

NETGEAR®

WN804 Access Point

User Manual



June 2013
202-11236-01

350 East Plumeria Drive
San Jose, CA 95134
USA

Support

Thank you for selecting NETGEAR products.

After installing your device, locate the serial number on the label of your product and use it to register your product at <https://my.netgear.com>. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit <http://support.netgear.com>.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at <http://support.netgear.com/general/contact/default.aspx>.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. © NETGEAR, Inc. All rights reserved.

Contents

Chapter 1 Getting Started

Package Contents	6
Hardware Features	6
Front Panel	7
Rear Panel	8
Product Label	8
Attach the Feet	9
Log In to the Access Point	9
Position the Access Point	10
Connect to the WiFi Network with WPS	11

Chapter 2 Basic Configuration

Home Screen	13
Specify IP Settings	14
Specify Wireless Settings	14
Wireless Settings Screen Fields	16
Change the Wireless Security Option	17
WPS Wizard for WiFi Connections	18
Set Up a Guest Network	19
View Attached Devices	21

Chapter 3 System Settings

View Logs of Web Access or Attempted Web Access	23
Manage the Configuration File	24
Back Up Settings	24
Restore Configuration Settings	24
Erase the Current Configuration Settings	25
Change the Password	25
Password Recovery	26
Wireless AP Update	27
Reboot the Access Point	27

Chapter 4 Advanced Configuration

Advanced Wireless Settings	30
Control the Wireless Radio	30
Set Up a Wireless Schedule	31
Enable or Disable 20/40 GHz Coexistence	31
View or Change WPS Settings	32

Set Up a Wireless Access List by MAC Address	33
Wireless Distribution System (WDS)	34
Set Up the Base Station	35
Set Up a Repeater	36

Chapter 5 Troubleshooting

Troubleshoot with the LEDs	39
No LEDs Are Lit on the Access Point	39
The WiFi LED Is Off	39
Login Prompt Does Not Display	39
No WiFi Access to the Internet or LAN	40
Time-Out Error for a URL or IP Address	40

Appendix A Supplemental Information

Factory Default Settings	42
Technical Specifications	43

Appendix B Notification of Compliance

1. Getting Started

1

This chapter covers the following topics:

- *Package Contents*
- *Hardware Features*
- *Attach the Feet*
- *Log In to the Access Point*
- *Position the Access Point*
- *Connect to the WiFi Network with WPS*

Package Contents

Open the box and remove the access point, cables, and installation guide.

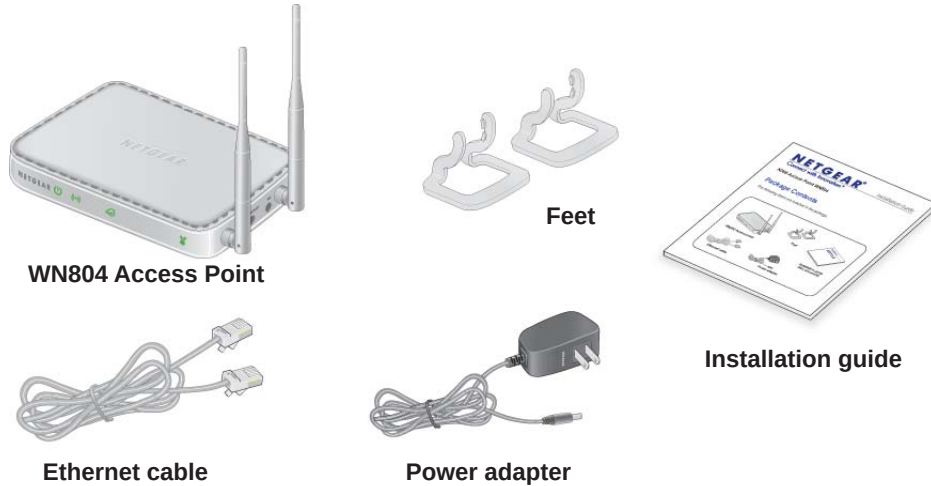


Figure 1. Check the package contents

Your box contains the following items:

- WN804 Access Point
- AC power adapter (plug varies by region)
- Category 5 (Cat 5) Ethernet cable
- Installation guide with cabling and access point setup instructions

If any parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton and original packing materials, in case you return the product for repair.

Hardware Features

Before you cable your access point, take a moment to become familiar with the front, side, and back panels and the label. Pay particular attention to the LEDs on the front panel.

Front Panel

The access point front panel has the status LEDs shown in the following figure.

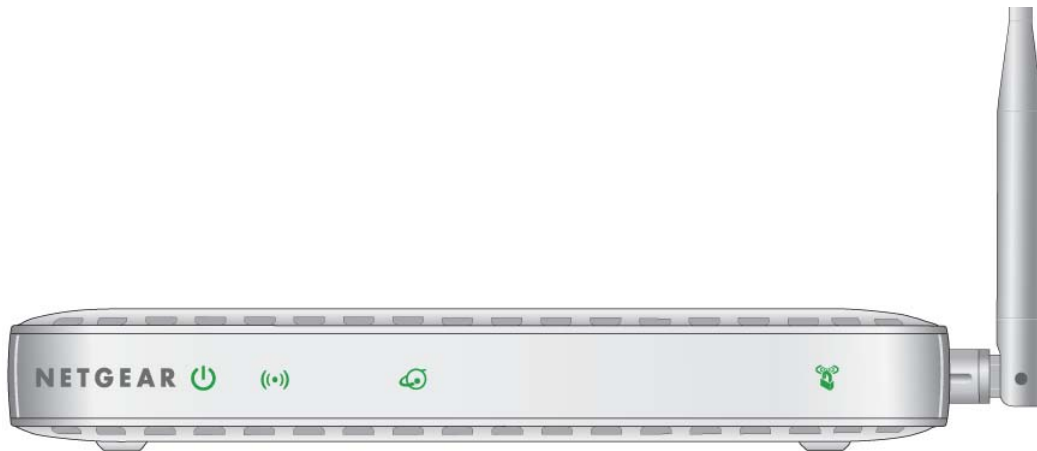


Figure 2. Access point front panel

Table 1. Front panel LED descriptions

LED	Description
Power 	Solid amber. The access point is starting up. Blinking amber. The firmware is upgrading, or the Reset button was pressed. Solid green. The access point is ready. Blinking green. The firmware is corrupted. Visit www.netgear.com/support. Off. Power is not supplied to the access point.
WiFi 	Solid green. The wireless radio is operating. Off. The wireless radio is off.
Internet 	Solid green. The Internet connection is ready. Solid amber. The Ethernet cable connection to the modem has been detected. Off. No Ethernet cable is connected to the modem.
WPS 	Slow blinking. The LED lights for 5 seconds if WPS setup fails. Blinking: WPS activity is in process. Off. No WPS activity or no WPS failure was detected.

The WiFi and WPS buttons on the side of the access point toggle the WiFi and WPS functions on and off.

- **WiFi On/Off button.** Pressing and holding this button for 2 seconds turns the wireless radio on and off. If the WiFi LED is lit, the wireless radios is on. If this LED is off, the wireless radio is turned off and you cannot connect wirelessly to the access point.
- **WPS button.** You can use this button to use WPS to add a wireless device or computer to your wireless network. The WiFi LED blinks blue when the access point is trying to add

the wireless device or computer. The LED stays solid blue when wireless security is enabled in the access point.

Rear Panel

The rear panel has the connections and buttons shown in the following figure.

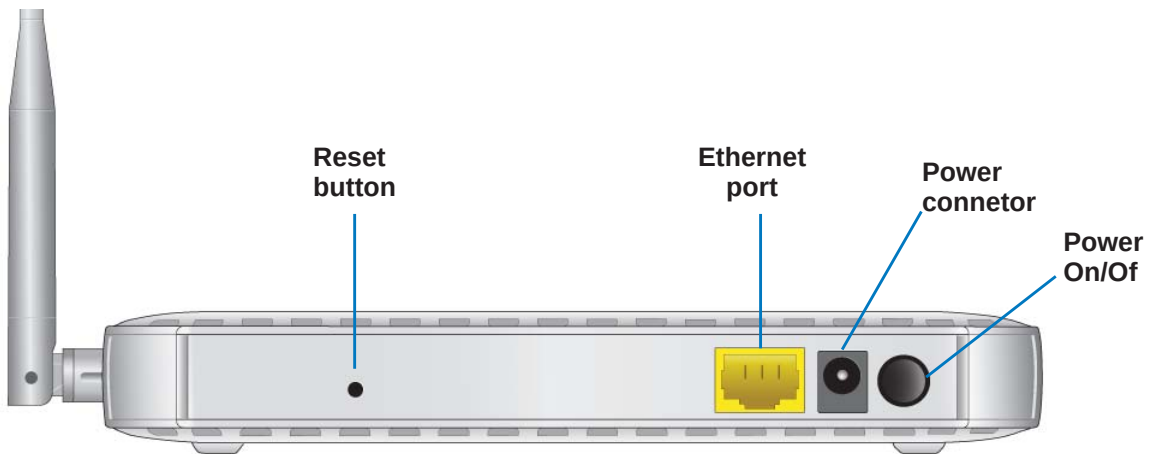
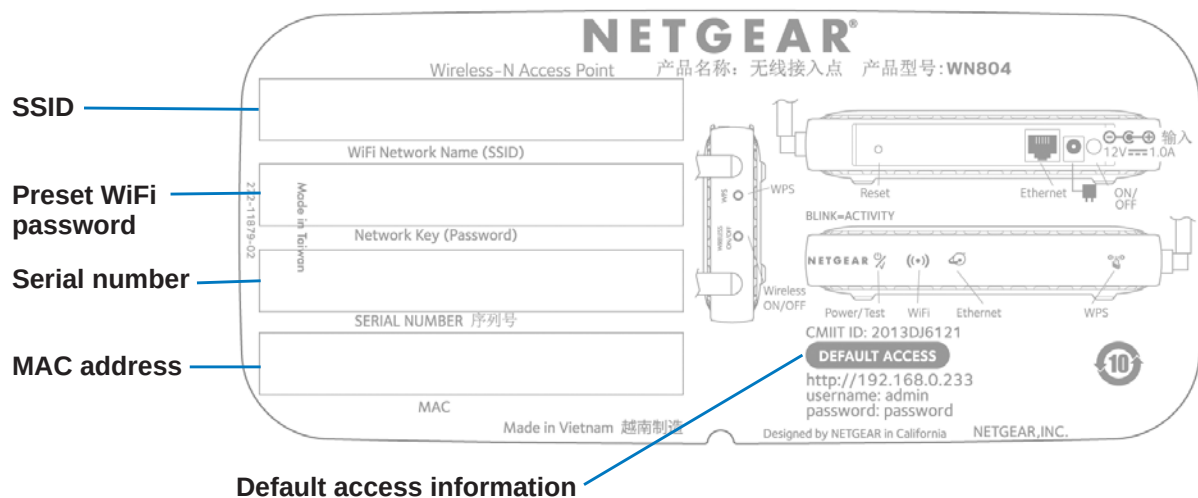


Figure 3. Access point rear panel

Pressing the Reset button restores the factory settings. See [Factory Default Settings](#) on page 42.

Product Label

The label on the bottom of the access point shows the login information, MAC address, and serial number.



Attach the Feet

Attach the feet to the access point as shown so that you can place it in a vertical position.



Figure 4. Attach the feet to the access point

Log In to the Access Point

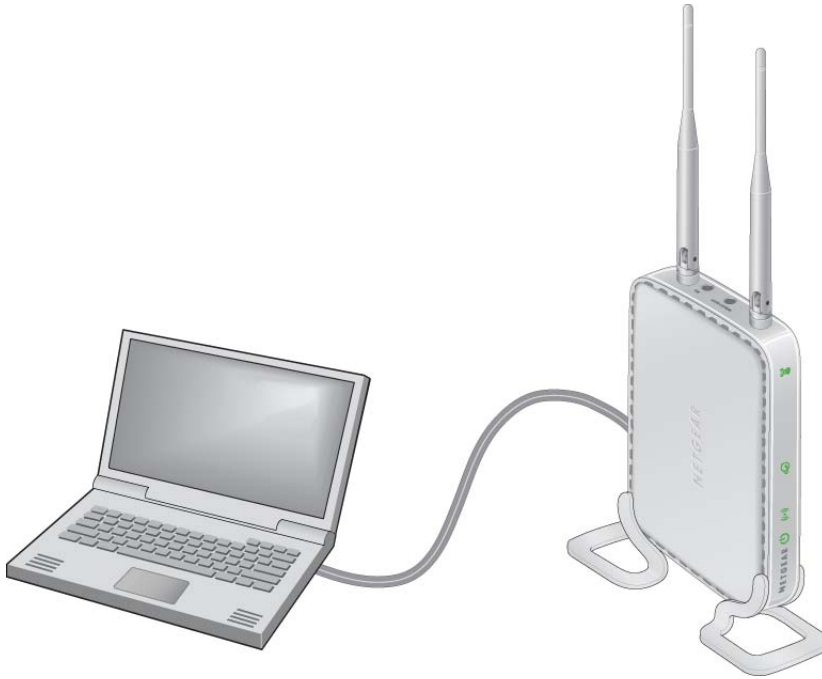
To log in, you need to use a computer with a fixed IP address.

➤ **To log in to the 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 192.168.0.210 and 255.255.255.0 as the subnet mask.

2. Use an Ethernet cable to connect the computer to the access point.



3. Launch a browser and enter **http://192.168.0.233** in the address field.
4. When prompted to log in, enter **admin** for the user name and **password** for the password, both in lowercase letters.

The web management interface of the access point displays.

Note: When you have finished changing the access point settings, you can reconfigure this computer back to its original TCP/IP settings.

Position the Access Point

The access point lets you access your network from anywhere within the operating range of your wireless network. However, the operating distance or range of your wireless connection can vary significantly depending on the physical placement of your access point. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your access point:

- Near the center of the area where your computers and other devices operate, and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the access point and your other devices to a minimum.

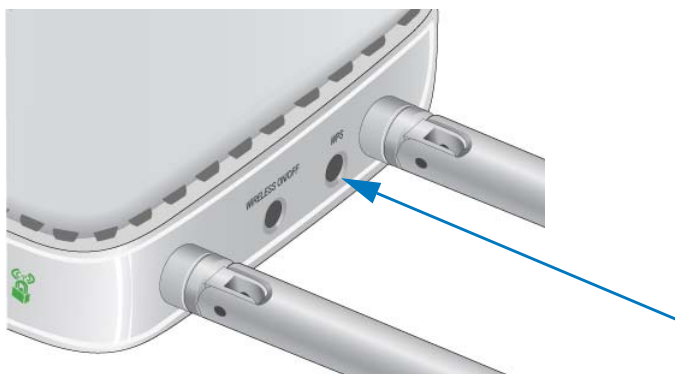
- Away from electrical devices that are potential sources of interference. Equipment that might cause interference includes ceiling fans, home security systems, microwaves, computers, the base of a cordless phone, or a 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

Connect to the WiFi Network with WPS

The WN804 Access Point supports WPS (Wi-Fi Protected Setup). You can use the WPS button to add WPS-capable wireless clients to the access point wireless network.

➤ **To use the WPS button on the access point to join the wireless network:**

1. Press the **WPS** button on the side of the access point.



2. Within 2 minutes, press the **WPS** button on your wireless device, or follow the WPS instructions that came with the device.

The WPS process automatically sets up your wireless computer or device with the network password and connects you to the wireless network.

2. Basic Configuration

2

This chapter covers the following topics:

- *Home Screen*
- *Specify IP Settings*
- *Specify Wireless Settings*
- *WPS Wizard for WiFi Connections*
- *Set Up a Guest Network*
- *View Attached Devices*

Home Screen

The Home screen shows information about the access point and its network settings.

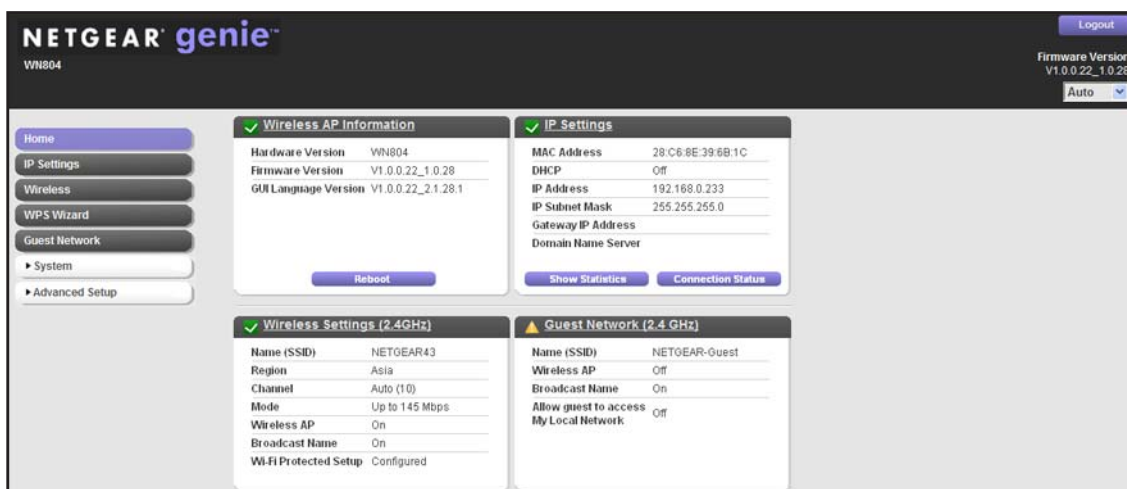


Figure 5. Home screen

The following menu selections are available:

- **Home.** This screen displays when you log in to the access point.
- **IP Settings.** Specify IP settings. See [Specify IP Settings](#) on page 14.
- **Wireless.** Specify wireless settings. See [Specify Wireless Settings](#) on page 14.
- **WPS Wizard.** See [WPS Wizard for WiFi Connections](#) on page 18.
- **Guest Network.** Set up a guest network to allow visitors to use your access point's Internet connection.
- **System.** Display a menu from which you can access administrative tasks such as backing up the configuration, and viewing a log. See [Chapter 3, System Settings](#).
- **Advanced Setup.** Display a menu from which you can access the Advanced Wireless Settings screen and the Wireless Repeating screen. See [Chapter 4, Advanced Configuration](#).

The panes on the Home screen provide the following information:

- **Wireless AP Information.** View the hardware version, GUI version, and the GUI language version.
- **IP Settings.** View the following:
 - MAC Address.
 - DHCP.
 - IP Address.
 - IP Subnet Mask.
 - Gateway IP Address.
 - Domain Name Server.

- Wireless Settings (2.4 GHz). These are the same settings that are specified in the Wireless Settings screen. See [Specify Wireless Settings](#) on page 14.
- Guest Network. These are the same settings that are specified in the Guest Network screen. See [Set Up a Guest Network](#) on page 19.

Specify IP Settings

You can assign an IP address to the access point.

➤ To specify the IP settings:

1. Select **IP Settings**:

2. If you want to use a dynamic IP address, select the **Get IP Address Dynamically** check box.

The IP Address field and the IP Subnet mask field are populated.

3. For a static IP address, fill in the IP Address and IP Subnet Mask fields.
4. (Optional) Select the **Get DNS Server Address Dynamically** check box.
5. Click **Apply**.

Specify Wireless Settings

The Wireless Settings screen lets you view or configure the wireless network setup.

The access point comes with preset security. This means that the Wi-Fi network name (SSID), network key (password), and security option (encryption protocol) are preset in the factory. You can find the preset SSID and password on the bottom of the unit.

Note: The preset SSID and password are uniquely generated for every device to protect and maximize your wireless security.

NETGEAR recommends that you do not change your preset security settings. If you change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

If you use a wireless computer to change the wireless network name (SSID) or other wireless security settings, you are disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the access point.

➤ **To view or change basic wireless settings:**

1. Select Wireless.

The screen sections, settings, and procedures are explained in the following sections.

2. Make any changes that are needed.

3. Click **Apply.**

Your settings are saved.

If you were connected wirelessly to the access point and you changed the SSID or wireless security, you are disconnected from the network.

4. If you changed the settings, make sure that you can connect wirelessly to the network with its new settings.

If you cannot connect wirelessly, check the following:

- Is your computer or wireless device connected to another wireless network in your area? Some wireless devices automatically connect to the first open network (without wireless security) that they discover.
- Is your computer or wireless device trying to connect to your network with its old settings (before you made changes)? If so, update the wireless network selection in your computer or wireless device to match the current settings for your network.

Wireless Settings Screen Fields

You can use this screen to view or change the wireless network settings and the security option.

Region. The location where the access point is used. Select from the countries in the list. In the United States, the region is fixed to United States and is not changeable.

Enable WMM. WMM means Wi-Fi Multimedia Quality of Service (WMM QoS). WMM QoS can prioritize wireless voice and video traffic over the wireless link. WMM QoS prioritizes wireless data packets from different applications based on four access categories: voice, video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application must have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is enabled by default. You can disable it by clearing the Enable WMM check box and clicking Apply.

Enable SSID Broadcast. This feature allows the access point to broadcast its SSID so wireless stations can see this wireless name (SSID) in their scanned network lists. This check box is selected by default. To turn off the SSID broadcast, clear this check box, and click Apply.

Name (SSID). The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive.

Channel. The wireless channel the access point uses. Select a value from 1 through 13. (For products in the North America market, only Channels 1 through 11 can be operated.) Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.

When you use multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is four channels (for example, use Channels 1 and 5, or 6 and 10).

Mode. Up to 145 Mbps is the default setting, which allows 802.11n and 802.11g wireless devices to join the network. The other settings are Up to 54 Mbps, and Up to 300 Mbps.

Security Options. The access point comes with unique preset wireless security. These settings are on the product label. NETGEAR recommends that you use preset security so that you can refer to the label if you forget the WiFi password. However, you can change the security option and passphrase.

Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. Wi-Fi Protected Access (WPA) has several options including pre-shared key (PSK) encryption.

WPA encryption is built into all hardware that has the Wi-Fi-certified seal. This seal means that the product is authorized by the Wi-Fi Alliance (<http://www.wi-fi.org/>) because it complies with the worldwide single standard for high-speed wireless local area networking.

WPA uses a passphrase for authentication and to generate the initial data encryption keys. Then it dynamically varies the encryption key. WPA-PSK uses Temporal Key Integrity Protocol (TKIP) data encryption, implements most of the IEEE 802.11i standard, and works with all wireless network interface cards, but not all wireless access points.

WPA2-PSK is stronger than WPA-PSK. It is advertised to be theoretically indecipherable due to the greater degree of randomness in encryption keys that it generates. WPA2-PSK gets higher speed because it is implemented through hardware, while WPA-PSK is usually implemented through software. WPA2-PSK uses a passphrase to authenticate and generate the initial data encryption keys. Then it dynamically varies the encryption key.

WPA-PSK + WPA2-PSK Mixed Mode can provide broader support for all wireless clients. WPA2-PSK clients get higher speed and security, and WPA-PSK clients get decent speed and security. For help with WPA settings on your wireless computer or device, see the instructions that came with your product.

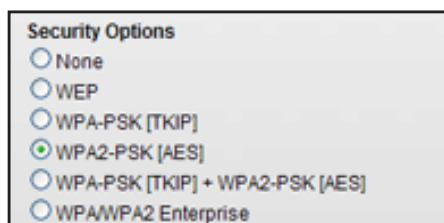
WEP is a legacy security option that can be used only with a wireless mode setting of Up to 54 Mbps.

Change the Wireless Security Option

NETGEAR recommends that you do not disable security.

➤ To change the WPA settings:

1. Select **Wireless Settings**.
2. Under Security Options, select the WPA option you want.



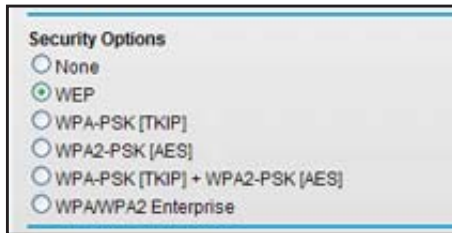
3. In the Passphrase field that displays when you select a WPA security option, enter the network key (password) that you want to use. It is a text string from 8 to 63 characters.
4. Write down the new password and keep it in a secure place for future reference.
5. Click **Apply**.

Your changes are saved.

➤ To set up WEP security:

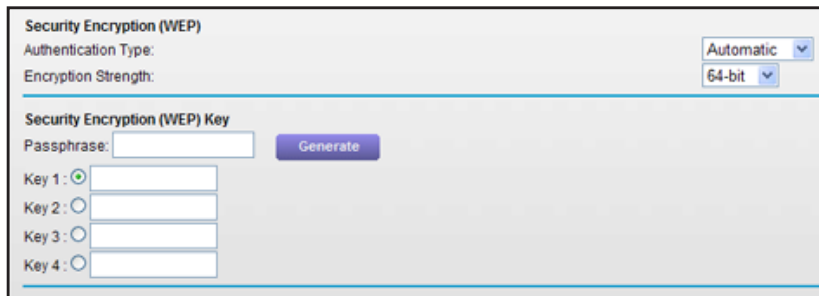
1. Select **Wireless Settings**.

- Under Security Options, select **WEP**.



The screenshot shows a 'Security Options' window with several radio button options. The 'WEP' option is selected, indicated by a green dot next to it. The other options are 'None', 'WPA-PSK [TKIP]', 'WPA2-PSK [AES]', 'WPA-PSK [TKIP] + WPA2-PSK [AES]', and 'WPA/WPA2 Enterprise'.

The screen adjusts.



The screenshot shows the 'Security Encryption (WEP)' configuration screen. It includes a dropdown for 'Authentication Type' set to 'Automatic' and another dropdown for 'Encryption Strength' set to '64-bit'. Below these, there is a 'Security Encryption (WEP) Key' section with a 'Passphrase' field and a 'Generate' button. Underneath, there are four key fields labeled 'Key 1', 'Key 2', 'Key 3', and 'Key 4', each with a radio button. 'Key 1' is selected.

- Select the authentication type from the drop-down list.

The default is Automatic.

- Select the encryption strength from the drop-down list, either 64-bit or 128 bit.

You can manually or automatically program the four data encryption keys. These values must be identical on all computers and wireless access points in your network. Select one of the following:

- **Automatic.** Enter a word or group of printable characters in the Passphrase field and click the **Generate** button. The four key fields are automatically populated with key values.
- **Manual.** Enter the number of hexadecimal digits appropriate to the encryption strength: 10 digits for 64-bit and 26 digits for 128-bit (any combination of 0–9, a–, or A–F).

- Select the radio button for the key to be used as the default key.

Data transmissions are always encrypted using the default key.

- Click **Apply**.

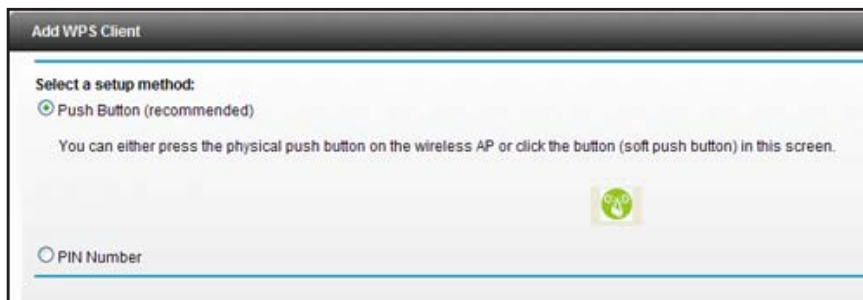
WPS Wizard for WiFi Connections

Wi-Fi Protected Setup (WPS) lets you connect to a secure WiFi network without typing its password. Instead, press a button or enter a PIN. NETGEAR calls WPS Push 'N' Connect.

The WPS Wizard helps you add a wireless computer or device to your WiFi network. On the computer or wireless device, either press its WPS button or locate its WPS PIN.

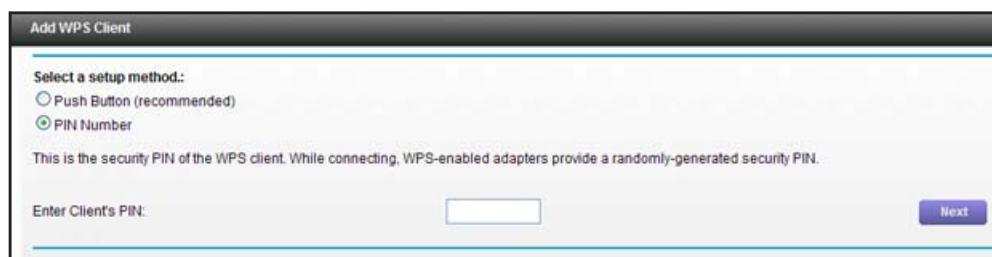
1. Select **WPS Wizard**.
2. Click **Next**.

The following screen lets you select the method for adding the WPS client (a wireless device or computer).



You can use either the push button or PIN method.

3. Select either **Push Button** or **PIN Number**.
 - To use the push button method, either click the **WPS** button on this screen, or press the **WPS** button on the side of the access point. Within 2 minutes, go to the wireless client and press its **WPS** button to join the network without entering a password.
 - To use the PIN method, select the **PIN Number** radio button, enter the client security PIN, and click **Next**.



Within 2 minutes, go to the client device and use its WPS software to join the network without entering a password.

The access point attempts to add the WPS-capable device. The WPS LED  on the front of the access point blinks green. When the access point establishes a WPS connection, the LED is solid green, and the access point WPS screen displays a confirmation message.

Set Up a Guest Network

A guest network allows you to let visitors use the Internet without using your wireless security key.

➤ To set up a guest network:

1. Select **Guest Network**.

2. Select any of the following wireless settings:

- **Enable Guest Network.** When this check box is selected, the guest network is enabled, and guests can connect to your network using the SSID of this profile.
- **Enable SSID Broadcast.** If this check box is selected, the wireless access point broadcasts its name (SSID) to all wireless stations. Stations with no SSID can adopt the correct SSID for connections to this access point.
- **Allow guest to access My Local Network.** If this check box is selected, anyone who connects to this SSID has access to your local network, not just Internet access.

3. Give the guest network a name.

The guest network name is case-sensitive and can be up to 32 characters. You then manually configure the wireless devices in your network to use the guest network name in addition to the main SSID.

4. Select a security option from the list.

The security options are described in [Wireless Security Options](#) on page 16.

5. Click **Apply**.

Your settings are saved.

View Attached Devices

You can view all computers or devices that are currently connected to your network.

➤ **To go to the Attached Devices screen:**

1. Select **Attached Devices**.



Wired devices are connected to the access point with Ethernet cables. Wireless devices have joined the wireless network. The following information is displayed:

- **#** (number). The order in which the device joined the network.
 - **IP Address**. The IP address that the access point assigned to this device when it joined the network. This number can change if a device is disconnected and rejoins the network.
 - **Device Name**. If the device name is known, it is shown here.
 - **MAC Address**. The unique MAC address for each device does not change. The MAC address is typically shown on the product label.
2. Click **Refresh** to update this screen.

3. System Settings

3

This chapter covers the following topics:

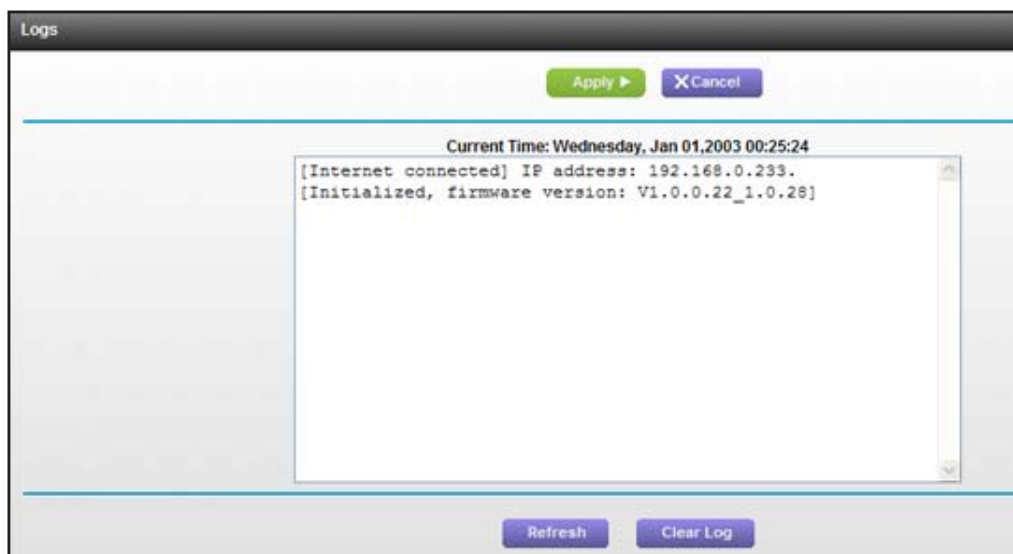
- *View Logs of Web Access or Attempted Web Access*
- *Manage the Configuration File*
- *Change the Password*
- *Password Recovery*
- *Wireless AP Update*
- *Reboot the Access Point*

View Logs of Web Access or Attempted Web Access

The log is a detailed record of the websites you have accessed or attempted to access. Up to 256 entries are stored in the log.

➤ **To view logs:**

Select **System > Logs**.



The Logs screen shows the following information:

- **Date and time.** The date and time the log entry was recorded.
- **Source IP.** The IP address of the initiating device for this log entry.
- **Target address.** The name or IP address of the website or news group visited or to which access was attempted.
- **Action.** The action that occurred.

To refresh the log screen, click the **Refresh** button.

To clear the log entries, click the **Clear Log** button.

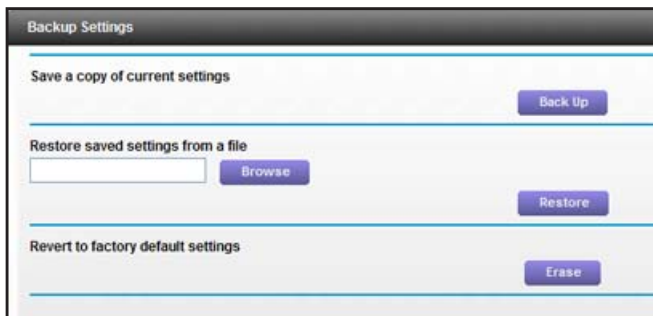
Manage the Configuration File

The configuration settings of the access point are stored within the access point in a configuration file. You can back up (save) this file to your computer, restore it, or reset it to the factory default settings.

Back Up Settings

➤ To back up the access point's configuration settings:

1. Select **System > Backup Settings**.



2. Click **Backup Settings**.
3. Specify a location to store the .cfg file.
A copy of the current settings is saved.

Restore Configuration Settings

➤ To restore configuration settings that you backed up:

1. Select **System > Backup Settings**.
2. Click the **Browse** button to find the .cfg file.
3. Click the **Restore** button.

The file is uploaded to the access point and the access point reboots.



WARNING:

Do not interrupt the reboot process.

Erase the Current Configuration Settings

You can use the Erase button to erase the configuration and restore the factory default settings. You might want to do this if you move the access point to a different network or if you changed the password and have forgotten what it is. (The default password is on the product label.)

You can also use the Reset button on the back of the access point to erase the configuration and restore the factory settings. (See [Factory Default Settings](#) on page 42.)

➤ **To erase the configuration settings:**

1. Select **System > Backup Settings**.
2. Click the **Erase** button.

The factory default settings are restored. The user name is admin, the password is password, and the LAN IP address is 192.168.1.1. DHCP is enabled.

Change the Password

This feature let you change the default password that is used to log in to the access point with the user name admin.

This is not the same as changing the password for wireless access. The label on the bottom of your access point shows your unique wireless network name (SSID) and password for wireless access (see [Label](#) on page 11).

➤ **To set the password for the user name admin:**

1. Select **System > Set Password**.

2. Type the old password, and type the new password twice.
3. If you want to be able to recover the password, select the **Enable Password Recovery** check box.
4. Click **Apply**.

Your changes take effect.

Password Recovery

NETGEAR recommends that you enable password recovery if you change the password for the access point user name admin. Then you can recover the password if it is forgotten. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➤ **To set up password recovery:**

1. Select **System > Set Password**.
2. Select the **Enable Password Recovery** check box.

3. Select two security questions, and provide answers to them.
4. Click **Apply**.

Your settings are saved.

➤ **To recover your password:**

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 192.168.0.210 and 255.255.255.0 as the subnet mask.
2. Use an Ethernet cable to connect the computer to the access point.
3. In the address field of your browser, type **http://192.168.0.233**.
A login window displays.
4. Click **Cancel**.
If password recovery is enabled, you are prompted to answer two security questions.
5. Enter the saved answers to the security questions.

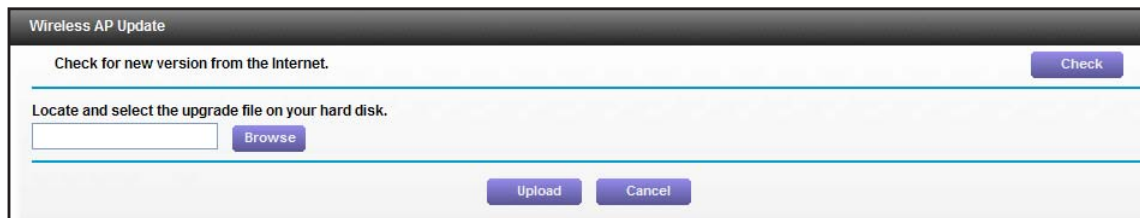
Wireless AP Update

The access point firmware (routing software) is stored in flash memory. You might see a message at the top of the genie screens when new firmware is available for your product.

You can use the Check button on the Wireless AP Update screen to check if new firmware is available, and to update your product.

➤ **To check for new firmware and update your access point:**

1. Select **Wireless AP Update**.



2. Click **Check**.

The access point finds new firmware information if any is available.

3. Click **Yes**.

The access point locates the firmware (the file ends in .img) and begins the update.



WARNING:

To avoid the risk of corrupting the firmware, do not interrupt the upgrade. For example, do not close the browser, click a link, or load a new page. Do not turn off the access point.

When the upload is complete, your access point restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to find out if you need to reconfigure the access point after upgrading.

Reboot the Access Point

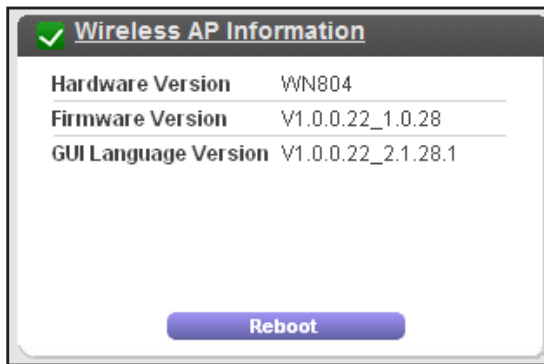
You can reboot the access point from the Home screen.

➤ **To reboot the access point:**

1. Log in to the access point.

The Home screen displays.

2. In the Wireless AP pane, click the **Reboot** button:



The access point reboots.

4. Advanced Configuration

4

This chapter covers the following topics:

- *Advanced Wireless Settings*
- *Wireless Distribution System (WDS)*

Advanced Wireless Settings

You can use this screen to turn the wireless radio on and off, to specify WPS settings, to use AP mode, and to set up a wireless access list.

The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options in this screen are reserved for wireless testing and advanced configuration only. Do not change these settings unless you have a specific reason to do so.

Control the Wireless Radio

By default, the wireless radio is enabled so that you can connect wirelessly to the access point. You can turn the wireless radio on or off in the Advanced Wireless Settings screen or by using the WiFi On/Off button on the access point front panel. When the wireless radio is off, you can still use an Ethernet cable for a LAN connection to the access point.

➤ **To turn the wireless radio on or off:**

1. Select **Advanced Setup > Wireless Settings**.

By default, the Enable Wireless AP Radio check box is selected.

2. Select or clear the **Enable Wireless AP Radio** check box.

If you clear this check box, this turns off the WiFi feature of the wireless access point.

3. (Optional) Select the **Turn off wireless signal by schedule** check box and fill in the fields to specify the times when you do not need a wireless connection.

For example, you could turn off the wireless signal for the weekend if you leave town.

4. Click **Apply**.

Your changes take effect.

Set Up a Wireless Schedule

You can use this feature to turn off the wireless signal from your access point at times when you do not need a wireless connection. For example, you could turn it off for the weekend if you leave town.

Note: Before you can set up a wireless schedule, the access point must connect to the Internet so that it can automatically set the correct system time.

➤ **To configure and enable the wireless schedule:**

1. Select **Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings screen displays.

2. Click the **Add a new period** button.

3. Use the radio buttons and check boxes to set up a period during which you want to turn off the wireless signal.

4. Click the **Apply** button.

The Advanced Wireless Settings screen displays.

5. Select the **Turn off wireless signal by schedule** check box to activate the schedule.
6. Click the **Apply** button.

Enable or Disable 20/40 GHz Coexistence

You can adjust this setting to fit the environment in which your wireless network operates. By default, the Enable 20/40 Hz Coexistence check box in the Advanced Wireless Settings screen is selected to avoid interference with other wireless networks in the area. If another wireless network is detected in the area, the coexistence feature might reduce the maximum speed of your 2.4 GHz wireless network by half.

Disabling the coexistence feature allows your 2.4 GHz wireless mode to support the maximum speed.

➤ **To change the coexistence setting:**

1. Select **Advanced Setup > Wireless Settings**.

2. Select or clear the **20/40 Hz Coexistence** check box.
3. Click **Apply**.
4. Your settings take effect.

View or Change WPS Settings

➤ **To specify WPS settings:**

1. Select **Advanced Setup > Wireless Settings**.

The Wireless AP's PIN field displays the PIN that you use on a registrar (for example, from the Network Explorer on a Vista Windows computer) to configure the access point's wireless settings through WPS.

2. (Optional) Select or clear the **Disable Wireless AP's PIN** check box.

The PIN function might temporarily be disabled when the access point detects suspicious attempts to access the network access point through WPS. You can manually enable the PIN function by clearing the Disable Wireless AP's PIN check box.

3. (Optional) Select or clear the **Keep Existing Wireless Settings** check box.

By default, the Keep Existing Wireless Settings check box is selected. NETGEAR recommends that you leave this check box selected.

If you clear this check box, the next time a new wireless client uses WPS to connect to the access point, the access point wireless settings change to an automatically generated random SSID and security key.

4. Click **Apply**.

Your settings are saved.

Set Up a Wireless Access List by MAC Address

You can set up a list of computers and wireless devices that are allowed to join the wireless network. This list is based on the unique MAC address of each computer and device.

Each network device has a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the wireless card or network interface device. If you do not have access to the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses in the Attached Devices screen.

➤ **To restrict access based on MAC addresses:**

1. Select **Advanced Setup > Wireless Settings**.
2. Click the **Setup Access List** button.

The screenshot shows the 'Wireless Card Access List' configuration window. At the top, there are three buttons: '+ Add', 'X Cancel', and 'G Refresh'. Below these is a table titled 'Available Wireless Cards' with two columns: 'Device Name' and 'MAC Address'. The table is currently empty. Below the table is a section titled 'Wireless Card Entry' which contains two input fields: 'Device Name' and 'MAC Address'.

3. Click **Add**.

The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.

4. If the computer or device you want is in the Available Wireless Cards list, select that radio button; otherwise, type a name and the MAC address.

You can usually find the MAC address on the bottom of the wireless device.

Tip: You can copy and paste the MAC addresses from the Attached Devices screen into the MAC Address field of this screen. To do this, use each wireless computer to join the wireless network. The computer should then appear in the Attached Devices screen.

5. Click **Add**.

The screen changes back to the list screen.

6. Add each computer or device you want to allow to connect wirelessly.
7. Select the **Turn Access Control On** check box.
8. Click **Apply**.

➤ To edit a wireless device or delete it from the access list:

1. Select **Advanced Setup > Wireless Settings**.

The Advanced Wireless Settings screen displays.

2. In the table, select the radio button next to the wireless device that you want to edit or delete.

3. Do one of the following:

- Click the **Edit** button.

The Edit Wireless Card screen displays.

a. Edit the address information.

b. Click the **Accept** button.

- Click the **Delete** button.

The address is removed from the table.

Wireless Distribution System (WDS)

You can set the access point up to be used as a wireless base station or a wireless repeater in a wireless distribution system (WDS). A WDS lets you expand a wireless network through multiple access points. A wireless base station connects to the Internet, can have wired and wireless clients, and sends its wireless signal to an access point that functions as a wireless repeater. A wireless repeater can also have wired and wireless clients, but connects to the Internet through the wireless base station. The following figure shows a wireless repeating scenario.

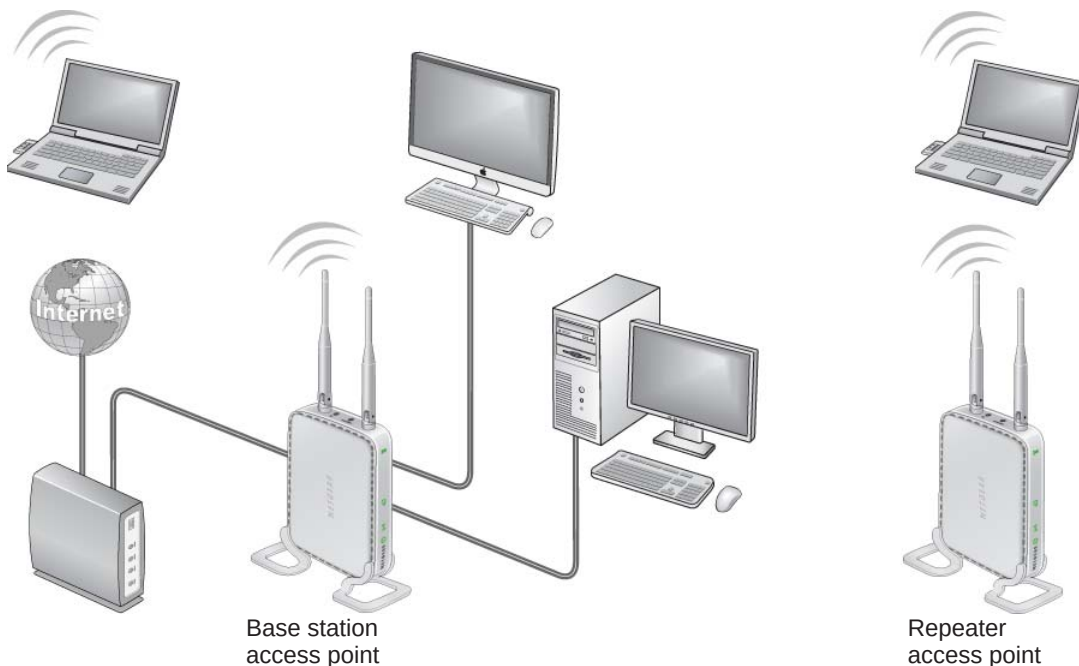


Figure 6. Wireless repeating scenario

Note: To use the wireless repeating function, you need to select None as the security option in the Wireless Settings screen, and you cannot select Auto Channel.

Wireless base station. The access point acts as the parent access point that bridges traffic to and from the child repeater access point. The base station also handles wireless and wired local computers. To configure this mode, you have to know the MAC addresses of the child repeater access point. Often, the MAC address is on the product label.

Wireless repeater. The access point sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you have to know the MAC address of the remote parent access point.

For you to set up a wireless network with WDS, both access points have to meet the following conditions:

- Both access points have to use the same SSID, wireless channel, and encryption mode.
- Both access points have to be on the same LAN IP subnet. That is, all of the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) are configured to operate in the same LAN network address range as the access points.

Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You have to know the wireless settings for both units. You have to know the MAC address of the remote unit. First, set up the base station. Then set up the repeater.

➤ **To set up the base station:**

1. Set up both units with the same wireless settings.

The SSID and mode need to be the same, and the wireless security option has to be set to None. (See [Basic Wireless Settings](#) on page 25.)

2. Select **Advanced Setup > Wireless Repeating**.
3. Select the **Enable Wireless Repeating Function** check box.

4. Select the **Wireless Base Station** radio button.

5. (Optional) Select the **Disable Wireless Client Association** check box to prevent wireless clients from associating with the base station and allowing LAN client associations only.
You can leave the check box cleared if you prefer wireless clients to be able to associate with the base stations.
6. In the Repeater MAC Address 1 through 4 fields, enter the MAC addresses for the access points that should function as repeaters.
If your access point is the base station, it can function as the “parent” for up to four other access points.
7. Click the **Apply** button.
Your changes are saved.

Set Up a Repeater

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

Note: If you are using the access point as the base station with a non-NETGEAR access point as the repeater, you might need to change more configuration settings. In particular, you should disable the DHCP server function on the access point that is the repeater.

➤ To configure the access point as a repeater:

1. For the access point that will be the repeater, verify that the wireless settings match the base unit exactly.

The wireless security option has to be set to **WEP** or **None**.

2. Select **Advanced Setup > Wireless Repeating Function**.
3. Select the **Enable Wireless Repeating Function** check box.
4. Select the **Wireless Repeater** radio button.

Wireless Repeating Function

Apply Cancel

☒ Enable Wireless Repeating Function (2.4GHz b/g/n)

Wireless MAC of this wireless AP 28:C6:8E:39:6B:1C

☒ Wireless Repeater

Repeater IP Address 192 168 0

☐ Disable Wireless Client Association

Base Station MAC Address

☐ Wireless Base Station

☐ Disable Wireless Client Association

Repeater MAC Address 1

Repeater MAC Address 2

Repeater MAC Address 3

Repeater MAC Address 4

5. Fill in the Repeater IP Address field.
This IP address has to be in the same subnet as the base station, but different from the LAN IP address of the base station.
6. (Optional) Select the **Disable Wireless Client Association** check box to prevent wireless clients from associating with the repeater and allowing LAN client associations only.
You can leave the check box cleared if you prefer wireless clients to be able to associate with the repeater.
7. In the Base Station MAC Address field, enter the MAC addresses for the access point that should function as the base station.
8. Click **Apply**.
Your settings are saved.
9. Verify connectivity across the LANs.
A computer on any wireless or wired LAN segment of the access point can connect to the Internet or share files and printers with any other computer or server connected to the other access point.

5. Troubleshooting

5

This chapter covers the following topics:

- *Troubleshoot with the LEDs*
- *Login Prompt Does Not Display*
- *No WiFi Access to the Internet or LAN*
- *Time-Out Error for a URL or IP Address*

Troubleshoot with the LEDs

This section provides some tips for correcting simple problems that you might encounter.

No LEDs Are Lit on the Access Point

The access point has no power. Check the following:

- The power adapter is connected to the access point and plugged in to a working power outlet or power strip.
- If a wall switch controls the power outlet, make sure that the switch is turned on.
- You are using the correct NETGEAR power adapter supplied with your access point.

The WiFi LED Is Off

The wireless connection does not work.

- If the WiFi LED stays off, disconnect the power adapter from its power source and plug it in again.
- Log in to the access point and verify that the wireless radio is turned on.
- Contact NETGEAR if the WiFi LED remains off.

Login Prompt Does Not Display

- Quit the browser, clear the cache, delete the cookies, and launch the browser again.
- Check these items:
- The access point is correctly installed, LAN connections are OK, and it is powered on.
- If DHCP is not enabled, make sure that you use the correct LAN IP address to access the wireless access point, and that you are on the same network segment.
- If DHCP is enabled, configure your DHCP server with a reserved IP address (based on the wireless access point's MAC address). You can then use it to create a fixed IP address for the wireless access point.
- If you have not yet deployed the wireless access point, and it is connected to your computer with an Ethernet cable, make sure that the connection is secure, and that you have configured your computer with a static IP address in the same subnet as the LAN IP of the wireless access point.

The default static IP address to use for your computer is 192.168.0.210; the default wireless access point LAN IP address is 192.168.0.233; and the default subnet mask is 255.255.255.0.

No WiFi Access to the Internet or LAN

There is a configuration problem.

- You might not have restarted the wireless device to let the TCP/IP changes take effect. Restart the computer.
- Make sure that the SSID and wireless security settings of the wireless device are the same as those of the access point.
- The wireless device might not have the correct TCP/IP settings to communicate with the network. Restart the wireless device and check that TCP/IP is set up correctly for that network. In Windows, the usual setting for Network Properties is to obtain an IP address automatically.
- The access point default values might not work with your network. Check the access point default configuration against the configuration of other devices in your network.

Time-Out Error for a URL or IP Address

If you get a time-out error when you enter a URL or IP address, a number of things could be causing this. Try the following troubleshooting steps.

- Check whether other computers work. If they do, ensure that your computer's IP address, subnet mask and default gateway settings are correct. If using a DNS server, check the primary and secondary DNS server addresses.
- If the computers are configured correctly, but still not working, ensure that the access point is connected and turned on. Connect to it and check its settings. If you cannot connect to it, check the LAN and power connections.
- If the access point is configured correctly, check your Internet connection (DSL/cable modem, and so on) to make sure that it is working.
- Try again.
- When entering configuration settings, be sure to click **Apply** before moving to another screen, or your changes are lost.
- Click **Refresh** or **Reload** in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

A Supplemental Information



This appendix covers the following topics:

- *Factory Default Settings*
- *Technical Specifications*

Factory Default Settings

You can return the access point to its factory settings. Use the end of a paper clip or a similar object to press and hold the **Reset** button on the back of the access point for at least 7 seconds. The access point resets and returns to the factory configuration settings shown in the following table.

Feature		Default behavior
Access point login	User login URL	http://192.168.0.233
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Ethernet connection	Ethernet MAC address	See the product label.
	Access point mode	On
	Port speed	10/100 Mbps
Local network (LAN)	LAN IP	192.168.0.233
	Subnet mask	255.255.255.0
	Gateway address	192.168.0.1
	DHCP client	Disabled
	Time zone	Pacific time
	Time zone automatically adjusts for daylight savings time	Disabled
Wireless	Wireless communication	Enabled
	SSID name	See the product label.
	Security	WPA2-PSK (AES)
	Broadcast SSID	Enabled
	Transmission speed	Auto ¹
	Country/region	Asia
	RF channel	Auto
	Operating mode	Up to 270 Mbps at 2.4GHz

1. Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput can vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.

Technical Specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE, PPTP, Bigpond, Dynamic DNS, UPnP, and SMB
Power adapter	- Input: 230V, 50 Hz, input - Output: 12V DC @ 2.5A
Dimensions	Without external antennas: 180.88x116.4x30mm (7.05x4.54x1.17 inches) External antenna length: 176mm (6.86 inches)
Weight	268g (0.69 lb)
Operating temperature	0° to 40° C (32° to 104° F)
Operating humidity	90% maximum relative humidity, noncondensing
Electromagnetic emissions	China SRRC
Ethernet	10BASE-T or 100BASE-Tx, RJ-45
Wireless	Maximum wireless signal rate complies with the IEEE 802.11 standard. See the footnote for the previous table.
Radio data rates	Auto Rate Sensing
Data encoding standards	IEEE 802.11n version 2.0 IEEE 802.11n, IEEE 802.11g, IEEE 802.11b 2.4 GHz
Maximum computers per wireless network	Limited by the amount of wireless network traffic generated by each node (typically 50–70 nodes).
Operating frequency range	2.4 GHz 2.400-2.4835GHz (China)
802.11 security	WPA-Enterprise WPA2-Enterprise

B. Notification of Compliance

B

NETGEAR wireless routers, gateways, APs

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.

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 – EU Declaration of Conformity

Products bearing the **CE** marking comply with the following EU directives:

- EMC Directive 2004/108/EC
- Low Voltage Directive 2006/95/EC

If this product has telecommunications functionality, it also complies with the requirements of the following EU Directive:

- R&TTE Directive 1999/5/EC

Compliance with these directives implies conformity to harmonized European standards that are noted in the EU Declaration of Conformity.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

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 20 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 WN804 Access Point complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- 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 uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- 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 radio 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.
- 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.
- For product available in the USA and Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.
- Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.
- Cet appareil et son antenne (s) ne doit pas être co-localisés ou fonctionnement en association avec une autre antenne ou transmetteur.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (WN804 Access Point) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

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.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

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 20cm between the radiator & your body.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Interference Reduction Table

The table below shows the recommended minimum distance between NETGEAR equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters