profile Definition (see Step 3) Authentication Settings (see Step 4) *Wireless Configuration and Security 37 ProSAFE Single Band 802.11n Wireless Access Point WN203* 3. Specify the settings of the Profile Definition section of the Edit Security Profile screen as described in the following table: Setting Profile Name Description Enter a unique name of the wireless security profile that makes it easy to recognize the profile. The default names are NETGEAR, NETGEAR-1, NETGEAR-2, and so on, through NETGEAR-7. You can enter a value of up to 32 alphanumeric characters.



[You're reading an excerpt. Click here to read official NETGEAR WN203 user guide](http://yourpdfguides.com/dref/5435532)
<http://yourpdfguides.com/dref/5435532>

The wireless network name (SSID) for the wireless security profile.

The default names are NETGEAR_11ng, NETGEAR_11ng-1, NETGEAR_11ng-2, and so on, through NETGEAR_11ng-7 for the eighth profile. Select the Yes radio button to enable the wireless access point to broadcast its SSID, allowing wireless clients that have a null (blank) SSID to adopt the wireless access point's SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button. SSID Broadcast Wireless Network Name (SSID)

4.

Specify the settings of the Authentication Settings section of the Edit Security Profile screen as described in the following table. Setting Network Authentication and Data Encryption Note: The data encryption fields that display onscreen depend on your selection from the Network Authentication drop-down menu. Description Open System This is the default setting. Use an open system without any encryption or with WEP encryption. For more information, see Configure an Open System with WEP or Shared Key with WEP on page 40.

Use WEP encryption and enter at least one shared key. For more information, see Configure an Open System with WEP or Shared Key with WEP on page 40. Configure the RADIUS server settings. Encryption is not supported. For more information, see Configure Legacy 802.1X on page 42. Configure the RADIUS server settings and select TKIP or TKIP + AES encryption. For more information, see Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 42. Shared Key Legacy 802.1X WPA with Radius WPA2 with Radius Configure the RADIUS server settings and select AES or TKIP + AES encryption.

For more information, see Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 42. Note: Select this setting only if all clients support WPA2. Wireless Configuration and Security 38 ProSAFE Single Band 802.11n Wireless Access Point WN203 Setting Network Authentication and Data Encryption (continued) Description WPA & WPA2 with Configure the RADIUS server setting. TKIP + AES Radius encryption is the default encryption. For more information, see Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 42. Note: This setting allows clients to connect through either WPA with TKIP or WPA2 with AES. WPA-PSK Enter a WPA passphrase and select TKIP or TKIP + AES encryption. For more information, see Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 43. Enter a WPA passphrase and select AES or TKIP + AES encryption.

For more information, see Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 43. Note: Select this setting only if all clients support WPA2. WPA-PSK & WPA2-PSK Enter a WPA passphrase. TKIP + AES encryption is the default encryption. For more information, see Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 43.

Note: This setting allows clients to connect through either WPA with TKIP or WPA2 with AES. WPA2-PSK Wireless Client Security Separation If you enable wireless client security separation by selecting Enable from the drop-down menu, the associated wireless clients cannot communicate with each other. By default, Disable is selected from the drop-down menu. This feature is intended for hotspots and other public access situations. From the drop-down menu, select how VLANs operate by making one of the following selections: • Disable.

Disables dynamic VLANs, and enables static VLANs. This is the default setting. • Optional. Enables dynamic VLANs, but if a RADIUS server does not return a VLAN ID, the wireless client is still allowed to connect to the wireless access point. • Required. Enables dynamic VLANs. If a RADIUS server does not return a VLAN ID, the wireless client is not authenticated and cannot connect to the wireless access point. For dynamic VLANs to operate (that is, the selection is Optional or Required), the following is required: • The hubs and switches on your LAN need to support the VLAN (802.1Q) standard. • The authentication is set to any RADIUS type authentication: either the network authentication in the wireless security profile or the remote MAC address database authentication for the MAC Authentication feature can be used.

Dynamic VLAN Wireless Configuration and Security 39 ProSAFE Single Band 802.11n Wireless Access Point WN203 Setting VLAN ID Description Enter the VLAN ID to be associated with this wireless security profile. The default VLAN ID is 1. The VLAN ID needs to match the VLAN ID that is used by the other devices in your network. Access control functions only when static VLANs are enabled, that is, you select Disable from the Dynamic VLAN drop-down menu. The Access Control radio buttons let you enable or disable access control through a RADIUS server for the wireless security the profile: • Disable. Access control is disabled. This is the default setting. • Enable. Access control is enabled, and wireless clients are authenticated through a RADIUS server.

Either the network authentication in the wireless security profile or the remote MAC address database authentication for the MAC Authentication feature needs to be enabled. Note: You can use access control even when you do not configure WPA with RADIUS or WPA2 with RADIUS. Access Control Access Control Policy Access control policy functions only when static VLANs are enabled, that is, you select Disable from the Dynamic VLAN drop-down menu and you select the Enable Access Control radio button. The Access Control Policy radio buttons let you enable or disable the access control policy for wireless clients: • Disable. If a RADIUS server does not return a (static) VLAN ID, the wireless client is still allowed to connect to the wireless access point. This is the default setting. • Enable. If a RADIUS server does not return a (static) VLAN ID, the wireless client is not authenticated and cannot connect to the wireless access point. 5. Click the Apply button.

Configure an Open System with WEP or Shared Key with WEP Whether you use an open system with WEP or shared key with WEP, configure the settings that are explained in Table 2 on page 41. • Open system with WEP An open system can function without any encryption or with pre-shared WEP key encryption without RADIUS authentication. The security level of static WEP is not very strong. When you select Open System from the Network Authentication drop-down menu and any selection other than None from the Data Encryption drop-down menu, the screen expands to display the WEP fields: Wireless Configuration and Security 40 ProSAFE Single Band 802.11n Wireless Access Point WN203 Figure 7. Open system with WEP • Shared key with WEP Shared key provides pre-shared WEP key encryption without RADIUS authentication. The security level of static WEP is not very strong. When you select Shared Key from the Network Authentication drop-down menu, the screen expands to display the WEP fields: Figure 8. Shared key with WEP Table 2.



[You're reading an excerpt. Click here to read official NETGEAR WN203 user guide](http://yourpdfguides.com/dref/5435532)
<http://yourpdfguides.com/dref/5435532>