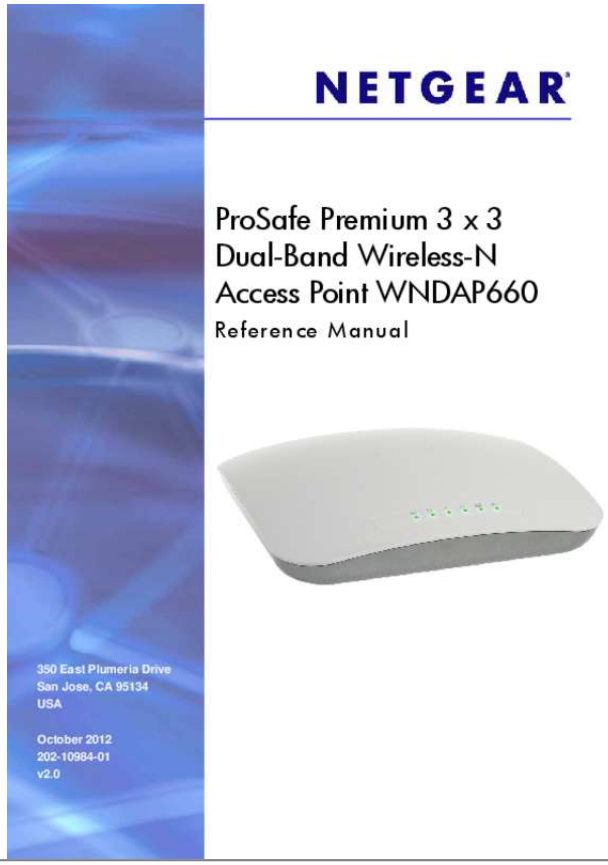

***Manual abstract:***

*@@NETGEAR recommends that you use only the official NETGEAR support resources. 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. Other brand and product names are registered trademarks or trademarks of their respective holders. 71 Restore the Wireless Access Point to the Factory Default Settings . 71 Reboot the Wireless Access Point without Restoring the Default Configuration . 123 Configure the Wireless Access Point to Repeat the Wireless Signal Using Point-to-Multipoint Bridge Mode . 134 You Cannot Access the Internet or the LAN from a Wireless-Capable Computer . 135 You Cannot Configure the Wireless Access Point from a Browser .*

*137 Test the Path from Your Computer to a Remote Device . Introduction 1 This chapter introduces the NETGEARÂ® ProSafeÂ® Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 and describes some of the key features. The chapter includes the following sections: â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ About the ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 What Is in the Box? System Requirements Key Features and Standards Hardware Description Register the Wireless Access Point Note: For more information about the topics covered in this manual, visit the Support website at http://support. Note: Firmware updates with new features and bug fixes are made available from time to time at downloadcenter. 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. About the ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 The ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660, going forward in this manual referred to as the wireless access point, is a powerful building block of a wireless LAN infrastructure. 11a/n connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Support for three 6 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 transmit radio chains and three receive radio chains, also referred to as 3x3 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 coverageâ□□interacting with a wireless network interface card (NIC) through an antenna.*

*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 128 clients in a range of several hundred feet. The throughput is shared between all clients. Make sure that you install a sufficient number of wireless access points to meet the required coverage, throughput, and quality of your wireless network. 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 450 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference. Advanced wireless features that are supported on the wireless access point include a wireless intrusion detection system (IDS), wireless intrusion prevention system (IPS), configurable wireless QoS policies, and band steering.*

*You can manage the wireless access point from either an IPv4 or IPv6 address, and the wireless access point can allocate either IPv4 or IPv6 DHCP addresses to its wireless clients. What Is in the Box? The product package contains the following items: â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Power adapter and cord (12 VCD, 1. 5A) Straight-through Category 5 Ethernet cable Installation guide Resource CD, which includes this manual Wall-mount kit made up of brackets and hardware Contact your reseller or customer support in your area if there are any missing or damaged parts. 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 Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 System Requirements Before installing the wireless access point, make sure that your system meets these requirements: â□¢ â□¢ â□¢ â□¢ â□¢ A 10/100/1000 Mbps local area network device such as a hub or switch The Category 5 UTP straight-through Ethernet cable with RJ-45 connector included in the package, or one like it A 100â□□120V, 50â□□60 Hz AC power source A computer with the TCP/IP protocol installed and a web browser for configuration, such as Microsoft Internet Explorer 6. 11a/n Standardsâ□□Based Wireless Networking Autosensing Ethernet Connections with Auto Uplink The wireless access point is easy to use and provides solid wireless and networking support. The wireless access point complies with the IEEE 802. 11a/b/g standards for wireless LANs and is Wi-Fi certified for 802.*

*The wireless access point provides WPA and WPA2 enterprise-class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. The WPA-PSK and WPA2-PSK pre-shared key authentication does not have the overhead of RADIUS servers but provides the strong security of WPA. When a wireless access point is connected to a wired network and a set of wireless stations, it is called a basic service set (BSS). The basic service set identifier (BSSID) is a unique identifier attached to the header of packets sent over a WLAN that differentiates one WLAN from another when a mobile device tries to connect to the network. The multiple BSSID feature allows you to configure up to 16 SSIDs (8 per radio) on your wireless access point and assign different configuration settings to each SSID.*

*All the configured SSIDs are active, and the network devices can connect to the wireless access point by using any of these SSIDs. â□¢ Introduction 8 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 â□¢ DHCP server and client.*

*The DHCP server of the wireless access point can provide a dynamic IPv4 or IPv6 address to wireless clients. The wireless access point can also act as a client and obtain an IPv4 or IPv6 address from a DHCP server on the LAN. sNMP.*

*The wireless access point supports Simple Network Management Protocol (SNMP) for Management Information Base (MIB) management. A network of computers can behave as if they are connected to the same network even though they might actually be physically on different segments of a LAN. Virtual LANs (VLANs) are configured through software rather than hardware, which makes them very flexible. VLANs are very useful for user and host management, bandwidth allocation, and resource optimization. â□¢ â□¢ â□¢ Key Features The wireless access point provides solid functionality , including the following features: â□¢ â□¢ Dual band. The wireless access point can operate concurrently in the 2. Band steering can ensure that a dual-band wireless station operates in the 5 GHz band rather than in the 2. 4 GHz band, which is often highly congested. Band steering can also move a wireless station that already operates in the 2. 4 GHz band to the 5 GHz band.*

*Band steering is an advanced wireless feature that reduces the client density in the 2. The wireless access point is manageable from either an IPv4 or IPv6 address, it can function as an IPv4 or IPv6 DHCP client, and its DHCP server can allocate either IPv4 or IPv6 addresses. In this mode, the wireless access point communicates only with another bridge-mode wireless station or wireless access point. Network authentication should be used to protect this communication. point-to-multipoint bridge. Select this option only if this wireless access point is the master for a group of bridge-mode wireless stations. The other bridge-mode wireless stations send all traffic to this master and do not communicate directly with each other. Network authentication should be used to protect this traffic. repeater. In this mode, the wireless access point 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.*

*Network authentication should be used to protect this communication. 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. introduction 9 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 â□¢ 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: The QoS settings let you prioritize traffic, such as voice and video traffic, so that packets do not get dropped. The QoS policies let you configure classifications (match clauses) and apply traffic to eight priority queues based on IP precedence, DSCP, MAC address, IP address, and other information that might be present in Layer 2 and Layer 3 packet headers. â□¢ Wireless IDS/IPS. The wireless intrusion detection system (IDS) and intrusion prevention system (IPS) can detect and prevent a variety of wireless attacks. attacks are covered by preconfigured policy rules.*

*When an attack occurs, the wireless access point can notify a network administrator though an email. hotspot support. You can allow all HTTP (TCP, port 80) requests to be captured and redirected to the URL you specify. rogue AP and ad hoc network detection. Rogue AP filtering and ad hoc network detection ensure that unknown APs and networks are not given access to any part of the secured wireless and wired LAN. access control. MAC address filtering can ensure that only trusted wireless stations 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. secure Telnet command-line interface. The secure Telnet command-line interface (CLI) enables direct secure access over the serial port and easy scripting of configuration of multiple wireless access points across an extensive network through the Ethernet interface. You can upgrade it easily, using only your web browser, and you can upgrade it remotely. You can also use the command-line interface. 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 one or two Ethernet ports. The wireless access point can receive all required power on one Ethernet port from a single PoE source.*

*However, with two Ethernet ports and two PoE sources, power redundancy ensures that if one Ethernet port is down, the other Ethernet port can still supply all power to the wireless access point for continued operation. Power/Test, Active, LAN, and WLAN for each radio mode are easily identified. â□¢ â□¢ â□¢ â□¢o the Internet, you have the option to register your product. At any time, you can register your product from the web management interface, or you can go to the NETGEAR website for registration at https://my. ÏØØ To register the wireless access point with NETGEAR: 1.*

*A new screen displays in your browser: Figure 5. 3. Enter the information in the blank fields. The serial number, model number, and date of purchase are entered automatically. 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. 11a/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: â□¢ â□¢ â□¢ â□¢ What You Need Before You Begin Install and Configure the Wireless Access Point Test Basic Wireless Connectivity Mount the Wireless Access Point What You Need Before You Begin â□¢ â□¢ â□¢ â□¢ â□¢ â□¢ Wireless Equipment Placement and Range Guidelines Ethernet Cabling Requirements LAN Configuration Requirements Hardware Requirements for Computers on Your LAN Operating Frequency (Channel) Guidelines Requirements for Entering IP Addresses You need to consider the following guidelines and requirements before you can set up your wireless access point.*

*see also System Requirements on page 8. 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. 17 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 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.*

*Note: Before you position and mount the wireless access point at its permanent position, first configure the wireless access point and test the computers on your LAN for wireless connectivity as explained in this chapter. For best results, place your wireless access point according to the following general guidelines: â□¢ â□¢ â□¢ â□¢ â□¢ 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). (An external antenna does not come standard with the wireless access point. ) 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). Â□¢ 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 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. Installation and Basic Configuration 18 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Hardware Requirements for Computers on Your LAN To connect to the wireless access point on your network, each computer needs to have an 802. NETGEAR recommends using the wireless access point with computers that have the NETGEAR N600 Wireless Dual Band USB Adapter (WNDA3100) installed. 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: â□¢ 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 use 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 5 channels (for example, use channels 1 and 6, or 6 and 11). In infrastructure mode (which is the default mode for the wireless access point), 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 is possible only if the wireless access points use the same SSID. Â□¢ â□¢ Requirements for Entering IP Addresses IPv4 The fourth octet of an IP address needs to be between 0 and 255 (both inclusive). This requirement applies to any IP address that you enter on a screen of the web management interface. IPv6 IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeroes within an IPv6 address can be reduced to a single zero or altogether omitted. The following errors invalidate an IPv6 address: â□¢ â□¢ â□¢ More than eight groups of hexadecimal quartets More than four hexadecimal characters in a quartet More than two colons in a row Installation and Basic Configuration 19 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Install and Configure the Wireless Access Point Install and configure your wireless access point in the order of the following sections: 1. 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 and 802.*

*11a/n wireless adapters are able to communicate with the Ethernet network. For this to work correctly, verify that you have met all the system requirements, shown in System Requirements on page 8. 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. ï□□ To set up the wireless access point: 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. Configure the computer with a static IP address of 192. Connect an Ethernet cable from the wireless access point to the computer (point A in the following figure).*

*4. Securely insert the other end of the cable into the wireless access pointâ□□s Ethernet port (point B in the following figure). Turn on your computer. 6. Connect the power adapter to the wireless access point.*

*tip: The wireless access point supports Power over Ethernet (PoE) with power redundancy. Both Ethernet ports can provide power. 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. The Power/Test LED blinks when the wireless access point is first turned on.*

*(To be exact, during startup, the LED is first steady amber, then goes off, and then blinks green. ) After about 45 seconds, the LED should stay lit (steady green). If after 1 minute the Power/Test LED is not lit or is still blinking, check the connections and see if the power outlet is controlled by a wall switch that is turned off. active LED. The Active LED is lit or blinks green when there is Ethernet traffic. lAN 1 LED. The LAN LED indicates the LAN speed for LAN port 1: green for 1000 Mbps, amber for 100 Mbps, and no light for 10 Mbps. If the LAN LED is not lit, make sure that the Ethernet cable is securely attached at both ends. lAN 2 LED.*

*The LAN LED indicates the LAN speed for LAN port 2: green for 1000 Mbps, amber for 100 Mbps, and no light for 10 Mbps.*

*If the LAN LED is not lit, make sure that the Ethernet cable is securely attached at both ends. 4 GHz WLAN LED is lit or blinks green when the wireless LAN (WLAN) is ready. wLAN LED. The 5 GHz WLAN LED is lit or blinks green 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. By default, the DHCP client on the wireless access point is disabled so you can log in using the default IP address. Connect to the wireless access point by entering its default address of 192. 100 into your browser (use http and not https). Enter the default user name of admin and the default password of password. The web browser displays the basic General system settings screen under the Configuration tab of the main menu as shown in Figure 11 on page 23.*

*Web Management Interface 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. installation and Basic Configuration 22 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Figure 9. The bottom right corner of all screens that allow you to make configuration changes show the Apply and Cancel buttons, and on several screens the Edit button. figure 10.*

*These buttons have the following functions: â□¢ â□¢ â□¢ Edit. Allows you to edit the existing configuration. cancel. Cancels all configuration changes that you made on the screen. apply.*

*Saves and applies all configuration changes that you made on the screen. Configure Basic General System Settings and Time Settings Note: After you have successfully logged in to the wireless access point, the basic General system settings screen displays. Configure the settings as explained in the following table: Table 2. basic general system settings Setting Access Point Name Description This unique name is the wireless access point NetBIOS name. The name is printed on the rear label of the wireless access point. The default is netgearxxxxxx, in which xxxxxx represents the last 6 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 list, 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 those identified in this field.*

*Configure the settings as explained in the following table: Table 3. Time system settings Setting Time Zone Current Time Description Select the time zone to match your location. This is a nonconfigurable field that displays the current date and time. installation and Basic Configuration 24 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Table 3. Time system settings (continued) Setting NTP Client Description 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. Note: If you use a host name, make sure that you have configured a DNS server. For more information, see the next section. Configure the IPv4 Settings Note: For information about how to configure the IPv6 settings, see Configure the IPv6 Settings on page 99. WARNING: If you enable the DHCP client, the IP address of the wireless access point changes when you click Apply, 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.*

*Configure the IPv4 settings as explained in the following table: Table 4. iPv4 settings 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 check box, 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. Enter the IP address of your wireless access point. The default IP address is 192.*

*To change the address, enter an unused IP address from the address range used on your LAN, or enable DHCP the server. Enter the network number portion of an IP address. Unless you are implementing subnetting, enter 255. Enter the IP address of the ISP gateway to which the wireless access point connects. Enter the IP address of the primary and secondary DNS servers. A DNS server is a host on the Internet that translates Internet names (such as www. 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 an address, you need to obtain it from the ISP and enter it manually in this field. Select this check box to validate that the upstream link is active before allowing wireless associations. Installation and Basic Configuration 26 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Configure the Optional DHCPv4 Server The wireless access point provides a built-in DHCPv4 server for wireless clients only, which can be especially useful in small networks.*

*When the DHCP server is enabled, the wireless access point provides preconfigured TCP/IP configurations to all connected wireless stations. Note: For information about how to configure the DHCPv6 server, see Configure the Optional DHCPv6 Server on page 101. The following figure displays the DHCPv4 server settings only. For information about the DHCPv6 server settings, see Configure the Optional DHCPv6 Server on page 101. Configure the settings as explained in the following table: Table 5. DHCP server settings for IPv4 Setting Description Select the DHCPv4 Server check box to enable the DHCP server. Use the default settings or specify the pool of IPv4 addresses to be assigned by setting the starting IPv4 address and ending IPv4 address. These addresses should be part of the same IPv4 address subnet as the wireless access pointâ□□s LAN IPv4 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 IPv4 addresses to be assigned to DHCP clients. The default address is 192. DHCP server settings for IPv4 (continued) Setting Ending IPv4 Address Description Enter the last address in the range of IPv4 addresses to be assigned to DHCP clients.*

*The default address is 192.*
*Enter the subnet mask to be used by DHCP clients. Enter the IPv4 address of the default routing gateway to be used by DHCP clients. The default address is 192. Enter the IP address of the primary Domain Name System (DNS) server available to DHCP clients. Subnet Mask Gateway IPv4 Address Primary DNS Address Secondary DNS Address Enter the IP address of the secondary DNS server available to DHCP clients.*
*Primary WINS Server Enter the IP address of the primary WINS server for the network, if there is any. 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 one day. Configure the Basic Wireless Settings For proper compliance and compatibility between similar products in your coverage area, you need to configure the 802. 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. 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 lose your wireless connection when you click Apply. You then need to change the wireless settings of your computer to match the wireless access pointâ□□s new settings. (The following figure shows the 11ng settings.*

*) Installation and Basic Configuration 28 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Note: The radio wave icon ( (b , bg , or ng). ) displays next to the enabled wireless mode Figure 15. 2. Specify the wireless mode in the 2. 11g-compliant devices can connect to the access point because they are backward compatible. 11n-compliant devices can 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 lists onscreen are masked out. 3. Turn on the radio by selecting the Turn Radio On check box. a pop-up screen displays.*
*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. The change does not take effect until you click the Apply button after you have completed the wireless configuration. installation and Basic Configuration 29 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 5. Specify the remaining wireless settings as explained the following table: Table 6.*
*basic 2. 4 GHz band wireless settings Setting Wireless Network Name (SSID) Descriptions Enter a 32-character (maximum) service set identifier (SSID); the characters are case-sensitive. the default is NETGEAR_11ng. The SSID assigned to a wireless device needs to match the wireless access pointâ□□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. 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 61. Select the Yes radio button to enable the wireless access point to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access pointâ□□s SSID. Yes is the default setting.*

*To prevent the SSID from being broadcast, select the No radio button. From the drop-down list, 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: It should not be necessary to change the wireless channel unless you experience interference (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see Operating Frequency (Channel) Guidelines on page 19. Note: For more information about available channels and frequencies, see Technical Specifications on page 140. 11ng mode only Note: For most networks, the default settings work fine. MCS Index / Data From the drop-down list, select a Modulation and Coding Rate 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 from in 11ng mode, see Factory Default Settings on page 143. channel Width From the drop-down list , 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 list, 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. 4 GHz band wireless settings (continued) Setting 11b and 11bg modes only Descriptions Data Rate From the drop-down list, select the transmit data rate of the wireless network.*
*the default setting is Best. For a list of all options that you can select from in 11b mode and 11bg mode, see Factory Default Settings on page 143. Output Power From the drop-down list, 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 Apply to save your settings and enable the selected wireless mode. Note: For information about how to configure advanced wireless settings, see Configure Advanced Wireless Settings on page 107. (The following figure shows the 802.*

*) displays next to the selected radio mode Installation and Basic Configuration 31 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Figure 16. 2. Specify the wireless mode in the 5 GHz band by selecting one of the following radio buttons: â□¢ 11a. 802. 11n-compliant devices can connect to the access point because they are backward compatible. â□¢ 11na. This is the default setting. 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 lists onscreen are masked out. 3. Turn on the radio by selecting the Turn Radio On check box. a pop-up screen displays. 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. The change does not take effect until you click the Apply button after you have completed the wireless configuration.*

*installation and Basic Configuration 32 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 5. Specify the remaining wireless settings as explained the following table: Table 7. Basic 5 GHz band wireless settings Setting Wireless Network Name (SSID) Descriptions Enter a 32-character (maximum) service set identifier (SSID); the characters are case-sensitive. the default is NETGEAR_11na. The SSID assigned to a wireless device needs to match the wireless access pointâ□□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. This is a nonconfigurable field that shows the status of the wireless scheduler. For more information, see Schedule the Wireless Radios to Be Turned Off on page 61. Select the Yes radio button to enable the wireless access point to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access pointâ□□s SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button. From the drop-down list, select the channel you wish to use on your wireless LAN. The wireless channels and frequencies depend on the country and wireless mode. the default setting is Auto. Note: It should not be necessary to change the wireless channel unless you experience interference (indicated by lost connections or slow data transfers).*

*If this happens, you might want to experiment with different channels to see which is the best. For more information, see the guidelines following this table. Note: For more information about available channels and frequencies, see Technical Specifications on page 140. 11na mode only Note: For most networks, the default settings work fine. MCS Index / Data From the drop-down list, select a Modulation and Coding Rate 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 from in 11na mode, see Factory Default Settings on page 143. channel Width From the drop-down list , select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, and 40 MHz. the default is Dynamic 20/40 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 list, 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. wireless On-Off Status Broadcast Wireless Network Name (SSID) Channel / Frequency Guard Interval Installation and Basic Configuration 33 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Table 7.*

*Basic 5 GHz band wireless settings (continued) Setting 11a mode only Descriptions Data Rate From the drop-down list, select the transmit data rate of the wireless network. the default setting is Best. For a list of all options that you can select from in 11a mode, see Factory Default Settings on page 143. Output Power From the drop-down list, 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 Apply to save your settings and enable the selected wireless mode. Note: For information about how to configure advanced wireless settings, see Configure Advanced Wireless Settings on page 107. Test Basic Wireless Connectivity After you have configured the wireless access point as explained in the previous sections, test the computers on your LAN for wireless connectivity before you position and mount the wireless access point at its permanent position. 11a/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.*

*5 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 6, Troubleshooting. Installation and Basic Configuration 34 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 NETGEAR recommends that you complete the following tasks before you deploy the wireless access point in your network: â□¢ â□¢ Configure wireless security and other wireless features as described in Chapter 3, Wireless Configuration and Security. Configure any additional features that you might need as described in Chapter 4, Management and Monitoring, 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. Mount the Wireless Access Point â□¢ â□¢ â□¢ Ceiling Installation Wall Installation Desk Installation Note: NETGEAR recommends that you review the information in Wireless Equipment Placement and Range Guidelines on page 17 before you mount the wireless access point at its permanent position. Note: The figures in the procedures in this section do not show the WNDAP660 wireless access point. However, the procedures are generic and do apply to the WNDAP660 wireless access point. Ceiling Installation The best location for ceiling installation is at the center of your wireless coverage area, and within line of sight of all mobile devices. Make sure the top (the dome side) of the wireless access point is directed toward the users and not the ceiling.*

*Installation and Basic Configuration 35 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Note: Do not place the wireless access point in a false ceiling space facing up. Ï□□ To install the wireless access point using the ceiling installation kit: 1. Verify the package contents of the ceiling installation kit. mounting plate Clamp with screws 2. Detach the mounting plate from the wireless access point.*

*3. Attach the clamp to the ceiling rail. installation and Basic Configuration 36 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 4. Attach the mounting plate to the clamp. 5.*

*Connect the cables to the wireless access point. 6. Attach the wireless access point to the mounting plate.*

*installation and Basic Configuration 37 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 7. Attach the cover to the wireless access point. Wall Installation The best location for wall installation is at the center of your wireless coverage area, and within line of sight of all mobile devices. Make sure the top (the dome side) of the wireless access point is directed toward the users and not the wall. ï To install the wireless access point using the wall installation kit: 1. Verify the package contents of the wall installation kit. installation and Basic Configuration 38 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Screws and wall supports Mounting plate 2.*

*Detach the mounting plate from the wireless access point. 3. Attach the mounting plate to the wall. 4. Connect the cables to the wireless access point. installation and Basic Configuration 39 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 5. Attach the wireless access point to the mounting plate. 6. Attach the cover to the wireless access point. Installation and Basic Configuration 40 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Desk Installation ï To install the wireless access point on a desk: Attach the rubber feet to the holes in the bottom of the wireless access point.*

*rubber feet Installation and Basic Configuration 41 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: â¢ â¢ â¢ â¢ â¢ 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 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, and configure the 802. 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 pointâs SSID, channel, or wireless security settings, you lose your wireless connection when you click Apply. You then need to change the wireless settings of your computer to match the wireless access pointâs new settings. 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. 42 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 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. figure 17. 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 (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 48. 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 60. 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 48. 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 Configure and Enable Security Profiles on page 48 and Configure an Open System with WEP or Shared Key with WEP on page 53. For information about how to configure Legacy 802.*

*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 Configure and Enable Security Profiles on page 48 and Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 55. WPA-PSK uses a pre-shared key (PSK) for authentication; for more information, see Configure and Enable Security Profiles on page 48 and Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 56.*

*â¢ 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 Configure and Enable Security Profiles on page 48 and Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 55.*

*WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see Configure and Enable Security Profiles on page 48 and Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 56. â¢ 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 Configure and Enable Security Profiles on page 48 and Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 55. WPA-PSK & WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see Configure and Enable Security Profiles on page 48 and Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 56.*

*Security Profiles â□¢ â□¢ Before You Change the SSID, WEP, and WPA Settings Configure and Enable Security Profiles 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 48). Wireless Configuration and Security 44 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 To set up a security profile, 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 that 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 about how to configure WPA2 settings. For information about the types of network authentication that the wireless access point supports, see Configure and Enable Security Profiles on page 48. Â□¢ Data encryption Select the data encryption that you want to use. The available options depend on the network authentication setting described earlier (otherwise, the default is None). The data encryption settings are explained in Configure and Enable Security Profiles on page 48. 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 48. VLAN ID If this feature is 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 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 48. Â□¢ â□¢ Some concepts and guidelines regarding the SSID are explained in the following list: â□¢ A basic service set (BSS) is a group of wireless stations and a single wireless access point, all using 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) is a group of wireless stations and multiple wireless access points, all using 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 stations to connect wirelessly when they physically move from one BSS to another one within the same ESS. The wireless station automatically changes to the wireless access point with the least interference or best performance. Â□¢ â□¢ â□¢ Wireless Configuration and Security 45 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Before You Change the SSID, WEP and WPA Settings , For a new wireless network, print or copy the following forms and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the country or region correctly as the first step. form for 802. 11b/bg/ng Modes Print this page and store the security information in a safe place: â□¢ 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. Â□¢ 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. Â□¢ WPA-PSK (pre-shared key) and WPA2-PSK Record the WPA-PSK passphrase: WPA-PSK passphrase: _____ Record the WPA2-PSK passphrase: WPA2-PSK passphrase: _____ â□¢ WPA RADIUS settings For WPA, record the following settings for the primary and secondary RADIUS servers: Server name/IP address: Primary _____ Secondary _____ Port: _____ Shared secret: _____ â□¢ 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: _____ ----------End of Form---------- Wireless Configuration and Security 46 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Form for 802. 11a/an Modes Print this page and store the security information in a safe place: â□¢ 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. Â□¢ 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. Â□¢ WPA-PSK (pre-shared key) and WPA2-PSK Record the WPA-PSK passphrase: WPA-PSK passphrase: _____ Record the WPA2-PSK passphrase: WPA2-PSK passphrase: _____ â□¢ WPA RADIUS settings For WPA, record the following settings for the primary and secondary RADIUS servers: Server name/IP address: Primary _____ Secondary _____ Port: _____ Shared secret: _____ â□¢ 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: _____ ----------End of Form---------- Wireless Configuration and Security 47 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Configure and Enable Security Profiles To configure and enable a security profile, you need to enable the associated radio: â□¢ â□¢ For 802.*

*11a/na modes, the 5 GHz radio needs to be enabled. Both radios can function concurrently. The Profile Settings screen for the 802. 11b/bg/ng modes displays, showing eight wireless security profiles. Optional: To display the Profile Settings screen for the 802.*
*This screen also shows eight wireless security profiles. (If the 5 GHz radio is disabled, the Enable column is masked out. ) Wireless Configuration and Security 48 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Figure 19. The following table explains the fields of the Profile Settings screen: Table 8. Profile settings 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 Apply. sSID Security VLAN Enable 3.*

*To configure a wireless security profile, select the corresponding radio button to the left of the wireless security profile. The Edit Security Profile screen opens for the selected wireless security profile (see the following figure). The screen has three sections: â□¢ Profile Definition (see Step 4) â□¢ â□¢ Authentication Settings (see Step 5) QoS Policies (see Step 6) Wireless Configuration and Security 49 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Figure 20. 4. Specify the settings of the Profile Definition section of the Edit Security Profile screen as explained in the following table: Table 9. Profile definition settings 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. The wireless network name (SSID) for the wireless security profile. The default names depend on the selected radio band: â□¢ 802.*
*11b/bg/ng. The default names are NETGEAR_11ng, NETGEAR_11ng-1, NETGEAR_11ng-2, and so on, through NETGEAR_11ng-7 for the eighth profile. The default names are NETGEAR_11na, NETGEAR_11na-1, NETGEAR_11na-2, and so on, through NETGEAR_11na-7 for the eighth profile. wireless Network Name (SSID) Wireless Configuration and Security 50 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Table 9. Profile definition settings (continued) Setting Broadcast Wireless Network Name (SSID) Description Select the Yes radio button to enable the wireless access point to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access pointâ□□s SSID.*
*Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button. 5. Specify the settings of the Authentication Settings section of the Edit Security Profile screen as explained in the following table. 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□¢ If you are using access point mode (which is the default mode if you did not enable wireless bridging), then all options are available. In other modes such as bridge mode, some options might 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 about how to configure WPA2 settings. â□¢ Table 10. Profile authentication settings Setting Network Authentication and Data Encryption Note: The data encryption fields that display onscreen depend on your selection from the Network Authentication drop-down list. description Open System This is the default setting. Use an open system without any encryption or with WEP encryption.*

*See Configure an Open System with WEP or Shared Key with WEP on page 53. Use WEP encryption and enter at least one shared key. See Configure an Open System with WEP or Shared Key with WEP on page 53. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 55. shared Key Legacy 802. 1X WPA with Radius WPA2 with Radius Configure the RADIUS server settings and select AES or TKIP + AES encryption. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 55. Note: Select this setting only if all clients support WPA2. wireless Configuration and Security 51 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 Table 10. Profile authentication settings (continued) Setting Network Authentication and Data Encryption (continued) Description WPA & WPA2 with Configure the RADIUS server setting. tKIP + AES Radius encryption is the default encryption. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS on page 55. Note: This setting allows clients to connect through either WPA with TKIP or WPA2 with AES. Note: Select this setting only if all clients support WPA2. Note: This setting allows clients to connect through either WPA with TKIP or WPA2 with AES.*
*Wireless Client Security Separation If you enable wireless client security separation by selecting Enable from the drop-down list, the associated wireless clients cannot communicate with each other. by default , Disable is selected from the drop-down list. This feature is intended for hotspots and other public access situations. 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. wPA2-PSK VLAN ID 6. Optional: In the QoS Policies section of the screen, select a QoS policy from the Incoming drop-down list, Outgoing drop-down list, or both. Depending on your selection, the policy is applied to incoming packets, outgoing packets, or both incoming and outgoing packets, and is displayed in the Policy Details fields. Note: To be able to select a QoS policy, you first need to have configured one or more policies (see Configure Quality of Service Policies on page 113). Wireless Configuration and Security 52 ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP660 WARNING: If you use a wireless computer to configure wireless security settings, you are 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. Ï□□ To change the QoS policy selection on the Edit Security Profile screen: 1. From the drop-down list from which you want select another QoS policy, select None.*