ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual

NETGEAR

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

202-10534-01
November 2009
v1.1

Manual abstract:

Support Information Phone: 1-888-NETGEAR, for US & Canada only. @@If your product does not contain a Resource CD, then see the Warranty and Customer Support Information card. Com Trademarks NETGEAR, the NETGEAR logo, ProSafe, Smart Wizard, and Auto Uplink are trademarks or registered trademarks of NETGEAR, Inc. microsoft , Windows , Windows NT and Vista are registered trademarks of Microsoft Corporation. Other brand and product names are registered trademarks or trademarks of their respective holders. Statement of Conditions In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein. Certificate of the Manufacturer/Importer It is hereby certified that the ProSafe Dual Band Wireless-NAccess Point WNDAP350 Reference Manual has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

The Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations. Voluntary Control Council for Interference (VCCI) Statement This equipment is in the Class B category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing ii v1. 1 , November 2009 Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas. When used near a radio or TV receiver, it may become the cause of radio interference. Read instructions for correct handling.

Regulatory Compliance Information This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority. NOTE: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product. Europe â EU Declaration of Conformity This device complies with the essential requirements of the R&TTE Directive 1999/5/EC.

The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC: EN60950-1: 2006 EN 50385: EN 300 328 V1. , declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. 1, November 2009 FCC Requirements for Operation in the United States FCC Information to User This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals. FCC Guidelines for Human Exposure This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 25 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. fCC Declaration Of Conformity We NETGEAR , Inc. ,350 east Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the model ProSafe Dual Band Wireless-N Access Point WNDAP350 complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: â¢ â¢ This device may not cause harmful interference, and This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: â¢ â¢ â¢ â¢ Reorient or relocate the receiving antenna Increase the separation between the equipment and the receiver Connect the equipment into an electrical outlet on a circuit different from that which the receiver is connected Consult the dealer or an experienced radio/TV technician for help. FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. For operation within 5. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. IMPORTANT NOTE: Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 25cm between the radiator & your body. v v1. 1, November 2009 This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

Industry Canada statements This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. IMPORTANT NOTE: Radiation Exposure Statement This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 25cm between the radiator & your body. This device has been designed to operate with an antenna having a maximum gain of 5 dBi Antenna having a higher gain is strictly prohibited per regulations of Industry Canada.
the required antenna impedance is 50 ohms. Caution: The device for the band 5150-5250 MHz is only for indoor usage to reduce potentail for harmful interference to cochannel mobile satellite systems. High power radars are allocated as primary users (meaning they have priority) of 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices. 4-10 Chapter 5 Troubleshooting and Debugging No lights are lit on the wireless access point. . 5-1 The Wireless LAN activity light does not light up. . 5-2 The LAN light is not lit. . 5-2 I cannot access the Internet or the LAN with a wireless capable computer.

. 5-2 I cannot connect to the WNDAP350 to configure it. . 5-3 When I enter a URL or IP address I get a timeout error. 1, November 2009 Contents About This Manual The ProSafeâ□¢ Dual Band Wireless-N Access Point WNDAP350 Reference Manual describes how to install, configure and troubleshoot the ProSafe Dual Band Wireless-N Access Point WNDAP350. The information in this manual is intended for readers with intermediate computer and Internet skills. Conventions, Formats, and Scope The conventions, formats, and scope of this manual are described in the following paragraphs: â□¢ Typographical Conventions. This manual uses the following typographical conventions: Italic Bold Fixed italic Emphasis, books, CDs, file and server names, extensions User input, IP addresses, GUI screen text Command prompt, CLI text, code URL links â□¢ Formats. This manual uses the following formats to highlight special messages: Note: This format is used to highlight information of importance or special interest. Tip: This format is used to highlight a procedure that will save time or resources.
Warning: Ignoring this type of note may result in a malfunction or damage to the equipment. Failure to take heed of this notice may result in personal injury or death. â□¢ Scope. This manual is written for the WNDAP350 wirelss access point according to these specifications: Product Version Manual Publication Date ProSafe Dual Band Wireless-N Access Point WNDAP350 November 2009 For more information about network, Internet, firewall, and VPN technologies, see the links to the NETGEAR website in Appendix B, â□□Related Documents. Â□□ Note: Product updates are available on the NETGEAR, Inc.
How to Print This Manual To print this manual, your computer must have the free Adobe Acrobat reader installed in order to view and print PDF files. The Acrobat reader is available on the Adobe Web site at http://www. Tip: If your printer supports printing two pages on a single sheet of paper, you can save paper and printer ink by selecting this feature. 1, November 2009 About This Manual Chapter 1 Introduction This chapter describes some of the key features of the ProSafe Dual Band Wireless-N Access Point WNDAP350. It also includes the minimum prerequisites for installation (â□□System Requirementsâ□□ on page 1-5.
) , package contents (â□□Whatâ□□s In the Box? Â□□ on page 1-6) and a description of the front and back panels of the WNDAP350 (â□□Hardware Descriptionâ□□ on page 1-6). About the ProSafe Dual Band Wireless-N Access Point WNDAP350 The ProSafe Dual Band Wireless-N Access Point WNDAP350is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radioequipped wireless notebook systems, desktop systems, print servers, and other devices. The WNDAP350 provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with a wireless network interface card (NIC) via an antenna. Typically, an individual in-building access point provides a maximum connectivity area of about a 500 foot radius. Consequently, the ProSafe Dual Band Wireless-N Access Point WNDAP350 can support a small group of users in a range of several hundred feet. Most access points can handle between 10 to 32 users simultaneously per radio. The WNDAP350 wirelss access point acts as a bridge between the wired LAN and wireless clients. Connecting multiple WNDAP350s via a wired Ethernet backbone can further lengthen the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another.

As a result, wireless clients can freely roam from one Access Point to another and still maintain seamless connection to the network. 1, November 2009 ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Supported Standards and Conventions The following standards and conventions are supported: â□¢ â□¢ Standards Compliance. The Wireless Access Point complies with the IEEE 802. WPA and WPA2 enterprise-class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. WPAPSK and WPA2-PSK preshared key authentication without the overhead of RADIUS servers but with all of the strong security of WPA. When a ve power (for battery powered equipment) and fine-tune power consumption. vLAN Security Profiles. Each Security Profile can be assigned a VLAN ID as each Security Profile is modified. It provides connectivity between Ethernet wired networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Additionally, the WNDAP350 supports the following wireless features: â□¢ Aggregation Support â□¢ Reduced Inter Frame Spacing support â□¢ Multiple Input, Multiple Output (MIMO) support â□¢ Distributed coordinated function (CSMA/CA, Back off procedure, ACK procedure, retransmission of unacknowledged frames) â□¢ RTS/CTS handshake â□¢ Beacon generation â□¢ Packet fragmentation and reassembly â□¢ Auto or long preamble â□¢ Roaming among access points on the same subnet Autosensing Ethernet Connections with Auto Uplink The WNDAP350 can connect to a standard Ethernet network.
The Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a â□□normalâ□□ connection such as to a computer or an â□□uplinkâ□□ connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates any concerns about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection. 1-4 v1. 1, November 2009 Introduction ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Compatible and Related NETGEAR Products For a list of compatible products from other manufacturers, see the Wireless Ethernet Compatibility Alliance Web site (WECA, see http://www.

The following NETGEAR products work with the WNDAP350 wirelss access point: â□¢ FS108P - ProSafe 8 Port 10/100 Switch with 4 Port PoE â□¢ FS116P ProSafe 16 Port 10/100 Desktop Switch with 8 Port PoE â□¢ FS726TP - ProSafe 24 Port 10/100 Smart Switch with 2 Gigabit Ports and 12 Port PoE â□¢ FS728TP - ProSafe 24+4 10/100 Smart Switch with full PoE â□¢ FS752TPS - ProSafe 48 Port 10/100 Stackable Smart Switch with 4 Gigabit Ports and 24 Port PoE â□¢ FSM7328PS - ProSafe 24-port 10/100 L3 Managed Stackable Switch with 24 PoE Ports â□¢ FSM7352PS â□¢ GS724TP â□¢ GS748TP â□¢ WNDA3100 - RangeMax Dual Band Wireless-N USB 2. 0 Adapter System Requirements Before installing the WNDAP350, make sure your system meets these requirements: â□¢ A 10/100/1000 Mbps Local Area Network device such as a hub or switch Introduction v1. 1, November 2009 1-5 ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual â□¢ â□¢ â□¢ â□¢ â□¢ The Category 5 UTP straight through Ethernet cable with RJ-45 connector included in the package, or one like it A 100-240 V, 50-60 Hz AC power source A Web browser for configuration such as Microsoft Internet Explorer 5. 0 or above , or Mozilla 3. 0 or above At least one computer with the TCP/IP protocol installed 802.

11a/n or 802. 11b/g/n-compliant devices, such as the NETGEAR WG511 Wireless Adapter Whatâ□□s In the Box? The product package should contain the following items: â□¢ ProSafe Dual Band Wireless-N Access Point WNDAP350 â□¢ Power adapter and cord (12 V dc, 1. 2 A) â□¢ Straight through Category 5 Ethernet cable â□¢ ProSafe Dual Band Wireless N Access Point WNDAP350 Installation Guide â□¢ Resource CD which includes a link to this manual. If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the firewall for repair. To qualify for product updates and product warranty registrations, we encourage you to register on the NETGEAR Web site at: http://www. Hardware Description This section describes the front and rear hardware functions of the WNDAP350. 1-6 v1. 1, November 2009 Introduction ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Front Panel The WNDAP350 front hardware functions are described below. 1 2 3 4 5 Figure 1-1 The following table explains the LED indicators: Table 1-1.

Indicates self test, loading software, or system fault (if continues). Note: This LED may blink for a minute before going off. The WNDAP350 provides two detachable dipole antennas. This socket connects to the WNDAP350 12V 1. Use the WNDAP350 Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or PoE switch. The restore to default button restores the WNDAP350 to the factory default settings. 1-8 v1. 1, November 2009 Introduction Chapter 2 Basic Installation and Configuration This chapter describes how to set up your ProSafe Dual Band Wireless-N Access Point WNDAP350for wireless connectivity to your LAN. This basic configuration will enable computers with 802. 11b/g/n or 802.

11a/n wireless adapters to do such things as connect to the Internet, or access printers and files on your LAN. 11a/na wireless networks at ranges of several hundred feet or more. This distance can allow for others outside your area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The WNDAP350 wirelss access point provides highly effective security features which are covered in detail in â□□Understanding Security Profilesâ□□ on page 2-23.

Deploy the security features appropriate to your needs. This chapter contains the following sections: 1. Â□□Restricting Wireless Access by MAC Address You need to prepare these three things before you can establish a connection through your wireless access point: â□¢ â□¢ â□¢ A location for the WNDAP350 that conforms to the â□□Wireless Equipment Placement and Range Guidelines below. The wireless access point connected to your LAN through a device such as a hub, switch, router, or Cable/DSL gateway. One or more computers with properly configured 802.

Wireless Equipment Placement and Range Guidelines The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices. Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the WNDAP350. For complete performance specifications, see Appendix A, â□□Default Settings and Technical Specifications. Â□□ For best results, place your wireless access point: â□¢ Near the center of the area in which your PCs will operate. Â□¢ In an elevated location such as a high shelf where the wirelessly connected PCs have line-ofsight access (even if through walls). The antenna provides better coverage above the access point. Place the access point so that it is either ceiling mounted or mounted on a wall facing the users. 2-2 v1. 1, November 2009 Basic Installation and Configuration ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual If you are using multiple access points for 11b/bg/ng, it is better if adjacent access points use different radio frequency channels to reduce interference.

The recommended Channel spacing between adjacent access points is 5 Channels (for example, use Channels 1 and 6, or 6 and 11). For 11a/na, the 6 Channel spacing is not needed. The time it takes to establish a wireless connection can vary depending on both your security settings and placement. Some types of security connections can take slightly longer to establish and can consume more battery power on a notebook computer. Understanding WNDAP350 Wireless Security Options Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WNDAP350 wirelss access point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs. Figure 2-1 There are several ways you can enhance the security of your wireless network: â□¢ Restrict Access Based on MAC address. You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WNDAP350.

MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

2-3 v1. 1, November 2009 Basic Installation and Configuration ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual â□¢ 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 â□□discoveryâ□□ feature of some products such as Windows XP, Vista and Unix systems but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.

WEP open authentication and WEP data encryption will block all but the most determined eavesdropper. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited. note: WEP and TKIP provide only legacy rates of operation. So, AES is the recommended solution to use the 802.

11n rates and speed. Â□¢ â□¢ Installing the WNDAP350 wirelss access point Before installing the ProSafe Dual Band Wireless-N Access Point WNDAP350, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802. 11b/g/n or 802. 11a/n wireless adapters will be able to communicate with computers on the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown on â□□System Requirementsâ□□ on page 1-5. Setting up the WNDAP350 wirelss access point Tip: Before mounting the WNDAP350 in a high location, first set up and test the WNDAP350 to verify wireless network connectivity. to set up the WNDAP350 wirelss access point: 1. 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 WNDAP350 to the computer. 4. Turn on your computer, connect the power adapter to the WNDAP350 and verify the following: â□¢ â□¢ â□¢ The PWR power light goes on. The LAN light of the wireless access point is lit when connected to a powered on computer. The WLAN LEDs should be blinking. Configuring LAN and Wireless Access To configure the WNDAP350 Ethernet port for LAN access: 1. Connect to the WNDAP350 by opening your browser and entering http://192. Enter admin for the user name and password for the password, both in lower case letters. The main menu of the WNDAP350 displays as shown in Figure 2-3.

Â□¢ â□¢ When the wireless access point is connected to the Internet, under the Support tab, select Documentation to view the documentation for the wireless access point. On the top-right of the screen, select Logout to exit the WNDAP350 setup screens. (You will automatically be logged out of the wireless access point after 5 minutes of no activity. Access Point Name: Enter the access point name of the WNDAP350. This unique name is the access point NetBIOS name. The default Access Point Name is located on the bottom label of WNDAP350. The default is netgearxxxxxx, where xxxxxx represents the last 6 digits of the WNDAP350 MAC address. You may modify the default name with a unique name up to 15 characters long. 5. From the Country/Region pull-down menu, select the region where the WNDAP350 can be used (the default Country/Region is the United States).

Note: If your country or region is not listed, please check with Netgear Support. Spanning tree protocol enables network traffic optimization in settings with multiple WNDAP350 wirelss access points. This section allows each Security Profile to be associated with the default VLAN for WNDAP350. (Useful primarily if the hubs/switches on your LAN support the VLAN 802. Untagged VLANs do not cause the outbound traffic to be tagged with the VLAN ID. Also, there can be only one Untagged VLAN. Management VLANs are used for managing traffic (Telnet, SNMP, and HTTP) to and from the Access Point. management VLANs also cause outbound traffic to be tagged with this VLAN ID. However, if their VLAN ID is same as the Untagged VLAN ID, then the outbound traffic is not tagged. There can be only one Management VLAN.

Figure 2-4 Time zone and system time related settings 9. Enter the Time Settings for your area. See the online help or â□□Configuring Time Settingsâ□□ on page 2-8 for more information about how to configure the settings on this screen. Configure the IP Address settings appropriate for your network. The default values are suitable for most users and situations. (See the online help or â□□Setting Basic IP Optionsâ□□ on page 2-13 for more information about how to configure the settings on this screen. Under the Configuration tab, select System from the main menu, select Basic, and then select Time. From the pull-down menu, select the local time zone for your wireless access point from a list of all available time zones. Enable NTP Client to synchronize the time of the access point with an NTP Server. the Default is Enabled.

Note: You must have an Internet connection to get the current time. â□□ â□□ Use Custom NTP Server. Check the option if you have a custom NTP server. Enter the host name or the IP address of the custom NTP server. 1, November 2009 2-9 ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Configuring Wireless Access To configure your wireless settings for 11b/bg/ng and 11a/na: 1.

Enter the wireless settings for your area. Figure 2-7 Basic Wireless Settings for 802. 11b/bg/ng When you have completed the setup steps, you can deploy the WNDAP350 in your network. If needed, you can now reconfigure the computer you used in step 1 (from the Static IP) back to its original TCP/IP settings. Deploying the WNDAP350 wirelss access point To deploy the WNDAP350 wirelss access point: 2-10 v1.

1 , November 2009 Basic Installation and Configuration ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual 1. Disconnect the WNDAP350 and position it where it will be deployed. The best location is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices. 2. Lift the antennae on either side so that they are vertical. Note: Refer to the antenna positioning and wireless mode configuration information in the Advanced Configuration chapter of the Reference Manual. 3. Connect an Ethernet cable from your WNDAP350 wirelss access point to a LAN port on your router, switch, or hub. note: By default , WNDAP350 is set with the DHCP client disabled. If your network uses dynamic IP addresses, you must change this setting.

To connect to the WNDAP350 after the DHCP server on your network assigns it a new IP address, enter the wireless access point name into your Web browser. The default wireless access point name is netgearxxxxxx, where xxxxxx represents the last 6 bytes of the MAC address.

The default name is printed on the bottom label of the WNDAP350. 4. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet. The PWR, LAN, and Wireless LAN lights and should light up. 11a/na wireless adapter with the correct wireless settings needed to connect to the WNDAP350 (SSID, WEP/WPA, MAC ACL, etc.), verify connectivity by using a browser such as Mozilla Firefox or Internet Explorer to browse the Internet, or check for file and printer access on your network. The default SSID for the 802. 11b/bg/ng wireless mode is NETGEAR_11g; the default SSID for the 802.

11a/na mode is NETGEAR_11a. The SSID of any wireless access adapters must match the SSID configured in the ProSafe Dual Band Wireless-N Access Point WNDAP350. If they do not match, no wireless connection will be made. Note: If you are unable to connect, see Chapter 5, â□□Troubleshooting and Debugging. â□□ Basic Installation and Configuration v1.

1, November 2009 2-11 ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Logging In Using the Default IP Address After you install the WNDAP350, log in to the wireless access point to configure the basic settings and the wireless settings. The WNDAP350 is set, by default, with the IP address of 192. Note: The computer you are using to connect to the WNDAP350 should be configured with an IP address that starts with 192. Connect to the WNDAP350 by entering its default address of http://192. Enter admin for the user name and password for the password, both in lower case letters. Figure 2-8 Connecting to the Access Point 3. click Login. Your Web browser should automatically find the WNDAP350 wirelss access point and display the home screen. 2-12 v1. 1, November 2009 Basic Installation and Configuration ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Setting Basic IP Options The basic IP settings for your wireless access point are entered on this screen. Most of the default settings will work in most cases. However, if your wireless access point is part of a more complex LAN network, then modify the settings to meet the requirements of your network based on the explanation of the various fields. To configure the basic IP settings of your wireless access point: 1. Enter the IP Address fields of the WNDAP350. If you have a DHCP server on your LAN and you enable DHCP, the wireless access point will get its IP address, subnet mask and default gateway settings automatically from the DHCP server on your network when you connect the WNDAP350 to your LAN.

iP Address. Enter the IP Address of your wireless access point. The default IP address is 192. To change it, enter an unused IP address from the address range used on your LAN; or enable DHCP. The Access Point will automatically calculate the subnet mask based on the IP address that you assign. Otherwise, you can use 255. Enter the IP address of the gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the wireless access point is connected. primary DNS Servers. The WNDAP350 will use this IP address as the primary Domain Name Server used by stations on your LAN.

secondary DNS Servers. The WNDAP350 will use this IP address as the secondary Domain Name Server used by stations on your LAN. network Integrity Check. Check this box to enable the WNDAP350 to validate that the upstream link is active before allowing wirelessassociations. If you set this option you must ensure your default gateway is configured.

Wireless Settings The following sections describe how to configure the wireless settings available in both the 802. 11b/bg/ng Wireless Settings To configure the wireless settings of your 802. The Wireless Settings screen of your 802. Configure the Wireless LAN settings based on the following field descriptions: â□¢ Wireless Mode. 11g wireless stations can still be used if they can operate in 802.

This is the default. If you select this option, then two additional options, Channel Width and Guard Interval, are displayed. Note: If you select one of these option and if other settings on this screen are disabled, then you must select the Turn Radio On radio button to enable available options on this screen. â□¢ Turn Radio On. On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities. wireless Network Name (SSID). This is the name of your wireless network. It is set to the default name of NETGEAR_11a for 802. If you disable broadcast of the SSID, only devices that have the correct SSID can connect.

This nullifies the wireless network â□□discoveryâ□□ feature of some products such as Windows XP, Vista and Unix systems but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. From the pull-down menu, select the channel you wish to use on your wireless LAN. The wireless channel in use will be between 1 to 11 for US and Canada, 1 to 13 for Europe and Australia. the default is channel Auto. It should not be necessary to change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers). Should this happen, you may need to experiment with different channels to see which is the best. Alternatively, you can select the Auto channel option for the AP to intelligently pick the channel with least interference. See the article on â□□Wireless Channelsâ□□ available on the NETGEAR website. (A link to this article and other articles of interest can be found in Appendix B, â□□Related Documents. â□□).

When selecting or changing channels, some points to bear in mind: â□□ Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).

If more than one access point can be used, the one with the strongest signal is used. This can only happen when the various access points are using the same SSID. â□¢ MCS Index/Data Rate. From the pull-down menu, select the available transmit data rate of the wireless network. Also, depending on the band selected, the set of rates will vary.

The possible data rates supported are: â□¢ Data Rates for Channel Width=20MHz and Guard Interval=short (400ms): Best, 7. 5 Mbps, 65 Mbps, 13 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 78 Mbps, 104 Mbps, 117 Mbps, 130 Mbps Data Rates for Channel Width=40MHz and Guard Interval=short: Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps Data Rates for Channel Width=40MHz and Guard Interval=long: Best, 13.

From the pull-down menu, select the desired channel width. Legacy clients will not be able to connect in this mode. From the pull-down menu, select the desired guard interval. The guard interval protects from interference from other transmissions. From the pull-down menu, select the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Minimum. Decrease the transmit power if two or more APs are close together and use the same channel frequency. the default is Full.

(The transmit power may vary depending on the local regulatory regulations. From the main menu under Configuration, select Wireless, and then select the 802. 11a/na tab. The Wireless Settings screen for your 11a/na access point displays as shown in Figure 211 below. Configure the Wireless LAN settings based on the following field descriptions: â□¢ Wireless Mode. 11a/na wireless modes can be selected from this menu. This is the default. Note: If you select one of these options and if other settings on this screen are disabled, then you must select the Turn Radio On radio button to enable available options on this screen. â□¢ Turn Radio On. On by default, you can also turn off the radio to disable access through this device.
This can be helpful for configuration, network tuning, or troubleshooting activities. wireless Network Name (SSID). This is the name of your wireless network. It is set to the default name of NETGEAR_11a for 802. If you disable broadcast of the SSID, only devices that have the correct SSID can connect.
This nullifies the wireless network â□□discoveryâ□□ feature of some products such as Windows XP, Vista and Unix systems but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. From the pull-down menu, select the channel you wish to use on your wireless LAN. the default is Auto. When you select Auto as the Channel Frequency, then the only available Channel Width is Dynamic: 20/40MHz. It should not be necessary to change the wireless channel unless you experience interference (shown by lost connections and/or slow data transfers).
Should this happen, you may want to experiment with different channels to see which is the best. See the article on â□□Wireless Channelsâ□□ available on the NETGEAR website. (A link to this article and other articles of interest can be found in Appendix B, â□□Related Documents. â□□). When selecting or changing channels, some points to bear in mind: â□□ Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 8 channels are available. Â□□ If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 8 channels (for example, use channels 36 and 44, or 44 and 52).

â□□ In â□□Infrastructureâ□□ mode , wireless stations normally scan all channels , looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only occur when the various access points are using the same SSID. â□¢ â□¢ MCS Index/Data Rate. From the pull-down menu, select the transmit data rate of the wireless network. Also, depending on the band selected, the set of rates will vary. When Channel Width selected is Dynamic 20/40MHz or when Guard Interval is selected is Auto, then the data rate for a client depends on associated clients channel width and guard interval capabilities. 5 Mbps, 65 Mbps, 13 Mbps, 26 Mbps, 39 Mbps, 52 Mbps, 78 Mbps, 104 Mbps, 117 Mbps, 130 Mbps Data Rates for Channel Width=40MHz and Guard Interval=short: Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps Data Rates for Channel Width=40MHz and Guard Interval=long: Best, 13. From the pull-down menu, select the desired channel width. From the pull-down menu, select the desired guard interval.
The guard interval protects from interference from other transmissions. the default is Auto. The data rates for different Channel Width and Guard Interval combinations are given above: â□¢ â□¢ Output Power. From the pull-down menu, select the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Minimum.
Decrease the transmit power if two or more APs are close together and use the same channel frequency. the default is Full. (The transmit power may vary depending on the local regulatory regulations. WMM allows wireless traffic to have a range of priorities, depending on the type of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic.
For WMM to function correctly, Wireless clients must also support WMM. to configure basic wireless QoS settings for 11b/bg/ng and 11a/na: 1. Under the Configuration tab, select Wireless from the main menu, select Basic, and then select QoS Settings from the left panel. Select the Disable radio button to disable WMM power save. 1, November 2009 2-21 ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Setting Up and Testing Basic Wireless Connectivity Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs. 1. From your Web browser, log in to the WNDAP350 using its default address of http://192. Use the default user name of admin and default password of password or use a new LAN address and password if you have set them up. Verify that the correct Country/ Region in which the wireless interface will operate has been selected.

Under the Configuration tab, select Wireless from the main menu, and then select your network, either the Wireless Settings 11b/bg/ng or Wireless Settings 11a/na. Ensure that the auto channel (default) feature is selected for your network. This feature selects a channel that has the least interference. It should not be necessary to change the wireless channel unless you notice interference problems or are near another wireless access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless access point. Under the Configuration tab, select Security from the main menu, and then select your network Security Profile settings, either Security Profile settings 11b/bg/ng or Security Profile settings 11a/na. For initial configuration and testing, the Security Profile Settings for Profile 1 (the default profile) are set to Open System and the SSID for 11a/na set to NETGEAR_11a and the SSID for 11b/bg/ng set to NETGEAR_11g (see â□□Understanding Security Profilesâ□□ on page 2-23 to configure a profile).

Note: The SSID of any station must match the SSID you configured in the WNDAP350 wirelss access point. If they do not match, you will not get a wireless connection to the WNDAP350. Configure and test your PCs for wireless connectivity 2-22 v1.

1, November 2009 Basic Installation and Configuration ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Program the wireless adapter of your PCs to have the same SSID that you configured in the WNDAP350. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WNDAP350. Note: If you are configuring the WNDAP350 from a wireless computer and you change the SSID, channel, or Security Profile settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the new settings. Once your PCs have basic wireless connectivity to the WNDAP350, you can configure the advanced wireless security functions.

Understanding Security Profiles Security Profiles let you configure unique security settings for each SSID. You can configure up to eight unique 802. 11b/bg/ng wireless security profiles or up to eight unique 802. 11a/na wireless security profiles on the WNDAP350 (see Figure 2-13). Note: If you are using a RADIUS Server, configure the RADIUS settings first, as described in the â□□Configuring WPA with RADIUSâ□□ on page 2-35.

basic Installation and Configuration v1. 1, November 2009 2-23 ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Figure 2-13 Security Profile Settings An overview of the information that is required to set up a Security Profile follows, including a description of the Network Authentication choices that are available: â□¢ Profile Definition. configure the following settings: â□¢ Security Profile Name. Use a name that makes it easy to recognize the profile, and to tell profiles apart. The rest of the profiles are disabled and must be enabled if configured. â□¢ Wireless Network Name (SSID). This is the name of your wireless network. It is set to the default name of NETGEAR_11a for 802. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network â□□discoveryâ□□ feature of some products such as Windows XP, Vista and Unix systems but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.

The WNDAP350 Access Point is set by default as an open system with no authentication. When setting up Network Authentication, bear in mind the following: â□□ â□□ If you are using Access Point mode, then all options are available. In bridge mode some options may be unavailable. Not all wireless adapters support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions on configuring WPA2 settings. You can configure the WNDAP350 to use the types of network authentication shown in the table below. 1x WPA with RADIUS Description Can be used with WEP encryption or no encryption. You must use WEP encryption and enter at least one shared key.

You must configure the RADIUS Server Settings to use this option. You must configure the RADIUS Server Settings to use this option. WPA2 with RADIUS Only select this if all clients support WPA2. If selected, you must use (WPA2 is a later version of WPA.) AES encryption and configure the RADIUS Server Settings.

WPA and WPA2 with RADIUS This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and configure the RADIUS Server Settings. You must use TKIP or TKIP + AES encryption and enter the WPA passphrase (Network key). Network Authentication Types Typea Description WPA2-PSK Only select this if all clients support WPA2. If selected, you must use (WPA2 is a later version of WPA) AES or TKIP + AES encryption and enter the WPA passphrase (Network key).

wPA-PSK and WPA2-PSK This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and enter the WPA passphrase (Network key). a. All options are available if using Access Point mode. In bridge modes some options may be unavailable. â□¢ Data Encryption. The available options depend on the Network Authentication setting selected (see Table 2-1 above); otherwise, the default is None. The Data Encryption settings are explained in the table below: Table 2-2. data Encryption Settings Data Encryption Type None Open WEP 64 bits WEP 128 bits WEP 152 bits WEP TKIP AES TKIP + AES Description No encryption is used. Can be used with WEP encryption or no encryption.

Proprietary mode that will only work with other wireless devices that support this mode. This is the standard encryption method used with WPA and WPA2. This is the standard encryption method for WPA2. This setting supports both WPA and WPA2. broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. â□¢ â□□ Use of Passphrases and Keys are explained below: Passphrase. To use the Passphrase to generate the WEP keys, enter a passphrase and click the Generate Keys button. You can also enter the keys directly. These keys must match the other wireless stations.

key 1 , Key 2 , Key 3 , Key 4. If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data. If using WPA-PSK or WPA2-PSK, enter the passphrase here.

All wireless stations must use the same passphrase (network key). The network key must be from 8 to 64 characters in length. â□¢ Wireless Client Security Separation. If enabled, the associated wireless clients will not be able to communicate with each other. @@If the hubs/switches on your LAN support the VLAN (802.

1Q) standard and this feature has been enabled, the default VLAN ID for WNDAP350 will be associated with each profile. The default Profile VLAN ID must match the IDs used by other network devices. â□¢ SSID and WEP/WPA Settings Setup Form 802. 11b/bg/ng Configuration For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step. Â□¢ SSID: The Service Set Identification (SSID) identifies the wireless local area network. nETGEAR_11g is the default WNDAP350 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

_____ *Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card.*

All wireless nodes in the same network must be configured with the same SSID: â□¢ Authentication: Circle one: Open System or Shared Key. (Choose Shared Key for more security.) Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the WNDAP350. 11a/n keys for the Key Size chosen. For WPA, record the following settings for the primary and secondary RADIUS servers: Server Name/IP Address: Primary _____ Secondary _____ Port: _____ Shared Secret: _____ 802. 11a/na Configuration For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step. Â□¢ SSID: The Service Set Identification (SSID) identifies the wireless local area network.

nETGEAR_11a is the default WNDAP350 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below. _____ Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID: â□¢ Authentication Circle one: Open System or Shared Key.

Choose Shared Key for more security. Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well and have the same keys in the same positions as those in the WNDAP350. 11b/bg/ng keys for the Key Size chosen. For WPA, record the following settings for the primary and secondary RADIUS servers: Server Name/IP Address: Primary _____ Secondary _____ Port: _____ Shared Secret: _____ Use the procedures described in the following sections to configure the WNDAP350. Store this information in a safe place.

Configuring the RADIUS Server Settings You can setup or modify the RADIUS Server settings to compliment Network Authentication security options. The RADIUS Server must be used with Legacy 802. 1x, and can be used with WPA and WPA2 Network Authentication. When using a RADIUS Server, the RADIUS Server settings must be configured before completing the Network Authentication security profile (see â□□Configuring WPA with RADIUSâ□□ on page 2-35, â□□Configuring WPA2 with RADIUSâ□□ on page 2-37, or â□□Configuring WPA and WPA2 with RADIUSâ□□ on page 2-38 for specifics on implementing these security options). note: The RADIUS Server Settings apply to all profiles. They only need to be configured once per wireless access point. to set up or modify the RADIUS Server Settings: 1. From your Web browser, log in to the WNDAP350 using the default LAN address of http://192. 237, user name admin and password password, or use the LAN address and password that you set up. 2.

Under the Configuration tab, select Security on the main menu, select Advanced from the left panel, and then select RADIUS Server Settings. This configuration is required for authentication using a RADIUS Server. The IP Address, Port Number, and Shared Secret are required for communication with the Primary RADIUS Server. You can also configure a Secondary RADIUS Server to use, if the Primary RADIUS Server fails. â□□ â□□ â□□ â□¢ IP Address. The IP address of the RADIUS Server. port Number. The port number of the RADIUS Server. This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client). accounting Server.

This configuration is required for accounting using a RADIUS Server. The IP Address, Port Number, and Shared Secret are required for communication with the Primary RADIUS Server. You can also configure a Secondary RADIUS Server to use if the Primary RADIUS Server fails. â□□ â□□ IP Address. The IP address of the RADIUS Server.

port Number. Port number of the RADIUS Server. This is shared between the Wireless Access Point and the RADIUS Server while authenticating the supplicant (wireless client). Setting up a Security Profile The WNDAP350 allows you to set up eight different security profiles for 802. 11b/bg/ng and eight different profiles for 802.

11a/na. Each profile can be configured with a different security option for network authentication. Note: If you are using a RADIUS Server, configure the RADIUS settings first, as described in the â□□Configuring the RADIUS Server Settingsâ□□ on page 2-29. From your Web browser, log in to the WNDAP350 using the default LAN address of http://192. 237, user name admin and password password, or use the LAN address and password that you set up. 2. @@The screen for the Profile Settings you selected displays as shown in Figure 2-15above. 3. Select the check box of the profile you want to modify and click Edit. The Security Profile Configuration screen for the selected profile displays (see Figure 2-16).

Figure 2-16 Edit a security profile 4. Give your profile a meaningful name so that you can remember it later. (If it is broadcast, it can be easily detected by other clients.) 7. From the Network Authentication pull-down menu, select the Network Authentication Type you want to use for this profile: â□¢ 2-32 v1. 1, November 2009 To configure WEP encryption for Open Systems or Shared Key, see â□□Configuring WEPâ□□ on page 2-33. Basic Installation and Configuration ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual â□¢ â□¢ â□¢ â□¢ â□¢ To configure WPA with RADIUS, see â□□Configuring WPA with RADIUSâ□□ on page 2-35. To configure WPA2 with RADIUS, see â□□Configuring WPA2 with RADIUSâ□□ on page 2-37. To configure WPA and WPA2 with RADIUS, see â□□Configuring WPA and WPA2 with RADIUSâ□□ on page 2-38. If enabled, the associated wireless clients will not be able to communicate with each other.

9. If the hubs/switches on your LAN support the VLAN (802. 1Q) standard and this feature has been enabled, the default VLAN ID for WNDAP350 will be associated with each profile. The default Profile VLAN ID must match the IDs used by other network devices. Your new settings will appear in the Security Profiles table identified by the Profile Name of the profile.

a VLAN ID will also be assigned to your profile. Note: Security Profiles that share the same type of network authentication need not share the same passphrase or keys. to enable your Security Profile: 1. Check the radio box in the Enable column next to your profile. From the Network Authentication drop-down menu, choose either Open System or Shared Key authentication.

From the Data Encryption drop-down menu, select encryption strength (64 bits, 128 bits, or 152 bits). 3. You manually or automatically program the four data encryption keys. @@@@The four key boxes will be automatically populated with key values. @@ figure 2-17 Configure WEP Shared Key 4. @@(Data transmissions are always encrypted using the default key. @@ 11 wireless communication standard. @@@@@@@@@@Configuring WPA with RADIUS Not all wireless adapters support WPA. furthermore , client software is required on the client. @@@@@@ to configure WPA , follow these steps: 1.

@@@@@@The screen for the Profile Settings you selected displays. @@Figure 2-18 Configure WPA with RADIUS 5. @@@@@@@@ furthermore , client software is required on the client. Make sure your client card supports WPA2. @@Figure 2-19 Configure WPA2 with RADIUS To configure WPA2 with RADIUS: 1. Under the Configuration tab, select Security on the main menu, select Advanced from the left panel, and then select RADIUS Server Settings. Enter the RADIUS settings as shown in â□□â□□Configuring the RADIUS Server Settingsâ□□ on page 2-29. @@A The screen for the Profile Settings you selected displays. When the Security Profile screen displays, check the check bb ox of the Security Profile you want to modify and click Edit. From the Network Authentication drop-down menu, select WPA2 with RADIUS from the list.

@@@@Configuring WPA and WPA2 with RADIUS Not all wireless adapters support WPA and WPA2. Client software is required on the client: â□¢ â□¢ Windows XP and Windows 2000 with Service Pack 3, or above, do include the client software that supports WPA. The wireless adapter hardware and driver must also support WPA. Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2.

The wireless adapter hardware and driver must also support WPA2. Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings. Figure 2-20 Configure WPA and WPA2 with RADIUS 2-38 v1. 1 , November 2009 Basic Installation and Configuration ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual To configure WPA and WPA2 with RADIUS: 1. Under the Configuration tab, select Security on the main menu, select Advanced from the left panel, and then select RADIUS Server Settings.

Enter the RADIUS settings as shown in â□□â□□Configuring the RADIUS Server Settingsâ□□ on page 2-29. @@The screen for the Profile Settings you selected displays. @@ 5. From the Network Authentication drop-down menu, select WPA & WPA2 with RADIUS from the list. @@@@Windows XP and Windows 2000 with Service Pack 3 or above include the client software that supports WPA. @@@@Enter the preshared key passphrase (Network Key). @@@@Make sure your client card supports WPA2. @@From the Network Authentication drop-down menu, select WPA2-PSK from the list. Enter the preshared key passphrase (Network Key). @@@@Client software is required on the client: â□¢ â□¢ @@The wireless adapter hardware and driver must also support WPA.

Service Pack 3 does not include the client software that supports WPA2. Make sure your client card supports WPA2. The wireless adapter hardware and driver must also support WPA2. Consult the product documentation for your wireless adapter; WPA client software for instructions on configuring WPA settings; and WPA2 client software for instructions on configuring WPA2 settings 2-42 v1. @@@@1, November 2009 2-43 ProSafe Dual Band Wireless-N Access Point WNDAP350 Reference Manual Restricting Wireless Access by MAC Address The optional Access Control window lets you block the network access privilege of any specified stations through the WNDAP350 wirelss access point. When you enable access control, the access point only accepts connections from clients on the selected access control list. this provides an additional layer of security. Note: If configuring the WNDAP350 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the wireless access point from a wired computer or from a wireless computer that is on the access control list to make any further changes. to restrict access based on MAC addresses: 1.

Log in to the WNDAP350 using the default address of http://192. 237, user name of admin and default password of password, or whatever LAN address and password you have set up. 2. Under the Configuration tab, select Security on the main menu, select Advanced from the left panel, and then select MAC Authentication. Check the Turn Access Control On radio box to enable Access Control feature.

The options are: â□¢ â□¢ Local MAC Address Database â□□ The Access Point will use the local MAC address table for Access Control. This is the default. RADIUS MAC Address Database â□□ The Access Point will use the MAC address table located on the external RADIUS server on the LAN for Access Control. If you choose this database, you must configure the RADIUS Server Settings first (see â□□Configuring the RADIUS Server Settingsâ□□ on page 2-29). 5.

The Trusted Wireless Stations list shows any wireless stations you have entered. If you have not entered any wireless stations this list will be empty. Click Refresh to refresh the Available Wireless Stations list found in your area. 7. Select the stations from the list of Available Wireless Stations found in your area, or enter the MAC address of a station to add a new station manually. (You can usually find the MAC address printed on the bottom of the wireless adapter. Click Add to add the wireless device to the Trusted Wireless Stations list. Repeat these steps for each additional device you want to add to the list. Now, only devices on this list will be allowed to wirelessly connect to the WNDAP350. 2-46 v1.

1, November 2009 Basic Installation and Configuration Chapter 3 Management This chapter describes how to use the management features of your ProSafe Dual Band WirelessN Access Point WNDAP350. To access these features, connect to the WNDAP350 as described in â□□Logging In Using the Default IP Addressâ□□ on page 2-12. Then select the category under either the Monitoring or Maintenance headings in the main menu of the browser interface. This chapter contains the following sections: 1. Â□□Restoring the WNDAP350 to the Factory Default Settings 6. Â□□Packet Capture Remote Management Both the SNMP and Remote Console are enabled by default, which allows for remote management of the WNDAP350 from a client running SNMP management software, as well as from a secure Telnet console. Under the Maintenance tab, select Remote Management, and then select SNMP from the left sidebar. the SNMP screen displays , as shown in Figure 3-1 below: Figure 3-1 Configure SNMP settings 2.