Chapter 4
Wireless Configuration

This chapter describes how to configure the wireless features of your WPNT834 router. In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your firewall in order to maximize the network speed. For further information on wireless networking, see "Wireless Communications" in Appendix B.

Observing Performance, Placement, and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless firewall. 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 router. For complete range and performance specifications, please see Appendix A, "Technical Specifications".

For best results, place your firewall:

- Near the center of the area in which your computers will operate.
- In an elevated location such as a high shelf where the wirelessly connected computers have line-of-sight access (even if through walls).
- Away from sources of interference, such as computers, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

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, WPA-PSK and WPA2-PSK encryption can consume more battery power on a notebook computer.

Implementing Appropriate Wireless Security

➡	**Note:** Indoors, computers can connect over 802.11b/g wireless networks at ranges of up to 300 feet. Such distances can allow for others outside of your immediate area to access your network.

Unlike wired network data, 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 WPNT834 router provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

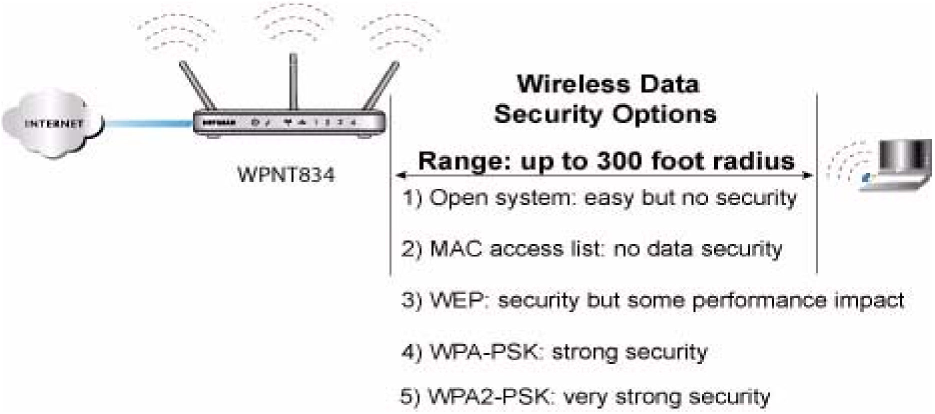

INTERNET
WPNT834
Wireless Data
Security Options
Range: up to 300 foot radius
1) Open system: easy but no security
2) MAC access list: no data security
3) WEP: security but some performance impact
4) WPA-PSK: strong security
5) WPA2-PSK: very strong security

Figure 4-1

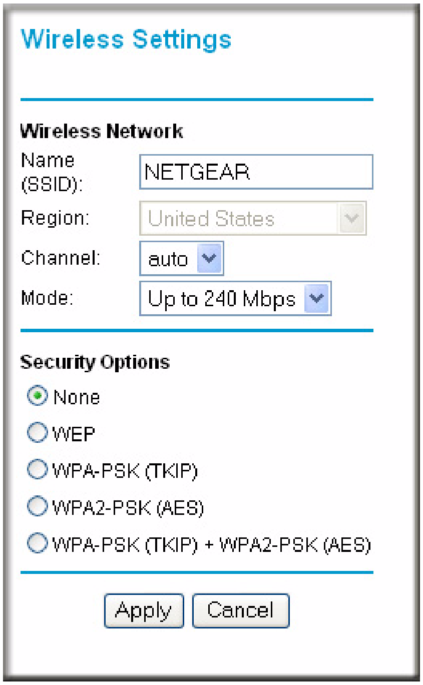
There are several ways you can enhance the security of your wireless network.

- **Restrict Access Based on MAC address.** You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the WPNT834. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network ‘discovery’ feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption block all but the most determined eavesdropper.

- **WPA-PSK** and **WPA2-PSK.** Wi-Fi Protected Access, Pre-Shared Key (WPA-PSK and WPA2-PSK) data encryption provide strong data security. WPA-PSK and WPA2-PSK block eavesdropping. Because these are new standards, wireless device driver and software availability may be limited.
- **Turn Off the Wireless LAN.** If you disable the wireless LAN, wireless devices cannot communicate with the router at all. You might choose to turn off the wireless LAN when you are away and other users of your network all use wired connections.

Understanding Wireless Settings

To configure the Wireless settings of your firewall, click the **Wireless** link in the main menu of the browser interface. The Wireless Settings menu appears, as shown below.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: United States

Channel: auto

Mode: Up to 240 Mbps

Security Options

● None

○ WEP

○ WPA-PSK (TKIP)

○ WPA2-PSK (AES)

○ WPA-PSK (TKIP) + WPA2-PSK (AES)

Figure 4-2

- **Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network will need to use this SSID for that network. The WPNT834 default SSID is: **NETGEAR**.
- **Region.** This field identifies the region where the WPNT834 can be used. It may not be legal to operate the wireless features of the wireless router in a region other than one of those identified in this field.

Note: The region selection feature may not be available in all countries.

- **Channel.** This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point. For more information on the wireless channel frequencies, see "Wireless Communications" in Appendix B.
- **Mode.** This field determines which data communications protocol is used. You can select "g only", "g and b", "Up To 126 Mbps", and "Up To 240 MBps". The "g only" option dedicates the WPNT834 to communicating with the higher bandwidth 802.11g wireless devices exclusively. The "g and b" mode provides backward compatibility with the slower 802.11b wireless devices while still enabling 802.11g communications. The "Up to 126 Mbps" mode provides two transmission streams with different data on the same channel at the same time. The "Up to 240 Mbps" uses channel expansion to achieve the 240 Mbps data rate. The WPNT834 router will use the channel you selected as the primary channel and expand to the secondary channel (primary channel +4 or -4) to achieve a 40MHz frame-by-frame bandwidth. The WPNT834 router will detect channel usage and will disable frame-by-frame expansion if the expansion would result in interference with the data transmission of other access points or clients.

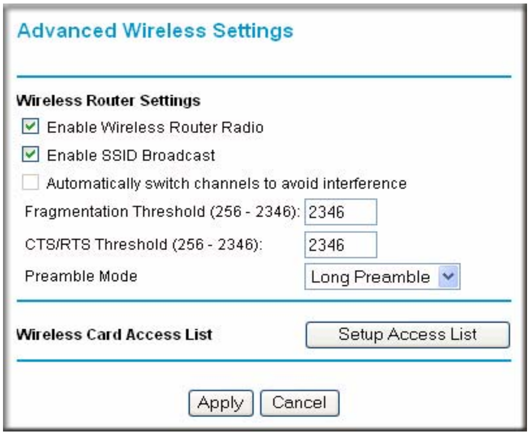
Note: The maximum wireless signal rate is derived from the IEEE Standard 802.11 Specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

- **Security Options.** These options are the wireless security features you can enable. The table below identifies the various basic wireless security options. A full explanation of these standards is available in "Wireless Communications" in Appendix B.

Table 4-1. Basic Wireless Security Options

Field	Description
None	No wireless security.
WEP	WEP offers the following options: • Open System With Open Network Authentication and 64- or 128-bit WEP Data Encryption, the WPNT834 *does* perform 64- or 128-bit data encryption but *does not* perform any authentication. • Shared Key Shared Key authentication encrypts the SSID and data. Choose the Encryption Strength (64- or 128-bit data encryption). Manually enter the key values or enter a word or group of printable characters in the Passphrase box. Manually entered keys *are* case sensitive but passphrase characters *are not* case sensitive. **Note**: Not all wireless adapter configuration utilities support passphrase key generation. • Auto The wireless router automatically detects whether Open System or Shared Key is used.
WPA-PSK **WPA2-PSK**	WPA-Pre-shared Key *does* perform authentication. WPA-PSK uses TKIP (Temporal Key Integrity Protocol) data encryption and WPA2-PSK uses AES (Advanced Encryption Standard) data encryption. Both dynamically change the encryption keys making them nearly impossible to circumvent. Enter a word or group of printable characters in the Password Phrase box. These characters *are* case sensitive. **Note**: Not all wireless adapter configuration utilities support WPA-PSK and WPA2-PSK. Furthermore, client software is required on the client. Windows XP Service Pack 2 and Windows XP Service Pack 1 with WPA patch do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA.

To configure the advanced wireless settings of your firewall, click the **Wireless Setup** link in the Advanced section of the main menu of the browser interface. The Advanced Wireless Settings menu appears, as shown below.



Advanced Wireless Settings

Wireless Router Settings

☑ Enable Wireless Router Radio

☑ Enable SSID Broadcast

□ Automatically switch channels to avoid interference

Fragmentation Threshold (256 - 2346): 2346

CTS/RTS Threshold (256 - 2346): 2346

Preamble Mode: Long Preamble

Wireless Card Access List

Figure 4-3

- **Enable Wireless Router Radio.** If you disable the wireless router radio, wireless devices cannot connect to the WPNT834.
- **Enable SSID Broadcast.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. Disabling SSID broadcast nullifies the wireless network 'discovery' feature of some products such as Windows XP.
- **Automatically switch channels to avoid interference.** If enabled, the WPNT834 router will periodically survey the wireless environment to ensure that it is using the clearest channel. If a clearer channel is available, it may automatically switch channels.

> **Note:** After the router switches channels, there may be a slight delay while your wirless computers reconnect to the router. If you want to avoid this possibility, leave this checkbox unselected.

- **Wireless Card Access List.** When the Trusted PCs Only radio button is selected, the WPNT834 checks the MAC address of the wireless station and only allows connections to computers identified on the trusted computers list.

> **Note:** The **Fragmentation Threshold**, **CTS/RTS Threshold**, and **Preamble Mode** options are reserved for wireless testing and advanced configuration only. Do not change these settings.

Information to Gather Before Changing Basic Wireless Settings

Before customizing your wireless settings, print this form and record the following information. If you are working with an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Otherwise, you must choose the settings for your wireless network. Either way, record the settings for your wireless network in the spaces below.

- **Wireless Network Name (SSID)*:*** ______________________________ The SSID identifies the wireless network. You can use up to 32 alphanumeric characters. The SSID *is* case sensitive. The SSID in the wireless adapter card must match the SSID of the wireless router. In some configuration utilities (such as in Windows XP), the term "wireless network name" is used instead of SSID.
- **If WEP Authentication is Used,** circle one: **Open System**, **Shared Key, or Auto**.

> **Note:** If you select **Shared Key**, the other devices in the network will not connect unless they are also set to Shared Key and are configured with the correct key.

- **WEP Encryption key size**. Choose one: **64-bit** or **128-bit**. Again, the encryption key size must be the same for the wireless adapters and the wireless router.
- **Data Encryption (WEP) Keys**. There are two methods for creating WEP data encryption keys. Whichever method you use, record the key values in the spaces below.
  - **Passphrase method**. ______________________________ These characters *are* case sensitive. Enter a word or group of printable characters and click the **Generate Keys** button. Not all wireless devices support the passphrase method.
  - **Manual method**. These values *are not* case sensitive. For 64-bit WEP, enter 10 hex digits (any combination of 0-9 or a-f). For 128-bit WEP, enter 26 hex digits.

Key 1: ___________________________________

Key 2: ___________________________________

Key 3: ___________________________________

Key 4: ___________________________________

- **If WPA-PSK or WPA2-PSK Authentication is Used:**
  – **Passphrase**: ________________________________ These characters *are* case sensitive. Enter a word or group of printable characters. When you use WPA-PSK, the other devices in the network will not connect unless they are set to WPA-PSK as well and are configured with the correct Passphrase. Similarly, when you use WPA2-PSK, the other devices in the network will not connect unless they are aslo set to WPA2-PSK and are configured with the correct Passphrase.

Use the procedures described in the following sections to configure the WPNT834. Store this information in a safe place.

Default Factory Settings

When you first receive your WPNT834, the default factory settings are in effect, as shown below. You can restore these defaults with the Factory Default Restore button on the rear panel. After you install the WPNT834 router, use the procedures below to customize any of the settings to better meet your networking needs.

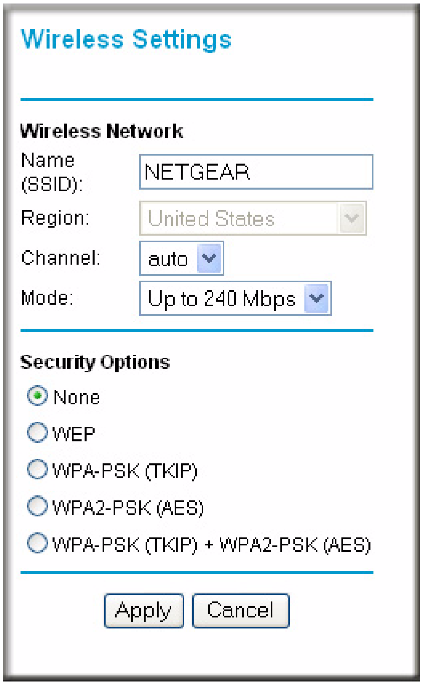
FEATURE	DEFAULT FACTORY SETTINGS
Wireless Router Radio	**Enabled**
Wireless Access List (MAC Filtering)	**All wireless stations allowed**
SSID broadcast	**Enabled**
SSID	**NETGEAR**
802.11b/g RF Channel	**Auto**
Mode	**Up to 240 Mbps**
Security	**None**
DHCP Server	**Enabled**
DHCP range	**192.168.1.2 to 192.168.1.254**

How to Set Up and Test Basic Wireless Connectivity

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

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

1. Log in to the WPNT834 firewall at its default LAN address of *http://www.routerlogin.net* (or *http://192.168.1.1*) with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Wireless Settings** in the main menu of the WPNT834 firewall.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: United States

Channel: auto

Mode: Up to 240 Mbps

Security Options

● None

○ WEP

○ WPA-PSK (TKIP)

○ WPA2-PSK (AES)

○ WPA-PSK (TKIP) + WPA2-PSK (AES)

Figure 4-4

3. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

> **Note:** The SSID is case sensitive; NETGEAR is not the same as nETgear. Also, the SSID of any wireless access adapters must match the SSID you configure in the RangeMax 240 Wireless Router WPNT834. If they do not match, you will not get a wireless connection to the WPNT834.

4. Set the Region. Select the region in which the wireless interface will operate.
5. Set the Channel. The default channel is Auto.

   This field determines which operating frequency is used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your firewall. For more information on the wireless channel frequencies, see "Wireless Communications" in Appendix B.
6. For initial configuration and testing, leave the Wireless Card Access List set to "Everyone" and the Encryption Strength set to "Disabled."
7. Click **Apply** to save your changes.

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

8. Configure and test your computers for wireless connectivity.

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

> **Warning:** The Network Name (SSID) is case sensitive. If NETGEAR is the Network Name (SSID) in your wireless router, you must enter NETGEAR in your computer's wireless settings. Typing nETgear will not work.

Once your computers have basic wireless connectivity to the firewall, you can configure the advanced wireless security functions of the firewall.

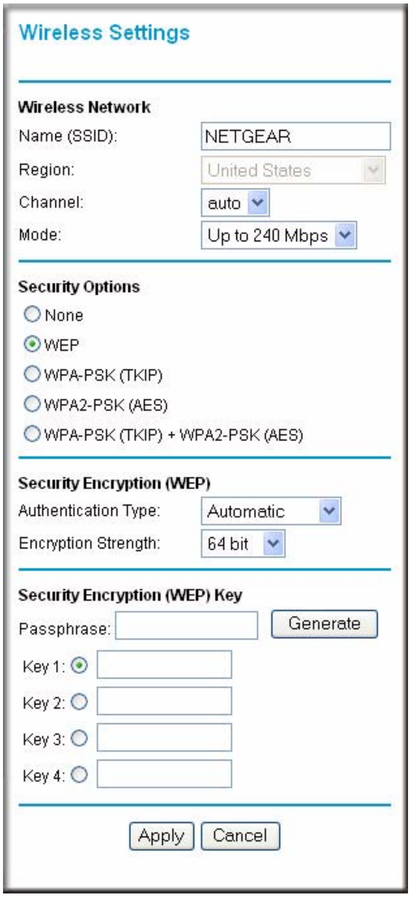
How to Configure WEP

To configure WEP data encryption, follow these steps:

➡	**Note:** If you use a wireless computer to configure WEP settings, you will be disconnected when you click **Apply**. You must then either configure your wireless adapter to match the wireless router WEP settings or access the wireless router from a wired computer to make any further changes.

1. Log in to the WPNT834 firewall at its default LAN address of *http://www.routerlogin.net* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Wireless Settings** in the main menu of the WPNT834 firewall.
3. From the Security Options menu, select **WEP**. The WEP options display.

4. Select the Authentication Type and Encryptions strength from the drop-down lists.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: United States

Channel: auto

Mode: Up to 240 Mbps

Security Options

○ None

● WEP

○ WPA-PSK (TKIP)

○ WPA2-PSK (AES)

○ WPA-PSK (TKIP) + WPA2-PSK (AES)

Security Encryption (WEP)

Authentication Type: Automatic

Encryption Strength: 64 bit

Security Encryption (WEP) Key

Passphrase:

Key 1: ●

Key 2: ○

Key 3: ○

Key 4: ○

Figure 4-5

5. You can manually or automatically program the four data encryption keys. These values must be identical on all computers and Access Points in your network.

- Automatic—Enter a word or group of printable characters in the Passphrase box and click the **Generate** button. The passphrase is case sensitive; NETGEAR is not the same as nETgear. The four key boxes is automatically populated with key values.
- Manual—Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F). These entries are not case sensitive; AA is the same as aa.
  Select which of the four keys to activate.

See “Wireless Communications” in Appendix B for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

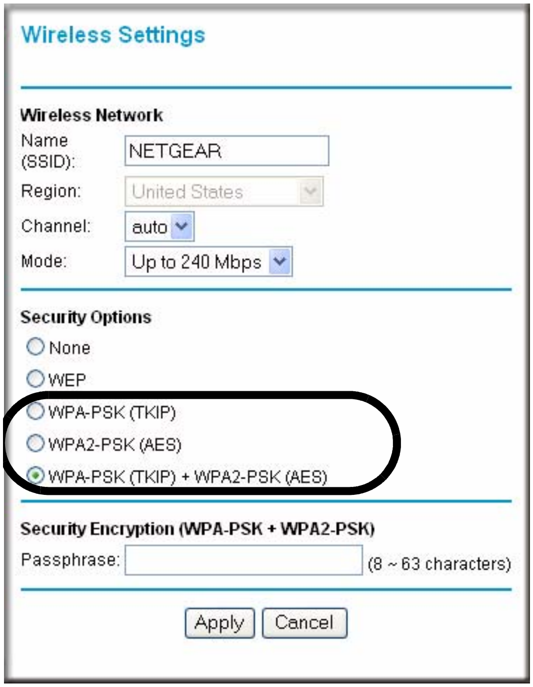
6. Click **Apply** to save your settings.

How to Configure WPA-PSK or WPA2-PSK Wireless Security

➡	**Note:** Not all wireless adapters support WPA. Furthermore, client software is also required. Windows XP with Service Pack 2 does include WPA support. Nevertheless, the wireless adapter hardware and driver must also support WPA. For instructions on configuring wireless computers or PDAs (Personal Digital Assistants) for WPA-PSK security, consult the documentation for the product you are using.

To configure WPA-PSK or WPA2-PSK, follow these steps:

1. Click **Wireless Settings** in the Setup section of the main menu and select one of the WPA-PSK or WPA2-PSK options for the Security Type. The third option (**WPA-PSK [TKIP] + WP2-PSK [AES]**) is the most flexible, since it allows clients using either WPA-PSK or WPA2-PSK.



Wireless Settings

Wireless Network

Name (SSID): NETGEAR

Region: United States

Channel: auto

Mode: Up to 240 Mbps

Security Options

○ None

○ WEP

○ WPA-PSK (TKIP)

○ WPA2-PSK (AES)

● WPA-PSK (TKIP) + WPA2-PSK (AES)

Security Encryption (WPA-PSK + WPA2-PSK)

Passphrase: (8 ~ 63 characters)

Figure 4-6

2. Enter a word or group of 8-63 printable characters in the Passphrase box.
3. Click **Apply** to save your settings.

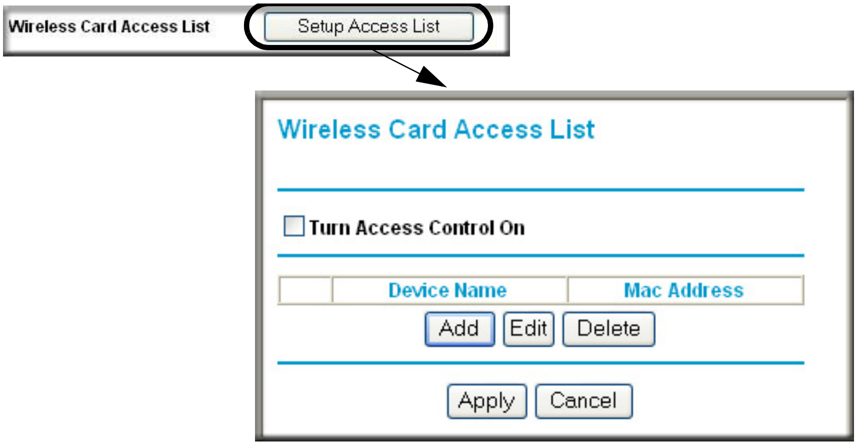
How to Restrict Wireless Access by MAC Address

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

1. Log in to the WPNT834 firewall at its default LAN address of *http://www.routerlogin.net* with its default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

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

2. Click **Wireless Settings** in the **Advanced** section of the main menu of the WPNT834 firewall.
3. From the Wireless Settings menu, click **Setup Access List** to display the Wireless Access menu shown below.



Wireless Card Access List

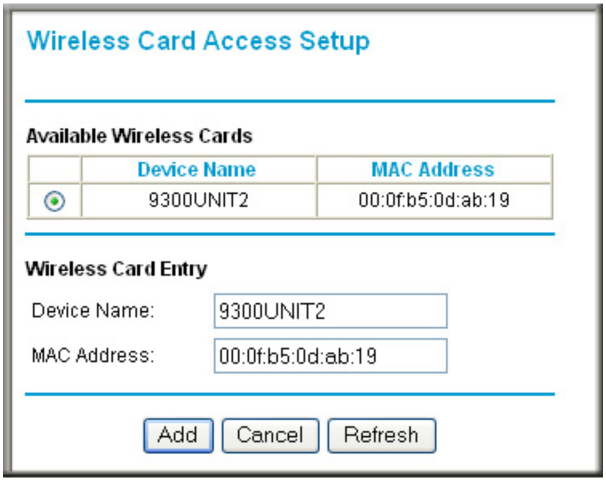
□ Turn Access Control On

	Device Name	Mac Address

Figure 4-7

4. Click the **Turn Access Control On** check box.

5. Click **Add** to add a wireless device to the wireless access control list. The Wireless Card Access Setup dialog displays.



Wireless Card Access Setup

Available Wireless Cards

	Device Name	MAC Address
●	9300UNIT2	00:0f:b5:0d:ab:19

Wireless Card Entry

Device Name: 9300UNIT2

MAC Address: 00:0f:b5:0d:ab:19

Figure 4-8

6. In the Available Wireless Cards list, either select from the list of available wireless cards the WPNT834 has found in your area, or enter the MAC address and device name for a device you plan to use. You can usually find the MAC address printed on the wireless adapter.

> **Note:** You can copy and paste the MAC addresses from the firewall's Attached Devices menu into the MAC Address box of this menu. To do this, configure each wireless computer to obtain a wireless link to the firewall. The computer should then appear in the Attached Devices menu.

7. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.

8. Repeat step 5 to step 7 for each additional device you wish to add to the list.

9. Be sure to click **Apply** to save your Wireless Card Access List settings.

Now, only devices on this list are allowed to wirelessly connect to the WPNT834.